1. Transcendance de e et de π.

2. Théorème de Lindemann et Weierstrass.

<u>Th</u> : Soient $a_1, \dots, a_n \in \overline{\mathbb{Q}}$ deux à deux distincts. Soient $b_1, \dots, b_n \in \overline{\mathbb{Q}}$ alors

$$b_1 e^{a_1} + \dots + b_n e^{a_n} = 0 \quad \Big| \quad e^{a_1}, \dots, e^{a_n} \text{ sont lin. indép sur } \overline{\mathbb{Q}}.$$

$$\Rightarrow \quad b_1, \dots, b_n = 0.$$

$$\overline{\mathbb{Q}} = \{ \alpha \in \mathbb{C} \text{ algébrique} \}.$$

<u>Cor</u>: Si $a \in \mathbb{C}$ algébrique non nul, alors e^a est transcendant.

<u>démo.</u> $n = 2$, $a_1 = 0$, $a_2 = a$. Si e^a est algébrique

$b_1 = -e^a$ et $b_2 = 1$:

$-e^a + e^a = 0$ en contradiction avec Lindemann-Weierstrass. $\square$

<u>Cor</u>: π est transcendant.

<u>démo</u> : $e^{i\pi} = -1$. algébrique $\Rightarrow$ $i\pi$ est transcendant

$\Rightarrow$ π est transcendant. $\square$

3. Valeurs de la fonction zêta aux entiers pairs.

$$\underset{\substack{Re(s) > 1 \\ s \in \mathbb{C}}}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Euler a calculé $\zeta(2k)$ pour tout $k \in \mathbb{N} \setminus \{0\}$.

- Définir la fonction zêta (définition, convergence, équation fonctionnelle, ...)

- Calcul de $\zeta(2k)$

- Calcul de $\zeta(2k)$.

$$\left.\begin{aligned} \zeta(2) &= \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} \\ \zeta(4) &= \sum_{n=1}^{\infty} \frac{1}{n^4} = \dots \end{aligned}\right\} \text{Transcendants.}$$

4. Irrationalité de $\zeta(3)$.

On croit que $\zeta(2k+1)$ est transcendant pour tout $k \in \mathbb{N} \setminus \{0\}$: $\zeta(3) = \sum \frac{1}{n^3}$, $\zeta(5) = \sum_{n=1}^{\infty} \frac{1}{n^5}, \dots$

On n'est pas capables de montrer ça.

<u>Th</u> (Apéry, 1979) : $\zeta(3)$ irrationnel.

5. <u>Réciprocité quadratique</u>

$2 \neq p$ premier impair $\quad \underbrace{\mathbb{Z}/p\mathbb{Z}}_{\text{corps}} = \{\text{classes résiduelles mod } p\}$

Racines carrées dans $\mathbb{Z}/p\mathbb{Z}$: $m \in \mathbb{Z}$,

est-ce que sa classe mod p a une racine carrée ?

<u>Exemple</u> : $m = -1$ on cherche $a \in \mathbb{Z}/p\mathbb{Z}$ t.q.

$$a^2 \equiv -1 \pmod p.$$

Dans ce cas la réponse est oui si et seulement si $p \equiv 1 \pmod 4$.

<u>$p=3$</u> : $\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$ $\quad \overline{-1} = \bar{2}$.

$$\bar{1} \cdot \bar{1} = \bar{1}, \quad \bar{0} \cdot \bar{0} = \bar{0}, \quad \overline{-1} \cdot \overline{-1} = \bar{1}.$$

Donc $\overline{-1}$ n'a pas de racine carrée.

$\underline{p=5}$: $\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ $\quad -1 \equiv 4 \pmod 5$.

$$4 = 2 \cdot 2 = 2^2 \equiv -1 \pmod 5$$

$\Rightarrow -1$ a une racine carrée.

$\underline{\text{Th (Gauss)}}$: Un entier m a une racine carré modulo p ssi $\underbrace{\ldots}$.

6. Polynômes cyclotomiques et construction des polygônes réguliers à la règle et au compas

$$\{\text{racines de l'unité}\} = \{\alpha \in \mathbb{C} : \alpha^n = 1, \exists n\}$$

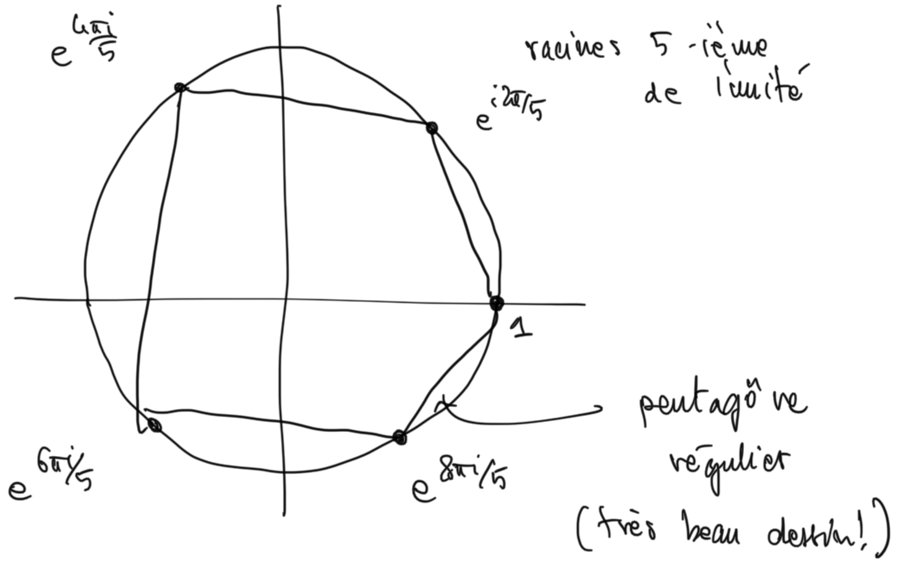
$1, -1, i, -i, e^{i\frac{2\pi}{3}}$

$$\left(e^{i\frac{2\pi}{3}}\right)^3 = e^{2\pi i} = 1.$$

$X^n - 1 \in \mathbb{Q}[X]$

$\alpha^n - 1 = 0 \Rightarrow \alpha$ est algébrique.

Polynômes cyclotomiques := polynômes minimaux des racines de l'unité



Gauss : on peut dessiner le N-gône regulier avec règle et compas ssi $e^{2\pi i/N}$ est un nombre algébrique constructible à la règle et au compas.

$\longrightarrow$ $N=17$ c'est vrai !

7. Pell-Fermat

$$x^2 - ny^2 = 1$$

$\longrightarrow$ solutions entières fournissent d'approximation de $\sqrt{n}$.

$\longrightarrow$ géométrie : dès qu'on a une solution, on peut en trouver une infinité d'autres (loi de groupe sur les solutions).

⚠ il y a toujours la solution $x=1$, $y=0$.

découvert par les mathématiciens indiens au XII siècle

8. Nombres p-adiques.

Au lieu d'utiliser la valeur absolue usuelle sur $\mathbb{Q}$, on utilise une autre valeur absolue (p-adique) pour construire des nombres différents : les p-adiques

9. Nombre de polynômes irréductibles sur un corps fini

$$\pi(x) = \{ p \text{ premier} : p \leq x \}$$

$$\pi(x) \sim \frac{x}{\log x}$$ (Théorème de nombres premiers).

analogue pour le nombre de polynômes

$\rightsquigarrow$ analogue pour le nombre de polynômes irréductibles sur $\mathbb{Z}/p\mathbb{Z}$ _