Constructibilité à la règle et au compas

réf: Gozard, Théorie de Galois p.47.
Ismann, Recatte, L'oral à l'agreg de maths, p219.

I - Points constructibles

P le plan affine euclidien.

Définition: On dit que $M \in P$ est constructible en un pas à partir de X si et seulement si il existe:
- deux droites distinctes de point distincts de X.
- deux cercles distincts de point de X
- ou bien une droite et d'un cercle.

dont M soit un point d'intersection.

Définition: Point Constructible

Soit B_0 une partie de P, avec $\text{card}(B_0) \geq 2$.

* On définit par récurrence $\forall i \in \mathbb{N}^*$, B_i = l'ensemble des points constructibles à la règle et au compas en un pas à partir de B_{i-1}. B_i est appelé l'ensemble des points constructibles à la règle et au compas en i pas à partir de B_0. La suite $(B_n)_{n\in\mathbb{N}}$ est croissante au sens de $\subseteq$.

* Pour $M \in P$, les conditions suivantes sont équivalentes:
  i) $M \in \bigcup_{n\in\mathbb{N}} B_n$
  ii) Il existe une suite finie $M_1, \dots, M_n$ de points de P telle que, notant $A_0 = B_0$ et pour chaque $i \in [\![1, n]\!]$, $A_i = A_{i-1} \cup \{M_i\}$ on ait:
  $M_n = M$ et ($\forall i \in [\![1, n]\!]$, M_i est constructible en un pas à partir de A_{i-1}).

Lorsqu'elles sont vérifiées, on dit que M est constructible à la règle et au compas à partir de B_0.

Proposition:
1) Si M est constructible, son symétrique par rapport à l'origine O l'est également.
2) Si A et B sont constructibles distincts, alors le milieu et la médiatrice de $[A,B]$ sont constructibles.
3) $\vec{0} = (0,1)$ est constructible.
4) Si A et B constructibles distincts et C constructibles, on peut construire à la règle et au compas la perpendiculaire à (AB) passant par C.

5) Si A et B constructibles distincts et C constructible, on peut construire à la règle et au compas la parallèle à (AB) passant par C.

II - Nombres constructibles

Proposition:
Soit $x \in \mathbb{R}$, les conditions suivantes sont équivalentes:
- le point $(x,0)$ est constructible.
- le point $(0,x)$ est constructible.

Lorsqu'elles sont vérifiées, on dit que x est un nombre constructible.

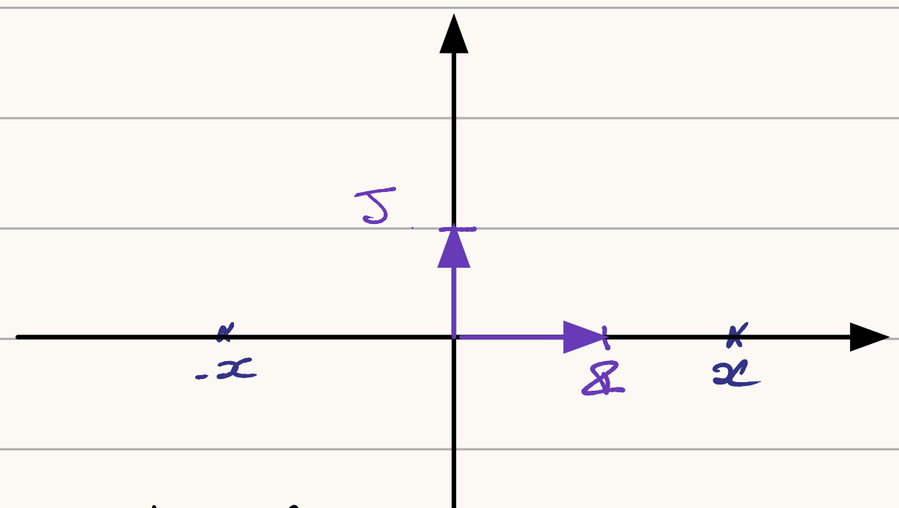
Proposition: $\mathbb{Q}$ est constructible

Preuve: Thalès.

Proposition: $M=(x,y)$ est constructible ssi x et y le sont.

Théorème: L'ensemble $\mathbb{E}$ des nombres réels constructibles est un sous-corps de $\mathbb{R}$ stable par racine carrée
i.e $\forall x \in \mathbb{E} \cap \mathbb{R}_+, \sqrt{x} \in \mathbb{E}$

Preuve:
- 0 et 1, abscisses respectives de O et I sont dans $\mathbb{E}$.
- Soit $x \in \mathbb{E}$ alors son symétrique par rapport à O l'est aussi donc $-x \in \mathbb{E}$.
- Soit $(u,v) \in \mathbb{E}^2$, la droite passant par $(0,u)$ et $(-u,0)$ et la droite passant par les points $(v,0)$ et (v,v) ont pour points d'intersection $(u, u+v)$ donc $u+v \in \mathbb{E}$.
- Soit $(u,v) \in \mathbb{E}^2$, par ce qui précède $v+1 \in \mathbb{E}$ et $v+1-u \in \mathbb{E}$. Alors droite passant par les points $(v+1-u, v+1)$ et (v,v) et la droite (OI) ont pour points d'intersection $(uv, 0)$ donc $uv \in \mathbb{E}$.
- Soit $x \in \mathbb{E} \setminus \{0\}$, la droite passant par $(0,1)$ et $(x,-1)$ et la droite passant par 0 et $(1,1)$ ont pour points d'intersections (x^{-1}, x^{-1}) donc $x^{-1} \in \mathbb{E}$. $\Rightarrow \mathbb{E}$ sous-corps de $\mathbb{Q}$.
- Soit $x \in \mathbb{E} \cap \mathbb{R}_+$ on a que $\frac{x+1}{2} \in E$, le cercle de centre $(\frac{x+1}{2}, 0)$ passant par O et la droite passant



par les points $(x,0)$ et (x,x) on pour points d'intersections $(x,\sqrt{x})$ et $(x,-\sqrt{x})$ donc $\sqrt{x}\in\mathbb{E}$.

II - Théorème de Wantzel

Rmq: On utilise que un cercle ou une droite de point de $F\times F$ à des coeffs dans F.

Théorème:

Soit $t\in\mathbb{R}$, t est constructible si et seulement si, il existe une suite finie $(L_0,L_1,\dots,L_p)$ de sous-corps de $\mathbb{R}$ tq:

- $L_0=\mathbb{Q}$
- $\forall i\in[\![0,p-1]\!]$, L_{i+1} est une extension quadratique de L_i
- $t\in L_p$

Preuve:

$\Rightarrow$: Supposons t constructible i.e $M=(t,0)$ constructible.

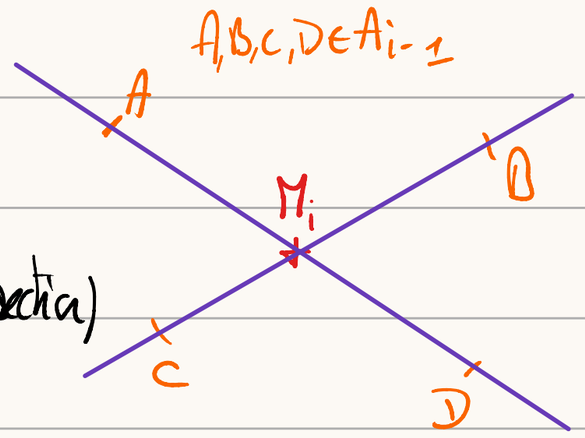
Il existe donc une suite finie $M_1,\dots,M_n$ de points de $\mathcal{P}$ telle que, en notant $A_0=\{0,I\}$ et $A_i=A_{i-1}\cup\{M_i\}$ on ait $M_n=M$ et que M_i est constructible en un pas à partir de A_{i-1}.

Pour tout $i\in[\![1,n]\!]$ on note $M_i=(x_i,y_i)$.

Ainsi si on pose $K_0=\mathbb{Q}$ et $K_i=K_{i-1}(x_i,y_i)=\mathbb{Q}(x_1,y_1,\dots,x_i,y_i)$ on a alors une suite de sous-corps de $\mathbb{R}$, $(K_0,K_1,\dots,K_n)$, croissante au sens de $\subseteq$ et $t=x_n\in K_n$.

Soit $i\in[\![1,n]\!]$, M_i est constructible en un point à partir de A_{i-1} et $A_{i-1}\subseteq(K_{i-1}\times K_{i-1})$ (-> point à coordonnée dans K_{i-1}), il y a donc 3 cas possibles.

<u>M_i est l'intersection de deux droites:</u>



Alors il existe $u_1,v_1,w_1\in K_{i-1}$ et $u_2,v_2,w_2\in K_{i-1}$ tel que:

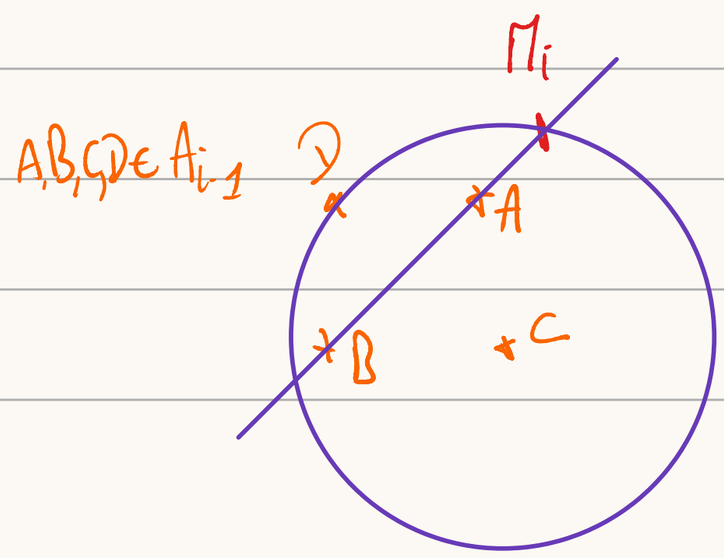
$$\begin{cases}u_1x_i+v_1y_i+w_1=0\\ u_2x_i+v_2y_i+w_2=0\end{cases}\quad\text{et}\quad\Delta=\begin{vmatrix}u_1&v_1\\u_2&v_2\end{vmatrix}\in K_{i-1}^{*}\ \text{(existence des point d'intersection)}$$

Alors par les formules de Cramer:

$$x_i=\begin{vmatrix}-w_1&v_1\\-w_2&v_2\end{vmatrix}\frac{1}{\Delta}\quad\text{et}\quad y_i=\begin{vmatrix}u_1&-w_1\\u_2&-w_2\end{vmatrix}\frac{1}{\Delta}$$

donc $x_i,y_i\in K_{i-1}$.

<u>M_i est l'intersection d'une droite et d'un cercle</u>: $(x,y)=(x_i,y_i)$



Ainsi il existe $a,b,c\in K_{i-1}$ et $u,v,w\in K_{i-1}$ tq:

$$\begin{cases}ux+vy+w=0 & \text{avec } (u,v)\neq(0,0).\\ x^2+y^2-2ax-2by+c=0\end{cases}$$

Comme x, y jouent des rôles symétriques on peut supposer $v \neq 0$.

Ainsi on obtient :

$$y = -\frac{u}{v}x - \frac{w}{v}$$

Ce qui donne :

$$\underbrace{\left(1 + \left(\frac{u}{v}\right)^2\right)}_{>0} x^2 + \ell\left(\frac{uw}{v^2} - a + \frac{bu}{v}x\right) + c + \ell b\frac{w}{v} + \left(\frac{w}{v}\right)^2 = 0$$

Ainsi x est zéro d'un polynôme de la forme $P(X) = X^2 + \lambda X + \mu$ avec $\lambda, \mu \in K_{i-1}$

Cas 1 : P_n est pas irréductible dans $K_{i-1}[X]$ donc s'écrit comme produit de deux polynôme unitaires de degré 1 à coefficients dans K_{i-1} donc $x \in K_{i-1}$

$$\text{et } y = -\frac{u}{v}x - \frac{w}{v} \in K_{i-1}$$

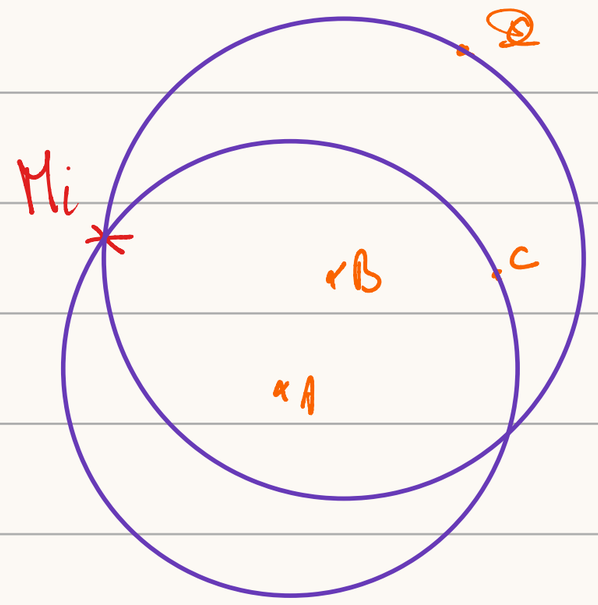
donc $K_i = K_{i-1}$

Cas 2 : P est irréductible dans $K_{i-1}[X]$ donc P est le polynôme minimale de x sur K_{i-1} donc $K_{i-1}(x)$ est une extension de degré $\deg(P) = \ell$ de K_{i-1} et

$$y = -\frac{u}{v}x - \frac{w}{v} \in K_i \quad (x)$$

Ainsi $K_i = K_{i-1}(x)$ et $[K_i : K_{i-1}] = \ell$.

M_i est l'intersection de deux cercles :



Alors il existe $a_1, b_1, c_1 \in K_{i-1}$ et $a_2, b_2, c_2 \in K_{i-1}$ tel que :

$$\begin{cases} x^2 + y^2 - \ell a_1 x - \ell b_1 x + c_1 = 0 \\ x^2 + y^2 - \ell a_2 x - \ell b_2 x + c_2 = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} \ell(a_2 - a_1)x + \ell(b_2 - b_1)x + c_2 - c_1 = 0 \\ x^2 + y^2 - \ell a_2 x - \ell b_2 x + c_2 = 0 \end{cases}$$

Avec $(a_2, b_2) \neq (a_1, b_1)$ car sinon ou $c_1 = c_2$ les cercles seraient confondus exclue.

ou $c_1 \neq c_2$ donc l'intersection serait vide exclue.

On a donc l'équation d'une droite et d'un cercle $\Rightarrow$ on revient au cas précédent.

Conclusion : On a donc montré que $K_i = K_{i-1}$ ou K_i est une extension de degré 2 de K_{i-1}.

Il suffit d'extraire de la suite $(K_0, \ldots, K_n)$ une suite strictement croissante en ne conservant que les

corps extension quadratique du précédent avec $L_0 = \mathbb{Q}$ et $L_p = K_n$ et on obtient le résultat.

$\Leftarrow$: Supposons qu'il existe une telle tour, montrons par récurrence que pour $j \in [\![0, p]\!]$, $L_j \subseteq \mathbb{E}$.

Cas $j=0$: $L_0 = \mathbb{Q} \subseteq \mathbb{E}$.

Supposons $L_j \subseteq \mathbb{E}$: Soit $x \in L_{j+1}$, $[L_{j+1} : L_j] = 2$ Ce famille $(1, x, x^2)$ est L_j-liée.

Donc il existe $(a,b,c) \in L_j^3 \setminus (0,0,0)$ tq :

$$ax^2 + bx + c = 0. \quad (1)$$

Si $a=0$: $x = -\frac{c}{b} \in L_j \subseteq \mathbb{E}$.

Si $a \neq 0$ On obtient que :

$$x \in \left\{ \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \right\} \qquad b^2 - 4ac \geq 0 \text{ car } (1) \text{ admet une solution réelle.}$$

Comme $\mathbb{E}$ est un sous-corps stable par racine carrée $x \in \mathbb{E}$ d'où le résultat.

$\square$

Corollaire : Soit $x \in \mathbb{R}$ constructible alors il existe $n \in \mathbb{N}$ tel que $[\mathbb{Q}(x) : \mathbb{Q}] = 2^n$.

Preuve : En notant $L_0, \dots, L_p$ la tour d'extension quadratique.

Alors $[L_p : \mathbb{Q}] = \prod_{i=1}^{p} [L_i : L_{i-1}] = 2^p$ car $L_0 = \mathbb{Q}$.

Comme $x \in L_p$ on a $\mathbb{Q}(x) \subseteq L_p$ donc

$$2^p = [L_p : \mathbb{Q}] = [L_p : \mathbb{Q}(x)][\mathbb{Q}(x) : \mathbb{Q}]$$

Donc il existe $n \in \mathbb{N}$ tq : $[\mathbb{Q}(x) : \mathbb{Q}] = 2^n$.

$\square$

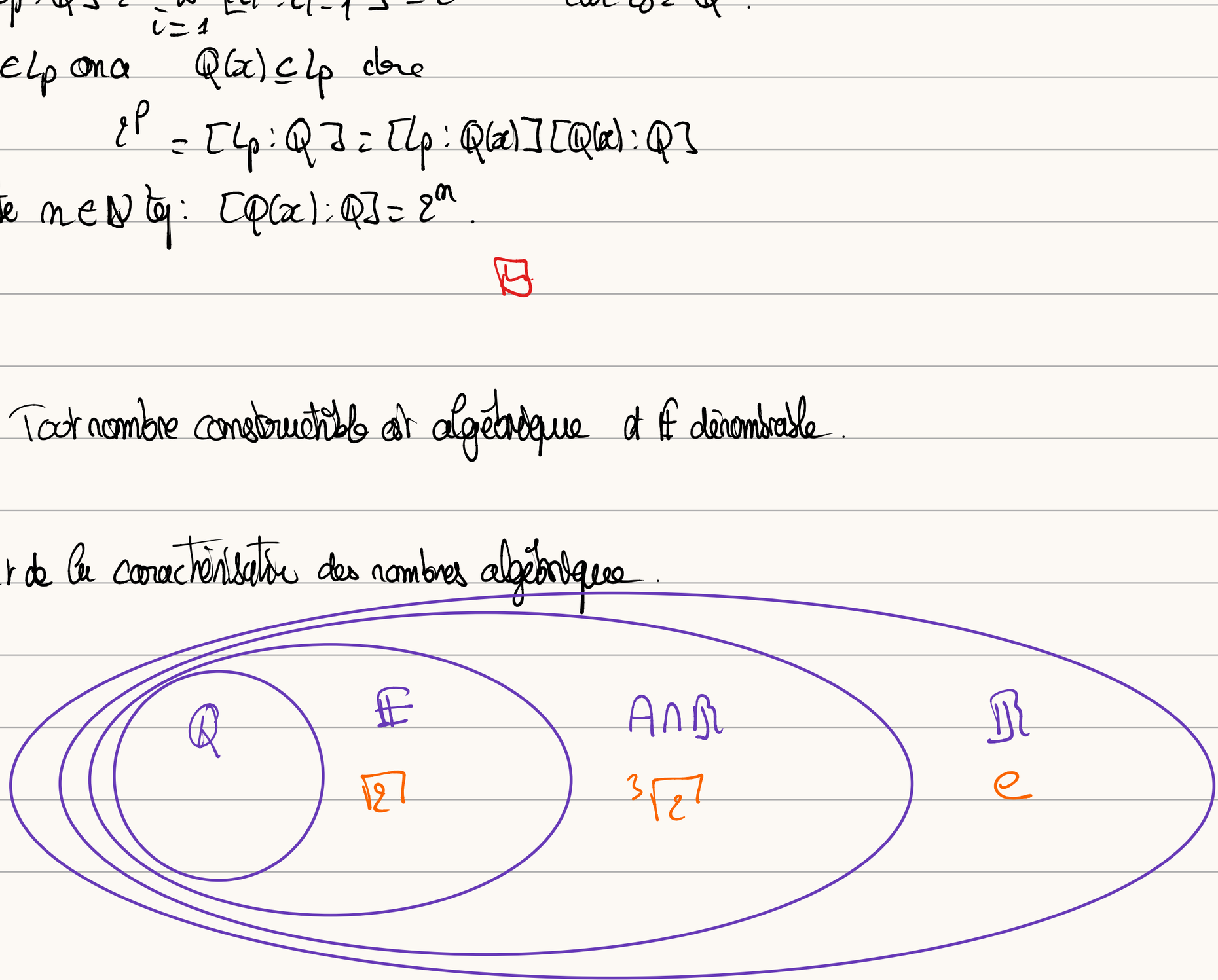
Rmq : La réciproque est fausse.

Corollaire : Tout nombre constructible est algébrique et $\mathbb{E}$ dénombrable.

Preuve : Vient de la caractérisation des nombres algébriques.

Rmq :

A = nombre algébrique



II - Polygones constructibles à la règle et au compas

Définition: Soit $n \in \mathbb{N}^*$.

On dit que le polygone régulier à n côtés est constructible ssi l'angle $\frac{2\pi}{n}$ est constructible

ssi $A = (\cos(\frac{2\pi}{n}), \sin(\frac{2\pi}{n}))$ est constructible

ssi $\cos(\frac{2\pi}{n})$ est constructible

ssi $\sin(\frac{2\pi}{n})$ est constructible

Lemme: Soit m et n deux entiers naturels ≥ 1 tq $m \wedge n = 1$. Le polygone régulier à mn côtés est constructible ssi les polygones réguliers à m côtés et n côtés sont tous deux constructibles.

Preuve:

$\Rightarrow$: On suppose l'angle $\frac{2\pi}{mn}$ constructible donc $a = \cos(\frac{2\pi}{mn}) \in \mathbb{E}$.

En notant $(T_k)_{k \in \mathbb{N}} \subset \mathbb{Z}[X]$ la suite de polynôme de Tchebychev on sait que:

$$\cos(\tfrac{2\pi}{n}) = T_m(\cos(\tfrac{2\pi}{mn})) \text{ et } \cos(\tfrac{2\pi}{m}) = T_n(\cos(\tfrac{2\pi}{mn}))$$

donc $\cos(\frac{2\pi}{n}) \subseteq \mathbb{Q}(a) \subseteq \mathbb{E}$

$\cos(\frac{2\pi}{m}) \subseteq \mathbb{Q}(a) \subseteq \mathbb{E}$.

d'où le résultat.

$\Leftarrow$: Supposons $\cos(\frac{2\pi}{m}) \in \mathbb{E}$ et $\cos(\frac{2\pi}{n}) \in \mathbb{E}$ donc

Comme $m \wedge n = 1$ il existe $(u,v) \in \mathbb{Z}^2$ tel que $mu + nv = 1$

$$\text{i.e } \frac{2\pi}{mn} = u\frac{2\pi}{n} + v\frac{2\pi}{m}$$

Donc $\cos(\frac{2\pi}{mn}) = \cos(u\frac{2\pi}{n} + v\frac{2\pi}{m})$

$= \cos(u\frac{2\pi}{n})\cos(v\frac{2\pi}{m}) - \sin(u\frac{2\pi}{n})\sin(v\frac{2\pi}{m})$.

$\in \mathbb{E}$.

Ainsi on peut remarquer que l'ensemble des angles constructibles est un sous-groupe de $(\mathbb{R}, +)$.

Lemme: Soit n un entier naturel ≥ 2 tq $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ (facteurs premiers).

Alors le polygone à n côtés est constructibles ssi les polygones réguliers à $p_i^{\alpha_i}$ côtés le sont.

Preuve: Récurrence avec le Lemme précédent.

Proposition :

1) Pour $\alpha \in \mathbb{N}^*$, le polygone régulier à 2^α côtés est constructible

2) Soit p un nbre premier ≥ 3, $\alpha \in \mathbb{N}^*$. Le polygone régulier à p^α côtés est constructible si et seulement si $\alpha = 1$ et p est un nombre premier de Fermat i.e $p = 2^{2^N}+1$.

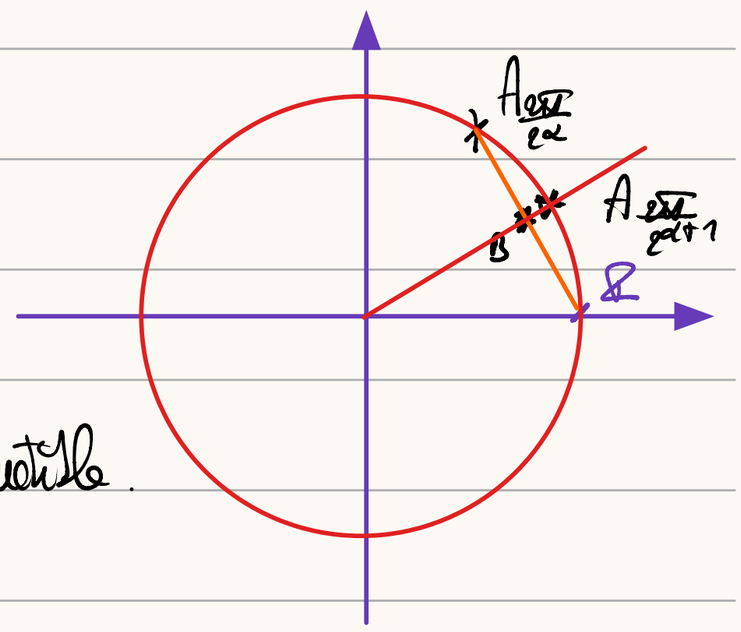
Preuve :

1) On procède par récurrence sur α.

- C'est clair pour $\alpha = 1$ car $\cos\left(\frac{2\pi}{2}\right) = -1 \in \mathbb{E}$
- C'est clair pour $\alpha = 2$ car $\cos\left(\frac{2\pi}{4}\right) = 0 \in \mathbb{E}$.
- Supposons la propriété vraie pour $\alpha \geq 2$, i.e $A_{\frac{2\pi}{2^\alpha}} = \left(\cos\left(\frac{2\pi}{2^\alpha}\right), \sin\left(\frac{2\pi}{2^\alpha}\right)\right)$ est constructible.

Ainsi le milieu de $[I, A_{\frac{2\pi}{2^\alpha}}]$, noté B, est constructible.

Et le point d'intersection entre le cercle et (OB) est $A_{\frac{2\pi}{2^{\alpha+1}}}$.



2)

$\Rightarrow$ On suppose le polygone régulier à p^α côtés constructible i.e $\cos\left(\frac{2\pi}{p^\alpha}\right)$ constructible.

Alors on sait qu'il existe $n \in \mathbb{N}$ tq :

$$[\mathbb{Q}(\cos(\tfrac{2\pi}{p^\alpha})) : \mathbb{Q}] = 2^n$$

Or par les extensions cyclotomiques :

$$[\mathbb{Q}(\cos(\tfrac{2\pi}{p^\alpha})) : \mathbb{Q}] = \frac{\varphi(p^\alpha)}{2} = \frac{1}{2}p^{\alpha-1}(p-1)$$

Ainsi on a :

$$2^n = p^{\alpha-1}\left(\frac{p-1}{2}\right). \text{ Ce qui donne } p^{\alpha-1}(p-1) = 2^{n+1}$$

Or si $\alpha \geq 2$, $p \mid p^{\alpha-1}(p-1)$ donc $p \mid 2^{n+1}$, absurde p impairs.

Ainsi $\alpha = 1$ et donc

$$p = 2^{n+1} + 1$$

Par un Lemme connue p est un nombre premier de Fermat.

$\Leftarrow$ réf : Ismann, Recatte, L'oral à l'agrég de maths, p219. (Idée de preuve)

On suppose qu'il existe $n \in \mathbb{N}$ tel que $p = 2^n + 1$, et on pose $\omega = e^{\frac{2i\pi}{p}}$ et $\mathbb{K} = \mathbb{Q}(\omega)$.

Alors $\cos(\frac{2\pi}{p}) \in \mathbb{Q}(\omega)$ et $[\mathbb{K} : \mathbb{Q}] = \varphi(p) = p - 1 = 2^q$.

Ainsi $\{\omega, \omega^2, \ldots, \omega^{p-1}\}$ est une base de $\mathbb{K}$ entant que $\mathbb{Q}$-espace vectoriel.

On s'intéresse donc à $G = Aut(\mathbb{K})$ (automorphisme de $\mathbb{K}$, $\mathbb{Q}$ linéaire) pour construire les corps intermédiaires

Étape 1 : $G \simeq (\mathbb{Z}/p\mathbb{Z})^\times$.

Soit $g \in G$ alors d'après la base B, g est entièrement déterminé par l'image de w.

De plus $\Phi_p(g(w)) = g(\Phi_p(w)) = g(0) = 0$.

Ainsi $g(w)$ est une racine primitive de l'unité donc il existe un unique $k \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que :

$$g(w) = w^k.$$

On définit ainsi un morphisme de groupe injectif :

$$\varphi : G \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$$
$$g \longmapsto k \text{ tq } g(w) = w^k$$

Il reste à montrer que φ est surjective.

Soit $k \in (\mathbb{Z}/p\mathbb{Z})^\times$ et construisons $g \in G$. Pour cela il suffit de définir g sur la base B, ainsi on définit g comme l'application $\mathbb{Q}$-linéaire tel que :

$$g(w^i) = w^{ik} \quad (\forall i \in [\![1, p-1]\!]).$$

Il est facile de vérifier que $g \in Aut(\mathbb{K}) = G$, ce qui donne la surjectivité de φ et que :

$$G \xrightarrow{\varphi} (\mathbb{Z}/p\mathbb{Z})^\times.$$

Étape 2 : Sous-corps intermédiaires.

Comme $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, G l'est aussi et on note g un tel générateur qui est donc d'ordre $p-1$.

Ainsi $B = \{w, g(w), \dots, g^{p-2}(w)\}$ est une $\mathbb{Q}$-base de $\mathbb{K}$.

On définit alors les sous-corps :

$$\mathbb{K}_i = \{z \in \mathbb{K} \mid g^i(z) = z\}.$$

On a $\mathbb{K}_0 = \{z \in \mathbb{K} \mid g(z) = z\} = \mathbb{Q}$ et $\mathbb{K}_i \subseteq \mathbb{K}_{i+1}$

$$\mathbb{K}_n = \{z \in \mathbb{K} \mid g^n(z) = g^{p-1}(z) = Id(z) = z\} = \mathbb{K}$$

Il reste à montrer que $[\mathbb{K}_{i+1} : \mathbb{K}_i] = l$ et les intersecter avec $\mathbb{R}$ pour avoir le résultat.

Z

Lemme : Soit $w_n = \exp\left(\frac{2i\pi l}{n}\right)$ une racine primitive n-ième de l'unité dans $\mathbb{C}$ (i.e $l \wedge n = 1$). Alors :

$$\mathbb{Q}\left(\cos\left(\frac{2i\pi l}{n}\right)\right) = \mathbb{Q}(w_n) \cap \mathbb{R}$$

et $\left[\mathbb{Q}\left(\cos\left(\frac{2i\pi l}{n}\right)\right) : \mathbb{Q}\right] = \frac{\varphi(n)}{2}$

Preuve : On sait que : $\cos\left(\frac{2i\pi\ell}{n}\right) = \frac{1}{2}(\omega_n + \overline{\omega_n}) = \frac{1}{2}\left(\omega_n + \frac{1}{\omega_n}\right)$ donc $\cos\left(\frac{2i\pi\ell}{n}\right) \in \mathbb{Q}(\omega_n)$.

donc $\mathbb{Q}\left(\cos\left(\frac{2i\pi\ell}{n}\right)\right) \subseteq \mathbb{Q}(\omega_n) \cap \mathbb{R}$.

- Soit $z \in \mathbb{Q}(\omega_n)$ alors $z \in \mathbb{R} \iff z = \overline{z} \iff z = \frac{1}{2}(z + \overline{z})$.

Or il existe $(a_0, \dots, a_{\varphi(n)-1}) \in \mathbb{Q}$ tq $z = a_0 + a_1\omega_n + \dots + a_{\varphi(n)-1}\omega_n^{\varphi(n)-1}$.

Ainsi :

$$z = \frac{1}{2}(z+\overline{z}) = a_0 + \frac{1}{2}a_1(\omega_n + \overline{\omega_n}) + \dots + \frac{1}{2}a_{\varphi(n)-1}\left(\omega_n^{\varphi(n)-1} + \overline{\omega_n}^{\varphi(n)-1}\right)$$

$$= \sum_{k=0}^{\varphi(n)-1} a_k \cos\left(k\frac{2i\pi\ell}{n}\right)$$

$$= \sum_{k=0}^{\varphi(n)-1} a_k T_k\left(\cos\left(\frac{2i\pi\ell}{n}\right)\right) \quad \text{où } T_k \text{ est le } k\text{-ième polynôme de Tchebichev.}$$

Ainsi $z \in \mathbb{Q}\left(\cos\left(\frac{2\ell i\pi}{n}\right)\right)$.

- On a :

$$\varphi(n) = \left[\mathbb{Q}(\omega_n) : \mathbb{Q}\right] = \left[\mathbb{Q}(\omega_n) : \mathbb{Q}(\cos(2i\pi\ell/n))\right]\left[\mathbb{Q}\left(\cos\left(\frac{2i\pi\ell}{n}\right)\right) : \mathbb{Q}\right].$$

On note $d = \left[\mathbb{Q}(\omega_n) : \mathbb{Q}\left(\cos\left(\frac{2i\pi\ell}{n}\right)\right)\right]$.

On sait que $\cos\left(\frac{2i\pi\ell}{n}\right) = \frac{1}{2}(\omega_n + \omega_n^{-1})$ ainsi ω_n est racine de :

$$X^2 - 2\cos\left(\frac{2i\pi\ell}{n}\right)X + 1$$

donc $d = 1$ ou 2.

$d = 1 \iff \omega_n \in \mathbb{R} \iff \frac{2\ell i\pi}{n} \in i\pi\mathbb{Z} \iff n \mid 2\ell \iff n \mid 2$ $(n \wedge \ell = 1)$.

Si $n \geq 3$, $d = 2$ d'où le résultat.

□

Lemme : Soit $q \in \mathbb{N}$ tq $2^q + 1$ premier alors $q = 0$ ou $q = 2^n$.

Preuve : Supposons $q \in \mathbb{N}^*$ et que q ne soit pas une puissance de 2 alors $q = k2^b$ avec $k \wedge 2 = 1$.

Ainsi $q = (2u+1)2^k$

Avec $\mathcal{D} = 2^{2^k}$ on a : $3 \leq \mathcal{D}+1 < 2^q + 1$ et

$$2^q + 1 = \mathcal{D}^{2a+1} - (-1)^{2a+1} = (\mathcal{D}+1)\sum_{i=0}^{2a}(-1)^i \mathcal{D}^{2a-i} \text{ donc } \mathcal{D}+1 \mid 2^q+1 \text{ d'où le résultat.}$$

□