Les nombres transcendants

Je me suis intéressé à la théorie des nombres transcendants, qui constitue un domaine de recherche actuel, et comme je l'ai constaté par l'intermédiaire de mes contacts, il reste de nombreux problèmes ouverts à ce jour. Pour ma part, j'ai essayé d'assimiler une partie de cette théorie, comprendre certains résultats fondamentaux, et surtout en saisir les démonstrations. Je me suis rendu compte au fur et à mesure de mes recherches et de mes échanges avec certains spécialistes qu'il n'existe pas réellement une théorie des nombres transcendants, au sens où très peu de théorèmes traitent de cas généraux. C'est pourquoi mon travail a plutôt consisté à expliquer différents aspects de cette théorie, qui n'ont pas nécessairement de liens immédiats entre eux.

Table des matières

1 Définitions et premiers résultats

1.1 Définitions

Définition 1 : *On dit que $\alpha \in \mathbb{C}$ est algébrique sur $\mathbb{Q}$ s'il existe $P \in \mathbb{Q}[X]$ tel que $P(\alpha) = 0, P \neq 0$.*

Définition 2 : *Un élément de $\mathbb{C}$ qui n'est pas algébrique sur $\mathbb{Q}$ est dit transcendant.*

On notera $\overline{\mathbb{Q}}$ l'ensemble des nombres algébriques, qui est un sous-corps de $\mathbb{C}$.

Définition 3 : *Pour α nombre algébrique, P_α son polynôme minimal est le polynome unitaire de plus petit degré tel que $P(\alpha) = 0$ et $P \neq 0$.*

Définition 4 : *Le degré d'un nombre algébrique est le degré de son polynôme minimal.*

Définition 5 : *Les conjugués de α, nombre algébrique, sont les racines de son pôlynome minimal*

Les trois définitions suivantes seront utilisées seulement dans la preuve du théorème de Gelfond-Schneider.

Définition 6 : *On dit que α est un entier algébrique s'il est algébrique et si son polynôme minimal est à coefficients entiers*

Théorème et Definition 7 : *Soit α un nombre algébrique. Alors, $\exists k \in \mathbb{N}$ tel que $k\alpha$ soit un entier algébrique. Alors, on appelle dénominateur de α, noté $den(\alpha)$ le plus petit entier positif k tel que $k\alpha$ soit un entier algébrique.*

On peut remarquer que pour un rationnel $\frac{p}{q}$, $den(\frac{p}{q}) = q$.

Définition 8 : *Soit α un nombre algébrique de degré d et soient $\alpha_1 = \alpha, \alpha_2, ..., \alpha_d$ les conjugués de α, la maison de α est définie par :*

$$\overline{|\alpha|} = \max_i |\alpha_i|$$

1.2 La non dénombrabilité des nombres transcendants

On peut montrer par différents procédés que l'ensemble des nombres algébriques est dénombrable, l'idée étant que l'on peut dénombrer les éléments de $\mathbb{Q}[X]$, qui ont eux-mêmes un nombre fini de racines.

$\mathbb{R}$ étant non dénombrable, on en déduit en procédant par l'absurde que *l'ensemble des nombres réels transcendants est non dénombrable.*

On sait alors notamment qu'il en existe, sans toutefois réussir à en exhiber de manière évidente. Cantor a d'ailleurs montré l'existence des nombres transcendants en réussissant à en exhiber seulement de manière implicite.

En effet, partant du fait que $\overline{\mathbb{Q}} \bigcap [0;1]$ est dénombrable, on peut lister ses éléments en écrivant sur chaque ligne d'un tableau infini leur développement en base 10 (par exemple) (à noter que si un nombre admet deux développements différents comme 0,1 et 0,0999... , chacun occupera une ligne distincte). Notons a_{ij} les élements de ce tableau. Considérons alors $b = 0, b_1 b_2 ... b_n ...$ avec $b_i \neq a_{ii}$. Alors b est transcendant, car si l'on suppose le contraire, il existe k tel que le développement de b soit sur la k-ième ligne, et donc cela contredit $b_k \neq a_{kk}$. On a ainsi expliqué le procédé dit de la diagonale de Cantor.

1.3 Nombres de Liouville

Le théorème de Liouville permet cette fois-ci de définir une classe de nombres transcendants et d'en construire de manière explicite et assez simplement, comme on le verra juste après la démonstration de ce théorème.

> Théorème de Liouville :
> *Soit α un nombre réel algébrique de degré $d \geqslant 2$ (donc irrationnel).Il existe alors $C > 0$ tel que, pour tout rationnel $\frac{p}{q}$, on ait :*
> $$\left|\alpha - \frac{p}{q}\right| \geqslant \frac{C}{q^d}$$

Preuve :

Soit $P \in \mathbb{Z}[X]$ obtenu après avoir multiplié le polynôme minimal de α par le PPCM de ses coefficients.

$$P(X) = a_d X^d + ... + a_1 X + a_0$$

$\forall p \in \mathbb{Z}, \forall q \in \mathbb{N}^*$,

$$P\left(\frac{p}{q}\right) = a_d \left(\frac{p}{q}\right)^d + ... + a_1 \frac{p}{q} + a_0$$

Ainsi, $q^d P\left(\frac{p}{q}\right) \in \mathbb{Z}^*$, et on en déduit immédiatement :

$$\left|P\left(\frac{p}{q}\right)\right| \geqslant \frac{1}{q^d}$$

Posons $M = \sup_{x \in [\alpha-1;\alpha+1]} |P'(x)|$. $M > 0$ car $\deg P \geqslant 1$. D'après l'inégalité des accroissements finis entre α et $\frac{p}{q} \in [\alpha - 1; \alpha + 1]$:

$$\left|P\left(\frac{p}{q}\right)\right| \leqslant M \left|\frac{p}{q} - \alpha\right|$$

car $P(\alpha) = 0$

On a alors, $\forall \frac{p}{q} \in [\alpha - 1; \alpha + 1]\,, \left|\alpha - \frac{p}{q}\right| \geqslant \frac{1}{Mq^d}$.

Et si $\frac{p}{q} \notin [\alpha - 1; \alpha + 1]$, $\left|\alpha - \frac{p}{q}\right| > 1 > \frac{1}{q^d}$.

Posant $C = \min\left(1, \frac{1}{M}\right)$, on a bien

$$\left|\alpha - \frac{p}{q}\right| \geqslant \frac{C}{q^d}, \forall \frac{p}{q} \in \mathbb{Q}$$

. □

Une idée importante qui ressort de ce théorème est qu'on approche moins bien les nombres algébriques que les nombres transcendants, par des nombres rationnels. Nous reviendrons sur ce point dans la dernière partie car cette notion d'approximation par des rationnels tient une grande place dans la théorie d'approximation diophantienne, qui a elle-même un lien très étroit avec l'univers des nombres transcendants.

Définition : *Un réel α est appelé nombre de Liouville s'il est irrationnel, et si $\forall n \in \mathbb{N}^*$, $\exists \frac{p_n}{q_n}$ avec $q_n > 0$, tel que $|\alpha - \frac{p_n}{q_n}| < \frac{1}{q_n^n}$*

D'après le théorème précédent, tout nombre de Liouville est transcendant.

Considérons par exemple

$$\alpha = \sum_{k=0}^{\infty} \frac{a_k}{10^{k!}}$$

où $a_k \in [\![0, 9]\!]$ est à support infini. Admettons ici que ce nombre est irrationnel et montrons que ce nombre est de Liouville.

$\forall n \in \mathbb{N}^*$, avec $p_n = 10^{n!} \sum_{k=0} n \frac{a_k}{10^{k!}}$ et $q_n = 10^{n!}$, on a :

$$0 \leqslant \alpha - \frac{p_n}{q_n} = \sum_{k=n+1}^{\infty} \frac{a_k}{10^{k!}} \leqslant \frac{9}{10^{(n+1)!}} \left(1 + \frac{1}{10} + \frac{1}{100} + ...\right) \leqslant \frac{10}{(10^{n!})^n \, 10^{n!}} \leqslant \frac{1}{(q_n)^n}$$

Donc α est un nombre de Liouville, donc transcendant. $\square$

Il s'agit d'un des rares critères de transcendance. En effet, il n'existe pas à proprement parler de théorie des nombres transcendants, mais plutôt quelques techniques permettant d'obtenir des résultats très partiels. Et cela a constitué une des difficultés majeures de mon TIPE.

2 Le théorème de Lindemann-Weierstrass et ses conséquences

Nous allons voir dans cette partie un théorème très fort d'indépendance algébrique, qui permet d'en déduire de nombreux nombres transcendants, parmi lesquels e et Π pour les plus connus.

2.1 Théorème de Lindemann-Weierstrass

Théorème de Lindemann-Weierstrass :
Soient $\alpha_1, ..., \alpha_t, b_1, ..., b_t$ des nombres algébriques avec les α_i deux à deux distincts et les b_i non nuls ; alors

$$b_1 e^{\alpha_1} + ... + b_t e^{\alpha_t} \neq 0$$

Une démonstration de ce théorème est donnée en annexe. Celle que j'ai décidé de présenter dans ce dossier est due à F. Beukers, J. P. Bézivin et P. Robba ; ce n'est pas celle que l'on trouve le plus souvent.

Grâce au développement en série entière de l'exponentielle, on se ramène à un problème concernant des séries. Puis, la théorie de Galois permet de nous ramener à des hypothèses plus favorables en considérant des éléments dans $\mathbb{Q}$. Comme dans toutes les preuves que j'ai pu rencontrée, on procède par l'absurde pour parvenir finalement à une contradiction lorsqu'on obtient une égalité entre deux fractions dont les pôles ne peuvent avoir mêmes ordres.

2.2 Conséquences du théorème de Lindemann-Weierstrass

On peut alors citer quelques théorèmes qui découlent directement du paragraphe précédent, suivi à chaque fois de quelques exemples de nombres transcendants.

<u>Théorème de Hermite-Lindemann</u> :
Soit α un nombre algébrique non nul. Alors e^{α} est transcendant.

<u>Preuve</u> : Supposons $b = e^{\alpha}$ algébrique alors, d'après le théorème de Lindemann-Weierstrass, $e^{\alpha} - b \neq 0$, ce qui est absurde. □

On sait alors que e est transcendant, ainsi que $e^2, \sqrt{e}, e^{\sqrt{2}}, \ldots$ par exemple.

<u>La transcendance de Π</u> provient directement du théorème de Hermite-Lindemann. En effet : Supposons que Π soit algébrique, alors $i\Pi$ l'est également, donc $e^{i\Pi} = -1$, est transcendant, ce qui est absurde. Donc Π est transcendant.

<u>Théorème</u> :
Si $x > 0$ et $x \neq 1$ alors l'un au moins des deux nombres x et $\ln(x)$ est transcendant.

<u>Preuve</u> :
Si x est algébrique, $\ln(x)$ est transcendant, faute de quoi $e^{\ln(x)} = x$ serait transcendant d'après le théorème de Hermite-Lindemann. Sinon, x est transcendant. □

Exemples : $\forall n \in \mathbb{N}, n \geqslant 2, \ln(n)$ est transcendant. $(\ln 2, \ln 3, \ldots)$

<u>Théorème</u> :
Si $a \neq 0$ est algébrique, $\sin(a), \cos(a)$ et $\tan(a)$ sont transcendants.

<u>Preuve</u> :
Supposons $\sin(a)$ algébrique alors d'après le théorème de Lindemann-Weierstrass, comme ia, $-ia$, $\frac{1}{2i}$ sont algébriques,

$$\frac{e^{ia} - e^{-ia}}{2i} - \sin(a) \neq 0$$

ce qui est absurde. On utilise de même la formule d'Euler pour $\cos(a)$. Et si $\tan(a)$ est algébrique, $1 + \tan^2(a) = \frac{1}{\cos^2(a)}$ est algébrique donc $\cos(a)$ est algébrique, d'où la contradiction. □

Exemples : $\sin(1), \cos(1), \cos\left(\sqrt{2}\right), \tan\left(\frac{1+\sqrt{5}}{2}\right), \ldots$

3 Théorème de Gelfond-Schneider

Nous nous intéresserons tout d'abord un théorème dû à Gelfond et Schneider qui démontre la transcendance d'une nouvelle classe de nombres du type α^{β} qui satisfont certaines hypothèses (e^{Π} et $\sqrt{2}^{\sqrt{2}}$ par exemple). Ensuite, nous verrons quelques nombres qui restent mystérieux en ce qui concerne leur caractère algébrique ou non, mais pour lesquels la théorie des nombres transcendants donnent malgré tout des résultats intéressants.

3.1 Le théorème de Gelfond-Schneider

Théorème :
Soit $\alpha \in \overline{\mathbb{Q}}$,$\alpha \notin \{0,1\}$. Soit β un nombre algébrique irrationnel. Alors, α^β est transcendant.

On utilise ici la détermination principale du logarithme complexe, que l'on définit sur $\mathbb{C}^*$ par :

$$\operatorname{Log} \alpha = \ln |\alpha| + i \arg \alpha$$

Ainsi, $\forall \alpha \in \mathbb{C}^*$ et $\forall \beta \in \mathbb{C}$, on a :

$$\alpha^\beta = e^{\beta \operatorname{Log} \alpha}$$

On peut en déduire immédiatement la transcendance de $\sqrt{2}^{\sqrt{2}}$. De plus, $e^\Pi = e^{-i \operatorname{Log}(-1)} = (-1)^{-i}$ est transcendant car -1 est algébrique et $-i$ est algébrique irrationnel. Je donne en annexe la démonstration de ce théorème que j'ai étudié et qui utilise une méthode dû à Schneider. Nous aurons tout d'abord besoin de différents théorèmes préliminaires qu'il m'a fallu étudier également, comme l'inégalité de la taille, le principe du maximum ou encore un lemme de Siegel pour les systêmes d'équation linéaire, dont les démonstrations ne seront pas données ici.

3.2 Quelques nombres encore mystérieux

Malgré les différents théorèmes que nous avons vu jusqu'ici, ceux-ci ne permettent pas de déterminer si certains nombres sont algébriques ou non.

Pour $e + \Pi$, $e - \Pi$, $e\Pi$, $\frac{\Pi}{e}$, $\frac{e}{\Pi}$, Π^Π, e^e ou Π^e, on ne sait pas s'ils sont algébriques ou non, d'ailleurs, on ne sait même pas s'ils sont tous irrationnels.

Cependant, le fait que $\overline{\mathbb{Q}}$ est algébriquement clos fournit des résultats intéressants.

Théorème :
$\overline{\mathbb{Q}}$ est algébriquement clos.

Ce résultat permet d'obtenir le théorème suivant :

Théorème :
Soit a et b deux nombres transcendants, alors l'un au moins des deux nombres ab et $a + b$ est transcendant

Preuve :
En effet, supposons le contraire, alors $P(X) = X^2 - (a + b) X + ab \in \overline{\mathbb{Q}}[X]$. Or $P(X) = (X - a)(X - b)$ et $\overline{\mathbb{Q}}$ est algébriquement clos, donc $(a, b) \in \overline{\mathbb{Q}}^2$ □

Ainsi, bien qu'on ne sache rien sur $e + \Pi$ et $e\Pi$, on peut être sur que l'un au moins de ses deux nombres est transcendant.

Conclusion :

J'ai pu, grâce à mes contacts, m'informer et être orienté sur différents aspects ou théorèmes intéressants relatifs aux nombres transcendants. Je me suis alors rendu compte de l'étendue d'un tel domaine des mathématiques qui fait encore l'objet de nombreuses recherches. Bien que maitriser la théorie des nombres transcendants nécessite une grande expérience dans ce domaine, j'ai voulu développer certains théorèmes abordables qui conduisent à de remarquables résultats de transcendance.

A Bibliographie

[1] Daniel Duverney, *Théorie des nombres, 2° édition* , Dunod, 2007.

[2] Hassan Boualem et Robert Brouzet, *La planète $\mathbb{R}$, Voyage au pays des nombres réels*, Dunod, 2002.

[3] Michel Waldschmidt, *Introduction to Diophantine methods : irrationality and transcendence*, http ://www.math.jussieu.fr/miw/coursHCMUNS2007.html, 2007.

[4] *The American Mathematical Monthly*, Volume 97, N°3, Mars 1990.

[5] Jean-Paul Delahaye, *Le fascinant nombre* Π.

[6] Pierre Eymard et Jean-Pierre Lafon, *Autour du nombre* Π.

[7] Sabah Al Fakir, *Algèbre et théorie des nombres, théorie de Galois et codes géométrie et arithmétique*, Ellipses.

[8] Nathan Jacobson, *Basic algebra 1, second edition.*

B Contacts

Michel Waldschmidt : Professeur à l'université Paris 6, membres de nombreuses institutions (European Mathematical Society, American Mathematical Society, ...), ancien président de la société mathématique de France jusqu'en 2004.

Daniel Duverney : Professeur de mathématiques spéciales au Lycée Baggio de Lille.

C Preuve du théorème de Lindemann-Weierstrass

Théorème de Lindemann-Weierstrass : *Soient $\alpha_1, ..., \alpha_t, b_1, ..., b_t$ des nombres algébriques avec les α_i deux à deux distincts et les b_i non nuls ; alors*

$$b_1 e^{\alpha_1} + ... + b_t e^{\alpha_t} \neq 0$$

Preuve :

Je vais ici commencer par présenter la trame générale de la preuve qui parait assez simple, mais repose sur un lemme, beaucoup plus technique, que je démontrerais par la suite.

Considérons

$$b_1 e^{\alpha_1 x} + ... + b_t e^{\alpha_t x} = \sum_{n=0}^{\infty} \frac{u_n}{n!} x^n$$

avec

$$u_n = \sum_{i=1}^{t} b_i \alpha_i^n$$

Considérons

$$v_n = n! \sum_{r=0}^{n} \frac{u_r}{r!}$$

On montre que :

Lemme (démontré plus loin) :

$$v(X) = \sum_{n=0}^{\infty} v_n X^n \in \mathbb{Q}(X)$$

Remarquons que

$$\frac{v_n}{n!} - \frac{v_{n-1}}{(n-1)!} = \frac{u_n}{n!}$$

Ainsi :

$$v_n - n v_{n-1} = u_n$$

D'où :

$$\sum_{n=0}^{\infty} (v_n - n v_{n-1}) X^n = \sum_{n=0}^{\infty} u_n X^n = \sum_{n=0}^{\infty} (\sum_{i=1}^{t} b_i \alpha_i^n) X^n = \sum_{i=1}^{t} b_i \sum_{n=0}^{\infty} (\alpha_i X)^n = \sum_{i=1}^{t} \frac{b_i}{1 - \alpha i X}$$

Cela signifie que

$$-X^2 \frac{dV(X)}{dX} + (1 - X) V(X) = \sum_{i=1}^{t} \frac{b_i}{1 - \alpha i X}$$

Or, $V(X) \in \mathbb{Q}(X)$ donc les pôles non nuls du membre de gauche ont un ordre au moins 2 tandis que les pôles du membres de droite sont d'ordre 1 (les α_i étant deux à deux distincts), d'où la contradiction qui conclut alors cette preuve. $\square$

<u>Lemme</u> :

$$v(X)=\sum_{n=0}^{\infty}v_nX^n\in\mathbb{Q}(X)$$

Soit

$$\prod_{i=1}^{t}(X-\alpha_i)=X^t-a_1X^{t-1}-...-a_t$$

Grâce à la théorie de Galois, on montre que l'on peut se ramener à $\sum_{i=1}^{t}bi'e^{\alpha_i'x}$ avec b_i' et α_i' tels que a_i' et u_i' soient rationnels. On peut alors se ramener à $u_n\in\mathbb{Z},n\in[\![0,t-1]\!]$ et les $a_i\in\mathbb{Q}$.
On conservera abusivement les notations $b_i,a_i,u_i,$ et α_i.
Ainsi $\forall i,\forall n\in\mathbb{Z}$, $\alpha_i^{t+n}=a_1\alpha_i^{t+n-1}+...+a_t\alpha_i^n$
et on a alors

$$u_{n+t}=a_1u_{n+t-1}+...+a_tu_n$$

Soit alors D un dénominateur commun aux $a_i,i=1,...,t$, cela implique $D^nu_n\in\mathbb{Z},\forall n\in\mathbb{N}$.

Posons $A=\max(1,|\alpha_i|)$ et $c_1=\max(|b_i|)$.
Il vient

$$|u_n|\leqslant c_1A^n,\forall n\in\mathbb{N}$$

Considérons

$$v_n=n!\sum_{r=0}^{n}\frac{u_r}{r!}$$

qui vérifie

$$|v_n|=n!\left|\sum_{r=0}^{n}\frac{u_r}{r!}\right|=n!\left|\sum_{r=n+1}^{\infty}\frac{u_r}{r!}\right|\leqslant n!c_1\sum_{r=n+1}^{\infty}\frac{A^r}{r!}\leqslant\frac{c_1A^{n+1}}{n+1}\sum_{r=n+1}^{\infty}\frac{(n+1)!A^r}{r!A^{n+1}}$$

Or,

$$\sum_{r=n+1}^{\infty}\frac{(n+1)!A^r}{r!A^{n+1}}=\sum_{r=0}^{\infty}\frac{(n+1)!A^r}{(r+n+1)!}\leqslant\sum_{r=0}^{\infty}\frac{A^r}{r!}=e^A$$

On a donc

$$|v_n|\leqslant c_2\frac{A^{n+1}}{n+1}$$

en posant $c_2=c_1e^A$
Etant donnée l'équation différentielle que l'on obtient à la fin de la preuve du théorème de Lindemann-Weierstrass (voir plus bas), on peut s'attendre à ce que $v(X)$ soit du type

$$v(X)=\frac{P(X)}{(1-a_1X-...-a_tX^t)^k}$$

où P est un polynôme.
Cela rend naturel le fait de s'intéresser alors à

$$\sum_{n=0}^{\infty}v_n(k)X^n=(1-a_1X-...-a_tX^t)^kv(X)$$

Remarquons que $\forall n\geqslant t,k\geqslant 0,\ v_n(k+1)=v_n(k)-a_1v_{n-1}(k)-...-a_tv_{n-t}(k)$
Posant $C=1+|a_1|+...+|a_t|$, cela permet de montrer les deux propriétés suivantes par récurrence, valables pour tout $n\geqslant kt$:
(1) $|v_n(k)|\leqslant c_2A^nC^k$ (2) $D^nv_n(k)\in\mathbb{Z}$

Démontrons maintenant (3) $k!$ divise $D^n v_n(k), \forall n \geqslant kt$.
On a :

$$v_n = u_n + nu_{n-1} + ... + n(n-1)...(n-k+2)u_{n-k+1} + w_n$$

où

$$w_n = n! \sum_{r=0}^{n-k} \frac{u_r}{r!} = n! \sum_{r=n-k+1}^{\infty} \frac{u_r}{r!}$$

Grâce à la première expression donnée de w_n, on constate que $D^{n-k} w_n \in \mathbb{Z}$ et que $k!$ divise $D^{n-k} w_n$.
Définissons

$$w(X) = \sum_{n=0}^{\infty} w_n X^n$$

Il s'ensuit

$$v(X) - w(X) = \sum_{n=0}^{\infty} (u_n + nu_{n-1} + ... + n(n-1)...(n-k+2)u_{n-k+1})X^n$$

Or, $\forall r$ tel que $0 \leqslant r \leqslant k-1$,

$$\sum_{n=0}^{\infty} n(n-1)...(n-r+1)u_{n-r} = \sum_{i=1}^{t} \sum_{n=r}^{\infty} r! \alpha_i^{-r} \binom{n}{r} b_i \alpha_i^n X^n = \sum_{i=1}^{t} r! b_i \alpha_i^{-r} \sum_{n=r}^{\infty} \binom{n}{r} (\alpha_i X)^n$$

Et

$$\begin{aligned}
\sum_{n=r}^{\infty} \binom{n}{r} (\alpha_i X)^n &= (\alpha_i X)^r + \sum_{n=r+1}^{\infty} (\alpha_i X)^n \frac{\prod_{k=0}^{n-r-1} (r+1+k)}{(n-r)!} \\
&= (\alpha_i X)^r + (\alpha_i X)^r \sum_{n=1}^{\infty} (\alpha_i X)^n \frac{\prod_{k=0}^{n-1} (r+1+k)}{n!} \\
&= (\alpha_i X)^r \frac{1}{(1-\alpha_i X)^{r+1}}
\end{aligned}$$

Donc

$$\sum_{n=0}^{\infty} n(n-1)...(n-r+1)u_{n-r} = \frac{Pr(X)}{(1 - a_1 X - ... - a_t X^t)^{r+1}}$$

avec $Pr(X)$ un polynôme de degré strictement inférieur à $t(r+1)$.
Finalement,

$$v(X) - w(X) = \frac{P(X)}{(1 - a_1 X - ... - a_t X^t)^k}$$

avec $P(X)$ un polynôme de degré strictement inférieur à tk. Ainsi, posant

$$\sum_{n=0}^{\infty} w_n(k) X^n = (1 - a_1 X - ... - a_t X^t)^k w(X)$$

on a $\forall n \geqslant kt, v_n(k) = w_n(k)$.
On a vu que par ailleurs $k!$ divise $D^{n-k} w_n$ donc a fortiori $k!$ divise $D^n w_n(k) = D^n v_n(k)$. On a donc démontré (3).

Il résulte de (1), (2) et (3) que si $v_n(k) \neq 0$ et $n \geqslant kt$,

$$k! \leqslant |D^n v_n(k)| \leqslant c_2 (AD)^n C^k$$

Ainsi, $k! > c_2(AD)^n C^k$ et $n \geqslant kt \Rightarrow v_n(k) = 0$. Choisissons alors k_0 tel que $k! > c_2(AD)^{10kt} C^k, \forall k \geqslant k_0$. Alors, $v_n(k) = 0 \forall k \geqslant k_0, kt \leqslant n \leqslant 10kt$. Ensuite, pour conclure, un dessin permet de mieux visualiser les différentes zones, et utilisant $v_n(k+1) = v_n(k) - a_1 v_{n-1}(k) - ... - a_t v_{n-t}(k)$, on en déduit que $v_n(k_0) = 0, \forall n \geqslant k_0 t$, donc

$$\sum_{n=0}^{\infty} v_n(k_0) X^n \in \mathbb{Q}[X]$$

Le lemme est alors démontré.

D Démonstration du théorème de Gelfond-Schneider

Quelques théorèmes préliminaires, dont les démonstrations ne seront pas donnés ici seront nécessaire à la preuve du théorème de Gelfond Schneider.

Soient α et β deux nombres algébriques. Alors :

$$\overline{|\alpha+\beta|} \leqslant \overline{|\alpha|} + \overline{|\beta|}$$

$$\overline{|\alpha\beta|} \leqslant \overline{|\alpha||\beta|}$$

Inégalité de la taille :
Soit α un nombre algébrique non nul, de degré d, alors :

$$(\overline{|\alpha|})^{-d+1}(den\alpha)^{-d} \leqslant |\alpha|$$

On définit (S) par :

$$A_{11}x_1 + ... + A_{1n}x_n = 0$$

$$A_{21}x_1 + ... + A_{2n}x_n = 0$$

$$A_{m1}x_1 + ... + A_{mn}x_n = 0$$

Lemme de Siegel :
Soit $\mathbb{K}$ un corps de nombres de degré d. Soient (A_{ij}), $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$, des entiers de $\mathbb{K}$, avec $n > dm$. Soit $A \in \mathbb{N}$, tel que :

$$\max_{i,j}(\overline{|A_{ij}|}) \leqslant A$$

Alors, il existe $(x_1, ..., x_n) \in \mathbb{Z}^n$, et un réel $M > 0$ indépendant de n et m, tels que :

$$0 < \max_i |x_i| \leqslant (nMA)^{\frac{dm}{n-dm}}$$

tel que (S) soit vérifié.

Principe du maximum :
Si f est analytique dans $D = \{z \in \mathbb{C} / |z| < R\}$ et si $0 < r < R$, alors :

$$|x| \leqslant r \Rightarrow |f(x)| \leqslant \max_{|z|=r} |f(z)|$$

Théorème de Gelfond-Schneider :
Soit $\alpha \in \overline{\mathbb{Q}}$, $\alpha \notin \{0,1\}$. Soit β un nombre algébrique irrationnel. Alors, α^β est transcendant.

Preuve :

Supposons au contraire $\gamma = \alpha^\beta$ algébrique. Notons $\mathbb{K} = \mathbb{Q}(\alpha,\beta,\gamma)$, de degré d. Soit M le nombre défini par le lemme de Siegel, $\lambda = den(\alpha)den(\beta)den(\gamma)$, $\mu = \overline{|\alpha|}\,\overline{|\gamma|}(1+\overline{|\beta|})$, $\nu = e^{2|\operatorname{Log}\alpha|}$.

Tout d'abord, $\exists N$ tel que $\forall n \geqslant N$:

$$\begin{array}{ll}
(1+|\beta|)(n+1)^5 \leqslant n^6 \leqslant \frac{1}{2}n^7 & ;(Mn^{11}n^{6n^8})^{\frac{d}{n-d}} \leqslant e^{n^8} \\
(4\nu)^{n^{10}}n^{-n^{10}} \leqslant e^{-n^{10}} & ;n^{11}e^{n^8}\mu^{(n+1)^8}(n+1)^{5n^8} \leqslant e^{n^9} \\
(\lambda\mu)^{n^8}n^{5n^8} \leqslant n^{6n^8} & ;n^{11}e^{n^8}e^{7n^8\operatorname{Log}n}e^{n^{10}|\operatorname{Log}\alpha|} \leqslant \nu^{n^{10}} \\
\lambda^{(n+1)^8} \leqslant e^{n^9} & ;(2d-1)n^9 < n^{10}
\end{array}$$

Etape 1 (Construction d'un polynôme) :
Soit

$$P(x,y) = \sum_{i=0}^{N^8-1}\sum_{j=0}^{N^3-1} a_{ij}x^iy^j$$

On souhaite trouver des a_{ij} de telle sorte que :

$$F(z) = P(z,\alpha^z) \text{ verifie } F(k+m\beta) = 0 \qquad \forall k,m \text{ tels que } 0 \leqslant k,m < N^5$$

La condition $F(k+m\beta)=0$ se traduit par le système suivant de N^{10} équations à N^{11} inconnues a_{ij}, dont les coefficients sont entiers après avoir multiplié chacune des équations par λ^{N^8} :

$$\sum_{i=0}^{N^8-1}\sum_{j=0}^{N^3-1} a_{ij}\lambda^{N^8}(k+m\beta)^i\alpha^{jk}\gamma^{jm} = 0$$

Donnons alors une majoration des coefficients du système :

$$\overline{\left|\lambda^{N^8}(k+m\beta)^i\alpha^{jk}\gamma^{jm}\right|} \leqslant \lambda^{N^8}(1+\overline{|\beta|})^{N^8}N^{5N^8}(\overline{|\alpha\gamma|})^{N^8} \leqslant N^{6N^8}$$

D'après le Lemme de Siegel, il existe des a_{ij} satisfaisant à ce système et tels que :

$$0 < \max_{i,j}|a_{ij}| \leqslant (N^{11}MN^{6N^8})^{\frac{d}{N-d}} \leqslant e^{N^8}$$

Deuxième étape :
On montre les deux propriétés suivantes $\forall n \geqslant N$:

$$(I)_n \qquad F(k+m\beta) = 0 \qquad 0 \leqslant k,m < n^5$$

$$(II)_n \max_{|z|\leqslant n^6}|F(z)| \leqslant e^{-n^{10}}$$

$(I)_N$ est la conclusion de la première étape.
$\forall n \geqslant N, (I)_n \Rightarrow (II)_n$:

$$\max_{|z|\leqslant n^7}|F(z)| \leqslant \sum_{i=0}^{N^8-1}\sum_{j=0}^{N^3-1}|a_{ij}|\,n^{7i}e^{jRe(z\operatorname{Log}\alpha)}$$

Or, $\max_{i,j}|a_{ij}| \leqslant e^{N^8}$ et $Re(z \operatorname{Log}\alpha) \leqslant |z \operatorname{Log}\alpha| \leqslant n^7 \operatorname{Log}\alpha$, donc on parvient après simplification et utilisation des inégalités préliminaires :

$$\max_{|z|\leqslant n^7} |F(z)| \leqslant \nu^{n^{10}}$$

Introduisons alors la fonction :

$$G(z) = \frac{F(z)}{\prod_{k=0}^{n^5-1}\prod_{m=0}^{n^5-1}(z-k-m\beta)}$$

β étant irrationel, les $k+m\beta$ sont deux à deux distincts et ce sont des zéros de F. La fonction G est donc entière et on peut lui appliquer le principe du maximum dans le disque $|z| \leqslant n^7$, il vient :

$$|z| \leqslant n^6 \Rightarrow |G(z)| \leqslant \max_{|z|\leqslant n^7}|G(z)| \leqslant \frac{\nu^{n^{10}}}{\prod_{k=0}^{n^5-1}\prod_{m=0}^{n^5-1}|n^7-|k+m\beta||}$$

Ainsi, $\forall\, |z| \leqslant n^6$, on a :

$$\begin{aligned} |F(z)| &\leqslant \nu^{n^{10}} \frac{\prod_{k=0}^{n^5-1}\prod_{m=0}^{n^5-1}(n^6+|k+m\beta|)}{\prod_{k=0}^{n^5-1}\prod_{m=0}^{n^5-1}|n^7-|k+m\beta||} \\ &\leqslant \nu^{n^{10}} \frac{\prod_{k=0}^{n^5-1}\prod_{m=0}^{n^5-1}(n^6+(1+|\beta|)n^5)}{\prod_{k=0}^{n^5-1}\prod_{m=0}^{n^5-1}|n^7-(1+|\beta|)n^5|} \\ &\leqslant \nu^{n^{10}} \frac{\prod_{k=0}^{n^5-1}\prod_{m=0}^{n^5-1}(2n^6)}{\prod_{k=0}^{n^5-1}\prod_{m=0}^{n^5-1}\frac{n^7}{2}} \end{aligned}$$

Finalement, on a donc bien $\max_{|z|\leqslant n^6}|F(z)| \leqslant (4\nu)^{n^{10}} n^{-n^{10}} \leqslant e^{-n^{10}}$ Donc $(I)_n \Rightarrow (II)_n$
Montrons $(II)_n \Rightarrow (I)_{n+1}$. Soient $0 \leqslant k, m < (n+1)^5$.
On a $|k+m\beta| \leqslant (1+|\beta|)(n+1)^5 \leqslant n^6$ donc $|F(k+m\beta)| \leqslant e^{-n^{10}}$ (par $(II)_n$).
On a en outre les majorations suivantes du dénominateur et de la maison de $F(k+m\beta)$:

$$den[F(k+m\beta)] \leqslant (den\beta)^{N^8}(den\alpha den\gamma)^{N^3(n+1)^5} \leqslant \lambda^{(n+1)^8} \leqslant e^{n^9}$$

$$\begin{aligned} \overline{|F(k+m\beta)|} &\leqslant N^8 N^3 e^{N^8}(1+\overline{|\beta|})^{N^8}(n+1)^{5N^8}(\overline{|\alpha|\,|\gamma|})^{N^3(n+1)^5} \\ &\leqslant n^{11} e^{n^8} \mu^{(n+1)^8}(n+1)^{5n^8} \leqslant e^{n^9} \end{aligned}$$

Supposons un instant $F(k+m\beta) \neq 0$, alors l'inégalité de la taille s'écrirait $e^{(1-2d)n^9} \leqslant e^{-n^{10}}$, ce qui fournit une contradiction, donc $(II)_n \Rightarrow (I)_{n+1}$.

Ainsi, $(I)_n$et$(II)_n$ sont vérifiés $\forall n \geqslant N$.

Soit $z \in \mathbb{C}$; alors $\forall n \geqslant N$ tel que $n^6 \geqslant |z|$, $|F(z)| \leqslant e^{-n^{10}}$ donc en passant à la limite $F(z) = 0$, cela signifie que $h(z) = \alpha^z$ est algébrique, ce qui fournit une contradiction.

Le théorème de Gelfond-Schneider est alors démontré. □