Nombres transcendants

Alexandre Bailleul

Encadrant : Éric Gaudron

Laboratoire de Mathématiques de Clermont-Ferrand

19 Mai 2014 - 27 Juin 2014

Table des matières

Introduction **2**

Partie I : Quelques notions de théorie algébrique des nombres **4**
1) Nombres algébriques, entiers algébriques 4
2) Corps de nombres algébriques 6
3) Valeurs absolues sur les corps de nombres 10
4) La formule du produit 15
5) Hauteur logarithmique de Weil 16

Partie II : Le théorème d'Hermite-Lindemann **19**
1) Énoncé du théorème et corollaires 19
2) Plan de la démonstration 20
3) Démonstration du théorème 22

Partie III : Le théorème de Lindemann-Weierstrass **29**
1) Énoncé du théorème et corollaires 29
2) Quelques lemmes de théorie de Galois 30
3) Démonstration du théorème 32

Conclusion **39**

Annexes **40**
Le théorème de Liouville 40
Le théorème de Gelfond-Schneider 42
Le théorème des six exponentielles 42
Le théorème de Baker 43
La conjecture de Schanuel 44

Bibliographie **45**

Introduction

Ce mémoire a été rédigé après six semaines de stage d'initiation à la recherche mathématique au Laboratoire de Mathématiques de Clermont-Ferrand, du 19 mai au 27 juin 2014, sous la direction d'Éric Gaudron. Je tiens à le remercier pour son aide constante tout au long de ce stage, notamment dans la mise en place des quelques démonstrations de transcendance que j'ai faites et que j'ai trouvées relativement compliquées, pour sa disponibilité et pour m'avoir permis d'assister à plusieurs séminaires de mathématiques du laboratoire.

On dit qu'un nombre complexe α est *algébrique* s'il est solution d'une équation polynomiale à coefficients rationnels (ou, ce qui est équivalent, à coefficients entiers) non tous nuls. Par exemple, tout nombre rationnel q est algébrique car solution de l'équation $X - q = 0$. Le nombre $\sqrt{2}$ est algébrique car solution de l'équation $X^2 - 2 = 0$.

A l'inverse, un nombre complexe qui n'est pas algébrique est dit *transcendant*. C'est le type de nombres qui va nous intéresser ici. Il n'est pas *a priori* évident de justifier l'existence de tels nombres. Celle-ci fut conjecturée par Lambert en 1761, après avoir démontré l'irrationalité de π, mais elle ne fut démontrée par Joseph Liouville qu'en 1844 ! Pour cela, il exhiba « tout simplement » un tel nombre.

Ce nombre est $\sum_{k=1}^{+\infty} 10^{-k!} = 0,110001000000000000000010...$, un nombre que l'on ne rencontre pas tous les jours en mathématiques... En fait, Liouville construisit explicitement ce nombre afin qu'il soit transcendant.

Presque trente ans plus tard, Charles Hermite démontra que le nombre e est transcendant. Puis, en 1882, Lindemann prouva la transcendance de π. Les grands écarts entre ces démonstrations montrent à quel point il est compliqué de montrer qu'un nombre est transcendant.

On peut montrer que l'ensemble des nombres algébriques est de mesure de Lebesgue nulle dans $\mathbb{C}$. Ainsi, *presque tous* les nombres complexes sont transcendants. Il peut paraître alors assez paradoxal que montrer qu'un nombre en particulier est transcendant soit si difficile ! Mais ceci vient du fait que la propriété d'*être transcendant* est une propriété de non-existence, la non-existence d'un polynôme à coefficients entiers annulant le nombre considéré. On doit donc raisonner par

l'absurde pour montrer qu'un nombre est transcendant.

Aujourd'hui, on connaît plusieurs résultats de transcendance sur certaines familles de nombres, on peut citer les théorèmes d'Hermite-Lindemann ou de Gelfond-Schneider par exemple, mais ceux-ci restent relativement limités et on ne connaît pas de méthode générale permettant de montrer la transcendance de n'importe quel nombre. Par exemple, on ne sait pas à l'heure actuelle si les nombres $\pi + \mathrm{e}$ et $\pi\mathrm{e}$ sont transcendants.

Nous verrons dans une première partie plusieurs notions, notamment de théorie algébrique des nombres, qui nous serviront à démontrer deux résultats de transcendance. Tout d'abord le théorème d'Hermite-Lindemann, qui donne la transcendance de e^{α} pour un nombre algébrique α non nul, et qui occupera la deuxième partie. Puis le théorème de Lindemann-Weierstrass, qui affirme que si α_1, ..., α_n sont des nombres algébriques linéairement indépendants sur $\mathbb{Q}$ alors pour tout polynôme à n variables non nul P à coefficients algébriques, $P(\mathrm{e}^{\alpha_1}, ..., \mathrm{e}^{\alpha_n}) \neq 0$, et qui occupera la troisième partie. Enfin en annexes nous verrons quelques résultats de transcendance plus récents que nous ne démontrerons pas et quelques conjectures encore non démontrées ou infirmées à ce jour.

Partie I : Quelques notions de théorie algébrique des nombres

Pour étudier les nombres transcendants, il faut étudier leurs camarades, les nombres algébriques. Supposons que l'on veuille montrer qu'un nombre β est transcendant. On va supposer par l'absurde que β est algébrique, et montrer qu'il ne possède pas une propriété vérifiée par tous les nombres algébriques. C'est pour cela qu'il faut connaître les nombres algébriques pour parvenir à des démonstrations de transcendance.

1) Nombres algébriques, entiers algébriques

Rappelons tout d'abord la définition d'un nombre algébrique.

Définition 1 *Un nombre complexe α est dit algébrique lorsqu'il est racine d'un polynôme à coefficients entiers, i.e. lorsqu'il existe*

$$P = a_n X^n + ... + a_1 X + a_0 \in \mathbb{Z}[X] \setminus \{0\}$$

tel que $P(\alpha) = 0$.

Exemples :

- Tout nombre rationnel $\frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ est algébrique car racine du polynôme $bX - a$.
- 2i est algébrique car racine du polynôme $X^2 + 4$.

Proposition 1 *L'ensemble des nombres algébriques $\overline{\mathbb{Q}}$ est dénombrable.*

Démonstration : $\mathbb{Z}[X]$ est dénombrable car

$$\mathbb{Z}[X] = \bigcup_{n=0}^{+\infty} \mathbb{Z}_n[X]$$

et $\forall n \in \mathbb{N}$, $\mathbb{Z}_n[X]$ est dénombrable (où $\mathbb{Z}_n[X]$ désigne l'ensemble des polynômes de degré au plus n à coefficients dans $\mathbb{Z}$, qui est équipotent à $\mathbb{Z}^{n+1}$). On écrit alors $\mathbb{Z}[X] = \{P_0, P_1, ...\}$. A chaque P_i on associe l'ensemble fini de ses racines Z_i, pour $i \in \mathbb{N}$. Ainsi on a $\overline{\mathbb{Q}} = \bigcup_{n=0}^{+\infty} Z_n$, et $\overline{\mathbb{Q}}$ est donc dénombrable par union dénombrable d'ensembles finis. □

Corollaire 2 *Il existe des nombres transcendants.*

En effet $\mathbb{C}$ est non dénombrable, donc $\overline{\mathbb{Q}} \neq \mathbb{C}$. Donc il existe des nombres qui ne sont pas algébriques, c'est-à-dire des nombres transcendants. On a également comme corollaire que $\lambda(\overline{\mathbb{Q}}) = 0$ où λ désigne la mesure de Lebesgue sur $\mathbb{C}$, ce qui justifie que *presque tous* les nombres complexes sont transcendants.

A chaque nombre algébrique, on peut associer un unique polynôme primitif sur $\mathbb{Z}$ de degré minimal :

Proposition 3 *Soit α un nombre algébrique. Il existe un unique $P = a_n X^n + ... + a_1 X + a_0 \in \mathbb{Z}[X]$ de degré minimal tel que $a_n \geq 0$, $PGCD(a_0, ..., a_n) = 1$ et $P(\alpha) = 0$. Ce polynôme est appelé polynôme minimal de α.*

Démonstration : Le nombre α est algébrique : par définition, il existe $Q \in \mathbb{Z}[X] \backslash \{0\}$ tel que $Q(\alpha) = 0$. Ainsi l'idéal $\{P \in \mathbb{Q}[X], P(\alpha) = 0\}$ n'est pas réduit à $\{0\}$. Puisque $\mathbb{Q}[X]$ est principal, cet idéal est engendré par un polynôme unitaire P^*.

Le polynôme P^* est de degré minimal car il divise tout polynôme de $\mathbb{Q}[X]$ annulant α, et il est unique, car si on suppose l'existence de $Q^* \in \mathbb{Q}[X]$ unitaire, annulant α, alors leur différence annule α et est de degré strictement inférieur, ce qui est absurde.

En multipliant P^* par le PPCM des valeurs absolues des dénominateurs de ses coefficients, on obtient un polynôme $P \in \mathbb{Z}[X] \setminus \{0\}$, de coefficient dominant positif et annulant α. Enfin, en divisant P par le PGCD de ses coefficients, on obtient l'unique polynôme recherché. □

Ce polynôme minimal et l'ensemble de ses racines jouent un rôle particulier dans l'étude du nombre α.

Définition 2 *Soient α un nombre algébrique et P son polynôme minimal. Les racines de P sont appelées les conjugués de α. On appelle degré de α le degré de son polynôme minimal.*

Proposition 4 *Soient α un nombre algébrique et P son polynôme minimal. Les racines de P sont deux à deux distinctes.*

Démonstration : On va bien sûr supposer $\deg P \geq 2$, le cas P de degré 1 étant trivial. Soit β une racine de P. Alors P est le polynôme minimal de β. En effet, soit Q le polynôme minimal de β. Puisque $P(\beta) = 0$, on a $Q|P$. Ainsi $P = QR$ avec R dans $\mathbb{Z}[X] \setminus \{0\}$. En particulier, $\deg R < \deg P$. Ainsi, $R(\alpha) \neq 0$ car P est de degré minimal. Donc $Q(\alpha) = 0$ car $\mathbb{Z}[X]$ est intègre et donc $P = Q$ car $P|Q$.

Supposons maintenant que β est racine d'ordre au moins 2 de P. Alors β est racine du polynôme dérivé P' de P. Or $P \neq 0$ donc $\deg P' < \deg P$. De plus $P' \in \mathbb{Z}[X] \setminus \{0\}$, et $P'(\beta) = 0$, ce qui est absurde car P est le polynôme minimal de β. Donc les racines de P sont simples, *i.e.* elles sont deux à deux distinctes. □

Définition 3 *Soit α un nombre algébrique de degré d, $\alpha = \alpha_1, \alpha_2, ..., \alpha_d$ ses conjugués. On appelle maison de α, notée $\overline{|\alpha|}$, le nombre réel $\max\limits_{1 \leq i \leq d} |\alpha_i|$.*

Définition 4 *Un nombre algébrique α est dit entier algébrique lorsque son polynôme minimal est unitaire.*

Proposition 5 *Soit α un nombre algébrique. Il existe un entier l tel que $l\alpha$ soit un entier algébrique.*

Démonstration : Soit $P = a_n X^n + a_{n-1} X^{n-1} ... + a_0$ le polynôme minimal de α. Puisque $P(\alpha) = 0$, $a_n^{n-1} P(\alpha) = 0$. Or $a_n^{n-1} P(\alpha) = a_n^n \alpha^n + a_n^{n-1} a_{n-1} \alpha^{n-1} ... + a_n^{n-1} a_0 = (a_n \alpha)^n + a_{n-1} (a_n \alpha)^{n-1} ... + a_n^{n-1} a_0$. Ainsi, $a_n^{n-1} \alpha$ est racine du polynôme $X^n + a_{n-1} X^{n-1} + ... + a_n^{n-1} a_0$ qui est unitaire et à coefficients entiers, donc $a_n^{n-1} \alpha$ est un entier algébrique. □

Les entiers algébriques interviendront dans le lemme de Siegel, que nous verrons lors de la démonstration du théorème d'Hermite-Lindemann.

2) Corps de nombres algébriques

Définition 5 *On appelle corps de nombres algébriques (ou plus couramment corps de nombres) toute extension de $\mathbb{Q}$ de degré fini sur $\mathbb{Q}$, i.e. tout corps K contenant $\mathbb{Q}$ tel que K soit un $\mathbb{Q}$-espace vectoriel de dimension finie. On note $[K : \mathbb{Q}]$ cette dimension.*

Les exemples les plus simples de corps de nombres sont les $\mathbb{Q}[\alpha]$ avec α un nombre algébrique :

Proposition 6 *Soit α un nombre algébrique de degré d. Alors $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$ et $\mathbb{Q}(\alpha)$ est un corps de nombres de degré d.*

Démonstration : Rappelons tout d'abord les définitions de $\mathbb{Q}[\alpha]$ et de $\mathbb{Q}(\alpha)$. Notons $ev_\alpha : P \mapsto P(\alpha)$. Alors $\mathbb{Q}[\alpha] := ev_\alpha(\mathbb{Q}[X])$ et $\mathbb{Q}(\alpha) := ev_\alpha(\mathbb{Q}(X))$. L'application ev_α est clairement un morphisme d'anneaux unitaires de $\mathbb{Q}(X) \to \mathbb{C}$.

Soit $P = a_d X^d + ... + a_0$ le polynôme minimal de α. Puisque P est le polynôme minimal de α on a que $\ker(ev_\alpha) = (P)$. Puisque P est irréductible et primitif dans $\mathbb{Z}[X]$, il est irréductible dans $\mathbb{Q}[X]$. Donc l'idéal de $\mathbb{Q}[X]$ engendré par P est maximal, et $\mathbb{Q}[x]/(P) \cong \mathbb{Q}[\alpha]$ est un corps. Puisque c'est un corps on a immédiatement que $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$.

Si on identifie α et $ev_\alpha(X)$, alors $(1, ..., \alpha^{d-1})$ est une famille libre de $\mathbb{Q}(\alpha)$ sur $\mathbb{Q}$. En effet s'il existe $b_0, ..., b_{d-1} \in \mathbb{Q}$ non tous nuls tels que $b_{d-1}\alpha^{d-1} + ... + b_0 = 0$, alors α est racine du polynôme $b_{d-1}X^{d-1} + ... + b_0 = 0$, qui est non nul et de degré strictement inférieur à $d = \deg(P)$, ce qui contredit le fait que P est le polynôme minimal de α. Donc $\mathbb{Q}(\alpha)$ est un corps de nombres et $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq d$.

De plus, puisque $a_d\alpha^d + ... + a_0 = 0$, on a $\alpha^d = -\frac{a_{d-1}}{a_d}\alpha^{d-1} - ... - \frac{a_0}{a_d}$ (le cas $a_d = 0$ correspond à $\alpha = 0$ et il est clair que $\mathbb{Q}(0) = \mathbb{Q}$ est un corps de nombres de degré 1). La famille $(1, X, X^2, ...)$ étant génératrice de $\mathbb{Q}[X]$, $(1, \alpha, \alpha^2, ...)$ est génératrice de $\mathbb{Q}(\alpha)$ et donc par la remarque précédente, $(1, ..., \alpha^{d-1})$ est également génératrice de $\mathbb{Q}(\alpha)$. Donc $\mathbb{Q}(\alpha)$ est un corps de nombres et $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$. □

En fait, il existe une réciproque à ce théorème, nous allons voir que pour tout corps de nombres K, il existe un nombre algébrique θ tel que $K = \mathbb{Q}(\theta)$. Nous aurons tout d'abord besoin d'un lemme, connu sous le nom de formule de multiplication des degrés :

Lemme 1 (Formule de multiplication des degrés) *Soient K un corps, L une extension de degré fini de K et M une extension de degré fini de L. Alors $[M : K] = [M : L][L : K]$.*

Démonstration : Posons $n = [M : L]$ et $p = [L : K]$. Soient $(l_1, ..., l_p)$ une base de L en tant que K-espace vectoriel, et $(m_1, ..., m_n)$ une base de M en tant que M-espace vectoriel. Montrons que $(l_i m_j, (i, j) \in \{1, ..., p\} \times \{1, ..., n\})$ est une base de M en tant que K-espace vectoriel :

— Libre : $\forall \lambda_{i,j} \in K$,

$$\sum_{i=1}^{n}\sum_{j=1}^{p} \lambda_{i,j} l_j m_i = 0$$

$$\Rightarrow \sum_{i=1}^{n}(\sum_{j=1}^{p} \lambda_{i,j} l_j) m_i = 0$$

$$\Rightarrow \forall i \in \{1,...,n\}, \sum_{j=1}^{p} \lambda_{i,j} l_j = 0 \text{ (car } (m_1,...,m_n) \text{ est libre sur } L)$$

$$\Rightarrow \forall (i,j) \in \{1,...,p\} \times \{1,...,n\}, \lambda_{i,j} = 0.$$

— Génératrice : Soit x dans M. $x = \sum_{i=1}^{n} x_i m_i$, avec $\forall i \in \{1,...,n\}, x_i \in L$, et $x_i = \sum_{j=1}^{p} \lambda_{i,j} l_j$, avec $\forall j \in \{1,...,p\}, \lambda_{i,j} \in K$. D'où $x = \sum_{i=1}^{n}\sum_{j=1}^{p} \lambda_{i,j} l_j m_i$.

Donc $(l_i m_j, (i,j) \in \{1,...,p\} \times \{1,...,n\})$ est une base de M en tant que K-espace vectoriel et donc $[M:K] = np = [M:L][L:K]$. □

Théorème 6 (Théorème de l'élément primitif) *Soit K un corps de nombres. Il existe un nombre algébrique θ tel que $K = \mathbb{Q}(\theta)$.*

Démonstration : Notons $d = [K:\mathbb{Q}]$. Tout élément de K est algébrique de degré inférieur ou égal à d. En effet, soit x dans K. La famille $(1, x, ..., x^d)$ est une famille de $d+1$ éléments de K, elle est donc liée sur $\mathbb{Q}$ car $dim_{\mathbb{Q}} K = d$.

Ainsi, $\exists b_0, ..., b_d \in \mathbb{Q}$ non tous nuls tels que $b_d x^d + ... + b_0 = 0$. Donc x est algébrique, de degré inférieur ou égal à d.

Montrons qu'il existe $n \in \mathbb{N}^*$ et $\alpha_1, ..., \alpha_n \in K$ tels que $K = \mathbb{Q}(\alpha_1, ..., \alpha_n)$.
Soit α_1 dans K. On a $\mathbb{Q}(\alpha_1) \subset K$. Si $\mathbb{Q}(\alpha_1) = K$, le résultat est démontré.
Sinon, soit α_2 dans $K \setminus \mathbb{Q}(\alpha_1)$. Alors $\mathbb{Q}(\alpha_1, \alpha_2) \subset K$ et

$$d \geq [\mathbb{Q}(\alpha_1,\alpha_2):\mathbb{Q}] = [\mathbb{Q}(\alpha_1,\alpha_2):\mathbb{Q}(\alpha_1)][\mathbb{Q}(\alpha_1):\mathbb{Q}] > [\mathbb{Q}(\alpha_1):\mathbb{Q}].$$

En effet $\alpha_2 \notin \mathbb{Q}(\alpha_1)$ et donc $[\mathbb{Q}(\alpha_1,\alpha_2):\mathbb{Q}(\alpha_1)] = [\mathbb{Q}(\alpha_1)(\alpha_2):\mathbb{Q}(\alpha_1)] > 1$.
Ce processus a une fin car $d < +\infty$. On a donc montré qu'il existe $n \in \mathbb{N}^*$ et $\alpha_1, ..., \alpha_n \in K$ tels que $K = \mathbb{Q}(\alpha_1, ..., \alpha_n)$.

Il reste à montrer que $\forall \alpha, \beta \in \overline{\mathbb{Q}}, \exists \theta \in \overline{\mathbb{Q}}, \mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\theta)$ et on obtiendra le théorème de l'élément primitif par récurrence.

Soient donc α et β deux nombres algébriques, que l'on supposera distincts (le résultat étant évident si $\alpha = \beta$), et soient P_α et P_β leurs polynômes minimaux respectifs. Soient $\alpha = \alpha_1, ..., \alpha_n$ et $\beta = \beta_1, ..., \beta_p$ les conjugués respectifs de α et β. D'après la proposition 4, ces nombres sont deux à deux distincts. Ainsi,

$$\forall i \in \{1, ..., n\}, \forall j \in \{2, ..., p\}, \exists! x \in \mathbb{C}, \alpha_i + x\beta_j = \alpha + x\beta.$$

On peut trouver γ dans $\mathbb{Z}^*$ ne vérifiant aucune de ces équations (il y en a un nombre fini). Posons $\theta = \alpha + \gamma\beta \in \mathbb{Q}(\alpha, \beta)$. Alors $\mathbb{Q}(\theta) \subset \mathbb{Q}(\alpha, \beta)$. Il reste à montrer $\mathbb{Q}(\alpha, \beta) \subset \mathbb{Q}(\theta)$, *i.e.* $\beta \in \mathbb{Q}(\theta)$ car $\alpha = \theta - \gamma\beta$.

Posons $Q(X) = P_\alpha(\theta - \gamma X)$. Puisque $P_\alpha \in \mathbb{Z}[X]$ et $\gamma \in \mathbb{Z}$, $Q \in \mathbb{Q}(\theta)[X]$. De plus $Q(\beta) = P_\alpha(\alpha) = 0$. La seule racine commune de Q et P_β est β, car si pour $j \geq 2, Q(\beta_j) = P_\alpha(\theta - \gamma\beta_j) = 0$ alors $\exists i \in \{1, ..., n\}, \theta - \gamma\beta_j = \alpha_i$, ce qui contredirait la définition de γ.

Maintenant notons $R = PGCD(Q, P_\beta)$. Puisque $Q \in \mathbb{Q}(\theta)[X]$ et $P_\beta \in \mathbb{Z}[X] \subset Q(\theta)[X]$, $R \in Q(\theta)[X]$. De plus R est nécessairement de degré 1 puisque Q et P_β ont une seule racine en commun. Donc $R = aX + b$ avec $a, b \in Q(\theta), a \neq 0$. Puisque $R(\beta) = 0, a\beta + b = 0$, *i.e.* $\beta = -\frac{b}{a} \in \mathbb{Q}(\theta)$. □

Maintenant que nous avons établi le théorème de l'élément primitif, nous allons pouvoir obtenir un résultat important sur les nombres algébriques :

Proposition 7 *L'ensemble $\overline{\mathbb{Q}}$ est un sous-corps de $\mathbb{C}$.*

Démonstration : Il suffit de montrer que si x et y sont deux nombres algébriques avec $x \neq 0$ alors $-x, \frac{1}{x}, x + y$ et xy sont algébriques.

Soit donc x un nombre algébrique non nul. Puisque $x \in \mathbb{Q}(x)$, et puisque $\mathbb{Q}(x)$ est un corps, $-x \in \mathbb{Q}(x)$ et $\frac{1}{x} \in \mathbb{Q}(x)$. Or on a vu dans la démonstration du théorème de l'élément primitif que tout élément de $\mathbb{Q}(x)$ est algébrique, ainsi $-x$ et $\frac{1}{x}$ sont algébriques.

Soient x et y deux nombres algébriques. On a $x + y \in \mathbb{Q}(x, y)$ et $xy \in \mathbb{Q}(x, y)$. D'après le théorème de l'élément primitif, il existe un nombre algébrique α tel que $\mathbb{Q}(x, y) = \mathbb{Q}(\alpha)$. Ainsi, comme précédemment, $x + y$ et xy sont algébriques. □

On peut également montrer que l'ensemble des entiers algébriques $\overline{\mathbb{Z}}$ est un sous-anneau de $\mathbb{C}$, mais nous allons uniquement montrer le résultat plus faible suivant :

Proposition 8 *Soit α un entier algébrique. Alors $\forall n \in \mathbb{Z}$, $n\alpha$ est un entier algébrique.*

Démonstration : Notons P le polynôme minimal de α, et d son degré. Alors $n\alpha$ est racine du polynôme $n^d P(\frac{X}{n})$, qui est à coefficients entiers et unitaire. □

3) Valeurs absolues sur les corps de nombres

Dans les deux démonstrations de transcendance que nous allons voir, nous allons utiliser ce que l'on appelle la *formule du produit*. Pour arriver à cette formule il faut étudier les différentes valeurs absolues définies sur un corps de nombres.

Définition 7 *Une valeur absolue sur une corps k est une application $|.| : k \to [0, +\infty[$ vérifiant :*
- $\forall x \in k, |x| = 0 \Leftrightarrow x = 0$
- $\forall x, y \in k, |xy| = |x||y|$
- $\forall x, y \in k, |x + y| \leq |x| + |y|$

On peut remarquer qu'une valeur absolue $|.|$ sur un corps k induit une topologie sur k par la distance $d : (x, y) \mapsto |x - y|$, qui en fait alors un espace métrique.

Pour l'instant, nous allons étudier les valeurs absolues sur le corps $\mathbb{Q}$. On a bien sûr la *valeur absolue triviale*, qui a x associe 0 si $x = 0$ et 1 sinon, et la *valeur absolue classique*, notée $|.|$. Mais il en existe beaucoup d'autres. Une certaine famille de valeurs absolues va jouer un rôle très important pour la suite, les *valeurs absolues p-adiques*.

Définition 8 *Soit p un nombre premier. On rappelle que la valuation p-adique d'un nombre entier a, notée $v_p(a)$ est le plus grand entier n tel que $p^n \mid a$ et $p^{n+1} \nmid a$ (par convention $v_p(0) = +\infty$), et la valuation p-adique d'un nombre rationnel $x = \frac{a}{b}$ est $v_p(x) = v_p(a) - v_p(b)$. On définit la valeur absolue p-adique sur $\mathbb{Q}$ par*

$$\forall x \in \mathbb{Q},\ |x|_p = p^{-v_p(x)}.$$

Comme son nom l'indique, la valeur absolue p-adique est une valeur absolue sur $\mathbb{Q}$. Elle est même ultramétrique :

$$\forall x, y \in \mathbb{Q},\ |x + y|_p \leq \max(|x|_p, |y|_p).$$

Une valeur absolue sur un corps K qui n'est pas ultramétrique est dite *archimédienne*.

On peut se poser la question de l'existence d'*autres* valeurs absolues sur $\mathbb{Q}$. On dira que deux valeurs absolues sur un corps K sont équivalentes si elles induisent

la même topologie sur K. On peut montrer que deux valeurs absolues sur K, $|.|_1$ et $|.|_2$ sont équivalentes si et seulement s'il existe un nombre réel $\alpha > 0$ tel que $|.|_1 = |.|_2^\alpha$.

Nous pouvons maintenant donner une description de toutes les valeurs absolues sur $\mathbb{Q}$ grâce au théorème d'Ostrowski, que nous allons admettre (voir [6]) :

Théorème 9 (Théorème d'Ostrowski) *Toute valeur absolue non triviale sur $\mathbb{Q}$ est équivalente soit à une valeur absolue p-adique, soit à la valeur absolue classique.*

A partir de maintenant, nous ne considérerons que des valeurs absolues normalisées : les valeurs absolues p-adiques ou la valeur absolue classique, un représentant par classes d'équivalence de valeurs absolues. On notera $M_\mathbb{Q}$ l'ensemble des valeurs absolues (normalisées) sur $\mathbb{Q}$.

Proposition 9 *Soit x dans $\mathbb{Q}^*$. Alors on a*

$$\prod_{v \in M_\mathbb{Q}} |x|_v = 1.$$

Démonstration : On a

$$\prod_{v \in M_\mathbb{Q}} |x|_v = |x| \prod_{p \text{ premier}} |x|_p$$

Or

$$|x| = \prod_{p \text{ premier}} p^{v_p(x)} \text{ et } \prod_{p \text{ premier}} |x|_p = \prod_{p \text{ premier}} p^{-v_p(x)}.$$

Seul un nombre fini de terme des produits est différent de 1, car tout entier naturel non nul a un nombre fini de diviseurs premiers, et on obtient le résultat en remarquant que chaque terme de l'un des produits a son inverse dans l'autre. □

Cette formule est appelée *formule du produit* sur $\mathbb{Q}$. La formule du produit que nous verrons plus tard est une généralisation de celle-ci sur les corps de nombres.

Maintenant que nous connaissons les valeurs absolues sur $\mathbb{Q}$, nous allons nous intéresser à leurs prolongements aux corps de nombres. Nous allons voir que le nombre de valeurs absolues sur un corps de nombres est lié au nombre de plongements de ce corps de nombres dans $\mathbb{C}$ et dans $\mathbb{C}_p$ (défini plus tard).

Définition 10 *Soit K un corps de nombres. On appelle plongement de K dans $\mathbb{C}$ (ou $\mathbb{C}_p$) tout morphisme de corps σ de K dans $\mathbb{C}$ (ou $\mathbb{C}_p$) laissant $\mathbb{Q}$ invariant, c'est-à-dire tel que $\sigma_{|\mathbb{Q}} = id$.*

Proposition 10 *Soient $K = \mathbb{Q}(\gamma)$ un corps de nombres de degré d, $\gamma = \gamma_1, ..., \gamma_d$ les conjugués de γ et $P = \sum_{i=0}^{d} a_i X^i$ le polynôme minimal de γ.*
Il existe exactement d plongements $(\sigma_1, ..., \sigma_d)$ de K dans $\mathbb{C}$, donnés par

$$\forall i \in \{1, ..., d\}, \sigma_i : \gamma \mapsto \gamma_i.$$

Démonstration : On remarque tout d'abord que puisque les γ_i sont deux à deux distincts, les σ_i le sont également et il y en a donc bien d.

Puisque $(1, \gamma, ..., \gamma^{d-1})$ est une base de $\mathbb{Q}(\gamma)$ en tant que $\mathbb{Q}$-espace vectoriel, σ_i est entièrement déterminé par l'image de γ, pour $i \in \{1, ..., d\}$.

Réciproquement, soit σ un plongement de K dans $\mathbb{C}$. Puisque $\sum_{i=0}^{d} a_i \gamma^i = 0$ et σ est un morphisme de corps laissant $\mathbb{Q}$ (et donc $\mathbb{Z}$) invariant, on a

$$\sigma(\sum_{i=0}^{d} a_i \gamma^i) = \sum_{i=0}^{d} a_i \sigma(\gamma)^i = P(\sigma(\gamma)) = 0.$$

Donc $\sigma(\gamma)$ est racine de P : il existe $i \in \{1, ..., d\}$ tel que $\sigma(\gamma) = \gamma_i$. □

On remarque que si σ est un plongement de K dans $\mathbb{C}$ alors deux cas se présentent :
— Si $\sigma(K) \subset \mathbb{R}$ alors $\overline{\sigma} = \sigma$.
— Si $\sigma(K) \not\subset \mathbb{R}$ alors $\overline{\sigma} \neq \sigma$ et $\overline{\sigma}$ est un autre plongement.
Dans le premier cas on dira que σ est un *plongement réel*, et dans le deuxième cas on dira que σ est un *plongement complexe*. Ainsi on voit que le nombre de plongements complexes est pair. Si r_1 est le nombre de plongements réels et $2r_2$ est le nombre de plongements complexes on a $d = r_1 + 2r_2$ d'après la proposition précédente.

Corollaire 11 *Soient α et β deux nombres algébriques. Alors :*
— $\overline{|\alpha + \beta|} \leq \overline{|\alpha|} + \overline{|\beta|}$
— $\overline{|\alpha\beta|} \leq \overline{|\alpha|}\,\overline{|\beta|}$

Démonstration : Notons $\sigma_1, ..., \sigma_d$ les plongements complexes de $\mathbb{Q}(\alpha, \beta)$. Alors $\overline{|\alpha + \beta|} = \max_{1 \leq i \leq d} |\sigma_i(\alpha + \beta)| \leq \max_{1 \leq i \leq d} |\sigma_i(\alpha)| + \max_{1 \leq i \leq d} |\sigma_i(\beta)|$. De plus, comme dans la démonstration de la proposition 10, pour tout plongement σ de $\mathbb{Q}(\alpha, \beta)$ dans $\mathbb{C}$, $\sigma(\alpha)$ est un conjugué de α, et $\sigma(\beta)$ est un conjugué de β, et donc on a $\max_{1 \leq i \leq d} |\sigma_i(\alpha)| \leq \overline{|\alpha|}$ et $\max_{1 \leq i \leq d} |\sigma_i(\beta)| \leq \overline{|\beta|}$. Donc on a bien $\overline{|\alpha + \beta|} \leq \overline{|\alpha|} + \overline{|\beta|}$.

La démonstration est similaire pour le produit. □

Nous noterons M_K l'ensemble des (classes d'équivalence de) valeurs absolues sur le corps K et M_K^∞ l'ensemble des (classes d'équivalences de) valeurs absolues archimédiennes sur K. Nous allons maintenant voir un lien entre le cardinal de M_K^∞ et le nombre de plongements de K dans $\mathbb{C}$.

Proposition 12 *Soit $K = \mathbb{Q}(\gamma)$ un corps de nombre de degré d admettant r_1 plongements réels et $2r_2$ plongements complexes.*
Alors il existe exactement $r_1 + r_2$ valeurs absolues archimédiennes sur K et ces valeurs absolues sont données par :

$$\textit{pour } v \in M_K^\infty, \exists \sigma \textit{ plongement de } K \textit{ dans } \mathbb{C}, |.|_v = |\sigma(.)|,$$

où $|.|$ représente le module complexe classique.

Démonstration : Soit σ un plongement de K dans $\mathbb{C}$. Puisque σ est un morphisme de corps, on a immédiatement que $|.|_\sigma : x \mapsto |\sigma(x)| \in M_K^\infty$ et que $|.|_{\overline{\sigma}} = |.|_\sigma$ car $\forall z \in \mathbb{C}, |z| = |\overline{z}|$. Les plongements non conjugués étant deux à deux distincts, leurs valeurs absolues archimédiennes associées sont deux à deux distinctes et trivialement non équivalentes. Ainsi il y a au moins $r_1 + r_2$ valeur absolue archimédienne sur K.

Réciproquement, soit v dans M_K^∞. Montrons que l'on peut lui associer un plongement réel σ ou un couple de plongements complexes conjugués σ et $\overline{\sigma}$ tel que $|.|_v = |.|_\sigma$.

On note K_v le complété de K par rapport à la topologie induite par v. Soit γ_v l'image de γ dans K_v. Notons P le polynôme minimal de γ. Puisque γ_v est racine de P, $\mathbb{R}(\gamma_v)$ est une extension de $\mathbb{R}$ de degré fini sur $\mathbb{R}$, donc est égal à $\mathbb{R}$ ou $\mathbb{C}$ (en fait $\mathbb{R}(\gamma_v) = \mathbb{R}$ si γ_v est racine d'un polynôme de degré 1 dans la décomposition de P en produit de facteurs irréductibles dans $\mathbb{R}[X]$ et $\mathbb{R}(\gamma_v) = \mathbb{C}$ sinon).

Ainsi on a un plongement $\sigma_v : \gamma \mapsto \gamma_v$ et on a $|.|_{\sigma_v} = |.|_v$ par définition. Il existe donc exactement une valeur absolue archimédienne sur K par plongement réel et une par couple de plongements complexes, il y en a donc $r_1 + r_2$. □

Corollaire 13 *Avec les notations de la démonstration précédente, en posant $d_v = [\mathbb{R}(\gamma_v) : \mathbb{R}]$ et $P = a_0X^d + ... + a_d$ on a :*

$$\prod_{v \in M_K^\infty} |\gamma|_v^{d_v} = \prod_{i=1}^{d} |\gamma_i| = |\frac{a_d}{a_0}|.$$

Démonstration : On a vu que les valeurs absolues archimédiennes sur K correspondent exactement aux plongements de K dans $\mathbb{C}$, ces plongements qui eux-mêmes correspondent chacun à un γ_i, d'où la première partie de l'égalité. La

dernière partie de l'égalité vient des relations coefficients-racines appliquées au polynôme P. □

Ce résultat peut paraître anodin, mais il va en fait nous permettre de démontrer la formule du produit.

À partir de maintenant, pour un corps de nombres k et une valeur absolue v sur k, on notera $d_v(k)$ (ou d_v lorsqu'il n'y a pas d'ambiguïté) le nombre $[k_v : \mathbb{Q}]$ ou $[k_v : \mathbb{Q}_p]$ selon si v est archimédienne ou ultramétrique et où k_v représente le complété de k par rapport à la topologie induite par v.

Nous allons maintenant obtenir des résultats similaires aux Propositions 9 et 10, mais avec les plongements de K dans $\mathbb{C}_p$, que nous définissons :

Définition 11 *Soit p un nombre premier. On définit $\mathbb{Q}_p$ comme le complété de $\mathbb{Q}$ par rapport à la topologie induite par $|.|_p$, et $\mathbb{C}_p$ comme la clôture algébrique de $\mathbb{Q}_p$.*

L'ensemble $\mathbb{Q}_p$ joue en fait un rôle similaire à $\mathbb{R}$ et $\mathbb{C}_p$, comme la notation l'indique, joue un rôle similaire à $\mathbb{C}$. Le but ici n'est pas de développer la théorie des corps p-adiques. (Voir [6])

Par des démonstrations similaires, on obtient la proposition suivante :

Proposition 14 *Soient p un nombre premier, $K = \mathbb{Q}(\gamma)$ un corps de nombres de degré d, P le polynôme minimal de γ et $\gamma_1^{(p)}, ..., \gamma_d^{(p)}$ les racines de P dans $\mathbb{C}_p$.*

Alors il y a exactement d plongements de K dans $\mathbb{C}_p$, donnés par $\sigma_i : \gamma \mapsto \gamma_i^{(p)}, 1 \leq i \leq d$.

Les prolongement de $|.|_p$ sur K correspondent exactement aux n-uplets de $\gamma_i^{(p)}$ conjugués, c'est-à-dire racines d'un des facteurs dans la décomposition en produit de facteurs irréductibles de P dans $\mathbb{Q}_p[X]$. Un tel prolongement sera caractérisé par $v \in M_K, v \mid p$.

On a alors

$$d = \sum_{v \in M_K, v|p} d_v.$$

L'unique différence avec le cas archimédien est que les $\gamma_i^{(p)}$ conjugués peuvent venir par n-uplets au lieu de singletons ou couples.

Corollaire 15 *Avec les notations de la proposition précédente et en posant $P = a_0 X^d + ... + a_d$, on a :*

$$\prod_{v \in M_K, v|p} |\gamma|_v^{d_v} = \prod_{i=1}^{d} |\gamma_i^{(p)}|_p = |\frac{a_d}{a_0}|_p.$$

4) La formule du produit

Soit K une extension d'un corps k, soient w dans M_K et v dans M_k. On notera $w \mid v$ si v est la restriction de w à k.

Nous aurons besoin d'un dernier lemme avant de démontrer la formule du produit :

Lemme 2 *Soit K une extension finie d'un corps de nombres k. Soit w dans M_K. Alors*

$$\sum_{w|v} d_w(K) = [K : k] d_v(k).$$

Démonstration : Soit γ dans K tel que $K = \mathbb{Q}(\gamma)$. On a alors $K = k(\gamma)$. Le polynôme minimal P de γ sur k, qui est de degré $[K : k]$ peut être décomposé en produit de facteurs irréductibles sur $k_v[X]$ sous la forme $P = \prod_{w|v} P_w$ avec $\deg(P_w) = [K_w : k_v]$.

Ainsi $\sum_{w|v} [K_w : k_v] = [K : v]$. Enfin, puisque pour $w \mid v$, $d_w(K) = [K_w : \mathbb{Q}] = [K_w : k_v][k_v : \mathbb{Q}] = [K_w : k_v] d_v(k)$ par la formule de multiplication des degrés, on a le résultat souhaité. □

Théorème 12 (Formule du produit) *Soit α un nombre algébrique non nul. Soit K un corps de nombres contenant α. Alors on a*

$$\prod_{v \in M_K} |\alpha|_v^{d_v} = 1.$$

Démonstration : On commence par un cas simple, en prenant $k = \mathbb{Q}(\alpha)$. En posant $P = a_0 X^d + ... + a_d$, alors d'après les corollaires 11 et 13 on a :

$$\prod_{v \in M_k^\infty} |\alpha|_v^{d_v} = |\frac{a_d}{a_0}|$$

$$\text{et} \prod_{v \in M_k, v|p} |\alpha|_v^{d_v} = |\frac{a_d}{a_0}|_p.$$

Ainsi

$$\prod_{v \in M_k} |\alpha|_v^{d_v} = \prod_{v \in M_\mathbb{Q}} |\frac{a_d}{a_0}|_v = 1$$

d'après la formule du produit sur $\mathbb{Q}$.

Maintenant par le lemme précédent, on peut remarquer que la quantité

$$(\prod_{v\in M_K} |\alpha|_v^{d_v})^{\frac{1}{[K:k]}}$$

est indépendante du corps de nombres K contenant α (qui est alors une extension finie de k).

En effet, on a $\prod_{w\in M_K} |\alpha|_w^{d_w(K)} = \prod_{v\in M_k} |\alpha|_v^{\sum_{w|v} d_w(K)} = \prod_{v\in M_k} |\alpha|_v^{[K:k]d_v(k)}$.
Donc pour tout corps de nombres K contenant α, on a

$$\prod_{v\in M_K} |\alpha|_v^{d_v} = (\prod_{v\in M_k} |\alpha|_v^{d_v})^{[K:k]} = 1.$$

□

La formule du produit sera au cœur des deux démonstrations de transcendance de ce mémoire.

5) Hauteur logarithmique de Weil

À tout nombre algébrique α nous allons pouvoir associer un nombre réel, noté $h(\alpha)$, appelé hauteur (logarithmique) de Weil de α.

Définition 13 *Soient α un nombre algébrique et K un corps de nombres contenant α. On appelle hauteur (logarithmique) de Weil de α le nombre $h(\alpha) = \frac{1}{[K:\mathbb{Q}]} \sum_{v\in M_K} d_v \log \max(1, |\alpha|_v)$.*

On peut remarquer que ce nombre ne dépend pas du corps de nombres K contenant α de la même manière que le nombre $(\prod_{v\in M_K} |\alpha|_v^{d_v})^{\frac{1}{[K:k]}}$ ne dépendait pas de K dans la démonstration de la formule du produit.

Proposition 16 *Soient α_1 et α_2 deux nombres algébriques. Alors*

$$h(\alpha_1\alpha_2) \leq h(\alpha_1) + h(\alpha_2)$$
$$h(\alpha_1 + \alpha_2) \leq \log 2 + h(\alpha_1) + h(\alpha_2).$$

Si α est un nombre algébrique non nul, alors

$$\forall n \in \mathbb{Z}, h(\alpha^n) = |n|h(\alpha).$$

Démonstration : La première inégalité vient du fait que

$$\forall x, y \in \mathbb{R}^+, \max(1, xy) \leq \max(1, x) \max(1, y).$$

La seconde inégalité vient du fait que

$$\forall x, y \in \mathbb{R}^+, \max(1, x + y) \leq 2 \max(1, x) \max(1, y).$$

Enfin, $\forall x > 0, \forall n \in \mathbb{N}^*, \max(1, x^n) = \max(1, x)^n$. Il reste donc à montrer que pour α un nombre algébrique non nul on a $h(\alpha) = h(\frac{1}{\alpha})$.

Soient donc α un nombre algébrique non nul et k un corps de nombres contenant α. On sait que pour $x > 0, \max(1, x) = x \max(1, \frac{1}{x})$.

Mais alors

$$\begin{aligned} h(\frac{1}{\alpha}) &= \frac{1}{[k : \mathbb{Q}]} \sum_{v \in M_k} d_v \log \max(1, \frac{1}{|\alpha|_v}) \\ &= \frac{1}{[k : \mathbb{Q}]} \sum_{v \in M_k} d_v \log \frac{\max(1, |\alpha|_v)}{|\alpha|_v} \\ &= h(\alpha) - \frac{1}{[k : \mathbb{Q}]} \sum_{v \in M_k} d_v \log(|\alpha|_v) \\ &= h(\alpha) - \frac{1}{[k : \mathbb{Q}]} \log(\prod_{v \in M_k} |\alpha_v|_v^{d_v}) \\ &= h(\alpha) \end{aligned}$$

par la formule du produit. □

En guise d'exemple, calculons la hauteur de Weil d'un nombre rationnel $\frac{a}{b}$:

On suppose a et b premiers entre eux et on prend $K = \mathbb{Q}$ puisque $\frac{a}{b} \in \mathbb{Q}$ et $\mathbb{Q}$ est bien entendu un corps de nombres.

Alors

$$\begin{aligned} h(\frac{a}{b}) &= \frac{1}{[\mathbb{Q} : \mathbb{Q}]} \sum_{v \in M_{\mathbb{Q}}} d_v \log \max(1, |\frac{a}{b}|_v) \\ &= \sum_{v \in M_{\mathbb{Q}}} \log \max(1, |\frac{a}{b}|_v) \end{aligned}$$

car $[\mathbb{Q} : \mathbb{Q}] = 1$ et pour tout v dans $M_{\mathbb{Q}}, d_v = 1$ (le polynôme minimal de $\frac{a}{b}$ est $bX - a$, qui est de degré 1).

Soit maintenant p un nombre premier. Puisque a et b sont premiers entre eux, 3 cas sont possibles :

— Soit $p \nmid a$ et $p \nmid b$, alors $|\frac{a}{b}|_p = 1$.
— Soit $p \mid a$ et $p \nmid b$, alors $|\frac{a}{b}|_p = p^{-v_p(a)} < 1$.
— Soit $p \nmid a$ et $p \mid b$, alors $|\frac{a}{b}|_p = p^{v_p(b)} > 1$.
D'où

$$\begin{aligned} h(\frac{a}{b}) &= \sum_{p|b} \log p^{v_p(b)} + \log \max(1, |\frac{a}{b}|) \\ &= \log |b| + \log \max(1, |\frac{a}{b}|) \\ &= \log \max(|a|, |b|) \end{aligned}$$

La hauteur de Weil d'un nombre algébrique α quantifie sa « complexité arithmétique ». Nous ne nous en servirons que lors de la démonstration du théorème d'Hermite-Lindemann, où l'on peut la faire apparaître de manière naturelle.

Partie II : Le théorème d'Hermite-Lindemann

Maintenant que nous avons étudié certaines propriétés des nombres algébriques, et notamment établi la formule du produit, nous allons pouvoir démontrer le premier résultat de transcendance de ce mémoire, le théorème d'Hermite-Lindemann, démontré par Lindemann en 1882.

1) Énoncé du théorème et corollaires

Énonçons tout d'abord le théorème et quelques corollaires immédiats.

Théorème 14 (Hermite-Lindemann) *Soit α un nombre algébrique non nul. Alors e^{α} est transcendant.*

Corollaire 17 *Le nombre* e *est transcendant.*

Démonstration : C'est immédiat en appliquant le théorème d'Hermite-Lindemann au nombre algébrique 1. □

Corollaire 18 *Le nombre π est transcendant.*

Démonstration : Supposons π algébrique. Alors $i\pi$ est algébrique puisque i est algébrique et $\overline{\mathbb{Q}}$ est un sous-corps de $\mathbb{C}$. Mais alors d'après le théorème d'Hermite-Lindemann, $-1 = \mathrm{e}^{\mathrm{i}\pi}$ est transcendant, ce qui est absurde. □

Corollaire 19 *Soit α un nombre algébrique non nul. Alors $\log(\alpha)$ est transcendant pour toute détermination non nulle du logarithme de α.*

Démonstration : En effet si $\log(\alpha)$ était algébrique alors d'après le théorème d'Hermite-Lindemann on aurait que $\mathrm{e}^{\log(\alpha)} = \alpha$ est transcendant, ce qui est absurde. □

Remarque : Ce dernier corollaire est même équivalent au théorème d'Hermite-Lindemann par le même type de raisonnement.

2) Plan de la démonstration

La démonstration du théorème d'Hermite-Lindemann que nous allons voir n'apparaît pas comme intuitive. Nous allons donc donner tout d'abord le plan de cette démonstration :

— On va considérer un nombre algébrique non nul α et supposer, par l'absurde, que e^{α} est algébrique.

— Ensuite, on va se placer dans $K = \mathbb{Q}(\alpha, e^{\alpha})$ qui est alors un corps de nombres par hypothèse.

— En utilisant ce qu'on appelle le lemme de Siegel, on va construire une fonction F_n dépendant d'un entier naturel n, polynomiale en X et e^X, ayant des coefficients « petits » et s'annulant en 0 et α à des ordres au moins n.

— Une étape importante sera de montrer que la fonction F_n n'est pas identiquement nulle.

— On va ensuite considérer la valeur algébrique non nulle en 0 ou en α d'une certaine dérivée de F_n, que l'on appellera β.

— On va majorer les différentes valeurs absolues de β sur le corps de nombres K puis on va majorer $|\beta|$ par des méthodes d'analyse complexe.

— Enfin, en appliquant la formule du produit et en faisant tendre n vers $+\infty$ on obtiendra la contradiction voulue.

Cette démonstration est inspirée de du Chapitre 12 de [7], la principale différence est que nous allons utiliser les valeurs absolues p-adiques et la formule du produit.

Les majorations que nous allons effectuer dans cette démonstration sont très brutales, seule la majoration par des méthodes d'analyse complexe a besoin d'être fine. Il nous reste deux résultats intermédiaires à obtenir pour pouvoir écrire notre démonstration du théorème d'Hermite-Lindemann. Le premier servira à montrer que la fonction F_n n'est pas identiquement nulle.

Lemme 3 *La fonction exponentielle est transcendante (sur $\mathbb{C}[X]$), i.e. si on pose $f = \exp$, on a*

$\forall d \in \mathbb{N}, \forall (P_i)_{0 \leq i \leq d} \in \mathbb{C}[X]^{d+1}, P_d \neq 0,$ *on a* $P_d f^d + P_{d-1} f^{d-1} + ... + P_1 f + P_0 \neq 0.$

Démonstration : Supposons que la fonction exponentielle n'est pas transcendante. Alors il existe $d \in \mathbb{N}$ et $(P_i)_{0\leq i\leq d} \in \mathbb{C}[X]^{d+1}$ avec $P_d \neq 0$ tels que $\forall x \in \mathbb{C}, P_d(x)\mathrm{e}^{dx} + P_{d-1}(x)\mathrm{e}^{(d-1)x} + ... + P_1(x)\mathrm{e}^x + P_0(x) = 0$.

Mais alors $\forall x \in \mathbb{C}, P_d(x) = -P_{d-1}(x)\mathrm{e}^{-x} - ... - P_1(x)\mathrm{e}^{-(d-1)x} - P_0(x)\mathrm{e}^{-dx}$. Le membre de droite tend vers 0 quand x est réel et tend vers $+\infty$, ce qui implique que $P_d = 0$, contradiction. □

Lemme 4 (Lemme de Siegel) *Soit K un corps de nombres de degré d. Soient $(A_{ij}), 1 \leq i \leq m, 1 \leq j \leq n$ des entiers algébriques de K avec $n > dm$. On pose B la matrice de taille $n \times m$ des A_{ij}.*

Soit A dans $\mathbb{N}$ tel que $\max\limits_{1\leq i\leq m, 1\leq j\leq n}(\overline{|A_{ij}|}) \leq A$.

Alors $\exists (x_i)_{1\leq i\leq n} = x \in \mathbb{Z}^n, 0 < \max\limits_{1\leq i\leq n} |x_i| \leq (n\sqrt{2}A)^{\frac{dm}{n-dm}}$ *et* ${}^tBx = 0$.

Démonstration : Démontrons tout d'abord une version plus faible ce lemme, dans le cas où $K = \mathbb{Q}$. On a ainsi $d = 1$.

Pour $1 \leq j \leq m$, notons $-V_j = \sum\limits_{i=1, A_{i,j}<0}^{n} A_{i,j}$ et $W_j = \sum\limits_{i=1, A_{i,j}>0}^{n} A_{i,j}$, respectivement l'opposé de la somme des $A_{i,j}$ négatifs et la somme des $A_{i,j}$ positifs. On a $\forall j \in \{1, ..., m\}, V_j + W_j \leq nA$.

Soit X un entier naturel. On définit

$$\phi : (x_i)_{1\leq i\leq n} \mapsto (\sum_{i=1}^{n} A_{i,j}x_i)_{1\leq j\leq m}$$

sur $\{0, ..., X\}^n$.

$\forall x \in \{0, ..., X\}^n, \forall j \in \{1, ..., m\}, -V_jX \leq (\phi(x))_j \leq W_jX$

On a donc $\#(\{0, ..., X\}^n) = (X + 1)^n$ et $\#(\phi(\{0, ..., X\}^n)) \leq (nAX + 1)^m$, où $\#E$ désigne le cardinal de l'ensemble E.

On choisit alors $X = \lfloor (nA)^{\frac{n}{n-m}} \rfloor$.

Alors on a $(X+1)^{n-m} > X^{n-m} \geq (nA)^m$. Donc $(X+1)^n > (X+1)^m(nA)^m \geq (nAX + 1)^m$.

Dans ce cas, ϕ ne peut être injective car le cardinal de son ensemble de départ est strictement supérieur au cardinal de son image, et donc

$$\exists x \in \{0, ..., X\}^m, x \neq 0 \text{ et } \phi(x) = 0$$

et ce x vérifie bien $0 < \max\limits_{1\leq i\leq n} |x_i| \leq (nA)^{\frac{n}{n-m}} \leq (n\sqrt{2}A)^{\frac{n}{n-m}}$.

Considérons maintenant le cas général, où K est un corps de nombres de degré $d > 1$.

Soit $(\omega_1, ..., \omega_d)$ une $\mathbb{Z}$-base du $\mathbb{Z}$-module des entiers de K (on admet le fait que cet ensemble forme bien un $\mathbb{Z}$-module libre).

Alors les $A_{i,j}$ vérifient :

$$\forall i \in \{1, ..., n\}, \forall j \in \{1, ..., m\}, A_{i,j} = \sum_{k=1}^{d} a_{i,j,k}\omega_k, \qquad (1)$$

avec les $a_{i,j,k}$ dans $\mathbb{Z}$ car les $A_{i,j}$ sont entiers sur K.

Le système à résoudre s'écrit donc

$$\forall j \in \{1, ..., m\}, \sum_{i=1}^{n}\sum_{k=1}^{d} x_i a_{i,j,k}\omega_k,$$

qui est équivalent au système suivant (puisque les ω_k forment une base de K) :

$$\forall j \in \{1, ..., m\}, \forall k \in \{1, ..., d\}, \sum_{i=1}^{n} a_{i,j,k}x_i,$$

système de dm équations à n inconnues, à coefficients entiers.

Puisque $n > dm$, on peut utiliser la version faible du lemme, et obtenir une solution $x \in \mathbb{Z}^n$ vérifiant $0 < \max\limits_{1\leq i\leq n} |x_i| \leq (n \max\limits_{i,j,k} |a_{i,j,k}|)^{\frac{dm}{n-dm}}$.

Notons $\sigma_1, ..., \sigma_d$ les d plongements de K dans $\mathbb{C}$. Alors en appliquant ces plongements à (1) on obtient les équations suivantes :

$$\forall i \in \{1, .., n\}, \forall j \in \{1, ..., m\}, \forall k \in \{1, ..., d\}, \sum_{h=1}^{d} a_{i,j,h}\sigma_k(\omega_h) = \sigma_k(A_{i,j}).$$

Avec les formules de Cramer, on peut obtenir une constante $M > 0$ ne dépendant ni de n ni de m telle que $\forall i, j, k, |a_{i,j,k}| \leq M \max\limits_{1\leq h\leq d} |\sigma_h(A_{i,j})| \leq MA$.

Enfin on peut améliorer cette constante en $\sqrt{2}$ et montrer que celle-ci est optimale (voir [4], Chapitre I).

On a donc une solution $x \in \mathbb{Z}^n$ vérifiant $0 < \max\limits_{1\leq i\leq n} |x_i| \leq (n\sqrt{2})^{\frac{dm}{n-dm}}$. □

3) Démonstration du théorème

Rappelons l'énoncé du théorème :

Théorème (Hermite-Lindemann) *Soit α un nombre algébrique non nul. Alors e^{α} est transcendant.*

Démonstration : Soit α un nombre algébrique non nul. Supposons e^{α} algébrique.

Alors $K = \mathbb{Q}(\alpha, e^{\alpha})$ est un corps de nombres, de degré d. Soient n, p et q dans $\mathbb{N}$ tels que $(p+1)(q+1) > 2dn$.

On considère la fonction F_n définie sur $\mathbb{C}$ par

$$\forall x \in \mathbb{C}, F_n(x) = \sum_{i=0}^{p} \sum_{j=0}^{q} a_{ij} x^i e^{jx}$$

avec $\forall i \in \{1, ..., p\}, \forall j \in \{1, ..., q\}, a_{ij} \in \mathbb{Z}$.

Utilisons le lemme de Siegel pour montrer que l'on peut choisir les a_{ij} de sorte que :

— $0 < \max\limits_{0 \leq i \leq p, 0 \leq j \leq q} |a_{ij}| \leq e^n$

— $F_n(0) = F_n'(0) = ... = F_n^{(n-1)}(0) = 0 \qquad (1)$

— $F_n(\alpha) = F_n'(\alpha) = ... = F_n^{(n-1)}(\alpha) = 0 \qquad (2)$

Par la formule de Leibniz, pour $k \in \{0, ..., n-1\}$ et $x \in \mathbb{C}$, on a

$$\begin{aligned} F_n^{(k)}(x) &= \sum_{i=0}^{p} \sum_{j=0}^{q} a_{ij} \sum_{l=0}^{k} \binom{k}{l} i(i-1)...(i-l+1) x^{i-l} j^{k-l} e^{jx} \\ &= \sum_{i=0}^{p} \sum_{j=0}^{q} a_{ij} A_{ij}'^{(k)}(x) \end{aligned}$$

Les conditions (1) et (2) nous donnent un système de $2n$ équations à $(p+1)(q+1)$ inconnues (les a_{ij}). Dans la suite, pour éviter les notations trop lourdes on aura toujours $i \in \{0, ..., p\}, j \in \{0, ...q\}$ et $k \in \{0, ..., n-1\}$.

On a $\forall i, j, k, A_{ij}'^{(k)}(0) \in K$ et $A_{ij}'^{(k)}(\alpha) \in K$ puisque $\alpha \in K$, $e^{\alpha} \in K$ et puisque K est un corps. Par la proposition 5, il existe $d_1 \in \mathbb{N}^*$ et $d_2 \in \mathbb{N}^*$ tels que $d_1\alpha$ et $d_2 e^{\alpha}$ soient des entiers algébriques. Alors $\forall i, j, k, d_1^p d_2^q A_{i,j}'^{(k)}(\alpha)$ est un entier algébrique.

On multiplie (1) et (2) par $D = d_1^p d_2^q$. On a alors le système de $2n$ équations à $(p+1)(q+1)$ inconnues équivalent suivant :

$$\forall k, \forall r \in \{0, \alpha\}, \sum_{i,j} a_{ij} A_{ij}^{(k)}(r) = 0,$$

avec $\forall i, j, k, r \in \{0, \alpha\}, A_{i,j}^{(k)}(r) = D A_{i,j}'^{(k)}(r)$ est un entier algébrique.

Puisqu'on a choisi $(p+1)(q+1) > 2dn$ et que les $A_{ij}^{(k)}$ sont entiers algébriques (Proposition 8), on a d'après le lemme de Siegel une solution $(a_{ij})_{i,j} \in \mathbb{Z}^{(p+1)(q+1)}$

vérifiant :

$$0 < \max_{i,j} |a_{ij}| \leq ((p+1)(q+1)\sqrt{2}A)^{\frac{2dn}{(p+1)(q+1)-2dn}}.$$

avec A dans $\mathbb{N}$ tel que $\max\limits_{i,j,k,r\in\{0,\alpha\}}(\overline{|A_{ij}^{(k)}(r)|}) \leq A$.

Il nous reste maintenant à montrer que l'on peut prendre A de sorte que $((p+1)(q+1)\sqrt{2}A)^{\frac{2dn}{(p+1)(q+1)-2dn}} \leq \mathrm{e}^n$.

Majorons donc $\overline{|A_{i,j}^{(k)}(0)|}$ et $\overline{|A_{i,j}^{(k)}(\alpha)|}$. Rappelons que

$$A_{i,j}^{(k)}(\alpha) = D\sum_{l=0}^{k}\binom{k}{l} i(i-1)...(i-l+1)\alpha^{i-l}j^{k-l}\mathrm{e}^{j\alpha}.$$

Posons $C = \max(1, \overline{|\alpha|}, \overline{|\mathrm{e}^{\alpha}|})$.

Alors

$$\begin{aligned}\overline{|A_{ij}^{(k)}(\alpha)|} &\leq D\sum_{l=0}^{k}\binom{k}{l} i!\overline{|\alpha|}^{i} j^{k}\overline{|\mathrm{e}^{\alpha}|}^{j} \\ &\leq D\sum_{l=0}^{k}\binom{k}{l} p^p q^n C^{p+q}\end{aligned}$$

en utilisant que $i \leq p, i! \leq p! \leq p^p$, que $j \leq q$ et que $k \leq n$.

Désormais on considère que $p = \lfloor \frac{n}{\log n} \rfloor$ et $q = \lfloor (\log n)^2 \rfloor$. On a bien que $(p+1)(q+1) > 2dn$ pour n assez grand (dès que $\log n > 2d$ pour être précis). On a donc $p^p \leq n^{\frac{n}{\log n}} = \mathrm{e}^n$ et $D \leq \mathrm{e}^n$ pour n assez grand.

En utilisant cela, et le fait que $\sum\limits_{l=0}^{k}\binom{k}{l} = 2^k \leq 2^n$ on obtient :

$$\begin{aligned}\overline{|A_{ij}^{(k)}(\alpha)|} &\leq \mathrm{e}^{2n}2^n(\log n)^{2n}C^{p+q} \qquad (3)\\ &\leq \mathrm{e}^{6n\log\log n} \qquad (4)\end{aligned}$$

pour n assez grand, car (3) est négligeable devant (4).

Procédons de même pour $|A_{ij}^{(k)}(0)| = D\binom{k}{i} i!j^{k-i}$:

$$\begin{aligned}\overline{|A_{ij}^{(k)}(0)|} &= |D\binom{k}{i} i!j^{k-i}| \\ &\leq \mathrm{e}^n 2^n p^p q^n \\ &\leq \mathrm{e}^{6n\log\log n}\end{aligned}$$

pour n assez grand.

Ainsi, $A = \lfloor \mathrm{e}^{6n\log\log n} \rfloor$ convient.

Alors

$$\begin{aligned}((p+1)(q+1)\sqrt{2}A)^{\frac{2dn}{(p+1)(q+1)-2dn}} &\leq (2\sqrt{2}n\log n\mathrm{e}^{6n\log\log n})^{\frac{2dn}{(p+1)(q+1)-2dn}} \\ &\leq \mathrm{e}^{7n\log\log n\times\frac{2d}{\log n-2d}} \\ &\leq \mathrm{e}^{n},\end{aligned}$$

les inégalités se produisant encore une fois pour n assez grand, le but étant de le faire tendre vers $+\infty$.

Récapitulons, on a montré l'existence de (a_{ij}) dans $\mathbb{Z}^{(p+1)(q+1)}$ tel que :
— $0 < \max\limits_{i,j} |a_{ij}| \leq \mathrm{e}^n$
— $F_n(0) = F_n'(0) = ... = F_n^{(n-1)}(0) = 0$
— $F_n(\alpha) = F_n'(\alpha) = ... = F_n^{(n-1)}(\alpha) = 0$

La fonction exp étant transcendante d'après le lemme 3, la fonction F_n n'est pas identiquement nulle. Puisqu'elle est holomorphe sur $\mathbb{C}$, elle est développable en série entière au voisinage de 0, et donc $\exists k \in \mathbb{N}^*, F_n^{(k)}(0) \neq 0$.

Soit m le plus grand entier tel que

$$\begin{aligned}F_n(0) = F_n'(0) = ... = F_n^{(m-1)}(0) \\ = F_n(\alpha) = F_n'(\alpha) = ... = F_n^{(m-1)}(\alpha) = 0\end{aligned}$$

Par définition, $m \geq n$. Ainsi $\exists r \in \{0, \alpha\}, F_n^{(m)}(r) \neq 0$. Notons β ce nombre. C'est un nombre algébrique car $\beta \in K$.

Nous allons maintenant majorer les différentes valeurs absolues sur K de β :

— Cas $\beta = F_n^{(m)}(\alpha) = \sum\limits_{i=0}^{p}\sum\limits_{j=0}^{q} a_{ij}\sum\limits_{l=0}^{m}\binom{m}{l} i(i-1)...(i-l+1)\alpha^{i-l}j^{m-l}\mathrm{e}^{j\alpha}$:
Soit v une valeur absolue ultramétrique sur K.

$$\begin{aligned}|F_n^{(m)}(\alpha)|_v &\leq \max_{i,j,0\leq l\leq m}\{|a_{ij}\binom{m}{l}i(i-1)...(i-l+1)j^{m-l}|_v|\alpha|_v^{i-l}|\mathrm{e}^{\alpha}|_v^{j}\} \\ &\leq \max(1,|\alpha|_v)^p\max(1,|\mathrm{e}^{\alpha}|_v)^q \qquad (\text{car } \forall a\in\mathbb{Z}, |a|_v \leq 1)\end{aligned}$$

Maintenant, soit v une valeur absolue archimédienne sur K.

$$\begin{aligned}|F_n^{(m)}(\alpha)|_v &\leq (p+1)(q+1)\mathrm{e}^n 2^m p^p q^m \max(1,|\alpha|_v)^p \max(1,|\mathrm{e}^\alpha|_v)^q \\ &\leq (10q)^m p^p \max(1,|\alpha|_v)^p \max(1,|\mathrm{e}^\alpha|_v)^q\end{aligned}$$

avec le même genre de majorations que précédemment.

— Cas $\beta = F_n^{(m)}(0) = \sum_{i=0}^{p}\sum_{j=0}^{q} a_{ij}\binom{m}{i} i!\, j^{m-i}$:

Soit v une valeur absolue ultramétrique sur K. Puisque $F_n^{(m)}(0) \in \mathbb{Z}$ et puisque v est ultramétrique, on a

$$\begin{aligned}|F_n^{(m)}(0)|_v &= 1 \\ &\leq \max(1,|\alpha|_v)^p \max(1,|\mathrm{e}^\alpha|_v)^q\end{aligned}$$

Et soit maintenant v une valeur absolue archimédienne sur K.

$$\begin{aligned}|F_n^{(m)}(0)|_v &\leq (p+1)(q+1)\mathrm{e}^n 2^m p^p q^m \\ &\leq (10q)^m p^p \max(1,|\alpha|_v)^p \max(1,|\mathrm{e}^\alpha|_v)^q\end{aligned}$$

On remarque que dans ce cas, les valeurs absolues de α et de e^α n'interviennent pas réellement, on les a introduites dans les majorations pour faire apparaître plus tard $h(\alpha)$ et $h(\mathrm{e}^\alpha)$.

Dans tous les cas, on a montré que :
— Pour v ultramétrique on a $|\beta|_v \leq \max(1,|\alpha|_v)^p \max(1,|\mathrm{e}^\alpha|_v)^q$.
— Pour v archimédienne on a $|\beta|_v \leq (10q)^m p^p \max(1,|\alpha|_v)^q \max(1,|\mathrm{e}^\alpha|_v)^p$.

En vu d'obtenir une absurdité dans la formule du produit appliquée à β (qui est par construction non nul), on va majorer finement $|\beta|$ grâce au principe du maximum.

La fonction F_n est holomorphe sur $\mathbb{C}$ et $\forall k \in \{0,...,m-1\}, F_n^{(k)}(0) = F_n^{(k)}(\alpha) = 0$.

Posons $G : z \mapsto \frac{F_n(z)}{z^m(z-\alpha)^m}$. Par la remarque précédente, G est aussi holomorphe sur $\mathbb{C}$, et on a $G(0) = \frac{1}{(-\alpha)^m}\frac{F_n^{(m)}(0)}{m!}$ et $G(\alpha) = \frac{1}{\alpha^m}\frac{F_n^{(m)}(\alpha)}{m!}$. Donc $|\beta| = |\alpha|^m m!|G(r)|$ avec $r \in \{0,\alpha\}$.

Soit R dans $\mathbb{R}^{+*}$ tel que $|\alpha| < R$. Par le principe du maximum on a

$$\begin{aligned}\forall z \in \mathbb{C}, |z| \leq |\alpha| \Rightarrow |G(z)| &\leq \sup_{|\omega|=R} |G(\omega)| \\ &\leq \frac{\sup\limits_{|\omega|=R} |F_n(\omega)|}{R^m(R-|\alpha|)^m} \\ &\leq \frac{2^m(p+1)(q+1)\mathrm{e}^n R^p \mathrm{e}^{Rq}}{R^{2m}}\end{aligned}$$

car $\frac{1}{R(R-|\alpha|)} \leq \frac{2}{R^2}$ pour R assez grand.

D'où

$$|\beta| \leq \frac{2^m|\alpha|^m(p+1)(q+1)\mathrm{e}^n R^p \mathrm{e}^{Rq} m!}{R^{2m}}$$

Enfin, en prenant $R = m^{\frac{2}{3}}$ (on a bien $R \geq |\alpha|$ pour n assez grand puisque $m \geq n$), et en utilisant que $m! \leq m^m$ on obtient :

$$|\beta| \leq \frac{(2|\alpha|)^m \mathrm{e}^{2m} m^m}{m^{\frac{4m}{3}}} \leq m^{-\frac{m}{6}}$$

pour n (et donc m) assez grand. En particulier, pour m assez grand, $|\beta| < 1$.

Puisqu'on a construit β de sorte qu'il soit non nul, on peut lui appliquer la formule du produit :

$$\prod_{v \in M_K} |\beta|_v^{d_v} = 1$$

Grâce aux majorations des différentes valeurs absolues de β on a :

$$\begin{aligned}\prod_{v \in M_K, v \neq |.|} |\beta|_v^{d_v} &\leq \prod_{v \in M_k, v|p} \max(1, |\alpha|_v)^{pd_v} \max(1, |\mathrm{e}^\alpha|_v)^{qd_v} \\ &\quad \times \prod_{v \in M_K^\infty, v \neq |.|} (10q)^{md_v} p^{pd_v} \max(1, |\alpha|_v)^{pd_v} \max(1, |\mathrm{e}^\alpha|_v)^{qd_v} \\ &\leq \prod_{v \in M_k, v|p} \max(1, |\alpha|_v)^{pd_v} \max(1, |\mathrm{e}^\alpha|_v)^{qd_v} \\ &\quad \times \prod_{v \in M_K^\infty} (10q)^{md_v} p^{pd_v} \max(1, |\alpha|_v)^{pd_v} \max(1, |\mathrm{e}^\alpha|_v)^{qd_v} \\ &\leq \mathrm{e}^{dph(\alpha)+dqh(\mathrm{e}^\alpha)} (10q)^{dm} p^{dp}\end{aligned}$$

Pour compléter ce produit afin d'obtenir 1 (formule du produit), il faut multiplier par $|\beta|$ ou $|\beta|^2$. Dans tous les cas, on multiplie par un nombre inférieur à $m^{-\frac{m}{6}}$.

On rappelle que $p = \lfloor \frac{n}{\log n} \rfloor$ et que $q = \lfloor (\log n)^2 \rfloor$, d'où, puisque $m \geq n$, on a

$$1 \leq m^{-\frac{m}{6}} \mathrm{e}^{dph(\alpha)+dqh(\mathrm{e}^{\alpha})} (10q)^{dm} p^{dp} \longrightarrow 0 \text{ quand } m \to +\infty$$

ce qui donne la contradiction recherchée. □

Remarque : On a utilisé ce que l'on appelle la méthode de Gelfond, qui se base sur l'identité $\exp' = \exp$. Une autre méthode est celle de Schneider, utilisant l'identité $\forall a, b \in \mathbb{C}, \mathrm{e}^a \mathrm{e}^b = \mathrm{e}^{a+b}$. Gelfond et Schneider ont démontré indépendamment, chacun avec sa méthode, en 1934, un célèbre résultat de transcendance, le théorème de Gelfond-Schneider sur lequel nous reviendrons en annexes.

Partie III : Le théorème de Lindemann-Weierstrass

Nous allons maintenant énoncer puis démontrer le théorème de Lindemann-Weierstrass, démontré par Weierstrass en 1885, et qui généralise le théorème d'Hermite-Lindemann en plus grande dimension.

1) Énoncé du théorème et corollaires

Définition 15 *Soient $\alpha_1, ..., \alpha_n$ des nombres complexes. On dit qu'ils sont algébriquement indépendants si $\forall P \in \overline{\mathbb{Q}}[X_1, ..., X_n] \setminus \{0\}, P(\alpha_1, ..., \alpha_n) \neq 0$.*

Théorème 16 (Lindemann-Weierstrass) *Soient $\alpha_1, ..., \alpha_n$ des nombres algébriques linéairement indépendants sur $\mathbb{Q}$. Alors $e^{\alpha_1}, ..., e^{\alpha_n}$ sont algébriquement indépendants.*

Le théorème d'Hermite-Lindemann en est un corollaire :

Corollaire 20 *Soit α un nombre algébrique non nul. Alors e^{α} est transcendant.*

Démonstration : Soit α un nombre algébrique non nul. Puisque $\alpha \neq 0$, $\{\alpha\}$ est une famille linéairement indépendante sur $\mathbb{Q}$. Donc d'après le théorème de Lindemann-Weierstrass, $\forall P \in \overline{\mathbb{Q}}[X] \setminus \{0\}, P(e^{\alpha}) \neq 0$. Donc e^{α} est transcendant. □

Le théorème de Lindemann-Weierstrass est un des seuls résultats d'indépendance algébrique connu à ce jour, mais on peut montrer qu'il est équivalent à une version faible d'indépendance linéaire :

Proposition 21 *Le théorème de Lindemann-Weierstrass est équivalent à l'énoncé suivant :*

Pour tous $b_1, ..., b_n$ dans $\mathbb{Z}$ non tous nuls et pour tous $\alpha_1, ..., \alpha_n$ dans $\overline{\mathbb{Q}}$ deux à deux distincts, on a $b_1 e^{\alpha_1} + ... + b_n e^{\alpha_n} \neq 0$. (E)

A partir de cet énoncé, on peut obtenir la transcendance de certains nombres tels que $\alpha = 2e^{\sqrt{2}} + 3e^{\sqrt{3}} + ... + ne^{\sqrt{n}}$ pour $n \geq 2$. En effet si ce nombre était algébrique, il vérifierait $2e^{\sqrt{2}} + 3e^{\sqrt{3}} + ... + ne^{\sqrt{n}} - \alpha e^0 = 0$ ce qui contredirait le théorème. Plus généralement, tout nombre de la forme $b_1 e^{\alpha_1} + ... + b_n e^{\alpha_n}$ avec les α_i algébriques non nuls deux à deux distincts et les b_i algébriques non nuls est transcendant.

Ainsi on a le corollaire suivant :

Corollaire 22 *Soit α un nombre algébrique non nul. Alors $\cos(\alpha), \sin(\alpha)$ et $\tan(\alpha)$ sont transcendants.*

Démonstration : Soit α un nombre algébrique non nul. Par les formules d'Euler, $\cos(\alpha) = \frac{e^{i\alpha}+e^{-i\alpha}}{2}$, et par la dernière remarque, ce nombre est transcendant. La démonstration est similaire pour $\sin(\alpha)$. Enfin, on a $\tan(\alpha) = -i\frac{e^{i\alpha}-e^{-i\alpha}}{e^{i\alpha}+e^{-i\alpha}}$ d'où $(\tan(\alpha)+i)e^{i\alpha} + (\tan(\alpha)-i)e^{-i\alpha} = 0$ ce qui est absurde si $\tan(\alpha)$ est algébrique.□

Remarque : On a de la même manière la transcendance de $\cosh(\alpha), \sinh(\alpha)$ et $\tanh(\alpha)$ pour α algébrique non nul.

2) Quelques lemmes de théorie de Galois

Pour démontrer la Proposition 21, puis la théorème de Lindemann-Weierstrass lui-même grâce à sa version d'indépendance linéaire, nous aurons besoin de quelques lemmes de théorie de Galois, que nous admettrons, car il ne s'agit pas de l'objet de ce mémoire.

Lemme 5 *Soit K un corps de nombres. Il existe un corps de nombres K' contenant K tel que les plongements de K' dans $\mathbb{C}$ forment un groupe (fini) pour la composition. En particulier, les plongements de K' dans $\mathbb{C}$ sont à valeurs dans K'. Un tel corps de nombres sera appelé extension galoisienne de $\mathbb{Q}$.*

Lemme 6 *Soient K un corps de nombres, et α dans K tels que pour tout plongement σ de K dans $\mathbb{C}$, $\sigma(\alpha) = \alpha$. Alors $\alpha \in \mathbb{Q}$.*

Démonstration de la Proposition 21 : L'implication « Le théorème de Lindemann-Weierstrass implique (E) » est évidente dans le cas où les α_i sont linéairement indépendants sur $\mathbb{Q}$, car $b_1X_1 + ... + b_nX_n$ est un polynôme non nul de $\mathbb{Z}[X]$ (et donc $\overline{\mathbb{Q}}[X]$).

Maintenant, supposons que la famille $\{\alpha_1, ..., \alpha_n\}$ soit liée sur $\mathbb{Q}$. Quitte à réordonner les α_i, on peut supposer $\alpha_n = \sum_{i=1}^{n-1} a_i\alpha_i$ avec $\forall i \in \{1, ..., n-1\}, a_i \in \mathbb{Q}$. On réitère ce processus jusqu'à ce que $\alpha_1, ..., \alpha_k$ soient linéairement indépendants sur $\mathbb{Q}$ et on obtient $\alpha_j = \sum_{i=1}^{k} a_{i,j}\alpha_i$ avec les $a_{i,j}$ dans $\mathbb{Q}$ pour $j \in \{k+1, ..., n\}$. Maintenant pour $j \geq k+1, \mathrm{e}^{\alpha_j} = \prod_{i=1}^{k} \mathrm{e}^{a_{i,j}\alpha_i}$.

Ainsi,

$$b_1\mathrm{e}^{\alpha_1} + ... + b_n\mathrm{e}^{\alpha_n} = b_1\mathrm{e}^{\alpha_1} + ... + b_k\mathrm{e}^{\alpha_k} + b_{k+1}\prod_{i=1}^{k}\mathrm{e}^{a_{i,k+1}\alpha_i} + ... + b_n\prod_{i=1}^{k}\mathrm{e}^{a_{i,n}\alpha_i} = 0 \quad (1)$$

À partir de maintenant, on va éliminer les exposants à coefficients négatifs devant les α_i. Notons $b_{i,j} = -a_{i,j}$ si $a_{i,j} < 0$, et $b_{i,j} = 0$ sinon. On multiplie (1) par $\mathrm{e}^{-a_{i,j}\alpha_i}$ dès que $a_{i,j} < 0$, de sorte que l'on ait :

$$\prod_{i=1}^{k}\prod_{j=k+1}^{n}\mathrm{e}^{b_{i,j}\alpha_i}(b_1\mathrm{e}^{\alpha_1} + ... + b_k\mathrm{e}^{\alpha_k} + b_{k+1}\prod_{i=1}^{k}\mathrm{e}^{a_{i,k+1}\alpha_i} + ... + b_n\prod_{i=1}^{k}\mathrm{e}^{a_{i,n}\alpha_i}) = 0 \quad (2)$$

Enfin pour $1 \leq i \leq k$, notons c_i le PPCM des dénominateurs des $a_{i,j} + b_{i,j}$ pour $k+1 \leq j \leq n$.

Alors (2) est une relation de dépendance algébrique de la famille $\{\mathrm{e}^{\frac{\alpha_1}{c_1}}, ..., \mathrm{e}^{\frac{\alpha_k}{c_k}}\}$ (tous les exposants devant les α_i sont positifs), alors que la famille $\{\frac{\alpha_1}{c_1}, ..., \frac{\alpha_k}{c_k}\}$ est linéairement indépendante sur $\mathbb{Q}$. Contradiction d'après le théorème de Lindemann-Weierstrass.

Réciproquement, supposons (E) et montrons par l'absurde le théorème de Lindemann-Weierstrass. Supposons qu'il existe $\alpha_1, ..., \alpha_n \in \overline{\mathbb{Q}}$, linéairement indépendants sur $\mathbb{Q}$ et un polynôme $Q \in \overline{\mathbb{Q}}[X] \setminus \{0\}$ tels que $Q(\mathrm{e}^{\alpha_1}, ..., \mathrm{e}^{\alpha_n}) = 0$. Soit K une extension galoisienne contenant les coefficients de Q (une telle extension existe d'après le lemme 5), et soient $\sigma_1, ..., \sigma_d$ les d plongements de K dans $\mathbb{C}$. Notons alors P le polynôme $\prod_{i=1}^{d}\sigma_i(Q)$ où pour un polynôme $R = \sum_{i=0}^{h} a_iX^i, \sigma_k(R)$ désigne le polynôme $\sum_{i=0}^{h}\sigma_k(a_i)X^i$.

On a $P(\mathrm{e}^{\alpha_1}, ..., \mathrm{e}^{\alpha_n}) = 0$ car Q est un des facteurs du produit définissant P (car $\sigma_1 = id$ est un plongement de K dans $\mathbb{C}$) et $P \neq 0$ car $\overline{\mathbb{Q}}[X_1, ..., X_n]$ est intègre. Par définition, $\forall i \in \{1, ..., d\}, \sigma_i(P) = P$. En effet, K est une extension galoisienne de $\mathbb{Q}$, et donc ses plongements forment un groupe fini pour la composition. Or dans un groupe fini, toute application translation est un automorphisme. Donc

les coefficients de P sont donc stables par tous les plongements de K dans $\mathbb{C}$ et donc d'après le lemme 6, les coefficients de P appartiennent à $\mathbb{Q}$. Quitte à multiplier P par le PPCM des dénominateurs de ses coefficients, on peut supposer $P \in \mathbb{Z}[X_1, ..., X_n] \setminus \{0\}$.

Mais alors $P(\mathrm{e}^{\alpha_1}, ..., \mathrm{e}^{\alpha_n}) = \sum_{\underline{i}} a_{\underline{i}} \mathrm{e}^{i_i\alpha_1 + ... + i_n\alpha_n} = 0$ avec les $a_{\underline{i}}$ dans $\mathbb{Z}$. Or puisque les α_i sont linéairement indépendants sur $\mathbb{Q}$, ils le sont sur $\mathbb{Z}$, et les exposants dans $P(\mathrm{e}^{\alpha_1}, ..., \mathrm{e}^{\alpha_n})$ sont donc algébriques et deux à deux distincts. L'égalité $P(\mathrm{e}^{\alpha_1}, ..., \mathrm{e}^{\alpha_n}) = 0$ est alors absurde d'après (E). □

3) Démonstration du théorème

Supposons par l'absurde qu'il existe $b_1, ..., b_n \in \mathbb{Z}$ non tous nuls et $\alpha_1, ..., \alpha_n \in \overline{\mathbb{Q}}$ deux à deux distincts tels que $b_1\mathrm{e}^{\alpha_1} + ... + b_n\mathrm{e}^{\alpha_n} = 0$. Par la Proposition 21 on aura démontré le théorème de Lindemann-Weierstrass en aboutissant à une contradiction.

On se place dans K, une extension galoisienne de $\mathbb{Q}$ contenant $\mathbb{Q}[\alpha_1, ..., \alpha_n]$ (une telle extension existe d'après le lemme 5) et soit d le degré de K. Posons tout d'abord la fonction $A : t \mapsto b_1\mathrm{e}^{\alpha_1 t} + ... + b_n\mathrm{e}^{\alpha_n t}$ définie sur $\mathbb{C}$. Par hypothèse on a $A(1) = 0$. Montrons que A n'est pas identiquement nulle.

Si $A \equiv 0$ alors $\forall h \in \mathbb{N}, A^{(h)}(0) = b_1\alpha_1^h + ...b_n\alpha_n^h = 0$, *i.e.*

$$\begin{pmatrix} 1 & ... & 1 \\ \alpha_1 & ... & \alpha_n \\ \vdots & & \vdots \\ \alpha_1^{n-1} & ... & \alpha_n^{n-1} \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = 0.$$

Ce système admet une solution non nulle, donc le déterminant de la matrice, qui est de Vandermonde, est nul. Ce déterminant vaut $\prod_{i<j}(\alpha_j - \alpha_i)$, qui ne peut être nul puisque les α_i sont deux à deux distincts. Donc A n'est pas identiquement nulle.

On peut voir A comme une série formelle en t. En effet, $\forall t \in \mathbb{C}$:

$$\begin{aligned} A(t) &= \sum_{i=1}^{n} b_i \mathrm{e}^{\alpha_i t} \\ &= \sum_{i=1}^{n} b_i \left(\sum_{h=0}^{+\infty} \frac{(\alpha_i t)^h}{h!}\right) \\ &= \sum_{h=0}^{+\infty} \left(\sum_{i=1}^{n} \frac{b_i \alpha_i^h}{h!}\right) t^h \end{aligned}$$

Montrons que l'on peut supposer $A \in \mathbb{Q}[[t]]$:

Posons, pour $t \in \mathbb{C}$, $B(t) = \prod_{\sigma}(b_1 \mathrm{e}^{\sigma(\alpha_1)t} + ... + b_n \mathrm{e}^{\sigma(\alpha_n)t}) \in \mathbb{C}[[t]]$, où les σ sont les plongements de K dans $\mathbb{C}$. En distribuant le produit, et en regroupant les termes avec mêmes exposants, on a clairement que B est de la forme $\sum_{i=1}^{n'} b'_i \mathrm{e}^{\alpha'_i t}$ avec les b'_i dans $\mathbb{Z}$, et les α'_i algébriques deux à deux distincts. Puisque $A(1) = 0$, on a $B(1) = 0$ (pour le plongement $\sigma = id$). En montrant que $B \in \mathbb{Q}[[t]]$, on pourra supposer $A \in \mathbb{Q}[[t]]$.

Pour N dans $\mathbb{N}^*$, on pose $B_N(t) = \prod_{\sigma}(\sum_{i=1}^{n} b_i(\sum_{h=0}^{N} \frac{(\sigma(\alpha_i)t)^h}{h!}))$. Pour calculer le coefficient d'ordre N de t dans $B(t)$ il suffit de calculer celui de $B_N(t)$. Or on remarque que pour tout plongement σ de K dans $\mathbb{C}$, $\sigma(B_N) = B_N$. Ainsi les coefficients de B_N (en tant que polynôme en t) sont rationnels d'après le lemme 6. En particulier, les coefficients de B (en tant que série formelle en t) sont rationnels, ce que l'on voulait montrer.

On a désormais $A(t) \in \mathbb{Q}[[t]]$. Soit σ un plongement de K dans $\mathbb{C}$. Alors $\forall t \in \mathbb{C}$,

$$\begin{aligned} b_1 \mathrm{e}^{\sigma(\alpha_1)t} + ... + b_n \mathrm{e}^{\sigma(\alpha_n)t} &= \sum_{h=0}^{+\infty}(\sum_{i=1}^{n} \frac{b_i \sigma(\alpha_i)^h}{h!})t^h \\ &= \sum_{h=0}^{+\infty} \sigma(\sum_{i=1}^{n} \frac{b_i \alpha_i^h}{h!})t^h \ (\text{car } \sigma_{|\mathbb{Q}} = id) \\ &= \sum_{h=0}^{+\infty}(\sum_{i=1}^{n} \frac{b_i \alpha_i^h}{h!})t^h \ (\text{car } A(t) \in \mathbb{Q}[[t]]) \\ &= A(t) \end{aligned}$$

Ainsi, pour tout plongement σ de K dans $\mathbb{C}$, $t \mapsto b_1 \mathrm{e}^{\sigma(\alpha_1)t} + ... + b_n \mathrm{e}^{\sigma(\alpha_n)t}$ n'est pas la fonction nulle, et $b_1 \mathrm{e}^{\sigma(\alpha_1)} + ... + b_n \mathrm{e}^{\sigma(\alpha_n)} = 0$.

Maintenant, pour $f : \mathbb{C} \to \mathbb{C}$ continue, posons

$$I_f : t \mapsto t\mathrm{e}^t \int_0^1 \mathrm{e}^{-tx} f(tx) dx.$$

Soit f une fonction polynomiale de $\mathbb{C}$ dans $\mathbb{C}$. Alors par intégration par parties :

$$\begin{aligned}\forall t \in \mathbb{C}^*, I_f(t) &= te^t \int_0^1 e^{-tx} f(tx)dx \\ &= te^t([-\frac{e^{-tx}}{t} f(tx)]_0^1 + \int_0^1 \frac{e^{-tx}}{t} tf'(tx)dx) \\ &= e^t f(0) - f(t) + te^t \int_0^1 e^{-tx} f'(tx)dx \\ &= e^t f(0) - f(t) + I'_f(t)\end{aligned}$$

En notant d le degré de f, on obtient par une récurrence immédiate :

$$\forall t \in \mathbb{C}, I_f(t) = e^t \sum_{j=0}^{d} f^{(j)}(0) - \sum_{j=0}^{d} f^{(j)}(t),$$

le résultat restant vrai pour $t = 0$. Puisque $\forall j > d, \forall t \in \mathbb{C}, f^{(j)}(t) = 0$, on peut réécrire cette formule sous une forme valable pour tout degré :

$$\forall t \in \mathbb{C}, I_f(t) = e^t \sum_{j\in\mathbb{N}} f^{(j)}(0) - \sum_{j\in\mathbb{N}} f^{(j)}(t).$$

On considère maintenant un entier $N \geq 3$ et le polynôme $f = \frac{((X-\alpha_1)...(X-\alpha_n))^N}{X-\alpha_1}$ de degré $Nn - 1$. Remarquons que α_1 est zéro d'ordre $N - 1$ de f et que pour $2 \leq i \leq n, \alpha_i$ est zéro d'ordre N de f. On pose $J = b_1 I_f(\alpha_1) + ... + b_n I_f(\alpha_n)$.

À partir de maintenant, on va montrer que $J \in \overline{\mathbb{Q}}$, majorer les différentes valeurs absolues de J dans K. En appliquant la formule du produit à J et en utilisant les majorations obtenues, on obtiendra une contradiction. Ceci impliquera $J = 0$, ce nous fera également aboutir à une contradiction.

Puisque $f \in \overline{\mathbb{Q}}[X]$, on a que $\forall j \in \mathbb{N}, f^{(j)} \in \overline{\mathbb{Q}}[X]$. Soit i dans $\{1, ..., n\}$. On sait que $I_f(\alpha_i) = e^{\alpha_i} \sum\limits_{j\in\mathbb{N}} f^{(j)}(0) - \sum\limits_{j\in\mathbb{N}} f^{(j)}(\alpha_i)$.

Donc

$$\begin{aligned}J &= \sum_{i=1}^{n} b_i I_f(\alpha_i) \\ &= \sum_{i=1}^{n} b_i e^{\alpha_i} (\sum_{j\in\mathbb{N}} f^{(j)}(0)) - \sum_{i=1}^{n} b_i \sum_{j\in\mathbb{N}} f^{(j)}(\alpha_i) \\ &= -b_1 f^{(N-1)}(\alpha_1) - \sum_{i=1}^{n} b_i \sum_{j=N}^{Nn} f^{(j)}(\alpha_i),\end{aligned}$$

la dernière égalité étant vraie car $\sum_{i=1}^{n} b_i e^{\alpha_i} = 0$ par hypothèse, α_i est zéro de f d'ordre N pour $i \in \{2, ..., n\}$ et α_1 est zéro de f d'ordre $N-1$.

Puisque $\forall j \in \mathbb{N}, f^{(j)} \in \overline{\mathbb{Q}}[X]$, et puisque la valeur prise en un nombre algébrique par un polynôme à coefficients algébrique est encore un nombre algébrique ($\overline{\mathbb{Q}}$ est un corps, en particulier un anneau), on a bien obtenu que $J \in \overline{\mathbb{Q}}$.

Passons maintenant aux majorations des valeurs absolues de J dans K. Soit v une valeur absolue ultramétrique de K. Alors

$$|J|_v = |\sum_{k=1}^{n} \sum_{j \in \mathbb{N}} f^{(j)}(\alpha_k)|_v \leq \max_{j \in \mathbb{N}, 1 \leq k \leq n} |f^{(j)}(\alpha_k)|_v = \max_{N-1 \leq j \leq Nn, 1 \leq k \leq n} |f^{(j)}(\alpha_k)|_v.$$

Deux cas se présentent :

— Si le max est atteint pour $k \neq 1$: $f(X) = (X - \alpha_k)^N \times Q_k(X)$ avec $Q_k(X) \in \overline{\mathbb{Q}}[X] \setminus \{0\}$.
Par la formule de Leibniz, on a

$$\begin{aligned} \forall j \geq N-1, \frac{f^{(j)}(X)}{j!} &= \sum_{h=0}^{j} \frac{((X-\alpha_k)^N)^{(h)}}{h!} \frac{Q_k^{(j-h)}(X)}{(j-h)!} \\ &= \frac{((X-\alpha_k)^N)^{(N)}}{N!} \frac{Q_k^{(j-N)}(X)}{(j-N)!} + (X-\alpha_k)R(X) \end{aligned}$$

avec $R(X) \in \overline{\mathbb{Q}}[X]$.

En appliquant cette relation en α_k on obtient

$$\begin{aligned} \forall j \geq N-1, \frac{f^{(j)}(\alpha_k)}{j!} &= \frac{Q_k^{(j-N)}(\alpha_k)}{(j-N)!} \\ &= \sum_i q_i(\alpha_1, ..., \alpha_n) \alpha_k^{N+i-j} \binom{i}{j-N} \end{aligned}$$

avec $\forall i, q_i(\alpha_1, ..., \alpha_n) \in \mathbb{Z}[\alpha_1, ..., \alpha_{k-1}, \alpha_{k+1}, ..., \alpha_n]$ de degré inférieur à $N(n-1)-1$.
D'où $|q_i(\alpha_1, ..., \alpha_n)|_v \leq \max(1, |\alpha_1|_v, ..., |\alpha_{k-1}|_v, |\alpha_{k+1}|_v, ..., |\alpha_n|_v)^{N(n-1)-1}$ et donc

$$\begin{aligned} \forall j \geq N-1, |f^{(j)}(\alpha_k)|_v &\leq |j!|_v \max(1, |\alpha_1|_v, ..., |\alpha_n|_v)^{N(n-1)-1} \\ &\leq |(N-1)!|_v \max(1, |\alpha_1|_v, ..., |\alpha_n|_v)^{Nn}. \end{aligned}$$

En effet, v étant ultramétrique, elle est associé à un nombre premier p de sorte que $|.|_v = |.|_p$ sur $\mathbb{Z}$. Pour $j \geq N-1, (N-1)! \mid j!$ et donc $|j!|_p \leq |(N-1)!|_p$.
Enfin $|J|_v \leq |(N-1)!|_v \max(1, |\alpha_1|_v, ..., |\alpha_n|_v)^{Nn}$.

— Si le max est atteint pour $k = 1$: le raisonnement précédent peut être répété, seul les exposants en $N(n-1)-1$ changent, mais on peut toujours les majorer par Nn, et donc on a encore $|J|_v \leq |(N-1)!|_v \max(1, |\alpha_1|_v, ..., |\alpha_n|_v)^{Nn}$.

Maintenant, remarquons que les plongements σ de K dans $\mathbb{C}$ respectent l'opérateur dérivation, dans le sens où $\forall P = \sum_{i=0}^{h} a_i X^i \in \overline{\mathbb{Q}}, \forall j \in \mathbb{N}, \sigma(P^{(j)}) = (\sigma(P))^{(j)}$ où $\sigma(P)$ désigne $\sum_{i=0}^{h} \sigma(a_i)X^i$. En effet, il suffit de le vérifier sur les monômes puisque σ est un morphisme de corps : soient j dans $\mathbb{N}^*$ et a dans $\overline{\mathbb{Q}}, \sigma((aX^j)') = \sigma(ajX^{j-1}) = \sigma(a)jX^{n-1} = (\sigma(aX^j))'$, et on obtient le résultat par récurrence.

Soit donc σ un plongement de K dans $\mathbb{C}$. Alors par intégration par parties, et puisque σ respecte la dérivation, on a comme précédemment

$$\begin{aligned}&\sum_{i=1}^{n} b_i \int_0^1 \sigma(\alpha_i) \mathrm{e}^{\sigma(\alpha_i)(1-x)} \sigma(f)(\sigma(\alpha_i)x)dx \\ &= \sum_{i=1}^{n} b_i \mathrm{e}^{\sigma(\alpha_i)} (\sum_{j\in\mathbb{N}} \sigma(f)^{(j)}(0)) - \sum_{i=1}^{n} b_i \sum_{j\in\mathbb{N}} \sigma(f)^{(j)}(\sigma(\alpha_i)).\end{aligned}$$

Or $\sum_{i=1}^{n} b_i \mathrm{e}^{\sigma(\alpha_i)} = 0$, donc

$$\sum_{i=1}^{n} b_i \int_0^1 \sigma(\alpha_i) \mathrm{e}^{\sigma(\alpha_i)(1-x)} \sigma(f)(\sigma(\alpha_i)x)dx = -\sum_{i=1}^{n} b_i \sum_{j\in\mathbb{N}} \sigma(f)^{(j)}(\sigma(\alpha_i)) = \sigma(J).$$

Majorons maintenant $|J|$. Puisque $J = \sum_{i=1}^{n} b_i I_f(\alpha_i)$, on a

$$|J| \leq n \max_{1\leq i\leq n}(|b_i|) \max_{1\leq i\leq n}(|I_f(\alpha_i)|).$$

Soit α_k tel que $|I_f(\alpha_k)| = \max_{1\leq i\leq n}(|I_f(\alpha_i)|)$. Puisque

$$I_f(\alpha_k) = \alpha_k \mathrm{e}^{\alpha_k} \int_0^1 \mathrm{e}^{-\alpha_k x} f(\alpha_k x)dx,$$

on a

$$|I_f(\alpha_k)| \leq |\alpha_k \mathrm{e}^{\alpha_k}| \max_{|x|\leq|\alpha_k|} |\mathrm{e}^{-x}| \max_{|x|\leq|\alpha_k|} |f(x)| = C_1 \max_{|x|\leq|\alpha_k|} |f(x)|,$$

avec C_1 une constante positive ne dépendant que des α_i.

Soit x dans $[0, \alpha_k]$. Alors

$$\begin{aligned}|f(x)| &= |x-\alpha_1|^{N-1}|x-\alpha_2|^N ... \ \ |x-\alpha_n|^N \\ &\leq (|\alpha_k|+|\alpha_1|)^{N-1}(|\alpha_k|+|\alpha_2|)^N ... \ \ (|\alpha_k|+|\alpha_n|)^N \text{ (car } |x| \leq |\alpha_k|) \\ &\leq 2^{Nn-1}\max(1,|\alpha_k|)^{Nn-1}\max(1,|\alpha_1|)^{N-1}\max(1,|\alpha_2|)^N ... \max(1,|\alpha_n|)^N \\ &\leq C_2^N \max(1,|\alpha_1|,...,|\alpha_n|)^{Nn}\end{aligned}$$

avec C_2 une constante positive ne dépendant que des α_i.

Ainsi

$$\begin{aligned}|J| &\leq n \max_{1\leq i\leq n}(|b_i|) C_1 C_2^N \max(1,|\alpha_1|,...,|\alpha_n|)^{Nn} \\ &\leq C_3^N \max(1,|\alpha_1|,...,|\alpha_n|)^{Nn},\end{aligned}$$

avec C_3 une constante positive ne dépendant que des α_i et des b_i (et donc pas de N).

Soit σ un plongement de K dans $\mathbb{C}$. Puisque

$$\sigma(J) = \sum_{i=1}^{n} b_i \int_0^1 \sigma(\alpha_i) \mathrm{e}^{\sigma(\alpha_i)(1-x)} \sigma(f)(\sigma(\alpha_i)x)dx,$$

on a de la même manière

$$|\sigma(J)| \leq C_\sigma \max(1,|\sigma(\alpha_1)|,...,|\sigma(\alpha_n|))^{Nn}$$

avec C_σ une constante positive ne dépendant que des α_i et des b_i (et donc pas de N).

Enfin, en posant $C = \max_\sigma(C_\sigma)$, on a que pour tout plongement σ de K dans $\mathbb{C}$:

$$|\sigma(J)| \leq C^N \max(1,|\sigma(\alpha_1)|,...,|\sigma(\alpha_n)|)^{Nn}.$$

Supposons maintenant $J \neq 0$. On peut alors lui appliquer la formule du produit :

$$\prod_{v\in M_K} |J|_v^{d_v} = 1.$$

Or

$$\begin{aligned}\prod_{v\in M_K}|J|_v^{d_v} &= \prod_{v\in M_K^\infty}|J|_v^{d_v}\times\prod_{v\in M_K,v|p}|J|_v^{d_v}\\ &\leq \prod_\sigma C^{Nd_v}\max(1,|\sigma(\alpha_1)|,...,|\sigma(\alpha_n|))^{Nnd_v}\\ &\quad\times\prod_{v\in M_K,v|p}|(N-1)!|_v^{d_v}\max(1,|\alpha_1|_v,...,|\alpha_n|_v)^{Nnd_v}\\ &\leq C'^N\times\prod_{v\in M_K,v|p}|(N-1)!|_v^{d_v}\end{aligned}$$

avec C' une constante positive ne dépendant pas de N.

De plus $\prod_{v\in M_K,v|p}|(N-1)!|_v^{d_v}=(N-1)!^{-d}$ par la formule du produit, donc

$$1=\prod_{v\in M_K}|J|_v^{d_v}\leq\frac{C'^N}{(N-1)!^d},$$

ce qui est absurde quand N est assez grand car $\frac{C'^N}{(N-1)!^d}\to 0$ quand $N\to+\infty$. Donc $J=0$ pour N assez grand.

Enfin, $J=-b_1f^{(N-1)}(\alpha_1)-\sum_{i=1}^n b_i\sum_{j=N}^{Nn}f^{(j)}(\alpha_i)$ donc $b_1f^{(N-1)}(\alpha_1)=-\sum_{i=1}^n b_i\sum_{j=N}^{Nn}f^{(j)}(\alpha_i)$.

Or $f^{(N-1)}(\alpha_1)=(N-1)!\prod_{i=2}^n(\alpha_1-\alpha_i)^N$ et par les mêmes majorations que précédemment, on a pour toute valeur absolue ultramétrique v sur K, $|\sum_{i=1}^n b_i\sum_{j=N}^{Nn}f^{(j)}(\alpha_i)|_v\leq |N!|_v\max(1,|\alpha_1|_v,...,|\alpha_n|_v)^{Nn}$.

Donc pour $N=p$ un nombre premier assez grand pour que $|b_1|_p=1$, pour v un valeur absolue ultramétrique sur K telle que $v\mid p$, et en simplifiant par $|(p-1)!|_p$ (qui vaut 1 car $p\nmid(p-1)!$ par le théorème de Gauss), on a

$$\prod_{i=2}^n|\alpha_1-\alpha_i|_v^p\leq|p|_p\max(1,|\alpha_1|_v,...,|\alpha_n|_v)^{pn}=\frac{\max(1,|\alpha_1|_v,...,|\alpha_n|_v)^{pn}}{p}.$$

Or on peut prendre p assez grand pour que tous les nombres

$$|\alpha_1-\alpha_2|_v,...,|\alpha_1-\alpha_n|_v,|\alpha_1|_v,...,|\alpha_n|_v$$

soient égaux à 1 (seul un nombre fini de termes dans la formule du produit sont différents de 1).

Alors on a obtenu $1\leq\frac{1}{p}$ pour p assez grand, ce qui est bien sûr absurde, et on a donc démontré le théorème de Lindemann-Weierstrass. □

Conclusion

L'existence de nombres transcendants remet en question la manière dont on construit intuitivement les nombres réels. En considérant $\mathbb{N}$ comme acquis, on enseigne aux élèves les nombres négatifs comme vérifiant des équations de la forme $X + a = 0$ avec a un entier naturel. Puis on leur enseigne les nombres rationnels sous forme de fractions $\frac{a}{b}$, vérifiant des équations de la forme $bX + (-a) = 0$. Enfin ceux-ci apprennent l'existence de nombres tels que $\sqrt{2}$, vérifiant $X^2 = 2$ ou $\sqrt{2+\sqrt{2}}$ vérifiant $(X^2-2)^2 = 2$ et ainsi de suite... Mais puisque $\mathbb{Q} \subset \overline{\mathbb{Q}}$ et $\mathbb{R} \not\subset \overline{\mathbb{Q}}$, comment peut-on leur définir des nombres transcendants tels que π ou e ? L'apparition des nombres transcendants se faisant lors du passage de $\mathbb{Q}$ à $\mathbb{R}$, on se rend compte que leur existence est en quelque sorte le « prix à payer »pour l'indénombrabilité de l'ensemble des nombres réels dont on souhaite disposer.

La théorie de la transcendance est un domaine de recherche encore actif de nos jours. Des théorèmes plus récents et plus généraux que les théorèmes que nous avons vu dans ce mémoire ont été établis, donnant la transcendance de plus grandes familles de nombres (Voir Annexes). Cependant, les démonstrations de transcendance sont en général techniques et compliquées comme nous avons pu le voir, et de nombreuses questions restent ouvertes de nos jours. On ne sait pas aujourd'hui si les nombres suivants sont transcendants (même s'il est conjecturé qu'ils le sont tous) : $\pi + \mathrm{e}, \pi\mathrm{e}, \mathrm{e}^{\mathrm{e}}, \pi^{\pi}, \zeta(3) = \sum_{n=1}^{+\infty} \frac{1}{n^3}$ et plus généralement $\zeta(2n+1)$ pour $n \in \mathbb{N}^*$, la constante d'Euler $\gamma = \lim_{n\to+\infty} (\sum_{k=1}^{n} \frac{1}{k} - \log n)$, la constante de Catalan $K = \sum_{n=0}^{+\infty} \frac{(-1)^n}{(2n+1)^2}$, *etc.*

La recherche en théorie de la transcendance a encore de nombreux défis devant elle, notamment la conjecture de Schanuel, sur laquelle nous reviendrons en annexes, et qui est, d'après les mots de Michel Waldschmidt, grand expert en théorie de la transcendance, encore inaccessible de nos jours.

Annexes

Nous allons voir dans ces annexes comment Liouville a découvert le premier nombre transcendant connu, et quelques résultats de transcendance plus puissants et plus récents que les théorèmes d'Hermite-Lindemann et de Lindemann-Weierstrass, que nous ne démontrerons pas et quelques conjectures encore non démontrées ou infirmées à ce jour.

Le théorème de Liouville

Le premier nombre transcendant découvert le fut par Liouville. Ce nombre est $\alpha = \sum_{k=1}^{+\infty} 10^{-k!}$. Comment Liouville a-t-il montré que ce nombre était transcendant ? On voit que des théorèmes tels que ceux d'Hermite-Lindemann et de Lindemann-Weierstrass ne permettent pas de conclure à la transcendance de ce nombre. En fait Liouville a découvert une propriété de mauvaise approximation rationnelle des nombres algébriques irrationnels. Ainsi, un nombre « trop bien approché » par des nombres rationnels sera nécessairement transcendant. C'est le cas de α défini ci-dessus.

Théorème 17 (Liouville) *Soit α un nombre algébrique de degré $d > 1$. Alors il existe une constante $C > 0$, telle que pour tout rationnel $\frac{p}{q}$ on a*

$$|\alpha - \frac{p}{q}| \geq \frac{C}{q^d}.$$

Démonstration : Soit donc un nombre rationnel $\frac{p}{q}$. Deux cas se présentent :

- Si $|\alpha - \frac{p}{q}| \geq 1$, on a immédiatement $|\alpha - \frac{p}{q}| \geq \frac{1}{q^d}$.
- Si $|\alpha - \frac{p}{q}| < 1$, soit P_α le polynôme minimal de α. Alors $q^d P_\alpha(\frac{p}{q}) \in \mathbb{Z}^*$ car $d > 1$ et donc P_α n'a pas de racine rationnelle. Ainsi

$$|q^d(P_\alpha(\frac{p}{q}) - P_\alpha(\alpha))| = |q^d P_\alpha(\frac{p}{q})| \geq 1.$$

Posons $M = \max_{x\in[\alpha-1,\alpha+1]} |P'_\alpha(x)| > 0$. Alors d'après l'inégalité des accroissements finis, on a

$$|P_\alpha(\frac{p}{q}) - P_\alpha(\alpha)| \leq M|\alpha - \frac{p}{q}|.$$

D'où

$$|\alpha - \frac{p}{q}| \geq \frac{1}{Mq^d}.$$

En posant $C = \min(1, \frac{1}{M})$, on obtient le résultat souhaité. □

Montrons maintenant, grâce au théorème de Liouville, que $\alpha = \sum_{k=1}^{+\infty} 10^{-k!}$ est transcendant.

Supposons α algébrique et soit d son degré. On a que $d > 1$. En effet, α n'est pas rationnel car son développement décimal n'est pas périodique. D'après le théorème de Liouville, il existe $C > 0$ tel que pour tout rationnel $\frac{p}{q}, |\alpha - \frac{p}{q}| \geq \frac{C}{q^d}$. Soit la suite de rationnels $(\frac{p_n}{q_n})_n$ définie par $\forall n \in \mathbb{N}^*, q_n = 10^{n!}$ et $p_n = q_n \sum_{k=1}^{n} 10^{-k!}$.

Alors $\forall n \in \mathbb{N}^*$,

$$|\alpha - \frac{p_n}{q_n}| = \sum_{k=n+1}^{+\infty} 10^{-k!} \leq \sum_{k=n+1} \frac{9}{10^{k!}} \leq \sum_{k=(n+1)!} \frac{9}{10^k} = \frac{1}{10^{(n+1)!-1}} \leq \frac{1}{q_n^n}.$$

Ainsi on a

$$\forall n \in \mathbb{N}^*, 0 < \frac{C}{q_n^d} \leq \frac{1}{q_n^n},$$

ce qui est absurde quand $n \to +\infty$. Donc α est transcendant.

De manière générale, si on considère un entier $b > 1$ et une suite $(a_k)_k$ non nulle d'entiers compris entre 0 et $b-1$, alors le nombre $\sum_{k=1}^{+\infty} \frac{a_k}{b^{k!}}$ est transcendant. De tels nombres sont appelés *nombre de Liouville*. L'ensemble des nombres de Liouville est indénombrable car on peut lui injecter l'ensemble des suites d'entiers naturels majorées, on obtient ainsi une autre démonstration de la *grandeur* de l'ensemble des nombres transcendants.

Ce théorème est en fait généralisé par le théorème de Roth, également appelé théorème de Thue-Siegel-Roth, qui permet d'améliorer l'exposant d :

Théorème 18 (Roth) *Soit α un nombre algébrique irrationnel. Pour tout $\epsilon > 0$, il existe une constante $C(\epsilon) > 0$, telle que pour tout rationnel $\frac{p}{q}$ on a*

$$|\alpha - \frac{p}{q}| \geq \frac{C(\epsilon)}{q^{2+\epsilon}}.$$

Ce théorème valut à Klaus Roth la médaille Fields en 1958.

Le théorème de Gelfond-Schneider

La démonstration de ce théorème constituait l'un des vingt-trois problèmes de Hilbert, posés en 1900 pour guider la recherche mathématique durant le XX$^{\text{ème}}$ siècle. Aleksandr Gelfond et Theodor Schneider le démontrèrent indépendamment et simultanément en 1934.

Théorème 19 (Gelfond-Schneider) *Soit α un nombre algébrique différent de 0 et de 1, et soit β un nombre algébrique irrationnel. Alors α^β est transcendant.*

On obtient immédiatement la transcendance de nombres tels que $2^{\sqrt{2}}$ ou $\sqrt{2}^{\sqrt{2}}$. On obtient moins immédiatement la transcendance de nombres tels que $\mathrm{e}^{-\frac{\pi}{2}}$ ou e^{π}. En effet, $\mathrm{e}^{-\frac{\pi}{2}} = (\mathrm{e}^{i\frac{\pi}{2}})^i = i^i$ et $\mathrm{e}^{\pi} = (\mathrm{e}^{-i\pi})^i = (-1)^i$ et i est irrationnel algébrique.

Par contraposée, on a également la transcendance de nombres tels que $\beta = \frac{\log p}{\log q}$ avec p et q des nombres premiers distincts. En effet, ce nombre est irrationnel car sinon il existerait des entiers naturels non nuls a et b tels que $a \log p = b \log q$, *i.e.* tels que $p^a = q^b$ ce qui contredirait l'unicité de la décomposition d'un nombre en produit de facteurs premiers. Ensuite, en remarquant que $q^\beta = q^{\frac{\log p}{\log q}} = p$ est algébrique, on obtient que β est nécessairement transcendant.

Le théorème des six exponentielles

Voici un résultat de transcendance assez surprenant, démontré par Serge Lang dans les années 60.

Théorème 20 (Six Exponentielles) *Soient a_1, a_2 et a_3 des nombres complexes linéairement indépendants sur $\mathbb{Q}$, et b_1 et b_2 des nombres complexes également linéairement indépendants sur $\mathbb{Q}$. Alors au moins l'un des six nombres*

$$\mathrm{e}^{a_1 b_1}, \mathrm{e}^{a_1 b_2}, \mathrm{e}^{a_2 b_1}, \mathrm{e}^{a_2 b_2}, \mathrm{e}^{a_3 b_1} \text{ et } \mathrm{e}^{a_3 b_2}$$

est transcendant.

Une conjecture encore non démontrée stipule que l'on peut réduire ce résultat à seulement quatre exponentielles :

Conjecture 1 (Quatre Exponentielles) *Soient a_1 et a_2 des nombres complexes linéairement indépendants sur $\mathbb{Q}$, et b_1 et b_2 des nombres complexes également linéairement indépendants sur $\mathbb{Q}$. Alors au moins l'un des quatre nombres*

$$\mathrm{e}^{a_1 b_1}, \mathrm{e}^{a_1 b_2}, \mathrm{e}^{a_2 b_1} \text{ et } \mathrm{e}^{a_2 b_2}$$

est transcendant.

Le théorème de Baker

Théorème 21 (Baker) *Soit $a_1, ..., a_n$ des nombres algébriques non nuls tels que $\log a_1, ..., \log a_n$ sont linéairement indépendants sur $\mathbb{Q}$. Alors $1, \log a_1, ..., \log a_n$ sont linéairement indépendants sur $\overline{\mathbb{Q}}$.*

Ce théorème fut démontré par Alan Baker en 1967, et lui valut la médaille Fields en 1970.

Le théorème de Baker implique les théorèmes d'Hermite-Lindemann et de Gelfond-Schneider :

En effet, soit α un nombre algébrique non nul. Supposons e^α algébrique. Puisque $\log(e^\alpha) = \alpha \neq 0$, $\{\log e^\alpha\}$ est une famille linéairement indépendante sur $\mathbb{Q}$, et donc, d'après le théorème de Baker, 1 et α sont linéairement indépendants sur $\overline{\mathbb{Q}}$, ce qui est absurde puisque $\alpha - \alpha \times 1 = 0$.

De même, soient α un nombre algébrique différent de 0 et de 1 et β un nombre algébrique irrationnel. Supposons α^β algébrique. Puisque $\log(\alpha^\beta) = \beta \log \alpha$ et $\log \alpha$ sont linéairement indépendants sur $\mathbb{Q}$ (β est irrationnel), on a que $1, \log \alpha$ et $\beta \log \alpha$ sont linéairement indépendants sur $\overline{\mathbb{Q}}$, ce qui est absurde puisque $\beta \times \log \alpha - \beta \log \alpha = 0$.

Grâce à ce théorème, on obtient la transcendance de nombres tels que $\sum_{i=1}^{n} a_i \log p_i$ avec $n \in \mathbb{N}^*, \forall i \in \{1, ..., n\}, a_i \in \overline{\mathbb{Q}} \setminus \{0\}$ et les p_i des nombres premiers deux à deux distincts. Supposons un tel nombre algébrique, et notons-le β. Les p_i sont premiers et donc algébriques non nuls, et leurs logarithmes sont linéairement indépendants sur $\mathbb{Q}$, comme précédemment, par l'unicité de la décomposition des entiers en produit de facteurs premiers. Mais alors $\beta - \sum_{i=1}^{n} a_i \log p_i = 0$ constitue une relation de dépendance linéaire sur $\overline{\mathbb{Q}}$ de $1, \log p_1, ... \log p_n$, ce qui est absurde. Donc β est transcendant.

Il existe une conjecture concernant un résultat plus puissant que le théorème de Baker :

Conjecture 2 (Baker) *Soit $a_1, ..., a_n$ des nombres algébriques non nuls tels que $\log a_1, ..., \log a_n$ sont linéairement indépendants sur $\mathbb{Q}$. Alors $\log a_1, ..., \log a_n$ sont algébriquement indépendants.*

La conjecture de Schanuel

Nous allons clore ces annexes par une conjecture énoncée par Stephen Schanuel dans les années 60. Cette conjecture implique la plupart des résultats de transcendance connus concernant la fonction exponentielle.

Conjecture 3 (Schanuel) *Soient $z_1, ..., z_n$ des nombres complexes linéairement indépendants sur $\mathbb{Q}$. Alors l'extension $\mathbb{Q}(z_1, ..., z_n, \mathrm{e}^{z_1}, ..., \mathrm{e}^{z_n})$ a un degré de transcendance sur $\mathbb{Q}$ d'au moins n, i.e. il existe une famille d'au moins n nombres parmi $\{z_1, ..., z_n, \mathrm{e}^{z_1}, ..., \mathrm{e}^{z_n}\}$ qui sont algébriquement indépendants.*

Dans le cas où les z_i sont algébriques, on obtient le théorème de Lindemann-Weierstrass. Dans le cas où les z_i sont des logarithmes de nombres algébriques, on obtient la conjecture de Baker.

Si la conjecture était prouvée, on pourrait obtenir l'indépendance algébrique de e et π (encore non démontrée à ce jour) en considérant $z_1 = 1$ et $z_2 = i\pi$. En effet, 1 et $i\pi$ sont linéairement indépendants sur $\mathbb{Q}$ (car π est transcendant) et donc d'après la conjecture de Schanuel, au moins deux des nombres parmi $\{1, i\pi, \mathrm{e}^1 = \mathrm{e}, \mathrm{e}^{i\pi} = -1\}$ forment une famille algébriquement indépendante. Or une famille de nombres contenant un nombre algébrique ne peut être algébriquement indépendante, car un polynôme à coefficients entiers (et donc algébriques) en une variable annule ce nombre (tout comme une famille de nombres contenant 0 ne peut être linéairement indépendante sur $\mathbb{Q}$). Ainsi e et $i\pi$ sont algébriquement indépendants, ce qui implique sur e et π le sont, puisque i est algébrique.

Enfin, voici quelques exemples de nombres dont on peut montrer la transcendance si la conjecture de Schanuel est vraie :

L'indépendance algébrique de e et π implique la transcendance de $\mathrm{e} + \pi, \mathrm{e}\pi, \frac{\mathrm{e}}{\pi}$ et $\frac{\pi}{\mathrm{e}}$.

En considérant $z_1 = 1$ et $z_2 = \mathrm{e}$, qui sont linéairement indépendants sur $\mathbb{Q}$, on a qu'au moins deux des nombres $1, \mathrm{e}$ et e^{e} forment une famille algébriquement indépendante. Puisque 1 est algébrique, la seule possibilité est que e et e^{e} soient algébriquement indépendants, ce qui implique en particulier que e^{e} est transcendant.

Enfin, soit α un nombre algébrique non nul. Alors α et e^{α} sont linéairement indépendants sur $\mathbb{Q}$ (e^{α} est transcendant d'après le théorème de Hermite-Lindemann). Donc au moins deux des nombres $\alpha, \mathrm{e}^{\alpha}$ et $\mathrm{e}^{\mathrm{e}^{\alpha}}$ forment un famille algébriquement indépendante. Puisque α est algébrique, il s'agit des deux derniers, et en particulier, $\mathrm{e}^{\mathrm{e}^{\alpha}}$ est transcendant. De même, si $\alpha \neq 1$, et en considérant $z_1 = \log \alpha$ et $z_2 = \log \log \alpha$, on obtient que $\log \log \alpha$ est transcendant.

Bibliographie

[1] M. Waldschmidt, « *Diophantine approximation on linear algebraic group* », Springer, 2000, 633 p.

[2] E. Burger, R. Tubbs, « *Making Transcendance Transparent* », Springer, 2004, 263 p.

[3] A. Baker, « *Transcendental Number Theory* », Cambridge Mathematical Library, 1990, 165 p.

[4] M. Waldschmidt, « *Nombres Transcendants* », Springer, 1974, 284 p.

[5] P. Samuel, « *Théorie Algébrique des Nombres* », Hermann, 1967, 131 p.

[6] N. Koblitz, « *p-adic Numbers, p-adic Analysis, and Zeta-Functions* », Springer, 1996, 153 p.

[7] D. Duverney, « *Théorie des Nombres* », Dunod, 2007, 272 p.