# Feuille de TD n° 9

**Exercice 1 (Le corps des nombres constructibles)** Soit $\mathcal{C}$ le plus petit sous-corps de $\mathbb{R}$ stable par $\sqrt{\ }$. On appelle $\mathcal{C}$ *le corps des nombres constructibles.*

a) Montrer que $\cos\frac{2\pi}{5}$, $\cos\frac{2\pi}{15}$ et $\cos\frac{2\pi}{17}$ sont constructibles.

b) Vérifier qu'un nombre est constructible si et seulement s'il existe une suite finie $a_1, ..., a_n \in \mathbb{R}_{>0}$ tels que

$$x \in \mathbb{Q}\left(\sqrt{a_1}, ..., \sqrt{a_n}\right)$$

et

$$\forall 1 \leq i \leq n,\ a_i \in \mathbb{Q}(\sqrt{a_1}, ..., \sqrt{a_{i-1}})\ .$$

Montrer que $x$ est constructible si et seulement si son polynôme minimal a un groupe de Galois de degré une puissance de 2 (autrement dit si et seulement si $x$ est dans une extension galoisienne de $\mathbb{Q}$ de degré une puissance de 2).

c) Montrer que $\sqrt[3]{2}$ n'est pas constructible. Et pour $\cos\frac{2\pi}{9}$ ?

d) Montrer que $\cos 2\pi/n$ est constructible si et seulement si $n = 2^r p_1 ... p_s$ où $p_1 < ... < p_s$ sont des nombres premiers de la forme : $p_i = 2^{2^{k_i}} + 1$.

**Exercice 2 (Un nombre de degré 4 non constructible)** Soit $P(X) = X^4 - X - 1 \in \mathbb{Q}[X]$.

a) Montrer que $P$ est irréductible $\bmod 2$. En déduire que $P$ est irréductible sur $\mathbb{Q}$.

b) On note $x_1, x_2, x_3, x_4$ les racines de $P$ dans $\mathbb{C}$. On pose $z_1 = x_1 + x_2$, $z_2 = x_1 + x_3$, $z_3 = x_1 + x_4$. En utilisant les relations entre les coefficients du polynôme $P$ et ses racines $x_i$, montrer que :

$$(X - z_1^2)(X - z_2^2)(X - z_3^2) = X^3 + 4X - 1\ .$$

c) En déduire que les $x_i$ ne sont pas constructibles ! *Indication. Le polynôme $X^3 + 4X - 1$ est irréductible sur $\mathbb{Q}$.*

**Exercice 3 (Les points constructibles à la règle et au compas)** Dans le plan $\mathbb{R}^2$ on définit par récurrence : $P_0 = \{0, 1\}$, et si $n \geq 1$, $P_n$ est l'ensemble des points de $P_{n-1}$ et des points obtenus de la manière suivante :

- on trace toutes les droites reliant deux points de $P_{n-1}$, tous les cercles centrés en un point de $P_{n-1}$ et de rayon une distance entre deux points de $P_{n-1}$ ;

– on prend toutes les intersections obtenues (entre deux droites, deux cercles, un cercle et une droite).

On appelle $\cup_{n\geq 0} P_n \subset \mathbb{R}^2$ l'ensemble des points *constructibles à la règle et au compas.*

(a) Déterminer $P_1$ et $P_2$.

(b) On rappelle que l'on peut construire à la règle et au compas la médiatrice de deux points, la perpendiculaire à une droite passant par un point donné, la parallèle à une droite passant par un point donné. En déduire que si $z_1, z_2$ sont constructibles, alors $z_1 + z_2, z_1 - z_2, z_1 z_2, z_1/z_2$ le sont aussi.

(c) Montrer que les racines carrées d'un nombre constructible le sont aussi.

(d) Montrer qu'un $x \in \mathbb{R}$ est constructible si et seulement si $x$ est l'abscisse d'un point dans $\mathbb{R}^2$ est constructible à la règle et au compas.

**Exercice 4 Extension cyclique de degré *p* en caractéristique *p***

Soit $k$ un corps de cractéristique $p > 0$.

a) Soit $a \in k$. Montrer que si le polynôme

$$X^p - X - a$$

n'a pas de racines dans $k$, alors il est irréductible sur $k$. *Indication. Vérifier que si $x$ est une racine, les autres sont les $x+i$, $i = 0, 1, ..., p-1 \in k$.*

Dans ce cas, si $x$ une racine de $X^p - X - a$ (*qui n'est pas dans $k$*), vérifier que l'extension

$$k(x)/k$$

est cyclique de degré $p$.

b) **Réciproquement.** Soit $K/$ une extension galoisienne cyclique de degré $p$. Montrer qu'il existe $x \in K$ tel que $K = k(x)$ et $x$ est racine d'un polynôme

$$X^p - X - a$$

pour un certain $a \in k$.

*Indication.* Soit $\sigma$ un générateur du groupe $\mathrm{Gal}(K/k)$. Montrer que le $k-$endomorphisme

$$\mathrm{Id} - \sigma \,:\, K \to K$$

est nilpotent. Soit $y \in \ker(\mathrm{Id} - \sigma)^2 \setminus \ker(I - \sigma)$. Poser

$$x = \frac{y}{\sigma(y) - y}\,,$$

vérifier que $\sigma(x) = x + 1$ et conclure.