Compte-rendu de projet: Constructions à la règle et au compas

Valérie ROBERT

Juin 2010

Table des matières

1 Nombres réels constructibles

La règle (non graduée) et le compas sont les outils de base permettant de travailler en géométrie.
Ainsi, Euclide a fondé sa géométrie sur un système d'axiomes qui assure en particulier qu'il est toujours possible de tracer une droite passant par deux points donnés et qu'il est toujours possible de tracer un cercle de centre donné et passant par un point donné. La géométrie euclidienne est donc la géométrie des droites et des cercles, donc de la règle et du compas.
Grâce à ces derniers, on peut dès lors, faire des constructions simples comme celles d'axe ou de centre de symétrie, de parallèle ou de perpendiculaire, ou plus élaborées comme le polygone à 17 côtés.

1.1 Points constructibles

On travaille dans tout ce qui suit, avec un plan euclidien $\mathscr{E}$.
On suppose donné un ensemble fini $\mathscr{P} = A_1, ..., A_n$ de points de $\mathscr{E}$ (avec $n \geq 2$), et on considère deux types de figures (que l'on dira *admissible* relativement à $\mathscr{P}$) :

1. les droites passant par deux points distincts de $\mathscr{P}$ (que l'on construit à la règle),

2. les cercles, centrés en un point de $\mathscr{P}$ et passant par un autre point de $\mathscr{P}$ (que l'on construit au compas).

Définition 1.1. *Un point M du plan est dit **constructible** en un pas à la règle et au compas à partir de $\mathscr{P}$ s'il existe des figures admissibles relativement à $\mathscr{P}$ dont M est un point d'intersection.*
En d'autres termes, il est constructible à partir de $\mathscr{E}$ si on peut le construire en un nombre fini de pas à partir de $\mathscr{P}$, id est, s'il existe des points $M_1, M_2, ..., M_r$ tels que $M_r = M$ et que pour i = 1,...,r-1 , M_{i+1} est constructible en un pas à partir de $\mathscr{P} \cup M_1, ..., M_i$.

1.2 Quelques constructions élémentaires

a) Médiatrice et perpendiculaire

Soit [AB] un segment.

- La médiatrice de $[AB]$ est l'ensemble des points équidistants de A et B. On la construit en traçant les cercles $\mathscr{C}_1$ et $\mathscr{C}_2$ de centre A (resp B) passant par B (resp.A) et en joignant leurs points d'intersection C et D, comme sur la figure 1.

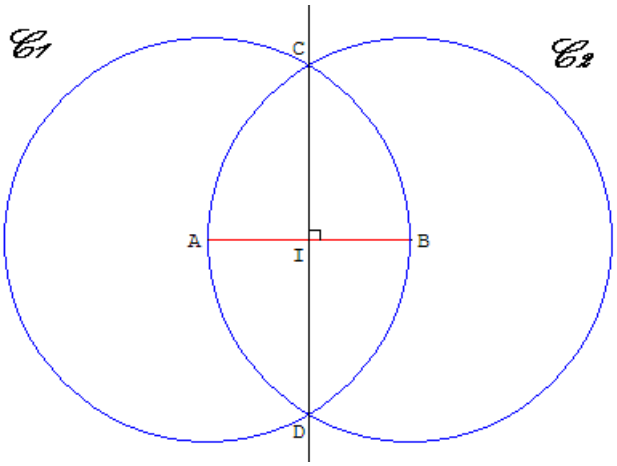

FIGURE 1

- La perpendiculaire à une droite (AB) passant par un point C n'appartenant pas à (AB) s'obtient en traçant les cercles de centres A et B qui passent par C. Ces cercles se recoupent en un point C' et la perpendiculaire est donc (CC').

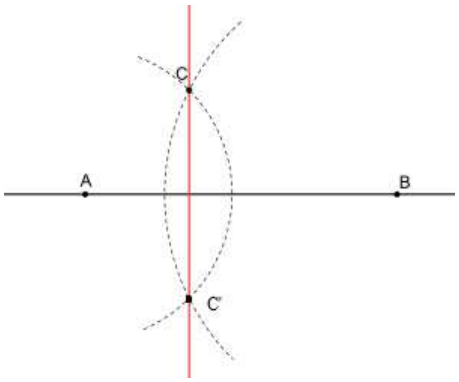

FIGURE 2

b) Parallèle et partage d'un segment

– Il s'agit de construire la parallèle à (AB) passant par C. Pour ce faire, on construit le milieu D du segment $[BC]$ (par exemple par la méthode des médiatrices),ensuite le cercle $\mathscr{C}$ de centre D et passant par A. Enfin, il suffit de tracer la droite $[AD]$, le second point d'intersection entre le cercle et cette dernière étant noté E.
La parallèle ainsi cherchée est la droite (EC).

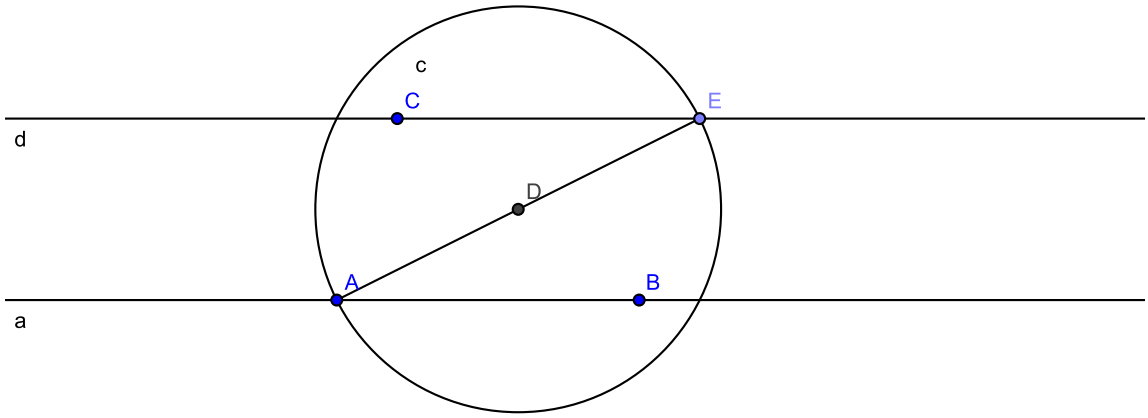

FIGURE 3

– Soit $[AB]$ un segment et p un entier. Il s'agit de partager ce segment en p parties égales. On trace dans un premier temps, une sécante à $[AB]$ passant par A.
Ensuite, on prend un écartement de compas et on reporte cet écartement p fois à partir de A. Le dernier point obtenu après p écartements est noté G .

Puis on trace la droite (GB).
Enfin, on construit à l'aide de la méthode précédente par exemple, les parallèles à (GB) qui passent par les points obtenus successivement après chaque écartement. Elles partagent ainsi, le segment en p parties égales(voir figure 4 où p=5).

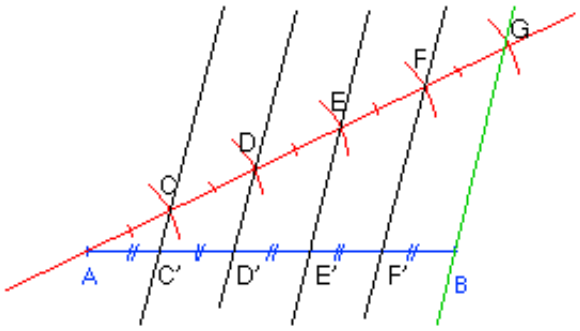

FIGURE 4

c) Report de compas et bissectrice

– Il s'agit lorsqu'on dispose de trois points O, A, B de construire le cercle de centre O et de rayon AB. On construit les parallèles à (AB) passant par O et à (OA) passant par B. Elles se coupent en C et comme $OABC$ est un parallélogramme, on a $AB = OC$. On construit alors le cercle de centre O passant par C.

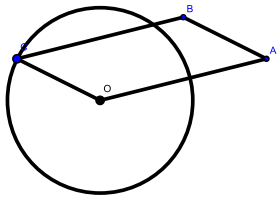

FIGURE 5

– On considère l'angle $\widehat{xOy}$
On pointe le compas au sommet de l'angle et on trace un premier arc de cercle. On marque les points d'intersection de cet arc avec les deux côtés de l'angle (sur la Figure 5 ils sont notés M et N).
Ensuite, on pointe successivement le compas aux points d'intersection M et N et on trace deux arcs de cercle de même rayon (en gardant le même écartement du compas entre les deux opérations). Enfin on note P le point d'intersection de ces deux arcs.
Ainsi la droite qui relie le sommet de l'angle et le point d'intersection des deux derniers cercles noté P est la bissectrice de l'angle $\widehat{xOy}$.

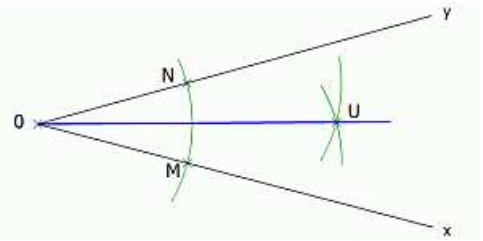

FIGURE 6

1.3 Réels constructibles

Définition 1.2. *Si t est un réel , on dit que t est un nombre constructible si et seulement si le point de l'axe Ox d'abscisse t est un point constructible (même résultat en remplaçant Ox par Oy et abscisse par ordonnée).*

1.4 Structure et propriétés de l'ensemble $\mathscr{K}$ des nombres constructibles

Nous allons montrer que l'ensemble $\mathscr{K}$ des nombres constructibles est un sous-corps de $\mathbb{R}$ qui contient $\mathbb{Q}$ et qui est stable par racine carrée.

Dans cette partie, on se donne O et I deux points dans $\mathscr{E}$ et on prend O comme origine et OI comme unité de longueur. On construit la droite (OI) que l'on prend comme axe des x. Ensuite, on construit le point I' symétrique de I par rapport à O et on trace la médiatrice de $[II']$ et un point J de cette médiatrice tel que $OI = OJ$. Ainsi, on prend O, I, J comme repère orthonormé et (OJ) comme axe des y.

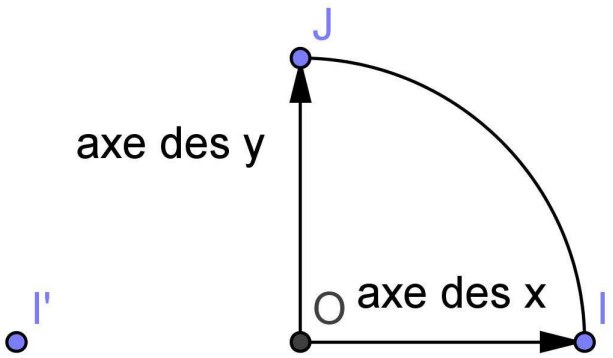

FIGURE 7

a) Les rationnels sont constructibles

Proposition 1.3. *Les nombres rationnels sont constructibles.*

Démonstration. Il suffit de montrer que que le point $(\frac{p}{q},0)$ est constructible où $(p,q) \in \mathbb{Z}\times\mathbb{Z}^*$. Pour ce faire, à partir du point $P=(p,0)$ qui est constructible, on prend le segment $[OP]$ et on le partage en q parties égales en utilisant la méthode du § b) du 1.2 .

b) Structure de corps

Théorème 1.4. *L'ensemble des nombres constructibles $\mathscr{K}$ est un sous-corps de $\mathbb{R}$.*

Démonstration. Il faut montrer que $\mathscr{K}$ est stable par $+$, - , $\times$ et $\div$, ie si x et y sont constructibles alors x+y, x - y, xy et $\frac{x}{y}$ sont constructibles.

1. Si $x \in \mathscr{K}$, alors -$x \in \mathscr{K}$.
   En effet, si A est le point de (Ox) d'abscisse x, en utilisant le cercle de centre O passant par A , on construit le point A' de (Ox) d'abscisse -x.
2. Si x et y sont dans $\mathscr{K}$, alors $x + y \in \mathscr{K}$.
   Soient A et B les points de (Ox) tels que $\overline{OA} = x$ et $\overline{AB} = y$; A est constructible et B aussi en utilisant le cercle de centre A et de rayon $|y|$. Ainsi, $\overline{OB} = x + y$ et donc $x + y \in \mathscr{K}$.
3. Si x et y sont dans $\mathscr{K}$, alors $xy \in \mathscr{K}$
   . Enlevons le cas trivial où xy=0.
   Soient A le point de (Ox) tel que $\overline{OA} = x$ et B le point de (Oy) tel que

$\overline{OB} = y$.
La parallèle à (IB) passant par A coupe (Oy) en C. D'après le théorème de Thalès, on a $\frac{\overline{OC}}{\overline{OB}} = \frac{\overline{OA}}{\overline{OI}}$, d'où $\overline{OC} = xy$.

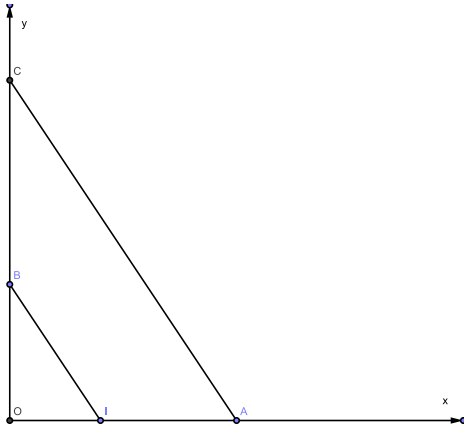

FIGURE 8

4. Si $x \in \mathscr{K}$, alors $\frac{1}{x} \in \mathscr{K}$.
Soit A sur (Ox) tel que $\overline{OA} = x$. La parallèle à (AJ) passant par I coupe (Oy) en B. D'après le théorème de Thalès, on a : $\frac{\overline{OB}}{\overline{OJ}} = \frac{\overline{OI}}{\overline{OA}}$. D'où $\overline{OB} = \frac{1}{x}$.

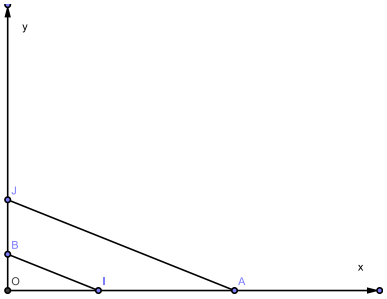

FIGURE 9

c) Stabilité par racine carrée

Proposition 1.5. *Si $x \in \mathscr{K}$ et $x \geqslant 0$, alors $\sqrt{x}$ est dans $\mathscr{K}$.*

Démonstration. Supposons $x > 0$ et soit A le point de l'axe (Ox) tel que $\overline{IA} = x$. On se ramène au cas $x > 1$ (si $x < 1$, on construit d'abord la racine de $\frac{1}{x}$ puis on prend l'inverse). On trace le demi-cercle de diamètre OM situé dans le demi-plan $y \geqslant 0$, puis la perpendiculaire à (OM) en I. Elle recoupe le demi-cercle en A. Le triangle OAM est rectangle donc $\cos \widehat{MOA} = \frac{OA}{OM} = \frac{OI}{OA}$. On en déduit que $OA^2 = OM \times OI = x$. Ainsi $OA = \sqrt{x}$ et on prend l'intersection du cercle de centre O passant par A avec l'axe des x pour obtenir le point cherché.

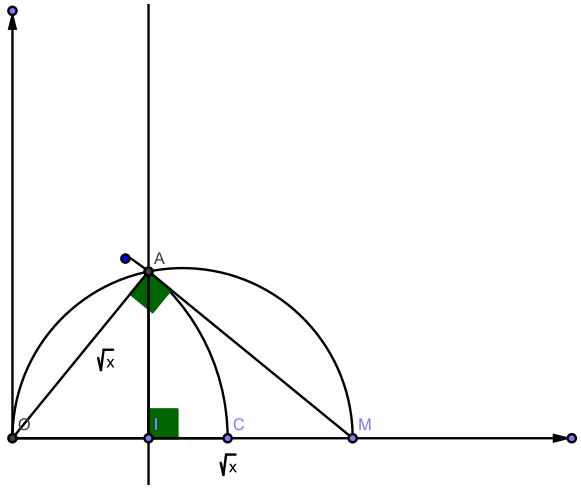

FIGURE 10

Remarque. Ainsi, grâce à ces propriétés que possède l'ensemble des nombres constructibles, on peut d'ores et déjà donner de nombreux exemples de nombres constructibles tels $-\frac{2}{3}$, $\sqrt[4]{3}$, $\frac{2+3\sqrt{2}}{\sqrt{3}}$.

1.5 Caractérisation des éléments de $\mathscr{K}$

Théorème 1.6 *Soit x un nombre réel. Alors x est constructible si et seulement si il existe une suite $\mathbb{K}_0, \mathbb{K}_1, \cdots, \mathbb{K}_r$ de sous-corps de $\mathbb{R}$ vérifiant les conditions suivantes :*

1. *on a $\mathbb{K}_0 = \mathbb{Q}$,*

2. *on a* $\mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_r$, *plus précisément, pour chaque* $i = 1, 2, \cdots, r$, *il existe* $d_i \in \mathbb{K}_{i-1}$ *tel que* $\mathbb{K}_i = \mathbb{K}_{i-1}(\sqrt{d_i})$,
3. *on a* $x \in \mathbb{K}_r$.

Remarques importantes.

1. Pour $i = 1, \cdots, r$ on a $\mathbb{K}_i = \mathbb{K}_{i-1}(\sqrt{d_i})$, et donc :

   $$[\mathbb{K}_i : \mathbb{K}_{i-1}] = \begin{cases} 1 & \text{si } \mathbb{K}_i = \mathbb{K}_{i-1} \\ 2 & \text{sinon car } X^2 - d_i \text{ est le polynôme minimal de } \sqrt{d_i} \text{ sur } \mathbb{K}_i. \end{cases}$$

   Dans les deux cas, on a :

   $$\begin{aligned} [\mathbb{K}_r : \mathbb{Q}] &= [\mathbb{K}_r : \mathbb{K}_{r-1}] \times [\mathbb{K}_{r-1} : \mathbb{K}_{r-2}] \times \cdots \times [\mathbb{K}_1 : \mathbb{Q}] \\ &= 2^j \text{ pour } 1 \leq j \leq r. \end{aligned}$$

   De plus, on a $\mathbb{Q} \subset \mathbb{Q}(x) \subset \mathbb{K}_r$ donc $[\mathbb{Q}(x) : \mathbb{Q}]$ est un diviseur de 2^j, c'est donc une puissance de 2 que nous noterons 2^p. Ainsi la famille à $2^p + 1$ éléments : $1, x, x^2, \cdots, x^{2^p}$ est liée dans $\mathbb{Q}(x)$ et il existe alors $\alpha_0, \alpha_1, \cdots, \alpha_{2^p}$ dans $\mathbb{Q}$ non tous nuls tels que $\alpha_0 + \alpha_1 x + \cdots + \alpha_{2^p} x^{2^p} = 0$.

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

2. **La réciproque du théorème 1.6 est fausse**
   Contre-exemple : Considérons le polynôme $P(X) = X^4 - X - 1$. Nous allons montrer grâce à un prochain théorème, que celui-ci est irréductible sur $\mathbb{Q}$ et qu'il possède une racine réelle α non constructible. Ainsi, on aura $[\mathbb{Q}(\alpha) : \mathbb{Q}]=4$ qui est une puissance de 2, et donc α est de degré une puissance de 2 mais non constructible.

Pour démontrer ce théorème, nous avons besoin d'un lemme préliminaire :

Lemme 1.7. *Soit* $\mathscr{P} = M_0 = O, M_1 = I, M_2, \cdots, M_r$ *un ensemble fini de points de points de* $\mathscr{E}$ *dont toutes les coordonnées sont dans un sous-corps* $\mathbb{K}$ *de* $\mathbb{R}$. *Soit* $M = (x, y)$ *un point construit en un pas à partir de* $\mathscr{P}$. *Alors, il existe un élément* $d \in \mathbb{K}$ *tel que* $x, y \in \mathbb{K}(\sqrt{d})$.

Démonstration. Notons $\mathscr{D}$ l'ensemble des droites joignant deux points de $\mathscr{P}$ et $\mathscr{C}$ l'ensemble des cercles centrés en un point de $\mathscr{P}$ et passant par un point de $\mathscr{P}$.
On sait que M est un point constructible donc il est intersection de deux éléments de $\mathscr{D}$ et/ou de $\mathscr{C}$. Il faut donc distinguer trois cas :

1. Si $M = (x, y)$ est intersection de deux droites Δ_1 et Δ_2 de $\mathscr{D}$ alors il vérifie l'équation à coefficients dans $\mathbb{K}$ de chacune des deux droites :

$$\begin{cases} ax + by + c & = 0 \\ a'x + b'y + c' & = 0 \end{cases}$$

Ainsi, on déduit x et y :

$$x = \frac{bc' - b'c}{ab' - a'b} \qquad\qquad y = \frac{-ac' + a'c}{ab' - a'b}.$$

On voit alors que x et y appartiennent à $\mathbb{K}(\sqrt{1})$.

2. Si $M = (x, y)$ est l'intersection d'une droite et d'un cercle , alors M vérifie les équations suivantes :

$$\begin{cases} ax + by + c & = 0 \\ x^2 + y^2 + \alpha x + \beta y + \gamma & = 0. \end{cases}$$

Si on suppose $b \neq 0$ (si $b = 0$ alors on a $a \neq 0$ et on procèdera de même) alors la première équation se réécrit $y = px + q$ avec $p, q \in \mathbb{K}$ On reporte cela dans la deuxième équation et on montre alors que x est solution de l'équation du second degré suivante :

$$(1 + p^2)x^2 + (2pq + \alpha + \beta p)x + q^2 + \beta q + \gamma = 0.$$

Alors si on note d le discriminant de cette équation, il est dans $\mathbb{K}$ et on a ainsi x qui est dans $\mathbb{K}(\sqrt{d})$. On en conclut aussi grâce aux équations que y est dans $\mathbb{K}(\sqrt{d})$.

3. Si $M = (x, y)$ est intersection de deux cercles de $\mathscr{C}$, alors M vérifie :

$$\begin{cases} x^2 + y^2 + \alpha x + \beta y + \gamma' & = 0 \\ x^2 + y^2 + \alpha' x + \beta' y + \gamma' & = 0. \end{cases}$$

Par différence, on se ramène au cas précédent.

Démonstration du Théorème 1.6. On montre par récurrence sur r la propriété $\mathrm{P}(r)$ suivante :

Si $\mathscr{P}$ $=M_0 = O, M_1 = I, M_2, \cdots, M_r$ sont des points du plan tels que, pour $i = 1, \cdots, r-1$, M_{i+1} soit construit en un pas à partir de $\mathscr{P}$, alors il existe une suite de corps $\mathbb{K}_0, \cdots, \mathbb{K}_r$ vérifiant les conditions du

théorème 1.6 et tels que les coordonnées de tous les M_i soient dans $\mathbb{K}_r$.

La propriété est vraie pour $r = 0$.
Supposons la propriété vraie pour r et montrons P(r+1).
Les coefficients des points $M_0, \cdots, M_r$ sont dans $\mathbb{K}_r$ par hypothèse de récurrence. On rajoute un point $M = M_{r+1}$ construit en un pas à partir des M_i. D'après le lemme 1.7 les coordonnées de M sont dans un corps $\mathbb{K} = \mathbb{K}(\sqrt{d})$ avec $d \in \mathbb{K}_r$, et on ajoute ainsi $\mathbb{K}_{r+1}$ à la suite des $\mathbb{K}_i$.

Théorème 1.7. *Soit x un nombre réel algébrique de polynôme minimal P. Alors x est constructible si et seulement si le corps de décomposition de P, $D_P(\mathbb{Q})$ est de degré une puissance de 2 sur $\mathbb{Q}$.*

Remarque. Pour démontrer ce dernier, il est nécessaire de faire appel à la théorie de Galois, notamment à son théorème fondamental et d'en préciser le cadre, mais également à quelques résultats d'algèbre.

Rappels sur la théorie de Galois

Définition 1.8. *Soit $\mathbb{L}$: $\mathbb{K}$ une extension de corps. Le groupe de Galois G associé à cette extension est l'ensemble des automorphismes de $\mathbb{L}$ fixant $\mathbb{K}$.*

Définition 1.9. *Notons $\mathscr{F}$ l'ensemble des extensions intermédiaires, id est l'ensemble des sous-corps $\mathbb{M}$ tels que $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ et $\mathscr{G}$ l'ensemble de tous les sous-groupes de G. On définit alors deux applications :*

$$\begin{aligned} * : \mathscr{F} &\longrightarrow \mathscr{G} \\ \mathbb{M} &\longmapsto \mathbb{M}^* \end{aligned}$$

et

$$\begin{aligned} \dagger : \mathscr{G} &\longrightarrow \mathscr{F} \\ H &\longmapsto H^\dagger \end{aligned}$$

telles que si $\mathbb{M} \in \mathscr{F}$, alors $\mathbb{M}^*$ est le groupe des automorphismes de $\mathbb{L}$ laissant invariant $\mathbb{M}$. Si $H \in \mathscr{G}$, alors $H^\dagger$ est le corps fixe de H, c'est à dire l'ensemble des x de $\mathbb{L}$ tels que $f(x) = x$ pour tout f de H.
Et on remarque de plus, que les applications sont décroissantes.

Théorème fondamental 1.10. *Si $\mathbb{L}$: $\mathbb{K}$ est une extension finie et normale alors :*

1. *Le groupe de Galois G est d'ordre* $[\mathbb{L} : \mathbb{K}]$.
2. *Si* $\mathbb{M}$ *est une extension intermédiaire, alors :*

$$\begin{cases} [\mathbb{L} : \mathbb{M}] & = \text{card}(M^*) \\ [\mathbb{M} : \mathbb{K}] & = \text{card(G)}/\text{card}(M^*). \end{cases}$$

3. *Les applications * et † sont bijectives, réciproques l'une de l'autre et sont décroissantes.*

Remarque. Une extension algébrique $\mathbb{L} : \mathbb{K}$ est dite normale si et seulement si tout morphisme de corps fixant $\mathbb{K}$ est un automorphisme de $\mathbb{L}$. Par exemple, un corps de décomposition d'un polynôme est une extension normale.

Résultats d'algèbre utiles

Lemme 1.11. *Si G est un groupe fini, considérons l'action de conjugaison de G sur lui-même. Notons* C_i *les classes de conjugaison associées, à savoir, pour tout g de G,* $C_i(g) = \{xgx^{-1}, x \in G\}$ *pour chaque* $i \leq$ *card(G).*
Alors le cardinal de chacune des classes de conjugaison divise l'ordre de G.

Démonstration. Ici, chacune des classes de conjugaison est en fait une orbite sous l'action de G. Or, une orbite $w(x)$ est de cardinal un diviseur de $\text{card}(G)$. En effet, on a l'égalité suivante :

$$\text{card}(w(x)) = \frac{\text{card}(G)}{\text{card}(\text{stab}_G(x))}$$

où $\text{Stab}_G(x) = \{g \in G, gxg^{-1} = x\}$ qui est un sous-groupe de G.

Lemme 1.12. *Si A est un groupe fini, dont l'ordre est divisible par un nombre premier p, alors il admet un élément d'ordre p.*

Lemme 1.13. *Si card(G)=*p^r*, alors Z(G) (l'ensemble des éléments de G qui commutent avec tout élément de G) contient un élément d'ordre p.*

Démonstration. Les cardinaux des classes divisent p^r par le lemme 1.11. Comme celle de 1 est réduite à 1, on déduit, grâce à l'équation aux classes ($1+C_1 + \cdots + C_k = p^r$,$k \leq p^r$) qu'il y en a d'autres qui sont de cardinal 1. Or, les classes de cardinal 1 sont celles des éléments du centre. Il en résulte que le centre n'est pas réduit à $\{1\}$ Comme c'est un sous groupe, son cardinal divise p^r, donc c'est un multiple de p. On conclut en utilisant le lemme 1.12.

Corollaire 1.14. *Si G est un groupe fini, et card(G)=2^r alors il existe une suite croissante $G_0 \subset \cdots \subset G_r$ de sous-groupes distingués de G tels que card(G_i) = 2^i pour tout $0 \leq i \leq r$.*

Démonstration. On montre par récurrence sur n la propriété $\mathrm{P}(r)$ suivante : Si G est un groupe fini, et card(G)= 2^r alors il existe une suite croissante $G_0 \subset \cdots \subset G_r$ de sous-groupes distingués de G tels que card(G_i) = 2^i pour tout $0 \leq i \leq r$.
Le cas $r = 0$ est trivial.
Soit $r \in \mathbb{N}^*$ et supposons $\mathrm{P}(r)$. Soit G un groupe fini de cardinal 2^{r+1}. Alors $\mathrm{Z}(G)$ admet un élément x d'ordre 2 par le lemme 1.13.
Considérons le sous-groupe $< x >$ engendré par cet élément qui est donc de cardinal 2. Le quotient $G/< x >$ existe et est de cardinal 2^r. On lui applique l'hypothèse de récurrence, donc il existe une suite croissante $G_0 \subset \cdots \subset G_r$ de sous-groupes distingués de G tels que card(G_i)=2^i pour tout $0 \leq i \leq r$. Ensuite, on considère leur image réciproque dans G et on obtient alors $\mathrm{P}(r+1)$.

Démonstration du Théorème 1.7. Soit x un nombre réel algébrique de polynôme minimal P. Notons $[D_P(\mathbb{Q}) : \mathbb{Q}]$ le degré de $D_P(\mathbb{Q})$ sur $\mathbb{Q}$ (cette extension vérifie les hypothèses du Théorème fondamental 1.10) et G le groupe de Galois associé.

Supposons que x soit constructible. D'après le Théorème 1.6, il existe une suite de sous-corps de $\mathbb{R}$, $\mathbb{K}_1 \subset \mathbb{K}_2 \subset \cdots \subset \mathbb{K}_r$ avec $\mathbb{K}_1 = \mathbb{Q}$, $x \in \mathbb{K}_r$ et pour $1 \leq i \leq r-1$, $[\mathbb{K}_{i+1} : \mathbb{K}_i]$=2.
On pourra démontrer que cette suite peut être prolongée en une suite $\mathbb{K}_1 \subset \cdots \subset \mathbb{K}_r \subset \cdots \subset \mathbb{K}_q$ avec pour $1 \leq i \leq q-1$ $[\mathbb{K}_{i+1} : \mathbb{K}_i]$=2 où $\mathbb{K}_q$ est une extension normale de $\mathbb{Q}$ contenant $D_P(\mathbb{Q})$. Comme $[D_P(\mathbb{Q}) : \mathbb{Q}]$ est un diviseur de $[\mathbb{K}_q : \mathbb{Q}]$=$2^{q-1}$, on en conclut que le corps de décomposition de P, $D_P(\mathbb{Q})$, est de degré une puissance de 2 sur $\mathbb{Q}$.

Réciproquement, supposons qu'il existe $r \in \mathbb{N}^*$ tel que $[D_P(\mathbb{Q}) : \mathbb{Q}]$= 2^r. Par le 1. du Théorème fondamental 1.10 de Galois, on en déduit que card(G)= 2^r.
Par le corollaire 1.14, on en déduit qu'il existe une suite croissante $G_0 \subset \cdots \subset G_r$ de sous-groupes distingués de G tels que card(G_i) = 2^i pour tout $0 \leq i \leq r$.
Notons pour $0 \leq i \leq r$, $\mathbb{K}_i$ le corps fixe de $G^{\dagger}_{r-i}$. Le 3. du Théorème fondamental de Galois 1.10 , montre que $[\mathbb{K}_{i+1} : \mathbb{K}_i]$ est égal à 2. Enfin, en utilisant le Théorème 1.6, on en conclut que x est constructible.

Retour sur la réciproque du Théorème 1.6 Comme nous l'avons dit précédemment, cette réciproque est fausse et désormais, nous disposons des outils nécessaires pour le prouver.
Considérons donc le polynôme $P(X) = X^4 - X - 1$. Il se décompose dans $\mathbb{R}[X]$ en un produit de deux polynômes du second degré :

$$P(X) = X^4 - X - 1 = (X^2 + aX + b)(X^2 + a'X + b')$$

où $a, b, a', b' \in \mathbb{R}$. On a alors par identification, les relations suivantes :

$$\begin{cases} a + a' = 0 \\ b + b' + aa' = 0 \\ ab' + a'b = -1 \\ bb' = -1. \end{cases} \iff \begin{cases} a' = -a \\ b + b' = a^2 \\ a(b' - b) = -1 \\ bb' = -1. \end{cases}$$

Il en résulte donc que b et b' sont racines de $X^2 - a^2X - 1 = 0$. Comme a et a' sont opposés, on peut supposer par exemple $a > 0$ d'où $b' < b$ et on obtient alors : $\begin{cases} b = \frac{a^2+\sqrt{a^4+4}}{2} \\ b' = \frac{a^2-\sqrt{a^4+4}}{2} \\ b' - b = -\sqrt{a^4+4} \\ a\sqrt{a^4+4} = 1. \end{cases}$

- Le polynôme X^2+aX+b a pour discriminant $\Delta_1 = -a^2-2\sqrt{a^4+4} < 0$ donc il a deux racines complexes μ et $\overline{\mu}$.

- Le polynôme $X^2+a'X+b'$ a pour discriminant $\Delta_2 = 2\sqrt{a^4+4}-a^2 > 0$. Il a donc deux racines réelles α et β.

- A partir de $a\sqrt{a^4+4} = 1$, on en déduit que a^2 est racine du polynôme $X^3 + 4X - 1$. On pourra montrer que ce polynôme n' a pas de racine dans $\mathbb{Q}$ et ainsi qu'il est irréductible dans $\mathbb{Q}[X]$. D'où a^2 est algébrique sur $\mathbb{Q}$ et de degré 3. Le Théorème 1.6 nous dit alors que a^2 n'est pas constructible, et donc que a n'est pas constructible. Comme $\alpha + \beta = -a' = a$, on peut affirmer que l'une au moins des deux racines n'est pas constructible. Ainsi, $P(X)$ a au moins un e racine réelle non constructible.

- a n'étant pas constructible, n'appartient pas à $\mathbb{Q}$ et la décomposition de $P(X)$ considérée plus haut, n'est pas une décomposition dans $\mathbb{Q}[X]$.

De plus X^2+aX+b n'a pas de racine réelle, d'où aucune autre décomposition ne peut se faire dans $\mathbb{Q}[X]$. $P(X)$ est alors irréductible dans $\mathbb{Q}$.

– $P(X)$ est le polynôme minimal de α sur $\mathbb{Q}$ et son corps de décomposition est $D_P(\mathbb{Q}) = \mathbb{Q}(\mu, \overline{\mu}, \alpha, \beta)$. On a par identification, $\mu + \overline{\mu} = -a$ et donc $a^2 \in D_P(\mathbb{Q})$. Or, a^2 est algébrique sur $\mathbb{Q}$ et de degré 3, il en découle alors que $[D_P(\mathbb{Q}) : \mathbb{Q}]$ est divisible par 3 et ainsi ce n'est pas une puissance de 2. Le Théorème 1.7 assure que α n'est pas constructible, et pourtant ce nombre est de degré 4 sur $\mathbb{Q}$, puisque P est irréductible sur $\mathbb{Q}$.

2 Applications

2.1 Duplication du cube, trisection de l'angle

1. Le problème de la duplication du cube consiste à considérer le cube unité de côté OI et de construire un cube de volume double, id est de construire le nombre $\sqrt[3]{2}$.

   Proposition 2.1. *$\sqrt[3]{2}$ n'est pas constructible, donc la duplication du cube est impossible.*

   Démonstration. Considérons le polynôme X^3-2. Si ce polynôme n'était pas irréductible dans $\mathbb{Q}$, alors il se décomposerait dans $\mathbb{Q}$ et un des facteurs serait forcément de degré 1. Ainsi, ce polynôme aurait une racine dans $\mathbb{Q}$. Or les seules racines de ce dernier sont $\sqrt[3]{2}, j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$. On va pouvoir conclure grâce à ce lemme suivant :

   Lemme 2.2. *$\sqrt[3]{2}$ est irrationnel.*

   Démonstration. Raisonnons par l'absurde en supposant que $\sqrt[3]{2}$ est rationnel, *idest* il existe p et q deux entiers avec $q \neq 0$ premiers entre eux tels que $\sqrt[3]{2} = \frac{p}{q}$. En élevant au cube on obtient : $2q^3 = p^3$ (1). Donc p est pair d'où il existe p' tel que $p = 2p'$ et en simplifiant dans (1) par 2 on a : $q^3 = 4p'^3$. Ainsi q aussi est pair, ce qui contredit le fait que p et q sont premiers entre eux.

   Ainsi $\sqrt[3]{2}, j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$ ne sont pas rationnels, donc le polynôme X^3-2 est irréductible sur $\mathbb{Q}$. De plus il est unitaire donc c'est le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbb{Q}$. Il en résulte que $\sqrt[3]{2}$ est algébrique sur $\mathbb{Q}$ et de degré 3. Donc par la contraposée du Théorème 1.6, on en déduit

que $\sqrt[3]{2}$ n'est pas constructible, et donc que la duplication du cube est impossible.

2. La trisection de l'angle consiste à tracer les deux demi-droites qui partagent un angle quelconque donné en trois angles égaux. Ce problème est aussi impossible car nous allons montrer que cos $\frac{\pi}{9}$ n'est pas constructible et donc que l'angle $\frac{\pi}{3}$ n'est pas trisectable.

Proposition 2.3. *le nombre cos $\frac{\pi}{9}$ n'est pas constructible et donc a fortiori que l'angle $\frac{\pi}{3}$ n'est pas trisectable.*

Démonstration. On a cos $3\theta = 4\cos^3\theta - 3\cos\theta$, donc cos $\frac{\pi}{9}$ est racine du polynôme $P(X) = 4X^3 - 3X - 1/2$. Montrons que ce dernier est irréductible sur $\mathbb{Q}$. Raisonnons par l'absurde et supposons qu'il le soit. Alors, un des facteurs de la décomposition est de degré 1 et a donc une racine dans $\mathbb{Q}$ qu'on note $\alpha = \frac{p}{q}$ avec p, q deux entiers tels que $q \neq 0$ et $pgcd(p, q) = 1$. On en déduit que p divise q^3 et q^2 divise $8p^3$. D'où $\alpha = 1, -1, 1/2$ ou $-1/2$. Or ces quatre nombres ne sont pas racines de $P(X)$. On en conclut dans ce cas, que $P(X)$ est irréductible sur $\mathbb{Q}$. Ainsi $\frac{P(X)}{4}$ est le polynôme minimal de cos $\frac{\pi}{9}$, et donc ce dernier est algébrique de degré 3 (qui n'est pas une puissance de 2) sur $\mathbb{Q}$.
Le Théorème 1.6 montre que cos $\frac{\pi}{9}$ n'est pas constructible et *a fortiori* $\frac{\pi}{3}$ n'est pas un angle trisectable.

Remarque. On pourra démontrer que :
Un angle θ est trisectable si et seulement si le polynôme $4X^3 - 3X - \cos\theta$ est réductible dans $\mathbb{Q}(\cos\theta)[X]$.

2.2 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. Si ceci était possible alors on pourrait construire un carré dont la longueur du côté serait $\sqrt{\pi}$. Or d'après le Théorème suivant, ceci n'est pas possible :

Théorème 2.4 (Lindemann 1882). *Les nombres π et $\sqrt{\pi}$ ne sont pas algébriques sur $\mathbb{Q}$ (donc non constructibles rendant la quadrature du cercle*

impossible).

2.3 Les polygones réguliers

Dans cette partie, le résultat le plus important est le suivant :

Théorème 3.1. *Soit n un entier supérieur ou égal à 3.*
Le polygone régulier à n côtés est constructible si et seulement si n est de la forme $n = 2^\alpha p_1 \cdots p_r$ avec $\alpha \geq 0, r \geq 0$, les p_i premiers, distincts et de la forme $2^{2^m} + 1$ (nombres de Fermat).

Remarque. Les seuls exemples de nombres de Fermat connus sont 3,5,17,257 et 65537.

Construction effective du pentagone

Dans le cas $n = 5 = 2^{2^1} + 1$, on peut en effet construire à la règle et au compas le pentagone car 5 vérifie les hypothèses du théorème précédent. Maintenant, pour réaliser une construction effective de ce polygone, on va utiliser la théorie de Galois afin de construire $\cos \frac{2\pi}{5}$. Si on note ζ qui vaut $e^{\frac{2i\pi}{5}}$, alors

$$\zeta^5 - 1 = (\zeta - 1)(1 + \zeta + \cdots + \zeta^4) = 0$$

. De plus, $\mathbb{Q}$ est inclus dans $\mathbb{Q}(\zeta)$ et $1+\zeta+\cdots+\zeta^4$ est irréductible et unitaire sur $\mathbb{Q}$ donc $[\mathbb{Q}(\zeta) : \mathbb{Q}\,]$ est égal à 4.
Par le Théorème 1.6 et le Théorème 1.7 , on en déduit qu'il existe une suite de sous-corps de $\mathbb{R}$:

$$\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2 = \mathbb{Q}(\zeta)$$

telle que chaque $i = 1, 2$,

$$[\mathbb{K}_i : \mathbb{K}_{i-1}] = 2.$$

Ensuite, on définit le groupe de Galois associé à l'extension $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ $G = Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ (l'ensemble des automorphismes de corps $\sigma : \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ tel que $\sigma_{|\mathbb{Q}} = \mathrm{Id}_{\mathbb{Q}}$). De plus, on peut montrer que le groupe de Galois G s'injecte dans $(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/4\mathbb{Z})$, mais ici ils sont isomorphes donc $\mathrm{card}(Gal(\mathbb{Q}(\zeta)/\mathbb{Q}))$est égal à 4.
En effet, si σ appartient à $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$, alors $\sigma(\zeta) = \zeta^{i_\sigma}$ où i_σ est tel que $pgcd(i_\sigma, n) = 1$. Ainsi, on a le lemme suivant :

Lemme 3.2.

$$\begin{aligned} \phi : Gal(\mathbb{Q}(\zeta/\mathbb{Q}) &\longrightarrow (\mathbb{Z}/n\mathbb{Z})^* \\ \sigma &\longmapsto i_\sigma \end{aligned}$$

est un homomorphisme.

Enfin, le Théorème fondamental 1.10 de Galois assure qu'il existe une bijection entre :

1. les extensions intermédiaires :

$$\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2 = \mathbb{Q}(\zeta). \tag{1}$$

2. les sous groupes de $G = Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$:

$$G_2 = (Id) \subset G_1 \subset G_0 = G$$

qui sont tels que pour chaque $i = 0, 1, 2$,

$$\text{card}(G_i) = 2^{2-i}, \tag{2}$$

$$\mathbb{K}_i = \mathbb{Q}(\zeta)^{G_i} = \{x \in \mathbb{Q}(\zeta) \text{ tel que } \forall g \in G_i, g(x) = x\} \tag{3}$$

et inversement,

$$G_i = Gal(\mathbb{Q}(\zeta)/\mathbb{K}_i) \tag{4}$$

Ainsi, il est toujours plus facile de trouver des sous-groupes que des extensions intermédiaires, là est tout l'intérêt du Théorème fondamental de Galois. Donc, il nous faut tout d'abord trouver des générateurs de $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \approx (\mathbb{Z}/4\mathbb{Z})$. Il est naturel d'essayer $\sigma_0 : \zeta \longmapsto \zeta^2$ et on se rend compte qu'il est bien d'ordre 4.
$\sigma_1 = \sigma_0^2 : \zeta \longmapsto \zeta^{-1}$ est donc d'ordre 2 et est générateur de G_1.
$\sigma_2 = \sigma_0^4 : \zeta \longmapsto \zeta$ est d'ordre 1 et est générateur de G_2.
Ainsi on remarque quelque chose qui va nous être utile dans la suite, à savoir : pour chaque $i = 1, 2$, si on note σ_i le générateur du groupe G_i, alors

$$\sigma_{i-1}^2 = \sigma_i. \tag{5}$$

Rappelons alors tout ce que nous savons :

$$\mathbb{Q} = \mathbb{K}_0 \overset{2}{\subset} \mathbb{K}_1 \overset{2}{\subset} \mathbb{K}_2 = \mathbb{Q}(\zeta).$$

$$\underbrace{G_2 = (Id)}_{=<\zeta \longmapsto \zeta>} \subset \underbrace{G_1}_{=<\zeta \longmapsto \zeta^{-1}>} \subset \underbrace{G_0 = G}_{=<\zeta \longmapsto \zeta^2>} .$$

Ainsi, notre but ici va être de rechercher des éléments appartenant à chacun des corps et grâce à la relation (1), on sait qu'on va atteindre un élément de $\mathbb{Q}$, qui lui, sera alors constructible. Pour réaliser cela, il nous suffira grâce à la relation (3), de trouver des éléments qui restent fixes par les générateurs de chacun des groupes. Pour construire de tels éléments, on utilisera le lemme suivant :

Lemme 3.3. *Pour chaque $i = 1, 2$, on note σ_i le générateur du groupe G_i. Supposons que σ_i fixe x. Si y est tel que $y = \sigma_{i-1}(x)$ alors $x + y$ et xy sont fixes par σ_{i-1}, et donc appartiennent à $\mathbb{K}_{i-1}$.*

Démonstration. Soient x et y comme dans le lemme ci-dessus. Alors :
$\sigma_{i-1}(x + y) = y + \sigma_{i-1}^2(x)$. Or d'après la relation (5), $\sigma_{i-1}^2 = \sigma_i$, d'où :

$$\begin{aligned} \sigma_{i-1}(x + y) &= y + \sigma_i(x) \\ &= y + x \end{aligned}$$

car σ_i fixe x. Ainsi $x+y$ appartient à $\mathbb{K}_{i-1}$. Comme σ_i pour tout $i = 1, \cdots, 4$ est un morphisme d'algèbre, il en est de même pour xy.

Posons $w_1 = \zeta$ qui est bien fixe par $\sigma_0^4 : \zeta \longmapsto \zeta$ (générateur du groupe G_2).
Ensuite, on pose $w_2 = \sigma_0^2(w_1)$. Alors, le lemme 3.3 affirme que :

$$\begin{aligned} z_1 &= w_1 + w_2 \\ &= \zeta + \zeta^{-1} \end{aligned}$$

est fixe par σ_0^2 (générateur du groupe G_1), et donc que z_1 appartient à $\mathbb{K}_1$.
Ensuite, on pose

$$\begin{aligned} z_2 &= \sigma_0(z_1) \\ &= \zeta^2 + \zeta^{-2}. \end{aligned}$$

De même :

$$\begin{aligned} y_1 &= z_1 + z_2 \\ &= \zeta + \zeta^{-1} + \zeta^2 + \zeta^{-2} \\ &= -1 \end{aligned}$$

est fixe par σ_0 (générateur du groupe G_0) et donc y_1 appartient à $\mathbb{K}_0 = \mathbb{Q}$. De même, le lemme 3.3 montre que :

$$\begin{aligned} y_3 &= z_1 z_2 \\ &= \zeta + \zeta^{-1} + \zeta^2 + \zeta^{-2} \\ &= -1 \end{aligned}$$

appartient à $\mathbb{K}_0 = \mathbb{Q}$.

Remarque. On sait par ailleurs, que z_1 et z_2 sont racines du polynôme du second degré à coefficients dans $\mathbb{Q}$:

$$P_0(X) = X^2 + X - 1$$

. **Conclusion** : On va réussir à construire $z_1 = 2\cos(\frac{2.\pi}{17})$ et donc le point d'abscisse $\cos(\frac{2.\pi}{17})$, le tout est de savoir construire les solutions d'une équation du second degré.

Méthode pour construire les solutions d'une équation du second degré.

Soient x_1 et x_2 tels que :

$$\begin{cases} x_1 + x_2 &= -b \\ x_1 x_2 &= c \end{cases}$$

avec $c \leq 0$. Pour construire ces deux points, il suffit de tracer le cercle Γ de centre $O(\frac{-b}{2}, \frac{1+c}{2})$ passant par les points (0,1) et (0,c). Alors x_1 et x_2 sont les deux points d'intersection du cercle avec l'axe des abscisses.

Démonstration. Cela vient de la proposition suivante :

Proposition 3.3 : Puissance d'un point par rapport à un cercle. *Soient M un point, Γ un cercle de centre O et de rayon R et (d) une droite passant par M et rencontrant le cercle en A et B. On appelle alors puissance du point M par rapport au cercle Γ le produit des mesures algébriques de MA et MB. Ce produit est indépendant de la droite choisie et vaut toujours* :

$$\overline{MA} \cdot \overline{MB} = MO^2 - R^2 = P_\Gamma(M).$$

Démonstration. Soit A' construit tel que $[AA']$ soit un diamètre de Γ. On écrit alors :

$$\begin{aligned}\overrightarrow{MA}.\overrightarrow{MB} &= \overrightarrow{MA}.\overrightarrow{MA'} \\ &= (\overrightarrow{MO}+\overrightarrow{OA}).(\overrightarrow{MO}+\overrightarrow{OA'}) \\ &= MO^2 - R^2.\end{aligned}$$

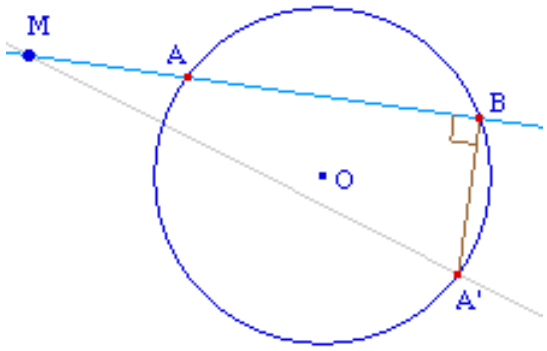

FIGURE 11

D'où $P_\Gamma(0) = x_1x_2 = 1.c$ (voir figure 12 avec $c = -3$ et $b = -4$)

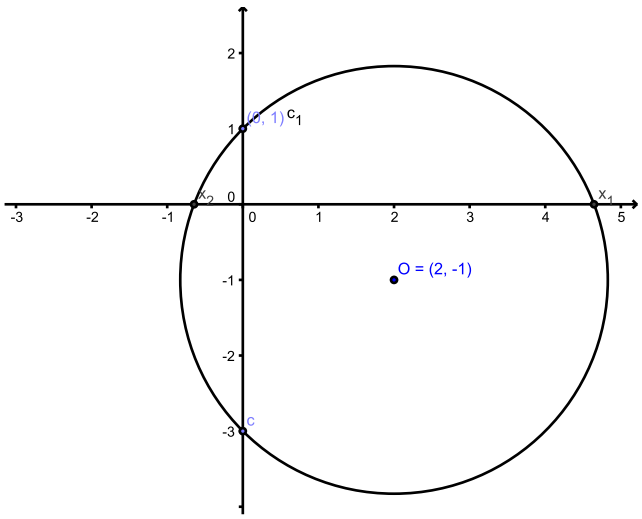

FIGURE 12

Ainsi, grâce à cette méthode on peut réaliser une construction du pentagone à la règle et au compas (voir figure 13).

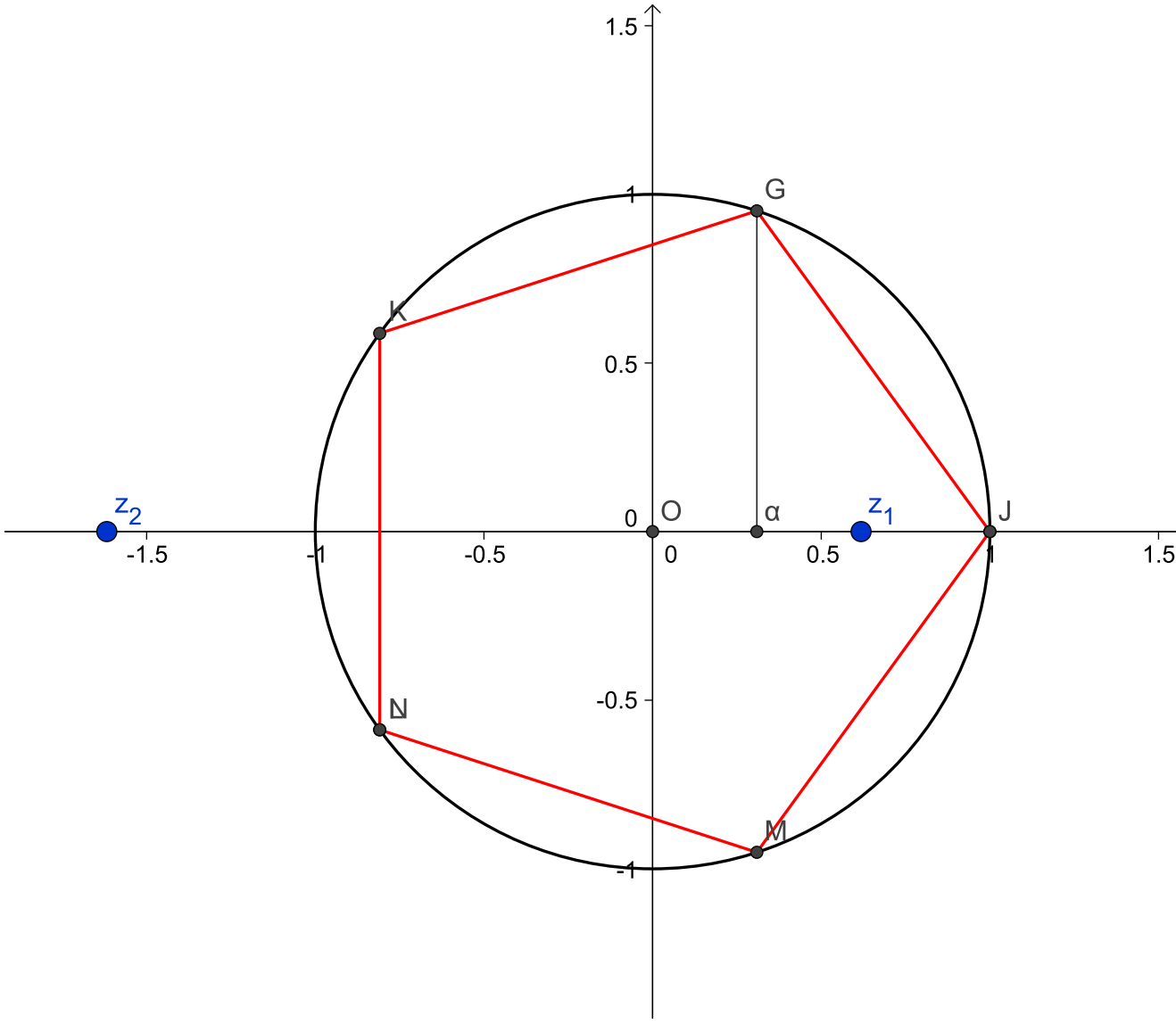

FIGURE 13

Construction effective du polygone à 17 côtés

De même, là aussi dans le cas $n = 17 = 2^{2^2} + 1$, on peut construire à la règle et au compas le polygone à 17 côtés car 17 vérifie les hypothèses du théorème précédent. Maintenant, pour réaliser une construction effective de ce polygone, on va utiliser la théorie de Galois afin de construire cos $\frac{2\pi}{17}$.
Si on note ζ qui vaut $e^{\frac{2i\pi}{17}}$, alors

$$\zeta^{17} - 1 = (\zeta - 1)(1 + \zeta + \cdots + \zeta^{16}) = 0$$

. De plus, $\mathbb{Q}$ est inclus dans $\mathbb{Q}(\zeta)$ et $1+\zeta+\cdots+\zeta^{16}$ est irréductible et unitaire sur $\mathbb{Q}$ donc $[\mathbb{Q}(\zeta) : \mathbb{Q}\ ]$ est égal à 16.
Par le Théorème 1.6 et le Théorème 1.7 , on en déduit qu'il existe une suite de sous-corps de $\mathbb{R}$:

$$\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \mathbb{K}_3 \subset \mathbb{K}_4 = \mathbb{Q}(\zeta)$$

telle que chaque $i = 0, 1, \cdots, 4$,

$$[\mathbb{K}_i : \mathbb{K}_{i-1}] = 2.$$

Ensuite, on définit le groupe de Galois associé à l'extension $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ $G = Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ (l'ensemble des automorphismes de corps $\sigma : \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ tel que $\sigma_{|\mathbb{Q}} = \mathrm{Id}_{\mathbb{Q}}$). De plus, d'après le lemme 3.2, $\mathrm{card}(Gal(\mathbb{Q}(\zeta)/\mathbb{Q}))$est égal à 16.
Enfin, le Théorème fondamental 1.10 de Galois assure qu'il existe une bijection entre :

1. les extensions intermédiaires :

$$\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \mathbb{K}_3 \subset \mathbb{K}_4 = \mathbb{Q}(\zeta). \tag{6}$$

2. les sous groupes de G=Gal$(\mathbb{Q}(\zeta)/\mathbb{Q})$:

$$G_4 = (Id) \subset G_3 \subset G_2 \subset G_1 \subset G_0 = G$$

qui sont tels que pour chaque $i = 0, 1, \cdots, 4$,

$$\mathrm{card}(G_i) = 2^{4-i}, \tag{7}$$

$$\mathbb{K}_i = \mathbb{Q}(\zeta)^{G_i} = \{x \in \mathbb{Q}(\zeta) \text{ tel que } \forall g \in G_i, g(x) = x\} \tag{8}$$

et inversement,

$$G_i = Gal(\mathbb{Q}(\zeta)/\mathbb{K}_i) \tag{9}$$

De même dans la construction du pentagone, il est toujours plus facile de trouver des sous-groupes que des extensions intermédiaires. Donc, il nous faut tout d'abord trouver des générateurs de $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \approx (\mathbb{Z}/16\mathbb{Z})$. Il est naturel d'essayer $\tau : \zeta \longmapsto \zeta^2$, mais on se rend compte très vite qu'il est seulement d'ordre 8.

Alors on essaie $\sigma_0 : \zeta \longmapsto \zeta^3$ et cette fois-ci cet élément est bien d'ordre 16.
$\sigma_1 = \sigma_0^2 : \zeta \longmapsto \zeta^{-8}$ est donc d'ordre 8 et est générateur de G_1.
$\sigma_2 = \sigma_0^4 : \zeta \longmapsto \zeta^{-4}$ est d'ordre 4 et est générateur de G_2.
$\sigma_3 = \sigma_0^8 : \zeta \longmapsto \zeta^{-1}$ est d'ordre 2 et est générateur de G_3.
$\sigma_4 = \sigma_0^{16} : \zeta \longmapsto \zeta$ est d'ordre 1 et est générateur de G_4.

Rappelons alors tout ce que nous savons :

$$\mathbb{Q} = \mathbb{K}_0 \overbrace{\subset}^{2} \mathbb{K}_1 \overbrace{\subset}^{2} \mathbb{K}_2 \overbrace{\subset}^{2} \mathbb{K}_3 \overbrace{\subset}^{2} \mathbb{K}_4 = \mathbb{Q}(\zeta).$$

$$\underbrace{G_4 = (Id)}_{=<\zeta\longmapsto\zeta>} \subset \underbrace{G_3}_{=<\zeta\longmapsto\zeta^{-1}>} \subset \underbrace{G_2}_{=<\zeta\longmapsto\zeta^{-4}>} \subset \underbrace{G_1}_{=<\zeta\longmapsto\zeta^{-8}>} \subset \underbrace{G_0 = G}_{=<\zeta\longmapsto\zeta^{3}>}.$$

On va là aussi rechercher des éléments appartenant à chacun des corps et grâce à la relation (6), on sait qu'on va atteindre un élément de $\mathbb{Q}$, qui lui, sera alors constructible. Pour réaliser cela, il nous suffira grâce à la relation (8), de trouver des éléments qui restent fixes par les générateurs de chacun des groupes. Pour construire de tels éléments, on utilisera le lemme 3.3.

Posons $w_1 = \zeta$ qui est bien fixe par $\sigma_0^{16} : \zeta \longmapsto \zeta$ (générateur du groupe G_4).
Ensuite, on pose $w_2 = \sigma_0^8(w_1)$. Alors, le lemme 3.3 affirme que :

$$\begin{aligned} z_1 &= w_1 + w_2 \\ &= \zeta + \zeta^{-1} \end{aligned}$$

est fixe par σ_0^8 (générateur du groupe G_3), et donc que z_1 appartient à $\mathbb{K}_3$.
Ensuite, on pose

$$\begin{aligned} z_2 &= \sigma_0^4(z_1) \\ &= \zeta^4 + \zeta^{-4}. \end{aligned}$$

De même :

$$\begin{aligned} y_1 &= z_1 + z_2 \\ &= \zeta + \zeta^{-1} + \zeta^4 + \zeta^{-4} \end{aligned}$$

est fixe par σ_0^4 (générateur du groupe G_2) et donc y_1 appartient à $\mathbb{K}_2$. De même, le lemme 3.3 montre que :

$$\begin{aligned} y_3 &= z_1 z_2 \\ &= \zeta^5 + \zeta^{-5} + \zeta^3 + \zeta^{-3} \end{aligned}$$

appartient à $\mathbb{K}_2$.

Remarques.

1. On sait par ailleurs, que z_1 et z_2 sont racines du polynôme du second degré à coefficients dans $\mathbb{K}_2$:

$$P_2(X) = X^2 - y_1 X + y_3$$

.

2. On vérifie que par le calcul que $\sigma_0(y_1) = y_3$.

On va réitérer ce processus jusqu'à atteindre des éléments de $\mathbb{Q}$. On pose :

$$\begin{aligned} y_2 &= \sigma_0^2(y_1) \\ &= \zeta^2 + \zeta^{-2} + \zeta^8 + \zeta^{-8}. \end{aligned}$$

Alors :

$$\begin{aligned} x_1 &= y_1 + y_2 \\ &= \zeta + \zeta^{-1} + \zeta^4 + \zeta^{-4} + \zeta^8 + \zeta^{-8} + \zeta^2 + \zeta^{-2} \end{aligned}$$

et $y_1 y_2 = \sum_{k=1}^{16} \zeta^k = -1$ sont fixes par σ_0^2 (générateur du groupe G_1) et appartiennent à $\mathbb{K}_1$.

Remarque. y_1 et y_2 sont racines du polynôme du second degré à coefficients dans $\mathbb{K}_2$:

$$P_1(X) = X^2 - x_1 X - 1$$

. Par ailleurs, on pose :

$$\begin{aligned} y_4 &= \sigma_0^2(y_3)(= \sigma_0(y_2)) \\ &= \zeta^6 + \zeta^{-6} + \zeta^7 + \zeta^{-7}. \end{aligned}$$

Ainsi,

$$\begin{aligned} x_2 &= y_3 + y_4 \\ &= \zeta^5 + \zeta^{-5} + \zeta^3 + \zeta^{-3} + \zeta^7 + \zeta^{-7} + \zeta^6 + \zeta^{-6}. \end{aligned}$$

et $y_3 y_4 = \sigma_0(y_1 y_2) = \sigma_0(-1) = -1$ sont fixes par σ_0^2 (générateur du groupe G_1) et appartiennent à $\mathbb{K}_1$.

Remarque. y_3 et y_4 sont racines du polynôme du second degré à coefficients dans $\mathbb{K}_1$:

$$P_{1\text{bis}}(X) = X^2 - x_2 X - 1$$

. Enfin, on note que :

$$\begin{aligned} x_2 &= \sigma_0(x_1) \\ &= \zeta^3 + \zeta^{-3} + \zeta^5 + \zeta^{-5} + \zeta^7 + \zeta^{-7} + \zeta^6 + \zeta^{-6} \end{aligned}$$

On en déduit alors que :

$$\begin{aligned} x_1 + x_2 &= \sum_{k=1}^{16} \zeta^k \\ &= -1 \end{aligned}$$

et $x_1 x_2 = r = \sum_{k=1}^{16} a_k \zeta^k (a_k \in \mathbb{N}^*)$ sont invariants par σ_0 (générateur du groupe G_0 et donc appartiennent à $\mathbb{K}_0 = \mathbb{Q}$.

Remarque. Pour trouver $r = x_1 x_2$, on procède de la façon suivante : on alors que $P(\zeta) = \sum_{k=1}^{16} a_k \zeta^k - r = 0$ est à coefficients dans $\mathbb{Q}$ et de degré 16. Or le polynôme minimal de ζ sur $\mathbb{Q}$ est $1 + \zeta + \cdots + \zeta^{16}$. Donc il existe λ tel que $\sum_{k=1}^{16} a_k \zeta^k - r = \lambda(1 + \zeta + \cdots + \zeta^{16})$. On a alors $r = -\lambda$ et il suffit donc par exemple de compter le nombre de termes en ζ dans le produit $x_1 x_2$. Il y en a 4, donc $r = x_1 x_2 = -4$.

D'où x_1 et x_2 sont racines du polynôme du second degré à coefficients dans $\mathbb{Q}$: $P_0(X) = X^2 + X - 4$, et donc sont constructibles par la proposition 1.3 et 1.5.

Conclusion : Grâce aux différentes relations, on peut remonter jusqu'à $z_1 = 2\cos(\frac{2\pi}{17})$ et construire pas à pas le point d'abscisse $\cos(\frac{2\pi}{17})$.
Tout d'abord, on construit x_1 et x_2 racines du polynôme $P_0(X) = X^2 + X - 4$ grâce à la méthode proposée précédemment pour construire les solutions d'une équation du second degré.

Ensuite, on construit y_1 et y_2 racines du polynôme $P_1(X) = X^2 - x_1X - 1$ ainsi que y_3 et y_4 racines du polynôme $P_{1\text{bis}}(X) = X^2 - x_2X - 1$.
Enfin, on construit z_1 et z_2 racines du polynôme $P_2(X) = X^2 - y_1X + y_3$.
Ainsi, on peut faire une construction effective du polygone à 17 côtés à la règle et au compas (voir figure 14).

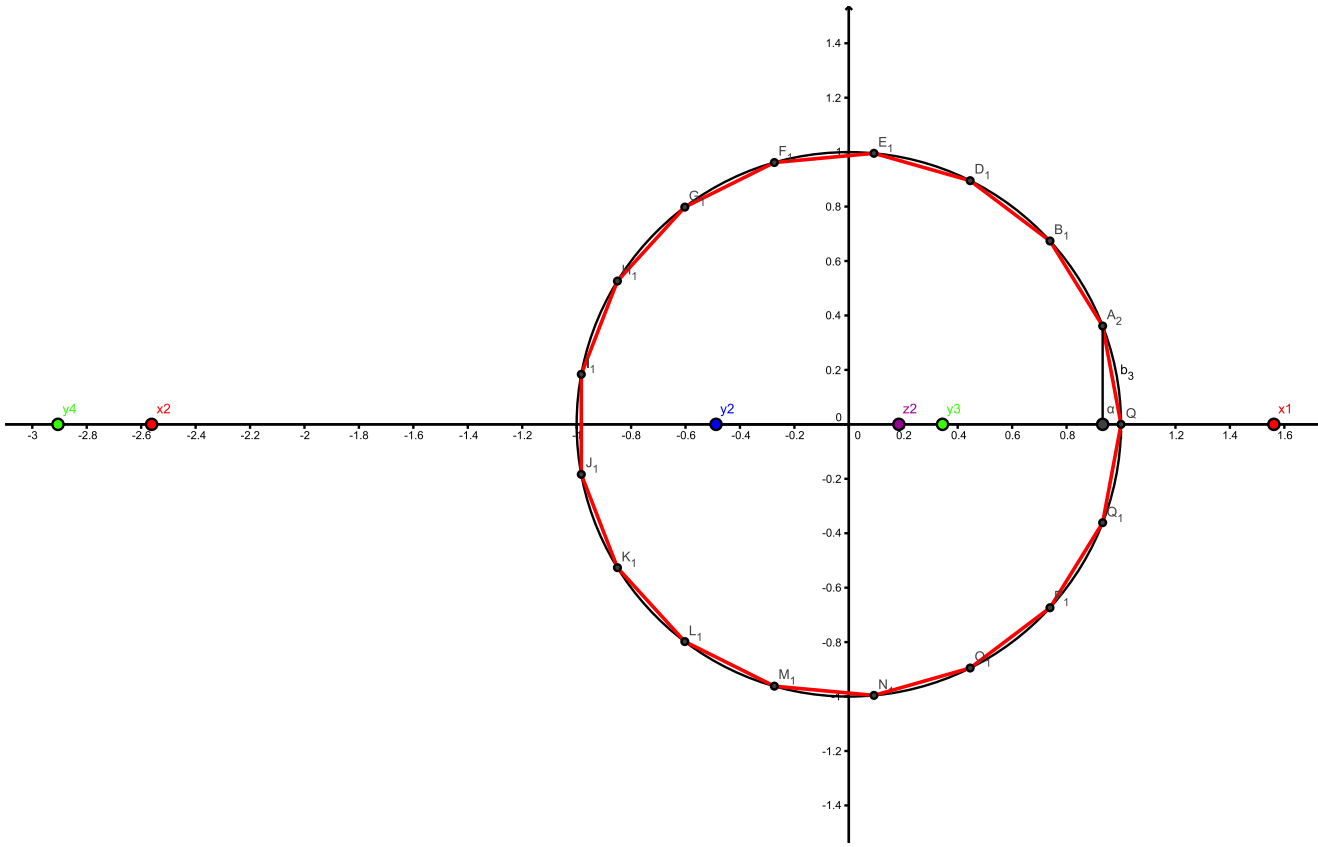

FIGURE 14