Polygones constructibles

Théorème. *Le polygone régulier à n coté est constructible si et seulement si n est produit de puissances de 2 et de nombres premiers de la forme 2^n+1 distincts.*

Notation : $w_n = \exp(2\pi i/n)$. Le polygone régulier à n coté est constructible si et seulement si il existe une tour d'extensions de degré consécutif 2, notées $\mathbb{Q} = K_0 \subset K_1 \subset .. \subset K_r$ telle que $w_n \in K_r$.

Lemme. *Soient n, m premiers entre eux, w_{nm} est constructible si et seulement si w_n et w_m le sont.*

Démonstration. On a $w_{nm}^n = w_m$, $w_{nm}^m = w_n$. Réciproquement, il existe $u, v \in \mathbb{Z}$ tels que $un + vm = 1$. Alors $w_{nm} = w_n^u w_m^v$. □

Lemme. *w_{2^n} est constructible et si p est un nombre premier impair tel que w_{p^n} est constructible, alors $n = 1$ et $p-1$ est une puissance de 2.*

Démonstration. w_{2^n} est constructible par construction de médiatrices successives du diamètre du cercle.
Si w_{p^n} est constructible, alors $[\mathbb{Q}(w_{p^n}) : \mathbb{Q}]$ est une puissance de 2.
Or, $[\mathbb{Q}(w_{p^n}) : \mathbb{Q}] = \deg(\phi_{p^n}) = \varphi(p^n) = p^{n-1}(p-1)$. Donc $p^{n-1} = 1$ et $(p-1)$ est une puissance de 2. □

Il suffit donc de montrer que les nombres premiers impairs p tels que $p-1$ est une puissance de 2 sont bien constructibles.

Démonstration. Soit p un tel nombre premier, G le groupe des $\mathbb{Q}$-automorphismes de $\mathbb{Q}(w_p)$, montrons que $G \cong (\mathbb{Z}/p\mathbb{Z})^*$.
Les racines de ϕ_p sont exactement les w_p^k, $k \in (\mathbb{Z}/p\mathbb{Z})^*$. Un élément de G est entièrement déterminé par sa valeur en w_p, ce qui donne un morphisme injectif :

$$\begin{cases} G \to (\mathbb{Z}/p\mathbb{Z})^* \\ \sigma \mapsto \sigma(w_p) \end{cases}$$

Il suffit de montrer la surjectivité. Soit $k \in (\mathbb{Z}/p\mathbb{Z})^*$. Les morphismes d'anneau suivants :
$Ev_1 : \begin{cases} \mathbb{Q}[X] \to \mathbb{Q}(w_n) \\ Q(X) \mapsto Q(w_p) \end{cases}$ et $Ev_k : \begin{cases} \mathbb{Q}[X] \to \mathbb{Q}(w_n) \\ Q(X) \mapsto Q(w_p^k) \end{cases}$ passent au quotient en des isomorphismes entre $\mathbb{Q}(w_n)$ et $\frac{\mathbb{Q}[X]}{(\phi_p)}$; composer les deux donne un automorphisme qui envoie w_p sur w_p^k, ce qui achève cette partie de la preuve.
G est donc cyclique : soit $\sigma \in G$ un générateur de G. σ est d'ordre $p-1 = 2^n$. On définie $K_k = \mathrm{Fix}(\sigma^{2^k})$, on considère la tour d'extension $K_0 \subset .. \subset K_n$.
- $K_n = \mathbb{Q}(w_p)$ car $\sigma^{2^n} = Id$.

- $K_0 = \mathbb{Q}$. En effet, $(w_p^k)_{k=1..p-1}$ est une $\mathbb{Q}$-base de $\mathbb{Q}(w_p)$ (par argument de dimension) et si $\sum_{k=1}^{p-1} \lambda_k w_p^k$ est fixé par σ, comme σ agit comme le générateur de $(\mathbb{Z}/p\mathbb{Z})^*$, il agit comme une permutation cyclique de $(\mathbb{Z}/p\mathbb{Z})^*$, donc tous les λ_k sont égaux et $\sum_{k=1}^{p-1} \lambda_k w_p^k = -\lambda_1 \in \mathbb{Q}$.
- $[K_{k+1} : K_k] \leq 2$: En effet, si on note $\tau_k = \sigma^{2^k}_{|K_{k+1}}$, alors c'est un K_k-endomorphisme linéaire de K_{k+1} (il suffit de vérifier que K_{k+1} est stable par σ^{2^k}). $\tau_k^2 = Id_{K_{k+1}}$ donc τ_k est diagonalisable de valeur propre ± 1. La valeur propre 1 est simple car son espace propre associé est K_k. La valeur propres -1 est simple car si v, w sont deux vecteurs propres de -1, alors v/w est un vecteur propre de 1, donc est dans K_k et v, w sont K_k-liés. Ainsi, $[K_{+1} : K_k] \leq 2$.

$\square$

Référence : Tauvel