# Construction de polygones réguliers
# Leçon d'agrégation

Bernard Le Stum*
Université de Rennes 1

Version (peut-être buggée) du 5 mars 2001

## 1 Critère de constructibilité

Nous allons donner la définition d'un polygone régulier constructible, énoncer le critère de constructibilité et faire les premiers dévissages de la démonstration.

**Définition 1.1** *Un nombre complexe $z$ est* constructible *s'il est contenu dans une extension quadratique itérée de* $\mathbf{Q}$*. On dit aussi que le point $P$ d'affixe $z$ est* constructible*.*

On rappelle qu'une extension quadratique itérée d'un corps $K$ est une extension de corps $L/K$ telle qu'il existe une suite d'extensions quadratiques (i.e. de degré 2) $K := K_0 \subset K_1 \subset \cdots \subset K_s = L$.

On démontre facilement que notre définition de point constructible coïncide avec la notion classique de point constructible à la règle et au compas.

Enfin, il est facile de voir que le degré d'un nombre constructible est une puissance de 2 (la réciproque est fausse).

**Définition 1.2** *Si $\zeta := e^{\frac{2i\pi}{n}}$, où $n$ est un entier naturel, est constructible, on dit que le polygone régulier à $n$ côtés est constructible.*

Ici encore, il est aisé de voir que notre définition de polygone constructible coïncide avec la notion classique de polygone régulier constructible à la règle et au compas.

*lestum@univ-rennes1.fr

**Théorème 1.3** *Le polygone régulier à $n$ côtés est constructible ssi*

$$n = 2^s p_1 \dots p_r$$

*ou les $p_i$ sont des premiers de Fermat distincts.*

On rappelle qu'un nombre premier $p$ est de Fermat si $p-1$ est une puissance de 2. Les nombres de Fermat sont les nombres de la forme $2^{2^r}+1$. Il est facile de voir qu'un nombre de Fermat qui est premier n'est autre qu'un premier de Fermat. Les seuls connus à ce jour sont 2, 3, 5, 17, 257 et 65537.

Les résultats énoncés dans le lemme suivant sont faciles à démontrer et laissés en exercice.

**Lemme 1.4** *i) Si le polygone régulier à $n$ côtés est constructible et $m|n$, alors le polygone régulier à $m$ côtés est constructible.*

*ii) Si $(m, n) = 1$ et si les polygones réguliers à $n$ et $m$ côtés sont constructibles, alors le polygone régulier à $mn$ côtés est constructible.*

*iii) Le polygone régulier à $2^s$ côtés est constructible*

Grâce au lemme précédent, il suffit de démontrer le théorème lorsque $n$ est une puissance d'un nombre premier. On démontrera plus tard le lemme suivant.

**Lemme 1.5** *Si $p$ est un premier impair, alors le polygone régulier à $p^2$ côtés n'est pas constructible.*

Grâce à se lemme, on peut supposer que $n$ est premier. Il restera donc à démontrer la proposition suivante.

**Proposition 1.6** *Si $p$ est un premier impair, alors le polygone régulier à $p$ côtés est constructible ssi $p$ est un nombre de Fermat.*

Nous aurons besoin pour cela d'un peu de théorie de Galois. Signalons tout de même qu'il existe une démonstration élémentaire, due a Gauss (voir [Hadlock, *Field theory and its classical problems*]). Mais cela revient à faire de la théorie de Galois sans le dire comme Monsieur Jourdain (qui faisait de la prose sans en connaître la cause et de la poésie sans en avoir envie).

## 2 Notions de théorie de Galois

Nous allons donner sans démonstration quelques résultats de théorie de Galois et en déduire le lemme 1.5 et la proposition 1.6, ce qui conclura la démonstration du critère de constructibilité.

**Définition 2.1** *Une extension finie de corps $L/K$ est* galoisienne *si pour tout $\alpha \in L$, le polynôme irréductible de $\alpha$ sur $K$ se décompose sur $L$ en produit de facteurs linéaires distincts.*

Si $\mathbf{Q} \subset K$, alors les facteurs linéaires sont nécessairement distincts et une extension galoisienne n'est autre qu'une extension normale (c'est-à-dire, un corps de décomposition).

Si $L/K$ est galoisienne, les $K$-automorphismes de $L$ (c'est a dire les homomorphismes d'anneaux $\sigma : L \to L$ tels que $\sigma_{|K} = Id_K$) forment un groupe $\mathrm{Gal}(L/K)$ d'ordre $[L : K]$.

Nous aurons besoin du résultat suivant dont la démonstration est loin d'être triviale.

**Proposition 2.2** *Si $\zeta := e^{\frac{2i\pi}{n}}$, alors $\mathbf{Q}(\zeta)/\mathbf{Q}$ est galoisienne et*

$$\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) \cong (\mathbf{Z}/n\mathbf{Z})^*.$$

On sait que $\varphi(n) = |\mathbf{Z}/n\mathbf{Z})^*|$ est la fonction $\varphi$ d'Euler. Par exemple, on sait que $\varphi(p) = p - 1$ et $\varphi(p^2) = p(p - 1)$ pour $p$ premier impair.

On en déduit immédiatement la nécessité de la condition dans la proposition 1.6. En effet, on sait que si $\zeta := e^{\frac{2i\pi}{p}}$, alors $[\mathbf{Q}(\zeta) : \mathbf{Q}] = p - 1$. On voit donc que si le polygone régulier à $p$ côtés est constructible, alors $p - 1$ est une puissance de 2.

Le lemme 1.5 en résulte aussi : si $\zeta := e^{\frac{2i\pi}{p^2}}$, on a $[\mathbf{Q}(\zeta) : \mathbf{Q}] = p(p - 1)$ qui ne peut pas être une puissance de 2.

On en vient maintenant à la théorie de Galois proprement dite. On se donne une extension galoisienne $L/K$ et on pose $G := \mathrm{Gal}(L/K)$. Si $K \subset M \subset L$ est une extension intermédiaire, alors $L/M$ est galoisienne et $H := \mathrm{Gal}(L/M)$ est un sous-groupe de $G$. Réciproquement, si $H \subset G$ est un sous-groupe, alors $M := L^H := \{\alpha \in L, \forall \sigma \in H, \sigma(\alpha) = \alpha\}$ est une extension de corps intermédiaire.

**Théorème 2.3** *Soit $L/K$ une extension galoisienne et $G := \mathrm{Gal}(L/K)$. Alors, les applications $M \mapsto H := \mathrm{Gal}(L/M)$ et $H \mapsto M := L^H$ établissent une bijection qui renverse l'inclusion entre les extensions intermédiaires $K \subset M \subset L$ et les sous-groupes $H$ de $G$. De plus, $M/K$ est galoisienne ssi $H$ est distingué (ou normal) dans $G$ et on a alors un isomorphisme canonique $\mathrm{Gal}(M/K) \cong G/H$.*

On ne va pas démontrer ce théorème mais on va en déduire que la condition de la proposition 1.6 est suffisante. On suppose donc que $p$ est

un premier de Fermat et on écrit $p-1=2^s$. On pose $\zeta := e^{\frac{2i\pi}{p}}$ et on écrit $G := \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$. On sait que $G$ est abélien et que $|G| = p-1 = 2^s$. Un tel groupe a une suite de décomposition $G_0 = G \supset G_1 \supset \cdots \supset G_s$ avec $[G_{i+1} : G_i] = 2$ (ça se démontre facilement par récurrence sur $s$). Le théorème fondamental de la théorie de Galois nous dit donc qu'il existe une suite d'extensions quadratiques $K_0 := \mathbf{Q} \subset K_1 \subset \cdots \subset K_s = \mathbf{Q}(\zeta)$.

Donc, c'est très simple. On peut regarder par exemple les bouquins [Stewart, *Galois Theory*] et [Nagata, *Field Theory*].