

Pierre Lissy

May 2, 2010

Lemme 1. *Si x est un réel constructible, alors x est algébrique sur $\mathbb{Q}$ et le polynôme minimal est de degré une puissance de 2.*

Proof. Par hypothèse on a existence d'une suite de parties de $\mathbb{R}^2$ notées $A_0 \subset \dots \subset A_n$ telles que

1. $A_0 = \{0, I\}$
2. $(x, 0) \in A_n$
3. $A_i = A_{i-1} \cap M_i$ où le point M_i est constructible à une pas à partir de A_{i-1} .

On considère K_i le sous-corps de $\mathbb{R}$ engendré par $\mathbb{Q}$ et les coordonnées de points de A_i . Par définition $K_0 = \mathbb{Q}$ et $x \in K_n$.

Lemme 2. $[K_i : K_{i-1}]$ vaut 1, 2, 4.

Proof. On a $A_i = A_{i-1} \cap (x_i, y_i)$ donc $K_i = K_{i-1}[x_i, y_i]$. Mais par définition M_i est une intersection de droites ou de cercles, qui vérifient toutes les deux des équations de degré inférieur ou égal à 2 (une droite s'écrit $ax + by = c$, un cercle s'écrit $(x - a)^2 + (y - b)^2 = R^2$). De plus, les coefficients qui apparaissent (à savoir les a, b, c, R^2) sont nécessairement des éléments de K_{i-1} . Pour la droite, c'est le cas car a, b, c s'expriment juste avec les opérations $+, -, \cdot, /$ à partir des coordonnées de points de K_{i-1} où elles passent et ce dernier est un corps, pour le cercle le centre est dans K_{i-1} donc a et b sont dans K_{i-1} et R^2 s'exprime juste avec $+, \cdot$ en fonction des coordonnées de points de A_{i-1} . Donc c'est ok: le couple (x_i, y_i) vérifie une équation dans $K_{i-1}[X, Y]$ de degré inférieur ou égal à 2. Ainsi, par la relation $[K_{i-1}(x_i, y_i) : K_{i-1}] = [K_{i-1}(x_i, y_i) : K_{i-1}(x_i)][K_{i-1}(x_i) : K_{i-1}]$, et par le fait que $[K_{i-1}(x_i) : K_{i-1}]$ vaut 1 ou 2 (puisqu'en utilisant les deux équations qui déterminent x_i on va en remplaçant y_i dans l'une des expressions obtenir une expression polynomiale de degré 1 ou 2 en x_i à coef dans K_{i-1}) et que $[K_{i-1}(x_i, y_i) : K_{i-1}(x_i)]$ vaut aussi 1 ou 2 (car une fois que x_i est connu, on obtient une équation de y_i de degré 1 ou 2 à coefficients dans $K_{i-1}(x_i)$), d'où le résultat voulu. $\square$

On en déduit trivialement par récurrence par multiplicativité des degrés qu'à fortiori $[K_n : \mathbb{Q}]$ est une puissance de 2. Mais $\mathbb{Q}[x]$ est un sous-corps de K_n puisque $x \in K_n$. Il est donc de degré fini et encore par multiplicativité des degrés, comme $2^n = [K_n : \mathbb{Q}[x]][\mathbb{Q}[x] : \mathbb{Q}]$ on a nécessairement que le polynôme minimal est de degré une puissance de 2. $\square$

Corollaire 1. *On ne peut pas à partir du cube unité construire à la règle et au compas un cube ayant le double de volume*

Proof. On cherche un cube d'arête a tel que le volume du cube, à savoir a^3 , soit égal à 2. Autrement dit, $a = \sqrt[3]{2}$. Si l'on pouvait construire un tel cube, à fortiori on serait arrivé en considérant par exemple le plan xOy à construire le réel a . Mais ce réel n'est pas constructible. En effet, on remarque que a annule $X^3 - 2$. Il reste donc à voir si c'est bien le polynôme minimal de a . D'abord, le polynôme minimal de A ne peut être de degré 1 car $\sqrt[3]{2} \notin \mathbb{Q}$. Rappelons brièvement pourquoi. Si $\sqrt[3]{2} = p/q$ avec p et q premiers entre eux, alors $p^3 = 2q^3$, avec p et q premiers entre eux. Soit s un facteur premier de p . Alors c'est un facteur premier de p^3 donc il divise $2q^3$. Il ne peut diviser q^3 car sinon pour une question de valuation il diviserait q . Il divise donc 2 et vaut 2. Ainsi, le seul facteur premier de p est 2, ce qui signifie que p est une puissance de 2, ie $p = 2^n$, avec $n \leq 1$ (car on ne peut avoir $p = 1$). Mais alors $q = 2^{n-1}$ et p et q ne sont premiers entre eux que si $q = 1$, dans ce cas $p^3 = 2$ avec p entier, ce n'est pas possible. Ainsi, le polynôme minimal est de degré 2 ou 3. Mais si il était de degré 2, alors sachant qu'il diviserait

$X^3 - 2 = (X - a)(X - ja)(X - j^2a)$, alors il vaudrait soit $(X - a)(X - ja)$, soit $(X - a)(X - j^2a)$, soit $(X - ja)(X - j^2a)$. Les deux premiers ne sont pas possible car le terme constant est complexe non réel. Le troisième n'est pas possible car le terme en X vaut au signe près $2a\cos(2\pi/3) = a$ dont on vient de montrer qu'il n'était pas rationnel. Ainsi le polynôme minimal de a sur $\mathbb{Q}$ est de degré 3 et donc a n'est pas constructible. $\square$

Corollaire 2. *Impossibilité de la trisection de l'angle: on ne peut pas couper à la règle et au compas l'angle $2\pi/3$ en 3 parties d'angles égaux.*

Proof. Si c'était le cas, alors notamment en faisant l'intersection du cercle unité (qui est constructible) et de la première droite trisectant l'angle on arriverait à atteindre le point de coordonnées $\cos(\pi/9), \sin(\pi/9)$, autrement dit on aurait construit à la règle et au compas notamment le réel $\cos(\pi/9) = x$. Mais on connaît la formule suivante : $\cos(3\theta) = 4\cos^3(\theta) - 3\cos\theta$. Ainsi, $\cos(3x) = \cos(\pi/3) = 1/2 = 4x^3 - 3x^2$, ce qui implique que x admet pour annulateur le polynôme à coefficients entiers $8x^3 - 6x^2 - 1$. On réduit modulo 5 ce polynôme pour obtenir $3x^3 - x^2 - 1$, qui est irréductible car si il était réductible il admettrait une racine dans F_5 , ce qui n'est pas le cas on le vérifie aisément. $\square$