P.-V Koseleff

Partiel

le 30 octobre 2007

Durée 2 heures.

Tous documents interdits. On attachera le plus grand soin à la qualité de la rédaction, à la présentation et à la rigueur des démonstrations. L'exercice 4 est indépendant des autres.

On rappelle, à toutes fins utiles, que dans un groupe fini, on a $\operatorname{ord}(a^k) = \dfrac{\operatorname{ord}(a)}{(k, \operatorname{ord}(a))}$.

EXERCICE 1. — Soit k un corps et P un polynôme unitaire de $k[X]$. On note P' le polynôme dérivé de P.

1. Soit $Q \in k[X]$. Montrer que si Q^2 divise P alors Q divise P'.
2. En déduire que si $(P, P') = 1$, P n'a pas de facteur carré dans sa décomposition en produits d'irréductibles dans $k[X]$.
3. Soit p un nombre premier ne divisant pas n et $P = X^n - 1$.
   (a) Montrer que $(P, P') = 1$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$.
   (b) En déduire que $X^n - 1$ n'a pas de facteur carré dans $(\mathbb{Z}/p\mathbb{Z})[X]$.
4. Montrer que $X^n - 1$ a n racines distinctes dans $\mathbb{C}$.

EXERCICE 2. — Polynômes cyclotomiques

Pour tout entier n, on note $\mathbb{C}_n = \{x \in \mathbb{C}; x^n = 1\}$, $H_n = \{x \in \mathbb{C}; \operatorname{ord}(x) = n\}$ et on pose $\Phi_n = \prod_{a \in H_n} (X - a)$.

On rappelle que $\mathbb{C}_n$ est un groupe cyclique de cardinal n.

1. Montrer que $\prod_{d|n} \Phi_d = X^n - 1$.
2. Calculer $\Phi_1, \Phi_2, \Phi_3, \Phi_4, \Phi_5, \Phi_6, \Phi_{12}$.
3. Montrer que pour tout $n \in \mathbb{N}$, Φ_n est unitaire et appartient à $\mathbb{Z}[X]$.
   (Ind : *on pourra faire une récurrence et utiliser la division euclidienne*)

EXERCICE 3. — Irréductibilité des polynômes cyclotomiques

Soit P un diviseur irréductible de $X^n - 1$ dans $\mathbb{Z}[X]$. Notons $X^n - 1 = PQ$.

1. Soit $\alpha \in \mathbb{C}$ tel que $P(\alpha) = 0$ et p un nombre premier ne divisant pas n. On suppose que $P(\alpha^p) \neq 0$.
   (a) Montrer que $Q(\alpha^p) = 0$.
   (b) En déduire que P divise $Q(X^p)$. (*Ind : on pourra considérer* $I = \{R \in \mathbb{Q}[X], R(\alpha) = 0\}$).
   (c) Montrer que $Q(X^p) = Q(X)^p$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$.
   (d) En déduire que $X^n - 1$ a un facteur carré dans $(\mathbb{Z}/p\mathbb{Z})[X]$.
2. Soit $\alpha \in \mathbb{C}$ tel que $P(\alpha) = 0$.
   (a) Soit p un nombre premier ne divisant pas n. Montrer que $P(\alpha^p) = 0$.
   (b) Soit k un entier premier avec n. Montrer que $P(\alpha^k) = 0$.
3. En déduire que Φ_n est irréductible dans $\mathbb{Z}[X]$.

EXERCICE 4. — Soit k un corps. On considère l'homomorphisme d'anneaux $\varphi : k[U,V] \longrightarrow k[X]$ défini par $\varphi(U) = X^3$ et $\varphi(V) = -X^2$ et tel que $\varphi(a) = a$ pour tout $a \in k$.

1. Quel est le noyau de φ ?
2. Déterminer le sous-anneau A de $k[X]$, image de φ.
3. Montrer que A est intègre et que son corps des fractions est isomorphe à $k(X)$.

EXERCICE 5. — BONUS

1. Quel est le degré de Φ_n ?
2. Montrer que si n est impair, $\Phi_{2n}(X) = (-1)^{\deg \Phi_n} \Phi_n(-X)$.
3. Montrer que si n est pair, $\Phi_{2n}(X) = \Phi_n(X^2)$.