Mahidol University, Bangkok October 29-31, 2009

Franco-Thai Seminar in Pure and Applied Mathematics,

http://www.sc.mahidol.ac.th/cem/franco_thai/

Criteria for linear independence and transcendence, following Yuri Nesterenko, Stéphane Fischler, Wadim Zudilin and Amarisa Chantanasiri

Michel Waldschmidt

Institut de Mathématiques de Jussieu & Paris VI

http://www.math.jussieu.fr/~miw/

Lecture given on October 31, 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, Liouville, Siegel,. . .
2. Irrationality criteria : Dirichlet, Minkowski, Hurwitz
3. Linear independence : Hermite, Siegel, Nesterenko
4. Algebraic independence : Lang, Philippon, Chudnovsky, Nesterenko, Schanuel, Roy, Chantanasiri,. . .

Numbers : algebraic, transcendental

Algebraic number : a complex number which is root of a non-zero polynomial with rational coefficients.

Examples :

- rational numbers : a/b, root of $bX - a$.
- $\sqrt{2}$, root of $X^2 - 2$.
- i, root of $X^2 + 1$.

The sum and the product of algebraic numbers are algebraic numbers. The set of complex algebraic numbers is a field, the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$.

A transcendental number is a complex number which is not algebraic.

Numbers : algebraic, transcendental

Algebraic number : a complex number which is root of a non-zero polynomial with rational coefficients.

Examples :

rational numbers : a/b, root of $bX - a$.
$\sqrt{2}$, root of $X^2 - 2$.
i, root of $X^2 + 1$.

The sum and the product of algebraic numbers are algebraic numbers. The set of complex algebraic numbers is a field, the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$.

A transcendental number is a complex number which is not algebraic.

Numbers : algebraic, transcendental

Algebraic number : a complex number which is root of a non-zero polynomial with rational coefficients.

Examples :

rational numbers : a/b, root of $bX - a$.
$\sqrt{2}$, root of $X^2 - 2$.
i, root of $X^2 + 1$.

The sum and the product of algebraic numbers are algebraic numbers. The set of complex algebraic numbers is a field, the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.

A transcendental number is a complex number which is not algebraic.

Numbers : algebraic, transcendental

Algebraic number : a complex number which is root of a non-zero polynomial with rational coefficients.

Examples :

rational numbers : a/b, root of $bX - a$.
$\sqrt{2}$, root of $X^2 - 2$.
i, root of $X^2 + 1$.

The sum and the product of algebraic numbers are algebraic numbers. The set of complex algebraic numbers is a field, the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$.

A transcendental number is a complex number which is not algebraic.

Numbers : algebraic, transcendental

Algebraic number : a complex number which is root of a non-zero polynomial with rational coefficients.

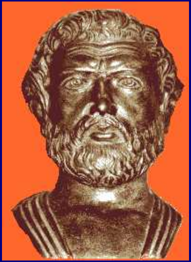
Examples :
rational numbers : a/b, root of $bX - a$.
$\sqrt{2}$, root of $X^2 - 2$.
i, root of $X^2 + 1$.

The sum and the product of algebraic numbers are algebraic numbers. The set of complex algebraic numbers is a field, the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$.

A transcendental number is a complex number which is not algebraic.

Irrationality of $\sqrt{2}$

Pythagoreas school

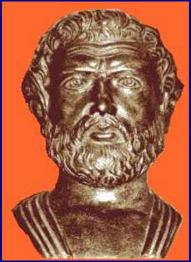


Hippasus of Metapontum (around 500 BC).

Sulba Sutras, Vedic civilization in India, ~800-500 BC.

Irrationality of $\sqrt{2}$

Pythagoreas school

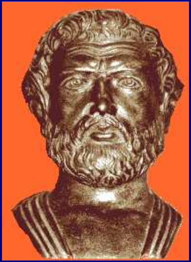


Hippasus of Metapontum (around 500 BC).

Sulba Sutras, Vedic civilization in India, ~800-500 BC.

Irrationality of $\sqrt{2}$

Pythagoreas school



Hippasus of Metapontum (around 500 BC).

Sulba Sutras, Vedic civilization in India, ∼800-500 BC.

Irrationality criteria

A real number is rational if and only if its binary (or decimal, or in any basis $b \geq 2$) expansion is *ultimately periodic*.

Also a real number is rational if and only if its continued fraction expansion is finite.

Consequence : it should not be so difficult to decide whether a given number is rational or not.

To prove that certain numbers (occurring as constants in analysis) are irrational is most often an impossible challenge. However to construct irrational (even transcendental) numbers is easy.

Irrationality criteria

A real number is rational if and only if its binary (or decimal, or in any basis $b \geq 2$) expansion is *ultimately periodic*.

Also a real number is rational if and only if its continued fraction expansion is finite.

Consequence : it should not be so difficult to decide whether a given number is rational or not.

To prove that certain numbers (occurring as constants in analysis) are irrational is most often an impossible challenge. However to construct irrational (even transcendental) numbers is easy.

Irrationality criteria

A real number is rational if and only if its binary (or decimal, or in any basis $b \geq 2$) expansion is *ultimately periodic*.

Also a real number is rational if and only if its continued fraction expansion is finite.

Consequence : it should not be so difficult to decide whether a given number is rational or not.

To prove that certain numbers (occurring as constants in analysis) are irrational is most often an impossible challenge. However to construct irrational (even transcendental) numbers is easy.

Irrationality criteria

A real number is rational if and only if its binary (or decimal, or in any basis $b \geq 2$) expansion is *ultimately periodic*.

Also a real number is rational if and only if its continued fraction expansion is finite.

Consequence : it should not be so difficult to decide whether a given number is rational or not.

To prove that certain numbers (occurring as constants in analysis) are irrational is most often an impossible challenge. However to construct irrational (even transcendental) numbers is easy.

Irrationality criteria

A real number is rational if and only if its binary (or decimal, or in any basis $b \geq 2$) expansion is *ultimately periodic*.

Also a real number is rational if and only if its continued fraction expansion is finite.

Consequence : it should not be so difficult to decide whether a given number is rational or not.

To prove that certain numbers (occurring as constants in analysis) are irrational is most often an impossible challenge. However to construct irrational (even transcendental) numbers is easy.

First decimals of $\sqrt{2}$

http://wims.unice.fr/wims/wims.cgi

1.41421356237309504880168872420969807856967187537694807317667973
7999073247846210703885038753432764157273501384623091229702492483
605585073721264412149709993583141322266592750559275579995050115
2782060571470109559971605970274534596862014728517418640889198 60
9552329230484308714321450839762603627995251407989687253396546 33
1808829640620615258352395054745750287759961729835575220337531 85
7011354374603408498847160386899970699004815030544027790316454 24
7823068492936918621580578463111596668713013015618568987237235 28
8509264861249497715421833420428568606014682472077143585487415 56
5706967765372022648544701585880162075847492265722600208558446 65
2145839889394437092659180031138824646815708263010059485870400 31
8648034219489727829064104507263688131373985525611732204024509 12
2770022694112757362728049573810896750401836986836845072579936 47
2906076299694138047565482372899718032680247442062926912485905 21
8100445984215059112024944134172853147810580360337107730918286 93
1471017111168391658172688941975871658215212822951848847 ...

First binary digits of $\sqrt{2}$

http://wims.unice.fr/wims/wims.cgi

1.011010100000100111100110011001111111001110111100110010010000
1000101100101111101100010011011001101110101001010111110100
1111100011101011011110110000010111010100010010011101110101 0000
1001100111011010001011110101100100000101100000110011001110 01100
1000101010100101011111100100000110000010000111010101110001 0100
0101100001110101000101100011111111001101111110111001000001 1110
1101100111001000001111011110100101010000101111001000001110 0111000
1111011010010100111100000000010010000111001101100011110111 11101
0001001110110100011010010001000000001011101000011101000010 10101
1110001111101001110010100110000010110011100011000000000100 01101
1110000110011011111011110010101011000110111100100100010001 01101
0001000001000101100010100100011000000101010111100011100100 010111
1011111000100111000110011110001101101010110101000101000111 0001
0111011011111110100111011100110010110010101001100011010000 11001
1000111111001111100100001001101111110101001011110001001000 0011111
0000011011011100101100000010111011110101010100100101000000 1000100
1100100000001000000011001010010010101000000010011100101001 010 ...

Euler–Mascheroni constant

Euler's Constant is

$$\gamma = \lim_{n\to\infty}\left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}-\log n\right)$$
$$= 0.577\,215\,664\,901\,532\,860\,606\,512\,090\,082\dots$$

Is–it a rational number ?

$$\gamma = \sum_{k=1}^{\infty}\left(\frac{1}{k}-\log\left(1+\frac{1}{k}\right)\right) = \int_1^{\infty}\left(\frac{1}{[x]}-\frac{1}{x}\right)dx$$
$$= -\int_0^1\int_0^1 \frac{(1-x)dxdy}{(1-xy)\log(xy)}.$$

Euler–Mascheroni constant

Euler's Constant is

$$\gamma = \lim_{n\to\infty}\left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}-\log n\right)$$
$$= 0.577\,215\,664\,901\,532\,860\,606\,512\,090\,082\ldots$$

Is–it a rational number ?

$$\gamma = \sum_{k=1}^{\infty}\left(\frac{1}{k}-\log\left(1+\frac{1}{k}\right)\right) = \int_1^{\infty}\left(\frac{1}{[x]}-\frac{1}{x}\right)dx$$
$$= -\int_0^1\int_0^1 \frac{(1-x)dxdy}{(1-xy)\log(xy)}\cdot$$

Riemann zeta function

The function

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$$

was studied by Euler (1707– 1783)
for integer values of s
and by Riemann (1859) for complex values of s.

Euler : for any even integer value of $s \geq 2$, the number $\zeta(s)$ is a rational multiple of π^s.

Examples : $\zeta(2) = \pi^2/6$, $\zeta(4) = \pi^4/90$, $\zeta(6) = \pi^6/945$, $\zeta(8) = \pi^8/9450 \cdots$

Coefficients : Bernoulli numbers.

Riemann zeta function

The function

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$$

was studied by Euler (1707– 1783)
for integer values of s
and by Riemann (1859) for complex values of s.

Euler : for any even integer value of $s \geq 2$, the number $\zeta(s)$ is a rational multiple of π^s.

Examples : $\zeta(2) = \pi^2/6$, $\zeta(4) = \pi^4/90$, $\zeta(6) = \pi^6/945$, $\zeta(8) = \pi^8/9450 \cdots$

Coefficients : Bernoulli numbers.

Riemann zeta function

The function
$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$$
was studied by Euler (1707– 1783)
for integer values of s
and by Riemann (1859) for complex values of s.

Euler : for any even integer value of $s \geq 2$, the number $\zeta(s)$ is a rational multiple of π^s.

Examples : $\zeta(2) = \pi^2/6$, $\zeta(4) = \pi^4/90$, $\zeta(6) = \pi^6/945$,
$\zeta(8) = \pi^8/9450 \cdots$

Coefficients : Bernoulli numbers.

Riemann zeta function

The function

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}$$

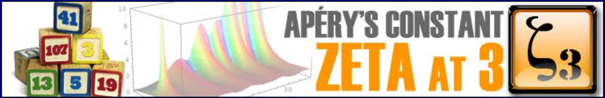
was studied by Euler (1707– 1783)
for integer values of s
and by Riemann (1859) for complex values of s.

Euler : for any even integer value of $s \geq 2$, the number $\zeta(s)$ is a rational multiple of π^s.

Examples : $\zeta(2) = \pi^2/6$, $\zeta(4) = \pi^4/90$, $\zeta(6) = \pi^6/945$, $\zeta(8) = \pi^8/9450 \cdots$

Coefficients : Bernoulli numbers.

Riemann zeta function



The number

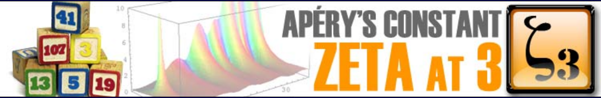
$$\zeta(3) = \sum_{n\geq 1} \frac{1}{n^3} = 1,202\,056\,903\,159\,594\,285\,399\,738\,161\,511\,\ldots$$

is irrational *(Apéry 1978)*.

Recall that $\zeta(s)/\pi^s$ is rational for any even value of $s \geq 2$.

Open question : Is the number $\zeta(3)/\pi^3$ irrational ?

Riemann zeta function



The number

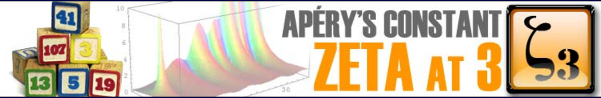
$$\zeta(3) = \sum_{n \geq 1} \frac{1}{n^3} = 1,202\,056\,903\,159\,594\,285\,399\,738\,161\,511\,\ldots$$

is irrational *(Apéry 1978)*.

Recall that $\zeta(s)/\pi^s$ is rational for any even value of $s \geq 2$.

Open question : Is the number $\zeta(3)/\pi^3$ irrational ?

Riemann zeta function



The number

$$\zeta(3) = \sum_{n \geq 1} \frac{1}{n^3} = 1,202\,056\,903\,159\,594\,285\,399\,738\,161\,511\,\ldots$$

is irrational *(Apéry 1978)*.

Recall that $\zeta(s)/\pi^s$ is rational for any even value of $s \geq 2$.

Open question : Is the number $\zeta(3)/\pi^3$ irrational ?

Riemann zeta function

Is the number

$$\zeta(5) = \sum_{n\geq 1} \frac{1}{n^5} = 1.036\,927\,755\,143\,369\,926\,331\,365\,486\,457\ldots$$

irrational ?

T. Rivoal (2000) : infinitely many $\zeta(2n+1)$ are irrational.

Riemann zeta function

Is the number

$$\zeta(5) = \sum_{n\geq 1} \frac{1}{n^5} = 1.036\,927\,755\,143\,369\,926\,331\,365\,486\,457\ldots$$

irrational ?

T. Rivoal (2000) : infinitely many $\zeta(2n+1)$ are irrational.

Motivations

- Squaring the circle
- Dynamical systems
- Solving Diophantine equations
- Theoretical computer sciences : rounding values
- Main goal : to understand the underlying theory.

Motivations

- Squaring the circle
- Dynamical systems
- Solving Diophantine equations
- Theoretical computer sciences : rounding values
- Main goal : to understand the underlying theory.

Motivations

- Squaring the circle
- Dynamical systems
- Solving Diophantine equations
- Theoretical computer sciences : rounding values
- Main goal : to understand the underlying theory.

Motivations

- Squaring the circle
- Dynamical systems
- Solving Diophantine equations
- Theoretical computer sciences : rounding values
- Main goal : to understand the underlying theory.

Motivations

- Squaring the circle
- Dynamical systems
- Solving Diophantine equations
- Theoretical computer sciences : rounding values
- Main goal : to understand the underlying theory.

Known results

Irrationality of the number π :

Āryabhaṭa, b. 476 AD : $\pi \sim 3.1416$.

Nīlakaṇṭha Somayājī, b. 1444 AD : *Why then has an approximate value been mentioned here leaving behind the actual value ? Because it (exact value) cannot be expressed.*

K. Ramasubramanian, *The Notion of Proof in Indian Science*, 13th World Sanskrit Conference, 2006.

Known results

Irrationality of the number π :

Āryabhaṭa, b. 476 AD : $\pi \sim 3.1416$.

Nīlakaṇṭha Somayājī, b. 1444 AD : *Why then has an approximate value been mentioned here leaving behind the actual value ? Because it (exact value) cannot be expressed.*

K. Ramasubramanian, *The Notion of Proof in Indian Science*, 13th World Sanskrit Conference, 2006.

Known results

Irrationality of the number π :

Āryabhaṭa, b. 476 AD : $\pi \sim 3.1416.$

Nīlakaṇṭha Somayājī, b. 1444 AD : *Why then has an approximate value been mentioned here leaving behind the actual value ? Because it (exact value) cannot be expressed.*

K. Ramasubramanian, *The Notion of Proof in Indian Science*, 13th World Sanskrit Conference, 2006.

Known results

Irrationality of the number π :

Āryabhaṭa, b. 476 AD : $\pi \sim 3.1416$.

Nīlakaṇṭha Somayājī, b. 1444 AD : *Why then has an approximate value been mentioned here leaving behind the actual value ? Because it (exact value) cannot be expressed.*

K. Ramasubramanian, *The Notion of Proof in Indian Science*, 13th World Sanskrit Conference, 2006.

Known results

Irrationality of the number π :

Āryabhaṭa, b. 476 AD : $\pi \sim 3.1416$.

Nīlakaṇṭha Somayājī, b. 1444 AD : *Why then has an approximate value been mentioned here leaving behind the actual value ? Because it (exact value) cannot be expressed.*

K. Ramasubramanian, *The Notion of Proof in Indian Science*, 13th World Sanskrit Conference, 2006.

Irrationality of π

Johann Heinrich Lambert (1728 - 1777)
Mémoire sur quelques propriétés remarquables des quantités transcendantes circulaires et logarithmiques,
Mémoires de l'Académie des Sciences de Berlin, **17** (1761), p. 265-322 ;
read in 1767 ; Math. Werke, t. II.

$\tan(v)$ is irrational for any rational value of $v \neq 0$
and $\tan(\pi/4) = 1$.

Irrationality of π

Johann Heinrich Lambert (1728 - 1777)
Mémoire sur quelques propriétés remarquables des quantités transcendantes circulaires et logarithmiques,
Mémoires de l'Académie des Sciences de Berlin, **17** (1761), p. 265-322 ;
read in 1767 ; Math. Werke, t. II.

$\tan(v)$ is irrational for any rational value of $v \neq 0$
and $\tan(\pi/4) = 1$.

Lambert and Frederick II, King of Prussia

— Que savez vous, Lambert ?
— Tout, Sire.
— Et de qui le tenez–vous ?
— De moi-même !

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 expansion.

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.

Irrationality of e, following J. Fourier

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

Multiply by $N!$:

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

Set

$$B_N = N!, \qquad A_N = \sum_{n=0}^{N} \frac{N!}{n!}, \quad R_N = \sum_{m \geq N+1} \frac{N!}{m!},$$

so that

$$B_N e = A_N + R_N.$$

Irrationality of e, following J. Fourier

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

Multiply by $N!$:

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

Set

$$B_N = N!, \qquad A_N = \sum_{n=0}^{N} \frac{N!}{n!}, \quad R_N = \sum_{m \geq N+1} \frac{N!}{m!},$$

so that

$$B_N e = A_N + R_N.$$

Irrationality of e, following J. Fourier

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

Multiply by $N!$:

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

Set

$$B_N = N!, \qquad A_N = \sum_{n=0}^{N} \frac{N!}{n!}, \quad R_N = \sum_{m \geq N+1} \frac{N!}{m!},$$

so that

$$B_N e = A_N + R_N.$$

Irrationality of e, following J. Fourier

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

$$0 < R_N = \frac{1}{N+1} + \frac{1}{(N+1)(N+2)} + \cdots < \frac{e}{N+1}.$$

In the formula

$$B_N e - A_N = R_N,$$

the numbers A_N and $B_N = N!$ are integers, while the right hand side is > 0 and tends to 0 when N tends to infinity. Hence $N!\, e$ is not an integer, therefore e is irrational.

Irrationality of e, following J. Fourier

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

$$0 < R_N = \frac{1}{N+1} + \frac{1}{(N+1)(N+2)} + \cdots < \frac{e}{N+1}.$$

In the formula

$$B_N e - A_N = R_N,$$

the numbers A_N and $B_N = N!$ are integers, while the right hand side is > 0 and tends to 0 when N tends to infinity.
Hence $N!\ e$ is not an integer, therefore e is irrational.

Irrationality of e, following J. Fourier

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

$$0 < R_N = \frac{1}{N+1} + \frac{1}{(N+1)(N+2)} + \cdots < \frac{e}{N+1}.$$

In the formula

$$B_N e - A_N = R_N,$$

the numbers A_N and $B_N = N!$ are integers, while the right hand side is > 0 and tends to 0 when N tends to infinity. Hence $N!\, e$ is not an integer, therefore e is irrational.

C.L Siegel (1949) : irrationality of e^{-1}

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

C.L. Siegel (1896 – 1981)

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.

e is not a quadratic irrationality (Liouville, 1840)

Write the quadratic equation as $ae + b + ce^{-1} = 0$.

$$bN! + \sum_{n=0}^{N} (a + (-1)^n c) \frac{N!}{n!}$$
$$= - \sum_{k \geq 0} \left(a + (-1)^{N+1+k} c\right) \cdot \frac{N!}{(N+1+k)!}.$$

Using Fourier's argument, we deduce that the LHS and RHS are 0 for any sufficiently large N.

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 $\vartheta \in \mathbb{R}$. 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.

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*

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

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

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*

$$L_0(X_0, X_1) = a_0X_0 + b_0X_1 \quad \textit{and} \quad L_1(X_0, X_1) = a_1X_0 + b_1X_1,$$

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*

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

(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*

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

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) $\Longleftrightarrow$ (ii)'

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

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

(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*

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

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 $|q\vartheta - p|$.

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*

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

(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*

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

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

Linear independence of $1, \vartheta_1, \dots, \vartheta_m$ 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 $(1, \vartheta_1, \dots, \vartheta_m)$ does not belong to H.

Transcendence of ϑ : means that $1, \vartheta, \vartheta^2, \dots, \vartheta^n \dots$ 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 $1 \leq k \leq m$, 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)

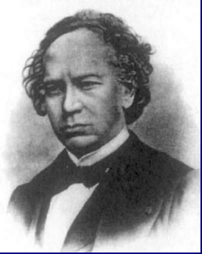
Let $(\vartheta_1, \ldots, \vartheta_m) \in \mathbf{R}^m$.
Then the following conditions are equivalent.
(i) *The numbers* $1, \vartheta_1, \ldots, \vartheta_m$ *are linearly independent over* $\mathbf{Q}$.
(ii) *For any* $\epsilon > 0$, *there exist* $m+1$ *linearly independent elements* $\mathbf{u}_0,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

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

with $q_i > 0$, *such that*

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

Hermite – Lindemann Theorem



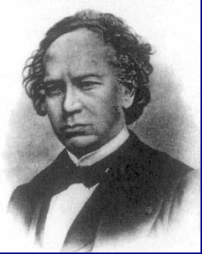
Hermite (1873) :
transcendence of e.

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



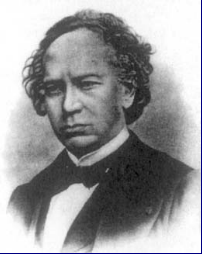
Hermite (1873) :
transcendence of e.

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



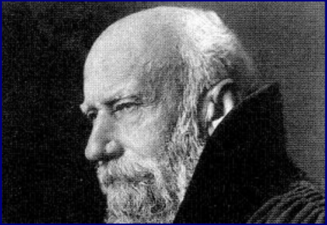
Hermite (1873) :
transcendence of e.

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 (1888)

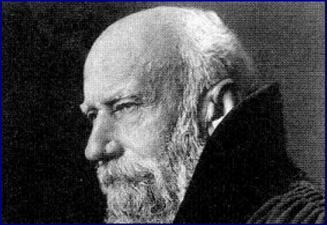


Let $\beta_1, \ldots, \beta_n$ be algebraic numbers which are linearly independent over $\mathbf{Q}$. Then the numbers $e^{\beta_1}, \ldots, e^{\beta_n}$ are algebraically independent over $\mathbf{Q}$.

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 (1888)



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 $1, \vartheta_1, \ldots, \vartheta_m$ 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.

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.

Criterion of Yu. V. Nesterenko

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

Yu.V.Nesterenko (1985)

Let m be a positive integer and α a positive real number satisfying $\alpha > m - 1$. 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 $\leq e^n$ 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 (2008).

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.*
Math. Annalen, to appear. Preprint MPIM 2009-35.

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.

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.

Amarisa Chantanasiri

Criteria for linear independence, transcendence and algebraic independence

Université P. et M. Curie (Paris VI), Ph.D. 2011 ?

New criterion for algebraic independence

Let $\vartheta_1, \ldots, \vartheta_m$ be real numbers and $(\tau_d)_{d\geq 1}$, $(\eta_d)_{d\geq 1}$ two sequences of positive real numbers satisfying

$$\frac{\tau_d}{d^{m-1}(1+\eta_d)} \longrightarrow +\infty.$$

Assume that for all sufficiently large d, there is a sequence $(P_n)_{n\geq n_0(d)}$ of polynomials in $\mathbf{Z}[X_1, \ldots, X_m]$, where P_n has degree $\leq d$ and height $\leq e^n$, such that

$$e^{-(\tau_d+\eta_d)n} \leq |P_n(\vartheta_1, \ldots, \vartheta_m)| \leq e^{-\tau_d n}.$$

Then $\vartheta_1, \ldots, \vartheta_m$ are algebraically independent.

Mahidol University, Bangkok October 29-31, 2009

Franco-Thai Seminar in Pure and Applied Mathematics,

http://www.sc.mahidol.ac.th/cem/franco_thai/

Criteria for linear independence and transcendence, following Yuri Nesterenko, Stéphane Fischler, Wadim Zudilin and Amarisa Chantanasiri

Michel Waldschmidt

Institut de Mathématiques de Jussieu & Paris VI

http://www.math.jussieu.fr/∼miw/

Lecture given on October 31, 2009.