Université Paris Diderot
Licence de Mathématiques

Algèbre
Année 2013-14
F. Liret, L. Merel

EXAMEN du 18 juin 2014

Durée : 3 h

L'usage des calculatrices et téléphones est interdit.
Document autorisé : une feuille de notes personnelles.

I

Soit G un groupe d'ordre 10.

1. Montrer que G admet un élément d'ordre 5. Notons-le ρ.
2. Montrer que G admet un unique 5-sous-groupe de Sylow, noté N.
3. Montrer que G admet un élément d'ordre 2. Notons le τ. Posons $T = \{1, \tau\}$.
4. Montrer que $G = \{\tau^i \rho^j, 0 \leq i \leq 1, 0 \leq j \leq 4\}$.
5. Supposons dans cette question que $\rho\tau = \tau\rho$. Montrer que G est cyclique d'ordre 10.
6. Supposons pour le reste de l'exercice que $\rho\tau \neq \tau\rho$. Montrer que la conjugaison par τ est un automorphisme de N. En déduire qu'on a un homomorphisme injectif de groupes $T \to \mathrm{Aut}(N)$ qui à t associe la conjugaison par t dans N.
7. Montrer qu'on a $\tau\rho^i\tau^{-1} = \rho^{-i}$ $(0 \leq i \leq 4)$. En déduire que G est un groupe diédral.
8. Montrer que G est isomorphe au sous-groupe du groupe symétrique $\mathcal{S}_5$ engendré par la double transposition $(1,4)(2,3)$ et le 5-cycle $(1,2,3,4,5)$. Le groupe G est-il isomorphe à un sous-groupe du groupe alterné $\mathcal{A}_5$?
9. Tout groupe d'ordre 20 est-il cyclique ou diédral ? Tout groupe d'ordre 40 est-il abélien ou diédral ?
10. Tout groupe d'ordre 80 n'admet-il qu'un seul 5-sous-groupe de Sylow ?

II

Soit $\mathbf{F}_2$ un corps à 2 éléments. Soit $\bar{\mathbf{F}}_2$ une clôture algébrique de $\mathbf{F}_2$. Pour m entier ≥ 1, on notera $\mathbf{F}_{2^m}$ le sous-corps de $\bar{\mathbf{F}}_2$ à 2^m éléments.
Posons $\alpha_0 = 1$ et $P_1 = X^2 + X + 1 \in \mathbf{F}_2[X]$. Soit $(\alpha_n)_{n\geq 1}$ une suite d'éléments de $\bar{\mathbf{F}}_2$, où α_n est une racine du polynôme $P_n = X^2 + X + \beta_{n-1} \in \bar{\mathbf{F}}_2[X]$ où $\beta_n = \alpha_1\alpha_2...\alpha_n$. Posons $K_n = \mathbf{F}_2(\alpha_1, \alpha_2...\alpha_n)$ (sous-corps de $\bar{\mathbf{F}}_2$ engendré par $\{\alpha_1, ..., \alpha_n\}$).

1. Montrer que les polynômes $X^2 + X + 1$ et $X^4 + X + 1$ sont irréductibles sur $\mathbf{F}_2$. Montrer que α_2 est racine de $X^4 + X + 1$.
2. Combien le corps $\mathbf{F}_2(\alpha_2)$ a-t-il d'éléments ? Le groupe multiplicatif $\mathbf{F}_2(\alpha_2)^*$ est-il engendré par α_2 ?
3. Montrer que les racines de P_n dans $\bar{\mathbf{F}}_2$ sont α_n et $\alpha_n + 1$.
4. Montrer que l'extension de corps $K_{n+1}|K_n$ est de degré 1 ou 2. En déduire que l'extension de corps $K_n|\mathbf{F}_2$ est de degré une puissance de 2.
5. Quels sont les ordres des sous-corps de $\mathbf{F}_{2^{2^n}}$? Montrer que K_n est un sous-corps de $\mathbf{F}_{2^{2^n}}$.
6. Montrer que $K_n = \mathbf{F}_{2^{2^n}}$ si et seulement si on a $\alpha_n \notin \mathbf{F}_{2^{2^{n-1}}}$.
7. Montrer que $\alpha_n \notin \mathbf{F}_{2^{2^{n-1}}}$ si et seulement si on a $\alpha_n^{2^{2^{n-1}}} \neq \alpha_n$.
8. Montrer que $\alpha_n^{2^{2^{n-1}}} = \alpha_n + S_{n-1}$, où $S_n = \sum_{i=0}^{2^n-1} \beta_n^{2^i}$.
9. Montrer que $S_n = 1$ (en montrant que $S_n = S_{n-1}$).
10. En déduire que $\mathbf{F}_{2^{2^n}} = \mathbf{F}_2(\alpha_n)$.