Master CSI 2 — 2008-2009

Arithmétique : DS du 3 novembre 2008

Durée : 1h30. Sans document. Les exercices sont indépendants.

– Exercice 1. Combien d'éléments contient le groupe multiplicatif A^* de l'anneau $A = \mathbb{F}_2[X]/(X^4+1)$? Faire la liste des éléments de A^*. Le groupe $(A^*, \times)$ est-il cyclique ?

– **Solution.** On a $X^4+1 = (X+1)^4$, ainsi les polynômes premiers avec X^4+1 sont les polynômes premiers avec $X+1$, c'est-à-dire les polynômes n'ayant pas 1 comme racine, ou encore les polynômes qui s'écrivent comme une somme d'un nombre impair de monômes. On a donc :

$$A^* = \{1, X, X^2, X^3, 1+X+X^2, 1+X+X^3, 1+X^2+X^3, X+X^2+X^3\}$$

et $|A^*| = 8$. On a clairement $X^4 = 1$ dans A, d'où $(X^i)^4 = (X^4)^i = 1$ et $(X^i + X^j + X^k)^4 = (X^i)^4 + (X^j)^4 + (X^k)^4 = (X^4)^i + (X^4)^j + (X^4)^k = 1+1+1 = 1$. Donc tous les éléments de A^* sont d'ordre au plus 4 et A^* n'est pas cyclique.

– Exercice 2.

a) Montrer que le polynôme $P(X) = X^6 + X + 1 \in \mathbb{F}_2[X]$ est irréductible et primitif.

– **Solution.** On vérifie que $P(X)$ n'est divisible ni par $X, X+1$, ni par $1+X+X^2$, ni par $1+X+X^3$, ni par $1+X^2+X^3$. Il n'est donc divisible par aucun polynôme irréductible de degré $1, 2, 3$ et est donc lui-même irréductible. Soit α la classe de X dans $K = \mathbb{F}_2[X]/(P)$. Les ordres des éléments de K^* sont des diviseurs de $2^6 - 1 = 63$. Tout diviseur propre de $63 = 3^2 \times 7$ est un diviseur de $9 = 3 \times 3$ ou de $21 = 3 \times 7$. Pour montrer que α est primitif il suffit de vérifier que $\alpha^9 \neq 1$ et $\alpha^{21} \neq 1$. Or le calcul montre que $\alpha^9 = \alpha^4 + \alpha$ et $\alpha^{21} = \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$.

b) Quels sont les sous-corps du corps $\mathbb{F}_{64}$ à 64 éléments ?

– **Solution.** Ce sont les sous-corps de la forme $\mathbb{F}_{2^i}$ où $i > 0$ est un diviseur de 6, soit $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_8$.

c) Soit α une racine de $P(X)$ dans $\mathbb{F}_{64}$. Soit $\beta = \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$. Montrer que β appartient au sous-corps à quatre éléments de $\mathbb{F}_{64}$.

– **Solution.** Il suffit de vérifier que $\beta^4 = \beta$ ou $\beta^3 = 1$. On peut utiliser le calcul de la question précédente qui a fait apparaître que $\beta = \alpha^{21}$ ou bien refaire un calcul.

d) Soit $\gamma = \alpha^4 + \alpha^3$. Combien d'éléments a le sous-corps $\mathbb{F}(\gamma)$ de $\mathbb{F}_{64}$?

– **Solution.** On a $\gamma^4 = \alpha^4 + \alpha^2 + \alpha \neq \alpha$ et $\gamma^8 = \gamma$. On en déduit que $\mathbb{F}(\gamma)$ a huit éléments.

e) Quel est le polynôme minimal de γ ?

– **Solution.** Le calcul montre que

$$\begin{aligned} \gamma &= \alpha^4 + \alpha^3 \\ \gamma^2 &= \alpha^3 + \alpha^2 + \alpha + 1 \\ \gamma^3 &= \alpha^3 + \alpha^2 + \alpha. \end{aligned}$$

On en déduit que $\gamma^3 + \gamma^2 + 1 = 0$ et donc que $P_\gamma(X) = X^3 + X^2 + 1$.

– Exercice 3.

a) Utiliser la factorisation de $X^{27} - X$ dans $\mathbb{F}_3[X]$ pour trouver le nombre de polynômes unitaires irréductibles de degré 3 sur $\mathbb{F}_3$.

– **Solution.** On a

$$\begin{aligned} X^{27} - X &= X^{3^3} - X \\ &= X(X-1)(X-2) \prod_{\deg P = 3, P \text{irréd}} P(X). \end{aligned}$$

Il y a donc $(27-3)/3 = 8$ polynômes unitaires irréductibles de degré 3.

b) Combien y a-t-il d'éléments primitifs dans le groupe multiplicatif de $\mathbb{F}_{27}$? en déduire le nombre de polynômes unitaires irréductibles primitifs de degré 3 sur $\mathbb{F}_3$.

– **Solution.** On a $\phi(26) = 12$ éléments primitifs dans $\mathbb{F}_{27}^*$, donc $12/3 = 4$ polynômes unitaires irréductibles primitifs de degré 3.

c) Montrer que le polynôme $P(X) = X^3 - X^2 + 1 \in \mathbb{F}_3[X]$ est irréductible.

– **Solution.** Il suffit de vérifier qu'il n'est pas divisible par un polynôme de degré 1, ou qu'il n'a pas de racine dans $\mathbb{F}_3$. Or $P(0) = 1, P(1) = 1, P(-1) = -1$.

d) Montrer que le polynôme $X^3 - X^2 + 1 \in \mathbb{F}_3[X]$ est primitif.

– **Solution.** L'ordre d'un élément non primitif de $\mathbb{F}_{27}^*$ est un diviseur propre de 26, donc divise 2 ou 13. Si α est la classe de X dans $\mathbb{F}_3[X]/(P)$, on a clairement $\alpha^2 \neq 1$ et le calcul montre que $\alpha^{13} = -1 \neq 1$.

e) Soit α une racine de $X^3 - X^2 + 1$ dans $\mathbb{F}_{27}$. Écrire tous les polynômes unitaires irréductibles primitifs de $\mathbb{F}_3[X]$ sous la forme

$$(X - \alpha^i)(X - \alpha^j)(X - \alpha^k).$$

– **Solution.** Ces polynômes sont de la forme $(X-\alpha^i)(X-\alpha^{3i})(X-\alpha^{9i})$ où i est premier avec 26. On trouve donc :

$$(X-\alpha)(X-\alpha^3)(X-\alpha^9)$$
$$(X-\alpha^5)(X-\alpha^{15})(X-\alpha^{19})$$
$$(X-\alpha^7)(X-\alpha^{21})(X-\alpha^{11})$$
$$(X-\alpha^{17})(X-\alpha^{25})(X-\alpha^{23}).$$

f) Quel est le plus petit entier $i>1$ tel que $\beta=\alpha^i$ *n'est pas* primitif ?

– **Solution.** C'est $i=2$.

g) Trouver le polynôme minimal $P_\beta(X)$ de β.

– **Solution.** Le calcul nous donne :

$$\begin{aligned}\beta &= \alpha^2\\ \beta^2 &= \alpha^2-\alpha-1\\ \beta^3 &= -\alpha^2-\alpha.\end{aligned}$$

D'où l'on déduit $\beta^3-\beta^2-\beta-1=0$. Le polynôme minimal de β est donc : $P_\beta(X)=X^3-X^2-X-1$.

h) Que vaut la période de la suite $(\beta^i)_{i\geqslant 0}$ dans $\mathbb{F}_{27}$? Que vaut la période π de la suite $(a_i)_{i\geqslant 0}$ définie par $a_i=\mathrm{Tr}(\beta^i)$ où Tr désigne l'application trace de $\mathbb{F}_{27}$ dans $\mathbb{F}_3$?

– **Solution.** La période de la suite (β^i) est l'ordre de $\beta=\alpha^2$, soit 13. La période π de $a_i=\mathrm{Tr}(\beta^i)$ est donc un diviseur de 13, et ce n'est pas 1 sinon on aurait $\mathrm{Tr}(\beta^i)=\mathrm{Tr}(1)=0$ pour tout i, et on aurait au moins 13 éléments distincts de $\mathbb{F}_{27}$ de trace nulle. Mais l'on sait que $\mathbb{F}_{27}$ contient autant d'éléments de trace 0, que de d'éléments de trace 1, que d'éléments de trace 2, soit 9 de chaque. Donc $\pi=13$.

i) Écrire les π premiers termes $a_0,a_1,\ldots,a_{\pi-1}$ de la suite (a_i).

– **Solution.** 0101200221222.