

Impossibilité de la duplication du cube, de la quadrature du disque et de la trisection de l'angle.

L'étude de ces trois célèbres problèmes de constructions géométriques à la règle et au compas nécessite quelques préliminaires algébriques. J'ai essayé de les réduire autant que possible et de revenir au plus vite aux problèmes qui nous intéressent.

I. Quelques éléments de théorie des corps.

Dans toute cette partie, on se place dans un corps commutatif \mathbb{K} . Pour fixer les idées, on pourra supposer que \mathbb{K} est \mathbb{R} ou \mathbb{C} . En fait, pour étudier nos problèmes de construction, nous nous placerons dans \mathbb{R} .

Nous allons nous intéresser dans ces préliminaires aux sous-corps de \mathbb{K} , c'est à dire aux parties de \mathbb{K} qui sont stables par produits, par inverses, et par différences. Par restrictions des opérations de \mathbb{K} , tout sous-corps de \mathbb{K} est muni d'une structure de corps. Commençons par cette première remarque :

PROPOSITION 1 : *Soit K et L deux sous-corps de \mathbb{K} tels que $K \subset L$. Alors L est naturellement muni d'une structure de K -espace vectoriel par restriction de l'addition et de la multiplication dans \mathbb{K} .*

PREUVE : On définit sur L la multiplication externe suivante :

$$\begin{aligned} K \times L &\longrightarrow L \\ (\lambda, u) &\longmapsto \lambda \cdot u \end{aligned}$$

où \cdot désigne le produit dans \mathbb{K} . Comme L est un sous-corps de \mathbb{K} contenant K , cette multiplication externe est bien définie. Il est ensuite facile de vérifier que L muni de son addition (L est un corps) et de cette multiplication externe vérifie les axiomes de définition des K -espaces vectoriels. \square

Nous nous intéresserons particulièrement au cas où L est un K -espace vectoriel de dimension finie, et nous utiliserons la notation suivante :

NOTATION : Soit $K \subset L$ deux sous-corps de \mathbb{K} tel que L soit un K -espace vectoriel de dimension finie. On note alors $[L : K]$ cette dimension.

Nous sommes en mesure maintenant d'énoncer un des deux résultats de théorie des corps dont nous avons besoin pour étudier notre problème :

PROPOSITION 2 : *Soit $K \subset L \subset E$ trois sous-corps de \mathbb{K} tels que E soit de dimension finie sur K . Alors L est de dimension finie sur K , E est de dimension finie sur L et on a l'identité suivante :*

$$[E : K] = [E : L] \times [L : K].$$

PREUVE : E est de dimension finie sur K et L est un sous K -espace vectoriel de E , donc L est de dimension finie sur K . De plus, toute famille génératrice de E en tant que K -espace vectoriel est

à fortiori une famille génératrice de E en tant que L -espace vectoriel. Par conséquent, E est un L -espace vectoriel de dimension finie.

On peut donc considérer $(u_i)_{1 \leq i \leq n}$ une base de L en tant que K -espace vectoriel et $(e_j)_{1 \leq j \leq m}$ une base de E en tant que L -espace vectoriel. On vérifie alors sans difficulté que la famille $(u_i \cdot e_j)_{1 \leq i \leq n; 1 \leq j \leq m}$ est une famille libre et génératrice de E en tant que K -espace vectoriel. \square

NOTATION : Soit K un sous-corps de \mathbb{K} et $(\alpha_1, \dots, \alpha_n)$ des éléments de \mathbb{K} . Nous notons $K(\alpha_1, \dots, \alpha_n)$ le plus petit sous-corps de \mathbb{K} qui contient à la fois K et tous les α_i . Ce sous-corps existe : c'est l'intersection de tous les sous-corps de \mathbb{K} qui contiennent K et les α_i .

PROPOSITION 3 : Soit K un sous-corps de \mathbb{K} et α un élément de \mathbb{K} n'appartenant pas à K . Supposons que α est racine d'un polynôme P à coefficients dans K de degré 2 ou 3 qui ne possède pas de racines dans K . Alors la dimension $[K(\alpha) : K]$ est égale au degré de P .

PREUVE : Par souci de concision, je ne donne ici que la démonstration du cas où P est de degré 3. Si le degré est 2, on peut suivre pas à pas la démonstration ci-dessous (elle se simplifie un peu) ; on peut également travailler à la main.

Comme $K(\alpha)$ est un K -espace vectoriel contenant 1 , α et α^2 , il contient le sous K -espace vectoriel L de \mathbb{K} engendré par 1 , α et α^2 . Nous nous proposons de montrer que $K(\alpha) = L$.

Montrons dans un premier temps que L est de dimension 3 sur K . Si ce n'est pas le cas, il existe λ et μ dans K tels que $\alpha^2 + \lambda\alpha + \mu = 0$. On peut alors considérer la division euclidienne de P par le polynôme $X^2 + \lambda X + \mu$:

$$P = (X^2 + \lambda X + \mu)Q + R$$

Les polynômes R et Q sont à coefficients dans K . De plus Q est de degré 1 et R de degré inférieur ou égal à 1. Comme α est une racine de P et $X^2 + \lambda X + \mu$, c'est aussi une racine de R . Mais α n'appartient pas à K , donc $R = 0$. Q est alors un polynôme de degré 1 à coefficients dans K qui nous fournit une racine de P dans K , ce qui est contraire à l'hypothèse. Par conséquent, L est de dimension 3.

Montrons maintenant que $K(\alpha) = L$. On vérifie facilement que $K(\alpha)$ est stable par produits et par différences. Il reste donc à voir que L est stable par inverse. Soit a_0 , a_1 et a_2 trois éléments non tous nuls de K . Nous allons montrer que l'inverse de $a_2\alpha^2 + a_1\alpha + a_0$ appartient à L . Pour cela, on considère le polynôme $a_2X^2 + a_1X + a_0$ et on fait la division euclidienne de P par ce polynôme :

$$P = Q_0(a_2X^2 + a_1X + a_0) + R_0.$$

Par le même argument que précédemment, le reste R_0 n'est pas nul, car sinon P posséderait une racine dans K . On peut donc faire la division euclidienne par R_0 :

$$a_2X^2 + a_1X + a_0 = Q_1R_0 + R_1$$

Tous les polynômes Q_0 , R_0 , Q_1 et R_1 sont à coefficients dans K . De plus R_1 est une constante et $d^\circ R_0 \leq 1$. Deux cas peuvent se présenter : soit R_1 est une constante non nulle de K , soit R_1 est nulle. Dans le premier cas, on vérifie que :

$$\frac{1}{R_1}(1 + Q_1(\alpha)Q_0(\alpha))$$

est l'inverse de $a_2\alpha^2 + a_1\alpha + a_0$. Dans le deuxième cas, R_1 est nulle, donc R_0 divise P . Mais comme P ne possède pas de racine dans K , R_0 ne peut pas être de degré 1. Par conséquent, R_0 est une constante non nulle de K . Mais alors, $\frac{1}{R_0}Q_0(\alpha)$ est l'inverse cherché. \square

II. Nombres constructibles à la règle et au compas.

Commençons dans un premier temps par définir la notion de point constructible à la règle et au compas à partir d'un sous-ensemble du plan affine euclidien que l'on identifie à \mathbb{R}^2 après l'avoir rapporté à un repère orthonormé.

DÉFINITIONS : Points traçables et constructibles à partir d'une partie.

Soit \mathcal{E} une partie de \mathbb{R}^2 .

- 1-) Je dirais qu'un cercle de \mathbb{R}^2 est traçable à partir de \mathcal{E} si son centre appartient à \mathcal{E} et son rayon est la distance entre deux points de \mathcal{E} .
- 2-) Je dirais qu'une droite est traçable à partir de \mathcal{E} si elle passe par deux points distincts de \mathcal{E} .
- 3-) Je dirais qu'un point est traçable à partir de \mathcal{E} si c'est l'intersection de deux cercles, de deux droites ou d'une droite et d'un cercle traçables à partir de \mathcal{E} .
- 4-) Un point M est constructible à partir de \mathcal{E} si il existe une chaîne finie de points M_1, \dots, M_n telle que :

M_1 appartient à \mathcal{E} ,

$M_n = M$,

pour tout i , M_{i+1} est traçable à partir de $\mathcal{E} \cup \{M_1, \dots, M_i\}$.

- 5-) Un nombre réel α est dit être constructible si le point $(\alpha, 0)$ est constructible à partir de des points $(0, 0)$ et $(1, 0)$.

Nous pouvons remarquer que les nombres rationnels sont constructibles. Nous avons même vu que l'ensemble des nombres constructibles est un sous-corps de \mathbb{R} qui est stable par racine carré.

C'est le théorème suivant qui va nous permettre de répondre négativement à nos trois problèmes de construction.

THÉORÈME DE WANTZEL (1837) : *Soit α un nombre réel constructible. Alors $\mathbb{Q}(\alpha)$ est un \mathbb{Q} -espace vectoriel de dimension une puissance finie de 2.*

PREUVE : Soit n un entier naturel. On considère $M_1(x_1, y_1), \dots, M_n(x_n, y_n)$ une chaîne de n points tels que M_1 soit $O(0, 0)$ ou $I(1, 0)$ et tels que $M_i(x_i, y_i)$ soit traçable à partir de $\{O, I, \dots, M_{i-1}\}$. Notons L le plus petit sous-corps de \mathbb{R} qui contient les coordonnées de tous les points M_i .

Nous allons montrer par récurrence sur n que L est un \mathbb{Q} -espace vectoriel de dimension une puissance finie de 2. Nous aurons alors montré le théorème, puisque nous aurons montré que si α est un nombre réel constructible alors $\mathbb{Q}(\alpha)$ est contenu dans un sous-corps L de dimension sur \mathbb{Q} une puissance finie de 2. Une application directe de la proposition 2 nous permettra alors de conclure.

Revenons donc à notre récurrence. Elle est trivialement initialisée pour $n = 1$, puisque $K = \mathbb{Q}$ (M_1 est O ou I). Soit $n \geq 2$ un entier naturel. Supposons que la propriété de dimension est vraie pour une chaîne de $n - 1$ points.

Considérons une chaîne de n points, M_1, \dots, M_n , tel que M_1 soit O ou I et M_i soit traçable à partir de $\{O, I, \dots, M_{i-1}\}$. Soit K le plus petit sous-corps de \mathbb{R} contenant les coordonnées de tous les M_i pour $1 \leq i \leq n - 1$ et $L = K(x_n, y_n)$, celui qui contient en plus les coordonnées de M_n . Alors, par hypothèse de récurrence, $[K : \mathbb{Q}]$ est une puissance finie de 2. Nous allons montrer que $[L : K]$ est de 2 ou 1. La proposition 2 nous permettra alors de conclure que $[L : \mathbb{Q}]$ est une puissance finie de 2.

Remarquons que M_n est un point traçable à partir de l'ensemble des points à coordonnées dans K . Par conséquent, on est dans un des trois cas suivant :

• M_n est l'intersection de deux droites passant par deux points à coordonnées dans K . Dans ce cas, il n'est pas difficile de voir que ces droites ont des équations cartésiennes à coefficients dans K . Par conséquent, leur point d'intersection est à coordonnée dans K et par conséquent $L = K$.

• M_n est l'intersection d'un cercle, dont les coordonnées du centre et le rayon appartiennent à K , et d'une droite passant par deux points à coordonnées dans K . Donc (x_n, y_n) est solution d'un système d'équations :

$$\begin{cases} ax + by + c = 0 \\ (x - d)^2 + (y - e)^2 - r^2 \end{cases}$$

où a, b, c, d, e et r appartiennent à K . De plus, a et b ne sont pas simultanément nuls, on peut donc supposer par exemple que b est non nul. On peut donc écrire $y_n = \lambda x_n + \mu$ avec λ et μ dans K . En substituant y_n par cette expression dans l'équation du cercle, on en déduit que x_n est racine d'un polynôme de degré 2 à coefficients dans K . Soit ce polynôme possède des racines dans K et auquel cas x_n et y_n sont dans K et $L = K$. Soit ce polynôme ne possède pas de racine dans K et alors, $K(x_n, y_n) = K(x_n)$ est d'après la proposition 2 de dimension 2 sur K . Ceci nous permet de conclure ce cas. Reste le troisième cas :

• M_n est l'intersection de deux cercles dont les coordonnées des centres et les rayons appartiennent à K . Donc (x_n, y_n) est solution d'un système :

$$\begin{cases} (x - a)^2 + (y - b)^2 - r^2 \\ (x - c)^2 + (y - d)^2 - s^2 \end{cases}$$

où a, b, c, d, r, s appartiennent à K . On peut alors écrire $(x - a)^2$ sous la forme $(x - c)^2 + \lambda(x - c) + \mu$ et $(y - b)^2$ sous la forme $(y - d)^2 + \lambda'(y - d) + \mu'$, avec λ, λ', μ et μ' dans K . En soustrayant alors les deux équations du système, on obtient un système équivalent de la forme :

$$\begin{cases} \lambda(x - c) + \lambda'(y - d) + \mu + \mu' - r^2 \\ (x - c)^2 + (y - d)^2 - s^2 \end{cases}$$

ce qui nous ramène au cas précédent : M_n est un point d'intersection d'un cercle et d'une droite traçables à partir de K . \square

III. Impossibilité des trois problèmes de construction.

Nous pouvons maintenant montrer que la quadrature du disque, la duplication du cube et la trisection d'un angle quelconque sont des problèmes de construction impossibles à réaliser à la règle et au compas.

QUADRATURE DU DISQUE.

Pour justifier l'impossibilité de la quadrature du disque, j'admettrai le résultat suivant :

THÉORÈME DE LINDEMANN (1882) : π n'est racine d'aucun polynôme à coefficient rationnel (autrement dit π est transcendant sur \mathbb{Q}). \square

COROLLAIRE : La quadrature du disque est impossible à la règle et au compas.

PREUVE : Supposons qu'il est possible de construire un carré d'aire π à partir de O et I . Le nombre $\sqrt{\pi}$ est alors constructible à la règle et au compas, et par conséquent π est également constructible. On déduit donc du théorème de Wantzel que $\mathbb{Q}(\pi)$ est un \mathbb{Q} -espace vectoriel de dimension finie,

mettons n . Par conséquent la famille $1, \pi, \dots, \pi^n$ est liée sur \mathbb{Q} , et par conséquent π est racine d'un polynôme de degré n . \square

DUPLICATION DU CUBE.

Construire un cube de volume 2 revient à construire la longueur d'un de ses cotés, donc $\sqrt[3]{2}$. Montrons dans un premier temps que $X^3 - 2$ ne possède pas de racine dans \mathbb{Q} .

PROPOSITION 3 : *Le polynôme $X^3 - 2$ ne possède pas de racine rationnelle.*

PREUVE : Supposons qu'une fraction irréductible $\frac{p}{q}$ soit une racine de $X^3 - 2$. Alors $p^3 = 2q^3$. Comme p et q sont premiers entre eux, p est un entier pair $2m$. Mais alors, $2^2m^3 = q^3$, et par conséquent q est pair, ce qui est contradictoire avec le fait que p et q sont premiers entre eux. \square

COROLLAIRE : $\sqrt[3]{2}$ n'est pas constructible à la règle et au compas.

PREUVE : D'après la proposition 3, $\mathbb{Q}(\sqrt[3]{2})$ est de dimension 3 sur \mathbb{Q} . Le théorème de Wantzel nous permet alors de conclure. \square

TRISECTION DE $\frac{\pi}{3}$.

L'angle $\frac{\pi}{3}$ est constructible puisque son cosinus $\frac{1}{2}$ l'est. Nous nous proposons de montrer que $\frac{\pi}{9}$ n'est pas trisectable. Construire une trisection de $\frac{\pi}{3}$ revient à construire $\cos \frac{\pi}{9}$. Or :

$$\cos(3\frac{\pi}{9}) = 4 \cos^3 \frac{\pi}{9} - 3 \cos \frac{\pi}{9} = \frac{1}{2}$$

Le cosinus de $\frac{\pi}{9}$ est donc racine du polynôme $8X^3 - 6X - 1$. Montrons que ce polynôme ne possède pas de racine dans \mathbb{Q} . Pour cela, procédons par l'absurde. Tout d'abord, 0 n'est pas racine de ce polynôme. Supposons qu'une fraction irréductible $\frac{p}{q}$ soit une racine de $8X^3 - 6X - 1$. On aurait alors :

$$(8p^2 - 6q^2)p = q^3.$$

Donc p est un diviseur de q^3 . Comme p et q sont premiers entre eux, ceci nous impose $p = 1$ et $q(q^2 + 6q) = 8$ avec $q \in \mathbb{Z}^*$. De la deuxième identité, on déduit que comme q divise 8, q est au signe près 1, 2, 4 ou 8. On vérifie alors que ces 8 cas sont impossibles.

COROLLAIRE : $\cos \frac{\pi}{9}$ n'est pas constructible, et par conséquent, $\frac{\pi}{3}$ n'est pas trisectable à la règle et au compas.

PREUVE : D'après la proposition 2, $\mathbb{Q}(\cos \frac{\pi}{9})$ est de dimension 3 sur \mathbb{Q} . Ce n'est pas une puissance finie de 2. Le théorème de Wantzel nous permet alors de conclure. \square