

Mémoire : Constructibilité des nombres à la règle et au compas,
promenade à travers des questions géométriques

Tatiana ORLOVIC

Juin 2020

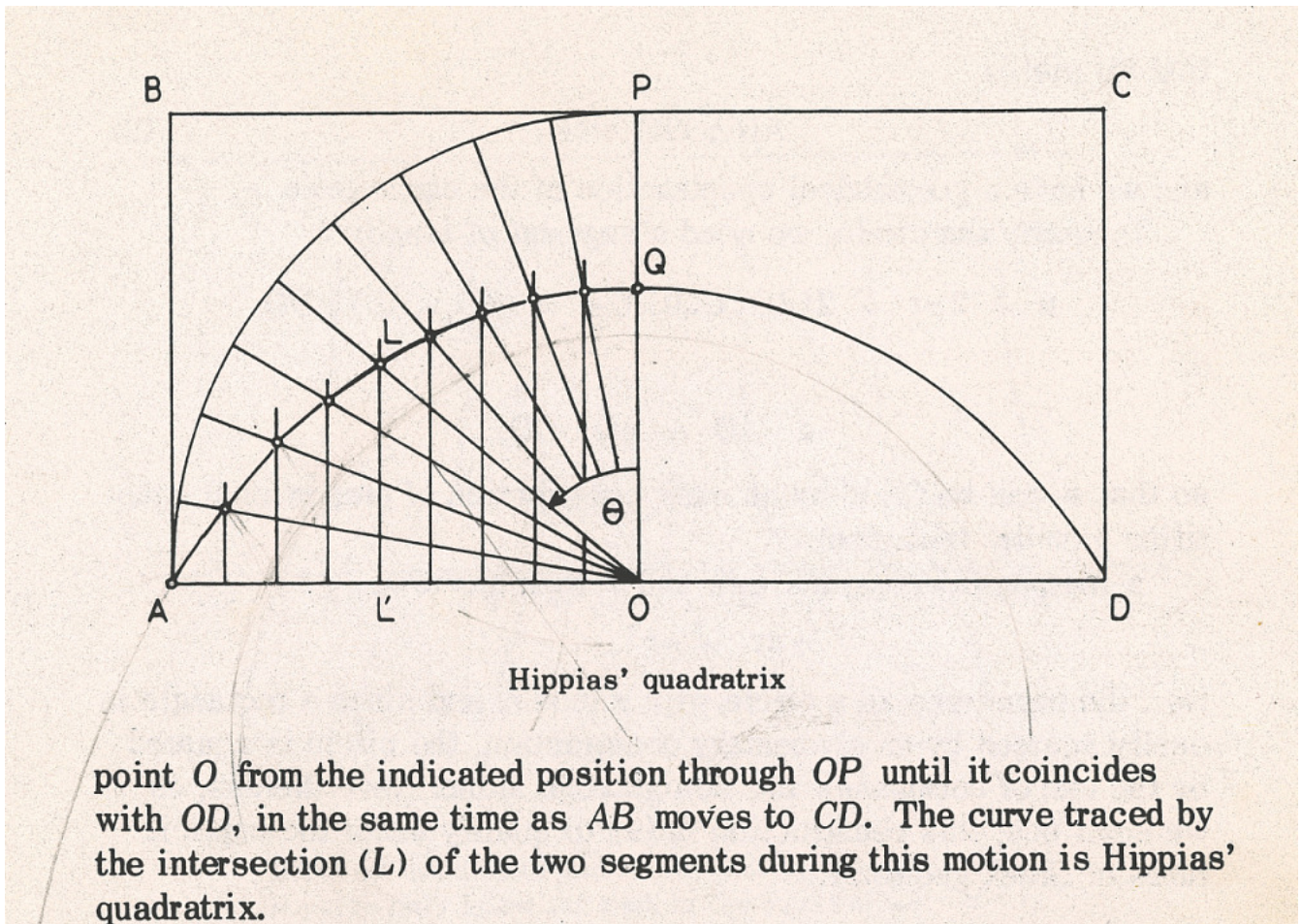


Table des matières

1	Partie 1 : Critères de constructibilité géométrique	4
1.1	Premières définitions	4
1.2	Addition et soustraction	5
1.3	Multiplication et division	6
1.4	Étendre le corps des constructibles avec $\sqrt{2}$	7
1.5	Passage à la racine : une opération non négligeable	7
2	Partie 2 : Constructible vs transcendant	8
2.1	Théorème de Wantzel : de la géométrie à l'algèbre	10
2.2	Transcendance de π et quadrature du cercle	13
3	Partie 3 : Les polygones réguliers	15
3.1	Le théorème de Wantzel-Gauss	16
3.2	Réflexion sur la construction du pentagone	20
3.3	Construction de l'heptadécagone : Poursuite des réflexions	22

Remerciements

Ce mémoire a été supervisé par Maxime Berger que j'aimerais remercier particulièrement. Très attentif sans être strict, il m'a laissé voguer à mon gré à travers mes très diverses questions. Me guidant toujours avec bienveillance et en m'aidant dans mes recherches d'articles, je peux dire qu'il a été très investi dans ce mémoire. C'est donc d'un vrai travail de coopération et d'équipe que ce mémoire s'est nourri ! Merci infiniment donc à Maxime pour sa patience et son investissement, cela aura été un réel plaisir et une grande chance de travailler sur ce projet commun. J'ai pris beaucoup de plaisir à découvrir deux domaines des mathématiques tout à fait inconnus pour moi. Je ne m'attendais pas à ressortir d'un mémoire de Mathématiques en aimant encore plus la discipline au départ, mais c'est le cas. J'espère que le plaisir ressenti à faire ce travail se ressentira dans la lecture de ce mémoire.

Merci également à Guillaume Vigerat et Jean-François Allemand. Peut-être plus indirectement mais tout de même très importants ! En plus de m'avoir guidée ces dernières années à propos de mes innombrables questions, vous m'avez aidée à orienter mon choix de sujet que je ne regrette pas du tout ! Ma gratitude dépasse largement le cadre de ce mémoire mais je tenais tout de même à en laisser une trace.

Introduction

Nous allons, à travers ce mémoire, explorer un lien entre Géométrie et Algèbre. Si l'on définit un nombre comme une coordonnée où une distance entre deux points du plan, comment construire des nombres à l'aide seule d'une règle et d'un compas ? Quels nombres construire ou non ? En combien d'étapes ? Peut-on estimer la complexité d'une construction ?

Pour pouvoir traiter ces questions, nous aurons besoin d'outils provenant de l'algèbre, notamment de Théorie des Corps. Nous allons considérer que les propriétés principales des corps et extensions de corps sont acquises pour nous concentrer directement sur le sujet qui nous intéresse. De plus, vous verrez que certaines parties très calculatoires ou techniques de quelques démonstrations seront admises. L'idée n'est pas de cacher des manques de compréhension, mais plutôt de ne pas alourdir ce mémoire de calculs lourds car ce n'est pas le but de la démarche. Nous ne chercherons pas à ré-écrire des calculs déjà très bien présentés dans d'autres travaux, mais plutôt d'en dégager les idées et les structures qui rendent ces preuves intéressantes. Des références vers des preuves complètes seront toujours données en bibliographies.

Bienvenue donc, dans une petite balade algebro-géométrique qui j'espère vous transcendera !

1 Partie 1 : Critères de constructibilité géométrique

1.1 Premières définitions

Nous commençons par définir notre mode de pensée. Nous considérerons qu'un nombre ici est vu comme la distance entre deux points. Nous pourrions également définir un sens au repère pour définir les nombres négatifs, mais ce ne sera un objet d'intérêt ici.

Si nous définissons deux points A et B, nous pouvons définir la distance entre ces deux points initiaux comme la distance unité. Nous pouvons alors tracer le cercle unité au compas de centre A et de rayon 1 passant par B. Nous pouvons également tracer un premier axe en traçant la droite passant par les points A et B.

Enfin, nous pouvons tracer la perpendiculaire à cet axe passant par le point A. Pour tracer une perpendiculaire, nous avons besoin de deux cercles de même rayons et de centres équidistants de A. Nous prenons donc B et C les points d'intersection de notre cercle et de l'axe. Tous deux sont à distance 1 de A. Puis nous traçons les cercles de centre B passant par C et inversement (donc de rayon 2). Nous prendrons les points d'intersection de ces deux cercles, la droite passant par ces deux points est la perpendiculaire recherchée, comme indiquée sur le schéma suivant :

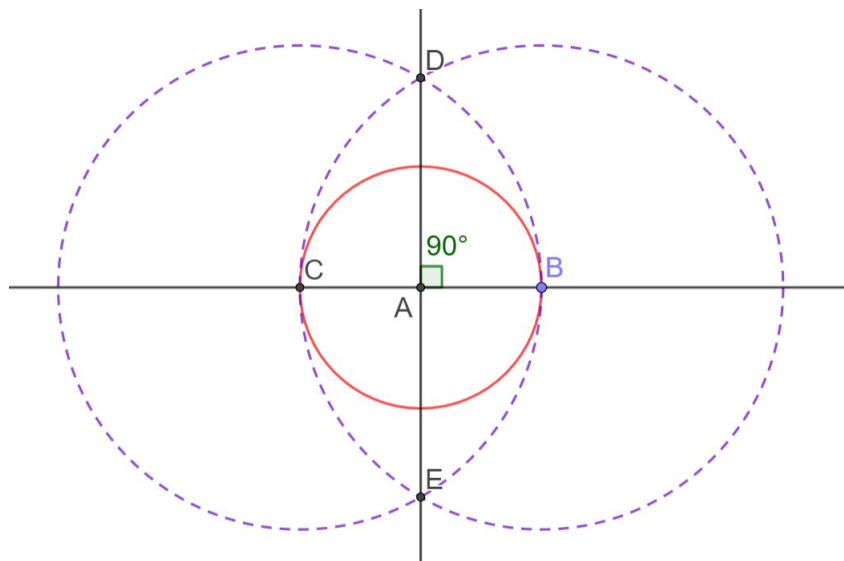


FIGURE 1 – Construction initiale : cercle unité et axes

Nous devons maintenant nous poser des questions plus précises. Qu'est-ce qu'un nombre constructible ? C'est une longueur entre deux points que l'on peut tracer par une suite d'intersections de droites et de cercles dans le plans.

Exemple 1. Prenons un premier exemple que nous reverrons dans la suite, $\sqrt{2}$ peut être vu géométriquement comme la diagonale du carré de côté 1. On peut également le voir comme la distance qui relie les points de coordonnées $(0,1)$ et $(1,0)$ que l'on construit à l'aide du cercle unité et des deux axes du plan.

Donnons maintenant la définition naturelle de la constructibilité.

Définition 2. *Nombre constructible, version géométrique*

Supposons que nos axes et le cercle unité soient construits, et que nous disposons déjà d'un nombre fini de points construits dans le plan. Un point du plan est dit constructible en une étape si il est intersection :

- de deux droites
- d'une droite et d'un cercle
- de deux cercles

Définition 3. *Nombre constructible en n étapes*

Un nombre, ou un point P du plan est dit constructible en n étapes si il existe une suite finie P_1, \dots, P_n de points du plan telle que $P_n = P$ et chaque P_i est constructible en une étape, à partir d'un ensemble de points déjà construits.

Remarque 4. Il n'y a pas unicité du procédé de construction. Il n'y a donc pas non plus unicité du nombre d'étapes pour construire un point dans le plan.

En se fondant sur ces définitions, quels sont les nombres que l'on peut construire ? Nous pouvons déjà nous douter que l'ensemble des nombres réels ne sera pas constructible. Plus loin, nous verrons même que l'ensemble des nombres constructibles est dénombrable.

1.2 Addition et soustraction

Comme vu précédemment, nous initialisons notre construction avec deux points de départ. A partir de ces deux points nous définissons le cercle unité et les axes du plan.

Puis, il suffit de reporter le cercle de rayon 1 sur chaque nouvelle unité qui intersecte l'axe, comme montré sur la figure 2 :

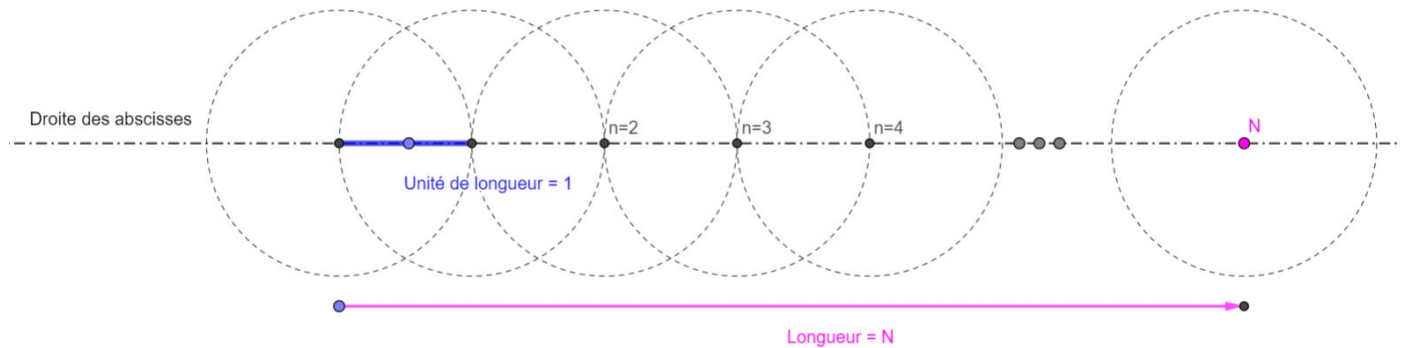


FIGURE 2 – Construction des entiers

Remarque 5. On peut également donner une orientation à notre graphe, ceci nous permet de définir $+1$ et -1 . Ainsi on peut construire \mathbb{Z} . On remarque alors que cet ensemble se construit par récurrence en ajoutant 1 ou en retirant 1 à l'étape $n-1$.

On utilise le même argument pour dire que \mathbb{Z} est un groupe engendré par l'élément 1.

Si l'on a deux nombres constructibles a et b , leur somme ainsi que leur différence est également constructible. La construction se fait en utilisant le cercle de centre b et de rayon a comme indiqué dans la figure 3.

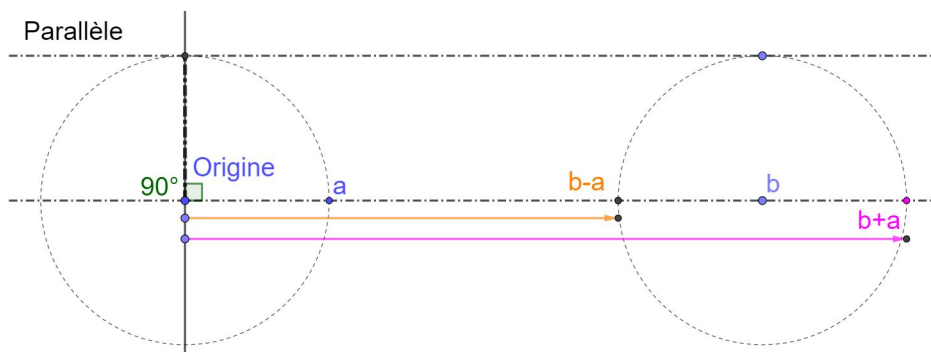
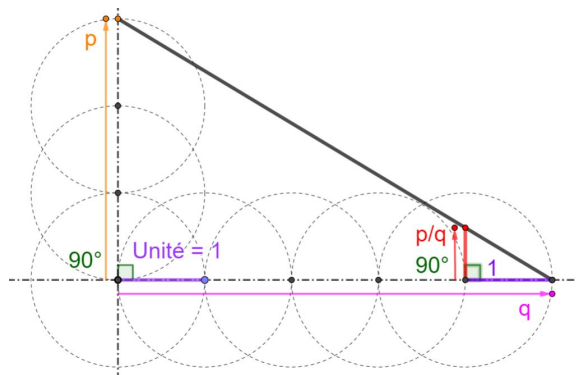


FIGURE 3 – Définition de la soustraction géométrique

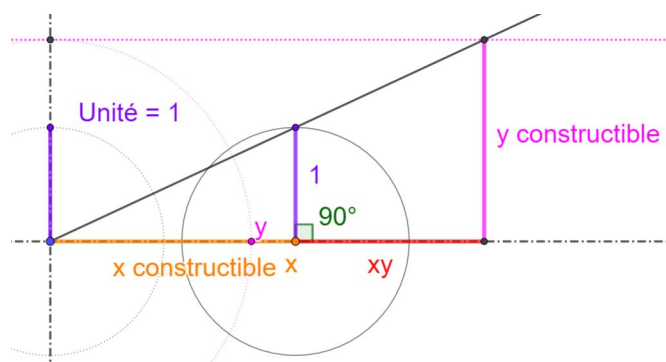
1.3 Multiplication et division

Les entiers sont donc construits. Pouvons-nous aller plus loin? Nous savons tracer la perpendiculaire à une droite, nous pouvons donc construire les deux axes du plan.

Grâce au Théorème de Thalès, en prenant un entier p sur l'axe des ordonnées, et un autre entier q sur l'axe des abscisses, nous pouvons construire p/q comme montré sur la Figure (a) :



(a) Construction du rationnel p/q



(b) Multiplication de deux nombres constructibles

Nous pouvons donc également construire l'ensemble des nombres rationnels. [7]

Le Théorème de Thalès nous permet aussi bien de diviser p et q que de les multiplier avec un autre arrangement qui est celui de la Figure (b).

Nous pouvons donc multiplier et diviser, additionner et soustraire tous les rationnels.

Nous reconnaissons alors une structure :

- on peut additionner de façon stable et commutative des nombres constructibles
- 0 est le neutre pour l'addition : On a un **groupe** abélien
- on peut multiplier et diviser de façon stable des constructibles : on a un **anneau**
- 1 est le neutre pour la multiplication : l'anneau est **unitaire**
- chaque élément constructible admet un opposé et un inverse pour la multiplication, excepté 0 : on a un **corps**

Remarque 6. Notons C l'ensemble des nombres constructibles. Nous remarquons que nous pouvons définir de façon équivalente :

- Les points constructibles dans le plan
- Les éléments constructibles dans \mathbb{C}
- En considérant la norme euclidienne : les nombres constructibles dans \mathbb{R}

On adaptera la définition en fonction du problème et de la construction, sans perte de généralité.

On peut donc maintenant définir l'ensemble des nombres constructibles à la règle et au compas.

Définition 7. *Le corps des constructibles C*

$$C := \{x \in \mathbb{R} : x = \|P\| \text{ ou } -\|P\| \text{ tel que } P \text{ est constructible}\}$$

Où constructible est entendu au sens de la première définition.

Cette définition est équivalente aux suivantes :

$$C := \{x = a + ib \in \mathbb{C} : a \text{ et } b \text{ sont constructibles}\}$$

$$C := \{x = (a, b) \in \mathbb{R}^2 : a \text{ et } b \text{ sont constructibles}\}$$

En utilisant toutes les propriétés précédemment démontrées, nous pouvons affirmer le théorème suivant :

Théorème 8. *L'ensemble des nombres constructibles C possède une structure de corps*

Pour l'instant, nous avons :

$$\mathbb{Q} \subset C$$

Peut-on aller plus loin dans l'explicitation de C ?

Nous allons utiliser la structure de corps de l'ensemble des nombres constructibles pour répondre à cette question. [4]

1.4 Étendre le corps des constructibles avec $\sqrt{2}$

Nous l'avons vu dans le premier exemple, $\sqrt{2}$ est constructible comme la diagonale du carré de côté 1.

En sommant deux longueurs, on peut construire $a + \sqrt{2}$, avec a dans C

On peut aussi effectuer une multiplication et construire $b\sqrt{2}$, avec b dans C

Alors, le nombre $x = a + b\sqrt{2}$ est constructible pour tout (a, b) dans C^2

Nous pouvons donc étendre le corps des constructibles à l'espace vectoriel défini par :

$$\{a + b\sqrt{2} : (a, b) \in C\}$$

Cet espace vectoriel est simplement la définition de l'extension quadratique $\mathbb{Q}[\sqrt{2}]$ du corps \mathbb{Q}

Ce qui revient à dire qu'en l'état actuel de notre analyse, nous avons :

$$\mathbb{Q}[\sqrt{2}] \subset C$$

Remarque 9. *nous avons étendu notre corps des constructibles grâce à une racine. Il se trouve que toute racine d'un point constructible l'est également. Ce résultat nous est donné par le Théorème de Pythagore, mais nous le verrons en détail plus loin.*

1.5 Passage à la racine : une opération non négligeable

Dans un cadre de géométrie euclidienne (celui dans lequel nous nous plaçons depuis le début), pour construire des nouveaux nombres nous avons à notre disposition deux outils très puissants :

- Le Théorème de Thalès : qui nous permet de multiplier et diviser

— Le Théorème de Pythagore : qui nous permet de passer à la racine

Proposition 10. : *Equivalence des constructibilités* Soit $x \in \mathbb{R}$ alors :

$$x \text{ est constructible} \iff \sqrt{x} \text{ est constructible}$$

Démonstration. **Démonstration Géométrique**

Nous allons procéder par double implication :

— \Rightarrow

Le sens direct est donné par le Théorème de Pythagore. En effet, on a :

$$\forall x \in \mathbb{R}, \left(\frac{x-1}{2}\right)^2 + (\sqrt{x})^2 = \left(\frac{x+1}{2}\right)^2$$

Donc en isolant \sqrt{x} , on peut le construire à partir de x qui est constructible. La construction géométrique est donnée sur le schéma sous la démonstration.

— \Leftarrow

La réciproque nous est donnée par le théorème de Thalès. Comme nous l'avons vu précédemment, ce théorème nous permet non seulement de construire \mathbb{Q} , mais il nous permet également de multiplier deux constructibles. Donc si \sqrt{x} est constructible, nous pouvons construire $\sqrt{x} \times \sqrt{x}$.

C'est à dire que x est constructible

□

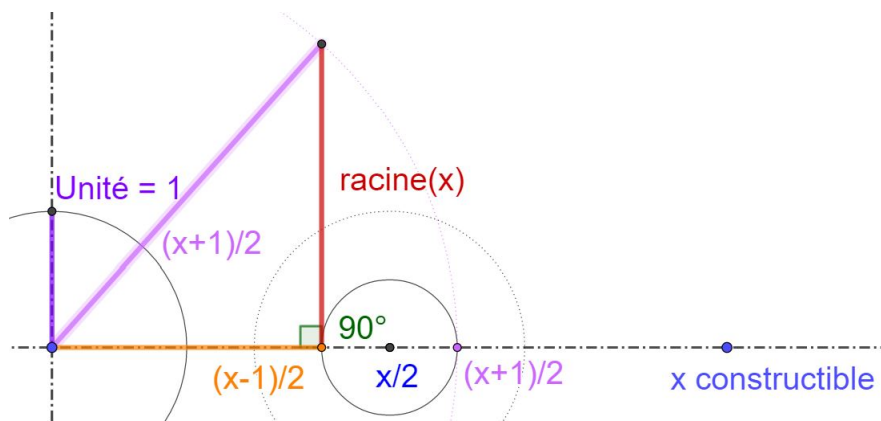


FIGURE 5 – Construction de la racine par le Théorème de Pythagore

Remarque 11. *Il semblerait que la racine ait un rôle important, que nous allons essayer de creuser un peu plus.*

Nous pouvons donc chercher à étendre l'ensemble des constructibles petit à petit comme nous l'avons fait dans les 3 derniers paragraphes. Mais la structure de corps que nous nous sommes efforcés de trouver et de construire va nous permettre de nous éloigner de la géométrie pour nous concentrer sur des critères algébriques de constructibilité. C'est justement l'objet de la partie suivante.

2 Partie 2 : Constructible vs transcendant

Nous entrons ici dans la partie "historique" et par conséquent très classique de ce mémoire. En effet, il y a maintenant plusieurs milliers d'années, les Grecs se posaient des questions de géométries, résolues

bien plus tard avec les outils algébriques que nous allons présenter. Mais quelles sont donc ces questions brûlantes qui ont tant posé problème aux mathématiciens ?

- **La quadrature du cercle** : Peut-on construire un carré de la même aire que le cercle ? Cercle question revient à se demander si l'on peut construire la longueur π avec une règle et un compas. Cette question peut nous sembler inutile, futile aujourd'hui, mais elle a tout de même mis plus de 2000 ans à être résolue. Posée d'abord en Egypte, puis formalisée par les grecs, les tentatives de quadratures du cercles sont apparues pour des histoires de motifs de "pavages" notamment. Il y a eu plusieurs phases d'engouement pour cette question. Le siècle des Lumières a été particulièrement marqué par un flot "d'amateurs" qui ont essayé de s'attaquer à cette question. Il était dans la conscience commune qu'il y aurait un grand prix à quiconque résolverait le problème de la quadrature du cercle. Ceci était faux mais il y eut un tel flot de "preuves" que l'Académie des Sciences refusa de les accepter. Si bien que même la preuve de Lindemann que nous verrons plus tard mit beaucoup de temps avant d'être validée.
- **La trisection de l'angle** : Peut-on diviser un angle en trois parts égales à l'aide seulement de la règle et du compas ?
- **duplication du cube** : Peut-on construire à partir d'un carré, un second carré d'aire double ? ou doubler le volume d'un cube ?

Ces questions ont été abordées par un nombre incalculable de personnes à travers l'histoire. Non seulement des mathématiciens, mais également des constructeurs, des artistes, des philosophes se sont emparés du sujet ! Certes, la question pouvait se trouver dénaturée du propos initial. Toujours est-il que le nombre π fascine depuis longtemps. Les questions géométriques sont partout, dans les mosaïques, les bâtiments religieux, les partitions des terres... Sans oublier tout le chemin qui a été fait pour arriver jusqu'à ces lignes, nous allons ici aborder les raisonnements modernes qui ont permis de conclure sur cette question. Attention spoilers ! Il se trouve que la règle et le compas seuls ne permettent pas de faire ces opérations. C'est désolant, mais pour compenser un peu la frustration, nous allons essayer de comprendre pourquoi la première opération est impossible.

Vous l'aurez compris, la Géométrie des Grecs Anciens ne suffit plus ! Heureusement, l'algèbre moderne arrive à notre rescousse. Elle va nous permettre en premier lieu de définir un critère de constructibilité beaucoup plus agréable à manipuler que de trouver toutes les constructions de tous les nombres possibles. Penchons-nous maintenant sur une approche algébrique de la constructibilité.

Premièrement, nous allons redéfinir certaines notions de théorie des corps. Ces caractérisations des nombres sont très importantes dans notre cadre et il est primordial de les avoir en tête.

Définition 12. *Nombre Algébrique*

Soient K un corps et a dans L/K une extension quelconque de ce corps K .

On dit que a est algébrique sur K si il est racine d'un polynôme P où $P \in K[x]$.

C'est à dire que a est racine d'un polynôme à coefficients dans K

Définition 13. *Nombre Transcendant*

Sous les mêmes hypothèses, on dit que a est transcendant sur K si il n'est racine d'aucun polynôme à coefficients dans K

Définition 14. *Polynôme minimal*

On définit maintenant le polynôme minimal d'un nombre a sur K comme le polynôme à coefficients dans K de plus petit degré annulant a .

Nous pourrions ici nous demander, pourquoi toutes ces définitions ? Souvenons-nous de la définition précédente d'un nombre constructible en n étapes ? Il existe une suite finie de points (donc de droites et de cercles) qui permet de construire une distance spécifique qu'est le nombre recherché. Nous allons essayer de lier cette définition à des notions algébriques. Nous allons voir dans la partie suivante que les polynômes

minimaux des nombres algébriques sont assez spéciaux. Les notions d'algebraicité et de transcendance vont nous permettre de distinguer algébriquement les nombres qui sont constructibles ou non. [2]

2.1 Théorème de Wantzel : de la géométrie à l'algèbre

Théorème 15. Théorème de Wantzel

Soit x un nombre réel ou complexe, ou un point du plan.

Alors x est constructible si et seulement si il existe une suite finie de corps $K_0 = \mathbb{Q} \subset K_1 \cdots \subset K_n \subset \mathbb{R}$ telle que :

- Cette suite soit croissante au sens de l'inclusion
- Pour chaque i , $[K_{i+1} : K_i] = 2$
- $x \in K_n$

Démonstration. La démonstration de ce théorème se fait par récurrence. Le plus important est de comprendre où interviennent les extensions de corps pour une construction qui se fait en une étape. C'est donc par là que nous allons commencer.

En effet, nous avons vu précédemment que si un point P est constructible en une étape, c'est qu'il est à l'intersection de deux droites, d'une droite et d'un cercle ou de deux cercles. Nous allons traiter ces cas séparément, On note le point $P := (x, y)$:

- Intersection de deux droites

En utilisant la définition d'une équation de droite, on a que (x, y) satisfait le système suivant :

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

Où $(a, b, c, a', b', c') \in K_{n-1}$ en utilisant l'hypothèse de récurrence où K_{n-1} est le corps des nombres constructibles construits à l'étape $n-1$.

On peut donc voir la contrainte ci-dessus comme le système d'équation :

$$AP + B = 0 \quad \text{avec} \quad A = \begin{pmatrix} a & b \\ a' & b' \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} c \\ c' \end{pmatrix}$$

Comme ces deux droites s'intersectent en P , c'est qu'elles ne sont pas parallèles, donc $\det(A) \neq 0$. Ce système est donc un système de Cramer.

On peut exprimer x et y en fonction de (a, b, c, a', b', c') qui sont des éléments de notre corps des constructibles actuel K , donc $(x, y) \in K^2$. Notre point est constructible en restant dans le corps K

- Intersection cercle-droite

Dans le cas de l'intersection entre un cercle et une droite, notre point satisfait le système suivant :

$$\begin{cases} ax + by + c = 0 \\ x^2 + y^2 + a'x + b'y + c' = 0 \end{cases}$$

Avec les mêmes hypothèses sur les constantes.

Dans le cas où $a \neq 0$, on peut exprimer x en fonction de y comme : $x = -\frac{by+c}{a}$

On peut alors remplacer cette expression de x dans la seconde équation, Puis en développant on obtient le trinôme du second degré suivant :

$$\left(1 + \left(\frac{b}{a}\right)^2\right)y^2 + \left(b' - \frac{a'b}{a} + \frac{2bc}{a^2}\right)y + \left(\left(\frac{c}{a}\right)^2 + c' - \frac{a'c}{a}\right) = 0$$

On remarque que le terme devant y^2 est strictement positif, donc on peut diviser l'équation par ce terme que l'on appellera α , on notera β et γ les deux autres combinaisons linéaires qui apparaissent dans le trinôme. Obtient donc :

$$P(y) := y^2 + \frac{\beta}{\alpha}y + \frac{\gamma}{\alpha} = 0$$

Qui est polynôme de degré 2 de $K[x]$.

-**Si P est réductible**, y est dans le corps constructible K et x également.

-**Si P est irréductible**, alors y est dans une extension algébrique du corps K que l'on notera $K[y]$, de plus, cette extension est quadratique.

Nous observons que la famille $(1, y)$ est génératrice de l'extension car en prenant S dans $K[X]$ tel que $S = PQ + R$ (par division euclidienne), on a que $S(y) = R(y)$, où $\deg(R) \leq 2$, donc $S(y)$ est bien une combinaison linéaire de y et d'éléments de K .

De plus, cette famille est libre, car autrement, on aurait que y est annulé par un polynôme non nul de degré 1, ce qui entrerait en contradiction avec le fait que P est irréductible et donc le polynôme minimal de y .

Donc nous avons bien une extension de corps de degré 2, c'est à dire que :

$$[K[y] : K] = 2$$

Si $a = 0$, on utilise le fait que $b \neq 0$ et on effectue un raisonnement analogue pour avoir le même résultat.

- Intersection cercle-cercle

Dans le dernier cas où P est à l'intersection entre deux cercles, il satisfait le système :

$$\begin{cases} x^2 + y^2 + ax + by + c = 0 \\ x^2 + y^2 + a'x + b'y + c' = 0 \end{cases}$$

Que l'on peut ramener, en soustrayant les deux lignes à :

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

Nous retrouvons l'intersection entre une droite et un cercle, et que l'on peut donc traiter de la même façon que le cas précédent.

Voici donc comment surviennent les extensions quadratiques de corps dans la construction de nouveaux points !

Naturellement, on a que $K \subset K[X]$

Procédons maintenant à la récurrence :

- Pour $n = 0$, c'est à dire $X \in K = \mathbb{Q}$, Il est évident que x est constructible.
- On suppose que pour tout point constructible à partir de \mathbb{Q} en n étapes, la propriété est vraie. Si on prend un point X constructible en $n + 1$ étapes, c'est qu'il existe une suite de $n + 1$ points $(P_i)_{1 \leq i \leq n+1}$ constructibles telle que $P_{n+1} = X$
Alors, P_n est constructible en n étapes et $P_n \in K_n$ par hypothèse de récurrence.
Donc, $P_n + 1$ est constructible en 1 étape à partir de K_n .

Sans refaire la preuve de pourquoi nous sommes dans une extension du corps, nous pouvons remarquer que y est algébrique sur K , et que dans ce cas, une extension de corps peut être vue comme l'espace vectoriel engendré par K et y .

Nous avons vu précédemment que : - Soit $P_n + 1$ est dans K_n , alors $K_n = K_{n+1}$ et la propriété est vérifiée pour X - Soit il est dans une extension quadratique de K_n , alors $K_{n+1} = K_n[P_{n+1}]$ et la propriété est encore vérifiée.

- En vertu du principe de récurrence, on a bien que tout point est constructible si il existe une suite croissante finie de corps telle que $[K_{i+1} : K_i] = 2$, et telle que le point voulu appartienne au dernier corps.

Ceci conclut cette (longue mais cruciale) preuve □

Remarque 16. Une conséquence très intéressante du théorème de Wantzel est que, si un nombre est constructible, alors **le degré de son polynôme minimal sur \mathbb{Q} est une puissance de deux.** Ce résultat se démontre par récurrence en utilisant le fait que toutes nos extensions de corps sont quadratiques et en utilisant la multiplicativité des degrés des extensions.

Nous avons désormais un critère clair de constructibilité! Si nous pouvons exprimer le polynôme minimal d'un nombre, nous savons directement s'il est constructible où non à partir de son degré! De plus, le fait que le polynôme minimal d'un nombre constructible soit une puissance de deux nous permet de percevoir une seconde conséquence de ce théorème peut être énoncée comme suit :

Proposition 17. *Étendre l'ensemble des constructibles avec une extension de corps quadratique correspond à la construction d'une racine en géométrie.*

Démonstration. On note le corps des constructibles actuel en n étapes de notre construction K Reprenons la preuve du Théorème de Wantzel, nous sommes arrivés à la conclusion qu'il y a extension de corps si et seulement si le polynôme suivant est irréductible :

$$P(y) := y^2 + \frac{\beta}{\alpha}y + \frac{\gamma}{\alpha} = 0$$

Où α , β et γ reprennent les mêmes expressions que dans la preuve précédente.

Si ce polynôme est irréductible, c'est que son déterminant Δ est strictement positif. Alors, il existe deux solutions distinctes de l'équation qui font intervenir $\sqrt{\Delta}$, qui est le seul élément n'appartenant pas au corps initial K

C'est donc bien l'apparition d'une racine qui permet de sortir du corps initial et de l'étendre quadratiquement. □

A partir de toutes ces considérations de constructibilité, nous aimerions ici poser un nouveau propos. En effet, une de nos grande question durant nos recherches à été d'essayer de comprendre mathématiquement ce que représente la complexité d'une construction. Si $\sqrt{2}$ est facile à construire, $\sqrt{\sqrt{\sqrt{2}}}$ l'est beaucoup moins et demande même une construction par récurrence. Construire un carré est également plus simple qu'un polygone à 128 côtés!

Mais comme nous l'avons précisé dans une remarque précédente, les chemins pour arriver à un nombre sont multiples! Comment alors pourrions nous hiérarchiser les constructions? Nous allons ici présenter une première idée, qui pourrait être le début de nouvelles considérations sur les constructions géométriques.

Remarque 18. Complexité d'une construction

Nous voudrions définir ici la "complexité" d'une construction géométrique. Nous pourrions imaginer que les véritables opérations importantes sont celles qui consistent à transporter notre construction actuelle dans un corps encore plus grand.

Cette opération consiste à construire une nouvelle racine, par le théorème de Pythagore ou un cercle de Carlyle comme nous le verrons plus tard.

Nous introduirons donc une notion de "coût" et de hiérarchie dans les opérations. Tracer une droite ne coûte rien. Un cercle non plus si il représente une addition ou une multiplication.

En revanche, tracer un cercle qui étend le corps des constructibles, ou procéder à un théorème de Pythagore sont des opérations qui nous font basculer dans une extension quadratique du corps précédent. On considérera donc que ces opérations coûtent 1.

Ces considérations reviennent à compter le nombre d'extensions nécessaires pour arriver jusqu'au nombre voulu. Plus il faut d'extensions, plus la construction est complexe. Nous allons donc dorénavant exprimer la complexité d'une construction au nombre de racines qu'il faut construire.

Nous remarquerons aussi qu'il est cohérent de ne considérer que ces opérations, car les chemins pour arriver à un nombre sans sortir du corps initial sont multiples. Il n'y a donc pas d'intérêt à chercher une construction "optimale" dans ce sens. En revanche, les opérations qui étendent le corps sont nécessaires et finies. Elles sont donc un bon indicateur de la complexité d'une construction de par leur "invariance".

2.2 Transcendance de π et quadrature du cercle

Le théorème et la preuve que nous allons présenter maintenant sont la raison historique de ce mémoire. Le problème posé est le suivant :

Peut-on construire un carré qui soit de même aire que le cercle unité ?

C'est à dire, peut-on construire un carré de longueur $\sqrt{\pi}$? Comme nous l'avons vu précédemment, il est équivalent de se demander si π est constructible.

La réponse à cette question est négative. En effet, π n'est racine d'aucun polynôme à coefficients dans \mathbb{Q} , il n'existe pas non plus de suite finie d'extensions de corps permettant d'arriver à π . Autrement dit, π est un nombre transcendant et nous allons le montrer.

Théorème 19. π est un nombre transcendant.

Démonstration. Cette preuve est une preuve par l'absurde. Nous allons la décortiquer en plusieurs étapes.

- Etape 1 : remplacement du problème.

Soit γ un nombre réel algébrique. γ est racine d'un polynôme à coefficients entiers :

$$\phi(z) = a_n z^n + a_{n-1} z^{n-1} + \dots + a_0$$

Tel que $a_n \neq 0$ et $n \geq 1$.

On admettra pour éviter des calculs peu utiles les résultats suivants :

- Si γ est algébrique, $i\gamma$ est également algébrique.

- Si z est algébrique sur \mathbb{Q} , alors il existe un entier c tel que cz est algébrique sur \mathbb{Z} . En l'occurrence, $a_n z$ est un entier algébrique.

Donc si π est algébrique, pour un certain c , $ci\pi$ est algébrique et on a $\phi(ci\pi) = 0$ où ϕ est un polynôme canonique, c'est à dire à coefficients entiers et unitaire.

Si on note maintenant $c\beta_1, \dots, c\beta_n$ les racines de ce polynôme, il y en a bien une telle que $\beta_q = i\pi$,

donc on peut appliquer la très fameuse formule d'Euler :

$$1 + e^{i\pi} = 0$$

De la même manière on a donc :

$$\prod_{i=0}^n (1 + e^{\beta_i}) = 0$$

En développant ce produit, on obtient une somme de 1 et de produits d'exponentielles, c'est à dire des exponentielles de sommes de β_i . Si on note $\alpha_1, \dots, \alpha_s$ toutes les sommes non nulles de nombres pris parmi les β_i et que l'on regroupe les 1, on obtient une équation de la forme :

$$k + e^{\alpha_1} + \dots + e^{\alpha_s} = 0 \quad (1)$$

En utilisant les propriétés des polynômes et des familles symétriques, on remarque que montrer que les $c\beta_i$ sont racines d'un polynôme canonique est équivalent à montrer que les $c\alpha_i$ sont racines d'un polynôme canonique.

$$\Lambda(x) = (x - c\alpha_1) \cdots (x - c\alpha_s)$$

- Étape 2 : Mettre en place une égalité qui s'avèrera impossible

On considère maintenant le polynôme :

$$P(x) = \frac{x^{p-1}}{(p-1)!} (\Lambda(cx))^p$$

Où p est un nombre premier quelconque. Ce polynôme est de degré $ps + p - 1$

On pose maintenant un autre (oui encore) polynôme :

$$Q_P(x) = P(x) + P'(x) + \dots + P^{(ps+p-1)}(x)$$

$Q_P(0)$ multiplié par l'égalité (1) nous donne l'équation suivante :

$$kQ_P(0) + \sum_{j=1}^s e^{\alpha_j} Q_P(0) = 0$$

Écartons-nous de ce calcul un moment pour ré-exprimer certains termes. Nous avons, par définition de Q_P (même si ce n'est pas immédiat pour s'en convaincre on en conviendra) que :

$$Q_P(\alpha) + e^\alpha \int_0^1 \alpha e^{-\alpha x} P(\alpha x) dx = Q_P(0)e^\alpha$$

On pose donc enfin $R_P(\alpha) = \alpha e^\alpha \int_0^1 \alpha e^{-\alpha x} P(\alpha x) dx$, et on a finalement l'égalité suivante :

$$Q_P(\alpha) + R_P(\alpha) = Q_P(0)e^\alpha$$

Donc en revenant à notre calcul, on obtient finalement cette égalité qui nous mènera à une absurdité.

$$kQ_P(0) + \sum_{j=1}^s Q_P(\alpha_j) = - \sum_{j=1}^s R_P(\alpha_j) \quad (2)$$

A partir de cette égalité, il reste encore deux étapes calculatoires que nous ne ferons pas mais nous allons tout de même expliquer l'idée de l'absurdité.

- Etape 3 : Montrer que le membre de gauche est un entier non nul.

Cette propriété est en fait une question d'intégrale. En utilisant la forme spécifique de P , on peut le décomposer en entiers divisibles par l'entier premier p , et par un autre entier non divisible par p . La somme des deux donne donc un entier non nul.

- Etape 4 : Montrer que le membre de droite tend vers 0.

Cette étape consiste à majorer l'intégrale que définit R_P . On obtient une majoration en $\frac{1}{(p-1)!}$, et comme p est un nombre premier arbitraire, on peut le rendre aussi grand que l'on veut, on peut donc faire tendre ce deuxième membre vers 0.

On obtient donc bien une contradiction, on remonte donc jusqu'à notre hypothèse qui était que π est racine d'un polynôme à coefficients dans \mathbb{Q} . C'est donc que ce n'est pas le cas et on obtient bien la transcendance de π .

[3][5]

□

Avant de passer à la partie suivante, nous aimerions ici faire un petit point "anecdotique". Durant nos recherches, nous nous sommes posés de nombreuses questions sur la transcendance. En effet, en plus d'avoir une appellation pour le moins interpellatrice, les nombres transcendants représentent un véritable mystère. Toutes les preuves de transcendances sont très complexes, très calculatoires et résultent souvent d'une suite "d'astuces" très particulières. Nous n'avons pas su en dégager d'idée générale sur la transcendance à notre niveau.

Nous nous sommes donc tournés vers Michel Waldschmidt, un mathématicien français "expert" de la transcendance. Très agréable, il nous a renvoyé une bibliographie assez complète pour nous aider à approfondir nos questions. Après la lecture de plusieurs articles, il se trouve en effet les études sur la transcendance sont extrêmement complexes et rapidement hors de notre portée. La vue "d'espaces multizetas de Riemann" dans un article peut être particulièrement déstabilisante.

Les preuves et quelques théorèmes que nous avons approchés étaient si calculatoires que nous nous sommes détournés de ces questions de transcendance, pour mieux retourner vers la géométrie!

3 Partie 3 : Les polygones réguliers

Un autre problème très classique dans le cadre de la constructibilité, est l'étude des polygones réguliers. L'étude des polygones est notamment importante car historiquement, c'est ce qui a permis d'approcher numériquement la valeur de π en augmentant le nombre de cotés, et donc en se rapprochant du périmètre du cercle. Nous allons nous y intéresser car ces polygones permettent de nous axer sur les structures que nous allons mettre au jour ici en connaissant déjà le nombre à construire. De plus, le fait que le degré de leur polynôme minimal soit connu est également très pratique pour notre étude. Ainsi nous nous pencherons sur les constructions de certains polygones particuliers pour explorer des propriétés plus générales de la constructibilité. [1]

La première question alors est : quels sont les polygones que l'on peut construire à la règle et au compas ?

3.1 Le théorème de Wantzel-Gauss

Nous allons d'abord présenter un résultat général avant de nous concentrer sur des cas particuliers pour explorer d'autres notions. Pour réduire notre étude dans la preuve finale, nous allons en premier lieu exposer quelques propriétés sur la constructibilité de certains cosinus. En effet, construire un polygone à n côtés revient à savoir construire $\cos\left(\frac{2\pi}{n}\right)$ comme nous aurons l'occasion de le répéter. Notons un premier fait :

Remarque 20. Étudier la constructibilité du polygone à p côtés est équivalent à étudier la constructibilité de $\cos\left(\frac{2\pi}{p}\right)$.

En effet, pour construire le polygone, il faut et il suffit de marquer sur le cercle unité :

$$e^{\frac{2i\pi}{p}} = \cos\left(\frac{2\pi}{p}\right) + i \sin\left(\frac{2\pi}{p}\right) = \cos\left(\frac{2\pi}{p}\right) + \sqrt{1 - \cos^2\left(\frac{2\pi}{p}\right)}$$

Puis il ne reste plus qu'à reporter la longueur de l'arc avec un compas tout autour du cercle pour compléter la construction. Un exemple sera vu plus tard avec la construction de l'Heptadécagone. Ce qui prouve bien l'équivalence des constructibilités.

Suite à cette première remarque, nous ajoutons une proposition. Celle-ci nous permettra de décomposer la construction d'un polygone à n côtés en utilisant sa décomposition en produit de facteurs premiers.

Proposition 21. Soient deux entiers n et m .

Si n et m sont premiers entre eux, alors :

$$\cos\left(\frac{2\pi}{nm}\right) \text{ est constructible} \Leftrightarrow \cos\left(\frac{2\pi}{n}\right) \text{ et } \cos\left(\frac{2\pi}{m}\right) \text{ sont constructibles}$$

Démonstration. - \Rightarrow

On suppose que $\cos\left(\frac{2\pi}{nm}\right)$ est constructible. On a que : $\frac{2\pi}{n} = m \frac{2\pi}{mn}$ et $\frac{2\pi}{m} = n \frac{2\pi}{mn}$.

Or on sait construire $\cos\left(\frac{2\pi}{nm}\right)$, en reportant n ou m fois la longueur de l'arc au compas sur le cercle unité, on peut donc bien construire $\cos\left(\frac{2\pi}{n}\right)$ et $\cos\left(\frac{2\pi}{m}\right)$

- \Leftarrow

Supposons maintenant que $\cos\left(\frac{2\pi}{n}\right)$ et $\cos\left(\frac{2\pi}{m}\right)$ sont constructibles.

Comme n et m sont premiers entre eux, le Théorème de Bézout nous permet de dire qu'il existe $(\lambda, \mu) \in \mathbb{Z}$ tels que :

$$\lambda n + \mu m = 1$$

C'est à dire :

$$\frac{2\pi}{mn} = \lambda \frac{2\pi}{m} + \mu \frac{2\pi}{n}$$

Et on en conclut que $\cos\left(\frac{2\pi}{nm}\right)$ est bien constructible par les mêmes arguments que précédemment \square

Remarque 22. Une conséquence directe de cette proposition est que, pour tout entier n , si on le décompose en produit de facteurs premiers : $n = \prod_{i=0}^k p_i^{\alpha_i}$ (où les p_i sont des nombres premiers et les α_i des entiers), alors le polygone à n côtés est constructible si et seulement si les polygones à $p_i^{\alpha_i}$ côtés sont tous constructibles.

Ainsi, résoudre notre problème revient à prouver le théorème suivant :

Théorème 23. Théorème de Gauss-Wantzel : constructibilité des polygones réguliers.

Le résultat s'énonce comme suit :

- Si $p = 2^\alpha$ où $\alpha \in \mathbb{N}$, le polygone à p côtés est constructible.
- Si p est premier, alors $\cos\left(\frac{2\pi}{p^\alpha}\right)$ est constructible si et seulement si $\alpha = 1$ et p est un nombre premier de Fermat : $p = 1 + 2^{(2^\beta)}$ avec $\beta \in \mathbb{N}$

Pour mener à bien cette preuve nous allons utiliser l'outil suivant :

Définition 24. Fonction indicatrice d'Euler

On définit cette indicatrice comme :

$$\varphi : \mathbb{N} \rightarrow \mathbb{N}$$

$$n \mapsto \text{card}\{m \leq n : m \text{ est premier avec } n\}$$

Remarque 25. Cette fonction peut se calculer en considérant la décomposition d'un nombre entier en produit de nombres premiers : $n = \prod_{i=0}^r p_i^{k_i}$ où les p_i sont les r nombres premiers qui constituent n .

Alors on a : $\varphi(n) = \prod_{i=0}^r (p_i - 1)p_i^{k_i - 1}$, c'est à dire $\varphi(n) = n \prod_{i=0}^r \left(1 - \frac{1}{p_i}\right)$

En particulier, si n est premier :

$$\varphi(n) = n - 1$$

Nous avons introduit cette application car elle nous donne des indications sur le polynôme minimal de $\cos\left(\frac{2\pi}{n}\right)$.

Démonstration. - la première partie est triviale : nous savons construire une bissectrice qui coupe un angle en deux. Donc à partir d'un diamètre on peut construire un carré, puis un octogone etc. en coupant toujours les angles en deux et en multipliant donc par un facteur 2 le nombre de côtés du polygone.

- pour la seconde partie, nous allons procéder par double implication :

- \Rightarrow on suppose que $\cos\left(\frac{2\pi}{p^\alpha}\right)$ est constructible.

1 - C'est à dire qu'il existe un $m \in \mathbb{N}$:

$$\left[\mathbb{Q} \left[\cos \left(\frac{2\pi}{p^\alpha} \right) \right] : \mathbb{Q} \right] = 2^m$$

2 - On pose $\omega = e^{\frac{2i\pi}{p^\alpha}}$ qui est une racine p^α de l'unité. Pour alléger les notations, on notera : $p^\alpha = q$
En effet, ω est racine du polynôme $X^q - 1 = 0$ donc ω est algébrique sur \mathbb{Q} .

- On introduit alors le q -ème polynôme cyclotomique. $P(X) = (X - w_1) \dots (X - w_k)$ où les w_1, \dots, w_k sont les k racines de l'unité telles que $w_1 = w$ et $w_i = w^i$ où i est premier avec q .

Ce polynôme a pour degré le nombre d'entiers i inférieurs à q tels que i est premier avec q . C'est à dire : $\deg(P) = p^{\alpha-1}(p - 1)$. On sait également que le polynôme cyclotomique est irréductible. Cette propriété que l'on admettra se démontre en utilisant des critères de divisibilité comme le théorème de Bezout et le critère d'Eisenstein.[8]

On en déduit donc que ω est algébrique tel que :

$$[\mathbb{Q}[\omega] : \mathbb{Q}] = p^{\alpha-1}(p - 1)$$

3 - Maintenant, on utilise le fait que $\omega + \omega^{-1} = 2 \cos\left(\frac{2i\pi}{p}\right)$. C'est donc que $\cos\left(\frac{2i\pi}{p}\right) \in \mathbb{Q}[\omega]$ où :

$$\omega^2 - 2\omega \cos\left(\frac{2i\pi}{p}\right) + 1 = 0$$

donc ω est algébrique de degré 2 sur $\mathbb{Q}\left[\cos\left(\frac{2i\pi}{p}\right)\right]$

4 - En combinant les degrés trouvés dans les étapes précédentes et en utilisant la multiplicativité des degrés des extensions de corps, on obtient :

$$[\mathbb{Q}[\omega] : \mathbb{Q}] = \left[\mathbb{Q}[\omega] : \mathbb{Q}\left[\cos\left(\frac{2\pi}{p^\alpha}\right)\right] \right] \cdot \left[\mathbb{Q}\left[\cos\left(\frac{2\pi}{p^\alpha}\right)\right] : \mathbb{Q} \right]$$

$$p^{\alpha-1}(p-1) = 2^m \cdot 2$$

Or $p \neq 2$ donc nécessairement : $\alpha = 1$ et :

$$p = 1 + 2^{m+1}$$

5- Il ne reste maintenant plus qu'à montrer que $m+1 = 2^\beta$

La décomposition de $m+1$ en facteurs premiers nous donne : $m+1 = \lambda 2^\beta$ où λ est un entier impair.

On a ainsi : $p = 1 + (2^{2^\beta})^\lambda$

Or λ est impair, c'est donc que le polynôme $1 + X^\lambda$ admet au moins une racine réelle qui est -1. Ce polynôme est divisible par $1 + X$. Ceci signifie que p est divisible par $1 + (2^{2^\beta})$, or p est premier. Donc on a finalement

$$p = 1 + (2^{2^\beta})$$

- \Leftarrow

Pour la réciproque, nous allons pas à pas dans les technicités. La raison de sa difficulté technique vient du raisonnement en lui-même : c'est un raisonnement par construction. Nous prendrons le temps et la place d'écrire cette construction car elle nous servira par la suite. Elle n'est généralement pas présentée dans la plupart des ouvrages car de moindre importance. En effet elle ne concerne qu'un nombre assez réduit de polygones étant donné que nous ne connaissons que 5 nombres premiers de Fermat.

Pour prouver le sens réciproque, l'idée est de construire directement et explicitement la tour d'extensions de corps qui permettra d'arriver jusqu'à ω .

On suppose que p est un nombre premier de Fermat. Il faut donc trouver la tour d'extensions quadratiques qui nous permettra de dire : $[\mathbb{Q}[\omega] : \mathbb{Q}] = 2^k$

Pour cela, On considère G le groupe des automorphismes de corps de $\mathbb{Q}(\omega)$.

Nous reprenons les notations du sens précédent en utilisant P comme le p -ème polynôme cyclotomique. Si nous prenons $g \in G$, par sa qualité d'automorphisme et en utilisant encore une fois le polynôme cyclotomique de p , il vient que $P(g(w)) = 0$ C'est donc que $g(w) = w^j$ où j est premier avec p et $j \leq p$. Ainsi on en déduit que g est entièrement déterminé par son image $g(\omega)$. De plus, on pourra dire que g est cyclique en parcourant la base des (ω^i) . On aura en effet $g^{p-1} = Id$ où $p-1 = 2^k$.

Réciproquement, on peut vérifier que pour tout entier k , la fonction $g_k : w \rightarrow w^k$ se prolonge en un automorphisme de $\mathbb{Q}(\omega)$.

Cette propriété nous permet donc de dire que G est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^*$. G est donc cyclique à $p-1$ éléments et admet un générateur. Nous pouvons également le voir comme le fait que l'application g représente une permutation circulaire des puissances de ω .

On choisit donc g un générateur de G . Puis on note G_i le sous-groupe engendré par g^{2^i} et K_i le sous-corps de $\mathbb{Q}[\omega]$ fixé par tous les éléments de G_i . C'est à dire que $G_i = \langle g^{2^i} \rangle$ et $K_i = \ker(g^{2^i} - Id)$
On a alors :

$$\mathbb{Q} \subset K_1 \subset \dots \subset K_k = \mathbb{Q}[\omega]$$

Nous allons ici essayer de comprendre un peu ce que représentent ces sous-corps. Premièrement, nous allons montrer que $K_0 = \mathbb{Q}$. En effet, on peut considérer que K_0 représente le corps des éléments z stabilisés ou invariants par g . C'est à dire que pour tout élément z de K_0 , $g(z) = z$.

On a de plus que la famille $\{\omega, g(\omega), \dots, g(\omega)^{p-2}\}$ est une famille de $p - 1$ puissances distinctes de ω , c'est donc une famille libre qui va générer $\mathbb{Q}[\omega]$. Si on le voit comme un espace vectoriel, on peut donc dire que cette famille est une base de $\mathbb{Q}[\omega]$.

Donc si on prends z dans K_0 , nous aurons :

$$z = \lambda_0\omega + \lambda_1g(\omega) + \dots + \lambda_{p-2}g^{p-2}(\omega)$$

Où les λ_i De plus, on sait que l'écriture dans une base est unique donc on peut en déduire les égalités suivantes :

$$\begin{aligned} z &= g(z) \\ &= \lambda_0g(\omega) + \dots + \lambda_{p-2}\omega \\ &= \lambda_0(\omega + g(\omega) + \dots + g^{p-2}(\omega)) \\ &= \lambda_0(\omega + \omega^2 + \dots + \omega^{p-2}) \\ &= -\lambda_0 \end{aligned}$$

Donc nous avons bien que z est dans \mathbb{Q} , et par conséquent $K_0 = \mathbb{Q}$.

Il reste à montrer que ces extensions sont strictes et quadratiques.

Pour le caractère stricte des extensions, nous passerons les calculs mais il se trouve que pour tout $i \geq 0$, l'élément $\sum_{j=0}^{2^k-i-1} g^{j2^i}(\omega)$ est dans K_i mais pas dans K_{i+1} . On passera les détails de ce calcul.

Regardons plus en détail les K_i . On peut les voir comme dit plus tôt comme :

$$K_i = \ker(g^{2^i} - Id)$$

C'est à dire que K_i est l'espace vectoriel qui est stable par g^{2^i} . On pourra donc constater qu'il faudra toujours deux fois plus de vecteurs pour générer K_i par rapport à K_{i-1} . (Nous le montrerons dans la construction de l'Heptadécagone). Nous percevons bien ici par cette idée la "quadraticité" des extensions de corps successives.

Plus rigoureusement, nous avons construit k extensions de corps pour arriver jusqu'à $\mathbb{Q}[\omega]$ qui est de degré 2^k . C'est donc que toutes ces extensions sont bien quadratiques.

Nous pourrions nous arrêter ici, mais nous allons inclure le cosinus dans la preuve de la constructibilité. C'est à dire que nous allons montrer la constructibilité de $\cos(\frac{2\pi}{p})$ en plus de celle de ω .

En effet, en utilisant l'élément cité précédemment pour montrer la stricte inclusion, on obtient également que :

$$\omega + g^{2^k-1}(\omega) \in K_{k-1}$$

$$\text{Or } g^{2^k-1}(\omega) = e^{\frac{2\pi(p-1)}{p}} = \bar{\omega}$$

Donc on a bien que $\omega + \bar{\omega} = 2\cos(\frac{2\pi}{p}) \in K_{k-1}$. C'est donc que l'on a une suite d'extensions quadratiques pour arriver jusqu'au cosinus de notre polynôme recherché.

Ainsi, le théorème est bien démontré et nous connaissons les critères pour qu'un polygone à n côtés soit constructible. \square

Remarque 26. On remarque deux choses à l'issue de cette démonstration :

- Il faut une extension quadratique en plus du cosinus pour avoir le ω recherché, c'est pour la construction du sinus.
- Le degré du polynôme minimal de $\cos(\frac{2\pi}{p})$ est $2^k/2$, comme nous le retrouverons plus tard.

3.2 Réflexion sur la construction du pentagone

Maintenant que nous connaissons les polygones constructibles avec les nombres premiers de Fermat : 5, 17, 257, 65537, nous allons nous pencher sur leurs constructions pour essayer de dégager les liens entre la complexité de leurs constructions et leurs polynômes minimaux.

Nous allons avoir besoin pour construire ces polygones d'un nouvel outil :

Définition 27. *Cercle de Carlyle*

Pour construire géométriquement une équation du second degré :

$$(E) : x^2 - sx + p = 0$$

Il suffit de tracer le cercle d'équation :

$$x(x - s) + (y - 1)(y - p) = 0$$

Qui coupe l'axe des abscisses ($y = 0$) en x_1 et x_2 les racines du trinôme précédent (ou ne coupe pas cet axe si il n'y a pas de solution).

On peut construire ce cercle à partir des deux points $A = (0, 1)$ et $B = (s, p)$ qui forment un diamètre du cercle de Carlyle.

Exemple 28. Voici un exemple d'utilisation des cercles de Carlyle.

Si on prend l'équation : $(E) : x^2 + 4x + 3 = 0$, on trouve que les racines sont $x_1 = -1$ et $x_2 = -3$. En construisant le cercle de Carlyle associé, on retrouve bien les solutions trouvées algébriquement :

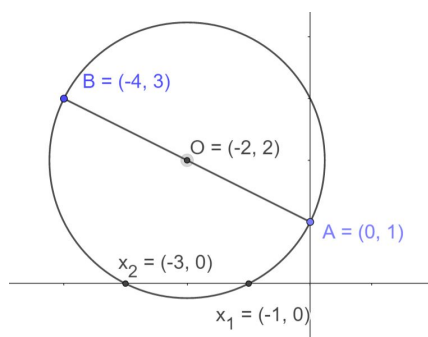


FIGURE 6 – Cercle de Carlyle associé à (E)

Ces cercles bien utiles vont nous servir pour construire le pentagone régulier avec le moins de cercles possibles.

Pour construire le pentagone régulier, il suffit de savoir construire $\cos(\frac{2\pi}{5})$. Une fois cette longueur trouvée, on y trace la perpendiculaire à l'axe des abscisses. Le point d'intersection avec le cercle unité sera $\omega = e^{\frac{2i\pi}{5}}$. Avec le compas, il suffit de tracer le cercle de centre ω passant par le point (1,0). L'intersection suivante désignera le deuxième sommet du polygone. On réitère cette opération jusqu'à retomber sur 1 pour trouver tous les sommets recherchés.

Nous savons que cela revient à résoudre la racine 5ème de l'unité, $z^5 - 1 = 0$. En supprimant la racine évidente 1, et en notant $w^i = e^{\frac{2i\pi}{5}}$, pour i dans $\{1, 2, 3, 4\}$ on a que w est solution de :

$$E_0 : z^4 + z^3 + z^2 + z + 1 = 0$$

On définit alors $p_1 := w + w^4 = 2 \cos(\frac{2\pi}{5})$ et $p_2 := w^2 + w^3 = 2 \cos(\frac{4\pi}{5})$

En utilisant le fait que $w = w^6$ et E_2 , on obtient :

$$\begin{cases} p_1 + p_2 = -1 \\ p_1 \cdot p_2 = -1 \end{cases}$$

Donc p_1 et p_2 sont solution de :

$$E_1 : x^2 + x - 1 = 0$$

Avec cette équation, on peut construire le pentagone en quelques étapes :

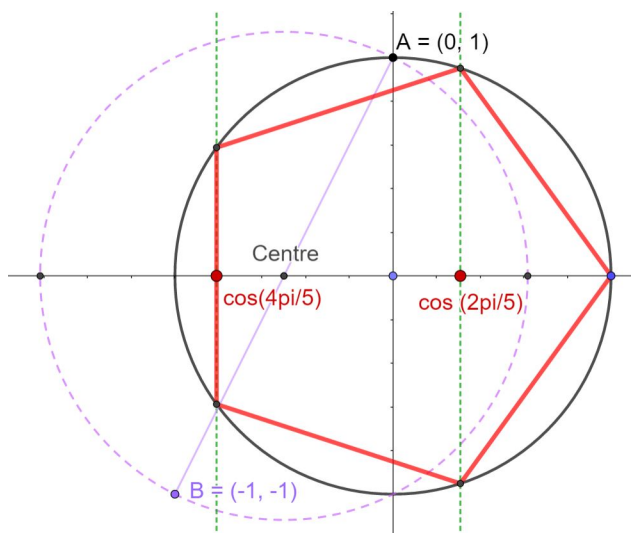


FIGURE 7 – Construction du Pentagone régulier

- Tracer le cercle unité et deux axes.
- Placer le point $A = (0, 1)$ et le point $B = (-1, -1)$ qui vont définir le diamètre du cercle de Carlyle
- Construire le milieu O du segment $[AB]$
- Tracer le cercle de centre O passant par A et B .
- Les points d'intersection du cercle avec l'axe des abscisses correspondent à p_1 et p_2 donc construire les milieux entre $p_{1/2}$ et O pour avoir $\cos(\frac{2\pi}{5})$ et $\cos(\frac{4\pi}{5})$
- Tracer les perpendiculaires aux abscisses passant par les deux cosinus.
- Les points d'intersections de ces droites avec le cercle correspondent aux sommets du pentagone qu'il suffit de relier.

On remarque qu'il a fallu construire un cercle de Carlyle pour obtenir le Pentagone.

Nous allons maintenant essayer de revenir un peu sur l'algèbre pour voir s'il n'y aurait pas des liens qui émergent entre la construction et le polynôme minimal lié au pentagone.

Nous allons ici réutiliser la fonction indicatrice d'Euler qui nous donne des indications sur le polynôme minimal de $\cos(\frac{2\pi}{n})$. En effet, si on note Q le polynôme minimal de $\cos(\frac{2\pi}{n})$ à coefficients dans \mathbb{Q} , on a que :

$$\deg(Q_n) = \frac{\varphi(n)}{2}$$

Et à partir de toutes ces informations, on remarque que avec le pentagone :

- Il faut construire un Cercle de Carlyle
- $\deg(Q_5) = (5 - 1)/2 = 2^1$
- $\cos(\frac{2\pi}{5}) = \frac{-1+\sqrt{5}}{4}$ qui fait intervenir une racine

Il semble qu'il y ait un lien entre toutes ces quantités car elles sont toutes liées à la notion d'extension de corps. Pour explorer un peu plus loin, nous allons regarder le polygone régulier à 17 côtés, qui est constructible d'après le théorème de Wantzel-Gauss

3.3 Construction de l'heptadécagone : Poursuite des réflexions

Cette fois, nous devons résoudre l'équation : $z^{17} - 1 = 0$ Nous allons procéder avec la même méthode que pour le pentagone, en substituant la solution évidente 1, on obtient que les 16 autres racines sont aussi racines de l'équation :

$$z^{16} + z^{15} + z^{14} + z^{13} + z^{12} + z^{11} + z^{10} + z^9 + z^8 + z^7 + z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0$$

Sans rentrer trop dans les détails qui ne nous intéressent pas ici, nous allons réarranger les solutions ω dans un ordre tel que : $w, w^g, w^{g^2}, \dots, w^{g^{16}} = w$. On choisit $g=3$ qui est le plus petit entier satisfaisant cette condition, en utilisant de plus le fait que $w = w^{18}$ on obtient la suite suivante :

$$w, w^3, w^9, w^{10}, w^{13}, w^5, w^{15}, w^{11}, w^{16}, w^{14}, w^8, w^7, w^4, w^{12}, w^2, w^6$$

Puis, de façon un peu plus sophistiquée que pour le pentagone, nous allons définir des **périodes**.

Par exemple, $\eta_{0,2} = w + w^9 + w^{13} + w^{15} + w^{16} + w^8 + w^4 + w^2$, que l'on notera sous la forme $\eta_{0,2} = (1, 9, 13, 15, 16, 8, 4, 2)$ est la somme des solutions en partant de la 1ère de la liste avec un pas de 2.

On utilise alors les périodes suivantes :

$$\eta_{0,2} = (1, 9, 13, 15, 16, 8, 4, 2) \tag{3}$$

$$\eta_{1,2} = (3, 10, 5, 11, 14, 7, 12, 6) \tag{4}$$

$$\eta_{0,4} = (1, 13, 16, 4) \tag{5}$$

$$\eta_{1,4} = (3, 5, 14, 12) \tag{6}$$

$$\eta_{2,4} = (9, 15, 8, 2) \tag{7}$$

$$\eta_{3,4} = (10, 11, 7, 6) \tag{8}$$

$$\tag{9}$$

Que l'on va mettre en relation pour trouver l'équation vérifiée par $\eta_{0,8} = \cos(\frac{2\pi}{17})$ et $\eta_{4,8} = \cos(\frac{8\pi}{17})$.

Pour la remarque, on retrouve ici le fait que $\{\eta_{0,2}, \eta_{1,2}\}$ va générer le corps K_1 de l'Heptadécagone, $\{\eta_{0,4}, \eta_{1,4}, \eta_{2,4}, \eta_{3,4}\}$ va générer le corps K_2 et la famille des permutations de degré 8 va générer le corps K_3 .

Notre but est de nous ramener à des équations du second degré, car nous savons les résoudre géométriquement avec les cercles de Carlyle. Après plusieurs calculs on en déduit les relations suivantes :

$$\eta_{0,8} + \eta_{4,8} = \eta_{0,4} \quad , \quad \eta_{0,8} \cdot \eta_{4,8} = \eta_{1,4} \quad \text{et} \quad \eta_{0,8} > \eta_{4,8} \tag{10}$$

$$\eta_{0,4} + \eta_{2,4} = \eta_{0,2} \quad , \quad \eta_{0,4} \cdot \eta_{2,4} = -1 \quad \text{et} \quad \eta_{0,4} > \eta_{2,4} \tag{11}$$

$$\eta_{1,4} + \eta_{3,4} = \eta_{1,2} \quad , \quad \eta_{1,4} \cdot \eta_{3,4} = -1 \quad \text{et} \quad \eta_{1,4} > \eta_{3,4} \tag{12}$$

$$\eta_{0,2} + \eta_{1,2} = -1 \quad , \quad \eta_{0,2} \cdot \eta_{1,2} = -4 \quad \text{et} \quad \eta_{0,2} > \eta_{1,2} \tag{13}$$

$$\tag{14}$$

Qui vont nous permettre d'exprimer les 4 équations du second degré permettant la construction de l'heptadécagone. Nous avons donc finalement :

- $\eta_{0,2}$ et $\eta_{1,2}$ sont solutions de $(E_2) : x^2 + x - 4 = 0$
- $\eta_{0,4}$ et $\eta_{2,4}$ sont solutions de $(E_3) : x^2 - \eta_{0,2}x - 1 = 0$
- $\eta_{1,4}$ et $\eta_{3,4}$ sont solutions de $(E_4) : x^2 - \eta_{1,2}x - 1 = 0$
- $\eta_{0,8}$ et $\eta_{4,8}$ sont solutions de $(E_5) : x^2 - \eta_{0,4}x + \eta_{1,4} = 0$

C'est à dire que nous avons 4 équations qui vont définir les 4 étapes de la construction de l'heptadécagone. Chaque étape se concluant par la construction du cercle de Carlyle associé à l'équation comme ci-dessus, en procédant dans l'ordre indiqué.

ces calculs nous permettent également de trouver le polynôme minimal de $\cos(\frac{2\pi}{17})$ et de l'exprimer comme :

$$16 \cos(\frac{2\pi}{17}) = -1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + \sqrt{68 + 2\sqrt{17} - 4\sqrt{34 - 2\sqrt{17}} - 8\sqrt{34 + 2\sqrt{17}}}$$

Si nous résumons comme pour le pentagone, nous avons avec la construction de l'heptadécagone :

- 4 cercles de Carlyle à construire (pour l'instant)
- $\deg(Q_{17}) = (17 - 1)/2 = 8 = \frac{2^4}{2}$
- 4 nouvelles racines à construire qui sont : $\sqrt{17}, \sqrt{34 - 2\sqrt{17}}, \sqrt{34 + 2\sqrt{17}}, \sqrt{68 + \dots}$

On reconnaît encore la même relation que dans le cas du pentagone : il y a autant de cercles de Carlyle à construire que de racines, et cette "complexité" semble liée à un facteur 2 près au degré du polynôme minimal du cosinus qui définit la construction du polygone que voici :

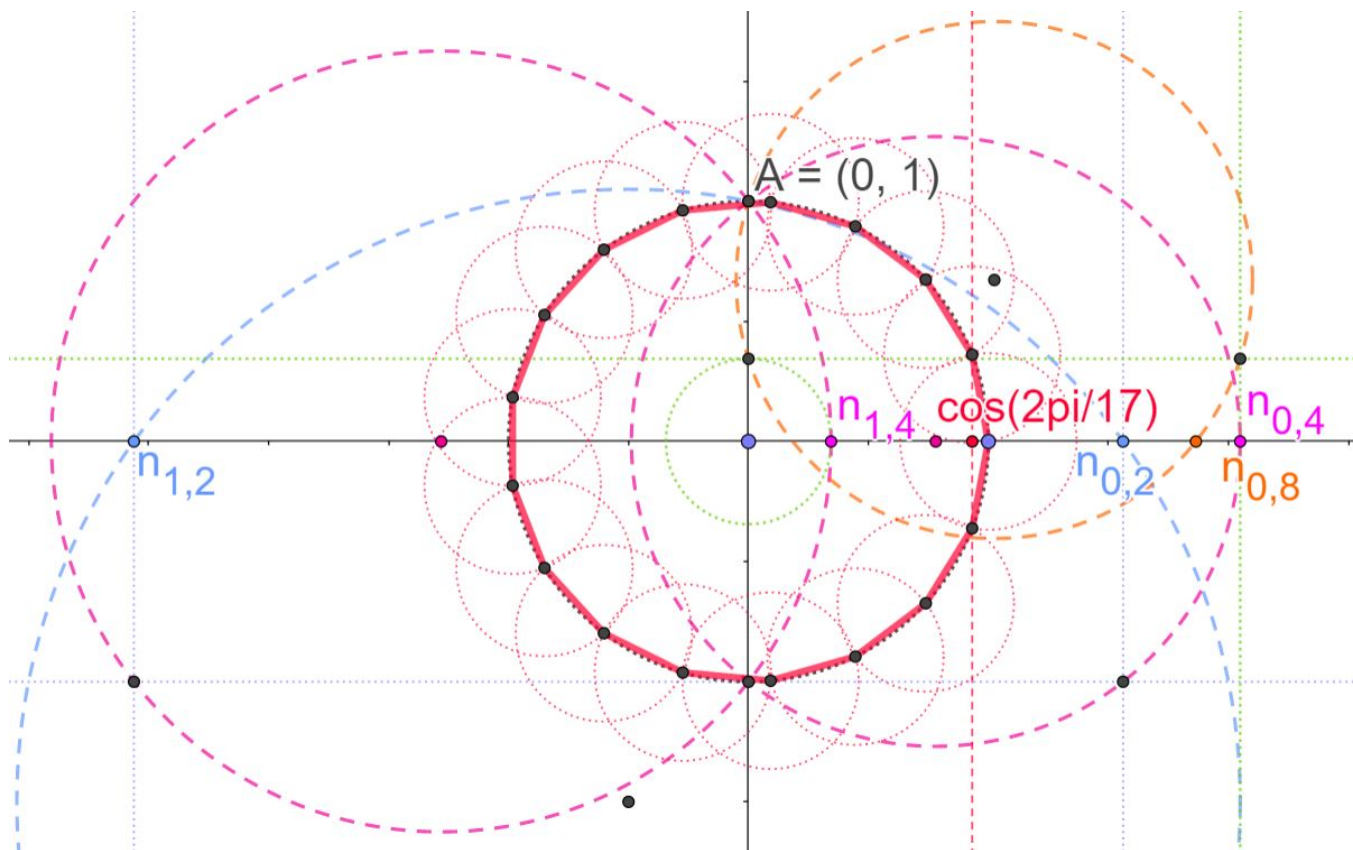


FIGURE 8 – Construction de l'Heptadécagone : polygone régulier à 17 côtés

Est-ce généralisable ?

Donc on peut déjà de demander si cette construction est-elle vraiment optimale ?

Nous allons appeler maintenant un nouveau Théorème, que nous ne montrerons pas car il n'est pas utile de voir la démonstration pour notre propos.

Théorème 29. Théorème de l'élément primitif

Soit K un corps, Si L/K est une extension finie du corps K , alors il existe $a \in L$ tel que $L = K(a)$, ou même $K[a]$ dans notre cas, c'est équivalent.

En utilisant la réciproque de la preuve de Wantzel-Gauss et en la combinant avec ce théorème, on voit que pour construire n'importe quel point constructible, il suffit de trouver l'élément primitif de chaque extension de corps quadratique les unes après les autres pour l'exprimer géométriquement sous la forme d'une racine et arriver après n extensions quadratiques au nombre voulu. En effet en reprenant cette preuve constructive, il suffit de voir que pour un ω de degré de polynôme minimal 2^n , on peut en effet construire une tour d'extension de n corps. Et nous avons vu que chaque extension quadratique est équivalente à un cercle de Carlyle ou un théorème de Pythagore (soit à la construction d'une racine). Pourquoi donc, pour l'Heptadécagone de degré minimal 2^3 , faut-il construire 4 Cercles ?

Nous pensons qu'en fait, cela n'est pas nécessaire et qu'il en suffirait de 3. Mais toute la difficulté va se trouver dans trouver l'élément primitif.

Concrètement, nous affirmons ici qu'il y a 3 extensions de corps :

- Nous savons que $K_0 = \mathbb{Q}$ qui est notre corps initial.
- Pour la deuxième étape, nous aurions $K_1 = \mathbb{Q}[\sqrt{17}]$ comme l'indique notre construction. L'élément primitif est ici directement trouvé. Il correspond au premier cercle de notre construction et à $\eta_{0,2}$.
- Maintenant, nous voulons affirmer qu'en fait, $\sqrt{34 - 2\sqrt{17}}$ et $\sqrt{34 + 2\sqrt{17}}$ sont dans la même extension de corps, c'est à dire que $\eta_{0,4}, \eta_{1,4}, \eta_{2,4}, \eta_{3,4}$ sont dans une même extension quadratique. Ainsi en trouvant l'élément primitif a de cette extension, nous pourrions exprimer ces racines à l'aide de puissances de a . Une fois ces expressions trouvées, nous pouvons retranscrire cela géométriquement en construisant a avec un seul cercle de Carlyle, puis en le manipulant avec Thalès pour retrouver les racines voulues. Finalement on a $K_2 = K_1[a] = \mathbb{Q}[\sqrt{17}, a]$
- La dernière extension et le troisième cercle de Carlyle nous est donné par la dernière équation du second degré, avec donc comme élément primitif $\sqrt{68 + \dots}$

A un élément primitif près, nous pourrions donc bien construire l'Heptadécagone avec seulement 3 cercles de Carlyle.

Nous remarquons que :

$$(\eta_{04} + 2\eta_{14})^2 = 6(-1) + 2\eta_{12} - 3(\eta_{04} + 2\eta_{14}) + 5\eta_{02} + 2\eta_{24}$$

Nous pouvons donc construire η_{24} à partir de $\eta_{04} + 2\eta_{14}$, et donc également

$$\begin{aligned} \eta_{04} &= \eta_{02} - \eta_{24} \\ 2\eta_{14} &= (\eta_{04} + 2\eta_{14}) - \eta_{04} \\ \eta_{34} &= \eta_{12} - \eta_{14} \end{aligned}$$

Maintenant que nous avons un élément primitif de l'extension de corps qu'est K_2 , cherchons son polynôme minimal sur K_2 . Peut-être que son conjugué est $\eta_{24} + 2\eta_{34}$? car leur somme est dans K_2 et leur produit ? Nous sommes très contents, le produit est effectivement dans K_2 .

$$(\eta_{24} + 2\eta_{34})(\eta_{04} + 2\eta_{14}) = 7(-1) + 4\eta_{12}$$

Ces deux nombres sont donc solutions de l'équation :

$$x^2 - (\eta_{12} - 1)x + 7(-1) + 4\eta_{12} = 0.$$

Qui sera donc l'équation de notre deuxième cercle de Carlyle.

En reprenant les expressions précédentes, nous trouvons donc une deuxième construction de l'Heptadécagone, cette fois-ci en utilisant seulement 3 cercles de Carlyle.

- η_{02} et η_{12} sont solutions de $(E_2) : x^2 + x - 4 = 0$
- $(\eta_{04} + 2\eta_{24})$ et $(\eta_{14} + \eta_{34})$ sont solutions de $(E_{3*}) : x^2 - (\eta_{12} - 1)x + 7(-1) + 4\eta_{12} = 0$
- η_{08} et η_{48} sont solutions de $(E_5) : x^2 - \eta_{04}x + \eta_{14} = 0$

Si nous allons plus loin, nous connaissons une construction avec les cercles de Carlyle pour le nombre de Fermat suivant qui est 257. La preuve utilise la même méthode que vue pour les deux polygones précédents et utilise 24 cercles de Carlyle. Dans notre cadre $\deg(Q_{257}) = \frac{2^8}{2} = 2^7$ suggérerait pourtant qu'il suffise de 7 cercles de Carlyle pour construire un tel polygone. La difficulté d'une telle construction serait cependant de trouver l'élément primitif de chacune de ces extensions. Puis il faudrait également trouver une construction adaptée. Il n'est pas encore clair que construire le nombre minimal de cercles de Carlyle en utilisant les éléments primitifs représente vraiment la solution la plus "simple" d'un polygone régulier.

En continuant, il reste le dernier nombre premier de Fermat connu : 65537. Le degré du polynôme minimal de $\cos(\frac{2\pi}{65537})$ serait égal à $\frac{2^{16}}{2} = 2^{15}$. En trouvant l'élément primitif de chaque extension, il suffirait donc de 15 cercles de Carlyle pour le construire. Pourtant, les méthodes connues de constructions en utilisent plus de 1000! On se dit quand même qu'il y aurait un gros gain dans la construction à calculer au préalable les éléments primitifs plutôt que de généraliser la méthode de construction du pentagone régulier.

Ainsi, nous pensons donc avoir montré qu'il suffirait d'autant de cercles de Carlyle que de $\log_2(\deg(Q_n))$ pour construire un polygone régulier de n côtés. Ceci particulièrement dans le cadre des nombres premiers. Sinon dès qu'il y a un nombre pair, on peut revenir jusqu'à des nombres premiers en remontant les bissectrices.

Conclusion

Pour conclure sur ce mémoire, nous dirons que nous avons essayé de rester le plus possible à l'interface entre géométrie et algèbre, contrairement aux nombreux papiers que nous avons étudié. On pourra penser que c'est grâce à cette constante interaction que nous avons pu comprendre beaucoup mieux certaines structures et les mettre en lien d'une manière qu'il nous semble assez inédite. Sans attentes particulières, c'est dans la recherche d'une expression plus satisfaisante de la "complexité" d'une construction que nous en sommes venus à nous pencher sur les cercles de Carlyle, puis sur les polynômes. Il semblerait que notre idée ait été très féconde et que le problème des polygones réguliers nous ait permis de concentrer notre problème sur des constructions très précises, nous permettant ainsi de mieux comprendre certaines structures.

Nous noterons aussi que la preuve de Gauss aura été essentielle pour conclure ce mémoire, en exprimant une nouvelle conséquence de théorème si crucial.

Mais finalement, nous avons étudié tout une théorie basée sur un outillage : la règle et le compas.

Pourtant, nous avons vu par le biais de plusieurs articles que si l'on autorise les plis, on peut alors résoudre les équations de degré 3, on peut également trisecter les angles très facilement.[6][9]

De plus, l'image de la page de garde montre la construction de la quadrature du cercle à l'aide d'un outil assez simple appelé la quadratrix de Hippias. Cet outil pas plus grand qu'une règle usuelle permet de trisecter les angles, quadraturer le cercle et bien d'autres choses encore! Ainsi, en modifiant légèrement un

outil, nous obtenons des constructions beaucoup plus puissantes ! Donc si étudier la restriction à la règle et au compas est très intéressante pour comprendre des propriétés des extensions de corps et autres faits d'algèbre, on se demande bien pourquoi ce sont ces deux outils qui sont restés dans les trousseaux depuis des centaines d'années.

Références

- [1] Wayne BISHOP. “How to Construct a Regular Polygon”. In : *The American Mathematical Monthly* 85.3 (mar. 1978), p. 186. ISSN : 00029890. DOI : 10.2307/2321061. URL : <https://www.jstor.org/stable/2321061?origin=crossref> (visité le 20/06/2020).
- [2] Jean-Claude CARREGA. *Théorie des corps : la règle et le compas*. Collection Formation des enseignants et formation continue 1402. OCLC : 20730313. Paris : Hermann, 1989. 277 p. ISBN : 978-2-7056-1402-7.
- [3] Avissa Hedayati Dezfouli Marc Laly Sheedy Shiwpursad Hedayati DEZFOULI, Marc LALY et Sheedy SHIWPURSAD. *Transcendance de e et pi pour les nuls*. Avec la coll. d’Alain PROUTÉ. 2009. URL : http://www.logique.jussieu.fr/~alp/e_et_pi_transcendants.pdf.
- [4] Jean-Pierre ESCOPIER. *Théorie de Galois : cours et exercices corrigés*. OCLC : 718086205. Paris : Dunod, 2006. ISBN : 978-2-10-007685-7.
- [5] V. A. GEYLER. “One More Construction Which is Impossible”. In : *The American Mathematical Monthly* 102.7 (août 1995), p. 632. ISSN : 00029890. DOI : 10.2307/2974560. URL : <https://www.jstor.org/stable/2974560?origin=crossref> (visité le 20/06/2020).
- [6] Daniel J. HEATH. “Straightedge and Compass Constructions in Spherical Geometry”. In : *Mathematics Magazine* 87.5 (déc. 2014), p. 350-359. ISSN : 0025-570X, 1930-0980. DOI : 10.4169/math.mag.87.5.350. URL : <https://www.tandfonline.com/doi/full/10.4169/math.mag.87.5.350> (visité le 20/06/2020).
- [7] David HERNANDEZ et Yves LASZLO. *Introduction à la théorie de Galois*. OCLC : 898244895. Palaiseau : Éditions de l’École Polytechnique, 2014. ISBN : 978-2-7302-1593-0.
- [8] Adrien LAURENT. *Irréductibilité des polynômes cyclotomiques*.
- [9] THOMAS C. HULL. “Solving Cubics With Creases : The Work of Beloch and Lill”. In : *The American Mathematical Monthly* 118.4 (2011), p. 307. ISSN : 00029890. DOI : 10.4169/amer.math.monthly.118.04.307. URL : <https://www.tandfonline.com/doi/full/10.4169/amer.math.monthly.118.04.307> (visité le 20/06/2020).