Université Paris 7-Denis Diderot
Maîtrise de mathématiques et informatique

Algèbre et Géométrie
Année 2002-03
L. Merel - P. Perrin

**EXAMEN PARTIEL du 4 décembre 2003**

**Durée : 3 h**

*L'usage des calculatrices, téléphones et de tout document est interdit.*

Soit $n$ un entier $\geq 1$. Soit $\zeta$ une racine primitive $n$-ième de l'unité dans $\mathbf{C}$ (c'est-à-dire un élément d'ordre $n$ de $\mathbf{C}^*$). Notons $\mathbf{Q}(\zeta)$ le sous-corps de $\mathbf{C}$ engendré par $\zeta$. Soit $P$ le polynôme minimal de $\zeta$ dans $\mathbf{Q}[X]$.

On note $\phi$ la fonction indicatrice d'Euler, *i.e.* $\phi(n)$ est l'ordre de $(\mathbf{Z}/n\mathbf{Z})^*$. On rappelle que tout polynôme unitaire de $\mathbf{Q}[X]$ divisant un polynôme unitaire de $\mathbf{Z}[X]$ est lui-même dans $\mathbf{Z}[X]$. On rappelle qu'un conjugué sur $\mathbf{Q}$ d'un nombre algébrique $x \in \mathbf{C}$ est un zéro du polynôme minimal de $x$ dans $\mathbf{Q}[X]$.

## I

**1.** Combien y a-t-il de racines primitives $n$-ièmes de l'unité dans $\mathbf{C}^*$ ?
**2.** Montrer que $P$ divise le polynôme $X^n - 1$ et que $P \in \mathbf{Z}[X]$.
**3.** Montrer que tout conjugué de $\zeta$ est une racine primitive $n$-ième de l'unité. En déduire que l'extension $\mathbf{Q}(\zeta)|\mathbf{Q}$ est de degré $\leq \phi(n)$.
**4.** Montrer que toute racine primitive $n$-ième de l'unité est une puissance de $\zeta$. En déduire que l'extension $\mathbf{Q}(\zeta)|\mathbf{Q}$ est normale.
**5.** Montrer que si pour tout entier $m > 0$, premier à $n$, $\zeta^m$ est une racine de $P$, le polynôme $P$ est de degré $\phi(n)$.

## II

Soit $p$ un nombre premier ne divisant pas $n$.

**1.** Montrer que le polynôme $X^n - 1 \in \mathbf{F}_p[X]$ n'a pas de racine double dans une clôture algébrique de $\mathbf{F}_p$.
**2.** Notons $Q$ le polynôme minimal de $\zeta^p$ dans $\mathbf{Z}[X]$. Montrer que $\zeta$ est une racine de $Q(X^p)$. En déduire que $P$ divise $Q(X^p)$.
**3.** Montrer que $Q(X^p) \equiv Q(X)^p \pmod{p}$.
**4.** Notons $\bar{P}$ et $\bar{Q}$ les images de $P$ et $Q$ dans $\mathbf{F}_p[X]$. Montrer que $\bar{P}$ divise $X^n - 1$ dans $\mathbf{F}_p[X]$. En supposant que $P \neq Q$, montrer que $PQ$ divise $X^n - 1$, puis que $\bar{Q}^2$ divise $X^n - 1 \in \mathbf{F}_p[X]$. En déduire que $P = Q$.
**5.** Démontrer, à l'aide de **I**, que $P$ est de degré $\phi(n)$.

## III

Notons $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ le groupe de Galois de l'extension $\mathbf{Q}(\zeta)|\mathbf{Q}$.

**1.** Montrer que pour tout $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$, il existe $i_\sigma \in \mathbf{Z}$ tel que $\sigma(\zeta) = \zeta^{i_\sigma}$.
**2.** Montrer que l'application $\sigma \mapsto i_\sigma + n\mathbf{Z}$ définit un isomorphisme de groupes $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) \simeq (\mathbf{Z}/n\mathbf{Z})^*$.
**3.** Lorsque $n = 125$, démontrer qu'il existe une extension cyclique $K|\mathbf{Q}$ de degré 4 telle que $K \subset \mathbf{Q}(\zeta)$.