# Théorème de Gauss-Wantzel :

## I Le développement

Le but de ce développement est de trouver une condition nécessaire et suffisante sur l'entier $n$ pour que le $n$-gone régulier soit constructible à la règle non graduée et au compas.

**Théorème 1 : Théorème de Gauss-Wantzel [Berhuy, p.795] :**
Soit $n$ un entier naturel supérieur ou égal à 2.

Le $n$-gone régulier est constructible à la règle non graduée et au compas si, et seulement si, $n$ s'écrit sous la forme $2^s \prod_{i=1}^{r} p_i$ avec $s, r \in \mathbb{N}$ et $p_1, ..., p_r$ des nombres premiers de Fermat distincts.

**Preuve :**
Soit $n$ un entier naturel supérieur ou égal à 2.

Le $n$-gone régulier est constructible si, et seulement si, $\zeta_n = e^{\frac{2i\pi}{n}}$ est constructible (car $\zeta_n$ est une racine primitive de l'unité donc engendre $\mathbb{U}_n$). Or, le polynôme minimal de $\zeta_n$ sur $\mathbb{Q}$ est $\Phi_n$ et son corps de décomposition est $\mathbb{Q}(\zeta_n)$ (car $\zeta_n$ est une racine primitive de l'unité), donc $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(\Phi_n) = \varphi(n)$. Ainsi, le $n$-gone régulier est constructible si, et seulement si, $\varphi(n)$ est une puissance de 2.

— Si $n$ est de la forme $2^s \prod_{i=1}^{r} p_i$ (avec $r, s \in \mathbb{N}$ et $p_1, ..., p_r$ des nombres premiers de Fermat distincts), on a :

$$\varphi(n) = \begin{cases} \prod_{i=1}^{r} (p_i - 1) & \text{si } s = 0 \\ 2^{s-1} \prod_{i=1}^{r} (p_i - 1) & \text{si } s > 0 \end{cases}$$

Ainsi, $\varphi(n)$ est une puissance de 2 puisque chaque $p_i$ est un nombre de Fermat (c'est-à-dire de la forme $2^{2^{k_i}} + 1$).

— Réciproquement, supposons que $\varphi(n)$ est une puissance de 2.

Posons $n = \prod_{i=1}^{s} q_i^{a_i}$ (décomposition en facteurs premiers). On a alors :

$$\varphi(n) = n \prod_{i=1}^{s} \left(1 - \frac{1}{q_i}\right) = \prod_{i=1}^{s} (q_i - 1) q_i^{a_i - 1}$$

Si $q_i$ est un nombre premier impair, alors on a $a_i = 1$ puisque $\varphi(n)$ est une puissance de 2 (donc pas de facteurs premiers impairs dans sa décomposition) et on a aussi que $q_i - 1$ est une puissance de 2 (car divise $\varphi(n)$). Or, si $q_i$ est un nombre premier de la forme $2^k + 1$, alors $k$ est une puissance de 2.

En effet, écrivons $k = a2^b$ (décomposition en facteurs premiers) et notons $c = 2^{2^b}$. On a alors :

$$q_i = 2^k + 1 = c^a + 1 \underset{a \text{ imp.}}{=} c^a - (-1)^a = (c+1) \sum_{i=0}^{a-1} (-1)^i c^i$$

Ainsi, $c + 1$ divise $q_i$ (qui est un nombre premier) et $c + 1$ est strictement plus grand que 1, donc $2^k + 1 = c + 1$ et ainsi $k = 2^b$.

On a donc montré que $n$ n'écrit comme un produit d'une puissance de 2 (potentiellement égale à 1) et de nombres premiers de Fermat distincts dont l'exposant est égal à 1.

On a ainsi démontré le théorème par double implication.

■

Nous allons désormais construire le 5-gone régulier en guise d'exemple :

**Exemple 2 : [Berhuy, p.805]**
Montrons tout d'abord que $\cos\left(\frac{2\pi}{5}\right) = \frac{\sqrt{5}-1}{4}$ :
On sait que, $\zeta_5$ et $\zeta_5^{-1}$ sont conjugués, donc :

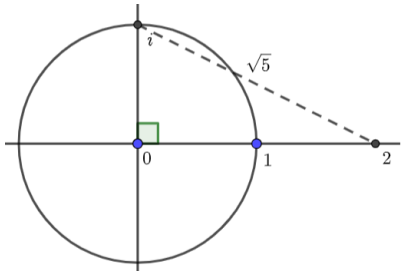
$$\begin{cases} \zeta_5 + \zeta_5^{-1} = \alpha = 2\,\mathrm{Re}(\zeta_5) \\ \zeta_5 \zeta_5^{-1} = 1 \end{cases}$$

De plus, on a $\zeta_5^2 + \zeta_5^{-2} + \zeta_5 + \zeta_5^{-1} + 1 = 0$. Or, $\alpha^2 = \zeta_5^2 + \zeta_5^{-2} + 2$, donc : $\alpha^2 + \alpha - 1 = 0$.

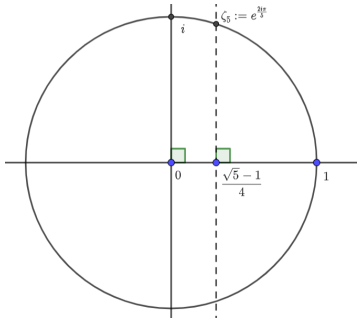
Ainsi, $\alpha = \dfrac{\sqrt{5}-1}{2}$ (puisque $\mathrm{Re}(\zeta_5) > 0$) et donc $\cos\left(\frac{2\pi}{5}\right) = \frac{\alpha}{2} = \frac{\sqrt{5}-1}{4}$.

Commençons la construction du 5-gone régulier :

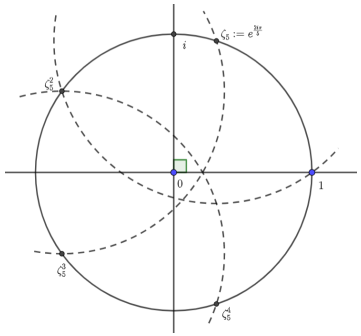
On commence avec les points 0 et 1, et on trace l'axe des réels. On construit ensuite l'axe des imaginaires purs (perpendiculaire de l'axe des réels passant par 0) ainsi que les nombres $i$ et 2 (respectivement en tant qu'intersection entre l'axe des imaginaires purs et du cercle de centre 0 et de rayon 1 et entre l'axe des réels et du cercle de centre 1 et de rayon 1). On peut alors tracer le segment joignant $i$ et 2 dont la longueur est $\sqrt{5}$ par le théorème de Pythagore et que l'on peut placer sur l'axe des réels en tant qu'intersection entre le cercle de centre 0 et de rayon $\sqrt{5}$ et l'axe des réels.




On peut ensuite construire $\frac{\sqrt{5}-1}{2}$ en tant que milieu du segment $[0;\sqrt{5}-1]$ puis enfin construire $\frac{\sqrt{5}-1}{4}$ en tant que milieu du segment $\left[0;\frac{\sqrt{5}-1}{2}\right]$. On obtient ainsi $\zeta_5$ en tant qu'intersection entre le cercle de centre 0 et de rayon 1 et la perpendiculaire de l'axe des réels et passant par $\frac{\sqrt{5}-1}{4}$.




On construit finalement le 5-gone régulier en reportant la longueur entre $\zeta_5$ et 1 sur le cercle unité.




# II Remarques sur le développement

## II.1 Résultat(s) utilisé(s)

Ici, chaque construction commencera de 0 et 1. Durant la construction, nous utiliserons seulement les règles suivantes :
$C1(\alpha,\beta)$ : De $\alpha \neq \beta$, on peut tracer la ligne $l$ qui passe par $\alpha$ et $\beta$.
$C2(\gamma,\alpha,\beta)$ : De $\alpha \neq \beta$ et $\gamma$, on peut dessiner le cercle $C$ de centre $\gamma$ dont le rayon est la distance entre $\alpha$ et $\beta$.
$P1$ : Le(s) point(s) d'intersection de deux lignes distinctes $\ell_1$ and $\ell_2$ construits comme ci-dessus.
$P2$ : Le(s) point(s) d'intersection d'une ligne $\ell$ et d'un cercle $C$ construits comme ci-dessus.
$P3$ : Le(s) point(s) d'intersection de deux cercles distincts $C_1$ and $C_2$ construits comme ci-dessus.

On rappelle également ce qu'est un nombre de Fermat :

**Définition 3 : Nombre de Fermat :**
Un nombre $m$ est appelé **nombre de Fermat** lorsqu'il peut s'écrire sous la forme $m = 2^{2^n}+1,\ n \in \mathbb{N}$.

Il vient alors la question : Quand $F_n := 2^{2^n}+1$ est-il un nombre premier ?
En 1640, Pierre de Fermat remarqua que $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ et $F_4 = 65537$ sont tous des nombres premiers. Il conjectura donc que tous les $F_n$ sont des nombres premiers, mais cette conjecture fût réfutée par Euler en 1732. Les seuls nombres premiers de Fermat connus sont ceux trouvés par Fermat lui-même.

Dans la démonstration du développement, nous avons utilisé de manière cruciale le résultat suivant :

**Théorème 4 : [Berhuy, p.929]**
Soient $\alpha \in \mathbb{C}$ algébrique sur $\mathbb{Q}$ et $\mathbb{L}$ le corps de décomposition du polynôme minimal de $\alpha$ sur $\mathbb{Q}$.
$\alpha$ est constructible si, et seulement si, $[\mathbb{L}:\mathbb{Q}]$ est une puissance de 2.

Ce résultat est très puissant mais est assez difficile à démontrer : il faut utiliser le fait que l'extension est galoisienne pour en déduire que le groupe de Galois est un 2-groupe pour en déduire qu'il est résoluble (les $p$-groupes le sont de manière générale) puis conclure avec la correspondance de Galois. Pour la réciproque, il faut utiliser la clôture galoisienne pour montrer que l'extension $\mathcal{C}/\mathbb{Q}$ est normale (avec $\mathcal{C}$ le corps des nombres constructibles à la règle non graduée et au compas) pour conclure grâce au théorème de l'élément primitif.

### II.2 Recasages

Recasages : 127 - 191.

## III Bibliographie

— Grégory Berhuy, *Algèbre : le grand combat*.