Algèbre 3 - Théorie de Galois
Construction à la règle et au compas

BRUKIER Pierre DESMONS Bertrand LUIJTEN Marjorie

17 avril 2007

3e Bac Math
Université de Mons-Hainaut

1 Introduction : pourquoi la règle et le compas ?

Depuis l'Antiquité (et notamment du temps de la Grèce antique), on n'autorise comme figure que les droites et les cercles ; les autres figures étant considérées comme "plus faibles". Cette idée amène alors des problèmes qui se révèlent pour eux fondamentaux ; les quatre plus célèbres étant :

- $\sqrt{2}$ est-il rationnel ?
- Etant donné un disque d'une aire donnée, est-il possible de construire un carré de même aire ?
- Est-il possible, grâce à la règle et le compas, de scinder tout angle en trois parties égales ?
- Etant donné un cube de volume donné, est-il possible de construire un côté d'un cube de volume double au premier ?

On sait (depuis Pythagore) que $\sqrt{2}$ est irrationnel ; les trois autres problèmes, majeurs depuis cette époque, n'ont été résolus que "tout récemment", c'est-à-dire en 1837 pour les deux derniers problèmes, et en 1882 pour le deuxième. C'est Fernand von Lindemann qui prouve l'irrationnalité du nombre π, permettant de répondre par la négative à la quadrature du cercle.

En ce qui concerne les deux dernières questions, un théorème de Pierre-Laurent Wantzel donne un critère de test (que nous allons prouver), permettant de savoir si un nombre "a des chances" d'être constructible à la règle et au compas. L'application de ce critère permettra de répondre aux deux questions.

Dans ce sujet, nous allons nous intéresser aux nombres constructibles ; c'est-à-dire ceux que l'on peut créer en utilisant une règle et un compas. Pour ce faire, on se fixera deux points (O et I) et on décide qu'ils sont distants d'une unité. Nous allons discuter de ce qui est constructible à partir de ces deux points, puis prouver un résultat qui montrera qu'on ne peut pas en "faire plus" ; de là seront déduits des réponses aux deux dernières questions. Mais dans un premier temps, rappelons les règles de base de construction.

2 Rappels de construction

2.1 Droites parallèles et perpendiculaires

On considère une droite D et un point p dans le plan. Pour construire la droite perpendiculaire à D passant par p, on procède comme suit :

- Compas centré en p, de rayon supérieur à la distance entre le point et la droite ; on trace un cercle et on considère a et b les deux points d'intersection.
- Compas centré en a et de même rayon : on trace le cercle (qu'on nomme C_1).
- Compas centré en b et de même rayon : on trace le cercle (qu'on nomme C_2).
- $C_1 \cap C_2$ consiste en deux points : [1] soit q un point de cette intersection, différent de p.
- La droite recherchée est celle qui passe par p et q ; on la trace à la règle.

[1] Remarquons que si p est sur D, la construction fonctionne encore, mais il faut augmenter le rayon pour tracer C_1 et C_2 pour obtenir deux points d'intersection distincts.

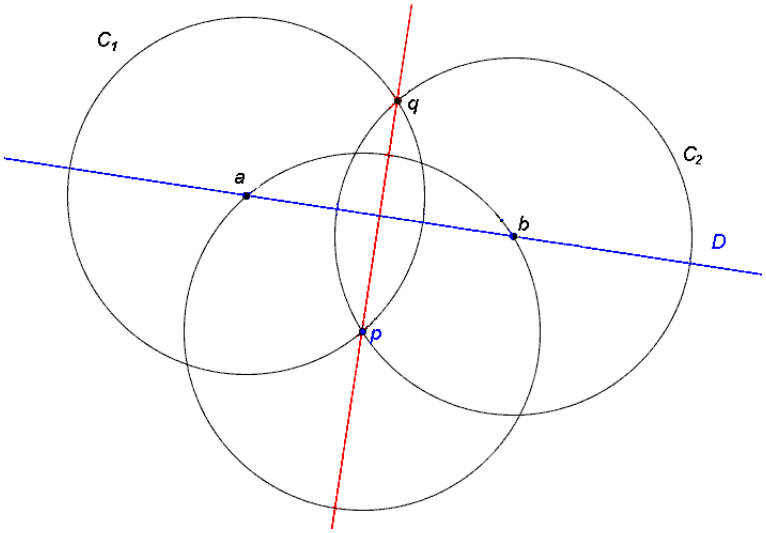

FIG. 1 – Construction d'une perpendiculaire

Concernant les droites parallèles, une idée pourrait être de construire deux fois des droites perpendiculaires ; mais il y a plus efficace, en procédant comme suit :

- Si p n'est pas sur D (sinon, c'est terminé...), on choisit q un point quelconque de D.
- On centre le compas en q et on trace le cercle qui passe par p ; posons r l'un des points d'intersection du cercle construit avec D.
- En gardant le même rayon, on trace C_1 le cercle centré en p et C_2 le cercle centré en r. Notons que q est un point commun aux deux cercles.
- On pose s l'autre point d'intersection ; alors la droite recherchée est celle passant par p et s ; on la trace à la règle.

2.2 Construction de nouveaux nombres

On crée de nouveaux nombres en additionnant deux nombres construits, ou en les multipliant. On va voir aussi qu'on peut construire la racine carrée d'un nombre. Pour cette partie, on pose les points p,q et r tels que la distance entre p et q désigne notre premier nombre, et la distance de p à r notre second nombre.

2.2.1 Addition

Pour l'addition de deux nombres, il suffit de mettre les deux nombres bout à bout. Pour être rigoureux, on doit prolonger (s'il y a lieu) la droite pq, tracer le cercle centré en q et de rayon $\overline{pr}$, et si on pose s le point d'intersection de la droite et du cercle le plus éloigné de p, alors la distance de p à s est le nombre voulu.

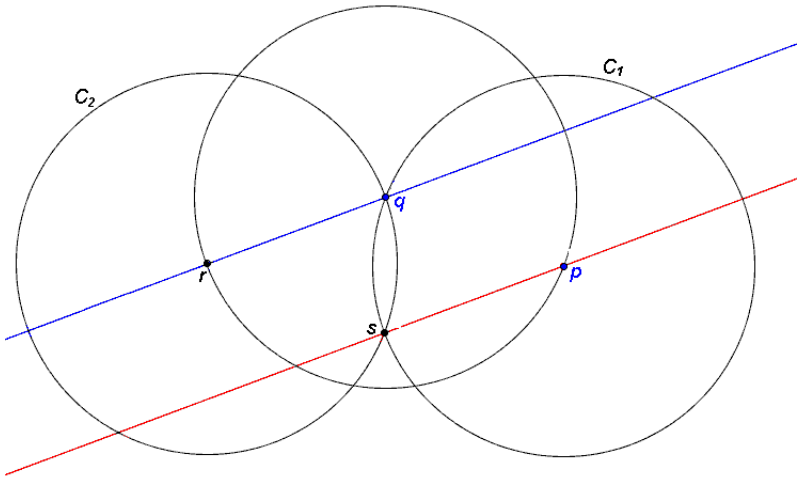

FIG. 2 – Construction d'une parallèle

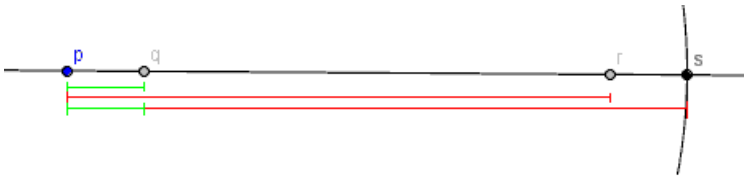

FIG. 3 – Somme de deux nombres constructibles

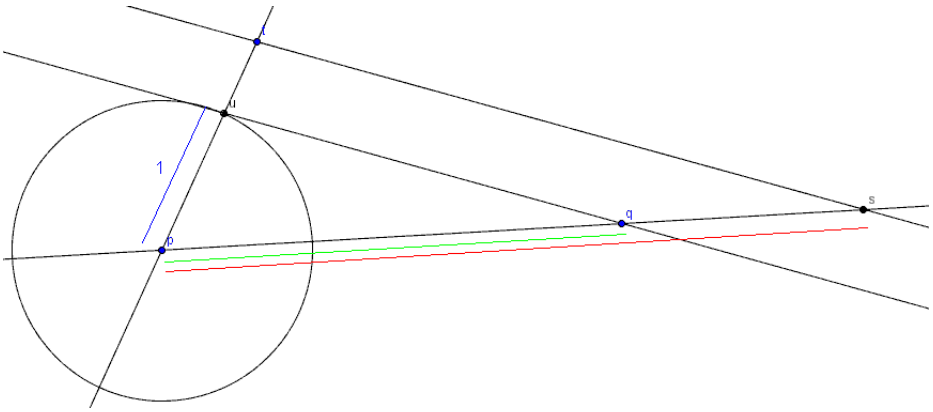

FIG. 4 – Produit de deux nombres constructibles

2.2.2 Produit

Le produit de deux nombres construits est un peu plus subtil. On procède comme suit :

- A partir de p, on trace un cercle de rayon 1 ; soit u un point de ce cercle, qui ne soit pas sur la droite pq (tant qu'on y est, si r n'est pas sur cette droite, u sera l'intersection de la droite ps avec le cercle tracé !)
- On trace la droite pu. Si r n'est pas sur cette droite, "on l'y met" en centrant notre compas en p et en traçant le cercle de rayon $\overline{pr}$; on pose alors t le point d'intersection de ce cercle avec la droite pu, tel que t soit plus près de u que de p. Si r était sur la droite pu, on l'appellle t.
- On utilise alors le théorème de Thalès comme suit. On trace la droite D_1 comprenant les points q et u ; D_2 s'obtient comme la parallèle à D_1 passant par t. Si s est le point d'intersection de D_2 avec la droite pq, alors la distance de p à r est le nombre recherché.

2.2.3 Extraction de racine carrée

Un autre théorème nous aidera à construire la racine carrée d'un nombre donné : c'est le théorème de Pythagore. On sait construire aisément le nombre $\sqrt{1+x^2}$, si x désigne la distance de p à q ; pour ce faire, on construit D la droite perpendiculaire à pq passant par p, et C un cercle de centre p et de rayon 1 ; si s est *un* point d'intersection de D et C, alors la distance de q à s est le nombre recherché.

Pour construire réellement $\sqrt{x}$, on doit travailler un peu plus. On utilise le fait que, dans un triangle qsu rectangle en s, si p est le pied de la hauteur issue de s, on a

$$pu \times pq = ps^2 \tag{1}$$

(c'est une conséquence immédiate du fait que les triangles pqs et usp sont semblables) et la propriété du triangle rectangle inscrit dans un demi-cercle (il est rectangle en un sommet si et seulement si le côté opposé à ce sommet est un diamètre du cercle circonscrit au triangle).

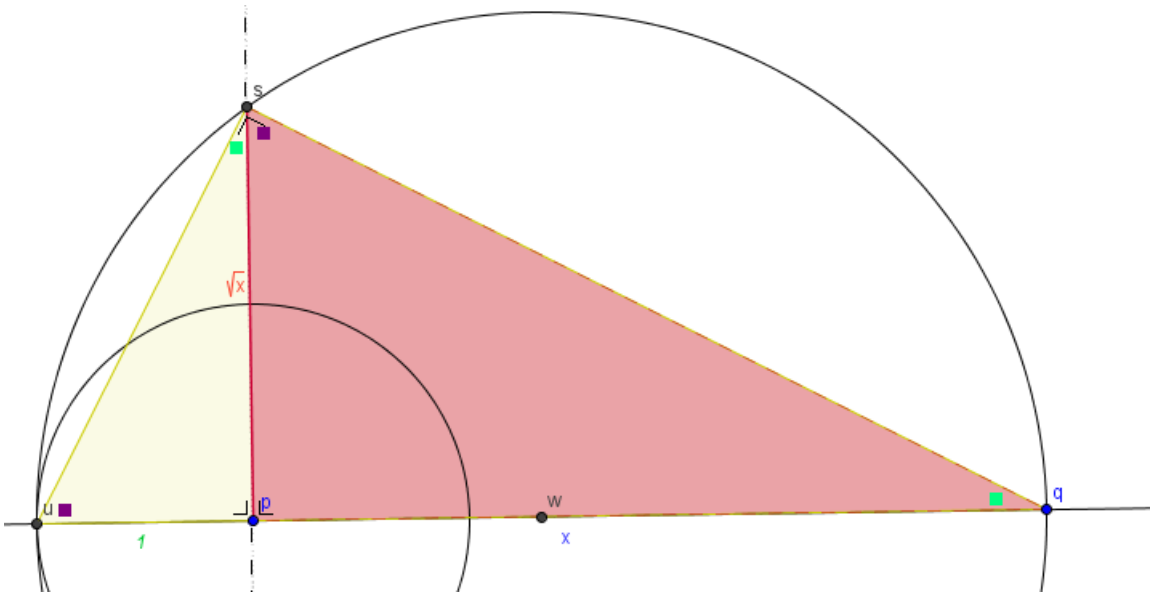

FIG. 5 – Racine carrée d'un nombre constructible

On pose $x = \overline{pq}$; et on procède de la manière suivante pour en construire sa racine carrée :

- On trouve u le point sur la droite pq tel que $\overline{pu} = 1$ et $\overline{pq} < \overline{uq}$ (pour ce faire, construire le cercle centré en p et de rayon 1, et prendre le bon point d'intersection) ;
- On trace C le cercle de diamètre uq (pour ce faire, on obtient aisément w le point milieu en reprenant la même construction que les droites perpendiculaires – cette fois, a et b sont respectivement u et q, et on a w comme point d'intersection de la droite construite avec la droite pq.)
- Soit s le point d'intersection de C avec la droite perpendiculaire à pq passant par p ;
- puisque les triangles pqs et qsu sont semblables (car le "grand" triangle uqs est rectangle en s et que les deux "petits" sont rectangles en p) on obtient (voir équation 1 et figure 5) que $\overline{ps} = \sqrt{x}$.

3 Nombres constructibles et extensions quadratiques

3.1 Qu'est-ce qu'un nombre constructible ?

Nous allons maintenant caractériser les nombres constructibles ; pour cela, on formalise la construction. Soient O et I deux points quelconques dans le plan ; on pose $\overline{OI} = 1$. On construit le point J comme intersection de la droite perpendiculaire à OI passant par O et du cercle de rayon 1 centré en O. Alors $\overline{OJ} = 1$ et les vecteurs $\overrightarrow{OI}$ et $\overrightarrow{OJ}$ sont orthogonaux. Grâce à cela, on va construire

des nombres en les considérant comme tels plutôt qu'en tant que distances entre points. On étend alors la définition de nombre constructible comme suit :

Définition 1. *Un nombre x est dit* constructible *s'il existe deux points A et B tels que :*

1. *A et B sont constructibles à la règle et au compas ;*
2. $\overline{AB} = |x|$.

En particulier x est constructible ssi le point de coordonnées $(x,0)$ *est constructible à la règle et au compas.*

Il n'est peut-être pas évident que les deux définitions sont équivalentes ; pourtant c'est bien le cas. En effet, la "remontée" est triviale ; pour "descendre", on construit le point $(x,0)$ comme point d'intersection de la droite OI avec le cercle centré en O et de rayon $\overline{AB}$, le plus proche de I si $x > 0$, le plus éloigné sinon. On constate facilement que, grâce cette définition :

- tous les nombres naturels sont constructibles, par addition ;
- tous les entiers aussi, par extension de la définition ;
- et on prouve maintenant via une petite manipulation, que tous leurs inverses aussi. Il s'agit en fait de la construction inverse à la multiplication ; en reprenant la figure 4 et en supposant les points p, $r(=t)$ et s connus, on trouve aisément le point q en prenant la droite parallèle à rs passant par u (rappelons que $\overline{pu} = 1$.)
- dès lors tous les nombres rationnels sont constructibles.
- Par la construction de racines carrées, on peut prendre les racines carrées des rationnels, et répéter diverses constructions...

Notre but est de donner une certaine limitation aux nombres constructibles ; ie donner une condition que satisfont tous ces nombres.

3.2 Formalisation des notions d'intersection

Nous avons jusqu'ici exploité de manière intuitive les intersections de droites et de cercles. Il est aisé de voir que les droites s'obtiennent à la règle, et les cercles au compas. Pour la suite, on se fixe un corps K qu'on suppose inclus à $\mathbb{R}$; mais nous nous intéresserons plus particulièrement à $K = \mathbb{Q}$, qui est à la base des questions.

Rappelons que l'équation générale d'une droite D dans le plan (ou de manière générale, dans $K \times K = K^2$) est de la forme

$$D \equiv ax + by + c = 0 \text{ pour certains } a,b,c \in K \text{ et } a,b \text{ non tous deux nuls.} \tag{2}$$

Si on voulait être très rigoureux, on devrait dire que D est l'ensemble des points qui vérifient l'équation, mais travailler sur ces ensembles revient principalement à travailler sur les équations ; d'où l'amalgame entre ensemble et équation.

De même, tout cercle dans le plan (ou dans K^2) admet pour équation

$$C \equiv (x-a)^2 + (y-b)^2 = c^2 \text{ pour certains } a,b,c \in K \tag{3}$$

où le point (a,b) est le centre et c le rayon du cercle (dans notre cadre de $K \subset \mathbb{R}$, on exige en plus que $c > 0$).

On va maintenant prouver quelques résultats qui formaliseront la notion d'intersection, et qui justifieront les constructions déjà réalisées dans l'introduction.

Proposition 1. *Soient D_1 et D_2 deux droites ; si elles ne sont pas parallèles, alors l'intersection des deux droites consiste en un et un seul point de K^2.*

Il est évident que dans le cas parallèle, soit les droites sont confondues, auquel cas il y a une infinité de points d'intersection (du moins, en caractéristique 0...) ; soit elles sont disjointes et il n'y a aucun point d'intersection.

Démonstration. On pose $D_1 \equiv ax+by+c=0$ et $D_2 \equiv dx+ey+f=0$; le fait de s'assurer que D_1 et D_2 ne soient pas parallèles implique que $\frac{a}{d} \neq \frac{b}{e}$; en d'autres termes, que $ae-bd \neq 0$. Dès lors, a et d ne peuvent être tous deux nuls, et on peut supposer sans perte de généralité que $a=1$. Ceci nous permet d'écrire

$$D_1 \equiv x+by+c=0 \text{ et } D_2 \equiv dx+ey+f=0 \tag{4}$$

Si $(x,y) \in D_1 \cap D_2$, on obtient directement par l'équation de D_1, que $x=-by-c$; cette relation injectée dans l'équation de D_2, donne

$$\begin{aligned} d(-by-c)+ey+f &= 0 \\ y(e-bd)+f-cd &= 0 \\ y(e-bd) &= cd-f \end{aligned}$$

et, puisque $ae-bd = e-bd \neq 0$, on obtient y en fonction des paramètres des équations ; et au final, le seul point d'intersection est le point $(-b\frac{cd-f}{e-bd}-c, \frac{cd-f}{e-bd})$. Il est aisé de voir qu'il s'agit d'un point de K^2, car on n'utilise que des additions, des multiplications, et des prises d'opposé et d'inverse. □

Proposition 2. *Soient D une droite et C un cercle ; alors l'intersection de D et C consiste en 0, 1 ou 2 points, et selon les cas :*

- *un unique point d'intersection sera dans K^2 ;*
- *deux points d'intersection seront tels que leurs coordonnées appartiennent à K ou à une de ses extensions quadratiques.*

Démonstration. On pose $D \equiv ax+by+c=0$ et $C \equiv (x-d)^2+(y-e)^2-f^2=0$; deux cas se présentent :

Soit $a=0$: alors on peut supposer sans perte de généralité, que $b=1$ car il sera non-nul ; alors $D \equiv y+c=0$. Un point dans l'intersection de D et C sera de la forme $(x,-c)$, tel que $x^2+kx+l=0$ avec $k=-2d$ et $l=d^2-f^2+(c+e)^2$. Par une manipulation algébrique qui correspond exactement au discriminant, on obtient $(x+\frac{k}{2})^2=u$ avec $u=\frac{k^2}{4}-l=d^2-l=$

$f^2-(c+e)^2$. Or ce dernier nombre pourrait ne pas être un carré dans K ; en fait tout dépend du signe de u. Si $u<0$, alors, puisqu'on s'intéresse aux sous-corps de $\mathbb{R}$, on dira qu'il n'y a pas de point d'intersection. Sinon, on est amené à discuter différents cas suivant l'existence de $w \in K$ tel que $w^2 = u$ (un tel w existe dans $\mathbb{R}$) :

1. si c'est le cas, on obtient $x+\frac{k}{2} = \pm w$, soit $x = -\frac{k}{2} \pm w$. On obtient alors au plus deux points à coordonnées dans K :

$$(x_1,y_1) = (-d-w,c) \text{ et } (x_2,y_2) = (-d+w,c) \tag{5}$$

   avec $w \in K$ tel que $w^2 = f^2-(c+e)^2$.

2. sinon, on se place dans $K(\sqrt{u})$, le plus petit corps contenant à la fois K et une racine du polynôme X^2-u (qui, clairement n'admet pas de racine dans K, donc est irréductible). Dans un tel corps, on trouve alors un w qui convient ; et on a les mêmes solutions qu'en 5 avec cette fois-ci $w = \pm\sqrt{u} \in K(\sqrt{u}) \supsetneq K$, avec $u = f^2-(c-e)^2$. Contrairement au point précédent, les points seront à coordonnées dans $K(\sqrt{u})$.

Soit $a \neq 0$: alors on pose $a = 1$ sans perdre de généralité ; l'équation de D se réduit à $x+by+c = 0$. Pour qu'un point (x,y) soit dans l'intersection, il faut que $x = -by-c$; cette relation, injectée dans l'équation de C, donne :

$$(-by-c-d)^2+(y-e)^2-f^2 = 0. \tag{6}$$

Si b est nul, alors on est ramenés comme précedemment à une équation du type y^2+ky+l, avec $k=-2e$ et $l = e^2+(c+d)^2-f^2$. On réapplique exactement le même raisonnement que ci-dessus pour obtenir $u = \frac{k^2}{4}-l = e^2-l = f^2-(c+d)^2$, et les solutions :

$$(x_1,y_1) = (-c,-e-w) \text{ et } (x_2,y_2) = (-c,-e+w) \tag{7}$$

avec w appartenant "au pire" à une extension quadratique de K (on rajoute à K une racine de X^2-u et on prend le plus petit corps engendré) ; tel que $w^2 = f^2-(c+d)^2$.
Sinon, à partir de 6, on obtient :

$$\begin{aligned} 0 = & \quad (-by-c-d)^2+(y-e)^2-f^2 \\ = & \quad b^2(y+\frac{c+d}{b})^2+(y-e)^2-f^2 \\ = & \quad y^2(b^2+1)+2y(bc+bd-e)+(c+d)^2+e^2-f^2 \\ = & \quad py^2+qy+r \end{aligned}$$

Puisque $K \subset \mathbb{R}$ on a $p>0$ (car c'est une somme de nombres positifs, dont un strictement). On obtient de nouveau une équation du type

$$(y+\frac{q}{2p})^2 = \frac{q^2}{4p^2}-\frac{r}{p} = \frac{q^2-4pr}{4p^2} \tag{8}$$

qui admet deux solutions (ou une "double") si et seulement si $q^2-4pr \geq 0$ (alors, les deux points recherchés sont de la forme

$$(x,y) = (-by_{1,2} - c, y_{1,2}) \text{ avec } y_{1,2} = \frac{-q \pm \sqrt{q^2-4pr}}{2p} \tag{9}$$

et qui n'en a pas si $q^2-4pr < 0$. Dans le cas de deux solutions, soit elles sont dans K, soit dans l'extension quadratique $K(\sqrt{q^2-4pr})$; dans le cas d'une seule solution, elle est dans K.

Conclusion, parmi tous les cas, on a au plus deux points d'intersection ; dans le cas d'un seul point, il est dans le plan de K, s'il y en a 2 soit ils sont dans K^2, soit leurs coordonnées sont dans une extension quadratique de K. □

Proposition 3. *L'intersection de deux cercles de K^2 non centrés en un même point [2] consiste en 0, 1 ou 2 points ; un point seul appartiendra à K^2, deux points auront leurs coordonnées dans K ou l'une de ses extensions quadratiques.*

Démonstration. Si $C_1 \equiv (x-a)^2+(y-b)^2 = c^2$ et $C_2 \equiv (x-d)^2+(y-e)^2 = f^2$, on réécrit les équations comme suit :

$$\begin{cases} C_1 \equiv & x^2+y^2+rx+sy+t = 0 \\ C_2 \equiv & x^2+y^2+ux+vy+w = 0 \end{cases} \tag{10}$$

Un point (x,y) appartiendra à $C_1 \cap C_2$ si et seulement s'il vérifie les équations 10 ; c'est équivalent au fait qu'il vérifie :

$$\begin{cases} C_1 \equiv & x^2+y^2+rx+sy+t = 0 \\ D_2 \equiv & (u-r)x+(v-s)y+(w-t) = 0 \end{cases} \tag{11}$$

soit l'intersection d'un cercle avec une droite [3], et on se ramène alors à la proposition précédente. □

3.3 Caractérisation des nombres constructibles – Théorème de Wantzel

Pour comprendre mieux la suite, on s'intéressa à $K = \mathbb{Q}$. On remarque que la construction de points donne lieu à des extensions quadratiques ; chaque fois qu'on considère l'intersection d'un cercle avec une droite ou un autre cercle, un nouveau nombre peut apparaître, et son polynôme minimal (irréductible) sera de degré 1 ou 2. Pour chacune des étapes, soit on garde le corps initial, soit on passe à une extension quadratique de ce corps. La définition suivante permet de "collecter" les extensions réellement utilisées.

[2] Si ce n'est pas le cas, alors on peut n'avoir aucun point d'intersection – si les rayons sont différents– ou une infinité de points d'intersection – cas de rayons égaux.

[3] c'en est une que si $u-r$ et $v-s$ sont non tous deux nuls. Si $u-r = v-s = 0$, on remarque qu'alors $a = d$ et $b = e$ dans les équations initiales, donc même centre, d'où violation des hypothèses.

Définition 2. *Une* tour d'extensions quadratiques *d'un corps K est une suite croissante – au sens de l'inclusion – de corps* $(K_0, K_1, ...K_n)$ *telle que :*

1. $K_0 = K$;
2. *pour tout* $1 \leq i \leq n$, K_i *est une extension quadratique de* K_{i-1}.

On remarque clairement que, pour tout i entre 0 et n, tout élément u d'une extension K_i de la tour quadratique est algébrique sur K_0, et de degré 2^i. En effet, on a $[K_i : K_0] = \prod_{j=1}^{i} [K_j : K_{j-1}] = \prod_{j=1}^{i} 2 = 2^i$.

Voici le théorème général qui décrit les nombres constructibles :

Théorème 1. ***Théorème de Wantzel***
Soit $c \in \mathbb{R}$ *; alors c est constructible si et seulement s'il existe une tour d'extensions quadratiques finie* $(K_0, K_1, ...K_n)$ *telle que* $K_0 = \mathbb{Q}$ *et* $c \in K_n$.

Ce théorème a été prouvé par Pierre-Laurent Wantzel en 1837 ; une copie de sa preuve est disponible à *http ://fr.wikisource.org/wiki/Théorème_de_Wantzel*. Nous n'allons pas la présenter ici, elle est un peu compliquée. Par contre, nous allons donner une caractérisation nécessaire pour qu'un nombre soit constructible :

Théorème 2. ***Critère de test d'un nombre constructible***
Soit $c \in \mathbb{R}$, *s'il est constructible alors il est algébrique sur* $\mathbb{Q}$ *et* $[\mathbb{Q}(c) : \mathbb{Q}]$ *est une puissance de 2.*

Ce test va s'avérer utile par sa réciproque : si pour un nombre donné, on trouve que le degré de son polynôme irréductible n'est pas une puissance de 2, alors il ne pourra être construit à la règle et au compas. Par contre, on ne pourra rien conclure si ce degré est une puissance de 2... par exemple, on peut montrer que le polynôme $X^4 + 2X - 2$ est bien irréductible de degré 4 mais que ses racines ne sont pas constructibles.

Démonstration. Par définition, c est constructible si et seulement si le point $(c, 0)$ peut être localisé de manière précise par une séquence finie de constructions à la règle et au compas commencant avec des points du plan de $\mathbb{Q}$.[4] Dans le déroulement de ces constructions, plusieurs points du plan seront déterminés comme intersection de droites ou cercles utilisés dans le processus de construction (seule possibilité de construire des nouveaux points en utilisant uniquement la règle et le compas). Le premier pas dans le processus de construction est la construction d'une droite ou d'un cercle, tous 2 complètement déterminés par 2 points.

Soit ces 2 points sont donnés dans le plan de $\mathbb{Q}$, soit ils seront choisis arbitrairement, auquel cas ils seront aussi dans $\mathbb{Q}^2$. De manière similaire, à chaque étape de la construction, les 2 points qui déterminent la droite ou le cercle peuvent être choisis comme points du plan de $\mathbb{Q}$ ou points

[4] A priori, on commence avec les points $(0,0)$ et $(1,0)$, mais on passe rapidement aux points à coordonnées entières puis rationnelles – voir page 7 pour la construction d'un rationnel.

construits dans les étapes précédentes. Par les propositions 1 à 3, le premier point ainsi construit sera dans le plan de l'extension quadratique $\mathbb{Q}(\sqrt{u})$ ($u \geq 0, u \in \mathbb{Q}$) de $\mathbb{Q}$ ou, de manière équivalente dans le plan d'une extension $\mathbb{Q}(v_1)$ de $\mathbb{Q}$ avec $v_1^2 \in \mathbb{Q}$. Comme une telle extension a un degré $1 = 2^0$ ou 2 sur $\mathbb{Q}$ (en effet, si $v_1 \in \mathbb{Q}$, $\mathbb{Q}(v_1) = \mathbb{Q}$ donc $[\mathbb{Q}(v_1) : \mathbb{Q}] = 1$; et si $v_1 \notin \mathbb{Q}$, le polynôme minimal irréductible de v_1 est $P := x^2 - v_1^2 \Rightarrow [\mathbb{Q}(v_1) : \mathbb{Q}] = 2$, degré de P).

Par un processus semblable , le point qui sera contruit par la suite sera dans le plan $\mathbb{Q}(v_1, v_2) = \mathbb{Q}(v_1)(v_2)$ avec $v_2^2 \in \mathbb{Q}(v_1)$. Et à un certain moment, on aura atteint c dans une extension quadratique d'une extension quadratique d'une ... d'une extension quadratique de $\mathbb{Q}$. On obtient alors la suite finie d'inclusions suivante :

$$\mathbb{Q} \subset \mathbb{Q}(v_1) \subset \mathbb{Q}(v_1, v_2) \subset \cdots \subset \mathbb{Q}(v_1, \cdots, v_n) \text{ avec } \forall 1 \leq i < n, v_{i+1}^2 \in \mathbb{Q}(v_1, \cdots, v_i) \text{ et } v_1^2 \in \mathbb{Q}. \quad (12)$$

et pour tout i entre 2 et n, $[\mathbb{Q}(v_1, \cdots, v_i) : \mathbb{Q}(v_1, \cdots, v_{i-1}] = 1$ ou 2 ;

Le point $(c, 0)$ ainsi construit se trouve dans le plan de $\mathbb{Q}(v_1, \cdots, v_n) =: F$, donc on obtient

$$\begin{aligned}
&[F : \mathbb{Q}] = [\mathbb{Q}(v_1, \cdots, v_n) : \mathbb{Q}] \\
&= [\mathbb{Q}(v_1, \cdots, v_n) : \mathbb{Q}(v_1, \cdots, v_{n-1})] \times [\mathbb{Q}(v_1, \cdots, v_{n-1} : \mathbb{Q}(v_1, \cdots, v_{n-2})] \\
&\times \cdots \times [\mathbb{Q}(v_1) : \mathbb{Q}] \\
&= 2^k \text{ pour un certain } k \leq n \text{ – formule de l'indice.}
\end{aligned}$$

ceci implique que c est algébrique sur $\mathbb{Q}$.

De plus, $\mathbb{Q} \subset \mathbb{Q}(c) \subset F$ et ce sont des extensions de corps ; donc $F/\mathbb{Q}(c)/\mathbb{Q}$ est une extension et $[F : \mathbb{Q}] = [F : \mathbb{Q}(c)] \times [\mathbb{Q}(c) : \mathbb{Q}] = 2^k$ d'où $[\mathbb{Q}(c) : \mathbb{Q}]$ divise $[F : Q] = 2^k$ et ne peut donc qu'être une puissance de 2. □

4 Applications du théorème

Le théorème de Wantzel, et plus exactement le critère démontré au théorème 2 nous permet de répondre aux questions de l'antiquité :

4.1 Trisection de l'angle

Proposition 4. *Un angle de 60° ne peut être divisé en 3 parties égales par construction à la règle et au compas*

Démonstration. Si il était possible de le faire, alors on pourrait construire un triangle rectangle avec un angle aigu de 20°. Donc on pourrait construire le nombre réel $\cos 20°$.

Cependant les formules trigonométriques permettent de prouver que $\forall \alpha, \cos(3\alpha) = 4\cos^3 \alpha - 3\cos \alpha$. Si $\alpha = 20°$, $\cos 3\alpha = \cos 60° = \frac{1}{2}$ et $\cos 20°$ est donc une racine de l'équation $\frac{1}{2} = 4x^3 - 3x$, ie du polynôme $8x^3 - 6x - 1$. Mais ce polynôme est irréductible dans $\mathbb{Q}[x]$ (un critère est de regarder les diviseurs du terme indépendant, les racines possibles seraient -1 et 1 et aucune d'entre elles n'annule le polynôme) et $\cos 20°$ a un degré 3 sur $\mathbb{Q}$. Conclusion, $\cos 20°$ ne peut être construit à la règle et au compas, par le théorème précédent. □

4.2 Duplication d'un cube

Proposition 5. *Il est impossible par constructions à la règle et au compas de dupliquer un cube de côté 1 (càd il est impossible de construire le côté d'un cube de volume 2).*

Démonstration. Si s est la longueur du côté d'un cube de volume 2, alors s est la racine (réelle) du polynôme $x^3 - 2$. Or, ce dernier est irréductible dans $\mathbb{Q}[x]$ (par le critère de Eisenstein appliqué avec $p = 2$) et est donc le polynôme minimal de s. Ce nombre, qui est donc de degré 3 sur $\mathbb{Q}$, n'est pas constructible par le théorème 2. □

Table des matières

Références

Ressources utilisées :

– T. HUNGERFORD, *Algebra*, coll. GTM n° 73, éd. Springer, 1974.
– WIKIPEDIA : *http ://fr.wikipedia.org*, articles *Nombre constructible* et *Théorème de Wantzel*.
– Les figures ont été réalisées avec le logiciel GeoGebra, disponible sur le web : *www.geogebra.org*.

Pour aller plus loin :

– J. - C. CARRÉGA, *Théorie des corps, la règle et le compas*, éd. Hermann, 1981 (réédité en 2001).
– Historique de la construction à la règle et au compas : *http ://fr.wikipedia.org/wiki/Construction_à_la_règle_et_au_compas*
– Extensions quadratiques, théorème de Wantzel : articles de WIKIPEDIA : *Tour d'extensions quadratiques*, et WIKISOURCE : *http ://fr.wikisource.org/wiki/Théorème_de_Wantzel*
– Duplication d'un cube : le mésolabe d'Eratostène – *http ://mathematiques.ac-bordeaux.fr/viemaths/hist/dossier/mesolabe/mesolabe.pdf*
– Trisection d'un angle : construction d'Abe, *http ://fr.wikipedia.org/wiki/Trisection_de_l'angle*