

Algèbre M1
Corrigé du devoir maison novembre 2011

Dans tout le problème, on considère le corps \mathbb{F}_{16} décrit de la manière suivante

$$\mathbb{F}_{16} = \mathbb{F}_2[X]/(X^4 + X^3 + 1)$$

et on note ω la classe de X dans \mathbb{F}_{16} .

1. (a) Montrer que ω engendre le groupe multiplicatif $\mathbb{F}_{16}^* = \mathbb{F}_{16} \setminus \{0\}$.
(b) Démontrer que $\omega, \omega^2, \omega^4$ et ω^8 sont les racines du polynôme $X^4 + X^3 + 1$.
(c) Démontrer que la famille $(\omega, \omega^2, \omega^4, \omega^8)$ est une base de \mathbb{F}_{16} sur \mathbb{F}_2 .
2. (a) Soit $a \in \mathbb{F}_{16}$. Résoudre dans \mathbb{F}_{16} l'équation $x^5 = a$, en discutant éventuellement selon les valeurs de a .
(b) Démontrer qu'il existe quatre éléments $\gamma \in \mathbb{F}_{16}$ tels que, pour chacun d'eux, la famille $(\gamma, \gamma^2, \gamma^4, \gamma^8)$ est une base de \mathbb{F}_{16} sur \mathbb{F}_2 telle que le produit de deux de ses éléments appartient à la base ou est égal à 1.

Corrigé

1. (a) Comme \mathbb{F}_{16}^* a 15 éléments il suffit de montrer que ω^3 et ω^5 sont différents de 1. C'est vrai pour le premier et aussi pour le deuxième: $\omega^5 = \omega^4 + \omega = \omega^3 + \omega + 1$
(b) Si x est racine de P alors

$$(x^2)^4 + (x^2)^3 + 1 = (x^3 + 1)^2 + x^6 + 1 = 0.$$

Comme ω est racine, il en est de même pour ω^{2^i} pour tout i . Le polynôme a au plus 4 racines et on a montré précédemment que ω engendrait \mathbb{F}_{16}^* . Ainsi les 4 éléments $\omega, \omega^2, \omega^4$ et ω^8 sont tous distincts. Ce sont donc les racines de P . (Remarque: $\omega^{16} = \omega$.)

- (c) Toute base de \mathbb{F}_{16} sur \mathbb{F}_2 a 4 éléments, donc il suffit de montrer que la famille est linéairement indépendante. On note également que $\omega^4 = \omega^3 + 1$ et $\omega^8 = \omega^6 + 1 = \omega^5 + \omega^2 + 1 = \omega^3 + \omega^2 + \omega$. Si l'on écrit une relation de liaison

$$a_0\omega + a_1\omega^2 + a_2\omega^4 + a_3\omega^8$$

On obtient alors

$$a_2 + (a_0 + a_3)\omega + (a_1 + a_3)\omega^2 + (a_2 + a_3)\omega^3 = 0$$

comme la famille $\{1, \omega, \omega^2, \omega^3\}$ forme une base, on en déduit $a_2 = 0 = a_3 = a_1 = a_0$, et donc la famille est libre.

2. (a) Si $a = 0$ il y a une seule solution $x = 0$.

Si $a \neq 0$ alors il existe un entier i tel que $a = \omega^i$. Si $x = \omega^j$ est solution de l'équation $x^5 = \omega^i$ alors $\omega^{5j-i} = 1$ et 15 divise $5j - i$. En particulier 5 divise i .

En première conclusion si $a = \omega^i$ avec $i \notin \{0, 5, 10\}$ alors l'ensemble des solutions est vide.

Comme \mathbb{F}_{16} est un corps l'ensemble des solutions de l'équation a au plus 5 éléments.

Pour $a = 1$, on doit résoudre $\omega^{5j} = 1$ soit 3 divise j . L'ensemble des solutions est donc $\{1, \omega^3, \omega^6, \omega^9, \omega^{12}\}$.

Pour $a = \omega^5$, on doit résoudre $\omega^{5j-5} = 1$ soit 3 divise $j - 1$. L'ensemble des solutions est donc $\{\omega, \omega^4, \omega^7, \omega^{10}, \omega^{13}\}$.

Pour $a = \omega^{10}$, on doit résoudre $\omega^{5j-10} = 1$ soit 3 divise $j - 2$. L'ensemble des solutions est donc $\{\omega^2, \omega^5, \omega^8, \omega^{11}, \omega^{14}\}$.

(b) Supposons qu'une telle famille existe, alors $\gamma\gamma^2 = \gamma^3 \in \{1, \gamma, \gamma^2, \gamma^4, \gamma^8\}$. Il est clair que $\gamma \in \mathbb{F}_{16}^*$ donc son ordre divise 15 et de plus $\gamma \neq 1$. En particulier on ne peut pas avoir $\gamma^3 \in \{\gamma, \gamma^2, \gamma^4\}$. Il nous reste les cas où $\gamma^3 = 1$ et $\gamma^3 = \gamma^8$ soit $\gamma^5 = 1$. Si $\gamma^3 = 1$ alors $\gamma^4 = \gamma$ ce qui contredirait le fait que γ et γ^4 sont deux éléments d'une base. Il nous reste le cas $\gamma^5 = 1$. Comme $\gamma \neq 1$ d'après la question précédente cela veut dire que $\gamma \in \{\omega^3, \omega^6, \omega^9, \omega^{12}\}$. Dans le premier cas on obtient la famille

$$\mathcal{F}_1 = \{\omega^3, \omega^6, \omega^{12}, \omega^9\}.$$

Comme $(\omega^9)^2 = \omega^3$, on obtient aussi cette famille dans tous les autres cas. Reste à montrer que c'est une base, puisqu'il est clair que le produit de deux de ces éléments vérifie la condition demandée.

On a par division euclidienne par le polynôme $X^4 + X^3 + 1$

$$\omega^3 = \omega^3, \quad \omega^6 = 1 + \omega + \omega^2 + \omega^3, \quad \omega^{12} = 1 + \omega, \quad \omega^9 = 1 + \omega^2.$$

Si l'on écrit une relation de liaison

$$a_0\omega^3 + a_1\omega^6 + a_2\omega^{12} + a_3\omega^9$$

On obtient alors

$$(a_1 + a_2 + a_3) + (a_1 + a_2)\omega + (a_1 + a_3)\omega^2 + (a_0 + a_1)\omega^3 = 0$$

comme la famille $\{1, \omega, \omega^2, \omega^3\}$ forme une base, on en déduit $a_1 = a_2 = a_3 = a_0$, puis $3a_0 = a_0 = 0$ et donc la famille est libre.