Des Droites et des Cercles :
Constructions à la Règle et au Compas

Mémoire de Bachelor

Pierre van Boxel
sous la direction de Jean-Philippe Michel

31 mai 2011

Table des matières

Chapitre 1

Prologue

Les mathématiques modernes ont leur berceau en Grèce Antique. Les mathématiques grecques anciennes sont souvent liées à l'ouvrage qui, jusqu'à aujourd'hui, est considéré comme l'un des écrits mathématiques les plus influents de l'histoire des sciences. Cet ouvrage est intitulé *Eléments* et fut écrit et compilé par Euclide au troisième siècle av. J.-C. Il est composé de 13 livres traitant principalement de géométrie, mais aussi de théorie élémentaire des nombres. Les centaines de constructions géométriques que l'on y trouve sont effectuées à la règle et au compas. Pourtant, même si les *Eléments* ont souvent été considérés comme la naissance des mathématiques modernes, des problèmes de constructions à la règle et au compas existent depuis bien avant Euclide. Quatre de ces problèmes ont traversé le temps et occupé l'esprit des plus grands mathématiciens de l'histoire : la duplication du cube, la trissection de l'angle, la quadrature du cercle, et la construction de polygones réguliers.

Ces problèmes furent formellement posés au cinquième siècle av. J.-C., et les nombreuses tentatives de l'époque pour les résoudre montrent que le but central des mathématiques grecques était de résoudre les problèmes de manière géométrique. De plus, il semble que l'énorme collection de théorèmes que l'on trouve dans les œuvres majeures des mathématiciens grecs servi en fait en donner des résultats sous-tendant les arguments logiques pour l'élucidation de ces quatre problèmes [Katz, p. 34]. Pourtant, il faudra attendre deux millénaires avant d'obtenir une solution satisfaisante à la règle et au compas.

Pourquoi ce limiter à ces deux instruments ? Les mathématiciens grecs vénéraient la règle et le compas, et croyaient sincèrement que les vraies mathématiques pouvaient se faire uniquement grâce à ses deux instruments. La première raison en est leur simplicité. Les deux courbes les plus simples que l'un peut tracer sont la droite et le cercle, et les instruments les plus simples pour les construire sont la règle et le compas. La deuxième raison provient directement de la philosophie Platoniste. Dans son Académie, Platon (423 – 348 av. J.-C.) enseigna que le cercle que l'on peut tracer à la main n'est qu'en fait une représentation imparfaite du cercle idéal qui n'existe que dans le monde des idées. Cela va de même pour toute figure géométrique. Platon avait en effet très peu d'estime pour les instruments de mesure et/ou de construction. Pourtant, il fit une exception pour ce qui est de la règle et du compas ; les deux instruments qui, selon lui, respectent encore la symétrie des configurations. Troisièmement, les *Eléments* ont eux aussi eu une énorme influence sur le regard porté sur la règle et le compas. A travers le travail d'Euclide, les savants grecs ne considéraient une démonstration convaincante que si celle-ci était accompagnée d'une figure claire effectué à la règle et au compas. La raison finale traite plus de théorie des nombres que de géométrie. Les entiers naturels et leurs fractions étaient bien connus des grecs anciens, et

l'on pensait que l'on pouvait mesurer n'importe quel segment en n'utilisant que ces nombres. Pourtant, comme nous en sommes bien conscients de nos jours, le Théorème de Pythagore (c. 550 av. J.-C.) allait s'avérer être une vraie révolution dans le monde savant de l'époque, car il introduisit les racines carrées. On peut donc spéculer, que la règle et le compas furent éventuellement mis au devant de la technologie de l'époque afin de servir de garantie géométrique aux nombres connus et mis en évidence par le Théorème de Pythagore. De plus, on prévenait ainsi aux sciences de subir d'autres crises du genre [Carrega, p. 4-6].

Donc, les mathématiciens de l'époque avaient développé une telle confiance en la règle et le compas (qui fonctionnaient fort bien pour toutes les constructions élaborées en ce temps-là), que jamais ils n'auraient pensé à ce que ces problèmes soient en fait irréalisables en ne se tenant qu'à ces instruments. Pourtant, grâce au travail de nombreux mathématiciens à travers les âges, c'est précisément cette impossibilité qui fut démontrée, notamment grâce à la traduction des quatre problèmes classiques en termes algébriques. Déjà en Grèce Antique, entre autres le travail d'Archimède (287 – 212 av. J.-C.) sur les coniques lui a permis de doubler le cube et de trissecter l'angle [Archimède, p. c-cxiv]. Mais, après l'antiquité hellénique, la géométrie grecque tombe dans l'oubli. L'algèbre par contre fleuri dans le monde arabe et perse, ce qui mena peut-être le mathématicien Abul Wafa à reprendre quelques constructions à la règle au dixième siècle de notre ère. Au $16^{\text{ième}}$ siècle, Charles Quint offre un prix à celui qui pourra résoudre la quadrature du cercle, montrant bien que l'enthousiasme pour les problèmes classiques reprend à cette époque. C'est d'ailleurs dans ces années là que, basé sur l'œuvre de Cardan (1501 – 1576), Viète (1540 – 1603) montre que la trissection de l'angle se ramène à construire les racines réelles d'une équation du troisième degré [Carrega, 10].

Le premier mathématicien à établir fermement le lien existant entre les constructions géométriques à la règle et au compas et la résolution d'équations du premier et second degré fut René Descartes (1596 – 1650) dans sa *Géométrie* (1637) [Carrega, 3, 10]. L'entrain que les problèmes antiques suscite est tel qu'en 1775, l'Académie des Sciences à Paris, étant submergée par des essais de trissecteurs, duplicateurs, et quadrateurs, refuse de lire d'autres documents du genre.

En 1796, l'illustre Karl Friedrich Gauss (1777 – 1855) construit à l'âge de 19 ans le polygone régulier à 17 côtés, et énonce ensuite une condition nécessaire et suffisante pour que le polygone régulier général soit constructible ; il démontra uniquement que cette condition est suffisante. Il publia sa démonstration dans son livre *Disquisitiones Arithmeticae* en 1801. Ce ne sera qu'en 1837 que la démonstration du Théorème de Gauss pour les polygones réguliers à n-côtés constructibles est complétée. Le résultat qui rendit cela possible est celui que l'on appelle aujourd'hui le Résultat de Wantzel. Il fut développé par Pierre Laurent Wantzel (1814 – 1848) et démontre l'impossibilité de la duplication du cube et de la trissection de l'angle, plus de deux milles ans après leurs énoncés. Il le publia dans un article dans le *Journal de Mathématiques* intitulé "Recherche sur les moyens de reconnaître si un problème de géométrie peut se résoudre à la règle et au compas". De plus, le Résultat de Wantzel permet aussi de mieux comprendre le problème de la quadrature : ce n'est pas la *valeur* de π qui compte, comme de nombreux l'ont pensé auparavant, mais bien sa *nature*.

C'est Ferdinand Lindemann (1852 – 1939) qui démontre en 1882 la transcendance de π, ce qui en conjonction avec le Résultat de Wantzel, dit bien que la quadrature du cercle est impossible à la règle et au compas. Il se basa sur Lambert (1728 – 1777) qui démontra que π est irrationnel en 1761, Legendre (1752 – 1833) qui démontra que π^2 est irrationnel en 1794, Liouville (1809 – 1882) qui démontra l'existence de nombres transcendants en 1844, et Hermite (1822 – 1901) qui démontra que e est transcendant [Carrega, 3, 11].

Dans le présent travail, nous examinerons ces fameux quatre problèmes antiques plus en détails, et nous retracerons leur histoire en exposant les résultats importants à leur résolution, i.e. :

1. le passage de la géométrie à l'algèbre,
2. le Résultat de Wantzel, et
3. le Théorème de Gauss.

Nous donnerons également les multiples résultats conduisant à ces résultats principaux et les liant les uns aux autres. Beaucoup d'exemples et de figures illustreront aussi cette fascinante odyssée mathématique.

NOTE : pour référence à quelque aspect algébrique utilisé dans ce travail mais supposé comme connu, l'ouvrage de Daniel Guin et Thomas Hausberger est excellent (voir la bibliographie).

Chapitre 2

Quatre Problèmes Antiques

Considérons ces fameux quatre problèmes classiques.

2.1 Duplication du Cube

La duplication du carré est facile (en construisant un autre carré sur sa diagonale) et était connue à l'époque. Ce problème est parfois appelé Problème de Délos en référence à la légende suivante : Un oracle promit que la peste qui faisait rage sur l'île de Délos cesserait si on construisait à Apollon un autel du double de volume de l'autel cubique existant. On construisit donc un autel du double de côté, une notion bien connue, mais la peste persista. L'oracle décréta qu'Apollon demandait un autel *exatement* double de l'ancien [Carrega, 8].

Soit un cube donné quelconque.
Construire à la règle et au compas l'arête d'un cube ayant un volume deux fois plus grand que celui du cube donné.

Hippocrates de Chios (c.470 – 410 av. J.-C) fut le premier à tenter de résoudre ce problème. Il se rendit certainement compte que ce problème est étroitement lié à la duplication du carré. Cette dernière se ramène à l'équation $b^2 = 2a^2$ avec b le côté du nouveau carré et a le côté du premier, ce qui implique que b est la moyenne géométrique entre a et $2a$, c'est-à-dire $\frac{a}{b} = \frac{b}{2a}$. Hippocrate prit ce procédé bien connu pour résoudre le problème du cube. Il l'écrit sous la forme $b^3 = 2a^3$, et prend donc deux moyennes géométriques b et c entre a et $2a$ pour que $\frac{a}{b} = \frac{b}{c} = \frac{c}{2a}$. Ceci implique que

$$\frac{a^3}{b^3} = \left(\frac{a}{b}\right)^3 = \left(\frac{a}{b}\right)\left(\frac{b}{c}\right)\left(\frac{c}{2a}\right) = \frac{a}{2a} = \frac{1}{2}.$$

Malgré, sans doute, de nombreux essais, Hippocrate ne réussit jamais à trouver ces moyennes géométriques b et c en utilisant les outils géométriques dont il disposait [Katz, 34].

Par contre, un siècle plus tard Ménechme construisit des courbes satisfaisant les propriétés algébriques énoncées par Hippocrate (des paraboles et une hyperbole) et trouva que l'intersection des ces courbes donnait les deux moyennes désirées. Il pu donc doubler le cube. On ne sait pas aujourd'hui comment il y est arrivé [Katz, 75], mais il est clair que les coniques sont bien entrées dans

les outils géométriques des savants grecs, puisqu'Archimède les a profondément étudiées par la suite.

Cette idée de trouver l'intersection de coniques fut reprise par les mathématiciens arabes, des siècles plus tard sous l'étude des équations cubiques. 'Umar ibn Ibrahin al-Kayyami (Omar Khayyam 1048 – 1131) fut le premier à les classifier systématiquement et les résoudre efficacement en offrant une méthode générale. Son œuvre est fortement inspirée par les *Eléments* d'Euclide, les *Coniques* d'Apollonius (c. 250 – 175 av. J.-C.), et le travail d'al-Khwarizmi (c. 780 – 850) sur la classification et la résolution d'équation du second degré [Katz, 173].

2.2 Trissection de l'Angle

Soit un angle donné quelconque.
Construire à la règle et au compas les demi-droites divisant cet angle en trois parties égales.

Ce problème est aussi tout à fait légitime, car construire la bissectrice d'un angle était bien connu, ainsi que trissecter un segment. Il serait donc logique de penser que la trissection d'un angle soit possible [Carrega, 8].

2.3 Quadrature du Cercle

Ce problème est sans doute le plus ancien de tous et le plus populaire. L'expression "C'est la quadrature du cercle" est même passée dans le langage courant pour désigner quelque chose d'impossible à réaliser. Au cinquième siècle av. J.-C., le poète Aristophane y fait allusion dans ses pièces, montrant que le problème était déjà célèbre à l'époque.

Soit un cercle donné quelconque.
Construire à la règle et au compas un carré ayant même aire que ce cercle.

Le problème consiste à ramener une aire circulaire à l'aire d'un carré. La pertinence de ce problème à l'époque est claire. Ayant une mauvaise connaissance de π, il était évidemment beaucoup facile pour des artisans ou des agriculteurs de calculer l'aire d'un carré plutôt que de calculer directement celle du cercle de même aire. Le premier document où est mentionné le but de quarrer le cercle est le célèbre papyrus de Rhind, écrit par le scribe Ahmès, datant de 1650 av. J.-C. Le papyrus dit que pour quarrer le cercle, il suffit de prendre le carré ayant pour côté $\frac{1}{9}$ du diamètre du cercle donné. Ce qui donne une approximation de π à $3,16$.

Le premier géomètre à s'attaquer à la quadrature du cercle après son énoncé formel au cinquième siècle av. J.-C. fut Hippocrate de Chios. Il n'a pas réussi mais a pu par contre quarrer des surfaces qu'il appelle 'lunules', c'est-à-dire des surfaces délimitées par des arcs de cercles (généralement en forme de lune).

Beaucoup ont essayé d'autres méthodes, mais comme nous l'avons vu dans le prologue, la vraie question qui se pose ici traite du nombre π. A travers les âges, le nombre sans doute le plus emblématique des mathématiques toutes entières fut approximé et étudié [Carrega, 6, 7].

Le premier à utiliser π pour symboliser le rapport entre la circonférence et le diamètre d'un cercle fut William Jones en 1706. Auparavant, il désignait

tout simplement la circonférence du cercle. Pourtant, sous l'influence d'Euler qui utilisa π en 1748 dans son livre *Introductio in analysin infinitorum* comme le suggéra Jones, le symbole π se popularisa rapidement.

Les mathématiciens et savants ont recherché ce nombre depuis 1800 av. J.-C. Pourquoi tant d'engouement ? Il y a plusieurs raisons, mais l'une des plus importantes est justement l'enthousiasme perpétuel pour le fameux problème de la quadrature du cercle. Regardons le parcourt historique de ce nombre avant qu'il soit jugé transcendant au $19^{\text{ième}}$ siècle [Joseph, 261-64].

c. 1650 av. J.-C. Le papyrus de Rhind (Egypte) donne $\pi \simeq 3,16$.

c. 1600 av. J.-C. La Tablette de Susa (Babylone) donne $\pi \simeq 3,236$ en prenant la proportion entre le périmètre de l'hexagone et de son rayon.

c. 800 – 500 av. J.-C. Le *Sulbasutras* (Inde), livre sacré de la religion Hindoue, donne une règle pour former un carré d'aire égale à celle d'un cercle afin de construire et sculpter des autels donnant $\pi \simeq 3,09$ [Joseph, 326, 327, 332-34].

c. 250 av. J.-C. Archimède (Grèce) calcule les périmètre de polygones réguliers inscrits dans un cercle jusqu'à 96 côtés et obtient $\frac{223}{71} < \pi < \frac{22}{7}$, qui donne donc $\pi \simeq 3,14$.

c. 260 de notre ère Liu Hui (Chine) reprend le travail d'Archimède et obtient $\pi = 3,1416$.

c. 480 Zu Chongzhi (Chine) continue le travail de Liu Hui et place π entre $3,1415926$ et $3,1415927$ en calculant le périmètre du polygone à 24.576 côtés !

c. 1400 Madhava (Inde) utilise les expansions de π en séries infinies et trouve $\pi \simeq 3,14159265359$, correct à 11 chiffres après la virgule.

1429 al-Kashi (Perse) trouve le périmètre du polygone à $3 \times 2^{28} = 805.306.368$ côtés, donnant π exact à 16 chiffres après la virgule : $3,1415926535897932$.

1579 Viète (France) calcule le périmètre du polygone à 393.216 côtés et donne $\pi \simeq 3,141592654$, ce qui est correct à 9 chiffres après la virgule.

2.4 Construction des Polygones Réguliers

Construire à la règle et au compas un polygone régulier à n côtés, pour chaque $n \geq 3$.

A nouveau, ce problème est légitime, puisqu'Euclide donne les constructions des polygones réguliers à 3, 4, 5, 6, 15 côtés et mentionne que l'on peut facilement doubler les côtés d'un polygone. Pourtant, ce ne fut qu'en 1796 que Gauss, du haut de ses 19 ans, construisit un sixième polygone régulier ayant 17 côtés [Carrega, 9].

Evidemment, comme tout mathématicien qui se respecte, beaucoup ont essayé de résoudre ces problèmes à la règle et au compas, et voyant que ce n'était pas possible (ou en tout cas beaucoup plus difficile qu'ils ne le pensaient), ont essayé d'autre moyens. Un de ces moyens est de passer par des courbes auxiliaires. Par exemple, et nous les étudierons plus tard, toujours en Grèce Antique, Dioclès trissecta l'angle et doubla le cube avec sa cissoïde, et Dinostrate réussi à quarrer le cercle grâce à sa quadratrice.

Chapitre 3

De la Géométrie à l'Algèbre

Les quatre problèmes que nous souhaitons résoudre sont purement géométriques en tant que tels. Toutefois, alors que les grecs étaient loin d'avoir cette puissance mathématique, il nous faut recourir à l'algèbre, afin de déterminer si ces problèmes sont résolubles à la règle et au compas. Le présent chapitre est consacré donc au passage de termes géométriques (points constructibles à la règle et au compas) à des termes algébriques (nombres dit constructibles). On pourra ensuite traduire les problèmes originaux dans un vocabulaire mathématique plus moderne.

3.1 Points et Nombres Constructibles

Essayons tout d'abord de comprendre de manière intuitive ce que pourrait être un point constructible à la règle et au compas.

3.1.1 L'idée

Soit un ensemble fini de points $\mathscr{P}$.

Ne travaillant qu'à la règle et au compas, les seuls objets géométriques que l'on utilise sont les droites et les cercles. Les deux types de construction offerts sont donc :

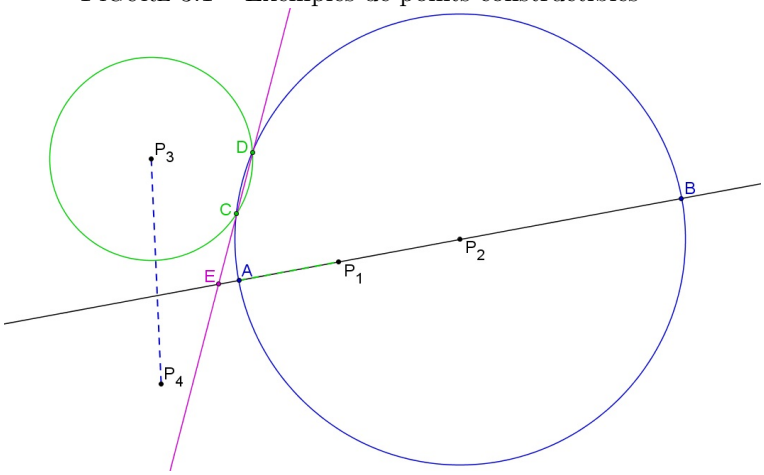
1. Tracer une droite passant par deux points de $\mathscr{P}$
2. Tracer un cercle centré en un point de $\mathscr{P}$, avec la distance entre deux points de $\mathscr{P}$ pour rayon.

En construisant de tels objets, de nouveaux points viennent à l'existence : les points d'intersections entre deux droites, une droite et un cercle, ou deux cercles. Ces points peuvent à leur tour être utilisés pour des constructions futures (tout comme les points de $\mathscr{P}$).

Exemple 1 (voir Figure 3.1)**.** Soit $\mathscr{P} = \{P_1, \ldots, P_4\}$. On trace une droite passant par P_1 et P_2 et un cercle de centre P_2 et de rayon $[P_3P_4]$, $C_{P_2,[P_3P_4]}$, coupant (P_1P_2) en A et B. On trace ensuite le cercle $C_{P_3,[AP_1]}$, qui coupe $C_{P_2,[P_3P_4]}$ en C et D. La droite (CD) peut être tracée, coupant (P_1P_2) en E. Beaucoup d'autres points d'intersections peuvent être obtenus en continuant cette construction, et tous peuvent être utilisés pour construire d'autres droites, cercles, points d'intersections, et ainsi de suite...

Un point constructible à la règle et au compas est donc un point créé par construction de droites et de cercles à partir de l'ensemble de points $\mathscr{P}$. Dans notre exemple 1, l'**ensemble des points constructibles** peut donc être noté :

FIGURE 3.1 – Exemples de points constructibles



$\mathscr{M} = \mathscr{P} \cup \{A, \ldots, E\} \cup \{$tous les autres points d'intersection que l'on peut obtenir par la suite$\}$. C'est cette notion intuitive qui amène à la définition formelle suivante :

Définition 1. [Carrega, 14] Soit $\mathcal{E}$ le plan euclidien et $\mathscr{P}$ un sous-ensemble fini de $\mathcal{E}$ ayant au moins deux éléments (appelés **points de base**). Un **point** M de $\mathcal{E}$ est dit **constructible** à la règle et au compas à partir de $\mathscr{P}$ s'il existe une suite de points de $\mathcal{E}$: $M_1, M_2, \ldots, M_n = M$ telle que pour tout $1 \leq i \leq n$, M_i est un point d'intersection :

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

ces droites et cercles étant obtenus à partir de l'ensemble de points

$$\mathscr{B}_i = \mathscr{P} \cup \{M_1, \ldots, M_{i-1}\},$$

de sorte que :

- chaque droite soit **constructible**, c'est-à-dire passe par deux points distincts de $\mathscr{B}_i$,
- chaque cercle soit **constructible**, c'est-à-dire centré en un point de $\mathscr{B}_i$ et a pour rayon la distance entre deux points de $\mathscr{B}_i$.

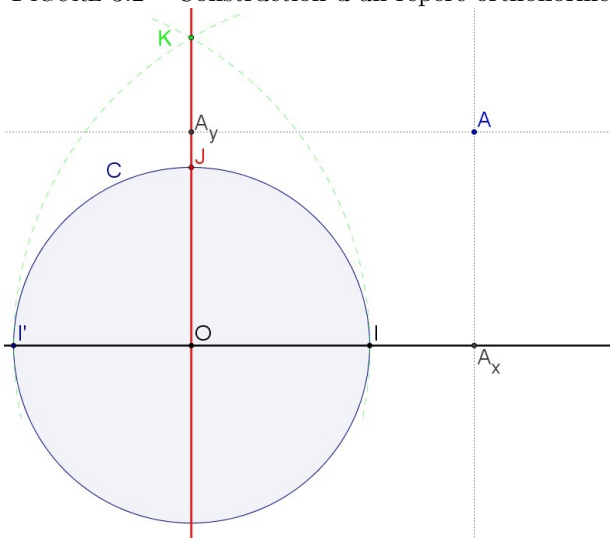
Remarque 1. Si $\mathscr{P}$ ne contient qu'un seul point de base, il est l'unique point constructible, puisque ni droites ni cercles ne peuvent être construits. Par contre, avec deux points de base, une droite et deux cercles sont constructibles, et forment à leur tour des points d'intersection constructibles et utilisables par la suite. Donc, comme le sous-entend la définition précédente, $\mathscr{P}$ peut être réduit à deux points de base, et c'est dans ce cadre que nous travaillerons dorénavant.

Afin de faciliter les arguments qui vont suivre, une convention importante doit être établie : le repère orthonormé. Ce repère est constructible à partir des deux points de base requis de $\mathscr{P}$, notés O et I.

3.1.2 Construction d'un Repère Orthonormé

On commence donc par $\mathscr{P} = \{O, I\}$ et la droite passant par ces deux points. Euclide a montré dans ses *Eléments* qu'il est possible de tracer la droite perpendiculaire à une droite donnée passant par un point quelconque, en l'occurence

FIGURE 3.2 – Construction d'un repère orthonormé



O [Euclide, 9, 10]. Nous notons J l'intersection de cette droite avec le cercle $\mathcal{C} = C_{O,[OI]}$ appelé le **cercle unité**. Le **repère orthonormé**, noté $\mathscr{R}(O, I, J)$, est ainsi construit, et tout point A est représenté par une abscisse A_x et une ordonnée A_y obtenues par **projection orthogonale** sur les axes x et y de $\mathscr{R}(O, I, J)$ (voir Figure 3.2).

3.1.3 Nombres Constructibles

Maintenant que les points constructibles sont bien définis et qu'un repère orthonormé est fondé, on peut définir les nombres constructibles :

Définition 2. [Carrega, 16] Un **nombre** réel est dit **constructible** si c'est une coordonnée d'un point constructible dans $\mathscr{R}(O, I, J)$. On note $\mathscr{C}$ l'**ensemble des nombres constructibles** obtenus à partir des points de bases O et I.

Exemple 2 (voir Figure 3.2)**.** Les points O, I, J, I', K formés dans la construction de $\mathscr{R}(O, I, J)$ étant tous constructibles, il est clair que $0, 1, -1, \sqrt{3}$ sont des nombres constructibles, puisqu'ils sont tous une coordonnée d'un de ces points.

Cette définition amène naturellement au résultat suivant :

PROPOSITION 1. *[Carrega, 18] Le nombre $a \in \mathbb{R}$ est constructible si et seulement si le point de l'axe des x de $\mathscr{R}(O, I, J)$ d'abscisse a est constructible.*

Démonstration. On suppose le point de l'axe des x de $\mathscr{R}(O, I, J)$ d'abscisse a constructible. Le réel a est donc constructible par définition (cf. Définition 2).

On suppose maintenant a constructible. Par définition toujours, c'est une coordonnée d'un point constructible A. Nous pouvons donc prendre les projections orthogonales de A sur les axes de $\mathscr{R}(O, I, J)$ (cf. Figure 3.2) et on obtient les points constructibles A_x et A_y.

Si a est l'abscisse de A, A_x est le point cherché.

Si a est l'ordonnée de A, le point cherché est le point d'intersection de l'axe des x avec le cercle constructible $C_{O,[OA_y]}$. □

Il est maintenant clair qu'il existe une forte relation entre les points et les nombres constructibles. Qu'en est-il de la notion d'angle constructible ?

3.1.4 Angles Constructibles

Tout d'abord prenons la définition classique d'un angle comme l'a donné Euclide.

Définition 3. La définition classique est comme suit : "Un angle plan est l'inclinaison l'une vers l'autre de deux droites dans un plan qui se coupent mais ne sont pas confondues" (traduction PvB [Euclide, 1]). En de termes plus modernes, un **angle** est formé par deux demi-droites se coupant en un seul point. Il est noté par un triplet ordonné orienté $(A, [AB), [AC))$, où $[AB), [AC)$ sont les demi-droites d'origine O passant par A, B respectivement.

Via la règle et le compas, on peut translater tout angle en un angle de la forme $(O, [OI), [OM))$ de même mesure, M étant un point de $\mathscr{C}$ uniquement déterminé [Euclide, 18]. La notion d'angle constructible se résume ainsi à la définition suivante.

Définition 4. Soit M un point de $\mathcal{C}$. L'**angle** $(O, [OI), [OM))$ est dit **constructible** si M est un point constructible. Notant $\widehat{IOM} = \theta \in [0, 2\pi]$ sa mesure, cela est équivaut à dire que $\cos\theta$ est un nombre constructible, par la proposition 1.

Remarque 2. Plus tard, on aura besoin de la notion d'**angle trissectable**. La définition d'un tel objet découle directement de la définition 4 : $(O, [OI), [OM'))$ est dit trissectable si le point M de $\mathcal{C}$ tel que $\dfrac{\widehat{IOM}}{3} = \dfrac{\theta}{3}$ est constructible à partir des points de base O, I, M. Ce qui équivaut à dire que $\cos\dfrac{\theta}{3}$ est un nombre constructible.

Il pourrait sembler que cette relation entre points, angles et nombres constructibles n'est qu'une différence d'interprétation, mais le point de vue géométrique et le point de vue algébrique sont en fait parfaitement complémentaires. Comme mentionné en introduction de ce chapitre, afin de pouvoir donner une solution satisfaisante aux quatre problèmes grecs, il faut passer d'un point de vue à l'autre afin de reformuler ces problèmes en termes algébriques. Etudions donc plus en détails le nouvel ensemble de nombres décrit dans cette section.

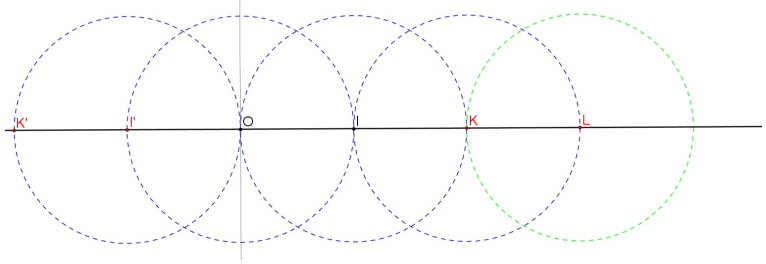
3.2 Le Corps des Nombres Constructibles

En quelques sortes, nous reprenons dans cette section le travail de Descartes qui, dans sa *Géométrie* (1637), montre que l'on peut construire des segments de longueurs $a+b, |a-b|, ab, \dfrac{a}{b}, \sqrt{a}$ à partir des segments a et b. Il démontre ensuite qu'à partir de longueurs données, toute longueur peut s'exprimer algébriquement et à l'aide des racines carrées [Carrega, 10]. Regardons donc concrètement ce que sont les nombres constructibles à la règle et au compas.

3.2.1 Recherche de Nombres Constructibles

- Etant donné la droite passant par O et I, on construit des cercles de rayon $[OI]$ et de centre O, I, ainsi que tous les points d'intersection entre ces cercles et la droite (OI) (voir figure 3.3). Il est facile de voir que cette construction forme l'anneau des entiers relatifs : O étant 0 ; I et I' étant 1 et -1 ; K et K', 2 et -2 ; L, 3 ; etc...
- La construction suivante permet de construire le corps de nombres rationnels. Elle utilise le Théorème de Thalès et nécessite donc deux droites se coupant en un point, par exemple le repère $\mathscr{R}(O, I, J)$ de la figure 3.2.

FIGURE 3.3 – Construction des entiers relatifs

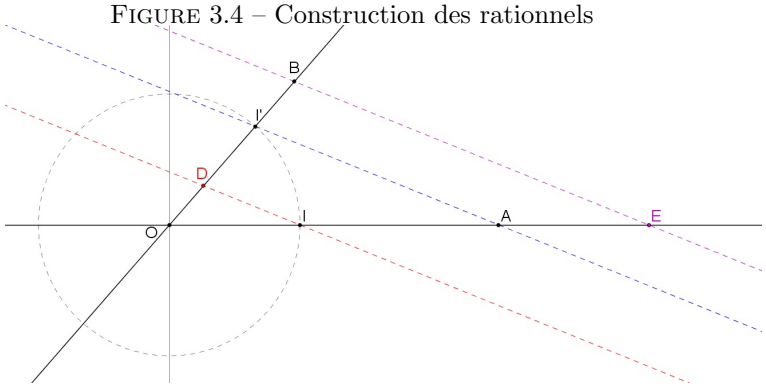


On se place plutôt dans la situation générale ici : On commence donc par la droite (OI) coupée par une autre droite en O, et sur lesquelles sont construits deux nombres a et b représentés par les points A et B. On reporte le point I sur l'autre droite à l'aide du cercle $\mathcal{C}$ et on nomme ce point I'. Les points A et I' peuvent, donc être reliés par une droite. Il est possible de construire la droite parallèle à (AI') passant par I et coupant (OB) en D [Euclide, (17, 18) 24]. On utilise maintenant le Théorème de Thalès :

$$\begin{aligned} & \frac{OI}{OA} = \frac{OD}{OI'} \\ \Leftrightarrow \quad & \frac{1}{a} = \frac{OD}{1} \end{aligned}$$

Donc le point D représente le nombre rationnel $\frac{1}{a}$.
De plus, la même construction (mais utilsant la parallèle à (AI') passant par B) donne le point E représentant le nombre constructible ab. Comme a et b sont arbitraires, il est donc évident que tous les nombres rationnels sont ainsi constructibles.

FIGURE 3.4 – Construction des rationnels

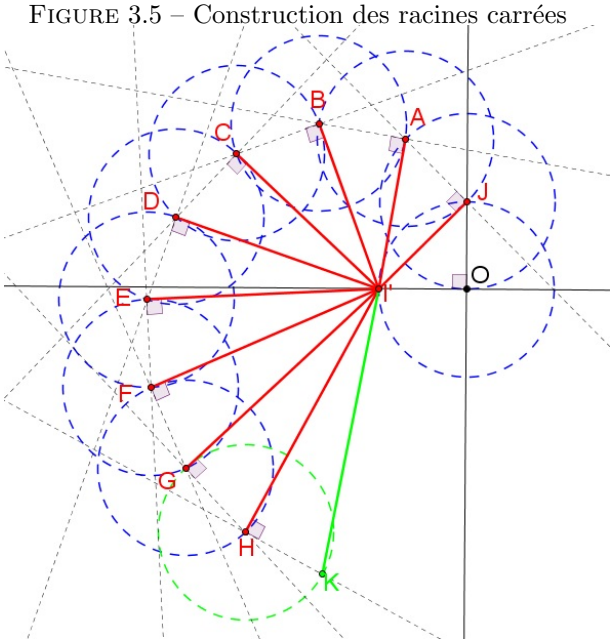


– En plus du corps des nombres rationnels, grâce au Théorème de Pythagore, les racines carrées sont aussi constructibles. On commence à nouveau par (OI) :
Comme nous travaillons avec des triangles rectangles, on se place dans $\mathscr{R}(O, I, J)$. Le segment $[I'J]$ mesure donc $\sqrt{2}$ (voir Figure 3.5). On construit alors le point d'intersection A entre la perpendiculaire à $[I'J]$ passant par

J, ainsi que le cercle $C_{J,1}$. Par le Théorème de Pythagore, on trouve :

$$\begin{aligned} & I'A = \sqrt{I'J^2 + JA^2} \\ \Leftrightarrow \quad & I'A = \sqrt{(\sqrt{2})^2 + 1^2} \\ \Leftrightarrow \quad & I'A = \sqrt{2+1} = \sqrt{3} \end{aligned}$$

FIGURE 3.5 – Construction des racines carrées



On reprend la même construction partant de $[JA]$: B est le point d'intersection entre la perpendiculaire à $[JA]$ passant par A et le cercle $C_{A,1}$. Par Pythagore, on trouve :

$$\begin{aligned} & I'B = \sqrt{I'A^2 + AB^2} \\ \Leftrightarrow \quad & I'B = \sqrt{3+1} = \sqrt{4} = 2 \end{aligned}$$

On obtient de la sorte : $I'C = \sqrt{5}$, $I'D = \sqrt{6}$, $I'E = \sqrt{7}$, $I'F = \sqrt{8}$, $I'G = \sqrt{9} = 3$, $I'H = \sqrt{10}$, $I'K = \sqrt{11}$, et ainsi de suite... Il est donc clair qu'il est possible en toute généralité de construire les racines de rationnels.

Forts de ces constructions concrètes de nombres constructibles, nous pouvons nous concentrer sur une étude formelle de $\mathscr{C}$, appelé le corps des nombres constructibles.

3.2.2 Etude Formelle du Corps des Nombres Constructibles

THEOREME 1. *L'ensemble des nombres constructibles $\mathscr{C}$ est le plus petit sous-corps de $\mathbb{R}$ stable par racine carrée.*

Démonstration. Le fait que $\mathscr{C} \subset \mathbb{R}$ est évident, par définition (cf. définition 2). Posons $\mathscr{C}_0$ le plus petit sous corps de $\mathbb{R}$ stable par racine carrée. Ce sous-corps de $\mathbb{R}$ existe car

$$\mathscr{C}_0 = \bigcap_{\substack{\{\mathbb{K} \text{ tel que } \mathbb{Q} \subset \mathbb{K} \subset \mathbb{R} \text{ et} \\ \mathbb{K} \text{ stable par racine carrée}\}}} \mathbb{K}.$$

Il nous faut donc montrer que $\mathscr{C} = \mathscr{C}_0$. Dans un premier temps on montre que $\mathscr{C}_0 \subset \mathscr{C}$, en montrant que $\mathscr{C}$ est un corps stable par racine carrée.

0. Il est clair que $0, 1 \in \mathscr{C}$, car ce sont les abscisses des points de bases O et I.
1. Soit $a \in \mathscr{C}$. $-a \in \mathscr{C}$: Par la figure 3.3, il est clair que si A est le point de l'axe des x d'abscisse a, on construit le point A' d'abscisse $-a$ en coupant la droite (OI) par $C_{O,[OA]}$.
2. Soient a et $b \in \mathscr{C}$. $a+b \in \mathscr{C}$: Par la figure 3.3, nous voyons clairement que si A et B sont deux points de l'axe des x d'abscisses a et b respectivement, on construit le point C d'abscisse $a + b$ en coupant la droite (OI) par $C_{B,[OB]}$.
3. Soient $a \in \mathscr{C}$. $\dfrac{1}{a} \in \mathscr{C}$: évident par la figure 3.4.
4. Soient a et $b \in \mathscr{C}$. $ab \in \mathscr{C}$: clair par la figure 3.4.

En effet, dans la figure 3.4, a, b sont supposés éléments de $\mathbb{N}$, mais il évident que la figure est valable pour tout $a, b \in \mathbb{R}^+$.

5. Soit $a \in \mathscr{C}$. $\sqrt{a} \in \mathscr{C}$: Nous avons montré qur si $a \in \mathbb{Q}$ alors $\sqrt{a} \in \mathscr{C}$. Il nous faut désormais montrer qu'étant donné $p \in \mathscr{C}, \sqrt{p}$ est constructible. Nous savons par les points 2. et 4. que $k = \dfrac{p-1}{2}$ et $h = \dfrac{p+1}{2}$ sont constructibles. Il est possible de construire un triangle rectangle ayant h pour son hypoténuse, et k et m pour ses autres côtés.
Par Pythagore on trouve bien :

$$\begin{aligned} m &= \sqrt{\left(\frac{p+1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2} \\ &= \sqrt{\frac{1}{4}(p^2 + 2p + 1 - p^2 + 2p - 1)} \\ &= \sqrt{p} \end{aligned}$$

Il nous reste à montrer l'autre inclusion : $\mathscr{C} \subset \mathscr{C}_0$, c'est-à-dire que $\mathscr{C}$ est *le plus petit* sous-corps de $\mathbb{R}$ stable par racine carrée. Pour cela, il faut montrer que tout point constructible a ses coordonnées dans $\mathscr{C}_0$. En d'autres termes, reprenant la définition 1, il nous faut montrer que le n-ième nombre construit est obtenu à partir des précédents par les opérations décrites ci-dessus. Pour montrer ceci, on utilise les lemmes suivants.

Lemme 1. *[Escofier, 71] Soit M l'ensemble des points dans $\mathscr{R}(O, I, J)$ de coordonnées dans un corps $\mathbb{K}$ tel que $\mathbb{Q} \subset \mathbb{K} \subset \mathbb{R}$. Toute droite constructible est donnée sous forme algébrique par*

$$ax + by - c = 0,$$

et tout cercle constructible par

$$(x - d)^2 + (y - e)^2 - f^2 = 0,$$

avec $a, \ldots, f \in \mathbb{K}$.

Démonstration. 1. Nous savons que l'équation de la droite passant par les points $A(a_1, a_2)$ et (b_1, b_2) se donne sous la forme

$$\begin{aligned} &(b_1 - a_1)(y - a_2) = (x - a_1)(b_2 - a_2) \\ \Leftrightarrow\ &(b_2 - a_2)x + (a_1 - b_1)y + (a_2 - b_2)a_1 + (b_1 - a_1)a_2 = 0, \end{aligned}$$

qui est de la forme recherchée et $a = a_2 - b_2, b = b_1 - a_1$, et $c = (a_1 - b_1)a_2 + (b_2 - a_2)a_1$ sont évidemment dans $\mathbb{K}$.

2. Nous savons que l'équation du cercle $C_{D,[AB]}$ centré en $D(d_1, d_2)$ et de rayon $[A(a_1, a_2)B(b_1, b_2)]$ se donne sous la forme

$$\begin{aligned}&(x-d_1)^2+(y-d_2)^2=(b_1-a_1)^2+(b_2-a_2)^2\\ \Leftrightarrow\ &x^2+y^2-2c_1x-2c_2y+c_1^2+c_2^2-(b_1-a_1)^2-(b_2-a_2)^2=0\end{aligned}$$

qui est de la forme recherchée et $a = c_1, b = c_2$, et $c = c_1^2+c_2^2-(b_1-a_1)^2-(b_2-a_2)^2$ sont évidemment dans $\mathbb{K}$.

□

Utilisons ce résultat dans le cadre de $\mathscr{C}$.

Lemme 2. *[Escofier, 72] Tout point constructible $M \in \mathscr{M}$ a ses coordonnées dans $\mathscr{C}_0$.*

Démonstration. Par définition, il existe une suite de points $M_1 = O, M_2 = I, \ldots, M_n = M$ (cf. Définition 1). Procédons par récurrence. Si $n = 1$ ou 2, tout est vérifié, puisque $0, 1 \in \mathscr{C}_0$. Supposons donc que $M_1, \ldots, M_{n-1}$ ont leurs coordonnées dans $\mathscr{C}_0$. Alors M est obtenu par intersection de i) deux droites, ii) une droite et un cercle, ou iii) deux cercles d'équations algébriques $ax+by-c = 0$ et $(x-d)^2+(y-e)^2-f^2 = 0$, avec $a, \ldots, f \in \mathscr{C}_0$.

i) Regardons le cas ou M est l'intersection de deux droites :
Nous devons résoudre le système d'équations

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

avec a' supposé non-nul, et $ab'-a'b \neq 0$, puisque nous supposons les deux droites sécantes. On trouve d'abord de la première équation que $x = \dfrac{-c-by}{a}$, ce qui par substitution dans la seconde équation donne que

$$y = \frac{a'c-ac'}{b'a-ba'} \quad \text{et} \quad x = \frac{-1}{a}\left(c+b\frac{a'c-ac'}{b'a-ba'}\right).$$

Comme, $a, b, c, a', b', c' \in \mathscr{C}_0$, on a $x, y \in \mathscr{C}_0$.

ii) Regardons le cas où M est l'intersection d'une droite et d'un cercle :
Nous devons résoudre le système d'équations

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

avec $a, b, c, a', b', c' \in \mathscr{C}_0$, et a supposé non-nul. Comme précédemment, $x = \dfrac{-c-by}{a}$, ce qui par substitution dans la seconde équation donne que

$$\begin{aligned}&\left(\frac{-c-by}{a}\right)^2-2a'\left(\frac{-c-by}{a}\right)+a'^2+y^2-2b'y+b'^2-c'^2=0\\ \Leftrightarrow&\frac{c^2+2cby+b^2y^2}{a^2}+\frac{2a'c+2a'by}{a}+a'^2+y^2-2b'y+b'^2-c'^2=0;\end{aligned}$$

ce qui à son tour nous donne l'équation :

$$\mathfrak{A}y^2+\mathfrak{B}y+\mathfrak{C}=0, \tag{3.1}$$

où $\mathfrak{A} = \dfrac{b^2}{a^2} + 1, \mathfrak{B} = \dfrac{2cb + 2a'ba}{a^2} - 2b',$ et $\mathfrak{C} = \dfrac{c^2 + 2a'ca}{a^2} + a'^2 + b'^2 - c'^2$ sont dans $\mathscr{C}_0$. L'équation (3.1) est de forme quadratique, se qui implique que

$$y = \frac{-\mathfrak{B} \pm \sqrt{\mathfrak{B}^2 - 4\mathfrak{A}\mathfrak{C}}}{2\mathfrak{A}} \quad \text{et} \quad x = \frac{-1}{a}\left(c + b\frac{-\mathfrak{B} \pm \sqrt{\mathfrak{B}^2 - 4\mathfrak{A}\mathfrak{C}}}{2\mathfrak{A}}\right)$$

sont donc dans $\mathscr{C}_0$.

iii) Regardons le cas oùM est l'intersection de deux cercles :
Nous devons résoudre le système de ces deux équations. Plusieurs cas s'offrent à nous :
- Si les cercles sont concentriques ($(a, b) = (a', b')$) :

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

  alors si $c = c'$ on a une infinité de solutions, sinon il n'y en a pas.
- Si les cercles ne sont pas concentriques ($(a, b) \neq (a', b')$), quelques manipulations sont nécessaires afin de rendre les calculs plus faciles.
  D'abord ramenons un des cercles au cercle unité par translation et homothétie :

$$\begin{cases} (x-a)^2 + (y-b)^2 - c^2 &= 0 \\ (x-a')^2 + (y-b')^2 - c'^2 &= 0 \end{cases} \Leftrightarrow \begin{cases} x^2 + y^2 - 1 &= 0 \\ (x-\mathsf{A})^2 + (y-\mathsf{B})^2 - \mathsf{C}^2 &= 0 \end{cases},$$

  où $\mathsf{A} = a' - a, \mathsf{B} = b' - b,$ et $\mathsf{C} = \dfrac{c'}{c}$ sont dans $\mathscr{C}_0$.
  Or, il est clair que ce dernier système d'équation se ramène au système suivant en soustrayant la seconde équation de la première :

$$\begin{cases} x^2 + y^2 - 1 &= 0 \\ 2\mathsf{A}x + 2\mathsf{B}y - \mathsf{A}^2 - \mathsf{B}^2 + \mathsf{C}^2 - 1 &= 0, \end{cases}$$

  ce qui nous ramène au cas précédent, puisque cette nouvelle seconde équation est de forme linéaire, et donc $x, y \in \mathscr{C}_0$.

□

D'après le lemme 2 tout nombre constructible est dans $\mathscr{C}_0$ i.e. $\mathscr{C} \subset \mathscr{C}_0$. L'ensemble des nombres constructibles $\mathscr{C}$ est donc bien le plus petit sous-corps de $\mathbb{R}$ stable par racine carrée par définition de $\mathscr{C}_0$, et nous arrivons donc à la même conclusion que Descartes tire au $17^{\text{ième}}$ siècle, à savoir que tout point constructible se trouve par résolution d'équations du premier et second degré. ■

Nous disposons maintenant de tous les outils nécessaires à la traduction des quatre problèmes antiques.

3.3 Traduction des Problèmes Géométriques en Problèmes Algébriques

Ecrivons donc les quatre problèmes sous forme algébrique.

3.3.1 Duplication du Cube

Soit un cube donné quelconque.
Construire à la règle et au compas l'arête d'un cube ayant un volume deux fois plus grand que celui du cube donné.

Etant donné un cube d'arête a, on cherche un cube d'arête ax tel que

$$(ax)^3 = 2a^3 \Leftrightarrow x^3 = 2.$$

La question est donc de savoir si le polynôme $P(X) = X^3 - 2$ admet une racine dans $\mathscr{C}$.

3.3.2 Trissection de l'Angle

Soit un angle donné quelconque.
Construire à la règle et au compas les demi-droites divisant cet angle en trois parties égales.

Remarque 3. Afin de rester dans la construction sur deux points de bases, on se réduit à la trissection des angles constructibles.

Nous avons vu précédemment dans la définition 4 et la remarque 2 qui la suit qu'un angle constructible de mesure θ est trissectable si et seulement si le nombre $\cos\frac{\theta}{3}$ est constructible. Or, on sait que $\cos 3\phi = 4\cos^3\phi - 3\cos\phi$. Donc, pour qu'un angle θ soit trissectable, $\cos\frac{\theta}{3}$ doit pouvoir annuler l'expression :

$$4x^3 - 3x - \cos 3\theta.$$

La question est donc de savoir si le polynôme $P(X) = 4x^3 - 3x - \cos 3\theta$ admet une racine dans $\mathscr{C}$.

3.3.3 Quadrature du Cercle

Soit un cercle donné quelconque.
Construire à la règle et au compas un carré ayant même aire que ce cercle.
Cela revient donc à construire, à partir d'un cercle d'aire πr^2, un carré de côté xr tel que

$$(xr)^2 = \pi r^2 \Leftrightarrow x^2 = \pi.$$

La question est donc de savoir si le polynôme $P(X) = X^2 - \pi$ admet une racine dans $\mathscr{C}$.

3.3.4 Construction des Polygones Réguliers

Construire à la règle et au compas un polygone régulier à n côtés, pour chaque $n \geq 3$.

Pour ce problème-ci, il est aussi question d'angles constructibles, car un polygone régulier à n côtés est constructible si et seulement si son angle central $\widehat{\frac{2\pi}{n}}$ est constructible, ou encore si et seulement si $\cos\frac{2\pi}{n}$ ou même $e^{\frac{2i\pi}{n}}$ sont constructibles.

Nous verrons plus en détails plus tard que ce problème se traduit comme suit : le polynôme régulier à n côtés est constructible si et seulement si le point $e^{\frac{2ik\pi}{n}}$ (d'abscisse $\cos\frac{2k\pi}{n}$), pour $1 \leq k \leq n$, est constructible pour $k \wedge n = 1$, c'est-à-dire si k et n sont premiers entre eux.

On introduit alors le polynôme nommé le **n-ième polynôme cyclotomique**

$$\Phi_n(X) = \prod_{k \wedge n = 1} X - e^{\frac{2ik\pi}{n}}.$$

La question est donc de savoir si le polynôme $\Phi_n(X)$ admet une racine dans $\mathscr{C}$.

Avant de pouvoir donner une solution à ces problèmes, une brève esquisse de la théorie des corps est nécessaire, ce qui est le sujet du prochain chapitre.

Chapitre 4

Rudiments de Théorie des Corps

Comme nous venons de l'établir, déterminer la constructibilité de points géométriques équivaut à trouver des racines de polynômes dans le corps $\mathscr{C}$. Certains résultats de la théorie des corps sont donc indispensables pour pouvoir continuer notre discussion vers la résolution des quatre problèmes originaux.

(Tous les corps mentionnés ci-après sont supposés commutatifs.)

4.1 Polynômes et Irréductibilité

L'ensemble des polynômes en l'indéterminée X et à coefficients dans le corps K est noté $K[X]$. C'est un anneau commutatif pour l'addition et la multiplication.

4.1.1 $\mathbb{Z}$ versus $K[X]$

L'anneau $K[X]$ et l'anneau $\mathbb{Z}$ partagent de nombreuses propriétés, car ils possèdent tous les deux une division euclidienne. Examinons cela plus en détails.

1. Propriétés de l'anneau $\mathbb{Z}$[Carrega, 171] :
   (a) Division euclidienne : $a, b \in \mathbb{Z}$, avec $b \neq 0, \Rightarrow \exists\ q, r \in \mathbb{Z}$ uniques, tels que $a = bq + r$ avec $0 \leq r < |b|$.
   (b) $\mathbb{Z}$ est principal : Tout idéal I de $\mathbb{Z}$, c'est-à-dire tout sous-groupe additif I de $\mathbb{Z}$ vérifiant : $ax \in \mathbb{Z}, \forall a \in \mathbb{Z}$ et $x \in I$, est de la forme $n\mathbb{Z} := \{na | a \in \mathbb{Z}\}$, pour $n \in \mathbb{N}$.
   (c) Théorème de Bezout : $a, b \in \mathbb{Z}$ tels que $a \wedge b = 1, \Rightarrow \exists u, v \in \mathbb{Z}$ tels que $au + bv = 1$.
   (d) Théorème de Gauss :
   – $a \wedge b = 1$ et $a|bc, \Rightarrow a|c$.
   – a premier et $a|bc, \Rightarrow a|b$ ou $a|c$.
   (e) $\mathbb{Z}$ est factoriel : Tout élément de $\mathbb{Z}$ (différent de 0, 1, -1) s'écrit de manière unique sous la forme $\pm p_1 p_2 \dots p_n$, où les p_i sont premiers.
2. Propriétés de l'anneau $K[X]$[Carrega, 171-74] :
   (a) Division euclidienne : $f, g \in K[X]$, avec $g \neq 0, \Rightarrow \exists\ q, r \in K[X]$ uniques, tels que $f = gq + r$ avec $r = 0$ ou $\deg r < \deg g$.
   (b) $K[X]$ est principal : Tout idéal I de $K[X]$ est de la forme $fK[X] := \{fq | q \in K[X]\}$, pour $f \in I$. On notera un tel idéal (f).

(c) Théorème de Bezout : $f, g \in K[X]$ tels que $f \wedge g = 1, \Rightarrow \exists u, v \in K[X]$ tels que $fu + gv = 1$.

Avant de pouvoir continuer par le Théorème de Gauss, il faut définir ce qu'est un polynôme irréductible.

Définition 5. [Carrega, 173] Soit $f \in K[X]$.
- Si $f = gh$, avec $g, h \in K[X]$ non-constants, alors f est un **polynôme** dit **réductible** dans $K[X]$.
- Si f n'est pas réductible est non-constant dans $K[X]$, f est dit **irréductible** dans $K[X]$.

2. (d) Théorème de Gauss : Soient $f, g, h \in K[X]$.
   - $f \wedge g = 1$ et $f|gh, \Rightarrow f|h$.
   - f irréductible et $f|gh, \Rightarrow f|g$ ou $f|h$. Plus généralement, $f|g_1 g_2 \dots g_n, \Rightarrow f|g_i$, pour un $i \in \{1, \dots, n\}$.

   (e) $K[X]$ est factoriel : Tout polynôme non-constant de $K[X]$ s'écrit de manière unique sous la forme $f = kf_1 f_2 \dots f_n$, avec $k \in K^*$, et les f_i étant des polynômes unitaires, c'est-à-dire ayant le coefficient de leur monôme de plus haut degré égal à 1, irréductibles dans $K[X]$.

Cela établi, regardons maintenant l'irréductibilité d'un polynôme plus en détails.

4.1.2 Irréductibilité

PROPOSITION 2. *[Carrega, 176] Si $f \in K[X]$ et $a \in K$, alors a est racine de f si et seulement si $(X - a)|f$.*

Démonstration. Par division euclidienne nous avons que

$$f = (X - a)q + r,$$

avec $r = 0$ ou $\deg r < 1$, c'est à dire $r \in \mathbb{R}$.

Si a est une racine de f, $f(a) = 0$ d'où $r = 0$ et $(X - a)|f$.

Réciproquement, si $(X - a)|f$ alors $r = 0$ et $f(a) = 0$. Donc, a est une racine de f. □

PROPOSITION 3. *[Carrega, 176] Soit $f \in K[X]$,*

1. $\deg f = 1 \Rightarrow f$ *est irréductible dans* $K[X]$
2. $\deg f \geq 2$ *et* f *irréductible* $\Rightarrow f$ *n'a pas de racine dans* K
3. $\deg f = 2$ *ou* 3 *et* f *n'a pas de racine dans* $K \Rightarrow f$ *est irréductible dans* $K[X]$.

Démonstration. 1. Evident.

2. Découle de la proposition 2
3. Par contraposée, nous supposons f réductible dans $K[X]$ et de degré 2 (resp. 3). Le polynôme f se décompose en un produit d'un facteur de premier degré en d'un autre de premier (resp. second) degré, tous deux à coefficients dans K. Donc f a une racine dans K.

□

Dans notre cas précis, nous avons surtout besoin de pouvoir déterminer si les polynômes trouvés à la fin du chapitre précédent sont irréductibles sur $\mathbb{Q}[X]$.

Les coefficients de f pouvant être réduis au même dénominateur, il existe $k \in \mathbb{N}^*$ tel que $kf \in \mathbb{Z}[X]$. Ceci nous permet donc d'étudier l'irréductibilité de polynômes dans $\mathbb{Z}[X]$, au lieu de $\mathbb{Q}[X]$ [Escofier, 50, 51].

1. Recherche de racines dans $\mathbb{Q}[X]$

Soit $f(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0$ un polynôme de $\mathbb{Z}[X]$, avec a_n et a_0 non-nuls. Soit $\frac{p}{q} \in \mathbb{Q}$ sous forme irréductible.

Si $\frac{p}{q}$ est racine de f, alors

$$q^n f\left(\frac{p}{q}\right) = a_n p^n + a_{n-1} p^{n-1} q + \ldots + a_0 q^n = 0,$$

et par le théorème de Gauss pour $\mathbb{Z}$, $p|a_0$ et $q|a_n$. Or, comme a_0 et a_n n'admettent qu'un nombre fini de diviseurs, il n' y a qu'un nombre fini de $\frac{p}{q}$ qui soient racines de f. Nous pouvons ensuite utiliser la proposition 3 qui nous donne :

- f possède une racine dans $\mathbb{Q}$ et $\deg f \geq 2 \Rightarrow f$ réductible dans $\mathbb{Q}[X]$,
- f n'a pas de racine dans $\mathbb{Q}$ et $\deg f = 2$ ou $3 \Rightarrow f$ est irréductible dans $\mathbb{Q}[X]$.

2. Réduction à $\frac{\mathbb{Z}}{p\mathbb{Z}}[X]$

Souvent il est pratique de passer de l'anneau $\mathbb{Z}$ aux anneaux $\frac{\mathbb{Z}}{p\mathbb{Z}}$.

S'il existe un nombre p premier tel que l'image du polynôme $P(X)$ dans $\frac{\mathbb{Z}}{p\mathbb{Z}}[X]$ soit un polynôme irréductible de même degré, $P(X)$ est alors irréductible si le pgcd de ces coefficients est 1. Par contre, si le degré de son image dans $\frac{\mathbb{Z}}{p\mathbb{Z}}[X]$ est strictement inférieur, on ne peut rien conclure.

On peut prouver l'irréductibilité d'un polynôme dans $\frac{\mathbb{Z}}{p\mathbb{Z}}[X]$ de manière suivante :

- Si P est de degré 2 ou 3, on peut tester les éléments de $\frac{\mathbb{Z}}{p\mathbb{Z}}[X]$ et voir s'ils sont racines de P.
- Si P est de degré n, on peut tester si les polynômes irréductibles de degré inférieur à $\frac{n}{2}$, étant de nombre fini, divisent P.

3. Autres méthodes

Il existe d'autres méthodes pour déterminer la réductibilité d'un polynôme à coefficients entiers de $\mathbb{Q}[X]$, comme le critère d'Eisenstein ; qui nous dit que s'il existe un nombre premier divisant tous les coefficients d'un polynôme à part celui du monôme de plus haut degré et de sorte que le carré de ce nombre premier ne divise pas le terme constant du polynôme, alors ce polynôme est irréductible dans $\mathbb{Q}[X]$; ou encore la méthode de changement de variables, mais comme nous n'en avons pas l'utilité dans le cadre présent, nous ne les développerons pas en long et en large.

Afin de répondre aux quatre problèmes du début, nous avons besoin d'un résultat bien précis qui caractérise tout nombre constructible à la règle et au compas. Pour cela, nous devons d'abord parler entre autres d'extension de corps et de nombres algébriques.

4.2 Extension de Corps

En termes simples, on dit que L est une **extension** de K si K est un sous-corps d'un corps L, et l'on note $K \subset L$. On peut considérer L comme un espace vectoriel sur K avec comme addition l'addition du corps L et comme multiplication externe la multiplication du corps L restreinte à $K \times L$. On appelle **degré de l'extension** L sur K la dimension de l'espace vectoriel L sur K. Il est noté $[L : K]$ [Carrega, 185-86].

Nous mentionnons le résultat suivant sans le démontrer, mais il sera néanmoins utile par la suite.

PROPOSITION 4. *[Carrega, 186] Soit $K \subset L \subset M$ où K, L, M sont des corps. Si $[M : L]$ et $[L : K]$ sont finis, alors $[M : K]$ est fini et $[M : K] = [M : K] \times [L : K]$.*

Aussi, si $a \in L$, on note $K(a)$ le plus petit sous-corps de L contenant K et a. Il est donné par l'intersection de tous les sous-corps de L contenant K et a.

Exemple 3. [Carrega, 23]

1. $\mathbb{Q}(3) = \mathbb{Q}(-\frac{9}{7}) = \mathbb{Q}$
2. $\mathbb{Q}(\sqrt{2}) = \{\alpha + \beta\sqrt{2} | \alpha, \beta \in \mathbb{Q}\}$
3. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{\alpha + \beta\sqrt{2} + \gamma\sqrt{3} + \delta\sqrt{6} | \alpha, \beta, \gamma, \delta \in \mathbb{Q}\}$
4. $\mathbb{R}(i) = \{\alpha + i\beta | \alpha, \beta \in \mathbb{R}\} = \mathbb{C}$

Exemple 4. [Carrega, 23]

- $\{1, \sqrt{2}\}$ est une base de $\mathbb{Q}(\sqrt{2})$ sur $\mathbb{Q} \Rightarrow [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$
- $\{1, \sqrt{3}\}$ est une base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sur $\mathbb{Q}(\sqrt{2}) \Rightarrow [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$
- $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \times [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \times 2 = 4$

Intéressons-nous maintenant aux nombres algébriques.

4.3 Nombres Algébriques et Polynôme Minimal

Définition 6. [Carrega, 186] Soit $K \subset L$ avec K, L deux corps. Si $a \in L$, on dit que a est **algébrique** sur K s'il existe un polynôme non-nul $P(X) \in K[X]$ tel que $P(a) = 0$.

Si a n'est pas algébrique sur K, il est dit **transcendant** sur K.

Exemple 5.

1. 3 est algébrique sur $\mathbb{Q}$, car 3 est racine de $X - 3$
2. $\sqrt{2}$ est algébrique sur $\mathbb{Q}$, car elle est racine de $P(X) = X^2 - 2$
3. De même, $\sqrt{3}$ est algébrique sur $\mathbb{Q}$, car $P(\sqrt{3}) = (\sqrt{3})^2 - 3 = 0$
4. i est algébrique sur $\mathbb{R}$ et sur $\mathbb{Q}$, car il est racine de $P(X) = X^2 + 1$

PROPOSITION 5. *[Carrega, 186] Si a algébrique sur K, alors il existe un polynôme unique $P(X) \in K[X]$, appelé le* **polynôme minimal***, tel que :*

- *$P(a) = 0$*
- *$P(X)$ est irréductible dans $K[X]$*
- *$P(X)$ est unitaire*

Démonstration. Posons F l'ensemble des $f \in K[X]$ tels que $f(a) = 0$. Il est clair que F est un idéal non-nul de $K[X]$, puisque a algébrique sur K et $(fh)(a) = 0$, $\forall h \in K[X]$.

L'anneau $K[X]$ étant principal, il existe un polynôme unitaire $P \in F$ tel que $F = \{Pq | q \in K[X]\}$. Donc $P(a) = 0$, P est unitaire, et divise tout polynôme de $K[X]$ ayant a pour racine.

Montrons que P est irréductible dans $K[X]$.

Par l'absurde, nous supposons P réductible, ce qui voudrait dire que $P = fg$ avec $f, g \in K[X]$ tels que $1 \leq \deg f < \deg P$, et $1 \leq \deg g < \deg P$. Or, $0 = P(a) = f(a)g(a)$ donc $f(a) = 0$ ou $g(a) = 0$ i.e. $f \in F$ ou $g \in F$, ce qui est impossible car le degré de f et de g est inférieur au degré de P. Donc, P doit être irréductible dans $K[X]$.

Montrons l'unicité de P.

Supposons que f vérifie les trois conditions du théorème. Conséquemment, P divise f et il existe $g \in K[X]$ tel que $f = Pg$. Or, f est irréductible et unitaire, et P est unitaire. Donc, $g = 1$ et $f = P$. □

Exemple 6.
1. Le polynôme minimal de 3 sur $\mathbb{Q}$ est $X - 3$
2. Le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$ est $X^2 - 2$.
3. De même pour $\sqrt{2}$ sur $\mathbb{Q}(\sqrt{3})$, car $X^2 - 2$ est irréductible dans $\mathbb{Q}(\sqrt{3})[X]$. Ceci revient à dire par la proposition 3 que $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$, ce qui est évident.
4. Le polynôme minimal de i sur $\mathbb{Q}$ et sur $\mathbb{R}$, est $X^2 + 1$

Une dernière proposition intéressante s'offre à nous.

PROPOSTION 6. *[Escofier, 52] Si a est algébrique sur K, $K(a)$ est isomorphe à $K[X]/(P)$, avec $P(X)$ le polynôme minimal de a, de plus*

$$[K(a) : K] = \deg P$$

appelé le degré de a.

Démonstration. Soit $f : K[X] \longrightarrow K(a)$ défini par $f(X) = a$ un morphisme d'anneau. On a

$$Q \in \ker f \Leftrightarrow Q(a) = 0,$$
$$\text{donc } \ker f = PK[X], \text{avec } P \text{ le polynôme de minimal } a.$$

On trouve donc $K[X] \twoheadrightarrow K[X]/(P) \hookrightarrow K(a)$.

Montrons que X a un inverse dans $K[X]/(P)$. On pose $P(X) = a + XQ(X)$, avec $a \in K$ non nul, puisque $P(X)$ est irréductible par la proposition 5. Donc on a

$$X^{-1} = -\frac{1}{a}Q(X),$$

d'où $K[X]/PK[X]$ est un corps et son image dans $K(a)$ contient K et a. On a donc bien un isomorphisme entre $K[X]/(P)$ et $K(a)$.

Or, on sait aussi que K[X]/(P), en tant que K-espace vectoriel, admet comme famille génératrice l'ensemble $\{a^k, 0 \leq k \leq \deg P - 1\}$. Cette famille est libre car s'il existe une combinaison linéaire non-triviale $\sum_{0 \leq k \leq \deg P - 1} \alpha_k a^k = 0$, avec $\alpha_k \in K$, alors on obtiendrait un polynôme non-nul annulant a et de degré strictement inférieur à celui de P, ce qui est absurde.

Or, on sait que $[K[X]/(P) : K] = \deg P$ qui est le cardinal de la base $\{X^k, 0 \leq k < \deg P\}$. Par l'isomorphisme trouvé plus haut, on a donc bien

$$[K(a) : K] = \deg P,$$

ce qu'il fallait démontrer. □

Tous les rudiments algébriques nécessaires pour notre discussion ont bien été établis. Nous pouvons donc maintenant exposer le résultat algébrique conduisant à une réponse aux quatre problèmes antiques.

Chapitre 5

Résultat de Wantzel et Conséquences

Le résultat principal de notre discussion est nommé Résultat de Wantzel. Pierre Laurent Wantzel se base sur les travaux de Descartes et utilise le langage algébrique d'Abel (1802 – 1829) pour donner une caractérisation algébrique des coordonnées des points constructibles à la règle et au compas [Carrega, 3, 11].

5.1 Résultat de Wantzel

Nous avons besoin d'abord du résultat suivant découlant directement du lemme 2 énnoncé au chapitre 3.

Lemme 3. *[Carrega, 25]*

1. *Une droite passant par les points $A(a_1, a_2) \neq B(b_1, b_2)$ a une équation de la forme $ax + by + c = 0$ avec $a, b, c \in \mathbb{Q}(a_1, a_2, b_1, b_2)$*
2. *Le cercle de centre de rayon $[A(a_1, a_2)B(b_1, b_2)]$ et de centre $C(c_1, c_2)$ a une équation de la forme $x^2 + y^2 - 2ax - 2by + c = 0$, avec $a, b, c \in \mathbb{Q}(a_1, a_2, b_1, b_2, c_1, c_2)$*

Voici donc le fameux résultat. Il est en fait une reformulation du théorème 1 sur $\mathscr{C}$ à l'aide des notions d'extensions de corps.

THEOREME 2 (Résulat de Wantzel)**.** *[Carrega, 28] Tout nombre constructible ($a \in \mathscr{C}$) est algébrique sur $\mathbb{Q}$ et son degré est une puissance de 2.*

Démonstration. Afin de démontrer ce théorème nous donnons le lemme important suivant :

Lemme 4. *[Carrega, 25] Le nombre $t \in \mathbb{R}$ est constructible si et seulement s'il existe une suite de sous-corps de $\mathbb{R}$*

$$\mathbb{Q} = L_1 \subset L_2 \subset \ldots \subset L_p \ni t \text{ pour } p \in \mathbb{N}^+$$

telle que pour $1 \leq j \leq p - 1$:

$$[L_{j+1} : L_j] = 2$$

Démonstration. Démontrons d'abord l'une des implications, puis sa réciproque.

– Nous supposons t constructible.
Par définition, t est l'abscisse d'un point constructible T de l'axe des x. T est donc, par la définition 1, le dernier point d'une suite de point : $0 = T_1, 1 = T_2, \ldots, T_n = T$. Posons (x_i, y_i) les coordonnées de T_i dans $\mathscr{R}(O, I, J)$, pour $i = 1, \ldots, n$. Posons maintenant :

$$\begin{aligned} K_1 = &\ \mathbb{Q}(x_1, y_1) = \mathbb{Q}(0,0) = \mathbb{Q} \\ K_2 = &\ \mathbb{Q}(x_1, y_1, x_2, y_2) = \mathbb{Q}(0,0,1,0) = \mathbb{Q} \\ &\ \vdots \\ K_i = &\ \mathbb{Q}(x_1, y_1, \ldots, x_i, y_i) \\ &\ \vdots \\ K_n = &\ \mathbb{Q}(x_1, y_1, \ldots, t = x_n, y_n) \end{aligned}$$

On a donc bien $K_1 \subset K_2 \subset \ldots \subset K_{i-1} \subset K_i \subset K_{i+1} \subset \ldots \subset K_n$, et nous avons la suite de corps que nous cherchons. Il faut donc maintenant montrer que pour tout $i = 1, 2, \ldots, n-1$, $K_i = K_{i+1}$ ou $[K_{i+1} : K_i] = 2$.
Il est clair que pour $i = 1, K_1 = K_2 = \mathbb{Q}$. Nous pouvons donc supposer $i \geq 2$.
Trois cas se présente à nous pour le point T_{i+1} :
– T_{i+1} est l'intersection de deux droites,
– T_{i+1} est l'intersection d'une droite et d'un cercle,
– T_{i+1} est l'intersection de deux cercles,
où ces droites et ces cercles sont définis par les points $T_1, \ldots, T_i$, avec des équations à coefficients dans K_i selon le lemme 3.
– Si $T_{i+1}(x_{i+1}, y_{i+1})$ est l'intersection de deux droites, il est solution du système :

$$\begin{cases} ax + by + c = 0 \\ a'x + b'y + c' = 0 \end{cases} \text{, avec } a, b, c, a', b', c' \in K_i.$$

On résout ce système (comme on l'a fait dans la démonstration du lemme 2) et on voit que la solution T_{i+1} a ses coordonnées dans K_i.
Donc, $K_{i+1} = K_i(x_{i+1}, y_{i+1}) = K_i$.
– Si $T_{i+1}(x_{i+1}, y_{i+1})$ est l'intersection d'une droite et d'un cercle, il est solution du système :

$$\begin{cases} ax + by + c = 0 \\ x^2 + y^2 - 2a'x - 2b'y + c' = 0 \end{cases} \text{, avec } a, b, c, a', b', c' \in K_i.$$

On résout ce système (comme on l'a fait dans la démonstration du lemme 2) et on a que deux cas :
– $y_{i+1} \in K_i$ et $x_{i+1} = \dfrac{-c - by_{i+1}}{a} \in K_i$, d'où $K_{i+1} = K_i$
– $y_{i+1} \notin K_i$ et y_{i+1} est algébrique sur K_i et de degré 1 ou 2, puisque l'équation est du second degré. On a donc :

$$K_{i+1} = K_i(x_{i+1}, y_{i+1}) = K_i(x_{i+1}) \text{ et } [K_{i+1} : K_i] \leq 2.$$

– Si $T_{i+1}(x_{i+1}, y_{i+1})$ est l'intersection de deux cercles, il est solution du système (après manipulation comme montré dans la démonstration du lemme 2) :

$$\begin{cases} x^2 + y^2 - 2ax - 2by + c = 0 \\ 2(a - a')x + 2(b - b')y - (a - a')^2 - (b - b')^2 + (c - c')^2 - 1 = 0, \end{cases}$$

et on est ramené au cas précédent.

Une suite de sous-corps de $\mathbb{R}$ est donc bien construite : $\mathbb{Q} = K_1 \subset \ldots \subset K_n \ni t$ telle que $K_{i+1} = K_i$ ou $[K_{i+1} : K_i] = 2$ pour $1 \leq i \leq n-1$. En supprimant les corps égaux l'un à l'autre, on rend cette suite strictement croissante. On obtient donc :

$$\mathbb{Q} = L_1, \ldots, L_p \ni t \text{ et } [L_{j+1} : L_j] = 2, \text{ pour } 1 \leq j \leq p-1.$$

- Réciproquement, on suppose $L_1 \subset \ldots \subset L_p$ une suite de sous-corps de $\mathbb{R}$ vérifiant les conditions requises. Pour montrer que $t \in \mathbb{R}$ est constructible, nous procédons par récurrence sur $j \in 1, \ldots, p$ et montrons que $L_j \subset \mathscr{C}$.
  - $L_1 = \mathbb{Q} \subset \mathscr{C}$
  - Supposons que $\mathscr{C}$ est bien une extension de corps de L_j et montrons que $L_{j+1} \subset \mathscr{C}$. Soit $k \in L_{j+1}$. Comme $[L_{j+1} : L_j] = 2$, il existe $a, b, c \in L_j$ non tous nuls tels que $ak^2 + bk + c = 0$
    - $a = 0 \Rightarrow k = \dfrac{-c}{b} \in L_j \subset \mathscr{C}$
    - $a \neq 0 \Rightarrow k = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a} \in \mathscr{C}$, car $\mathscr{C}$ est stable par racine carrée.

  Le réel $t \in L_j, 1 \leq j \leq p$ est donc bien un nombre constructible.

Le présent lemme est donc bien démontré. □

Pour démontrer le Résultat de Wantzel, nous supposons $t \in \mathbb{R}$ constructible. D'après le lemme que nous venons de démontrer, il existe une suite de sous-corps $\mathbb{R} : \mathbb{Q} = L_1, \ldots, L_p \ni t$ telle que $L_j \subset L_{j+1}$ et $[L_{j+1} : L_j] = 2$ pour $1 \leq j \leq p-1$.
D'après la proposition 4,

$$[L_p : \mathbb{Q}] = [L_p : L_{p-1}] \times [L_{p-1} : L_{p-2}] \times \ldots [L_2 : \mathbb{Q}] = 2^{p-1}.$$

Or, nous avons aussi que

$$\mathbb{Q} \subset \mathbb{Q}(t) \subset L_p \Rightarrow 2^{p-1} = [L_p : \mathbb{Q}] = [L_p : \mathbb{Q}(t)] \times [\mathbb{Q}(t) : \mathbb{Q}],$$

ce qui implique que $[\mathbb{Q}(t) : \mathbb{Q}] | 2^{p-1}$, c'est-à-dire $[\mathbb{Q}(t) : \mathbb{Q}]$ est une puissance de 2 que nous nommons 2^d.
Il est donc maintenant clair que t est algébrique sur $\mathbb{Q}$ de degré $[\mathbb{Q}(t) : \mathbb{Q}] = 2^d$, ce qu'il fallait démontrer. ■

Remarque 4. La réciproque de ce résultat n'est pas vraie : Le nombre réel a algébrique sur $\mathbb{Q}$ de degré 2^n n'est *pas nécessairement* constructible.
On peut par exemple prendre $P(X) = X^4 - X - 1$, polynôme irréductible sur $\mathbb{Q}[X]$. On peut montrer que $P(X)$ possède une racine réelle non constructible, alors qu'elle est de degré 4 [Carrega, 39-41].

Le Résultat de Wantzel va nous permettre de donner une solution satisfaisante aux quatre problèmes originaux.

5.2 Solutions aux Quatre Problèmes Grecs

5.2.1 Duplication du Cube

Le polynôme $P(X) = X^3 - 2$ admet-il une racine dans $\mathscr{C}$?
Si ce polynôme se décomposait dans $\mathbb{Q}[X]$, il serait de la forme

$$P(X) = X^3 - 2 = (X + a)(X^2 + bX + c),$$

avec $a, b, c \in \mathbb{Q}$, et il aurait une racine (en l'occurence a) dans $\mathbb{Q}$. Or, il est évident que $\sqrt[3]{2}$ est la seule racine réelle de $P(X)$. Est-elle dans $\mathbb{Q}$? Supposons que $\sqrt[3]{2}$ est

effectivement un rationnel. Donc, $\sqrt[3]{2} = \frac{p}{q}$, avec $p \in \mathbb{N}^+, q \in \mathbb{Z}^*$, tels que $p \wedge q = 1$; on obtient $2q^3 = p^3$, et alors $p|2q^3$.

Par le théorème de Gauss énoncé lors de la discussion sur l'anneau $\mathbb{Z}$ (cf. Section 4.1.1), nous voyons que

$$p|2q^3 \Rightarrow p|2, \text{ ainsi } p \in \{1, 2\}.$$

1. $p = 1 \Rightarrow 2q^3 = 1 \Rightarrow q^3 = \frac{1}{2}$ **impossible !** car $q \in \mathbb{Z}*$.
2. $p = 2 \Rightarrow 2q^3 = 2 \Rightarrow q^3 = 1$ et donc $\sqrt[3]{2} = \frac{p}{q} = 2$ **impossible !**

Il est donc clair que $P(X) = X^3 - 2$ est irréductible sur $\mathbb{Q}[X]$, et par définition $P(X)$ est le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbb{Q}$ (cf. Proposition 5). Ceci veut donc dire que $\sqrt[3]{2}$ est algébrique sur $\mathbb{Q}$ de degré 3.

Par le Résultat de Wantzel, $\sqrt[3]{2} \notin \mathscr{C}$.

Il est donc impossible de construire à la règle et au compas un point sur l'axe des x d'abscisse $\sqrt[3]{2}$, et donc de construire l'arête d'un cube de volume double du volume d'un autre cube donné.

5.2.2 Trissection de l'Angle

Le polynôme $P(X) = 4x^3 - 3x - \cos 3\theta$ admet-il une racine dans $\mathscr{C}$?

Comme dans la situation précédente, si ce polynôme se décomposait dans $\mathbb{Q}[X]$ il aurait un facteur du premier degré. Donc, $P(a) = 0$, avec $a \in \mathbb{Q}$, qui s'écrit sous la forme :

$$a = \frac{p}{q}, \text{ avec } p \in \mathbb{N}^+, q \in \mathbb{Z}^*, \text{ tels que } p \wedge q = 1.$$

Regardons un cas particulier et voyons si l'angle $\frac{2\pi}{3}$ est trissectable. Par définition, on sait que $\frac{2\pi}{3}$ est un angle constructible (cf. Définition 4). Il nous faut donc montrer si $\cos\frac{2\pi}{9}$ est un nombre constructible ou non. S'il l'est,

$$\begin{aligned}
& 4\left(\frac{p^3}{q^3}\right) - 3\left(\frac{p}{q}\right) - \cos\frac{2\pi}{3} = 0 \\
\Leftrightarrow \quad & 4\left(\frac{p^3}{q^3}\right) - 3\left(\frac{p}{q}\right) + \frac{1}{2} = 0 \\
\Leftrightarrow \quad & 6pq^2 - 8p^3 = q^3 \\
\Leftrightarrow \quad & p(\underbrace{6q^2 - 8p^2}_{\in\mathbb{Z}}) = q^3 \text{ et } -8p^3 = q^2(\underbrace{q - 6p}_{\in\mathbb{Z}}),
\end{aligned}$$

d'ou $p|q^3$ et $q^2|8p^3$. Comme $p \wedge q = 1$, cela implique que $p = 1$ et $q \in \{\pm 1, \pm 2\}$. Nous voyons donc clairement qu'en substituant les valeurs trouvées pour p et q, on a que les rationnels $\frac{p}{q}$ ne peuvent pas être racines de $P(X)$:

1. $6(1)(1) - 8(1) = \pm 1$ **impossible !**
2. $6(1)(4) - 8(1) = \pm 2$ **impossible !**

$P(X)$ est donc irréductible sur $\mathbb{Q}[X]$, $\frac{P(X)}{4} = X^3 - \frac{3}{4}X + \frac{1}{8}$ est le polynôme minimal de $\cos\frac{2\pi}{9}$ sur $\mathbb{Q}$, et $\cos\frac{2\pi}{9}$ est algébrique de degré 3 sur $\mathbb{Q}$.

Selon le Résultat de Wantzel, $\cos\frac{2\pi}{9} \notin \mathscr{C}$.

Il est donc impossible de construire à la règle et au compas un point sur l'axe des x d'abscisse $\cos\frac{2\pi}{9}$, et donc de diviser l'angle $\frac{2\pi}{3}$ (et donc en général un angle donné quelconque) en trois parties égales.

Remarque 5. 1. Si un angle est constructible, alors il est évident que ces multiples le sont aussi. Donc, une fois un angle jugé non-constructible, il est évident que ces diviseurs sont aussi non-constructibles.

Exemple 7. [Carrega, 34] Comme $\frac{2\pi}{9} = 40^o$ n'est pas constructible, $\frac{\pi}{9} = 20^o$, $\frac{\pi}{18} = 10^o$, $\frac{\pi}{36} = 5^o$, $\frac{\pi}{45} = 4^o$, $\frac{\pi}{90} = 2^o$, $\frac{\pi}{180} = 1^o$, sont tous non-constructibles.

Exemple 8. Toujours dans notre situation, on voit que $\frac{2\pi}{3} = 120^o$, $\frac{\pi}{3} = 60^o$, $\frac{\pi}{6} = 30^o$, $\frac{\pi}{12} = 15^o$, $\frac{\pi}{15} = 12^o$, $\frac{\pi}{30} = 6^o$, $\frac{\pi}{60} = 3^o$, sont tous non-trissectables, étant les multiples de 3 respectifs d'angles non-constructibles.

2. [Carrega, 34] Si un angle est trissectable, son demi l'est aussi. Ceci est clair, car
$$\frac{1}{2}\left(\frac{\theta}{3}\right) = \frac{1}{3}\left(\frac{\theta}{2}\right).$$
Autrement dit, la bissectrice du tiers d'un angle donne la trissection du demi de l'angle.

Exemple 9. Nous savons que $2\pi = 360^o$ est trissectable car $\frac{2\pi}{3} = 120^o$ est constructible. Donc, $\pi = 180^o$ est aussi trissectable : $\frac{1}{2}\left(\frac{2\pi}{3}\right) = \frac{\pi}{3} = 60^o$. En général, on voit que tous les angles de la forme $\frac{2\pi}{2^n} = \frac{\pi}{2^{n-1}}$ sont trissectables [Carrega, 35].

Une discussion plus approfondie de la notion d'angle constructible suivra lors de la discussion des polygones réguliers.

5.2.3 Quadrature du Cercle

Le polynôme $P(X) = X^2 - \pi$ admet-il une racine dans $\mathscr{C}$?

Tout comme avec la duplication du cube, ce qu'il nous faut montrer ici est si $\sqrt{\pi}$ est constructible ou non.

Il fut démontré par Lindemann en 1882, quelques années après la publication du Résultat de Wantzel, que le nombre π est en fait un nombre transcendant sur $\mathbb{Q}$. On peut se référer au chapitre X, section 5, de la *Théorie des Corps* de Jean-Paul Carrega pour une démonstration formelle du résultat de Lindemann [Carrega, 242-48].

Donc, le Résultat de Wantzel nous dit que $\pi \notin \mathscr{C}$.

Il n'est donc pas possible de construire à la règle et au compas un point sur l'axe des x d'abscisse $\sqrt{\pi}$, et donc de construire le côté d'un carré d'aire égale à celle d'un cercle donné.

Remarque 6. Il en est de même pour construire un carré de périmètre égal à la circonférence d'un cercle donné, car cela revient à construire π, ce qui est impossible par la transcendance de π.

5.2.4 Construction des Polygones Réguliers

Soit le n-ième polynôme cyclotomique

$$\Phi_n(X) = \prod_{k \wedge n = 1} X - e^{\frac{2ik\pi}{n}}.$$

Le polynôme $\Phi_n(X)$ admet-il une racine dans $\mathscr{C}$?

Pour pouvoir utilisé Wantzel ici, il nous faut en premier lieu formellement définir et étudier les polynômes cyclotomiques. Selon leurs propriétés – sur quel corps sont-ils définis ? Sont-ils irréductibles, et si oui, où ? Quel est leur degré ? – on pourra ensuite voir si leurs racines sont constructibles ou non. Tout cela est le sujet du chapitre suivant.

Chapitre 6

Les Polygones Réguliers

Comme nous l'avons vu brièvement plus haut, une polgone régulier à n côtés est constructible si $\widehat{\frac{2\pi}{n}}$ est un angle constructible, ou encore si $\cos\frac{2\pi}{n} \in \mathscr{C}$. Pour pouvoir donner un solution satisfaisante à ce problème, le résultat clé est le Théorème de Gauss, qui repose sur l'étude des polynômes cyclotomiques et le Résultat de Wantzel. Voyons donc tout cela de plus près.

6.1 Racines Primitives de l'Unité

Nous avons brièvement mentionné les racines n-ième de l'unité lors de la section 3.3.4, mais voici une définition plus complète.

Définition 7. [Carrega, 204] Le polynôme $X^n - 1$, pour $n \geq 1$ admet n racines dans $\mathbb{C}$ qui sont de la forme

$$\omega_k = e^{\frac{2ik\pi}{n}} = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}.$$

Ces racines sont appelées **racines n-ième de l'unité**.

De plus, on note U_n l'**ensemble des racines n-ième de l'unité**. C'est un sous-groupe de $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.

Remarque 7. [Carrega, 204] On voit que $\omega_k = \omega_1^k$, pour $1 \leq k \leq n$, et donc U_n est un groupe cyclique engendré par ω_1.

PROPOSITION 7. *[Carrega, 204] Si k est tel que $1 \leq k \leq n$, les propositions suivantes sont équivalentes :*

1. *ω_k est d'ordre n.*
2. *ω_k est un générateur de U_n.*
3. *ω_1 est une puissance de ω_k.*
4. *$k \wedge n = 1$.*

Démonstration. $1 \Rightarrow 2$ **:** ω_k étant d'ordre n, le sous-groupe qu'il engendre est aussi d'ordre n.

$2 \Rightarrow 3$ **:** Par définition.

$3 \Rightarrow 4$ **:** On a $\omega_1 = \omega_k^p \Rightarrow \frac{2\pi}{n} = \frac{2kp\pi}{n} + \lambda 2\pi$, avec $\lambda \in \mathbb{Z}$. Ainsi, $1 = kp + \lambda n$, ce qui est une relation de Bezout, et donc $k \wedge n = 1$ (cf. Section 4.1.1).

$4 \Rightarrow 1$ **:** Comme $k \wedge n = 1$, on a une relation de Bezout $1 = kp + \lambda n \Rightarrow \dfrac{2kp\pi}{n} + \lambda 2\pi = \dfrac{2\pi}{n}$. Ainsi, $\omega_k^p = \omega_1$. Comme ω_1 est un générateur de U_n par la remarque 7, ω_k est donc aussi un générateur de U_n et est d'ordre n.

□

Cette proposition nous permet d'écrire la définition suivante.

Définition 8. [Carrega, 205] Une **racine** *primitive* n**-ième de l'unité** est une racine n-ième de l'unité vérifiant une des conditions de la proposition 7.

Exemple 10. Pour tout $n \geq 1$: $\omega_1 = \cos\dfrac{2\pi}{n} + i\sin\dfrac{2\pi}{n}$ est racine primitive n-ième de l'unité. Donnons les racines primitives n-ième de l'unité pour $n \leq 6$:

$n = 1$ **:** $\omega_1 = \cos 2\pi + i\sin 2\pi = 1$.

$n = 2$ **:** $\omega_1 = \cos\pi + i\sin\pi = -1$.

$n = 3$ **:** $\omega_1 = \cos\dfrac{2\pi}{3} + i\sin\dfrac{2\pi}{3} = -\dfrac{1}{2} + i\dfrac{\sqrt{3}}{2} =: j$.
$\omega_2 = j^2 = -\dfrac{1}{2} - i\dfrac{\sqrt{3}}{2}$.

$n = 4$ **:** $\omega_1 = \cos\dfrac{\pi}{2} + i\sin\dfrac{\pi}{2} = i$.
$\omega_3 = i^3 = -i$.

$n = 5$ **:** $\omega_1 = \cos\dfrac{2\pi}{5} + i\sin\dfrac{2\pi}{5} = e^{\frac{2\pi}{5}}$.
$\omega_2 = e^{\frac{4\pi}{5}}$.
$\omega_3 = e^{\frac{6\pi}{5}}$.
$\omega_4 = e^{\frac{8\pi}{5}}$.

$n = 6$ **:** $\omega_1 = \cos\dfrac{\pi}{3} + i\sin\dfrac{\pi}{3} = \dfrac{1}{2} + i\dfrac{\sqrt{3}}{2} = -j^2$.
$\omega_5 = -j$.

A partir des racines primitives de l'unité nous définissons les polynômes cyclotomiques.

6.2 Polynômes Cyclotomiques

Nous avons brièvement mentionné les polynômes cyclotomiques lors de la discussion de la section 3.3.4, mais une définition plus formelle est nécessaire.

Définition 9. [Carrega, 205] Si $n \geq 1$, le n**-ième polynôme cyclotomique** est noté $\Phi_n(X)$ et est le polynôme de $\mathbb{C}[X]$ unitaire dont les racines sont les racines primitives n-ième de l'unité. Il est de degré $\phi(n)$ (nommé **indicateur d'Euler**), qui est évidemment le nombre de racines primitives n-ième de l'unité pour un certain n. On a donc :

$$\Phi_n(X) = (X - \alpha_1)(X - \alpha_2)\dots(X - \alpha_{\phi(n)}),$$

avec $\alpha_1, \dots, \alpha_{\phi(n)}$ les racines primitives n-ième de l'unité.

Exemple 11. Listons les polynômes cyclotomiques pour $n \leq 6$:

$n = 1$ **:** $\Phi_1(X) = X - 1$.

$n = 2$ **:** $\Phi_2(X) = X + 1$.

$n = 3$: $\Phi_3(X) = (X - j)(X + j) = X^2 + X + 1$.
$n = 4$: $\Phi_4(X) = (X - i)(X + i) = X^2 + 1$.
$n = 5$: $\Phi_5(X) = \dfrac{(X - e^{\frac{2\pi}{5}})(X - e^{\frac{4\pi}{5}})(X - e^{\frac{6\pi}{5}})(X - e^{\frac{8\pi}{5}})(X - 1)}{X - 1} = \dfrac{X^5 - 1}{X - 1} = X^4 + X^3 + X^2 + X + 1$.
$n = 6$: $\Phi_6(X) = (X + j)(X + j^2) = X^2 - X + 1$.

PROPOSITION 8. *[Escofier, 133] Si $n \geq 1$, on a*

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Démonstration.

$$\begin{aligned} X^n - 1 &= \prod_{1 \leq k \leq n} (X - e^{\frac{2ik\pi}{n}}), \text{ par la définition 7} \\ &= \prod_{d|n} \prod_{k \wedge n = \frac{n}{d}} (X - e^{\frac{2ik\pi}{n}}) \\ &= \prod_{d|n} \prod_{k' \wedge n = 1} (X - e^{\frac{2ik'\pi}{d}}), \text{ avec } k' = \frac{kd}{n} \\ &= \prod_{d|n} \Phi_d(X), \text{par la définition 9.} \end{aligned}$$

□

PROPOSITION 9. *[Carrega, 206] Pour $n \geq 1$,*

$$\Phi_n(X) \in \mathbb{Z}[X].$$

Démonstration. Opérons par récurrence sur n.

Il est clair que $\Phi_1 = X - 1 \in \mathbb{Z}[X]$

On suppose la proposition vraie pour $d < n$. Par la proposition précédente, on a

$$\begin{aligned} X^n - 1 &= \prod_{d|n} \Phi_d(X) \\ &= \Phi_n(X) \prod_{\substack{d|n \\ d \neq n}} \Phi_d(X). \end{aligned}$$

Le polynôme $\prod_{\substack{d|n \\ d \neq n}} \Phi_d(X) \in \mathbb{Z}[X]$, par récurrence sur n, et il est unitaire par la définition 9. Supposons que $\Phi_n(X) = X^h + a_{h-1}X^{h-1} + \ldots + a_1X + a_0$ n'est pas dans $\mathbb{Z}[X]$. Alors

$$X^n - 1 = (X^h + \ldots + a_{k+1}X^{k+1} + a_kX^k + \ldots + a_0) \prod_{\substack{d|n \\ d \neq n}} \Phi_d(X),$$

avec k le plus grand indice tel que $a_k \notin \mathbb{Z}$. Ceci nous donne

$$\underbrace{(X^n-1)-(X^h+\ldots+a_{k+1}X^{k+1})\prod_{\substack{d|n\\ d\neq n}}\Phi_d(X)}_{\in\mathbb{Z}[X]}=(a_kX^k+\ldots+a_0)\prod_{\substack{d|n\\ d\neq n}}\Phi_d(X).$$

Le polynôme de droite doit être aussi dans $\mathbb{Z}[X]$, ce qui voudrait dire que $a_k \in \mathbb{Z}$ ce qui est absurde.

Donc, $\Phi_n(X)$ est bien un polynôme de $\mathbb{Z}[X]$. □

THEOREME 3. *[Escofier, 138] Pour $n \geq 1$,*

$$\Phi_n(X) \text{ est irréductible sur } \mathbb{Q}.$$

Démonstration. Soit ω une racine primitive n-ième de l'unité de polynôme minimal P sur $\mathbb{Q}$. Notons

$$E = \{\omega_i \in \mathbb{C} | P(\omega) = 0\},$$
$$F = \{\omega_i \in \mathbb{C} | \omega_0 \text{ racine primitive } n\text{-ième de l'unité}\}.$$

Nous allons montrer que $E = F$.

Evidemment, $\Phi_n(\omega) = 0$, donc $P|\Phi_n \Rightarrow E \subset F$. Procédons par l'absurde.

On suppose qu'il existe $\omega \in E$ et p premier ne divisant pas n tels que $\omega^p \notin E$, et on note $X^n - 1 = P(X)S(X)$.

Ceci implique que $P(X^p)S(X^p) = X^{np} - 1 \Leftrightarrow P(\omega^p)S(\omega^p) = \omega^{np} - 1 = 0$, et donc $P(\omega^p) = 0$ ou $S(\omega^p) = 0$. Mais comme $\omega^p \notin E$, $P(\omega^p) \neq 0$.

Il est évident que $P|S(X^p)$, puisqu'il est le polynôme minimal de ω ; donc $S(X^p) = P(X)T(X)$, avec $T \in \mathbb{Z}[X]$ et P unitaire.

On se place maintenant dans $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$, et on note les images des polynômes de $\mathbb{Z}$ dans $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ par un indice z. On a par propriété de l'anneau $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$

$$S_z(X^p) = S_z(X)^p = P_z(X)T_z(X).$$

Tout facteur irréductible unitaire U_z de P_z divise S_z, $\dfrac{\mathbb{Z}}{p\mathbb{Z}}[X]$ étant factoriel. Ce qui entraîne que

$$U_z(X)|P_z(X) \Rightarrow U_z(X)^2|P_z(X)^2T_z = P_z(X)S_z(X) = X^n - 1, \text{ d'où}$$

$$U_z(X)|nX^{n-1},$$

et comme $p \wedge n = 1$, $U_z(X) = X$, ce qui est absurde car P est de coefficient constant de module 1.

Donc, il n'existe pas de $\omega \in E$ et p premier ne divisant pas n tels que $\omega^p \notin E$, et E est bien stable par puissance p-ième.

Soit maintenant $\xi \in F$. Il existe $u \wedge n = 1$ tel que $\xi = \omega^u$. On décompose u en facteurs premier et on note : $u = \prod_{1\leq i\leq r} p_i^{k_i} \Rightarrow \omega^u = \omega^{p_1^{k_1}\cdots p_r^{k_r}}$.

Par la stabilité de E pas puissance p-ième, $\omega^u \in E$.

Donc $E = F$, d'où $\Phi_n = P$, avec P minimal. Φ_n est irréductible sur $\mathbb{Q}$. □

Pour référence dans la démonstration du Théorème de Gauss, nous donnons ici une proposition intéressante sur le degré des polynômes cyclotomiques.

PROPOSITION 10. *Soit $p \geq 3$ premier. Pour p^α une puissance de p,*

$$\phi(p^\alpha) = p^{\alpha-1}(p-1),$$

où $\phi(n)$ est l'indicateur d'Euler, i.e. le degré de $\Phi_n(X)$.

Démonstration. Pour trouver le degré de $\Phi_{p^\alpha}(X)$, il faut en fait trouver le nombres de $k \in \mathbb{N}$ tels que $k \wedge p^\alpha = 1$ et $1 \leq k \leq p^\alpha$. Comme p est premier, parmi les entiers k compris entre 1 et p^α, les multiples de p (c'est-à-dire $p, 2p, 3p, \ldots, p^\alpha$) sont les seuls à ne pas être premiers avec p^α. Il y en a bien $p^{\alpha-1}$ et donc le degré de $\Phi_n(X)$ est $\phi(n) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$. Donc

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = p^{\alpha-1}(p-1). \tag{6.1}$$

□

6.3 Théorème de Gauss

Avant de pouvoir énoncer le résultat attendu nous avons besoin de deux courtes propositions.

PROPOSITION 11. *[Carrega, 48] L'angle $\dfrac{\widehat{2\pi}}{mn}$, avec $m \wedge n = 1$, est constructible si et seulement si $\dfrac{\widehat{2\pi}}{m}$ et $\dfrac{\widehat{2\pi}}{n}$ sont constructibles.*

Démonstration.

– Nous voyons clairement que

$$\frac{\widehat{2\pi}}{m} = n\frac{\widehat{2\pi}}{mn} \quad \text{et} \quad \frac{\widehat{2\pi}}{n} = m\frac{\widehat{2\pi}}{mn}.$$

Comme le multiple d'un angle constructible (dans ce cas $\dfrac{\widehat{2\pi}}{mn}$) est facilement construit, il est évident que les deux angles ci-dessus sont bien contructibles.

– Supposons maintenant que $\dfrac{\widehat{2\pi}}{m}$ et $\dfrac{\widehat{2\pi}}{n}$ sont constructibles.
D'après la relation de Bezout, comme $m \wedge n = 1$, il existe λ et $\mu \in \mathbb{Z}$ tels que $\lambda n + \mu m = 1$. On a donc

$$\frac{\widehat{2\pi}}{nm} = \lambda\frac{\widehat{2\pi}}{m} + \mu\frac{\widehat{2\pi}}{n}.$$

Il est clair que la somme de deux angles constructibles est elle-même constructible puisqu'il suffit de construire les deux angles sommés adjacents l'un à l'autre. L'angle ci-dessus est donc bien constructible.

□

PROPOSITION 12. *[Carrega, 49] Si $n \geq 3$ a pour décomposition en facteurs premiers $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, le polygone régulier à n côtés est constructible si et seulement si $\dfrac{\widehat{2\pi}}{p_1^{\alpha_1}}, \ldots, \dfrac{\widehat{2\pi}}{p_k^{\alpha_k}}$ sont constructibles.*

Démonstration. Soit $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, et procédons par récurrence sur k.

La proposition précédente, assure l'initialisation ($k = 2$) et d'après la proposition 11 $\dfrac{\widehat{2\pi}}{n}$ est constructible si et seulement si

$$\frac{\widehat{2\pi}}{p_1^{\alpha_1} \ldots p_{k-1}^{\alpha_{k-1}}} \text{ et } \frac{\widehat{2\pi}}{p_k^{\alpha_k}}$$

sont constructibles, et par hypothèse de récurrence, la proposition est démontrée. □

Voici donc le résultat qui nous permettra de trouver les polygones réguliers constructibles. Enoncé par Karl Friedrich Gauss en 1801, donc bien avant Wantzel, il semble que ce résultat est en fait la conclusion générale que Gauss tira de sa construction du polygone régulier à 17 côtés qu'il fit en 1796 [Carrega, 3,11]. Néanmoins, n'ayant pas le Résultat de Wantzel à sa disposition, il ne démontre que l'une des implications du théorème, celle qui est donc suffisante pour pouvoir construire tout polygone régulier, dont celui à 17 côtés. Nous ne donnerons malheureusement pas cette construction ici en raison de sa complexité et de sa longueur, mais Jean-Claude Carrega la retranscrit dans son livre *Théorie de Corps : La Règle et le Compas* aux pages 55 - 63.

THEOREME 4 (Théorème de Gauss)**.** *[Carrega, 51] Les polygones réguliers constructibles sont ceux dont le nombre de côtés n est de la forme 2^α avec $\alpha \geq 2$ ou de la forme $2^\alpha p_1 \dots p_r$, avec $\alpha \in \mathbb{N}$ et où les p_i sont des nombres de Fermat premiers et distincts.*

Démonstration. Via la proposition 12, ce théorème est en fait équivalent au lemme suivant.

Lemme 5. *[Carrega, 49]*

1. *Les angles de la forme $\dfrac{\widehat{2\pi}}{2^\alpha}$ sont constructibles.*
2. *Si $p \geq 3$ est premier, $\dfrac{\widehat{2\pi}}{p^\alpha}$ est constructible si et seulement si $\alpha = 1$ et p est un nombre de Fermat, c'est-à-dire un nombre de la forme $1 + 2^{2^\beta}$.*

Démonstration.

1. Les angles $\dfrac{\widehat{2\pi}}{2^\alpha}$ sont évidemment constructibles, puisqu'il suffit de construire des bissectrices. On peut évidemment démontrer ceci par récurrence sur α.

2. Supposons $p \geq 3$ premier et $\dfrac{\widehat{2\pi}}{p^\alpha}$ constructible avec $\alpha \in \mathbb{N}^*$.

   Donc, $\cos \dfrac{2\pi}{p^\alpha}$ est un nombre constructible, et **par le Résultat de Wantzel** on a
   $$\left[\mathbb{Q}\left(\cos \frac{2\pi}{p^\alpha}\right) : \mathbb{Q}\right] = 2^m, \tag{6.2}$$
   pour un certain $m \in \mathbb{Z}$.
   Considérons la racine primitive p^α-ième de l'unité $\omega = \cos \dfrac{2\pi}{p^\alpha} + i \sin \dfrac{2\pi}{p^\alpha}$, qui est donc racine du polynôme cyclotomique Φ_{p^α} de degré $\phi(p^\alpha)$ (cf. Théorème 3). Ce dernier étant irréductible, le degré algébrique de ω est donné par $\phi(p^\alpha) = p^{\alpha-1}(p-1)$ (cf. Proposition 10).
   Nous savons aussi que
   $$\begin{aligned}
   \omega + \omega^{-1} &= e^{\frac{2i\pi}{p^\alpha}} + e^{-\frac{2i\pi}{p^\alpha}} \\
   &= e^{i\frac{2\pi}{p^\alpha}} + e^{i\frac{-2\pi}{p^\alpha}} \\
   &= \left(\cos \frac{2\pi}{p^\alpha} + i \sin \frac{2\pi}{p^\alpha}\right) + \left(\cos \frac{2\pi}{p^\alpha} - i \sin \frac{2\pi}{p^\alpha}\right) \\
   &= 2 \cos \frac{2\pi}{p^\alpha}.
   \end{aligned}$$

Donc, il est clair que $\cos\dfrac{2\pi}{p^\alpha} \in \mathbb{Q}(\omega)$. De plus

$$\begin{aligned} 0 &= \omega^2 - \omega^2 - 1 + 1 \\ &= \omega^2 - \omega(\omega + \omega^{-1}) + 1 \\ &= \omega^2 - 2\omega\cos\frac{2\pi}{p^\alpha} + 1, \end{aligned}$$

et donc ω est algébrique de degré 1 ou 2 sur $\mathbb{Q}\left(\cos\dfrac{2\pi}{p^\alpha}\right)$:

$$\left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\frac{2\pi}{p^\alpha}\right)\right] \leq 2. \tag{6.3}$$

Des équations (6.1), (6.2), et (6.3), on obtient

$$\begin{aligned} [\mathbb{Q}(\omega) : \mathbb{Q}] &= \left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\frac{2\pi}{p^\alpha}\right)\right] \times \left[\mathbb{Q}\left(\cos\frac{2\pi}{p^\alpha}\right) : \mathbb{Q}\right] \\ \Leftrightarrow p^{\alpha-1}(p-1) &= 2^n, \text{ avec } n = m \text{ ou } n+1 \end{aligned}$$

et comme $p \geq 3$ est premier, $p \wedge 2 = 1, \alpha = 1$ et $p = 1 + 2^{m+1}$.
Il nous reste à prouver que p est bien un nombre de Fermat, c'est-à-dire que $m+1$ est une puissance de 2.
En décomposant $m+1$ en facteurs premiers, on peut l'écrire sous la forme $\lambda 2^\beta$, avec $\beta \in \mathbb{N}$ et $\lambda \in \mathbb{N}^*$ premier impair. Donc

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

Mais comme λ est impair, on sait que le polynôme $X^\lambda + 1$ est divisible par $X + 1$, ce qui entraîne que $(1 + 2^{2^\beta})|p$.
Mais p est premier. Donc on a bien que

$$p = 1 + 2^{2^\beta},$$

et est ainsi un nombre de Fermat, ce qu'il fallait démontrer.

□

Le Théorème de Gauss est donc bien démontré. ■

Remarque 8. L'autre implication – si p est un nombre premier de Fermat, alors $\widehat{\dfrac{2\pi}{p}}$ (et donc le polygone régulier à p côtés) est constructible – n'est pas présentée ici, mais on peut trouver cette démonstration aux pages 214 à 219 de la *Théorie des Corps* de Carrega.

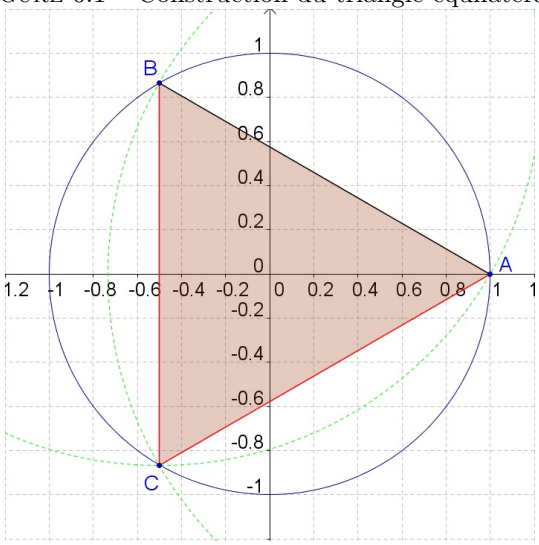
6.4 Exemples de Construction

Euclide donna les constructions du triangle équilatéral, du carré, du pentagone, et du pentadecagone. Ce sont donc précisément les polygones que nous allons étudier ici. Chaque polygone sera introduit d'abord par sa construction grecque classique, suivi pas une brève analyse algébrique de cette construction si cela est pertinent, et ensuite nous donnerons la construction faisant intervenir le Théorème de Gauss. On rappelle qu'on se place ici dans le cercle unité $\mathcal{C}$ centré en O de rayon 1. Tous les angles sont donc de sommet O et définis par le point $I(1,0)$ et un autre point sur $\mathcal{C}$.

6.4.1 Le Triangle Equilatéral

La construction classique du triangle équilatéral consiste à prendre un segment $[AB]$, et de construire les deux cercles $C_{A,[AB]}$ et $C_{B,[BA]}$. Les points d'intersections de ces deux cercles forment les points C et D. On construit les segments $[AC]$ et $[BC]$. Le triangle ABC est équilatéral [Euclide, 3]. Le fait que cette construction est correcte est évident, puisque le point C et le point d'intersection de deux cercles partageant le même rayon $[AB]$.

FIGURE 6.1 – Construction du triangle équilatéral



En utilisant le Théorème de Gauss, on doit aussi pouvoir construire un polygone régulier à 3 côtés, c'est-à-dire construire l'angle $\widehat{\frac{2\pi}{3}}$, ou encore le nombre constructible $\cos\frac{2\pi}{3} = -\frac{1}{2}$. On se place dans $\mathcal{C}$ et on place le point $A(1,0)$. Les points B et C ont pour abscisse $-\frac{1}{2}$. On les obtient par intersection de $\mathcal{C}$ et de la perpendiculaire à l'axe des x passant par $(-\frac{1}{2},0)$. On a alors le triangle équilatéral recherché.

6.4.2 Le Carré

Les deux constructions (classique et algébrique) sont quasi identiques. Du point de vue classique il faut construire deux diamètres perpendiculaires d'un cercle, joindre leurs points extrémaux [Euclide, 88], et on obtient le carré de côté $r\sqrt{2}$, pour r le rayon du cercle circonscrit. Du point de vue algébrique on place les quatre points

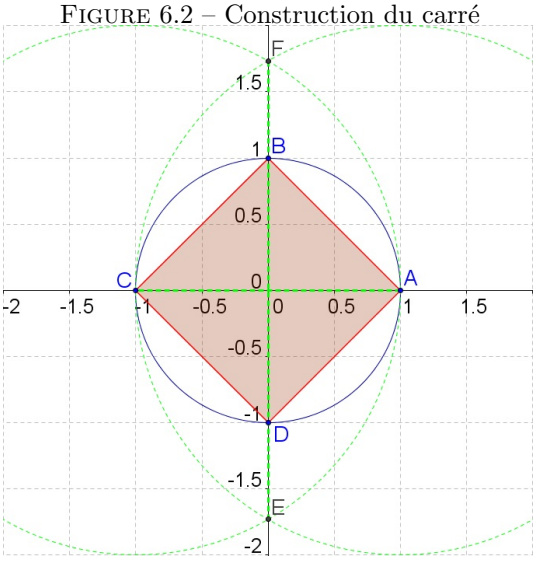
$$A(1,0),\ B(0,1),\ C(-1,0),\ D(0,-1)$$

et on les joint par des segments. Le carré de côté $\sqrt{2}$ est donc formé (voir Figure 6.2).

6.4.3 Le Pentagone

Pour le pentagone, Euclide commence par un triangle isocèle ABD tel que $\widehat{DAB} = \widehat{DBA} = 2\widehat{ADB}$ inscrit dans un cercle. Pour construire un tel triangle, on part d'un segment [BD] et on construit un point C sur ce segment, tel que

FIGURE 6.2 – Construction du carré

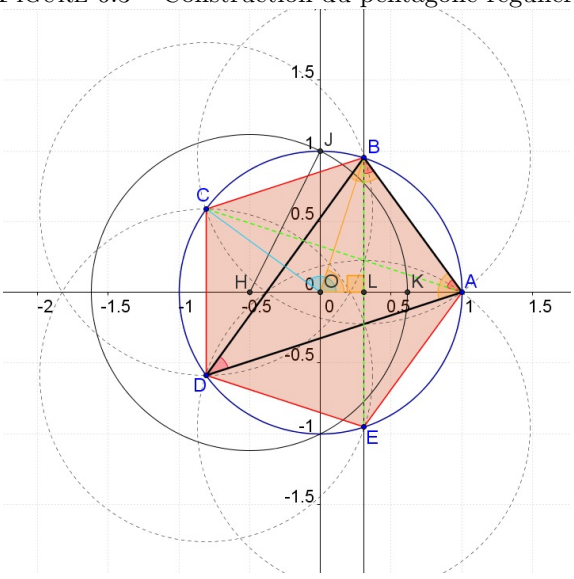


$[BD]\cdot[BF] = [DF]^2$. On trace ensuite $C_{D,[BD]}$, et $C_{B[DF]}$. Le point d'intersection de ces deux cercles est A, et on peut prouver que le triangle ABD est bien le triangle recherché [Euclide, 91], mais nous y reviendrons plus tard. Ce qui est intéressant est qu'en construisant ce triangle, on construit en fait l'angle $\frac{\widehat{\pi}}{5}$:

$$\widehat{DAB} + \widehat{DBA} + \widehat{ADB} = 5\widehat{ADB} = \pi,$$

par la propriété bien connue des triangles [Euclide, 24]. Ce triangle étant inscrit dans un cercle, on voit que le segment $[AB]$ est de la longueur requise, puisque l'angle central pour ce segment est $\frac{\widehat{2\pi}}{5}$ [Euclide, 66]. Euclide continue en construisant ensuite les bissectrices des angles $\widehat{DAB}$ et $\widehat{DBA}$ coupant le cercle en C et E respectivement. Le polygone $ABCDE$ est un pentagone régulier [Euclide, 92].

FIGURE 6.3 – Construction du pentagone régulier



La construction algébrique est un peu plus simple, car elle ne demande pas de partir de ce triangle isocèle spécial. Il nous faut exprimer $\cos\frac{2\pi}{5}$ sous une forme que l'on peut utiliser pour construire le pentagone. Nous savons que $\omega = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$ est une racine 5-ième de l'unité et donc un racine de $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$ (cf. Exemple 11), et donc $\omega^4 + \omega^3 + \omega^2 + \omega + 1$. Or, il est facile de voir que ω^4 est conjugué de ω et ω^3 de ω^2 (cf Exemple 10). Donc, $\omega + \omega^4 = 2\cos\frac{2\pi}{5}$ et $\omega^2 + \omega^3 = 2\cos\frac{4\pi}{5}$. Nous avons donc maintenant

$$2\cos\frac{2\pi}{5} + 2\cos\frac{4\pi}{5} + 1 = 0 \Leftrightarrow \cos\frac{2\pi}{5} + \cos\frac{4\pi}{5} = -\frac{1}{2}.$$

Regardons donc maintenant le produit $\left(\cos\frac{2\pi}{5}\right)\left(\cos\frac{4\pi}{5}\right)$, qui est par identité trigonométrique

$$\begin{aligned}
&\frac{1}{2}\left(\cos\frac{(4+2)\pi}{5} + \cos\frac{(4-2)\pi}{5}\right)\\
=&\frac{1}{2}\left(\cos\frac{6\pi}{5} + \cos\frac{2\pi}{5}\right)\\
=&\frac{1}{2}\left(\cos\frac{4\pi}{5} + \cos\frac{2\pi}{5}\right)\\
=&\frac{1}{2}\left(-\frac{1}{2}\right)\\
=&-\frac{1}{4}
\end{aligned}$$

Par la somme et le produit que nous venons de trouver, on voit que $\cos\frac{2\pi}{5}$ et $\cos\frac{4\pi}{5}$ sont racines de

$$X^2 + \frac{1}{2}X - \frac{1}{4} = 0$$

Donc, sachant que $\cos\frac{4\pi}{5} < 0 < \cos\frac{2\pi}{5}$, en utilisant la formule quadratique nous trouvons que :

$$\cos\frac{2\pi}{5} = \frac{-\frac{1}{2} + \sqrt{\frac{5}{4}}}{2}.$$

On peut donc maintenant entamer la construction. On prend d'abord le point $H\left(-\frac{1}{2}, 0\right)$. On a directement par Pythagore que $[HJ] = \sqrt{\frac{5}{4}}$ (voir Figure 6.2), et l'on peut reporter cette distance sur l'axe des x par le cercle $C_{H,[HJ]}$. On construit ainsi le point $K\left(-\frac{1}{2} + \sqrt{\frac{5}{4}}, 0\right)$. On prend maintenant le milieu de $[OK]$ et on trouve le point $L\left(\frac{-\frac{1}{2} + \sqrt{\frac{5}{4}}}{2} = \cos\frac{2\pi}{5}, 0\right)$. On trace maintenant la droite perpendiculaire à l'axe de x passant par L et on trouve le point B et $[AB]$ étant le premier côté du pentagone régulier. En reportant cette distance le long du cercle, on construit le pentagone régulier $ABCDE$ [Carrega, 53].

Remarque 9. Examinons en détails le triangle isocèle ABD proposé par Euclide, semblant quelque peu mystérieux, et montrons qu'il est effectivement bien le triangle qu'il nous faut. La dernière construction nous donne que $[OL] = \cos\frac{2\pi}{5} = \frac{-\frac{1}{2}+\sqrt{\frac{5}{4}}}{2} = \frac{\sqrt{5}-1}{4}$. Nous savons que $[LB] = \sin\frac{2\pi}{5}$. En prenant ce résultat et $[LA] = 1 - \cos\frac{2\pi}{5}$, on trouve encore par Pythagore que le côté du pentagone régulier inscrit dans $\mathcal{C}$ mesure

$$\sqrt{(1-\cos\frac{2\pi}{5})^2+\sin^2\frac{2\pi}{5}} = \sqrt{2-2\cos\frac{2\pi}{5}} = \sqrt{2-\frac{\sqrt{5}-1}{2}} = \sqrt{\frac{5-\sqrt{5}}{2}}.$$

Or, on sait qu'Euclide construit un point F sur un des côtés égaux du triangle isocèle de départ, disons BD, de sorte que $[BD]\cdot[BF] = [DF]^2$ et que $[AB]$, le côté du pentagone régulier, est égal à $[DF]$ [Euclide, 47]. Donc,

$$[AD]\cdot[AD-AB] = [AB]^2 = \frac{5-\sqrt{5}}{2}.$$

Notons $[AD] = a, [AB = b]$. On a :

$$\begin{aligned} a^2 - ab = b^2 &\Leftrightarrow b^2 + ab - a^2 = 0 \\ &\Leftrightarrow 0 < b = \frac{-a+\sqrt{5a^2}}{2} \\ &\Leftrightarrow b = a\left(\frac{\sqrt{5}-1}{2}\right). \end{aligned}$$

Cherchons a. Le point D est donné par $e^{\frac{4i\pi}{5}}$, ce qui donne les coordonnées $(\cos\frac{4\pi}{5}, \sin\frac{4\pi}{5})$ dans le repère $\mathscr{R}(O,I,J)$. On procède à nouveau par Pythagore :

$$\sqrt{(1-\cos\frac{4\pi}{5})^2+\sin^2\frac{4\pi}{5}} = \sqrt{2-2\cos\frac{4\pi}{5}} = \sqrt{2+\frac{\sqrt{5}+1}{2}} = \sqrt{\frac{5+\sqrt{5}}{2}},$$

d'où $a^2\left(\frac{\sqrt{5}-1}{2}\right)^2 = \left(\frac{5+\sqrt{5}}{2}\right)\left(\frac{3-\sqrt{5}}{2}\right) = \frac{5-\sqrt{5}}{2} = b^2$. Le triangle ABD, avec $[AB] = \sqrt{\frac{5-\sqrt{5}}{2}}, [AD] = [BD] = \sqrt{\frac{5+\sqrt{5}}{2}}$, est donc bien le triangle donnant le côté du pentagone inscrit dans $\mathcal{C}$.

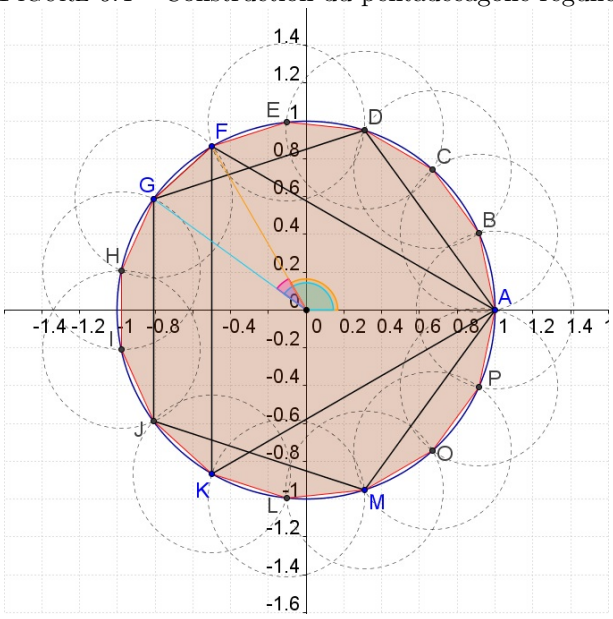
6.4.4 le Pentadecagone

Comme pour le carré, les deux constructions sont identiques pour le pentadecagone régulier. Euclide prend le pentagone et le triangle équilatéral partageant un sommet (le point I par exemple), et tous deux inscrits dans le même cercle ($\mathcal{C}$ en l'occurence). La distance entre le deuxième sommet du triangle et le troisième sommet du pentagone forme le côté du pentadecagone régulier et l'on peut reporter la distance le long du cercle pour construire le polygone régulier cherché [Euclide, 98].

Algébriquement, cela ce traduit en une relation de Bezout entre 3 et 5 : $2\times 3 - 5 = 1$. On a donc [Carrega, 54] :

$$2\widehat{\frac{2\pi}{5}} - \widehat{\frac{2\pi}{3}} = \widehat{\frac{2\pi}{15}}.$$

FIGURE 6.4 – Construction du pentadecagone régulier



Or, à partir des constructions du triangle équilatéral et du pentagone régulier on peut construire les points $F, G \in \mathcal{C}$ tels que $\widehat{AOG} = 2\dfrac{\widehat{2\pi}}{5}$ et $\widehat{AOF} = \dfrac{\widehat{2\pi}}{3}$. Ce qui nous donne $\widehat{FOG} = 2\dfrac{\widehat{2\pi}}{5} - \dfrac{\widehat{2\pi}}{3} = \dfrac{\widehat{2\pi}}{15}$ et l'on reporte au compas cette quantité le long du cercle.

6.4.5 Autres Polygones

A partir de polygones réguliers, il est possible de construire les poylgones ayant le double de côtés en utilisant les bissectrices des angles centraux. Par exemple, à partir du triangle équilatéral, on peut construire l'hexagone régulier, le dodecagone régulier, le 24-gone régulier,... A partir du carré, l'octogone, le 16-gone, ... A partir du pentagone, le decagone, le 20-gone, ... Et à partir du pentadcagone, le 30-gone, 60-gone, etc...

Comme nous le savons, tous les polygones ne sont pas constructibles. En effet, un polygone n'est constructible que si son angle central l'est. Par exemple, nous avons vu dans la section 5.2.2, que l'angle $\dfrac{\widehat{2\pi}}{3}$ n'est pas trissectable, car $\dfrac{\widehat{2\pi}}{9}$ n'est pas constructible, donc le nonogone régulier n'est pas constructible à la règle et au compas.

Chapitre 7

Des Cercles, des Droites et des Courbes Mécaniques

Comme nous l'avons vu maintenant en profondeur, la règle et le compas ne sont pas suffisant pour doubler un cube, trissecter un angle quelconque, ou quarrer un cercle. Mais, on peut utiliser ces instrument en conjonction avec d'autres courbes pour pouvoir effectivement résoudre ces problèmes. Ce travail commença déjà en Grèce Antique quand certains mathématiciens ont remarqué l'impossibilité éventuelle de résoudre ces problèmes à la règle et au compas. Certains sont parvenu à donner une résolution graphique ou mécanique. Nous en examinerons un exemple de chaque type de courbe. La Cissoïde de Dioclès est une **courbe** *dite* **graphique**, *c'est-à-dire que tout au moins de nombreux points de cette courbe sont constructibles, et l'on peut ensuite complèter la courbe. Elle donnera la duplication du cube. Pour la trissection et la quadrature, nous ferons appel à la Quadratrice de Dinostrate qui est une* **courbe mécanique**, *c'est-à-dire qu'un système mécanique précis peut la tracer [Carrega, 67, 68].*

7.1 La Cissoïde de Dioclès

Le mathématicien Dioclès inventa cette courbe au $2^{\text{ième}}$ siècle av. J.-C. Pour la construire, on se place évidemment dans $\mathscr{R}(O, I, J)$, et l'on considère le cercle $C_{K,[KI]}$, où K est le point du milieu de $[OI]$ (on retire le point O du cercle), ainsi que la droite $\mathcal{D}$ perpendiculaire à (OI) en I.

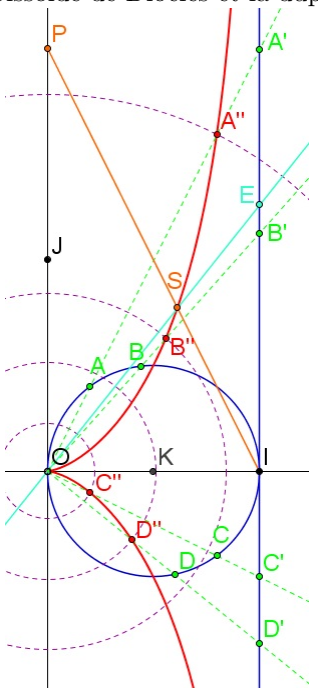
Pour obtenir la courbe recherchée, on fait correspondre au point $M \in C_{K,[KI]}$ un autre point M'' de sorte que $\overrightarrow{OM''} = \overrightarrow{MM'}$, où M' est l'intersection de (OM) et $\mathcal{D}$. Comme le montre la figure 6.3, lorsque M parcoure le cercle, le point M'' décrit cette courbe qu'est la **cissoïde de Dioclès** (voir Figure 7.1). Cette courbe est donc constructible à la règle et au compas point par point.

L'équation de $C_{K,[KI]}$ en coordonnées polaires est $\rho = \cos\theta$ et $\mathcal{D}$ par $\rho = \dfrac{1}{\cos\theta}$. Donc, la cissoïde est donnée par l'équation $\rho = \dfrac{1}{\cos\theta} - \cos\theta = \dfrac{\sin^2\theta}{\cos\theta}$, qui s'exprime en coordonnées cartésiennes par l'équation cubique $x(x^2+y^2)-y^2 = 0$ [Carrega, 77, 78].

7.1.1 La Duplication du Cube

On prend le point $P(0, 2)$ et on trace le segment $[PI]$, qui tombe sur la droite d'équation : $y = 2 - 2x$. Ce segment coupe la cissoïde au point $S(x_S, y_S)$ dont

FIGURE 7.1 – Cissoïde de Dioclès et la duplication du cube

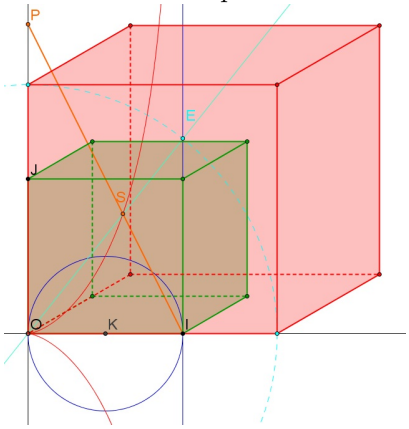


les coordonnées vérifient :

$$\begin{cases} y_S = 2 - 2x_S \\ x_S(x_S^2 + y_S^2) - y_S^2 = 0 \end{cases} \Leftrightarrow \begin{cases} y_S = 2(1 - x_S) \\ y_S^2(1 - x_S) = x_S^3, \end{cases}$$

d'où, par substitution, $y_S^3 = 2x_S^3$ i.e. $y_S = \sqrt[3]{2}x_S$, l'équation de la droite (OS) [Carrega, 78]. Donc, (OS) coupe $\mathcal{D}$ au point $E(1, \sqrt[3]{2})$, ce qui permet la duplication du cube en rapportant E au compas sur l'axe des x (formant le point E_x) et en construisant le cube recherché sur le segment $[OE_x]$.

FIGURE 7.2 – La duplication du cube

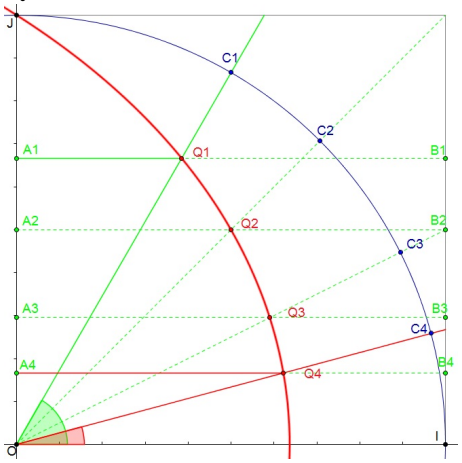


7.2 La Quadratrice de Dinostrate

La quadratrice est plus ancienne, inventée au $5^{\text{ième}}$ siècle av. J.-C. par Hippias d'Elis qui l'utilisa pour trissecter l'angle. Malheureusement pour lui, Dinostrate en fit usage un siècle plus tard pour quarrer le cercle et emporta le privilège de lui donné son nom. Pour construire cette courbe, on prend d'abord le carré sur $[OI]$ dans le premier quadrant. Comme on le voit dans la figure 7.3, on considère la droite (OC) qui tourne uniformément de la position (OJ) à (OI), le point C étant donc sur $\mathcal{C}$, le cercle unité. On prend aussi la droite (A_i, B_i) qui tombe de manière uniforme de l'arête supérieure du carré à l'arête inférieur $[OI]$. On suppose que ces deux droites quittent leurs positions initiales au même instant et arrivent à leurs positions finales au même moment. La **quadratrice de Dinostrate** est formée par le mouvement du point d'intersection Q des droites décrites.

Cette courbe n'est pas constructible à la règle et au compas, mais en partant d'angles constructibles $\widehat{IOC}$ et en formant des bissectrices en séries, on peut construire beaucoup de points de position particulière des deux droites. Donc, même si la courbe n'est pas constructible à la règle et au compas, on peut théoriquement en trouver une approximation aussi précise que l'on veut. Par contre, il est imaginable de construire un système d'engrenages pouvant tracer cette courbe mécaniquement [Carrega, 82-85].

FIGURE 7.3 – Quadratrice de Dinostrate et la trissection de l'angle



7.2.1 Trissection de l'Angle

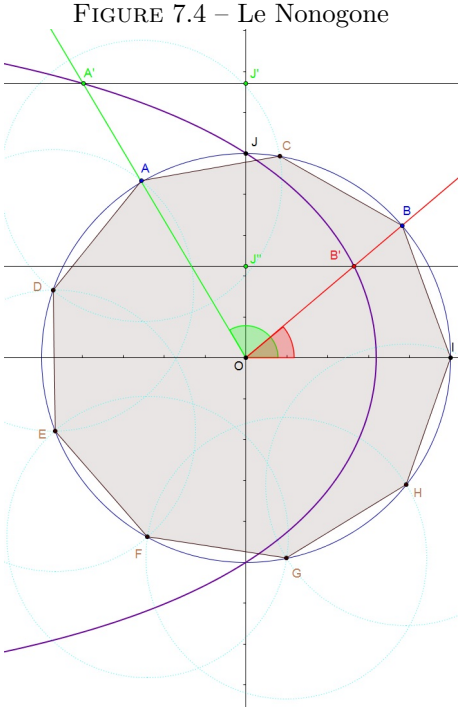
Toujours en se référant à la figure 7.3, trissectons un angle aigu $\widehat{IOC_1}$ quelconque.

On part du fait que tout point $C \in \mathcal{C}$ est directement associé à un point J_i du segment $[OJ]$, comme on le voit clairement dans la figure. Ceci veut dire que les mouvements respectifs des deux points correspondent, ainsi au tiers du parcours de C_1 vers I correspond le tiers du parcours de A_1 vers O. Via Thalès on peut trouver ce point qui est donné par A_4. On trace la droite (A_4B_4) et l'on note le point d'intersection avec la quadratice Q_4. On peut ensuite tracer la droite (OQ_4) qui coupe $\mathcal{C}$ en C_4. L'arc de cercle IC_4 étant le tiers de l'arc IC_1, (OC_4) est la trissectrice de $\widehat{IOC_1}$ [Carrega, 84].

Ceci fonctionne donc pour un angle aigu. Pour un angle obtus, il suffit d'appliquer la remarque 5 du chapitre 5 et on se réduit au cas de l'angle aigu en trissectant le demi de l'angle obtus et doublant cette trissection. Pourtant, on peut

aussi utiliser l'extension de la quadratrice et appliquer le même processus pour trissecter un angle obtus. Par exemple, comme nous l'avons mentionné dans la section 6.4.5, l'angle $\widehat{\frac{2\pi}{9}}$ n'est pas constructible à la règle et au compas. Grâce à la quadratrice, on peut trissecter $\widehat{\frac{2\pi}{3}}$, rendant la construction du nonogone régulier possible. La figure de départ est un peu différente. Il s'avère que l'équation de la quadratrice est $\rho = \frac{2\theta}{\pi \sin\theta}$ sous forme polaire et $\cot\left(\frac{y}{x}\right) - \frac{\pi}{2}y = 0$. La courbe s'étend donc plus loin que le carré unité que l'on utilise plus haut. Cela étant donné, on peut trissecter $\widehat{\frac{2\pi}{3}}$ de manière complètement analogue à celle décrite précédemment. Une fois $\widehat{\frac{2\pi}{9}}$ trouvé, on construit le nonogone régulier en reportant la distance requise le long de $\mathcal{C}$ (cf. Figure 7.4).

FIGURE 7.4 – Le Nonogone



7.2.2 Quadrature du Cercle

Il est évident selon l'équation cartésienne de la quadratrice de Dinostrate que le point d'intersection de cette courbe avec l'axe des x n'est pas défini et donc non-constructible à la règle et au compas, mais comme mentionné précédemment, nous pouvons en trouver un très bonne approximation. Il suffit de prendre la limite de $\rho(\theta)$ lorsque θ tend vers 0.

$$\lim_{\theta \to 0} \frac{2\theta}{\pi \sin\theta} = \frac{2}{\pi},$$

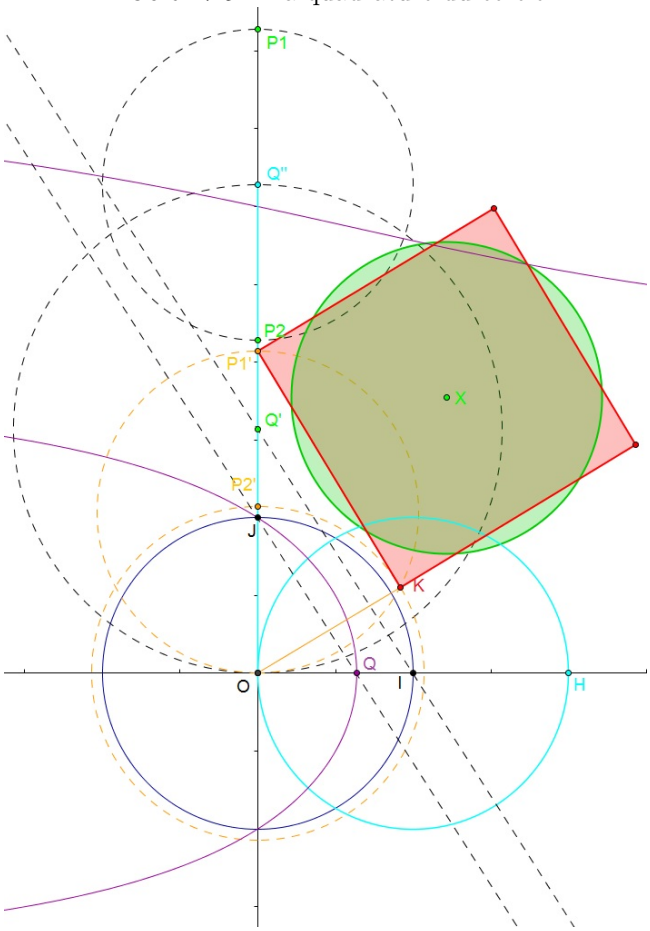
en passant par la règle de L'Hôpital. Nous avons donc un point d'abscisse $\frac{2}{\pi}$ où la quadratrice coupe l'axe des x [Carrega, 84,85].

Une fois ce point $Q\left(\frac{2}{\pi}, 0\right)$ trouvé, on peut facilement quarrer le cercle :
Par Thalès, on construit le point $Q'\left(0, \frac{\pi}{2}\right)$ (cf. Section 3.2.1) ; point qu'on peut amener à $Q''(0, \pi)$ (cf. Section 3.2.1 et Figure 7.3). Il est déjà intéressant de noté que le segment $[OQ'']$ est donc une représentation du nombre π, c'est-à-dire la longueur du demi-cercle OH ou encore l'air de $\mathcal{C}$.
On veut construire un segment de longeur $\sqrt{\pi}$. Donc partant de $[OQ''] = \pi$ on suit la démarche montrée lors de la démonstration du théorème 1 et l'on construit d'abord les points $P_1(0, \pi + 1)$ et $P_2(0, \pi - 1)$. Ensuite, on trouve les milieux des segments $[OP_1]$ et $[OP_2]$, $P_1'\left(0, \frac{\pi+1}{2}\right), P_2'\left(0, \frac{\pi-1}{2}\right)$ respectivement. Afin d'avoir un triangle rectangle d'hypothènuse $[OP_1']$ et ayant $\frac{\pi-1}{2}$ pour côté on trouve le point d'intersection K du cercle de diamètre $[OP_1]$ et du cercle $C_{O,[OP_2']}$ [Euclide, 73]. On trouve donc par Pythagore que

$$[KP_2'] = \sqrt{\left(\frac{\pi+1}{2}\right)^2 - \left(\frac{\pi-1}{2}\right)^2} = \sqrt{\pi}.$$

Le carré construit sur $[KP_2']$ a donc bien une aire de π et donc égale à celle du cercle centré en X, le centre du carré, et de rayon 1.

FIGURE 7.5 – La quadrature du cercle



Chapitre 8

Epilogue

Il fallu donc plus de 2300 ans pour que les problèmes de la duplication du cube, la trissection de l'angle, la quadrature du cercle, et la construction de polygones réguliers soient élucidés. Tous les grands mathématiciens de l'histoire y ont travaillé, amenant aux résultats grandioses de Descartes, Gauss, et Wantzel. Il est rare de trouver des problèmes mathématiques ayant le pouvoir de traverser les âges et d'émerveiller les mathématiciens jusqu'à aujourd'hui. Le bagage mathématique qu'ils renferment – géométrie classique, algèbre, théorie des corps, racines primitives de l'unité, polynômes cyclotomiques – est très riche. Examiner son histoire fait découvrir l'aspect collectif de leur développement de siècle en siècle et démontre la fabuleuse capacité qu'ont les mathématiques de transcender le temps.

Bibliographie

[Archimède] Archimède. trad. Sir Thomas L. Heath *The Works of Archimedes*. Dover, New York 2002. ISBN : 0 4864 2084 4.

[Carrega] Carrega, Jean-Claude. *Théorie des Corps : La Règle et le Compas*. 2nde éd. Hermann, Paris 1981. ISBN : 2 7056 1402 8.

[Escofier] Escofier, Jean-Pierre. *Théorie de Galois*. 2nde éd. Dunod, Paris 1997. ISBN : 2 1000 7685 X.

[Euclide] Euclide. trad. Sir Thomas L Heath *Euclid's Elements : all thirteen books complete in one volume*. 3ème éd. Dana Densmore. Green Lion P, Santa Fe, NM 2002. ISBN : 1 8880 0919 5.

[Guin et Hausberger] Guin et Thomas Hausberger. *Algèbre I : Groupes, Corps et Théorie de Galois*. EDP Sciences, Les Ulis 2008. ISBN : 2 8688 3974 6.

[Joseph] Joseph, George Gheverghese. *The Crest of the Peacock : Non-European Roots of Mathematics*. 3ème éd. Princeton UP 2011. ISBN : 0 6911 3526 7.

[Katz] Katz, Victor J. *A History of Mathematics : Brief Edition*. Pearson, Boston 2004. ISBN : 0 9211 6193 9.

Index