Recasages possibles : 125, 127, 148, 191
Référence : Théorie de Galois, Gozard (p. 50-54) ; Cours d'algèbre, Perrin (p. 68-70).

Développement

Soit $\mathbb{E}$ le sous-corps de $\mathbb{R}$ des nombres constructibles.

Lemme 1 $\mathbb{E}$ est stable par racine carrée : $x \in \mathbb{E} \Rightarrow \sqrt{x} \in \mathbb{E}$.

Lemme 2 Soit $\{O, I\} = A_0 \subset \cdots \subset A_n$ une suite de parties de $\mathbb{R}^2$ telles que pour tout $i \in [\![0, n-1]\!]$, $A_{i+1} = A_i \cup \{M_{i+1}\}$ où $M_{i+1} = (x_{i+1}, y_{i+1})$ est un point constructible en un pas à partir de A_i. Si on note $K_i = \mathbb{Q}\big((x_j, y_j)_{j \leqslant i}\big)$, alors pour tout $i \in [\![0, n-1]\!]$, $[K_{i+1} : K_i] \in \{1, 2\}$.

Théorème 3 (Wantzel) Soit $x \in \mathbb{R}$. Alors, x est constructible si et seulement s'il existe une suite finie $L_1 \subset \cdots \subset L_p$ de sous-corps de $\mathbb{R}$ telle que $L_0 = \mathbb{Q}$, $x \in L_p$ et $[L_{i+1} : L_i] = 2$ pour tout $i \in [\![0, p-1]\!]$.

Corollaire 4 Si x est un réel constructible, alors $[\mathbb{Q}(x) : \mathbb{Q}] = 2^d$, avec $d \in \mathbb{N}$.

Corollaire 5 (Duplication du cube) Il n'est pas possible en général, à partir d'un cube donné, de construire à la règle et au compas l'arête d'un cube de volume double.

Corollaire 6 (Trisection de l'angle) Il n'est pas possible en général de trisecter un angle à la règle et au compas.

- *Preuve du Lemme 1* : Soit $x \in \mathbb{E}$. On veut construire un point $M = (x_M, y_M)$ dont l'abscisse ou l'ordonnée vaut $\sqrt{x}$. Par définition, les points $A = (x, 0)$ et $B = (x, x)$ sont constructibles, soit donc $\mathcal{D}$ la droite (AB). Comme $\mathbb{E}$ est un corps, le point $\Omega = (\frac{x+1}{2}, 0)$ est constructible. Notons $\mathcal{C}$ le cercle de centre Ω et de rayon $\left\|\overrightarrow{O\Omega}\right\| = \frac{x+1}{2}$. La droite $\mathcal{D}$ intersecte le cercle $\mathcal{C}$ en deux points, notons $M = (x_M, y_M)$ celui d'ordonnée positive. Alors, dans le triangle ΩAM rectangle en A, le théorème de Pythagore donne l'égalité $y_M^2 = \left(\frac{x+1}{2}\right)^2 - \left(x - \frac{x+1}{2}\right)^2 = x$. On obtient bien $y_M = \sqrt{x}$, et comme M est constructible, $\sqrt{x} \in \mathbb{E}$.

- *Preuve du Lemme 2* : Fixons $i \in [\![0, n-1]\!]$. On a $K_{i+1} = K_i(x_{i+1}, y_{i+1})$ par définition. Plusieurs cas se présentent :

  · Si M_{i+1} est l'intersection de deux droites $\mathcal{D}_1$ et $\mathcal{D}_2$ distinctes passant par des points de A_i, alors ses coordonnées vérifient un système de la forme

  $$\begin{cases} ax_{i+1} + by_{i+1} + c &= 0 \quad \text{(équation de } \mathcal{D}_1\text{)} \\ a'x_{i+1} + b'y_{i+1} + c' &= 0 \quad \text{(équation de } \mathcal{D}_2\text{)} \end{cases}$$

  avec $a, b, c, a', b', c' \in K_i$. Ainsi, en résolvant ce système (qui est de Cramer car les droites ne sont pas parallèles), on obtient $x_{i+1}, y_{i+1} \in K_i$ et donc $[K_{i+1} : K_i] = 1$.

  · Si M_{i+1} est une intersection d'une droite $\mathcal{D}$ et d'un cercle $\mathcal{C}$ construits à partir de points de A_i, alors ses coordonnées vérifient un système de la forme

  $$\begin{cases} ax_{i+1} + by_{i+1} + c &= 0 \quad \text{(équation de } \mathcal{D}\text{)} \\ (x_{i+1} - a')^2 + (y_{i+1} - b')^2 + c' &= 0 \quad \text{(équation de } \mathcal{C}\text{)} \end{cases}$$

  avec $a, b, c, a', b', c' \in K_i$. Alors, en supposant quitte à échanger a et b que $b \neq 0$, on peut exprimer y_{i+1} en fonction de x_{i+1} dans la première égalité ce qui montre que $K_{i+1} = K_i(x_{i+1})(y_{i+1}) = K_i(x_{i+1})$. En injectant cette expression dans la deuxième égalité, on voit que x_{i+1} est solution d'une équation polynômiale de degré 2 à coefficients dans K_i, donc $[K_i(x_{i+1}) : K_i] \leqslant 2$. Ainsi, on a bien $[K_{i+1} : K_i] \leqslant 2$, *i.e* $[K_{i+1} : K_i] \in \{1, 2\}$.

  · Enfin si M_{i+1} est une intersection de deux cercles $\mathcal{C}_1$ et $\mathcal{C}_2$ distincts construits à partir de points de A_i, alors ses coordonnées vérifient un système de la forme

  $$\begin{cases} (x_{i+1} - a)^2 + (y_{i+1} - b)^2 + c &= 0 \quad \text{(équation de } \mathcal{C}_1\text{)} \\ (x_{i+1} - a')^2 + (y_{i+1} - b')^2 + c' &= 0 \quad \text{(équation de } \mathcal{C}_2\text{)} \end{cases}$$

  avec $a, b, c, a', b', c' \in K_i$. En soustrayant la deuxième équation à la première, on voit que les coordonées de M_{i+1} vérifient le système :

  $$\begin{cases} 2(a' - a)x + 2(b' - b)y + (c - c' + a^2 - a'^2 + b^2 - b'^2) &= 0 \\ (x_{i+1} - a')^2 + (y_{i+1} - b')^2 + c' &= 0 \end{cases}$$

  Or, on a $(a' - a, b' - b) \neq (0, 0)$ car sinon, $c = c'$ et donc $\mathcal{C}_1 = \mathcal{C}_2$ ce qui est exclu. Ainsi, on s'est ramenés au cas précédent, et donc on a toujours $[K_{i+1} : K_i] \in \{1, 2\}$.

- *Preuve du Théorème 3* :

($\Rightarrow$) Supposons x constructible, c'est-à-dire $M = (x, 0)$ constructible. Par définition, il existe $M_1, \dots, M_n$ des points du plan tels que $M_n = M$ et, en notant $A_0 = \{O, I\}$ et pour $i \in [\![0, n-1]\!]$, $A_{i+1} = A_i \cup \{M_{i+1}\}$, on ait que M_{i+1} est constructible en un pas à partir de A_i. Notons $K_0 = \mathbb{Q}$ et pour $i \in [\![1, n]\!]$, $M_i = (x_i, y_i)$ et $K_i = \mathbb{Q}(x_1, y_1, \dots, x_i, y_i)$. Remarquons que $x = x_n \in K_n$. Alors, on se retrouve exactement dans les conditions du **Lemme 2**, et donc on a nécessairement $[K_{i+1} : K_i] \in \{1, 2\}$ pour tout $i \in [\![0, n-1]\!]$. Il nous suffit donc d'extraire de cette suite de corps une suite $(L_0, \dots, L_p)$ en ne gardant que les K_i qui sont quadratiques sur K_{i-1}. On a bien sûr $L_0 = \mathbb{Q}$, $x \in L_p = K_n$, et par choix des L_i, on a bien $[L_{i+1} : L_i] = 2$ pour tout $i \in [\![0, p-1]\!]$.

($\Leftarrow$) Supposons qu'il existe une suite finie $L_1 \subset \cdots \subset L_p$ de sous-corps de $\mathbb{R}$ telle que $L_0 = \mathbb{Q}$, $x \in L_p$ et $[L_{i+1} : L_i] = 2$ pour tout $i \in [\![0, p-1]\!]$. On souhaite montrer que $x \in \mathbb{E}$, ou plus généralement que $L_p \subset \mathbb{E}$. Montrons par récurrence finie sur $j \in [\![0, p]\!]$ que $L_j \subset \mathbb{E}$:

- $L_0 = \mathbb{Q} \subset \mathbb{E}$
- Supposons que $L_j \subset \mathbb{E}$ pour un $j \in [\![0, p-1]\!]$. Soit $y \in L_{j+1}$. Comme $[L_{j+1} : L_j] = 2$, la famille $(1, y, y^2)$ est liée sur L_j, donc il existe $a, b, c \in L_j$ non tous nuls tels que $ay^2 + by + c = 0$. Si $a = 0$, alors $b \neq 0$ (sinon $c = 0$ et on aurait $a = b = c = 0$ ce qui est exclu), et on a $y = -\frac{c}{b} \in L_j \subset \mathbb{E}$. Sinon, $a \neq 0$ et donc y est racine du trinôme du second degré $aX^2 + bX + C$. Comme $y \in \mathbb{R}$, le discriminant $\Delta = b^2 - 4ac$ de ce trinôme est positif, et on a $y \in \{\frac{-b \pm \sqrt{\Delta}}{2a}\}$. Or, $a, b, c \in L_j \subset \mathbb{E}$, donc $\Delta \in \mathbb{E}$ car $\mathbb{E}$ est un corps et d'après le **Lemme 1**, $\sqrt{\Delta} \in \mathbb{E}$. À nouveau puisque $\mathbb{E}$ est un corps, on obtient $y \in \mathbb{E}$. Ceci étant valable pour tout $y \in L_{j+1}$, on obtient bien $L_{j+1} \subset \mathbb{E}$, ce qui achève la récurrence.

En particulier, on obtient que $L_p \subset \mathbb{E}$, et donc que $x \in \mathbb{E}$.

- *Preuve du Corollaire 4* : Soit $x \in \mathbb{E}$. D'après le **Théorème 4**, il existe une suite finie $\mathbb{Q} = L_0, \dots, L_p$ de sous-corps de $\mathbb{R}$ tels que $x \in L_p$ et pour tout $i \in [\![0, p-1]\!]$, $[L_{i+1} : L_i] = 2$. D'après le théorème de la base télescopique, on a $[L_p : \mathbb{Q}] = \prod_{i=0}^{p-1} [L_{i+1} : L_i] = 2^p$. Or, comme $x \in L_p$, on a $\mathbb{Q}(x) \subset L_p$ et donc par le même théorème, $[L_p : \mathbb{Q}] = [L_p : \mathbb{Q}(x)][\mathbb{Q}(x) : \mathbb{Q}]$. Ainsi, $[\mathbb{Q}(x) : \mathbb{Q}]$ divise $[L_p : \mathbb{Q}] = 2^p$, d'où l'existence de $d \in \mathbb{N}$ tel que $[\mathbb{Q}(x) : \mathbb{Q}] = 2^d$.

- *Preuve du Corollaire 5* : Soit a la longueur de l'arête du cube de départ. Pour obtenir un cube de volume double, il faut constuire une arête de longueur $a\sqrt[3]{2}$. Or, montrons que le nombre $\sqrt[3]{2}$ n'est pas constructible. Le polynôme $X^3 - 2$ de $\mathbb{Z}[X]$ annule $\sqrt[3]{2}$ et est irréductible d'après le critère d'Eisenstein appliqué avec le nombre premier 2. Ainsi, c'est le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbb{Q}$, et donc $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ n'est pas une puissance de 2, donc d'après le **Corollaire 4**, $\sqrt[3]{2}$ n'est pas constructible. En particulier, il n'est pas possible de dupliquer à la règle et au compas un cube d'arête 1.

- *Preuve du Corollaire 6* : Trissecter l'angle $\frac{\pi}{3}$ revient à construire le réel $\cos(\frac{\pi}{9})$. Or, en utilisant la formule trigonométrique $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$, on obtient $\frac{1}{2} = \cos(\frac{\pi}{3}) = 4\cos^3(\frac{\pi}{9}) - 3\cos(\frac{\pi}{9})$, donc $\cos(\frac{\pi}{9})$ est annulé par le polynôme $8X^3 - 6X - 1 \in \mathbb{Z}[X]$. La réduction de ce polynôme dans $\mathbb{F}_5[X]$ n'admet aucune racine dans $\mathbb{F}_5$, donc est irréductible sur $\mathbb{F}_5$ (car de degré 3), donc est irréductible sur $\mathbb{Q}$ d'après le critère par réduction. Ainsi, $[\mathbb{Q}(\cos(\frac{\pi}{9}) : \mathbb{Q}] = 3$ n'est pas une puissance de 2, et donc d'après le **Corollaire 4**, $\cos(\frac{\pi}{9})$ n'est pas constructible.