Carrega

Théorème de Gauss (polygones constructibles)

L'objectif est ici de décrire l'ensemble des polygones constructibles à la règle et au compas, ce qui revient à décrire les entiers $n \geq 2$ tels que $\zeta_n = \exp\left(\frac{2i\pi}{n}\right)$ soit constructible.

On rappelle le théorème de Wantzel ci-dessous, qui sera ensuite admis :

<u>Théorème (Wantzel):</u> Soit $z \in \mathbb{C}$. Alors z est constructible si et seulement s'il existe un entier $p \geq 1$ et une suite de sous-corps de $\mathbb{C}$, notée $K_1, \dots, K_p$, telle que $K_1 = \mathbb{Q}$, $z \in K_p$ et, pour tout $j \in [\![1, p-1]\!]$, on ait $K_i \subset K_{i+1}$ et $[K_{i+1} : K_i] = 2$.

On peut à présent passer au théorème principal :

<u>Théorème (Gauss):</u> Soit $n \geq 2$ un entier. Alors ζ_n est constructible si et seulement si les seuls facteurs premiers de n sont 2 ou des nombres premiers de Fermat (i.e des nombres premiers de la forme $2^n + 1$).

<u>Démonstration:</u>

- Soient $n, m \in \mathbb{N}^*$ premiers entre eux. Alors ζ_n et ζ_m sont constructibles si et seulement si ζ_{nm} l'est. En effet, si ζ_{nm} est constructible, $\zeta_n = \zeta_{nm}^m$ l'est aussi.
$\zeta_m = \zeta_{nm}^n$

Réciproquement, on suppose ζ_n et ζ_m constructibles. Le théorème de Bézout permet de fixer $a, b \in \mathbb{Z}$ tels que $an + bm = 1$. On a $\zeta_{nm} = \zeta_{nm}^{an+bm} = \zeta_{nm}^{an}\,\zeta_{nm}^{bm} = \zeta_m^a\,\zeta_n^b$, donc ζ_{nm} est constructible.

- Pour tout $n \in \mathbb{N}^*$, ζ_{2^n} est constructible.

- Soient p un nombre premier impair, et $\alpha \in \mathbb{N}^*$. Alors ζ_{p^α} est de degré $p^{\alpha-1}(p-1)$ sur $\mathbb{Q}$ (car son polynôme minimal sur $\mathbb{Q}$ est Φ_{p^α}), donc n'est pas constructible si $\alpha > 1$ par Wantzel, car son degré sur $\mathbb{Q}$ ne saurait alors être une puissance de 2.

• Soit p un nombre premier impair. On suppose ζ_p constructible. Par Wantzel, le degré de ζ_p sur $\mathbb{Q}$, qui vaut $p-1$, doit être une puissance de 2, ce qui force p à être de la forme 2^n+1, avec $n \in \mathbb{N}^*$.

• Soit $p = 2^n+1$ un nombre premier de Fermat. On va montrer que ζ_p est constructible. On pose $K = \mathbb{Q}(\zeta_p)$. On remarque ensuite que l'extension $K/\mathbb{Q}$ est de degré $p-1$, et qu'une $\mathbb{Q}$-base de K est donnée par $\mathcal{B} := (1, \zeta_p, \dots, \zeta_p^{p-2})$, ou encore par $\mathcal{B}' = (\zeta_p, \dots, \zeta_p^{p-1})$. On note G le groupe des automorphismes de K, qui induisent l'identité sur $\mathbb{Q}$. Un élément de G est de plus entièrement déterminé par son action sur ζ_p.

Soit $m \in \mathbb{N}^*$ premier à p. On va montrer qu'il existe un unique élément $g_m \in G$ tel que $g_m(\zeta_p) = \zeta_p^m$.

On considère pour cela les morphismes d'algèbre

$$ev_{\zeta_p} : \begin{array}{ccc} \mathbb{Q}[X] & \longrightarrow & \mathbb{C} \\ P(X) & \longmapsto & P(\zeta_p) \end{array} \qquad , \text{ qui induisent}$$

$$ev_{\zeta_p^m} : \begin{array}{ccc} \mathbb{Q}[X] & \longrightarrow & \mathbb{C} \\ P(X) & \longmapsto & P(\zeta_p^m) \end{array}$$

des isomorphismes de corps $\widetilde{ev}_{\zeta_p} : \mathbb{Q}[X]/(\Phi_p(X)) \longrightarrow \mathbb{C}$. Le morphisme de

$$\widetilde{ev}_{\zeta_p^m} : \mathbb{Q}[X]/(\Phi_p(X)) \longrightarrow \mathbb{C}$$

corps $g_m = \widetilde{ev}_{\zeta_p^m}^{-1} \circ \widetilde{ev}_{\zeta_p}$ convient alors.

L'application $\varphi : \begin{array}{ccc} G & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^* \\ g_k & \longmapsto & \overline{k} \end{array}$ est alors bien définie, et est un isomorphisme de groupes. En particulier, G est un groupe cyclique, dont on note g un générateur (qui est donc d'ordre 2^n). Pour tout $i \in [\![\,, n]\!]$, on pose $\tau_i := g^{2^i}$, et on note G_i le sous-groupe de G engendré par τ_i, qui est d'ordre 2^{n-i}.

On remarque de plus que l'on a $\{id_K\} = G_n \subset G_{n-1} \subset \dots \subset G_1 \subset G_0 = G$.

Pour tout $i \in [\![1, m]\!]$, on pose $K_i = \{x \in K \,/\, \tau_i(x) = x\}$, qui est un sous-corps de K contenant $\mathbb{Q}$. On a de plus $K_0 \subset K_1 \subset \dots \subset K_{m-1} \subset K_m$.

On va commencer par montrer que $K_0 = \mathbb{Q}$. Soit $x \in K_0$, que l'on écrit $x = \sum_{i=0}^{p-2} d_i \, g^i(\zeta_p)$ (décomposition dans $\mathcal{B}'$). On a $g(x) = \sum_{i=0}^{p-2} d_i \, g^{i+1}(\zeta_p) = d_{p-2}\zeta_p + \sum_{i=1}^{p-2} d_{i-1}\, g^i(\zeta_p)$, donc l'égalité $g(x) = x$ donne $d_0 = \dots = d_{p-2}$ (car $\mathcal{B}'$ est une $\mathbb{Q}$-base de K), donc $x = d_0 \sum_{i=0}^{p-2} g^i(\zeta_p) = d_0 \sum_{i=1}^{p-1} \zeta_p^i = -d_0 \in \mathbb{Q}$. Comme $\mathbb{Q} \subset K_0$, on a bien $K_0 = \mathbb{Q}$.

L'égalité $K_m = K$ vient du constat $\tau_m = \mathrm{id}_K$.

On va enfin prouver que, pour tout $i \in [\![1, m]\!]$, on a $[K_{i+1} : K_i] \leq 2$. Soit $i \in [\![1, m]\!]$.

On a $\tau_i(K_{i+1}) = K_{i+1}$, ce qui permet de parler de l'application K_i-linéaire $\tau_{i\,|K_{i+1}} : K_{i+1} \to K_{i+1}$.

On a $\tau_{i\,|K_{i+1}} \circ \tau_{i\,|K_{i+1}} = \tau_{i+1\,|K_{i+1}} = \mathrm{id}_{K_{i+1}}$, donc $\tau_{i\,|K_{i+1}}$ est annulé par le polynôme $X^2 - 1$, et est donc diagonalisable, de valeurs propres ± 1. Le sous-espace propre de $\tau_{i\,|K_{i+1}}$ associé à la valeur propre 1 est K_i. On pose $E_i = \ker(\tau_{i\,|K_{i+1}} + \mathrm{id}_{K_{i+1}})$. On a $K_{i+1} = K_i \oplus E_i$.

On suppose E_i non nul. Soient $x, x' \in E_i$ non nuls. On a $\tau_i\left(\frac{x}{x'}\right) = \frac{\tau_i(x)}{\tau_i(x')} = \frac{x}{x'}$, donc $\frac{x}{x'} =: d \in K_i$, ce qui donne $x = dx'$, puis $\dim_{K_i} E_i = 1$.

Ceci prouve que $[K_{i+1} : K_i] \leq 2$.

Par théorème de la base télescopique, on a $2^m = [K : \mathbb{Q}] = \prod_{i=0}^{m-1} \underbrace{[K_{i+1} : K_i]}_{\leq 2}$, donc $[K_{i+1} : K_i] = 2$ pour tout $i \in [\![0, m-1]\!]$. Par théorème de Wantzel, $\zeta_p \in K = \mathbb{Q}(\zeta_p)$ est constructible. Ceci achève la preuve du théorème.

On peut le mettre dans la leçon sur les anneaux principaux car on utilise des polynômes minimaux, un lemme des noyaux, (un théorème ?).