Université Paul Sabatier — Novembre 2014

Devoir L3 — **Algèbre**

Dans tout ce qui suit, un nombre premier impair p est fixé. On suppose choisie une fois pour toutes une racine p-ème de l'unité $\zeta \neq 1$. On pose $\lambda = 1 - \zeta$.

On rappelle que le polynôme cyclotomique associé à p est :

$$\Phi_p = 1 + X + X^2 + \cdots + X^{p-1}\,.$$

1) Montrer sans calculs que l'ensemble

$$\mathbf{Q}[\zeta] = \{a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1} \mid (a_0, \ldots, a_{p-1}) \in \mathbf{Q}^p\}$$

est un sous-anneau de $\mathbf{C}$.

2) Montrer qu'il existe un unique isomorphisme d'anneaux

$$\mathbf{Q}[X]/(\Phi_p) \simeq \mathbf{Q}[\zeta]$$

qui envoie la classe de X sur ζ.

3) Montrer que

$$\mathbf{Z}[\zeta] = \{a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1} \mid (a_0, \ldots, a_{p-1}) \in \mathbf{Z}^p\}$$

est un sous-anneau de $\mathbf{C}$ et qu'il existe un unique isomorphisme d'anneaux

$$\mathbf{Z}[X]/(\Phi_p) \simeq \mathbf{Z}[\zeta]$$

qui envoie la classe de X sur ζ.

4) Déduire de la question 3) que, pour tout entier i tel que $\zeta^i \neq 1$, il existe un unique morphisme d'anneaux

$$\pi_i : \mathbf{Q}[\zeta] \to \mathbf{Q}[\zeta]$$

qui envoie ζ sur ζ^i. Déduire de la question 4) que le morphisme π_i induit un isomorphisme de $\mathbf{Z}[\zeta]$ sur lui-même.

4 bis) Montrer que tout morphisme d'anneaux $\varphi : \mathbf{Q}[\zeta] \to \mathbf{Q}[\zeta]$ est de la forme $\varphi = \pi_i$ pour un certain entier i tel que $\zeta^i \neq 1$. Donner une description explicite du groupe des automorphismes du corps $\mathbf{Q}[\zeta]$ (i.e. des morphismes d'anneaux bijectifs de $\mathbf{Q}[\zeta]$ vers lui même).

5) Déduire de la factorisation de Φ_p en produits de facteurs premiers dans $\mathbf{C}[X]$ que

$$\prod_{i=1}^{p-1}(1 - \zeta^i) = p\,.$$

6) Montrer qu'il existe un unique morphisme d'anneaux

$$\mathbf{F}_p \to \mathbf{Z}[\zeta]/(\lambda)$$

et que ce dernier est bijectif.

7) Montrer que, pour $1 \leqslant i \leqslant p-1$, le quotient $\varepsilon_i = \frac{1-\zeta^i}{1-\zeta}$ est dans $\mathbf{Z}[\zeta]$. En déduire que ε_i est inversible dans $\mathbf{Z}[\zeta]$. Montrer que

$$p = \varepsilon \lambda^{p-1}$$

où on a posé $\varepsilon = \varepsilon_1 \cdots \varepsilon_{p-1}$.

On note

$$N : \mathbf{Q}[\zeta] \to \mathbf{Q}$$

l'application définie comme suit. Pour $x \in \mathbf{Q}[\zeta]$, la multiplication par x définit une application $\mathbf{Q}$-linéaire

$$\begin{aligned} m_x : \mathbf{Q}[\zeta] &\to \mathbf{Q}[\zeta] \\ y &\mapsto xy \end{aligned}$$

et on pose

$$N(x) = \det(m_x)\,.$$

On remarque immédiatement que $N(x) = 0$ si et seulement si $x = 0$ et que $N(xy) = N(x)N(y)$ pour tous $x, y \in \mathbf{Q}[\zeta]$.

8) Soit x un élément de $\mathbf{Z}[\zeta]$. Montrer que x est inversible dans $\mathbf{Z}[\zeta]$ si et seulement si $|N(x)| = 1$.