Les nombres Constructibles

Parimaths, 25 octobre 2014

Quelques problèmes anciens (datant du V$^{\text{ème}}$ siècle avant J.-C.)

Toutes les constructions sont censées être faites à la règle et au compas.

1. *La quadrature du cercle*
   Construire un carré ayant la même aire qu'un cercle donné.
2. *La duplication du cube (le problème de Délos)*
   Construire l'arête d'un cube ayant un volume deux fois plus grand que le volume d'un cube donné.
3. *La trisection de l'angle*
   Construire les demi-droites partageant un angle quelconque en trois angles égaux.
4. *Le problème des polygones reguliers*
   Construire, pour chaque $n \geq 3$, un polygone regulier ayant n côtés.

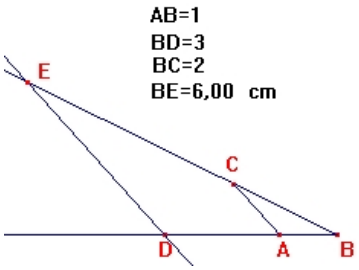
Les trois derniers problèmes ont été résolus en 1837, le premier en 1882. On essaiera ici de comprendre ces solutions.

La géométrie de Descartes

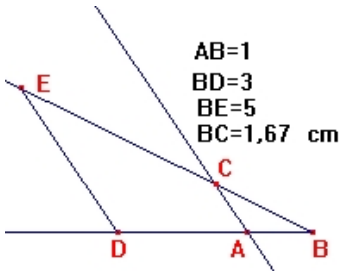
Voici les toutes premières lignes du livre *La géométrie* de Descartes :

Tous les Problèmes de Géométrie se peuvent facilement réduire à tels termes, qu'il n'est besoin par après que de connaître la longueur de quelques lignes droites, pour les construire. Et comme toute l'Arithmétique n'est composée, que de quatre ou cinq opérations, qui sont l'Addition, la Soustraction, la Multiplication, la Division, et l'Extraction des racines, qu'on peut prendre pour une espèce de Division : Ainsi n'a-t-on autre chose à faire en Géométrie touchant les lignes qu'on cherche, pour les préparer à être connues, que leur en ajouter d'autres, ou en ôter, ou bien en ayant une, que je nommerai l'unité pour la rapporter d'autant mieux aux nombres, et qui peut ordinairement être prise à discrétion, puis en ayant encore deux autres, en trouver une quatrième, qui soit à l'une de ces deux, comme l'autre est à l'unité, ce qui est le même que la Multiplication ; ou bien en trouver une quatrième qui soit à l'une de ces deux, comme l'unité est à l'autre, ce qui est le même que la Division ; ou enfin trouver une, ou deux, ou plusieurs moyennes proportionnelles entre l'unité, et quelque autre ligne ; ce qui est le même que tirer la racine carrée, ou cubique, etc. Et je ne craindrai pas d'introduire ces termes d'Arithmétique en la Géométrie, afin de me rendre plus intelligible.

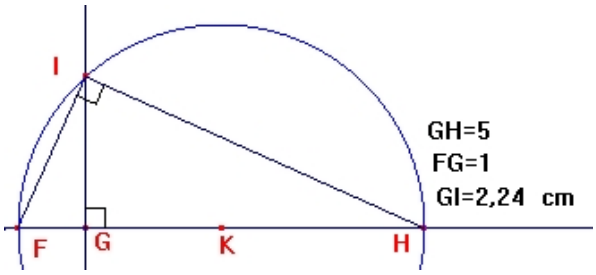
En des termes bien plus intelligibles, Descartes nous dit qu'en géométrie on a des équivalents à l'addition et la soustraction (cela est facile), mais aussi à la multiplication, la division et l'extraction de racines carrées. En voici des exemples :



Multiplication de 2 par 3



Division de 5 par 3



Extraction de la racine carrée de 5

Exercice 1
Expliquer pourquoi ces figures représentent bien la multiplication la division et l'extraction de racines carrées.

Points constructibles

Pour arriver à construire quoi que ce soit sur le plan avec seulement la règle et le compas, il faut bien qu'il y ait déjà quelques points marqués dessus sur lesquels on pourra ensuite rapporter nos règles et compas. Étant donné alors un ensemble fini de points sur le plan, on s'intéresse à tous les autres points que l'on peut construire à partir d'eux rien qu'avec ces deux outils. La définition (très lourde) suivante va dans ce sens :

Définition 1. Soit $\mathcal{P}$ le plan euclidien et soit $\mathcal{B}$ un ensemble fini de points dans $\mathcal{P}$.

* Un point M de $\mathcal{P}$ est dit *constructible* à partir de $\mathcal{B}$ s'il existe une suite finie $M_1, M_2, \ldots, M_n$ de points de $\mathcal{P}$ telle que $M_n = M$ et, pour tout $1 \leq i \leq n$, M_i est un point d'intersection
  — soit de deux droites,
  — soit d'une droite et un cercle,
  — soit de deux cercles,
  ces droites et cercles étant obtenus à l'aide de l'ensemble $E_i = \mathcal{B} \cup \{M_1, M_2, \ldots, M_{i-1}\}$ de la façon suivante :
  — chaque droite passe par (au moins) deux points distincts de E_i,
  — chaque cercle est centré en un point de E_i et a pour rayon la distance entre deux points de E_i.
* Une droite passant par deux points constructibles est dite *constructible*.
* Un cercle centré en un point constructible et ayant pour rayon la distance entre deux points constructibles est dit *constructible*.
* Un angle dessiné par deux droites constructibles est dit *constructible*.

Pour résoudre les problèmes qui nous intéressent depuis le début, il suffira de considérer un ensemble de base $\mathcal{B}$ composé de seulement deux points, i.e. $\mathcal{B} = \{O, I\}$. Pour fixer les idées, nous supposerons en plus que ces deux points sont à une distance égale à 1 (vous pourriez alors associer O et I respectivement aux points $(0, 0)$ et $(1, 0)$ du plan cartésien si vous voulez). Un point sera désormais dit constructible si et seulement s'il l'est à partir de cet ensemble.

Exercice 2 : Quelques résultats élémentaires
Montrer que :

— Le point J qui se trouve à une distance 1 de O et tel que l'angle IOJ est droit est constructible.
  Remarquez qu'on a désormais un repère orthonormé (O, I, J) du plan et on notera alors Ox et Oy respectivement les axes correspondant à ce repère (ce sont bien évidemment les droites OI et OJ).
— Si D est une droite constructible et A un point constructible, la perpendiculaire à D passant par A est une droite constructible.
— Si D est une droite constructible et A un point constructible, la parallèle à D passant par A est une droite constructible.

— Si A et B sont des points constructibles, le milieu et la médiatrice du segment AB sont constructibles.
— Si D et D' sont deux droites constructibles concourantes, les bissectrices des angles déterminés par ces dux droites sont constructibles.

Nombres constructibles

Toutes les nouvelles notions qui apparaîtront dans les sections qui suivent seront expliquées pendant la séance.

Définition 2. Un nombre réel t est dit *constructible* si c'est une des coordonnées dans le repère (O, I, J) d'un point constructible. Autrement dit, t est constructible si et seulement s'il existe un point $A \in \mathcal{P}$ tel que l'une de ses projections respectives sur les axes Ox et Oy se trouve à une distance t de O.

Exercice 3
Montrer que :
— $t \in \mathbb{R}$ est constructible si et seulement si le point de l'axe Ox d'abscisse t est constructible. (L'un des sens de cette affirmation est évident)
— Si A est un point constructible et t un nombre constructible, le cercle de centre A et rayon $|t|$ est constructible.

Exercice 4*
Montrer que l'ensemble $\mathcal{C}$ des nombres constructibles est un sous-corps de $\mathbb{R}$ stable par racine carrée (i.e. tel que pour tout $\alpha \in \mathcal{C}$ positif on a $\sqrt{\alpha} \in \mathcal{C}$).
Indication : on fera appel à la géométrie de Descartes.

Un peu d'algèbre : extensions de corps

Définition 3. Soit K un corps. Un corps L est dit une *extension* du corps K s'il existe une application $\iota : K \to L$ qui respecte l'addition et la multiplication. Une telle application est par ailleurs dite un *morphisme de corps.*

Exercice 5
Montrer qu'une telle application doit forcément être injective et qu'alors K peut être vu comme un sous-corps de L.

Soit $K \subset L$ une extension de corps (cette notation a un sens d'après l'exercice précédent). Pour $a_1, \ldots, a_n \in L$, on note $K(a_1, \ldots, a_n)$ le plus petit sous-corps de L contenant K et $a_1, \ldots, a_n$.

Exercice 6
Montrer que :
— $\mathbb{Q}(1) = \mathbb{Q}\left(\frac{2}{3}\right) = \mathbb{Q}$,
— $\mathbb{Q}(\sqrt{2}) = \{\alpha + \beta\sqrt{2} \,|\, \alpha, \beta \in \mathbb{Q}\}$,
— $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{\alpha + \beta\sqrt{2} + \gamma\sqrt{3} + \delta\sqrt{6} \,|\, \alpha, \beta, \gamma, \delta \in \mathbb{Q}\}$,
— $\mathbb{Q}(i) = \{\alpha + \beta i \,|\, \alpha, \beta \in \mathbb{Q}\}$,
— $\mathbb{R}(i) = \{\alpha + \beta i \,|\, \alpha, \beta \in \mathbb{R}\} = \mathbb{C}$.

On voit avec cet exercice que, étant donnée une extension de corps $K \subset L$, les éléments de L peuvent être décrits comme des sommes de quelques éléments fixes de L multipliés par des coéfficients convenables de K. Autrement dit :

Exercice 7
Soit $K \subset L$ une extension de corps. Montrer que L est un *espace vectoriel* sur K.

Définition 4. Soit $K \subset L$ une extension de corps.
— La dimension de L en tant qu'espace vectoriel sur K est dite le *degré de l'extension* $K \subset L$ et est noté $[L : K]$.

— Un élément $a \in L$ est dit *algébrique sur* K s'il existe un polynôme non nul $P(X) \in K[X]$ tel que $P(a) = 0$.
— Si a n'est pas algébrique sur K, on dit qu'il est *transcendant sur* K.

Exercice 8
Soit $K \subset L$ une extension de corps et soit $L \subset M$ une deuxième extension de corps (il va de soi alors que $K \subset M$ est aussi une extension de corps). Montrer que $[M : K] = [M : L] \cdot [L : K]$.

Exercice 9*
Soit $K \subset L$ une extension de corps et soit $a \in L$ un élément algébrique sur K. Montrer que $[K(a) : K]$ est fini. Si l'on note $n = [K(a) : K]$, montrer qu'il existe un *unique* polynôme $P(X) \in K[X]$ de degré n, unitaire et tel que $P(a) = 0$. Montrer en plus qu'il n'existe pas de polynôme non nul Q de degré inférieur tel que $Q(a) = 0$. Montrer enfin que l'on a

$$K(a) = \{\alpha_1 + \alpha_2 a + \cdots + \alpha_n a^{n-1} \,|\, \alpha_1, \alpha_2, \ldots, \alpha_n \in K\}.$$

Indication : on raisonnera de façon analogue à celle de l'exercice 6.

Définition 5. Pour $a \in L$ comme ci-dessus, le polynôme P est dit le *polynôme minimal de* a. On dit alors que a est algébrique de degré n sur K.

Retour aux nombres constructibles : le théorème de Wantzel

Exercice 10
Soit $K \subset L$ une extension de corps telle que $[L : K] = 2$. Montrer qu'il existe $a \in K$ tel que $L = K(\sqrt{a})$.
Indication : on montrera au préalable que pour $a \in L$ et $b \in K$, on a $K(a) = K(a + b)$.

Exercice 11*
Démontrer le théorème de Wantzel :

Théorème (Wantzel, 1837)**.** *Soit $t \in \mathbb{R}$; t est un nombre constructible si et seulement si il existe un entier $p \geq 1$ et une suite $L_1, L_2, \ldots, L_p$ de sous-corps de $\mathbb{R}$ telle que :*
— $L_1 = \mathbb{Q}$,
— *pour* $1 \leq j \leq p-1$, $L_j \subset L_{j+1}$ *et* $[L_{j+1} : L_j] = 2$,
— $t \in L_p$.

On pourra utiliser à cet effet le lemme suivant (qu'on pourra démontrer en exercice aussi !) :

Lemme. *Soit D une droite de $\mathcal{P}$ passant par les points $A = (a_1, a_2)$ et $B = (b_1, b_2)$ (notations dans le repère (O, I, J)). Alors D est décrite par une équation de la forme $\alpha x + \beta y + \gamma = 0$ avec $\alpha, \beta, \gamma \in \mathbb{Q}(a_1, a_2, b_1, b_2)$.*

De même, soit C un cercle de $\mathcal{P}$ de centre $A = (a_1, a_2)$ et rayon égal à la distance entre les points $B = (b_1, b_2)$ et $C = (c_1, c_2)$. Alors C est décrit par une équation de la forme $x^2 + y^2 - 2\alpha x - 2\beta y + \gamma = 0$ avec $\alpha, \beta, \gamma \in \mathbb{Q}(a_1, a_2, b_1, b_2, c_1, c_2)$.

Exercice 12
À partir du théorème de Wantzel, démontrer le corollaire suivant :

Corollaire. *Tout nombre constructible est algébrique sur $\mathbb{Q}$ et son degré est une puissance de* 2.

Retour aux problèmes anciens

Commençons par le problème de Délos :

Exercice 13
Montrer que la duplication du cube est impossible.
Indication : on utilisera le corollaire au théorème de Wantzel.

Traitons ensuite la trisection de l'angle. Pour montrer l'impossibilité de cette construction en général, il suffira de montrer qu'il existe un angle bien précis qui ne peut pas être trisecté :

Exercice 14
Montrer que la trisection de l'angle de $\frac{\pi}{3}$ (i.e. $60°$) est impossible.
Indication : on trouvera au préalable la formule pour exprimer $\cos(3\theta)$ *en fonction de* $\cos(\theta)$*, puis on montrera que* $\cos(\frac{\pi}{9})$ *n'est pas constructible.*

Pour traiter la quadrature du cercle, il nous faudra encore un résultat profond, dont on admettra la démonstration (on essaiera de la présenter au tableau) :

Théorème (Lindemann, 1882)**.** *Le nombre* π *est transcendant sur* $\mathbb{Q}$*.*

Exercice 15
En déduire que la quadrature du cercle est impossible.

Enfin, pour le problème des polygones reguliers, on se contentera du résultat suivant, qu'on ne démontrera que partiellement ici car il fait appel à la *théorie de Galois*, notamment pour les *corps cyclotomiques*. Ceux qui sont intéressés pourront regarder le livre de Jean-Claude Carréga *Théorie des corps : La règle et le compas.*

Théorème (Gauss, 1801 ; Wantzel, 1837)**.** *Un polygone régulier à* n *côtés est constructible si et seulement si* n *est le produit d'une puissance de* 2 *et d'un nombre quelconque de nombres premiers de Fermat distincts.*
(Un nombre est dit "de Fermat" s'il est de la forme $2^{(2^n)} + 1$ *avec* $n \in \mathbb{N}$*.)*

Exercice 16
Démontrer le lemme suivant :

Lemme. *Soient* $m, n \geq 1$ *deux entiers premiers entre eux. Alors l'angle de* $\frac{\pi}{mn}$ *est constructible si et seulement si ceux de* $\frac{\pi}{m}$ *et* $\frac{\pi}{m}$ *le sont.*

En déduire que le théorème de Gauss-Wantzel se réduit à montrer que, pour $n = p^\alpha$ avec p premier, le polygone régulier à n côtés est constructible si et seulement si $p = 2$ ou bien $\alpha = 1$ et p est un nombre de Fermat.

Exercice 17
Montrer que l'angle de $\frac{\pi}{2^\alpha}$ est constructible pour tout $\alpha \in \mathbb{N}$.