I Enoncé

Soit p premier et soit $\alpha \geq 1$. Le $p^\alpha-$gone régulier est constructible à la règle et au compas si et seulement si $p = 2$ ou $\alpha = 1$ et p est de Fermat.

II Lemmes

Théorème 1 (Wantzel)**.** *Un nombre ω est constructible à la règle et au compas si et seulement si il existe n entier naturel et une tour d'extension $K_0, \ldots, K_n$ vérifiant $K_0 = \mathbb{Q}$, $\omega \in K_n$ et $[K_{i+1} : K_i] \leq 2$.*

Démonstration. Le théorème est, pour la formalisation, assumée. On l'utilisera en tant que définition d'être constructible. Si le temps le permet, on le montrera en construisant les nombres constructibles de manière inductive selon le « Cours d'algèbre »de Perrin. □

Corollaire 2. Si ω est constructible, alors $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2^m$ pour un certains m.

Démonstration. On utilise la multiplicativité des degrés dans le théorème de Wantzel. □

Lemme 3. Soit p premier. Si $p = 2^m + 1$ pour un certains m, alors p est de Fermat et réciproquement.

Démonstration. On fait chaque sens séparément, je l'ai déjà implémenté sur L∃∀N. □

III Squelette de la preuve

On fixe p premier.

III.1 Sens direct

On suppose le p^α-gone constructible. C'est-à-dire $\omega := \mathrm{e}^{\frac{2i\pi}{p^\alpha}}$ constructible. Par le corollaire du théorème de Wantzel, $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2^m$ pour un certains entier m (on en fixe un pour la suite). Or, $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg \mu_{\omega,\mathbb{Q}} = \deg \Phi_{p^\alpha}$ car $\Phi_{p^\alpha,\mathbb{Q}}$ est irréductible sur $\mathbb{Q}[X]$ et annule ω. Or, $\deg \Phi_{p^\alpha} = \varphi(p^\alpha) = (p-1)p^{\alpha-1}$.

D'où $2^m = (p-1)p^{\alpha-1}$. Si $\alpha = 1$, alors $p = 2^m + 1$ et donc par le lemme 3, p est de Fermat.
Si $\alpha > 1$, comme 2 est premier, par unicité de la décomposition en facteur premier, $p = 2$.

III.2 Sens réciproque

Soit $\omega := \mathrm{e}^{\frac{2i\pi}{p}}$, $p = 2^{2^m} + 1$.
1) On montre que ω est une racine primitive $p-$ième de l'unité.
2) On montre que $\mathbb{Q}(\omega)$ est l'extension cyclotomique de degré p sur $\mathbb{Q}$: cela permettra d'utiliser les fonctions implémentées dans $L\exists\forall N$ sur les extensions cyclotomiques.
3) L'extension est galoisienne.
4) $Gal(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ (le premier isomorphisme étant déjà disponible sur Mathlib dans les extensions cyclotomiques). En particulier, $Gal(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}/2^{2^m}\mathbb{Z}$, donc le groupe de Galois est cyclique (donc résoluble) d'ordre 2^m. Il admet donc un générateur ζ.
5) Notons $G_i := \langle \zeta^{2^i} \rangle$ pour tout $i \in [\![0, m]\!]$. Alors $G_0 = Gal(\mathbb{Q}(\omega)/\mathbb{Q})$, $G_m = \{1\}$, $G_{i+1} \subset G_i$ pour tout i, G_{i+1} est un sous-groupe normal de G_i et G_i/G_{i+1} est abélien comme quotient de groupes abéliens. On en déduit que la suite $(G_i)_i$ est une suite résoluble pour G.
6) Comme $[G_i : G_{i+1}] = 2$ pour tout i, la correspondance de Galois nous donne une tour d'extension $K_i := \mathbb{Q}(\omega)^{G_i}$ vérifiant $K_0 = \mathbb{Q}$, $K_m = \mathbb{Q}(\omega)$ et $[K_{i+1} : K_i] = 2$. Par Wantzel, ω est bien constructible.