ENS Lyon — Algèbre 2
L3 — 2016-2017

DM n°2

On identifie le plan et le corps $\mathbb{C}$. On défini par récurrence $P_0 = \{0, 1\}$, et si $n \geqslant 1$, P_n est l'union de P_{n-1} et de l'ensemble des points de $\mathbb{C}$ constructibles (à la règle et au compas) en un coup à partir de P_{n-1}. On note $\mathcal{C} = \bigcup_{n\geqslant 0} P_n \subset \mathbb{C}$, c'est-à-dire l'ensemble des points constructibles à la règle et au compas. On admet le résultat ci-dessous :

Exercice 1. [Généralités sur les points constructibles]

1. Déterminer P_1 et P_2.
2. Montrer que si $z_1, z_2 \in \mathbb{C}$ sont dans $\mathcal{C}$, alors $z_1 + z_2$, $z_1 - z_2$, $z_1 z_2$ et z_1/z_2 le sont aussi.
3. Montrer que si $z \in \mathbb{C}$ est dans $\mathcal{C}$ alors ses racines carrées le sont aussi.

Exercice 2. [Constructibilité des polygones réguliers]
Pour cet exercice, nous utiliserons le résultat ci-dessous (admis) :

Théorème 1. Un point $z \in \mathbb{C}$ appartient à $\mathcal{C}$ si et seulement s'il appartient à une extension normale de $\mathbb{Q}$ de degré une puissance de 2.

Dans cet exercice, on notera μ_n l'ensemble des racines n-ième de l'unité, et μ_n^* le sous-ensemble des racines primitives n-ième de l'unité. On note $\mathbb{Q}(\mu_n)$ l'extension de $\mathbb{Q}$ engendrée par les éléments de μ_n.

1. Montrer que $\mathbb{Q}(\mu_n)/\mathbb{Q}$ est une extension normale.
2. Montrer que le groupe des $\mathbb{Q}$-automorphismes de $\mathbb{Q}(\mu_n)$ est isomorphe à un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$.
3. On rappelle que le n-ème polynôme cyclotomique est le polynôme $\phi_n(X) = \prod_{\zeta\in\mu_n^*}(X - \zeta)$. C'est un polynôme de $\mathbb{Z}[X]$, unitaire de degré $\varphi(n)$ et on a que $X^n - 1 = \prod_{d|n} \phi_d(X)$. L'objectif de cette question est de montrer que ϕ_n est le polynôme minimal sur $\mathbb{Q}$ de tout élément de μ_n^*. On considère donc $\zeta \in \mu_n^*$ quelconque et P son polynôme minimal sur $\mathbb{Q}$.
   (a) Montrer que $P \in \mathbb{Z}[X]$ et qu'il existe $Q \in \mathbb{Q}[X]$ tel que $X^n - 1 = PQ$.
   (b) Soit p un entier premier quelconque. Supposons que ζ^p n'est pas une racine de P. Montrer qu'il existe $R \in \mathbb{Z}[X]$ tel que $Q(X^p) = PR$.
   (c) En réduisant modulo p, montrer que dans $\mathbb{F}_p[X]$, on a : $(X^n - 1)^p = P(X)^{p+1}R(X)$.
   (d) En déduire une contradiction.
   (e) Montrer alors que $P = \phi_n$.
4. Montrer que $[\mathbb{Q}(\mu_n) : \mathbb{Q}] = \varphi(n)$ et que le groupe des $\mathbb{Q}$-automorphismes de $\mathbb{Q}(\mu_n)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$.
5. Dans ce qui suit, on note P_n le polygone régulier à n côtés (inscrit dans le cercle de centre 0 et de rayon 1. Nous nous proposons de montrer que P_n est constructible (i.e ses sommets appartiennent à $\mathcal{C}$) si et seulement si $n = 2^r p_1 ... p_s$, où p_i est un nombre premier de la forme $2^{2^{k_i}} + 1$, avec $k_i \in \mathbb{N}$.
   (a) Montrer que P_n est constructible si et seulement si $\zeta_n = e^{\frac{2i\pi}{n}} \in \mathcal{C}$.
   (b) Montrer que $\zeta_n \in \mathcal{C}$ équivaut à dire que $\varphi(n)$ est une puissance de 2.
   (c) Soit p un nombre premier impair tel que $p - 1$ est une puissance de 2. Montrer alors qu'il existe $k \in \mathbb{N}$ tel que $p = 2^{2^k} + 1$.
   (d) Conclure.

Exercice 3. [Un élément algébrique de degré 4 non constructible]

1. Montrer que le polynôme $P(X) = X^4 - X - 1$ est irréductible sur $\mathbb{Q}$ et possède 4 racines distinctes notées z_1, z_2, z_3, z_4 dans $\mathbb{C}$.
2. Montrer que $u = z_1 z_2 + z_3 z_4$ est racine du polynôme $X^3 + 4X - 1$ (ind. on pourra remarquer que $u = t - 1/t$ où $t = z_1 z_2$ et calculer $u^4 + 4u^2 - u$).
3. En déduire que, pour tout i, z_i n'appartient pas à $\mathcal{C}$.