Travail d'étude et de recherche

Maîtrise de Mathématiques

Construction géométrique et algébrique à la règle et au compas

Sabine Pérès

Encadrants : A.M Bayad

2000-2001

Université d'Évry-Val d'Essonne

Table des matières

0.1 Introduction

La partie des mathématiques grecques la plus célèbre est la géométrie, dont la résolution de problèmes nécessitait uniquement la règle et le compas : instrument canonique du géomètre. Ces instruments ont permis à Euclide dans ses Eléments d'illustrer ses démonstrations de figures bien faites qui faisaient parfois partie intégralement de ses démonstrations.
De plus vers 550 avant J.C, n'étant connue que les entiers naturels et les fractions d'entiers naturels, le théorème de Pythagore met en évidence de nouveaux nombres constructibles à la règle et au compas, par exemple : $\sqrt{2}$=diagonale d'un carré de côtés de longueur 1.
De plus, quelques problèmes se sont instaurés comme la quadrature du cercle, la duplication du cube, la trisection de l'angle et le polygone régulier à n côtés.
La quadrature du cercle : Les grecques de l'antiquité cherchaient à obtenir l'aire du cercle mais comme ils avaient une mauvaise connaissance du nombre π, ils voulaient ramener ce calcul à un calcul plus simple, celui de l'aire du carré.
La duplication du cube : Etant facile de dupliquer un carré (construire un nouveau carré ayant pour côté la diagonale du premier), la duplication du cube a dû se poser de façon assez naturelle. Une légende explique l'origine de ce problème de la façon suivante : la peste régnait à Délos. L'oracle consulté déclara qu'Appolon voulait qu'on lui érigeat un autel double de l'autel cubique qui lui était consacré. On construisit un autel de côté double, la peste continua. L'oracle déclara qu'Appolon n'avait pas eu satisfaction. A cause de cette légende, ce problème porte aussi le nom de *problème de Délos*.
La trisection de l'angle est un problème assez naturel puisque l'on savait à la règle et au compas construire la bissectrice d'un angle.
Dans ses Eléments, Euclide donne les constructions des polygones réguliers à 3, 4, 5, 6, 15 côtés et on ne put en obtenir d'autres jusqu'en 1796 où Gauss alors agé de 19 ans démontra que le polygone régulier à 17 côtés était constructible à la règle et au compas.
Ces quatres problèmes seront énoncés clairement dans le chapitre 1 après avoir définit les notions de points constructibles et les problèmes résolubles à l'aide de la règle et du compas. On résolvera ces problèmes dans le chapitre 2 à l'aide des résultats de Wantzel sur les nombres réels constructibles que l'on démontrera, puis on donnera une caractérisation de ces nombres grâce à une version complexe du théorème de Wantzel.
On donnera des exemples de construction uniquement au compas (le problème de Napoléon : construction du centre d'un cercle) et à la règle seule dans le chapitre 4, puis on démontrera les résultats de Mohr et de Mascheroni disant que les points que l'on peut construire à la règle et au compas sont en fait constructibles uniquement avec le compas.

Chapitre 1

Constructions géométriques et algébriques à la règle et au compas

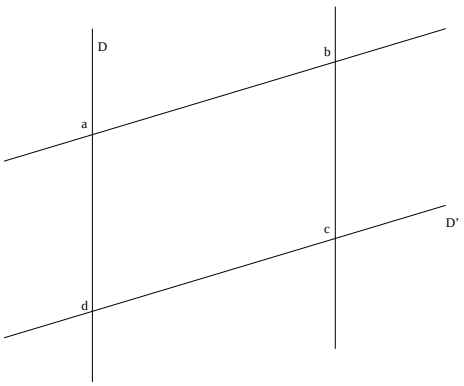
1.1 Géométrie affine

On note P un plan affine euclidien orienté. Soit $R = (O, \overrightarrow{i}, \overrightarrow{j})$ un repère orthonormé direct de P. On note $I = O + \overrightarrow{i}$ et $J = O + \overrightarrow{j}$. Pour chaque point M de P, $M = O + x\overrightarrow{i} + y\overrightarrow{j}$, où $(x, y) \in \mathbb{R}^2$ sont ses coordonnées dans R.

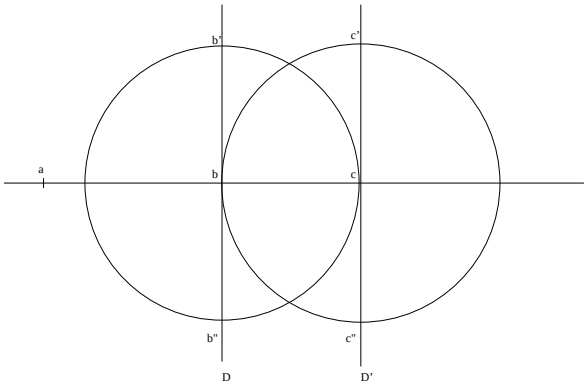
Définition 1 : Soit X une partie de P tels que $card(X) \geq 2$.
Soient $A = \{(ab); (a, b) \in X^2, a \neq b\}$, l'ensemble des droites affines passant par deux points distincts de X.
$B = \{C(a, \|ab\|), (a, b) \in X^2, a \neq b\}$, l' ensemble des cercles centrés en un point de X et passant par un autre point de X.
On dit que M est **constructible** en un pas à partir de X si et seulement si M est un point d'intersection de deux droites distinctes de A, de deux cercles distincts de B ou bien d'une droite de A et d'un cercle de B.

Remarque : *on peut remplacer B par $B' = \{C(a, \|bc\|), (a, b, c) \in X^3, b \neq c\}$, l' ensemble des cercles centrés en un point de X et de rayon la distance entre deux points de X.*

Preuve : Soient G l'ensemble des points constructibles à partir de A et B et G' l'ensemble des points constructibles à partir de A et B'.
• $\forall c \in B$, on a $c \in B' \Longrightarrow G \subseteq G'$.
• Pour montrer que $G' \subseteq G$, on va montrer que :
a, b, c sont trois points distincts de $G \Longrightarrow \exists x \in C(a, \|bc\|)$ tels que $x \in G$.
Si $a \notin (bc)$, soient D=la parallèle à (bc) passant par a et D'=la parallèle à (ab) passant par c. On a bien $D \in A$ et $D' \in A$.
Alors $d = D \cap D' \in G$ et par construction $\|ad\| = \|bc\| \Longrightarrow C(a, \|bc\|) = C(a, \|ad\|)$ $\Longrightarrow G' \subseteq G$.



Si $a \in (bc)$, soient D=la perpendiculaire à (bc) passant par b et D'=la perpendiculaire à (bc) passant par c.
Soient $\{b';b''\} = D \cap C(b, \|bc\|)$, $\{c';c''\} = D' \cap C(c, \|bc\|)$. On a b', b'', c', c'' appartiennent à G.
Or suivant la position des points, on a $\|bc\| = \|b'c'\|$ ou $\|b'c''\|$. Quitte à changer les noms, supposons $\|bc\| = \|b'c'\|$ et comme $a \neq (b'c')$, on est ramené au cas précédent.



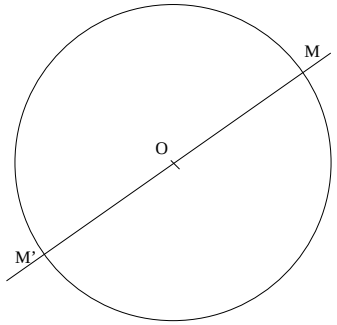
Définition 2 : Soit $B_0 \subseteq$P, avec card$(B_0) \geq 2$.
On définit par récurrence : $\forall i \in I\!N^*$, B_i=$\{$l'ensemble des **points constructibles** à la règle et au compas en un pas à partir de B_{i-1} $\}$. B_i est appelé l'ensemble des points constructibles à la règle et au compas en i pas à partir de B_0.

Remarque : $(B_n)_{n \in I\!N}$, est une suite croissante au sens de l'inclusion.
Un point M du plan est constructible en n étapes à partir de B_0 s'il existe une suite finie $M_1, M_2, ..., M_n$ de points de P telle que $M_n = M$ et que pour $i = 1, .., n$ M_i soit constructible en une étape à partir de $B_0 \cup \{M_j, j < i\}$
Un point M du plan est dit constructible à partir de B_0 s'il existe un entier n tel que M soit constructible en n étapes à partir de B_0 .
Si B_0 n'a qu'un seul élément on peut rien construire de nouveau à partir de B_0 .

1.2 Problèmes résolubles à l'aide de la règle et du compas

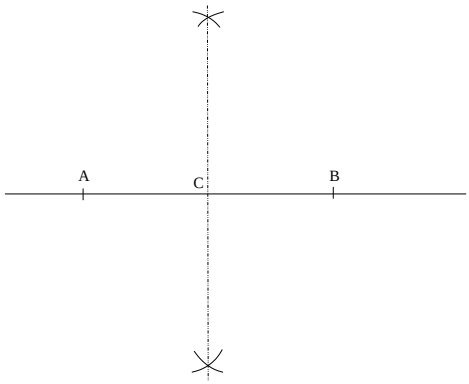
Soit $B_0 = \{O, I\}$. Dans la suite, on emploiera "constructible" au lieu de constructible à la règle et au compas à partir de B_0.

1) *M constructible $\Longrightarrow$ son symétrique M' par rapport à O l'est aussi.*
En effet,si $M = O$ alors $M' = O$.
sinon, on a $M' = (OM) \cap C(O, \|OM\|)$.

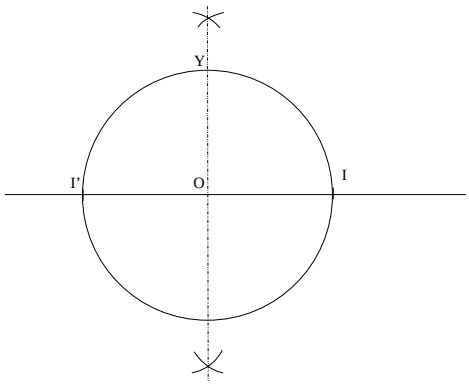


Symétrique par rapport à un point

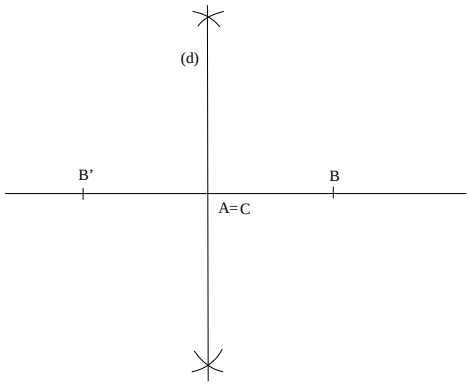
2) *A et B constructibles distincts $\Longrightarrow$ le milieu et la médiatrice du segment $[A; B]$ sont constructibles.*
En effet, comme $A \neq B$, $C(A, \|AB\|) \cap C(B, \|AB\|) = \{U, V\}$.
On a : (UV)=médiatrice de $[A; B]$
$C = (UV) \cap (AB)$=milieu de $[A; B]$.



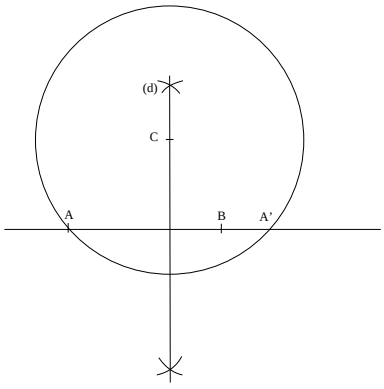
3) *$J = (O, 1)$ est constructible.*
En effet, soit I' le symétrique de I par rapport à O, constructible par 1). On peut construire (Oy) la médiatrice de $[I; I']$ par 2). On a alors $J = C(O, \|OI\|) \cap (Oy)$.



4) $A \neq B$ *constructibles et* C *constructible* $\Longrightarrow$ d=*la perpendiculaire à* (AB) *passant par* C *est constructible.*
Si $A = C$, on construit B' le symétrique de B par rapport à A par 1), puis on construit (d) la médiatrice de $[B; B']$ par 2).



Sinon, soit $A' = C(C, \|AC\|) \cap (AB)$
Si $A = A'$ alors $d = (AC)$
Sinon d=médiatrice de $[A; A']$



5) *$A \neq B$ constructibles et C constructible $\Longrightarrow$ d=la parallèle à (AB) passant par C est constructible.*
Si $C \in (AB)$, alors $d = (AB)$.
Sinon soit d' : la perpendiculaire à (AB) passant par C constructible par 4), et on peut donc construire d :la perpendiculaire à d' passant par C.

Enoncés des problèmes :

Bien avant les Eléments d'Euclide les mathématiciens grecs se sont intéressés à la règle et au compas et très tôt ils se sont heurtés à de grandes difficultés. Les problèmes que l'on n'arrivait pas à résoudre à la règle et au compas sont apparus dès le cinquième siècle avant J.C et sont devenus célèbre après les échecs de mathématiciens réputés ; comme Hippocrate de Chios qui parvint à quarrer certaines lunule en cherchant à résoudre la quadrature du cercle. Parmi ces problèmes, les plus célèbres sont :

Problème 1 : La quadrature du cercle.
La quadrature du cercle consiste à construire à la règle et au compas un carré ayant même aire qu'un cercle donné.

Problème 2 : La duplication du cube.
La duplication du cube consiste à construire à la règle et au compas l'arête d'un cube ayant un volume égal au double du volume du cube donné.

Problème 3 : La trisection de l'angle.
La trisection de l'angle consiste à construire à la règle et au compas les demi-droites partageant un angle quelconque en trois angles égaux.

Problème 4 : Le problème des polygones réguliers.
Le problème des polygones réguliers consiste à construire à la règle et au compas pour chaque n$\geq$3 un polygone régulier ayant n côtés.

Ces problèmes ont été résolus au 19$^{\text{ième}}$ siècle, grâce aux travaux de trois mathématiciens :

En 1796, **Karl Friedrich Gauss** (1777-1855) démontre la condition suffisante pour construire le polygone régulier à n côtés et montre que le polygone à 17 côtés est constructible.

En 1837, **Pierre Laurent Wantzel** (1814-1848) donne une caractérisation algébrique des points que l'on peut construire à la règle et au compas, en déduit l'impossibilité de la duplication du cube et de la trisection de l'angle, et complète la démonstration de Gauss sur

la construction des polygones réguliers.

Théorème de Gauss Wantzel : Soient $n \geq 2$, $n = 2^{\alpha_0} P_1^{\alpha_1} ... P_r^{\alpha_r}$ avec $\alpha_i \geq 0$, P_i premier impair. Alors :
Le polygone régulier à n côtés dont l'un des sommet est $(1, 0)$ est constructible à la règle et au compas (i.e. le point $(cos\frac{2\pi}{n}, sin\frac{2\pi}{n})$ est constructible à la règle et au compas.) $\Longleftrightarrow$ on a α_1,...,$\alpha_n \in \{0, 1\}$ et pour $\alpha_i = 1$ $(i \geq 1)$ on a $P_i = 1 + 2^{2^{\gamma_i}}$ (i.e. P_i est un nombre premier de Fermat).

Théorème de Wantzel : Soit $t \in I\!R$, t est constructible $\Longleftrightarrow$ il existe une suite finie (L_0,L_1,...,L_p) de sous corps de $I\!R$ vérifiant :

$$L_0 = \mathbb{Q}$$

$\forall i \in [0; p-1]$, L_{i+1} est une extension quadratique de L_i
$t \in L_p$.

En 1882, **Ferdinand Lindemann** (1852-1939) montre que π est un nombre transcendant (il n'est pas racine d'un polynôme non nul à coefficient entier) et en déduit l'impossibilité de la quadrature du cercle.

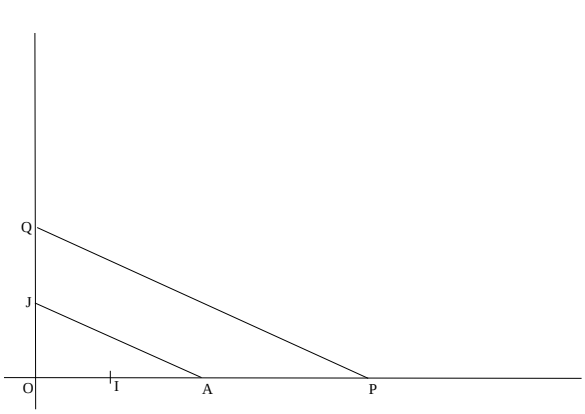
1.3 Propriétés algèbriques

Définition 1 : Soit $x \in \mathbb{R}$ on dit que x est constructible si $(x, 0)$ ou $(0, x)$ est constructible.

Remarque : Pour $x \in \mathbb{R}$, on a :$(x, 0)$ constructible $\Longleftrightarrow$ $(0, x)$ constructible.
En effet, si $x = 0$ c'est évident,
Sinon on a : $(0, x)$ constructible $\Longrightarrow (x, 0) = (OI) \cap C(O, \|Ox\|)$
$(x, 0)$ constructible $\Longrightarrow (0, x) = (OJ) \cap C(O, \|Ox\|)$

Proposition 2 : *Tout élément de $\mathbb{Q}$ est constructible.*

Preuve :
Soit $z \in \mathbb{Z}$, $(z, 0)$ est constructible, donc tout élément de $\mathbb{Z}$ est constructible.
Soient $(p, q) \in \mathbb{Z} * \times \mathbb{N}*$, $P = (p, 0)$ et $Q = (0, q)$; on a P et Q constructibles.
Soient d=la parallèle à (PQ) passant par J et $A = d \cap (OI)$.



Par Thalès dans le triangle OPQ, on a :
$\frac{|OA|}{|OP|}=\frac{|OJ|}{|OQ|}$
$\iff |OA|=\frac{|OP|}{|OQ|}$
$\iff |OA|=\frac{p}{q}$
Donc $A=(\frac{p}{q},0)$ d'où $\frac{p}{q}$ est constructible.

Proposition 3 : *$M=(x,y)$ constructible $\iff$ x et y sont constructibles.*

Preuve :
$(\Longrightarrow)$
$M=(x,y)$ constructible $\Longrightarrow$ d=parallèle à (OJ) passant par M et d'= parallèle à (OI) passant par M sont constructibles.
$\Longrightarrow (x,0)=(OI)\cap d$ et $(0,y)=(OJ)\cap d'$.
$\Longrightarrow x$ et y sont constructibles.

$(\Longleftarrow)$
x et y sont constructibles $\Longrightarrow (x,0)$ et $(0,y)$ sont constructibles par la remarque.
On a d_1=parallèle à (OJ) passant par $(x,0)$ et d_2=parallèle à (OI) passant par $(0,y)$ sont constructibles.
$\Longrightarrow (x,y)=d_1\cap d_2$.
$\Longrightarrow M=(x,y)$ est constructible.

Théorème 4 : Soit $E=\{$nombres réels constructibles$\}$, E est un sous-corps de $\mathbb{R}$ stable par racine carré ($\forall$ x $\in E\cap\mathbb{R}^+$, $\sqrt{x}\in E$).

Preuve :
$E\neq\emptyset$ car 0 et 1$\in E$.

$\forall x\in E$, $(x,0)$ constructible $\Longrightarrow$ son symétrique par rapport à O : $(-x,0)$ est constructible.
$\Longrightarrow -x\in E$.

Soit $(U,V) \in E^2$, $((0,U);(-U,0)) \cap ((V,0);(V,V)) = (V, U+V)$
$\Longrightarrow U+V \in E$.

Soit $(U,V) \in E^2$, on a $V+1 \in E$ et $V+1-U \in E$ de plus $((V+1-U;V+1);(V,V)) \cap (OI) = (UV;0)$
$\Longrightarrow UV \in E$.

$\forall x \in E \backslash \{0\}$, $((1,0);(x,-1)) \cap (0;(1,1)) = (x^{-1}, x^{-1})$
$\Longrightarrow x^{-1} \in E$.

Donc E est un sous corps de $\mathbb{R}$.

$\forall x \in E$ tels que $x > 0$, $\frac{x+1}{2} \in E$ car E est un sous corps de $\mathbb{R}$.
Soit $A = (\frac{x+1}{2}; 0)$, on a $C(A, \|OA\|) \cap ((x,0);(x,x)) = \{(x;\sqrt{x});(x;-\sqrt{x})\}$
$\Longrightarrow \sqrt{x} \in E$.

Donc E est stable par racine carré.

On verra dans le chapitre IV que E est le plus petit sous-corps de $\mathbb{R}$ stable par racine carré.

Chapitre 2

Théorème de Wantzel

2.1 Nombres réels constructibles

En 1837, P.L Wantzel, jeune répétiteur à l'école Polytechnique, donna une démonstration satisfaisante de la duplication et de la trisection qu'il fit dans un article publié au journal de mathématiques : "Recherches sur les moyens de connaître si un problème de géométrie peut se résoudre par la règle et le compas". Cet article permet aussi de mieux situer le problème de la quadrature du cercle : ce n'est pas la valeur de π qui importe mais sa nature, s'il est algébrique ou transcendant. Pour obtenir ces résultats, il dut caractériser les nombres réels constructibles de manière purement algébrique.

Théorème de Wantzel :
Soit $t \in \mathbb{R}$, t est constructible $\Longleftrightarrow$ il existe une suite finie (L_0,L_1,...,L_p) de sous corps de $\mathbb{R}$ vérifiant :
L_0=$\mathbb{Q}$
$\forall i \in [0; p-1]$, L_{i+1} **est une extension quadratique de** L_i
t$\in L_p$**.**

Remarques :
• $\forall t \in \mathbb{Q}$, t est constructible, on a $p = 0$ et L_0=$\mathbb{Q}$.
• Si $t \in \mathbb{R}\backslash\mathbb{Q}$ et t est constructible alors $p \geq 1$.
• On peut choisir p tel que $t \in L_p\backslash L_{p-1}$.

Proposition 1 : Soient F un sous-corps de $\mathbb{R}$ et $U = F \times F$ l'ensemble des coordonnées dans F.
D : ensemble des droites passant par deux points distincts de U.
C : ensemble des cercles centrés en un point de U et de rayon égal à la distance de deux points distincts de U.
On a alors les résultats suivant :

1) $d \in D \Longrightarrow d$ admet au moins une équation à coefficient dans F.
2) $\gamma \in C \Longrightarrow \gamma$ admet au moins une équation à coefficient dans F.
3) Si d et d' sont deux droites de D sécantes en M alors $M \in U$.
4) $d \in D$ et $\gamma \in C$, soit $M \in d \cap \gamma \Longrightarrow M \in U$ ou bien il existe G une extension quadratique de F tels que les coordonnées de M appartiennent à G.
5) $\gamma \in C$ et $\gamma' \in C$ et $\gamma \neq \gamma'$, soit $M \in \gamma \cap \gamma' \Longrightarrow M \in U$ ou bien il existe G une extension quadratique de F tels que les coordonnées de M appartiennent à G.

Preuve :
1) Soit $d = (AB) \in D$ où $A = (a, a') \in U$ et $B = (b, b') \in U$.
On a $M = (x, y) \in d$
$\Longleftrightarrow det|\overrightarrow{AM}\overrightarrow{AB}| = det \begin{vmatrix} (x-a) & (b-a) \\ (y-a') & (b'-a') \end{vmatrix} = 0$
$\Longleftrightarrow (b'-a')x - (b-a)y + a'b - ab' = 0$ est une équation de d à coefficients dans F.

2) $\gamma = C(A, \|BC\|)$ où $A = (a, a') \in U$, $B = (b, b') \in U$, $C = (c, c') \in U$ avec $B \neq C$.
On pose $R = \|BC\|$ et par Pythagore, on a : $R^2 = (c-b)^2 + (c'-b')^2 \in F$.
(x,y)$\in\gamma \Longleftrightarrow$ R^2=(x-a)^2+(y-a')^2
$\Longleftrightarrow x^2 + y^2 - 2ax - 2a'y + a^2 + a'^2 - R^2 = 0$ est une équation de γ à coefficients dans F.

3) Soient l'équation de d : $ux + vy + w = 0$ et l'équation de d' : $u'x + v'y + w = 0$ à coefficients dans F.
Pour $M = (x, y) \in d \cap d'$, on a :

$$\begin{cases} ux + vy = -w \\ u'x + v'y = -w' \end{cases}$$

Comme les droites sont sécantes, on a : $\Delta = \begin{vmatrix} u & v \\ u' & v' \end{vmatrix} \in F^*$.
Soient $\Delta 1 = \begin{vmatrix} -w & v \\ -w' & v' \end{vmatrix} \in F$ et $\Delta 2 = \begin{vmatrix} u & -w \\ u' & -w' \end{vmatrix} \in F$.

Par la formule de Cramer, on obtient :

$x = \frac{\Delta 1}{\Delta}$ et $y = \frac{\Delta 2}{\Delta}$ d'où $M \in U$.

4) Soient l'équation de d : $ux + vy + w = 0$ à coefficient dans F et l'équation de γ : $x^2 + y^2 - 2ax - 2by + c = 0$ à coefficient dans F, $M = (x, y) \in d \cap \gamma$ vérifie les deux équations.
On a $(u, v) \neq (0, 0)$; supposons que $v \neq 0$ (le cas est similaire pour $u \neq 0$) :
D'après l'équation de d :

$$y = -\frac{u}{v}x - \frac{w}{v}$$

en substituant dans l'autre équation, on a :

$$\left(1+(\frac{u}{v})^2\right)x^2+2\left(\frac{uw}{v^2}-a+\frac{bu}{v}\right)x+\left(c+2\frac{bw}{v}+(\frac{w}{v})^2\right)=0$$

Donc x est zéro d'un polynôme de la forme $P(X)=X^2+AX+B$ où $(A,B)\in F^2$.

Si $P(X)$ est non irréductible dans $F[X]$ alors $P(X)=(X-a_1)(X-a_2)$ où $(a_1,a_2)\in F^2$.
Comme $P(x)=0 \Longrightarrow x=a_1$ ou $x=a_2$
$\Longrightarrow$ x $\in F$ et donc

$$y=-\frac{u}{v}x-\frac{w}{v}\in F$$

$\Longrightarrow$ M$\in$ U.

Sinon $P(X)$ est le polynôme minimal de l'élément x sur le corps F.
Soit $G=F(x)$, on a $[G:F]=degP=2$.
Donc G est une extension quadratique de F.
On a évidemment $x\in G$ donc

$$y=-\frac{u}{v}x-\frac{w}{v}\in G$$

Donc $M\in G$.

5) Soient l'équation de γ : $x^2+y^2-2ax-2by+c=0$ et l'équation de γ' : $x^2+y^2-2a'x-2b'y+c'=0$.
Pour M=(x,y)$\in\gamma\cap\gamma$', on a :

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

Si $(a'-a,b'-b)=(0,0)$ alors : soit $c=c' \Longrightarrow \gamma=\gamma'$ (exclu) soit $c\neq c' \Longrightarrow \gamma\cap\gamma'=\emptyset$ (exclu).
Donc $(a'-a,b'-b)\neq(0,0)$. (*) est une équation de droite à coefficients dans F ; on applique le 4) puis on conclut.
D'où la démonstration de la proposition 1.

Preuve du théorème de Wantzel :
($\Longrightarrow$)
Soit $t\in\mathbb{R}$ constructible $\Longrightarrow M=(t,0)$ est constructible $\Longrightarrow$ il existe une suite finie $M_1,M_2,...,M_n$ de point de P tels que $\forall i\in[\![1;n]\!]$, $A_i=A_{i-1}\cup\{M_i\}$ où $A_0=\{O,I\}$, $M_n=M$ et $\forall i\in[\![1;n]\!]$, M_i est constructible en un pas à partir de A_{i-1}.
$\forall i\in[\![1;n]\!]$, on pose $M_i=(x_i,y_i)$, $K_0=\mathbb{Q}$ et $K_i=K_{i-1}(x_i,y_i)$ On a $K_i=\mathbb{Q}(x_1,y_1,...,x_i,y_i)$ donc $(K_0,...,K_n)$ est une suite de sous-corps de $\mathbb{R}$ croissante au sens de l'inclusion, et $t=x_n\in K_n$.
Comme M_i est constructible en un pas à partir de A_{i-1}, les équations des cercles et des

droites avec lesquels on construit M_i sont à coefficients dans K_{i-1}. On applique la proposition précédente :
Soit $M_i \in K_{i-1}$: $x_i \in K_{i-1}$ et $y_i \in K_{i-1}$, donc $K_{i-1} = K_i$.
Soit $\exists G$ extension quadratique de K_{i-1} telle que $M_i \in G$: $x_i \in G$ et $y_i \in G$, et donc $[G : K_{i-1}] = 2$.
$\Longrightarrow$ (K_0,...,K_n) est une suite de sous-corps de $\mathbb{R}$ croissante au sens de l'inclusion, telle que $K_0=\mathbb{Q}$, $t = x_n$, et $\forall\ i \in [\![1; n]\!]$, $[K_i: K_{i-1}\ ]=1$ ou 2.
On extrait de cette suite une suite strictement croissante (L_0,...,L_p) en ne conservant que les extensions quadratiques avec $L_0=\mathbb{Q}$ et $L_p=K_n$.
$\Longrightarrow$ (L_0,...,L_p) vérifie donc les trois conditions demandées.

($\Longleftarrow$)
Soit E le corps des nombres réels constructibles. On veut montrer par récurrence que $\forall i \in [\![1; p]\!] L_i \subseteq E$.
$L_0=\mathbb{Q} \Longrightarrow L_0 \subseteq E$ car $\mathbb{Q}$ est constructible.
On suppose que $L_i \subseteq E$. Soit $x \in L_{i+1} \backslash L_i$. Comme $[L_{i+1} : L_i] = 2$ donc $(1, x)$ est une base de L_{i+1} sur L_i.
$\Longrightarrow (1, x, x^2)$ est liée dans L_i .
$\Longrightarrow \exists\ (a, b, c) \in {L_i}^3$ avec $(a, b, c) \neq (0, 0, 0)$ tels que $ax^2 + bx + c = 0$.
si $a = 0$ alors $x = -c/b \in L_i$ donc $x \in E$.
sinon on résout l'équation du second degré, et on obtient :

$$x \in \left\{ \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \right\}$$

or E est un sous-corps stable par racine carrée, donc $x \in E$.
Donc $L_{i+1} \subseteq E$.
Donc $L_p \subseteq E \Longrightarrow t$ est constructible.

Conséquence du théorème de Wantzel :

Corollaire 2 : Soit $x \in \mathbb{R}$, x est constructible $\Longrightarrow \exists\ e \in \mathbb{N}$ tels que $[\mathbb{Q}(x) : \mathbb{Q}] = 2^e$.

Preuve :
x est constructible $\Longrightarrow \exists$ une suite finie (L_0,L_1,...,L_p) de sous corps de $\mathbb{R}$ vérifiant :
$L_0=\mathbb{Q}$, $\forall i \in [\![0; p-1]\!]$, $[L_{i+1}: L_i]=2$ et $x \in L_p$ par le théorème de Wantzel.
Or

$$[L_p : \mathbb{Q}] = \prod_{i=1}^{p} [L_i : L_{i-1}] = 2^p$$

et $[L_p : \mathbb{Q}] = [L_p : \mathbb{Q}(x)]\ [\mathbb{Q}(x) : \mathbb{Q}]$ (car $\mathbb{Q} \subseteq \mathbb{Q}(x)$ et $(x \subseteq L_p \Longrightarrow \mathbb{Q}(x) \subseteq L_p)$)
comme $[\mathbb{Q}(x) : \mathbb{Q}]$ divise $[L_p : \mathbb{Q}] \Longrightarrow \exists\ e \in \mathbb{N}$ tels que $[\mathbb{Q}(x) : \mathbb{Q}] = 2^e$.

Corollaire 3 : Tout nombre constructible est algébrique.

Preuve :
Soit x constructible, par le corollaire 2, $\exists\ e \in \mathbb{N}$ tels que $[\mathbb{Q}(x) : \mathbb{Q}] = 2^e < +\infty$.
Donc x est algébrique sur $\mathbb{Q}$.

Remarque : on donnera un contre-exemple pour montrer que la réciproque est fausse dans la démonstration de la proposition 2 du paragraphe 2.2.

2.2 Application des résultats aux problèmes grecs classiques

a) La quadrature du cercle

On veut construire à la règle et au compas un carré ayant même aire qu'un cercle donné, c'est à dire un carré ayant un côté de longueur $R\sqrt{\pi}$ si R désigne le rayon du cercle.

Lemme 1 : *Soit $a \in \mathbb{R}^+$, a transcendant $\Longleftrightarrow$ $\sqrt{a}$ transcendant.*

Preuve :
On va montrer la contraposé : a algébrique $\Longleftrightarrow$ $\sqrt{a}$ algébrique.
($\Longrightarrow$)
On a a algébrique, soit P le polynôme minimal de a sur $\mathbb{Q}$: $P(a) = 0$.
soit $Q(x) = P(x^2)$ alors $Q(x) \in \mathbb{Q}[x] \backslash 0$ (car P est non nul). On a $Q(\sqrt{a}) = 0$ donc $\sqrt{a}$ est algébrique.

($\Longleftarrow$)
On a $\sqrt{a}$ algébrique, $\mathbb{Q}(\sqrt{a}) = \{b + c\sqrt{a} / (b, c) \in \mathbb{Q}^2\}$
$\{1, \sqrt{a}\}$ est une base de $\mathbb{Q}(\sqrt{a})$ sur $\mathbb{Q}$.
Donc $[\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 2 < +\infty$.
On a : $a \in \mathbb{Q}(\sqrt{a}) \Longrightarrow \mathbb{Q}(a) \subseteq \mathbb{Q}(\sqrt{a})$
$\Longrightarrow [\mathbb{Q}(a) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt{a}) : \mathbb{Q}]$
$\Longrightarrow [\mathbb{Q}(a) : \mathbb{Q}] < +\infty$ donc a est algébrique.

On admet le théorème de Lindemann : π est transcendant.

Par le lemme, on en déduit que $\sqrt{\pi}$ est transcendant. Or si est $\sqrt{\pi}$ non algébrique alors $\sqrt{\pi}$ n'est pas constructible. Si R est le rayon d'un disque, on ne peut pas construire $R\sqrt{\pi}$: la longueur d'un côté du carré voulu.

La quadrature du cercle est donc impossible.

b) La duplication du cube

On veut construire à la règle et au compas l'arête d'un cube ayant un volume double de celui du cube donné. Si a est la longueur de l'arête du cube de départ, la longueur de l'arête du cube cherché est $a\sqrt[3]{2}$.

Proposition 2 : *$\sqrt[3]{2}$ n'est pas constructible.*

Preuve :
Soit P(X) = X^3- 2, on a P(X)$\in \mathbb{Q}$[X].
On a P($\sqrt[3]{2}$)=0, c(P)=1, 2 divise 2, 2 ne divise pas 1 et 2^2 ne divise pas 2 donc par le critère d'Eisenstein, on en déduit que P est irréductible.
Donc P(X) est le polynôme minimal de $\sqrt[3]{2}$ sur le corps $\mathbb{Q}$.
[$\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$]=deg P=3 n'est pas une puissance de 2.
Donc $\sqrt[3]{2}$ n'est pas constructible.

Remarque : *$\sqrt[3]{2}$ est un nombre algébrique non constructible.*

La duplication du cube est donc impossible.

c) La trisection de l'angle

On veut construire à la règle et au compas les demi-droites qui partagent un angle donné en trois angles égaux.

Proposition 3 : *A_θ= (cos(θ) ; sin(θ)) est constructible $\Longleftrightarrow$ cos(θ) est constructible.*

Preuve :
($\Longrightarrow$)
par la proposition 3 du chapitre 1 paragraphe 3.
($\Longleftarrow$)
cos(θ) est constructible $\Longrightarrow$ (cos(θ),0) est constructible.
Soit d la parallèle à (OJ) passant par (cos(θ),0), on a alors $A_\theta = d \cap C(O, \|OI\|)$.
D'où A_θ est constructible.

Définition 4 : Soit $\theta \in \mathbb{R}$
- $M \in P$, M est θ-constructible $\Longleftrightarrow$ M est constructible à partir de $B_0 = \{O, I, A_\theta\}$.
- $a \in \mathbb{R}$, a est θ-constructible $\Longleftrightarrow$ a est l'une des coordonnées d'un point θ-constructible.
- θ est trisectable $\Longleftrightarrow$ $A_{\frac{\theta}{3}}$ est θ-constructible.

$\Longleftrightarrow$ cos($\frac{\theta}{3}$) est θ-constructible.

Proposition 5 : *Soit E_θ=\{ nombres réels θ-constructible\} alors E_θ est un sous corps de $\mathbb{R}$ stable par racine carré, et $\mathbb{Q}(\cos(\theta)) \subseteq E_\theta$.*

Preuve : $\mathbb{Q} \subseteq E_\theta$ et $\cos(\theta) \subseteq E_\theta$ donc $\mathbb{Q}(\cos(\theta)) \subseteq E_\theta$.
La démonstration est identique à celle du II 4 du chapitre 1.

Remarque : La proposition 1, le théorème de Wantzel et le corollaire 2 restent valable si on remplace constructible par θ-constructible, E par E_θ et $\mathbb{Q}$ par $\mathbb{Q}(\cos(\theta))$.

Proposition 6 : *Si cos(θ) est constructible alors : constructible $\iff$ θ-constructible.*

Preuve :
($\Longrightarrow$)
On a $\{O, I\} \subseteq \{O, I, A_\theta\}$ donc constructible $\Longrightarrow$ θ-constructible.
($\Longleftarrow$)
Si de plus $\cos(\theta)$ est constructible alors A_θ=($\cos(\theta)$;$\sin(\theta)$) est constructible à partir de $\{O, I\}$.
Donc θ-constructible $\Longrightarrow$ constructible.

On en déduit que :
si cos(θ) est constructible alors : θ est trisectable $\iff$ cos (θ/3) est constructible.

Remarque :
Soit $\theta \in \mathbb{R}$, par les formules trigonométriques on a :
cos (3ϕ)=4 $\cos^3(\phi)$-3$\cos(\phi)$
Donc pour $P(X) = 4X^3 - 3X - \cos(\theta)$ on a $P(\cos(\theta/3))$=0
et pour $P_\theta(X) = X^3 - 3X - 2\cos(\theta)$ on a $P_\theta(2\cos(\theta/3))$=0.

Exemples :

1) π est trisectable :
On a $\cos(\pi)$=-1 est constructible et de plus cos $(\pi/3)$=1/2 constructible donc π est trisectable.

2) $\pi/2$ est trisectable :
On a cos $(\pi/2)$=0 constructible , montrons que cos $(\pi/6)$ est constructible.
On construit J, soit J' le milieu de $[O, J]$, soit D la parallèle à (OI) passant par J'. On construit $A_{\pi/6} = D \cap C(O, \|OI\|) = (\frac{\sqrt{3}}{2}, \frac{1}{2})$
$\Longrightarrow$ cos $(\pi/6) = \frac{\sqrt{3}}{2}$ est constructible.
$\Longrightarrow$ $\pi/2$ est trisectable.

Théorème 7 : $\frac{\pi}{3}$ n'est pas trisectable.

Preuve :
On a cos($\frac{\pi}{3}$)=1/2 qui est constructible et $P_{\frac{\pi}{3}}(X) = X^3-3X-1 \in \mathbb{Q}[X]$.
Soit $(p,q) \in \mathbb{Z}^* \times \mathbb{N}^*$ tels que pgcd(p,q)=1.
Si $P_{\frac{\pi}{3}}(\frac{p}{q})$=0 alors p|(-1) et q|1. On en déduit que $\frac{p}{q} \in \{-1;1\}$.
Comme $P_{\frac{\pi}{3}}(-1)\neq 0$ et $P_{\frac{\pi}{3}}(1)\neq 0 \Longrightarrow P_{\frac{\pi}{3}}$ est irréductible dans $\mathbb{Q}$.
Donc d'après la remarque, $P_{\frac{\pi}{3}}(X)$ est le polynôme minimal de 2cos($\frac{\pi}{9}$) sur $\mathbb{Q}$.
Or $[\mathbb{Q}(2\cos(\frac{\pi}{9})) : \mathbb{Q}]$=deg $P_{\frac{\pi}{3}}(X)$=3 et comme $\mathbb{Q}(2\cos(\frac{\pi}{9}))=\mathbb{Q}(\cos(\frac{\pi}{9}))$, on a $[\mathbb{Q}(\cos(\frac{\pi}{9})) : \mathbb{Q}]$=3 n'est pas une puissance de 2, d'où cos($\frac{\pi}{9}$) n'est pas constructible et donc $\frac{\pi}{3}$ n'est pas trisectable.

Proposition 8 : *Soit $\theta \in \mathbb{R}$, θ est trisectable $\Longleftrightarrow$ $P_\theta(X)=X^3-3X-2cos(\theta)$ a une racine dans $\mathbb{Q}(cos(\theta))$.*

Preuve :
Notons x=cos($\frac{\theta}{3}$), $\mathbb{Q}_\theta=\mathbb{Q}(\cos(\theta))$, et $K=\mathbb{Q}(\cos(\theta))(\cos(\frac{\theta}{3}))=\mathbb{Q}(\cos(\theta))(2\cos(\frac{\theta}{3}))=\mathbb{Q}_\theta(2x)$
Or θ est trisectable $\Longleftrightarrow$ x=cos($\frac{\theta}{3}$) est θ-constructible.
$\Longleftrightarrow \exists$ une suite finie (L_0,L_1,...,L_n) de sous corps de $\mathbb{R}$ vérifiant :
$L_0=\mathbb{Q}_\theta$, $\forall\, i \in [0;p-1]$, $[L_{i+1} : L_i]$=2 et $x \in L_p$ par le théorème de Wantzel dans $\mathbb{Q}(\cos(\theta))$.
$\Longrightarrow \exists$ e$\in\mathbb{N}$ tels que $[K : \mathbb{Q}_\theta]=2^e$. De plus $P_\theta(2x)=P_\theta(2\cos(\frac{\theta}{3}))=0$.

($\Longrightarrow$)
Par la contraposée :
Si $P_\theta(X)$ n'a pas de zéro dans $\mathbb{Q}_\theta$, alors il est irréductible sur $\mathbb{Q}_\theta$.
$\Longrightarrow$ [K :$\mathbb{Q}_\theta$]=deg(P_θ)=3 n'est pas une puissance de deux, donc θ n'est pas trisectable.

($\Longleftarrow$)
Si $P_\theta(X)$ a un zéro dans $\mathbb{Q}_\theta$, alors il est réductible sur $\mathbb{Q}_\theta$.
Soit $M(X)$ le polynôme minimal de $2x$ sur $\mathbb{Q}_\theta$, qui est un diviseur irréductible de $P_\theta(X)$ dans $\mathbb{Q}_\theta[X]$.
On a deg M =1 ou 2.
Or [K :$\mathbb{Q}_\theta$]=deg M,
Si deg $M=1$ alors $x \in \mathbb{Q}_\theta$, donc x est θ-constructible.
Si deg $M=2$ alors K est une extension quadratique de $\mathbb{Q}_\theta$, donc x=cos($\frac{\theta}{3}$) est θ-constructible par Wantzel.
Dans les deux cas θ est trisectable.

Exemple : $\frac{\pi}{4}$ est trisectable.
Pour $P_{\frac{\pi}{4}}(X) = X^3-3X-\sqrt{2}= (X+\sqrt{2})(X^2-\sqrt{2}X-1)$

On a $P_{\frac{\pi}{4}}(-\sqrt{2}) = 0$ et $-\sqrt{2} \in \mathbb{Q}(\frac{\sqrt{2}}{2})$=$\mathbb{Q}(\cos(\frac{\pi}{4}))$.

d) Le polygone régulier

Théorème de Gauss Wantzel : Soient $n \geq 2$, $n = 2^{\alpha_0} P_1^{\alpha_1} ... P_r^{\alpha_r}$ avec $\alpha_i \geq 0$, P_i premier impair. Alors les propriétés suivantes sont équivalentes :
i) Le polygone régulier à n côtés dont l'un des sommet est $(1, 0)$ est constructible à la règle et au compas (i.e. le point ($\cos\frac{2\pi}{n}$,$\sin\frac{2\pi}{n}$) est constructible à la règle et au compas.)
ii) on a α_1,...,$\alpha_n \in \{0, 1\}$ et pour α_i=1 ($i \geq 1$) on a $P_i = 1 + 2^{2^{\gamma_i}}$ (i.e. P_i est un nombre premier de Fermat).

Preuve :
i)$\Longrightarrow$ii)
($\cos\frac{2\pi}{n}$,$\sin\frac{2\pi}{n}$) est constructible à la règle et au compas
$\Longrightarrow$(par le corollaire 2) $\exists\ \alpha \in \mathbb{N}$ tels que $[\mathbb{Q}(\cos\frac{2\pi}{n}) : \mathbb{Q}]$=$2^\alpha$
Soit ξ=$\cos\frac{2\pi}{n} + i.\sin\frac{2\pi}{n}$, on a ξ^{-1}=$\cos\frac{2\pi}{n} - i.\sin\frac{2\pi}{n} \in \mathbb{Q}(\xi)$ car $\mathbb{Q}(\xi)$ est un corps. Donc $\xi + \xi^{-1}$=$2\cos(\frac{2\pi}{n}) \in \mathbb{Q}(\xi)$
$\Longrightarrow \mathbb{Q}(\cos\frac{2\pi}{n}) \subseteq \mathbb{Q}(\xi)$

On a $P(\xi)$=$\xi^2 - 2\xi\cos\frac{2\pi}{n} + 1 = 0$
En effet, $\xi^2 - 2\xi\cos\frac{2\pi}{n} + 1 = \xi(\xi - 2cos\frac{2\pi}{n} + \xi^{-1})$=$\xi(2\cos\frac{2\pi}{n} - 2\cos\frac{2\pi}{n})$=0.
$\Longrightarrow [\mathbb{Q}(\xi) : \mathbb{Q}(\cos\frac{2\pi}{n})] \leq 2$

Or $\mathbb{Q}(\xi) \not\subset \mathbb{R}$ et $\mathbb{Q}(\cos\frac{2\pi}{n}) \subset \mathbb{R} \Longrightarrow [\mathbb{Q}(\xi) : \mathbb{Q}(\cos\frac{2\pi}{n})] \neq 1$.
D'où $[\mathbb{Q}(\xi) : \mathbb{Q}(\cos\frac{2\pi}{n})]$=2.

$\Longrightarrow [\mathbb{Q}(\xi) : \mathbb{Q}]$= $[\mathbb{Q}(\xi) : \mathbb{Q}(\cos\frac{2\pi}{n})].[\mathbb{Q}(\cos\frac{2\pi}{n}) : \mathbb{Q}]$=$2.2^\alpha$=$2^{\alpha+1}$
Or ξ est une racine primitive (racine de X^n-1) donc $[\mathbb{Q}(\xi) : \mathbb{Q}]$=$\varphi(n)$ (indicateur d'Euler)

On pose n=$2^{\alpha_0} P_1^{\alpha_1} ... P_r^{\alpha_r}$ sa décomposition en nombres premiers avec $\alpha_i \geq 1$, $r \geq 1$ et P_i premier impairs.
On a :
$\varphi(P_1^{\alpha_1} ... P_r^{\alpha_r}) = 2^{\alpha'}$
$= P_1^{\alpha_1} ... P_r^{\alpha_r}(1 - \frac{1}{P_1}) ... (1 - \frac{1}{P_r})$
$= P_1^{\alpha_1 - 1} ... P_r^{\alpha_r - 1}(P_1 - 1) ... (P_r - 1)$

Or $(2,P_i)$=1 $\forall\ i \in [\![0; r]\!] \Longrightarrow P_1^{\alpha_1 - 1} ... P_r^{\alpha_r - 1}$=1
$\Longrightarrow \forall\ i \in [\![0; r]\!]\ \alpha_i$=1
D'où

$$\prod_{i=1}^{r} (P_i - 1) = 2^\alpha$$

$\Longrightarrow$ (P_i-1)=2^{β_i} car 2 est premier.
On peut écrire β_i comme : β_i=$2^{\gamma_i}\lambda_i$ avec $2\nmid\lambda_i$
$\Longrightarrow$ (P_i-1)=2^{β_i} =$2^{2^{\gamma_i}\lambda_i}$
$\Longrightarrow$ P_i=1+$2^{2^{\gamma_i}\lambda_i}$
Or 1+X^q=$(1+X)P(X)$ où $P(X)\in\mathbb{Z}[X]$
$\Longrightarrow$ $P_i=(1+2^{2^{\gamma_i}}).P(2^{2^{\gamma_i}})$
Or P_i est premier $\Longrightarrow$ $P(2^{2^{\gamma_i}})$=1
$\Longrightarrow$ $P_i=(1+2^{2^{\gamma_i}})$ et comme P_i=1+$2^{2^{\gamma_i}\lambda_i}$, on a λ_i=1
Donc P_i est un nombre premier de Fermat.

ii)$\Longrightarrow$i)
Par les bissectrices on peut construire le point (cos$\frac{2\pi}{2^{\alpha_0}}$,sin$\frac{2\pi}{2^{\alpha_0}}$)
Montrons que (cos$\frac{2\pi}{P_i}$, sin$\frac{2\pi}{P_i}$) est constructible :
Soient ξ=cos$\frac{2\pi}{P_i}+i.$sin$\frac{2\pi}{P_i}$ et $G=gal(\mathbb{Q}(\xi)/\mathbb{Q})$.
$G\cong\left(\frac{\mathbb{Z}}{P_i\mathbb{Z}}\right)^\times$ car $\sigma(\xi)=\xi^m$ avec $\sigma\in G$ et (m,P_i)=1
Or $\left(\frac{\mathbb{Z}}{P_i\mathbb{Z}}\right)^\times$ est un groupe cyclique d'ordre (P_i-1)=$2^{2^{\gamma_i}}$
Par la classification des groupes cycliques : $\forall\ 0\leq t\leq 2^{2^{\gamma_i}}\ \exists!\ G_t$ sous-groupe de G d'ordre 2^t.

Soit L^{G_t}=$\{x\in\mathbb{Q}(\xi)/\sigma(x)=x\ \forall x\in G_t\}$
Par la théorie de Galois, on a : [$\mathbb{Q}(\xi)$:L^{G_t}]=O(G$_t$)=2^t
On a L$_1$=$\mathbb{Q}(\xi+\xi^{-1})$=$\mathbb{Q}$(cos$\frac{2\pi}{P_i}$).
On a :$L_1\supset L_2\supset ...\supset L_s$=$\mathbb{Q}$ et comme [$\mathbb{Q}$(cos$\frac{2\pi}{P_i}$,sin$\frac{2\pi}{P_i}$) :$\mathbb{Q}$ (cos$\frac{2\pi}{P_i}$)]=1 ou 2, alors [$\mathbb{Q}$(cos$\frac{2\pi}{P_i}$,sin$\frac{2\pi}{P_i}$) :$\mathbb{Q}$]=[$\mathbb{Q}$(cos
(cos$\frac{2\pi}{P_i}$)].[$\mathbb{Q}$ (cos$\frac{2\pi}{P_i}$) :$\mathbb{Q}$]=$2^{t'}$ avec $t'=t$ ou $t+1$
Par le théorème de Wantzel, (cos$\frac{2\pi}{P_i}$, sin$\frac{2\pi}{P_i}$) est constructible.

Par Bezout, $\exists\ \lambda_0,\lambda_1,...,\lambda_r\in\mathbb{Z}$ avec 1=$\lambda_0\frac{n}{2^{\alpha_0}}$+...+$\lambda_r\frac{n}{P_r^{\alpha_r}}$
Comme (cos$\frac{2\pi}{2^{\alpha_0}}$,sin$\frac{2\pi}{2^{\alpha_0}}$) et (cos$\frac{2\pi}{P_i}$, sin$\frac{2\pi}{P_i}$) sont constructibles, alors (cos($\frac{2\pi}{n}$), sin($\frac{2\pi}{n}$)) est constructible.

Chapitre 3

Caractérisation des nombres réels constructibles

Dans le chapitre I, on a noté E l'ensemble des nombres réels constructibles.

3.1 Théorème de Wantzel dans $\mathbb{C}$

Définition 1 : *Soit $E(i)$ l'ensemble des nombres complexes constructibles. $E(i)$ est le plus petit sous-corps de $\mathbb{C}$ contenant E et i donc on a :*
$E(i) = \{a + ib; (a, b) \in E^2\}$.

Lemme 2 : *$E(i)$ est un sous-corps de $\mathbb{C}$ stable par racine carré.*

Preuve :
Soit $\alpha \in E(i)$, on a $\alpha = a + ib$ avec $(a, b) \in E^2$.
On veut montrer que si $\alpha = (u + iv)^2$ alors $(u, v) \in E^2$.
On a : $\alpha = (u + iv)^2 \iff \begin{cases} a = u^2 - v^2 \\ b = 2uv \end{cases}$
$\iff \begin{cases} v = \frac{b}{2u} \\ a = u^2 - \frac{b^2}{4u^2} \end{cases}$
$\iff \begin{cases} v = \frac{b}{2u} \\ u^4 - au^2 - \frac{b^2}{4} = 0 (*) \end{cases}$
Soit $P(X) = X^2 - aX - \frac{b^2}{4}$, alors on a : $P(u^2) = 0$.

Or $u = \frac{b}{2v}$, en le substituant dans (*) on a :
$\frac{b^4}{2^4 v^4} - a\frac{b^2}{4v^2} - \frac{b^2}{4} = 0 \iff \frac{b^2}{4v^4} - av^2 - 1 = 0$
$\iff v^4 + av^2 - \frac{b^2}{4} = 0.$
On a aussi $P(-v^2) = 0$.

Or $P(X) = X^2 - aX - \frac{b^2}{4} = 0$
$\Longrightarrow \Delta = a^2$+b^2 et $\{u^2; -v^2\} \in \{\frac{a \pm \sqrt{a^2+b^2}}{2}\}$
$\Longrightarrow$ u=$\pm\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}}$ et v=$\pm\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}$
$\Longrightarrow u \in E$ et $v \in E$ car E est stable par racine carré.
Donc pour $\alpha \in E(i)$, on a $\sqrt{\alpha} \in E(i)$.
D'où $E(i)$ est stable par racine carré.

Théorème 3 (Wantzel dans $\mathbb{C}$) : Soit $z \in \mathbb{C}$, $z \in E(i) \Longleftrightarrow$ il existe une suite finie (L_0,L_1,...,L_q) de sous corps de $\mathbb{C}$ vérifiant :
L_0=$\mathbb{Q}$
$\forall$**i**$\in [0; q-1]$,L_{i+1} **est une extension quadratique de** L_i
$z \in L_q$**.**

Preuve :
($\Longrightarrow$)
Soit $z \in$ E(i), on peut construire $M = (Re(z),\ Im(z))$.
Par le théorème de Wantzel dans $\mathbb{R}$, on construit (L_0,L_1,...,L_p) de sous corps de $\mathbb{R}$ vérifiant :
L_0=$\mathbb{Q}$
$\forall i \in [0; p-1]$, L_{i+1} est une extension quadratique de L_i
$Re(z) \in L_p$ et $Im(z) \in L_p$.
On a donc $z \in L_p(i)$ où $L_p(i) = \{a + ib; (a, b) \in L_p^2\}$
Soit $\Pi_i(X, L_p) = X^2 + 1$,
$\Pi_i(X, L_p)$ est irréductible dans L_p car si $\frac{p}{q}$ est racine alors $\frac{p}{q} \in \{-1; 1\}$ mais $\Pi_i(-1, L_p) \neq 0$ et $\Pi_i(1, L_p) \neq 0$.
Donc $[L_p(i)\ :\ L_p] = deg\Pi_i(X, L_p) = 2$.
Si on pose $q = p+1$ et $L_q = L_p(i)$, on a la tour d'extension quadratique complexe cherchée.

($\Longleftarrow$)
Démontrons par récurrence sur n, $W(n)$: Si (K_0,K_1,...,K_n) T.E.Q complexe de $\mathbb{Q}$ alors K$_n$ $\subseteq E(i)$.

Pour $n = 0$, on a K_0=$\mathbb{Q}$ donc $K_0 \subseteq E(i)$, d'où $W(0)$ est vérifiée.
On suppose $K_j \subseteq E(i)$, et soit $x \in K_{j+1} \backslash K_j$.
On a $[K_{j+1} : K_j]$=2 donc $(1, x, x^2)$ est liée dans K_j
$\Longrightarrow \exists (a, b, c) \in K_j^3$ et $(a, b, c) \neq 0$ tels que $ax^2 + bx + c = 0$.

Si $a = 0$: $x = -\frac{b}{c} \in K_j$.
Sinon :
si $b^2 - 4ac > 0$, $x \in \{\frac{-b \pm \sqrt{b^2-4ac}}{2a}\} \in E(i)$ car $E(i)$ est stable par racine carrée.
sinon $x \in \{\frac{-b \pm i\sqrt{b^2-4ac}}{2a}\} \in E(i)$.
Donc $x \in E(i) \Longrightarrow K_{j+1} \subseteq E(i)$: $W(j+1)$ est bien vérifiée.
D'où $K_n \subseteq E(i)$ et donc z est constructible.

Corollaire 4 : *Si $\alpha \in E(i)$ alors $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ est une puissance de 2.*

Preuve :
La démonstration est identique a celle du corollaire 2 du chapitre II.

3.2 Théorème de caractérisation

Théorème 1 : *Soit $x \in \mathbb{R}$ algébrique sur $\mathbb{Q}$. Soit $\Pi(X)$ son polynôme minimal, $D_{\mathbb{Q}}(\Pi)$ le corps des racines de $\Pi(X)$. Alors :*
x est constructible $\Longleftrightarrow$ $[D_{\mathbb{Q}}(\Pi) : \mathbb{Q}]$ est une puissance de 2.

Preuve :
($\Longrightarrow$)
Soit x constructible, par le théorème de Wantzel il existe une suite finie (L_0,L_1,...,L_p) de sous corps de $\mathbb{R}$ vérifiant :
L_0=$\mathbb{Q}$
$\forall$i$\in [0; p-1]$, L_{i+1} est une extension quadratique de L_i
$x \in L_p$.
Soit N la clôture normale de $L_p/\mathbb{Q}$: N est un élément minimale de l'ensemble des extensions de L_p qui sont normale sur $\mathbb{Q}$, ($L_p \subseteq N$).
$\Pi(X)$ est irréductible sur $\mathbb{Q}$ et possède une racine dans N : x. Donc il possède toutes ses racines dans N, d'où Π est scindé sur N.
On a $\mathbb{Q} \subseteq N$ et les racines de Π sont dans N, donc $D_{\mathbb{Q}}(\Pi) \subseteq N$.
Soit $\sigma : L_p \longrightarrow \mathbb{C}$ un $\mathbb{Q}$-homomorphisme.
σ est injectif donc $\sigma(L_{i+1}) \subseteq \sigma(L_i)$.
On a $(\sigma(L_0), ..., \sigma(L_p))$ est une tour d'extension vérifiant :
$\sigma(L_0)$=$\mathbb{Q}$ et $\forall$i$\in [0; p-1]$, $[\sigma(L_{i+1}) : \sigma(L_i)]$=2 car $\{1, x\}$ est une base de L_{i+1} sur L_i donc $\{1, \sigma(x)\}$ est une base de $\sigma(L_{i+1})$ sur $\sigma(L_i)$.
Donc d'après le théorème de Wantzel dans $\mathbb{C}$, on a : $\sigma(L_p) \subseteq$E(i).

Soit $H = \{ \sigma : L_p \longrightarrow \mathbb{C} / \ \sigma$ soit un $\mathbb{Q}$-homomorphisme $\}$, H est fini par Hermit.
On a : $N = \mathbb{Q}(\bigcup_{\sigma \in H} \sigma(L_p)) \Longrightarrow$ N$\subseteq$E(i).
$\Longrightarrow [N : \mathbb{Q}] < +\infty$.

On a caract($\mathbb{Q}$)=0 donc tous les polynômes irreductibles de $\mathbb{Q}[X]$ sont séparables, et comme leurs racines sont dans N, $N/\mathbb{Q}$ est une extension séparable.

Comme $[N : \mathbb{Q}] < +\infty$, d'après le théorème de l'élément primitif :
$\exists \alpha \in N$ tels que $N = \mathbb{Q}(\alpha)$

Or $\alpha \in E(i) : \exists\ p \in \mathbb{N}$ tels que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^p$
Donc $[N : \mathbb{Q}]=2^p$
Or $\mathbb{Q} \subseteq D_{\mathbb{Q}}(\Pi) \subseteq N$
Donc $[N : \mathbb{Q}]=[N : D_{\mathbb{Q}}(\Pi)].[D_{\mathbb{Q}}(\Pi) : \mathbb{Q}]=2^p$
$\Longrightarrow [D_{\mathbb{Q}}(\Pi) : \mathbb{Q}]$ divise $[N : \mathbb{Q}]$
$\Longrightarrow \exists\ e \in \mathbb{N}$ tels que $[D_{\mathbb{Q}}(\Pi) : \mathbb{Q}]=2^e$.

($\Longleftarrow$)
Supposons qu'il existe e $\in \mathbb{N}$ tels que $[D_{\mathbb{Q}}(\Pi) : \mathbb{Q}]=2^e$.
caract$(\mathbb{Q})=0 \Longrightarrow D_{\mathbb{Q}}(\Pi)$ est une extension galoisienne de $\mathbb{Q}$.
Soit $G = Gal(D_{\mathbb{Q}}(\Pi)/\mathbb{Q})$, on a alors $O(G)=[D_{\mathbb{Q}}(\Pi) : \mathbb{Q}]=2^e$.

G possède une suite de sous-groupe décroissante : $G = G_0 \supseteq G_1 \supseteq ... \supseteq G_{e-1}=\{id\}$ tels que $\forall i \in [0; e]$, $O(G_i) = 2^{e-i}$.
Par la correspondance de Galois, on obtient : $\mathbb{Q} = L_0 \subseteq L_1 \subseteq ... \subseteq L_e = D_{\mathbb{Q}}(\Pi)$ avec $\forall i \in [0; e-1]$ $[Li + 1 : L_i]=2$.
Par le théorème de Wantzel, $D_{\mathbb{Q}}(\Pi) \subseteq E(i)$ donc $x \in E(i)$ et comme $x \in \mathbb{R}$, on a donc $x \in E$.

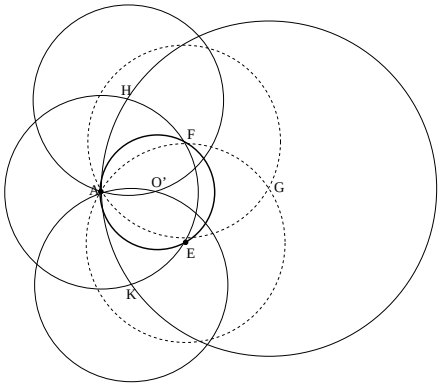
Chapitre 4

Construction au compas seul ou à la règle seule

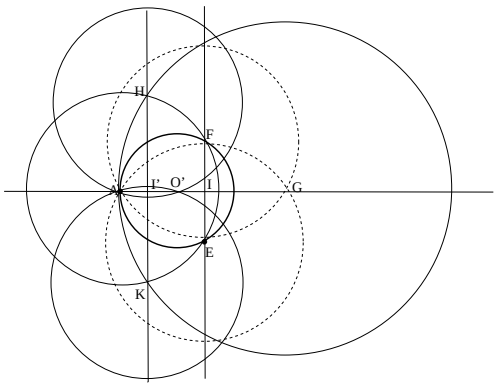
4.1 Le compas seul

Le problème de Napoléon : comment retrouver le centre d'un cercle à l'aide d'un compas uniquement ?

Construction du centre du cercle :
Soit C le cercle donné.
Soit A et E deux points non diamétralement opposés de C.
Soient Γ le cercle de centre A passant par E et $F{=}\Gamma{\cap}C$.
Soit G l'intersection des cercles de centre E et F passant par A.
Soient C' le cercle de centre G passant par A et $\{H;K\}{=}\Gamma{\cap}C'$.
Soit O' l'intersection des cercles de centre H et K passant par A.



Montrons que O' est le centre du cercle :



Soit D la droite (OA). Soient $I = (EF) \cap D$ et $I' = (HK) \cap D$
On a I milieu de $[GA]$. En effet, par construction de G : $\|GE\|=\|GF\|=\|EA\|$ de plus $\|AF\|=\|AE\|$, donc $AEGF$ est un losange, ses diagonales $[FE]$ et $[GA]$ sont perpendiculaires et se coupent en leur milieu. Donc I est le milieu de $[AG]$.
On a I' milieu de $[O'A]$. En effet, par construction de O' : $\|HO'\|=\|HA\|$ et $\|KO'\|=\|KA\|$ de plus $\|AH\|=\|AK\|$, donc $AHO'K$ est un losange, ses diagonales $[HK]$ et $[O'A]$ sont perpendiculaires et se coupent en leur milieu. Donc I' est le milieu de $[O'A]$.
Soit O le centre du cercle, comme I' est le milieu de $[O'A]$ alors : Si on montre que I' est le milieu de $[OA]$ alors $O = O'$.

Soient R, R' et r les rayons de C, C', Γ. On sait que $(IE) \perp (OA)$ donc OIE et IAE sont deux triangles rectangles. On a $\|OE\|=R$ et $\|AE\|=r$.
Par Pythagore, $r^2=IA^2+IE^2$ et $R^2=OI^2+IE^2$
$\Longrightarrow r^2=IA^2+R^2-OI^2$
$\Longrightarrow IA^2-OI^2= r^2-R^2$.

Or $IA^2-OI^2=(\overline{IA}-\overline{IO})(\overline{IA}+\overline{IO})$
On a $(\overline{IA}-\overline{IO})=\overline{OA}=R$ et $\overline{IO}=\overline{AO}+\overline{IA}$

Donc $IA^2 - OI^2 = R\ (\overline{AO} + 2\overline{IA}) = r^2 - R^2$.
$\Longrightarrow -\overline{OA} + 2\overline{IA} = \frac{r^2-R^2}{R}$
$\Longrightarrow \overline{IA} = \frac{1}{2}(\frac{r^2-R^2}{R} + R)$
D'où $\overline{IA} = \frac{r^2}{2R}$

De la même façon on obtient : $\overline{I'A} = \frac{r^2}{2R'}$

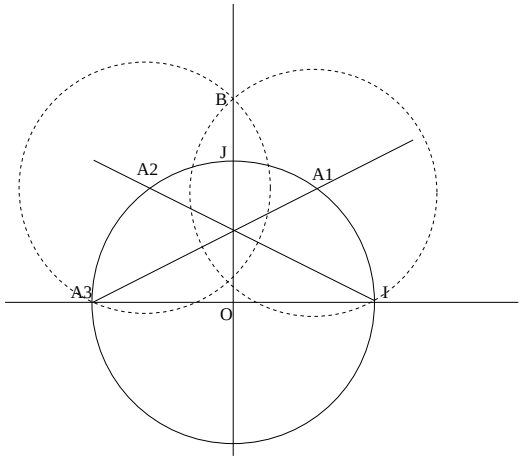
Comme I est le milieu de $[GA]$: $\overline{IA} = \frac{R'}{2} = \frac{r^2}{2R}$
$\Longrightarrow \frac{r^2}{2R'} = \frac{R}{2}$
$\Longrightarrow \overline{I'A} = \frac{R}{2}$
$\Longrightarrow I'$ est le milieu de $[OA]$
$\Longrightarrow O = O'$.

4.2 Le théorème de Mohr Mascheroni

Théorème : Tout point constructible à la règle et au compas est constructible avec le compas seulement.

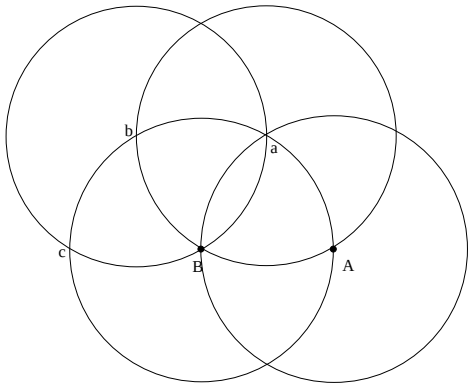
Résultats préliminaires :
Soit $B = \{O; I\}$ les points de base.

J est constructible uniquement au compas :
Soit Γ le cercle de centre O passant par I.
On construit A_1, A_2, A_3 sur Γ à l'aide d'une ouverture de compas égale à $\|OI\|$ partant de I. A_3 est alors diamétralement opposé à I sur Γ.
Les triangles IA_3A_2 et IA_1A_3 sont rectangles et $\widehat{A_3IA_1}=\pi/3$, $\widehat{IA_3A_2}=\pi/3$.
$\sin(\frac{\pi}{3})=\frac{A_1A_3}{2OI}=\frac{\sqrt{3}}{2} \Longrightarrow \|A_1A_3\|=\sqrt{3}\|OI\|$.
De même on a $\|IA_2\|=\sqrt{3}\|OI\|$.
Les cercles de rayon $\|IA_2\|=\|A_1A_3\|=\sqrt{3}\|OI\|$ de centres I et A_3 se coupent en B.
B est donc sur la médiatrice de $[A_3I]$ donc OBI est un triangle rectangle.
Par pythagore, on a : $OB^2 = IB^2 - OI^2 = IA_2^2 - OI^2 = 3OI^2 - OI^2 = 2OI^2$ donc $\|OB\|=\sqrt{2}\|OI\|$.
$\|OB\|$ est la longueur de la diagonale du carré construit à partir du côté OI.
Donc $J=\Gamma \cap C(I, \|OB\|)$.



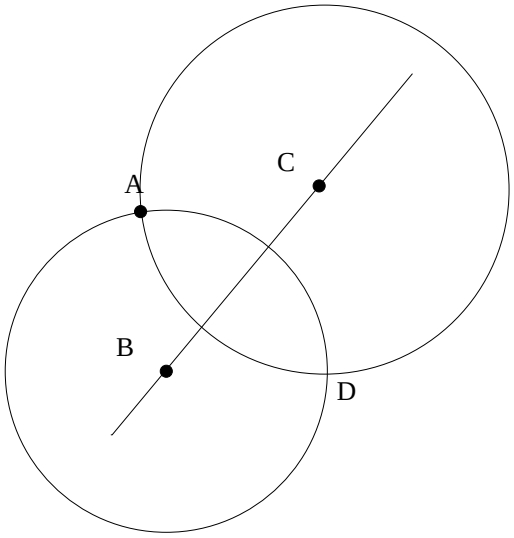
Dans le chapitre 1, on a noté E l'ensemble des nombres réels constructibles à la règle et au compas. Notons E' l'ensemble des points constructibles au compas seulement.
On a evidemment $E' \subseteq E$.
La démonstration du théorème consiste à montrer que $E \subseteq E'$. On montrera tout d'abord quelques résultats préliminaires.

Etape 1 : *Si A et B sont des points constructibles au compas alors le symétrique de A par rapport à B est constructible au compas.*



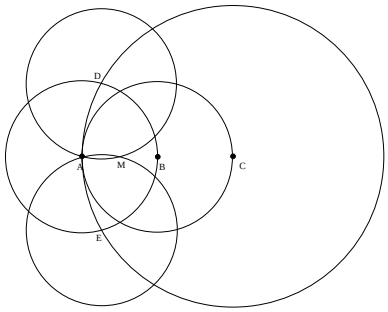
Soit $\Gamma = C(B, \|AB\|)$, avec une ouverture de compas égale à AB, on construit sur Γ partant de A : a, b, c.
c est bien le point cherché, car ABa, aBb et bBc sont des triangles équilatéraux et donc $\widehat{ABc}$=3.π/3=π.

Etape 2 : *Si A, B, C sont des points constructibles au compas avec $B \neq C$, le symétrique D de A par rapport à la droite (BC) est constructible au compas.*



On construit D de façon à ce que (BC) soit la médiatrice de $[AD]$:
$D = C(B, \|AB\|) \cap C(C, \|CA\|)$.

Etape 3 : *Si A et B sont des points constructibles au compas alors le milieu du segment $[AB]$ est constructible au compas.*

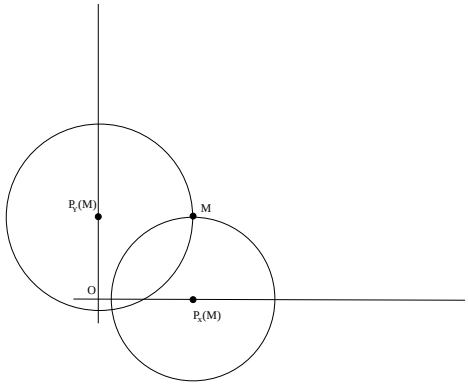


Par l'étape 1, on construit C le symétrique de A par rapport à B.
Soient $\{D; E\} = C(C, \|AC\|) \cap C(A, \|AB\|)$ et $M = C(D, \|AD\|) \cap C(E, \|AE\|)$
M est le milieu de $[AB]$ car si on note A' le symétrique de A par rapport C et N la projection orthogonale de D et E sur (AB), on a dans le triangle ADA' : $AD^2 = AN.AA'$
En effet :
$\overrightarrow{AN}.\overrightarrow{AA'} = (\overrightarrow{AD} + \overrightarrow{DN}).(\overrightarrow{AD} + \overrightarrow{DA'}) = AD^2 + \overrightarrow{AD}.\overrightarrow{DA'} + \overrightarrow{DN}.\overrightarrow{AA'} = AD^2$.
D'où $AB^2 = AN.(4AB) \Longrightarrow AN = AB/4$
Or N est par construction le milieu de $[AM]$ (car (DE) est la médiatrice de $[AM]$), donc $AM = 2AN$.
Ainsi $AM = AB/2$.

Etape 4 : *Si M est un point du plan, M est constructible au compas si et seulement si ses projections sur les axes (ox) et (oy) du repère (O, I, J) sont constructibles au compas.*

$(\Longrightarrow)$
Soit M constructible au compas.
Si M est sur (ox) alors M est sa projection orthogonale sur (ox).
Sinon, on construit M' le symétrique de M par rapport à (ox) et L le symétrique de O par rapport à (MM') d'après l'étape 2.
$P_x(M)$: le projeté orthogonale de M sur (ox) est le milieu de $[OL]$ car $[MM']$ est la médiatrice de $[OL]$. $P_x(M)$ est constructible d'après l'étape 3.
On construit de la même façon $P_y(M)$: le projeté orthogonale de M sur (oy).

$(\Longleftarrow)$

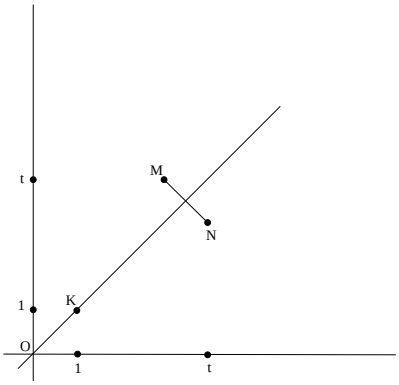


Si les projections $P_x(M)$ et $P_y(M)$ de M sont constructibles au compas, M est constructible au compas car : $M = C(P_x(M), \|OP_y(M)\|) \cap C(P_y(M), \|OP_x(M)\|)$

Etape 5 : *E' est l'ensemble des abscisses des points de l'axe (ox) constructibles au compas, ainsi que l'ensemble des ordonnées des points de l'axe (oy) constructibles au compas.*

Notons X : l'ensemble des abscisses des points de l'axe (ox) constructibles au compas.
Soit $t \in X$, on a $M = (t, t') \in E$' alors $P_x(M) \in E'$ d'aprés l'étape 4) donc $t \in E'$.
On a donc $X \subseteq E'$.

Soit $t \in E'$, t est l'abscisse ou l'ordonné d'un point M constructible au compas.
Si $M = (t, t')$ alors $P_x(M) = t$ et d'après l'étape 4), il est constructible au compas.
Donc $t \in X$.
Si $M = (t', t)$: soit $K = (1, 1)$, K est constructible au compas d'après l'étape 4 car on a I et J.
Soit N le symétrique de M par rapport à la droite (OK). N est constructible par l'étape 2).
On a $N = (t, t')$ et on est ramené au cas précédent.
Donc $t \in X$.



La démonstration est identique pour les ordonnées.

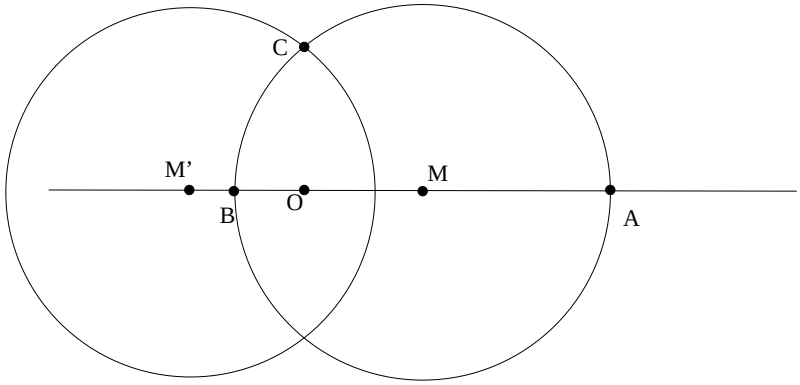
Lemme 2 : *E' est un sous-corps de $\mathbb{R}$ stable par racine carré.*

Preuve :
On a 0 et $1 \in E$ car ce sont les abscisses de (O, I). Donc $E' \neq \emptyset$.

1) Soit $u \in E'$.
Soit $M = (u, 0)$, par l'étape 5, M est constructible au compas.
Par l'étape 1, M' son symétrique par rapport à O est constructible.
On a $M' = (-u, 0)$ donc $-u \in E'$.

2) Soit $u, v \in E'$.
Soient $M = (u, 0)$ et $N = (v, 0)$, M et N sont constructibles au compas.
Par l'étape 3), on peut construire le milieu w de $[uv]$.
On a $w{=}\frac{u+v}{2}$.
Par l'étape 1), on peut construire O' le symétrique de O par rapport à w.
$O' = 2w = u + v$ donc $u + v \in E'$.
Donc E' est stable pour l'addition.

3) Soit $(u, v) \in E'^2$ avec $u{>}0$ et $v{>}0$.
Si $u = v$ alors $\sqrt{uv}{=}u \in E'$.
Sinon : soit $A = (u, 0)$ et $B = (-v, 0)$.



Par l'étape 3, on construit M le milieu de $[AB]$.
Soit $C = C(M,\|MB\|)\cap(Oy)$.
C est bien constructible au compas, car on peut construire M' le symétrique de M par rapport à O.
$C = C(M,\|MA\|)\cap C(M',\|MB\|)$ car (Oy) est la médiatrice de $[M, M']$.
D'où $C \in E'$.
De plus $OC = \sqrt{uv}$, en effet :
$OC^2{=}AC^2{-}OA^2$ et $OC^2{=}\ BC^2{-}OB^2$.
Or $AB^2{=}\ AC^2{+}BC^2$
Donc $2OC^2{=}\ AB^2{-}(OA^2{+}OB^2){=}\ (u+v)^2{-}u^2{-}v^2{=}\ 2uv$.
Donc $OC = \sqrt{uv}$ et donc $\sqrt{uv} \in E'$.

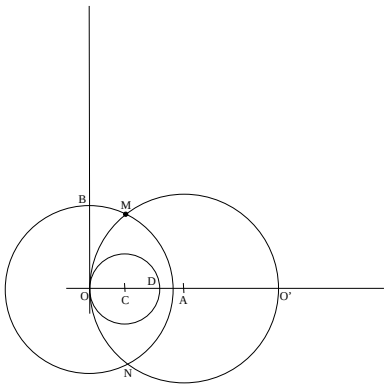
Donc pour $v = 1$, $u{\in}E'$, $u{>}0 \Longrightarrow \sqrt{u} \in E'$.
Donc E' est stable par racine carré.

4) Soient $u, v, w \in E'$ tels que w$\neq$0.
On a :

$$\frac{uv}{w} = \frac{(\sqrt{uv})^2}{w}$$

or $\sqrt{uv} \in E'$ donc il suffit de montrer $\frac{t^2}{w} \in E'$.

Soient $A=(w,0), B=(0,t)$ et $\{M,N\}=C(A,\|OA\|)\cap C(O,\|OB\|)$



Par l'étape 1), on construit O' le symétrique de O par rapport à A et par l'étape 4), on construit $C=P_x(M)$.
Or dans OMO' : $OM^2=\overline{OC}.\overline{OO'}$
$\Longrightarrow t^2=\overline{OC}.(2w)$
$\Longrightarrow 2\overline{OC}=\frac{t^2}{w}$
Par l'étape 1), on construit D le symétrique de O par rapport à C et donc $\overline{OD}=2\overline{OC}=\frac{t^2}{w}$
$\Longrightarrow E'$ est stable pour la multiplication et l'inversion.

Lemme 3 : *E est le plus petit sous-corps de $\mathbb{R}$ stable par racine carré.*

Soit K un sous-corps de $\mathbb{R}$ stable par racine carré.
Soit $t\in E$, par le théorème de Wantzel, $\exists$ (L_0,...,L_p) sous-corps de $\mathbb{R}$ tels que $L_0=\mathbb{Q}$, t $\in L_p$ et $\forall$i$\in[1;p-1]$ $[L_{i+1}:L_i]=2$.
Montrons par récurrence que : $\forall$i$\in[1;p]$ $L_i\subseteq K$.
$L_0=\mathbb{Q}\subseteq K$ car $\mathbb{Q}$ est le plus petit sous-corps de $\mathbb{R}$.
On suppose que $L_i\subseteq K$. Soit $x\in L_{i+1}\backslash L_i$. Comme $[L_{i+1}: L_i]=2$ donc $(1,x)$ est une base de L_{i+1} sur L_i.
$\Longrightarrow (1,x,x^2)$ est liée dans L_i .
$\Longrightarrow \exists\ (a,b,c)\in \mathrm{L_i}^3$ avec $(a,b,c)\neq(0,0,0)$ tels que $ax^2+bx+c=0$.
si $a=0$ alors $x=-c/b\in L_i$ donc $x\in K$.
sinon on résout l'équation du second degré, et on obtient :

$$x\in\left\{\frac{-b\pm\sqrt{b^2-4ac}}{2a}\right\}$$

or K est un sous-corps stable par racine carrée, donc $x\in K$.
Donc $L_{i+1}\subseteq K$.
Donc $t\in L_p\subseteq K\Longrightarrow E\subseteq K$.

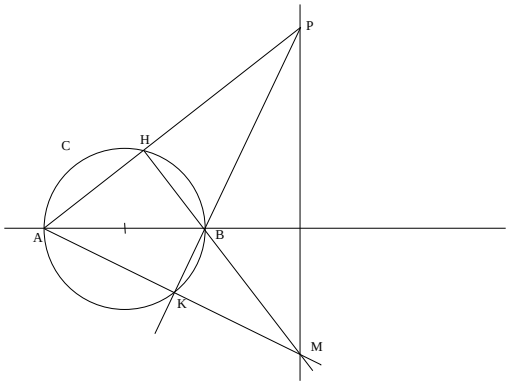
Preuve du théorème de Mohr Mascheroni :

D'après le théorème 4 du chapitre 1, E est un sous-corps de $\mathbb{R}$ stable par racine carré et c'est le plus petit. Comme E' est un sous-corps de $\mathbb{R}$, on en déduit que $E \subseteq E'$.
Si $M = (x, y)$ est un point constructible à la règle et au compas, alors $x \in E$ et $y \in E$. Donc $x \in E'$ et $y \in E'$.
D'après l'étape 5), $x = P_x(M)$ et $y = P_y(M)$ sont constructibles au compas.
D'après l'étape 4), M est constructible au compas.

4.3 Exemples de construction à la règle seule.

Soit C un cercle, A et B deux points diamétralement opposés de C et P un point du plan . On veut construire la perpendiculaire à (AB) passant par P.

On trace les droites (PA) et (PB) ; soient $H = (PA) \in C$ et $K = (PB) \in$ C . Remarquons que ABH et ABK sont deux triangles rectangles en H et K. Soit $M = (HB) \in (AK)$, donc (MH) et (PK) sont les hauteurs du triangles APM. Elles se coupent en B, donc $[AB]$ est une hauteur de APM, et on a bien $(AB) \perp (PM)$.



Bibliographie

[1] Jean-Claude Carrega. *Théorie des corps, La règle et le compas*. 1989.

[2] Jean-Pierre Escofier. *Théorie de Galois*. 1997.

[3] Jean Fresnel. *Méthodes modernes en géométrie*. 1996.

[4] Ivan Gozard. *Théorie de Galois*. 1997.