P. Maurer

ENS Rennes

Référence : Carrega, Théorie des corps.

Inspiré du travail de Florent Lemonnier et de Laura Gay.

Recasages : *(102), 125, 144, 151, 191.*

Théorème de Gauss-Wantzel

On commence par des rappels sur les nombres constructibles.

Définition 1. *Soit E un sous ensemble du plan $\mathbb{R}^2$.*

- *On dit qu'un point (x, y) est constructible sur E en une étape si (x,y) est l'intersection de deux objets parmi :*

  1. *L'ensemble des droites affines qui passent par deux éléments distincts de E*
  2. *L'ensemble des cercles dont le centre est un élément de E et le rayon est la distance. entre deux points distincts de E.*

  On note $C(E)$ l'ensemble des points constructibles sur E en une étape.

- *On définit par récurrence l'ensemble $C_n(E)$ des points constructibles sur E en n étapes par $C_{n+1}(E) = C(C_n(E))$.*

- *On dit que le point (x, y) est constructible sur E si $(x, y) \in \bigcup_{n=0}^{+\infty} C_n(E)$.*

- *Finalement, on dit qu'un nombre réel x est constructible si $(x, 0)$ est constructible sur $\{(0, 0), (0, 1)\}$.*

Proposition 2. *Soit x, y des nombres constructibles.*

Alors :

- *La somme $x + y$ est constructible.*
- *La différence $x - y$ est constructible.*
- *Le produit xy est constructible.*
- *Si $y \neq 0$, le quotient x / y est constructible.*
- *La racine carrée $\sqrt{x}$ est constructible.*

Théorème 3. *(Wantzel, 1837)*

Un nombre réel a est constructible si et seulement si il existe $n \in \mathbb{N}$ et une suite finie de corps $(L_i)_{1 \leq i \leq n}$ tels que :

- $L_0 = \mathbb{Q}$,
- $\forall i \in [\![1, n-1]\!] \quad L_i \subset L_{i+1}$ *et* $[L_{i+1} \colon L_i] = 2$,
- $a \in L_n$.

En particulier, tout nombre constructible est algébrique sur $\mathbb{Q}$ et son degré est une puissance de 2.

On trouve la preuve de ce théorème dans le Carrega, page 25.

Définition 4. *Soit $\theta \in \mathbb{R}$. On note $\hat{\theta}$ l'angle orienté dont une mesure en radian est θ. L'angle $\hat{\theta}$ est dit constructible si le point M du cercle de centre $O = (0,0)$ et de rayon 1 tel que $(\overrightarrow{\mathrm{OI}}, \overrightarrow{\mathrm{OM}}) = \hat{\theta}$, où $I = (1,0)$, est un point constructible.*

Proposition 5. *L'angle $\hat{\theta}$ est constructible si et seulement si le réel $\cos(\theta)$ est constructible.*

Lemme 6.

1. *Les angles de la forme $\dfrac{\widehat{2\pi}}{2^\alpha}$ sont constructibles pour $\alpha \in \mathbb{N}$.*
2. *Soient $n, m \in \mathbb{N}^*$ premiers entre eux. Alors l'angle $\dfrac{\widehat{2\pi}}{mn}$ est constructible si et seulement si les angles $\dfrac{\widehat{2\pi}}{m}$ et $\dfrac{\widehat{2\pi}}{n}$ le sont.*

Démonstration.

1. On construit l'angle $\dfrac{\widehat{2\pi}}{2}$ en traçant la bissectrice de l'angle $\widehat{2\pi}$, donc $\dfrac{\widehat{2\pi}}{2}$ est constructible. Par récurrence, on en déduit que $\dfrac{\widehat{2\pi}}{2^\alpha}$ est constructible pour $\alpha \in \mathbb{N}$.

2. Si $\dfrac{\widehat{2\pi}}{mn}$ est constructible, alors on a $\dfrac{\widehat{2\pi}}{m} = n \times \dfrac{\widehat{2\pi}}{mn}$ et $\dfrac{\widehat{2\pi}}{n} = m \times \dfrac{\widehat{2\pi}}{mn}$ donc $\dfrac{\widehat{2\pi}}{m}$ et $\dfrac{\widehat{2\pi}}{n}$ sont constructibles comme produits de nombres constructibles.

   Réciproquement, si $\dfrac{\widehat{2\pi}}{m}$ et $\dfrac{\widehat{2\pi}}{n}$ sont constructibles, le théorème de Bézout affirme qu'il existe $\lambda, \mu \in \mathbb{Z}$ tel que $\lambda m + \mu n = 1$, d'où $\dfrac{\widehat{2\pi}}{mn} = \dfrac{\widehat{2\pi}}{mn}(\lambda m + \mu n) = \lambda \dfrac{\widehat{2\pi}}{n} + \mu \dfrac{\widehat{2\pi}}{m}$. On en déduit que $\dfrac{\widehat{2\pi}}{mn}$ est constructible comme combinaison linéaire de nombres constructibles. □

Théorème 7. *(Gauss-Wantzel)*

Soit p un nombre premier impair, et $\alpha \in \mathbb{N}^*$. Alors l'angle $\dfrac{\widehat{2\pi}}{p^\alpha}$ est constructible si et seulement si $\alpha = 1$ et p est un nombre premier de Fermat, c'est-à-dire $p = 1 + 2^{2^\beta}$ pour un certain $\beta \in \mathbb{N}$.

Démonstration.

$\boxed{\Longrightarrow}$ On note $\omega = \exp\left(\dfrac{2i\pi}{p^\alpha}\right)$.

L'angle $\widehat{\frac{2\pi}{p^\alpha}}$ étant constructible, le réel $\cos\left(\frac{2\pi}{p^\alpha}\right)$ est constructible, donc d'après le théorème de Wantzel, $\cos\left(\frac{2\pi}{p^\alpha}\right)$ est algébrique sur $\mathbb{Q}$ et il existe $n \in \mathbb{N}^*$ tel que $\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{p^\alpha}\right)\right) : Q\right] = 2^n$.

Par ailleurs, on a $\omega + \omega^{-1} = 2\cos\left(\frac{2\pi}{p^\alpha}\right)$ donc $\omega^2 - 2\cos\left(\frac{2\pi}{p^\alpha}\right) + 1 = 0$.

On en déduit que $\left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\left(\frac{2\pi}{p^\alpha}\right)\right)\right] = 2$, donc par multiplicativité des degrés,

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = 2^{n+1}.$$

Or on sait que ω a pour polynome minimal sur $\mathbb{Q}$ le polynôme cyclotomique $\Phi_{p^\alpha} = \prod_{\zeta \in \mu_{p^\alpha}^*} X - \zeta$, dont le degré est donné par $\varphi(p^\alpha) = p^\alpha(p-1)$. Aussi, il vient $2^{n+1} = p^\alpha(p-1)$.

Comme p est un nombre premier impair, il faut que $\alpha = 0$ et on en déduit $p = 2^{n+1} + 1$, donc p est un nombre premier de Fermat.[1]

$\boxed{\Longrightarrow}$ Soit $p = 2^n + 1$ un nombre premier de Fermat, avec $n = 2^\beta$.

On va utiliser le théorème de Wantzel pour démontrer que $\cos\left(\frac{2\pi}{p}\right)$ est constructible. Montrons que ses hypothèses sont vérifiées.

Etape 1 : construction de la tour d'extensions quadratiques.

Notons $\omega = e^{\frac{2i\pi}{p}}$. Alors ω est une racine primitive $p^{\text{ème}}$ de l'unité, et en posant $K = \mathbb{Q}(\omega)$, le degré $[K : \mathbb{Q}]$ est égal au degré du $p^{\text{ème}}$ polynôme cyclotomique Φ_p, qui est le polynôme minimal de ω sur $\mathbb{Q}$. On en déduit que $[K : \mathbb{Q}] = p - 1 = 2^n$.

Ainsi, une base de K sur $\mathbb{Q}$ est donnée par $\mathcal{B} = \{1, \omega, \ldots, \omega^{p-2}\}$. Notons $G = \mathrm{Aut}(K)$ le groupe des automorphismes de corps de K sur lui-même. Un élément $g \in \mathrm{Aut}(K)$ fixe $\mathbb{Q}$ puisqu'il vérifie $g(1) = 1$ et $g(\alpha) = \alpha g(1) = \alpha$ pour $\alpha \in \mathbb{Q}$, et au vu de la base $\mathcal{B}$ de K sur $\mathbb{Q}$, g est donc entièrement déterminé par sa valeur en ω.

De plus, pour $g \in G$, on a $\Phi_p(g(\omega)) = g(\Phi_p(\omega)) = 0$, donc $g(\omega)$ est une racine primitive $p^{\text{ème}}$ de l'unité. On en déduit que G est un groupe d'ordre $p - 1$, et on peut alors écrire

$$G = \{1_K = g_1, g_2, \ldots, g_{p-1}\},$$

où pour tout $k \in [\![1, p-1]\!]$, g_k est déterminé par $g_k(\omega) = \omega^k$. Par ailleurs, l'application

$$\varphi : \left\{ \begin{array}{ccc} G & \to & (\mathbb{Z}/p\mathbb{Z})^* \\ g_k & \mapsto & \overline{k} \end{array} \right.$$

est un isomorphisme de groupe. Comme $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique, il en résulte qu'il existe $g \in G$ d'ordre $p - 1$ et on a ainsi $G = \{g^k : 0 \leq k \leq p-1\} = \{g^i : 1 \leq i \leq 2^n\}$, où $g^{p-1} = g^{2^n} = 1_K$.

Pour $i \in [\![0, n]\!]$, on pose alors $K_i := \{z \in K : g^{2^i}(z) = z\}$. Il est alors clair que $K_n = K$.

1. Pour justifier ce fait, posons $n + 1 = \lambda 2^\beta$ avec λ impair et $\beta \in \mathbb{N}$. On a alors $p = 1 + (2^{2^\beta})^\lambda = 1^\lambda - (-2^{2^\beta})^\lambda$ puisque λ est impair. La formule de Bernouilli donne $p = (1 - (-2^{2^\beta})) \cdot \sum_{k=0}^{\lambda-1} (-2^{2^\beta})^k$, donc $1 + 2^{2^\beta}$ divise p. Comme p est premier, il vient $p = 1 + 2^{2^\beta}$ donc $\lambda = 1$.

Etape 2 : on montre que les inclusions $K_i \subset K_{i+1}$ sont strictes pour $i \in [\![0, n-1]\!]$.

Vérifions tout d'abord que $K_0 \subsetneq K_1$: il s'agit de trouver $z \in K$ tel que $g^2(z) = z$ mais $g(z) \neq z$. On pose $z = \omega + g^2(\omega) + \cdots + g^{2^n-2}(\omega)$. Alors $g^2(z) = g^2(\omega) + g^4(\omega) + \cdots + g^{2^n}(\omega) = z$, mais

$$g(z) = g(\omega) + g^3(\omega) + \cdots + g^{2^n-1}(\omega) \neq z \quad \text{par unicité de la décomposition de } z \text{ dans } \mathcal{B}'.$$

De même, en considérant $z_i = \omega + g^{2^{i+1}}(\omega) + \cdots + g^{2^{i+1}[2^{n-i-1}-1]}(\omega)$, on vérifie que $g^{2^{i+1}}(z) = z$ mais $g^{2^i}(z) \neq z$ pour les mêmes raisons. Ainsi, on a $K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_n = K$.

Etape 3 : on vérifie que $K_0 = \mathbb{Q}$ et que $\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) \subset K_{n-1}$.

$\boxed{K_0 = \mathbb{Q}}$

D'une part, on a $\mathbb{Q} \subset K_0$ puisque g fixe les rationnels en tant qu'automorphisme de corps sur K. D'autre part, pour $z \in K_0$, décomposons z dans la base[2] $\mathcal{B}' = \{\omega, \ldots, \omega^{p-1}\} = \{\omega, g(\omega), \ldots, g^{p-2}(\omega)\}$:

$$z = z_0\, \omega + z_1\, g(\omega) + \cdots + z_{p-2}\, g^{p-2}(\omega).$$

On a alors

$$g(z) = z_0\, g(\omega) + \cdots + z_{p-3}\, g^{p-2}(\omega) + z_{p-2}\, \omega.$$

Comme $g(z) = z$, on en déduit que $z_0 = z_1 = \cdots = z_{p-2}$, et donc

$$z = z_0(\omega + g(\omega) + \cdots + g^{p-2}(\omega)) = z_0\,(\omega + \omega^2 + \cdots + \omega^{p-1}) = -z_0 \in \mathbb{Q}$$

Donc $\mathbb{Q} = K_0$.

$\boxed{\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) \subset K_{n-1}}$ [3]

On note $f = g^{2^{n-1}}$, de sorte que $K_{n-1} = \{z \in K \ : \ f(z) = z\}$. Par hypothèse, f est déterminée par $f(\omega) = \omega^\lambda$ pour un certain $\lambda \in \mathbb{Z}$. De plus, on a $f^2 = g^{2^{n-1} \times 2} = 1_K$, donc

$$\omega = f^2(\omega) = f(f(\omega)) = f(\omega^\lambda) = (f(\omega))^\lambda = (\omega^\lambda)^\lambda = \omega^{\lambda^2}.$$

Ainsi, on a $\omega^{\lambda^2 - 1} = 1$. Il s'en suit que p divise $\lambda^2 - 1$, donc dans $\mathbb{Z}/p\mathbb{Z}$, on a l'égalité $\overline{\lambda}^2 = \overline{1}$, donc $\overline{\lambda} = \pm\overline{1}$. Il est clair que $\overline{\lambda} \neq \overline{1}$ puisque dans ce cas, on aurait $f = 1_K$, donc $\overline{\lambda} = \overline{-1}$, et $f(\omega) = \omega^{-1}$.

Ainsi,

$$f\left(\cos\left(\frac{2\pi}{p}\right)\right) = f\left(\frac{1}{2}(\omega + \omega^{-1})\right) = \frac{1}{2}\,(f(\omega) + f(\omega)^{-1}) = \frac{1}{2}\,(\omega + \omega^{-1}) = \cos\left(\frac{2\pi}{p}\right).$$

Donc $\cos\left(\frac{2\pi}{p}\right) \in K_{n-1}$, et de fait, $\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) \subset K_{n-1}$.

2. On sait que $\mathcal{B} = \{1, \omega, \ldots, \omega^{p-2}\}$ est une base de K, donc on peut en déduire que $\mathcal{B}$ est aussi une base au vu de la relation $\omega^{p-1} = -\omega^{p-2} - \cdots - \omega - 1$.

3. En fait, on peut se passer de ce résultat en remarquant simplement que $\left[\mathbb{Q}(\omega) \colon \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)\right] = 2$, comme on l'a démontré dans le sens direct. Il s'en suit en effet que $\cos\left(\frac{2\pi}{p}\right) \in \mathbb{Q}(\omega) = K = K_n$, ce qui suffit pour avoir le troisième point dans les hypothèses du théorème de Wantzel. Le théorème étant déjà long, il vaut sans doute mieux procéder ainsi à l'oral.

Etape 4 : conclusion.

Par multiplicativité des degrés, on a $2^n = [\mathbb{Q}(\omega) \colon \mathbb{Q}] = \prod_{i=0}^{n-1} [K_{i+1} \colon K_i]$, où $[K_{i+1} \colon K_i] \geq 2$ d'après l'étape 2. On en déduit que $[K_{i+1} \colon K_i]$ vaut exactement 2.

En particulier, comme $\left[\mathbb{Q}(\omega) \colon \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)\right] = 2$ et que $\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) \subset K_{n-1}$, on en déduit l'égalité $\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) \subset K_{n-1}$.

D'après le théorème de Wantzel, il suit que $\cos\left(\frac{2\pi}{p}\right)$ est constructible, et donc l'angle $\widehat{\frac{2\pi}{p}}$ est constructible. $\square$