Rappel: Un nombre complexe $\alpha \in \mathbb{C}$ est algébrique s'il existe un polynôme non nul $P \in \mathbb{Q}[x]$ t.q. $P(\alpha) = 0$.

Exemples: tout nombre rationnel, $\sqrt[n]{a}$ $(a \in \mathbb{Q}, n \geq 1)$.

polynôme $X^n - a$.

Aujourd'hui:

- Montrer que l'ensemble des nombre algébriques est un corps: la somme, la différence, de nombres algébriques est algébrique, et la multiplication ainsi l'inverse d'un nombre algébrique non nul.
- Montrer les nombres constructibles à la règle et au compas sont algébriques.

On a montré: $|\{\text{algébriques}\}| = |\mathbb{N}|$.

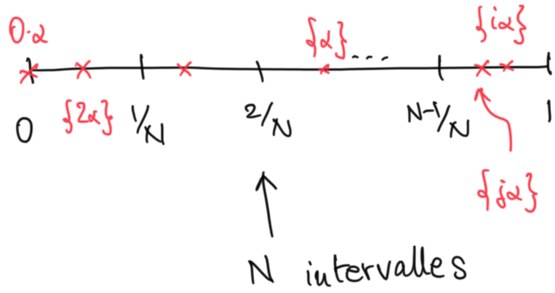
$|\{\text{transcendents}\}| = |\mathbb{C}| > |\mathbb{N}|$.

Approximation diophantienne:

Thm (Dirichlet): Soit $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Alors il existe une infinité de $x = \frac{p}{q} \in \mathbb{Q}$ avec $p, q \in \mathbb{Z}$, $(p,q) = 1$ et $q \geq 1$ t.q.

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

démo: On fixe un entier $N \geq 1$:



Pour $i = 0, \dots, N$

$\{i\alpha\} = i\alpha - [i\alpha]$ ← partie entière

$\{i\alpha\} \in [0,1]$.

$$0 = \{0\alpha\}, \{\alpha\}, \{2\alpha\}, \dots, \{N\alpha\} \qquad N+1 \text{ nombres}$$

Donc il existe $0 \leq i < j \leq N$ t.q.

$$|\{j\alpha\} - \{i\alpha\}| < \frac{1}{N}$$

$$\begin{aligned} |\{j\alpha\} - \{i\alpha\}| &= |j\alpha - [j\alpha] - i\alpha + [i\alpha]| \\ &= |(j-i)\alpha - ([j\alpha] - [i\alpha])| = |q\alpha - p|. \end{aligned}$$

On pose $p := [j\alpha] - [i\alpha]$ et $q = (j-i)$.

En divisant par q :

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{N} \cdot \frac{1}{q} \leq \frac{1}{q^2}.$$

$$0 \leq i < j \leq N \rightarrow 0 < q = j - i \leq N$$

Ceci montre que, pour tout $N \geq 1$, il existe $p \in \mathbb{Z}$ et $1 \leq q \leq N$ un entier t.q.

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q} \cdot \frac{1}{N}.$$

Pourquoi y en a-t-il une infinité ? Supposons qu'il n'existe qu'un nombre fini de rationnels $x_1, \dots, x_n \in \mathbb{Q}$ t.q.

$$|\alpha - x_i| < \frac{1}{q_i^2} \quad \text{avec} \quad x_i = \frac{p_i}{q_i}$$

$p_i, q_i \in \mathbb{Z}$, $q_i \geq 1$
$(p_i, q_i) = 1$.

On prend $N \geq 1$. Il existe $i \in \{1, \dots, n\}$ t.q.

$1 \leq q_i \leq N$ et

$$\left| \alpha - \frac{p_i}{q_i} \right| < \frac{1}{q_i} \cdot \frac{1}{N}$$

Puisqu'il n'y a qu'un nombre fini de tel x_i, il y a une suite strictement croissante

$N_1 < N_2 < \dots$ et $i \in \{1, \dots, n\}$ t.q.

$$\left| \alpha - \frac{p_i}{q_i} \right| < \frac{1}{q_i} \cdot \frac{1}{N_k} \quad \text{pour tout } k \in \mathbb{N}$$

$$\frac{1}{q_i} \cdot \frac{1}{N_k} \xrightarrow{k \to +\infty} 0$$

$$\Rightarrow \left| \alpha - \frac{p_i}{q_i} \right| = 0$$

$$\Rightarrow \alpha = \frac{p_i}{q_i}$$

α irrationnel $\Rightarrow$ il y a une infinité de tels $x = \frac{p}{q}$. $\square$

<u>Thm</u> (Liouville) Soit $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ algébrique de degré $d \geq 2$. Alors, il existe $C > 0$ t.q. pour tout $x = p/q \in \mathbb{Q}$, $p, q \in \mathbb{Z}$, $q \geq 1$, $(p,q) = 1$, on a

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

<u>démo.</u> Soit $P \in \mathbb{Q}[x]$ le polynôme minimal de α : c'est le générateur unitaire de l'idéal

$$I_\alpha = \{ f \in \mathbb{Q}[x] : f(\alpha) = 0 \}$$

plus petit

On encore, c'est le polynôme unitaire $\underset{\mathbb{Q}[x]}{\cap}$ de plus petit degré s'annulant en α. Par définition,

$$\deg(\alpha) := \deg P.$$

(e.g. $\alpha = \sqrt{2}$, $P(x) = x^2 - 2$, $\deg(\sqrt{2}) = 2$.

Dans ce cas l'énoncé est

$$\left|\sqrt{2} - \frac{p}{q}\right| \geq \frac{c}{q^2}. \quad)$$

- On développe P autour de α :

$$P(x) = \underbrace{P(\alpha)}_{=0} + (x-\alpha)P'(\alpha) + (x-\alpha)^2 \frac{P''(\alpha)}{2} + \dots + (x-\alpha)^d \frac{P^{(d)}(\alpha)}{d!} = \sum_{i=1}^{d} \frac{P^{(i)}(\alpha)}{i!}(x-\alpha)^i$$

Taylor

Soit $p/q \in \mathbb{Q}$ t.q. $|\alpha - p/q| \leq 1$.

$$\left|P\left(\frac{p}{q}\right)\right| = \left|\sum_{i=1}^{d} \frac{P^{(i)}(\alpha)}{i!}\left(\frac{p}{q} - \alpha\right)^i\right|$$

$$\leq \sum_{i=1}^{d} \left|\frac{P^{(i)}(\alpha)}{i!}\right| \left|\frac{p}{q} - \alpha\right|^i$$

$$\overset{\left|\frac{p}{q} - \alpha\right| \leq 1}{\leq} \left|\frac{p}{q} - \alpha\right| \left(\sum_{i=1}^{d} \left|\frac{P^{(i)}(\alpha)}{i!}\right| \underbrace{\left|\frac{p}{q} - \alpha\right|^{i-1}}_{\leq 1}\right)$$

$$\leq \left|\frac{p}{q} - \alpha\right| \underbrace{\left(\sum_{i=1}^{d} \frac{|P^{(i)}(\alpha)|}{i!}\right)}_{\text{ne dépend pas de } p/q}$$

Je l'appelle C_0.

- Minoration de $\left|P\left(\frac{p}{q}\right)\right|$:

On sait que le polynôme P est à coefficients rationnels :

$$P(x) = \sum_{i=0}^{d} a_i x^i \qquad a_i \in \mathbb{Q}. \quad \text{et} \quad a_d = 1.$$

Soit $N \in \mathbb{N} \setminus \{0\}$ t.q. $N P(x) \in \mathbb{Z}[x]$.

N ne dépend pas de P/q.

$$\left| N P\left(\frac{p}{q}\right) \right| = \left| \sum_{i=0}^{d} \underbrace{N a_i}_{\text{entiers}} \left(\frac{p}{q}\right)^i \right|$$

comme P est le polynôme de α et α n'est pas rationnel, P ne s'annule pas en P/q

↳ sinon on peut diviser P par $(x - \frac{p}{q})$ et obtenir un polynôme de degré strictement plus petit qui s'annule en α, Impossible par minimalité du degré de P.

$$= \frac{1}{q^d} \underbrace{\left| \sum_{i=0}^{d} \underbrace{N a_i p^i q^{d-i}}_{\text{entiers}} \right|}_{\text{entier non nul}} \geq \frac{1}{q^d}.$$

$$\Downarrow$$

$$\frac{1}{q^d} \leq \left| N P\left(\frac{p}{q}\right) \right| \leq (N C_0) \cdot \left| \alpha - \frac{p}{q} \right|$$

$$C := \frac{1}{N C_0}.$$

$$\rightarrow \left| \alpha - \frac{p}{q} \right| \geq \frac{C}{q^d}. \qquad \square$$

Exemple explicite de nombre transcendant

$$\lambda = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$$

$$= \frac{1}{10} + \frac{1}{100} + \frac{1}{10^6} + \frac{1}{10^{24}} + \cdots$$

$0,1100010000000000000000010\ldots$

le prochain 1

est en position
$5! = 120$

Supposons par l'absurde que ce nombre soit algébrique de degré $d \geq 2$. Pour $N \geq 1$

$$\mathbb{Q} \ni x_N = \sum_{n=1}^{N} \frac{1}{10^{n!}} = \frac{1}{\underbrace{10^{N!}}_{q_N}} \Bigg(\overbrace{\underbrace{\sum_{n=1}^{N} 10^{N!-n!}}_{1 + \text{ multiple de } 10.}}^{p_N} \Bigg)$$

$n = N$

$x_N = \frac{p_N}{q_N}$ $\quad q_N \geq 1$

$(p_N, q_N) = 1.$

$p_N, q_N \in \mathbb{Z}.$

$$\lambda - x_N = \sum_{n=N+1}^{\infty} \frac{1}{10^{n!}} = \frac{1}{10^{(N+1)!}} \Bigg(\sum_{n=N+1}^{\infty} \frac{1}{10^{n! - (N+1)!}} \Bigg).$$

$$\underbrace{1 + \sum_{k=2}^{\infty} \frac{1}{10^{(N+k)! - (N+1)!}}}_{\leq 2.}$$

$$\leq \frac{2}{10^{(N+1)!}} = \frac{2}{10^{N+1}} \cdot \frac{1}{10^{N!}}$$

$$q_N^{d+1} = (10^{N!})^{d+1} = 10^{N! \cdot (d+1)} \underset{N+1 \geq d+1}{\leq} 10^{(N+1)!}$$

Donc on a trouvé que pour tout $N+1 \geq d+1$

$$|\lambda - x_N| \leq \frac{2}{q_N^{d+1}}$$

Par le théorème de Liouville il existe $C > 0$ t.q.

$$\frac{2}{q_N^{d+1}} \geq |\lambda - x_N| \geq \frac{C}{q_N^d}$$

$$\longrightarrow \quad \frac{C}{2} \leq \frac{1}{q_N} \xrightarrow[N \to \infty]{} 0$$

$\Longrightarrow$ $C = 0$. en contradiction avec $C > 0$!

$\square$