Constructions à la règle et au compas

Yannick VINCENT

Novembre 2023

Table des matières

Introduction

Les problèmes de construction à la règle et au compas sont des problèmes qui ont structuré le développement des mathématiques depuis leurs origines. Dès l'antiquité, les Grecs s'étaient posés ce genre de questions, se heurtant notamment au problème de la duplication du cube, de la trissection de l'angle et de la quadrature du cercle. Ces problèmes resteront ouverts jusqu'au XIX^{e} siècle lorsque Pierre Wantzel parvint à caractériser complètement les points constructibles à la règle et au compas et montrer ainsi l'impossibilité de ces trois problèmes.

Il est intéressant de noter que ce que Wantzel ramène ces questions géométriques à une question portant sur la nature algébrique des coordonnées du point à construire. Cette dualité de considérations théorie des nombres / géométrie était d'ailleurs déjà présente chez les grecs. Il suffit de penser par exemple à la crise des indivisibles engendrée par la découverte de ce que nous appelons aujourd'hui l'irrationalité de $\sqrt{2}$, pourtant constructible à la règle et au compas grâce à la diagonale d'un carré de côté 1.

Le texte ci-dessous présente les problèmes de la construction à la règle et au compas en utilisant la théorie des corps. Après avoir défini la notion de constructibilité dans la partie 1, on démontre le Théorème de Wantzel dans la partie 2 et on l'applique dans la partie suivante afin de démontrer l'impossibilité des trois problèmes classiques énoncés par les grecs. La suite utilise la théorie de Galois, la correspondance de Galois étant utile dans la partie 5 pour caractériser complètement les polygones constructibles. Cela permettra de revenir sur des résultats connus et énoncés par le jeune Gauß, avec par exemple la construction du heptadécagone (polygone à 17 côtés).

I. Définitions et premières constructions

Définition .1

Soit $\mathscr{P}$ un plan euclidien et E un sous-ensemble fini de $\mathscr{P}$ ayant au moins deux éléments.
Un point $M \in \mathscr{P}$ est dit constructible à la règle et au compas à partir de E s'il existe une suite finie de points $M_1, \dots, M_n$ telle que $M_n = M$ et telle que pour tout $1 \leqslant i \leqslant n$, M_i est un point d'intersection :

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

ces droites et cercles étant obtenus à l'aide de l'ensemble $E_i = E \cup \{M_1, \dots, M_{i-1}\}$.
Plus précisément, à chaque étape, on peut construire

- des droites passant par deux points distincts de E_i ;
- des cercles centrés en un point de E_i et ayant pour rayon la distance entre deux points de E_i.

Histoire – Euclide et les constructions à la règle et au compas.

Vers -300 av.J.C., dans les *Éléments*, Euclide base toute sa théorie géométrique sur les droites et les cercles. Le premier postulat énonce en effet « qu'il soit demandé de mener une ligne droite de tout point à tout point » et le troisième « qu'il soit demandé de décrire un cercle à partir dez tout centre et au moyen de tout intervalle ». L'intuition d'Euclide était que tout nombre pouvait être construit à l'aide de ces deux instruments.

Euclide [a]

a. Gravure inspirée de l'ouvrage d'André Thevet, Les vrais portraits et vies des hommes illustres grecs, latins et payens, 1584, livre II.

Exemple
Il est facile de construire :
- la parallèle et la perpendiculaire à une droite passant par un point ;
- la médiatrice d'un segment et donc son milieu ;
- la bissectrice d'un angle.

Dans toute la suite, on se place dans un plan euclidien muni d'un repère orthonormé (O, I, J) et on considère le cas où E = {O, I}.

Remarque
On peut supposer, de manière équivalente, que E = {O, I, J} étant donné que J est facilement constructible à partir de O et I.

Définition .2
Un nombre réel est dit constructible si c'est une des coordonnées dans le repère (O, I, J) d'un point constructible. On note $\mathscr{C}$ l'ensemble des nombres réels constructibles.

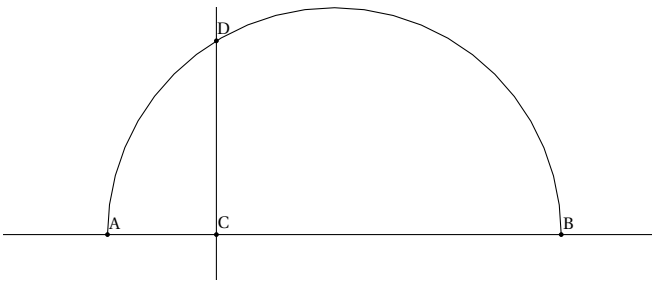
Définition .3
En identifiant le plan $\mathscr{P}$ au corps des complexes, on dit que $z \in \mathbb{C}$ est constructible si le point d'affixe z est constructible. Autrement dit, $z \in \mathbb{C}$ est constructible si $\mathrm{Re}(z)$ et $\mathrm{Im}(z)$ sont des réels constructibles.

Proposition 1
L'ensemble des nombres complexes constructibles est le corps $\mathscr{C}(i)$. Il est stable par racine carrée complexe c'est-à-dire que si $\delta^2 \in \mathscr{C}(i)$ (où $\delta \in \mathbb{C}$), alors $\delta \in \mathscr{C}(i)$.

Démonstration. Il est clair que tout élément de $\mathscr{C}(i)$ est constructible. Réciproquement si $z \in \mathbb{C}$ est constructible, sa partie réelle et sa partie imaginaire le sont donc il appartient à $\mathscr{C}(i)$.
La stabilité par racine carrée découle également de la stabilité de $\mathscr{C}$ par racine carrée réelle étant donné que la racine carrée complexe d'un nombre z s'exprime sous forme algébrique en fonction de $\mathrm{Re}(z)$ et de $\mathrm{Im}(z)$ (avec des sommes, produits, inverse et racines carrées).

Théorème 2
$\mathscr{C}$ est un sous-corps de $\mathbb{R}$ stable par racine carrée, c'est-à-dire que pour tout $x \in \mathscr{C} \cap \mathbb{R}^+$, $\sqrt{x} \in \mathscr{C}$.

Démonstration. Soient $x, y \in \mathscr{C}$. Il est clair, en reportant les longueurs x et y au compas que $x+y$ et que $x-y$ sont également constructibles donc que $x+y \in \mathscr{C}$ et que $x-y \in \mathscr{C}$.
Par ailleurs, si $y \neq 0$, $\dfrac{x}{y}$ se construit aisément à l'aide du théorème de Thalès. Le réel $xy = \dfrac{x}{\frac{1}{y}}$ se construit alors de la même manière.
Enfin, si $x \in \mathscr{C} \cap \mathbb{R}^+$, on peut construire $\sqrt{x}$ grace au théorème de Pythagore. Plus précisément, sur la figure ci-dessous composée d'un demi-cercle et avec (AB) et (CD) perpendiculaires, si AC = 1 et BC = x, alors CD = $\sqrt{x}$.



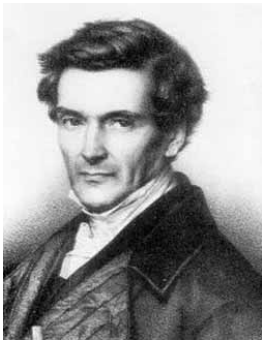
II. Théorème de Wantzel

Théorème 3 – Wantzel

Soit $z \in \mathbb{C}$. Les conditions suivantes sont équivalentes :
(i) z est constructible ;
(ii) il existe une suite finie de corps $(K_i)_{0\leqslant i\leqslant n} \subset \mathbb{C}$ telle que $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n$, telle que $z \in K_n$ et telle que pour tout $i \leqslant 0 \leqslant n-1$, $[K_{i+1} : K_i] = 2$.

Histoire – Théorème de Wantzel

Pierre Wantzel (1814-1848) est un mathématicien français formé à l'École polytechnique. En 1837, il a publié dans le *Journal de Liouville* le théorème qui porte son nom dans un article intitulé « Recherche sur les moyens de reconnaître si un problème de géométrie peut se résoudre à la règle et au compas ». Cela a permis de répondre à des problèmes ouverts depuis l'Antiquité tels que la duplication du cube, la trissection de l'angle et plus tard à la quadrature du cercle.



Pierre Wantzel

Démonstration.
(i) $\Longrightarrow$ (ii) : Soit $z = x + iy \in \mathbb{C}$ constructible en un nombre fini d'étapes à partir d'intersections de deux droites, d'une droite et d'un cercle ou de deux cercles. Supposons qu'un point $M(x, y)$ soit construit à partir de points ayant tous leurs coordonnées dans un corps $\mathbb{K}$.

- Si M est l'intersection de deux droites, ses coordonnées sont des éléments de $\mathbb{K}$ (on résout simplement un système linéaire à coefficients dans $\mathbb{K}$ pour les déterminer).

- Si M est l'intersection d'une droite et d'un cercle, (x, y) est solution d'un système de la forme suivante (où l'on peut supposer, par exemple, $b \neq 0$) :

$$\begin{cases} ax + by + c = 0 \\ (x - x_0)^2 + (y - y_0)^2 = r^2 \end{cases} \iff \begin{cases} y = -\dfrac{c}{b} - \dfrac{a}{b}x \\ (x - x_0)^2 + (-\dfrac{c}{b} - \dfrac{a}{b}x - y_0)^2 = r^2 \end{cases}$$

  L'abscisse x vérifie donc une équation du second degré. Ses coordonnées sont donc dans $\mathbb{K}(\sqrt{\Delta})$ qui est de degré 1 ou 2 sur $\mathbb{K}$. La même chose vaut pour y.
- Si M est l'intersection de deux cercles, (x, y) est solution d'un système de la forme suivante :

$$\begin{cases} (x - x_0)^2 + (y - y_0)^2 = r^2 \\ (x - x_0')^2 + (y - y_0')^2 = r'^2 \end{cases} \iff \begin{cases} x^2 + y^2 - 2(x_0 x + y_0 y) + x_0^2 + y_0^2 = r^2 \\ x^2 + y^2 - 2(x_0' x + y_0' y) + x_0'^2 + y_0'^2 = r'^2 \end{cases}$$

  En faisant, la différence des deux lignes, on voit que le système se rammène la résolution d'un système composé d'une équation de degré 2 et d'une équation de degré 1 comme dans le cas de l'intersection d'une droite et d'un cercle. On peut alors conclure de la même manière que les coordonnées x et y sont dans un corps de degré 1 ou 2 sur $\mathbb{K}$.

Ainsi, on en déduit que si z est constructible en un nombre fini d'étapes N, il existe une suite d'extensions $(K_i)_{1\leqslant i\leqslant n}$ telle que $K_0 = \mathbb{Q}$, $z \in K_N$ et $[K_{i+1} : K_i] = 1$ ou 2. Il suffit d'enlever les corps K_i tels que $[K_{i+1} : K_i] = 1$ de la suite afin d'obtenir la suite d'extensions quadratique souhaitée.

(i) $\Longrightarrow$ (ii) : Supposons que tous les éléments de K_i sont constructibles et montrons par récurrence que tous les éléments de K_{i+1} sont également constructibles (l'initialisation est immédiate). Comme $[K_{i+1} : K_i] = 2$, cela signifie que $K_{i+1} = K_i(\delta)$ où $\delta^2 \in K_i$ (δ est de degré 2). Or, comme il est possible de construire toute racine carrée (réele donc complexe) d'éléments déjà construits, δ sera constructible et donc tous les éléments de K_{i+1} également.

Remarque
Si $x \in \mathbb{R}$ est constructible, il est possible de construire une suite de corps $(K_i) \subset \mathbb{R}$. Pour le voir, il suffit de considérer, à partir de la suite $(K_i) \subset \mathbb{C}$, la suite d'extensions $K_i \cap \mathbb{R}$.

Corollaire 4

Si $z \in \mathbb{C}$ est constructible, il est algébrique sur $\mathbb{Q}$ et le degré de z sur $\mathbb{Q}$ est une puissance de 2

Démonstration. Soit $(K_i)_{0 \leqslant i \leqslant n}$ la suite d'extensions quadratiques définies dans le théorème 3.
On a $\mathbb{Q} \subset \mathbb{Q}(z) \subset K_n$. Comme $[K_n : \mathbb{Q}]$ est une puissance de 2, on déduit, par multiplicativité des degrés, que $[\mathbb{Q}(z) : \mathbb{Q}]$ est une puissance de 2.

Remarque
La réciproque du corollaire 4 est fausse. On peut considérer par exemple le polynôme

$$P(X) = X^4 - 4X + 2 \in \mathbb{Q}[X]$$

irréductible sur $\mathbb{Q}$ (critère d'Eisenstein). Si ζ est une racine de P, on a $[Q(\zeta) : \mathbb{Q}] = 4$. Pourtant les racines de P ne sont pas constructibles.
En effet, P a exactement deux racines réelles et est de la forme $P(X) = (X - r)(X - s)(X^2 + aX + b)$.
En identifiant les coefficients, et en posant $t = b + rs$, on peut montrer que t est racine de $Q(X) = X^3 - 8X + 16$.
Or Q est irréductible sur $\mathbb{Q}$ (il n'a pas de racine dans $\mathbb{Q}$). Ainsi, $[\mathbb{Q}(t) : \mathbb{Q}] = 3$ donc $t \notin \mathscr{C}$.
De plus, $r \notin \mathscr{C}$ et $s \notin \mathscr{C}$. En effet, sinon on aurait $t = (r + s)^2 \in \mathscr{C}$.

Corollaire 5

$\mathscr{C}$ est le plus petit sous-corps de $\mathbb{R}$ stable par racine carrée.

Démonstration. $\mathscr{C}$ est un sous-corps de $\mathbb{R}$ stable par racine carrée. De plus, si $\mathscr{C}'$ est un autre sous-corps stable par racine carrée, on a nécessairement $\mathscr{C} \subset \mathscr{C}'$.
En effet, soit $x \in \mathbb{C}$. Il existe, d'après le théorème de Wantzel, une suite (K_i) d'extensions quadratiques telle que $x \in \mathbb{K}_n$. Par stabilité de $\mathscr{C}'$ par racine carrée, il est clair qu'il contient tous les K_i (raisonnement par récurrence) et donc que $x \in \mathscr{C}'$.

Corollaire 6

$\mathscr{C}(i)$ est le plus petit sous-corps de $\mathbb{C}$ stable par racine carrée.

Démonstration. La preuve est identique à celle du Corollaire 5

III. Impossibilité de trois problèmes classiques

1. Duplication du cube

Le problème de la duplication du cube consiste à construire, à partir d'un cube de volume 1, un cube de volume 2. Cela revient à se poser la question de la constructibilité de $\sqrt[3]{2}$.

Histoire – Problème de Délos

Le problème de Délos a son origine dans une légende rapportée entre autres par Ératosthène dans *Le Platonicien*. Face à une épidémie de peste dans la ville de Délos de la Grèce antique, un oracle aurait exigé la construction d'un autl exactement deux fois plus grand que l'autel cubique qui existait déjà dans la ville. Un autel fut construit en doublant les dimensions mais l'épidémie de peste continua. Les architectes allèrent trouver Platon pour savoir que faire. Ce dernier leur répondit que le dieu n'avait certainement pas besoin d'un autel double, mais qu'il leur faisait reproche, par l'intermédiaire de l'oracle, de négliger la géométrie.

Théorème 7

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

Démonstration. Le polynôme minimal de $\sqrt[3]{2}$ est X^3-2 (il est irréductible d'après le critère d'Eisenstein). Comme il est de degré 3, on déduit du corollaire du théorème de Wantzel (Corollaire 4) que $\sqrt[3]{2}$ n'est pas constructible.

2. Trisection de l'angle

On suppose avoir construit un angle θ. On se demande alors s'il est possible de construire l'angle $\frac{\theta}{3}$. Cela revient à se poser la question de la constructibilité de $\cos\left(\frac{\theta}{3}\right)$ à partir de $\cos(\theta)$.

Théorème 8

L'angle θ est trisectable si, et seulement si, le polynôme $4X^3-3X-\cos(\theta)$ est réductible dans $\mathbb{Q}(\cos(\theta)[X]$.

Histoire – Trissection de l'angle

Le problème de la trissection de l'angle fut posé vers -450 av. J.C. par le grec Hippias d'Élis. Dès le III^{e} sicèle av. J.C., Archimède imagine une solution avec un compas et une règle graduée. Un siècle plus tard, Nicomède utilisa une courbe auxiliaire, la conchoïde de droite pour déterminer la solution. Ce n'est, là encore, qu'au *xix*^{e} siècle que Wantzel a pu prouver l'impossibilité de la trissection de tous les angles au compas et à la règle non graduée.

Archimède [a]

a. Par Domenico Fetti, 1620, Musée Alte Meister, Dresde (Allemagne).

Démonstration. La preuve repose sur le fait que $\cos(\theta)=4\cos^3\left(\frac{\theta}{3}\right)-3\cos\left(\frac{\theta}{3}\right)$.

- Supposons que $\theta=\widehat{\mathrm{IOM}}$ est trisectable. En généralisant le théorème de Wantzel, on peut dire qu'il existe une suite de corps $(K_i)_{0\leqslant i\leqslant n}$ telle que $\cos\left(\frac{\theta}{3}\right)\in K_n$, que $K_0=\mathbb{Q}(\cos(\theta))$, et telle que chaque corps K_{i+1} est une extension quadratique de K_i. Ainsi, $\mathbb{Q}(\cos(\theta))\left(\cos\left(\frac{\theta}{3}\right)\right)$ est de degré une puissance de 2 sur $\mathbb{Q}(\cos(\theta))$. On en déduit que $4X^3-3X-\cos(\theta)$ (dont $\cos\left(\frac{\theta}{3}\right)$ est une racine) ne peut pas être irréductible sur $\mathbb{Q}(\cos(\theta))$.
- Réciproquement, supposons que $P(X)=4X^3-3X-\cos(\theta)$ soit réductible dans $\mathbb{Q}(\cos(\theta)[X]$.
  Alors, comme $\cos\left(\frac{\theta}{3}\right)$ est une racine de P elle est soitt racine d'un polynôme de degré 1 sur $\mathbb{Q}(\cos(\theta)[X]$, soit racine d'un polynôme de degré 2 sur $\mathbb{Q}(\cos(\theta)[X]$. Dans tous les cas, par stabilité des nombres constructibles par racine carrée, on en déduit que $\cos\left(\frac{\theta}{3}\right)$ est constructible à partir de $\cos(\theta)$ et donc que $\frac{\theta}{3}$ est trisectable.

Corollaire 9

L'angle $\frac{\pi}{3}$ n'est pas trisectable.

Démonstration. Il suffit d'appliquer le Théorème 8 pour $\theta=\frac{\pi}{3}$.
Le polynôme $P(X)=4X^3-3X-\frac{1}{2}$ est en effet irréductible sur $\mathbb{Q}\left(\cos\left(\frac{\pi}{3}\right)\right)=\mathbb{Q}$ car il n'admet pas de racine dans $\mathbb{Q}$.

Remarque
Les angles de la forme $\frac{\pi}{9k}$ (avec $k \in \mathbb{N}^*$) ne sont pas constructibles. Sinon, il serait facile de construire $\frac{\pi}{9}$ qui est un multiple de ces angles.

Remarque
Il existe des angles trisectables qui ne sont pas constructibles. On peut par exemple trouver un angle θ tel que $P(X) = 4X^3 - 3X - \cos(\theta)$ est réductible sur $\mathbb{Q}(\cos(\theta))$ mais tel que $\cos(\theta)$ (ou $\cos\left(\frac{\theta}{3}\right)$) a un polynôme minimal de degré 3 sur $\mathbb{Q}$.
En effet, d'après le théorème des valeurs intermédiaires, il existe θ_0 tel que $\cos\left(\frac{\theta_0}{3}\right) = \cos(\theta_0) + \frac{1}{2}$.
Ainsi, le polynôme P admet une racine dans $\mathbb{Q}(\cos(\theta_0))$ donc il est réductible sur $\mathbb{Q}(\cos(\theta_0))$.
En revanche, comme $\cos^3\left(\frac{\theta_0}{3}\right) - 3\cos\left(\frac{\theta_0}{3}\right) = \cos(\theta_0) = \cos\left(\frac{\theta_0}{3}\right) - \frac{1}{2}$, on voit que $\cos\left(\frac{\theta_0}{3}\right)$ est racine de $Q(X) = 4X^3 - 4X + \frac{1}{2}$.
Comme Q est irréductible sur $\mathbb{Q}$ (il n'a pas de racine dans $\mathbb{Q}$), on en déduit que $\cos\left(\frac{\theta_0}{3}\right)$ n'est pas constructible. Par suite, $\cos(\theta_0)$ n'est pas constructible non plus.

3. Quadrature du cercle

Le problème de la quadrature du cercle consiste à construire un carré de même aire qu'un cercle de rayon 1. Autrement dit, on se demande si $\sqrt{\pi}$ (et donc π) est constructible ou non.

Théorème 10 – Lindemann (admis)
π est transcendant.

Histoire – Transcendance de e et π
En 1873, Charles Hermite (1822-1901) avait démontré que e est un nombre transcendant. En 1882, Ferdinand von Lindemann (1852-1939) parvient à démontrer que si a est un nombre algébrique, alors e^a est transcedant. Comme on sait que $e^{i\pi} = -1$ est algébrique, c'est donc que π est lui-même transcendant. Ce résultat sera généralisé quelques années plus tard par Karl Weierstraß (1815-1897) et porte le nom de théorème de Lindemann-Weierstraß.


Ferdinand von Lindemann

Corollaire 11
π n'est pas constructible.

IV. Constructibilité et théorie de Galois

1. Rappels de théorie de Galois

Théorème 12 – Élément primitif
Soit $K \subset \mathbb{C}$ un corps. Pour toute extension finie L de K, il existe $\zeta \in L$ tel que $L = K(\zeta)$.

Définition .4
Une extension $K \subset L$ est normale si tout polynôme $P \in \mathbb{K}[X]$ admettant une racine dans L admet toutes ses racines dans L.

Proposition 13

Une extension $N \subset \mathbb{C}$ algébrique et de degré fini d'un corps K est normale si, et seulement si, tout K-homomorphisme $\sigma : N \longrightarrow \mathbb{C}$ a une image contenue dans N.

Proposition 14

Soit $K \subset \mathbb{C}$, un corps. Le corps de décomposition d'un polynôme $P \in \mathbb{K}[X]$ est une extension normale de K.

Définition .5

Soit $K \subset \mathbb{C}$ et L une extension algébrique de K. La cloture normale de L sur $\mathbb{K}$ est la plus petite extension normale N de K contenant L.

Proposition 15

Soit $K \subset \mathbb{C}$ et $L = K[a_1, \ldots, a_n] \subset \mathbb{C}$ une extension de degré fini. La cloture normale N de L sur K est l'extension de K par l'ensemble des conjugués sur K des éléments $a_1, \ldots, a_n$.

Définition .6

Soit K un corps et L une extension de K. L'ensemble des K-automorphismes de L est un groupe appelé groupe de Galois de L sur K et noté $Gal(L|K)$.

Définition .7

Si P est un polynôme sur $K \subset \mathbb{C}$ et N son corps de décomposition, on appelle groupe de Galois de P le groupe $Gal(N|K)$.

Proposition 16

Soit $K \subset \mathbb{C}$ et N une extension normale de K de degré fini. L'ordre du groupe $Gal(N|K)$ est $[N : K]$.

Théorème 17 – Correspondance de Galois

Soit K un corps, N une extension normale de degré fini de K. On note $mathcal$E l'ensemble des extensions intermédiaires entre K et N et $\mathcal{G}$ l'ensemble des sous-groupes de $Gal(N|K)$.
Soit $I : \mathcal{G} \longrightarrow \mathcal{E}$ l'application qui à un sous groupe H associe l'ensemble des invariants de H.
Soit $G : \mathcal{E} \longrightarrow \mathcal{G}$ l'application, qui associe à une extension L le groupe $Gal(N|L)$.
Alors I et G sont des bijections réciproques, décroissantes pour l'inclusion.
De plus, si L et L′ sont des extensions intermédiaires entre K et N avec $L \subset L'$, alors :

$$[L' : L] = \frac{\#Gal(N|L)}{\#Gal(N|L')}$$

2. Constructibilité et corps de décomposition

On a vu que si x est un nombre algébrique de degré une puissance de 2, x n'est pas nécessairement constructible. Considérer le corps de décomposition du polynôme minimal de x va en revanche permettre d'établir une CNS de constructibilité.

Théorème 18

Soit $z \in \mathbb{C}$ un nombre algébrique sur $\mathbb{Q}$ de polynôme minimal P. On note D le corps de décomposition de P. Les conditions suivantes sont équivalentes :
(i) z est constructible ;
(ii) $[D : \mathbb{Q}]$ est une puissance de 2.

Démonstration.
(i) $\Longrightarrow$ (ii) : Soit $z \in \mathbb{C}$ constructible. D'après le théorème de Wanzel, il existe $K_0 = \mathbb{Q} \subset K_1 \subset \cdots \subset K_n$ une suite d'extensions quadratiques avec $z \in K_n$. Soit L la cloture normale de K_n. Comme $z \in L$, P est scindé sur L.
De plus, L est de degré fini sur $\mathbb{Q}$ (car c'est la cloture normale d'une extension de degré fini sur $\mathbb{Q}$) et est inclus dans $\mathscr{C}(i)$.
En effet, pour tout $\mathbb{Q}$ homomorphisme $\sigma : K_n \longrightarrow C$, $\sigma(K_n) \subset \mathscr{C}(i)$. Cela vient simplement du fait que pour tout i, $[\sigma(K_{i+1} : \sigma(K_i)] = 2$.
Ainsi, $\mathscr{C}(i)$ est une extension normale de K_n et contient donc la cloture normale L.
Enfin, en considérant un élément primitif ζ de L, on a $L = \mathbb{Q}(\zeta)$. Or, ζ est constructible donc $[L : \mathbb{Q}]$ est une puissance de 2.
On conclut par la multiplicativité des degrés :

$$[L : \mathbb{Q}] = [L : D] \times [D : \mathbb{Q}]$$

et on en déduit donc que $[D : \mathbb{Q}]$ est une puissance de 2.

(ii) $\Longrightarrow$ (i) : Supposons que $[D : \mathbb{Q}] = 2^k$. Le corps de décomposition D est une extension normale de $\mathbb{Q}$ et on a $\#Gal(D : \mathbb{Q}) = 2^k$.
D'après la théorie des groupes, il existe une suite croissante (G_i) de sous groupes de $Gal(D|\mathbb{Q})$ telle que

$$G_0 = Gal(D|\mathbb{Q}) \supset G_1 \subset \ldots \subset G_n = \{id\}$$

avec $[G_i : G_{i+1}] = 2$.
La correspondance de Galois (D est une extension normale) fournit donc une suite de corps : $L_0 = \mathbb{Q} \subset \ldots \subset L_n = D$ telle que $[L_{i+1} : L_i] = 2$ pur tout i. Ainsi, $z \in D$ est bien constructible.

Corollaire 19

Si z_1 et z_2 sont deux nombres algébriques conjugués (ayant même polynôme minimal), alors z_1 est constructible si, et seulement si, z_2 l'est.

Exemple
En reprenant l'exemple du polynôme $P(X) = X^4 - 4X + 2$, on voit que le degré du corps de décomposition n'est pas une puissance de 2. En effet, P admet deux racines réelles r et s et deux racines complexes conjuguées z_0 et $\overline{z_0}$.
On a $D = \mathbb{Q}(r, s, z_0)$. Avec $t = (r+s)^2$, on a vu que $[\mathbb{Q}(t) : \mathbb{Q}] = 3$. Comme $\mathbb{Q}(t) \subset D$, on en déduit, avec la multiplicativité des degrés, que $[D : \mathbb{Q}]$ est divisible par 3 et que les racines de P ne sont pas constructibles.

V. Construction des polygones réguliers

1. Rappel sur les racines de l'unité

On note $\mathbb{U}_n$ l'ensemble des racines n-ième de l'unité et $\widetilde{\mathbb{U}_n}$ l'ensemble des racines primitives de l'unité.
On a

$$X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega)$$

Définition .8

Le n-ième polynôme cyclotomique est

$$\Phi_n(X) = \prod_{\omega \in \widetilde{\mathbb{U}_n}} (X - \omega)$$

Proposition 20

Pour tout $n \geqslant 1$, $\Phi_n \in \mathbb{Z}[X]$ et Φ_n est irréductible sur $\mathbb{Q}$.

Proposition 21

Φ_n est de degré $\varphi(n)$ (l'indicatrice d'Euler) et on a :
- $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ pour tout entier premier p et tout $\alpha \in \mathbb{N}^*$.
- $\varphi(nm) = \varphi(n)\varphi(m)$ pour tous entiers n et m premiers entre eux.

2. Constructibilité des polygones réguliers

Savoir si l'on peut construire un polygone régulier à n côtés revient à se poser la question de la constructibilité d'un angle de mesure $\frac{2\pi}{n}$ et donc de la constructibilité de $e^{\frac{2i\pi}{n}}$

Proposition 22

Soient n et m deux entiers naturels premiers entre eux.
$e^{\frac{2i\pi}{nm}}$ est constructible si, et seulement si, $e^{\frac{2i\pi}{n}}$ et $e^{\frac{2i\pi}{m}}$ sont constructibles.

Démonstration.
(i) $\Longrightarrow$ (ii) : Si $e^{\frac{2i\pi}{nm}}$ est constructibles alors $e^{\frac{2i\pi}{n}}$ et $e^{\frac{2i\pi}{m}}$ le sont car $\frac{2\pi}{n}$ et $\frac{2\pi}{m}$ sont des multiples de $\frac{2\pi}{nm}$.

(ii) $\Longrightarrow$ (i) : Si n et m sont premiers entre eux, d'après Bézout, il existe $\alpha, \beta \in \mathbb{Z}$ tels que $\alpha n + \beta m = 1$.
Ainsi,

$$\frac{2\pi}{nm} = \frac{2\pi}{nm}(\alpha n + \beta m) = \alpha\frac{2\pi}{m} + \beta\frac{2\pi}{n}.$$

On a donc

$$e^{\frac{2i\pi}{nm}} = \left(e^{\frac{2i\pi}{m}}\right)^\alpha \left(e^{\frac{2i\pi}{n}}\right)^\beta.$$

et $e^{\frac{2i\pi}{nm}}$ est donc constructible.

Remarque
En décomposant n en produit de facteurs premiers, la Proposition 22 permet de ramener l'étude de la constructibilité des polygones réguliers au cas où $n = p^\alpha$ avec p premier.
Dans le cas $p = 2$, tous les polygones réguliers à 2^α côtés (où $\alpha \geqslant 1$) sont constructibles. En effet, on les construit par récurrence en construisant, à chaque étape, la bissectrice de l'angle $\frac{2\pi}{2^k}$. Le théorème suivant donne une condition de constructibilité d'un polygone régulier à $n = p^\alpha$ côtés pour p premier impair.

Théorème 23 – Gauß

Un polygone régulier à n côtés est constructible si, et seulement si,

$$n = 2^\alpha p_0 \dots p_r$$

où α est quelconque et les p_i sont des nombres premiers de Fermat distincts (de la forme $2^{2^k}+1$).

Histoire – Théorème de Gauß

À 19 ans, en 1796, **Carl Friedrich Gauß** (1777-1855) propose une construction du polygone à 17 côtés et énonce le théorème caractérisant les polygones constructibles à l'aide des nombres de Fermat. Il ne démontre cependant qu'une implication du théorème, la réciproque étant démontrée par Pierre Laurent Wantzel (1814-1848) en 1837 avec le théorème qui porte son nom. Satisfait de son résultat, Gauß demanda que soit gravé un polygone à 17 côtés sur sa tombe. Après sa mort, et face aux difficultés techniques que cela présentait, cela ne fut jamais réalisé.

Carl Friedrich Gauß

Démonstration. D'après la Proposition 22 et la remarque précédente, il suffit de montrer qu'un polygone régulier à p^α côtés (avec p premier impair) est constructible si, et seulement si, p est un nombre de Fermat et $\alpha = 1$.
Or, le polynôme minimal de $e^{2i\pi}p^\alpha$ est Φ_{p^α} et le corps de décomposition de Φ_{p^α} est $\mathbb{Q}(e^{2i\pi}p^\alpha)$ qui est de degré $\varphi(p^\alpha)$ sur $\mathbb{Q}$.
D'après le Théorème 18, $e^{2i\pi}p^\alpha$ est donc constructible si, et seulement si, $\varphi(p^\alpha)$ est une puissance de 2.
Or, $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ donc c'est une puissance de 2 si, et seulement si, $\alpha = 1$ et $p-1$ est une puissance de 2. Autrement dit, il existe $m \in \mathbb{N}^*$ tel que $p = 2^m + 1$.
On peut alors montrer que m est en fait une puissance de 2.
En effet, supposons par l'absurde que m n'est pas une puissance de 2. On pose $m = 2^k n$ (avec $n \geqslant 3$ impair).
On a alors

$$\begin{aligned} p &= 2^m + 1 \\ &= 2^{2^k n} + 1 \\ &= \left(2^{2^k}\right)^n - (-1)^n \qquad \text{(car } n \text{ est impair)} \\ &= \left(2^{2^k} + 1\right)\left(\sum_{i=0}^{n-1} \left(2^{2^k}\right)^i \times (-1)^{n-1-i}\right) \end{aligned}$$

Ainsi, p ne serait pas premier, ce qui est absurde. On a donc montré que $p = 2^{2^k} + 1$ est un nombre premier de Fermat.

3. Constructions des polygones en pratique

Conformément à ce que nous avons expliqué, il est facile de doubler le nombre d'un côté d'un polygone déjà construit. Si l'on a construit les polygones à n côtés et à m côtés avec n et $m$premier entre eux, on peut également construire le polygone à nm côtés en utilisant une relation de Bézout. D'après le Théorème de Gauß (Théorème 23), il reste donc à s'intéresser au cas des nombres premiers de Fermat. Le cas $n = 3$ correspond au triangle équilatéral qui se construit facilement à la règle et au compas. On traitera les cas $n = 5$ et $n = 17$.

a. Construction du pentagone

Proposition 24

$$\cos\left(\frac{2\pi}{5}\right) = \frac{\sqrt{5}-1}{4}$$

Démonstration. Soit $\omega = e^{\frac{2i\pi}{5}}$
On a $1 + \omega + \omega^2 + \omega^3 + \omega^4 = 0$.
Or, $\omega^4 = \overline{\omega}$ et $\omega^3 = \overline{\omega^2}$ Ainsi, en utilisant la formule $z + \overline{z} = 2\mathrm{Re}(z)$, on obtient :
$1 + 2\cos\left(\frac{2\pi}{5}\right) + 2\cos\left(\frac{4\pi}{5}\right) = 0$.
Or, $\cos\left(\frac{4\pi}{5}\right) = 2\cos^2\left(\frac{2\pi}{5}\right) - 1$ donc on obtient l'égalité suivante :

$$1 + 2\cos\left(\frac{2\pi}{5}\right) + 2\left(2\cos^2\left(\frac{2\pi}{5}\right) - 1\right) = 0.$$

et il en résulte que $\cos\left(\frac{2\pi}{5}\right)$ est solution de l'équation :

$$4X^2 + 2X - 1 = 0$$

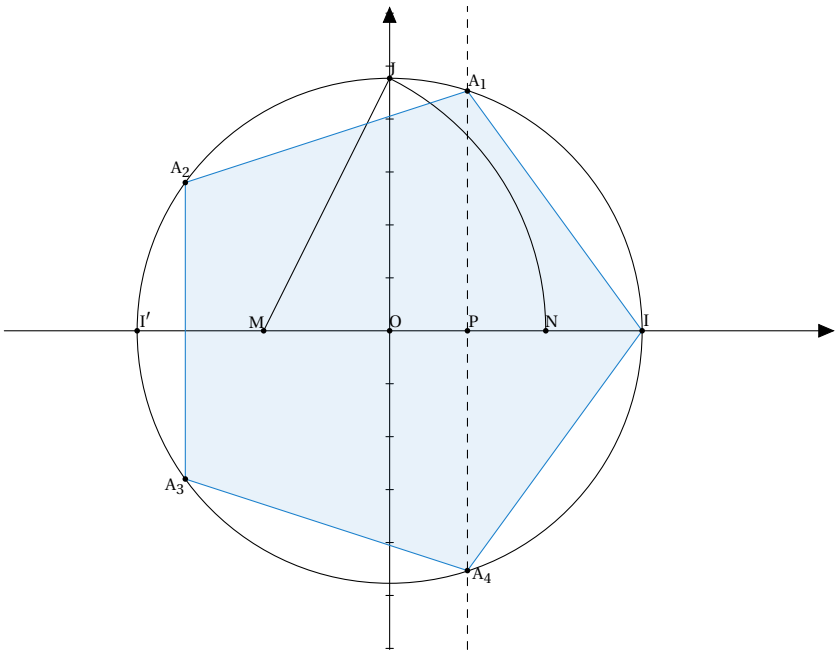
La valeur de $\cos\left(\frac{2\pi}{5}\right)$ est alors obtenue comme la solution positive de cette équation du second degré.

Proposition 25

Pour construire un pentagone inscrit dans un cercle, on construit successivement comme sur le dessin :

- le point M, milieu de [OI′]
- le point N au compas tel que MJ = MN
- le point P milieu de ON
- le point A_1, intersection du cercle et de la perpendiculaire à (OI) passant par P.

Le point A_1 est alors un des points du pentagone de côté (A_1I).



b. Construction de l'héptadécagone

Pour construire un polygone à 17 côtés, on peut se servir de la formule suivante :

Proposition 26

$$\cos\left(\frac{2\pi}{17}\right) = \frac{1}{16}\left[-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+\sqrt{68+12\sqrt{17}+2(-1+\sqrt{17})\sqrt{34-2\sqrt{17}}-16\sqrt{34+2\sqrt{17}}}\right]$$

Démonstration. Pour déterminer $\cos\left(\frac{2\pi}{17}\right)$ il faut rassembler les racines de l'unité comme nous l'avons fait dans le cas du pentagone. Nous allons justement voir comment les regrouper.
On note $\omega = e^{\frac{2i\pi}{17}}$. Comme $\Phi_{17} = 1+X+X^2+\ldots+X^{16}$ est de degré 16, $\mathbb{Q}(\omega)$ est de degré 16 sur $\mathbb{Q}$.
La preuve du Théorème 18 indique que la suite d'extensions quadratiques (K_i) entre $\mathbb{Q}$ et $\mathbb{Q}(\omega)$ qu'il est possible de construire (car le polygone est constructible) est en bijection avec une suite de sous-groupes du groupe de Galois $Gal(\mathbb{Q}(\omega)|\mathbb{Q})$. Or, ce groupe est cyclique, isomorphe à $(\mathbb{Z}/17\mathbb{Z})^*$. L'isomorphisme en question est simplement

$$\left\{\begin{array}{ccc}(\mathbb{Z}/17\mathbb{Z})^* & \longrightarrow & Gal(\mathbb{Q}(\omega)|\mathbb{Q}) \\ k & \longmapsto & \sigma_k \text{ tel que } \sigma_k(\omega)=\omega^k\end{array}\right.$$

Cela indique que pour trouver la suite d'extension de corps (K_i) et savoir comment rassembler les racines, il faut connaitre les sous-groupes de $(\mathbb{Z}/17\mathbb{Z})^*$. Or, 3 est un générateur de $(\mathbb{Z}/17\mathbb{Z})^*$. On le vérifie facilement grace au tableau suivant :

$\alpha\, mod(17)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$3^\alpha\, mod(17)$	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

Autrement dit, σ_3 est un générateur de $Gal(\mathbb{Q}(\omega)|\mathbb{Q})$. Avec $G_1 =< (\sigma_3)^2 >$, G_1 est un sous groupe d'indice 2 de $(\mathbb{Z}/17\mathbb{Z})^*$ et l'ensemble des invariants de G_1 est donc une extension de degré 2 sur $\mathbb{Q}$.
Par conséquent, la somme obtenue en regroupant un terme sur 2 $(\omega + \omega^9 + \omega^{13} + \omega^{15} + \omega^{16} + \omega^8 + \omega^4 + \omega^2)$ qui est invariante par tout élément de G_1 (car invariante par $(\sigma_3)^2$) sera dans cette extension de degré 2 sur $\mathbb{Q}$ et sera donc constructible. On itère ensuite le procédé.

Plus précisément, on pose :

$$u_1 = \omega + \omega^9 + \omega^{13} + \omega^{15} + \omega^{16} + \omega^8 + \omega^4 + \omega^2$$

$$u_2 = \omega^3 + \omega^{10} + \omega^5 + \omega^{11} + \omega^{14} + \omega^7 + \omega^{12} + \omega^6$$

Ensuite, afin d'obtenir de nouveau une extension de degré 2, on prend un terme sur deux dans chaque somme. On pose ainsi,

$$v_1 = \omega_1 + \omega_{13} + \omega_{16} + \omega_4$$

$$v_2 = \omega_9 + \omega_{15} + \omega_8 + \omega_2$$

$$v_3 = \omega_3 + \omega_5 + \omega_{14} + \omega_{12}$$

$$v_4 = \omega_{10} + \omega_{11} + \omega_7 + \omega_6$$

Pour tout k, $\omega_{17-k} = \overline{\omega_k}$ donc $\omega_k + \omega_{17-k} = 2\cos\left(\dfrac{2k\pi}{17}\right)$.
On a donc, en posant $\theta = \dfrac{2\pi}{17}$:

$$u_1 = 2(\cos(\theta) + \cos(2\theta) + \cos(4\theta) + \cos(8\theta))$$
$$u_2 = 2(\cos(3\theta) + \cos(5\theta) + \cos(6\theta) + \cos(7\theta))$$
$$v_1 = 2(\cos(\theta) + \cos(4\theta))$$
$$v_2 = 2(\cos(2\theta) + \cos(8\theta))$$
$$v_3 = 2(\cos(3\theta) + \cos(5\theta))$$
$$v_4 = 2(\cos(6\theta) + \cos(7\theta))$$

On pose enfin

$$w_1 = 2\cos(\theta)$$
$$w_2 = 2\cos(4\theta)$$

(les autres valeurs des cosinus ne seront pas utiles).

Nous allons maintenant déterminer u_1 et u_2 afin de déterminer ensuite les valeurs des v_i puis en déduire la valeur de $w_1 = 2\cos\left(\dfrac{2\pi}{17}\right)$.
$u_1 + u_2$ est la somme des 16 racines donc $u_1 + u_2 = -1$. Par ailleurs, en effectuant le produit $u_1 u_2$ et en utilisant le fait que $2\cos(a)\cos(b) = \cos(a+b) + \cos(a-b)$, on montre que

$$u_1 u_2 = 8(\cos(4\theta) + \cos(2\theta) + \cos(6\theta) + \cos(7\theta) + \cos(5\theta) + \cos(8\theta) + \cos(\theta) + \cos(3\theta))$$

Ainsi, on a $u_1 u_2 = 4(u_1 + u_2)$ et donc $u_1 u_2 = -4$.
Finalement, u_1 et u_2 sont solutions du système $\begin{cases} u_1 + u_2 = -1 \\ u_1 u_2 = -4 \end{cases}$ et sont donc racines du polynôme

$$X^2 + X - 4.$$

(On retrouve bien le fait que u_1 et u_2 sont dans une extension quadratique de $\mathbb{Q}$). Ainsi, étant donné que $u_1 > u_2$ (car $u_1 > 0$), on a :

$$u_1 = \frac{-1+\sqrt{17}}{2} \qquad \text{et} \qquad u_2 = \frac{-1-\sqrt{17}}{2}$$

On calcule ensuite les v_i de la même manière. On sait que $v_1 + v_2 = u_1$.
De plus, on montre, comme précédemment, que $v_1 v_2 = -1$. Ainsi, v_1 et v_2 sont racines du polynôme

$$X^2 - u_1 X - 1.$$

Comme $v_2 < v_1$ (la fonction cosinus est décroissante sur $[0,\pi]$), on a :

$$v_1 = \frac{u_1 + \sqrt{u_1^2+4}}{2} = \frac{-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}}{4} \qquad \text{et} \qquad v_2 = \frac{u_1 - \sqrt{u_1^2+4}}{2} = \frac{-1+\sqrt{17}-\sqrt{34-2\sqrt{17}}}{4}$$

On obtient de la même manière les valeurs de v_3 et v_4 :

$$v_3 = \frac{u_2 + \sqrt{u_2^2+4}}{2} = \frac{-1-\sqrt{17}+\sqrt{34+2\sqrt{17}}}{4} \qquad \text{et} \qquad v_4 = \frac{u_2 - \sqrt{u_2^2+4}}{2} = \frac{-1-\sqrt{17}-\sqrt{34+2\sqrt{17}}}{4}$$

Enfin, $w_1 + w_2 = v_1$ et on montre que $w_1 w_2 = v_3$. Les réels w_1 et w_2 sont donc racines du polynôme

$$X^2 - v_1 X + v_3.$$

Cela nous donne

$$w_1 = 2\cos\left(\frac{2\pi}{17}\right) = \frac{v_1 + \sqrt{v_1^2 - 4v_3}}{2},$$

ce qui conduit, après calculs, à la formule souhaitée :

$$\cos\left(\frac{2\pi}{17}\right) = \frac{1}{16}\left[-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+\sqrt{68+12\sqrt{17}+2(-1+\sqrt{17})\sqrt{34-2\sqrt{17}}-16\sqrt{34+2\sqrt{17}}}\right]$$

4. Nombre de polyèdres constructibles

En pratique, on ne connait que 5 nombres premiers de Fermat (pour $k \in \{0,1,2,3,4\}$) :

$$p_0 = 3,\ p_1 = 5\ p_2 = 17,\ p_3 = 257\ p_4 = 65537.$$

Au delà, on n'a pas trouvé de nombre premier de la forme $2^{2^k}+1$ même si la question de savoir s'il y en a d'autres reste un problème ouvert. Nous allons admettre la conjecture selon laquelle p_0, p_1, p_2, p_3 et p_4 sont les seuls nombres premiers de Fermat afin d'estimer le nombre asymptotique de polyèdres constructibles et dont le nombre de côtés est inférieur ou égal à un entier N donné.

Sous cette hypothèse, l'algorithme ci-dessous établit la liste de tous les polyèdres constructibles dont le nombre de côtés est inférieur ou égal à un entier N. Pour N = 100, on obtient la liste suivante :

$$[2,3,4,5,6,8,10,12,15,16,17,20,24,30,32,34,40,48,51,60,64,68,80,85,96]$$

```
#La liste FermatProd contient la liste de tous les produits de nombres de
    Fermat
FermatProd=[]
for k in range(2):
    for l in range(2):
        for m in range(2):
            for n in range(2):
                for o in range(2):

    FermatProd.append((3**k)*(5**l)*(17**m)*(257**n)*(65537**o))


def polyedres(n):
    #Etabli la liste des polyedres constructibles a k cotes (k<=n)
    Liste_polyedres=[]
    for k in FermatProd:
        while k<=n:
            Liste_polyedres.append(k)
            k=2*k
    Liste_polyedres.sort()
    Liste_polyedres.remove(1)
    return Liste_polyedres
```

Proposition 27

Soit $N \in \mathbb{N}^*$. Le nombre de polyèdres constructibles dont le nombre de côtés est inférieur ou égal à N est équivalent à

$$32\log_2(N)$$

Démonstration. Supposons que n est suffisament grand (supérieur au produit $P = p_0 p_1 p_2 p_3 p_4$).
Soit $k \in \{1,2,3,4,5\}$, on va dénombrer l'ensemble des entiers de la forme $2^\alpha p_{i_1} \dots p_{i_k}$ inféieurs ou égaux à 2^n (k est le nombre de nombres premiers de Fermat apparaissant dans la décomposition). Pour tout k-uplet $(i_1, \dots, i_k)$ on pose $l_{i_1,\dots,i_k}$ le plus petit entier l tel que $p_{i_1} \dots p_{i_k} \leqslant 2^l$. Ainsi, pour un k-uplet fixé $(i_1, \dots, i_k)$, le nombre de valeurs de α telles que $2^\alpha p_{i_1} \dots p_{i_k} \leqslant n$ est

$$n - l_{i_1,\dots,i_k}$$

Au total, le nombre d'entiers de la forme $2^\alpha p_{i_1} \dots p_{i_k}$ inférieurs ou égaux à $2n$ est :

$$\sum_{0 \leqslant i_1 < \dots < i_k \leqslant 4} n - l_{i_1,\dots,i_k} = \binom{5}{k} n + o(n)$$

car tous les $l_{i_1,\dots i_k}$ sont bornés. Finalement, en sommant tous les cas possibles pour $1 \leqslant k \leqslant 5$, on voit que le nombre de polyèdres constructibles et dont le nombre de côtés est inférieur ou égal à 2^n est

$$\sum_{k=1}^{5} \binom{5}{k} n + o(n) = 2^5 n + o(n)$$

Avec $N = 2^n$, on voit que le nombre cherché est bien $32\log_2(N)$.

Remarque
Pour $N = 2^{10\,000}$, l'algorithme Python ci-dessus indique qu'il y a 319 504 polyèdres constructibles dont le nombre de côtés est inférieur ou égal à N, ce qui est à rapproché de l'équivalent donné : $32\log_2(N) = 320\,000$