Quelques résultats de trancendance

Dans ce texte, nous allons passer en revue quelques résultats et conjectures classiques de transcendance. Nous verrons au fur et à mesure un certain nombre d'applications élémentaires des résultats énoncés.

Notre propos ici n'est pas de donner les démonstrations de ces résultats, qui sont pour la plupart assez techniques.

1 Les théorèmes

Rappelons tout d'abord quelques définitions. Un nombre complexe α est dit algébrique s'il est racine d'un polynôme (non nul) à coefficients entiers. Dans le cas contraire, α est dit transcendant.

On note $\bar{\mathbb{Q}}$ l'ensemble des nombres algébriques.

Proposition 1.1 *$\bar{\mathbb{Q}}$ est un sous-corps de $\mathbb{C}$.*

N.B. Cette propriété est un peu moins évidente à démontrer qu'il n'y paraît. Nous en donnons une preuve en annexe A.

1.1 Un premier exemple de nombre trancendant

Le premier nombre transcendant a été construit par Liouville en 1844. Il s'agit d'un nombre qui admet de très bonnes approximations par des rationnels, en l'occurrence $\sum_{k=1}^{\infty} 10^{-k!}$.

Bien que la méthode classique pour montrer qu'il est transcendant soit assez particulière (elle ne se transpose pas pour e ou π par exemple), nous allons l'exposer. Le point intéressant ici est justement que ce nombre est "trop près" d'une suite de rationnels pour pouvoir être algébrique.

Théorème 1.2 *Le nombre de Liouville $l = \sum_{k=1}^{\infty} 10^{-k!}$ est transcendant.*

N.B. Tout d'abord, l est irrationnel. Dans le cas contraire, si l'on écrit $l = \dfrac{p}{q}$, on aurait $lq = p$ entier, ce qui n'est pas possible : si $n \geq 2$ est tel que $10^{n!} \geq q$, alors :

$$lq10^{n!} = \sum_{k=1}^{n} \frac{q10^{n!}}{10^{k!}} + q \sum_{k=n+1}^{\infty} \frac{q10^{n!}}{10^{k!}}$$

Dans cette égalité, on a $lq10^{n!} = p10^{n!}$ entier, la somme $\sum_{k=1}^{n} \dfrac{q10^{n!}}{10^{k!}}$ qui est entière elle aussi, mais le dernier terme $q \sum_{k=n+1}^{\infty} \dfrac{q10^{n!}}{10^{k!}}$, strictement positif, peut facilement être majoré strictement par 1. On obtient donc une contradiction, c'est-à-dire que l est irrationnel.

Démonstration Soit $\mathrm{P} = a_n \mathrm{X}^n + \ldots + a_0$ un polynôme à coefficients entiers qui annule le nombre de Liouville l. Si $\frac{p}{q}$ est un rationnel, on peut alors calculer la valeur de P en $\frac{p}{q}$:

$$\mathrm{P}\left(\frac{p}{q}\right) = a_n \left(\frac{p}{q}\right)^n + \ldots + a_0 = \frac{a_n p^n + a_{n-1} p^{n-1} q + \ldots + a_0 q^n}{q^n} = \frac{m}{q^n}$$

où m est un entier. Or P a un nombre fini de zéros, on peut donc se restreindre à un intervalle dans lequel l est le seul zéro de P. Dans un tel intervalle, comme l est irrationnel, $\frac{p}{q}$ ne peut être racine de P.

L'entier m obtenu sera alors non nul, d'où la minoration :

$$|\mathrm{P}\left(\frac{p}{q}\right)| \geq \frac{1}{q^n}$$

Or $\mathrm{P}\left(l\right) = a_n l^n + \ldots + a_0 = 0$. En combinant cette égalité avec ce qui précède, on obtient :

$$|a_n \left(\left(\frac{p}{q}\right)^n - l^n\right) + \ldots + a_1 \left(\frac{p}{q} - l\right)| = |\mathrm{P}\left(\frac{p}{q}\right)| \geq \frac{1}{q^n}$$

On peut factoriser par $\frac{p}{q} - l$ dans le membre de gauche, ce qui donne :

$$|\frac{p}{q} - l|.|a_n \sum_{i=0}^{n-1} \left(\frac{p}{q}\right)^i l^{n-1-i} + \ldots + a_1| \geq \frac{1}{q^n}$$

Pour obtenir une minoration effective de $|\frac{p}{q} - l|$, il ne nous reste plus qu'à majorer l'autre valeur absolue, soit l'expression $|a_n \sum_{i=0}^{n-1} \left(\frac{p}{q}\right)^i l^{n-1-i} + \ldots + a_1|$. Or on s'aperçoit facilement que l est plus petit que 1, par exemple, aussi on peut également se restreindre à l'intervalle $]\,0\,;1\,[$ pour le rationnel $\frac{p}{q}$.

L'expression peut alors être majorée par :

$$\max_{i \leq n} |a_i| \left(n + (n-1) + \ldots + 1\right) = \max_{i \leq n} |a_i| \frac{n\left(n+1\right)}{2}$$

c'est-à-dire une constante C qui ne dépend que du polynôme P.

On obtient alors la minoration :

$$\boxed{|\frac{p}{q} - l| \geq \frac{1}{\mathrm{C} q^n}}$$

Mais considérons plus attentivement le nombre l. Des approximations rationnelles naturelles pour l sont bien sûr les sommes finies du type $\sum_{k=1}^{\mathrm{N}} 10^{-k!}$, dont le dénominateur est $10^{\mathrm{N}!}$. Le résultat précédent nous dit donc qu'à partir d'un certain rang :

$$l - \sum_{k=1}^{\mathrm{N}} 10^{-k!} = \sum_{k=\mathrm{N}+1}^{\infty} 10^{-k!} \geq \frac{1}{\mathrm{C}10^{n\mathrm{N}!}}$$

(En effet il faut pour cela que la somme partielle $\sum_{k=1}^{\mathrm{N}} 10^{-k!}$ soit dans l'intervalle dans lequel l est seul racine du polynôme. Comme ces sommes partielles constituent une suite croissante qui tend vers l, tous ces termes sont dans l'intervalle en question à partir d'un certain rang.)

Nous allons voir qu'en prenant N assez grand, on obtient une contradiction. Rappelons que n et C sont fixés, ne dépendent donc pas de q, c'est-à-dire de N.

Nous pouvons alors majorer la somme $\sum_{k=\mathrm{N}+1}^{\infty} 10^{-k!}$ par $2.10^{-(\mathrm{N}+1)!}$, c'est à dire deux fois le premier terme de la somme (cette majoration se comprend facilement si l'on considère les développement décimaux de ces deux valeurs : la somme $\sum_{k=\mathrm{N}+1}^{\infty} 10^{-k!}$ a un développement de la forme $0,0\ldots010\ldots010\ldots$, le premier 1 étant en $(\mathrm{N}+1)$!-ème position après la virgule. Ce nombre est clairement plus petit que le deuxième, dont l'écriture décimale est $0,0\ldots02$, où le chiffre 2 apparaît là aussi en $(\mathrm{N}+1)$!-ème position après la virgule.)

L'assertion précédente implique alors que pour tout N, on a l'inégalité :

$$2.10^{-(\mathrm{N}+1)!} \geq \frac{1}{\mathrm{C}10^{n\mathrm{N}!}}$$

soit de manière équivalente $10^{\mathrm{N}!(n-\mathrm{N}-1)} \geq \dfrac{1}{2\mathrm{C}}$. Or la quantité $10^{\mathrm{N}!(n-\mathrm{N}-1)}$ tend bien sûr vers 0 lorsque N tend vers l'infini, d'où une contradiction.

Notre hypothèse, à savoir que l est racine d'un polynôme à coefficients entiers, est donc absurde, et l est bien transcendant.

$\square$

1.2 Théorèmes classiques de transcendance

Un manière d'obtenir d'autres nombres transcendants est de prendre la valeur de certaines fonctions en des points algébriques ; dans cette perspective, on a le théorème suivant :

Théorème 1.3 (Hermite-Lindemann) *Soit α un nombre complexe non nul, algébrique. Alors $\exp(\alpha)$ est transcendant.*

Corollaire 1.4 *Les nombres π et e sont donc transcendants.*

Démonstration du corollaire :

- 1 est rationnel, donc algébrique. D'après le théorème précédent, $e = e^1$ est donc transcendant.
- Pour ce qui est de π, c'est le contraire : si π était algébrique, alors $i\pi$ le serait aussi (i est bien sûr algébrique, et l'ensemble des nombres algébriques $\bar{\mathbb{Q}}$ est un sous-corps de $\mathbb{C}$). Le théorème d'Hermite-Lindemann nous assurerait alors que $e^{i\pi}$ est transcendant. Mais comme $e^{i\pi} = -1$, ceci est absurde, et donc π est bien transcendant. $\square$

N.B. Historiquement, c'est Hermite qui a démontré la transcendance de e en 1873, puis Lindemann celle de π en 1882. On peut trouver un exposé clair et complet de leurs méthodes dans [1], chapitre 2.

N.B. Ce théorème implique aussi que $\log(2)$ est transcendant ; il en est de même du logarithme de tout nombre algébrique différent de 0 et 1 (La démonstration de la transcendance de π s'applique telle quelle).

On a aussi le théorème suivant, démontré indépendamment (et par des méthodes différentes) par Gel'fond et Schneider, en 1934 :

Théorème 1.5 (Gel'fond-Schneider) *Soient α et β algébriques, avec α non nul et β non rationnel. Soit $\log(\alpha)$ une détermination quelconque, non nulle, du logarithme de α. Alors $\alpha^\beta = \exp(\beta \log(\alpha))$ est transcendant.*

Les théorèmes cités jusqu'à présent permettent d'exhiber des nombres transcendants (par exemple $e^{\sqrt{2}}$, $2^{\sqrt{3}}$ et $\dfrac{\log(3)}{\log(2)}$). Ils sont démontrés en appendice de [3] ou au Chapitre III de [2] (ces démonstration sont assez complexes et nécessitent quelques notions sur les extensions de corps et d'analyse complexe). Dans le Chapitre II de ce même ouvrage, on peut trouver une démonstration du théorème suivant, attribué en général à Siegel, Lang et Ramachandra :

Théorème 1.6 (des six exponentielles) *Soient x_1 et x_2 des nombres complexes, linéairement indépendants sur $\mathbb{Q}$. Soient y_1, y_2 et y_3 des nombres complexes, linéairement indépendants sur $\mathbb{Q}$. Alors l'un au moins des six nombres $\exp(x_i y_j)$ ($i \in \{1,2\}$, $j \in \{1,2,3\}$) est transcendant.*

N.B. Lorsque l'on parle d'indépendance linéaire sur $\mathbb{Q}$ d'une famille de nombres complexes, l'on se place dans le corps $\mathbb{C}$ des complexes, considéré alors comme un espace vectoriel sur le corps $\mathbb{Q}$ des rationnels. Une famille linéairement indépendante sur $\mathbb{Q}$ est une famille libre de vecteurs. Par exemple, la famille (x_1, x_2) est liéairement indépendante sur $\mathbb{Q}$ si, quel que soit le couple (λ_1, λ_2) de rationnels distinct du couple $(0,0)$, la combinaison linéaire $\lambda_1 x_1 + \lambda_2 x_2$ est non nulle.

Corollaire 1.7 *Soit t un nombre complexe tel que 2^t, 3^t et 5^t soient entiers. Alors t est un entier.*

Démonstration du corollaire : Dans un premier temps, montrons que t est un nombre rationnel. Si ce n'était pas le cas, la famille $(1, t)$ serait libre sur $\mathbb{Q}$. Or on voit facilement que la famille $(\log(2), \log(3), \log(5))$ est libre sur $\mathbb{Q}$:

Soient $\lambda_1, \lambda_2, \lambda_3$ des rationnels tels que :

$$\lambda_1 \log(2) + \lambda_2 \log(3) + \lambda_3 \log(5) = 0$$

Quitte à multiplier l'expression précédente par un dénominateur commun à λ_1, λ_2, et λ_3, on peut les supposer entiers. Mais alors, en passant aux exponentielles dans cette expression, on obtient :

$$e^{\lambda_1 \log(2)}.e^{\lambda_2 \log(3)}.e^{\lambda_3 \log(5)} = 1$$

c'est-à-dire $2^{\lambda_1}.3^{\lambda_2}.5^{\lambda_3} = 1$. Par unicité de la décomposition en facteurs premiers (car $\mathbb{Z}$ est un anneau factoriel !), on en déduit $\lambda_1 = \lambda_2 = \lambda_3 = 0$. C'est-à-dire que la famille $(\log(2), \log(3), \log(5))$ est bien libre sur $\mathbb{Q}$.

On obtient alors une contradiction avec le théorème 1.6 : les six exponentielles obtenues sont 2^1, 3^1, 5^1, 2^t, 3^t et 5^t. Elles sont toutes entières, donc algébriques. D'où $t \in \mathbb{Q}$.

On a donc $t = \dfrac{p}{q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^\star$. Par hypothèse, $2^{\frac{p}{q}}$ est un entier m, ce qui s'écrit $2^p = m^q$. Par unicité de la décomposition en facteurs premiers, m est nécessairement une puissance (entière) de 2, ce qui montre que $t = \dfrac{p}{q}$ est en fait un entier.

$\square$

2 Les conjectures

2.1 Indépendance algébrique et degré de transcendance

Ce paragraphe est consacré au rappel de quelques définitions classiques qui serviront dans la suite de cette section.

Définition Des complexes $\alpha_1, \ldots, \alpha_n$ sont dits *algébriquement indépendants* (sur $\mathbb{Q}$) s'il n'existe aucun polynôme $\mathrm{P}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$ non nul, à coefficients entiers, tel que $\mathrm{P}(\alpha_1, \ldots, \alpha_n) = 0$.

Exemple : Les deux réels $\alpha_1 = l$ et $\alpha_2 = l^2$, tous deux transcendants, ne sont pas algébriquement indépendants (l est le nombre de Liouville étudié dans la première partie). En effet, on a par définition $\alpha_2 = \alpha_1^2$, c'est-à-dire que le polynôme $\mathrm{P}\left(\mathrm{X}_1, \mathrm{X}_2\right) = \mathrm{X}_2 - \mathrm{X}_1^2$, à coefficients entiers, est tel que $\mathrm{P}\left(\alpha_1, \alpha_2\right) = 0$.

N.B. On définit de même l'indépendance algébrique sur $\bar{\mathbb{Q}}$, en considérant les polynômes P à coefficients algébriques. On montre qu'une famille de nombres complexes est algébriquement indépendante sur $\mathbb{Q}$ si, et seulement si, elle l'est sur $\bar{\mathbb{Q}}$. On pourra donc parler d'indépendance algébrique sans préciser le corps de base ; il est sous-entendu que dans ce cas il s'agira de $\mathbb{Q}$ ou de $\bar{\mathbb{Q}}$, et les deux sont équivalents.

Notation Soient $\alpha_1, \ldots, \alpha_n$ des nombres complexes. On note $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ le plus petit sous-corps de $\mathbb{C}$ (pour l'inclusion) qui contienne $\alpha_1, \ldots, \alpha_n$.

Définition On appelle *degré de transcendance* (sur $\mathbb{Q}$) d'un sous-corps L de $\mathbb{C}$ le nombre maximal d'éléments de L algébriquement indépendants sur $\mathbb{Q}$.

Exemples :

- Les corps inclus dans $\bar{\mathbb{Q}}$ sont exactement ceux qui ont un degré de transcendance nul sur $\mathbb{Q}$.
- Le degré de transcendance sur $\mathbb{Q}$ de $\mathbb{Q}(\pi)$ est 1, car π est transcendant.
- Le corps $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ a un degré de transcendance sur $\mathbb{Q}$ égal à n si, et seulement si, les nombres $\alpha_1, \ldots, \alpha_n$ sont algébriquement indépendants sur $\mathbb{Q}$.

2.2 Quelques conjectures

La conjecture suivante est probablement la plus vaste concernant la fonction exponentielle :

Conjecture 2.1 (Schanuel) *Soient* $x_1, \ldots, x_n$ *des nombres complexes, pris linéairement indépendants sur* $\mathbb{Q}$. *Alors le degré de transcendance (sur* $\mathbb{Q}$*) du corps* $\mathbb{Q}(x_1, \ldots, x_n, \exp(x_1), \ldots, \exp(x_n))$ *est supérieur ou égal à* n.

N.B. La conclusion de cette conjecture signifie que parmi les $2n$ nombres $x_1, \ldots, x_n, \exp(x_1), \ldots, \exp(x_n)$, on peut en trouver au moins n qui soient algébriquement indépendants sur $\mathbb{Q}$. C'est bien sûr le maximum possible en général : si l'on prend pour les x_i des nombres de la forme $\log(p_i)$, avec les p_i des nombres premiers deux à deux distincts, un raisonnement analogue à celui utilisé pour démontrer le corollaire 1.7 nous assure que les nombres x_i sont linéairement indépendants sur $\mathbb{Q}$. Et comme pour tout i, $\exp(x_i) = p_i$ est entier donc rationnel, le degré de transcendance de $\mathbb{Q}(x_1, \ldots, x_n, \exp(x_1), \ldots, \exp(x_n))$ est au plus égal à n.

En prenant $x_1 = 1$ et $x_2 = i\pi$, on déduit de cette conjecture que e et π sont algébriquement indépendants ; démontrer cette indépendance constitue un problème ouvert.

Dans le théorème des six exponentielles, il est tentant de remplacer 6 par 4 ; cela mène à la conjecture suivante,

Conjecture 2.2 (des quatre exponentielles) *Soient* x_1 *et* x_2 *des nombres complexes, linéairement indépendants sur* $\mathbb{Q}$.

Soient y_1 *et* y_2 *des nombres complexes, linéairement indépendants sur* $\mathbb{Q}$.

Alors l'un au moins des quatre nombres $\exp(x_i y_j)$ *(*$i \in \{1,2\}$, $j \in \{1,2\}$*) est transcendant.*

Tout comme le théorème des six exponentielles implique le corollaire 1.7, cette conjecture implique la suivante :

Conjecture 2.3 *Si* x *est un nombre complexe tel que* 2^x *et* 3^x *soient entiers, alors* x *est un entier.*

Démonstration (de l'implication) : Soit x un nombre complexe tel que 2^x et 3^x soient entiers. D'abord, la conjecture des quatre exponentielles implique qu'un tel x est rationnel :

Sinon la famille $1, x$ est linéairement indépendante sur $\mathbb{Q}$. Or nous avons vu que la famille $\log(2)$, $\log(3)$, $\log(5)$ est linéairement indépendante sur $\mathbb{Q}$, en particulier la sous-famille $\log(2), \log(3)$ l'est aussi (plus simplement, ceci revient à dire que le rapport $\dfrac{\log(2)}{\log(3)}$ n'est pas rationnel. Et la relation $\dfrac{\log(2)}{\log(3)} = \dfrac{p}{q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^\star$ s'écrirait aussi $\log(2^q) = \log(3^p)$, d'où $2^q = 3^p$, ce qui est contradictoire.)

En appliquant la conjecture des quatre exponentielles, on aurait alors l'un des quatre nombres $e^{1.\log(2)}$, $e^{1.\log(3)}$, $e^{x.\log(2)}$, ou $e^{x.\log(3)}$ qui serait transcendant. Mais ces nombres sont respectivement égaux à 2, 3, 2^x, et 3^x, donc tous entiers par hypothèse. Nous obtenons donc une contradiction avec la conjecture 2.2, et donc x est bien rationnel.

Là encore, on conclut que x est entier par le même argument :

On a $x = \dfrac{p}{q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^\star$. Par hypothèse, $2^{\frac{p}{q}}$ est un entier m, ce qui s'écrit $2^p = m^q$. Par unicité de la décomposition en facteurs premiers, m est nécessairement une puissance (entière) de 2, ce qui montre que $x = \dfrac{p}{q}$ est en fait un entier.

La conjecture des quatre exponentielles implique bien la conjecture 2.3.

□

N.B. On peut remarquer que l'hypothèse 2^x, 3^x et 5^x entiers permet d'affirmer que x est entier (corollaire 1.7). Si l'on enlève l'hypothèse 5^x entier, cela devient une conjecture. En revanche, celle-ci est "minimale", car l'hypothèse encore plus faible 2^x entier n'implique pas que x est entier.

Par exemple, pour $x = \dfrac{\log(3)}{\log(2)}$, on a :

$$2^x = e^{x \log(2)} = e^{\log(3)} = 3$$

c'est-à-dire que 2^x est entier, or nous avons montré que le rapport $\dfrac{\log(3)}{\log(2)}$ n'est pas rationnel. *A fortiori* il ne peut être entier.

Annexe : L'ensemble $\bar{\mathbb{Q}}$ des nombres algébriques est un corps

L'ensemble $\bar{\mathbb{Q}}$ est, comme nous l'avons vu, l'ensemble des nombres qui sont racine d'un polynôme à coefficients rationnels (ou entiers, ce qui revient au même).

Comme tout polynôme à coefficients dans $\mathbb{C}$ a ses racines dans $\mathbb{C}$ (ce qui se dit aussi en terme savants : "le corps $\mathbb{C}$ des complexes est algébriquement clos"), $\bar{\mathbb{Q}}$ est un sous ensemble de $\mathbb{C}$. Il nous suffit donc de montrer que $\bar{\mathbb{Q}}$ est un sous-corps de $\mathbb{C}$, c'est-à-dire qu'il est stable par passage à l'opposé, à l'inverse, par addition et par multiplication.

Pour tout ceci, nous allons utiliser le :

Lemme .1 *Soit α un complexe contenu dans une extension de $\mathbb{Q}$ de degré fini. Alors α est algébrique.*

Démonstration : C'est ni plus ni moins qu'une reformulation de la définition d'un nombre algébrique. Soit donc α un complexe contenu dans une extension de $\mathbb{Q}$ de degré fini. Cette extension est à la fois un corps et un espace vectoriel sur $\mathbb{Q}$, de dimension finie n.

C'est un corps, donc elle contient toutes les puissances de α, *i.e.* la suite $1, \alpha, \alpha^2, \ldots$

Comme c'est un espace vectoriel de dimension n sur $\mathbb{Q}$, la famille à $n+1$ élements $\left(1, \alpha, \alpha^2, \ldots, \alpha^n\right)$ est liée sur $\mathbb{Q}$, c'est-à-dire qu'il existe des rationnels $a_0, a_1, \ldots, a_n$ non tous nuls, et tels que

$$a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n = 0$$

Mais alors le polynôme $\mathrm{P} = \sum_{k=0}^{n} a_k \mathrm{X}^k$ est un polynôme à coefficients rationnels qui annule α, et donc α est algébrique.

$\square$

Nous sommes désormais en mesure de démontrer que $\bar{\mathbb{Q}}$ est un corps :
soit α un nombre algébrique. Soit $\mathbb{Q}[\alpha]$ le corps engendré par $\mathbb{Q}$ et α. Le corps $\mathbb{Q}[\alpha]$ est une extension de $\mathbb{Q}$ de degré fini, qui contient $-\alpha$ et $\frac{1}{\alpha}$ ($\frac{1}{\alpha}$ peut s'exprimer comme un polynôme en α). D'après le lemme, ces deux nombres sont donc eux-mêmes algébriques.

Soit maintenant deux nombres algébriques α et β. β est racine d'un polynôme à coefficients rationnels donc dans $\mathbb{Q}[\alpha]$. β est donc dans une extension de degré fini de $\mathbb{Q}[\alpha]$, notée $\mathbb{Q}[\alpha, \beta]$. Mais alors $\mathbb{Q}[\alpha, \beta]$ est un espace vectoriel de dimension finie sur $\mathbb{Q}[\alpha]$, qui est lui-même de dimension finie sur $\mathbb{Q}$. $\mathbb{Q}[\alpha, \beta]$ est donc une extension finie de $\mathbb{Q}$.

Or les nombres $\alpha + \beta$ et $\alpha\beta$ sont tous deux dans $\mathbb{Q}[\alpha, \beta]$, extension de $\mathbb{Q}$ de degré fini. Ils sont donc algébriques d'après le lemme.

En conclusion, $\bar{\mathbb{Q}}$ est un sous ensemble de $\mathbb{C}$ stable par passage à l'opposé, à l'inverse, par addition et par multiplication. $\bar{\mathbb{Q}}$ est donc un sous-corps de $\mathbb{C}$.

Références

[1] A.N. Parshin, I.R. Shafarevich (Eds.), *Number Theory IV*, Springer, Encyclopaedia of Mathematical Sciences vol 44, 1998.

[2] S. Lang, *Introduction to transcendental numbers*, Addison-Wesley, 1966.

[3] S. Lang, *Algebra*, Addison-Wesley, 1984, 2^{nd} ed.