Nombres transcendants

Liouville 1844

Existence de nombres transcendants

$$\sum_{n \geq 0} b^{-n!} \qquad b \text{ entier } \geq 2$$

Inégalité de Liouville

$m \in \mathbb{Z}$, $n \neq 0 \Rightarrow |n| \geq 1$

Si $\alpha \in \mathbb{R}$ algébrique de degré d, il existe $c(\alpha) > 0$ telle que $\forall\, p/q \in \mathbb{Q}$, $p/q \neq \alpha$ on ait

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

Corollaire. $\alpha \in \mathbb{R}$. Supp. $\forall\, \kappa > 0\ \exists\, \frac{p}{q} \in \mathbb{Q}$,

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^\kappa}, \quad q \geq 2$$

alors α est transcendant.

1873. Hermite e est transcendant.

1882 Lindemann. π est transcendant.

La quadrature du cercle est impossible.

π n'est pas constructible.

Théorème de Hermite-Lindemann.

(1) β alg. $\neq 0$, $\beta \in \mathbb{C}$ $\Rightarrow e^\beta$ est transcendant

(2) α alg. $\neq 0$, $\alpha \in \mathbb{C}$. $\log \alpha$ un logarithme de α. Supp. $\log \alpha \neq 0$. Alors $\log \alpha$ est transcendant.

Rappel : $x_1, \dots, x_n \in \mathbb{C}$ lin. ind. sur $\mathbb{Q}$

si $(a_1, \dots, a_n) \in \mathbb{Q}^n$, $a_1 x_1 + \dots + a_n x_n = 0$ $\Rightarrow a_1 = \dots = a_n = 0$

Déf. $x_1, \dots, x_n \in \mathbb{C}$ algébriquement dépendants (liés) sur $\mathbb{Q}$ s'il existe $P \in \mathbb{Q}[X_1, \dots, X_n]$, $P \neq 0$, $P(x_1, \dots, x_n) = 0$

Théorème de Lindemann-Weierstrass.

(1) $\beta_1, \dots, \beta_m$ algébriques 2 à 2 distincts. Alors $e^{\beta_1}, \dots, e^{\beta_m}$ sont linéairement indépendants sur $\mathbb{Q}$.

(2) $\gamma_1, \dots, \gamma_n$ algébriques linéairement indépendants sur $\mathbb{Q}$. Alors $e^{\gamma_1}, \dots, e^{\gamma_n}$ sont alg. ind. sur $\mathbb{Q}$.

LW $\Rightarrow$ HL

① β alg $\neq 0$.

$0, \beta, 2\beta, \dots, (m-1)\beta$

2 à 2 distincts

LW $\Rightarrow 1, e^\beta, (e^\beta)^2, \dots, (e^\beta)^{m-1}$ sont lin. ind. $/\mathbb{Q}$.

$\Leftrightarrow e^\beta$ transcendant.

② $m = 1$ $\gamma_1 = \beta$ $P \in \mathbb{Q}[X_1]$ $P \neq 0$

$P(\gamma_1) \neq 0$

$e^{\gamma_1} = e^\beta$ est transcendant.

1900 Hilbert 23 problèmes ouverts

7^e Euler 1737. $2^{\sqrt{2}}$

$2^{\sqrt{2}}$ est transcendant ?

e^{π} est transcendant ?

<u>Pb</u> α alg $\neq 0$ $\log\alpha \neq 0$ $\alpha^{\beta} = e^{\beta\log\alpha}$

β alg $\notin \mathbb{Q}$ est transcendant ?

$\alpha = -1$ $\log\alpha = i\pi$ $\alpha^{\beta} = e^{\beta i\pi} = e^{\pi}$

$\beta = -i$

<u>Enoncé équivalent</u> : α_1, α_2 algébriques $\neq 0$

$\log\alpha_1$, $\log\alpha_2$ linéairement indépendants sur $\mathbb{Q}$.

$\Rightarrow \log\alpha_1 / \log\alpha_2$ est transcendant.

1914 Polya.

Fonctions entières à valeurs entières

$f : \mathbb{C} \longrightarrow \mathbb{C}$ $f(0), f(1), \ldots \in \mathbb{Z}$

<u>Exples</u>. 1) $\mathbb{Z}[z]$

2) $\frac{z(z+1)}{2}$ $\frac{z(z+1)\cdots(z+n-1)}{n!}$

$n \geq 1$

3) $2^z = \exp(z\log 2)$

2^z est la fonction entière non polynomiale "la plus petite" $R \longmapsto \sup_{|z|\leq R} |f(z)|$

Fonction transcendante.

D ouvert connexe $\subset \mathbb{C}$

$\mathcal{M}(D)$ le corps des fonctions méromorphes sur D.

$\mathbb{C}(z) \subset \mathcal{M}(D)$ extension de corps.

$\qquad\qquad\quad \ni f$

f est algébrique sur $\mathbb{C}(z)$ s'il existe

$P \in \mathbb{C}(z)[T]$, $P \neq 0$, $P(f) = 0$.

$\Longleftrightarrow$ il existe $A \in \mathbb{C}[X,Y]$, $A \neq 0$,

$A(z, f(z)) = 0$ $\forall z \in D$.

<u>Exemple</u>. $\sqrt{1-z}$ $|z| < 1$. $A(X,Y) = Y^2 + X - 1$

Une fonction transcendante (sur $\mathbb{C}(z)$) est une fonction qui n'est pas algébrique (sur $\mathbb{C}(z)$)

Cas $D = \mathbb{C}$ $\mathcal{M}(\mathbb{C})$ = quotients de fonctions entières.

<u>Exercice</u>.

Si $f \in \mathcal{M}(\mathbb{C})$ est algébrique sur $\mathbb{C}(z)$, alors $f \in \mathbb{C}(z)$.

<u>Indication</u>. commencer par montrer que si f est entière algébrique sur $\mathbb{C}(z)$, alors f est un polynôme.

<u>Exemple</u> e^z est une fonction transcendante.

1929 Gel'fond fonctions entières f

$f(\mathbb{Z}[i]) \subset \mathbb{Z}[i]$.

Si f n'est pas un polynôme,

f croît au moins comme e^{cz^2}

Supposer $e^{\pi} \in \mathbb{Q}$.

$e^{\pi z}$ $\quad z = a+bi \quad (e^{\pi})^a \cdot e^{i\pi b}$

$\cap$

$\mathbb{Q}$.

Gel'fond :

transcendance de e^{π}

Kusmin $2^{\sqrt{2}}$ transcendant.

1934. Gel'fond et Schneider

(GS) transcendance de α^{β}, $\log\alpha_1/\log\alpha_2$.

1968 Baker.

(B) $\alpha_1, \dots, \alpha_n$ nombres algébriques $\neq 0$

Supp $\log\alpha_1, \dots, \log\alpha_n$ linéairement indépendants sur $\mathbb{Q}$. Soient $\beta_0, \beta_1, \dots, \beta_n$ algébriques.

Supp. $\beta_0 + \beta_1 \log\alpha_1 + \dots + \beta_n \log\alpha_n = 0$

Alors $\beta_0 = \beta_1 = \dots = \beta_n = 0$.

(B) $\Longrightarrow$ (GS)

Exercice. (B) $\Longrightarrow$

$\alpha_1, \dots, \alpha_m$ algébriques $\neq 0$ $\quad \log\alpha_i \neq 0$

$\beta_1, \dots, \beta_m$ algébriques $\neq 0$

supp. $\alpha_1^{\beta_1} \cdots \alpha_m^{\beta_m}$ algébrique.

Alors $\log\alpha_1, \dots, \log\alpha_m$ sont linéairement dépendants sur $\mathbb{Q}$

<u>ou</u> $1, \beta_1, \dots, \beta_m$ sont linéairement dépendants sur $\mathbb{Q}$.

Conjecture de Schanuel.

$x_1, \dots, x_n \in \mathbb{C}$ linéairement indépendants sur $\mathbb{Q}$. Alors parmi les nombres

$x_1, \dots, x_n, e^{x_1}, \dots, e^{x_n}$

il y en a au moins n algébriquement indépendants.

Vérifier : Schanuel $\Longrightarrow$ LW $\Longrightarrow$ HL

Schanuel $\Longrightarrow$ B $\Longrightarrow$ HL

B $\Longrightarrow$ GS

Schanuel $\Downarrow$ les nombres $e, \pi, \log 2, \log\pi, 2^{\sqrt{2}}, e^e, \pi^e, 2^{\log 2}, \log\log 2$ sont algébriquement indépendants

Anneaux : commutatifs, unitaires $1 \neq 0$

intègres

Caractéristique $\quad \mathbb{Z} \longrightarrow A$, $\quad n \longmapsto n.1$

Homomorphisme

noyau = idéal de $\mathbb{Z}$

$\mathbb{Z} \subset A$ car. 0 $\quad \begin{cases} (0) & \text{caract. de } A = 0 \\ p\mathbb{Z} & p \text{ premier, caract. de } A = p \end{cases}$

$\mathbb{Z}/p\mathbb{Z} \subset A$ car. p.

K corps $\quad K[X]$ Euclidien $\Rightarrow$ principal $\Rightarrow$ factoriel.

$\mathbb{Z}$ principal $\quad \mathbb{Z}[X]$ pas principal.

A anneau factoriel $\Rightarrow A[X]$ est factoriel.

Intersection de sous-anneaux est un sous-anneau

A anneau $\quad$ B sous-anneau de A

E sous-ensemble de A

L'intersection de tous les sous-anneaux de A qui contiennent E et B est un sous-anneau de A qui contient E et B = le + petit s/anneau de A contenant E et B

On le note $B[E]$

Si $E = \{\alpha\}$ on écrit $B[\alpha]$ au lieu de $B[\{\alpha\}]$

Si $E = \{\alpha_1, \ldots, \alpha_m\}$

on écrit $B[\alpha_1, \ldots, \alpha_m]$

le sous-anneau de A engendré par $\alpha_1, \ldots, \alpha_m$ sur B.

$$B[\alpha_1, \ldots, \alpha_m] = \{ f(\alpha_1, \ldots, \alpha_m) \,;\, f \in B[X_1, \ldots, X_m] \}$$

Déf. A est de type fini sur B s'il existe $E \subset A$ fini tel que $B[E] = A$.

Extensions de corps

$K \subset L \quad$ L corps, K sous-corps de L.

$\{0, 1\} = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$

$K \subset L \quad$ extension $\quad$ (L/K une extension)

E sous-ensemble de L

$$K(E) = \bigcap F$$

F sous-corps de L contenant K et contenant E

:= sous-corps de L engendré par E sur K

$$\begin{array}{c} L \\ | \\ F \\ | \\ K \end{array}$$

$E = \{\alpha_1, \ldots, \alpha_m\}$

$$K(\alpha_1, \ldots, \alpha_m) = \{ R(\alpha_1, \ldots, \alpha_m) \,;\, R \in K(X_1, \ldots, X_m)$$

dénominateur de R pas nul au point $\alpha_1, \ldots, \alpha_m \}$.

Extension de type fini : L/K

telle qu'il existe $\{\alpha_1, \dots, \alpha_m\}$ partie finie de L vérifiant $L = K(\alpha_1, \dots, \alpha_m)$.

Extension monogène. $L|K$

$\exists \alpha \in L, \quad L = K(\alpha)$.

Exemples 1) $L = K$ $\quad \alpha \in L$ quelconque $L = K(\alpha)$

L est une ext. monogène de K

2) $\mathbb{C}$ est une extension monogène de $\mathbb{R}$

$\alpha = i \quad \mathbb{C} = \mathbb{R}(i)$

En fait $\forall \alpha \in \mathbb{C} \setminus \mathbb{R}$, on a $\mathbb{C} = \mathbb{R}(\alpha)$

3) $\mathbb{Q}(i)$ ext. monogène de $\mathbb{Q}$.

$\mathbb{Q}(\sqrt{d}) \qquad d \in \mathbb{Z}$ non carré dans $\mathbb{Z}$

ext. monogène de $\mathbb{Q}$.

4) K corps $\quad L = K(X)$ corps des fractions rationnelles à coeff. ds K.

L est une extension monogène de K

$\alpha = X$

5) Exemple d'extension de type fini non monogène : $L = K(X_1, X_2)$

fractions rationnelles en 2 variables.

6) Extensions pas de type fini $K(X_i \,;\, i \in I)$

I infini

$\mathbb{R}/\mathbb{Q}$ pas de type fini

Extensions finies

L/K une extension.

Alors L est un espace vectoriel sur K

$$\begin{tikzcd} L \times L \arrow[r] & L \\ K \times L \arrow[u, phantom, "\cup"] \arrow[ur] & \end{tikzcd}$$

Exple $\mathbb{C}$ est un $\mathbb{R}$-e-v.

L'extension $L|K$ est finie si $[L:K] = \dim_K L < \infty$

dim. e.v.

Une extension finie est de type fini

$K(X)|K$ est monogène (donc de type fini) infinie.