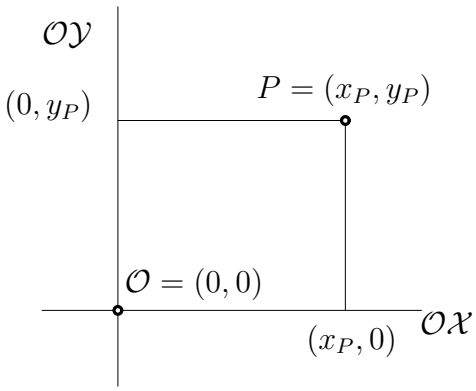
Un théorème de Descartes et quelques conséquences

Avant de commencer, je tiens à préciser une chose, ce n'est pas parce que les preuves des résultats sont là qu'il est obligatoire de les lire. Je ne les ai mises que pour permettre à ceux qui le désirent d'y avoir accès. Ceci étant dit, intéressons-nous à ce famuex théorème de Descartes.

La première remarque, banale en apparence, est de mettre en bijection, en préservant les distances, l'ensemble $\mathbb{R}$ des nombres réels et une droite. Explicitement, choissisons $\mathcal{O}$ un point de la droite correspondant au nombre 0 qu'on appelle l'origine et un autre point $\mathbf{1}$ distinct de $\mathcal{O}$ correspondant au nombre 1. Ceci revient à choisir une unité de longueur pour les segments en disant que la longueur du segment $[\mathcal{O}, \mathbf{1}]$ est égale à 1, ainsi qu'une orientation de la droite.

Le choix de deux points du plan définit donc un système d'axes orthonormés, puisque le premier point peut être choisi comme origine la droite passant par les deux points comme le premier axe et la droite perpendiculaire à ce dernier passant par l'origine comme le second axes. Les deux points ont dans ce système d'axes les coordonnées $(0,0)$ et $(1,0)$.



Ceci permet de déterminer tout point de l'espace par la donnée de deux nombres réels par le choix d'une origine et d'un système d'axes.

Tout objet géométrique peut donc être déterminer par une équation. Les points formant l'objet étant les seuls satisfaisant cette dernière.

A priori, cette idée d'introduire des équations pour décrire des objets géométriques semble banale, mais ce fut le premier pas pour montrer que les trois fameux problèmes grecs non résolus (trissection de l'angle, duplication du cube et quadrature du cercle) étaient impossibles.

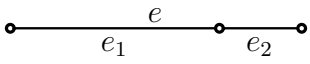
Pour cela, il faut démontrer le théorème de Descartes suivant qui permet de caractériser les points constructibles à la règle et au compas à l'aide d'un critère algébrique sur les composantes.

Théorème 0.0.1. *Soient les points de coordonnées* $(0,0)$ *et* $(1,0)$. *Un point de coordonnées* (α, β) *est constructible à la règle et au compas si et seulement si les nombres* α *et* β

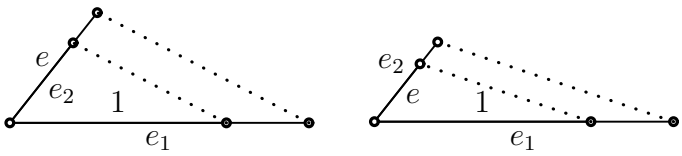
s'écrivent comme expression finie ne contenant que des nombres entiers, les quatres opérations (+, −, ∗, /), ainsi que le symbole $\sqrt[2]{\ }$.

Pour un nombre x décrit par une expression E, notons $\#(E)$ le nombre de termes dans l'expression. Par exemple $\#(2) = 1$, $\#(\sqrt[2]{3}) = 2$, $\#(4/3 + 2/3) = 7$ et $\#(\sqrt[2]{2/3}) = 4$. Il est à remarquer que le nombre de termes dépend de l'expression et non pas seulement du nombre décrit (en effet $2 = 4/3 + 2/3$).
La démonstration de ce résultat se fait par récurrence.
Démonstration "⇐" On suppose que α et β sont des nombres réels qui peuvent s'écrire comme des expressions ne contenant que des nombres entiers, les quatres opérations et le symbole racine carrée, et il faut démontrer que le point de coordonnées (α, β) peut être construit à la règle et au compas (i.e. que l'on peut construire un segment à la règle et au compas dont la longueur vaut α et de même pour β). Il suffit de le faire pour α.
Démontrons cette implication par récurrence sur le nombre de termes dans l'expression représentant α.
Le premier pas de récurrence (ancrage) dit que toute expression ne contenant qu'un seul terme est constructible à la règle et au compas. Or les expressions ne contenant qu'un terme et représentant un nombre sont uniquement de la forme $n \in \mathbb{N}$. Tout nombre entier peut être construit, puisque les points P_0 (resp. P_1) de coordonnées $(0, 0)$ (resp. $(1, 0)$) sont donnés. Le segment $[P_0, P_1]$ est de longueur 1. En reportant ce segment n fois sur la droite P_0P_1 on obtient un segment de longueur n.
Pas d'induction :
Hypothèse d'induction : Toute expression e contenant au plus n termes est constructible à la règle et au compas.
A voir : Toute expression e contenant $n+1$ termes est constructible à la règle et au compas.

i) Si $e = e_1 + e_2$ ou $e = e_1 - e_2$ et que $\#(e) = n + 1$, alors $\#(e_1) + \#(e_2) = n$ et donc, par hypothèse d'induction, e_1 et e_2 sont constructibles à la règle et au compas. Comme de plus, l'addition et la soustraction sont évidentes par les axiomes d'Euclide, e est constructible à la règle et au compas.

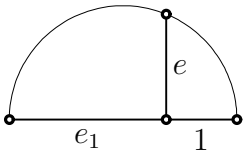


ii) Si $e = e_1 * e_2$ ou $e = e_1/e_2$ et que $\#(e) = n + 1$, de la manière qu'en i), e_1 et e_2 sont constructibles à la règle et au compas. En employant le théorème de Thales $e = e_1 * e_2$ et $e = e_1/e_2$ le sont aussi (par Thales).



iii) Si $e = \sqrt[2]{e_1}$ et $\#(e) = n + 1$, alors $\#(e_1) = n$ et e_1 est donc constructible. Par le

théorème de la hauteur, si e_1 est constructible, alors $e = \sqrt[2]{e_1}$ l'est aussi.



Démontrons maintenant l'implication réciproque.
"⇒" On suppose que α et β sont les coordonnées d'un point constructible à la règle et au compas et on doit démontrer qu'il existe des expressions ne contenant que des nombres entiers, les quatres opérations et le symbole racine carrée représentant α et β.
Construire à la règle et au compas veut dire que l'on obtient le point $P = (\alpha, \beta)$, partant des points $(0, 0)$ et $(0, 1)$, par une suite finie d'intersections d'une droite avec une autre droite, d'une droite avec un cercle et de deux cercles.
Notre démonstration se fait par récurrence sur le nombre de pas de la construction. Remarquons tout d'abord qu'étant donnés les points $(0, 0)$ et $(0, 1)$, on peut construire tous les points à coordonnées entières et même à coordonnées rationnelles par Thales. De plus, un point (α, β) est constructible à la règle et au compas s'il peut être obtenu comme

1. l'intersection de deux droites,
2. l'intersection d'une droite et d'un cercle,
3. ou comme l'intersection de deux cercles.

Etudions les analogues algébriques de ces trois cas. Premièrement si le point est l'intersection de deux droites d_1 et d_2 données par quatre points $Q_1 = (x_i, y_i)$ pour $i = 1, ..., 4$ (i.e $d_1 = Q_1Q_2$ et $d_2 = Q_3Q_4$), et que chacun des quatre points Q_i ont leurs coordonnées de la forme algébrique voulue, alors les équations des droites d_1 et d_2 sont données par

$$d_1 : \quad y = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1) + y_1 \qquad d_2 : \quad y = \frac{y_4 - y_3}{x_4 - x_3}(x - x_3) + y_3$$

On en déduit que l'intersection des deux droites a comme abscisse x une expression fractionnaire en les x_1, x_2, x_3, x_4, y_1, y_2, y_3 et y_4. Donc x a la forme algébrique voulue.
En remplaçant la valeur de x dans l'équation de d_1, on obtient de même une expression algébrique pour y. Remarquons que si une droite contient deux points dont les coordonnées sont des expressions ne contenant que des nombres entiers, les quatre opérations et la racine carrée, alors si l'équation de la droite est $y = ax + b$, les paramètres a et b sont aussi de cette forme.
Deuxièmement, supposons que le point $P = (\alpha, \beta)$ soit l'intersection d'un cercle $\mathcal{C}$ de rayon r centré au point de coordonnées $Q = (c, d)$ et d'une droite δ d'équation $y = ax+b$. Comme l'équation du cercle est $(x - c)^2 + (y - d)^2 = r^2$, en substituant $y = ax + b$ dans l'équation du cercle et en développant, on obtient :

$$(1 + a^2)x^2 + (2ab - 2c - 2ad)x + (c^2 + b^2 + d^2 - 2db - r^2) \; = \; 0.$$

Par la formule de résolution d'une équation du second degré, on obtient les valeurs de x :

$$x_{1,2} \; = \; \frac{-(2ab - 2c - 2ad) \pm \sqrt[2]{\Delta}}{2(1 + a^2)},$$

où $\Delta = (2ab-2c-2ad)^2-4(1+a^2)(c^2+b^2+d^2-2db-r^2)$ est le discriminant de l'équation. Pour que l'équation ait des solutions réelles, il faut et suffit que $\Delta \geq 0$. En développant, on obtient que

$$\frac{\Delta}{4} = r^2(1+a^2) - (ac+b-d)^2 \geq 0 \quad \Leftrightarrow \quad r^2 \geq \frac{(ac+b-d)^2}{(1+a^2)} = \mathrm{dist}(\delta, Q)^2,$$

ce qui montre bien que les intersections entre la droite δ et le cercle $\mathcal{C}$ existent si et seulement si $\Delta \geq 0$. Dans le cas où ces intersections existent et si les nombres a, b, c, d et r peuvent s'écrire comme expression ne contenant que des entiers, les quatre opérations et la racine carrée, alors x s'écrit aussi sous une telle forme et par suite, $y = ax + b$ aussi.
Troisièment, si le point est l'intersection de deux cercles, il suffit de se rendre compte que si les deux cercles s'intersectent, alors leurs points d'intersection définissent une droite dont on peut calculer l'équation (si les deux points d'intersection sont confondus, la droite est tangente). L'étude de l'intersection de deux cercles peut donc se ramener au cas de l'intersection d'une droite et d'un cercle vu précédemment. Il faut néanmoins se convaincre que les paramètres de la droite d'intersection ont bien la forme algébrique voulue. Comme les coordonnées des centres des cercles sont de la forme algébrique voulue, la pente de la droite entre eux l'est aussi. Ceci démontre déjà que la droite passant par les intersections des deux cercles a une pente ayant la bonne forme algébrique. Il reste à montrer qu'un point sur cette droite a des coordonnées de la bonne forme. Le point d'intersection entre la droite reliant les deux centres et celle reliant les deux intersections satisfait cela.
Pour conclure, il faut donc supposer par induction que le point $P = (\alpha, \beta)$ se construit en $n+1$ pas élémentaires. Si P est obtenu comme l'intersection de deux droites alors la construction de chacune d'elle se fait en au plus n pas et donc, par hypothèse de récurrence, les deux droites ont des équations dont les paramètres sont des expressions ne contenant que des entiers, les quatre opérations et la racine carrée. Par le point 1, cela implique que les coordonnées de P sont aussi de telles expressions. Dans le cas où P est l'intersection d'un cercle et d'une droite (respectivement de deux cercles), on conclut de façon similaire en utilisant le cas 2 (respectivement le cas 3). Cqfd

Pour s'assurer que certains nombres ne peuvent pas être construit à la règle et au compas, il faut encore le lemme suivant.

Définition 0.0.2. Pour un polynôme $P(x)$, on dit que ξ est racine de P si $P(\xi) = 0$.

Lemme 0.0.3. *Si $P(x) = x^3 + ax^2 + bx + c$ est un polynôme à coefficiaents rationnels qui n'a pas de racine dans $\mathbb{Q}$, alors aucune racine de P ne peut s'écrire comme une expression arithmétique bien formée ne contenant que des nombres entiers, les quatre opérations et la racine carrée.*

Preuve : Commençons par les remarques suivantes :

1. On peut simplifier l'équation par le changement de variables $y = x + u$. Ce type de changement fut utilisé par Ferrari, Cardano et Tartaglia pour résoudre l'équation du

troisième degré par radicaux, c'est-à-dire pour trouver une formule explicite donnant les racines d'un polynôme de degré 3.

$$\tilde{P}(y) = P(x+u) = (x+u)^3 + a(x+u)^2 + b(x+u) + c = x^3 + (3u+a)x^2 + ...$$

En posant $u = -a/3$ le polynôme se simplifie en un polynôme du type $\tilde{P}(y) = y^3 + Ay + B$. De plus, si le lemme est démontré pour tout polynôme du type $\tilde{P}$, alors il le sera pour tout $P(x)$. En effet, par contraposée, si η est une racine de $\tilde{P}$, alors $\eta - u$ est une racine de P.

On notera dès à présent $P(x) = x^3 + ax + b$.

2. Si on développe $P(\eta) = P(p + q\sqrt{R})$, on obtient

$$\begin{aligned} P(p+q\sqrt{R}) &= (p+q\sqrt{R})^3 + a(p+q\sqrt{R}) + b \\ &= (p^3 + 3pq^2R + ap + b) \\ &\quad +(3p^2q + q^3R + aq)\sqrt{R} \\ &= M + N\sqrt{R}, \text{ avec } M = p^3 + 3pq^2R + ap + b \\ &\quad \text{ et } N = 3p^2q + q^3R + aq. \end{aligned}$$

Un calcul similaire montre que $P(\overline{\eta}) = P(p - q\sqrt{R}) = M - N\sqrt{R}$.

3. Supposons que η_1, η_2 et η_3 soient les trois racines de $P(x)$, on obtient

$$P(x) = x^3 + ax + b = (x-\eta_1)\cdot(x-\eta_2)\cdot(x-\eta_3) = x^3 + (-\eta_1 - \eta_2 - \eta_3)x^2 + ...$$

Ainsi, le coefficient de x^2, dans notre cas égal à 0, est égal à $(-\eta_1 - \eta_2 - \eta_3)$. En développant complétement le calcul précédent, chaque coefficient donne une relation entre les diverses racines du polynôme de départ.

Nous allons maintenant démontrer le lemme par récurrence sur le nombre $\mathcal{N}$ d'expression de la forme $\sqrt{e}$ avec des e distincts, mais pouvant éventuellement contenir le même type d'expression.

Par exemple, l'expression $\sqrt{\sqrt{\sqrt{2}+\sqrt{3}}+\sqrt{2}}$ contient les quatre expressions de la forme $\sqrt{e}$ suivantes :

$$\sqrt{2}; \sqrt{3}, \sqrt{\sqrt{2}+\sqrt{3}}, \sqrt{\sqrt{\sqrt{2}+\sqrt{3}}}$$

On ne compte pas deux fois la même expression (dans notre cas $\sqrt{2}$).

Premier pas de la récurrence : Si $\mathcal{N} = 1$, cela revient à dire qu'il n'y a qu'une expression de la forme $\sqrt{e}$ dans η. La forme la plus générale que peut prendre η est alors

$$\frac{\alpha + \beta\sqrt{R}}{\delta + \gamma\sqrt{R}}$$

avec α, β, δ, γ et R rationnels. En amplifiant cette fraction par $\delta - \gamma\sqrt{R}$, on obtient $\eta = p + q\sqrt{R}$ avec p et q rationnels. Mais pour cela, il faut s'assurer que $\delta - \gamma\sqrt{R} \neq 0$.

Ceci est le cas, car si $\delta - \gamma\sqrt{R} = 0$, ceci revient à dire que $\sqrt{R}$ est rationnel et donc que le polynôme P admet une racine rationnelle, ce qui est faux par hypothèse.
Si $P(\eta) = P(p + q\sqrt{R}) = 0$, par le calcul fait à la remarque 2, on obtient $P(p + q\sqrt{R}) = M + N\sqrt{R} = 0$. Ceci implique $N = 0$, sinon $\sqrt{R} = M/N$ serait rationnel, ce que l'on vient de démontrer impossible. Donc $N = 0$, il suit que $M = 0$ et donc comme $P(p - q\sqrt{R}) = M - N\sqrt{R}$, le nombre $\overline{\eta} = p - q\sqrt{R}$ est aussi racine de P. Ceci implique, par la troisième remarque préliminaire, que η_3, la troisième racine de P, est donnée par

$$\eta_3 = -(\eta + \overline{\eta}) = 2p \in \mathbb{Q}$$

Ceci est impossible.

Pas de récurrence

Hypothèse de récurrence : Il n'existe pas de racine de P admettant une expression arithmétique ne contenant que des entiers, les quatre opérations et le symbole racine carrée et contenant au plus $\mathcal{N}$ symboles $\sqrt{e}$ pour des e distincts.

Conclusion : Il n'existe pas de racine de P admettant une expression arithmétique ne contenant que des entiers, les quatre opérations et le symbole racine carrée et contenant $\mathcal{N} + 1$ symboles $\sqrt{e}$ pour des e distincts.

Preuve du pas de récurrence : On suppose que dans dans toute expression arithmétique de η, le nombre minimal d'expressions de la forme $\sqrt{e}$ est $\mathcal{N} + 1$. Parmi ces $\mathcal{N} + 1$ expressions distinctes contenues dans η, choisissons-en une qui contient le plus grand nombre de racines emboitées $\sqrt{\sqrt{\sqrt{\sqrt{\ldots}}}}$ et notons-la comme auparavant $\sqrt{R}$. η peut à nouveau s'écrire de manière unique comme

$$\frac{\alpha + \beta\sqrt{R}}{\delta + \gamma\sqrt{R}}$$

avec α, β, δ, γ ne contenant plus $\sqrt{R}$ et contenant donc au plus $\mathcal{N}$ expressions distinctes de la forme $\sqrt{e}$. La preuve du pas de récurrence est identique à celle du premier pas de récurrence, il faut juste donner les raisons pour lesquels les mêmes arguments peuvent être utilisés.

L'argument important dans le premier pas est que $\sqrt{R}$ n'est pas rationnel. Ceci permet de d'affirmer que $\delta + \gamma\sqrt{R} \neq 0$. Dans notre cas, le choix de $\sqrt{R}$ et la minimalité de $\mathcal{N}$ impliquent que $\delta + \gamma\sqrt{R} \neq 0$, d'où le fait que η peut s'écrire $\eta = p + q\sqrt{R}$, avec p et q ne contenant que $\mathcal{N}$ symboles $\sqrt{e}$ distincts.

Pour la même raison, $p - q\sqrt{R}$ est aussi non nul. On peut donc déduire comme précédemment que $M + N\sqrt{R} = 0$.

Ceci implique à nouveau $N = 0$, sinon $\sqrt{R} = M/N$ s'exprimerait en les $\mathcal{N}$ autres termes apparaissant dans η ce qui contredirait une fois de plus la minimalité de l'écriture initiale de η. On a donc $N = 0$. Il suit que $M = 0$ et donc comme $P(p - q\sqrt{R}) = M - N\sqrt{R}$, le nombre $\overline{\eta} = p - q\sqrt{R}$ est aussi racine de P. Ceci implique, par la troisième remarque préliminaire, que η_3, la troisième racine de P est donnée par

$$\eta_3 = -(\eta + \overline{\eta}) = 2p \in \mathbb{Q}$$

Ceci est impossible, car η_3 ne contient que $\mathcal{N}$ termes distincts de la forme $\sqrt{e}$, ce qui n'est pas possible par hypothèse de récurrence. Cqfd

Pourquoi donc ceci suffit-il pour s'assurer que la trissection d'un angle est impossible. Donner un angle β revient au même que de donner le sinus de cet angle. Supposons qu'on connaisse $\sin(\beta)$. Pour trissecter β, il faudrait réussir à construire $\sin(\alpha)$ avec $\beta = 3\alpha$. La triganométrie nous dit que

$$\sin(\beta) = \sin(3\alpha) = 3\sin(\alpha)\cos^2(\alpha) - \sin^3(\alpha).$$

En posant $x = \sin(\alpha)$, trissecter un angle revient à résoudre l'équation

$$b = -4x^3 + 3x \qquad \text{avec } b = \sin(\beta).$$

Il existe des angles β tel que $\sin(\beta)$ est rationnel et pour lesquels l'équation $\sin(\beta) = -4x^3 + 3x$ n'a pas de solutions rationnelles. Ce sont ces angles qui ne peuvent pas être trissectés à la règle et au compas.