TIFR, Mumbai October 5–9, 2009

International conference on “Analytic Number Theory”

www.math.tifr.res.in/∼ant2009

Criteria for irrationality, linear independence, transcendence and algebraic independence

Michel Waldschmidt

Institut de Mathématiques de Jussieu & Paris VI

http://www.math.jussieu.fr/∼miw/

Lecture given on October 8, 2009.

Abstract

Most irrationality proofs rest on the following criterion :

A real number x is irrational if and only if, for any $\epsilon > 0$, there exist two rational integers p and q with $q > 0$, such that

$$0 < |qx - p| < \epsilon.$$

We survey generalisations of this criterion to linear independence, transcendence and algebraic independence.

Table of contents

1. Irrationality results : Euler, Fourier, Beukers, Apéry...
2. Irrationality criteria : Dirichlet, Minkowski, Hurwitz
3. Linear independence : Hermite, Siegel, Nesterenko
4. Transcendence : Liouville, Gel'fond, Durand, Laurent, Roy...
5. Algebraic independence : Lang, Philippon, Chudnovsky, Nesterenko, Schanuel, Roy...

Leonhard Euler (1707 – 1783)

1748 : Irrationality of the number
$e = 2.718\,281\,828\,459\,0\ldots$

The number

$$e = \sum_{n\geq 0} \frac{1}{n!}$$

is irrational

Continued fractions expansions.

http://www-history.mcs.st-andrews.ac.uk/

Joseph Fourier (1768 - 1830)

Proof of Euler's 1748 result on the irrationality of the number e by truncating the series

$$e = \sum_{n \geq 0} \frac{1}{n!}.$$

Course of analysis at the École Polytechnique Paris, 1815.

Frits Beukers (2008) : irrationality of e^{-1}

$$N!e^{-1} = \sum_{n=0}^{N} \frac{(-1)^n N!}{n!} + \sum_{m\geq N+1} \frac{(-1)^m N!}{m!}.$$

Take for N a large odd integer and set

$$A_N = \sum_{n=0}^{N} \frac{(-1)^n N!}{n!}.$$

Then $A_N \in \mathbf{Z}$ and

$$A_N < N!e^{-1} < A_N + \frac{1}{N+1}.$$

Hence e^{-1} is irrational.

Irrationality proof

Let $\vartheta \in \mathbf{Q}$, say $\vartheta = a/b$. Then for any $p/q \in \mathbf{Q}$ with $p/q \neq \vartheta$ we have

$$|q\vartheta - p| \geq \frac{1}{b}.$$

Proof : $|qa - pb| \geq 1$.

Consequence. *Let* $\vartheta \in \mathbb{R}$. *Assume that for any* $\epsilon > 0$, *there exists* $p/q \in \mathbf{Q}$ *with*

$$0 < |q\vartheta - p| < \epsilon.$$

Then ϑ *is irrational.*

Irrationality proof

Let $\vartheta \in \mathbf{Q}$, say $\vartheta = a/b$. Then for any $p/q \in \mathbf{Q}$ with $p/q \neq \vartheta$ we have

$$|q\vartheta - p| \geq \frac{1}{b}.$$

Proof : $|qa - pb| \geq 1$.

Consequence. *Let $\vartheta \in \mathbf{R}$. Assume that for any $\epsilon > 0$, there exists $p/q \in \mathbf{Q}$ with*

$$0 < |q\vartheta - p| < \epsilon.$$

Then ϑ is irrational.

Irrationality proof

Let $\vartheta \in \mathbf{Q}$, say $\vartheta = a/b$. Then for any $p/q \in \mathbf{Q}$ with $p/q \neq \vartheta$ we have

$$|q\vartheta - p| \geq \frac{1}{b}.$$

`Proof` : $|qa - pb| \geq 1$.

Consequence. *Let $\vartheta \in \mathbf{R}$. Assume that for any $\epsilon > 0$, there exists $p/q \in \mathbf{Q}$ with*

$$0 < |q\vartheta - p| < \epsilon.$$

Then ϑ is irrational.

Irrationality of $\zeta(3)$, following Apéry (1978)

There exist two sequences of rational numbers $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$, such that $a_n \in \mathbf{Z}$ and $d_n^3 b_n \in \mathbf{Z}$ for all $n \geq 0$, with

$$\lim_{n\to\infty} |2a_n\zeta(3) - b_n|^{1/n} = (\sqrt{2}-1)^4,$$

where d_n is the lcm of $1, 2, \ldots, n$.

We have $d_n = e^{n+o(n)}$ and $e^3(\sqrt{2}-1)^4 < 1$.

Set $q_n = d_n^3 b_n$, $p_n = 2d_n^3 a_n$, so that

$$0 < |q_n\zeta(3) - p_n| < \epsilon_n \quad \text{with} \quad \epsilon_n \to 0.$$

Irrationality of $\zeta(3)$, following Apéry (1978)

There exist two sequences of rational numbers $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$, such that $a_n \in \mathbf{Z}$ and $d_n^3 b_n \in \mathbf{Z}$ for all $n \geq 0$, with

$$\lim_{n\to\infty} |2a_n\zeta(3) - b_n|^{1/n} = (\sqrt{2}-1)^4,$$

where d_n is the lcm of $1, 2, \ldots, n$.

We have $d_n = e^{n+o(n)}$ and $e^3(\sqrt{2}-1)^4 < 1$.

Set $q_n = d_n^3 b_n$, $p_n = 2d_n^3 a_n$, so that

$$0 < |q_n\zeta(3) - p_n| < \epsilon_n \quad \text{with} \quad \epsilon_n \to 0.$$

Irrationality of $\zeta(3)$, following Apéry (1978)

There exist two sequences of rational numbers $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$, such that $a_n \in \mathbf{Z}$ and $d_n^3 b_n \in \mathbf{Z}$ for all $n \geq 0$, with

$$\lim_{n\to\infty} |2a_n\zeta(3) - b_n|^{1/n} = (\sqrt{2}-1)^4,$$

where d_n is the lcm of $1, 2, \ldots, n$.

We have $d_n = e^{n+o(n)}$ and $e^3(\sqrt{2}-1)^4 < 1$.

Set $q_n = d_n^3 b_n$, $p_n = 2d_n^3 a_n$, so that

$$0 < |q_n\zeta(3) - p_n| < \epsilon_n \quad \text{with} \quad \epsilon_n \to 0.$$

Infinitely many odd zeta are irrational

Tanguy Rivoal (2000)

Let $\epsilon > 0$*. For any sufficiently large odd integer* a*, the dimension of the* $\mathbf{Q}$*–vector space spanned by the numbers* $1,\ \zeta(3),\ \zeta(5),\ \cdots,\zeta(a)$ *is at least*

$$\frac{1-\epsilon}{1+\log 2}\log a.$$

References

Stéphane Fischler
Irrationalité de valeurs de zêta, (d'après Apéry, Rivoal, ...),
Sém. Nicolas Bourbaki, 2002-2003,
N° 910 (Novembre 2002).

http://www.math.u-psud.fr/~fischler/publi.html

Christian Krattenthaler and Tanguy Rivoal

http://www-fourier.ujf-grenoble.fr/~rivoal/articles.html

C. Krattenthaler et T. Rivoal, *Hypergéométrie et fonction zêta de Riemann,* Mem. Amer. Math. Soc. **186** (2007), 93 p.

Criterion : necessary and sufficient condition

We saw that any $\vartheta \in \mathbf{R}$ for which there exists a sequence $(p_n/q_n)_{n\geq 0}$ of rational numbers with

$$0 < |q_n\vartheta - p_n| < \epsilon_n \quad \text{with} \quad \epsilon_n \to 0$$

is irrational.

Conversely, given $\vartheta \in \mathbf{R} \setminus \mathbf{Q}$, there exists a sequence $(p_n/q_n)_{n\geq 0}$ with

$$0 < |q_n\vartheta - p_n| < \epsilon_n \quad \text{and} \quad \epsilon_n \to 0.$$

More precisely, given $\vartheta \in \mathbf{R}$, for each real number $Q > 1$, there exists $p/q \in \mathbf{Q}$ with

$$|q\vartheta - p| \leq \frac{1}{Q} \quad \text{and} \quad 0 < q < Q.$$

Hence, for $\vartheta \notin \mathbf{Q}$, there exists a sequence $(p_n/q_n)_{n\geq 0}$ with

$$0 < |q_n\vartheta - p_n| < \frac{1}{q_n} \quad \text{and} \quad q_n \to \infty.$$

Criterion : necessary and sufficient condition

We saw that any $\vartheta \in \mathbf{R}$ for which there exists a sequence $(p_n/q_n)_{n\geq 0}$ of rational numbers with

$$0 < |q_n\vartheta - p_n| < \epsilon_n \quad \text{with} \quad \epsilon_n \to 0$$

is irrational.
Conversely, given $\vartheta \in \mathbf{R} \setminus \mathbf{Q}$, there exists a sequence $(p_n/q_n)_{n\geq 0}$ with

$$0 < |q_n\vartheta - p_n| < \epsilon_n \quad \text{and} \quad \epsilon_n \to 0.$$

More precisely, given $\vartheta \in \mathbf{R}$, for each real number $Q > 1$, there exists $p/q \in \mathbf{Q}$ with

$$|q\vartheta - p| \leq \frac{1}{Q} \quad \text{and} \quad 0 < q < Q.$$

Hence, for $\vartheta \notin \mathbf{Q}$, there exists a sequence $(p_n/q_n)_{n\geq 0}$ with

$$0 < |q_n\vartheta - p_n| < \frac{1}{q_n} \quad \text{and} \quad q_n \to \infty.$$

Criterion : necessary and sufficient condition

We saw that any $\vartheta \in \mathbf{R}$ for which there exists a sequence $(p_n/q_n)_{n\geq 0}$ of rational numbers with

$$0 < |q_n\vartheta - p_n| < \epsilon_n \quad \text{with} \quad \epsilon_n \to 0$$

is irrational.

Conversely, given $\vartheta \in \mathbf{R} \setminus \mathbf{Q}$, there exists a sequence $(p_n/q_n)_{n\geq 0}$ with

$$0 < |q_n\vartheta - p_n| < \epsilon_n \quad \text{and} \quad \epsilon_n \to 0.$$

More precisely, given $\vartheta \in \mathbf{R}$, for each real number $Q > 1$, there exists $p/q \in \mathbf{Q}$ with

$$|q\vartheta - p| \leq \frac{1}{Q} \quad \text{and} \quad 0 < q < Q.$$

Hence, for $\vartheta \notin \mathbf{Q}$, there exists a sequence $(p_n/q_n)_{n\geq 0}$ with

$$0 < |q_n\vartheta - p_n| < \frac{1}{q_n} \quad \text{and} \quad q_n \to \infty.$$

Criterion : necessary and sufficient condition

We saw that any $\vartheta \in \mathbf{R}$ for which there exists a sequence $(p_n/q_n)_{n\geq 0}$ of rational numbers with

$$0 < |q_n\vartheta - p_n| < \epsilon_n \quad \text{with} \quad \epsilon_n \to 0$$

is irrational.

Conversely, given $\vartheta \in \mathbf{R} \setminus \mathbf{Q}$, there exists a sequence $(p_n/q_n)_{n\geq 0}$ with

$$0 < |q_n\vartheta - p_n| < \epsilon_n \quad \text{and} \quad \epsilon_n \to 0.$$

More precisely, given $\vartheta \in \mathbf{R}$, for each real number $Q > 1$, there exists $p/q \in \mathbf{Q}$ with

$$|q\vartheta - p| \leq \frac{1}{Q} \quad \text{and} \quad 0 < q < Q.$$

Hence, for $\vartheta \notin \mathbf{Q}$, there exists a sequence $(p_n/q_n)_{n\geq 0}$ with

$$0 < |q_n\vartheta - p_n| < \frac{1}{q_n} \quad \text{and} \quad q_n \to \infty.$$

Gustave Lejeune–Dirichlet (1805 - 1859)

G. Dirichlet

1842 : Box (pigeonhole) principle

A map $f : E \to F$ *with* $\mathrm{Card} E > \mathrm{Card} F$ *is not injective.*

A map $f : E \to F$ *with* $\mathrm{Card} E < \mathrm{Card} F$ *is not surjective.*

Pigeonhole Principle

More holes than pigeons

More pigeons than holes

Existence of rational approximations

For any $\vartheta \in \mathbf{R}$ *and any real number* $Q > 1$, *there exists* $p/q \in \mathbf{Q}$ *with*

$$|q\vartheta - p| \le \frac{1}{Q}$$

and $0 < q < Q$.

Proof. For simplicity assume $Q \in \mathbf{Z}$. Take

$$E = \{0, \{\vartheta\}, \{2\vartheta\}, \ldots, \{(Q-1)\vartheta\}, 1\} \subset [0,1],$$

where $\{x\}$ denotes the fractional part of x, F is the partition

$$\left[0, \frac{1}{Q}\right), \left[\frac{1}{Q}, \frac{2}{Q}\right), \ldots, \left[\frac{Q-2}{Q}, \frac{Q-1}{Q}\right), \left[\frac{Q-1}{Q}, 1\right],$$

of $[0,1]$, so that

$$\mathrm{Card} E = Q + 1 > Q = \mathrm{Card} F,$$

and $f : E \to F$ maps $x \in E$ to $I \in F$ with $I \ni x$.

Existence of rational approximations

For any $\vartheta \in \mathbf{R}$ *and any real number* $Q > 1$, *there exists* $p/q \in \mathbf{Q}$ *with*

$$|q\vartheta - p| \leq \frac{1}{Q}$$

and $0 < q < Q$.

Proof. For simplicity assume $Q \in \mathbf{Z}$. Take

$$E = \Bigl\{0,\ \{\vartheta\},\ \{2\vartheta\}, \ldots, \{(Q-1)\vartheta\},\ 1\Bigr\} \subset [0,1],$$

where $\{x\}$ denotes the fractional part of x, F is the partition

$$\left[0, \frac{1}{Q}\right), \left[\frac{1}{Q}, \frac{2}{Q}\right), \ldots, \left[\frac{Q-2}{Q}, \frac{Q-1}{Q}\right), \left[\frac{Q-1}{Q}, 1\right],$$

of $[0,1]$, so that

$$\mathrm{Card} E = Q + 1 > Q = \mathrm{Card} F,$$

and $f : E \to F$ maps $x \in E$ to $I \in F$ with $I \ni x$.

Hermann Minkowski (1864 - 1909)

H. Minkowski

1896 : Geometry of numbers.

The set

$$\mathcal{C} = \{(u,v) \in \mathbf{R}^2 \; ; |v| \le Q, \\ |v\vartheta - u| \le 1/Q\}$$

is convex, symmetric, compact, with volume 4.

Hence $\mathcal{C} \cap \mathbf{Z}^2 \ne \{(0,0)\}$.

Adolf Hurwitz (1859 - 1919)

A. Hurwitz

1891

For any $\vartheta \in \mathbf{R} \setminus \mathbf{Q}$*, there exists a sequence* $(p_n/q_n)_{n\geq 0}$ *of rational numbers with*

$$0 < |q_n\vartheta - p_n| < \frac{1}{\sqrt{5}q_n}$$

and $q_n \to \infty$*.*

Methods : Continued fractions, Farey sections.

Best possible for the Golden ratio

$$\frac{1+\sqrt{5}}{2} = 1.618\,033\,988\,749\,9\ldots$$

Irrationality criterion

Let ϑ be a real number. The following conditions are equivalent.

(i) ϑ *is irrational.*

(ii) *For any* $\epsilon > 0$, *there exists* $p/q \in \mathbf{Q}$ *such that*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{\epsilon}{q}.$$

(iii) *For any real number* $Q > 1$, *there exists an integer* q *in the interval* $1 \leq q < Q$ *and there exists an integer* p *such that*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{1}{qQ}.$$

(iv) *There exist infinitely many* $p/q \in \mathbf{Q}$ *satisfying*

$$\left|\vartheta - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

Irrationality criterion (continued)

Let ϑ be a real number. The following conditions are equivalent.

(i) ϑ *is irrational.*

(ii)' *For any* $\epsilon > 0$, *there exist two linearly independent linear forms*

$$L_0(X_0, X_1) = a_0 X_0 + b_0 X_1 \quad \textit{and} \quad L_1(X_0, X_1) = a_1 X_0 + b_1 X_1,$$

with rational integer coefficients, such that

$$\max\left\{ |L_0(1, \vartheta)|\ ,\ |L_1(1, \vartheta)| \right\} < \epsilon.$$

Proof of (ii) $\iff$ (ii)'

(ii) *For any* $\epsilon > 0$, *there exists* $p/q \in \mathbf{Q}$ *such that*

$$0 < \left| \vartheta - \frac{p}{q} \right| < \frac{\epsilon}{q}.$$

(ii)' *For any* $\epsilon > 0$, *there exist two linearly independent linear forms* L_0, L_1 *in* $\mathbf{Z}X_0 + \mathbf{Z}X_1$ *such that*

$$\max\left\{ |L_0(1,\vartheta)|\ ,\ |L_1(1,\vartheta)| \right\} < \epsilon.$$

Proof of (ii)' $\Longrightarrow$ (ii)

Since L_0, L_1 are linearly independent, one at least of them does not vanish at $(1,\vartheta)$. Write it $pX_0 - qX_1$.

Proof of (ii) $\Longrightarrow$ (ii')

Using (ii), set $L_0(X_0, X_1) = pX_0 - qX_1$, and use (ii) again with ϵ replaced by $|q\vartheta - p|$.

Proof of (ii) $\Longleftrightarrow$ (ii)'

(ii) *For any* $\epsilon > 0$*, there exists* $p/q \in \mathbf{Q}$ *such that*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{\epsilon}{q}.$$

(ii)' *For any* $\epsilon > 0$*, there exist two linearly independent linear forms* L_0*,* L_1 *in* $\mathbf{Z}X_0 + \mathbf{Z}X_1$ *such that*

$$\max\left\{|L_0(1,\vartheta)|\,,\ |L_1(1,\vartheta)|\right\} < \epsilon.$$

Proof of (ii)' $\Longrightarrow$ (ii)

Since L_0, L_1 are linearly independent, one at least of them does not vanish at $(1,\vartheta)$. Write it $pX_0 - qX_1$.

Proof of (ii) $\Longrightarrow$ (ii')

Using (ii), set $L_0(X_0,X_1) = pX_0 - qX_1$, and use (ii) again with ϵ replaced by $|q\vartheta - p|$.

Proof of (ii) $\iff$ (ii)'

(ii) *For any* $\epsilon > 0$, *there exists* $p/q \in \mathbf{Q}$ *such that*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{\epsilon}{q}\cdot$$

(ii)' *For any* $\epsilon > 0$, *there exist two linearly independent linear forms* L_0, L_1 *in* $\mathbf{Z}X_0 + \mathbf{Z}X_1$ *such that*

$$\max\bigl\{|L_0(1,\vartheta)|\ ,\ |L_1(1,\vartheta)|\bigr\} < \epsilon.$$

Proof of (ii)' $\Longrightarrow$ (ii)
Since L_0, L_1 are linearly independent, one at least of them does not vanish at $(1,\vartheta)$. Write it $pX_0 - qX_1$.
Proof of (ii) $\Longrightarrow$ (ii')
Using (ii), set $L_0(X_0, X_1) = pX_0 - qX_1$, and use (ii) again with ϵ replaced by $|q\vartheta - p|$.

Irrationality of at least one number

Let $\vartheta_1, \ldots, \vartheta_m$ be real numbers. The following conditions are equivalent

(i) *One at least of $\vartheta_1, \ldots, \vartheta_m$ is irrational.*

(ii) *For any $\epsilon > 0$, there exist $p_1, \ldots, p_m, q$ in $\mathbf{Z}$ with $q > 0$ such that*

$$0 < \max_{1 \le i \le m} \left| \vartheta_i - \frac{p_i}{q} \right| < \frac{\epsilon}{q}.$$

(iii) *For any $\epsilon > 0$, there exist $m+1$ linearly independent linear forms $L_0, \ldots, L_m$ with coefficients in $\mathbf{Z}$ in $m+1$ variables $X_0, \ldots, X_m$, such that*

$$\max_{0 \le k \le m} |L_k(1, \vartheta_1, \ldots, \vartheta_m)| < \epsilon.$$

(iv) *For any real number $Q > 1$, there exists $(p_1, \ldots, p_m, q)$ in $\mathbf{Z}^{m+1}$ such that $1 \le q \le Q$ and*

$$0 < \max_{1 \le i \le m} \left| \vartheta_i - \frac{p_i}{q} \right| \le \frac{1}{qQ^{1/m}}.$$

Linear independence

Irrationality of ϑ : means that $1, \vartheta$ are linearly independent over $\mathbf{Q}$.

Irrationality of at least one of $\vartheta_1, \ldots, \vartheta_m$: means $(\vartheta_1, \ldots, \vartheta_m) \notin \mathbf{Q}^m$. Also : means that the dimension of the $\mathbf{Q}$–vector space spanned by $1, \vartheta_1, \ldots, \vartheta_m$ is ≥ 2.

Linear independence of $1, \vartheta_1, \ldots, \vartheta_m$ over $\mathbf{Q}$: means that for any hyperplane H : $a_0 z_0 + \cdots + a_m z_m = 0$ of $\mathbf{R}^{m+1}$ rational over $\mathbf{Q}$ (i.e. $a_i \in \mathbf{Q}$), the point $(1, \vartheta_1, \ldots, \vartheta_m)$ does not belong to H.

Transcendence of ϑ : means that $1, \vartheta, \vartheta^2, \ldots, \vartheta^n \ldots$ are linearly independent over $\mathbf{Q}$.

Linear independence

Irrationality of ϑ : means that $1, \vartheta$ are linearly independent over $\mathbf{Q}$.

Irrationality of at least one of $\vartheta_1, \ldots, \vartheta_m$: means $(\vartheta_1, \ldots, \vartheta_m) \notin \mathbf{Q}^m$. Also : means that the dimension of the $\mathbf{Q}$–vector space spanned by $1, \vartheta_1, \ldots, \vartheta_m$ is ≥ 2.

Linear independence of $1, \vartheta_1, \ldots, \vartheta_m$ over $\mathbf{Q}$: means that for any hyperplane H : $a_0 z_0 + \cdots + a_m z_m = 0$ of $\mathbf{R}^{m+1}$ rational over $\mathbf{Q}$ (i.e. $a_i \in \mathbf{Q}$), the point $(1, \vartheta_1, \ldots, \vartheta_m)$ does not belong to H.

Transcendence of ϑ : means that $1, \vartheta, \vartheta^2, \ldots, \vartheta^n \ldots$ are linearly independent over $\mathbf{Q}$.

Linear independence

Irrationality of ϑ : means that $1, \vartheta$ are linearly independent over $\mathbf{Q}$.

Irrationality of at least one of $\vartheta_1, \ldots, \vartheta_m$: means $(\vartheta_1, \ldots, \vartheta_m) \notin \mathbf{Q}^m$. Also : means that the dimension of the $\mathbf{Q}$–vector space spanned by $1, \vartheta_1, \ldots, \vartheta_m$ is ≥ 2.

Linear independence of $1, \vartheta_1, \ldots, \vartheta_m$ over $\mathbf{Q}$: means that for any hyperplane $H : a_0 z_0 + \cdots + a_m z_m = 0$ of $\mathbf{R}^{m+1}$ rational over $\mathbf{Q}$ (i.e. $a_i \in \mathbf{Q}$), the point $(1, \vartheta_1, \ldots, \vartheta_m)$ does not belong to H.

Transcendence of ϑ : means that $1, \vartheta, \vartheta^2, \ldots, \vartheta^n \ldots$ are linearly independent over $\mathbf{Q}$.

Linear independence

Irrationality of ϑ : means that $1, \vartheta$ are linearly independent over $\mathbf{Q}$.

Irrationality of at least one of $\vartheta_1, \ldots, \vartheta_m$: means $(\vartheta_1, \ldots, \vartheta_m) \notin \mathbf{Q}^m$. Also : means that the dimension of the $\mathbf{Q}$–vector space spanned by $1, \vartheta_1, \ldots, \vartheta_m$ is ≥ 2.

Linear independence of $1, \vartheta_1, \ldots, \vartheta_m$ over $\mathbf{Q}$: means that for any hyperplane $H : a_0 z_0 + \cdots + a_m z_m = 0$ of $\mathbf{R}^{m+1}$ rational over $\mathbf{Q}$ (i.e. $a_i \in \mathbf{Q}$), the point $(1, \vartheta_1, \ldots, \vartheta_m)$ does not belong to H.

Transcendence of ϑ : means that $1, \vartheta, \vartheta^2, \ldots, \vartheta^n \ldots$ are linearly independent over $\mathbf{Q}$.

Charles Hermite (1822 - 1901)

Charles Hermite

1873 : Hermite's method for proving linear independence. Let $\vartheta_1, \ldots, \vartheta_m$ be real numbers and a_0, $a_1, \ldots,$ a_m rational integers, not all of which are 0. The goal is to prove that the number

$$L = a_0 + a_1\vartheta_1 + \cdots + a_m\vartheta_m$$

is not 0.

Hermite's idea is to approximate simultaneously $\vartheta_1, \ldots, \vartheta_m$ by rational numbers $p_1/q, \ldots, p_m/q$ with the same denominator $q > 0$.

$$L = a_0 + a_1\vartheta_1 + \cdots + a_m\vartheta_m$$

Let $q, p_1, \ldots, p_m$ be rational integers with $q > 0$. For $1 \le k \le m$, set

$$\epsilon_k = q\vartheta_k - p_k.$$

Then $qL = M + R$ with

$$M = a_0 q + a_1 p_1 + \cdots + a_m p_m \in \mathbf{Z}$$

and

$$R = a_1\epsilon_1 + \cdots + a_m\epsilon_m \in \mathbf{R}.$$

If $M \neq 0$ and $|R| < 1$ we deduce $L \neq 0$.

Zero estimate

Main difficulty : to check $M \neq 0$.

We wish to find a simultaneous rational approximation $(q, p_1, \ldots, p_m)$ to $(\vartheta_1, \ldots, \vartheta_m)$ outside the hyperplane $a_0 z_0 + a_1 z_1 + \cdots + a_m z_m = 0$ of $\mathbf{Q}^{m+1}$.

This needs to be checked for all hyperplanes.

Solution : to construct not only one tuple $\mathbf{u} = (q, p_1, \ldots, p_m)$ in $\mathbf{Z}^{m+1} \setminus \{0\}$, but $m+1$ such tuples which are linearly independent.

This yields $m+1$ pairs (M_k, R_k), $k = 0, \ldots, m$ in place of a single pair (M, R), and from $(a_0, \ldots, a_m) \neq 0$ one deduces that one at least of $M_0, \ldots, M_m$ is not 0.

Zero estimate

Main difficulty : to check $M \neq 0$.

We wish to find a simultaneous rational approximation $(q, p_1, \ldots, p_m)$ to $(\vartheta_1, \ldots, \vartheta_m)$ outside the hyperplane $a_0 z_0 + a_1 z_1 + \cdots + a_m z_m = 0$ of $\mathbf{Q}^{m+1}$.

This needs to be checked for all hyperplanes.

Solution : to construct not only one tuple $\mathbf{u} = (q, p_1, \ldots, p_m)$ in $\mathbf{Z}^{m+1} \setminus \{0\}$, but $m+1$ such tuples which are linearly independent.

This yields $m+1$ pairs (M_k, R_k), $k = 0, \ldots, m$ in place of a single pair (M, R), and from $(a_0, \ldots, a_m) \neq 0$ one deduces that one at least of $M_0, \ldots, M_m$ is not 0.

Zero estimate

Main difficulty : to check $M \neq 0$.

We wish to find a simultaneous rational approximation $(q, p_1, \ldots, p_m)$ to $(\vartheta_1, \ldots, \vartheta_m)$ outside the hyperplane $a_0 z_0 + a_1 z_1 + \cdots + a_m z_m = 0$ of $\mathbf{Q}^{m+1}$.

This needs to be checked for all hyperplanes.

Solution : to construct not only one tuple $\mathbf{u} = (q, p_1, \ldots, p_m)$ in $\mathbf{Z}^{m+1} \setminus \{0\}$, but $m + 1$ such tuples which are linearly independent.

This yields $m + 1$ pairs (M_k, R_k), $k = 0, \ldots, m$ in place of a single pair (M, R), and from $(a_0, \ldots, a_m) \neq 0$ one deduces that one at least of $M_0, \ldots, M_m$ is not 0.

Zero estimate

Main difficulty : to check $M \neq 0$.

We wish to find a simultaneous rational approximation $(q, p_1, \ldots, p_m)$ to $(\vartheta_1, \ldots, \vartheta_m)$ outside the hyperplane $a_0 z_0 + a_1 z_1 + \cdots + a_m z_m = 0$ of $\mathbf{Q}^{m+1}$.

This needs to be checked for all hyperplanes.

Solution : to construct not only one tuple $\mathbf{u} = (q, p_1, \ldots, p_m)$ in $\mathbf{Z}^{m+1} \setminus \{0\}$, but $m+1$ such tuples which are linearly independent.

This yields $m+1$ pairs (M_k, R_k), $k = 0, \ldots, m$ in place of a single pair (M, R), and from $(a_0, \ldots, a_m) \neq 0$ one deduces that one at least of $M_0, \ldots, M_m$ is not 0.

Zero estimate

Main difficulty : to check $M \neq 0$.

We wish to find a simultaneous rational approximation $(q, p_1, \ldots, p_m)$ to $(\vartheta_1, \ldots, \vartheta_m)$ outside the hyperplane $a_0 z_0 + a_1 z_1 + \cdots + a_m z_m = 0$ of $\mathbf{Q}^{m+1}$.

This needs to be checked for all hyperplanes.

Solution : to construct not only one tuple $\mathbf{u} = (q, p_1, \ldots, p_m)$ in $\mathbf{Z}^{m+1} \setminus \{0\}$, but $m+1$ such tuples which are linearly independent.

This yields $m+1$ pairs (M_k, R_k), $k = 0, \ldots, m$ in place of a single pair (M, R), and from $(a_0, \ldots, a_m) \neq 0$ one deduces that one at least of $M_0, \ldots, M_m$ is not 0.

Rational approximations (following Michel Laurent)

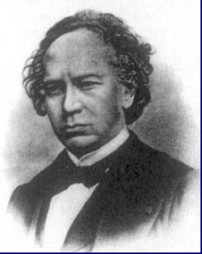
Let $(\vartheta_1, \ldots, \vartheta_m) \in \mathbf{R}^m$.
Then the following conditions are equivalent.
(i) *The numbers* $1, \vartheta_1, \ldots, \vartheta_m$ *are linearly independent over* $\mathbf{Q}$.
(ii) *For any* $\epsilon > 0$, *there exist* $m+1$ *linearly independent elements* $\mathbf{u}_0, \mathbf{u}_1, \ldots, \mathbf{u}_m$ *in* $\mathbf{Z}^{m+1}$, *say*

$$\mathbf{u}_i = (q_i, p_{1i}, \ldots, p_{mi}) \quad (0 \leq i \leq m)$$

with $q_i > 0$, *such that*

$$\max_{1 \leq k \leq m} \left| \vartheta_k - \frac{p_{ki}}{q_i} \right| \leq \frac{\epsilon}{q_i} \quad (0 \leq i \leq m).$$

Hermite – Lindemann Theorem



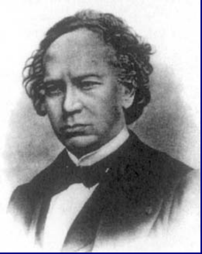
Hermite (1873) :
transcendence of e.

Lindemann (1882) :
transcendence of π.

Hermite – Lindemann Theorem
For any non–zero complex number z, at least one of the two numbers z, e^z is transcendental.

Corollaries : transcendence of $\log\alpha$ and e^β for α and β non–zero algebraic numbers with $\log\alpha \neq 0$.

Hermite – Lindemann Theorem



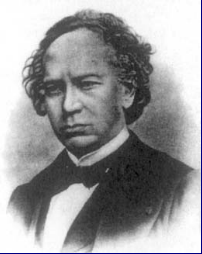
Hermite (1873) :
transcendence of e.

Lindemann (1882) :
transcendence of π.

Hermite – Lindemann Theorem
For any non–zero complex number z, at least one of the two numbers z, e^z is transcendental.

Corollaries : transcendence of $\log\alpha$ and e^β for α and β non–zero algebraic numbers with $\log\alpha \neq 0$.

Hermite – Lindemann Theorem



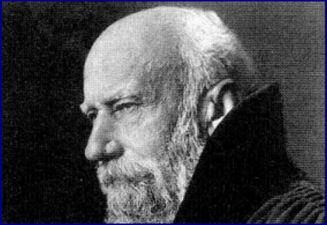
Hermite (1873) :
transcendence of e.

Lindemann (1882) :
transcendence of π.

Hermite – Lindemann Theorem
For any non–zero complex number z, at least one of the two numbers z, e^z is transcendental.

Corollaries : transcendence of $\log\alpha$ and e^β for α and β non–zero algebraic numbers with $\log\alpha \neq 0$.

Lindemann – Weierstraß Theorem

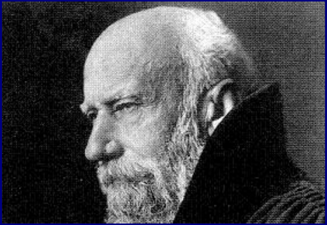


Let $\beta_1, \ldots, \beta_n$ be algebraic numbers which are linearly independent over $\mathbf{Q}$. Then the numbers $e^{\beta_1}, \ldots, e^{\beta_n}$ are algebraically independent over $\mathbf{Q}$.

Equivalent to :

Let $\alpha_1, \ldots, \alpha_m$ be distinct algebraic numbers. Then the numbers $e^{\alpha_1}, \ldots, e^{\alpha_m}$ are linearly independent over $\mathbf{Q}$.

Lindemann – Weierstraß Theorem

Let $\beta_1, \ldots, \beta_n$ be algebraic numbers which are linearly independent over $\mathbf{Q}$. Then the numbers $e^{\beta_1}, \ldots, e^{\beta_n}$ are algebraically independent over $\mathbf{Q}$.

Equivalent to :

Let $\alpha_1, \ldots, \alpha_m$ be distinct algebraic numbers. Then the numbers $e^{\alpha_1}, \ldots, e^{\alpha_m}$ are linearly independent over $\mathbf{Q}$.

Carl Ludwig Siegel (1896 - 1981)

Siegel's method for proving linear independence.
Let $\vartheta_1, \ldots, \vartheta_m$ be complex numbers.

C.L. Siegel

1929 :
Assume that, for any $\epsilon > 0$, there exists $m+1$ linearly independent linear forms $L_0, \ldots, L_m$, with coefficients in $\mathbf{Z}$, such that

$$\max_{0 \le k \le m} |L_k(1, \vartheta_1, \ldots, \vartheta_m)| < \frac{\epsilon}{H^{m-1}}$$

where $H = \max_{0 \le k \le m} H(L_k)$.

Then $1, \vartheta_1, \ldots, \vartheta_m$ are linearly independent over $\mathbf{Q}$.

Linear independence, following Siegel (1929)

Height of a linear form : $H(L) = \max|\text{coefficients of } L|$.

Example : $m = 1$ (irrationality criterion). *A real number ϑ is irrational if and only, for any $\epsilon > 0$, if there exists two linearly independent linear forms $L_0(X_0, X_1)$ and $L_1(X_0, X_1)$ in $\mathbf{Z}X_0 + \mathbf{Z}X_1$ such that $|L_i(1, \vartheta)| < \epsilon$.*

Sketch of proof of Siegel's criterion. Assume $1, \vartheta_1, \ldots, \vartheta_m$ are linearly dependent over $\mathbf{Q}$. Let $L \in \mathbf{Z}X_0 + \cdots + \mathbf{Z}X_m$ be a non–zero linear form vanishing at $(1, \vartheta_1, \ldots, \vartheta_m)$. Among $L_0, \ldots, L_m$, select m linear forms, say $L_1, \ldots, L_m$, which constitute with L a complete system of linearly independent forms in $m + 1$ variables. The determinant Δ of $L, L_1, \ldots, L_m$ is a non–zero integer, hence its absolute value is ≥ 1. Inverting the matrix, write Δ as a linear combination with integer coefficients of the $L_i(1, \vartheta_1, \ldots, \vartheta_m)$ $(1 \leq i \leq m)$ and estimate the coefficients.

Linear independence, following Siegel (1929)

Height of a linear form : $H(L) = \max|\text{coefficients of } L|$.

Example : $m = 1$ (irrationality criterion). *A real number ϑ is irrational if and only, for any $\epsilon > 0$, if there exists two linearly independent linear forms $L_0(X_0, X_1)$ and $L_1(X_0, X_1)$ in $\mathbf{Z}X_0 + \mathbf{Z}X_1$ such that $|L_i(1, \vartheta)| < \epsilon$.*

Sketch of proof of Siegel's criterion. Assume $1, \vartheta_1, \dots, \vartheta_m$ are linearly dependent over $\mathbf{Q}$. Let $L \in \mathbf{Z}X_0 + \cdots + \mathbf{Z}X_m$ be a non–zero linear form vanishing at $(1, \vartheta_1, \dots, \vartheta_m)$. Among $L_0, \dots, L_m$, select m linear forms, say $L_1, \dots, L_m$, which constitute with L a complete system of linearly independent forms in $m+1$ variables. The determinant Δ of $L, L_1, \dots, L_m$ is a non–zero integer, hence its absolute value is ≥ 1. Inverting the matrix, write Δ as a linear combination with integer coefficients of the $L_i(1, \vartheta_1, \dots, \vartheta_m)$ $(1 \leq i \leq m)$ and estimate the coefficients.

Linear independence, following Siegel (1929)

Height of a linear form : $H(L) = \max|\text{coefficients of } L|$.

Example : $m = 1$ (irrationality criterion). *A real number* ϑ *is irrational if and only, for any* $\epsilon > 0$*, if there exists two linearly independent linear forms* $L_0(X_0, X_1)$ *and* $L_1(X_0, X_1)$ *in* $\mathbf{Z}X_0 + \mathbf{Z}X_1$ *such that* $|L_i(1, \vartheta)| < \epsilon$*.*

Sketch of proof of Siegel's criterion. Assume $1, \vartheta_1, \ldots, \vartheta_m$ are linearly dependent over $\mathbf{Q}$. Let $L \in \mathbf{Z}X_0 + \cdots + \mathbf{Z}X_m$ be a non–zero linear form vanishing at $(1, \vartheta_1, \ldots, \vartheta_m)$. Among $L_0, \ldots, L_m$, select m linear forms, say $L_1, \ldots, L_m$, which constitute with L a complete system of linearly independent forms in $m + 1$ variables. The determinant Δ of $L, L_1, \ldots, L_m$ is a non–zero integer, hence its absolute value is ≥ 1. Inverting the matrix, write Δ as a linear combination with integer coefficients of the $L_i(1, \vartheta_1, \ldots, \vartheta_m)$ $(1 \leq i \leq m)$ and estimate the coefficients.

Linear independence, following Siegel (1929)

Height of a linear form : $H(L) = \max |\text{coefficients of } L|$.

Example : $m = 1$ (irrationality criterion). *A real number ϑ is irrational if and only, for any $\epsilon > 0$, if there exists two linearly independent linear forms $L_0(X_0, X_1)$ and $L_1(X_0, X_1)$ in $\mathbf{Z}X_0 + \mathbf{Z}X_1$ such that $|L_i(1, \vartheta)| < \epsilon$.*

Sketch of proof of Siegel's criterion. Assume $1, \vartheta_1, \ldots, \vartheta_m$ are linearly dependent over $\mathbf{Q}$. Let $L \in \mathbf{Z}X_0 + \cdots + \mathbf{Z}X_m$ be a non–zero linear form vanishing at $(1, \vartheta_1, \ldots, \vartheta_m)$. Among $L_0, \ldots, L_m$, select m linear forms, say $L_1, \ldots, L_m$, which constitute with L a complete system of linearly independent forms in $m+1$ variables. The determinant Δ of $L, L_1, \ldots, L_m$ is a non–zero integer, hence its absolute value is ≥ 1. Inverting the matrix, write Δ as a linear combination with integer coefficients of the $L_i(1, \vartheta_1, \ldots, \vartheta_m)$ $(1 \leq i \leq m)$ and estimate the coefficients.

Linear independence, following Siegel (1929)

Height of a linear form : $H(L) = \max |\text{coefficients of } L|$.

Example : $m = 1$ (irrationality criterion). *A real number ϑ is irrational if and only, for any $\epsilon > 0$, if there exists two linearly independent linear forms $L_0(X_0, X_1)$ and $L_1(X_0, X_1)$ in $\mathbf{Z}X_0 + \mathbf{Z}X_1$ such that $|L_i(1, \vartheta)| < \epsilon$.*

Sketch of proof of Siegel's criterion. Assume $1, \vartheta_1, \ldots, \vartheta_m$ are linearly dependent over $\mathbf{Q}$. Let $L \in \mathbf{Z}X_0 + \cdots + \mathbf{Z}X_m$ be a non–zero linear form vanishing at $(1, \vartheta_1, \ldots, \vartheta_m)$. Among $L_0, \ldots, L_m$, select m linear forms, say $L_1, \ldots, L_m$, which constitute with L a complete system of linearly independent forms in $m + 1$ variables. The determinant Δ of $L, L_1, \ldots, L_m$ is a non–zero integer, hence its absolute value is ≥ 1. Inverting the matrix, write Δ as a linear combination with integer coefficients of the $L_i(1, \vartheta_1, \ldots, \vartheta_m)$ $(1 \leq i \leq m)$ and estimate the coefficients.

Linear independence, following Siegel (1929)

Height of a linear form : $H(L) = \max|\text{coefficients of } L|$.

Example : $m = 1$ (irrationality criterion). *A real number ϑ is irrational if and only, for any $\epsilon > 0$, if there exists two linearly independent linear forms $L_0(X_0, X_1)$ and $L_1(X_0, X_1)$ in $\mathbf{Z}X_0 + \mathbf{Z}X_1$ such that $|L_i(1, \vartheta)| < \epsilon$.*

Sketch of proof of Siegel's criterion. Assume $1, \vartheta_1, \dots, \vartheta_m$ are linearly dependent over $\mathbf{Q}$. Let $L \in \mathbf{Z}X_0 + \cdots + \mathbf{Z}X_m$ be a non–zero linear form vanishing at $(1, \vartheta_1, \dots, \vartheta_m)$. Among $L_0, \dots, L_m$, select m linear forms, say $L_1, \dots, L_m$, which constitute with L a complete system of linearly independent forms in $m + 1$ variables. The determinant Δ of $L, L_1, \dots, L_m$ is a non–zero integer, hence its absolute value is ≥ 1. Inverting the matrix, write Δ as a linear combination with integer coefficients of the $L_i(1, \vartheta_1, \dots, \vartheta_m)$ $(1 \leq i \leq m)$ and estimate the coefficients.

Linear independence, following Siegel (1929)

Height of a linear form : $H(L) = \max|\text{coefficients of } L|$.

Example : $m = 1$ (irrationality criterion). *A real number ϑ is irrational if and only, for any $\epsilon > 0$, if there exists two linearly independent linear forms $L_0(X_0, X_1)$ and $L_1(X_0, X_1)$ in $\mathbf{Z}X_0 + \mathbf{Z}X_1$ such that $|L_i(1, \vartheta)| < \epsilon$.*

Sketch of proof of Siegel's criterion. Assume $1, \vartheta_1, \ldots, \vartheta_m$ are linearly dependent over $\mathbf{Q}$. Let $L \in \mathbf{Z}X_0 + \cdots + \mathbf{Z}X_m$ be a non–zero linear form vanishing at $(1, \vartheta_1, \ldots, \vartheta_m)$. Among $L_0, \ldots, L_m$, select m linear forms, say $L_1, \ldots, L_m$, which constitute with L a complete system of linearly independent forms in $m+1$ variables. The determinant Δ of $L, L_1, \ldots, L_m$ is a non–zero integer, hence its absolute value is ≥ 1. Inverting the matrix, write Δ as a linear combination with integer coefficients of the $L_i(1, \vartheta_1, \ldots, \vartheta_m)$ $(1 \leq i \leq m)$ and estimate the coefficients.

Criterion of Yu. V. Nesterenko

Let $\vartheta_1, \dots, \vartheta_m$ be complex numbers.

Yu.V.Nesterenko (1985)

Let α and β be two positive numbers satisfying $\alpha > \beta(m-1)$. Assume there is a sequence $(L_n)_{n\geq 0}$ of linear forms in $\mathbf{Z}X_0 + \mathbf{Z}X_1 + \dots + \mathbf{Z}X_m$ of height $\leq e^{\beta n}$ such that

$$|L_n(1, \vartheta_1, \dots, \vartheta_m)| = e^{-\alpha n + o(n)}.$$

Then $1, \vartheta_1, \dots, \vartheta_m$ are linearly independent over $\mathbf{Q}$.

Example : $m = 1$ – irrationality criterion.

Simplified proof of Nesterenko's Theorem

Francesco Amoroso

Pierre Colmez

Refinements : Raffaele Marcovecchio, Pierre Bel.

Irrationality measure for $\log 2$: history

$$\left|\log 2 - \frac{p}{q}\right| > \frac{1}{q^\mu}$$

Hermite–Lindemann, Mahler, Baker, Gel'fond, Feldman,... :
transcendence measures

G. Rhin 1987	$\mu(\log 2) < 4.07$
E.A. Rukhadze 1987	$\mu(\log 2) < 3.89$
R. Marcovecchio 2008	$\mu(\log 2) < 3.57$

Recent developments

Stéphane Fischler and Wadim Zudilin, *A refinement of Nesterenko's linear independence criterion with applications to zeta values.* Preprint MPIM 2009-35.

Recent developments

Stéphane Fischler and Tanguy Rivoal, *Irrationality exponent and rational approximations with prescribed growth.* *Trans. Amer. Math. Soc.* , to appear.

J. Liouville (1809 – 1882)

Liouville's inequalities

easiest : integers
$a \in \mathbf{Z}$, $a \neq 0 \Rightarrow |a| \geq 1$.

rational numbers :
$r = a/b \in \mathbf{Q}$, $r \neq 0 \Rightarrow$
$|r| \geq 1/b$.

algebraic numbers :
$\alpha \in \overline{\mathbf{Q}}$, $\alpha \neq 0 \Rightarrow$
$$|\alpha| \geq \frac{1}{H(\alpha)+1}.$$

1844
Existence of transcendental numbers

Criteria for transcendence and algebraic independence

A complex number ϑ is *transcendental* if and only if $1, \vartheta, \vartheta^2, \ldots, \vartheta^n \ldots$ are linearly independent (over $\mathbf{Q}$).

Complex numbers $\vartheta_1, \ldots, \vartheta_m$ are *algebraically independent* if and only if the numbers $\vartheta_1^{i_1} \cdots \vartheta_m^{i_m}$, $((i_1, \ldots, i_m) \in \mathbf{Z}_{\geq 0}^m$ are linearly independent.

Hence, criteria for linear independence yield criteria for transcendence and for algebraic independence.

Furthermore, criteria for transcendence are special case $(m = 1)$ of criteria for algebraic independence.

Criteria for transcendence and algebraic independence

A complex number ϑ is *transcendental* if and only if $1, \vartheta, \vartheta^2, \ldots, \vartheta^n \ldots$ are linearly independent (over $\mathbf{Q}$).

Complex numbers $\vartheta_1, \ldots, \vartheta_m$ are *algebraically independent* if and only if the numbers $\vartheta_1^{i_1} \cdots \vartheta_m^{i_m}$, $((i_1, \ldots, i_m) \in \mathbf{Z}_{\geq 0}^m$ are linearly independent.

Hence, criteria for linear independence yield criteria for transcendence and for algebraic independence.

Furthermore, criteria for transcendence are special case $(m = 1)$ of criteria for algebraic independence.

Criteria for transcendence and algebraic independence

A complex number ϑ is *transcendental* if and only if $1, \vartheta, \vartheta^2, \dots, \vartheta^n \dots$ are linearly independent (over $\mathbf{Q}$).

Complex numbers $\vartheta_1, \dots, \vartheta_m$ are *algebraically independent* if and only if the numbers $\vartheta_1^{i_1} \cdots \vartheta_m^{i_m}$, $((i_1, \dots, i_m) \in \mathbf{Z}_{\geq 0}^m$ are linearly independent.

Hence, criteria for linear independence yield criteria for transcendence and for algebraic independence.

Furthermore, criteria for transcendence are special case $(m = 1)$ of criteria for algebraic independence.

Criteria for transcendence and algebraic independence

A complex number ϑ is *transcendental* if and only if $1, \vartheta, \vartheta^2, \dots, \vartheta^n \dots$ are linearly independent (over $\mathbf{Q}$).

Complex numbers $\vartheta_1, \dots, \vartheta_m$ are *algebraically independent* if and only if the numbers $\vartheta_1^{i_1} \cdots \vartheta_m^{i_m}$, $((i_1, \dots, i_m) \in \mathbf{Z}_{\geq 0}^m$ are linearly independent.

Hence, criteria for linear independence yield criteria for transcendence and for algebraic independence.

Furthermore, criteria for transcendence are special case $(m = 1)$ of criteria for algebraic independence.

Transcendence and Diophantine approximation by algebraic numbers

Recall : Criterion for irrationality. *A real number ϑ is* irrational *if and only if there is a sequence of good rational approximations $(p_n/q_n)_{n\geq 0}$ with $p_n/q_n \neq \vartheta$.*

Generalization for fixed degree : *given a positive integer d, a complex number ϑ is* not algebraic of degree $\leq d$ *if and only if there is a sequence of good algebraic approximations $(\alpha_n)_{n\geq 0}$ with α_n algebraic of degree $\leq d$ and $\alpha_n \neq \vartheta$.*

Durand's criterion for transcendence (1974) : *a complex number ϑ is* transcendental *if and only if there is a sequence of good algebraic approximations $(\alpha_n)_{n\geq 0}$ with α_n algebraic and $\alpha_n \neq \vartheta$.*

Transcendence and Diophantine approximation by algebraic numbers

Recall : Criterion for irrationality. *A real number ϑ is* irrational *if and only if there is a sequence of good rational approximations $(p_n/q_n)_{n\geq 0}$ with $p_n/q_n \neq \vartheta$.*

Generalization for fixed degree : *given a positive integer d, a complex number ϑ is* not algebraic of degree $\leq d$ *if and only if there is a sequence of good algebraic approximations $(\alpha_n)_{n\geq 0}$ with α_n algebraic of degree $\leq d$ and $\alpha_n \neq \vartheta$.*

Durand's criterion for transcendence (1974) : *a complex number ϑ is* transcendental *if and only if there is a sequence of good algebraic approximations $(\alpha_n)_{n\geq 0}$ with α_n algebraic and $\alpha_n \neq \vartheta$.*

Transcendence and Diophantine approximation by algebraic numbers

Recall : Criterion for irrationality. *A real number* ϑ *is* irrational *if and only if there is a sequence of good rational approximations* $(p_n/q_n)_{n\geq 0}$ *with* $p_n/q_n \neq \vartheta$.

Generalization for fixed degree : *given a positive integer* d*, a complex number* ϑ *is* not algebraic of degree $\leq d$ *if and only if there is a sequence of good algebraic approximations* $(\alpha_n)_{n\geq 0}$ *with* α_n *algebraic of degree* $\leq d$ *and* $\alpha_n \neq \vartheta$.

Durand's criterion for transcendence (1974) : *a complex number* ϑ *is* transcendental *if and only if there is a sequence of good algebraic approximations* $(\alpha_n)_{n\geq 0}$ *with* α_n *algebraic and* $\alpha_n \neq \vartheta$.

Alain Durand (1949–1986)

Cinquante Ans de Polynômes – Fifty Years of Polynomials Lecture Notes in Mathematics, Springer Verlag **1415** (1990).

Proceedings of a Conference held in honour of Alain Durand at the Institut Henri Poincaré Paris, France, May 26–27, 1988

Transcendence and Diophantine approximation by polynomials

A complex number ϑ is transcendental if and only if there is a sequence $(P_n)_{n\geq 0}$ of polynomials in $\mathbf{Z}[X]$ such that $|P_n(\vartheta)|$ is non–zero and small, in terms of the degree d_n and the *height* (maximum of the absolute values of the coefficients) of P_n.

Existence of a sequence : *Dirichlet's box principle*. Given $\vartheta \in \mathbf{C}$, there exists $P \in \mathbf{Z}[X] \setminus \{0\}$ such that $|P_n(\vartheta)|$ is small. If ϑ is transcendental, then $|P_n(\vartheta)|$ is non–zero.

Lower bound : *Liouville's inequality*. If ϑ is algebraic and $|P_n(\vartheta)|$ is non–zero, then $|P_n(\vartheta)|$ cannot be two small.

Transcendence and Diophantine approximation by polynomials

A complex number ϑ is transcendental if and only if there is a sequence $(P_n)_{n\geq 0}$ of polynomials in $\mathbf{Z}[X]$ such that $|P_n(\vartheta)|$ is non–zero and small, in terms of the degree d_n and the *height* (maximum of the absolute values of the coefficients) of P_n.

Existence of a sequence : *Dirichlet's box principle*. Given $\vartheta \in \mathbf{C}$, there exists $P \in \mathbf{Z}[X] \setminus \{0\}$ such that $|P_n(\vartheta)|$ is small. If ϑ is transcendental, then $|P_n(\vartheta)|$ is non–zero.

Lower bound : *Liouville's inequality*. If ϑ is algebraic and $|P_n(\vartheta)|$ is non–zero, then $|P_n(\vartheta)|$ cannot be two small.

Transcendence and Diophantine approximation by polynomials

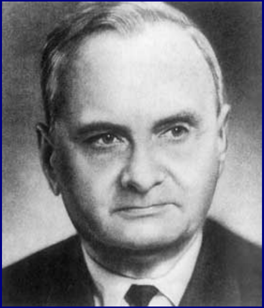
A complex number ϑ is transcendental if and only if there is a sequence $(P_n)_{n\geq 0}$ of polynomials in $\mathbf{Z}[X]$ such that $|P_n(\vartheta)|$ is non–zero and small, in terms of the degree d_n and the *height* (maximum of the absolute values of the coefficients) of P_n.

Existence of a sequence : *Dirichlet's box principle*. Given $\vartheta \in \mathbf{C}$, there exists $P \in \mathbf{Z}[X] \setminus \{0\}$ such that $|P_n(\vartheta)|$ is small. If ϑ is transcendental, then $|P_n(\vartheta)|$ is non–zero.

Lower bound : *Liouville's inequality*. If ϑ is algebraic and $|P_n(\vartheta)|$ is non–zero, then $|P_n(\vartheta)|$ cannot be two small.

Aleksandr Osipovich Gelfond (1906 - 1968)

Dirichlet : *Given* $\vartheta \in \mathbf{R}$, $d > 0$ *and* $H > 0$, *there exists a non–zero polynomial* $P \in \mathbf{Z}[X]$ *of degree* $\leq d$ *and height* $\leq H$ *such that* $|P(\vartheta)| \leq c(\vartheta)^d H^{-d}$.



For some specific ϑ, d, H, much smaller values for $|P(\vartheta)|$ can be reached.

Of course, this happens when ϑ is algebraic of degree $\leq d$, but also for instance when ϑ is a Liouville number and $d = 1$.

Fundamental result by Gel'fond : *If there is a "regular" sequence of* P_n *such that* $|P_n(\vartheta)|$ *is quite small, then* ϑ *is algebraic and all* $P_n(\vartheta)$ *vanish.*

Algebraic independence method of Gel'fond

A.O. Gel'fond (1948)

The two numbers $2^{\sqrt[3]{2}}$ and $2^{\sqrt[3]{4}}$ are algebraically independent.

More generally, if α is an algebraic number, $\alpha \neq 0$, $\alpha \neq 1$ and if β is a algebraic number of degree $d \geq 3$, then two at least of the numbers

$$\alpha^{\beta},\ \alpha^{\beta^2},\ \ldots,\alpha^{\beta^{d-1}}$$

are algebraically independent.

Gel'fond's transcendence criterion (1949)

Simple form : *Given a complex number ϑ, if there exists a sequence $(P_n)_{n\geq 1}$ of non–zero polynomials in $\mathbf{Z}[X]$, with P_n of degree $\leq n$ and height $\leq e^n$, such that*

$$|P_n(\vartheta)| \leq e^{-6n^2}$$

for all $n \geq 1$, then ϑ is algebraic and $P_n(\vartheta) = 0$ for all $n \geq 1$.

Rob Tijdeman and Dale Brownawell

70's : Simplification et extensions due to R. Tijdeman, W.D. Brownawell,...

http://www.wiskundemeisjes.nl/20080830/ridder-tijdeman/

Gel'fond's transcendence criterion

First extension : Replace the upper bound for the degree by d_n, the upper bound for the height by e^{h_n}, and the upper bound for $|P_n(\vartheta)|$ by $e^{-\nu_n}$.

Assumptions on the sequences $(d_n)_{n\geq 1}$, $(h_n)_{n\geq 1}$ and $(\nu_n)_{n\geq 1}$:

$$d_n \leq d_{n+1} \leq \kappa d_n, \qquad d_n \leq h_n \leq h_{n+1} \leq \kappa h_n,$$

with some constant $\kappa \geq 1$ independent of n, and (main assumption)

$$\nu_n / d_n h_n \to \infty.$$

Gel'fond's transcendence criterion

First extension : Replace the upper bound for the degree by d_n, the upper bound for the height by e^{h_n}, and the upper bound for $|P_n(\vartheta)|$ by $e^{-\nu_n}$.

Assumptions on the sequences $(d_n)_{n\geq 1}$, $(h_n)_{n\geq 1}$ and $(\nu_n)_{n\geq 1}$:

$$d_n \leq d_{n+1} \leq \kappa d_n, \qquad d_n \leq h_n \leq h_{n+1} \leq \kappa h_n,$$

with some constant $\kappa \geq 1$ independent of n, and (main assumption)

$$\nu_n / d_n h_n \to \infty.$$

Transcendence criterion with multiplicities

With derivatives : *Given a complex number ϑ, assume that there exists a sequence $(P_n)_{n\geq 1}$ of non–zero polynomials in $\mathbf{Z}[X]$, with P_n of degree $\leq d_n$ and height $\leq e^{h_n}$, such that*

$$\max\bigl\{\bigl|P_n^{(j)}(\vartheta)\bigr| \ ; \ 0 \leq j < t_n\bigr\} \leq e^{-\nu_n}$$

for all $n \geq 1$. Assume $\nu_n t_n / d_n h_n \to \infty$. Then ϑ is algebraic.

Due to M. Laurent and D. Roy (1999), applications to algebraic independence with interpolation determinants.

Transcendence criterion with multiplicities

With derivatives : *Given a complex number ϑ, assume that there exists a sequence $(P_n)_{n\geq 1}$ of non–zero polynomials in $\mathbf{Z}[X]$, with P_n of degree $\leq d_n$ and height $\leq e^{h_n}$, such that*

$$\max\left\{\left|P_n^{(j)}(\vartheta)\right| \ ; \ 0 \leq j < t_n\right\} \leq e^{-\nu_n}$$

for all $n \geq 1$. Assume $\nu_n t_n / d_n h_n \to \infty$. Then ϑ is algebraic.

Due to M. Laurent and D. Roy (1999), applications to algebraic independence with interpolation determinants.

Criterion with several points

Goal : *Given a sequence of complex numbers* $(\vartheta_i)_{i\geq 1}$, *assume that there exists a sequence* $(P_n)_{n\geq 1}$ *of non–zero polynomials in* $\mathbf{Z}[X]$, *with* P_n *of degree* $\leq d_n$ *and height* $\leq e^{h_n}$, *such that*

$$\max\left\{\left|P_n^{(j)}(\vartheta_i)\right| \; ; \; 0\leq j < t_n, \; 1\leq i\leq s_n\right\} \leq e^{-\nu_n}$$

for all $n\geq 1$. *Assume* $\nu_n t_n s_n / d_n h_n \to \infty$.
We wish to deduce that the numbers ϑ_i *are algebraic.*

D. Roy : Not true in general, but true in some special cases with a structure on the sequence $(\vartheta_i)_{i\geq 1}$.
Combines the elimination arguments used for criteria of algebraic independence and for zero estimates.

Criterion with several points

Goal : *Given a sequence of complex numbers $(\vartheta_i)_{i\geq 1}$, assume that there exists a sequence $(P_n)_{n\geq 1}$ of non–zero polynomials in $\mathbf{Z}[X]$, with P_n of degree $\leq d_n$ and height $\leq e^{h_n}$, such that*

$$\max\left\{\left|P_n^{(j)}(\vartheta_i)\right| \;;\; 0\leq j<t_n,\; 1\leq i\leq s_n\right\}\leq e^{-\nu_n}$$

for all $n\geq 1$. Assume $\nu_n t_n s_n/d_n h_n \to \infty$.
We wish to deduce that the numbers ϑ_i are algebraic.

D. Roy : Not true in general, but true in some special cases with a structure on the sequence $(\vartheta_i)_{i\geq 1}$.
Combines the elimination arguments used for criteria of algebraic independence and for zero estimates.

Criterion with several points

Goal : *Given a sequence of complex numbers $(\vartheta_i)_{i\geq 1}$, assume that there exists a sequence $(P_n)_{n\geq 1}$ of non–zero polynomials in $\mathbf{Z}[X]$, with P_n of degree $\leq d_n$ and height $\leq e^{h_n}$, such that*

$$\max\left\{\left|P_n^{(j)}(\vartheta_i)\right| \; ; \; 0 \leq j < t_n, \; 1 \leq i \leq s_n\right\} \leq e^{-\nu_n}$$

for all $n \geq 1$. Assume $\nu_n t_n s_n / d_n h_n \to \infty$.
We wish to deduce that the numbers ϑ_i are algebraic.

D. Roy : Not true in general, but true in some special cases with a structure on the sequence $(\vartheta_i)_{i\geq 1}$.
Combines the elimination arguments used for criteria of algebraic independence and for zero estimates.

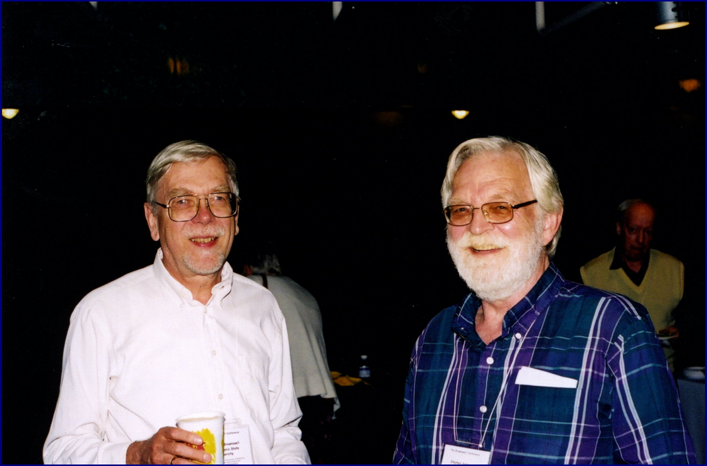
Schanuel's Conjecture

Let $x_1, \ldots, x_n$ *be* $\mathbf{Q}$*-linearly independent complex numbers.*
Then at least n *of the* $2n$ *numbers*
$x_1, \ldots, x_n, \; e^{x_1}, \ldots, e^{x_n}$
are algebraically independent.

In other terms, the conclusion is

$$\operatorname{tr\,deg}_{\mathbf{Q}} \mathbf{Q}\bigl(x_1, \ldots, x_n, \; e^{x_1}, \ldots, e^{x_n}\bigr) \geq n.$$

Dale Brownawell and Stephen Schanuel



How could we attack Schanuel's Conjecture ?

Let $x_1, \ldots, x_n$ be $\mathbf{Q}$–linearly independent complex numbers. Following the transcendence methods of Hermite, Gel'fond, Schneider..., one may start by introducing an auxiliary function

$$F(z) = P(z, e^z)$$

where $P \in \mathbf{Z}[X_0, X_1]$ is a non–zero polynomial. One considers the derivatives of F

$$F^{(k)} = \left(\frac{d}{dz}\right)^k F$$

at the points

$$m_1 x_1 + \cdots + m_n x_n$$

for various values of $(m_1, \ldots, m_n) \in \mathbf{Z}^n$.

How could we attack Schanuel's Conjecture ?

Let $x_1, \ldots, x_n$ be $\mathbf{Q}$–linearly independent complex numbers. Following the transcendence methods of Hermite, Gel'fond, Schneider..., one may start by introducing an auxiliary function

$$F(z) = P(z, e^z)$$

where $P \in \mathbf{Z}[X_0, X_1]$ is a non–zero polynomial. One considers the derivatives of F

$$F^{(k)} = \left(\frac{d}{dz}\right)^k F$$

at the points

$$m_1 x_1 + \cdots + m_n x_n$$

for various values of $(m_1, \ldots, m_n) \in \mathbf{Z}^n$.

The derivation

Let $\mathcal{D}$ denote the derivation

$$\mathcal{D} = \frac{\partial}{\partial X_0} + X_1 \frac{\partial}{\partial X_1}$$

over the ring $\mathbf{C}[X_0, X_1]$, so that for $P \in \mathbf{C}[X_0, X_1]$ the derivatives of the function

$$F(z) = P(z, e^z)$$

are given by

$$\left(\frac{d}{dz}\right)^k F = (\mathcal{D}^k P)(z, e^z).$$

The derivation

Let $\mathcal{D}$ denote the derivation

$$\mathcal{D} = \frac{\partial}{\partial X_0} + X_1 \frac{\partial}{\partial X_1}$$

over the ring $\mathbf{C}[X_0, X_1]$, so that for $P \in \mathbf{C}[X_0, X_1]$ the derivatives of the function

$$F(z) = P(z, e^z)$$

are given by

$$\left(\frac{d}{dz}\right)^k F = (\mathcal{D}^k P)(z, e^z).$$

Auxiliary function

Recall that $x_1, \ldots, x_n$ are $\mathbf{Q}$–linearly independent complex numbers. Let $\alpha_1, \ldots, \alpha_n$ be non–zero complex numbers. The transcendence machinery produces a sequence $(P_N)_{N\geq 0}$ of polynomials with integer coefficients satisfying

$$\left| (\mathcal{D}^k P_N)\Bigl(\sum_{j=1}^n m_j x_j, \prod_{j=1}^n \alpha_j^{m_j}\Bigr) \right| \leq \exp(-N^u)$$

for any non-negative integers k, $m_1, \ldots, m_n$ with $k \leq N^{s_0}$ and $\max\{m_1, \ldots, m_n\} \leq N^{s_1}$.

Auxiliary function

Recall that $x_1, \ldots, x_n$ are $\mathbf{Q}$–linearly independent complex numbers. Let $\alpha_1, \ldots, \alpha_n$ be non–zero complex numbers. The transcendence machinery produces a sequence $(P_N)_{N\geq 0}$ of polynomials with integer coefficients satisfying

$$\left| \left(\mathcal{D}^k P_N\right) \left(\sum_{j=1}^n m_j x_j, \prod_{j=1}^n \alpha_j^{m_j} \right) \right| \leq \exp(-N^u)$$

for any non-negative integers k, $m_1, \ldots, m_n$ with $k \leq N^{s_0}$ and $\max\{m_1, \ldots, m_n\} \leq N^{s_1}$.

Roy's approach to Schanuel's Conjecture (1999)

Following D. Roy, one may expect that the existence of a sequence $(P_N)_{N\geq 0}$ producing sufficiently many such equations will yield the conclusion :

$$\operatorname{tr}\deg_{\mathbf{Q}}\mathbf{Q}\bigl(x_1,\ldots,x_n,\alpha_1,\ldots,\alpha_n\bigr)\geq n.$$

New conjecture equivalent to Schanuel's one, in the spirit of known transcendence criteria by Gel'fond (1949), Chudnovsky, Philippon, Nesterenko, Laurent...

D. Roy. *An arithmetic criterion for the values of the exponential function.* Acta Arith., **97** N° 2 (2001), 183–194.

TIFR, Mumbai October 5–9, 2009

International conference on "Analytic Number Theory"

www.math.tifr.res.in/∼ant2009

Criteria for irrationality, linear independence, transcendence and algebraic independence

Michel Waldschmidt

Institut de Mathématiques de Jussieu & Paris VI

http://www.math.jussieu.fr/∼miw/

Lecture given on October 8, 2009.