Sur les nombres constructibles

Introduction : Depuis l'antiquité grecque, et même avant, la question de savoir quelles sont les figures ou les nombres constructibles à la règle et au compas est un point central des mathématiques. Pourquoi la règle et le compas ? Probablement parceque, bien qu'approximatifs, ce sont les instruments les seuls plus précis. Il est en effet plus difficile de construire une équerre aussi précise, par exemple... Mais il se peut aussi que la préférence de Platon pour ces deux instruments ait été motivée par bien d'autres raisons, pour certaines d'ordre philosophiques.

Mais l'histoire des constructions géométriques remonte plus loin que Platon. L'école de Pythagore, notamment, s'installe dans le sud de l'Italie actuelle au VI^e siècle av. J.-C., et développe de nombreuses constructions géométriques, qui étaient l'un des moyens priviligiés pour l'étude des nombres à une époque où l'on avait pas encore inventé le formalisme actuel de l'algèbre. Ainsi, ils ont probablement démontré les premiers l'irrationnalité de $\sqrt{2}$, par une méthode géométrique.

Enfin, outre l'intérêt des constructions géométriques pour l'étude même des nombres, c'est bien sûr un domaine dans lequel on arrive à formuler de manière simple et concrète une multitude de problèmes. Les grecs nous en ont d'ailleurs laissé de célèbres, dont celui de la quadrature du cercle, de la duplication du cube, ou encore de la trisection de l'angle. Pour une histoire plus complète de la genèse de la géométrie, voir par exemple G Godefroy, L'aventure des nombres ([**?**]). Citons enfin l'ouvrage de J.C Carrega, Théorie des corps : La règle et le compas ([**?**]), qui passe en revue de manière complète les problèmes que nous venons de citer, tant d'un point de vue historique que mathématique, ou encore le Cours d'algèbre, de D. Perrin ([**?**]).

1 Premiers exemples de nombres constructibles

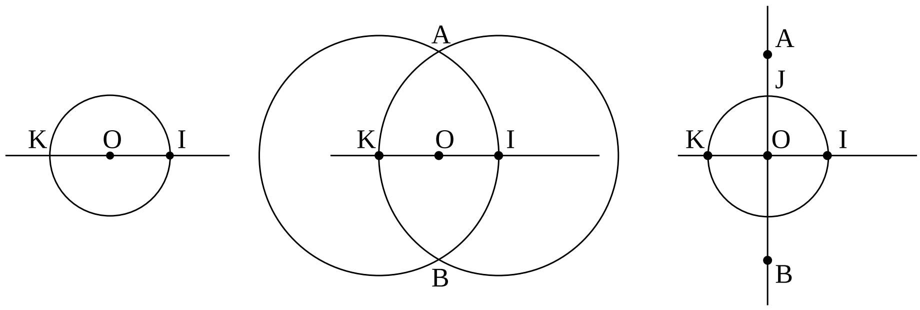
1.1 Points et réels constructibles

Pour réaliser une construction à la règle et au compas, on se donne deux points O et I, qui définissent un axe, muni d'une unité de longueur (la distance OI). Puis, à chaque étape, on a un certain nombre de points déjà construits (deux au départ), et l'on s'autorise uniquement à tracer une droite joignant deux de ces points, ou un cercle centré en l'un de ces points et de rayon la distance entre deux de ces points. Les intersections de ces objets définissent alors de nouveaux points dits constructibles. Par abus de language, on parle également de droites, de cercles, d'ensembles de points constructibles...

– De façon plus formelle, si $\mathcal{E}$ désigne un ensemble fini de points du plan, on considère l'ensemble $\mathcal{P}$ des droites joignant deux de ces points et des cercles centrés en l'un de ces points et de rayon la distance entre deux de ces points. On appelle "points construits à partir de E à la règle et au compas" l'ensemble des intersections des éléments de P.
– Un point M du plan est alors dit "constructible" s'il existe une suite de points $\mathrm{M}_1, \mathrm{M}_2, \ldots, \mathrm{M}_n = \mathrm{M}$ telle que pour tout $i \leq n$, M_i soit un point construit à partir de l'ensemble $\{\mathrm{O}, \mathrm{I}, \mathrm{M}_1, \ldots, \mathrm{M}_{i-1}\}$.

Bien sûr, toutes les constructions usuelles rentrent dans ce cadre. Ainsi, à partir de trois points $\mathrm{A}, \mathrm{B}, \mathrm{C}$ non alignés, le quatrième sommet D du parallélogramme ABCD est un point construit à partir de $\{\mathrm{A}, \mathrm{B}, \mathrm{C}\}$ à la règle et au compas : c'est en effet l'intersection des cercles C_1 et C_2, ou C_1 est le cercle de centre A et de rayon BC et C_2 le cercle de centre C et de rayon AB.

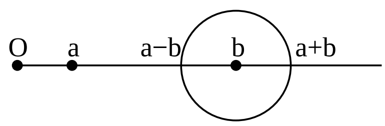
N.B. A partir des points O et I, de départ, on peut construire un repère du plan $\mathrm{O}, \mathrm{I}, \mathrm{J}$ orthonormé : d'abord, on construit le point K symétrique de I par rapport à O (intersection de la droite (OI) et du cercle C de centre O et de rayon OI). Ensuite, l'axe (OJ) comme médiatrice du segment [IK].Le point J est alors intersection de cet axe avec le cercle C déjà construit.



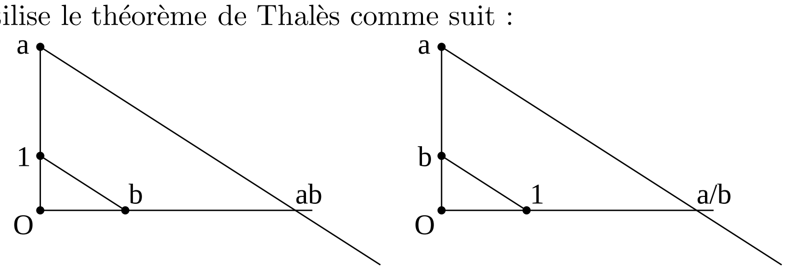
Enfin, un réel x est dit "constructible" s'il est l'abscisse ou l'ordonnée d'un point constructible. De manière équivalente, x est constructible s'il est l'abscisse d'un point de (OI) constructible.

1.2 L'ensemble des nombres constructibles

– On vérifie aisément que, si a et b sont deux nombres constructibles, il en est de même pour leur somme, leur différence :

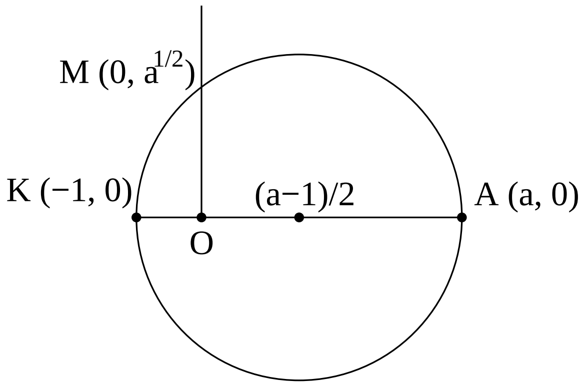


– Pour ce qui est du produit ou du rapport de deux nombres constructibles, on utilise le théorème de Thalès comme suit :



Nous avons vu précédemment comment construire une parallèle à une droite donnée passant par un point donné. Pour l'obtention du produit ab, par exemple, on construit le quatrième sommet du parallélogramme de sommets A $(0, a)$, J $(0, 1)$ et B $(b, 0)$¿

– Enfin, on peut construire la racine carrée d'un nombre a. La figure qui suit nécessite quelques explications : le point M construit a pour ordonnée $\sqrt{a}$. En effet M est sur le cercle de diamètre $a + 1$, donc le triangle qu'il forme avec les points K d'abscisse -1 et A d'abscisse a est rectangle. Les triangles AOM et KOM sont donc semblable, et l'on obtient $\frac{\text{OK}}{\text{OM}} = \frac{\text{OM}}{\text{OA}}$, soit $\text{OM}^2 = a$.



De ce qui précède, on tire le

Théorème 1.1 *L'ensemble $\mathcal{C}$ des nombres constructibles est un sous-corps de $\mathbb{R}$, stable par racine carrée.*

En effet l'ensemble $\mathcal{C}$ contient 0 et 1, donc est non vide. C'est un sous ensemble de $\mathbb{R}$ stable par addition et soustraction, c'est donc un sous-groupe de $(\mathbb{R}, +)$. Et comme $\mathcal{C}$ est stable par multiplication et par inverse, c'est un sous-corps de $\mathbb{R}$.

Comme $\mathcal{C}$ contient 1, on a $\mathbb{Q} \subset \mathcal{C}$. En effet $\mathbb{Q}$ est le sous-corps de $\mathbb{R}$ engendré par l'élément 1 : comme notre partie est stable par addition, elle contient tous les entiers, par récurrence ($2 = 1 + 1 \in \mathcal{C}$, et ainsi de suite, idem pour les entiers négatifs, $-1 = 0 - 1$...). Ensuite, comme $\mathcal{C}$ contient tous les entiers et est stable par quotient, on a immédiatement $\mathbb{Q} \subset \mathcal{C}$.

La stabilité par racine carrée a elle aussi été démontrée. Ceci nous permet d'affirmer que $\mathcal{C}$ est strictement plus gros que $\mathbb{Q}$: par exemple $\sqrt{2} \in \mathcal{C}$, et bien sûr $\sqrt{2}$ n'est pas rationnel.

2 Des conditions de constructibilité

2.1 Quelques propriétés des extensions de corps

Rappelons tout d'abord qu'un complexe α est dit algébrique s'il est racine d'un polynôme à coefficients rationnels, transcendant sinon. On note usuellement $\bar{\mathbb{Q}}$ l'ensemble des nombres algébrique. (Attention : $\bar{\mathbb{Q}}$ est un sous-corps de $\mathbb{C}$ et non de $\mathbb{R}$. Par exemple i est algébrique, puisque racine du polynôme X^2+1.)

Soit $\mathbb{K}$ un sous-corps de $\mathbb{R}$. Un réel α est dit algébrique sur $\mathbb{K}$ s'il est racine d'un polynôme à coefficients dans $\mathbb{K}$.

On notera $\mathbb{K}[\mathrm{X}]$ l'anneau des polynômes à coefficients dans $\mathbb{K}$.

Lemme 2.1 *Soit $\mathbb{K}$ un sous-corps de $\mathbb{R}$, et α un réel algébrique sur $\mathbb{K}$.*

Soit $\mathrm{I}(\alpha)$ l'ensemble des polynômes de $\mathbb{K}[\mathrm{X}]$ qui annulent α. Alors $\mathrm{I}(\alpha)$ est de la forme :

$$\mathrm{I}(\alpha) = \{\mathrm{P}, \exists \mathrm{Q} \in \mathbb{K}[\mathrm{X}], \mathrm{P} = \mathrm{M}_\alpha.\mathrm{Q}\}$$

où M_α est un polynôme défini de manière unique, à constante multiplicative près. On dit que M_α est un générateur de $\mathrm{I}(\alpha)$.

Démonstration Pour le lecteur familier avec la notion d'idéal, $\mathrm{I}(\alpha)$ est clairement un idéal de $\mathbb{K}[\mathrm{X}]$. Comme $\mathbb{K}[\mathrm{X}]$ est principal, $\mathrm{I}(\alpha)$ est engendré par un polynôme M_α et le résultat en découle.

L'unicité du polynôme M_α, à constante multiplicative près, est facile à obtenir. Si l'on a deux générateurs M_α et N_α, alors nécessairement M_α divise N_α et réciproquement, c'est-à-dire que M_α et N_α sont égaux à une constante multiplicative près. Nous allons toutefois redémontrer tout ceci sans utiliser le language des idéaux.

Soit donc $\mathrm{I}(\alpha)$ l'ensemble des polynômes qui annulent α. Cet ensemble contient des polynômes non nuls, puisque α est algébrique. Soit $\mathrm{A}(\alpha)$ l'ensemble des degrés des polynômes non nuls éléments de $\mathrm{I}(\alpha)$. $\mathrm{A}(\alpha)$ est une partie non vide de $\mathbb{N}^*$, elle admet donc un plus petit élément $d \geq 1$. Soit alors M_α un polynôme de $\mathrm{I}(\alpha)$ de degré d. Nous allons montrer que M_α vérifie la conclusion de notre lemme.

Tout d'abord $\mathrm{M}_\alpha \in \mathrm{I}(\alpha)$ donc M_α annule α, et il en est de même pour tous les multiples de M_α. C'est-à-dire que l'on a :

$$\{\mathrm{P}, \exists \mathrm{Q} \in \mathbb{K}[\mathrm{X}], \mathrm{P} = \mathrm{M}_\alpha.\mathrm{Q}\} \subset \mathrm{I}(\alpha)$$

Inversement, soit P un polynôme de $\mathrm{I}(\alpha)$. Effectuons la division euclidienne de P par M_α. Il existe deux polynômes Q et R vérifiant $\mathrm{P} = \mathrm{QM}_\alpha + \mathrm{R}$, où le polynôme R est de degré strictement inférieur à d, le degré de M_α. Mais alors, en appliquant cette égalité de polynômes à la valeur α, on obtient :

$$\mathrm{P}(\alpha) = \mathrm{Q}(\alpha)\,\mathrm{M}_\alpha(\alpha) + \mathrm{R}(\alpha)$$

Or par hypothèse $\mathrm{P} \in \mathrm{I}(\alpha)$, donc $\mathrm{P}(\alpha) = 0$. De même pour M_α. Après simplification, on obtient donc :

$$\mathrm{R}(\alpha) = 0 \text{ soit } \mathrm{R} \in \mathrm{I}(\alpha)$$

Mais alors R est un polynôme qui annule α, de degré strictement inférieur à d. Comme par construction d est le degré minimal des polynômes non nuls annulant α, on en déduit que R est le polynôme nul. D'où $\mathrm{P} = \mathrm{QM}_\alpha$, c'est-à-dire que tout polynôme de $\mathrm{I}(\alpha)$ est multiple de M_α, et nous avons bien le résultat annoncé :

$$\mathrm{I}(\alpha) = \{\mathrm{P}, \exists \mathrm{Q} \in \mathbb{K}[\mathrm{X}], \mathrm{P} = \mathrm{M}_\alpha.\mathrm{Q}\}$$

□

N.B. Nous avons en fait ici refait la démonstration du caractère principal de l'anneau $\mathbb{Q}[X]$.

Par définition, le polynôme M_α unitaire obtenu (ainsi on a bien l'unicité) est appelé polynôme minimal de α sur $\mathbb{K}$. Son degré est le degré de α sur $\mathbb{K}$.

N.B. Nécessairement le polynome minimal d'un réel α est irréductible dans $\mathbb{K}[X]$: sinon, on pourrait écrire $M_\alpha = PQ$ et donc $0 = M_\alpha(\alpha) = P(\alpha)\,Q(\alpha)$. Autrement dit α serait racine de P ou de Q, *i*.e. d'un polynôme de degré strictement inférieur à celui de M_α.

N.B. Si le degré de α sur $\mathbb{K}$ est 1, alors $\alpha \in \mathbb{K}$, et réciproquement. En effet, si le degré de α sur $\mathbb{K}$ est 1, alors il existe un polynôme P de degré 1 à coefficients dans $\mathbb{K}$ dont α est racine. P est de la forme $aX+b$, avec a et b dans $\mathbb{K}$, son unique racine est alors $\alpha = -\dfrac{b}{a}$, et $-\dfrac{b}{a} \in \mathbb{K}$ puisque $\mathbb{K}$ est un corps. Réciproquement, si $\alpha \in \mathbb{K}$ alors α est racine du polynôme $X - \alpha$, de degré 1 et à coefficients dans $\mathbb{K}$.

Enfin, on note $\mathbb{K}[\alpha]$ le $\mathbb{K}$-espace vectoriel engendré par les puissance de α.

$$\mathbb{K}[\alpha] = \{x, x = \sum_{p=0}^{q} x_p \alpha^p, q \in \mathbb{N}, x_p \in \mathbb{K}\}$$

Théorème 2.2 .

- $\mathbb{K}[\alpha]$ *possède une structure d'anneau.*
- *Si* α *est algébrique sur* $\mathbb{K}$*, de degré* d*, alors le* $\mathbb{K}$*-espace vectoriel* $\mathbb{K}[\alpha]$ *est de dimension finie* d*. Il est engendré par la famille* $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$.
- *Si* α *est transcendant sur* $\mathbb{K}$*, alors le* $\mathbb{K}$*-espace vectoriel* $\mathbb{K}[\alpha]$ *est de dimension infinie.*
- *Si* α *est algébrique sur* $\mathbb{K}$*, alors* $\mathbb{K}[\alpha]$ *est un corps.*

Démonstration Le premier point est immédiat : $\mathbb{K}[\alpha]$ est un sous-anneau de $\mathbb{R}$, en effet il contient 0, et est clairement stable par somme, inverse et multiplication.

Supposons α algébrique sur $\mathbb{K}$, de degré d. soit P un polynôme de degré d qui annule α. Tous les éléments de $\mathbb{K}[\alpha]$ sont des polynômes en α. Soit $x \in \mathbb{K}[\alpha]$ et $Q \in \mathbb{K}[X]$ tel que $x = Q(\alpha)$. Effectuons la division euclidienne de Q par P : il existe deux polynômes S et R, avec R de degré au plus $d-1$, tels que $Q = SP + R$. Appliquée à α, cette relation nous donne ;

$$x = Q(\alpha) = S(\alpha)\,P(\alpha) + R(\alpha)$$

Mais comme P annule α, on obtient $x = R(\alpha)$, c'est-à-dire que x peut s'écrire comme un polynôme en α de degré au plus $d-1$, ou si l'on préfère, que x est combinaison linéaire des éléments $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$.

Autrement dit, la famille $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ engrendre $\mathbb{K}[\alpha]$, qui est donc de dimension finie. Enfin cette famille est libre sur $\mathbb{K}$, car sinon on aurait une combinaison linéaire nulle des éléments $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ dont les coefficient ne seraient pas tous nuls, c'est-à-dire que l'on aurait un polynôme de degré au plus $d-1$ qui annulerait α, ce qui contredirait la définition de d.

$\mathbb{K}[\alpha]$ est donc de dimension exactement d.

Si α n'est pas algébrique sur $\mathbb{K}$, alors la famille $(\alpha^n)_{n\in\mathbb{N}}$ est libre sur $\mathbb{K}$ (le fait qu'elle soit liée veut dire exactement qu'il y a un polynôme sur $\mathbb{K}$ qui annule α). Donc $\mathbb{K}[\alpha]$ contient une famille libre infinie, donc est de dimension infinie.

Enfin, si α est algébrique sur $\mathbb{K}$, $\mathbb{K}[\alpha]$ est un corps : nous savons déjà que c'est un sous-anneau de $\mathbb{R}$, reste à montrer qu'il est stable par passage à l'inverse. Soit x un élément non nul de $\mathbb{K}[\alpha]$. D'après ce qui précède, nous savons que x peut s'écrire sous la forme :

$$x = \mathrm{P}(\alpha), \text{ avec P de degré au plus } d-1.$$

Or nous avons vu que le polynôme minimal M_α de α, de degré d, est irréductible. Donc P et M_α sont premiers entre eux : les seuls diviseurs de M_α sont 1 et lui-même, et M_α ne peut diviser P puisque P est de degré strictement plus petit.

Le théorème de Bézout nous assure qu'il existe deux polynômes U et V tels que $\mathrm{PU} + \mathrm{M}_\alpha \mathrm{V} = 1$. Appliquant cette relation à α, et remarquant une fois de plus que $\mathrm{M}_\alpha(\alpha) = 0$, on obtient :

$$x\mathrm{U}(\alpha) = 1$$

Or $\mathrm{U}(\alpha)$ est un élément de $\mathbb{K}[\alpha]$, donc l'inverse de x est dans $\mathbb{K}[\alpha]$, qui est donc bien un sous-corps de $\mathbb{R}$.

□

2.2 Extensions quadratiques et constructibilité

Si α est un nombre algébrique de degré 2 sur un sous corps $\mathbb{K}$, on dit alors que $\mathbb{K}[\alpha]$ est une extension quadratique de $\mathbb{K}$.

Lemme 2.3 *Si α est de degré 2 sur un sous-corps $\mathbb{K}$ de $\mathbb{R}$, alors il existe un réel positif $k \in \mathbb{K}$ tel que $\mathbb{K}[\alpha] = \mathbb{K}[\sqrt{k}]$.*

Démonstration Soit P un polynôme de degré 2 à coefficients dans $\mathbb{K}$ qui annule α. P est de la forme $a\mathrm{X}^2 + b\mathrm{X} + c$, avec a, b, et c dans $\mathbb{K}$.

Le réel α est racine de P, donc P a ses racines réelles. En particulier son discriminant $\Delta = b^2 - 4ac$ est positif.

- Si $\Delta = 0$, alors $-\dfrac{b}{2a}$ est racine double de P, ce qui n'est pas possible puisque α est racine de P et $\alpha \notin \mathbb{K}$. Or $-\dfrac{b}{2a} \in \mathbb{K}$ donc $\alpha \neq \dfrac{-b}{2a}$.
- Donc $\Delta > 0$, $\Delta \in \mathbb{K}$, et l'on a $\alpha = \dfrac{-b \pm \sqrt{\Delta}}{2a}$. Mais alors $\alpha \in \mathbb{K}[\sqrt{\Delta}]$ donc $\mathbb{K}[\alpha] \subset \mathbb{K}[\sqrt{\Delta}]$.

Réciproquement, $\sqrt{\Delta} = \pm(2a\alpha + b)$ donc $\sqrt{\Delta}$ est un polynôme en α, *i.e.* $\sqrt{\Delta} \in \mathbb{K}[\alpha]$ et donc $\mathbb{K}[\sqrt{\Delta}] \subset \mathbb{K}[\alpha]$.

On a bien $\mathbb{K}[\alpha] = \mathbb{K}[\sqrt{\Delta}]$, avec $\Delta > 0$ et $\Delta \in \mathbb{K}$.

Théorème 2.4 *Soit α un réel de degré 2 sur un sous-corps $\mathbb{K}$ de $\mathbb{R}$ Soit M le point de coordonnées $(\alpha, 0)$.*

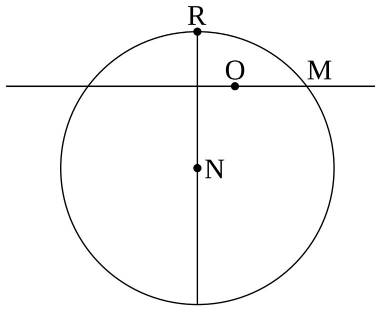
Alors il existe un ensemble fini de points $\mathcal{E} = \{\mathrm{M}_1, \ldots, \mathrm{M}_r\}$ à coordonnées dans $\mathbb{K}$ tels que le point M soit un point construit à partir de $\mathcal{E}$ à la règle et au compas.

Démonstration Soit $\mathrm{P} = a\mathrm{X}^2 + b\mathrm{X} + c$ un polynôme de degré 2 à coefficients dans $\mathbb{K}$, tel que α est racine de P. On suppose de plus $a = \frac{1}{2}$, quitte à changer pour cela P en $\frac{\mathrm{P}}{2a}$.

On sait qu'alors $\alpha = \frac{-b \pm \sqrt{\Delta}}{2a} = -b \pm \sqrt{\Delta}$. Supposons par exemple que l'on est dans le cas :

$$\alpha = -b + \sqrt{\Delta}$$

Alors $\Delta = b^2 - 4ac$ est un élément de $\mathbb{K}$, b également, et l'on obtient le point voulu par la construction suivante, à partir des points $\mathrm{N}\left(-b, \frac{1-\Delta}{2}\right)$ et $\mathrm{R}\left(-b, 1\right)$:



En effet, tout comme pour la construction de la racine carrée d'un nombre a (cf figure précédente), le point M construit est à distance $\sqrt{\Delta}$ de la droite (NR) d'équation $x = -b$. M a donc pour abscisse $-b + \sqrt{\Delta}$.

□

2.3 Quels sont les points constructibles ?

Définition Une suite finie $(\mathbb{K}_i)_{i \leq n}$ de sous-corps de $\mathbb{R}$ est dite avoir la propriété **P** si l'on a :
- (P1) $\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_n$.
- (P2) Pour tout $0 \leq i \leq n-1$, le corps $\mathbb{K}_{i+1}$ est une extension quadratique de $\mathbb{K}_i$.

Théorème 2.5 *Soit* M *un point du plan. Il y a équivalence entre :*

(i) *M est constructible.*

(ii) *Il existe une suite finie $(\mathbb{K}_i)_{i \leq n}$ de sous-corps de $\mathbb{R}$ ayant la propriété* **P**, *telle que les coordonnées de* M *sont dans $\mathbb{K}_n$.*

Démonstration Soit M un point constructible. Il existe une suite de points du plan $\mathrm{M}_1, \mathrm{M}_2, \ldots, \mathrm{M}_n = \mathrm{M}$ telle que pour tout $i \leq n$, M_i soit un point construit à partir de l'ensemble $\{\mathrm{O}, \mathrm{I}, \mathrm{M}_1, \ldots, \mathrm{M}_{i-1}\}$.

Soit alors, pour tout i, $\mathbb{K}_i$ le sous-corps de $\mathbb{R}$ engendré par les coordonnées de $\mathrm{O}, \mathrm{I}, \mathrm{M}_1, \ldots, \mathrm{M}_i$.

Alors $\mathbb{K}_0$ est le corps engendré par les coordonnés de O et I, c'est-à-dire par 0 et 1. Donc $\mathbb{K}_0 = \mathbb{Q}$.

Par définition de $\mathbb{K}_n$, les coordonnées de M sont dans $\mathbb{K}_n$.

Enfin, pour $i \leq n-1$, M_{i+1} est construit à partir des points $\mathrm{O}, \mathrm{I}, \mathrm{M}_1, \ldots, \mathrm{M}_i$, c'est à dire est l'intersection de deux objets qui sont :

- soit des droites joignant deux de ces points,
- soit des cercles centrés en l'un de ces points et de rayon la distance entre deux de ces points.

Or une droite passant par les points $\mathrm{A}\,(a_1, b_1)$ et $\mathrm{B}\,(a_2, b_2)$ a pour équation :

$$\begin{vmatrix} x - a_1 & x - a_2 \\ y - b_1 & y - b_2 \end{vmatrix} = 0$$

Et un tel cercle, de centre $\mathrm{C}\,(\alpha, \beta)$, et de rayon la distance entre les points $\mathrm{D}\,(a_3, b_3)$ et $\mathrm{E}\,(a_4, b_4)$ a une équation de type :

$$(x-\alpha)^2 + (y-\beta)^2 = (a_3 - a_4)^2 + (b_3 - b_4)^2$$

Dans tous les cas, les coordonnées de M_{i+1} sont solutions d'un système de deux équations de degrés 1 ou 2 à coefficients dans $\mathbb{K}_i$.

- Le cas de l'intersection de deux droites est trivial : dans ce cas les coordonnées x_{i+1} et y_{i+1} du point M_{i+1} sont encore dans $\mathbb{K}_i$.
- Pour ce qui est de l'intersection d'une droite et d'un cercle, on s'aperçoit que, par remplacement, on obtient une équation de degré 2 en x et d'expression de y en fonction de x sous la forme $\lambda x + \mu$, avec λ et μ dans $\mathbb{K}_i$ (ou l'inverse). Dans ce cas, x_{i+1} et y_{i+1} sont donc tous deux dans une même extension quadratique de $\mathbb{K}_i$.
- Le cas de deux cercles est un peu plus subtil : le couple (x, y) cherché est solution d'un système à coefficients dans $\mathbb{K}_i$ du type :

  $$\begin{cases} x^2 + y^2 + ax + by + c = 0 \\ x^2 + y^2 + dx + ey + f = 0 \end{cases}$$

  Mais ce système est équivalent au système :

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

  c'est-à-dire que le point construit peut aussi être construit comme l'intersection d'un cercle et d'une droite obtenus à partir de points à coordonnées dans $\mathbb{K}_i$. D'après ce qui précède, les coordonnées x_{i+1} et y_{i+1} sont là aussi dans une même extension quadratique $\mathbb{K}_{i+1}$ du corps $\mathbb{K}_i$.

Réciproquement, s'il existe une suite finie $(\mathbb{K}_i)_{i \leq n}$ de sous-corps de $\mathbb{R}$ ayant la propriété P, telle que les coordonnées de M sont dans $\mathbb{K}_n$, alors le point M est constructible. Nous allons montrer ce résultat par récurrence sur n.

Le cas $n = 0$ est évident : le corps K_n n'est autre que le corps $\mathbb{Q}$, et nous avons vu que les rationnels sont constructibles. Si M est un point du plan de coordonnées rationnelles, on sait construire le point H de l'axe des abscisse de même abscisse que M et le point K des axes des ordonnées de meme ordonnée que M. La construction de M à partr de ces deux points est alors on ne peut plus simple (M est le quatrième sommet du parallélogramme OHMK).

Supposons le résultat établi pour un entier n. Soit alors une suite finie $(\mathbb{K}_i)_{i \leq n+1}$ de sous-corps de $\mathbb{R}$ ayant la propriété **P**,et M un point à coordonnées (x_{n+1}, y_{n+1}) dans $\mathbb{K}_{n+1}$.

Soit H son projeté orthogonal sur l'axe des abscisses, K son projeté orthogonal sur l'axe des ordonnées.

x_{n+1} est dans une extension quadratique de $\mathbb{K}_n$, donc le théorème **??** nous assure que le point H de coordonnées $(x_{n+1}, 0)$ est construit à la règle et au compas à partir d'un ensemble de points à coordonnées dans $\mathbb{K}_n$, eux-même constructibles par hypothèse de récurrence. Donc H est constructible.

De la même façon, le point H$'$ de coordonnées $(y_{n+1}, 0)$ est constructible. On peut donc construire le point K de coordonnées $(0, y_{n+1})$, comme l'intersection de l'axe des ordonnées et du cercle de centre O et de rayon OH$'$.

La construction de M à partir des points O H et K est là encore immédiate, donc M est constructible. On conclut par le principe de récurrence.

$\square$

Théorème 2.6 *Pour qu'un nombre α soit constructible, il faut que son degré sur $\mathbb{Q}$ soit de la forme 2^n, où n est un entier.*

Démonstration C'est une conséquence assez directe du théorème précédent. Le réel α est constructible si et seulement si il existe un point M constructible dont l'une des coordonnées est α.

Soit donc α un réel constructible et M un point constructible dont l'une des coordonnées est α. Tout d'abord α est constructible donc algébrique. Soit d son degré.

Soit $(\mathbb{K}_i)_{i \leq n}$ une suite de sous-corps de $\mathbb{R}$ ayant la propriété **P**, telle que M ait ses coordonnées dans $\mathbb{K}_n$. Alors $\alpha \in \mathbb{K}_n$ donc $\mathbb{Q}[\alpha] \subset \mathbb{K}_n$. $\mathbb{Q}[\alpha]$ est donc un sous-corps de $\mathbb{K}_n$, donc $\mathbb{K}_n$ est un espace vectoriel sur $\mathbb{Q}[\alpha]$, de dimension d'.

Mais nous savons que $\mathbb{Q}[\alpha]$ et $\mathbb{K}_n$ sont tous deux des espaces vectoriels sur $\mathbb{Q}$, de dimensions respectives d et 2^n. On a donc $2^n = dd'$, c'est-à-dire que d divise 2^n, et donc d est une puissance de 2.

$\square$

Corollaire 2.7 *La duplication du cube est impossible avec pour seuls instruments la règle et le compas.*

En effet, disposant d'un cube de volume 1, on voudrait construire un cube de volume 2, c'est-à-dire de côté $\sqrt[3]{2}$.

Mais le réel $\sqrt[3]{2}$ est de degré 3 sur $\mathbb{Q}$. En effet, il est racine du polynôme $\mathrm{X}^3 - 2$. Et ce polynôme est irréductible sur $\mathbb{Q}$, car sinon il aurait un facteur de degré 1, donc une racine rationnelle. Or ses racines dans $\mathbb{C}$ sont $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$, aucun de ces trois complexes n'étant rationnel (ici, j désigne le complexe $e^{-\frac{2i\pi}{3}} = -\dfrac{1}{2} + i\dfrac{\sqrt{3}}{2}$).

Donc $\sqrt[3]{2}$ est de degré 3 sur $\mathbb{Q}$, et donc n'est pas constructible. $\square$

Références

[1] G. Godefroy *L'aventure des nombres*, Odile Jacob, 1997.

[2] J.C. Carrega *Théorie des corps ; La règle et le compas*, Hermann, 1981.

[3] D. Perrin, *Cours d'algèbre*, Ecole Normale Supérieure, 1990.