Sandrine CARUSO

Polygones réguliers constructibles

Références : Carrega, Escofier (Théorie de Galois), Perrin ou toute référence sur les groupes

On rappelle (sans démonstration) la caractérisation suivante des nombres constructibles.

Théorème 1. *Soit $z \in \mathbb{C}$. Alors z est constructible si et seulement si il existe une suite de sous-corps de $\mathbb{C}$, $K_0 = \mathbb{Q} \subset K_1 \subset \cdots \subset K_m$, tels que $z \in K_m$ et pour $i \in \{0, \ldots, m-1\}$, $[K_{i+1} : K_i] = 2$.*

Théorème 2. *Le polygone régulier à n côtés est constructible à la règle et au compas si et seulement si $\varphi(n)$ est une puissance de 2, ce qui équivaut encore au fait que n soit de la forme $n = 2^\alpha p_1 \cdots p_r$ où $\alpha \in \mathbb{N}$ et les p_i sont des nombres premiers de Fermat distincts.*

Le polygone régulier à n côtés est constructible si et seulement si une racine primitive n-ième ζ_n de l'unité est constructible. On s'intéresse donc à l'extension cyclotomique $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.

Lemme 3. *Le degré $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ de l'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est égal à $\varphi(n)$.*

Démonstration. Le polynôme cyclotomique Φ_n étant irréductible sur $\mathbb{Q}$, c'est le polynôme minimal de ζ_n. Donc $\mathbb{Q}(\zeta_n) \simeq \mathbb{Q}[X]/(\Phi_n)$ qui est bien de degré $\deg \Phi_n = \varphi(n)$ sur $\mathbb{Q}$. □

1. Condition nécessaire de constructibilité de ζ_n

Lemme 4. *Si ζ_n est constructible, alors $\varphi(n)$ est une puissance de 2.*

Démonstration. Si ζ_n est constructible, d'après le théorème 1, il existe une tour d'extensions $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_m$ avec $\zeta_n \in K_m$ et $[K_{i+1} : K_i] = 2$. En particulier, $\mathbb{Q}(\zeta_n) \subset K_m$. L'extension intermédiaire $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est une sous extension de $K_m/\mathbb{Q}$ qui est de degré 2^m. Donc $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ divise 2^m, et est donc une puissance de 2.

Comme $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, le lemme s'ensuit. □

Nous allons désormais nous pencher sur la réciproque de ce lemme, qui utilise la théorie de Galois.

2. Condition suffisante de constructibilité

Proposition 5. *Si $z \in L$, où $L/\mathbb{Q}$ est une extension galoisienne de degré 2^k ($k \in \mathbb{N}$), alors z est constructible.*

Démonstration. Montrons l'existence d'une suite d'extensions comme dans le théorème 1. Nous allons montrer par récurrence forte sur k la propriété suivante : « Toute extension galoisienne L/K de degré 2^k peut se scinder en une tour d'extensions $K = K_0 \subset K_1 \subset \cdots \subset K_k = L$ de degrés successifs $[K_{i+1} : K_i] = 2$. »

Le résultat est évident si $k = 0$ ou $k = 1$. Supposons que $k \geqslant 2$. Pour établir l'hérédité, il suffit de montrer l'existence d'un corps M, $K \subsetneq M \subsetneq L$, tel que l'extension M/K soit galoisienne (l'extension L/M l'est automatiquement car L/K l'est, et on applique l'hypothèse de récurrence à L/M et M/K).

D'après la correspondance de Galois, cela revient à montrer que $\mathrm{Gal}(L/K)$ admet un sous-groupe distingué non trivial (en d'autres termes, qu'il n'est pas simple). Or, $|\mathrm{Gal}(L/K)| = 2^k$. Le résultat est une conséquence du lemme plus général suivant :

Lemme 6. *Soit p un nombre premier, et G un p-groupe, différent de $\mathbb{Z}/p\mathbb{Z}$. Alors G n'est pas simple.*

Démonstration. Notons p^k le cardinal de G ($k \geqslant 2$). Si G est commutatif, il suffit de remarquer que G admet au moins un sous-groupe non trivial. Par exemple, on peut invoquer le fait que G admet un élément d'ordre p, donc un sous-groupe de cardinal p.

Supposons maintenant G non commutatif. Alors le centre de G, $Z(G)$, n'est pas égal à G. Montrons qu'il n'est pas non plus égal à $\{1\}$. Le groupe G agit sur lui-même par conjugaison. La formule des classes affirme alors que le cardinal de toute orbite $\mathcal{O}(g)$ divise $|G| = p^k$, donc est une puissance de p. En particulier, les orbites qui ne sont pas réduites à un point ont un cardinal divisible par p. Par définition, $Z(G)$ est exactement l'ensemble des points fixes de cette action, et on écrit

$$|G| = |Z(G)| + \sum_{g \in A} |\mathcal{O}(g)|$$

où A est un ensemble de représentants de chaque orbite non réduite à un point. Modulo p, on obtient $|Z(G)| \equiv 0 \pmod{p}$. En particulier, $|Z(G)| \neq 1$ et donc $Z(G) \neq \{1\}$. Par conséquent, $Z(G)$ est un sous-groupe distingué non trivial de G. □

On a donc montré que $\mathrm{Gal}(L/K)$ admet un sous-groupe distingué non trivial, et ceci conclut la récurrence.

En appliquant ce résultat avec $K = \mathbb{Q}$, et en utilisant le théorème 1, on a bien démontré la proposition. □

3. Réciproque du lemme 4

Proposition 7. *Si $\varphi(n)$ est une puissance de 2, alors ζ_n est constructible.*

Démonstration. En vertu du lemme 3, il suffit de prouver que si $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ est une puissance de 2, alors ζ_n est constructible.

Montrons tout d'abord que l'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est galoisienne. Si f est un $\mathbb{Q}$-morphisme de $\mathbb{Q}(\zeta_n)$ dans $\mathbb{C}$, f est entièrement défini par l'image de ζ_n ; $f(\zeta_n)$ est nécessairement une racine (primitive) n-ième de l'unité, et par conséquent il existe k tel que $f(\zeta_n) = \zeta_n^k$. En particulier, $f(\zeta_n) \in \mathbb{Q}(\zeta_n)$, et f est à valeurs dans $\mathbb{Q}(\zeta_n)$. Donc $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est galoisienne.

Alors, en appliquant le théorème 5, on en déduit que, si $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ est une puissance de 2, ζ_n est constructible. □

4. Caractérisation de la constructibilité de ζ_n

On a donc montré, avec les lemmes 4 et 7, le résultat suivant.

Lemme 8. *Le nombre ζ_n est constructible si et seulement si $\varphi(n)$ est une puissance de 2.*

Caractérisons les entiers n tels que $\varphi(n)$ est une puissance de 2.

On écrit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ la décomposition de n en facteurs premiers. Alors $\varphi(n) = (p_1 - 1)p_1^{\alpha_1 - 1} \cdots (p_r - 1)p_r^{\alpha_r - 1}$. Pour que $\varphi(n)$ soit une puissance de 2, et faut et il suffit que

– les $p_i - 1$ soient des puissances de 2,
– si $\alpha_i > 1$, p_i soit une puissance de 2.

Or, pour $p_i \neq 2$, p_i et $p_i - 1$ ne peuvent être tous les deux des puissances de 2. Donc si $p_i \neq 2$, $\alpha_i = 1$. En outre, p_i est de la forme $2^{m_i} + 1$. Si un nombre impair q divise m_i, alors $2^{m_i/q} + 1$ divise $2^{m_i} + 1$, et $2^{m_i} + 1$ ne peut être premier (sauf si $q = 1$). Donc m_i est lui aussi une puissance de 2. Au final, on a bien montré (quitte à renuméroter les p_i) que

$$n = 2^\alpha p_1 \cdots p_r$$

où $\alpha \in \mathbb{N}$ et où les p_i sont des nombres premiers de Fermat.