Université Paris 7-Denis Diderot — Algèbre
M1 mathématiques — Année 2007-08
L. Merel – R. Mneimné

EXAMEN du 18 janvier 2008

Durée : 3 h

L'usage de tout document autre que le polycopié ou une feuille de notes personnelles est interdit.

Pour n entier impair ≥ 3, considérons ζ_n une racine primitive n-ème de l'unité dans $\mathbf{C}$. Notons $\Phi_n \in \mathbf{Z}[X]$ le n-ème polynôme cyclotomique. Posons $\alpha_n = \zeta_n + \zeta_n^{-1}$. Notons $\phi(n)$ le cardinal de $(\mathbf{Z}/n\mathbf{Z})^*$. On rappelle que le polynôme Φ_n est de degré $\phi(n)$ et est irréductible sur $\mathbf{Q}$.

Considérons le polynôme $\Phi_n^+ = \prod_k (X - \zeta_n^k - \zeta_n^{-k})$, où k parcourt les entiers premiers à n vérifiant $1 \leq k \leq n/2$.

On rappelle que l'extension $\mathbf{Q}(\zeta_n)|\mathbf{Q}$ est galoisienne de groupe de Galois canoniquement isomorphe à $(\mathbf{Z}/n\mathbf{Z})^*$; cet isomorphisme associe à σ la classe modulo n d'un entier k tel que $\sigma(\zeta_n) = \zeta_n^k$.

I

1. Montrer que le groupe (multiplicatif) $(\mathbf{Z}/63\mathbf{Z})^*$ est isomorphe au groupe (additif) $\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$.
2. Ces groupes sont-ils isomorphes à l'un des groupes suivants : $\mathbf{Z}/36\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$?
3. Suivant les valeurs du nombre premier p, combien la composante p-primaire de $\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ possède-t-elle d'éléments ?
4. Montrer que tout sous-groupe d'ordre 4 de $\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ est égal à la composante 2-primaire du groupe $\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$.
5. Montrer que $(\mathbf{Z}/63\mathbf{Z})^*$ possède un unique sous-groupe d'ordre 4, que l'on donnera explicitement.

II

1. Calculer Φ_7 et Φ_9.
2. Montrer que $X^{\phi(n)/2}\Phi_n^+(X + X^{-1}) = \Phi_n(X)$.
3. Calculer Φ_7^+ et Φ_9^+.
4. Montrer que la réduction modulo 3 de Φ_7^+ est irréductible sur le corps $\mathbf{F}_3$.
5. Sur quels corps finis de caractéristique 3 cette réduction est-elle scindée ?

III

1. Montrer que $\mathbf{Q}(\zeta_{63}) = \mathbf{Q}(\zeta_7, \zeta_9)$. Placer dans un diagramme les corps $\mathbf{Q}$, $\mathbf{Q}(\zeta_7)$, $\mathbf{Q}(\zeta_9)$ et $\mathbf{Q}(\zeta_{63})$. On indiquera les degrés des extensions qui interviennent.
2. Montrer que $\mathbf{Q}(\alpha_n) \subset \mathbf{Q}(\zeta_n)$ et que $\mathbf{Q}(\alpha_n) \subset \mathbf{R}$.
3. Montrer que l'extension $\mathbf{Q}(\zeta_n)|\mathbf{Q}(\alpha_n)$ est de degré 2. Quel est le degré de l'extension $\mathbf{Q}(\alpha_n)|\mathbf{Q}$? Application à $n = 9$ et $n = 7$.
4. Reprendre le diagramme tracé dans la première question en ajoutant les corps $\mathbf{Q}(\alpha_7)$, $\mathbf{Q}(\alpha_9)$ et $\mathbf{Q}(\alpha_7, \alpha_9)$. Montrer que l'extension $\mathbf{Q}(\zeta_{63})|\mathbf{Q}(\alpha_7, \alpha_9)$ est de degré ≤ 4 (on pourra considérer le corps $\mathbf{Q}(\zeta_7, \alpha_9)$).
5. En déduire que l'extension $\mathbf{Q}(\alpha_7, \alpha_9)|\mathbf{Q}$ est de degré ≥ 9, puis qu'elle est de degré 9.

IV

1. L'extension $\mathbf{Q}(\alpha_n)|\mathbf{Q}$ est-elle galoisienne ?
2. Quel est le sous-groupe H_n de $(\mathbf{Z}/n\mathbf{Z})^*$ dont $\mathbf{Q}(\alpha_n)$ est le corps des invariants ?
3. Quel est le sous-groupe de $(\mathbf{Z}/63\mathbf{Z})^*$ dont $\mathbf{Q}(\alpha_7, \alpha_9)$ est le corps des invariants ?
4. Montrer que l'extension $\mathbf{Q}(\alpha_7, \alpha_9)|\mathbf{Q}$ est galoisienne et que le groupe de Galois correspondant est isomorphe à $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$?
5. Donner une extension de degré 12 de $\mathbf{Q}$ qui est contenue dans $\mathbf{Q}(\zeta_{63})$.