Théorème de Gauss Wantzel

↳ Refs : Carrega et Gozard

Rappels : On ne rappelle pas la définition d'un point constructible, cependant : on dit qu'un nombre complexe est constructible si c'est l'affixe d'un point constructible. Autrement dit, si $\mathcal{E}$ est le corps des réels constructibles, alors $z \in \mathbb{C}$ est constructible si $z \in \mathcal{E}(i) = \{a+ib, (a,b) \in \mathcal{E}\}$.
De plus $\mathcal{E}(i)$ est un sous corps de $\mathbb{C}$ stable par racine carrée.
↳ il suffit de montrer ces propriétés pour $\mathcal{E}$ puisque $z = x+iy \in \mathcal{E}(i)$ ssi $x, y \in \mathcal{E}$, donc pour la somme, le produit, l'inverse c'est clair, et pour la racine : $\sqrt{z} = \sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} \pm i \sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}$, ce qui suffit à faire le lien.

Et on a un théorème de Wantzel complexe :
$z \in \mathbb{C}$ est constructible ssi il existe une tour d'extension quadratique complexe $(L_0, L_1, \dots L_q)$ de $\mathbb{Q}$ telle que $z \in L_q$ ie une suite $\underset{\mathbb{Q}}{L_0} \subset L_1 \subset \dots \subset \underset{\mathbb{C}}{L_q}$ de sous corps telle que $L_0 = \mathbb{Q}$, $\forall i\ [L_{i+1} : L_i] = 2$ et $z \in L_q$.

↳ en corollaire : $z \in \mathcal{E}(i) \Rightarrow z$ alg. sur $\mathbb{Q}$ et $[\mathbb{Q}(z):\mathbb{Q}] = 2^m$

Enfin, on dit que le polygone régulier à n côtés est constructible si $e^{2i\pi/n}$ est constructible. On a alors les théorèmes suivants :

Théorème 1 : 1) Pour $\alpha \in \mathbb{N}^*$, le polygone régulier à 2^α côtés est constructible.
2) Soit p un nombre premier ≥ 3, et $\alpha \in \mathbb{N}^*$. Le polygone régulier à p^α côtés est constructible ssi $\alpha = 1$ et p est un nombre de Fermat (premier)

BONUS

Lemme : * Soit $m, n \in \mathbb{N}^*$ tels que $m \wedge n = 1$, alors $e^{\frac{2i\pi}{mn}}$ est constructible ssi $e^{\frac{2i\pi}{m}}$ et $e^{\frac{2i\pi}{n}}$ sont constructibles
* Si $n \geq 3$ a pour décomposition $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, alors le polygône régulier à n côtés est constructibles ssi $e^{\frac{2i\pi}{p_1^{\alpha_1}}}, \dots e^{\frac{2i\pi}{p_k^{\alpha_k}}}$ sont constructible

Théorème 2 : (Gauss) Soit n un entier ≥ 2, on peut construire le polygone régulier à n côtés ssi $n = 2^\alpha$ avec $\alpha \in \mathbb{N}^*$ ou $n = 2^\alpha p_1 \dots p_k$ où $\alpha \in \mathbb{N}$ et les $p_1, \dots p_k$ sont des nombres de Fermat premiers distincts

Preuve du théorème 1 : 1) (pas plus de détail à l'oral) On obtient le résultat par récurrence puisque l'on sait construire des bissectrices.

2) Soit p un nombre premier $p \geq 3$.
"$\Rightarrow$" Supposons qu'il existe $\alpha \in \mathbb{N}^*$ tel que $\omega = e^{\frac{2i\pi}{p^\alpha}}$ soit constructible
Alors d'après le théorème de Wantzel, il existe $m \in \mathbb{N}$ tel que $[\mathbb{Q}(\omega):\mathbb{Q}] = 2^m$

Or le polynôme minimal de ω est Φ_{p^α}, de degré $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.
Ainsi $p^{\alpha-1}(p-1) = [\mathbb{Q}(\omega) : \mathbb{Q}] = 2^m$. Par unicité de la décomposition en facteurs premiers, on a donc $\alpha = 1$ et $p = 1 + 2^m$. Ainsi p est un nombre de Fermat.

"$\Leftarrow$" Supposons que p soit un nombre de Fermat, $p = 1+2^n$ pour $n \geq 1$ (en fait n est une puissance de 2 mais ce n'est pas important ici)
Nous allons essayer de construire une tour d'extensions quadratiques sur $\mathbb{Q}$ contenant $\omega := e^{2i\pi/p}$. Pour cela, nous allons donc considérer $K = \mathbb{Q}(\omega)$, et plus précisément nous allons nous intéresser au groupe des automorphismes de K : $G := \mathrm{Aut}(K)$.

- Premièrement, nous allons montrer que G est cyclique, et $G \simeq (\mathbb{Z}/p\mathbb{Z})^\times$.
Soit $\sigma \in G$. Puisque σ fixe $\mathbb{Q}$ (car $\sigma(1) = 1$ et σ est additif),
on a : $\Phi_p(\sigma(\omega)) = \sigma(\Phi_p(\omega)) = \sigma(0) = 0$.
coeff dans $\mathbb{Q}$ (en fait dans $\mathbb{Z}$)

Ainsi $\sigma(\omega)$ est une racine de Φ_p, et donc une racine p-ième de l'unité. Ainsi il existe $k_\sigma \in [\![1, p-1]\!]$ tel que $\sigma(\omega) = \omega^{k_\sigma}$. On peut donc définir l'application $\varphi : \begin{array}{ccc} G & \mapsto & (\mathbb{Z}/p\mathbb{Z})^\times \\ \sigma & \mapsto & \overline{k_\sigma} \end{array}$. Elle est de plus injective (si $k_\sigma = k_{\sigma'} [p]$, $\sigma(\omega) = \omega^{k_\sigma} = \omega^{k_{\sigma'}} = \sigma'(\omega)$ car $\omega^p = 1$, donc σ et σ' coïncident sur ω et sur $\mathbb{Q}$, donc sur K tout entier)

De plus, φ est surjective. En effet, si $k \in [\![1, p-1]\!]$, l'application $\begin{array}{ccc} \mathbb{Q}[X] & \to & K \\ P & \mapsto & P(\omega^k) \end{array}$ est un morphisme d'anneaux surjectif (car $\mathbb{Q}(\omega) = \mathbb{Q}(\omega^k)$ puisque $k \wedge p-1$), de noyau $\langle \Phi_p \rangle$.
On peut donc passer au quotient, et l'on obtient un morphisme de corps $\begin{array}{ccc} \mathbb{Q}[X]/\langle\Phi_p\rangle & \to & K \\ \overline{X} & \mapsto & \omega^k \end{array}$, et en composant par l'isomorphisme $\begin{array}{ccc} K & \to & \mathbb{Q}[X]/\langle\Phi_p\rangle \\ \omega & \mapsto & \overline{X} \end{array}$,
on obtient un automorphisme $\sigma_k : \begin{array}{ccc} K & \mapsto & K \\ \omega & \mapsto & \omega^k \end{array}$.

Ainsi, φ est bijective, et il s'agit d'un morphisme de groupes. Ainsi G est, tout comme $(\mathbb{Z}/p\mathbb{Z})^\times$, cyclique d'ordre $p-1 = 2^n$.
Soit g un générateur de G.

- Maintenant, nous allons construire la tour d'extensions quadratiques
Le groupe G est d'ordre 2^n, et on va considérer les groupes $G_i = \langle g^{2^i} \rangle$ pour $i \in [\![0, n]\!]$, qui sont respectivement d'ordre 2^{n-i}, et se contiennent successivement : $G = G_0 \supset G_1 \supset \dots \supset G_n = \{id_K\}$. A cette suite de sous groupes, nous allons associer une suite de sous corps de K.
Pour $i \in [\![0, n]\!]$, on note $K_i := \{z \in K,\ g^{2^i}(z) = z\} = \{z \in K,\ \forall \sigma \in G_i,\ \sigma(z) = z\}$
Alors les K_i sont des sous corps de K et $\mathbb{Q} \subset K_0 \subset K_1 \subset \dots \subset K_n = K$.

Montrons que pour tout $i \in [\![0,n-1]\!]$, $K_i \subsetneq K_{i+1}$. Soit $i \in [\![0,n-1]\!]$.

On considère $z = \omega + g^{2^{i+1}}(\omega) + g^{2^{i+2}}(\omega) + \cdots + g^{2^{i+1}(2^{n-i-1}-1)}(\omega)$

$$= \sum_{k=0}^{2^{n-i-1}-1} g^{2^{i+1}k}(\omega)$$

Alors $g^{2^{i+1}}(z) = z$, et d'autre part,

$$g^{2^i}(z) = g^{2^i}(\omega) + g^{3\times 2^i}(\omega) + \cdots + g^{2^i(2^n-2^{i+1})}(\omega) = \sum_{k=1}^{2^{n-i}-1} g^{2^i k}(\omega)$$

$\neq z$ (par unicité de l'écriture dans la base $\{g^k(\omega),\ 0 \le k \le 2^n-1\} = \{\omega^k,\ 1 \le k \le p-1\}$

Ainsi $z \in K_{i+1} \setminus K_i$.

D'après le théorème de la base télescopique, on obtient :

$$2^n = p-1 = [K:\mathbb{Q}] = \prod_{k=0}^{n-1} [K_{i+1}:K_i] \times [K_0:\mathbb{Q}].$$

Or d'après ce qu'il précède, $\forall i \in [\![0,n-1]\!]$, $[K_{i+1}:K_i] > 1$, donc $[K_{i+1}:K_i] = 2$ et $[K_0:\mathbb{Q}] = 1$ d'où $K_0 = \mathbb{Q}$. On a donc obtenu notre tour d'extensions quadratiques, ce qui conclut d'après le théorème de Wantzel

Bonus : Preuve du lemme : 1) "$\Rightarrow$" Si $e^{\frac{2i\pi}{nm}}$ est constructible, alors $\left(e^{\frac{2i\pi}{nm}}\right)^n$ et $\left(e^{\frac{2i\pi}{nm}}\right)^m$ aussi puisque $\mathbb{E}(i)$ est un sous corps de $\mathbb{C}$.

"$\Leftarrow$" Supposons $e^{\frac{2i\pi}{n}}$ et $e^{\frac{2i\pi}{m}}$ constructibles. Le théorème de Bézout nous fournit $(u,v) \in \mathbb{Z}^2$ tels que $un + vm = 1$, et alors $\left(e^{\frac{2i\pi}{m}}\right)^u \left(e^{\frac{2i\pi}{n}}\right)^v = e^{\frac{2i\pi}{nm}(nu+mv)} = e^{2i\pi/nm}$ est constructible.

Le point 2) s'en déduit en itérant, et le théorème 2 se déduit du point 2) et du théorème

Remarques : * Concernant les nombres de Fermat : on appelle n-ième nombre de Fermat le nombre $F_n = 2^{2^n} + 1$ pour $n \in \mathbb{N}$.

En fait si $2^q + 1$ est premier, alors $q = 0$ ou q est une puissance de 2.

(en effet, si $q \in \mathbb{N}^*$ n'est pas une puissance de 2, alors $q = (2a+1)2^b$ avec $a \in \mathbb{N}^*$ et $b \in \mathbb{N}$. Alors $D = 2^{2^b}$ vérifie $2 \le D+1 < 2^q+1$ et $2^q + 1 = D^{2a+1} - (-1)^{2a+1} = (D+1)\sum_{i=0}^{2a}(-1)^i D^{2a-i}$ est divisible par $D+1$, donc $1+2^q$ n'est pas premier).

En revanche, tous les F_n ne sont pas premiers ! Les cinq premiers sont tous premiers : $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\,537$.

Cependant F_5 n'est pas premier, et cela continue jusqu'au moins F_{21}. Aucun autre premier n'a été découvert pour l'instant.

(En revanche il existe un test de primalité : le test de Pépin).

* Ainsi pour $n \in \{2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20\}$, le polygone régulier à n côtés est constructible (cf annexe pour des exemples), mais il ne l'est pas pour $n \in \{7, 9, 11, 13, 14, 18, 19\}$.

* la technique utilisée pour la réciproque est """"naturelle"""" en théorie de Galois grâce à la correspondance de Galois :
Si L/K est galoisienne (ssi $|Aut_K(L)| = [L:K]$), ssi L est le corps de décomposition sur K d'un polynôme séparable de $K[X]$, alors en notant $Gal(L/K) = Aut_K(L)$,
$P \wedge P' = 1$

$$\left\{ \begin{array}{c} \text{sous groupes} \\ \text{de } Gal(L/K) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{corps intermédiaires} \\ M \ (K \subseteq M \subseteq L) \end{array} \right\}$$

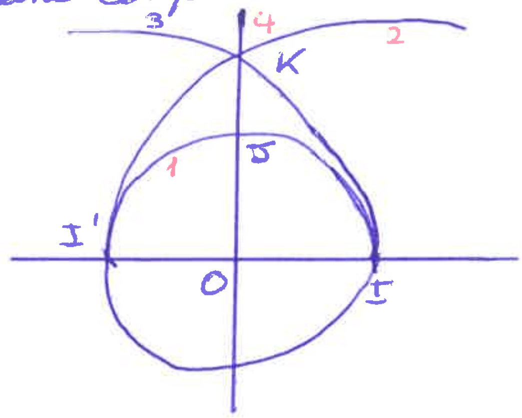
$$H \longmapsto L^H = \{x \in L \mid \forall \sigma \in H, \sigma(x) = x\}$$

$$\{\sigma \in G, \sigma_{|M} = id_M\} = Gal(L/M) \longleftarrow M$$

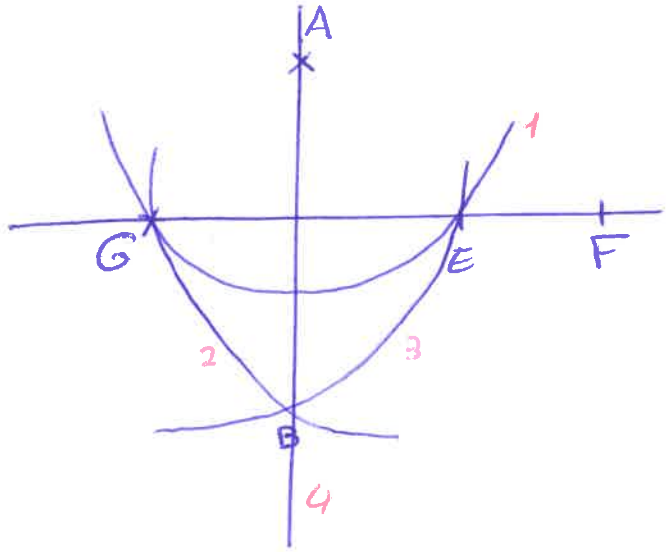
Bon on ne va pas creuser plus mais ça a le mérite de donner du recul

Annexe : Quelques constructions "de base" à savoir faire :
(faites sans compas...)

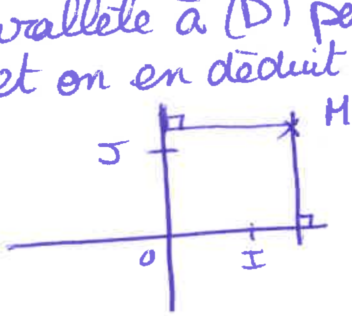
* Les points "classiques"



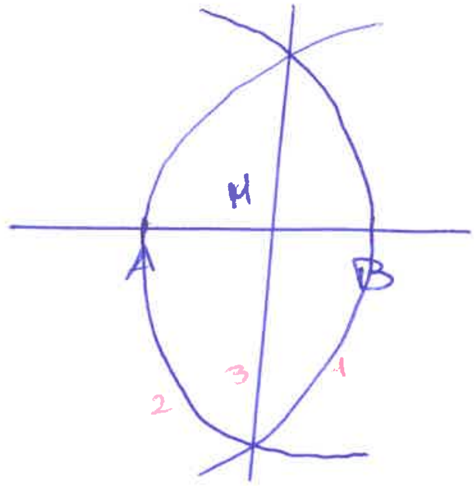
* la perpendiculaire à $[EF]$ passant par A



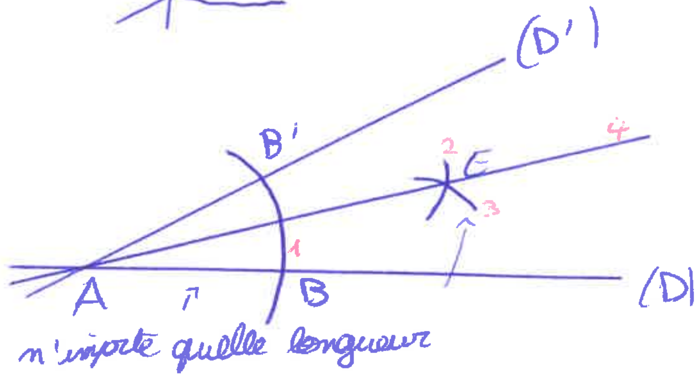
▷ on en déduit la parallèle à (D) passant par A en utilisant 2 fois cette technique, et on en déduit également le projeté de $M(x,y)$ sur (OI) et (OJ) :



* la médiatrice de [AB]
  (et le milieu de [AB])



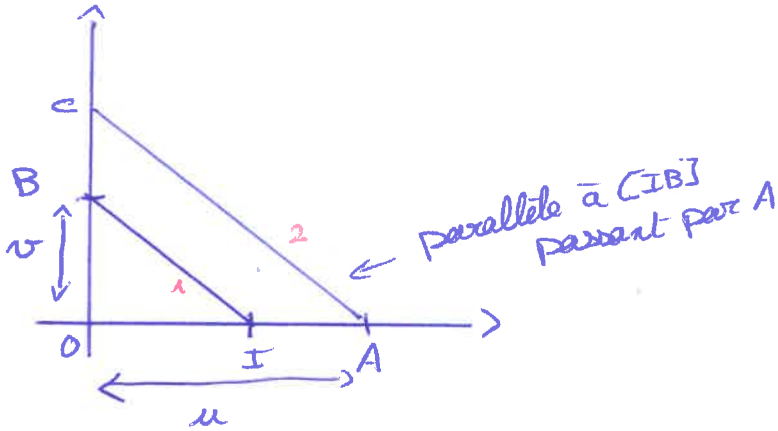
* la bissectrice d'un angle :



* le produit de u et v :

Thalès : $\frac{OI}{OA} = \frac{OB}{OC}$

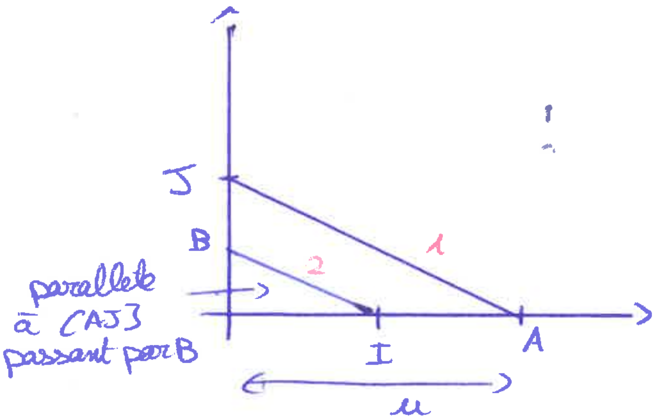
$\frac{1}{u} = \frac{v}{OC} \Rightarrow OC = uv$



* L'inverse de u :

Thalès : $\frac{OI}{OA} = \frac{OB}{OJ}$

$\frac{1}{u} = OB$

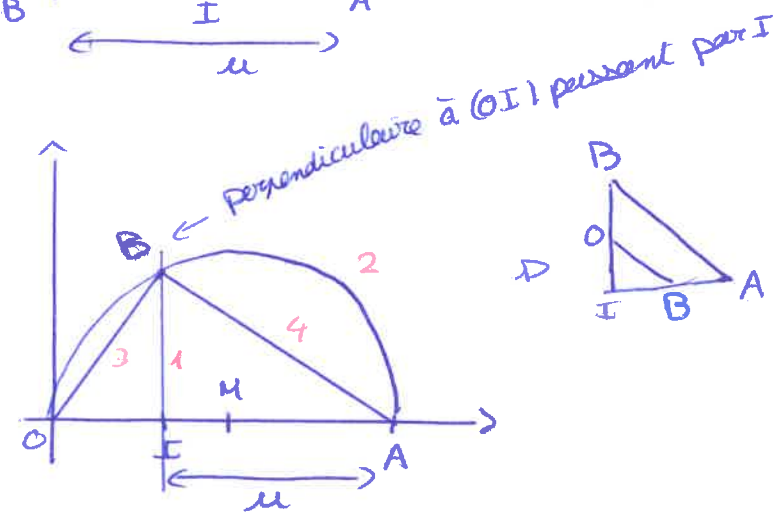


* la racine de u :

Thalès : $\frac{IB}{IA} = \frac{IO}{IB}$

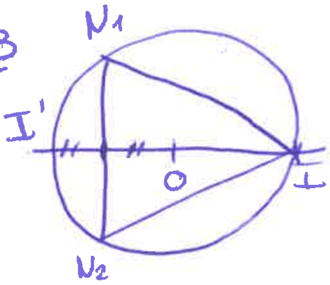
$\frac{IB}{u} = \frac{1}{IB}$

$\Rightarrow IB^2 = u$

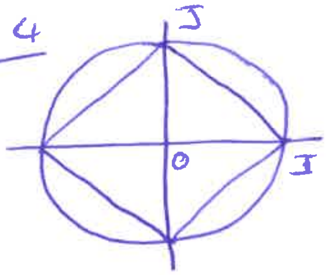


* Construction de quelques polygones réguliers :

$n=3$



$n=4$



$n=5$ $\Rightarrow$ Calculons $\cos\left(\frac{2\pi}{5}\right)$:

$\omega = \cos\left(\frac{2\pi}{5}\right) + i\sin\left(\frac{2\pi}{5}\right) \Rightarrow \omega^5 - 1 = 0$ donc $\omega^4 + \omega^3 + \omega^2 + \omega^1 + 1 = 0$ (*)

$\omega^4 = \overline{\omega}$ et $\omega^3 = \overline{\omega^2}$ donc $\omega + \omega^4 = 2\cos\left(\frac{2\pi}{5}\right)$ et $\omega^2 + \omega^3 = 2\cos\left(\frac{4\pi}{5}\right)$

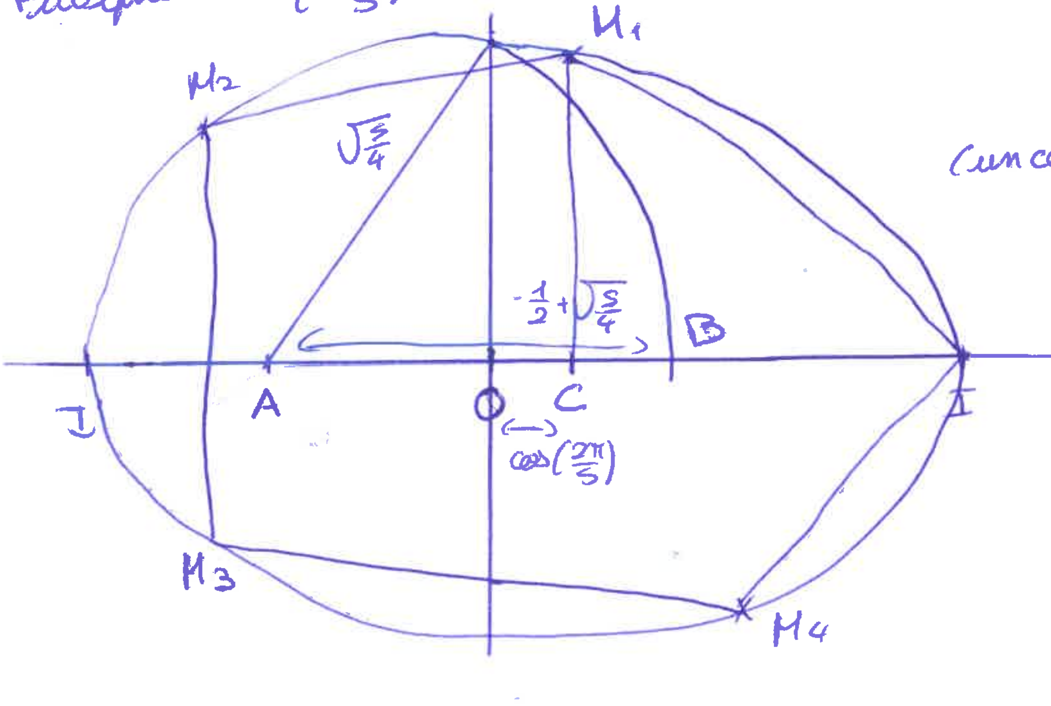
(*) $\Rightarrow 2\cos\left(\frac{2\pi}{5}\right) + 2\cos\left(\frac{4\pi}{5}\right) + 1 = 0$ (**)

De plus $\cos\left(\frac{2\pi}{5}\right)\cos\left(\frac{4\pi}{5}\right) = \frac{1}{2}\left(\cos\left(\frac{6\pi}{5}\right) + \cos\left(\frac{2\pi}{5}\right)\right) = \frac{1}{2}\left(\cos\left(\frac{4\pi}{5}\right) + \cos\left(\frac{2\pi}{5}\right)\right)$

Alors $\begin{cases} \cos(\ ) + \cos(\ ) = -\frac{1}{2} \\ \cos(\ )\cos(\ ) = -\frac{1}{4} \end{cases}$ donc ils sont racines de $X^2 + \frac{X}{2} - \frac{1}{4}$

Puisque $\cos\left(\frac{4\pi}{5}\right) < 0 < \cos\left(\frac{2\pi}{5}\right)$, on en déduit $\cos\left(\frac{2\pi}{5}\right) = \frac{-1+\sqrt{5}}{4}$

$= \frac{-\frac{1}{2} + \sqrt{\frac{5}{4}}}{2}$



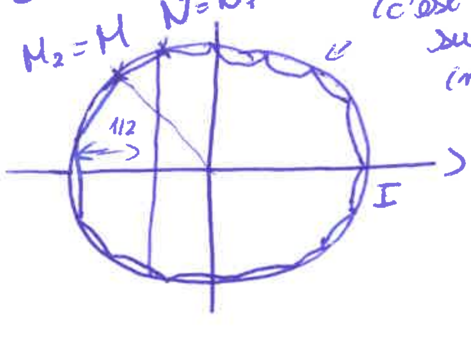
(un cercle pitoyable mais bon, l'idée est là)

Une construction à la règle et au compas ... sans règle et sans compas

$n=15$ $\quad 2\times 3 - 5 = 1 \Rightarrow \frac{2\pi}{15} = 2\times\frac{2\pi}{5} - \frac{2\pi}{3}$

M et N tels que $(\widehat{\vec{OI}, \vec{OM}}) = 2\times\frac{2\pi}{5}$

et $(\widehat{\vec{OI}, \vec{ON}}) = \frac{2\pi}{3}$



(c'est parti en sucette) (mais l'idée est là)

(à partir de 17 c'est massi dur)