Développement: Polygones constructibles à la règle et au compas

Arthur Maritch-Roy

Dans ce développement, on cherche à quelle condition sur n le polygone régulier à n côtés est constructible à la règle et au compas.

Théorème 1. (de Gauss-Wantzel)
Le nombre $\mathrm{e}^{2\mathrm{i}\pi/n}$ est constructible à la règle et au compas si et seulement s'il s'écrit comme une puissance de deux fois un produit de nombres premiers de Fermat distincts, c'est-à-dire de la forme $2^{2^\alpha}+1$.

Démonstration. On peut se ramener à une puissance de nombre premier par Bezout. En effet, si a et b sont premiers entre eux, on peut écrire $au+bv=1$ une relation de Bezout, et alors

$$\mathrm{e}^{\frac{2\mathrm{i}\pi}{ab}} = \left(\mathrm{e}^{\frac{2\mathrm{i}\pi}{ab}}\right)^{au+bv} = \left(\mathrm{e}^{\frac{2\mathrm{i}\pi}{b}}\right)^{u}\left(\mathrm{e}^{\frac{2\mathrm{i}\pi}{a}}\right)^{v},$$

donc si les deux sont constructibles, alors le premier l'est. Réciproquement on a aussi le résultat puisqu'un produit de nombres constructibles est constructible.

Maintenant, on peut traiter de manière élémentaire le cas des puissances de 2, puisque l'on sait construire des bissectrices. Soit donc p premier impair et $\alpha\in\mathbb{N}^*$, on est ramenés au cas $n=p^\alpha$.

Si $\omega := \mathrm{e}^{\frac{2\mathrm{i}\pi}{p^\alpha}}$ est constructible, alors le degré de son polynôme minimal est une puissance de deux notée 2^m. Mais ce polynôme minimal n'est autre que Φ_{p^α}, qui est de degré $\varphi(p^\alpha)=p^{\alpha-1}(p-1)=2^m$. Par unicité de la décomposition en produit de facteurs premiers, α vaut 1 et p vaut 2^m+1. Montrons alors qu'un nombre premier de cette forme est nécessairement un premier de Fermat. Si m' est impair et tel que $m=2^\beta m'$, alors

$$p = 1+(2^{2^\beta})^{m'} = (1+2^{2^\beta})\sum_{k=0}^{m'-1}(-2^{2^\beta})^k,$$

donc $1+2^{2^\beta}$ donc égale p, ce qu'on voulait démontrer.

Réciproquement, soit p un nombre premier de Fermat, noté de la même manière $p=1+2^{2^\beta}$ avec $m=2^\beta$. On étudie les automorphismes du groupe $\mathrm{Aut}(K)=:G$ avec $K:=\mathbb{Q}(\omega)$ (c'est un corps car le polynôme minimal en question est un polynôme cyclotomique). On va montrer que $G\simeq(\mathbb{Z}/p\mathbb{Z})^*$. Pour cela soit $\sigma\in G$, alors

$$0=\sigma(0)=\sigma(\Phi_p(\omega))=\Phi_p(\sigma(\omega)),$$

où l'on a utilisé le morphisme de Frobenius. Donc $\sigma(\omega)$ est une racine de Φ_p, donc un élément de la forme ω^k avec $k\in\{1,\dots,p-1\}$. Il existe donc k_σ tel que $\sigma(\omega)=\omega^{k_\sigma}$. On pose alors naturellement $\psi : G\to(\mathbb{Z}/p\mathbb{Z})^*$ qui à σ associe k_σ, qui est un morphisme de groupes (c'est une vérification). Elle est injective car si deux automorphismes coïncident sur $\mathbb{Q}$ et $\{\omega\}$ alors ils coïncident sur K et est surjective puisque cela revient à passer au quotient le morphisme

d'évaluation en un ω^k (ils ont tous le même polynôme minimal). Ainsi G est cyclique d'ordre 2^m. Remarquons qu'alors pour σ_0 un générateur de G, $(\sigma_0^i(\omega))_{0\leq i\leq p-2}$ est une base de K.

Puisque notre groupe est cyclique, on peut bâtir une suite de sous-groupes

$$G =: G_0 \supset \cdots \supset G_m = \{\mathrm{id}_K\},$$

avec G_i engendré par $\sigma_0^{2^i}$. À partir de cette suite de sous-groupes, on construit les sous-corps de K suivants :

$$K_i := \{z \in K, \forall \sigma \in G_i, \sigma(z) = z\} = \{z \in K, \sigma_0^{2^i}(z) = z\},$$

où la deuxième égalité est due au fait que l'on a pris un générateur de G_i. Si $z \in K_0$, on a, en utilisant le fait que $\sigma_0(z) = z$ et en décomposant selon la base que l'on a exhibée, $z \in \mathbb{Q}$ donc $K_0 = \mathbb{Q}$. On vérifie alors que

$$z := \sum_{l=0}^{2^{m-i-1}-1} \sigma_0^{2^{i+1}l}(\omega) \in K_{i+1}\backslash K_i.$$

Finalement : $2^m = p - 1 = [\mathbb{Q}(\omega) : \mathbb{Q}] = \prod_{i=1}^m [K_i : K_{i-1}]$. Chaque terme est plus grand que 2 est le produit est une puissance de deux donc chaque degré vaut 2, on peut appliquer le théorème de Wantzel. □

Remarque 2. En général, le théorème de Wantzel est toujours énoncé pour des *réels* constructibles. Voyons donc comment le généraliser pour des complexes constructibles, et donc pouvoir éviter des vérifications pénibles.

On part de la remarque suivante : le point $M(x, y)$ est constructible si et seulement si les points $A(x, 0)$ et $B(0, y)$ sont constructibles.

Définition 3. On définit E(i) l'ensemble des complexes constructibles (où E est l'ensemble des réels constructibles).

Lemme 4. C'est un sous-corps de $\mathbb{C}$ stable par racine carrée.

Démonstration. Cela se montre comme sur $\mathbb{R}$, en remarquant que les parties réelle, imaginaire d'une racine carrée de z s'expriment comme des sommes, produits, racines carrées réelles des parties réelle, imaginaire de z. □

Théorème 5. (de Wantzel, version complexe)
Soit $z \in \mathbb{C}$. Alors $z \in$ E(i) si et seulement s'il existe une tour d'extensions quadratiques (de sous-corps de $\mathbb{C}$) $(L_0, \ldots, L_p)$ avec $\mathbb{Q} = L_0$ et $z \in L_p$.

Démonstration. Pour le sens direct, la preuve de Wantzel réel donne une tour d'extensions réelles $(K_0, \ldots, K_q)$ avec $K_0 = \mathbb{Q}$ et $\mathrm{Re}(z)$ et $\mathrm{Im}(z)$ qui sont dans K_q. On pose alors $K_{q+1} = L_p(\mathrm{i})$, qui est bien une extension de L_p de dimension 2 ($\pi_{\mathrm{i},Lp} = X^2 + 1$). Ainsi, $(K_0, \ldots, K_{q+1})$ donne la tour voulue.

Réciproquement, par récurrence, si $K_j \subset$ E(i), considérons $x \in K_{j+1}\backslash K_j$. Puisque $[K_{j+1} : K_j] = 2$, il existe b, c dans K_j tels que $x^2 + bx + c = 0$. Soit alors δ une racine complexe de $\Delta = b^2 - 4c$, on a $\frac{-b\pm\delta}{2}$ mais $\Delta \in K_j \subset$ E(i) qui est stable par racine carrée donc $\delta \in$ E(i) et x également. □