Université Paris 7-Denis Diderot
Licence de mathématiques et informatique

Algèbre et Géométrie
Année 2003-04
M. Fouquet, L. Merel

EXAMEN du 15 décembre 2003

Durée : 3 h

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

Notons $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$ le corps à 2 éléments. Soit n un entier ≥ 1. Posons $P_n = X^{2^n} + X + 1 \in \mathbf{F}_2[X]$.

Soit k un corps de décomposition de P_n, *i.e.* le polynôme P_n est scindé sur k et le corps k est engendré par $\mathbf{F}_2$ et les racines de P_n. C'est un corps fini contenant $\mathbf{F}_2$. Notons E_n l'ensemble des racines de P_n dans k.

Lorsque q est une puissance d'un nombre premier p, on rappelle que le corps $\mathbf{F}_q$ est un corps de décomposition du polynôme $X^q - X$ sur $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. On a de plus que $\mathbf{F}_q$ est précisément l'ensemble des racines du polynôme $X^q - X$. On rappelle que tout corps fini à q éléments est isomorphe à $\mathbf{F}_q$, pour q puissance d'un nombre premier p. On identifie tout sous-corps de k à l'un de ces corps $\mathbf{F}_q$.

I

1. Démontrer que P_1 n'a pas de racine dans $\mathbf{F}_2$. Démontrer que P_1 est irréductible sur $\mathbf{F}_2$.
2. Démontrer que l'anneau quotient $\mathbf{F}_2[X]/P_1$ est un corps à quatre éléments.
3. Soit α_1 une racine de P_1. Démontrer que $\mathbf{F}_4 = \mathbf{F}_2(\alpha_1)$.
4. Démontrer qu'on a une application $\mathbf{F}_2 \times E_1 \to E_1$ qui à (x, α) associe $x + \alpha$, puis que cette application définit une opération du groupe $\mathbf{F}_2$ sur E_1. En déduire que E_1 est une droite affine sur le corps $\mathbf{F}_2$.

II

1. Démontrer que k est un corps fini de caractéristique 2, que tout élément x d'un sous-corps $\mathbf{F}_q$ de k vérifie $x^q + x = 0$, et enfin que $\mathbf{F}_q = \{x \in k / x^q + x = 0\}$.
2. Démontrer que P_n n'a pas de racine multiple. Quel est le cardinal de E_n ?
3. Soient α_n, $\alpha'_n \in E_n$. Démontrer que $x = \alpha_n - \alpha'_n$ vérifie $x^{2^n} + x = 0$. En déduire que $x \in \mathbf{F}_{2^n}$.
4. Démontrer que $\alpha_n^{2^n} + \alpha_n \neq 0$. En déduire que α_n n'appartient pas à $\mathbf{F}_{2^n}$.
5. Démontrer que $\alpha_n^{2^{2n}} + \alpha_n = 0$. En déduire que α_n appartient à $\mathbf{F}_{2^{2n}}$.
6. En déduire que $E_n = \{\alpha_n + x / x \in \mathbf{F}_{2^n}\}$, puis que $k = \mathbf{F}_{2^{2n}}$.
7. Démontrer que le polynôme P_n divise le polynôme $X^{2^{2n}} + X$ dans $\mathbf{F}_2[X]$.
8. Quels sont les degrés des extensions $\mathbf{F}_{2^{2n}} | \mathbf{F}_{2^n}$ et $\mathbf{F}_{2^{2n}} | \mathbf{F}_2$?
9. Le polynôme P_2 est-il irréductible sur $\mathbf{F}_2$? Le polynôme P_n est-il irréductible sur $\mathbf{F}_2$ lorsque $n > 1$?
10. Quelles sont les valeurs de q pour lesquelles k possède un sous-corps à q éléments ?