IMPOSSIBILITÉ DE CERTAINES CONSTRUCTIONS GÉOMÉTRIQUES

par Jacques Bordier,
Collège Jean de Brébeuf

I - INTRODUCTION:

Le but de cet article est de montrer comment, à l'aide de résultats de l'algèbre moderne, on peut prouver l'impossibilité de certains problèmes de constructions géométriques posés par les Grecs. On verra aussi que de tels résultats n'auraient pu être obtenus sans la création de la géométrie analytique qui permet de relier les objets géométriques à des objets algébriques.

Avec une règle et un compas, il est possible de faire des constructions très complexes; donnons deux exemples.

PROBLEME D'APOLLONIUS: Construction de tous les cercles tangents à trois cercles donnés

PROBLEME DE MALFATTI: Construction dans chaque angle d'un triangle, d'un cercle de telle façon que chaque cercle soit tangent aux deux autres ainsi qu'aux deux côtés de l'angle.

Cependant certains problèmes apparaissant au premier abord assez simples, par exemple la trisection de l'angle, problème consistant à construire un angle de mesure $\theta/3$ à partir d'un angle de mesure θ, avaient résisté aux efforts des Grecs et de leurs successeurs. La raison de l'insuccès de leurs efforts réside dans le fait que cette construction particulière est impossible si on se limite aux instruments prescrits. Nous allons prouver l'impossibilité de cette construction à partir d'un critère général que nous établirons. Nous examinerons aussi le problème de la duplication du cube et de la quadrature du cercle. Les Grecs ont dû pressentir l'impossibilité de ces constructions mais ils étaient loin de posséder les outils permettant de le prouver.

II - PRÉLIMINAIRES ALGÉBRIQUES

Voici quelques définitions et résultats algébriques à l'aide desquels sera construit le critère de non-constructibilité.

Rappelons la définition de "corps" (1)

Nous appellerons "corps" tout sous-ensemble non-vide K des nombres complexes qui possède les propriétés suivantes:

(1) Si $a \in K$ et $b \in K$ alors $a + b \in K$ et $ab \in K$

(2) Si $a \in K$ alors $-a \in K$ et $a^{-1} \in K$ $(a \neq 0)$

(1) Comme dans les applications nous n'avons pas besoin de résultats sur les corps abstraits, nous limitons notre étude aux corps numériques.

EXEMPLES: (1) F_0 l'ensemble des nombres rationnels

(2) R l'ensemble des nombres réels

(3) C l'ensemble des nombres complexes

(4) F_2 l'ensemble des nombres réels de la forme $a + b\sqrt{2}$ avec $a, b \in F_0$

EXERCICE: Montrer que F_0 est le plus petit corps.

Soit F un corps; un corps K est dit une <u>extension</u> de F si K contient F.

EXEMPLES: R est une extension de F_0; F_2 est une extension de F_0

Si K est une extension de F on a évidemment:

(a) K est un groupe akélien sous l'opération +

(b) Pour tout $c \in F$ et $k \in K$ le produit ck est défini et est un élément de K

(c) Si $c, c_1, c_2 \in F$ et $k, k_1, k_2 \in K$ alors

$c(k_1 + k_2) = ck_1 + ck_2$

$(c_1 + c_2)k = c_1k + c_2k$

$(c_1c_2)k = c_1 (c_2k)$

$1 \cdot k = k$

Tout cela pour dire que K peut être considéré comme un espace vectoriel sur F. On peut ainsi parler de la dimension de K sur F. Dans ce contexte-ci on emploie le mot degré de K sur F au lieu de dimension de K sur F. Le degré de K sur F sera noté $[K:F]$.

On vérifie facilement que $[F_2 : F_0] = 2$, une base de F_2 sur F_0 étant 1 et $\sqrt{2}$; de même $[C : R] = 2$ en prenant par exemple 1 et i comme base.

Parfois le degré est infini, $[R : F_0]$ est un exemple de cette possibilité, les éléments $1, \sqrt{2}, \sqrt{3}, \ldots$ étant linéairement indépendants. Le seul cas qui va nous intéresser est celui où $[K:F]$ est fini. On dira alors que K est une extension finie de F.

<u>THÉORÈME I</u>: Si L est une extension finie de K et si K est une extension finie de F, alors 1) L est une extension de F et

2) $[L:F] = [L:K][K:F]$

Preuve: Nous allons construire une base de L sur F contenant m x n éléments où $m = [L:K]$ et $n = [K:F]$

Soit $v_1, v_2, \ldots, v_m$ une base de L sur K et $w_1, w_2, \ldots, w_n$ une base de K sur F. Considérons les m x n éléments $v_i w_j$ $\begin{cases} i = 1, 2, \ldots m \\ j = 1, 2, \ldots n \end{cases}$ et montrons premièrement que chaque élément de L peut s'écrire comme une combinaison linéaire de ces m x n éléments avec coefficients dans F; puis on vérifiera que ces éléments sont linéairement indépendants.

Soit $t \in L$, alors $t = k_1 v_1 + \ldots + k_m v_m$ où $k_i \in K$ $i = 1, 2, \ldots m$
Comme tout élément de K est une combinaison linéaire des w_i avec coefficients dans F on peut écrire $k_i = a_i w_1 + \ldots + a_{in} w_n$ où chaque a_{ij} est dans F. On obtient ainsi

$$t = a_{11} v_1 w_1 + \ldots + a_{1n} v_1 w_n + \ldots a_{mn} v_m w_n$$

en remplaçant les k_i et en multipliant. Ainsi les m x n éléments $v_i w_j$ engendrent bien L sur F.

Considérons une combinaison quelconque des $v_i w_j$

$b_{11} v_1 w_1 + \ldots\ldots + b_{mn} v_m w_n = 0$ avec b_{ij} F

On doit montrer que chaque $b_{ij} = 0$
Groupons les éléments comme suit: $(b_{11} w_1 + \ldots + b_{1n} w_n)$

$v_1 + \ldots + (b_{n1} w_1 + .. + b_{mn} w_n) v_m = 0$

Les coefficients sont dans K car $w_i \in K$ et $K \supset F$.

Mais $v_1 v_2, \ldots v_m$ formant une base de L sur K il s'ensuit que chaque coefficient est 0. Les w_i étant linéairement indépendants sur F chaque b_{ij} est 0

- - - - - - - - - - - - - - - - - - -

- Soit K une extension de F et soit $a \in K$.

Nous allons construire le plus petit sous-corps de K contenant F et a. Considérons l'ensemble de tous les éléments dans K qui peuvent s'exprimer sous la forme $B_0 + B_1 a + \ldots + B_s a^s$ où $B_i \in F$ et s est un entier non négatif. Comme éléments de K deux quelconques de ces éléments peuvent être divisés à moins que le deuxième ne soit 0.
Soit U l'ensemble de tous les quotients de ces éléments.

EXERCICE: Vérifier que U est un sous-corps de K et que c'est le plus petit sous-corps de K. On dit que le sous-corps U est obtenu par l'adjonction de a à F.
Le sous-corps U sera noté F(a).

EXEMPLES: 1) Adjoignons $\sqrt{2}$ à F_0; on obtient un sous-corps $F_0(\sqrt{2})$ de C.

On vérifie immédiatement que
$F_0(\sqrt{2}) = \{ a + b\sqrt{2},\ a, b \in F_0 \}$

2) Adjoignons i à R ; on obtient R(i) qui est C car
$R(i) = \{ a + bi, a, b \in R \}$

On doit parfois considérer des extensions successives d'un corps par l'adjonction de plusieurs éléments $a_1, a_2, \ldots a_n$. Soit $T_1 = F(a_1)$, $T_2 = T_1(a_2), \ldots\ldots, T_n = T_{n-1}(a_n)$; on emploiera alors la notation suivante: $Tn = F(a_1, a_2, .., a_n)$
Le théorème I se généralise naturellement à ce cas.

- - - - - - - - - - - - - - - - - - -

Définition: Un élément $a \in K$ est dit algébrique sur F s'il existe des éléments $b_0, b_1, b_2, \ldots, b_n$ dans F non tous 0, tels que

$$b_n a^n + b_{n-1} a^{n-1} + \ldots + b_0 = 0$$

EXEMPLES: (1) Tout nombre rationnel a/b est algébrique sur F_0 car il satisfait l'équation $ax - b = 0$

(2) De même $\sqrt{2}$ et i sont algébriques sur F_0 car ils satisfont respectivement $x^2 - 2 = 0$ et $x^2 + 1 = 0$.

Il existe un nombre infini de nombres non algébriques sur F_0 mais il est toujours difficile de prouver qu'un nombre donné n'est pas algébrique. Les nombres π et e ne sont pas algébriques sur F_0.

Définition: L'élément $a \in K$ est dit algébrique de degré n sur F s'il satisfait un polynôme non nul de degré n sur F mais aucun polynôme non nul de degré inférieur.

EXEMPLES: (1) $\sqrt{2}$ est algébrique de degré 2 sur F_0

(2) i est algébrique de degré 2 sur F_0

Voici le théorème fondamental pour l'étude que nous faisons.

THÉORÈME 2: Si $a \in K$ est algébrique de degré n sur F alors F(a) est une extension finie de F de degré n et les éléments $a^0, a^1, a^2, \ldots, a^{n-1}$ forment une base de F(a) sur F.

Preuve: On sait que F(a) est formé par l'ensemble des éléments de la forme $p(a)/q(a)$ où $p(x)$ et $q(x)$ sont des polynômes à coefficients dans F avec $q(a) \neq 0$

On doit montrer que tout élément de F(a) peut s'écrire d'une façon unique comme un polynôme en a de degré au plus n-1
Soit m(x) le polynôme de plus petit degré satisfait par a. On a: degré m(x)=n. On a 1°) $m(x)$ ne divise pas $q(x)$ car autrement $q(x) = m(x)\, h(x)$ et $q(a) = 0$

2°) Aucun polynôme non constant ne divise m(x) (On dit que m(x) est irréductible sur F). En effet si $m(x) = q(x)\, k(x)$ on aurait alors $q(a)=0$ ou $k(a) = 0$ en contradiction avec la minimalité du degré de m(x).

Ainsi m(x) et q(x) sont relativement premiers par un résultat élémentaire de la théorie des polynômes il existe des polynômes a(x) et b(x) tels que $a(x)\, m(x) + b(x)\, q(x) = 1$
Cette relation entraîne $b(a)\, q(a) = 1$. Ainsi $p(a)/q(a) = p(a)\, b(a)$ i.e. chaque élément de F(a) est un polynôme en a.
Soit maintenant f(a) un élément quelconque de F(a). On sait par l'algorithme de division qu'il existe des polynômes g(x) et r(x) tels que

$f(x) = g(x)\, m(x) + r(x)$ où deg $r(x) <$ deg $m(x)$
Ainsi $f(a) = r(a)$
Si $r(x) = a$ alors $f(a) = 0 = 0 + 0.a + \ldots + 0\ a^{n-1}$
Si $r(x) \neq 0$ alors deg $r(x) < n$ et ainsi $f(a)$ est bien un polynôme de degré au plus $n-1$

Il reste à montrer que la représentation est unique.
Supposons $f(a) = a_0 + a_1 a + \ldots + a_{n-1} a^{n-1} = b_0 + b_1 a + \ldots + b_{n-1} a^{n-1}$

i.e. $\sum_{i=0}^{n-1} (a_i - b_i)\, a^i = 0$. Si certains des termes $a_i - b_i$ étaient différents de 0 le polynôme $\sum_{i=0}^{n-1} (a_i - b_i)\, x^i$ s'annulerait pour $x=a$ contrairement à la minimalité du degré de $m(x)$.

III: CONSTRUCTIONS GÉOMÉTRIQUES

Dans une construction géométrique pour laquelle les instruments permis sont la règle et le compas, la règle sert à construire la droite joignant 2 points donnés et le compas à construire un cercle si le centre et un segment sont donnés.

Toute construction débute avec certains éléments donnés, points, droites, segments, arcs de cercle, etc. Chacun de ces objets géométriques est entièrement déterminé par la donnée d'un certain ensemble de points.

Lorsqu'on effectue des constructions, de nouveaux points peuvent être obtenus à partir des points donnés de 3 façons.

(1°) Intersection de 2 droites
(2°) Intersection d'une droite et d'un cercle
(3°) Intersection de deux cercles

Dénotons par K_n l'ensemble des points connus après n constructions.
K_0 dénote l'ensemble des points donnés au départ.
La construction est terminée si pour un certain n, K_n contient des points tels que la figure désirée puisse être tracée à partir d'eux.

THÉORÈME 3: Soit XOY un système de coordonnées introduit dans le plan où s'effectue la construction géométrique. Considérons l'ensemble S_n des nombres tenant lieu de coordonnées des points de K_n (Par exemple si $K_0 = \{(0,0), (1,0)\}$ i.e. si seulement un segment unité est donné alors $S_0 = \{0,1\}$). Soit L_n le plus petit sous-corps des nombres réels contenant S_n (Par exemple $L_0 = F_0$ si $S_0 = \{0,1\}$)
Alors les coordonnées de tout point construit à l'étape suivante sont dans $L_n(\sqrt{r})$ ou $r \geq 0$ (une telle extension de L_n obtenue par adjonction d'une racine carrée est appelée une extension quadratique de L_n).

Preuve: On n'a qu'à considérer les coordonnées des points pouvant survenir dans une construction des types (1°) (2°) et (3°); On verra que ces nombres ou bien restent dans L_n ou bien ne sortent pas de L_n $(\sqrt{r})$

Voici quelques préliminaires.

Associons aux objets géométriques (droites et cercles) pouvant être construits à partir des points de K_n des objets algébriques.

Soient (a_1, b_1) et (a_2, b_2) deux points distincts de K_n.

Si $a_1 = a_2$ l'équation de la droite les reliant est $x = a_1$

Si $a_1 = a_2$ l'équation de la droite les reliant est $y-b_1 = m(x-a_1)$ $m=\frac{b_2-b_1}{a_2-a_1}$

On constate que dans chaque cas les coefficients de l'équation sont dans L_n car L_n est un corps.

Le carré de la distance entre les deux points est $r^2 = (a_2-a_1)^2 + (b_2-b_1)^2$ et $r^2 \in L_n$.

L'équation d'un cercle de centre (a_1,b_1) et de rayon r est

$$(x-a_1)^2 + (y-b_1)^2 = r^2$$ et les coefficients sont dans L_n.

Examinons maintenant les coordonnées du ppint obtenu par une construction du type (1°). Ces coordonnées sont la solution d'un système

$$\left.\begin{aligned} a_1x + b_1y &= c_1 \\ a_2x + b_2y &= c_2 \end{aligned}\right\}$$ et par les remarques précédentes tous les coefficients sont dans L_n

L_n étant un corps la solution de ces équations est aussi dans L_n. Ainsi une construction du type (1°) ne nous fait pas sortir de L_n.

L'intersection d'une droite et d'un cercle correspond à la solution d'un système de la forme $\begin{cases} a_1x + b_1y = C_1 \\ x^2 + y^2 + a^2x + b^2y = C_2 \end{cases}$ où tous les coefficients sont dans L_n.

Si on solutionne ce système pour y on voit que y satisfait une équation quadratique de la forme $ay^2 + by + c = 0$ où $a, b, c \in L_n$.

On trouve ainsi que $y= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ et $x= \frac{c_1}{a_1} - \frac{b_1}{a_1}$ y

Ainsi les 4 nombres apparaissant comme coordonnées des points de rencontre sont contenus dans L_n $(\sqrt{r})$ ou $r = b^2 - 4ac$.

Le dernier cas correspond à la solution d'un système de la forme

$$\left.\begin{aligned} x^2+y^2+a_1x + b_1y + c_1 &= 0 \\ x^2+y^2+a_2x + b_2y + c_2 &= 0 \end{aligned}\right\}$$ avec coefficients dans L_n

L'équation de la corde commune est:

$$(a_1 - a_2)x + (b_1 - b_2)y + (c_1 - c_2) = 0;$$ les coefficients

sont dans L_n et les points d'intersection des deux cercles sont les mêmes que les points d'intersection d'un cercle et d'une droite (la corde commune). Le théorème est donc prouvé.

Définition. Un nombre a est dit constructible s'il est possible de construire en un nombre fixe d'étapes un point dont une des coordonnées soit a.

Il est clair que a est constructible si et seulement si on peut construire un segment de longueur a.

Voici un corollaire du théorème 3.

COROLLAIRE Supposons que $K_0 = \{(0,0), (1,0)\}$. Si a est constructible à partir de K_0 alors il existe une suite finie d'extension de F_0 : $F_0 \subset F_1 \subset \ldots \subset F_n$ telle que $a \in F_n$ pour un certain n où $F_1 = F_0(\sqrt{r_1})$, $F_2 = F_1(\sqrt{r_2})$, ..., $F_n = F_{n-1}(\sqrt{r_n})$
i.e. $a \in F_0(\sqrt{r_1}, \sqrt{r_2}, \ldots \sqrt{r_n})$

Preuve: La première étape de la construction ou bien nous laisse dans F_0 ou bien nous fournit des nombres dans $F_0(\sqrt{r_1})$. A la deuxième étape, ou bien on reste dans $F_0(\sqrt{r_1})$ ou au plus dans $F_1(\sqrt{r_2}) = F_0(\sqrt{r_1}, \sqrt{r_2})$, etc.

THÉORÈME 4: Si a est constructible à partir de $K_0 = \{(0,0),(1,0)\}$ alors a est contenu dans une extension K de F_0 dont le degré $[K:F_0]$ est une puissance de 2.

Preuve: Par le corollaire précédent $a \in F_0(\sqrt{r_1}, \ldots \sqrt{r_n})$
Mais par le théorème 1
$[F_0(\sqrt{r_1}, \sqrt{r_2}, \ldots \sqrt{r_n}) : F_0] = [F_0(\sqrt{r_1}):F_0] \times [F_1(\sqrt{r_2}):F_1] \ldots [F_n(\sqrt{r_n}) : F_{n-1}]$

Mais $[F_i(\sqrt{r_i}) : F_{i-1}] = \begin{cases} 2 \text{ si } r_i \text{ n'est pas un carré} \\ 1 \text{ si } r_i \text{ est un carré} \end{cases}$

Donc $[F_0(\sqrt{r_1}, \sqrt{r_2}, \ldots \sqrt{r_n}) : F_0] = 2^r$ où r est le nombre de facteurs égaux à 2.

Voici maintenant le critère de non-constructibilité.

THÉORÈME 5: Si le nombre a est algébrique de degré k sur F_0 et si k n'est pas une puissance de 2 alors a n'est pas constructible à partir du segment unité.

Preuve: Si a est algébrique de degré k alors par le théorème 2, $[F_0(a) : F_0] = k$.

Si a est constructible à partir du segment unité alors $a \in K$ où $[K:F_0] = 2^r$ pour un certain r.

On a alors la chaîne suivante:

$F_0 \subset F_0(a) \subset K$ où $F_0(a)$ est le plus petit sous-corps de contenant F et a; et K contient F et a.

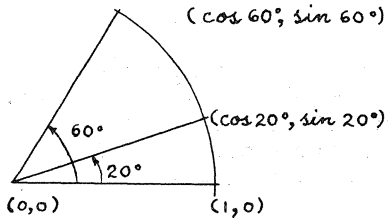
Par le théorème 1, $[F_0(a) : F_0]$ doit diviser $[K:F_0]$ ce qui est impossible si k n'est pas une puissance de 2.

- - - - - - - - - - - - - - - - - - -

IV CAS PARTICULIERS

a) TRISECTION D'UN ANGLE DE 60^0

Un angle de 60^0 est donné ainsi que les points (0,0) et (1,0) i.e. un segment-unité. Les points (0,0) (1,0) et (cos 60^0, sin 60^0) déterminent complètement les objets géométriques donnés. Ainsi $S_0 = \{0, 1, 1/2, \sqrt{3/2}\}$; mais il est facile de voir que les nombres 1/2 et $\sqrt{3/2}$ sont constructibles à partir du segment-unité. Le problème de trisection de cet angle est donc équivalent à celui de la construction des nombres cos 20^0 et sin 20^0 à partir du segment-unité. Montrons que a= cos 20^0 n'est pas constructible à partir du segment-unité.



Considérons l'identité $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ et posons $\theta = 20^0$. On obtient $8a^3 - 6a - 1 = 0$. Ainsi le nombre a qu'on doit construire satisfait aucune équation de degré inférieur à 3 alors a est algébrique de degré 3 sur F_0 et par le théorème 5, a n'est pas constructible.

Montrons que 1^0 Si a satisfait une équation de degré inférieur à 3, alors $8x^3 - 6x - 1 = 0$ est factorisable et

2^0 $8x^3 - 6x - 1 = 0$ n'est pas factorisable.

Soit $p(x) = 8x^3 - 6x - 1$ et q(x) un polynôme de degré inférieur à 3 tel que q(a) = 0
Soit h(x) le p.g.c.d. de p(x) et q(x); on sait qu'alors il existe des polynômes a(x) et b(x) tels que h(x) = a(x) p(x) + b(x) q(x) ce qui entraîne que h(a) = 0. h(x) ne peut être constant car il serait 0; ainsi p(x) est factorisable.

Pour montrer que p(x) n'est pas factorisable, servons-nous d'un résultat dû à Gauss. "Si un polynôme avec des coefficients entiers ne peut être factorisé au moyen de polynômes ayant des coefficients entiers, alors il ne peut être factorisé avec des polynômes à coefficients rationnels"

Pour voir que $8x^3 - 6x - 1$ ne peut être factorisé à l'aide de polynômes à coefficients entiers, il suffit d'écrire $8x^3 - 6x - 1 = (ax+b)(cx^2 + dx + e)$;

de multiplier et d'égaler les coefficients des mêmes puissances de x; on obtient alors une contradiction.

b) DUPLICATION DU CUBE

Construire un cube de volume égal au double du volume d'un cube donné.

En prenant comme unité une arête du cube donné, ce problème est équivalent à construire un nombre a tel que $a^3 = 2$.

Mais $\sqrt[3]{2}$ est algébrique de degré 3 sur F_0 (Prouver), donc la construction est impossible.

c) QUADRATURE DU CERCLE

Construire un carré d'aire égale à l'aire d'un cercle donné.

En prenant comme unité le rayon du cercle donné, ce problème est équivalent à construire le nombre $\sqrt{\pi}$ à partir du segment-unité.

Si a est constructible à partir du segment-unité on sait que a est contenu dans une extension finie de F_0 du type $F_0(\sqrt{r_1}, \sqrt{r_2}, \ldots \sqrt{r_n})$. Mais il est facile de prouver que les éléments d'une extension finie de F_0 sont tous algébriques sur F_0. Ainsi π n'étant pas algébrique sur F_0,* n'est pas dans une extension finie de F_0 et la quadrature du cercle est impossible.

* Lindemann en 1882 a prouvé que π n'est pas algébrique sur F_0.