Construction des polygones réguliers

Introduction : la question de savoir quelles sont les figures ou les nombres constructibles à la règle et au compas est un point central des mathématiques depuis l'Antiquité grecque, et même avant. C'est même en un sens le problème fondateur. Il a fallu environ vingt siècles avant que ne soient réalisés des progrès significatifs dans ce domaine, grâce à des travaux de Gauss notamment. Pour une histoire plus complète de la genèse de la géométrie, voir par exemple G. Godefroy, L'aventure des nombres ([1]).

Pourquoi la règle et le compas ? Probablement parce que, bien qu'approximatifs, ce sont des instruments à la fois simples et assez précis. Il est en effet plus difficile de construire une équerre aussi précise, par exemple, sans parler des trace-ellipses et autres instruments encore plus fantaisistes. Il se peut aussi que la préférence de Platon pour ces deux instruments ait été motivée par bien d'autres raisons, d'ordre philosophique.

Dès lors, une des questions les plus simples à formuler dans ce domaine est la suivante : quels sont les polygones réguliers constructibles à la règle et au compas ? C'est d'ailleurs le quatrième grand problème qu'ont laissé derrière elles les écoles de mathématiciens grecs, avec les problèmes de quadrature du cercle, de duplication du cube, ou de trisection de l'angle. C'est de ce problème que nous allons parler ici.

Afin de clarifier le problème, donnons tout de suite la :

Définition (Polygone régulier) Dans toute la suite, on appellera polygone régulier à n côtés (n un entier) le polygone à n cotés de même longueur, et dont les sommets sont situés sur le cercle unité, le premier sommet étant pris sur l'axe des abscisses.

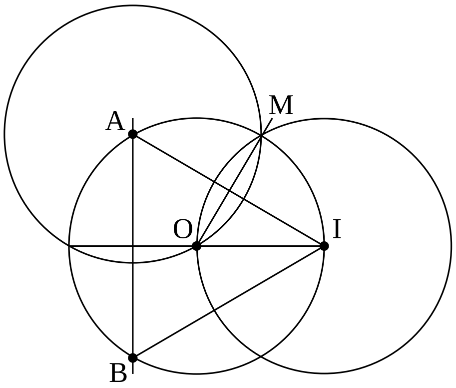
Cette définition peut sembler restrictive, cependant il est assez aisé de voir que l'on peut déduire ce polygone de n'importe quel polygone du plan ayant n côtés égaux (non nécessairement centrés à l'origine, et quelle que soit la loongueur du côté), et ce par une construction géométrique élémentaire. Pour ce faire, on peut construire le "même" polygone centré en l'origine, et ayant son premier sommet sur l'axe des abscisses (tracer un cercle de même rayon que son cercle circonscrit, puis reporter la longueur du côté sur le cercle). Puis, il suffit de faire une homothétie pour ramener les sommets sur le cercle unité (les sommets sont construit comme intersections du cercle unité avec les demi-droites d'origine O et passant par les sommets du polygone précédent).

1 Les polygones constructibles

Savoir construire un polygone régulier, à n côtés, c'est essentiellement savoir construire le point de coordonnées $\left(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n}\right)$. Ayant ainsi construit un côté de ce polygone, il suffit alors de reporter de proche en proche sa longueur sur le cercle unité.

Le cas n pair n'est pas très intéressant, puisque l'on sait construire la bissectrice d'un angle, et donc passer aisément du polygone régulier à $n/2$ côtés au polygone régulier à n côtés (le passage inverse est encore plus simple, il suffit de prendre un sommet sur deux).

Exemple Pour passer du triangle équilatéral IAB à l'hexagone régulier, on construit comme dans la figure suivante le point M (entre I et A) comme l'intersection du cercle unité avec la bissectrice de l'angle $\widehat{\mathrm{IOA}}$. Cette bissectrice est aussi la médiatrice du segment [IA], c'est comme telle qu'on l'a construite (c'est la méthode générique utilisée pour construire la bissectrice d'un angle).



1.1 Réduction du problème

D'ailleurs, on peut raffiner la remarque précédente grâce au résultat suivant :

Théorème 1.1 (Gauss) *Soit n et m sont deux entiers naturels premiers entre eux. Le polygone à nm côtés est constructible à la règle et au compas si et seulement si les polygones à n côtés et à m côtés sont constructibles.*

Démonstration En effet, le théorème de Bezout nous permet de dire que, si m et n sont premiers entre eux, il existe deux entiers relatifs u et v tels que $um + vn = 1$. Multipliant l'expression par $\frac{2\pi}{mn}$, il vient :

$$u\frac{2\pi}{n} + v\frac{2\pi}{m} = \frac{2\pi}{mn}$$

C'est-à-dire que l'on obtient l'angle $2\pi/mn$, sur le cercle unité, en reportant u fois l'angle $2\pi/n$ et v fois l'angle $2\pi/m$, angles déjà construits.

Réciproquement, on a bien sûr immédiatement les polygones à m ou à n côtés à partir du polygone à mn côtés. Il suffit pour cela de ne conserver que les sommets voulus !

$\square$

A la lumière de ce résultat, seule la construction des polygones à p^α côtés, avec p premier, reste intéressante : si l'on décompose un entier n en produit de facteurs premier $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, construire le polygone régulier à n côtés revient à construire les polygones à respectivement $p_1^{\alpha_1}, \dots, p_r^{\alpha_r}$ côtés.

1.2 Le théorème de Gauss

Théorème 1.2 *(Gauss)*

Soit p un nombre premier supérieur ou égal à 3, α un entier. Alors le polygone régulier à p^α côtés est constructible si et seulement si $\alpha = 1$ et p est un nombre de Fermat, i.e. *p est de la forme $2^{2^\beta} + 1$, avec β un entier.*

La démonstration de ce théorème étant un peu technique, nous la mettons en annexe. Nous pouvons désormais énoncer le critère le plus général de constructibilité des polygones réguliers :

Théorème 1.3 *Soit n un entier.*

Le polygone régulier à n côtés est constructible à la règle et au compas si et seulement si l'entier n a une décomposition en facteurs premiers de la forme :

$$n = 2^m \mathrm{F}_1 \dots \mathrm{F}_r$$

où les F_i sont des nombres premiers de Fermat deux à deux distincts.

Démonstration Si le polygone régulier à n côtés est constructible à la règle et au compas, alors il en est de même pour tous les polygones réguliers à d côtés, avec d un diviseur de n.

En particulier, si la décomposition en facteurs premiers de n est de la forme $p_1^{\alpha_1} \dots p_k^{\alpha_k}$, avec les p_i deux à deux distincts, alors les polygones réguliers à $p_i^{\alpha_i}$ côtés doivent être constructibles.

Mais en vertu du théorème de Gauss, si $p_i \geq 3$, alors $\alpha_i = 1$ et p_i est un nombre de Fermat (si $p_i = 2$, il n'y a pas de restriction à apporter sur α_i).

Donc n a bien la décomposition annoncée.

Réciproquement, si n est un entier qui s'écrit sous la forme d'un produit $2^m \mathrm{F}_1 \dots \mathrm{F}_r$, où les F_i sont des nombres premiers de Fermat deux à deux distincts, alors les polygones réguliers à F_i côtés sont constructibles par le théorème de Gauss, et en appliquant $r-1$ fois le théorème 1.1, on obtient une construction du polygone à $\mathrm{F}_1 \dots \mathrm{F}_r$. Le facteur 2^m ne pose ensuite aucun problème : il suffit en pratique de faire m bissectrices successives.

□

N.B. On ne connaît qu'assez peu de nombres premiers de Fermat. Pour l'instant, seuls $\mathrm{F}_0, \mathrm{F}_1, \mathrm{F}_2, \mathrm{F}_3$ et F_4 sont connus.

$$\mathrm{F}_0 = 2^{2^0} + 1 = 3, \qquad \mathrm{F}_1 = 2^{2^1} + 1 = 5, \qquad \mathrm{F}_2 = 2^{2^2} + 1 = 17,$$
$$\mathrm{F}_3 = 2^{2^3} + 1 = 257 \quad \mathrm{F}_4 = 2^{2^4} + 1 = 65537$$

En revanche, $\mathrm{F}_5 = 4294967297 = 641 \times 6700417$ n'est pas premier.

Le nombre de polygones réguliers constructibles à la règle et au compas est donc très restreint : sauf à trouver de nouveaux nombres de Fermat premiers (mais de toutes façon il ne peut y en avoir beaucoup, au sens ou la suite $(\mathrm{F}_n)_{n \in \mathbb{N}}$

croît très rapidement), il n'y a que $2^5 = 32$ possibilités pour le produit $\mathrm{F}_1 \ldots \mathrm{F}_r$ du théorème précédent.

C'est-à-dire que tous les polygones réguliers constructibles connus peuvent être répartis dans 32 classes correspondant à 32 polygones "élémentaires", les autres étant obtenus par divisions sucessives des angles par 2.

La construction du polygone régulier à 17 côtés fût l'un des tous premiers résultats de Gauss. On pourra en trouver une esquisse en annexe de ce texte, ainsi qu'une explication assez complète dans [2].

Corollaire 1.4 *La trisection de l'angle n'est pas réalisable à partir des seuls règles et compas.*

En effet, le polygone régulier à 9 côtés n'est pas constructible à la règle et au compas. c'est-à-dire que l'on ne sait pas construire l'angle $\dfrac{2\pi}{9}$.

Or si l'on savait trisecter un angle, il nous suffirait de trisecter l'angle $\dfrac{2\pi}{3}$, qui lui est bien sûr constructible, pour obtenir l'angle $\dfrac{2\pi}{9}$ désiré.

Par contraposée, on conclut qu'il n'y a pas de méthode systématique pour trisecter un angle à la règle et au compas.

□

1.3 De la théorie à la pratique

Nous savons que le pentagone est constructible à la règle et au compas $(5 = 2^{2^1} + 1)$. Il s'agit maintenant d'en trouver une construction effective. c'est-à-dire de trouver une construction de $\cos \dfrac{2\pi}{5}$.

Or $\cos \dfrac{2\pi}{5}$ est racine du polynôme $4\mathrm{X}^2 + 2\mathrm{X} - 1$. Considérons pour cela l'équation $\mathrm{X}^5 = 1$. Dans $\mathbb{C}$, ses racines sont les $e^{\frac{2ik\pi}{5}}$ $(1 \leq k \leq 5)$, de somme nulle. (Ce sont les affixes des sommet du pentagone régulier). En prenant leurs parties réelles, on obtient l'égalité :

$$\cos \frac{2\pi}{5} + \cos \frac{4\pi}{5} + \cos \frac{6\pi}{5} + \cos \frac{8\pi}{5} + 1 = 0$$

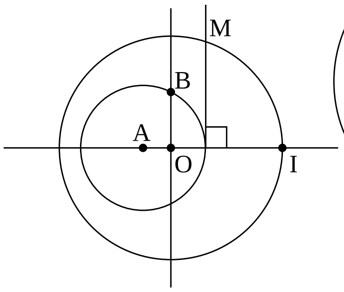
Par symétrie par rapport à l'axe réel, on trouve les relations $\cos \dfrac{8\pi}{5} = \cos \dfrac{2\pi}{5}$ et $\cos \dfrac{6\pi}{5} = \cos \dfrac{4\pi}{5} = 2\cos^2 \dfrac{2\pi}{5} - 1$ (on utilise ici la relation $\cos 2x = 2\cos^2 x - 1$). En remplaçant tout ceci dans l'égalité précédente, on obtient bien :

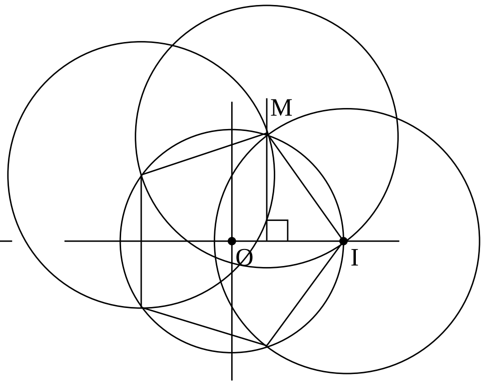
$$4\cos^2 \frac{2\pi}{5} + 2\cos \frac{2\pi}{5} - 1 = 0$$

Les racines de ce polynôme sont $\dfrac{-1+\sqrt{5}}{4}$ et $\dfrac{-1-\sqrt{5}}{4}$. Comme $0 \leq \dfrac{2\pi}{5} \leq \dfrac{\pi}{2}$, on sait que $\cos \dfrac{2\pi}{5}$ est positif. Donc

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

Or, on peut construire la longueur $\frac{\sqrt{5}}{4}$ comme l'hypothénuse d'un triangle rectangle de côtés $\frac{1}{2}$ et $\frac{1}{4}$. d'où la construction suivante :

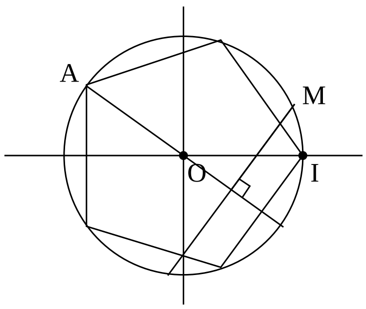




Les points A $\left(-\frac{1}{4}, 0\right)$ et B $\left(0, \frac{1}{2}\right)$ s'obtiennent bien sur de façon élémentaire à partir des point O et I (on fait pour cela deux médiatrices). Il suffit ensuite de tracer le cercle de centre A passant par B. Le théorème de Pythagore nous dit qu'il est de rayon $\frac{\sqrt{5}}{4}$. Son intersection avec l'axe des abscisses est donc le point de coordonnées $\left(\frac{-1+\sqrt{5}}{4}, 0\right) = \left(\cos\frac{2\pi}{5}, 0\right)$.

On obtient bien le deuxième sommet M du pentagone régulier comme l'intersection de la droite perpendiculaire à l'axe des abscisses en ce point et du cercle unité. Pour obtenir les sommet suivants, il suffit de reporter la longueur IM sur le cercle unité.

Appliquant le théorème 1.1, ou plutôt le principe de sa démonstration, on en déduit une construction du polygone régulier à 15 côtés : $3 \cdot 2 - 5 = 1$ donc $\frac{2\pi}{15} = 2 \cdot \frac{2\pi}{5} - \frac{2\pi}{3}$.



Partant du point A, définit par l'angle $\frac{4\pi}{5}$, on obtient le premier sommet M du polygone régulier à 15 côtés en construisant un angle de $\frac{2\pi}{3}$ dans le sens horaire.

2 Recherche de polynômes minimaux

Pour ce qui est des "petits" entiers, on peut s'en sortir "à la main", c'est-à-dire sans le théorème de Gauss qui est un résultat plus difficile. Il s'agit ici de trouver les polynômes minimaux des nombres $\cos\left(\frac{2\pi}{n}\right)$, pour de petites valeurs de n.

Le polynôme minimal d'un nombre algébrique α sur un corps $\mathbb{K}$ est le polynôme à coefficients dans $\mathbb{K}$ et de degré minimal parmis tous les polynômes non nuls (à coefficients dans $\mathbb{K}$) qui annulent α. Celui-ci est toujours unique à constante multiplicative près (voir par exemple le texte "Sur les nombres constructibles" pour une étude plus complète).

La notion de polynôme minimal est fondamentale pour l'étude des problèmes de construction à la règle et au compas. En effet, pour déterminer si un nombre est ou non constructible, la connaissance de son degré, c'est-à-dire le degré de son polynôme minimal, nous donne de précieux renseignements. Rappelons à ce sujet les résultats suivants :

Théorème 2.1 *(CNS de constructibilité)*
Soit M *un point du plan. Il y a équivalence entre :*

(i) *M est constructible.*

(ii) *Il existe une suite finie croissante* $(\mathbb{K}_i)_{i\leq n}$ *de sous-corps de* $\mathbb{R}$ *telle que les coordonnées de* M *sont dans* $\mathbb{K}_n$, *la suite vérifiant :* $\mathbb{Q} = \mathbb{K}_0$, *et pour tout* i, $\mathbb{K}_{i+1}$ *est une extension quadratique de* $\mathbb{K}_i$.

Comme corollaire de ce théorème, on obtient la condition nécessaire suivante :

Théorème 2.2 *Pour qu'un nombre* α *soit constructible, il faut que son degré sur* $\mathbb{Q}$ *soit de la forme* 2^n, *où* n *est un entier.*

Pour la démonstration de ces résultats, se reporter au texte intitulé "Sur les nombres constructibles".

2.1 Une famille de polynômes

Nous allons ici étudier une suite de polynômes qui, sans être précisément les polynômes minimaux des nombres $\cos\left(\frac{2\pi}{n}\right)$, sont néanmoins des polynômes qui annulent ces nombres, *i.*e. ayant ces nombres pour racines, et donc permettent d'obtenir des renseignements sur leur degré.

Soit donc la suite de polynômes définie par :

$$\begin{cases} \mathrm{P}_0(\mathrm{X}) = 1, \quad \mathrm{P}_1(\mathrm{X}) = 2\mathrm{X}+1 \\ \forall n \in \mathbb{N}, \quad \mathrm{P}_{n+2}(\mathrm{X}) = 2\mathrm{X}\mathrm{P}_{n+1}(\mathrm{X}) - \mathrm{P}_n(\mathrm{X}) \end{cases}$$

Lemme 2.3 *Les seules racines rationnelles possibles de* P_n *sont les rationnels* $\frac{1}{2}$ *et* $-\frac{1}{2}$.

Introduisons les polynômes $\mathrm{Q}_n(\mathrm{X}) = \mathrm{P}_n\left(\frac{\mathrm{X}}{2}\right)$.

Ils vérifient $\mathrm{Q}_0(\mathrm{X}) = 1, \mathrm{Q}_1(\mathrm{X}) = \mathrm{X}+1$ et pour tout n entier,

$$\mathrm{Q}_{n+2}(\mathrm{X}) = \mathrm{X}\mathrm{Q}_{n+1}(\mathrm{X}) - \mathrm{Q}_n(\mathrm{X})$$

Par une récurrence immédiate, on sait que les polynômes Q_n sont à coefficients entiers. Le coefficient dominant de Q_n est 1 et son coefficient constant est $(-1)^{n+1}$. On peut donc écrire Q_n sous la forme $(-1)^{n+1} + \sum_{i=1}^{n-1} a_i \mathrm{X}^i + \mathrm{X}^n$, avec a_i entier pour tout i.

Soit $\frac{p}{q}$ un rationnel, écrit sous forme irréductible, racine de Q_n. On peut également supposer q positif. On a :

$$(-1)^n + \sum_{i=1}^{n-1} a_i \left(\frac{p}{q}\right)^i + \left(\frac{p}{q}\right)^n = 0$$

soit
$$q^n (-1)^n + \sum_{i=1}^{n-1} a_i p^i q^{n-i} + p^n = 0$$

Comme q divise l'expression $q^n (-1)^n + \sum_{i=1}^{n-1} a_i p^i q^{n-i}$, q divise p^n. Donc $q = 1$. De la même façon, p divise l'expression $\sum_{i=1}^{n-1} a_i p^i q^{n-i} + p^n$, donc p divise $q^n (-1)^n$, soit $p = \pm 1$.

Le rationnel $\frac{p}{q}$ est donc égal à 1 ou -1. Les racines rationnelles de $\mathrm{P}_n(\mathrm{X}) = \mathrm{Q}_n(2\mathrm{X})$, si elles existent, ne peuvent alors être que $\frac{1}{2}$ ou $-\frac{1}{2}$.

□

Lemme 2.4 *Soit θ un réel, $\theta \notin 2\pi\mathbb{Z}$.*

Pour tout n, on a $\mathrm{P}_n(\cos\theta) = \dfrac{\sin\left(n + \frac{1}{2}\right)\theta}{\sin\frac{\theta}{2}}$.

Pour $n = 0$, le résultat est évident : on a $\mathrm{P}_0(\cos\theta) = 1 = \dfrac{\sin\frac{1}{2}\theta}{\sin\frac{\theta}{2}}$.

Pour $n = 1$, on a $\mathrm{P}_n(\cos\theta) = 2\cos\theta + 1$. Or $\sin\frac{3}{2}\theta = \sin\theta\cos\frac{\theta}{2} + \sin\frac{\theta}{2}\cos\theta$, donc $\dfrac{\sin\frac{3}{2}\theta}{\sin\frac{\theta}{2}} = 2\left(\cos\frac{\theta}{2}\right)^2 + \cos\theta = 2\cos\theta + 1$. La relation annoncée en découle.

Supposons le résultat établi jusqu'à l'ordre $n+1$. La relation trigonométrique $\sin a + \sin b = 2\sin\frac{a+b}{2}\cos\frac{a-b}{2}$, appliquée aux deux réels $a = \left(n + \frac{5}{2}\right)\theta$ et $b = \left(n + \frac{1}{2}\right)\theta$ nous donne :

$$\sin\left(n + \frac{5}{2}\right)\theta = 2\sin\left(n + \frac{3}{2}\right)\theta\cos\theta - \sin\left(n + \frac{1}{2}\right)\theta$$

donc $$\frac{\sin\left(n+\frac{5}{2}\right)\theta}{\sin\frac{\theta}{2}} = 2\cos\theta\frac{\sin\left(n+\frac{3}{2}\right)\theta}{\sin\frac{\theta}{2}} - \frac{\sin\left(n+\frac{1}{2}\right)\theta}{\sin\frac{\theta}{2}}$$

Soit, en utilisant l'hypothèse de récurrence :

$$\frac{\sin\left(n+\frac{5}{2}\right)\theta}{\sin\frac{\theta}{2}} = 2\cos\theta \mathrm{P}_{n+1}(\cos\theta) - \mathrm{P}_n(\cos\theta) = \mathrm{P}_{n+2}(\cos\theta)$$

Le résultat est donc établi par récurrence.

□

Du lemme précédent, on tire immédiatement les racines du polynôme P_n :

$$\begin{aligned} \mathrm{P}_n(\cos\theta) = 0 &\iff \frac{\sin\left(n+\frac{1}{2}\right)\theta}{\sin\frac{\theta}{2}} = 0 \\ &\iff \begin{cases} \sin\left(n+\frac{1}{2}\right)\theta = 0 \\ \sin\frac{\theta}{2} \neq 0 \end{cases} \end{aligned}$$

Les solutions d'un tel système sont ici les valeurs de la forme $\frac{2k\pi}{2n+1}$, où k est un entier non multiple de $2n+1$. Ce qui nous donne n racines du polynôme P_n, à savoir

$$\{\cos\frac{2k\pi}{2n+1}, \quad 1 \leq k \leq n\}$$

2.2 Des polygones constructibles ou non

Soit $n = 2k+1$ un entier impair. D'après ce qui précède, $\cos\frac{2\pi}{n}$ est racine du polynome P_k. Nous allons étudier le cas de quelques valeurs de k.

- Pour $k = 2$, soit $n = 5$, $\mathrm{P}_2(\mathrm{X})$ est le polynôme

  $$2\mathrm{XP}_1(\mathrm{X}) - \mathrm{P}_0(\mathrm{X}) = 4\mathrm{X}^2 + 2\mathrm{X} - 1$$

  C'est un polynôme de degré 2. Or le théorème 2.2 nous permet d'affirmer que tout élément d'une extension quadratique de $\mathbb{Q}$ est constructible. Nous retrouvons ainsi la construction à la règle et au compas du pentagone régulier.

- Pour $k = 3$, soit $n = 7$, $\mathrm{P}_3(\mathrm{X})$ est le polynôme

  $$2\mathrm{XP}_2(\mathrm{X}) - \mathrm{P}_1(\mathrm{X}) = 8\mathrm{X}^3 + 4\mathrm{X}^2 - 4\mathrm{X} - 1$$

  Nous avons vu que ses seules racines rationnelles possibles sont $\frac{1}{2}$ et $-\frac{1}{2}$. Or ni l'une ni l'autre n'est racine, donc le polynôme P_3 n'a pas de racine dans $\mathbb{Q}$. Comme il est de degré 3, il est irréductible sur $\mathbb{Q}$ (sinon, il y aurait nécessairement un facteur de degré 1 dans sa décomposition, donc une racine rationnelle).

$P_3(X)$ est donc le polynôme minimal de $\cos\dfrac{2\pi}{7}$, de degré 3. Le réel $\cos\dfrac{2\pi}{7}$ n'est donc pas constructible, d'après le théorème 2.2. L'heptagone régulier n'est donc pas constructible à la règle et au compas.

- Pour $k = 4$, soit $n = 9$, le polynôme $P_4(X)$ est alors

$$2XP_3(X) - P_2(X) = 16X^4 + 8X^3 - 12X^2 - 4X + 1$$

On s'aperçoit que $P_4\left(\dfrac{-1}{2}\right) = 0$. (En effet $-\dfrac{1}{2} = \cos\dfrac{6\pi}{9}$).

Et alors $$P_4(X) = (2X+1)\left(8X^3 - 6X + 1\right)$$

et donc $\cos\dfrac{2\pi}{9}$ est racine du polynôme $8X^3 - 6X + 1$. Cette fois ni $\dfrac{1}{2}$ ni $-\dfrac{1}{2}$ n'est racine de ce polynôme, donc il est irréductible sur $\mathbb{Q}$, car de degré 3. Aussi le réel $\cos\dfrac{2\pi}{9}$ est de degré 3 sur $\mathbb{Q}$, et le polygone régulier à 9 côtés n'est pas constructible à la règle et au compas.

Au passage, nous obtenons une fois de plus le corollaire 1.4, sans passer par le théorème de Gauss.

Annexe : Démonstration du théorème de Gauss

Théorème (Gauss)

Soit p un nombre premier supérieur ou égal à 3, α un entier. Alors le polygone régulier à p^α côtés est constructible si et seulement si $\alpha = 1$ et p est un nombre de Fermat, i.e. p est de la forme $2^{2^\beta} + 1$, avec β un entier.

Démonstration L'un des sens de l'équivalence est plus facile que l'autre : si p est un nombre premier supérieur ou égal à 3, α un entier, et le polygone régulier à p^α côtés est constructible alors $\alpha = 1$ et p est un nombre de Fermat.

Soit en effet un tel couple d'entiers (p, α). Le réel $\cos\dfrac{2\pi}{p^\alpha}$ est constructible, donc son degré sur $\mathbb{Q}$ est une puissance de 2 en vertu du théorème 2.2. Soit m l'entier tel que $[\mathbb{Q}\left(\cos\dfrac{2\pi}{p^\alpha}\right) : \mathbb{Q}] = 2^m$.

D'autre part, le complexe $\omega = e^{\frac{2i\pi}{p^\alpha}}$ est racine de $X^2 - 2\cos\dfrac{2\pi}{p^\alpha}X + 1$, donc de degré 2 sur $\mathbb{Q}\left(\cos\dfrac{2\pi}{p^\alpha}\right)$. Soit $[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\dfrac{2\pi}{p^\alpha}\right)] = 2$ et donc $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2 \times 2^m = 2^{m+1}$.

Or ω est une racine primitive p^α-ième de l'unité, son polynôme minimal sur $\mathbb{Q}$ est donc le p^α-ième polynôme cyclotomique $\mu_{p^\alpha}(X)$, qui est de degré $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ où φ est l'indicatrice d'Euler. (pour la démonstration de l'irréductibilité sur $\mathbb{Q}$ des polynômes cyclotomiques, voir par exemple [3]).

On obtient donc l'équation à variables entières

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

De cela, on tire immédiatement $\alpha = 1$. En effet, on aurait sinon $\alpha - 1 \geq 1$, et donc p diviserait 2^{m+1}, ce qui est absurde puisque p est un nombre premier supérieur ou égal à 3. On obtient alors $p = 1 + 2^{m+1}$.

Écrivons ensuite $m+1$ sous la forme $2^\beta \times \lambda$, où λ est un entier impair (β est la plus grande puissance de 2 qui divise $m+1$). Supposons donc que $m+1$ n'est pas une puissance de 2, c'est-à-dire que $\lambda \geq 3$.

Alors
$$\begin{aligned} p &= 1 + \left(2^{2^\beta}\right)^\lambda \\ &= \left(1 + 2^{2^\beta}\right)\left(1 - 2^{2^\beta} + \left(2^{2^\beta}\right)^2 - \ldots + \left(2^{2^\beta}\right)^{\lambda-1}\right) \end{aligned}$$

p admet alors un diviseur strict $1 + 2^{2^\beta}$, ce qui est absurde puisque p est premier. En conclusion, $m+1$ s'écrit sous la forme 2^β, et donc p est bien un nombre de Fermat.

La réciproque est de moindre importance, attendu que les seuls nombres premiers de Fermat connus sont $\mathrm{F}_0, \mathrm{F}_1, \mathrm{F}_2, \mathrm{F}_3$ et F_4. Comme $\mathrm{F}_0 = 3$ et $\mathrm{F}_1 = 5$ sont des cas déjà résolus, il suffirait en un sens de donner des constructions des polygones réguliers à $\mathrm{F}_2 = 17, \mathrm{F}_3 = 257$ et $\mathrm{F}_4 = 65537$ côtés... Ceci est cependant manifestement assez fastidieux au moins pour ce qui est de F_3 et F_4 ! En fait, la construction du polygone régulier à 17 côtés, découverte par Gauss, découle assez directement de la preuve de ce théorème, qui utilise des idées de théorie de Galois.

Nous allons montrer que si p est un nombre premier de la forme $2^n + 1$, alors le polygone régulier à p côtés est constructible. Et d'après ce qui précède, un nombre premier de la forme $2^n + 1$ est nécessairement un nombre de Fermat.

Soit $p = 2^n + 1$ un nombre premier. Soit $\omega = e^{\frac{2i\pi}{p}}$, racine primitive p-ième de l'unité, et affixe du second sommet du polygone régulier à p côtés.

Alors ω a pour polynôme minimal sur $\mathbb{Q}$ le p-ième polynôme cyclotomique $\mu_p(\mathrm{X}) = \mathrm{X}^{p-1} + \mathrm{X}^{p-2} + \ldots + 1$. Ce polynôme est irréductible sur $\mathbb{Q}$ (parceque c'est un polynôme cyclotomique ! Plus simplement, on peut montrer que ce polynôme est irréductible sur $\mathbb{Q}$ en appliquant le critère d'Eisenstein à $\mu_p(\mathrm{X}+1)$.) Le complexe ω est donc de degré $p - 1 = 2^n$ sur $\mathbb{Q}$.

Soit $\mathbb{K}$ le corps $\mathbb{Q}(\omega)$ et G son groupe d'automorphismes sur $\mathbb{Q}$ (*i.e.* le groupe des automorphismes de corps de $\mathbb{K}$ laissant fixant tous les rationnels). Alors tout élément g de G est déterminé par l'image $g(\omega)$. En effet, connaissant $g(\omega)$, on connaît $g\left(\omega^i\right) = g(\omega)^i$ pour tout entier i. Et comme tout élément de $\mathbb{K}$ est un polynôme en ω à coefficients rationnels, g est entièrement déterminé par $g(\omega)$.

Ensuite, on doit avoir la relation $\mu_p(g(\omega)) = 0$, donc $g(\omega)$ est une puissance de ω. Réciproquement, il est immédiat de vérifier que pour tout entier k, la fonction $g_k : \omega \mapsto \omega^k$ se prolonge effectivement en un automorphisme de $\mathbb{K}$. On a donc pour groupe G, en utilisant la notation que nous venons d'introduire :

$$\mathrm{G} = \{\mathrm{Id}_{\mathbb{K}} = g_1, \ldots, g_{p-1}\}$$

G est un groupe à $p-1$ éléments, isomorphe au groupe multiplicatif des racines p-ième (primitives) de l'unité $\{\omega, \omega^2, \ldots, \omega^{p-1}\}$. Donc G est cyclique, *i.e.* engendré par un élément g.

g est désormais fixé. Soit, pour $0 \leq i \leq n$, G_i le sous-groupe de G engendré par g^{2^i}, sous groupe de cardinal 2^{n-i}. Soit également $\mathbb{K}_i$ le sous-corps de $\mathbb{K}$ fixé par tous les éléments de G_i. On a immédiatement les inclusions :

$$\mathbb{Q} \subset \mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_n = \mathbb{K}$$

Nous allons montrer que $\mathbb{Q} = \mathbb{K}_0$ et que toutes les extensions sont quadratiques, c'est-à-dire de degré 2.

$\{\omega, g(\omega), \ldots, g^{p-2}(\omega)\}$ est une famille de $p-1$ puissances distinctes de ω, c'est donc une famille libre, donc une base de $\mathbb{K}$ en tant qu'espace vectoriel sur $\mathbb{Q}$. Il en est de même pour la famille $\{g(\omega), \ldots, g^{p-1}(\omega) = \omega\}$.

Soit donc $z = \lambda_0\omega + \lambda_1 g(\omega) + \ldots + \lambda_{p-2} g^{p-2}(\omega)$ un élément de $\mathbb{K}_0$, fixé par g. En appliquant g à l'égalité précédente, on trouve :

$$z = g(z) = \lambda_0 g(\omega) + \lambda_1 g^2(\omega) + \ldots + \lambda_{p-2}\omega$$

L'écriture de z dans la base $\{\omega, \ldots, g^{p-2}(\omega)\}$ est unique, donc $\lambda_0 = \ldots = \lambda_{p-2}$.

Soit
$$\begin{aligned} z &= \lambda_0\left(\omega + g(\omega) + \ldots + g^{p-2}(\omega)\right) \\ &= \lambda_0\left(\omega + \omega^2 + \ldots + \omega^{p-1}\right) \\ &= -\lambda_0 \end{aligned}$$

C'est-à-dire que z est dans $\mathbb{Q}$, et donc $\mathbb{K}_0 = \mathbb{Q}$.

Ensuite, les extension sont strictes, en effet pour tout $i > 0$, l'élément $\sum_{k=0}^{2^{n-i}-1} g^{k2^i}(\omega)$ est dans $\mathbb{K}_i$ mais pas dans $\mathbb{K}_{i-1}$.

Les n extensions successives $\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_n = \mathbb{K}$ sont strictes, et telles que $\mathbb{K}$ est de degré 2^n sur $\mathbb{Q}$. Donc toutes les extensions sont de degré 2 (si l'une d'entre elles était de degré plus grand, le produit serait strictement plus grand que 2^n).

Pour terminer la démonstration, il ne reste plus à montrer que l'égalité $\mathbb{K}_{n-1} = \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)$. Pour cela, remarquons que la conjugaison complexe est un automorphisme de $\mathbb{K}$, donc un élément de G, d'ordre 2. Comme G est cyclique, c'est le seul élément d'ordre 2, et donc $g^{2^{n-1}}$ est la conjugaison. Or, à l'étape $n-1$, on a dans $\mathbb{K}_{n-1}$ l'élément :

$$\sum_{k=0}^{2^{n-(n-1)}-1} g^{k2^{n-1}}(\omega) = \omega + g^{2^{n-1}}(\omega)$$

c'est-à-dire $\omega + \overline{\omega} = 2\cos\left(\frac{2\pi}{p}\right) \in \mathbb{K}_{n-1}$, donc $\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) \subset \mathbb{K}_{n-1}$. Or ω est racine du polynôme $\mathrm{X}^2 - 2\cos\left(\frac{2\pi}{p}\right)\mathrm{X} + 1$, donc $[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)] = 2$.

On a bien
$$\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) = \mathbb{K}_{n-1}$$

$\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_{n-1} = \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)$ est une suite d'extensions quadratiques réelles, et donc $\cos\left(\frac{2\pi}{p}\right)$ est constructible à la règle et au compas. Le polygone régulier à p côtésest donc lui-même constructible.

□

N.B. Pour la mise en oeuvre pratique de ces idées, la seule difficulté est de trouver un générateur g du groupe G. Dans le cas $p = 17$, il est naturel d'essayer par exemple $g : \omega \mapsto \omega^2$. Malheureusement, en itérant l'élément g, on ne trouve que 8 puissances distinctes de ω, cet automorphisme est donc d'ordre 8, il n'engendre pas le groupe. En revanche, $\omega \mapsto \omega^3$ convient. En l'appliquant à ω, on trouve dans l'ordre :

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

Pour construire le polygone à 17 côtés, on commence alors par introduire les deux sommes (qui seront dans $\mathbb{K}_1$, donc constructibles) construites en prenant un terme sur deux dans la suite précédente :

$$x_1 = \omega + \omega^2 + \omega^4 + \omega^8 + \omega^9 + \omega^{13} + \omega^{15} + \omega^{16}$$

et
$$x_2 = \omega^3 + \omega^5 + \omega^6 + \omega^7 + \omega^{10} + \omega^{11} + \omega^{12} + \omega^{14}$$

Alors on calcule $x_1 + x_2 = -1$ et $x_1 x_2 = -4$. x_1 et x_2 sont donc les racines de $X^2 + X - 4$, soit respectivement $\dfrac{-1+\sqrt{17}}{2}$ et $\dfrac{-1-\sqrt{17}}{2}$ (pour les distinguer, une considération géométrique permet de voir que $x_1 > 0$ et $x_2 < 0$).

Une fois construits x_1 et x_2, on peut introduire les quatre éléments de $\mathbb{K}_2$:

$$y_1 = \omega + \omega^4 + \omega^{13} + \omega^{16}, \qquad y_2 = \omega^2 + \omega^8 + \omega^9 + \omega^{15}$$
$$y_3 = \omega^3 + \omega^5 + \omega^{12} + \omega^{14}, \quad y_4 = \omega^6 + \omega^7 + \omega^{10} + \omega^{11}$$

Ils sont solutions d'équations du second degré à coefficients dans $\mathbb{K}_1$, permettant de les construire ($y_1 + y_2 = x_1$ et $y_1 y_2 = -1$...)

Enfin, l'on introduit les sommes $z_1 = \omega + \omega^{16} = 2\cos\left(\dfrac{2\pi}{17}\right)$ et $z_2 = \omega^4 + \omega^{13}$. On trouve $z_1 + z_2 = y_1$ et $z_1 z_2 = y_3$, on peut ainsi construire z_1 et donc $\cos\left(\dfrac{2\pi}{17}\right)$!

Références

[1] G. Godefroy *L'aventure des nombres*, Odile Jacob, 1997.

[2] J.C. Carrega *Théorie des corps ; La règle et le compas*, Hermann, 1981.

[3] D. Perrin, *Cours d'algèbre*, Ecole Normale Supérieure, 1990.