## 2.15 Théorème de Gauss-Wantzel et polygônes constructibles à la règle et au compas (102, 125, 127, 191) [9]

La règle et le compas furent les outils principaux de construction de figures géométriques pour les grecs anciens. Ces outils permettaient de construire les figures simples les plus répandues : la droite et le cercle. Il était donc naturel d'utiliser ces instrument, mais l'influence de Platon, pour qui mesurer des longueurs et des angles ne pouvait permettre de construire les figures "parfaites" qui appartiennent au monde des idées, donnait d'autant plus de poids à l'utilisation de la règle et du compas seuls. Également, les grecs utilisaient beaucoup de figures pour accompagner leurs démonstrations : c'étaient en fait, une partie intégrante des démonstrations ! Enfin, la construction à la règle et au compas permettait d'étendre la notion de "nombres" que les grecs avaient à l'époque : ils comprenaient bien les entiers et les nombres rationnels, mais, depuis le théorème de Pythagore, un nouveau nombre a fait son apparition : un nombre dont le carré vaut 2. Ce nombre, qu'on a noté $\sqrt{2}$, ne pouvait s'écrire comme une fraction rationnelle ! Ainsi, les grecs ont pu étendre la notion de nombre à ces nombres que l'on pouvait construire à la règle et au compas.

À partir de là, les mathématiciens jusqu'au XIX$^{e}$ siècle ont étudié ces nombres constructibles à la règle et au compas, notamment pour répondre à 3 problèmes grecs sur la constructibilité à la règle et au compas :

1. peut-on construire un cube ayant le double du volume d'un cube fixé (duplication du cube),
2. peut-on construire, à partir d'un secteur angulaire donné, deux droites qui coupent ce secteur en 3 (trisection de l'angle),
3. peut-on constuire un carré dont l'aire est égale à l'aire d'un cercle donné (quadrature du cercle).

Ces trois problèmes peuvent en fait être reformulés ainsi, en terme de nombres constructibles :

1. $\sqrt[3]{2}$ est-il constructible à la règle et au compas,
2. A-t-on, pour tout $\theta \in \mathbb{R}$ tel que $\cos(\theta)$ soit constructible à la règle et au compas, que $\cos\left(\frac{\theta}{3}\right)$ est constructible à la règle et au compas,
3. $\sqrt{\pi}$ est-il constructible à la règle et au compas.

Répondre à ces problèmes fut un véritable casse-tête pendant près de 2000 ans. Une réponse a pu être donnée de manière définitive grâce au critère de Wantzel de constructibilité à la règle et au compas :

**Théorème 2.41** (Wantzel, 1837)**.** Un nombre $\alpha \in \mathbb{C}$ est constructible à la règle et au compas si, et seulement si, il existe une suite finie d'extensions $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n$ telle que :

1. $\forall i \in [\![1, n]\!], \quad [K_i : K_{i-1}] = 2,$
2. $\alpha \in K_n$.

En particulier, si $\alpha \in \mathbb{C}$ est constructible à la règle et au compas, alors le degré de l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est une puissance de 2.

Ce résultat, dont la démonstration n'est pas forcément compliquée mais assez pénible à écrire, se base sur le fait que l'ensemble des nombres constructibles à la règle et au compas est un corps stable par racine carrée, et sur le fait qu'un nombre constructible se construit à partir de points d'intersection de deux droites, d'une droite et d'un cercle, ou de deux cercles, formant alors des équations successives de degré 1 ou 2 pour le nombre $\alpha$. Ce théorème a donc permis de répondre, par la négative, aux trois problèmes ci-dessus :

1. $\sqrt[3]{2}$ est algébrique sur $\mathbb{Q}$, de degré 3 : son polynôme minimal est $X^3 - 2$. Ce n'est donc pas une puissance de 2 et $\sqrt[3]{2}$ n'est donc pas constructible à la règle et au compas.
2. La relation :

$$\cos(3\theta) = 4\cos(\theta)^3 - 3\cos(\theta)$$

donne donc que $\cos\left(\frac{\pi}{9}\right)$ est racine du polynôme $4X^3 - 3X - \frac{1}{2}$. On vérifie que ce polynôme est irréductible sur $\mathbb{Q}$ et donc que $\cos\left(\frac{\pi}{9}\right)$ est algébrique de degré 3 sur $\mathbb{Q}$. Il n'est donc pas constructible à la règle et au compas.

3. Si $\sqrt{\pi}$ était constructible à la règle et au compas, alors $\pi$ le serait aussi. Or, le théorème de Lindemann assure que $\pi$ est transcendant et donc il n'est pas constructible à la règle et au compas. Ainsi, $\sqrt{\pi}$ ne l'est pas non plus.

Ce résultat très fort de constructibilité permet de donner un critère de constructibilité à la règle et au compas des polygônes réguliers :

**Théorème 2.42** (Gauss, Wantzel)**.** Le nombre $e^{\frac{2i\pi}{n}}$ est constructible à la règle et au compas si, et seulement si, $n$ est une puissance de 2 ou $n$ s'écrit comme produit de facteurs premiers :

$$n = 2^\alpha p_1 \dots p_k, \quad \alpha \in \mathbb{N}.$$

avec $p_1, \dots, p_k$ des nombres premiers de Fermat, c'est-à-dire de la forme $2^{2^\beta} + 1$ avec $\beta \in \mathbb{N}$.

*Démonstration.* Considérons donc le nombre $e^{\frac{2i\pi}{n}}$. Écrivons le dénominateur $n$ en produit de facteurs premiers $2^\alpha p_1^{\alpha_1} \dots p_k^{\alpha_k}$. On va se ramener à étudier chaque facteur premier séparément.

**Étape 1 : Séparer les facteurs premiers**

Pour cela, on montre que, si $n_1$ et $n_2$ sont deux entiers premiers entre eux, alors $e^{\frac{2i\pi}{n_1 n_2}}$ est constructible à la règle et au compas si et seulement si $e^{\frac{2i\pi}{n_1}}$ et $e^{\frac{2i\pi}{n_2}}$ sont tous deux constructibles à la règle et au compas. Pour cela, on utilise le fait que l'ensemble des nombres constructibles à la règle et au compas forme un corps. Ainsi, si $e^{\frac{2i\pi}{n_1 n_2}}$ est constructible à la règle et au compas, alors :

$$e^{\frac{2i\pi}{n_1}} = \left(e^{\frac{2i\pi}{n_1 n_2}}\right)^{n_2} \quad \text{et} \quad e^{\frac{2i\pi}{n_2}} = \left(e^{\frac{2i\pi}{n_1 n_2}}\right)^{n_1}$$

sont constructibles à la règle et au compas. Réciproquement, supposons que $e^{\frac{2i\pi}{n_1}}$ et $e^{\frac{2i\pi}{n_2}}$ soient constructibles à la règle et au compas. Étant donné que $n_1$ et $n_2$ sont premiers entre eux, on a une relation de Bézout :

$$\exists u, v \in \mathbb{Z}, \quad u n_1 + v n_2 = 1.$$

Ainsi, on a :

$$\left(e^{\frac{2i\pi}{n_1}}\right)^v \left(e^{\frac{2i\pi}{n_2}}\right)^u = e^{\frac{2i\pi}{n_1 n_2}}$$

qui est donc constructible à la règle et au compas. On a donc que $e^{\frac{2i\pi}{n}}$ est constructible à la règle et au compas si et seulement si :

$$e^{\frac{2i\pi}{2^\alpha}} \quad \text{et} \quad e^{\frac{2i\pi}{p_j^{\alpha_j}}}, \ j \in [\![1, k]\!]$$

sont constructibles à la règle et au compas. On est donc ramené à caractériser les nombres premiers $p$ et les entiers $\beta \in \mathbb{N}$ tels que $e^{\frac{2i\pi}{p^\beta}}$ est constructible à la règle et au compas.

**Étape 2 : $e^{\frac{2i\pi}{2^\alpha}}$ est constructible**

Cela se voit sans soucis par récurrence sur $\alpha$ : on extrait successivement une racine carrée de 1, qui est constructible (il s'agit de l'un des points de base de constructibilité). Plus géométriquement, cela revient à construire successivement des bissectrices de l'angle $2\pi$.

**Étape 3 : Le cas des nombres premiers impairs**

Jusqu'ici, nous avons raisonné par équivalence. Il ne nous reste plus qu'à montrer que, si $p \geqslant 3$ est un nombre

premier, alors $e^{\frac{2i\pi}{p^\alpha}}$ est constructible à la règle et au compas si et seulement si $\alpha = 1$ et $p$ est un nombre premier de Fermat.
$\Rightarrow$ : Supposons $\omega := e^{\frac{2i\pi}{p^\alpha}}$ constructible à la règle et au compas. On utilise alors le fait que le polynôme minimal de cet élément est le polynôme cyclotomique $\Phi_{p^\alpha}$ qui est de degré $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$. Or, d'après le théorème de Wantzel, on doit avoir :

$$\exists m \in \mathbb{N}, \quad p^{\alpha-1}(p-1) = [\mathbb{Q}(\omega) : \mathbb{Q}] = 2^m.$$

Par unicité de la décomposition en produit de facteurs premiers, on a donc $\alpha = 1$ et donc $p = 1 + 2^m$ pour un certain $m \in \mathbb{N}$. Montrons que $m$ doit nécessairement être une puissance de 2. On écrit alors $m = 2^\beta m'$ avec $m'$ impair, de sorte que :

$$p = 1 + \left(2^{2^\beta}\right)^{m'}.$$

Or, on a la factorisation :

$$1 + X^{m'} = (1+X)\sum_{k=0}^{m'-1}(-X)^k,$$

de sorte que $1 + 2^{2^\beta}$ divise $p$. Ainsi, par primalité de $p$, on a donc $p = 1 + 2^{2^\beta}$. $p$ est donc un nombre premier de Fermat ! Ce sens de l'équivalence est dû à Wantzel, mais la réciproque est due à Gauss, qui l'a donc montré sans le théorème de Wantzel, ce que nous ne ferons pas ici.
$\Leftarrow$ : Soit $p$ un nombre premier de Fermat. Il s'écrit alors $1+2^m$. Montrons que le nombre $\omega := e^{\frac{2i\pi}{p}}$ est constructible à la règle et au compas. Pour cela, on va utiliser le théorème de Wantzel et la "correspondance de Galois" (c'est le terme savant mais on remontre tout à la main, ne vous inquiétez pas !). La clef est de considérer le corps $K := \mathbb{Q}(\alpha)$ et ses automorphismes. Notons $G := \mathrm{Aut}(K)$ le groupe des automorphismes de corps de $K$ et décrivons ses éléments :

**Étape 4 : $G$ est isomorphe au groupe $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$**

Soit $\sigma \in G$. Étant donné que $\sigma$ fixe $\mathbb{Q}$ (car $\sigma(1)$ doit être égal à 1 et est additif), on a que :

$$0 = \sigma(0) = \sigma\left(\Phi_p(\omega)\right) = \Phi_p\left(\sigma(\omega)\right).$$

Ainsi, $\sigma(\omega)$ est une racine de $\Phi_p$. $p$ étant premier, les racines primitives $p$-ièmes de l'unité sont les $\omega^k$ pour $k \in [\![1, p-1]\!]$. Ainsi, il existe un (unique) entier $k_\sigma \in [\![1, p-1]\!]$ tel que :

$$\sigma(\omega) = \omega^{k_\sigma}.$$

L'application :

$$\begin{array}{rccc} \psi & : & G & \longrightarrow & \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \\ & & \sigma & \longmapsto & \overline{k_\sigma} \end{array}$$

est alors bien définie et est injective. En effet, si $\sigma, \sigma' \in G$ sont tels que $k_\sigma \equiv k_{\sigma'}\ [p]$, alors :

$$\sigma(\omega) = \omega^{k_\sigma} = \omega^{k_{\sigma'}} = \sigma'(\omega)$$

étant donné que $\omega^p = 1$. Ainsi, $\sigma$ et $\sigma'$ sont deux morphismes de corps, ils coïncident donc sur $\mathbb{Q}$ et de plus, ils coïncident sur $\omega$. Ainsi, ils coïncident sur le corps engendré par $\omega$ qui est $\mathbb{Q}(\omega) = K$ ! Ainsi, $\sigma = \sigma'$. L'application $\psi$ est également surjective. En effet, si $k \in [\![1, p-1]\!]$, alors l'application :

$$\begin{array}{rcl} \mathbb{Q}[X] & \longrightarrow & K \\ a \in \mathbb{Q} & \longmapsto & a \\ X & \longmapsto & \omega^k \end{array}$$

est bien définie et passe au quotient en un morphisme de corps :

$$\begin{array}{ccc} \frac{\mathbb{Q}[X]}{(\Phi_p)} & \longrightarrow & K \\ \overline{X} & \longmapsto & \omega^k. \end{array}$$

Ainsi, en composant par un isomorphisme entre $K$ et $\frac{\mathbb{Q}[X]}{(\Phi_p)}$ envoyant $\overline{X}$ sur $\omega$, on a donc l'existence d'un morphisme de corps $\sigma : K \longrightarrow K$ tel que $\sigma(\omega) = \omega^k$. Il s'agit bien d'un automorphisme de $K$ car l'image de $\sigma$ est un corps contenant $\omega^k$, et donc $\omega$ car $k$ et $p$ sont premiers entre eux et on a donc une relation de Bézout :

$$uk + vp = 1$$

donnant :

$$\left(\omega^k\right)^u = \omega^{1-vp} = \omega.$$

Ainsi, l'image de $\sigma$ est bien $K$. Ainsi, $\psi$ est bijective et il s'agit bien d'un morphisme de groupes. Ainsi, $G$, comme $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ est cyclique, d'ordre $p-1 = 2^m$. Soit $\sigma_0 \in G$ un générateur de $G$. On a alors que la famille $\mathscr{B}' := \left(\sigma_0^i(\omega)\right)_{i\in[\![0,p-2]\!]}$ est une base de l'extension $K/\mathbb{Q}$. En effet, les $\sigma_0^i(\omega)$ sont de la forme $\omega^{k_i}$ et les $k_i$ sont tous distincts. Ainsi, il s'agit de la famille $(\omega, \ldots, \omega^{p-1})$ qui est bien une base de $K$.

**Étape 5 : Construction de la tour d'extensions.**

À partir de là, on veut pouvoir construire des extensions successives de degré 2 $K_0 = \mathbb{Q} \subset K_1 \subset \ldots \subset K_\ell = K$. La lectrice habituée à la théorie de Galois connaît la marche à suivre ! Détaillons-la. Étant donné que $G$ est d'ordre $2^m$, on peut considérer les sous-groupes $G_i$ de $G$ engendrés par $\sigma_0^{2^i}$, pour $i \in [\![0, m]\!]$. Ce sont des sous-groupes d'ordre $2^{n-i}$ et ces sous-groupes se contiennent successivement :

$$G = G_0 \supset G_1 \supset \ldots \supset G_m = \{\mathrm{id}_K\}.$$

À partir de cette suite de sous-groupes, construisons une suite de sous-corps : soit $K_i$ défini ainsi :

$$K_i := \{z \in K \mid \forall \sigma \in G_i, \quad \sigma(z) = z\}.$$

On a, du fait que $G$ est engendré par $\sigma_0^{2^i}$, que :

$$K_i = \left\{z \in K \;\middle|\; \sigma_0^{2^i}(z) = z\right\}.$$

Cette description de $K_i$ montre facilement qu'il s'agit d'un sous-corps de $K$ et la première description montre qu'on a :

$$K_0 \subset K_1 \subset \ldots \subset K_m = K.$$

Montrons alors que $K_0 = \mathbb{Q}$ et que les inclusions $K_i \subset K_{i+1}$ sont strictes. On a bien sûr $\mathbb{Q} \subset K_0$. Prenons donc $z \in K_0$. En l'écrivant dans la base $\mathscr{B}'$, on a :

$$z = \sum_{i=0}^{p-2} \lambda_i \sigma_0^i(\omega).$$

Ainsi, l'égalité $\sigma_0(z) = z$ donne :

$$\sum_{i=0}^{p-2} \lambda_i \sigma_0^i(\omega) = \sum_{i=1}^{p-2} \lambda_{i-1} \sigma_0^i(\omega) + \lambda_{p-2}\omega.$$

Ainsi, en identifiant les deux écritures, on a :

$$\lambda_0 = \ldots = \lambda_{p-2}.$$

D'où :

$$z = \lambda_0 \sum_{i=0}^{p-2} \sigma_0^i(\omega) = \lambda_0 \sum_{i=1}^{p-1} \omega^i = -\lambda_0 \in \mathbb{Q},$$

car $\omega$ est racine de $\Phi_p = \sum_{i=0}^{p-1} X^i$. Enfin, pour montrer que $K_i \neq K_{i+1}$, il suffit de considérer le nombre :

$$z = \sum_{h=0}^{2^{n-i-1}-1} \sigma_0^{2^{i+1}h}(\omega).$$

On a bien $z \in K_{i+1}$ car :

$$\sigma_0^{2^{i+1}}(z) = \sum_{h=1}^{2^{n-i-1}} \sigma_0^{2^{i+1}h}(\omega) = z$$

étant donné que $\sigma_0^{2^m} = \mathrm{id}_K$, et on a bien que $\sigma_0^{2^i}(z) \neq z$ en l'écrivant dans la base $\mathscr{B}'$. On a donc :

$$2^m = p - 1 = [\mathbb{Q}(\omega) : \mathbb{Q}] = \prod_{i=1}^{m} [K_i : K_{i-1}]$$

par multiplicativité des degrés. Il y a $m$ termes dans ce produit et ces termes sont tous supérieurs ou égaux à 2 étant donné que les inclusions sont strictes. Ainsi, on a bien que les extensions successives sont de degré 2 ! Ainsi, par le théorème de Wantzel, on a que $e^{\frac{2i\pi}{p}}$ est constructible. Cela termine donc cette belle démonstration ! □

**Remarque 2.15.1** (Cékoi du coup la correspondance de Galois ? Et quels sont les résultats sur lesquels il faut être solide pour ce développement ?)**.** *J'ai dit dans la preuve qu'on allait utiliser la "correspondance de Galois". Mais qu'es aquo ? En fait, si on a une extension finie $L/K$ galoisienne, c'est-à-dire que tout élément de $L$ a son polynôme minimal sur $K$ scindé et à racines simples dans $L$, on a une correspondance entre les sous-groupes normaux $H$ d'indice $m$ du groupe $G$ des automorphismes de $L$ fixant $K$ et les extensions intermédiaires $M$ de $K$ de degré $m$ :*

$$\begin{array}{rcl} \{H \lhd G \mid [G:H] = m\} & \longrightarrow & \{K \subset M \subset L \mid [M:K] = m\} \\ H & \longmapsto & L^H := \{x \in L \mid \forall \sigma \in H, \quad \sigma(x) = x\} \\ \mathrm{Gal}(L/M) := \{\sigma \in G \mid \sigma_{|M} = \mathrm{id}_M\} & \longleftarrow & M. \end{array}$$

*D'où l'idée, à partir des sous-groupes $G_i$ de la preuve, de considérer les extensions $K_i$ qui sont fixes par les éléments de $G_i$ ! La connaissance de la correspondance de Galois est un vrai plus pour avoir du recul sur la démonstration de ce résultat, mais n'est pas nécessaire en soi. En revanche, il faut être très solide sur les résultats suivants :*

- *Pour tout $n \in \mathbb{N}^*$, le polynôme cyclotomique $\Phi_n$ est à coefficients dans $\mathbb{Z}$, et il est irréductible dans $\mathbb{Q}[X]$ (et aussi dans $\mathbb{Z}[X]$).*
- *Les corps de rupture : comment on les construit, comment définir facilement des morphismes de corps en fixant l'image du générateur, éventuellement le lien entre les morphismes de corps $\sigma : K(\alpha) \longrightarrow \mathbb{C}$ prolongeant un morphisme fixé $\sigma_0 : K \longrightarrow \mathbb{C}$ et les racines du polynôme minimal $\pi_\alpha$.*
- *Le fait que les nombres constructibles forment un corps stable par racine carrée ! C'est un ingrédient central de la preuve ! La stabilité par somme ou différence se fait facilement, et la stabilité par produit et par inverse utilise le théorème de Thalès.*

*Vous trouverez ces résultats dans le Perrin ([26]), le Gozard ([21]) et le Carréga, qui est la référence de ce développement ([9]).*