De la constructibilité des nombres

Victor Lecerf *

Résumé

Nous proposons ici d'étudier des propriétés sur les points constructibles à la règle et au compas, ainsi que certaines propriétés d'algèbre corporelle. L'objectif principal est d'apporter une démonstration au théorème de Wantzel, et d'étudier ensuite ses conséquences sur des problèmes de la Grèce antique.

Abstract

We aim to study properties of points constructibles with only straightedge and compass, as well as field algebra properties. The main aim is to bring a proof to Wantzel's theorem, and then study its consequences on ancient Greece problems.

Table des matières

Notations Si $A \subset \mathbb{R}^2$ est un sous-ensemble de point, on notera $\mathcal{D}_A$ l'ensemble des droites passants par deux points distincts de A. L'ensemble des cercles dont le centre et au moins un point de la circonférence sont deux points distincts de A sera noté $\mathcal{C}_A$. La distance euclidienne entre A et $B \in \mathbb{R}^2$ sera notée $\mathrm{d}(A, B)$.

1 Considérations géométriques

1.1 Définitions

Définition 1.1.1. *Soit $A \subset \mathbb{R}^2$. Un point est dit constructible en une étape à partir de A si il est intersection de deux éléments distincts de $\mathcal{D}_A \cup \mathcal{C}_A$, ou s'il est égale à $O = (0,0)$ ou $I = (1,0)$. Notons que nous pouvons construire l'axe des abscisses et des ordonnées facilement. L'axe des abscisses est traçable puisqu'on a O et I*

Définition 1.1.2. *Un point P est dit constructible en n étapes à partir de {O,I} si il existe $n+1$ points constructibles $P_0, \dots, P_n$ tels que :*

- $P_0 \in \{O, I\}$
- *Pour tous $k \in [\![0, n-1]\!]$, P_{k+1} est constructible en une étape depuis $\{O, I\} \cup \{P_0, \dots, P_n\}$*
- $P_n = P$

*Les recherches ont été réalisées avec Victor Sannier.

Exemple : *On peut construire* $(0,1)$ *car ce point est intersection du cercle de centre* O *passant par* I*, et de l'abscisse. Notons que nous pouvons construire l'axe des abscisses et des ordonnées facilement. L'axe des abscisses est traçable puisqu'on a* O *et* I*, et on trace ensuite l'axe des ordonnées comme la médiatrice du segment* (I, I') *avec* $I' = (-1, 0)$*.*

Définition 1.1.3. *Un nombre* $a \in \mathbb{R}$ *est dit constructible si* $(a, 0)$ *est constructible.*

On note $\mathbb{E}$ l'ensemble des nombres constructibles.

1.2 Constructions

Proposition 1.2.1. *Un nombre* $x \in \mathbb{R}_+$ *est constructible si et seulement si il existe* A *et* $B \in \mathbb{E}^2$ *tels que* $\mathrm{d}(A, B) = x$*.*

Démonstration. $\boxed{\Longrightarrow}$ Soit $x \in \mathbb{E}$ positif. Par définition on peut construire $(x, 0)$.

$\boxed{\Longleftarrow}$ Soient A et B des points de $\mathbb{E}^2$ tels que $\mathrm{d}(A, B) = x$. Montrons que l'on peut construire $(x, 0)$. Dans un premier temps, on peut tracer le cercle de centre B et de rayon $|x|$. On peut alors créer un nouveau point $\widetilde{A}$ tel que O, $\widetilde{A}$ et B soient alignés et la distance entre $\widetilde{A}$ et B soient toujours $|x|$. On trace alors les cercles centrés en O de rayons respectifs $\mathrm{d}(O, \widetilde{A})$ et $\mathrm{d}(O, B)$. On crée les points A' et B' intersectant l'axe des abscisses. Ces points vérifient encore $\mathrm{d}(A', B') = |x|$. On construit maintenant A'' l'autre intersection de A' avec le cercle de centre O et de rayon $\mathrm{d}(O, A')$. On construit maintenant le point M milieu du segment $[A'', B]$. On a alors $\mathrm{d}(O, M) = \dfrac{|x|}{2}$. En effet, on a :

$$\overrightarrow{OM} + \overrightarrow{OM} = \overrightarrow{OA'} + \overrightarrow{A'B'} + \overrightarrow{B'M} + \overrightarrow{OM} = \overrightarrow{A''O} + \overrightarrow{A'B'} + \overrightarrow{MA''} + \overrightarrow{OM} = \overrightarrow{A'B'} + \overrightarrow{MO} + \overrightarrow{OM} = \overrightarrow{AB}$$

□

Proposition 1.2.2. *Soient* $(a, b) \in \mathbb{R} \times \mathbb{R}^*$ *deux nombres constructibles. Sont alors constructibles les nombres :* $a + b$*,* $a - b$*,* ab*,* $\frac{a}{b}$*,* $\sqrt{a}$*.*

Remarque On en déduit que $\mathbb{E}$ est un sous-corps de $\mathbb{R}$. Puisque c'est un sous-corps de $\mathbb{R}$, il contient en particulier $\mathbb{Q}$.

2 Considérations algébriques

Dans toute cette section, $\mathcal{M}$ désignera un sous-corps de $\mathbb{R}$.

2.1 Équations des droites et des cercles dans un sous-corps de $\mathbb{R}$

Lemme 2.1.1. *Toute droite ou cercle défini(e) par des éléments de* $\mathcal{M}$ *admet une équation polynomiale à coefficients dans* $\mathcal{M}$*.*

Démonstration. — Soit une droite passant par les points $P = (a, b)$ et $P' = (a', b')$ dans $\mathcal{M}^2$. On a alors que pour tout (x, y) point de la droite :

$$\begin{vmatrix} x - a & b - a \\ y - a' & b' - a' \end{vmatrix} = 0$$

— Soit Σ un cercle de centre $(c, c') \in \mathcal{M}^2$ de rayon R. $(x, y) \in \mathbb{R}^2$ *si et seulement si* $(x - c)^2 + (y - c')^2 = R^2$

□

2.2 Algèbre corporelle

Définition 2.2.1. *Soit $\mathbb{K}$ un corps. Une extension de $\mathbb{K}$ est un corps $\mathbb{L}$ possédant un sous-corps $\mathcal{H}$ isomorphe à $\mathbb{K}$.*

En particulier, on peut définir une loi de composition externe telle que $\mathbb{L}$ soit un $\mathbb{K}$-espace vectoriel. On appelle son degré $[\mathbb{L} : \mathbb{K}] = \dim_{\mathbb{K}}(\mathbb{L})$. Une extension de degré 2 est dite quadratique.

Définition 2.2.2. *Soit $\mathbb{L}$ une extension du corps $\mathbb{K}$. Soit $\alpha \in \mathbb{L}$. On note $\mathbb{K}[\alpha]$ la plus petite extension de $\mathbb{K}$ contenant α.*

Lemme 2.2.1. *Soit $\mathbb{L}$ un corps et $\mathbb{K}$ un sous-corps. Soit $\alpha \in \mathbb{L}\backslash\mathbb{K}$. Si le polynôme minimal de α est de degré 2, alors $\mathbb{K}[\alpha]$ est une extension quadratique de $\mathbb{K}$.*

Démonstration. Soit Π le polynôme minimal de $x \in \mathbb{L}\backslash\mathbb{K}$. Alors $\mathrm{dg}(\Pi) = 2$, ce qui signifie que $(1, x, x^2)$ est lié. Pourtant, $(1, x)$ est libre car x est dans $\mathbb{L}$ mais pas dans $\mathbb{K}$. Soit $y \in K[x]$. Il existe $P \in \mathbb{K}[X]/(\Pi)$ tel que $y = P(x)$. La division euclidienne de P par Π donne :

$$P(X) = Q\Pi(X) + (aX + b)$$

Avec a et b dans $\mathbb{K}$. Alors $y = P(x) = Q(x)\Pi(x) + (ax + b) = ax + b$. $(1, x)$ est donc génératrice. Ainsi : $[\mathbb{K}[x] : \mathbb{K}] = 2$.

□

2.3 Théorème

Théorème 2.3.1. *Soit $P = (x, y) \in \mathbb{R}^2$ un point constructible à partir d'éléments de $\mathcal{M}^2$. Alors les coordonnées de P sont contenus soit dans $\mathcal{M}$, soit dans une extension quadratique de $\mathcal{M}$.*

Démonstration. On étudie trois cas :

— Si P est intersection de deux droites distinctes, ses coordonnées vérifient :

$$\begin{cases} ax + by + c &= 0 \\ a'x + b'y + c' &= 0 \end{cases}$$

où les différents coefficients sont dans $\mathcal{M}$. Avec les formules de Cramer, on peut exprimer x et y en fonctions de ces derniers.

— Si P est intersection d'une droite et d'un cercle, on a :

$$\begin{cases} ax + by + c &= 0 \\ (x - a')^2 + (y - b')^2 - c'^2 &= 0 \end{cases}$$

Ainsi, x est annulé par un polynôme de degré 2. Si ce polynôme est irréductible, le lemme précédent nous permet d'affirmer que $\mathcal{M}[x]$ est une extension de $\mathcal{M}$ de degré 2. Sinon, par linéarité $x \in \mathcal{M}$. La première relation permet de vérifier que x et y sont bien dans le même corps.

— Si P est intersection de deux cercles, notons les équations :

$$\begin{cases} (x - a)^2 + (y - b)^2 - c^2 &= 0 \\ (x - a')^2 + (y - b')^2 - c'^2 &= 0 \end{cases}$$

On a alors $(x-a)^2+(y-b)^2-c^2 = (x-a')^2+(y-b')^2-c'^2 = 0$. En développant cette équation, on obtient :

$$2(a' - a)x + 2(b' - b)y + a^2 - a'^2 + b^2 - b'^2 - c^2 + c'^2 = 0$$

Cette équation est bien à coefficient dans $\mathcal{M}$.

□

Théorème 2.3.2 (Wantzel)**.** *Un nombre réel x est constructible* si et seulement si *il existe une suite fini $(L_0, L_1, \ldots, L_p)$ de sous-corps de $\mathbb{R}$ vérifiant :*

i. $L_0 = \mathbb{Q}$

ii. $\forall i \in [\![0, p-1]\!]$, $L_i \subset L_{i+1}$

iii. $x \in L_p$

Démonstration. — Si une telle tour d'extensions quadratiques, les L_i sont des sous-corps de $\mathbb{E}$, donc $x \in \mathbb{E}$.

— Si x est constructible, il existe une famille $(P_0, P_1, \ldots, P_p)$ de points de $\mathbb{R}^2$ tels que :

1. $P_0 \in \{O, I\}$.
2. $\forall i \in [\![0, p-1]\!]$, P_{i+1} est constructible à partir de $\{O, I\} \bigcup \{P_0, P_1, \ldots, P_i\}$
3. $P_p = (x, 0)$

Le lemme précédent permet de construire une tour d'extensions quadratiques vérifiant les hypothèses. □

Proposition 2.3.1 (Condition nécessaire)**.** *Si a est constructible, alors le degré de son polynôme minimal dans $\mathbb{Q}[X]$ est une puissance de 2.*

Démonstration. Soit a un réel constructible. Selon le théorème de Wantzel, il existe une tour d'extension quadratique $(L_0, L_1, \ldots, L_p)$ avec $L_0 = \mathbb{Q}$ et $a \in L_p$.

$$\forall i \in \mathbb{N}, [L_{i+1} : L_i] = 2$$

Par le théorème de la base télescopique, $[L_p : L_0] = 2^p$. Ce théorème nous indique aussi que $[L_p : \mathbb{Q}] = [L_p : \mathbb{Q}(x)][\mathbb{Q}(x) : \mathbb{Q}]$. Puisque $[L_p : \mathbb{Q}]$ est une puissance de deux, ses deux facteurs le sont aussi. En particulier, $[\mathbb{Q}(x) : \mathbb{Q}]$ est une puissance de deux.

□

Corollaire 1. *On ne peut pas dupliquer un cube à la règle et au compas.*

Démonstration. Le polynôme minimal de $\sqrt[3]{2}$ est $X^3 - 2$, de degré 3.

□

3 Applications

3.1 Irréductibilité

Définition 3.1.1. *On appelle contenu d'un polynôme de $\mathbb{Z}[X]$ le pgcd de ses coefficients.*

Lemme 3.1.1. *Soient P et $Q \in \mathbb{Z}[X]$. Alors $c(PQ) = c(P)c(Q)$.*

Démonstration. Posons $P_1 = \dfrac{1}{c(P)}P$ et $Q_1 = \dfrac{1}{c(Q)}Q$. Supposons par l'absurde que $c(P_1Q_1) \neq 1$. Il existe alors p premier divisant $c(P_1Q_1)$, donc tous les coefficients. On a alors dans $(\mathbb{Z}/p\mathbb{Z})[X]$:

$$\overline{P_1Q_1} = \overline{P_1}\,\overline{Q_1} = \overline{0}$$

Par intégrité, p divise tous les coefficients de P_1 ou de Q_1. Alors p diviserait le contenu d'un des deux polynômes. p divise 1, ce qui est absurde. Ainsi, $c(P_1Q_1) = 1$. D'où $c(PQ) = c(P)c(Q)c(P_1Q_1) = c(P)c(Q)$.

□

Lemme 3.1.2. *Si $PQ \in \mathbb{Z}[X]$ avec P et $Q \in \mathbb{Q}[X]$ unitaires. Alors, P et $Q \in \mathbb{Z}[X]$.*

Démonstration. On écrit $P(X) = \displaystyle\sum_{i=0}^{n} \frac{\alpha_i}{\beta_i}$ et $Q(X) = \displaystyle\sum_{i=0}^{m} \frac{\gamma_i}{\delta_i}$ en supposant les fractions irréductibles. On note $\beta = \text{ppcm}(\beta_1, \ldots, \beta_n)$ et $\delta = \text{ppcm}(\delta_1, \ldots, \delta_m)$. Par le lemme de Gauss :

$$c(\beta P \delta Q) = c(\beta P)c(\delta Q)$$

De plus, $c(\beta P \delta Q) = \beta\delta c(PQ)$. Montrons que $c(\beta P) = 1$. On a que $\beta P = \sum_{i=0}^{n} \alpha_i \frac{\beta}{\beta_i}$ et

$$c(\beta P) = \bigwedge_{i=0}^{n} \left(\frac{\alpha_i}{\beta_i} \bigvee_{j=0}^{n} \beta_j \right)$$

Supposons par l'absurde qu'il existe p premier divisant $c(\beta P)$. Ainsi :

$$\forall i \in [\![0, n]\!],\ p \mid \alpha_i \frac{\beta}{\beta_i}$$

Ainsi, $p \mid \alpha_n \frac{\beta}{\beta_n}$ donc $p \mid \beta$. Posons $A = \{v_p(\beta_k) \mid k \in [\![0, n]\!]\}$. C'est une partie non vide de $\mathbb{N}$ majorée, elle admet donc un minimum qu'on note $v_p(\beta_k)$ (puisqu'un tel k existe). Par définition de β et de k, on sait que $v_p(\beta_k) = v_p(\beta)$ donc :

$$v_p\left(\frac{\beta}{\beta_k}\right) = 0$$

Il en découle que p ne divise pas $\frac{\beta}{\beta_k}$, p divise donc a_k. Enfin, p divise a_k et β_k avec $a_k \wedge \beta_k = 1$. Nécessairement, $p = 1$.

□

On peut maintenant démontrer le critère d'Eisenstein.

Théorème 3.1.1 (Critère d'Eisenstein)**.** *Soit $P(X) = \sum_{k=0}^{n} a_k X^k$ un polynôme à coefficient entier. Supposons qu'il existe p premier tel que :*

i. $\forall k \in [\![0, n-1]\!],\ p \mid a_k$

ii. $p \nmid a_n$

iii. $p^2 \nmid a_0$

Alors P est irréductible dans $\mathbb{Q}[X]$.

Démonstration. On réduit P modulo p. Ainsi, P est de la forme cX^n dans $(\mathbb{Z}/p\mathbb{Z})[X]$. Supposons par l'absurde $P = QR$. Q et R peuvent être supposer à coefficients entiers selon le lemme de Gauss. Ainsi, $Q(X) = dX^k$ et $R(X) = eX^{n-k}$ avec $k < n$ et $de = c$. $Q(0)$ et $R(0)$ sont donc divisibles par p donc $Q(0)R(0) = a_0$ est divisible par p^2. C'est absurde.

□

3.2 Duplication du cube (voire plus)

Définition 3.2.1. *On appelle hypercube de dimension $n \in \mathbb{N}^*$ de côté 1 la boule fermée $\mathcal{B}_f(0, 1/2)$ de $(\mathbb{R}^n, \|\cdot\|_\infty)$.*

Nous avons vu qu'il est possible de doubler un nombre constructible par la structure de corps de $\mathbb{E}$. Géométriquement parlant, on peut dupliquer "la ligne". On peut aussi dupliquer l'aire d'un carré. Pouvons déterminer s'il est possible de dupliquer un cube en dimension quelconque ?

Définition 3.2.2. *Un hypercube en dimension $n \in \mathbb{N}^*$ est dit constructible lorsque la longueur de son côté est constructible.*

Théorème 3.2.1. *Un hypercube est duplicable si et seulement si sa dimension est une puissance de 2.*

Démonstration.

$\boxed{\Longleftarrow}$ Si sa dimension n est une puissance de deux, notons la $n = 2^p$. Puisque d'un nombre on peut construire sa racine carré, on peut construire la racine 2^n-ème du côté de l'hypercube.

$\boxed{\Longrightarrow}$ Si n n'est pas une puissance de 2, alors $\sqrt[n]{2}$ n'est pas constructible. En effet, d'après le critère d'Eisenstein, $X^n - 2$ est le polynôme minimal de $\sqrt[n]{2}$. Selon le corollaire de Wantzel, ce nombre n'est pas constructible.

□

Références

[Aud06] Michèle Audin, *Géométrie*, Chapitre iv, 2006

[Goz97] Ivan Gozard, *Théorie de Galois*, Chapitre iv, 1997

[Gou09] Xavier Gourdon, *Les maths en tête : Algèbre*, Chapitre ii, 2009

[Per96] Daniel Perrin, *Cours d'algèbre*, Chapitre iii, 1996