Prérequis. Irréductibilité des polynômes cyclotomiques ; points et nombres constructibles. La définition suivante au grand minimum est à mettre dans le plan :

Définition 0.0.1. Un point P du plan euclidien est *constructible (à la règle et au compas)* s'il est égal à $(0,0)$, à $(1,0)$, ou s'il est intersection de deux objets distincts parmi l'ensemble des droites qui passent par deux points constructibles distincts et l'ensemble des cercles de centre un point constructible passant par un autre point constructible. Un nombre réel a est *constructible* s'il est l'abscisse d'un point constructible.

Théorème 0.0.2 (Wantzel)**.** *Un nombre réel a est constructible si et seulement s'il existe une suite finie de corps $(\mathbf{L}_i)_{0\leqslant i\leqslant n}$ tels que :*

- $\mathbf{L}_0 = \mathbf{Q}$ *;*
- $\mathbf{L}_{i+1}$ *est une extension quadratique de* $\mathbf{L}_i$ *pour tout* $i < n$ *;*
- $a \in \mathbf{L}_n$*.*

Démonstration. Si a est constructible, il est l'abscisse d'un point constructible M que l'on peut supposer situé sur l'axe Ox. Soit $M_1 = (0,0), M_2 = (1,0), M_3, \ldots, M_n = M$ la suite des points construits pour obtenir M. Pour tout i, on note $M_i = (x_i, y_i)$. On pose alors :

$$K_i = \mathbf{Q}(x_1, y_1, \ldots, x_i, y_i).$$

On a clairement $K_1 \subset \cdots \subset K_n$, $K_1 = K_2 = \mathbf{Q}$ et $a = x_n \in K_n$. Il reste à montrer que K_{i+1}/K_i est soit triviale soit de degré deux.

C'est évident pour $i = 1$. Ensuite, si M_{i+1} est l'intersection de deux droites, les nombres x_{i+1} et y_{i+1} sont solutions d'un système de la forme :

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

avec $\alpha, \beta, \gamma, \alpha', \beta', \gamma' \in K_i$. Ce système se résout dans K_i, et alors $K_{i+1} = K_i(x_{i+1}, y_{i+1}) = K_i$.

Si M_{i+1} est l'intersection d'une droite et d'un cercle, cette fois x_{i+1} et y_{i+1} sont solutions d'un système de la forme :

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

Si β n'est pas nul, on peut exprimer y en fonction de x et injecter dans la deuxième équation qui devient de degré deux en x. De même si α n'est pas nul.

Enfin, si M_{i+1} est l'intersection de deux cercles, le système est de la forme :

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

qui équivaut à :

$$\begin{cases} x^2 + y^2 - 2\alpha x - 2\beta y + \gamma = 0 \\ 2(\alpha - \alpha')x + 2(\beta - \beta')y - (\gamma - \gamma') = 0 \end{cases}$$

et l'on se ramène au cas de l'intersection entre une droite et un cercle.

Réciproquement, supposons qu'il existe une suite de corps $\mathbf{Q} = \mathbf{L}_1 \subset \mathbf{L}_2 \subset \cdots \subset \mathbf{L}_p \subset \mathbf{R}$, chaque extension $\mathbf{L}_{i+1}/\mathbf{L}_i$ étant de degré deux, avec $a \in \mathbf{L}_p$. On montre par récurrence sur i que chaque élément de $\mathbf{L}_i$ est constructible.

C'est clairement vrai pour $i = 1$ car tous les nombres rationnels sont constructibles. Supposons alors que $\mathbf{L}_i$ soit un corps de nombres constructibles, et montrons qu'il en est de même pour $\mathbf{L}_{i+1}$. Pour $x \in \mathbf{L}_{i+1}$, la famille $(1, x, x^2)$ est liée donc x est solution d'une équation polynomiale de degré deux de la forme $\alpha x^2 + \beta x + \gamma = 0$. Si α est nul alors $x \in \mathbf{L}_i$ et il n'y a rien à démontrer. Sinon, on a $x = \frac{-\beta \pm \sqrt{\beta^2 - 4\alpha\gamma}}{2\alpha}$ et il est alors clair que x est constructible (on sait construire des racines carrées à la règle et au compas). □

Corollaire 0.0.3. *La quadrature du cercle, la trisection de l'angle et la duplication du cube sont impossibles à réaliser.*

Démonstration. Respectivement parce que π est transcendant, parce que $\cos(\pi/9)$ est de degré trois (donc on ne peut pas trisecter $\pi/3$), et parce que $\sqrt[3]{2}$ est de degré trois. □

Théorème 0.0.4 (Gauss)**.** *Si un polygone régulier à n côtés est constructible à la règle et au compas, alors la décomposition de n en facteurs premiers est :*

$$n = 2^\alpha p_1 \cdot \ldots \cdot p_r$$

où $\alpha \in \mathbf{N}$ et les p_i sont des nombres premiers de Fermat (de la forme $2^{2^k} + 1$).

Démonstration. On commence par un lemme.

Lemme 0.0.5. *Si m et n sont deux entiers premiers entre eux, alors l'angle $\widehat{\frac{2\pi}{mn}}$ est constructible si et seulement si les angles $\widehat{\frac{2\pi}{m}}$ et $\widehat{\frac{2\pi}{n}}$ le sont.*

Démonstration. Si $\widehat{\frac{2\pi}{mn}}$ est constructible, on peut le reporter respectivement n et m fois pour construire ses multiples que l'on cherche. Réciproquement, on écrit une relation de Bézout $\lambda n + \mu m = 1$ et alors on sait facilement construire :

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

□

Ainsi, en écrivant n en produit de puissances de nombres premiers p^s, l'angle $\widehat{\frac{2\pi}{n}}$ est constructible si et seulement si chaque $\widehat{\frac{2\pi}{p^s}}$ l'est. Le cas $p = 2$ est facile à construire, soit alors p un nombre premier impair. On montre que si $\widehat{\frac{2\pi}{p^\alpha}}$ est constructible alors p est de Fermat et $\alpha = 1$. Posons $q = p^\alpha$.

Comme cet angle est constructible, le nombre $\cos\frac{2\pi}{q}$ est constructible, et d'après Wantzel on a :

$$[\mathbf{Q}(\cos\frac{2\pi}{q}) : \mathbf{Q}] = 2^m.$$

Le nombre complexe $\omega = \cos\frac{2\pi}{q} + \mathrm{i}\sin\frac{2\pi}{q}$ est en particulier algébrique sur $\mathbf{Q}$, avec $[\mathbf{Q}(\omega) : \mathbf{Q}] = \varphi(q) = p^{\alpha-1}(p-1)$.

D'autre part, ω est solution de l'équation $\omega^2 - 2\omega\cos\left(\frac{2\pi}{q}\right) + 1$ donc $[\mathbf{Q}(\omega) : \mathbf{Q}(\cos\frac{2\pi}{q})] = 2$. Finalement :

$$p^{\alpha-1}(p-1) = [\mathbf{Q}(\omega) : \mathbf{Q}] = 2^{m+1}.$$

Comme p est impair on en déduit que $\alpha = 1$, et que $p = 1 + 2^{m+1}$. Il reste à montrer que $m+1$ est une puissance de 2. On écrit alors $m+1 = 2^\beta\lambda$ avec λ impair, et l'on remarque que :

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

Comme λ est impair, $1 + X^\lambda$ est multiple de $1 + X$ donc p est multiple de $1 + 2^{2^\beta}$. Comme il est premier, il y a égalité et le résultat est démontré. □

Remarques.

- Tout cela est trop long à démontrer en quinze minutes. Il faut alors choisir ce que l'on fait. En général, il vaut mieux choisir en fonction de la leçon dans laquelle on place le développement. Dans les leçons sur les corps on préférera passer du temps sur le théorème de Gauss, et dans les leçons géométriques on préférera passer du temps sur celui de Wantzel.
- Il est inutile d'écrire, ni même de justifier le corollaire au milieu. Il est là pour la culture, et c'est bien de le connaître car il peut apparaître comme question du jury. En tout cas, il montre qu'on a du recul sur le théorème de Wantzel. D'ailleurs, Wantzel a démontré son théorème avant la démonstration de la transcendance de π, donc on ne savait pas à l'époque déduire du théorème de Wantzel que la quadrature du cercle était impossible. La transcendance de π a d'ailleurs été démontrée en 1882, c'est-à-dire 36 ans après la mort en 1848 de Wantzel.
- Pour la démonstration du théorème de Wantzel, si on n'a pas le temps car on veut passer au théorème de Gauss, on peut se garder d'écrire les équations en entier. On écrit juste une équation de droite et une équation de cercle, et on explique à l'oral que les solutions sont soit dans le corps de base, soit dans une extension de degré deux.
- C'est bien, pour montrer qu'on a du recul, de savoir en déduire une construction d'un polygone non trivial comme par exemple le pentagone (même si ce n'est pas la construction optimale). Cela revient à écrire $\cos\frac{2\pi}{5}$ avec des radicaux, et à en déduire une construction.
- Dans le même ordre d'idée, il faut savoir que le théorème de Gauss est une équivalence. On n'en démontre qu'une implication, car la réciproque est trop difficile à faire à l'agreg (elle demande trop de théorie de Galois pour une leçon).
- Il faut savoir démontrer que les rationnels sont constructibles. On sait facilement tracer l'axe des abscisses à la règle puis tous les entiers avec un compas, et le théorème de Thalès nous permet de découper un segment en n parties égales, donc on a tous les rationnels.

- Il faut aussi savoir pourquoi la formule $x = \frac{-\beta \pm \sqrt{\beta^2 - 4\alpha\gamma}}{2\alpha}$ permet de dire que x est constructible. Les scalaires α, β et γ sont par hypothèse constructibles, donc il suffit de savoir mettre au carré, faire des multiplications, des additions et soutractions, des racines carrées et des divisions. Pour faire une multiplication (et donc une mise au carré) ou une division, on utilise le théorème de Thalès. Pour tracer la racine carrée d'un nombre constructible ξ, on trace un demi-cercle de diamètre $\xi + 1$, et on trace la perpendiculaire au diamètre qui se trouve à distance 1 de l'un de ses sommets. La distance entre l'angle droit et l'intersection de la perpendiculaire avec le demi-cercle est $\sqrt{\xi}$.
- Il faut enfin savoir pourquoi $[\mathbf{Q}(\omega) : \mathbf{Q}] = \phi(q)$. C'est parce que le polynôme minimal d'une racine primitive q-ème de l'unité est Φ_q, qui est de degré $\varphi(q)$. On doit admettre ceci dans le développement, car montrer que Φ_q est le polynôme minimal de ω est à lui seul à développement, lorsque l'on montre que les polynômes cyclotomiques sont irréductibles sur $\mathbf{Q}$ (cf Perrin, page 83).
- Le théorème de Gauss est extrêmement restrictif, car l'on ne connaît aujourd'hui que cinq nombres premiers de Fermat (les cinq premiers : 3, 5, 17, 257 et 65 537). Fermat pensait que tous les nombres de la forme $1 + 2^{2^n}$ étaient premiers, mais il n'avait vérifié que les cinq premiers, et le sixième est composé. Le septième aussi, le huitième aussi, [...], le trente-troisième aussi. À partir de $1 + 2^{2^{33}}$, on ne sait pas. Le plus grand nombre de Fermat connu comme étant composé en 2013 est $1 + 2^{2^{2747497}}$. Bref, les polygones réguliers à un nombre impair de côtés étant actuellement démontrés constructibles sont donc au nombre de $2^5 = 32$.

Recasages.

- 102 : On utilise bien dans le théorème de Gauss les propriétés des racines de l'unité. C'est super si on rajoute juste avant dans le plan le fait que leur polynôme minimal est cyclotomique, et si l'on expose le théorème de Gauss comme une conséquence. Il faut un peu éclipser Wantzel ici.
- 121 : Le théorème de Gauss permet d'introduire les nombres premiers de Fermat, et la discussion sur l'existence ou non d'autres nombres de Fermat qui sont premiers. Encore une fois, il faut passer un peu Wantzel.
- 125 : C'est parfait, à la fois pour le théorème de Wantzel et pour le théorème de Gauss. C'est bien alors de faire les parties de chaque démonstration qui sont vraiment à propos d'extensions de corps, et de passer rapidement sur le reste (mais il ne faut pas non plus trop négliger la géométrie).
- 144 : C'est limite, mais les polynômes minimaux des nombres algébriques jouent un rôle crucial ici, que ce soit dans la démonstration ou encore mieux dans la recherche d'un procédé de construction à la règle et au compas d'un polygone régulier donné. Et le théorème de Wantzel est une application assez spectaculaire de la formule pour les racines d'un polynôme de degré deux.
- 151 : On fait apparaître des conditions nécessaires pour un problème géométrique à travers des degrés d'extensions de corps, c'est-à-dire des dimensions d'espaces vectoriels. Si on appuie sur ce point, le développement est vraiment joli dans cette

leçon.

— 191 : Tout est dans le titre de la leçon, c'est même difficile de faire mieux que ce développement ici.