Théorème de Gauss-Wantzel

Leçons concernées

* **102 :** Groupe des nombres complexe de module 1. Sous-groupes des racines de l'unité. Applications.
* **125 :** Extensions de corps. Exemples et applications.
* **144 :** Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.
* **151 :** Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.
* **191 :** Exemples d'utilisation des techniques d'algèbre en géométrie.

Réference

* *Carrega - Théorie des corps*

Théorème. *Soit p un nombre premier impair. Soit $a \in \mathbb{N}^*$. Alors le polygone régulier à p^a côtés est constructible si et seulement si $a = 1$ et s'il existe $n \in \mathbb{N}$ tel que $p = 2^n + 1$ (nombre premier de Fermat).*

La preuve sera évidemment basée sur une double implication.

Sens direct : Commençons par le sens le plus simple. Soit p un nombre premier impair, et soit $\omega = e^{\frac{2i\pi}{p^a}}$. Son polynôme minimal sur $\mathbb{Q}$ est Φ_{p^a}, le p^a-ème polynôme cyclotomique. Ce faisant, $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(p^a) = p^{a-1}(p-1)$. Mais d'après le corollaire de Wantzel, puisque nous avons supposé ω constructible, il existe un entier $n \in \mathbb{N}$ tel que $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2^n$. Donc p est tel que $p^{a-1}(p-1) = 2^n$. p étant supposé impair, le terme de gauche ne peut être pair que si $a = 1$. Donc $a = 1$ et $p = 2^n + 1$.

Sens réciproque : Le plus difficile ! Soit p un nombre premier impair que nous écrivons comme $p = 2^n + 1$. Posons $\omega = e^{\frac{2i\pi}{n}}$. Son polynôme annulateur est le polynôme cyclotomique $\Phi_p(X) = \sum_{i=0}^{p-1} X^i$, de degré $p-1$. Ce faisant, $\mathcal{B} = \{\omega, \omega^2, ..., \omega^{p-1}\}$ est une base de $\mathbb{K} = \mathbb{Q}(\omega)$.

Soit $G = Aut_{\mathbb{Q}}(\mathbb{K})$ le groupe des $\mathbb{Q}$-automorphismes de $\mathbb{K}$. Montrons tout d'abord que ce groupe est un groupe cyclique d'ordre $p-1$.

Pour ce faire, soit $g \in G$. Alors $g(\omega)$ est une racine de Φ_p. En effet, $\Phi_p \in \mathbb{Z}[X]$. Or, g est un automorphisme de corps $\mathbb{Q}$-linéaire (en particulier, il fixe les rationnels). On a donc : $\Phi_p(g(\omega)) = g(\Phi_p(\omega))) = g(0) = 0$. ω étant une racine primitive :

$$\exists k \in [\![1; p-1]\!],\ g(\omega) = \omega^k$$

Ceci nous permet alors de définir $\varphi : G \longrightarrow \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$, en envoyant k sur sa classe de conjugaison modulo p. Nous définissons ainsi un morphisme de groupe injectif. En effet, le caractère injectif est direct, puisque g, automorphisme de corps, est entièrement déterminé par sa valeur en ω. De plus, si $g_1, g_2 \in G$ vérifient $g_1(\omega) = \omega^{k_1}$ et $g_2(\omega) = \omega^{k_2}$ avec $k_1, k_2 \in [\![1; p-1]\!]$, alors $g_1 \circ g_2(\omega) = g_1(\omega^{k_2}) = \omega^{k_1 k_2}$. Donc

$\varphi(g_1 \circ g_2) = \varphi(g_1)\varphi(g_2)$.
De plus, ce morphisme est surjectif. Soit en effet $\overline{k} \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ avec $k \in [\![1; p-1]\!]$. On cherche $g \in G$ qui envoit ω sur ω^k. Pour définir un tel élément, il suffit de donner son image sur les éléments de la base $\mathcal{B}$ de $\mathbb{K}$:

$$\forall i \in [\![1; p-1]\!], g(\omega^i) = \omega^{ik}$$

Vérifions que l'application $\mathbb{Q}$-linéaire ainsi définie est bien un morphisme de corps. Tout d'abord :

$$g(1) = g(-\sum_{i=1}^{p-1} \omega^i) = -\sum_{i=1}^{p-1} \omega^{ik} = \sum_{i=1}^{p-1} \omega^i = 1$$

car k est inversible modulo p.
Vérifions sa compatibilité avec la multiplication. En décomposant dans la base $\mathcal{B}$, on se rends compte qu'il suffit de montrer que $\forall i \in \mathbb{Z}$, $g(\omega^i) = g(\omega)^i$. Soit alors un entier i. Alors :

$$g(\omega^i) = g(\omega^{i \ mod \ p}) = \omega^{(i \ mod \ p)k} = \omega^{ik} = g(\omega)^i$$

Finalement, on a bien $g \in G$. Le morphisme φ est donc surjectif, d'où $G \cong \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$.

Nous avons alors montré, par cet isomorphisme, que G était cyclique d'ordre $p-1$. Soit alors $g \in G$ un générateur. En considérant l'ensemble des points fixes de ses itérés, nous pourrons trouver l'extension de corps quadratique qui va nous permettre de montrer que ω est constructible.

D'après ce que nous avons vu tout à l'heure sur la définition de g, nous avons $\mathcal{B} = \{\omega, g(\omega), g^2(\omega), ..., g^{p-2}(\omega)\}$. Définissons alors $\forall i \in [\![0; n]\!], \mathbb{K}_i = \{z \in \mathbb{K} \mid g^{2^i}(z) = z\}$. g étant un automorphisme, nous avons alors définit des sous-corps de $\mathbb{K}$ tels que $\mathbb{K}_i \subset \mathbb{K}_{i+1}$. En particulier, puisque g est d'ordre $p-1 = 2^n$, $\mathbb{K}_n = \mathbb{Q}(\omega)$.

Observons à présent comment g se comporte sur les coordonnées d'un élément $z \in \mathbb{K}$ dans la base $\mathcal{B}$. Notons $z = (z_0, z_1, ..., z_{p-2})$. Alors $z = \sum_{i=0}^{p-2} z_i g^i(\omega)$. Donc $g(z) = \sum_{i=0}^{p-2} z_i g^{i+1}(\omega)$. Ainsi : $g(z_0, ..., z_{p-2}) = (z_{p-2}, z_0, z_1, ..., z_{p-3})$ (intuitivement, on décale les coordonnées d'un cran vers la droite). Ce faisant, pour tout $a \in \mathbb{N}$, $g^a(z) = z$ si et seulement si $\forall j \in [\![0; p-2]\!], z_{j+a} = z_j$ où les indices sont pris modulo p. En particulier, $z \in \mathbb{K}_0$ si et seulement si $\forall j \in [\![0; p-2]\!], z_{j+1} = z_j$. Donc, dans ce cas, $z = z_0 \sum_{j=0}^{p-2} g^j(\omega) = -z_0 \in \mathbb{Q}$. Au final, on a obtenu $\mathbb{K}_0 = \mathbb{Q}$, ce qui marque le début de notre tour d'extension. Son sommet contient bien ω, donc il reste à montrer que les extensions intermédiaires sont quadratiques.

Soit alors $i \in [\![0; n]\!]$. $z \in \mathbb{K}_i$ si et seulement si $z_{j+2^i} = z_j$ pour tout j. On remarque alors que, puisque les coordonnées distantes de 2^i sont les mêmes, il me suffit juste de donner les 2^i premières. On voit déjà que la dimension sera 2^i. Si on veut une base explicite, notons e l'élément de $\mathbb{K}$ de coordonnées dans $\mathcal{B}$:

$$e = (1, 0, ..., 0, \ 1, 0, ..., 0, \ ... \ 1, 0, ..., 0) = \sum_{j=0}^{2^{n-i}-1} g^{j2^i}(\omega)$$

Regardons ses itérés :

$$g(e) = (0, 1, 0..., 0, \ 0, 1, 0, ..., 0, \ ... \ 0, 1, 0, ..., 0)$$

$$g^2(e) = (0,0,1,0,...,0,\ 0,0,1,0,...,0,\ ...\ 0,0,1,0,...,0)$$

$$...$$

$$g^{2^i-1}(e) = (0,...,0,1,\ 0,...,0,1,\ ...\ 0,...,0,1)$$

où chaque paquets sont de longueurs 2^i.

D'après sa définition en coordonnées, la famille $C = \{e, g(e), ..., g^{2^i-1}(e)\}$ est une famille linéairement indépendante. De plus, elle génère trivialement $\mathbb{K}_i$. Nous avons alors $[\mathbb{K}_i : \mathbb{Q}] = 2^i$. Ainsi, si $i \neq n$, par théorème de la base téléscopique, $[\mathbb{K}_{i+1} : \mathbb{K}_i] = 2$.

Nous avons alors trouvé une tour d'extension quadratique dont le sommet contient ω. Par théorème de Wantzel, ω est donc constructible, et donc son polygone aussi.

Théorème (Théorème de Gauss-Wantzel)**.** *Le polygone régulier à n côtés est constructible si et seulement si n est produit d'une puissance de 2 et de nombres premiers de Fermat distincts deux à deux.*

Sens réciproque Si le polygone régulier à n côtés est constructible, alors il en est de même pour celui à $2n$ côtés. En effet, $e^{\frac{2i\pi}{n}}$ est constructible, et la bissectrice d'un angle constructible est constructible, d'où le résultat.
Ainsi, il suffit de démontrer que si n est produit de nombres premiers de Fermat, alors le polygone est constructible. Pour ajouter les puissances de 2, il suffira alors de multiplier par 2 autant de fois que nécessaire. Soient alors p et q deux nombres premiers de Fermat distincts. Alors ils sont premiers entre eux : il existe u et v deux entiers tels que $pu + qv = 1$. Ainsi :

$$\frac{2i\pi}{pq} = u\frac{2i\pi}{q} + v\frac{2i\pi}{p}$$
$$\Rightarrow e^{\frac{2i\pi}{pq}} = \left(e^{\frac{2i\pi}{q}}\right)^u \times \left(e^{\frac{2i\pi}{p}}\right)^v$$

L'ensemble des nombres constructibles étant un corps, le polygone à pq côtés est donc constructible, ce qui démontre le sens réciproque.

Sens direct Pour le sens direct, il suffit de remarquer que si d est un diviseur de n, et que le polygone régulier à n côtés est constructible, alors il en est de même pour celui à d côtés (qui est inclut dans celui à n côtés). Ainsi, si on applique ceci à un terme p^a de la décomposition en facteurs premiers de n où p est impair, on trouve que $a = 1$ et p est un nombre premier de Fermat d'après le théorème précédent.