Nombres transcendants

Antoine Chambert-Loir

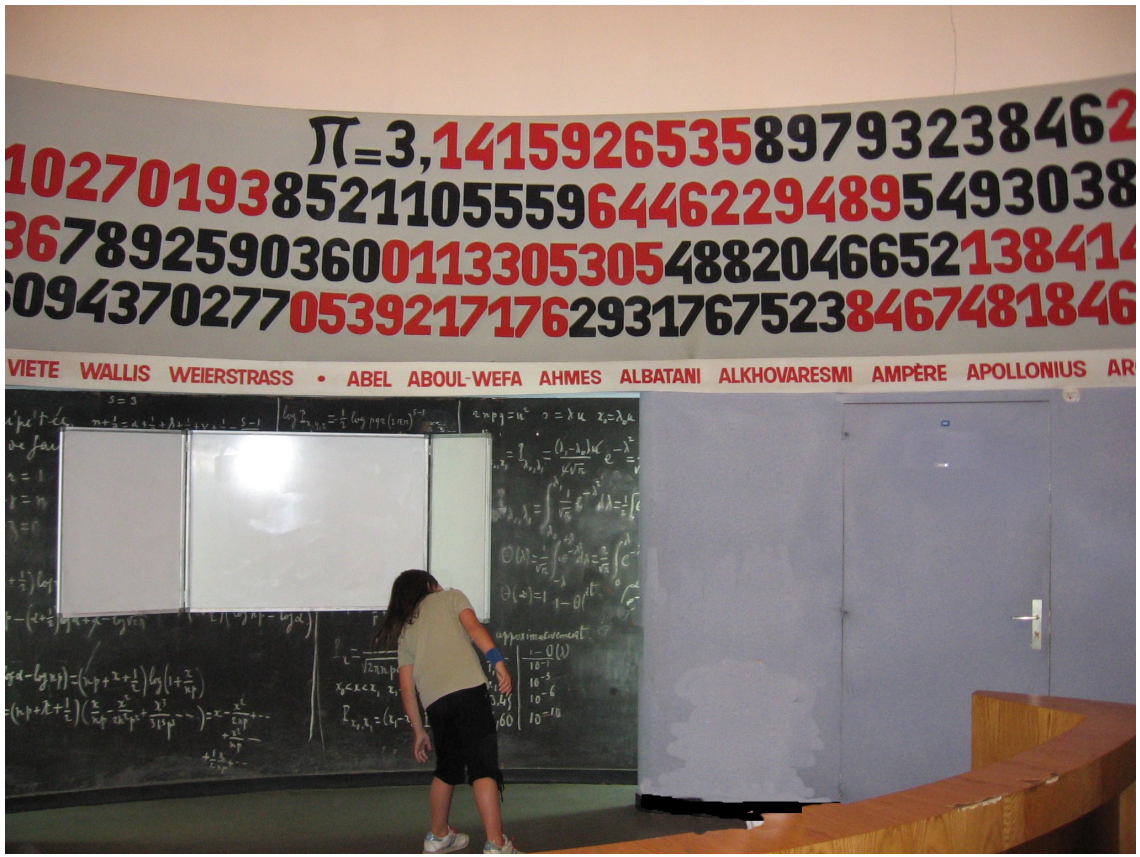
Institut de recherche mathématique de Rennes, Université de Rennes 1

Mathematic Park à Chateaubriand
15 novembre 2011

La surface du cercle

On sait aujourd'hui que la surface S d'un cercle de rayon r est πr^2, où π est une constante fondamentale :

$$\pi \simeq 3{,}141\,592\,653\,589\,793\,238\,462\,643\,383\,279\,502\,884\ldots$$



Gimme a slice of π !

La surface du cercle, dans l'Antiquité

Bible (Livre des Rois, **7** 23) : « Il fit la mer de fonte. Elle avait dix coudées d'un bord à l'autre, une forme entièrement ronde, cinq coudées de hauteur, et une circonférence que mesurait un cordon de trente coudées. »

Papyrus Rhind (1800 av. J.C.) : $\pi \sim \frac{256}{81} \simeq 3{,}16$

Archimède (250 av. J.C.) : $3 + \frac{10}{71} < \pi < 3 + \frac{1}{7}$

Meilleure approximation : $\frac{1351}{390} < \pi < \frac{530}{153}$

La surface du cercle, dans l'Antiquité

Bible (Livre des Rois, **7** 23) : « Il fit la mer de fonte. Elle avait dix coudées d'un bord à l'autre, une forme entièrement ronde, cinq coudées de hauteur, et une circonférence que mesurait un cordon de trente coudées. »

Papyrus Rhind (1800 av. J.C.) : $\pi \sim \frac{256}{81} \simeq 3{,}16$

Archimède (250 av. J.C.) : $3 + \frac{10}{71} < \pi < 3 + \frac{1}{7}$

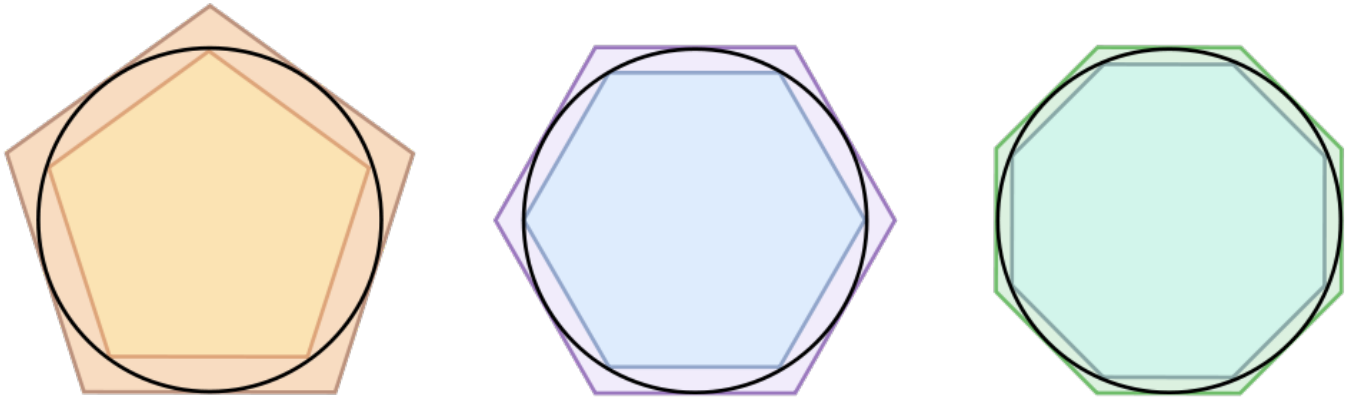
Meilleure approximation : $\frac{1351}{390} < \pi < \frac{530}{153}$

La surface du cercle, dans l'Antiquité

Bible (Livre des Rois, **7** 23) : « Il fit la mer de fonte. Elle avait dix coudées d'un bord à l'autre, une forme entièrement ronde, cinq coudées de hauteur, et une circonférence que mesurait un cordon de trente coudées. »

Papyrus Rhind (1800 av. J.C.) : $\pi \sim \frac{256}{81} \simeq 3{,}16$

Archimède (250 av. J.C.) : $3 + \frac{10}{71} < \pi < 3 + \frac{1}{7}$



Meilleure approximation : $\frac{1351}{390} < \pi < \frac{530}{153}$

La quadrature du cercle

Pour les Grecs, les nombres n'avaient pas le statut qu'ils ont aujourd'hui : seuls existaient des rapports de longueurs, des rapports de surfaces.
Au V^{e} siècle av. J.C., apparaît le problème de **construction** géométrique d'un carré ayant même aire qu'un cercle de rayon unité : c'est la **quadrature du cercle**, ou, en grec : ὸ τετραγωνισμός.

Rectifications et quadratures

Pour les Grecs, une surface était mesurée si l'on montrait qu'elle était équivalente à une surface formée de petits carrés. Le mot « quadrature » signifie donc **mesurer une surface**.
Hippocrate a pu quarrer des **lunules**, zone délimitée par certains arcs de cercle.

Dans le même genre : « rectifier », rendre droite, signifie mesurer une longueur — la rectification des ellipses sera un sujet fondamental des mathématiciens du XIX^{e} siècle.

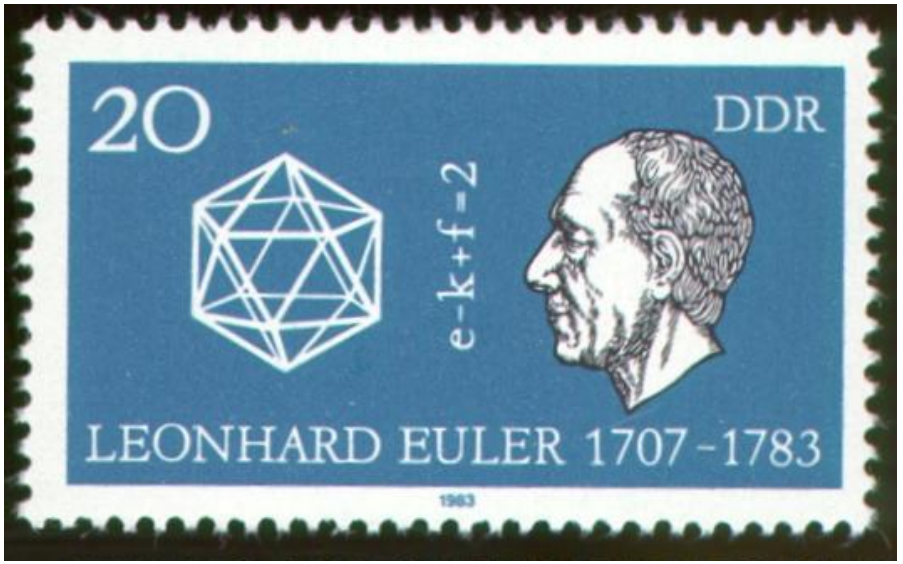
Mais tout ceci ne prendra sa figure moderne qu'avec l'invention du **calcul infinitésimal** par Newton et Leibniz au XVII^{e} siècle, le développement de l'analyse (Cauchy, Heine, Weierstrass) au XIX^{e} siècle, l'intégrale de Lebesgue (XX^{e} siècle).

Irrationalité de e

1737. Leonhard **Euler** prouve que e est irrationnel.

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

$$e^{i\pi} + 1 = 0$$



Irrationalité de e

le nombre e, base des logarithmes néperiens, est donné comme somme de la série infinie

$$1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \ldots$$

Irrationalité de e

le nombre e, base des logarithmes néperiens, est donné comme somme de la série infinie

$$1 + \frac{1}{1} + \frac{1}{1 \cdot 2} + \frac{1}{1 \cdot 2 \cdot 3} + \frac{1}{1 \cdot 2 \cdot 3 \cdot 4} + \ldots$$

Irrationalité de e

le nombre e, base des logarithmes néperiens, est donné comme somme de la série infinie

$$1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \ldots$$

Irrationalité de e

le nombre e, base des logarithmes néperiens, est donné comme somme de la série infinie

$$1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \ldots + \frac{1}{n!} + \ldots$$

Irrationalité de e

le nombre e, base des logarithmes néperiens, est donné comme somme de la série infinie

$$1+\frac{1}{1!}+\frac{1}{2!}+\frac{1}{3!}+\frac{1}{4!}+\ldots+\frac{1}{n!}+\ldots$$

La somme des n premiers termes est de la forme $A/n!$, où $A=n!+\frac{n!}{2}+\cdots+n+1$ est un entier.
De plus,

$$\frac{A}{n!}<e<\frac{A}{n!}+\frac{R}{(n+1)!}$$

avec

$$R=1+\frac{1}{(n+2)}+\frac{1}{(n+2)(n+3)}+\ldots$$
$$<1+\frac{1}{2}+\frac{1}{3!}+\ldots \qquad <e.$$

Irrationalité de e (fin)

Conclusion :

$$A < n!e < A + \frac{e}{n+1}.$$

Supposons **par l'absurde** que $e = p/q$ et prenons $n \geqslant \max(q, 2)$.
Alors, $n!e$ est un nombre entier, de même que A. Mais comme $e \approx 2{,}718 < 3 \leqslant n+1$, il n'y a pas de nombre entier entre A et $A + e/(n+1)$. **Contradiction.**

Slogan : e est très bien approché par la somme des n premiers termes de la série d'Euler. Mais un nombre rationnel est très mal approché par un autre nombre rationnel (sauf par lui-même).

Irrationalité de e (fin)

Conclusion :

$$A < n!e < A + \frac{e}{n+1}.$$

Supposons **par l'absurde** que $e = p/q$ et prenons $n \geqslant \max(q, 2)$.
Alors, $n!e$ est un nombre entier, de même que A. Mais comme $e \approx 2{,}718 < 3 \leqslant n+1$, il n'y a pas de nombre entier entre A et $A + e/(n+1)$. **Contradiction.**

Slogan : e est très bien approché par la somme des n premiers termes de la série d'Euler. Mais un nombre rationnel est très mal approché par un autre nombre rationnel (sauf par lui-même).

Irrationalité de e (fin)

Conclusion :

$$A < n!e < A + \frac{e}{n+1}.$$

Supposons **par l'absurde** que $e = p/q$ et prenons $n \geqslant \max(q, 2)$.
Alors, $n!e$ est un nombre entier, de même que A. Mais comme $e \approx 2{,}718 < 3 \leqslant n+1$, il n'y a pas de nombre entier entre A et $A + e/(n+1)$. **Contradiction.**

Slogan : e est très bien approché par la somme des n premiers termes de la série d'Euler. Mais un nombre rationnel est très mal approché par un autre nombre rationnel (sauf par lui-même).

Irrationalité et transcendance de π

1768. Johann Heinrich **Lambert** prouve que π est irrationnel et conjecture qu'il est transcendant : **il n'est racine d'aucun polynôme non nul à coefficients entiers**.

1837. Pierre-Laurent **Wantzel** établit une propriété des nombres que l'on peut construire à la règle et au compas. Ils sont tous algébriques (racine d'un polynôme à coefficients entiers).

La question de la quadrature du cercle serait donc résolue (négativement) si l'on démontrait que π est un nombre transcendant.

Irrationalité et transcendance de π

1768. Johann Heinrich **Lambert** prouve que π est irrationnel et conjecture qu'il est transcendant : **il n'est racine d'aucun polynôme non nul à coefficients entiers**.

1837. Pierre-Laurent **Wantzel** établit une propriété des nombres que l'on peut construire à la règle et au compas. Ils sont tous algébriques (racine d'un polynôme à coefficients entiers).

La question de la quadrature du cercle serait donc résolue (négativement) si l'on démontrait que π est un nombre transcendant.

Irrationalité et transcendance de π

1768. Johann Heinrich **Lambert** prouve que π est irrationnel et conjecture qu'il est transcendant : **il n'est racine d'aucun polynôme non nul à coefficients entiers**.

1837. Pierre-Laurent **Wantzel** établit une propriété des nombres que l'on peut construire à la règle et au compas. Ils sont tous algébriques (racine d'un polynôme à coefficients entiers).

La question de la quadrature du cercle serait donc résolue (négativement) si l'on démontrait que π est un nombre transcendant.

Nombres rationnels, algébriques transcendants

Récapitulons : Un nombre (réel ou complexe) est

- **rationnel** : si c'est le quotient de deux nombres entiers (exemples : 2/3, 22/7,...)
- **algébrique** : s'il est racine d'un polynôme à coefficients entiers (exemples : $\sqrt{2}$, $\sqrt{7-\sqrt{2}}$,...)
- **transcendant** : sinon.

Les nombres rationnels sont stables par addition, soustraction, multiplication, quotient : c'est le calcul usuel des fractions. On dit qu'ils forment un **corps**.

Nombres rationnels, algébriques transcendants

Récapitulons : Un nombre (réel ou complexe) est

- **rationnel** : si c'est le quotient de deux nombres entiers (exemples : 2/3, 22/7,...)
- **algébrique** : s'il est racine d'un polynôme à coefficients entiers (exemples : $\sqrt{2}$, $\sqrt{7-\sqrt{2}}$,...)
- **transcendant** : sinon.

Les nombres rationnels sont stables par addition, soustraction, multiplication, quotient : c'est le calcul usuel des fractions. On dit qu'ils forment un **corps**.

Il en est de même des nombres algébriques, mais c'est plus délicat.

Nombres rationnels, algébriques transcendants

Récapitulons : Un nombre (réel ou complexe) est

- **rationnel** : si c'est le quotient de deux nombres entiers (exemples : 2/3, 22/7,...)
- **algébrique** : s'il est racine d'un polynôme à coefficients entiers (exemples : $\sqrt{2}$, $\sqrt{7-\sqrt{2}}$,...)
- **transcendant** : sinon.

Les nombres rationnels sont stables par addition, soustraction, multiplication, quotient : c'est le calcul usuel des fractions. On dit qu'ils forment un **corps**.

Il en est de même des nombres algébriques, mais c'est plus délicat.

Les premiers nombres transcendants

1844. Joseph **Liouville** construit les premiers **nombres transcendants**.

Par exemple : $L = \sum 10^{-n!}$.

La série ci-dessus converge extrêmement vite donc la somme des n premiers termes approche vraiment très bien la somme de la série infinie.

Si $S = \sum_{m=0}^{n} 10^{-m!}$, on a $S = A/10^{n!}$, avec A entier, et

$$0 < L - \frac{A}{10^{n!}} < \frac{1}{10^{(n+1)!}} + \cdots \lessapprox \left(\frac{1}{10^{n!}}\right)^{n+1}$$

Nombres de Liouville

Slogan : Un nombre algébrique n'est pas trop bien approché par un nombre rationnel.

Inégalité de Liouville : si un irrationnel α est racine d'un polynôme à coefficients entiers de degré d, alors

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

Preuve

Un nombre α est appelé **nombre de Liouville** s'il existe pour tout entier n un nombre rationnel p/q tel que

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}.$$

Les nombres de Liouville sont donc transcendants, mais tous les nombres transcendants ne sont pas des nombres de Liouville...

Nombres de Liouville

Slogan : Un nombre algébrique n'est pas trop bien approché par un nombre rationnel.

Inégalité de Liouville : si un irrationnel α est racine d'un polynôme à coefficients entiers de degré d, alors

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

▸ Preuve

Un nombre α est appelé **nombre de Liouville** s'il existe pour tout entier n un nombre rationnel p/q tel que

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}.$$

Les nombres de Liouville sont donc transcendants, mais tous les nombres transcendants ne sont pas des nombres de Liouville...

Nombres de Liouville

Slogan : Un nombre algébrique n'est pas trop bien approché par un nombre rationnel.

Inégalité de Liouville : si un irrationnel α est racine d'un polynôme à coefficients entiers de degré d, alors

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

▸ Preuve

Un nombre α est appelé **nombre de Liouville** s'il existe pour tout entier n un nombre rationnel p/q tel que

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}.$$

Les nombres de Liouville sont donc transcendants, mais tous les nombres transcendants ne sont pas des nombres de Liouville...

Nombres de Liouville

Slogan : Un nombre algébrique n'est pas trop bien approché par un nombre rationnel.

Inégalité de Liouville : si un irrationnel α est racine d'un polynôme à coefficients entiers de degré d, alors

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

▸ Preuve

Un nombre α est appelé **nombre de Liouville** s'il existe pour tout entier n un nombre rationnel p/q tel que

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}.$$

Les nombres de Liouville sont donc transcendants, mais tous les nombres transcendants ne sont pas des nombres de Liouville...

La sublime décennie

- **1873. Hermite** : *e* est transcendant. ▸ Preuve
- **1874. Cantor** prouve que l'ensemble des nombres transcendants est non dénombrable, mais que celui des nombres algébriques est dénombrable.
- **1882. Lindemann** : π est transcendant.

Le théorème de Lindemann-Weierstrass (1885)

Théorème

Soit $a_1, \ldots, a_n$, des nombres algébriques non tous nuls.
Soit $b_1, \ldots, b_n$ sont des nombres algébriques deux à deux distincts.
Alors $a_1 e^{b_1} + \cdots + a_n e^{b_n} \neq 0$.

Reformulation : Les exponentielles des nombres algébriques sont linéairement indépendantes sur le corps des nombres algébriques.

Le théorème de Lindemann-Weierstrass (1885)

Théorème

Soit $a_1, \ldots, a_n$, des nombres algébriques non tous nuls.
Soit $b_1, \ldots, b_n$ sont des nombres algébriques deux à deux distincts.
Alors $a_1 e^{b_1} + \cdots + a_n e^{b_n} \neq 0$.

Reformulation : Les exponentielles des nombres algébriques sont linéairement indépendantes sur le corps des nombres algébriques.

Le théorème de Gel'fond-Schneider

En 1900, David **Hilbert** pose 23 problèmes à la communauté mathématique.
Le 7^{e} demande de prouver que si a et b sont des nombres algébriques, $a \notin \{0, 1\}$, b irrationnel, alors a^b est transcendant.

Exemple $\sqrt{2}^{\sqrt{2}}$.

Il est résolu en 1934 par **Gelfond** et **Schneider**, indépendamment.

Le théorème de Gel'fond-Schneider

En 1900, David **Hilbert** pose 23 problèmes à la communauté mathématique.
Le 7^{e} demande de prouver que si a et b sont des nombres algébriques, $a \notin \{0, 1\}$, b irrationnel, alors a^b est transcendant.

Exemple $\sqrt{2}^{\sqrt{2}}$.

Il est résolu en 1934 par **Gelfond** et **Schneider**, indépendamment.

Formes linéaires de logarithmes

Reformulation du théorème de Gelfond-Schneider

Si u et v sont des logarithmes de nombres algébriques, linéairement indépendant sur $\mathbf{Q}$, ils sont linéairement indépendants sur $\bar{\mathbf{Q}}$.

(Sinon : $u = av$, $a \notin \mathbf{Q}$, $e^u = (e^v)^a$ est algébrique.)

Théorème (Baker, 1967–69)

Si $u_1, \ldots, u_n$ sont des logarithmes de nombres algébriques, $a_0, a_1, \ldots, a_n$ des nombres algébriques non tous nuls. Alors $a_0 + a_1 u_1 + \cdots + a_n u_n \neq 0$.

Formes linéaires de logarithmes

Le théorème de Baker a énormément de conséquences et Alan **Baker** a eu la médaille Fields en 1970 pour ce résultat.
Par exemple ($u_1 = i\pi = \log(-1)$, $u_2 = 2$) :

$$\int_0^1 \frac{dx}{1+x^3} = \frac{\pi}{3\sqrt{3}} + \frac{1}{2}\log 2$$

est transcendant.

Il y a des « versions quantitatives » (aussi dues à Baker) et elles sont très utiles en théorie des nombres.

Conjecture de Schanuel

Conjecture (1960)

Soit $a_1, \ldots, a_n$ des nombres complexes linéairement indépendants sur $\mathbf{Q}$.
Alors parmi $a_1, \ldots, a_n, e^{a_1}, \ldots, e^{a_n}$, on peut trouver n nombres, disons $u_1, \ldots, u_n$ qui sont algébriquement indépendants : si P est un polynôme non nul, à coefficients dans $\mathbf{Q}$, $P(u_1, \ldots, u_n) \neq 0$.

Par exemple e, π, e^π, e^e, $\log 2$, $2^{\sqrt{2}}$ doivent être algébriquement indépendants.
... On n'en sait (presque) rien !

Théorème (Nesterenko, 1997)

π et e^π sont algébriquement indépendants.

Démonstration de l'inégalité de Liouville

$P = c_d X^d + \cdots + c_0$ polynôme à coefficients entiers de degré d

$\alpha = \alpha_1, \ldots, \alpha_d$ les racines de P, de sorte que
$P = c_d(X - \alpha)(X - \alpha_2)\ldots(X - \alpha_d)$.
Soit p/q une approximation rationnelle de α (avec $q \geqslant 1$).
On voit que $q^d P(p/q)$ est un entier **non nul**
Donc $|P(p/q)| \geqslant 1/q^d$.

Par ailleurs, pour p/q proche de α

$$P(p/q) = P(p/q) - P(\alpha) \approx \left(\frac{p}{q} - \alpha\right) P'(\alpha)$$

et $P'(\alpha) \neq 0$ (parce que P est irréductible).
Alors,

$$\left|\alpha - \frac{p}{q}\right| \gtrapprox \frac{1}{|P'(\alpha)|\, q^d}.$$

Retour

Démonstration de l'inégalité de Liouville

$P = c_d X^d + \cdots + c_0$ polynôme à coefficients entiers de degré d

$\alpha = \alpha_1, \ldots, \alpha_d$ les racines de P, de sorte que $P = c_d(X - \alpha)(X - \alpha_2)\ldots(X - \alpha_d)$.

Soit p/q une approximation rationnelle de α (avec $q \geqslant 1$).

On voit que $q^d P(p/q)$ est un entier **non nul**

Donc $|P(p/q)| \geqslant 1/q^d$.

Par ailleurs, pour p/q proche de α

$$P(p/q) = P(p/q) - P(\alpha) \approx \left(\frac{p}{q} - \alpha\right) P'(\alpha)$$

et $P'(\alpha) \neq 0$ (parce que P est irréductible).

Alors,

$$\left|\alpha - \frac{p}{q}\right| \gtrapprox \frac{1}{|P'(\alpha)|\, q^d}.$$

Retour

Démonstration de l'inégalité de Liouville

$P = c_d X^d + \cdots + c_0$ polynôme à coefficients entiers de degré d

$\alpha = \alpha_1, \ldots, \alpha_d$ les racines de P, de sorte que

$P = c_d(X - \alpha)(X - \alpha_2)\ldots(X - \alpha_d)$.

Soit p/q une approximation rationnelle de α (avec $q \geqslant 1$).

On voit que $q^d P(p/q)$ est un entier **non nul**

Donc $|P(p/q)| \geqslant 1/q^d$.

Par ailleurs, pour p/q proche de α

$$P(p/q) = P(p/q) - P(\alpha) \approx \left(\frac{p}{q} - \alpha\right) P'(\alpha)$$

et $P'(\alpha) \neq 0$ (parce que P est irréductible).

Alors,

$$\left|\alpha - \frac{p}{q}\right| \gtrapprox \frac{1}{|P'(\alpha)|\, q^d}.$$

Retour

Démonstration de l'inégalité de Liouville

$P = c_d X^d + \cdots + c_0$ polynôme à coefficients entiers de degré d

$\alpha = \alpha_1, \ldots, \alpha_d$ les racines de P, de sorte que

$P = c_d(X - \alpha)(X - \alpha_2)\ldots(X - \alpha_d)$.

Soit p/q une approximation rationnelle de α (avec $q \geqslant 1$).

On voit que $q^d P(p/q)$ est un entier **non nul**

Donc $|P(p/q)| \geqslant 1/q^d$.

Par ailleurs, pour p/q proche de α

$$P(p/q) = P(p/q) - P(\alpha) \approx \left(\frac{p}{q} - \alpha\right) P'(\alpha)$$

et $P'(\alpha) \neq 0$ (parce que P est irréductible).

Alors,

$$\left|\alpha - \frac{p}{q}\right| \gtrapprox \frac{1}{|P'(\alpha)|\, q^d}.$$

Retour

Démonstration de l'inégalité de Liouville

$P = c_d X^d + \cdots + c_0$ polynôme à coefficients entiers de degré d

$\alpha = \alpha_1, \ldots, \alpha_d$ les racines de P, de sorte que

$P = c_d(X - \alpha)(X - \alpha_2)\ldots(X - \alpha_d)$.

Soit p/q une approximation rationnelle de α (avec $q \geqslant 1$).

On voit que $q^d P(p/q)$ est un entier **non nul**

Donc $|P(p/q)| \geqslant 1/q^d$.

Par ailleurs, pour p/q proche de α

$$P(p/q) = P(p/q) - P(\alpha) \approx \left(\frac{p}{q} - \alpha\right) P'(\alpha)$$

et $P'(\alpha) \neq 0$ (parce que P est irréductible).

Alors,

$$\left|\alpha - \frac{p}{q}\right| \gtrapprox \frac{1}{|P'(\alpha)|\, q^d}.$$

Retour

Démonstration de l'inégalité de Liouville

$P = c_d X^d + \cdots + c_0$ polynôme à coefficients entiers de degré d, **irréductible**
$\alpha = \alpha_1, \ldots, \alpha_d$ les racines de P, de sorte que
$P = c_d(X - \alpha)(X - \alpha_2)\ldots(X - \alpha_d)$.
Soit p/q une approximation rationnelle de α (avec $q \geqslant 1$).
On voit que $q^d P(p/q)$ est un entier **non nul**
Donc $|P(p/q)| \geqslant 1/q^d$.

Par ailleurs, pour p/q proche de α

$$P(p/q) = P(p/q) - P(\alpha) \approx \left(\frac{p}{q} - \alpha\right) P'(\alpha)$$

et $P'(\alpha) \neq 0$ (parce que P est irréductible).
Alors,

$$\left|\alpha - \frac{p}{q}\right| \gtrapprox \frac{1}{|P'(\alpha)|\, q^d}.$$

Retour

Démonstration de l'inégalité de Liouville

$P = c_d X^d + \cdots + c_0$ polynôme à coefficients entiers de degré d, **irréductible**
$\alpha = \alpha_1, \ldots, \alpha_d$ les racines de P, de sorte que
$P = c_d(X - \alpha)(X - \alpha_2)\ldots(X - \alpha_d)$.
Soit p/q une approximation rationnelle de α (avec $q \geqslant 1$).
On voit que $q^d P(p/q)$ est un entier **non nul**
Donc $|P(p/q)| \geqslant 1/q^d$.

Par ailleurs, pour p/q proche de α

$$P(p/q) = P(p/q) - P(\alpha) \approx \left(\frac{p}{q} - \alpha\right) P'(\alpha)$$

et $P'(\alpha) \neq 0$ (parce que P est irréductible).
Alors,

$$\left|\alpha - \frac{p}{q}\right| \gtrapprox \frac{1}{|P'(\alpha)|\, q^d}.$$

Retour

Démonstration de l'inégalité de Liouville

$P = c_d X^d + \cdots + c_0$ polynôme à coefficients entiers de degré d, **irréductible**
$\alpha = \alpha_1, \ldots, \alpha_d$ les racines de P, de sorte que
$P = c_d(X - \alpha)(X - \alpha_2)\ldots(X - \alpha_d)$.
Soit p/q une approximation rationnelle de α (avec $q \geqslant 1$).
On voit que $q^d P(p/q)$ est un entier **non nul**
Donc $|P(p/q)| \geqslant 1/q^d$.

Par ailleurs, pour p/q proche de α

$$P(p/q) = P(p/q) - P(\alpha) \approx \left(\frac{p}{q} - \alpha\right) P'(\alpha)$$

et $P'(\alpha) \neq 0$ (parce que P est irréductible).
Alors,

$$\left|\alpha - \frac{p}{q}\right| \gtrapprox \frac{1}{|P'(\alpha)|\, q^d}.$$

Retour

Démonstration de l'inégalité de Liouville

$P = c_d X^d + \cdots + c_0$ polynôme à coefficients entiers de degré d, **irréductible**
$\alpha = \alpha_1, \ldots, \alpha_d$ les racines de P, de sorte que
$P = c_d(X - \alpha)(X - \alpha_2)\ldots(X - \alpha_d)$.
Soit p/q une approximation rationnelle de α (avec $q \geqslant 1$).
On voit que $q^d P(p/q)$ est un entier **non nul**
Donc $|P(p/q)| \geqslant 1/q^d$.

Par ailleurs, pour p/q proche de α

$$P(p/q) = P(p/q) - P(\alpha) \approx \left(\frac{p}{q} - \alpha\right) P'(\alpha)$$

et $P'(\alpha) \neq 0$ (parce que P est irréductible).
Alors,

$$\left|\alpha - \frac{p}{q}\right| \gtrapprox \frac{1}{|P'(\alpha)|\, q^d}.$$

Retour

Transcendance de e, d'après Hilbert

Si f est un polynôme de degré N, on pose

$$I(f,x) = \int_0^1 x e^{x(1-u)} f(xt)\,\mathrm{d}t.$$

Lemme

- $I(f;x) = e^x \sum_{k=0}^{N} f^{(k)}(0) - \sum_{k=0}^{N} f^{(k)}(x)$;
- $|I(f;x)| \leqslant x^{N+1} e^x \, \|f\|_{[0;x]}$;
- Pour tout k, $f^{(k)}(x)/k!$ est un polynôme à coeff. entiers.

Démonstration :

- Intégration par parties
- Majoration de l'intégrande
- Si $f(x) = x^m$,
  $f^{(k)}(x) = m(m-1)\ldots(m-k+1)x^{m-k} = k!\binom{m}{k}x^{m-k}$.

Transcendance de e (2)

On raisonne **par l'absurde** et on suppose qu'il existe des entiers $a_0, \ldots, a_n$, non tous nuls, tels que $a_0 + a_1 e + \cdots + a_n e^n = 0$. On peut supposer $a_0 \neq 0$.

On va prendre $f(x) = x^{p-1}(x-1)^p \ldots (x-n)^p$, où p est un nombre premier, et on pose

$$J_p = a_0 I(f;0) + a_1 I(f;1) + \cdots + a_n I(f;n).$$

Majoration de J_p.
Sur l'intervalle $[0;n]$, $|f(x)| \leqslant (n!)^p$.
Le lemme entraîne que $|J_p| \ll (n!)^p$.

Minoration de J_p.
On va démontrer que lorsque $p > n$ n'est pas multiple de a_0, on a $|J_p| \geqslant (p-1)!$.

Quand p tend vers l'infini, ces deux inégalités sont contradictoires, d'où la transcendance de e.

Transcendance de e (2)

On raisonne **par l'absurde** et on suppose qu'il existe des entiers $a_0, \ldots, a_n$, non tous nuls, tels que $a_0 + a_1 e + \cdots + a_n e^n = 0$. On peut supposer $a_0 \neq 0$.
On va prendre $f(x) = x^{p-1}(x-1)^p \ldots (x-n)^p$, où p est un nombre premier, et on pose

$$J_p = a_0 I(f;0) + a_1 I(f;1) + \cdots + a_n I(f;n).$$

Majoration de J_p.
Sur l'intervalle $[0;n]$, $|f(x)| \leqslant (n!)^p$.
Le lemme entraîne que $|J_p| \ll (n!)^p$.

Minoration de J_p.
On va démontrer que lorsque $p > n$ n'est pas multiple de a_0, on a $|J_p| \geqslant (p-1)!$.

Quand p tend vers l'infini, ces deux inégalités sont contradictoires, d'où la transcendance de e.

Transcendance de e (2)

On raisonne **par l'absurde** et on suppose qu'il existe des entiers $a_0, \ldots, a_n$, non tous nuls, tels que $a_0 + a_1 e + \cdots + a_n e^n = 0$. On peut supposer $a_0 \neq 0$.
On va prendre $f(x) = x^{p-1}(x-1)^p \ldots (x-n)^p$, où p est un nombre premier, et on pose

$$J_p = a_0 I(f;0) + a_1 I(f;1) + \cdots + a_n I(f;n).$$

Majoration de J_p.
Sur l'intervalle $[0;n]$, $|f(x)| \leqslant (n!)^p$.
Le lemme entraîne que $\left|J_p\right| \ll (n!)^p$.

Minoration de J_p.
On va démontrer que lorsque $p > n$ n'est pas multiple de a_0, on a $\left|J_p\right| \geqslant (p-1)!$.

Quand p tend vers l'infini, ces deux inégalités sont contradictoires, d'où la transcendance de e.

Transcendance de e (2)

On raisonne **par l'absurde** et on suppose qu'il existe des entiers $a_0, \ldots, a_n$, non tous nuls, tels que $a_0 + a_1 e + \cdots + a_n e^n = 0$. On peut supposer $a_0 \neq 0$.
On va prendre $f(x) = x^{p-1}(x-1)^p \ldots (x-n)^p$, où p est un nombre premier, et on pose

$$J_p = a_0 I(f;0) + a_1 I(f;1) + \cdots + a_n I(f;n).$$

Majoration de J_p.
Sur l'intervalle $[0;n]$, $|f(x)| \leqslant (n!)^p$.
Le lemme entraîne que $|J_p| \ll (n!)^p$.

Minoration de J_p.
On va démontrer que lorsque $p > n$ n'est pas multiple de a_0, on a $|J_p| \geqslant (p-1)!$.

Quand p tend vers l'infini, ces deux inégalités sont contradictoires, d'où la transcendance de e.

Transcendance de e (2)

On raisonne **par l'absurde** et on suppose qu'il existe des entiers $a_0, \ldots, a_n$, non tous nuls, tels que $a_0 + a_1 e + \cdots + a_n e^n = 0$. On peut supposer $a_0 \neq 0$.
On va prendre $f(x) = x^{p-1}(x-1)^p \ldots (x-n)^p$, où p est un nombre premier, et on pose

$$J_p = a_0 I(f;0) + a_1 I(f;1) + \cdots + a_n I(f;n).$$

Majoration de J_p.
Sur l'intervalle $[0;n]$, $|f(x)| \leqslant (n!)^p$.
Le lemme entraîne que $|J_p| \ll (n!)^p$.

Minoration de J_p.
On va démontrer que lorsque $p > n$ n'est pas multiple de a_0, on a $|J_p| \geqslant (p-1)!$.

Quand p tend vers l'infini, ces deux inégalités sont contradictoires, d'où la transcendance de e.

Transcendance de e (3)

Il reste donc à **minorer** J_p.
On a $f(x) = x^{p-1}(x-1)^p \dots (x-n)^p$ et
$J_p = \sum_{m=0}^{n} \sum_{k=0}^{N} a_m f^{(k)}(m)$. C'est un nombre entier.

On remarque que $f^{(k)}(0)$ est un entier, multiple de $p!$, sauf pour $k = p-1$ où on a $f^{(p-1)}(0) = (-1)^{np}(n!)^p(p-1)!$.
Par contre, pour tout k et tout $m \in \{1, \dots, n\}$, $f^{(k)}(m)$ est un entier multiple de $p!$.
$\Rightarrow$ Il existe des entiers A et B tels que
$J_p = A(p-1)! + Bp! = (p-1)!(A + pB)$.

Si $p > n$ et p ne divise pas a_0, alors A n'est pas multiple de p, donc $|A + pB| \geqslant 1$, d'où $|J_p| \geqslant (p-1)!$, comme on voulait.

Retour

Transcendance de e (3)

Il reste donc à **minorer** J_p.
On a $f(x) = x^{p-1}(x-1)^p \dots (x-n)^p$ et
$J_p = \sum_{m=0}^{n} \sum_{k=0}^{N} a_m f^{(k)}(m)$. C'est un nombre entier.

On remarque que $f^{(k)}(0)$ est un entier, multiple de $p!$, sauf pour $k = p-1$ où on a $f^{(p-1)}(0) = (-1)^{np}(n!)^p(p-1)!$.
Par contre, pour tout k et tout $m \in \{1, \dots, n\}$, $f^{(k)}(m)$ est un entier multiple de $p!$.
$\Rightarrow$ Il existe des entiers A et B tels que
$J_p = A(p-1)! + Bp! = (p-1)!(A + pB)$.

Si $p > n$ et p ne divise pas a_0, alors A n'est pas multiple de p, donc $|A + pB| \geqslant 1$, d'où $|J_p| \geqslant (p-1)!$, comme on voulait.

Retour

Transcendance de e (3)

Il reste donc à **minorer** J_p.
On a $f(x) = x^{p-1}(x-1)^p \dots (x-n)^p$ et
$J_p = \sum_{m=0}^{n} \sum_{k=0}^{N} a_m f^{(k)}(m)$. C'est un nombre entier.

On remarque que $f^{(k)}(0)$ est un entier, multiple de $p!$, sauf pour $k = p-1$ où on a $f^{(p-1)}(0) = (-1)^{np}(n!)^p(p-1)!$.
Par contre, pour tout k et tout $m \in \{1, \dots, n\}$, $f^{(k)}(m)$ est un entier multiple de $p!$.
$\Rightarrow$ Il existe des entiers A et B tels que
$J_p = A(p-1)! + Bp! = (p-1)!(A + pB)$.

Si $p > n$ et p ne divise pas a_0, alors A n'est pas multiple de p, donc $|A + pB| \geqslant 1$, d'où $|J_p| \geqslant (p-1)!$, comme on voulait.

Retour

Transcendance de e (3)

Il reste donc à **minorer** J_p.
On a $f(x) = x^{p-1}(x-1)^p \dots (x-n)^p$ et
$J_p = \sum_{m=0}^{n} \sum_{k=0}^{N} a_m f^{(k)}(m)$. C'est un nombre entier.

On remarque que $f^{(k)}(0)$ est un entier, multiple de $p!$, sauf pour $k = p-1$ où on a $f^{(p-1)}(0) = (-1)^{np}(n!)^p(p-1)!$.
Par contre, pour tout k et tout $m \in \{1, \dots, n\}$, $f^{(k)}(m)$ est un entier multiple de $p!$.
$\Rightarrow$ Il existe des entiers A et B tels que
$J_p = A(p-1)! + Bp! = (p-1)!(A + pB)$.

Si $p > n$ et p ne divise pas a_0, alors A n'est pas multiple de p, donc $|A + pB| \geqslant 1$, d'où $|J_p| \geqslant (p-1)!$, comme on voulait.

Retour

Transcendance de e (3)

Il reste donc à **minorer** J_p.
On a $f(x) = x^{p-1}(x-1)^p \dots (x-n)^p$ et
$J_p = \sum_{m=0}^{n} \sum_{k=0}^{N} a_m f^{(k)}(m)$. C'est un nombre entier.

On remarque que $f^{(k)}(0)$ est un entier, multiple de $p!$, sauf pour $k = p-1$ où on a $f^{(p-1)}(0) = (-1)^{np}(n!)^p(p-1)!$.
Par contre, pour tout k et tout $m \in \{1, \dots, n\}$, $f^{(k)}(m)$ est un entier multiple de $p!$.
$\Rightarrow$ Il existe des entiers A et B tels que
$J_p = A(p-1)! + Bp! = (p-1)!(A + pB)$.

Si $p > n$ et p ne divise pas a_0, alors A n'est pas multiple de p, donc $|A + pB| \geqslant 1$, d'où $\left|J_p\right| \geqslant (p-1)!$, comme on voulait.

Retour