Théorème de Gauss Wantzel

Nico

Prérequis : Irréductibilité du polynôme cyclotomique dans $\mathbb{Q}$, cyclicité de $(\mathbb{Z}/p\mathbb{Z})^*$, théorème de Wantzel, théorème de la base télescopique.

La preuve de ce théorème a été adaptée pour ne faire mention d'aucune théorie de Galois.
Commençons par énoncer le théorème principal :

Théorème de Gauss Wantzel : Soit $n \in \mathbb{N}^*$, le polygone régulier à n côtés est constructible à la règle et au compas si et seulement si soit $n = 2^m$ où $m \geq 2$, soit $n = 2^m p_1 \dots p_r$ où $m \in \mathbb{N}$, $r \geq 1$ et les p_i sont des nombres premiers de Fermat distincts.

Ce résultat étant un peu trop long à montrer, on se proposera de juste démontrer le passage délicat de la preuve :

Théorème : Si p est un nombre premier de Fermat, alors $\zeta := e^{\frac{2i\pi}{p}}$ est constructible à la règle et au compas.

Commençons par introduire quelques notations :

- On notera $p = 1+2^n$ car si $1+2^n$ est premier, alors il est un nombre de Fermat $(= 1 + 2^{2^k})$
- $\mathbb{K} := \mathbb{Q}(\zeta)$. On sait que par irréductibilité du polynôme cyclotomique dans $\mathbb{Q}$, $\mathbb{Q}(\zeta) = \mathbb{Q}[\zeta]$, $[\mathbb{K} : \mathbb{Q}] = p - 1 = 2^n$.
- $\mathcal{B} := (1, \zeta, \dots, \zeta^{p-2})$ une $\mathbb{Q}$-base de $\mathbb{K}$.
- $G := \mathrm{Aut}_{\mathbb{Q}}(\mathbb{K})$ le groupe des automorphismes de $\mathbb{K}$, $\mathbb{Q}$-linéaires [(1)].

La preuve se découpera en deux parties : on prouvera que G est cyclique, en établissant un isomorphisme avec $(\mathbb{Z}/p\mathbb{Z})^*$. On construira ensuite notre tour d'extension quadratique $\mathbb{Q} = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \cdots \subseteq \mathbb{K}_n = \mathbb{K}$.

(1). En fait, les automorphismes de $\mathbb{K}$ sont nécessairement $\mathbb{Q}$-linéaires dans ce cas. Mais on se préserve de le démontrer pour ne pas alourdir la preuve. On remarquera aussi qu'on évitera de parler de groupe de Galois ici.

Démonstration. Etape 1 : Montrer que G est cyclique
Soit $g \in G$, alors g est entièrement déterminé par son image $g(\zeta)$.

Or si l'on note Φ_p le p-ième polynome cyclotomique, on a que $\Phi_p(g(\zeta)) = g(\Phi_p(\zeta)) = g(0) = 0$ par $\mathbb{Q}$-linéarité. D'où $g(\zeta) \in \{\zeta, \dots, \zeta^{p-1}\}$. D'où $|G| \leq p-1$.

De plus, si l'on note $z := \sum_{i=0}^{p-2} \lambda_i \zeta^i \in \mathbb{K}$ l'écriture de z dans la base $\mathcal{B}$, où les λ_i sont dans $\mathbb{Q}$. Alors l'application $g_k : z \mapsto \sum_{i=0}^{p-2} \lambda_i (\zeta^i)^k$ est un automorphisme de $\mathbb{K}$, $\mathbb{Q}$-linéaire, pour tout $k \in [\![1, p-1]\!]$. D'où $|G| \geq p-1$. D'où $|G| = p-1$. On note alors $G = \{g_1, \dots, g_{p-1}\}$.

Considérons l'application :

$$\psi : \left\{ \begin{array}{ccc} (G, \circ) & \longrightarrow & ((\mathbb{Z}/p\mathbb{Z})^*, \cdot) \\ g_k & \longmapsto & \overline{k} \end{array} \right.$$

Il est clair que l'application est bien définie et bijective par construction. Montrons qu'il s'agit en plus d'un isomorphisme : Soient $k, k' \in [\![1, \dots, p-1]\!]$:

$$\psi(g_k \circ g_{k'}) = \psi(g_{kk'}) = \overline{kk'} = \overline{k}\ \overline{k'} = \psi(g_k)\psi(g_{k'})$$

D'où $G \simeq (\mathbb{Z}/p\mathbb{Z})^*$, et d'où G est cyclique par cyclicité de $(\mathbb{Z}/p\mathbb{Z})^*$.

Etape 2 : Construction de la tour d'extension quadratique
Soit g un générateur de G, d'ordre $p-1 = 2^n$. On construit une nouvelle base de $\mathbb{K}$:
$\mathcal{B}' := (\zeta, g(\zeta), \dots, g^{p-2}(\zeta))$.

On définit aussi une suite de groupes cycliques : $G_k =< g^{2^k} >$, $\forall k \in [\![0, n]\!]$ et on a que :

$$\{\mathrm{Id}_{\mathbb{K}}\} = G_n \leq G_{n-1} \leq \cdots \leq G_0 = G$$

Cette série d'inclusion nous motive à définir $\forall i \in [\![0, n]\!]$ l'ensemble $\mathbb{K}_i := \{z \in \mathbb{K} : g^{2^i}(z) = z\}$ qui est un sous corps de $\mathbb{K}$. On remarque que :

$$\mathbb{Q} \subseteq \mathbb{K}_0 \subseteq \cdots \subseteq \mathbb{K}_n = \mathbb{K}$$

car $\forall i \in [\![0, n-1]\!]$, $\forall z \in \mathbb{K}_i$, $g^{2^{i+1}}(z) = g^{2^i}\left(g^{2^i}(z)\right) = g^{2^i}(z) = z$. D'où $\mathbb{K}_i \subseteq \mathbb{K}_{i+1}$.

Montrons que $\mathbb{K}_0 = \mathbb{Q}$, soit $z \in \mathbb{K}_0$, alors son écriture dans la base $\mathcal{B}'$ est :

$$z = \sum_{i=0}^{p-2} \lambda_i g^i(\zeta)$$

Et puisque $z = g(z)$, en composant par g :

$$z = \sum_{i=0}^{p-2} \lambda_i g^{i+1}(\zeta) = \sum_{i=1}^{p-2} \lambda_{i-1} g^i(\zeta) + \lambda_{p-2} g^{p-1}(\zeta)$$

Or $g^{p-1} = \mathrm{Id} = g^0$, d'où $\lambda_{p-2} g^{p-1}(\zeta) = \lambda_{p-2}\zeta$. Il vient que par unicité de l'écriture de z dans la base $\mathcal{B}'$, $\lambda_0 = \ldots = \lambda_{p-2}$. D'où :

$$z = \lambda_0 \sum_{i=0}^{p-2} g^i(\zeta) = \lambda_0 g(\Phi_p(\zeta) - \zeta^{p-1}) = -\lambda_0 \in \mathbb{Q}$$

D'où $\mathbb{K}_0 = \mathbb{Q}$.

Montrons maintenant que pour tout i, $\mathbb{K}_i \subsetneq \mathbb{K}_{i+1}$. Montrons dans un premier temps que $\mathbb{K}_0 \subsetneq \mathbb{K}_1$. On cherche à construire un élément de $\mathbb{K}_1 \backslash \mathbb{K}_0$.

$$z := \zeta + g^2(\zeta) + g^4(\zeta) + \ldots + g^{2^n-2}(\zeta) = \sum_{i=0}^{2^{n-1}-1} g^{2i}(\zeta)$$

En composant par g^2 :

$$g^2(z) = \sum_{i=0}^{2^{n-1}-1} g^{2(i+1)}(\zeta) = \sum_{i=1}^{2^{n-1}} g^{2(i)}(\zeta) = z$$

Car $g^{2^n} = \mathrm{Id} = g^0$. D'où $z \in \mathbb{K}_1$. Mais si l'on ne composait que par g :

$$g(z) = \sum_{i=0}^{2^{n-1}-1} g^{2i+1}(\zeta)$$

D'où $g(z) \neq z$ par unicité de l'écriture de z dans la base $\mathcal{B}'$. D'où $z \notin \mathbb{K}_0$.

On peut montrer de même que pour tout j, $\mathbb{K}_j \subsetneq \mathbb{K}_{j+1}$ en considérant l'élément :

$$z = \sum_{i=0}^{2^{n-j-1}-1} g^{2^{j+1}i}(\zeta) \in \mathbb{K}_{j+1} \backslash \mathbb{K}_j$$

D'où

$$\mathbb{Q} = \mathbb{K}_0 \subsetneq \mathbb{K}_1 \subsetneq \cdots \subsetneq \mathbb{K}_n = \mathbb{K}$$

Or par le théorème de la base télescopique :

$$2^n = [\mathbb{K} : \mathbb{Q}] = \prod_{i=0}^{n-1} \underbrace{[\mathbb{K}_{i+1} : \mathbb{K}_i]}_{\geq 2}$$

D'où $\forall i \in [\![0, n-1]\!]$, $[\mathbb{K}_{i+1} : \mathbb{K}_i] = 2$. Ainsi, par le théorème de Wantzel, ζ est constructible à la règle et au compas. □

On énonce maintenant quelques arguments pour venir à bout de la preuve du théorème de Gauss Wantzel car c'est quand même très stylé de savoir le montrer complètement

Preuve de l'implication directe :

Soit $n = 2^\alpha p_1^{\alpha_1} \dots p_r^{\alpha_r}$ écrit sous sa décomposition en facteurs premiers. Posons $\zeta := e^{\frac{2i\pi}{n}}$. Alors $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ où φ désigne l'indicatrice d'Euler.

Or $\varphi(n) = \varphi(2^\alpha) \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) = 2^{\alpha-1} \prod_{i=1}^{r} \left(p_i^{\alpha_i - 1}(p_i - 1) \right)$. Par le théorème de Wantzel, $\varphi(n)$ est une puissance de 2. Donc $(p_i^{\alpha_i-1}(p_i - 1))$ est une puissance de 2. Et donc $p_i^{\alpha_i-1}$ et $(p_i - 1)$ sont des puissances de 2. D'où $\alpha_i = 1$ et p_i est de la forme $2^{n_i} - 1$.

Preuve que n peut s'écrire comme un produit de p_i distincts

Soient $n, m \in \mathbb{N}^*$ tels que $\zeta_n = e^{\frac{2i\pi}{n}}$ et $\zeta_m = e^{\frac{2i\pi}{m}}$ sont constructibles. Montrons que si n et m sont premiers entre eux, alors ζ_{nm} est constructible.

Par le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $nu + mv = 1$. Alors

$$\zeta_{nm} = e^{\frac{2i\pi}{nm}} = e^{\frac{2i\pi}{nm}(nu+mv)} = e^{\frac{2i\pi mv}{n}} e^{\frac{2i\pi nu}{m}} = \zeta_m^v \zeta_n^u$$

D'où ζ_{nm} est constructible puisque l'ensemble des nombres constructibles est un corps stable par racine carrée.

Le théorème est ainsi démontré

□

Référence

Carrega, Jean-Claude (1989). *Théorie des corps. La règle et le compas.* Nouvelle édition. Editeurs des sciences et des arts.

Recasages

- Leçon 102 : Groupe des nombres complexes de module 1. Racines de l'unité. Applications.
- Leçon 104 : Groupes finis. Exemples et applications. (?)
- Leçon 108 : Exemples de parties génératrices d'un groupe. Applications.

- Leçon 121 : Nombres premiers. Applications. (insister sur importance de (Z/pZ)* cyclique)

- Leçon 125 : Extensions de corps. Exemples et applications.

- Leçon 127 : Exemples de nombres remarquables. Exemples d'anneaux de nombres remarquables. Applications.

- Leçon 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

- Leçon 144 : Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications. (?)

- Leçon 148 : Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications. (insister sur importance du degré d'une extension = dimension d'un Q-ev)

- Leçon 191 : Exemples d'utilisation de techniques d'algèbre en géométrie. (Donner à la fin des exemples de polygones constructibles et non constructibles)