Université Paris 7-Denis Diderot — Algèbre et Géométrie
Licence de mathématiques et informatique — Année 2003-04

Corrigé de l'EXAMEN du 15 décembre 2003

Soit K un corps de caractéristique 2. On a $2x = 0$ et donc $x = -x$, $(y+z)^2 = x^2 + 2xy + y^2 = y^2 + z^2$ et donc, en itérant cette identité, $(y+z)^{2^m} = y^{2^m} + z^{2^m}$ (x, $y \in K$, m entier ≥ 0).

I

1. On a, dans $\mathbf{F}_2 = \{0,1\}$, $P_1(0) = 1$ et $P_1(1) = 1$; c'est pourquoi P_1 n'a pas de racine dans $\mathbf{F}_2$. Si P_1 n'était pas irréductible sur $\mathbf{F}_2$, ce serait un produit de deux polynômes de degrés 1 ; or de tels polynômes ont des racines dans $\mathbf{F}_2$, et P_1 aurait alors aussi des racines dans $\mathbf{F}_2$, ce qui est impossible d'après ce qu'on vient de voir.
2. Comme P_1 est irréductible, l'anneau $\mathbf{F}_2[X]/P_1$ est un corps, qui est une extension de $\mathbf{F}_2$ de degré égale au degré de P_1. Ce corps possède donc $2^2 = 4$ éléments.
3. Comme P_1 est irréductible et comme α_1 est une racine de P_1, on a un isomorphisme de corps entre $\mathbf{F}_2(\alpha_1)$ et $\mathbf{F}_2[X]/P_1$. C'est pourquoi $\mathbf{F}_2(\alpha_1)$ est un corps à 4 éléments contenu dans k ; c'est donc $\mathbf{F}_4$.
4. Montrons que si $(x,\alpha) \in \mathbf{F}_2 \times E_1$, $x+\alpha \in E_1$. On a $(x+\alpha)^2+x+\alpha+1 = x^2+x+\alpha^2+\alpha+1 = x^2-x+0 = 0$ car α vérifie $\alpha^2 + \alpha + 1 = 0$ et x, étant un élément de $\mathbf{F}_2$, vérifie $x^2 - x = 0$.

On a bien une opération de groupe, en effet, on a $0 + \alpha = \alpha$ et $x + (y + \alpha) = (x + y) + \alpha$ ($\alpha \in E_1$, $x, y \in \mathbf{F}_2$).

Pour montrer que E_1 est une droite affine sur $\mathbf{F}_2$, il suffit de montrer que c'est un espace affine de dimension 1 sur $\mathbf{F}_2$. Démontrons que la direction de E_1 est $\mathbf{F}_2$, qui est un espace vectoriel de dimension 1. Pour cela il suffit de montrer que pour tout α, $\beta \in E_1$ il existe un unique $x \in \mathbf{F}_2$ tel que $\beta = x + \alpha$. L'unicité de x est claire. Montrons l'existence. Plus précisément, montrons que $\beta - \alpha \in \mathbf{F}_2$. Le polynôme P_1, étant de degré 2, ne possède que deux racines dans k. D'après ce qui précède, si α est une racine de P_1, $\alpha + 1$ l'est aussi. On a donc $\beta = \alpha$ ou $\beta = \alpha + 1$. Dans chaque cas, on a bien $\beta - \alpha \in \mathbf{F}_2$.

II

1. Le corps k est une extension de $\mathbf{F}_2$, il a donc même caractéristique que $\mathbf{F}_2$. Comme k est de caractéristique 2, on a $x = -x$ ($x \in k$). Dans un corps fini à q éléments, tout élément x vérifie $x^q - x = 0$. Comme $\mathbf{F}_q$ est un sous-corps de k, on a bien $x^q + x = x^q - x = 0$ ($x \in \mathbf{F}_q$).
2. Examinons la dérivée de P_n. C'est $P_n' = 2^n X^{2^n-1} + 1 = 1$ car $2^n = 0$ dans tout corps de caractéristique 2. La dérivée de P_n ne s'annule jamais. C'est pourquoi les racines de P_n sont simples.

Comme E_n est l'ensemble des racines de P_n dans k, comme P_n est scindé sur k, et comme P_n n'a pas de racine multiple, le cardinal de E_n est égal au degré de P_n, *i.e.* 2^n.
3. On a, en utiliant les relations $\alpha_n^{2^n} + \alpha_n + 1 = 0$ et $\alpha_n'^{2^n} + \alpha_n' + 1 = 0$, $x^{2^n} + x = (\alpha_n - \alpha_n')^{2^n} + \alpha_n - \alpha_n' = \alpha_n^{2^n} = \alpha_n^{2^n} + \alpha_n + \alpha_n'^{2^n} + \alpha_n' = 1 + 1 = 0$. D'après le critère de la question 1., on a bien $x \in \mathbf{F}_{2^n}$.
4. On a $\alpha_n^{2^n} + \alpha_n + 1 = 0$ et donc $\alpha_n^{2^n} + \alpha_n \neq 0$. D'après le critère de la question 1., on a bien $\alpha_n \notin \mathbf{F}_{2^n}$.
5. On a $\alpha_n^{2^{2n}} + \alpha_n = (\alpha_n^{2^n})^{2^n} + \alpha_n = (1 + \alpha_n)^{2^n} + \alpha_n = 1 + \alpha_n^{2^n} + \alpha_n = 0$. D'après le critère de la question 1., on a bien $\alpha_n \in \mathbf{F}_{2^{2n}}$.
6. Soit $x \in \mathbf{F}_{2^n}$. On a $(x + \alpha_n)^{2^n} + (x + \alpha_n) + 1 = x^{2^n} + \alpha_n^{2^n} + x + \alpha_n + 1 = x^{2^n} + x + \alpha_n^{2^n} + \alpha_n + 1 = 0$ et donc $x + \alpha_n \in E_n$. Cela montre que $\{\alpha_n + x / x \in \mathbf{F}_{2^n}\} \subset E_n$. L'inclusion inverse a été montrée en 3.

Comme toute racine de P_n est contenue dans $\mathbf{F}_{2^{2n}}$, on a $k \subset \mathbf{F}_{2^{2n}}$. Le nombre d'éléments de k est donc de la forme 2^m avec $m|2n$. Par ailleurs E_n contient 2^n éléments et est contenu dans k. Le corps k contient

donc au moins 2^n éléments. On a donc $m \geq n$. On a donc $m = n$ ou $m = 2n$. Comme les racines de P_n ne sont pas contenues dans $\mathbf{F}_{2^n}$, on a $m \neq n$. On donc $m = 2n$.
7. Les racines du polynôme $X^{2^{2n}} + X$ sont les éléments de $\mathbf{F}_{2^{2n}}$ qui contient l'ensemble E_n des racines de P_n. Comme les racines de P_n sont simples et sont des racines de $X^{2^{2n}} + X$, on a bien $P_n | X^{2^{2n}} + X$.
8. Soit q une puissance d'un nombre premier. Soient d et r des entiers ≥ 1. Si d est le degré de l'extension $\mathbf{F}_{q^r}|\mathbf{F}_q$, $\mathbf{F}_{q^r}$ est un espace vectoriel de dimension d sur $\mathbf{F}_q$ et possède donc q^d éléments. C'est pourquoi on a $r = d$.

Appliquons cela à $q = 2^n$ et $r = 2$. L'extension $\mathbf{F}_{2^{2n}}|\mathbf{F}_{2^n}$ est de degré 2.

Appliquons cela à $q = 2$ et $r = 2n$. L'extension $\mathbf{F}_{2^{2n}}|\mathbf{F}_2$ est de degré $2n$.
9. On a $P_2 = X^4 + X + 1$. Si P_2 était réductible sur $\mathbf{F}_2$, il s'écrirait comme produit de polynômes irréductibles de degré ≤ 3. Soit Q un facteur irréductible de P_2 dans $\mathbf{F}_2[X]$. Si Q est de degré 3, P_2/Q est un facteur irréductible de degré 1 de P_2, qui admet donc une racine dans $\mathbf{F}_2$, ce qui est impossible d'après 5. Si Q est de degré 2, P_2/Q est un facteur irréductible de degré 2 de P_2, et donc les racines de Q sont de degré 2 sur $\mathbf{F}_2$ et sont donc dans $\mathbf{F}_4$. Cela contredit 5. Si Q est de degré 1, il admet une racine dans $\mathbf{F}_2$. C'est absurde. Donc Q est de degré 4. Donc P_2 est irréductible sur $\mathbf{F}_2$.

Si P_n est irréductible, le corps de décomposition k de P_n s'identifie à $\mathbf{F}_2[X]/P_n$, qui est de degré 2^n sur $\mathbf{F}_2$. Or ce corps est de degré $2n$ d'après 8. Comme $2^n > 2n$, pour $n > 2$, le polynôme P_n n'est pas irréductible lorsque $n > 2$.
10. D'après le cours, le corps $\mathbf{F}_{2^m}$ admet $\mathbf{F}_{2^{2n}}$ comme extension si et seulement si $m|2n$. Les sous corps de k sont donc les corps $\mathbf{F}_{2^m}$ pour $m|2n$.