Développement : Théorème de GAUSS pour les polygones constructibles

ALGÈBRE & GÉOMÉTRIE

Référence : [BER] BERHUY G., *Algèbre : le grand combat*, Calvage & Mounet, 2018, p796.

Pour les leçons :
- 102 : Groupe des nombres complexes de module 1. Racines de l'unité. Applications.
- 104 : Groupes finis. Exemples et applications.
- 121 : Nombres premiers. Applications.
- 125 : Corps finis. Applications.
- 127 : Exemples de nombres remarquables. Exemples d'anneaux de nombres remarquables. Applications.
rupture. Exemples et applications.
- 148 : Dimension d'un espace vectoriel de dimension finie. Exemples et applications.
endomorphisme en dimension finie. Applications.
- 191 : Exemples d'utilisation de techniques d'algèbre en géométrie.

Si $n \in \mathbb{N}$, on pose $\omega_n = e^{\frac{2i\pi}{n}}$, et on suppose connu (à mettre dans le plan dans tous les cas) que le n-gone régulier est constructible si, et seulement si ω_n est constructible, ainsi que d'autres résultats qui seront utilisés dans le développement et que vous pourrez retrouver dans la référence (y compris le critère de WANTZEL).
On rappelle la définition suivante :

Définition 1.

Soit $m \in \mathbb{N}$. On appelle *m-ième nombre de* FERMAT l'entier $F_m = 1 + 2^{2^m}$. On dit en outre qu'un entier $n \in \mathbb{N}$ est *un nombre de* FERMAT s'il s'écrit $n = F_m$ pour un entier $m \in \mathbb{N}$.

On note $\mathbb{P}$ l'ensemble des nombres premiers.

Lemme 2.

Soient $m, n \geqslant 2$ des entiers premiers entre eux. Alors, ω_{nm} est constructible si, et seulement si ω_n et ω_m sont constructibles.

PREUVE : Si ω_{nm} est constructible, alors $\omega_n = \omega_{nm}^m$ et $\omega_m = \omega_{n,m}^n$ sont directement constructibles. Il s'agit donc de démontrer l'implication réciproque.
Supposons ω_n et ω_m constructibles. Comme $n \wedge m = 1$, d'après le théorème de BÉZOUT :

$$\exists (u, v) \in \mathbb{Z}^2 \quad nu + mv = 1.$$

Donc :

$$\begin{aligned} \omega_{nm} &= \omega_{nm}^{an+bm} \\ &= (\omega_{nm}^n)^a (\omega_{nm}^m)^b \\ &= \omega_m^a \omega_n^b, \end{aligned}$$

et ω_{nm} est constructible par produit de nombres constructibles. □

Lemme 3.

Pour tout $\alpha \in \mathbb{N}^*$, ω_{2^α} est constructible.

PREUVE : C'est une récurrence facile : si $\alpha = 0$, $\omega_1 = 1$ est constructible, et si ω_{2^α} est constructible, alors construire $\omega_{2^{\alpha+1}} = (\omega_{2^\alpha})^{1/2}$ revient à construire la bissectrice de l'angle $\dfrac{2\pi}{2^\alpha}$, ce qui est possible à la règle et au compas. La preuve peut donc être dite à l'oral sans être écrite au tableau. □

Théorème 4. ***Théorème de GAUSS pour les polygones constructibles.***

Soit $n \geqslant 2$ entier. Alors, le n-gone régulier est constructible si, et seulement si n est le produit d'une puissance de 2 et de nombres de FERMAT premiers deux à deux distincts.

PREUVE : Le n-gone régulier est constructible si, et seulement si ω_n est constructible.
D'après les lemmes précédents, cela revient à montrer que pour tout $p \in \mathbb{P}$ impair et $\alpha \in \mathbb{N}^*$, ω_{p^α} est constructible si, et seulement si $\alpha = 1$ et p est un nombre de FERMAT. En effet, le lemme 2 donne le fait que, en notant $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

la décomposition en facteurs premiers de n, ω_n est constructible si, et seulement si tous les $\omega_{p_i^{\alpha_i}}$ sont constructibles. Si l'un des p_i est pair (i.e. $p = 2$), il est immédiatement constructible par le lemme précédent.

Soient donc $p \in \mathbb{P}$ impair et $\alpha \in \mathbb{N}^*$.
$\boxed{\Longrightarrow}$ Supposons ω_{p^α} constructible. C'est une racine primitive de l'unité, donc son polynôme minimal dans $\mathbb{Q}[X]$ est le p^α-ième polynôme cyclotomique Φ_{p^α}, de degré $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$. Ainsi :

$$[\mathbb{Q}(\omega_{p^\alpha}) : \mathbb{Q}] = \deg(\Phi_{p^\alpha}) = p^{\alpha-1}(p-1).$$

Si $\alpha \neq 1$, $p^{\alpha-1}$ est impair, donc ω_{p^α} a un degré qui n'est pas une puissance de 2. D'après le critère de Wantzel, ω_{p^α} n'est pas constructible dans ce cas, ce qui n'est pas possible par hypothèse.
Si $\alpha = 1$, alors ω_{p^α} est de degré $p-1$, qui est alors une puissance de 2 par le critère de Wantzel (car il est constructible). Donc $p - 1 = 2^n$ avec $n \in \mathbb{N}$.
Montrons que n est encore une puissance de 2. Écrivons $n = a2^b$, avec $a \in \mathbb{N}^*$ impair et $b \in \mathbb{N}$. Posons $c = 2^{2^b}$. Alors :

$$\begin{aligned} p &= 2^n + 1 \\ &= 2^{a2^b} + 1 \\ &= c^a + 1 \\ &= (c+1)\sum_{k=0}^{a-1} c^k (-1)^{a-1-k}. \end{aligned}$$

Donc $p \in \mathbb{P}$ est divisible par $c + 1$, et donc $c + 1 = p$. Donc p est un nombre premier de Fermat.
$\boxed{\Longleftarrow}$ Supposons $\alpha = 1$ et $p = 1 + 2^n$ un nombre premier de Fermat.
$\star$ Soit $G = \mathrm{Aut}(\mathbb{Q}(\omega_p)/\mathbb{Q})$ le groupe des automorphismes de $\mathbb{Q}(\omega_p)$ induisant l'identité sur $\mathbb{Q}$.
Comme $p \in \mathbb{P}$, $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p - 1$. Il en est donc de même de G.
Soit ρ un générateur de G. Pour $i \in [\![0; n]\!]$, on pose $G_i = \langle \rho^{2^i} \rangle$, et $L_i = \mathbb{Q}(\omega_p)^{G_i} \subset \mathbb{Q}(\omega_p)$ l'ensemble des éléments de $\mathbb{Q}(\omega_p)$ fixés par tout élément de G_i.
On remarque que :

$$\{\mathrm{Id}\} = G_n \subset G_{n-1} \subset \cdots \subset G_0 = G.$$

Donc :

$$L_0 \subset \cdots \subset L_n = \mathbb{Q}(\omega_p).$$

Chaque élément de G est déterminé de façon unique par l'image de ω_p par lui, avec ω_p qui est une racine primitive p-ième de l'unité. Ainsi, $\omega_p, \rho(\omega_p), \ldots, \rho^{p-2}(\omega_p)$ sont les $p - 1$ puissances non triviales de ω_p, et ils forment en outre une famille $\mathbb{Q}$-libre, donc une $\mathbb{Q}$-base, de $\mathbb{Q}(\omega_p)$ (qui est de dimension $\varphi(p) = p - 1$).
$\star$ Montrons que $L_0 = \mathbb{Q}$.
Maintenant, soit $z \in L_0 = \mathbb{Q}(\omega_p)^G$. On écrit $z = a_0\omega_p + \cdots + a_{2p-2}\rho^{p-2}(\omega_p)$, avec les $a_i \in \mathbb{Q}$. Comme $z \in L_0$ et $\rho^{p-1} = \mathrm{Id}$, on a :

$$z = \rho(z) = a_0\rho(\omega_p) + \cdots + a_{2p-2}\omega_p.$$

Comme $\omega_p, \rho(\omega_p), \ldots, \rho^{p-2}(\omega_p)$ est $\mathbb{Q}$-libre, on en déduit que $a_0 = \cdots = a_{p-2}$, ce qui prouve que :

$$z = a_0 \left(\sum_{k=0}^{p-2} \omega_k \right) = -a_0 \in \mathbb{Q}.$$

Donc $L_0 \subset \mathbb{Q}$, i.e. $L_0 = \mathbb{Q}$.
$\star$ Soit $i \in [\![1; n]\!]$. Montrons que $[L_i : L_{i-1}] = 2$ et que, en posant $\alpha_i = \displaystyle\sum_{k=0}^{2^{n-i}-1} \rho^{2^i k}(\omega_p)$, on a :

$$L_i = L_{i-1}(\alpha_i).$$

On a :

$$\begin{aligned} \rho^{2^i}(\alpha_i) &= \sum_{k=0}^{2^{n-i}-1} \rho^{2^i(k+1)}(\omega_p) \\ &= \sum_{k=1}^{2^{n-i}} \rho^{2^i k}(\omega_p) \\ &= \sum_{k=1}^{2^{n-i}-1} \rho^{2^i k}(\omega_p) + \rho^{2^n}(\omega_p). \end{aligned}$$

Comme $p = 1 + 2^n$, $\rho^{2^n} = \rho^{p-1} = \mathrm{Id}$ et donc $\rho^{2^i}(\omega_p) = \omega_p$. Ainsi, comme $G_i = \langle \rho^{2^i} \rangle$, α_i est fixé par tout élément de G_i, et donc $\alpha_i \in L_i$. En outre, en repartant de la définition de α_i,

$$\rho^{2^{i-1}}(\alpha_i) = \sum_{k=0}^{2^{n-i}-1} \rho^{2^i k + 2^{i-1}}(\omega_p).$$

Or, en regardant chaque puissance de ρ dans la somme, pour $k \in [\![0; 2^{n-i} - 1]\!]$:

$$1 \leqslant 2^{i-1} \leqslant 2^i k + 2^{i-1} \leqslant 2^n - 2^{i-1} = p - 1 - 2^{i-1} \leqslant p - 2.$$

Par conséquent, il n'y a aucune puissance de ρ égale à 0 ou à $p-1$, et ω_p n'apparaît donc pas dans l'écriture dans la $\mathbb{Q}$-base $\omega_p, \rho(\omega_p), \ldots, \rho^{p-2}(\omega_p)$ de $\rho^{2^{i-1}}(\alpha_i)$, contrairement au terme $k = 0$ dans α_i. Par unicité de l'écriture dans cette $\mathbb{Q}$-base, $\rho^{2^{i-1}}(\alpha_i) \neq \alpha_i$, ce qui prouve que $\alpha_i \notin L_{i-1}$.
Par conséquent, $[L_i : L_{i-1}] \geqslant 2$. D'autre part,

$$\prod_{i=0}^{n-1} [L_{i+1} : L_i] = [L_n : L_0] = [\mathbb{Q}(\omega_p) : \mathbb{Q}] = p - 1 = 2^n.$$

Donc :

$$\forall i \in [\![1; n]\!] \quad [L_i : L_{i-1}] = 2.$$

Enfin, $\alpha_i \in L_i \backslash L_{i-1}$, la famille $(1, \alpha_i)$ est L_{i-1}-libre dans L_i, c'en est donc une base de L_i.
En particulier, $L_i = L_{i-1}(\alpha_i)$.
$\star$ En résumé, $\mathbb{Q}(\omega_p)/\mathbb{Q}$ est une extension 2-décomposable de $\mathbb{Q}$.
On en conclut que ω_p est constructible. $\square$

Remarque 5.

Ce développement est très long, donc il faut choisir le jour de l'oral ce sur quoi on mettra l'accent. Il y a des passages qu'on pourra toujours passer dans un premier temps, mais avec ce document, normalement, il y a de quoi à peu près tout comprendre de ce développement (enfin, peut-être regarder la preuve du critère de Wantzel, mais c'est dans la référence de toute façon).

Et aussi, si on prend ce développement, il faut pouvoir construire à la règle et au compas certains nombres constructibles, et être un peu à l'aise avec ça. Cela est expliqué dans la référence, mais l'application mobile *Euclidea* permet de s'entraîner à le faire aussi.