Contructions à la règle et au compas.

Par Nicolas Lanchier [1]

1 Le corps des réels constructibles.

Définition 1.1 — Soient E un ensemble de points du plan, D_E l'ensemble des droites du plan passant par deux points distincts de E et C_E la collection des cercles du plan de centre un point de E et de rayon la distance entre deux points de E. Un point du plan est dit constructible en une étape à partir de E s'il est à l'intersection

1. de deux droites de D_E
2. de deux cercles de C_E
3. ou d'une droite de D_E et d'un cercle de C_E.

Définition 1.2 — Un point P est dit constructible (en n étapes) à partir de E s'il existe une suite de points $P_1,\ P_2,\ \ldots,\ P_n$ tels que pour tout $1 \leq i \leq n$, P_i soit constructible en une étape à partir de $E \cup \{P_j\,;\, j < i\}$, avec $P_n = P$.

Dans toute la suite, on supposera que $E = \{O, I\}$, où $O = (0, 0)$ et où $I = (1, 0)$.

Définition 1.3 (réel constructible) — Un réel x est dit constructible si le point de coordonnées $(x, 0)$ est constructible à la règle et au compas.

Proposition 1.4 — L'ensemble des réels constructibles est un sous-corps de $\mathbb{R}$ stable par racine carrée. En particulier, les rationnels sont constructibles. [1], Sect. 2.13

Preuve — Sachant qu'il est possible de tracer la parallèle à une droite passant par un point donné du plan, la structure de corps des réels constructibles est assurée par le théorème de Thalès. La stabilité par racine carrée est quant à elle donnée par le théorème de Pythagore. Enfin, la constructibilité des rationnels résulte du simple fait que $\mathbb{Q}$ est le plus petit sous-corps de $\mathbb{R}$. □

2 Condition nécessaire de constructibilité.

Théorème 2.1 — Un réel x est constructible si et seulement s'il existe une suite $K_0,\ K_1,\ \ldots,\ K_n$ de sous-corps de $\mathbb{R}$ tels que $K_0 = \mathbb{Q}$, $[K_i : K_{i-1}] = 2$ et $x \in K_n$. [1], Sect. 2.22

Preuve — La condition suffisante est une conséquence simple de la stabilité des réels constructibles par racine carrée. Pour établir la réciproque, considérons un réel x constructible. Par hypothèse, il existe une suite croissante $A_0 \subset \cdots \subset A_n$ de parties de $\mathbb{R}^2$ telles que (i) $A_0 = \{O, I\}$, (ii) $A_i = A_{i-1} \cup \{P_i\}$ avec P_i constructible en une étape à partir de A_{i-1} et (iii) $(x, 0) \in A_n$. Notons alors K_i le corps engendré par les coordonnées des points de A_i de sorte que $K_0 = \mathbb{Q}$ et $x \in K_n$. Les équations de droites ou de cercles étant de degré ≤ 2, il est facile de montrer que $[K_i : K_{i-1}] \leq 2$. En particulier, quitte à extraire une sous-suite, on peut supposer que $[K_i : K_{i-1}] = 2$ ce qui établit la condition nécessaire. □

Corollaire 2.2 — L'ensemble des réels constructibles est le plus petit sous-corps de $\mathbb{R}$ stable par racine carrée. [1], Sect. 3.1

Théorème 2.3 (Wantzel) — Tout réel constructible est algébrique sur $\mathbb{Q}$ de degré une puissance de 2. [1], Sect. 2.22

PREUVE — C'est une conséquence immédiate du théorème 2.1 et de la formule de multiplicativité des degrés $[K_n : \mathbb{Q}] = [K_n : K_{n-1}] \cdots [K_1 : \mathbb{Q}] = 2^n$. □

COROLLAIRE 2.4 — Il est impossible de dupliquer un cube à la règle et au compas.

PREUVE — En tant que racine du polynôme irréductible $X^3 - 2$, le réel $\sqrt[3]{2}$ est algébrique sur $\mathbb{Q}$ de degré 3. Il résulte du théorème de Wantzel que $\sqrt[3]{2}$ n'est pas constructible à la règle et au compas d'où bien sûr l'impossibilité de dupliquer un cube. □

COROLLAIRE 2.5 — Il est impossible de trisecter un angle à la règle et au compas.

PREUVE — Montrons par exemple que l'angle $\pi/3$ ne peut pas être trisecté, i.e. que le réel $a = \cos(\pi/9)$ n'est pas constructible. L'équation $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ montre que a est racine du polynôme irréductible $4X^3 - 3X - 1$. En particulier, a est algébrique de degré 3 donc non constructible en vertu du théorème de Wantzel. □

COROLLAIRE 2.6 (LINDEMANN) — Le nombre π est transcendant sur $\mathbb{Q}$. En particulier, d'après le théorème de Wantzel, le problème la quadrature du cercle est impossible. [5], Sect. 3.1

DÉFINITION 2.7 — On appelle nombre de Fermat tout entier s'écrivant $F_n = 2^{2^n} + 1$, $n \in \mathbb{N}$.

THÉORÈME 2.8 — Pour $n \geq 3$, notons P_n le polygone régulier à n côtés. Si P_n est constructible à la règle et au compas alors $n = 2^r\, p_1 \ldots p_s$ où les p_k sont des nombres premiers de Fermat deux à deux distincts. [3], Ex 4.15

PREUVE — Notons $n = 2^r\, p_1^{\alpha_1} \ldots p_s^{\alpha_s}$ la décomposition de n en produit de facteurs premiers et supposons par l'absurde qu'il existe k tel que $\alpha_k \geq 2$. L'entier n étant alors divisible par p_k^2 il est facile de voir que le polygone régulier à p_k^2 côtés est constructible. Calculons maintenant le degré d'algébricité de $z = \exp(2i\pi/p_k^2)$. Tout d'abord, en notant respectivement x et y les parties réelle et imaginaire de z, il résulte du théorème 2.3 que

$$[\mathbb{Q}(x,y,i) : \mathbb{Q}] \;=\; [\mathbb{Q}(x,y,i) : \mathbb{Q}(x,y)]\,[\mathbb{Q}(x,y) : \mathbb{Q}] \;=\; 2 \times [\mathbb{Q}(x,y) : \mathbb{Q}]$$

est une puissance de 2. En tant que sous-corps de $\mathbb{Q}(x,y,i)$, le corps $\mathbb{Q}(z)$ est donc, en vertu de la formule de multiplicativité des degrés, une extension de degré 2^q de $\mathbb{Q}$, avec $q \in \mathbb{N}$. On considère maintenant le polynôme

$$P(X) \;=\; X^{(p_k-1)p_k} \;+\; \cdots \;+\; X^{2p_k} \;+\; X^{p_k} \;+\; 1.$$

En prenant la réduction modulo p de $P(X+1)$, une simple application du critère d'Eisenstein permet d'établir l'irréductibilité de P. Comme de plus $P(z) = 0$, le polynôme P est le polynôme minimal de z sur $\mathbb{Q}$. En particulier, z est algébrique de degré $2^q = (p_k - 1)p_k$ ce qui, compte tenu de l'imparité de p_k, est absurde. En définitive, $k = 1$ et $n = 2^r\, p_1 \ldots p_s$.

L'idée pour montrer que p_k est un nombre de Fermat est la même que précédemment en raisonnant cette fois sur le degré d'algébricité de $z = \exp(2i\pi/p_k)$. En utilisant tout d'abord la constructibilité du polygone régulier à p_k côtés, on obtient d'après le théorème 2.3 l'existence d'un entier $q \geq 0$ tel que $[\mathbb{Q}(z) : \mathbb{Q}] = 2^q$. Le polynôme minimal de z étant par ailleurs donné par

$$P(X) \;=\; X^{p_k-1} \;+\; \cdots \;+\; X \;+\; 1$$

il en résulte que $p_k = 2^q + 1$. Si q n'est pas une puissance de 2, q peut s'écrire $q = p\,m$ avec p impair. Les polynômes $X^p + 1$ et $X + 1$ s'annulant tous deux pour $X = -1$, l'entier $2^m + 1$ divise $p_k = 2^q + 1$ ce qui contredit la primalité de p_k. En conclusion, q est une puissance de 2 et p_k un nombre de Fermat. □

3 Condition suffisante de constructibilité.

LEMME 3.1 — Etant donné G est un p-groupe d'ordre p^n il existe une suite $G_0 \subset \cdots \subset G_n$ de sous-groupes distingués de G tels que $|G_i| = 2^i$ pour tout $0 \leq i \leq n$. [3], Ex. 1.4

THÉORÈME 3.2 — Soient L un sous-corps de $\mathbb{R}$ et (x, y) un élément de L^2. Si l'extension $\mathbb{Q} \subset L$ est normale de degré une puissance de 2 alors le point de coordonnées (x, y) est constructible à la règle et au compas. [3], Ex 4.14

PREUVE — Posons $G = \mathrm{Gal}(L \,|\, \mathbb{Q})$. L'extension $\mathbb{Q} \subset L$ étant normale, il résulte du théorème de correspondance de Galois que $|G| = [L : \mathbb{Q}\,] = 2^n$. En particulier, d'après le lemme 3.1, il existe une suite croissante $G_0 \subset \cdots \subset G_n$ de sous-groupes distingués de G tels que $|G_i| = 2^i$ pour tout $0 \leq i \leq n$. Notons $K_i = \mathrm{inv}(G_{n-i})$ le corps des invariants de G_{n-i} soit

$$K_i \;=\; \{\, x \in L \,;\, \sigma(x) = x \text{ pour tout } \sigma \in G_{n-i} \,\}.$$

Il est clair que $K_0 = \mathbb{Q}$ et $K_n = L$. Par ailleurs, comme $(G_{n-i} : G_{n-i-1}) = 2$, G_{n-i-1} est également distingué dans G_{n-i}. Une nouvelle application du théorème de correspondance nous permet alors d'affirmer que

$$[K_{i+1} : K_i] \;=\; |\,\mathrm{Gal}(K_{i+1} \,|\, K_i)| \;=\; (G_{n-i} : G_{n-i-1}) \;=\; 2.$$

Il résulte alors du théorème 2.1 que les éléments de L sont constructibles. □

THÉORÈME 3.3 (RÉCIPROQUE DU THÉORÈME 2.8) — Si $n = 2^r\, p_1 \ldots p_s$ où les p_k sont des nombres premiers de Fermat deux à deux distincts alors le polygone P_n est constructible à la règle et au compas. [3], Ex 4.15

PREUVE — Notons tout d'abord que si n et m sont premiers entre eux, le théorème de Bezout assure l'existence de a, $b \in \mathbb{Z}$ tels que

$$\frac{2\pi}{n\,m} \;=\; a\,\frac{2\pi}{n} \;+\; b\,\frac{2\pi}{m}.$$

En particulier, si P_n et P_m sont constructibles, le polygone P_{nm} l'est également. On est donc ramené à l'étude de la constructibilité de P_n pour (i) $n = 2^r$ et (ii) $n = p_k$, $1 \leq k \leq s$.

(i) $n = 2^r$. Dans ce cas, la constructibilité de P_n est une conséquence simple de la constructibilité de la bissectrice d'un angle.

(ii) $n = p_k$. Posons $z = \exp(2i\pi/p_k)$ et $K = \mathbb{Q}(z) \cap \mathbb{R}$. D'après le théorème 3.2, il suffit de montrer que l'extension $\mathbb{Q} \subset K$ est normale de degré une puissance de 2, ce qui établira la constructibilité de $\mathrm{Re}(z) = \cos(2\pi/p_k)$ et par conséquent celle de P_n. En tant que corps de décomposition du polynôme irréductible

$$P(X) \;=\; X^{p_k-1} \;+\; \cdots \;+\; X \;+\; 1,$$

le corps $\mathbb{Q}(z)$ est une extension de degré $p_k - 1 = 2^{2^m}$ de $\mathbb{Q}$. Par multiplicativité des degrés, l'extension $\mathbb{Q} \subset K$ est donc également de degré une puissance de 2. Considérons maintenant le groupe de Galois $G = \mathrm{Gal}(\mathbb{Q}(z) \,|\, \mathbb{Q})$. L'ensemble $\{1, z, \ldots, z^{p_k-1}\}$ formant une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(z)$, les éléments de G sont donnés par les automorphismes σ_i définis par

$$\sigma_i \;:\; z \;\longmapsto\; z^i \qquad \text{pour} \quad 0 \;\leq\; i \;\leq\; p_k - 1.$$

En particulier, le groupe G est abélien de sorte que $\mathrm{Gal}(\mathbb{Q}(z) \,|\, K) \lhd \mathrm{Gal}(\mathbb{Q}(z) \,|\, \mathbb{Q})$. Il résulte alors du théorème de correspondance de Galois que l'extension $\mathbb{Q} \subset K$ est normale. □

Références

[1] Jean-Claude Carrega. *Théorie des corps. La règle et le compas.* Hermann, 1989.

[2] Jean-Pierre Escofier. *Théorie de Galois, cours et exercices corrigés.* Dunod, 1997.

[3] Hervé Francinou, Serge Gianella. *Exercices de mathématiques pour l'agrégation, algèbre 1.* Masson, 1995.

[4] Xavier Gourdon. *Les maths en tête. Algèbre.* Ellipses, 1994.

[5] Daniel Perrin. *Cours d'algèbre.* Ellipses, 1996.