Développement : Théorème de Gauss-Wantzel

Thomas W.

23 juillet 2023

Leçons concernées :

- 102 : Groupe des nombres complexes de module 1. Racines de l'unité. Applications. *****
- 104 : Groupes finis. Exemples et applications. ****
- 120 : Anneau $\frac{\mathbf{Z}}{n\mathbf{Z}}$. Applications. *****
- 121 : Nombres premiers. Applications. *****
- 125 : Extensions de corps. Exemples et applications. *****
- 151 : Dimension d'un espace vectoriel. Rang. Exemples et applications. *****
- 191 : Exemples d'utilisation de techniques d'algèbre en géométrie. *****

Référence :

- L'oral à l'agrégation de mathématiques, Une sélection de développements, L. Isenmann, T. Pecatte
- Théorie de Galois, I. Gozard

Attention ! Lorsque j'ai passé l'agrégation (2023) le livre de développements d'Isenmann et Pecatte était interdit, notamment à cause des plans qui se trouvaient à la fin du livre. Pensez bien à prendre la version rééditée dans laquelle les plans de leçon n'apparaissent plus (en cours de réédition au moment où j'écris, juillet 2023). Sinon, ce développement est trouvable dans le livre *Théorie des corps, Carrega*. Le livre d'Isenmann et Pecatte vaut vraiment le détour car les développements sont souvent bien détaillés et les résultats à connaître sont rappelés en début de chaque développement. Il y a également toujours des approfondissements, ce qui est indispensable à la préparation d'un développement. C'est un travail de recherche qui est prémâché pour nous, et c'est très appréciable car c'est assez pénible de scruter des dizaines de livres à la recherche d'un résultat précis.
Je précise que j'ai un peu modifié la preuve qui est faîte dans Isenmann et Pecatte pour qu'elle rentre mieux dans les leçons 104 et 120.
Pour finir, ce développement parle de constructibilité à la règle et au compas. Il serait du plus mauvais goût de ne pas savoir faire concrètement quelques

constructions. J'en reparlerai en fin de document. Je vous recommande l'application *Euclidea* qui est utile pour faire des constructions à la règle et au compas rapidement sur le téléphone ou l'ordinateur, sans avoir à sortir son compas, sa règle...

Commençons par citer le résultat qui fait l'objet de ce développement :

Théorème (Gauss-Wantzel)
On dit que le polygône régulier à n côtés est constructible si le nombre complexe $e^{\frac{2i\pi}{n}}$ est constructible.
Remarque : *Le premier sommet de ce polygône régulier est placé en le point $I(1,0)$. Si on arrive à construire $e^{\frac{2i\pi}{n}}$, on aura tous les autres sommets en reportant la longueur qui sépare I et $e^{\frac{2i\pi}{n}}$ sur le cercle unité (ils seront bien à l'intersection de deux cercles), d'où la définition qui se réduit à ne construire que le deuxième sommet.*

1. *Soit $n \in \mathbf{N}$ un entier naturel non nul et soit ω une racine n-ème primitive de l'unité.*
   Alors, le groupe $Aut(\mathbb{Q}(\omega)/\mathbb{Q})$ des automorphismes de $\mathbb{Q}(\omega)$ qui fixent $\mathbb{Q}$ est isomorphe à $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$.
2. *Soit p un nombre premier impair. Alors, le polygône régulier à p^a côtés est constructible à la règle et au compas ssi $a = 1$ et s'il existe $N \in \mathbb{N}$ tel que $p = 2^N + 1$ (p est un nombre premier de Fermat).*

Citons maintenant les résultats que nous allons utiliser pour prouver ce théorème. Je ne rappelle pas les définitions de constructibilité à la règle et au compas, ni de nombre réel constructible. C'est trouvable dans le Gozard par exemple.
Habituellement, le théorème de Wantzel est cité ainsi :

Théorème (Wantzel)
Soit $t \in \mathbb{R}$. t est constructible si et seulement si il existe une suite finie $(L_0, \dots, L_p)$ de sous-corps de $\mathbb{R}$ vérifiant :

- *$L_0 = \mathbb{Q}$.*
- *Pour tout i, L_{i+1} est une extension quadratique (i.e. de degré 2) de L_i.*
- *$t \in L_p$.*

La preuve de ce théorème peut faire un développement pour la leçon 125. Mais bon, je ne vois pas beaucoup de recasage. Il est bon d'avoir l'idée de la preuve en tête : Si un nombre est constructible à la règle et au compas, alors on peut l'atteindre en construisant des points intermédiaires les uns après les autres comme intersection de deux droites, de deux cercles ou d'une droite et d'un cercle (il faut biensûr préciser les centres et les rayons des cercles, les points par lesquels passent les droites...). Or, un point $M(x, y)$ qui appartient par exemple à l'intersection d'un cercle et d'une droite va

vérifier deux équations polynômiales de degrés 2 et de degré 1 en x et en y. En exprimant y en fonction de x on trouve que x est racine d'un polynôme de degré 2. Alors, soit ce polynôme est irréductible et l'extension $\mathbb{K}(x)$ est de degré 2, soit il n'est pas irréductible et $x \in \mathbb{K}$. En ne considérant que les extensions qui sont de degré 2 jusqu'à atteindre le point désiré, on a notre tour d'extension quadratique.
Nous aurons besoin cependant d'une version complexe de ce résultat pour notre développement. C'est faisable avec la version réelle, dans ce cas nous essaierons de construire $cos(\frac{2\pi}{n})$, mais ça complique un peu les choses car on doit se ramener à des sous-corps de $\mathbb{R}$ pour l'appliquer.

Théorème (Wantzel version complexe)
Soit $z \in \mathbb{C}$. On dit que z est constructible si $(Re(z), Im(z))$ est constructible. Alors, z est constructible si et seulement il existe une suite finie $(L_0, \ldots, L_q)$ de sous-corps de $\mathbb{C}$ vérifiant :

- $L_0 = \mathbb{Q}$.
- *Pour tout i, L_{i+1} est une extension quadratique (i.e. de degré 2) de L_i.*
- $z \in L_q$.

Voir Gozard chapitre 16 pour la preuve.
Un corollaire classique est le suivant :

Corollaire
Si $z \in \mathbb{C}$ est constructible, alors $[\mathbb{Q}(z) : \mathbb{Q}]$ est une puissance de deux.

On en déduit par exemple que la racine cubique de deux n'est pas constructible à la règle et au compas. Passons maintenant à la preuve du théorème cité au tout début.

Démonstration

1. *Comme ω est une racine n-ème primitive, son polynôme minimal est le n-ième polynôme cyclotomique Φ_n (Je mettrai des rappels sur Φ_n en fin de document). Soit $\sigma \in Aut(\mathbf{Q}(\omega)/\mathbf{Q})$. Comme σ fixe $\mathbb{Q}$ et est un morphisme de corps, on a $\Phi_n(\sigma(\omega)) = \sigma(\Phi_n(\omega)) = \sigma(0) = 0$. Donc $\sigma(\omega)$ est une racine de Φ_n, c'est à dire une racine n-ième primitive de l'unité. L'ensemble des racines n-ièmes de l'unité est un groupe cyclique, dont les générateurs sont les racines n-ièmes primitives de l'unité (par définition). Or, on sait que dans un groupe cyclique $G =< a >$, d'ordre n, les autres générateurs de G sont les a^k où $k \in \{1, \ldots, n-1\}$ est premier avec n. Ainsi, il existe $k \in \{1, \ldots, n-1\}$ premier avec n tel que $\sigma(\omega) = \omega^k$. Cela nous permet de définir l'application*

$$Aut(\mathbb{Q}(\omega)/\mathbb{Q}) \longrightarrow (\frac{\mathbb{Z}}{n\mathbb{Z}})^*$$

qui à σ associe $\overline{k}$ où $\sigma(\omega) = \omega^k$. Comme k est premier avec n on est bien dans le groupe des inversibles de $\frac{\mathbb{Z}}{n\mathbb{Z}}$. Cette application est

injective car tout élément de $Aut(\mathbb{Q}(\omega)/\mathbb{Q})$ est entièrement déterminé par l'image de ω (car l'extension est monogène, engendrée par ω). Montrons la surjectivité : Il faut montrer que, étant donnée une autre racine n-ième primitive de l'unité de la forme ω^k, k premier avec n, il existe un élément $\sigma \in Aut(\mathbb{Q}(\omega)/\mathbb{Q})$ tel que $\sigma(\omega) = \omega^k$.
Ici, un diagramme est plus que bienvenu dans la présentation orale. Φ_n étant irréductible sur $\mathbb{Q}$, on a que $\frac{\mathbb{Q}[X]}{(\Phi_n)}$ est un corps. ω et ω^k étant deux racines distinctes de Φ_n, on a deux isomorphismes de corps :

$$ev_\omega : \frac{\mathbb{Q}[X]}{(\Phi_n)} \longrightarrow \mathbb{Q}(\omega) \text{ et } ev_{\omega^k} : \frac{\mathbb{Q}[X]}{(\Phi_n)} \longrightarrow \mathbb{Q}(\omega^k)$$

qui consistent à évaluer en ω et ω^k. On en déduit un isomorphisme de $\mathbb{Q}(\omega)$ dans $\mathbb{Q}(\omega^k)$ qui envoie ω sur ω^k : On pose $\sigma = ev_{\omega^k} \circ (ev_\omega)^{-1}$. Et alors ce σ convient, car $\mathbb{Q}(\omega) = \mathbb{Q}(\omega^k)$ (Pourquoi ?). D'où la surjectivité.
Montrons que c'est un morphisme de groupes :
Soient $\sigma, \sigma' \in Aut(\mathbb{Q}(\omega)/\mathbb{Q})$. On a

$$\sigma \circ \sigma'(\omega) = \sigma(\sigma'(\omega)) = \sigma(\omega^{k'}) = \sigma(\omega)^{k'} = \omega^{kk'}$$

D'où le résultat.

2. *" $\Longrightarrow$ " Supposons que le polygône régulier à p^a côtés soit constructible, avec p premier impair. Alors $\omega = e^{\frac{2i\pi}{p^a}}$ est constructible et c'est une racine p^a-ième primitive de l'unité. D'après le corollaire du théorème de Wantzel, on a donc $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2^N$ où N est un entier naturel. Mais le polynôme minimal de ω est Φ_{p^a}, qui est irréductible de degré $\phi(p^a) = p^{a-1}(p-1)$. Donc on a l'égalite $2^N = p^{a-1}(p-1)$. Comme p est impair, cela implique que $a = 1$ et on a $p = 2^N + 1$ est un nombre premier de Fermat.*
" $\Longleftarrow$ " Réciproquement, supposons que p premier soit de la forme $p = 2^N + 1$. Soit $\omega = e^{\frac{2i\pi}{p}}$. ω est une racine p-ième primitive de l'unité. D'après le premier point, on a que $Aut(\mathbb{Q}(\omega)/\mathbb{Q})$ est isomorphe à $(\frac{\mathbb{Z}}{p\mathbb{Z}})^*$. Or, $(\frac{\mathbb{Z}}{p\mathbb{Z}})^*$ est cyclique, Donc $Aut(\mathbb{Q}(\omega)/\mathbb{Q})$ est aussi cyclique. On a d'autre part que $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(p) = p - 1 = 2^N$ (cette extension est de degré une puissance de 2, c'est bien parti) donc la famille $B = (\omega, \omega^2, \ldots, \omega^{p-1})$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\omega)$ (habituellement on prends plutôt $(1, \omega, \ldots, \omega^{p-2})$ mais ici cette base nous arrange mieux). Comme $Aut(\mathbb{Q}(\omega)/\mathbb{Q})$ est cyclique, il existe un élément g d'ordre $p-1$. Donc la famille $(\omega, g(\omega), \ldots, g^{p-2}(\omega))$ est encore une base (c'est la base précédente permutée). Pour tout $i \in \{1, \ldots, N\}$, on pose $K_i = \left\{z \in \mathbb{Q}(\omega), g^{2^i}(z) = z\right\}$. Ce sont des sous-corps de $\mathbb{Q}(\omega)$ (Donc de $\mathbb{C}$) car ce sont les corps fixes de certains $\mathbb{Q}$-automorphismes de $\mathbb{Q}(\omega)$. (Sinon, ça se vérifie assez facilement à la main, mais ce genre

d'argument revient quand on étudie les corps finis avec le morphisme de Frobenius, et dans la correspondance de Galois). Remarquons tout de suite que $K_N = \mathbb{Q}(\omega)$. Montrons que $K_0 = \mathbb{Q}$:
Soit $z \in K_0$. On décompose z dans la base précédente : $z = \sum_{i=0}^{p-2} z_i g^i(\omega)$. On écrit alors plus simplement, en identifiant z avec ses coordonnées dans cette base, $z = (z_0, \dots, z_{p-2})$. On a alors $g(z) = (z_{p-2}, z_0, \dots, z_{p-3})$. Mais comme $z \in K_0$, on a $g(z) = z$ et, en regardant les coordonnées, cela donne $z_0 = z_1 = \dots = z_{p-2}$. Donc $z = z_0 \sum_{i=0}^{p-2} g^i(\omega) = z_0 \sum_{i=1}^{p-1} \omega^i = z_0 \times \omega \frac{1-\omega^{p-1}}{1-\omega} = -z_0$ et donc $z \in \mathbb{Q}$. D'où $K_0 \subseteq \mathbb{Q}$ et l'inclusion réciproque est évidente. Cette suite de K_i est donc bien partie pour être notre tour d'extensions quadratiques. Montrons maintenant que $[K_i : K_0] = 2^i$ pour tout i. Je le présente de manière non rigoureuse pour faire passer l'idée à l'oral, le travail de rédaction au niveau des indices est un peu plus pénible et c'est fait dans le Isenmann et Pecatte. A vous de voir ce que vous préférez.
Commençons par K_1 pour voir ce qu'il se passe. On identifie encore un élément $z \in \mathbb{Q}(\omega)$ avec ses coordonnées dans la base de tout à l'heure. On a cette fois $g^2(z) = z$. Donc on a $(z_{p-3}, z_{p-2}, z_0, z_1, \dots, z_{p-4}) = (z_0, z_1, z_2, z_3, \dots, z_{p-1})$ ce qui donne $z_0 = z_2 = \dots = z_{p-3}$ et $z_1 = z_3 = \dots = z_{p-2}$. Ainsi, $z = (z_0, z_1, \dots, z_0, z_1)$. Notons $e = (1, 0, \dots, 1, 0)$. Alors, $g(e) = (0, 1, \dots, 0, 1)$ et donc, d'après ce qui précède, $(e, g(e))$ est une $\mathbb{Q}$-base de K_1. D'où $[K_1 : K_0] = 2$. Précisons que ceci n'est pas une démonstration par récurrence, c'est juste pour sentir ce qui va arriver. Je vous invite à montrer de la même manière que $[K_2 : K_0] = 4$. Dans le cas général, i.e. si $i \in \{1, \dots, N\}$, si $z \in K_i$, on aura $g^{2^i}(z) = z$. On note cette fois $e = (1, 0, \dots, 0, 1, 0, \dots, 0, \dots, 1, 0, \dots, 0)$, où chaque bloc $(1, 0, \dots, 0)$ possède $2^i - 1$ zéros car g^{2^i} décale 2^i fois les coordonnées vers la droite. On a alors que $(e, g(e), \dots, g^{2^i-1}(e))$ est une $\mathbb{Q}$ base de $\mathbb{Q}(\omega)$, donc $[K_i : K_0] = 2^i$.
Enfin, il est facile de voir que l'on a $K_i \subseteq K_{i+1}$. D'après le théorème de la base téléscopique, on a alors

$$[K_{i+1} : K_0] = [K_{i+1} : K_i][K_i : K_0]$$

Et on déduit de ce qui précède $[K_{i+1} : K_i] = 2$. D'où ω est constructible d'après la version complexe du théorème de Wantzel.

Quelques résultats supplémentaires

Comme bien souvent dans un anneau factoriel, les raisonnements sur les éléments irréductibles permettent de passer au cas général. D'où mon recasage dans la leçon sur les nombres premiers. Si vous souhaitez que le dévéloppement rentre plus dans la leçon sur les nombres premiers, vous pouvez démontrer le point 1) directement pour p premier. Nous pouvons maintenant déterminer précisément quels sont les polygones réguliers constructibles

à la règle et au compas à partir du résultat précédent. On a besoin du lemme suivant :

Lemme

Soient n et m deux entiers premiers entre eux. Alors le polygone régulier à nm côtés est constructible ssi les polygones réguliers à n côtés et m côtés sont constructibles.

Démonstration

" $\Longrightarrow$ " *Plus généralement, si le polygone régulier à n côtés est constructible, alors, pour tout diviseur d de n, le polygone régulier à d côtés est constructible. On écrit $n = dd'$. Notons $\{A_1, \ldots, A_n\}$ les sommets du polygone régulier à n côtés. Alors $\{A_1, A_{d'}, \ldots, A_n\}$ sont les sommets du polygone régulier à d côtés. Ce n'est pas rigoureux, mais ça se voit bien sur une figure).*

" $\Longleftarrow$ " *Si les polygones réguliers à n et m côtés sont constructibles, alors les complexes $e^{\frac{2i\pi}{n}}$ et $e^{\frac{2i\pi}{m}}$ sont constructibles. On montre alors que le complexe $e^{\frac{2i\pi}{nm}}$ est constructible.*

Comme n et m sont premiers entre eux, il existe u et v dans $\mathbb{Z}$ tels que $un + vm = 1$. Mais alors, $e^{\frac{2i\pi}{nm}} = e^{v\frac{2i\pi}{n}} e^{u\frac{2i\pi}{m}} = (e^{\frac{2i\pi}{n}})^v (e^{\frac{2i\pi}{m}})^u$ est constructible car l'ensemble des nombres complexes constructibles est un sous-corps de $\mathbb{C}$.

On en déduit la classification des polygones réguliers constructibles, qu'on appelle encore théorème de Gauss-Wantzel :

Théorème (Gauss-Wantzel)

Soit $n \in \mathbb{N}, n \geq 2$. On peut construire le polygone régulier à n côtés ssi

1. *Ou bien n est une puissance de deux*
2. *Ou bien il existe $\alpha \in \mathbb{N}$ et des nombres premiers de Fermat distincts $p_1, \ldots, p_k$ tels que $n = 2^\alpha p_1 \ldots p_k$*

Démonstration

On décompose n en produit de facteurs premiers : $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$. D'après le lemme précédent (généralisé), le polygone régulier à n côtés est constructible ssi chaque polygone régulier à $p_k^{\alpha_k}$ côtés est constructible. Ainsi, tous les nombres premiers impairs qui apparaissent dans la décomposition en facteurs premiers de n doivent apparaître une seule fois et être des nombres premiers de Fermat. Pour la puissance de 2, c'est simplement dû au fait qu'on peut couper un angle en deux à la règle et au compas (bissecter). Donc, dès qu'on sait faire un polygone régulier à d côtés, on sait faire tous les polygones réguliers à $2^k d$ côtés.

Concernant la constructibilité à la règle et au compas, il est bon de savoir démontrer le résultat suivant :

Théorème

L'ensemble des nombres réels constructibles à la règle et au compas est un sous-corps de $\mathbb{R}$ qui contient $\mathbb{Q}$ et qui est stable par racine carrée.

J'ai vu des rapports d'oraux où les candidats se voyaient demander de démontrer ceci. Mais bon, je pense que ce n'est pas trop grave de ne pas y arriver, sachant que c'est du bachotage pur et dur (apprendre par coeur les droites et cercles à considérer...). Peut-être que je me trompe et que certains jurys verraient ça d'un mauvais oeil. A vous de voir. C'est bien aussi de savoir tracer une bissectrice, la perpendiculaire à une droite passant par un point donné... Voir *Euclidea* comme ce que j'ai dis au début.
Par contre, il me semble très important de savoir construire à la règle et au compas le pentagone et l'hexagone régulier. Pour l'hexagone c'est facile, on reporte juste la longueur 1 partout sur le cercle à partir de $I(1,0)$. Pour le pentagone, c'est là qu'on commence à comprendre ce qu'on fait. On va construire le réel $cos(\frac{2\pi}{5})$. Calculons tout d'abord ce cosinus. On note $\omega = e^{\frac{2i\pi}{5}}$. On a $1+\omega+\omega^2+\omega^3+\omega^4 = 0$ (somme géométrique). Mais $\omega^3 = \overline{\omega}$ et $\omega^4 = \overline{\omega^2}$. Ceci donne $1 + \omega + \overline{\omega} + \omega^2 + \overline{\omega^2} = 0$. Notons $X = \omega + \overline{\omega}$. On a alors $X^2 = \omega^2 + \overline{\omega^2} + 2$. On en déduit que $X^2 + X - 1 = 0$ et donc que X vaut $\frac{\sqrt{5}-1}{2}$. Or, X=$2Re(\omega) = 2cos(\frac{2\pi}{5})$. D'où

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

Voici alors une construction de $\frac{\sqrt{5}-1}{4}$. On note I,J,K et L les points $I(1,0), J(0,1), K(-1,0), L(0,-1)$.

1. Placer D le milieu de $[OK]$. La longueur DJ vaut $\frac{\sqrt{5}}{2}$.
2. Placer E, le point d'intersection du cercle de centre D de rayon DJ avec le segment $[OI]$. La longueur OE vaut $\frac{\sqrt{5}-1}{2}$.
3. Placer F le milieu de $[OE]$. La longueur OF vaut $\frac{\sqrt{5}-1}{4}$.
4. La perpendiculaire à $[OI]$ passant par E coupe le cercle unité en le deuxième sommet du pentagone régulier.

Pour terminer la construction du pentagone régulier, reporter la distance entre I et le sommet construit sur le cercle. jusqu'à retomber sur I.
Gauss avait donné une méthode de construction du polygone régulier à 17 côtés. Pour cela, la démarche est exactement la même, sauf que le calcul de $cos(\frac{2\pi}{17})$ est beaucoup plus compliqué, et même la construction des racines imbriquées qui apparaissent dans l'expression de $cos(\frac{2\pi}{17})$ est assez terrible à réaliser en pratique. Mais ça se fait. Il existe des animations en ligne. En fait, la démonstration que l'on a vue dans ce développement permet de donner une méthode pour calculer ce cosinus. C'est expliqué dans le Gozard (et sur Wikipédia). Mais j'avoue ne pas avoir approfondi ce point là et je ne pourrai pas donner plus d'explications.

Passons aux quelques rappels sur les polynômes cyclotomiques.

Définition
Soit n un entier naturel non nul. On note μ_n l'ensemble des racines n-ièmes de l'unité et μ_n^* l'ensemble des racines n-ièmes primitives de l'unité (i.e. les générateurs de μ_n).

On sait que les racines n-ièmes de l'unité sont algébriques sur $\mathbb{Q}$ (même des entiers algébriques mais on en a pas besoin ici) car sont annulées par le polynôme $X^n - 1$. Soit $\xi \in \mu_n^*$. On cherche le polynôme minimal de ξ. Tout d'abord, voyons pourquoi on s'intéresse aux racines primitives. Soit $z \in \mu_n$. Parmi les polynômes de la forme $X^m - 1$ qui annulent z, celui de degré le plus petit est $X^d - 1$, où d est l'ordre de z dans μ_n. Mais z est une racine d-ième primitive de l'unité. Cela revient donc à étudier directement les racines primitives.
On note $\Pi_{\xi,\mathbb{Q}}$ le polynôme minimal de ξ sur $\mathbb{Q}$. On sait alors déjà que $\Pi_{\xi,\mathbb{Q}}$ divise $X^n - 1$ dans $\mathbb{Q}$. Or, $X^n - 1 = \prod_{\omega \in \mu_n} (X - \omega)$. Ainsi, $\Pi_{\xi,\mathbb{Q}}$ est scindé sur $\mathbb{C}$ et ses racines, simples, sont des racines de l'unité. Pour poursuivre l'intuition, on peut tester à la main les polynômes minimaux de quelques racines de l'unité simples comme i ou j (faîtes-le) et se rendre compte que n'interviennent dans le produit que les racines primitives. Ceci nous invite à poser :

$$\Phi_n(X) = \prod_{\xi \in \mu_n^*} (X - \xi)$$

Ainsi, Φ_n est un polynôme de degré $\phi(n)$ car il existe $\phi(n)$ racines n-ièmes primitives de l'unité.
Si on connaît un peu la théorie de Galois, on pouvait aussi intuiter la forme de Φ_n. Mais il me semble que les polynômes cyclotomiques étaient connus avant la théorie de Galois. En effet, les autres racines de $\Pi_{\xi,\mathbb{Q}}$ sont les images de ξ par les $\mathbb{Q}$ automorphismes du corps de décomposition de $\Pi_{\xi,\mathbb{Q}}$ sur $\mathbb{Q}$. J'ai démontré ceci en fin de document sur mon développement "Théorème de Burnside (Groupes simples)". Or, il est facile de voir que ces images vont encore être des racines n-ièmes primitives de l'unité. Maintenant ce n'est pas évident (me semble-t-il), qu'elles apparaissent toutes.
Le n-ième polynôme cyclotomique, a donc de grandes chances d'être irréductible et d'être le polynôme minimal des racines n-ièmes primitives de l'unité. Mais ce n'est pas facile à démontrer et peut faire l'objet d'un développement. Une méthode, celle de Schur, est faîte dans le sujet X-ENS Maths A 2019. Cela peut être un bon exercice pour se préparer à l'écrit de l'agrégation et se familiariser avec les polynômes cyclotomiques. Une autre méthode (que je préfère) est celle faîte dans le Perrin. Il y a un exercice dans le Gourdon Algèbre qui démontre ça aussi. Sachez que les polynômes cyclotomiques se recasent dans pas mal de leçons donc c'est très rentable d'investir du temps de travail là-dedans. Caldero a fait des vidéos dans lesquelles il calcule des polynômes cyclotomiques (plus d'une centaine), ça peut être pas mal de re-

garder ça pour se familiariser avec la notion. Les polynômes cyclotomiques interviennent par exemple dans la preuve des résultats suivant : Théorème de Gauss-Wantzel, Théorème de Dirichlet faible, Théorème de Wedderburn, et le fait que les tables des caractères des groupes symétriques sont à valeurs dans $\mathbb{Z}$. Je vous laisse le soin d'étudier tout ceci.
Pour finir ce document, donnons une preuve du théorème de Gauss-Wantzel avec la correspondance de Galois. Je précise une dernière fois que ce n'est pas du tout nécessaire de savoir faire ça. Je le mets juste si jamais certaines personnes ont envie d'approfondir. Rappelons un énoncé de la correspondance de Galois, ainsi que quelques notations. Ici, je ne ferai presque que recopier le Gozard.

Définition
Soient K un corps et L une extension de K. On note $\mathcal{M}$ l'ensemble des corps M tels que $K \subseteq M \subseteq L$ (les corps intermédiaires) et on note $\mathcal{G}$ l'ensemble des sous-groupes de $Gal(L/K)$.
Pour $M \in \mathcal{M}$, on note $M^\circ = Gal(L/M)$. M° est un sous-groupe du groupe de Galois.
Pour $H \in \mathcal{G}$, on note $H^\dagger$ (Lire "H dague" à l'oral) le corps fixe par H : $H^\dagger = \{x \in L / \forall h \in H, h(x) = x\}$. $H^\dagger$ est un corps intermédiaire pour l'extension L/K.

La correspondance de Galois dit qu'il y a une correspondance bijective réciproque décroissante entre les éléments de $\mathcal{G}$ et $\mathcal{M}$ lorsque L/K est galoisienne finie. Je ne connais pas la théorie de Galois infinie, mais j'ai lu quelque part que la correspondance de Galois est fausse dans le cas infini (à vérifier). Pour une extension non galoisienne c'est faux aussi. Le contre-exemple classique est l'extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

Théorème (Correspondance de Galois)
Soient K un corps, et L une extension de K galoisienne, finie. Alors, les deux applications $\circ$ et $\dagger$ sont décroissantes, bijectives et réciproques l'une de l'autre.

On aura besoin de cet autre théorème, qu'on utilise souvent pour expliciter concrètement la correspondance de Galois :

Théorème
Soit K un corps. Soit L une extension galoisienne de K. Soit $M \in \mathcal{M}$.

- *Les conditions suivantes sont équivalentes :*
  1. *M est une extension galoisienne finie de K.*
  2. *M° est distingué dans $Gal(L/K)$.*
  3. *$\forall g \in Gal(L/K), g(M) = M$*
- *Si elles sont remplies, $Gal(M/K)$ est isomorphe au groupe quotient $Gal(L/K)/(Gal(L/M)$.*

Passons à la preuve du théorème de Gauss-Wantzel avec ce résultat.

Théorème (Gauss-Wantzel)

1. *Soit $n \in \mathbf{N}$ un entier naturel non nul et soit ω une racine n-ème primitive de l'unité.*
   Alors, le groupe $Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ est isomorphe à $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$.
2. *Soit p un nombre premier impair. Alors, le polygone régulier à p^a côtés est constructible à la règle et au compas ssi $a = 1$ et s'il existe $N \in \mathbb{N}$ tel que $p = 2^N + 1$ (p est un nombre premier de Fermat).*

Démonstration

1. *Déjà fait, ce n'est qu'une reformulation du premier énoncé.*
2. *Le sens " $\Longrightarrow$ " ne change pas par rapport à ce qui a été fait.*
   " $\Longleftarrow$ " L'extension $\mathbb{Q}(\omega)/\mathbb{Q}$ est galoisienne finie, car c'est une extension de décomposition de Φ_n sur $\mathbb{Q}$ qui est finie. (Pour rappel, pour des extensions de degré fini, il y a équivalence entre "être normale" et "être le corps de décomposition d'un polynôme"). De plus, on a vu que $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2^N$. Comme l'extension est galoisienne, on a $|Gal(\mathbb{Q}(\omega)/\mathbb{Q})| = [\mathbb{Q}(\omega) : \mathbb{Q}] = 2^N$. (Pour rappel, on a toujours $|Gal(L/K)| \leq [L : K]$ mais pas toujours égalité. On a égalité dans le cas fini ssi L est galoisienne). D'après le premier point, $Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ est cyclique car isomorphe à $(\frac{\mathbb{Z}}{p\mathbb{Z}})^*$. Soit g un générateur. Soit, pour tout $i \in \{0, \ldots, N\}$, $H_i =< g^{2^i} >$. Les H_i sont exactement les sous-groupes de $Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ (dans un groupe cyclique, pour tout diviseur d de l'ordre du groupe, il existe un unique sous-groupe d'ordre d qui est cyclique) et on a

$$\{Id\} = H_N \subseteq H_{N-1} \subseteq \ldots \subseteq H_0 = Gal(\mathbb{Q}(\omega)/\mathbb{Q})$$

La correspondance de Galois va donner une tour d'extensions (qui sera biensûr quadratique) de $\mathbb{Q}(\omega)/\mathbb{Q}$ rangée dans l'autre ordre :

$$\{Id\}^\dagger = H_N^\dagger \supseteq H_{N-1}^\dagger \supseteq \ldots \supseteq H_0^\dagger = Gal(\mathbb{Q}(\omega)/\mathbb{Q})^\dagger$$

Notons $K_i = H_i^\dagger$ (Remarquer qu'on retrouve les K_i de la première preuve). On a, par correspondance de Galois, $K_0 = \mathbb{Q}$ et $K_N = \mathbb{Q}(\omega)$. Il ne reste plus qu'à montrer que c'est une tour d'extensions quadratiques. Tout d'abord, comme $Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ est cyclique, c'est en particulier un groupe abélien et donc tous ses sous-groupes sont distingués. On a donc K_i° distingué dans $Gal(\mathbb{Q}(\omega)/\mathbb{Q})$, et donc $Gal(K_i/K)$ est isomorphe au groupe quotient $Gal(\mathbb{Q}(\omega)/\mathbb{Q})/Gal(\mathbb{Q}(\omega)/K_i)$. Mais $Gal(\mathbb{Q}(\omega)/K_i) = K_i^\circ = H_i^{\dagger\circ} = H_i$ et donc on a

$$[K_i : \mathbb{Q}] = |Gal(K_i/\mathbb{Q})| = \frac{|Gal(\mathbb{Q}(\omega)/\mathbb{Q})|}{|Gal(\mathbb{Q}(\omega)/K_i)|} = \frac{[\mathbb{Q}(\omega) : \mathbb{Q}]}{|H_i|} = \frac{2^N}{2^N - i} = 2^i$$

La première égalité étant dûe au fait que $K_i : \mathbb{Q}$ est galoisienne car K_i° est distingué dans $Gal(\mathbb{Q}(\omega)/\mathbb{Q})$. On conclut comme dans la première version avec le théorème de la base téléscopique.
Il existe un argument qui se passe du fait que le groupe de Galois est cyclique : c'est un 2-groupe, et on sait que dans un p-groupe en général il existe une suite de sous-groupes imbriqués $H_0 \subseteq H_1 \subseteq \ldots \subseteq H_N = G$ telle que $|H_i| = p^i$, et chaque sous-groupe est distingué dans celui qui le contient (ou dans tout G ? Je ne sais plus, à vérifier). La correspondance de Galois donne alors tout de suite le résultat.

Un dernier conseil pour la route : intéressez-vous aux nombres premiers de Fermat, surtout si vous voulez mettre ce développement dans la leçon sur les nombres premiers. Le livre d'Isenmann et Pecatte en parle un peu.