1

ÉTUDES

La règle, le compas et la théorie des corps

par J.-C. CARREGA, Université Claude Bernard, Lyon ;
avec des remarques de A. FAISANT, A. BOUVIER, J.-L. OVAERT.

La théorie des extensions de corps permet de caractériser les constructions de géométrie plane s'effectuant uniquement avec la règle et le compas. C'est ainsi qu'au cours du XIXème siècle on a pu trancher très simplement des conjectures célèbres depuis l'antiquité :

1°/ *La quadrature du cercle :*

Construire à la règle et au compas un carré ayant même aire qu'un cercle de rayon unité.

Figure 1

2°/ *La duplication du cube :*

Construire à la règle et au compas le côté d'un cube ayant un volume deux fois plus grand que celui d'un cube de côté unité.

Figure 2

3°/ *La trisection de l'angle :*

Partager à la règle et au compas un angle quelconque en trois angles égaux.

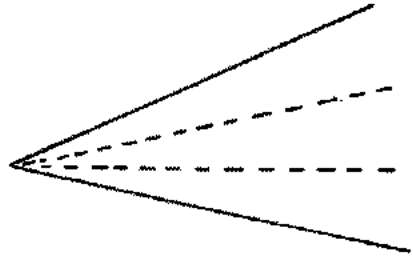

Figure 3

4°/ Quels sont les *polygones réguliers* constructibles à la règle et au compas ?

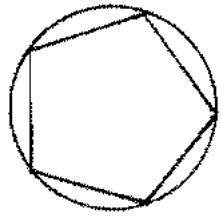

Figure 4

I. Points et nombres constructibles

Avant de poursuivre, précisons ce que l'on entend exactement par construction à la règle et au compas.

On considère au départ un plan euclidien P, ainsi que deux points distincts de P, noté O et I, appelés points de base.

Une construction à la règle et au compas est définie par une suite finie d'opérations de l'un des deux types suivants :

> 1/ Tracer la droite passant par deux points distincts A et B ; A et B étant des points de base ou des points déjà construits.
>
> 2/ Tracer le cercle de centre C et de rayon AB ; A, B, C étant des points de base ou des points déjà construits.

On dira qu'un *point M de P est constructible* si M est :

a/ Soit l'intersection de deux droites distinctes du type 1/

b/ Soit un point d'intersection de deux cercles distincts du type 2/

c/ Soit un point d'intersection d'une droite du type 1/ et d'un cercle du type 2/.

On dira aussi, qu'une droite du type 1/ est une *droite constructible* et qu'un cercle du type 2/ est un *cercle constructible.*

Bien sûr au départ, la seule chose qu'il nous est possible de faire est de tracer la droite passant par O et I. Ensuite on peut par exemple tracer le cercle Γ de centre O et de rayon OI. A l'intersection de ce cercle et de la droite OI on obtient un point I'. Soit C le cercle de centre I de rayon II' et C' le cercle de centre I' et de rayon I'I. A l'intersection de ces cercles on trouve le point K. La droite

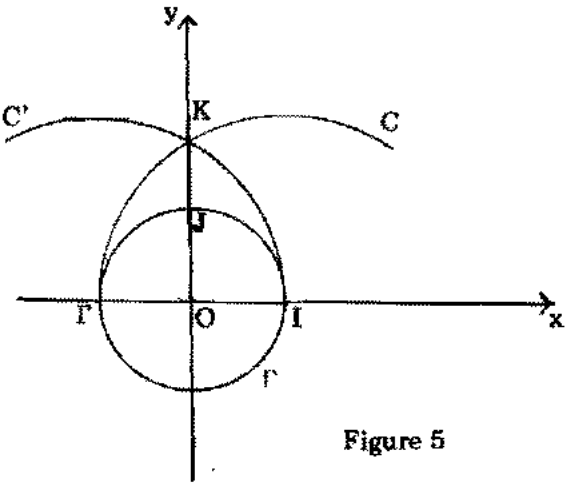

Figure 5

OK est perpendiculaire à la droite OI, elle coupe le cercle Γ en un point J.

Sur cet exemple, nous avons mis en évidence les points constructibles O, I, I', K, J. Nous avons mis aussi en évidence un repère (O, I, J) du plan P à partir duquel chaque point de P pourra être repéré par ses coordonnées.

Nous dirons qu'un *nombre réel est constructible* si c'est une des coordonnées, dans le repère (O, I, J), d'un point constructible.

Afin de simplifier les constructions ultérieures, signalons ici quelques résultats élémentaires.

R_1 : Si D est une droite constructible et A un point constructible, la perpendiculaire à D passant par A est une droite constructible.

La droite D étant constructible, elle contient au moins deux points constructibles E et F. Le cercle de centre A et de rayon AE coupe D en G. A partir de G et E comme centres on construit les cercles de rayon GE qui se coupent en B. La droite AB est la perpendiculaire cherchée. (Cette construction suppose $A \neq E$; dans le cas $A = E$ on utilise bien sûr le point F)

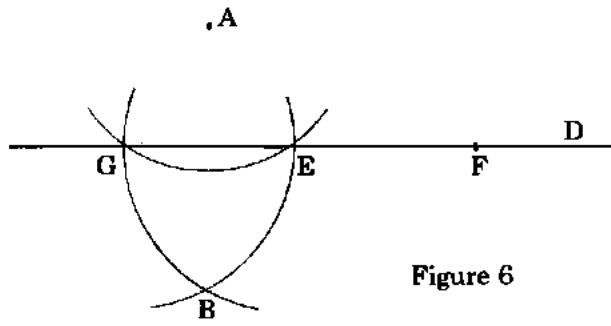

Figure 6

La première démonstration de ce résultat est attribuée au grec Oenepide de Chios.

R_2 : Si D est une droite constructible et A un point constructible, la parallèle à D passant par A est une droite constructible.

On utilise deux fois le résultat précédent. Une fois pour construire la perpendiculaire D' en A à D, une autre fois pour construire la perpendiculaire en A à D' qui est la droite cherchée.

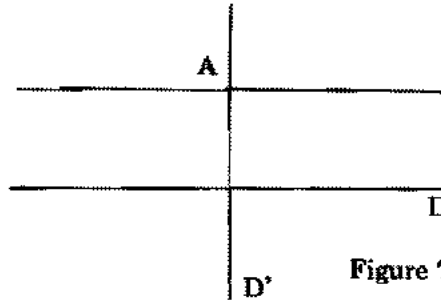

Figure 7

R_3 : Soit $t \in R$, t est un nombre constructible si et seulement s'il existe un point constructible de l'axe Ox d'abscisse t

* Si t est constructible, t est une coordonnée d'un point constructible P. Les projections orthogonales P_1 et P_2 de P sur les axes de coordonnées Ox et Oy sont des points constructibles d'après R_1.

— Si t est l'abscisse de P, c'est l'abscisse de P_1 et le résultat est démontré.

— Si t est l'ordonnée de P, c'est l'ordonnée de P_2. En utilisant le cercle de centre O et de rayon OP_2, on construit alors un point P_2' de l'axe Ox d'abscisse t et le résultat est démontré.

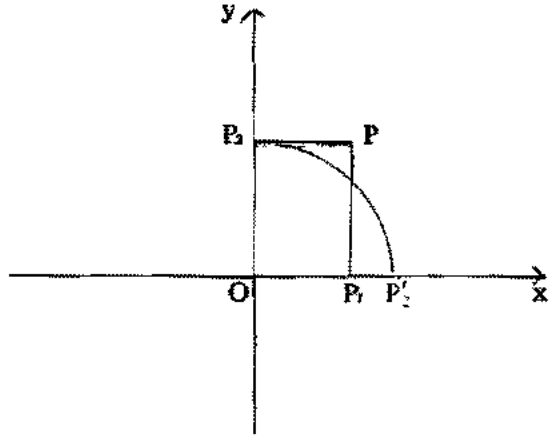

Figure 8

* Réciproquement, si t est l'abscisse d'un point constructible de l'axe Ox, t est un nombre constructible par définition d'un nombre constructible.

Comme conséquence de R_3 nous obtenons que l'ensemble des nombres constructibles est l'ensemble des abscisses des points constructibles de l'axe Ox.

R_4 : Si A est un point constructible et $x > 0$ un nombre constructible, le cercle de centre A et de rayon x est constructible.

Si P est le point de l'axe Ox d'abscisse x, ce point est constructible, d'après R_3. Le cercle de centre A et de rayon x est alors le cercle de centre A et de rayon OP.

R_5 : Si A et B sont des points constructibles, le milieu du segment AB est un point constructible.

On utilise une démonstration analogue à celle de R_1 pour montrer que la médiatrice du segment AB est une droite constructible, d'où le résultat.

II. Le corps des nombres constructibles

L'ensemble $\mathcal{C}$ des nombres constructibles est un sous-corps de R.

Nous savons déjà que $\mathcal{C}$ contient les nombres 0 et 1 qui sont les abscisses des points de base O et I.

En effet, soit A tel que $\overline{OA} = x$ et B tel que $\overline{AB} = y$ alors $\overline{OB} = x+y$. A est constructible d'après R_3 et B l'est aussi d'après R_4 en utilisant le cercle de centre A et de rayon $|y|$.

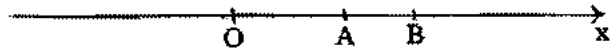

Figure 9

2/ Si $x \in \mathcal{C}$ alors $-x \in \mathcal{C}$

Si A est le point de l'axe Ox d'abscisse x, en utilisant le cercle de centre O et de rayon $|x|$ on construit le point A' d'abscisse $-x$.

3/ Si $x \in \mathcal{C}$ et $y \in \mathcal{C}$ alors $xy \in \mathcal{C}$.
Ecartons le cas trivial où $xy = 0$; soit alors A sur Ox tel que $\overline{OA} = x$ et B sur Oy tel que $\overline{OB} = y$. La parallèle à IB passant par A coupe Oy en C.
D'après Thalès on a :

$$\frac{\overline{OC}}{\overline{OB}} = \frac{\overline{OA}}{\overline{OI}} \text{ d'où } \overline{OC} = xy$$

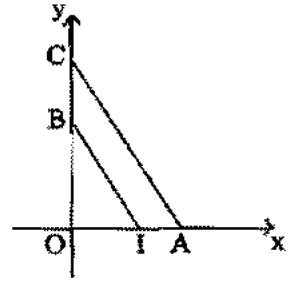

Figure 10

4/ Si $x \in \mathcal{C}$ et $x \neq 0$ alors $\frac{1}{x} \in \mathcal{C}$
Soit A sur Ox tel que $\overline{OA} = x$. La parallèle à AJ passant par I coupe Oy en B.
D'après Thalès on a :

$$\frac{\overline{OB}}{\overline{OJ}} = \frac{\overline{OI}}{\overline{OA}} \text{ d'où } OB = \frac{1}{x}$$

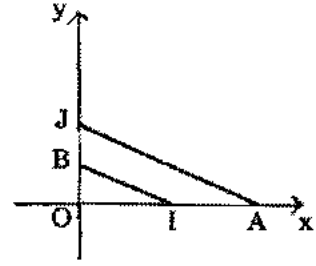

Figure 11

Ainsi, on a démontré que $\mathcal{C}$ est un sous-corps de $\mathbf{R}$, comme $\mathbf{Q}$ est le plus petit sous-corps de $\mathbf{R}$ nous avons donc :

$$\mathbf{Q} \subset \mathcal{C} \subset \mathbf{R}$$

$\mathcal{C}$ vérifie de plus une propriété intéressante non vérifiée par $\mathbf{Q}$ mais vérifiée par $\mathbf{R}$:

5/ Si $x \in \mathcal{C}$ et $x \geqslant 0$ alors $\sqrt{x} \in \mathcal{C}$.
Supposons $x > 0$. Soit A le point de l'axe Ox tel que $\overline{IA} = x$. Soit M le milieu du segment OA, c'est un point constructible donc le cercle de centre M et de rayon MO est constructible. La perpendiculaire en I à Ox coupe ce cercle en B. Le triangle OBA étant rectangle nous avons $IB^2 = IO.IA$ d'où $IB = \sqrt{x}$.

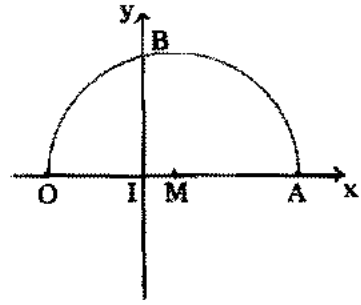

Figure 12

Remarque : Sachant que $\mathcal{C}$ est un corps contenant $\mathbf{Q}$ et vérifiant la propriété 5/, on peut donner de nombreux exemples de nombres constructibles :

$$\sqrt{2}, \sqrt{\frac{2}{3}}, \sqrt[4]{3}, \frac{\sqrt{3}-\sqrt[8]{5}}{\sqrt{2}}, \frac{2+3\sqrt{2}-\sqrt{5}}{7} \ldots\ldots\ldots$$

De plus en utilisant les constructions élémentaires 1/ 2/ 3/ 4/ 5/ on peut effectivement construire à la règle et au compas les points de l'axe Ox ayant pour abscisses les nombres précédents.

III. Caractérisation des nombres constructibles

Si $a \in \mathbf{R}$, on note $\mathbf{Q}(a)$ le plus petit sous-corps de $\mathbf{R}$ contenant a. Plus généralement si $a_1, a_2, \ldots a_n$ sont dans $\mathbf{R}$, $\mathbf{Q}(a_1, a_2, \ldots a_n)$ désigne le plus petit sous-corps de $\mathbf{R}$ contenant $a_1, a_2, \ldots a_n$. Ce sous-corps existe car c'est l'intersection de tous les sous-corps de $\mathbf{R}$ contenant $a_1, a_2, \ldots a_n$.

Par exemple :

$$\mathbf{Q}(1) = \mathbf{Q}\left(\frac{1}{2}\right) = \mathbf{Q}\left(-\frac{2}{3}\right) = \mathbf{Q}$$

$$\mathbf{Q}(\sqrt{2}) = \{\alpha + \beta\sqrt{2} \,/\, \alpha, \beta \in \mathbf{Q}\}$$

$$\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \{\alpha + \beta\sqrt{2} + \gamma\sqrt{3} + \delta\sqrt{6} \,/\, \alpha, \beta, \gamma \in \mathbf{Q}\}$$

On pourra consulter à ce sujet [2].

Si M est un point du plan P de coordonnées a_1 et a_2 dans (O, I, J), on notera $M(a_1, a_2)$.

Lemme : 1/ Si D est une droite de P passant par les points distincts $A(a_1, a_2)$ et $B(b_1, b_2)$ alors D a une équation de la forme $\alpha x + \beta y + \gamma = 0$ avec $\alpha, \beta, \gamma \in \mathbf{Q}(a_1, a_2, b_1, b_2)$.

2/ Soient $A(a_1, a_2)$, $B(b_1, b_2)$, $C(c_1, c_2)$ trois points de P. Le cercle de centre A et de rayon BC a une équation de la forme :

$$x^2 + y^2 - 2\alpha x - 2\beta y + \gamma = 0$$

avec $\alpha, \beta, \gamma \in \mathbf{Q}(a_1, a_2, b_1, b_2, c_1, c_2)$.

1/ Si $a_1 = b_1$ D a pour équation $x - a_1 = 0$

Si $a_1 \neq b_1$ D a pour équation $y - a_2 = (x - a_1)\dfrac{(b_2 - a_2)}{b_1 - a_1}$

qui se met sous la forme :

$$\alpha x + \beta y + \gamma = 0 \text{ avec } \alpha, \beta, \gamma \in \mathbf{Q}(a_1, a_2, b_1, b_2).$$

2/ Le cercle de centre A et de rayon BC a pour équation :

$$(x - a_1)^2 + (y - a_2)^2 = (c_1 - b_1)^2 + (c_2 - b_2)^2$$

qui se met sous la forme $x^2 + y^2 - 2\alpha x - 2\beta y + \gamma = 0$ avec $\alpha, \beta, \gamma \in \mathbf{Q}(a_1, a_2, b_1, b_2, c_1, c_2)$.

Rappels sur les extensions de corps : Pour les démonstrations des résultats donnés ici on pourra consulter [1] ou [2].

1/ Si K et L sont des corps tels que K soit un sous-corps de L on dit que L est une *extension* de K, on l'indique simplement par $K \subset L$. On peut alors considérer L comme un espace vectoriel sur K ; la dimension de cet espace, lorsqu'elle est finie, est notée $[L : K]$ et s'appelle le *degré* de L sur K. Si K, L, M sont des corps tels que $K \subset L \subset M$ on a la relation :

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

Par exemple

$$[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}] = [\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}(\sqrt{2})] \times [\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2 \times 2 = 4.$$

2/ Si $K \subset L$ et $a \in L$, a est dit *algébrique* sur K s'il existe un polynome non nul $P(x) \in K[x]$ tel que $P(a) = 0$. Si a n'est pas algébrique sur K on dit que a est *transcendant* sur K. Par exemple $\sqrt{2}$ est algébrique sur $\mathbf{Q}$ puisqu'il est racine du polynome $x^2 - 2$. Hermite a montré en 1873 que le nombre e, base des logarithmes népériens, est transcendant sur $\mathbf{Q}$. Lindemann a montré en 1882 que le nombre π est transcendant sur $\mathbf{Q}$.

3/ Si a est algébrique sur K il existe un polynome $P(x) \in K[x]$ unique tel que :

- $P(a) = 0$
- $P(x)$ est irréductible dans $K[x]$
- Le coefficient du monome de plus haut degré de $P(x)$ est 1 (unité de K).

Ce polynome est appelé le *polynome minimal* de a sur K. Si n est le degré de $P(x)$ alors on a $[K(a) : K] = n$ et une base du K- espace vectoriel $K(a)$ est donnée par $\{1, a, a^2, \ldots a^{n-1}\}$. ($K(a)$ désigne le plus petit sous-corps de L contenant a et K).

On dit que a est algébrique et de *degré* n sur K.

Par exemple, $\sqrt{2}$ est algébrique sur $\mathbf{Q}$ et de degré 2, son polynome minimal sur $\mathbf{Q}$ est $x^2 - 2$, une base de $\mathbf{Q}(\sqrt{2})$ sur $\mathbf{Q}$ est

$$\{1, \sqrt{2}\}$$

4/ Si $K \subset L$ l'ensemble des éléments de L algébriques sur K est un sous-corps de L contenant K.

5/ Dedekind a montré en 1873 que l'ensemble des nombres réels algébriques sur $\mathbf{Q}$ est un corps dénombrable [4].

Théorème : Soit $t \in \mathbf{R}$; t est un nombre constructible si et seulement s'il existe un entier $p \geqslant 1$ et une suite de sous-corps de $\mathbf{R}$, $L_1, L_2, \ldots L_p$ tels que :

- $L_1 = \mathbf{Q}$
- Pour $1 \leqslant j \leqslant p-1$, $L_j \subset L_{j+1}$ et $[L_{j+1} : L_j] = 2$
- $t \in L_p$

Si t est constructible, t est l'abscisse d'un point constructible M de l'axe Ox. Ce point M est obtenu à partir des points de base O et I en utilisant un certain nombre de fois les constructions décrites au paragraphe I. Soit $M_1, M_2, \ldots M_n = M$ la suite des points successivement construits pour obtenir M. Les points M_1 et M_2 sont nécessairement les points de base. (Par exemple, au paragraphe I, pour obtenir le point J la suite des points était : O, I, I', K, J.)

Pour $i = 1, 2, \ldots n$, appelons a_i et b_i les coordonnées de M_i dans le repère (O, I, J). On a en particulier :

$$a_1 = b_1 = 0,\ a_2 = 1,\ b_2 = 0,\ a_n = t,\ b_n = 0.$$

Posons $K_1 = \mathbf{Q}(a_1, b_1)$

$K_2 = \mathbf{Q}(a_1, b_1, a_2, b_2)$

.....

$K_i = \mathbf{Q}(a_1, b_1, a_2, b_2, \ldots a_i, b_i)$

.....

$K_n = \mathbf{Q}(a_1, b_1, \ldots\ldots a_n, b_n)$

On a en particulier : $K_1 = \mathbf{Q}$, $K_2 = \mathbf{Q}$, $t \in K_n$.

Nous allons démontrer que pour tout i, $1 \leqslant i \leqslant n-1$, $K_{i+1} = K_i$ ou $[K_{i+1} : K_i] = 2$.

Le résultat est évident pour $i = 1$ car $K_2 = K_1$. Supposons donc $i \geqslant 2$. Trois cas se présentent pour le point M_{i+1} suivant qu'il est à l'intersection de deux droites, d'une droite et d'un cercle ou de deux cercles définis par les points précédents $M_1, M_2, \ldots M_i$. Mais d'après le lemme du début du paragraphe les droites et les cercles construits à l'aide des points $M_1, M_2, \ldots M_i$ ont des équations à coefficients dans $K_i = Q(a_1, b_1, \ldots a_i, b_i)$.

1) Si M_{i+1} est à l'intersection de deux droites, a_{i+1} et b_{i+1} sont alors solutions d'un système de la forme :

$$\begin{cases} \alpha x + \beta y + \gamma = 0 \\ \alpha' x + \beta' y + \gamma' = 0 \end{cases}$$

avec $\alpha, \beta, \gamma, \alpha', \beta', \gamma' \in K_i$. En résolvant ce système on constate que a_{i+1} et b_{i+1} appartiennent aussi à K_i. D'où

$$K_{i+1} = K_i(a_{i+1}, b_{i+1}) = K_i$$

2) Si M_{i+1} est à l'intersection d'une droite et d'un cercle, a_{i+1} et b_{i+1} sont alors solutions d'un système de la forme

$$\begin{cases} \alpha x + \beta y + \gamma = 0 \\ x^2 + y^2 - 2\alpha' x - 2\beta' y + \gamma' = 0 \end{cases}$$

avec $\alpha, \beta, \gamma, \alpha', \beta', \gamma' \in K_i$.

• Si $\beta \neq 0$, on a $y = -\frac{1}{\beta}(\alpha x + \gamma)$, on forme alors l'équation aux abscisses qui est une équation du second degré à coefficients dans K_i et a_{i+1} est racine de cette équation.

* Si $a_{i+1} \in K_i$ alors

$$b_{i+1} = -\frac{1}{\beta}(\alpha a_{i+1} + \gamma) \in K_i \text{ et } K_{i+1} = K_i$$

* Si $a_{i+1} \notin K_i$ alors a_{i+1} est algébrique sur K_i et de degré 2. Dans ce cas

$$K_{i+1} = K_i(a_{i+1}, b_{i+1}) = K_i(a_{i+1}) \text{ et } [K_{i+1} : K_i] = 2$$

• Si $\beta = 0$, alors $\alpha \neq 0$, on procède de même en formant l'équation aux ordonnées.

3) Si M_{i+1} est à l'intersection de deux cercles, a_{i+1} et b_{i+1} sont alors solutions d'un système de la forme :

$$\begin{cases} x^2 + y^2 - 2\alpha x - 2\beta y + \gamma = 0 \\ x^2 + y^2 - 2\alpha' x - 2\beta' y + \gamma' = 0 \end{cases}$$

avec $\alpha, \beta, \gamma, \alpha', \beta', \gamma' \in K_i$. Ce système est équivalent au système :

$$\begin{cases} x^2 + y^2 - 2\alpha x - 2\beta y + \gamma = 0 \\ 2(\alpha - \alpha')x + 2(\beta - \beta')y - (\gamma - \gamma') = 0 \end{cases}$$

et on est ramené au cas précédent.

Nous avons ainsi construit une suite de corps $K_1 \subset K_2 \subset \cdots \subset K_n$ telle que $K_1 = \mathbf{Q}$, $t \in K_n$ et pour

$$1 \leqslant i \leqslant n-1 \text{ , } K_{i+1} = K_i \text{ ou } [K_{i+1} : K_i] = 2.$$

Nous pouvons rendre cette suite strictement croissante en supprimant les corps superflus, on obtient alors une suite

$$L_1 \subset L_2 \subset \cdots \subset L_p$$

telle que $L_1 = \mathbf{Q}$, $t \in L_p$ et pour $1 \leqslant j \leqslant p-1$ $[L_{j+1} : L_j] = 2$,

—— Réciproquement, supposons qu'il existe une suite $L_1 \subset L_2 \subset \cdots \subset L_p$ de sous-corps de $\mathbf{R}$ telle que $L_1 = \mathbf{Q}$, $t \in L_p$ et pour $1 \leqslant j \leqslant p-1$, $[L_{j+1} : L_j] = 2$. Nous allons montrer par récurrence sur j que $L_j \subset \mathcal{C}$; il en résultera bien que t est un nombre constructible.

• $L_1 \subset \mathcal{C}$ car $L_1 = \mathbf{Q}$ et on sait que $\mathbf{Q} \subset \mathcal{C}$

• Supposons que $L_j \subset \mathcal{C}$ et montrons que $L_{j+1} \subset \mathcal{C}$. Soit $a \in L_{j+1}$ et montrons que $a \in \mathcal{C}$.

— Si $a \in L_j$ alors $a \in \mathcal{C}$ car $L_j \subset \mathcal{C}$

— Si $a \notin L_j$, considérons $L_j \subset L_j(a) \subset L_{j+1}$, on a :

$$2 = [L_{j+1} : L_j] = [L_{j+1} : L_j(a)] \times [L_j(a) : L_j]$$

Comme $a \notin L_j$ on a $L_j \neq L_j(a)$ et $[L_j(a) : L_j] \neq 1$ d'où $[L_j(a) : L_j] = 2$.

Il en résulte que le polynome minimal de a sur L_j est de degré 2 et ainsi a est racine d'une équation de la forme $x^2 + \alpha x + \beta = 0$ avec $\alpha, \beta \in L_j$. On a donc

$$\alpha^2 - 4\beta \geqslant 0 \text{ et } a = \frac{-\alpha \pm \sqrt{\alpha^2 - 4\beta}}{2}.$$

Comme $L_j \subset \mathcal{C}$ et que $\mathcal{C}$ vérifie la propriété 5 du paragraphe II on a $a \in \mathcal{C}$.

Remarque : A l'aide du théorème que nous venons d'établir il est facile de démontrer que le corps C des nombres constructibles est le plus petit des sous-corps L de R vérifiant la propriété : Si $x \in L$ et $x \geqslant 0$ alors $\sqrt{x} \in L$.

Mais nous allons plutôt nous intéresser à un autre corollaire du théorème qui est un résultat décisif pour le problème des conjectures. Ce résultat a été établi pour la première fois par WANTZELL (1814 — 1848), alors qu'il était répétiteur à l'école polytechnique.

Résultat de WANTZELL : Tout nombre constructible est algébrique sur Q et son degré est une puissance de 2.

Si $t \in \mathbf{R}$ est constructible, d'après le théorème précédent il existe une suite de sous-corps de R, $L_1 \subset L_2 \subset \cdots \subset L_p$ telle que $L_1 = \mathbf{Q}$, $t \in L_p$ et pour $1 \leqslant j \leqslant p-1$, $[L_{j+1} : L_j] = 2$.

On obtient alors :

$$[L_2 : \mathbf{Q}] \times [L_3 : L_2] \times \ldots \times [L_p : L_{p-1}] = [L_p : \mathbf{Q}] = 2^{p-1}$$

On a aussi :

$\mathbf{Q} \subset \mathbf{Q}(t) \subset L_p$ d'où $[L_p : \mathbf{Q}] = [L_p : \mathbf{Q}(t)] \times [\mathbf{Q}(t) : \mathbf{Q}]$.

Il en résulte que $[\mathbf{Q}(t) : \mathbf{Q}]$ est un diviseur de 2^{p-1}, donc $[\mathbf{Q}(t) : \mathbf{Q}]$ est une puissance de 2.

Notons $[\mathbf{Q}(t) : \mathbf{Q}] = 2^q$. Considérons les vecteurs $1, t, t^2, \ldots, t^{2^q}$, ils forment une famille ayant $2^q + 1$ éléments, elle est donc liée sur Q ; il existe donc des éléments de Q $a_0, a_1, \ldots a_{2^q}$ non tous nuls tels que $a_0 + a_1 t + a_2 t^2 + \ldots + a_{2^q} t^{2^q} = 0$, ceci montre que t est algébrique sur Q. De plus, d'après les rappels le degré de t est donné par $[\mathbf{Q}(t) : \mathbf{Q}]$ qui est égal à 2^q, d'où le résultat.

Exemples : Le résultat de Wantzell est très utile pour montrer qu'un nombre n'est pas constructible.

1/ π n'est pas constructible ; en effet si π était constructible, d'après Wantzell il serait algébrique, or on sait qu'il est transcendant.

2/ $\sqrt[3]{2}$ n'est pas constructible. $\sqrt[3]{2}$ est algébrique sur $\mathbf{Q}$ et son polynome minimal est $X^3 - 2$, il en résulte que

$$[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$$

et ainsi $\sqrt[3]{2}$ est algébrique et de degré 3.

IV. Applications

Le résultat de Wantzell va nous permettre de répondre par la négative aux trois premiers problèmes posés en introduction et de trouver les naturels n pour lesquels il est possible de construire à la règle et au compas les polygones réguliers à n côtés.

1/ *La quadrature du cercle :*

Si la quadrature était possible, on pourrait construire à la règle et au compas un carré dont la longueur du côté serait $\sqrt{\pi}$. Grâce au compas on pourrait alors reporter cette longueur et construire un point de Ox d'abscisse $\sqrt{\pi}$, $\sqrt{\pi}$ serait alors un nombre constructible ; comme l'ensemble C des nombres constructibles est un corps $\pi = (\sqrt{\pi})^2$ serait aussi un nombre constructible, or nous avons vu à la fin du paragraphe précédent que cela n'est pas possible. Wantzell, lui-même, n'a pas pu résoudre le problème de la quadrature car à son époque on ne connaissait pas encore la nature du nombre π. Rappelons en effet que c'est en 1761 que Lambert montre que π est irrationnel et en 1794 que Legendre montre que π^2 est irrationnel. C'est en 1844 que Liouville montre l'existence de nombres transcendants, résultat confirmé par la théorie des cardinaux de Cantor en 1873. Mais il fallut attendre 1882 avec Lindemann pour savoir que π est transcendant.

2/ *La duplication du cube :*

Si x désigne la longueur du côté du cube à construire, $x^3 = 2$. Ainsi si la duplication du cube était possible $\sqrt[3]{2}$ serait constructible, or nous avons vu à la fin du paragraphe précédent que $\sqrt[3]{2}$ n'est pas constructible.

3/ *La trisection de l'angle*

On note $\widehat{\theta}$ l'angle dont une mesure en radians est le nombre réel θ. Soit M le point du cercle Γ de centre 0 et de rayon 1 tel que $\widehat{\theta} = \widehat{(\overrightarrow{OI}, \overrightarrow{OM})}$; on dit que $\widehat{\theta}$ est un *angle constructible*

si M est un point constructible ; il résulte de cette définition que l'angle $\widehat{\theta}$ est constructible si et seulement si cos θ est un nombre constructible.

Si $0 \leqslant \theta \leqslant \pi$, on dit que $\widehat{\theta}$ est *trisectable* si $\frac{\widehat{\theta}}{3}$ est constructible ; il résulte de cette définition que $\widehat{\theta}$ est trisectable si et seulement si cos $\frac{\theta}{3}$ est un nombre constructible. Remarquons que d'après la formule : $\cos \theta = 4 \cos^3 \frac{\theta}{3} - 3 \cos \frac{\theta}{3}$, si $\widehat{\theta}$ est trisectable alors $\widehat{\theta}$ est constructible.

Certains angles constructibles sont trisectables, c'est le cas par exemple pour $\widehat{\frac{\pi}{2}}$ car $\cos \frac{\pi}{6} = \frac{\sqrt{3}}{2}$ est un nombre constructible, mais ils ne le sont pas tous, nous allons monter par exemple que $\widehat{\frac{\pi}{3}}$, qui est constructible ($\cos \frac{\pi}{3} = \frac{1}{2}$), n'est pas trisectable.

Tout revient pour cela à démontrer que $\cos \frac{\pi}{9}$ n'est pas un nombre constructible. D'après la formule

$$\cos \theta = 4 \cos^3 \frac{\theta}{3} - 3 \cos \frac{\theta}{3} \quad , \cos \frac{\pi}{9}$$

est racine du polynome $P(x) = 4x^3 - 3x - \frac{1}{2}$. Montrons que $P(x)$ est irréductible dans $\mathbb{Q}[x]$. Sinon il existe un rationnel de forme irréductible $\frac{p}{q}$ tel que $P(\frac{p}{q}) = 0$ soit $8p^3 - 6pq^2 = q^3$. Il en résulte que p divise q^3 d'où $p = \pm 1$ et que q^2 divise $8p^3$ d'où $q = \pm 1$ ou ± 2 ; d'où $\frac{p}{q} = \pm 1$ ou $\pm \frac{1}{2}$. On vérifie alors directement que ces quatre nombres ne sont pas racines de $P(x)$. $P(x)$ est donc irréductible, il en résulte que $\frac{P(x)}{4}$ est le polynome minimal de $\cos \frac{\pi}{9}$ sur $\mathbb{Q}$ et ainsi $\cos \frac{\pi}{9}$ est algébrique sur $\mathbb{Q}$ et de degré 3, d'après le résultat de Wantzell $\cos \frac{\pi}{9}$ n'est pas un nombre constructible. Plus généralement, on peut démontrer le résultat suivant :

> Si $\widehat{\theta}$ est un angle constructible, $\widehat{\theta}$ est trisectable si et seulement si le polynome $4x^3 - 3x - \cos \theta$ est réductible dans $\mathbb{Q}(\cos \theta)[x]$.
> Pour la démonstration, on pourra consulter [8].

4/ *Les polygones réguliers*

La construction à la règle et au compas d'un polygone régulier à n côtés se ramène à la construction de l'angle $\widehat{\frac{2\pi}{n}}$. On dira donc qu'un polygone régulier à n côtés est *constructible* si l'angle $\widehat{\frac{2\pi}{n}}$ est constructible.

Lemme : Si m et n sont premiers entre eux, $\widehat{\frac{2\pi}{m}}$ et $\widehat{\frac{2\pi}{n}}$ sont constructibles si et seulement si $\widehat{\frac{2\pi}{mn}}$ est constructible.

— Si $\widehat{\frac{2\pi}{mn}}$ est constructible alors $\widehat{\frac{2\pi}{n}}$ et $\widehat{\frac{2\pi}{m}}$ le sont aussi car

$\widehat{\frac{2\pi}{m}} = m\widehat{\frac{2\pi}{mn}}$ et $\widehat{\frac{2\pi}{m}} = n\widehat{\frac{2\pi}{mn}}$ et il est aisé à partir d'un angle de construire un multiple de cet angle en reportant avec le compas un certain nombre de fois la corde déterminée par cet angle sur le cercle Γ de centre 0 et de rayon 1.

— Si $\widehat{\frac{2\pi}{n}}$ et $\widehat{\frac{2\pi}{m}}$ sont constructibles alors $\widehat{\frac{2\pi}{mn}}$ l'est aussi car d'après l'identité de Bezout il existe λ et μ dans Z tels que $\lambda n + \mu m = 1$ d'où $\widehat{\frac{2\pi}{mn}} = \lambda\widehat{\frac{2\pi}{m}} + \mu\widehat{\frac{2\pi}{n}}$. Il suffit alors de savoir construire la somme de deux angles constructibles ce qui se fait en construisant des représentants de ces angles avec un côté adjacent.

Compte tenu de ce lemme, pour savoir si le polygone à n côtés est constructible, on décompose n en facteurs premiers :

$$n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$$

le polygone sera constructible si et seulement si les angles $\widehat{\frac{2\pi}{p_1^{\alpha_1}}}, \ldots \widehat{\frac{2\pi}{p_k^{\alpha_k}}}$ sont constructibles.

Nous sommes donc ramenés à déterminer les angles constructibles de la forme $\frac{2\pi}{p^\alpha}$ où p est premier et $\alpha \in \mathbb{N}_*$.

1er cas : $p = 2$.

> Les angles de la forme $\widehat{\frac{2\pi}{2^\alpha}}$ sont constructibles.

Cela se démontre par récurrence sur $\alpha \in \mathbb{N}_*$; en fait, il suffit de montrer qu'il est possible de construire à la règle et au compas la bissectrice d'un angle. C'est une construction élémentaire qui ne pose aucun problème.

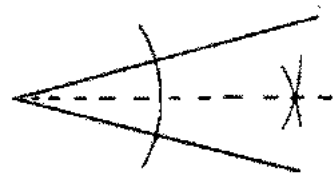

Figure 13

2ème cas : $p \geqslant 3$.

> Si $\widehat{\frac{2\pi}{p^\alpha}}$ est constructible alors $\alpha = 1$ et p est un nombre de Fermat premier, c'est-à-dire un nombre premier de la forme $1 + 2^{(2^\beta)}$.

Supposons que $\widehat{\frac{2\pi}{p^\alpha}}$ soit constructible, alors $\cos\left(\frac{2\pi}{p^\alpha}\right)$ est un nombre constructible et d'après le résultat de Wantzell il existe un entier m tel que

$$[\mathbf{Q}\left(\cos\left(\frac{2\pi}{p^\alpha}\right)\right) : \mathbf{Q}] = 2^m \qquad (1)$$

Pour simplifier posons $q = p^\alpha$. Considérons

$$\omega = \cos\frac{2\pi}{q} + i \sin\frac{2\pi}{q} .$$

ω est une racine $q^{\text{ième}}$ de l'unité, ω est racine du polynome $X^q - 1$ donc est algébrique sur $\mathbf{Q}$.

Nous admettrons ici que le polynome minimal de ω sur $\mathbf{Q}$ est donné par :

$$P(X) = (X - \omega_1)(X - \omega_2) \ldots (X - \omega_h)$$

où les ω_i $1 \leqslant i \leqslant h$ sont les racines primitives $q^{\text{ièmes}}$ de l'unité,

c'est-à-dire que les ω_i sont de la forme $\cos\frac{2k\pi}{q} + i \sin\frac{2k\pi}{q}$ avec k premier avec q et $1 \leqslant k < q$. $P(X)$ est appelé le qième polynome cyclotomique, on pourra consulter à ce sujet [1].

Pour trouver le degré h de $P(X)$, il suffit donc de connaître le nombre h d'entiers k tels que $1 \leqslant k < q$ et k premier avec $q = p^\alpha$. On obtient $h = p^{\alpha-1}(p-1)$. Nous avons donc

$$[\,\mathbf{Q}(\omega) : \mathbf{Q}\,] = p^{\alpha-1}(p-1) \qquad (2)$$

D'autre part, nous avons $\omega + \omega^{-1} = 2\cos\frac{2\pi}{p^\alpha}$, il en résulte que $\cos\left(\frac{2\pi}{p^\alpha}\right) \in \mathbf{Q}(\omega)$ et que $\omega^2 - 2\omega\cos\frac{2\pi}{p^\alpha} + 1 = 0$. Ainsi ω est algébrique et de degré 2 sur $\mathbf{Q}\left(\cos\left(\frac{2\pi}{p^\alpha}\right)\right)$, d'où

$$[\,\mathbf{Q}(\omega) : \mathbf{Q}\left(\cos\left(\frac{2\pi}{p^\alpha}\right)\right)\,] = 2 \qquad (3)$$

A partir des relations (1) (2) (3) et sachant que

$$[\mathbf{Q}(\omega) : \mathbf{Q}] = [\mathbf{Q}(\omega) : \mathbf{Q}(\cos(\tfrac{2\pi}{p^\alpha}))] \times [\mathbf{Q}(\cos(\tfrac{2\pi}{p^\alpha})) : \mathbf{Q}]$$

on obtient :

$$p^{\alpha-1}(p-1) = 2^{m+1}.$$

Il en résulte $\alpha = 1$ et $p = 1 + 2^{m+1}$.

Montrons alors que $m + 1$ est une puissance de 2. A partir de la décomposition de $m + 1$ en facteurs premiers, on obtient $m + 1 = \lambda\, 2^\beta$ avec $\beta \in \mathbf{N}$ et $\lambda \in \mathbf{N}_*$ impair.

$$p = 1 + 2^{m+1} = 1 + 2^{(\lambda\, 2^\beta)} = 1 + (2^{2^\beta})^\lambda.$$

λ étant impair, le polynome $1 + X^\lambda$ est divisible par $1 + X$, il en résulte que p est divisible par $1 + 2^{(2^\beta)}$, mais comme p est premier, on a $p = 1 + 2^{(2^\beta)}$. Ceci démontre le résultat annoncé.

Réciproquement, on pourrait montrer en utilisant la théorie de Galois que si p est un nombre de Fermat premier alors $\widehat{\frac{2\pi}{p}}$ est constructible. [2]

On obtient alors le résultat suivant :

Théorème : Les polygones réguliers constructibles sont ceux pour lesquels le nombre de côtés n est de la forme $2^k\ p_1\ p_2\ \ldots\ p_r$ où $k \in \mathbb{N}$ et où les p_i sont des nombres de Fermat premiers distincts.

Les cinq premiers nombres de Fermat sont 3, 5, 17, 257, 65537 obtenus à partir de la formule $p = 1 + 2^{(2^\beta)}$ pour $\beta = 0, 1, 2, 3, 4$. Ces cinq nombres de Fermat sont premiers. Pour l'instant, on ne connaît pas d'autres nombres de Fermat qui soient premiers. C'est Euler qui s'aperçut le premier que pour $\beta = 5$ le nombre de Fermat correspondant n'était pas premier. On pourra consulter avec intérêt [5] .

Exemples :

1) Pour $n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20$ les polygones réguliers à n côtés sont constructibles, pour $n = 7, 9, 11, 13, 14, 18, 19$ ils ne le sont pas. Euclide connaissait les constructions pour $n = 3, 4, 5, 15$ et il savait doubler le nombre de côtés d'un polygone constructible. On ne sut rien faire de mieux jusqu'en 1796 où Gauss à l'âge de 19 ans montra que le polygone régulier à 17 côtés est constructible. De plus, il énonça la condition nécessaire et suffisante (du théorème précédent) pour que n soit le nombre de côtés d'un polygone constructible. Il démontra seulement que la condition est suffisante, il est vrai qu'il ne disposait pas, à l'époque, du résultat de Wantzell. On pourra consulter à ce sujet [6]. On trouve aussi une construction du polygone régulier à 17 côtés dans [2].

2) Donnons ici la construction bien classique du pentagone régulier. Nous allons essayer de la justifier en exprimant $\cos\frac{2\pi}{5}$ sous une forme qui permette la construction effective d'un point d'abscisse $\cos\frac{2\pi}{5}$. $\omega = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$ est racine du polynome $X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1)$. Nous avons donc $\omega^4 + \omega^3 + \omega^2 + \omega + 1 = 0$, que l'on peut écrire sous la forme :

$$\left(\omega^2 + \frac{1}{\omega^2}\right) + \left(\omega + \frac{1}{\omega}\right) + 1 = 0 .$$

Cette transformation est assez naturelle car

$$\cos\frac{2\pi}{5} = \frac{1}{2}\left(\omega + \frac{1}{\omega}\right).$$

En posant $u = \cos\frac{2\pi}{5} = \frac{1}{2}\left(\omega + \frac{1}{\omega}\right)$ on a :

$$\omega + \frac{1}{\omega} = 2u, \quad \omega^2 + \frac{1}{\omega^2} = \left(\omega + \frac{1}{\omega}\right)^2 - 2 = 4u^2 - 2$$

d'où $$(4u^2 - 2) + 2u + 1 = 0.$$

On obtient ainsi que $u = \cos\frac{2\pi}{5}$ est racine du polynome $4X^2 + 2X - 1$. Ceci permet d'exprimer $\cos\frac{2\pi}{5}$ par

$$\cos\frac{2\pi}{5} = \frac{-1 + \sqrt{5}}{4}$$

$$\cos\frac{2\pi}{5} = \frac{-\frac{1}{2} + \sqrt{\frac{5}{4}}}{2}$$

Soit A le milieu du segment OI', alors

$$AJ = \sqrt{\frac{5}{4}}$$

Par un cercle de centre A et de rayon AJ, construisons H sur Ox tel que $\overline{AH} = AJ$, on a alors

$$\overline{OH} = -\frac{1}{2} + \sqrt{\frac{5}{4}}$$

Si P est le milieu du segment OH on a alors

$$\overline{OP} = \cos\frac{2\pi}{5}.$$

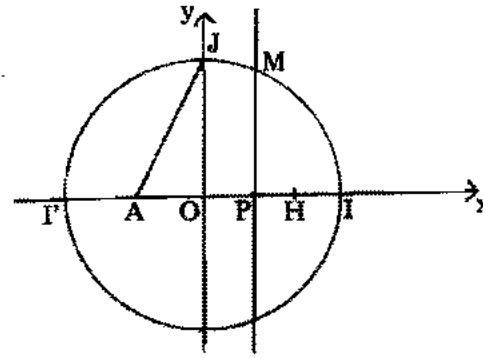

Figure 14

La perpendiculaire en P à Ox permet d'obtenir le point M du cercle tel que

$$\widehat{(\vec{OI}, \vec{OM})} = \widehat{\frac{2\pi}{5}}.$$

V. Compléments

En 1672, Mohr démontra que toute construction à la règle et au compas pouvait être réalisée en utilisant seulement le compas. Ce résultat est plus communément attribué à Mascheroni (1797). Bonaparte qui l'avait rencontré pendant les guerres d'Italie se signala à l'académie des Sciences en proposant la construction au compas seulement du centre d'un cercle donné. On trouvera cette construction dans [3].

Il existe de nombreuses variantes aux constructions à la règle et au compas : constructions à la règle seulement, constructions à la règle seulement mais en se donnant un cercle fixé, etc. On trouvera des informations à ce sujet dans [7].

BIBLIOGRAPHIE

[1] *Algebra*. Serge LANG, Addison-Wesley publishing company. 1974. Reading (Massachusetts).

[2] *Galois theory*. Ian STEWART. Chapman and Hall. London. 1973.

[3] *La quadrature du cercle*. François LE LIONNAIS. Revue du palais de la découverte, vol. 3, n° 30.

[4] *Correspondance Cantor-Dedekind. Philosophie mathématique*. Jean CAVAILLES. Hermann. 1962.

[5] *Les nombres de Fermat*. Jean DE BIASI. Bulletin A.P.M.E.P. n° 313.

[6] *Disquisitiones arithmeticae*. C.F. GAUSS. Yale University Press. New-Haven.
Il est disponible en français sous le titre : Recherches arithmétiques. Edition Blanchard. 1953.

[7] *Famous problems and others monographs*. F. KLEIN. Chelsea New-York. 1962.

[8] *Introduction to Field Theory*. I.T. ADAMSON. Gliver and Boyd. Edinburgh. 1964.