Théorème de Gauss-Wantzel

Théo Jaudon

Au-delà de la notion de point constructible qui n'est pas rappelé ici, quelques prérequis sont nécessaires avant d'aborder ce développement.

Définition 1. *On dit qu'un nombre complexe $z \in \mathbb{C}$ est constructible si c'est l'affixe d'un point constructible.*

Définition 2. *On dit que le polygone régulier à n côtés est constructible à la règle et au compas si le nombre complexe $e^{i\frac{2\pi}{n}}$ est constructible.*

Théorème 3. *L'ensemble des nombres complexes constructibles est un sous-corps de $\mathbb{C}$ stable par racine carrée.*

Enfin le résultat crucial dans la preuve du développement est le théorème de Wantzel énoncé ci-dessous.

Théorème 4. *Soit $z \in \mathbb{C}$. Alors z est constructible si et seulement si il existe une suite finie de sous corps de la forme*

$$\mathbb{Q} = L_0 \subset L_1 \subset \dots L_n \subset \mathbb{C}$$

où $z \in L_n$ et $[L_{i+1} : L_i] = 2$ pour tout $i \in [\![0, n-1]\!]$.

Corollaire 5. *Soit $z \in \mathbb{C}$ un nombre constructible. Alors z est algébrique sur $\mathbb{Q}$ et le degré de l'extension $\mathbb{Q}(z)/\mathbb{Q}$ est une puissance de 2.*

Lemme 6. *Soit $n \in \mathbb{N}^*$ tel que $2^n + 1$ soit premier. Alors n est une puissance de 2.*

Preuve. On peut écrire $n = 2^m(2r+1)$ où $m, r \in \mathbb{N}$. Supposons par l'absurde que $r \geq 1$. Alors

$$2^n + 1 = (2^{2^m})^{2r+1} - (-1)^{2r+1} = (2^{2^m} + 1) \sum_{0 \leq i \leq 2r} (-1)^i 2^{2^m(2r-i)}.$$

Mais $3 \leq 2^{2^m} + 1 \leq 2^n + 1$ ce qui contredit le fait que $2^n + 1$ soit premier.

Définition 7. *Les nombres de Fermat sont définies pour $n \in \mathbb{N}$ par $F_n = 2^{2^n} + 1$. Les nombres $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257$ et $F_4 = 65537$ sont premiers et les suivants qui nous sont connus ne le sont pas.*

C'est ici que le développement commence.

Proposition 8. *Soient $n, m \in \mathbb{N}^*$ deux entiers premiers entre eux. Alors le polygone régulier à nm côtés est constructible si et seulement si les polygones réguliers à n et m côtés le sont.*

Preuve. Pour $k \in \mathbb{N}^*$ on note $\zeta_k = e^{i\frac{2\pi}{k}}$ et on raisonne sur les nombres complexes constructibles.
Supposons que le nombre ζ_{nm} soit constructible. Comme l'ensemble des nombres complexes constructibles forme un sous-corps de $\mathbb{C}$, les nombres $\zeta_n = \zeta_{nm}^m$ et $\zeta_m = \zeta_{nm}^n$ sont constructibles. Réciproquement supposons que les nombres ζ_n et ζ_m soient constructibles. D'après le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tels que $un + vm = 1$. Mais alors le nombre $\zeta_m^u \zeta_n^v = e^{i\frac{2u\pi}{m}} e^{i\frac{2v\pi}{n}} = e^{i\frac{2(un+vm)\pi}{nm}} = \zeta_{nm}$ est constructible.

Par conséquent on se ramène à la question de savoir si le polygone régulier à p^α côtés est constructible lorsque p est premier et $\alpha \in \mathbb{N}^*$.

Proposition 9. *Pour tout $\alpha \in \mathbb{N}$, le polygone régulier à 2^α côtés est constructible.*

Preuve. On sait construire des bissectrices, le résultat en découle par récurrence immédiate sur $\alpha \in \mathbb{N}$.

Théorème 10. *Soit p un nombre premier impair et $\alpha \geq 1$. Alors le polygone régulier à p^α côtés est constructible si et seulement si $\alpha = 1$ et p est un nombre premier de Fermat.*

Preuve. Supposons que le nombre $e^{i\frac{2\pi}{p^\alpha}}$ soit constructible. D'après le corollaire 5 il existe $n \in \mathbb{N}$ tel que

$$[\mathbb{Q}(e^{i\frac{2\pi}{p^\alpha}}) : \mathbb{Q}] = \varphi(p^\alpha) = p^{\alpha-1}(p-1) = 2^n.$$

Par unicité de la décomposition en facteurs premiers et sachant que p est impair on en déduit que $\alpha = 1$ et que $p = 2^n + 1$. D'après le lemme 6, on en déduit que n est une puissance de 2 autrement dit p est un nombre premier de Fermat.
Réciproquement supposons que p soit de la forme $2^n + 1$ (où n est une puissance de 2) et montrons que le nombre $\zeta = e^{i\frac{2\pi}{p}}$ est constructible. D'après le théorème de Wantzel, il faut montrer que ζ appartient à une tour d'extensions quadratiques et cela va passer par l'étude du groupe de Galois de l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. On note $G = Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ le groupe des automorphismes du corps $\mathbb{Q}(\zeta)$. Notons que les éléments de G sont $\mathbb{Q}$-linéaires. Ainsi un élément $\sigma \in G$ est entièrement déterminé par l'image de ζ.
De plus le polynôme cyclotomique Φ_p est à coefficients rationnels de sorte que

$$\Phi_p(\sigma(\zeta)) = \sigma(\Phi_p(\zeta)) = \sigma(0) = 0$$

autrement dit $\sigma(\zeta)$ est une racine primitive p-ième de l'unité et il existe $k \in [\![1, p-1]\!]$ tel que $\sigma(\zeta) = \zeta^k$. Réciproquement pour $k \in [\![1, p-1]\!]$, l'application

$$\begin{array}{ccc} \mathbb{Q}[X] & \to & \mathbb{Q}(\zeta) \\ P & \mapsto & P(\zeta^k) \end{array}$$

est un morphisme d'anneaux surjectif et passe au quotient en un automorphisme de corps

$$\begin{array}{rccc} \sigma_k : & \mathbb{Q}[X]/\langle\Phi_p\rangle \simeq \mathbb{Q}(\zeta) & \to & \mathbb{Q}(\zeta) \\ & \zeta & \mapsto & \zeta^k \end{array}$$

On en déduit que l'application

$$\begin{array}{rcl}(\mathbb{Z}/p\mathbb{Z})^\times & \to & G \\ \overline{k} & \mapsto & \sigma_k\end{array}$$

est bien définie et est un isomorphisme de groupes.
Comme p est premier, le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique de cardinal $p-1=2^n$. On se donne g un générateur de G. On dispose d'une suite de sous-groupes

$$G = G_0 > G_1 > \cdots > G_n = 1$$

où $G_i = \langle g^{2^i} \rangle$. On en déduit une suite de sous-corps

$$\mathbb{Q} \subset L_0 \subset L_1 \subset \cdots \subset L_n = \mathbb{Q}(\zeta)$$

où $L_i = \mathbb{Q}(\zeta)^{G_i} = \mathbb{Q}(\zeta)^{g^{2^i}} = \{x \in \mathbb{Q}(\zeta) \quad | \quad g^{2^i}(x) = x\}$. Par multiplicativité du degré il vient

$$2^n = p - 1 = \varphi(p) = [\mathbb{Q}(\zeta) : \mathbb{Q}] = [L_0 : \mathbb{Q}] \prod_{0 \leq i \leq n-1} [L_{i+1} : L_i].$$

Pour en déduire que $[L_{i+1} : L_i] = 2$ pour tout $i \in [\![0, n-1]\!]$ et que $L_0 = \mathbb{Q}$ il suffit de montrer que L_i est strictement inclus dans L_{i+1} pour $i \in [\![0, n-1]\!]$.
Examinons le cas $L_0 \neq L_1$. On considère

$$z = \zeta + g^2(\zeta) + \cdots + g^{2n-2}(\zeta) = \sum_{h=0}^{2^{n-1}-1} g^{2h}(\zeta).$$

et comme g^{2^n} est l'identité on trouve

$$g^2(z) = g^2(\zeta) + g^4(\zeta) + \cdots + g^{2^n}(\zeta) = z$$

autrement dit $z \in L_1$. D'autre part la famille

$$\{\ g^i(\zeta) \quad | \quad i \in [\![0, 2^n - 1]\!]\ \} = \{\ g(\zeta^i) \quad | \quad i \in [\![0, 2^n - 1]\!]\ \}$$

est une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\zeta)$ en tant qu'image de la base $(1, \zeta, \ldots, \zeta^{2^n-1})$ par l'automorphisme $\mathbb{Q}$-linéaire g. On en déduit que

$$g(z) = g(\zeta) + g^3(\zeta) + \cdots + g^{2^n-1}(\zeta) \neq z$$

autrement dit $z \notin L_0$.
De façon similaire on montre que $L_i \neq L_{i+1}$ pour $i \in [\![1, n-1]\!]$. On considère pour cela

$$z = \zeta + g^{2^{i+1}}(\zeta) + g^{2^{i+2}}(\zeta) + \cdots + g^{2^{i+1}(2^{n-i-1}-1)}(\zeta) = \sum_{h=0}^{2^{n-i-1}-1} g^{2^{i+1}h}(\zeta).$$

On trouve d'une part

$$g^{2^{i+1}}(z) = g^{2^{i+1}}(\zeta) + g^{2^{i+2}}(\zeta) + \cdots + g^{2^n}(\zeta) = z$$

et d'autre part

$$g^{2^i}(z) = g^{2^i}(\zeta) + g^{3\times 2^i}(\zeta) + \cdots + g^{2^i(2^n - 2^{i+1})}(\zeta) = \sum_{h=0}^{2^{n-i-1}-1} g^{2^i(2h+1)}(\zeta) \neq z.$$

de sorte que $z \in L_{i+1} \setminus L_i$.

De tout ce qui précède on déduit le théorème de Gauss-Wantzel.

Théorème 11. *Soit $n \geq 2$. Alors le polygone régulier à n côtés est constructible à la règle et au compas si et seulement si n est de la forme $2^\alpha p_1 \dots p_r$ où $\alpha \in \mathbb{N}$ et $p_1, \dots, p_r$ sont des nombres premiers de Fermat deux à deux distincts.*

Exemple 12. *Les polygones réguliers à 3, 4, 5, 6, 8, 10, 12, 15, 16, 17 et 20 côtés sont constructibles mais les polygones réguliers à 7, 9, 11, 13, 14, 18 et 19 côtés ne le sont pas.*

Quelques remarques et compléments sur ce développement :

On peut tout à fait présenter le développement sans mentionner Galois mais l'idée générale de la théorie de Galois permet d'avoir un certain recul sur la preuve.

En général on parle plutôt de nombre réel constructible, qui sont les réels x tels que le point $(x, 0)$ soit constructible, et dont l'ensemble $\mathbb{E}$ forme un sous-corps de $\mathbb{R}$ stable par racine carrée. L'ensemble des nombres complexes constructibles est alors naturellement le sous corps $\mathbb{E}(i)$. Travailler directement sur les nombres complexes constructibles permet ici d'économiser un dévissage par la conjugaison complexe dans la tour d'extensions quadratiques : on construit $e^{i\frac{2\pi}{p}}$ et non pas $\cos(\frac{2\pi}{p})$.

Il vaut mieux maitriser les constructions élémentaires à la règle et au compas tels que :

1. Construire la parallèle à une droite passant par un point.
2. Construire la perpendiculaire à une droite passant par un point.
3. Construire la médiatrice d'un segment.
4. Construire la bissectrice d'un angle.
5. Construire la racine de x à partir de x.

Exemple 13. *Construction du pentagone régulier.*
On cherche à exprimer $\cos(\frac{2\pi}{5})$ *par radicaux. En exploitant les relations coefficients-racines pour le polynôme* $\Phi_5 = 1+X+X^2+X^3+X^4$ *et les formules de trigonométrie on trouve* $\cos(\frac{2\pi}{5}) = \frac{\sqrt{5}-1}{4} = \frac{\sqrt{\frac{5}{4}}-\frac{1}{2}}{2}$. *On en déduit une construction du pentagone régulier. On note O le point $(0,0)$ et on construit les points $A = (-1, 0)$ et $B = (0, 1)$. On construit ensuite le point $M = (-\frac{1}{2}, 0)$ qui est le mileu du segment OA. D'après le théorème de Pythagore, le segment MB est de longueur $\sqrt{\frac{5}{4}}$. Le cercle de centre M passant B intersecte l'axe des abcisses au point $C = (\sqrt{\frac{5}{4}} - \frac{1}{2}, 0)$. Reste à construire le milieu du segment OC et on termine facilement la construction du pentagone.*

La réciproque du corollaire 5. est fausse en général. En revanche, avec la théorie de Galois et en reprenant l'idée de la démonstration du théorème, c'est-à-dire le dévissage d'un 2-groupe puis la correspondance de Galois, on prouve le résultat suivant.

Théorème 14. *Soit $z \in \mathbb{C}$ un nombre algébrique. On note K le corps de décomposition du polynôme minimal de z sur $\mathbb{Q}$. Alors z est constructible si et seulement si $[K : \mathbb{Q}]$ est une puissance de 2.*

Recasages : 102, 125, 141, 151, 191 etc ?
Références : Théorie des corps, Carréga.