Constructions géométriques par intersections de coniques(*)

Jean-Marie Arnaudiès
et Pierre Delezoide

2. Aperçus algébriques

2.1. Caractérisation algébrique de la constructibilité à la règle et au compas

Introduction

On se place ici dans un plan affine euclidien. Il sera question principalement de constructibilité et de non constructibilité à la règle et au compas dans cette partie. Les termes « constructibilité » ou « constructible » sans précisions devront être pris en ce sens.

L'objectif de ce qui suit est en particulier de distinguer les angles qui sont trisécables à la règle et au compas de ceux qui ne le sont pas. On peut considérer qu'un angle est la donnée du centre O d'un cercle et de deux points A et B sur le cercle ; un tel angle peut être trisécable à la règle et au compas à partir de O, A, B sans que B soit constructible à partir de O et de A. De manière générale, une figure géométrique peut être déterminée par un ensemble de points, les points initiaux, fixés arbitrairement, et on se pose la question de savoir si tel ou tel point déterminé par les points initiaux est constructible à la règle et au compas à partir de ces points initiaux.

Nous voulons caractériser les points constructibles à partir des points initiaux par les propriétés algébriques de leurs coordonnées ; mais alors se pose le problème de savoir dans quel repère. Il est clair que le repère choisi doit être lié aux points initiaux. D'autre part il serait absurde de lier la constructibilité de tel ou tel point à des propriétés directement métriques ; si un point est constructible à partir d'un ensemble de points initiaux, ils le sera tout autant si on multiplie toutes les distances par $\sqrt[3]{2}$ ou par π. Nous verrons dans la suite quels repères utiliser.

Constructibilité à la règle et au compas

Définition 2.1

Soit D *une partie du plan affine euclidien ; une droite sera dite définie à partir de* D *si elle passe par deux points de* D *distincts. Un cercle sera dit défini à partir de* D *si son centre appartient à* D *et s'il passe par un point de* D.

(*) Suite du Bulletin 446, p. 367-382.

Définition 2.2

Soit D *un ensemble de points du plan ; un ensemble* D′ *est dit directement constructible à partir de* D *s'il existe deux figures distinctes* F_1 *et* F_2 *(cercles ou droites) définies à partir de* D *telles que* $D' \subset D \cup (F_1 \cap F_2)$.

Définition 2.3

Une suite finie $D = D_0 \subset \ldots \subset D_n$ *de parties du plan telle que, pour tout* $k \in [1, n-1]$, D_{k+1} *soit directement constructible à partir de* D_k *sera appelée une construction géométrique.*

Définition 2.4

Soit D *une partie du plan ; un point* M *du plan sera dit* D*-constructible s'il existe une construction géométrique* $D = D_0 \subset \ldots \subset D_n$ *telle que* $M \in D_n$. *Une partie* D′ *du plan sera dite* D*-constructible si tous ses éléments sont* D*-constructibles.*

Afin de ne pas alourdir cet exposé, nous admettrons les deux résultats suivants, qui sont d'ailleurs intuitifs.

Théorème 2.1

Soient D, D′ *des parties du plan telles que* $D \subset D'$ *; tout point* D*-constructible est aussi* D′*-constructible.*

Théorème 2.2

Soit D *une partie du plan et* D′ *une partie* D*-constructible, tout point* D′*-constructible est aussi* D*-constructible.*

Constructibilité par intersection de droites, de cercles et de coniques

Rappelons que par cinq points du plan, dont trois quelconques ne sont pas alignés, passe une conique propre (c'est-à-dire qui n'est pas réunion de droites) et une seule. Les définitions relatives à la constructibilité par intersection de droites, cercles et coniques peuvent être calquées sur les définitions relatives à la constructibilité à la règle et au compas, à la différence près que dans la définition de la D-constructibilité directe, on s'autorise à utiliser, en plus des droites et des cercles définis à partir de D, les coniques propres passant par cinq points de D.

Extensions quadratiques

Proposition 2.1

Soit K *un sous-corps de* **R** *et* $d \in K$, $d \geq 0$ et $\sqrt{d} \notin K$. *L'ensemble des réels de la forme* $\lambda + \mu\sqrt{d}$ *où* $(\lambda, \mu) \in K^2$, *est un sous-corps de* **R**. *Ce corps est noté* $K(\sqrt{d})$, *c'est un* K*-espace vectoriel de dimension* 2.

Démonstration :

L'ensemble $K(\sqrt{d})$ est le sous-K-espace vectoriel de **R** engendré par 1 et $\sqrt{d}$; il est de dimension 2. C'est un sous-anneau car $1 = 1 + 0 \times \sqrt{d} \in K(\sqrt{d})$ et, pour tous λ_1, λ_2, μ_1, μ_2 dans K :

$$(\lambda_1 + \mu_1 \sqrt{d})(\lambda_2 + \mu_2 \sqrt{d}) = \lambda_1\lambda_2 + \mu_1\mu_2 d + (\lambda_1\mu_2 + \lambda_2\mu_1)\sqrt{d} \in \mathrm{K}(\sqrt{d}).$$

Soit $x = \lambda + \mu\sqrt{d}$ non nul (avec λ et μ dans K), ce qui équivaut à $(\lambda, \mu) \neq (0,0)$ et entraîne $\lambda - \mu\sqrt{d} \neq 0$; on a :

$$\frac{1}{x} = \frac{1}{\lambda + \mu\sqrt{d}} = \frac{\lambda - \mu\sqrt{d}}{\lambda^2 - \mu^2 d} \in \mathrm{K}(\sqrt{d}).$$

L'ensemble $\mathrm{K}(\sqrt{d})$ est donc un sous-corps de **R**.

Définition 2.5

Soit K *un sous-corps de* **R** *; les corps* $\mathrm{K}(\sqrt{d})$*, où d est un élément positif de* K *et* $\sqrt{d} \notin \mathrm{K}$*, sont les extensions quadratiques réelles de* K.

Repères géométriques et tours d'extensions quadratiques

Définition 2.6

Un repère du plan affine euclidien sera dit géométrique s'il est orthogonal et si ses vecteurs de base sont de même norme.

Proposition 2.2

Soit $\mathcal{R}$ *un repère géométrique et* A_1 *et* A_2 *deux points distincts dont les coordonnées dans* $\mathcal{R}$ *sont dans un sous-corps* K *de* **R** *; le cercle de centre* A_1 *passant par* A_2 *a une équation dont les coefficients sont dans* K.

Démonstration :

Soient (a_1, b_1) les coordonnées de A_1 et (a_2, b_2) celles de A_2. Notons λ le carré scalaire des vecteurs de la base. Une équation du cercle de centre A_1 passant par A_2 est :

$$\lambda(x - a_1)^2 + \lambda(y - b_1)^2 = \lambda(a_2 - a_1)^2 + \lambda(b_2 - b_1)^2.$$

Une équation équivalente est :

$$x^2 + y^2 - 2a_1x - 2b_1y = a_2^2 + b_2^2 - 2a_1a_2 - 2b_1b_2.$$

Les coefficients de cette équation sont dans K.

Lemme 2.1

Si les coordonnées des éléments de l'ensemble D *dans un certain repère géométrique* $\mathcal{R}$ *du plan sont dans un sous-corps* K *de* **R***, et si* D′ *est directement constructible à partir de* D*, alors il existe un corps* K′ *qui est* K *ou une extension quadratique réelle de* K*, contenant l'ensemble des coordonnées dans* $\mathcal{R}$ *des éléments de* D′.

Démonstration :

Reprenons les notations de la définition 2.2 ; si les figures F_1 et F_2 sont deux droites définies à partir de D, il est clair qu'on peut prendre K′ = K.

Supposons que F_1 soit une droite et F_2 un cercle. Comme la droite F_1 passe par deux éléments de D, elle a une représentation paramétrique de la forme :

$$x = a + tu,$$
$$y = b + tv.$$

où a, b, u, v sont des éléments de K. En exprimant x et y en fonction de t dans une équation à coefficients dans K du cercle F_2, on obtient une équation du second degré à coefficients dans K, de discriminant $d \geq 0$, $d \in$ K, dont les solutions sont les paramètres des points d'intersection. Si $\sqrt{d} \in$ K, les coordonnées des éléments de D′ seront toutes dans K et sinon elles seront dans le corps $K(\sqrt{d})$, qui est une extension quadratique de K.

Si F_1 et F_2 sont deux cercles définis par des éléments de D, on se ramène au cas précédent en considérant l'intersection de l'un des cercles avec l'axe radical des deux cercles, dont une équation est la différence des équations des cercles (de termes de degré 2 égaux à $x^2 + y^2$), à coefficients dans K.

Théorème 2.3

Si les coordonnées dans un repère géométrique $\mathcal{R}$ des éléments d'un ensemble D *sont dans un sous corps* K *de* **R**, *pour tout point* M *constructible à partir de* D, *il existe une tour d'extensions quadratiques réelles, c'est-à-dire une suite croissante* $K_0 \subset \ldots \subset K_n$ *de sous-corps de* **R** *où, pour tout* $k \in [1, n]$, K_k *est une extension quadratique de* K_{k-1}, *telle que* $K_0 = K$ *et telle que les coordonnées de* M *appartiennent à* K_n.

Démonstration :

Par définition de la constructibilité (à la règle et au compas), il existe une construction géométrique $D = D_0 \subset D_1 \subset \ldots \subset D_n$ telle que $M \in D_n$. D'après le lemme 2.1, on peut associer à ces parties une suite croissante de sous-corps de **R**, $K = K_0 \subset K_1 \subset \ldots \subset K_n$, telle que les coordonnées de M appartiennent à K_n et telle que pour $k \in [1, n]$ le corps K_k soit K_{k-1} ou une extension quadratique réelle de K_{k-1} ; en supprimant les corps superflus, on obtient une tour d'extensions quadratiques réelles vérifiant les conditions.

Repères géométriques associés et réels constructibles

Définition 2.7

Soit D *une partie du plan ; le repère géométrique* $\mathcal{R} = \left(O, \vec{u}, \vec{v}\right)$ *sera dit associé à* D *si* O *et* $I = O + \vec{u}$ *appartiennent à* D.

Théorème 2.4

Soit D *une partie du plan, on appelle corps associé à* D, *noté* K_D, *le sous-corps de* **R** *engendré par les coordonnées des éléments de* D *dans un repère* $\mathcal{R}$ *associé à* D. *Ce corps ne dépend pas du repère* $\mathcal{R}$.

Démonstration :

Soient $\mathcal{R}_1 = \left(O_1, \overrightarrow{O_1I_1}, \overrightarrow{v_1}\right)$ et $\mathcal{R}_2 = \left(O_2, \overrightarrow{O_2I_2}, \overrightarrow{v_2}\right)$ deux repères géométriques associés à D et K_1, K_2 les sous-corps de **R** engendrés par les coordonnées des éléments de D, respectivement dans $\mathcal{R}_1$, $\mathcal{R}_2$. Comme les points O_2 et I_2 appartiennent à D, les coordonnées (a_2, b_2) de $\overrightarrow{O_2I_2}$ dans $\mathcal{R}_1$ sont dans le corps K_1. On voit facilement que, comme $\mathcal{R}_1$ est un repère géométrique, les coordonnées dans $\mathcal{R}_1$ du vecteur $\overrightarrow{v_2}$, qui est orthogonal à $\overrightarrow{O_2I_2}$ et de même carré scalaire, sont nécessairement $(-b_2, a_2)$ ou $(b_2, -a_2)$. Les coefficients de la matrice de passage P de la base $\left(\overrightarrow{O_1I_1}, \overrightarrow{v_1}\right)$ vers la base $\left(\overrightarrow{O_2I_2}, \overrightarrow{v_2}\right)$ sont donc dans le corps K_1. Les coefficients du vecteur colonne Ω des coordonnées dans $\mathcal{R}_1$ de la nouvelle origine O_2 sont aussi dans K_1. Pour tout point $M \in D$, si X_1 est le vecteur colonne de ses coordonnées dans $\mathcal{R}_1$, le vecteur colonne de ses coordonnées dans $\mathcal{R}_2$ est

$$X_2 = P^{-1}(X_1 - \Omega).$$

Cela prouve que les coordonnées dans $\mathcal{R}_2$ de M appartiennent au corps K_1. Comme ceci est vrai pour tout point $M \in D$, on en déduit $K_2 \subset K_1$; on a bien sûr de même $K_1 \subset K_2$, d'où $K_2 = K_1$.

Définition 2.8

Soit K *un sous-corps de* **R** ; *on dit qu'un réel x est* K-constructible *s'il existe une tour d'extensions quadratiques réelles* $K = K_0 \subset \ldots \subset K_n$ *telle que* $x \in K_n$.

Théorème 2.5

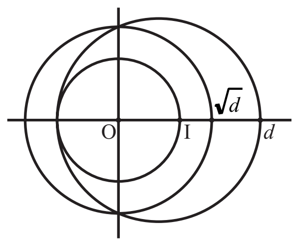
Soit D *un ensemble de points du plan et* $\mathcal{R}$ *un repère géométrique associé à* D ; *l'ensemble des coordonnées dans* $\mathcal{R}$ *des points* D-constructibles *est un corps contenant* K_D, *c'est l'ensemble des réels* K_D-constructibles. *Ce corps ne dépend pas de* $\mathcal{R}$, *il sera noté* $K_D^{[2]}$. *Les points* D-constructibles *sont les points dont les deux coordonnées dans* $\mathcal{R}$ *appartiennent à* $K_D^{[2]}$.

Démonstration :

Fixons pour l'instant le repère géométrique $\mathcal{R}$ associé à D et montrons que l'ensemble K' des coordonnées dans $\mathcal{R}$ des points D-constructibles est un sous-corps de **R** contenant le corps K_D engendré par les coordonnées dans $\mathcal{R}$ des éléments de D. Nous utiliserons de nombreuses fois de manière implicite les théorèmes 2.1 et 2.2.

Posons $\mathcal{R} = \left(O, \overrightarrow{OI}, \overrightarrow{OJ}\right)$; il est clair que J est D-constructible. Soit M un point D-constructible dont les coordonnées dans $\mathcal{R}$ sont (x, y) ; les points de coordonnées $(0, y)$, $(y, 0)$, $(x, 0)$ sont {O, I, J, M}-constructibles et comme {O, I, J, M} est D-constructible, ces points sont D-constructibles. L'ensemble K' est donc l'ensemble des réels x tels que le point de coordonnées $(x, 0)$ dans $\mathcal{R}$ soit D-constructible. Comme $O \in D$, on en déduit $0 \in K'$; si x_1 et x_2 sont dans K', il est clair que le point $(x_1 - x_2, 0)$ est D-constructible, donc $x_1 - x_2 \in K'$; K' est donc un sous-groupe additif. Comme le point I de coordonnées $(1, 0)$ est par hypothèse dans D, on en déduit $1 \in K'$; le rapport de deux éléments non nuls de K' est dans K' (Thalès), donc $K' \setminus \{0\}$ est stable par l'inverse et le produit. L'ensemble K' est donc un corps ; les coordonnées des éléments de D appartiennent à K′, puisque D est D-constructible ; K′ contient donc le sous-corps engendré dans **R** par les coordonnées des éléments de D, c'est-à-dire $K_D \subset K'$.

Montrons maintenant que K′ est l'ensemble des réels K_D-constructibles. Soit $x \in K'$, c'est par définition une coordonnée dans $\mathcal{R}$ d'un point D constructible M ; comme les coordonnées dans $\mathcal{R}$ des éléments de D appartiennent à K_D, d'après le théorème 2.3 et la définition 2.8, les coordonnées de M dans $\mathcal{R}$ sont K_D-constructibles, donc en particulier x est K_D-constructible. Réciproquement, il s'agit de démontrer que tout réel K_D-constructible est élément de K′, ou encore que, si $K_D = K_0 \subset \dots \subset K_n$ est une tour d'extensions quadratiques réelles, alors $K_n \subset K'$. C'est vrai si $n = 0$ puisque $K_D \subset K'$; supposons le résultat vrai pour $n - 1$. L'extension $K_{n-1} \subset K_n$ étant quadratique réelle, il existe un élément $d > 0$ dans K_{n-1} tel que $K_n = K_{n-1}(\sqrt{d})$; d'après l'hypothèse de récurrence, $d \in K'$; le point de coordonnées $(d, 0)$ est donc D-constructible. On construit le point de coordonnées $(\sqrt{d}, 0)$ à la règle et au compas à partir de O, I et du point de coordonnées $(d, 0)$; ce point est par conséquent D-constructible, d'où $\sqrt{d} \in K'$. Plus généralement, comme $K_{n-1} \subset K'$, $\sqrt{d} \in K'$ et que K′ est un corps, on a $K_n = K_{n-1}(\sqrt{d}) \subset K'$; cela termine la démonstration par récurrence.



Comme le corps K_D ne dépend pas de $\mathcal{R}$ et que K′ est l'ensemble des réels qui sont K_D-constructibles, il est clair que K′ ne dépend que de D, ce qui justifie la notation $K_D^{[2]}$. On dira qu'un sous-corps K de **R** est stable par racine carrée si $\forall\, d \in K \cap \mathbf{R}_+$, $\sqrt{d} \in K$. On peut remarquer que $K_D^{[2]}$ est le plus petit des sous-corps de **R** stables par racine carrée et contenant K_D.

Si M est D-constructible, par définition, ses deux coordonnées dans $\mathcal{R}$ appartiennent à $K_D^{[2]}$. Réciproquement, si les coordonnées x, y dans $\mathcal{R}$ d'un point M appartiennent $K_D^{[2]}$, comme les points $(x, 0)$ et $(0, y)$ sont D-constructibles. M est aussi D-constructible.

2.2. À propos de la trisection

Nous reprenons dans cette partie les hypothèses générales de la partie précédente ; nous utiliserons le théorème 2.5 pour démontrer la non trisécabilité de certains angles.

Un outil algébrique

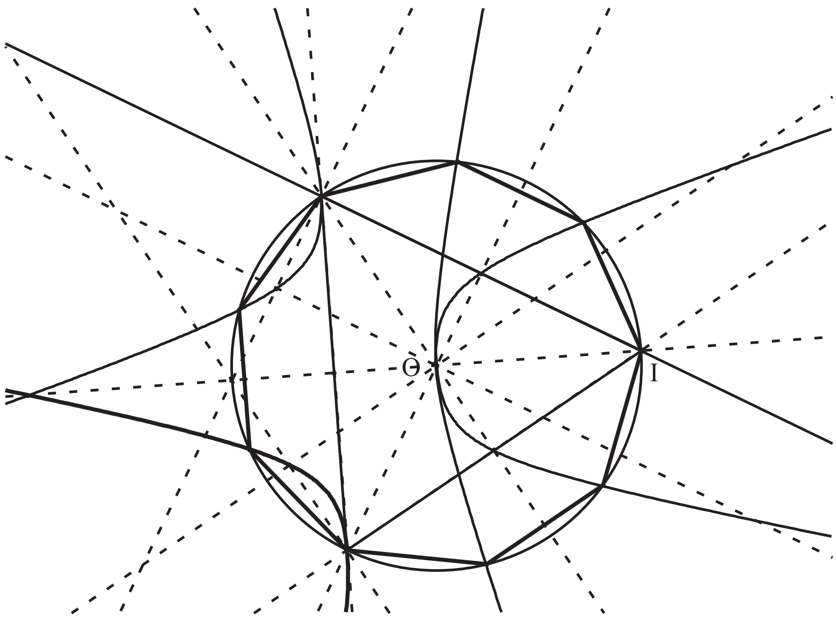
Théorème 2.6

Soit K *un sous-corps de* **R** *et* $P \in K[X]$ *un polynôme de degré* 3 *; si* P *a un zéro* K*-constructible, alors il a un zéro dans* K.

Démonstration :

Supposons $P(\beta) = 0$ où β est K-constructible ; soit une tour d'extensions quadratiques réelles $K = K_0 \subset K_1 \subset \ldots \subset K_p$ telle que $\beta \in K_p$. Soit r le plus petit entier dans $[0, p]$ tel que P ait au moins un zéro dans K_r ; si on avait $r > 0$, le polynôme P aurait un zéro $\alpha \in K_r$ et $\alpha \notin K_{r-1}$; comme K_r est de dimension 2 sur K_{r-1}, $(1, \alpha, \alpha^2)$ est une famille de K_r qui est liée sur K_{r-1} ; de plus $(1, \alpha)$ est libre sinon $\alpha \in K_{r-1}$, donc α annule un polynôme $A \in K_{r-1}[X]$ de degré exactement 2. Dans $K_{r-1}[X]$ on peut effectuer la division euclidienne $P = D\,A + R$ où R est de degré < 2 ; mais comme $R(\alpha) = (P - DA)(\alpha) = 0$, le polynôme R ne peut pas être de degré 1, sinon $\alpha \in K_{r-1}$; donc il est constant et constant nul. Cela prouve $P = D\,A$ dans $K_{r-1}[X]$; mais D est de degré 1 et par conséquent P a un zéro dans K_{r-1}, ce qui contredit la minimalité de r. On en déduit $r = 0$; par conséquent le polynôme P a un zéro dans K.

Non constructibilité de l'ennéagone



Nous nous plaçons dans un plan euclidien dans lequel on a choisi deux points initiaux O et I distincts. Nous nous proposons de montrer que l'ennéagone, c'est-à-dire le polygone régulier à 9 côtés, de centre O et dont un sommet est I, n'est pas constructible à la règle et au compas à partir de O et de I. Cela revient à dire que l'angle de mesure $2\pi/9$ n'est pas constructible à la règle et au compas.

Théorème 2.7

L'ennéagone n'est pas constructible à la règle et au compas à partir de son centre et de l'un de ses sommets.

Démonstration :

On pose $\theta = 2\pi/9$ et $x = \cos(\theta)$. On a :

$$\cos(3\theta) = \cos(2\pi/3) = -1/2$$

d'où, d'après la formule de trigonométrie :

$$4\cos^3(\theta) - 3\cos(\theta) = \cos(3\theta),$$

l'égalité :

$$4x^3 - 3x + \frac{1}{2} = 0$$

soit

$$8x^3 - 6x + 1 = 0.$$

Montrons que le polynôme $P(x) = 8x^3 - 6x + 1$ n'a aucun zéro rationnel. Supposons qu'il existe des entiers premiers entre eux p et q, $q \in \mathbf{N}^*$, tels que $P(p/q) = 0$; alors $8p^3 - 6pq^2 + q^3 = 0$, d'où $q^3 = 2p(3q^2 - 4p^2)$. On en déduit que p divise q^3 et, comme p est premier avec q^3, $p = \pm 1$. On a aussi $q^2(6p - q) = 8p^3$, donc q est pair et ne peut être que 2 puisque q^2 divise 8 ; on en déduit $3p - 1 = p^3 = p$, ce qui est impossible. D'après le théorème 2.6, le réel $x = 2\pi/9$ n'est donc pas **Q**-constructible.

L'ensemble D des points initiaux est ici constitué de l'origine O et d'un sommet I de l'ennéagone. Un repère géométrique associé à D est de la forme $\mathcal{R} = \left(O, \overrightarrow{OI}, \vec{v}\right)$.

Le corps K engendré par les coordonnées dans $\mathcal{R}$ des éléments de D est le plus petit corps contenant 0 et 1, c'est **Q**. D'après le théorème 2.5, les points D-constructibles sont les points dont les deux coordonnées dans $\mathcal{R}$ sont **Q**-constructibles ; comme ce n'est pas le cas pour $\cos(2\pi/9)$ d'après ce qui précède, on en déduit que le sommet de l'ennéagone dont l'affixe dans $\mathcal{R}$ est $e^{2i\pi/9}$ n'est pas constructible à la règle et au compas à partir de O et I.

Mais l'ennéagone est constructible par intersection de coniques par trisection de l'angle de mesure $\pi/3$ (voir la première partie de cet exposé dans le Bulletin vert 446), ce qui donne la figure du début de ce paragraphe.

Un angle trisécable, mais non constructible

Nous nous plaçons ici dans le plan affine euclidien $\mathbf{R}^2$, muni de son repère canonique.

Il existe un réel $\theta \in [0, \pi/2]$ tel que $\varphi(\theta) = \cos(\theta/3) - \cos(\theta) = 1/2$, puisque $\varphi(0) = 0$ et $\varphi(\pi/2) = \cos(\pi/6) > 1/2$. Pour une telle valeur de θ, l'angle $\widehat{IOM}$, où $O = (0,0)$, $I = (1,0)$, $M = (\cos(\theta), \sin(\theta))$ est évidemment trisécable à la règle et au compas à partir des points initiaux O, I, M, mais nous allons montrer que le point M n'est pas constructible à la règle et au compas à partir des point initiaux O, I.

D'après la formule de trigonométrie: $4\cos^3(\theta/3) - 3\cos(\theta/3) = \cos(\theta)$, la condition $\cos(\theta/3) - \cos(\theta) = 1/2$ est vérifiée si, et seulement si, en posant $x = \cos(\theta/3)$, on a :

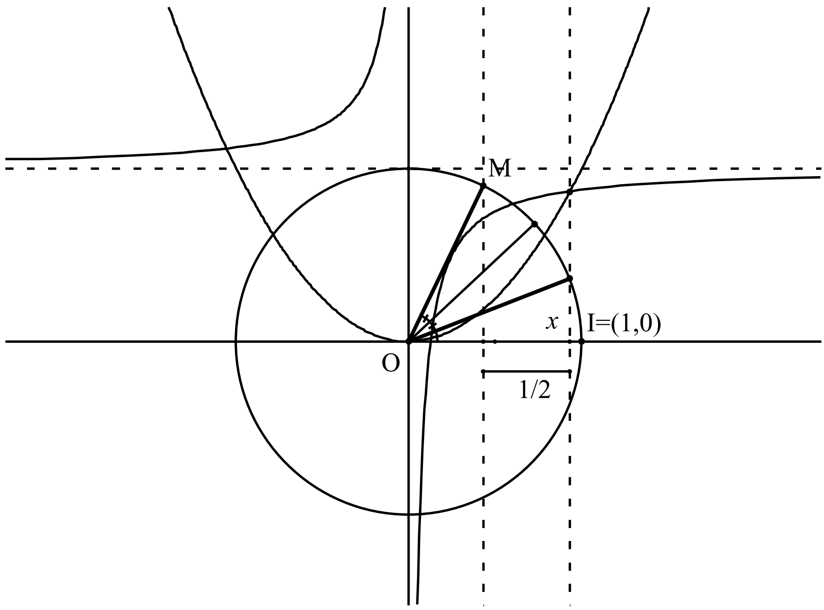
$$x - (4x^3 - 3x) = \frac{1}{2},$$

soit

$$8x(1 - x^2) = 1.$$

Il est assez facile de voir que le point M est constructible à la règle et au compas à partir de O et de I si, et seulement si, le point de coordonnées $(x, 0)$ l'est. Un repère associé aux points initiaux est le repère canonique et le corps engendré par les coordonnées des points initiaux est le corps des rationnels. Par conséquent, d'après les théorèmes 2.5 et 2.6, le point M ne sera pas constructible à la règle et au compas à partir de O et I si le polynôme $P = 8X(1 - X^2) - 1$ n'a pas de zéro rationnel. Ceci se démontre sans difficultés en utilisant la même méthode que dans l'exemple précédent.

Le point M n'est donc pas constructible à la règle et au compas à partir de O et I, mais il l'est par intersection de coniques. Les racines de l'équation $8X(1 - X^2) = 1$ sont les coordonnées x des points d'intersection de la parabole d'équation $y = x^2$ et de l'hyperbole équilatère d'équation $8x(1 - y) = 1$ (c'est la méthode de Descartes). Il est facile de voir que ces deux coniques propres passent par cinq points à coordonnées rationnelles, donc constructibles à partir des point initiaux O et I.



2.3. Construction de l'heptagone

Nous allons maintenant décrire et justifier une construction de l'heptagone régulier par intersection de coniques, à partir de son centre O et de l'un de ses sommets I. Un repère géométrique $\mathcal{R}$ associé à l'ensemble des points initiaux $D = \{O, I\}$ est de la forme $\left(O, \overrightarrow{OI}, \vec{v}\right)$. Les sommets de l'heptagone régulier sont les points dont les affixes z dans $\mathcal{R}$ vérifient $z^7 = 1$: ce sont les éléments du groupe des racines septièmes de l'unité dans $\mathbf{C}$. Ce groupe multiplicatif sera noté $\mathbf{U}_7$.

• Description de la construction

Soit $\omega \in \mathbf{U}_7\backslash\{1\}$; on sait que $\mathbf{U}_7$ est l'ensemble des puissances de ω, ce que l'on peut écrire :

$$\mathbf{U}_7 = \{1, \omega, \omega^2, \omega^3, \omega^{-1}, \omega^{-2}, \omega^{-3}\}.$$

On pose $p = \omega + \omega^2 + \omega^4$ et $q = \omega^3 + \omega^6 + \omega^5 = \omega^{-4} + \omega^{-1} + \omega^{-2}$. Comme $p + q + 1$ est la somme des zéros du polynôme $X^7 - 1$, on a $p + q + 1 = 0$, soit $p + q = -1$. D'autre part :

$$\begin{aligned} pq &= (\omega+\omega^2+\omega^4)(\omega^{-1}+\omega^{-2}+\omega^{-4}) \\ &= \omega^0+\omega^{-1}+\omega^{-3}+\omega^1+\omega^0+\omega^{-2}+\omega^3+\omega^2+\omega^0 = 2. \end{aligned}$$

Les complexes p et q sont donc les zéros du polynôme $X^2 + X + 2$.

Les complexes ω, ω^2, ω^4 sont les zéros du polynôme $X^3 - pX^2 + qX - 1$, puisque $\omega\,\omega^2\,\omega^4 = 1$ et $\omega\,\omega^2 + \omega\,\omega^4 + \omega^2\,\omega^4 = \omega^3 + \omega^{-2} + \omega^{-1} = q$. L'objectif est d'obtenir les points d'affixes ω, ω^2, ω^4 comme intersections du cercle $\mathcal{C}$ de centre O passant par I avec une hyperbole équilatère, mais si le cercle unité coupe une hyperbole équilatère en ces trois points, il y a un quatrième point dans l'intersection. Nous pouvons fixer arbitrairement ce point à I. Le polynôme unitaire qui a $(1, \omega, \omega^2, \omega^4)$ pour zéros est :

$$\begin{aligned} P &= (X-1)(X^3-pX^2+qX-1) \\ &= X^4-(p+1)X^3+(p+q)X^2-(1+q)X+1 \\ &= X^4+qX^3-X^2+pX+1. \end{aligned}$$

Les zéros de ce polynôme sont de module 1 ; en divisant l'équation $P(z) = 0$ par z^2 et en remplaçant $1/z$ par $\bar{z}$, on obtient l'équation complexe :

$$z^2+\bar{z}^2+\bar{p}z+p\bar{z}=1.$$

En posant $p = a + ib$, où a, b sont réels, et $z = x + iy$, l'équation devient :

$$x^2-y^2+ax+by=\frac{1}{2},$$

soit :

$$\left(x+\frac{a}{2}\right)^2-\left(y-\frac{b}{2}\right)^2=\frac{1}{2}+\frac{a^2}{4}-\frac{b^2}{4}.$$

Les complexes $1, \omega, \omega^2, \omega^4$ sont donc les affixes des intersections avec le cercle $\mathcal{C}$ de l'hyperbole équilatère $\mathcal{H}$ de centre le point Ω d'affixe $\dfrac{-a+ib}{2}=-\dfrac{\bar{p}}{2}=-\dfrac{q}{2}$, de directions asymptotiques les droites d'équations $x = \pm y$ passant par I. Les conjugués $1, \omega^{-1}, \omega^{-2}, \omega^{-4}$ sont évidemment les intersections avec $\mathcal{C}$ de l'hyperbole $\mathcal{H}'$, symétrique de $\mathcal{H}$ par rapport à Ox, de centre Ω' d'affixe $-\dfrac{p}{2}$.

Les centres Ω et Ω' de ces hyperboles sont constructibles à la règle et au compas à partir de $\{O, I\}$; en effet on peut remarquer que $-\dfrac{p}{2}-\dfrac{q}{2}=\dfrac{1}{2}$ et donc que Ω et Ω'

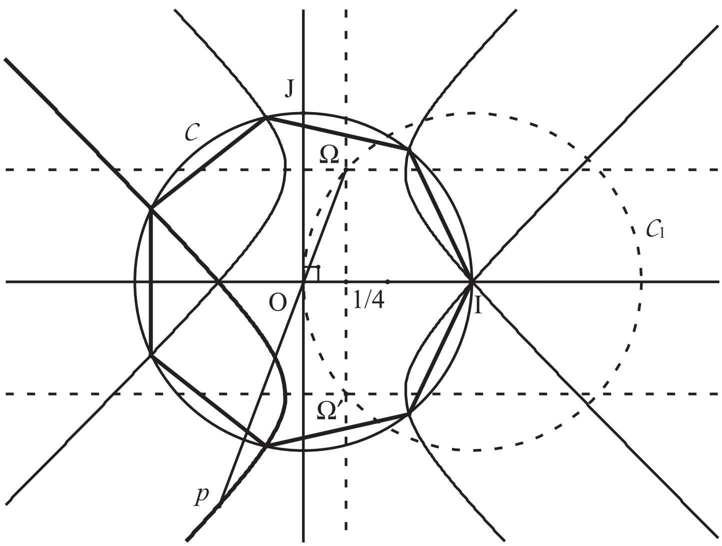
sont symétriques par rapport à l'axe Ox sur la droite d'équation $x = \frac{1}{4}$ et que d'autre part

$$\left|-\frac{p}{2}-1\right|^2 = \left(\frac{p}{2}+1\right)\left(\frac{q}{2}+1\right) = \frac{pq}{4}+\frac{p+q}{2}+1 = \frac{1}{2}-\frac{1}{2}+1 = 1.$$

Par conséquent Ω et Ω′ sont les intersections de la droite d'équation $x = \frac{1}{4}$ et du cercle $\mathcal{C}_1$ d'équation complexe $|z - 1| = 1$, de centre I et passant par O. L'hyperbole $\mathcal{H}$ passe par I et les symétriques de I par rapport aux axes de symétrie de l'hyperbole, ce qui fait quatre points ; elle passe aussi par le point d'affixe p puisque :

$$p^2 + \overline{p}^2 + \overline{p}p + p\overline{p} = (p+\overline{p})^2 = (p+q)^2 = 1.$$

Ces cinq points sont constructibles à la règle et au compas à partir de {O, I} et déterminent l'hyperbole $\mathcal{H}$. On obtient donc ainsi une construction, utilisant les intersections d'un cercle avec deux hyperboles équilatères, d'un heptagone régulier à partir de son centre et de l'un de ses sommets.



• Aperçu rapide sur les motivations algébriques

Le lecteur a pu remarquer que la clé de la construction est l'utilisation des sommes $p = \omega + \omega^2 + \omega^4$ et $q = \omega^{-1} + \omega^{-2} + \omega^{-4}$, qui sont les racines d'une équation du second degré à coefficients entiers. Ces sommes sont ce qu'on appelle des périodes de Gauss. C'est à l'aide d'une construction analogue que Gauss a pu prouver la constructibilité à la règle et au compas du 17-gone régulier. Ces regroupements de racines ne sont évidemment pas faits au hasard. On peut vérifier que chacune de ces sommes est la somme des puissances 1, 2, 4 de chacun de ses termes. Par exemple :

$$\omega^{-1}+\omega^{-2}+\omega^{-4}=\left(\omega^{-2}\right)^{1}+\left(\omega^{-2}\right)^{2}+\left(\omega^{-2}\right)^{4}.$$

Les calculs des puissances peuvent se faire modulo 7, puisque $\omega^7 = 1$. Introduisons l'anneau $\mathbf{Z}/7\mathbf{Z}$ des classes d'entiers modulo 7 et son groupe multiplicatif des classes non nulles, noté $(\mathbf{Z}/7\mathbf{Z})^*$, de cardinal 6. La partie $\{1, 2, 4\}$ de ce groupe est le sous-groupe des carrés. En effet, modulo 7, $1^2 \equiv (-1)^2 \equiv 1$, $2^2 \equiv (-2)^2 \equiv 4$ et $3^2 \equiv (-3)^2 \equiv 2$. Ce sous-groupe est le seul sous-groupe de cardinal 3, il est l'ensemble des puissances de la classe de $2 \equiv 3^2$; alors que le groupe entier est l'ensemble des puissances de la classe de 3. Ce sont ces propriétés algébriques de l'ensemble $\{1, 2, 4\}$ qui déterminent le comportement des périodes de Gauss associées p et q.

Le lecteur intéressé par le sujet pourra retrouver sur le site de 1'APMEP une étude des constructions de l'heptagone, du 13-gone régulier et du 17-gone régulier, ce par quoi tout a commencé pour Gauss et pour beaucoup de concepts algébriques actuellement utilisés, dont probablement la théorie de Galois. Le lien entre les sous-groupes des groupes multiplicatifs $(\mathbf{Z}/p\mathbf{Z})^*$ et la résolution des équations $z^p = 1$, pour $p = 7, 13, 17$, y sera décrit. Le lecteur pourra ainsi avoir des idées concrètes sur quelques applications de la théorie de Galois. Il y trouvera aussi une bibliographie sur le sujet plus riche que celle figurant ci-après.

BIBLIOGRAPHIE

[1] Lebesgue H. *Leçons sur les constructions géométriques*, Gauthier-Villars, Paris, 1950.

[2] Martin G.E., *Geometric constructions*, Springer-Verlag, New York, 1997.

[3] Carrega J.-C., *Théorie des corps, la règle et le compas*, Hermann, Paris, 2001.

[4] Gleason A.M., *Angle trisection, the heptagon, and the triskaidecagon*, Amer. Math. Monthly **95**, n° 3, p. 185-194, 1988.