# Nombres transcendants

Armentia Julien  Embry Romain
Le Manach Florian

12 mai 2012

# Sommaire

# Introduction

L'objectif principal du mémoire est de montrer la transcendance de $e$ et $\pi$. Nous allons d'abord montrer qu'ils sont irrationnels, sans quoi ils ne pourraient être transcendants. Leur irrationalité a été prouvée respectivement par Euler en 1737 et d'Alembert en 1761. Nous montrerons ensuite l'existence de nombres transcendants par une méthode constructive établie par Liouville en 1844. Cantor a prouvé en 1874 que l'ensemble des nombres transcendants est même non dénombrable. Finalement, nous prouverons le théorème d'Hermite établi en 1873 portant sur la transcendance de $e$ et le théorème de Lindemann qui a établi en 1882 la transcendance de $\pi$.

# Définitions

**Définition 1** *Soit exp la fonction définie sur* $\mathbb{C}$ *par*

$$exp(z) = \sum_{k=0}^{\infty} \frac{z^k}{k!}.$$

*On note* $exp(z) = e^z$ *et* $e = exp(1)$.

*Remarque :* L'exponentielle étant bien définie sur $\mathbb{C}$, on a en particulier

$$\forall z \in \mathbb{C},\ \lim_{n\to\infty} \frac{z^n}{n!} = 0.$$

Les propriétés suivantes de la fonction exponentielle sont admises :

- *exp* est un morphisme de groupe : $\forall (u,v) \in \mathbb{C},\ e^{u+v} = e^u e^v$ ;
- *exp* est surjective : $\forall z \in \mathbb{C}^*,\ \exists w \in \mathbb{C},\ z = e^w$ ;
- *exp* est continue sur $\mathbb{C}$ ;
- $\forall z \in \mathbb{C},\ |z| = 1 \Rightarrow \exists t \in \mathbb{R},\ z = e^{it}$ ;
- la restriction de l'exponentielle à $\mathbb{R}$ définit un homéomorphisme croissant de $\mathbb{R}$ sur $\mathbb{R}_+^*$.

**Définition 2** *Soit* $H = \{t \in \mathbb{R}, e^{it} = 1\}$.
*H est un sous groupe de* $(\mathbb{R}, +)$ *non nul et non dense donc* $\exists! a \in \mathbb{R}_+^*$ *tel que* $H = a\mathbb{Z}$. *On définit*

$$\pi = \frac{a}{2} = \min\{t \in \mathbb{R}_+^*\ ,\ e^{2it} = 1\}.$$

***Démonstration :***
H est un sous groupe de $(\mathbb{R}, +)$.
En effet, $0 \in H$ et $\forall (u,v) \in H^2,\ e^{i(u-v)} = \frac{e^{iu}}{e^{iv}} = 1$.

H est non nul. En effet $|i| = 1$ donc $\exists t \in \mathbb{R}$, $i = e^{it}$.
Ainsi $(e^{it})^4 = e^{i4t} = 1$ et $t \neq 0$ car $e^0 = 1 \neq i$. Donc $4t \in H \setminus \{0\}$.

Supposons que H soit dense. Soit $t \in \mathbb{R}$ tel que $i = e^{it}$.
$\exists (t_n) \in H^{\mathbb{N}}$ tel que $\lim t_n = t$.
Par continuité de l'exponentielle, $i = e^{it} = \lim e^{it_n} = 1$, ce qui est absurde.

H est donc un sous groupe de $(\mathbb{R}, +)$ non nul et non dense ce qui entraîne l'existence et l'unicité de $\pi$. □

**Définition 3** *On définit maintenant les fonctions trigonométriques.*
*Soit* cos *la fonction définie sur* $\mathbb{R}$ *par*

$$\cos(t) = \Re(e^{it}) = \frac{e^{it} + e^{-it}}{2}.$$

*Soit* sin *la fonction définie sur* $\mathbb{R}$ *par*

$$\sin(t) = \Im(e^{it}) = \frac{e^{it} - e^{-it}}{2i}.$$

Les propriétés suivantes des fonctions trigonométriques sont admises :

- cos et sin sont de classe $C^\infty$ sur $\mathbb{R}$ ;
- $\cos' = -\sin$ et $\sin' = \cos$ ;
- les fonctions cos et sin sont $2\pi$-périodiques ;
- cos est positive sur $[0; \frac{\pi}{2}] \cup [\frac{3\pi}{2}; 2\pi]$ et négative sur $[\frac{\pi}{2}; \frac{3\pi}{2}]$ ;
- sin est positive sur $[0; \pi]$ et négative sur $[\pi; 2\pi]$ ;
- $\cos(0) = 1$ , $\sin(0) = 0$ ;
- $\cos(\pi) = -1$ , $\sin(\pi) = 0$ ;
- $\cos(\frac{\pi}{2}) = 0$ , $\sin(\frac{\pi}{2}) = 1$.

*Remarque* : Il est facile de montrer que $e^{i\pi} = -1$.
On a $(e^{i\pi})^2 = 1$ et $e^{i\pi} \neq 1$ car $0 < \pi < 2\pi = \min\{t \in \mathbb{R}_+^* \ , \ e^{it} = 1\}$.

# Irrationalité de $e$ et $\pi$

On peut d'abord voir que si on prend un entier $q > 0$ et que l'on gradue la droite des réels avec la grandeur $\frac{1}{q}$ alors tout nombre irrationnel $\alpha$ se trouvera entre les graduations. Ainsi on peut trouver un rationnel de la forme $\frac{p}{q}$ qui soit assez proche de $\alpha$ (d'une distance au moins inférieure à $\frac{1}{2q}$). Ceci motive à chercher de « bonnes » approximations par des rationnels. Si on arrive à trouver une approximation assez fine on pourra montrer que le nombre est irrationnel.

**Définition 4** Approximation diophantienne
*Soit $\alpha \in \mathbb{R}$.*
*Une approximation diophantienne de $\alpha$ est une suite de rationnels $(\frac{p_n}{q_n})$ qui vérifie :*

$$0 < \left|\alpha - \frac{p_n}{q_n}\right| \leq f(n, q_n) \underset{n\to\infty}{\longrightarrow} 0.$$

*On dit que c'est une bonne approximation diophantienne s'il existe une suite $\varepsilon(n)$ qui tend vers 0 et tel que*

$$0 < \left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{\varepsilon(n)}{q_n}.$$

*Dans ce cas $\alpha$ est irrationnel.*

Il est facile de voir que si $\alpha = \frac{p}{q}$ est rationnel, alors pour $n$ tel que $\varepsilon(n) < \frac{1}{2q}$ on a

$$0 < |qq_n\alpha - qp_n| < \frac{1}{2}.$$

Ceci est absurde car $|qq_n\alpha - qp_n|$ est entier.

*Remarque* : La réciproque est vraie, tout nombre irrationnel admet une bonne approximation diophantienne.

**Théorème 1** *e est irrationnel.*

***Démonstration :***
On a défini $e$ de manière explicite.
Il est donc facile de l'encadrer dans le but d'obtenir une bonne approximation diophantienne.
Nous allons dans un premier temps encadrer $e$.

$$e = \sum_{k=0}^{\infty} \frac{1}{k!} = \sum_{k=0}^{N} \frac{1}{k!} + R_N, \text{ avec } R_N = \sum_{k=N+1}^{\infty} \frac{1}{k!}.$$

Comme $\frac{1}{k!} > 0$, on a $R_N > 0$, et donc,

$$\forall N \in \mathbb{N} \ , \ S_N = \sum_{k=0}^{N} \frac{1}{k!} < e.$$

Majorons $R_N$.

$$R_N = \frac{1}{(N+1)!} \sum_{k=N+1}^{\infty} \frac{(N+1)!}{k!}.$$

Or $\forall$ k > N, $\frac{(N+1)!}{k!} \leq (\frac{1}{N+2})^{k-N-1}$.
En effet,

$$\frac{(N+1)!}{k!} \leq \prod_{i=N+2}^{k} \frac{1}{i} \leq \prod_{i=N+2}^{k} \frac{1}{N+2} \leq \left(\frac{1}{N+2}\right)^{k-N-1}.$$

On a donc,

$$\begin{aligned} R_N &\leq \frac{1}{(N+1)!} \sum_{k=N+1}^{\infty} \left(\frac{1}{N+2}\right)^{k-N-1} \\ &\leq \frac{1}{(N+1)!} \frac{1}{1 - \frac{1}{N+2}} \\ &\leq \frac{1}{(N+1)!} \frac{N+2}{N+1}. \end{aligned}$$

Si N > 0, on a donc $R_N < \frac{1}{NN!}$ car $N(N+2) < (N+1)^2$.
Ainsi,

$$\forall N > 0 \ , \ S_N < e < S_N + \frac{1}{NN!}. \tag{1}$$

Nous allons maintenant montrer que $e$ est irrationnel.
Pour cela raisonnons par l'absurde et supposons que

$$\exists\ (a,b) \in \mathbb{Z} \times \mathbb{N}^*\ ,\ e = \frac{a}{b}.$$

D'après (1), on a $S_b < \frac{a}{b} < S_b + \frac{1}{bb!}$.
En multipliant cette inégalité par b ! on obtient

$$b!S_b < a(b-1)! < b!S_b + \frac{1}{b}.$$

Mais $a(b-1)! \in \mathbb{Z}$ et $b!S_b \in \mathbb{Z}$ car $\forall\ k \leq b$, $\frac{b!}{k!} \in \mathbb{Z}$.
Ceci est absurde car $\frac{1}{b} \leq 1$.
$e$ est donc irrationnel. □

**Théorème 2** *$\pi$ est irrationnel.*

Contrairement à $e$, $\pi$ n'est ici pas donné explicitement. Il n'est donc pas facile de l'encadrer et de trouver une bonne approximation diophantienne. Nous allons utiliser les propriétés de $\pi$ et des fonctions trigonométriques pour déduire une absurdité du fait qu'il soit rationnel. Cette absurdité sera du même type qu'avec $e$, c'est à dire créer un entier compris strictement entre deux entiers consécutifs.
Commençons par énoncer la formule d'Hermite.

**Lemme 1** *Soit $P$ un polynôme de degré 2n.*

$$Soit\ F = \sum_{k=0}^{n} (-1)^k P^{(2k)}.$$

*On a alors $(F' \sin - F \cos)' = P \sin$ et la formule d'Hermite*

$$\int_0^{\pi} P(t) sin(t) dt = F(0) + F(\pi). \tag{2}$$

***Démonstration*** (du Lemme 1) :

$$\begin{aligned}
(F' \sin - F \cos)' &= F'' \sin + F' \cos - F' \cos + F \sin \\
&= (F'' + F) \sin \\
&= \left( \sum_{k=0}^{n} (-1)^k P^{(2k)} - (-1)^{k+1} P^{(2k+2)} \right) \sin \\
&= (P - (-1)^{n+1} P^{(2n+2)}) \sin \\
&= P \sin
\end{aligned}$$

Ceci car $\deg P = 2n$.

De plus, $\cos(\pi) = -1$ et $\sin(\pi) = 0$ donc

$$\int_0^\pi P(t)sin(t)dt = [F'(t)\sin(t) - F(t)\cos(t)]_0^\pi = F(0) + F(\pi).$$

□

***Démonstration*** (du Théorème 2) :
Raisonnons par l'absurde et supposons que [1]

$$\exists\ (a,b) \in \mathbb{N} \times \mathbb{N}^*\ ,\ \pi = \frac{a}{b}.$$

*Idée de la preuve :*
Soit $I_P = \int_0^\pi P(t)sin(t)dt$.
Le but est de trouver un polynôme $P$ qui vérifie $0 < I_P < 1$ et $I_P \in \mathbb{Z}$.
Cherchons d'abord un polynôme $P$ vérifiant $I_P \in \mathbb{Z}$.
Il faut d'après (2) que $F(0) + F(\pi) \in \mathbb{Z}$.

$$\text{Or } F = \sum_{k=0}^{n} (-1)^k P^{(2k)}.$$

Donc pour simplifier cette condition, imposons à $P$ que $\forall k \in \mathbb{N}$, $P^{(k)}(0) \in \mathbb{Z}$ et $P^{(k)}(\pi) \in \mathbb{Z}$.
Si on pose $Q = P(\pi - X)$, alors $P^{(k)}(\pi) \in \mathbb{Z} \Leftrightarrow Q^{(k)}(0) \in \mathbb{Z}$.
Il suffit donc que $P \in \mathbb{Z}[X]$ et $P(\pi - X) \in \mathbb{Z}[X]$, ce qui est possible car $\pi \in \mathbb{Q}$.
La condition la plus contraignante est que l'on doit avoir $0 < I_P < 1$.
Il faut donc essayer de minimiser la valeur de $P(x)$ pour $x \in [0, \pi]$.
Cherchons le plus grand $K > 1$ tel que l'on ait toujours $\frac{1}{K}P^{(k)}(0) \in \mathbb{Z}$. Si $P = \sum a_k X^k$ alors $P^{(k)}(0) = k!a_k$ donc on peut prendre $K = min(k!, a_k \neq 0)$.
On voit donc que pour avoir $K$ grand il faut prendre $P$ avec un grand degré et 0 doit être une racine d'ordre maximale. Avec le même raisonnement sur $Q$, on voit que $\pi$ doit être une racine d'ordre maximal de $P$. Ainsi pour $P$ de degré 2n on peut prendre

$$P = \frac{1}{n!}X^n(a - bX)^n.$$

*Preuve :*
Soit $P_n = \frac{1}{n!}X^n(a - bX)^n$ pour $n \in \mathbb{N}$.
Posons

$$I_n = \int_0^\pi P_n(t)sin(t)dt \quad \text{et} \quad F_n = \sum_{k=0}^{n} (-1)^k P_n^{(2k)}.$$

1. $\pi \geq 0$ par définition

Montrons que la suite $(I_n)$ vérifie :

$$(i)\ I_n > 0 \qquad (ii)\ \lim I_n = 0 \qquad (iii)\ I_n \in \mathbb{Z}$$

Ce qui aboutira à une absurdité ($\exists N$ tel que $I_N \in \mathbb{Z}$ et $0 < I_N < 1$).

$(i) : t \mapsto P_n(t)\sin(t)$ est positive et continue sur $[0, \pi]$.
De plus, $P_n(\frac{\pi}{2})\sin(\frac{\pi}{2}) \neq 0$.
Ainsi $I_n > 0$.

$(ii) : \forall\ x \in [0, \pi]$, $0 \leq x(a - bx) = -b(x - \frac{a}{2b})^2 + \frac{a^2}{4b} \leq \frac{a^2}{4b}$.
Donc $\forall\ x \in [0, \pi]$, $P_n(x) \leq \frac{1}{n!}(\frac{a^2}{4b})^n$.
Ainsi, $I_n \leq \frac{1}{n!}(\frac{a^2}{4b})^n \int_0^\pi \sin(t)dt \leq \frac{2}{n!}(\frac{a^2}{4b})^n$.
On a bien $\lim I_n = 0$. [2]

$(iii) : I_n = F_n(0) + F_n(\pi)$ d'après (2).
De plus,

$$P_n(\pi - X) = P_n\left(\frac{a}{b} - X\right) = \frac{1}{n!}\left(\frac{a}{b} - X\right)^n (bX)^n = P_n.$$

Donc, $P_n^{(k)} = (-1)^k P_n^{(k)}(\pi - X)$. Ainsi $P_n^{(2k)}(0) = P_n^{(2k)}(\pi)$ et $F_n(0) = F_n(\pi)$.
Il suffit de montrer que, $\forall k \in [\![0, n]\!]$, $P_n^{(2k)}(0) \in \mathbb{Z}$.
Or,

$$P_n = \frac{1}{n!}X^n \sum_{k=0}^{n} \binom{n}{k} a^{n-k}(-bX)^k = \sum_{k=n}^{2n} \frac{1}{n!}\binom{n}{k-n} a^{2n-k}(-b)^{k-n}X^k.$$

Donc,

$$\forall k \in [\![0, n-1]\!],\quad P_n^{(k)}(0) = 0.$$

$$\forall k \in [\![n, 2n]\!],\quad P_n^{(k)}(0) = \frac{k!}{n!}\binom{n}{k-n} a^{2n-k}(-b)^{k-n} \in \mathbb{Z}$$

car $n \leq k$.
Donc $F_n(0) = F_n(\pi) \in \mathbb{Z}$, ainsi $I_n \in \mathbb{Z}$.

Les propriétés $(i)$, $(ii)$ et $(iii)$ sont vérifiées.
Mézalor, $\exists N$ tel que $I_N \in \mathbb{Z}$ et $0 < I_N < 1$, ce qui est absurde.
On a donc montré l'irrationalité de $\pi$. □

2. Car l'exponentielle est bien définie.

# Existence de nombres transcendants

À partir du monoïde commutatif $(\mathbb{N}, +)$, on peut définir le groupe $(\mathbb{Z}, +)$ en construisant les entiers négatifs. En fait, après définition de la multiplication, on voit même que $(\mathbb{Z}, +, \times)$ est un anneau intègre. Il est ensuite naturel de regarder le corps des fractions de l'anneau $\mathbb{Z}$, on définit ainsi l'ensemble $\mathbb{Q}$ des nombres rationnels. L'étape suivante est de considérer la clôture algébrique du corps $\mathbb{Q}$. Il s'agit du corps des nombres algébriques. On peut maintenant légitimement se demander si le corps des nombres algébriques est égal à $\mathbb{R}$, ce qui reviendrait à construire $\mathbb{R}$ uniquement à partir d'opérations algébriques.

**Définition 5** *Soit $\alpha \in \mathbb{C}$.*
*On dit que $\alpha$ est algébrique s'il est racine d'un polynôme non nul à coefficients entiers, c'est à dire si*

$$\exists P \in \mathbb{Z}[X] \setminus \{0\},\ P(\alpha) = 0.$$

*Sinon $\alpha$ est dit transcendant et on a*

$$\forall P \in \mathbb{Z}[X] \setminus \{0\},\ P(\alpha) \neq 0.$$

*Si $\alpha$ est algébrique, on note $P_\alpha$ l'unique polynôme unitaire qui engendre l'idéal $\{P \in \mathbb{Q}[X],\ P(\alpha) = 0\}$ dans $\mathbb{Q}[X]$.*
*$P_\alpha$ est aussi le polynôme unitaire de $\mathbb{Q}[X]$ de degré minimal qui annule $\alpha$.*
*$P_\alpha$ est appelé polynôme minimal de $\alpha$ et on note $\deg \alpha = \deg P_\alpha$.*

**Lemme 2** *Soit $\alpha \in \mathbb{C}$ algébrique.*
*Soit $P \in \mathbb{Q}[X]$ unitaire tel que $P(\alpha) = 0$.*
*On a alors : $P$ est le polynôme minimal de $\alpha$ si et seulement si $P$ est irréductible dans $\mathbb{Q}[X]$.*

***Démonstration*** :
Si $P$ est le polynôme minimal de $\alpha$, alors $\forall (R,S) \in \mathbb{Q}[X]^2$ qui vérifie $P = RS$, on a $R(\alpha) = 0$ ou $S(\alpha) = 0$.
Donc $R$ ou $S$ appartient à $\{Q \in \mathbb{Q}[X],\ Q(\alpha) = 0\} = P\mathbb{Q}[X]$. Ainsi $R$ ou $S$ est associé à $P$ et l'autre est dans $\mathbb{Q}^\times$. Donc $P$ est bien irréductible.
Réciproquement, si $P$ est irréductible, comme $P(\alpha) = 0$, $P_\alpha | P$. Or $P_\alpha \notin \mathbb{Q}$, donc $P$ et $P_\alpha$ sont associés et comme ils sont tous deux unitaires $P = P_\alpha$ est le polynôme minimal de $\alpha$. □

Nous avons vu grâce aux approximations diophantiennes que pour avoir un nombre irrationnel il faut réussir à rendre la quantité $|\alpha - \frac{p}{q}|$ « petite » devant $\frac{1}{q}$. Nous avons cependant un théorème qui modère la convergence de cette quantité pour les nombres algébriques. Ce théorème dit que la quantité $|\alpha - \frac{p}{q}|$ est « grande » devant une certaine puissance de $\frac{1}{q}$. Cela vient du fait qu'un polynôme tend relativement « doucement » vers ces racines.

**Théorème 3** *Soit $\alpha$ un nombre algébrique réel irrationnel.*

$$\exists d \in \mathbb{N},\ \exists C > 0,\ \forall (p,q) \in \mathbb{Z} \times \mathbb{N}^*,\ \left|\alpha - \frac{p}{q}\right| \geq \frac{C}{q^d}. \tag{3}$$

*On peut prendre en particulier $d = \deg \alpha$ et $C = \min\left(1, \frac{1}{C'}\right)$ avec $C' = sup\{|P'(x)|,\ x \in ]\alpha - 1, \alpha + 1[\} < +\infty$ et $P = \frac{1}{cont(P_\alpha)} P_\alpha$ son « polynôme minimal » dans $\mathbb{Z}[X]$.*

***Démonstration :***

*Idée de la preuve :*
Malgré l'allure globale de ce théorème, son intérêt se situe au voisinage de $\alpha$. En effet, en dehors d'un voisinage de $\alpha$ du type $]\alpha - \varepsilon, \alpha + \varepsilon[$ on a,

$$\forall d \in \mathbb{N},\ \left|\alpha - \frac{p}{q}\right| \geq \varepsilon \geq \frac{\varepsilon}{q^d}.$$

$\alpha$ est algébrique irrationnel donc $\exists P \in \mathbb{Z}[X]$ tel que $\deg P = d \geq 2$ et $P(\alpha) = 0$.
Ce théorème repose sur le fait que P converge « moins vite » qu'une certaine fonction f vers $\alpha$. Plus précisément, soit f la fonction définie sur $\mathbb{Q} \cup \{\alpha\}$ par

$$\forall (p,q) \in \mathbb{Z} \times \mathbb{N}^*, \text{ avec } p \wedge q = 1,\ f\left(\frac{p}{q}\right) = \frac{1}{q^d} \text{ et } f(\alpha) = 0.$$

On a alors dans un voisinage $V = ]\alpha - \varepsilon, \alpha + \varepsilon[$ de $\alpha$ sur lequel $P$ ne s'annule qu'en $\alpha$ (ce qui existe car P est non nul donc a un nombre fini de racines) $f\left(\frac{p}{q}\right) \leq \left|P\left(\frac{p}{q}\right)\right|$.
Ainsi,

$$\left|\frac{f\left(\frac{p}{q}\right) - f(\alpha)}{\frac{p}{q} - \alpha}\right| \leq \left|\frac{P\left(\frac{p}{q}\right) - P(\alpha)}{\frac{p}{q} - \alpha}\right| \leq K,\ K \in \mathbb{R}_+^*.$$

La dernière inégalité venant du théorème des accroissements finis. On obtient ainsi le résultat escompté.

*Preuve :*
Soit $\varepsilon = \min(|\alpha - a_i|) > 0$, avec $(a_i)$ la suite finie des racines réelles de P différentes de $\alpha$.
Soit $V = ]\alpha - \varepsilon, \alpha + \varepsilon[$.
On a alors,

$$\forall (p,q) \in \mathbb{Z} \times \mathbb{N}^* \text{ tel que } \frac{p}{q} \notin V, \text{ on a } \left|\alpha - \frac{p}{q}\right| \geq \frac{\varepsilon}{q^d}.$$

De plus, $\forall x \in V \setminus \{\alpha\}$, $P(x) \neq 0$.
Soit $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $\frac{p}{q} \in V$, alors $P\left(\frac{p}{q}\right) \neq 0$ car $\alpha$ est irrationnel.
Or, $q^d P\left(\frac{p}{q}\right) \in \mathbb{Z}$, donc $1 \leq \left|q^d P\left(\frac{p}{q}\right)\right|$.
Ainsi on obtient,

$$\frac{1}{q^d} \leq \left|P\left(\frac{p}{q}\right) - P(\alpha)\right| \leq K\left|\frac{p}{q} - \alpha\right|$$

en posant $K = \|P'_{|V}\|_\infty$ et en utilisant le théorème des accroissements finis ($P$ continue sur $V$, dérivable sur $V$ et $P'$ borné sur $V$).
Or $K \neq 0$ car sinon $P' = 0$ (car $P'$ aura une infinité de racines) et $P \in \mathbb{Z}$.
En posant $C = \min\left(\varepsilon, \frac{1}{K}\right)$, on obtient finalement,

$$\forall (p,q) \in \mathbb{Z} \times \mathbb{N}^*,\ \left|\alpha - \frac{p}{q}\right| \geq \frac{C}{q^d}.$$

Pour avoir la forme explicite du théorème on peut prendre $d = \deg P_\alpha$ et $C = \min\left(1, \frac{1}{C'}\right)$ avec $C' = \min\{|P'(x)|, x \in ]\alpha - 1, \alpha + 1[\}$ et $P = \frac{1}{cont(P_\alpha)} P_\alpha$.
Ceci car $P_\alpha$ étant irréductible sur $\mathbb{Q}$ et de degré supérieur à 2, il ne s'annule pas sur $\mathbb{Q}$. □

Le but de ce paragraphe est de trouver des nombres transcendants. Il est donc naturel de chercher des nombres ne vérifiant pas le théorème précédent (de Liouville).

**Définition 6** *On appelle nombre de Liouville, un nombre irrationnel $\alpha$ vérifiant :*

$$\forall n \in \mathbb{N},\ \exists (p,q) \in \mathbb{Z} \times \mathbb{N} \setminus \{0,1\},\ \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}. \tag{4}$$

*Remarque :* On prend $q \neq 1$ car sinon tout nombre irrationnel serait de Liouville. En effet $|\alpha - E(\alpha)| < 1$.

**Théorème 4** *Tout nombre de Liouville est transcendant.*

***Démonstration :***
Supposons que $\alpha$ soit un nombre de Liouville algébrique de degré d.
D'après (3) et (4) (le théorème 3 et la définition 6),

$$\exists C > 0,\ \forall n \in \mathbb{N},\ \exists (p,q) \in \mathbb{Z} \times \mathbb{N} \setminus \{0,1\},\ \frac{C}{q^d} \leq \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}.$$

Ainsi $\exists C > 0,\ \forall n > d,\ \exists q \in \mathbb{N} \setminus \{0,1\},\ C < \frac{1}{q^{n-d}} \leq \frac{1}{2^{n-d}}$.
On a alors $0 < \frac{C}{2^d} \leq \frac{1}{2^n}$.
Ceci est absurde car par passage à la limite on a $0 < \frac{C}{2^d} \leq 0$ ($C$ et $d$ sont bien indépendants de $n$). □

Un nombre $\alpha$ admettant une suite de rationnels qui converge « rapidement » vers $\alpha$ est de Liouville. C'est pourquoi on s'intéresse à la série de Engel $\sum \frac{1}{10^{k!}}$ qui converge « très vite » vers sa somme.

**Corollaire 1**

$$\alpha = \sum_{k=0}^{\infty} \frac{1}{10^{k!}} \text{ est un nombre transcendant.}$$

***Démonstration :***
Pour tout $n \in \mathbb{N}$, soit

$$p_n = \sum_{k=0}^{n} \frac{10^{n!}}{10^{k!}} \text{ et } q_n = 10^{n!}.$$

$S_n = \frac{p_n}{q_n}$ est la somme partielle de la série. On a donc

$$\begin{aligned}
\left|\alpha - \frac{p_n}{q_n}\right| &= \left|\sum_{k=n+1}^{\infty} \frac{1}{10^{k!}}\right| \\
&\leq \frac{1}{10^{(n+1)!}} \sum_{k=0}^{\infty} \frac{1}{10^k} \qquad (5) \\
&\leq \frac{1}{10^{(n+1)!}} \frac{1}{1-\frac{1}{10}} \\
&\leq \frac{1}{(10^{n!})^n} \frac{10}{10^{n!} \times 9} \\
&< \frac{1}{(q_n)^n}.
\end{aligned}$$

Montrer (5) revient à montrer que

$$\forall k > n,\ \frac{10^{(n+1)!}}{10^{k!}} \leq \frac{1}{10^{k-n-1}},$$

c'est à dire $k! - (n+1)! \geq k - n - 1$.
Pour $k = n+1$ l'inégalité est évidente.
Pour $k > n+1$,

$$k! \geq k(n+1)! \geq (n+1)! + (k-1)(n+1)! \geq (n+1)! + (k-n-1).$$

Ainsi $\forall n \in \mathbb{N}$, $(p_n, q_n) \in \mathbb{Z} \times \mathbb{N} \setminus \{0,1\}$ et $\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{(q_n)^n}$.

Donc $\alpha$ est un nombre de Liouville, il est donc transcendant. □

*Remarque :* Toute somme de série de la forme $r + \sum \frac{1}{n^{k!}}$, $(r,n) \in \mathbb{Q} \times \mathbb{N} \setminus \{0,1\}$ est également un nombre de Liouville.

Nous avons ainsi obtenu notre premier nombre transcendant. Cependant ce nombre a été construit pour être transcendant et n'est pas très naturel. On peut se demander si d'autres nombres déjà utilisés en mathématiques sont transcendants. En attendant, on a répondu à la question posée en début de chapitre : $\mathbb{R}$ est différent de la clôture algébrique de $\mathbb{Q}$.
D'après l'hypothèse du continu, tout ensemble infini inclus dans $\mathbb{R}$ est soit dénombrable, soit en bijection avec $\mathbb{R}$. On peut maintenant se demander à quelle catégorie appartient l'ensemble des nombres algébriques. Cantor a répondu à cette question avec le théorème suivant.

**Théorème 5** *L'ensemble des nombres algébriques est dénombrable.*
*L'ensemble des nombres transcendants est non dénombrable.*

***Démonstration :***
Il existe une injection de $\mathbb{Z}[X] \setminus \{0\}$ dans $\cup_{i=1}^{\infty} \mathbb{Z}^i$.
En effet, à chaque polynôme de degré i on peut associer le (i+1)-uplet de ses coefficients.
Or $\cup_{i=1}^{\infty} \mathbb{Z}^i$ est dénombrable comme union dénombrable d'ensembles dénombrables, donc $\mathbb{Z}[X] \setminus \{0\}$ est dénombrable.
L'ensemble des nombres algébriques est égal à

$$\bigcup_{P \in \mathbb{Z}[X] \setminus \{0\}} \{z \in \mathbb{C}, P(z) = 0\}$$

qui est dénombrable en tant qu'union dénombrable d'ensembles finis.
Ensuite, comme $\mathbb{R}$ est non dénombrable, il vient que l'ensemble des nombres transcendants est non vide et même en infinité non dénombrable (car sinon $\mathbb{R}$ serait dénombrable comme union de deux ensembles dénombrables).

# Transcendance de $e$ et $\pi$

Depuis l'antiquité, les mathématiciens ont cherché à déterminer quels nombres étaient constructibles à la règle et au compas. En 1837, Wantzel établit un théorème donnant une condition nécessaire et suffisante pour qu'un nombre soit constructible. En particulier, il en découle que tout nombre constructible est nécessairement algébrique de degré $2^q$, $q \in \mathbb{N}$. Ainsi, si un nombre est transcendant, il est clair qu'il ne peut être constructible. En particulier, la transcendance de $\pi$ entraînerait l'impossibilité de la quadrature du cercle.

Commençons par introduire une intégrale qui nous servira, comme dans la démonstration de l'irrationalité de $\pi$, à construire, dans le cas où $e$ et $\pi$ seraient algébriques, des entiers strictement compris entre 0 et 1.

**Lemme 3** *Soit $P \in \mathbb{R}[X]$ et $z \in \mathbb{C}$. On pose*

$$I(P,z) = ze^z \int_0^1 e^{-tz} P(tz)dt = z \int_0^1 e^{(1-t)z} P(tz)dt.$$

*On a alors,*

$$|I(P,z)| \leq |z|e^{|z|} \sup_{t\in[0,1]} (|P(tz)|)$$

*et*

$$I(P,z) = e^z \sum_{k=0}^{\infty} P^{(k)}(0) - \sum_{k=0}^{\infty} P^{(k)}(z).$$

***Démonstration :***
Commençons par majorer $|I(P,z)|$.

$$\begin{aligned}
|I(P,z)| &= \left| z\int_0^1 e^{(1-t)z}P(tz)dt \right| \\
&\leq |z|\int_0^1 |e^{(1-t)z}||P(tz)|dt \\
&\leq |z|\int_0^1 e^{(1-t)\Re(z)} \sup_{x\in[0,1]}(|P(xz)|)dt \\
&\leq |z|\int_0^1 e^{(1-t)|z|} \sup_{x\in[0,1]}(|P(xz)|)dt \\
&\leq |z|e^{|z|} \sup_{x\in[0,1]}(|P(xz)|)
\end{aligned}$$

ceci car $\forall z \in \mathbb{C},\ |e^z| = |e^{\Re(z)}||e^{i\Im(z)}| = e^{\Re(z)}$ et car $e^{\Re(z)} \leq e^{|z|}$.
En effet, $\Re(z) \leq |\Re(z)| \leq \sqrt{\Re(z)^2 + \Im(z)^2} \leq |z|$ et l'exponentielle réelle est une fonction croissante.

Montrons maintenant l'égalité.
Si $z = 0$, on a bien l'égalité voulue. En effet, on a $e^0 = 1$, donc

$$I(P,0) = 0 = e^0 \sum_{k=0}^{\infty} P^{(k)}(0) - \sum_{k=0}^{\infty} P^{(k)}(0).$$

Si $z \neq 0$, on peut faire une intégration par parties en dérivant le polynôme.

$$\begin{aligned}
I(P,z) &= ze^z \int_0^1 e^{-tz}P(tz)dt \\
&= ze^z \left( \left[ \frac{e^{-tz}}{-z}P(tz) \right]_0^1 - \int_0^1 \frac{e^{-tz}}{-z} zP'(tz)dt \right) \\
&= ze^z \left( \frac{P(0)}{z} - \frac{e^{-z}P(z)}{z} \right) + ze^z \left( \int_0^1 e^{-tz}P'(tz)dt \right) \\
&= e^z P(0) - P(z) + I(P',z).
\end{aligned}$$

Donc, si pour $n \in \mathbb{N}$ on a

$$I(P,z) = e^z \sum_{k=0}^{n-1} P^{(k)}(0) - \sum_{k=0}^{n-1} P^{(k)}(z) + I(P^{(n)},z),$$

comme $I(P^{(n)},z) = e^z P^{(n)}(0) - P^{(n)}(z) + I(P^{(n+1)},z)$, on obtient

$$I(P,z) = e^z \sum_{k=0}^{n} P^{(k)}(0) - \sum_{k=0}^{n} P^{(k)}(z) + I(P^{(n+1)},z).$$

Par récurrence on a que

$$I(P,z) = e^z \sum_{k=0}^{\infty} P^{(k)}(0) - \sum_{k=0}^{\infty} P^{(k)}(z)$$

car pour $n > \deg P$, $P^{(n)} = 0$ et $I(P^{(n)}, z) = 0$. □

**Lemme 4** *Soit $P \in \mathbb{Z}[X]$.*

$$\forall n \in \mathbb{N},\ \exists P_n \in \mathbb{Z}[X],\ P^{(n)} = n! P_n.$$

***Démonstration :***
Soit $P \in \mathbb{Z}[X]$ de degré $m$. $\exists (a_k) \in \mathbb{Z}^{m+1}$ tel que $P = \sum_{k=0}^{m} a_k X^k$.
Si $n > m$, on a $P^{(n)} = 0 = n! P_n$ avec $P_n = 0 \in \mathbb{Z}[X]$.
Si $n \leq m$,

$$\begin{aligned} P^{(n)} &= \sum_{k=n}^{m} a_k \frac{k!}{(k-n)!} X^{k-n} \\ &= n! \sum_{k=n}^{m} a_k \frac{k!}{(k-n)!n!} X^{k-n}. \end{aligned}$$

Donc si $n \leq m$, on a $P^{(n)} = n! P_n$ avec $P_n = \sum_{k=n}^{m} a_k \binom{k}{n} X^{k-n} \in \mathbb{Z}[X]$. □

Le théorème de d'Alembert-Gauss nous dit que tout polynôme de $\mathbb{C}[X]$ est scindé dans $\mathbb{C}[X]$.

*Notation :*
Soit $P \in \mathbb{C}[X]$ de degré $d$. $P$ est scindé sur $\mathbb{C}$, notons $(a_k)_{1 \leq k \leq d}$ ses racines.
Si f est une application de $\mathbb{C}$ dans $\mathbb{C}$, on note

$$\sum_{P(\alpha)=0} f(\alpha) = \sum_{k=1}^{d} f(a_k).$$

**Théorème 6** *e est transcendant.*

***Démonstration :***
Supposons $e$ algébrique.
$\exists n \in \mathbb{N},\ \exists (a_i) \in \mathbb{Z}^{n+1} \setminus \{0\}$ tels que

$$\sum_{i=0}^{n} a_i e^i = 0.$$

Quitte à diviser par $e^k$ avec $k = \inf\{i \in [\![0,n]\!],\ a_i \neq 0\}$, on choisit $a_0 \neq 0$. Pour tout $p \in \mathbb{N} \setminus \{0,1\}$, on pose

$$Q_p = \frac{1}{(p-1)!} X^{p-1} \prod_{i=1}^{n} (X-i)^p$$

et

$$J_{Q_p} = \sum_{i=0}^{n} a_i I(Q_p, i)$$

avec

$$I(Q_p, i) = ie^i \int_0^1 e^{-ti} Q_p(ti) dt.$$

On veut obtenir une absurdité similaire à celles des démonstrations de l'irrationalité de $e$ et $\pi$. On va d'abord montrer que pour tout entier $p \geq 2$, on a $\lim J_{Q_p} = 0$ et $J_{Q_p} \in \mathbb{Z}$. Ensuite, nous montrerons qu'il existe un nombre premier p assez grand tel que $J_{Q_p} \neq 0$, d'où l'absurdité.

Montrons d'abord qu'il existe $B$ et $C$ tels que pour tout p, $|J_{Q_p}| \leq C\frac{B^{p-1}}{(p-1)!}$. D'après le lemme 3 on a, $\forall i \in [\![0,n]\!]$,

$$|I(Q_p, i)| \leq ie^i \sup_{t\in[0,i]} (|Q_p(t)|) \leq ne^n \frac{n^{p-1} n^{np}}{(p-1)!}$$

car $\forall (i,k) \in [\![0,n]\!]^2$, $\forall t \in [0,i]$, $|t-k| \leq n$.
Ainsi,

$$|J_{Q_p}| \leq (n+1) \max_{i\in[\![0,n]\!]} (|a_i|) ne^n \frac{n^{p-1} n^{np}}{(p-1)!} \leq C \frac{B^{p-1}}{(p-1)!}$$

avec $B = n^{n+1}$ et $C = (n+1)n^{n+1}e^n \max(|a_i|)$.

Or, $\lim\limits_{p\to\infty} \dfrac{B^{p-1}}{(p-1)!} = 0$. Ainsi, $\lim\limits_{p\to\infty} J_{Q_p} = 0$.

Montrons maintenant que pour tout p, $J_{Q_p} \in \mathbb{Z}$.
D'après le lemme 3 on a

$$\begin{aligned}
J_{Q_p} &= \sum_{i=0}^{n} a_i \left( e^i \sum_{j=0}^{\infty} Q_p^{(j)}(0) - \sum_{j=0}^{\infty} Q_p^{(j)}(i) \right) \\
&= \left( \sum_{i=0}^{n} a_i e^i \right) \left( \sum_{j=0}^{\infty} Q_p^{(j)}(0) \right) - \sum_{i=0}^{n} a_i \left( \sum_{j=0}^{\infty} Q_p^{(j)}(i) \right) \\
&= -\sum_{i=0}^{n} a_i \left( \sum_{j=0}^{\infty} Q_p^{(j)}(i) \right), \text{ car } \sum_{i=0}^{n} a_i e^i = 0.
\end{aligned}$$

Pour tout $i \in [\![0, n]\!]$, i est une racine de $Q_p$ d'ordre supérieur à $p-1$.
Si $j < p-1$,

$$Q_p^{(j)}(i) = 0.$$

Si $j \geq p-1$,

$$Q_p^{(j)}(i) \in \mathbb{Z}.$$

En effet, $(p-1)!Q_p \in \mathbb{Z}[X]$ donc, d'après le lemme 4,

$$(p-1)!Q_p^{(j)} \in j!\mathbb{Z}[X] \subset (p-1)!\mathbb{Z}[X].$$

Ainsi $J_{Q_p} \in \mathbb{Z}$.

On a montré que $\lim J_{Q_p} = 0$ et $J_{Q_p} \in \mathbb{Z}$. Donc $\exists N$, $\forall p \geq N$, $|J_{Q_p}| < 1$ et ainsi $J_{Q_p} = 0$.

Montrons maintenant qu'il existe un nombre premier $p > N$ tel que $J_{Q_p} \neq 0$.
Comme précédemment,
$\forall i \in [\![0, n]\!]$,
Si $j < p-1$,

$$Q_p^{(j)}(i) = 0.$$

Si $j > p-1$,

$$Q_p^{(j)}(i) \in p\mathbb{Z}.$$

En effet, $(p-1)!Q_p \in \mathbb{Z}[X]$ donc, d'après le lemme 4,

$$(p-1)!Q_p^{(j)} \in j!\mathbb{Z}[X] \subset p!\mathbb{Z}[X].$$

Si $j = p-1$,

$$\forall i \in [\![1, n]\!],\ Q_p^{(p-1)}(i) = 0.$$

De plus,

$$Q_p = \frac{1}{(p-1)!} X^{p-1} R_p, \text{ où } R_p = \prod_{i=1}^{n} (X-i)^p.$$

Ainsi, en appliquant la formule de Leibniz, on a

$$Q_p^{(p-1)} = R_p + \sum_{k=1}^{p-1} \binom{p-1}{k} \frac{1}{k!} X^k R_p^{(k)}.$$

En évaluant en 0, on obtient donc

$$Q_p^{(p-1)}(0) = R_p(0) = (-1)^{pn}(n!)^p.$$

Finalement,

$$\begin{aligned} J_{Q_p} &= -a_0 Q_p^{(p-1)}(0) - \sum_{i=0}^{n} a_i \left( \sum_{j=p}^{\infty} Q_p^{(j)}(i) \right) \\ &\in a_0(-1)^{pn+1}(n!)^p + p\mathbb{Z}. \end{aligned}$$

Cette relation est vraie pour tout entier p supérieur à 2.
On choisit de prendre p un nombre premier supérieur à $n!|a_0| + N + 12$.
Ainsi, p ne divise pas $a_0(-1)^{pn+1}(n!)^p$ car sinon, par le lemme de Gauss, p diviserait $|a_0|$ ou $n!$ qui sont tous deux non nuls et inférieurs à p.
Donc p ne divise pas $J_{Q_p}$ et ainsi $J_{Q_p} \neq 0$.
Ceci est absurde car $p > N$.
$e$ est donc transcendant. □

Intéressons-nous maintenant à la transcendance de $\pi$. Nous allons tenter de suivre un schéma similaire à la démonstration de la transcendance de $e$. Au vu de la définition de $\pi$, il est naturel de s'intéresser au nombre $i\pi$. D'où le lemme suivant.

**Lemme 5** *Soit $\alpha$ un nombre algébrique. Alors $i\alpha$ est un nombre algébrique.*

***Démonstration :***
Comme $\alpha$ est algébrique, $\exists P \in \mathbb{Z}[X]$ tel que $P(\alpha) = 0$.
On a donc $P(-i(i\alpha)) = 0$.
Le polynôme $P(-iX)$ annule $i\alpha$, mais il est à coefficients dans $\mathbb{Z}[i]$. On le multiplie par son « conjugué » pour obtenir un polynôme de $\mathbb{Z}[X]$.
Posons $Q = P(-iX)P(iX)$. On a $Q(i\alpha) = 0$. De plus, si $P = \sum a_j X^j$,

$$\begin{aligned} Q &= \left( \sum_{j=0}^{n} (-i)^j a_j X^j \right) \left( \sum_{k=0}^{n} i^k a_k X^k \right) \\ &= \sum_{j=0}^{n} \sum_{k=0}^{n} (-1)^j i^{j+k} a_j a_k X^{j+k} \\ &= \sum_{p=0}^{2n} \sum_{j+k=p} (-1)^j i^p a_j a_k X^p. \end{aligned}$$

Si p est pair, on a $i^p = (-1)^{p/2}$ et donc $\sum_{j+k=p} (-1)^j i^p a_j a_k \in \mathbb{Z}$.
Si p impair, $\sum_{j+k=p} (-1)^j i^p a_j a_k = 0$ car $(-1)^j a_j a_k = -(-1)^k a_k a_j$.
Donc $Q \in \mathbb{Z}[X]$ et $i\alpha$ est bien algébrique. □

*Remarque :* Dans le cas général si $\alpha$ et $\beta$ sont algébriques alors $\alpha\beta$ est aussi algébrique. Il suffit de considérer le polynôme $R(Y) = res_X(P(X), X^n Q(\frac{Y}{X}))$ avec $P(\alpha) = 0$, $Q(\beta) = 0$ et $\deg Q = n$. On a donc $R \in \mathbb{Z}[Y]$ et $R(\alpha\beta) = 0$ car $P(\alpha) = 0$ et $\alpha^n Q(\frac{\alpha\beta}{\alpha}) = 0$.

**Théorème 7** *$\pi$ est transcendant.*

***Démonstration :***
Supposons $\pi$ algébrique. Intéressons nous à $i\pi$, qui est également algébrique d'après le lemme 5.
$\exists P \in \mathbb{Z}[X]$ tel que $P(i\pi) = 0$.
Soit $(\alpha_k)_{1\leq k\leq n}$ les racines complexes de $P$ et $\lambda$ son coefficient dominant.
$\exists q \in [\![1, n]\!]$ tel que $\alpha_q = i\pi$.
Or $e^{i\pi} = -1$, donc

$$\prod_{k=1}^{n}(1 + e^{\alpha_k}) = 0.$$

En développant le produit, on a

$$\prod_{k=1}^{n}(1 + e^{\alpha_k}) = \sum_{(\varepsilon_k)\in\{0,1\}^n} \exp\left(\sum_{k=1}^{n} \varepsilon_k\alpha_k\right) = 0.$$

En effet, ce résultat peut se montrer par récurrence. Pour toute famille $(\alpha_k)$ à un seul élément le résultat est clair. Supposons que ce résultat soit vrai pour toute famille à n éléments. Soit $(\alpha_k)$ une famille à n+1 éléments.

$$\begin{aligned}
\prod_{k=1}^{n+1}(1 + e^{\alpha_k}) &= (1 + e^{\alpha_{n+1}}) \sum_{(\varepsilon_k)\in\{0,1\}^n} \exp\left(\sum_{k=1}^{n} \varepsilon_k\alpha_k\right) \\
&= \sum_{(\varepsilon_k)\in\{0,1\}^n} \exp\left(\sum_{k=1}^{n} \varepsilon_k\alpha_k + 0 \times \alpha_{n+1}\right) + \\
&\quad \sum_{(\varepsilon_k)\in\{0,1\}^n} \exp\left(\sum_{k=1}^{n} \varepsilon_k\alpha_k + 1 \times \alpha_{n+1}\right) \\
&= \sum_{(\varepsilon_k)\in\{0,1\}^{n+1}} \exp\left(\sum_{k=1}^{n+1} \varepsilon_k\alpha_k\right).
\end{aligned}$$

D'où le résultat.

*Remarque :* On peut voir qu'il y a un lien étroit entre l'absurdité que l'on veut obtenir et celle de la démonstration du théorème d'Hermite sur la transcendance de $e$.
En effet, dans la preuve du théorème d'Hermite, on voulait montrer que $\sum a_k e^k = 0$ était absurde. Pour cela on a considéré $Q_p = \frac{1}{(p-1)!}X^{p-1}R^p$, avec $R$ le polynôme unitaire qui annule les entiers de 1 à n. On remarque que les racines de $R$ sont les exposants de $e$, sans 0, dans la somme. On va construire une absurdité sur le même modèle.

Soit

$$R = \prod_{(\varepsilon_k)\in\{0,1\}^n} \left( X - \sum_{k=1}^{n} \varepsilon_k \alpha_k \right) = \prod_{j=1}^{2^n} (X - \beta_j).$$

Montrons que $R \in \mathbb{Q}[X]$. Pour cela nous pouvons utiliser les polynômes symétriques élémentaires.

**Définition 7** $\forall n \in \mathbb{N}^*$, $\forall k \in [\![1, n]\!]$,

$$\Sigma_k^n = \sum_{1\leq i_1<\cdots<i_k\leq n} \prod_{j=1}^{k} X_{i_j}$$

*est le k-ième polynôme symétrique élémentaire en n variables.*
*On appellera polynôme symétrique un polynôme invariant par permutation des variables.*
*On note* $\mathbb{Z}[X_1, \cdots, X_n]^{sym}$ *le sous anneau des polynômes symétriques de* $\mathbb{Z}[X_1, \cdots, X_n]$.

*Remarque :* Un résultat important des polynômes symétriques élémentaires est que $\mathbb{Z}[X_1, \cdots, X_n]^{sym} = \mathbb{Z}[\Sigma_1^n(X_1, \cdots, X_n), \cdots, \Sigma_n^n(X_1, \cdots, X_n)]$.

Montrons que $R \in \mathbb{Q}[X]$.

$$R = X^{2^n} + \sum_{k=1}^{2^n} (-1)^k \Sigma_k^{2^n}(\beta_1, \cdots, \beta_{2^n}) X^{2^n-k}.$$

Or, $\forall j \in [\![1, 2^n]\!]$, $\beta_j \in \mathbb{Z}[\alpha_1, \cdots, \alpha_n]$.
Donc, $\forall k \in [\![1, 2^n]\!]$, $\Sigma_k^{2^n}(\beta_1, \cdots, \beta_{2^n}) \in \mathbb{Z}[\alpha_1, \cdots, \alpha_n]$.

Soit $\sigma \in S_n$.
On définit le morphisme d'anneaux $\check{\sigma}$ par

$$\begin{array}{rccc} \check{\sigma}: & \mathbb{Z}[\alpha_1, \cdots, \alpha_n] & \longrightarrow & \mathbb{Z}[\alpha_1, \cdots, \alpha_n]\ . \\ & m \in \mathbb{Z} & \longmapsto & m \\ & \alpha_k & \longmapsto & \alpha_{\sigma(k)} \end{array}$$

On a alors $\check{\sigma}(\beta_j) = \sum \varepsilon_k \alpha_{\sigma(k)} = \beta_p$.

Donc posons $\begin{array}{rccc} \overline{\sigma}: & [\![1,2^n]\!] & \longrightarrow & [\![1,2^n]\!] \\ & j & \longmapsto & p = \text{indice}(\check{\sigma}(\beta_j)) \end{array}$.

$\overline{\sigma}$ est bijective car $\sigma$ l'est. Ainsi, $\overline{\sigma} \in S_{2^n}$.
Donc,

$$\begin{aligned} \check{\sigma}\left(\Sigma_k^{2^n}(\beta_1, \cdots, \beta_{2^n})\right) &= \Sigma_k^{2^n}(\check{\sigma}(\beta_1), \cdots, \check{\sigma}(\beta_{2^n})) \\ &= \Sigma_k^{2^n}(\beta_{\overline{\sigma}(1)}, \cdots, \beta_{\overline{\sigma}(2^n)}) \\ &= \Sigma_k^{2^n}(\beta_1, \cdots, \beta_{2^n}) \end{aligned}$$

car $\Sigma_k^{2^n}$ est un polynôme symétrique et $\overline{\sigma}$ une permutation.
Ainsi

$$\begin{aligned} \Sigma_k^{2^n}(\beta_1, \cdots, \beta_{2^n}) &\in \mathbb{Z}[\alpha_1, \cdots, \alpha_n]^{sym} \\ \Sigma_k^{2^n}(\beta_1, \cdots, \beta_{2^n}) &\in \mathbb{Z}[\Sigma_1^n(\alpha_1, \cdots, \alpha_n), \cdots, \Sigma_n^n(\alpha_1, \cdots, \alpha_n)] \\ \Sigma_k^{2^n}(\beta_1, \cdots, \beta_{2^n}) &\in \mathbb{Q} \end{aligned}$$

car $\forall k \in [\![1,n]\!]$, $\Sigma_k^n(\alpha_1, \cdots, \alpha_n) \in \frac{1}{\lambda}\mathbb{Z}$, ceci car $P = \lambda \prod_{k=1}^{n} (X - \alpha_k) \in \mathbb{Z}[X]$.

Soit $S = \frac{1}{cont(R)} R \in \mathbb{Z}[X]$. Comme 0 est une racine de R, soit $k \in \mathbb{N}^*$ l'ordre de la racine 0 de R. Les racines de $S$ sont les mêmes que celles de $R$. Donc il existe $T \in \mathbb{Z}[X]$ tel que $T(0) \neq 0$ et $S = X^k T$. Et, par définition de $R$, on a

$$k + \sum_{T(\alpha)=0} e^{\alpha} = \sum_{S(\alpha)=0} e^{\alpha} = \sum_{(\varepsilon_k)\in\{0,1\}^n} \exp\left(\sum_{k=1}^{n} \varepsilon_k \alpha_k\right) = 0.$$

Pour montrer que ceci est absurde, on considère, comme dans la démonstration de la transcendance de $e$, le polynôme $Q_p = \frac{1}{(p-1)!} X^{p-1} T^p,\ p \in \mathbb{N}^*$.
On définit

$$J_{Q_p} = \sum_{T(\alpha)=0} I(Q_p, \alpha)$$

avec

$$I(Q_p, \alpha) = \alpha e^{\alpha} \int_0^1 e^{-t\alpha} Q_p(t\alpha) dt.$$

On veut obtenir une absurdité similaire à celles des démonstrations précédentes. On souhaiterait montrer que pour tout entier $p \geq 2$, on a $\lim J_{Q_p} = 0$ et $J_{Q_p} \in \mathbb{Z}$. Cependant la deuxième assertion n'est pas vérifiée ici car $T$ n'est pas unitaire. On va donc multiplier $J_{Q_p}$ par une certaine puissance de $\mu$, le coefficient dominant de $T$. Notons $s = 2^n - k$ le degré de $T$.

On va montrer que pour tout entier $p \geq 2$, on a $\lim \mu^{ps} J_{Q_p} = 0$ et $\mu^{ps} J_{Q_p} \in \mathbb{Z}$. Ensuite, nous montrerons qu'il existe un nombre premier p assez grand tel que $\mu^{ps} J_{Q_p} \neq 0$, d'où l'absurdité.

Montrons d'abord qu'il existe $B$ et $C$ tels que pour tout p, $|\mu^{ps} J_{Q_p}| \leq C \frac{B^{p-1}}{(p-1)!}$.
D'après le lemme 3 on a, $\forall \alpha \in \{z \in \mathbb{C},\ T(z) = 0\}$,

$$\begin{aligned} |I(Q_p, \alpha)| &\leq |\alpha| e^{|\alpha|} \sup_{t \in [0,1]} (|Q_p(t\alpha)|) \\ &\leq re^r \frac{\sup\{|z^{p-1}(T(z))^p|,\ z \in D\}}{(p-1)!} \\ &\leq re^r \frac{r^{p-1}(\sup\{|T(z)|,\ z \in D\})^p}{(p-1)!} \end{aligned}$$

avec $r = \sup\{|z|,\ T(z) = 0\}$ et $D = \{|z| \leq r\}$ indépendants de $\alpha$.
Donc

$$|\mu^{ps} J_{Q_p}| \leq \mu^{ps} sre^r \frac{r^{p-1}(\sup\{|T(z)|,\ z \in D\})^p}{(p-1)!} \leq C \frac{B^{p-1}}{(p-1)!}$$

avec $B = \mu^s r \sup\{|T(z)|,\ z \in D\}$ et $C = Bse^r$ indépendants de p.

Or, $\lim\limits_{p \to \infty} \dfrac{B^{p-1}}{(p-1)!} = 0$. Ainsi, $\lim\limits_{p \to \infty} \mu^{ps} J_{Q_p} = 0$.

Montrons maintenant que pour tout p, $\mu^{ps} J_{Q_p} \in \mathbb{Z}$.
D'après le lemme 3 on a

$$\begin{aligned} \mu^{ps} J_{Q_p} &= \mu^{ps} \sum_{T(\alpha)=0} \left( e^\alpha \sum_{j=0}^{\infty} Q_p^{(j)}(0) - \sum_{j=0}^{\infty} Q_p^{(j)}(\alpha) \right) \\ &= \mu^{ps} \left( \sum_{T(\alpha)=0} e^\alpha \right) \left( \sum_{j=0}^{\infty} Q_p^{(j)}(0) \right) - \mu^{ps} \sum_{T(\alpha)=0} \left( \sum_{j=0}^{\infty} Q_p^{(j)}(\alpha) \right) \\ &= -k\mu^{ps} \left( \sum_{j=0}^{\infty} Q_p^{(j)}(0) \right) - \sum_{j=0}^{\infty} \left( \sum_{T(\alpha)=0} \mu^{ps} Q_p^{(j)}(\alpha) \right) \end{aligned}$$

car $\sum\limits_{T(\alpha)=0} e^\alpha = -k$.

0 est une racine de $Q_p$ d'ordre $p-1$ car $T(0) \neq 0$.
Si $j < p-1$,

$$Q_p^{(j)}(0) = 0.$$

Si $j > p-1$,

$$Q_p^{(j)}(0) \in p\mathbb{Z}.$$

En effet, $(p-1)!Q_p \in \mathbb{Z}[X]$ donc, d'après le lemme 4,

$$(p-1)!Q_p^{(j)} \in j!\mathbb{Z}[X] \subset p!\mathbb{Z}[X].$$

Si $j = p-1$,

$$Q_p = \frac{1}{(p-1)!}X^{p-1}T^p.$$

Ainsi, en appliquant la formule de Leibniz, on a

$$Q_p^{(p-1)} = T^p + \sum_{k=1}^{p-1} \binom{p-1}{k} \frac{1}{k!} X^k (T^p)^{(k)}.$$

En évaluant en 0, on obtient donc

$$Q_p^{(p-1)}(0) = (T(0))^p \in \mathbb{Z}^*.$$

Toutes les racines de $T$ sont des racines de $Q_p$ d'ordre supérieur à $p$.
Si $j < p$,

$$\sum_{T(\alpha)=0} \mu^{ps} Q_p^{(j)}(\alpha) = 0.$$

Si $j \geq p$, on a, d'après le lemme 4, $\exists \tilde{Q}_p \in \mathbb{Z}[X]$, tel que $(p-1)!Q_p^{(j)} = j!\tilde{Q}_p$.
Donc,

$$\sum_{T(\alpha)=0} \mu^{ps} Q_p^{(j)}(\alpha) = \frac{j!}{(p-1)!} \sum_{T(\alpha)=0} \mu^{ps} \tilde{Q}_p(\alpha).$$

De plus, $\deg \tilde{Q}_p = \deg Q_p^{(j)} = p - 1 + ps - j = m$. Donc, $\tilde{Q}_p = \sum_{l=0}^{m} \gamma_l X^l$.
Ainsi,

$$\sum_{T(\alpha)=0} \mu^{ps} \tilde{Q}_p(\alpha) = \sum_{l=0}^{m} \mu^{ps-l} \gamma_l \sum_{T(\alpha)=0} \mu^l \alpha^l.$$

$\mu^{ps-l} \in \mathbb{Z}$ car $\mu \in \mathbb{Z}$ et $ps - l \geq ps - m \geq 1 - p + j \geq 0$, car $j \geq p$.
De plus, $\forall l \in \mathbb{N}$,

$$\sum_{T(\alpha)=0} \mu^l \alpha^l \in \mathbb{Z}.$$

En effet, si $l = 0$, on a le résultat.
Et si $l > 0$, on pose

$$\begin{aligned}\tilde{T} &= \prod_{T(\alpha)=0} (X - \mu\alpha) \\ &= X^s + \sum_{t=1}^{s} (-1)^t \Sigma_t^s(\mu\alpha_1, \cdots, \mu\alpha_s) X^{s-t} \\ &= X^s + \sum_{t=1}^{s} (-1)^t \mu^t \Sigma_t^s(\alpha_1, \cdots, \alpha_s) X^{s-t}.\end{aligned}$$

Or, $\mu\Sigma_t^s(\alpha_1, \cdots, \alpha_s) \in \mathbb{Z}$ car $T = \mu \prod (X - \alpha_t) \in \mathbb{Z}[X]$.
Donc $\tilde{T} \in \mathbb{Z}[X]$.
Ainsi,

$$\sum_{T(\alpha)=0} \mu^l \alpha^l = \sum_{\tilde{T}(\alpha)=0} \alpha^l$$

est un polynôme symétrique à coefficients entiers en les racines de $\tilde{T}$. Il s'écrit donc comme un polynôme à coefficients entiers en les coefficients de $\tilde{T}$, qui sont en fait les polynômes symétriques élémentaires en les racines de $\tilde{T}$, car $\tilde{T}$ est unitaire.
$\tilde{T}$ étant à coefficients entiers, on a $\sum_{T(\alpha)=0} \mu^l \alpha^l \in \mathbb{Z}$.

Finalement,

$$\sum_{T(\alpha)=0} \mu^{ps} \tilde{Q}_p(\alpha) \in \mathbb{Z}$$

puis,

$$\sum_{T(\alpha)=0} \mu^{ps} Q_p^{(j)}(\alpha) \in \frac{j!}{(p-1)!}\mathbb{Z} \subset p\mathbb{Z}$$

car $j \geq p$.

Revenons au résultat souhaité.
On a

$$\mu^{ps} J_{Q_p} = -k\mu^{ps} \left( \sum_{j=0}^{\infty} Q_p^{(j)}(0) \right) - \sum_{j=0}^{\infty} \left( \sum_{T(\alpha)=0} \mu^{ps} Q_p^{(j)}(\alpha) \right)$$

avec

$$-k\mu^{ps} \left( \sum_{j=0}^{\infty} Q_p^{(j)}(0) \right) \in -k\mu^{ps} T(0)^p + p\mathbb{Z}$$

et

$$-\sum_{j=0}^{\infty} \left( \sum_{T(\alpha)=0} \mu^{ps} Q_p^{(j)}(\alpha) \right) \in p\mathbb{Z}.$$

Ainsi $\mu^{ps} J_{Q_p} \in -k\mu^{ps} T(0)^p + p\mathbb{Z}$ et en particulier $\mu^{ps} J_{Q_p} \in \mathbb{Z}$.

On a montré que $\lim \mu^{ps} J_{Q_p} = 0$ et $\mu^{ps} J_{Q_p} \in \mathbb{Z}$.
Donc $\exists N$, $\forall p \geq N$, $|\mu^{ps} J_{Q_p}| < 1$ et ainsi $\mu^{ps} J_{Q_p} = 0$.

Montrons qu'il existe un nombre premier $p > N$ tel que $\mu^{ps} J_{Q_p} \neq 0$.
On a montré précédemment que $\mu^{ps} J_{Q_p} \in -k\mu^{ps} T(0)^p + p\mathbb{Z}$, ceci pour tout $p \geq 2$.
On choisit de prendre p un nombre premier supérieur à $k|\mu|^s|T(0)| + N + 42$.
Ainsi, p ne divise pas $-k\mu^{ps} T(0)^p$ car sinon, par le lemme de Gauss, p diviserait $k$ ou $|\mu|^s$ ou $|T(0)|$ qui sont tous non nuls et inférieurs à p.
Donc p ne divise pas $\mu^{ps} J_{Q_p}$ et ainsi $\mu^{ps} J_{Q_p} \neq 0$.
Ceci est absurde car $p > N$.
$\pi$ est donc transcendant. □

*Remarque :* Nous avons donc montré la transcendance de $e$ et de $\pi$. Nous avons vu que les $I(P, z)$ jouaient un rôle essentiel pour trouver une absurdité dans ces démonstrations. Les deux démonstrations se ressemblent, mais pour $\pi$, nous avons du utiliser des résultats supplémentaires, notamment sur les polynômes symétriques.
De plus, la transcendance de $e$ et de $\pi$ impliquent leur irrationalité.

# Annexes

## Historique

Ce n'est qu'à partir du XVII$^{\text{ème}}$ siècle que l'on commence à distinguer la notion de nombre algébrique de celle de nombre réel.
Il faut encore attendre deux siècles de plus pour qu'en 1844 Liouville démontre, par une preuve constructive, l'existence des nombres transcendants. Quelques décennies plus tard, Cantor démontre en 1874 que ces nombres sont même en infinité non dénombrable.
Hermite et Lindemann ont démontré la transcendance de $e$ et $\pi$ respectivement en 1873 et 1882. Plus précisément, Lindemann a démontré le théorème dit d'Hermite-Lindemann qui a pour corollaire la transcendance de $e$ et $\pi$.
Il faut ensuite attendre 1929 pour que de nouveaux résultats significatifs soient démontrés.

# Quelques résultats

Le théorème d'Hermite-Lindemann est un des premiers résultats importants sur les nombres transcendants.

**Théorème d'Hermite-Lindemann**
*Soit $\alpha$ un nombre algébrique non nul. Alors $e^{\alpha}$ est transcendant.*

En 1934, un résultat complétant ce théorème a été démontré, le théorème de Gelfond-Schneider.

**Théorème de Gelfond-Schneider**
*Soient $\alpha$ un nombre algébrique différent de 0 et de 1 et $\beta$ est un nombre algébrique irrationnel. Alors $\alpha^{\beta}$ est un nombre transcendant.*

On en déduit que $e$, $\pi$, $2^{\sqrt{2}}$ et $\ln(2)$ sont des exemples de nombres transcendants.
Cependant il existe encore de nombreux problèmes ouverts. Par exemple, on sait que $e^{\pi}$ est transcendant mais on ignore si $\pi^{e}$ l'est. On ignore également si $\gamma$, la constante d'Euler, est transcendante, on ne sait même pas si elle est irrationnelle. On sait que l'un au moins des nombres $e + \pi$ et $e\pi$ est transcendant.

L'ensemble des nombres de Liouville possède également plusieurs propriétés intéressantes. Cet ensemble est dense dans $\mathbb{R}$, de mesure de Lebesgue nulle, mais non dénombrable.
De plus, Erdös a établi en 1962 le résultat remarquable suivant :

**Théorème d'Erdös**
*Tout nombre réel peut s'écrire comme somme et comme produit de deux nombres de Liouville.*

# Bibliographie


[1] D. Duverney, *Théorie des nombres*, Dunod

[2] P. Tauvel, *Corps commutatifs et théorie de Galois*, Calvage & Mounet

[3] A. Prouté, *Transcendance de e et π pour les nuls* :
http://people.math.jussieu.fr/~alp/e_et_pi_transcendants.pdf

[4] G. Villemin, *Nombres transcendants* :
http://villemin.gerard.free.fr/Wwwgvmm/Type/Transcen.htm