DM

à rendre le 8 avril

Exercice 1.

Soit $n \in \mathbb{N}^*$ un entier, $\mathbb{U}_n \subset \mathbb{C}$ l'ensemble des racines n-ièmes de l'unité et $\mathbb{U}_n^*$ l'ensemble des racines primitives n-ièmes de l'unité, c'est-à-dire l'ensemble des générateurs de $\mathbb{U}_n$. On note $\Phi_n(X) = \prod_{x \in \mathbb{U}_n^*} (X - x)$, que l'on appelle n-ième polynôme cyclotomique.

1. (a) Montrer que $X^n - 1 = \prod_{d|n} \Phi_d(X)$.
   (b) Montrer que $\Phi_n \in \mathbb{Z}[X]$.
   (c) Montrer que pour tous $s \geqslant 1$ réel et $n \geqslant 2$ entier, $|\Phi_n(s)| > |s-1|$.
2. Soit K un corps de caractéristique ne divisant pas n. Montrer que $X^n - 1 \in K[X]$ n'a pas de facteur carré.
3. On se propose de montrer que Φ_n est irréductible dans $\mathbb{Q}[X]$.
   (a) Justifier qu'il existe deux polynômes F et G de $\mathbb{Z}[X]$, avec F irréductible, tels que $\Phi_n = FG$.
   (b) Montrer que pour tout nombre premier p ne divisant pas n, les polynômes $F(X)$ et $G(X^p)$ sont premiers entre eux dans $\mathbb{Z}[X]$.
   (c) En déduire que pour tout p premier ne divisant pas n, l'ensemble des racines de F dans $\mathbb{C}$ est stable par l'application $x \mapsto x^p$.
   (d) Conclure.
4. Soit A un anneau fini, unitaire, dont tout élément non nul possède un inverse. Le but de cette question est de montrer que A est commutatif.
   (a) Soit K le centre de A. Montrer que K est un corps fini.
   (b) On note $q = |K|$. Soit B un sous-anneau de A contenant K. Montrer qu'il existe $n \geqslant 1$ et r divisant n tels que $|A| = q^n$ et $|B| = q^r$.
   (c) Pour $x \in A \setminus \{0\}$, on note $C_x = \{yxy^{-1} \mid y \in A \setminus \{0\}\}$. Montrer qu'il existe $r \geqslant 1$ divisant n tel que $|C_x| = \frac{q^n-1}{q^r-1}$.
   (d) En décomposant $A \setminus \{0\}$ en réunion de parties de la forme C_x, montrer que $\Phi_n(q)$ divise $q-1$, où Φ_n est le n-ième polynôme cyclotomique.
   (e) En déduire que $n = 1$. Conclure.
   On pourra utiliser la question 1.(c).

Exercice 2.

1. Soit K un corps de caractéristique $p > 0$. Soit L une extension finie de K, avec $[L : K] \wedge p = 1$. Montrer que c'est une extension séparable.
2. Soit $K = \mathbb{Q}(\sqrt{5})$ et $L = \mathbb{Q}(\sqrt{1+\sqrt{5}})$. Montrer que $K/\mathbb{Q}$ et L/K sont des extensions normales. L'extension $L/\mathbb{Q}$ est-elle normale ?