Master CSI 1 — 2010-2011

Arithmétique : DS du 18 octobre 2010

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

– Exercice 1. Soit A l'anneau $A = \mathbb{F}_2[X]/(X^4+X^3+X^2+1)$. Combien le groupe multiplicatif A^* contient-il d'éléments ? Montrer que ce groupe est cyclique.

– **Solution.** On remarque que $X^4 + X^3 + X^2 + 1 = (X^3 + X + 1)(X + 1)$. Les éléments de l'anneau A sont donc représentés par les polynômes de degré au plus 3 qui ne sont multiples, ni de $X + 1$, ni de $X^3 + X + 1$. On a donc :

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

L'ordre de tout élément de A divise $|A| = 7$; comme 7 est premier, tout élément de A différent de 1 engendre A qui est donc cyclique.

– Exercice 2. On considère le polynôme $P_1(X) = X^7 + X + 1$ dans $\mathbb{F}_2[X]$.

a) En calculant $X^8, X^{16}, X^{32}, \ldots$ dans $\mathbb{F}_2[X]/(P_1)$, calculer X^{128} et en déduire l'ordre multiplicatif de X dans $\mathbb{F}_2[X]/(P_1)$.

– **Solution.** L'égalité $X^7 = X + 1$ dans $\mathbb{F}_2[X]/(P_1)$ nous donne :

$$\begin{aligned} X^8 &= X^2 + X \\ X^{16} &= X^4 + X^2 \\ X^{32} &= X^8 + X^4 = X^4 + X^2 + X \\ X^{64} &= X^8 + X^4 + X^2 = X^4 + X \\ X^{128} &= X^8 + X^2 = X. \end{aligned}$$

Comme X est clairement premier avec P_1, il est inversible modulo P_1 et on en déduit

$$X^{127} = 1$$

dans $\mathbb{F}_2[X]/(P_1)$. Comme 127 est premier l'ordre de X ne peut être que 127.

b) En déduire que $P_1(X)$ est un polynôme irréductible de $\mathbb{F}_2[X]$.

– **Solution.** Dans $\mathbb{F}_2[X]/(P_1)$ le sous-groupe multiplicatif engendré par X contient 127 éléments. Il n'y a donc pas d'élément non nul de $\mathbb{F}_2[X]/(P_1)$ qui ne soit pas dans ce sous-groupe, et en particulier tous les éléments non nuls de $\mathbb{F}_2[X]/(P_1)$ sont inversibles. L'anneau $\mathbb{F}_2[X]/(P_1)$ est donc un corps ce qui est équivalent à l'irréductibilité de P_1.

c) Le polynôme $P_1(X)$ est-il primitif ?

– **Solution.** Oui, car l'on vient de voir que l'ordre de X dans $\mathbb{F}_2[X]/(P_1)$ est 127.

d) Traiter le cas des polynômes $P_2(X) = X^7+X^2+1$ et $P_3(X) = X^7+X^3+1$. Sont-ils irréductibles ? Primitifs ?

– **Solution.** Des calculs similaires à ceux de la question **a)** montrent que :

$$X^{128} = X^5 + X^2 + X + 1 \mod (P_2)$$
$$X^{128} = X \mod (P_3).$$

On en déduit que P_3 est irréductible primitif comme P_1. Par contre P_2 n'est pas irréductible. S'il l'était, le groupe multiplicatif de $\mathbb{F}_2[X]/(P_2)$ serait de cardinal $128-1 = 127$, et l'on devrait avoir (Lagrange) $X^{127} = 1 \mod (P_2)$.
Remarque. Ce raisonnement vaut pour tout polynôme de $\mathbb{F}_2[X]$ d'un quelconque degré n. Si P est irréductible, alors $X^{2^n-1} = 1 \mod (P)$.

e) Soit $K_1 = \mathbb{F}_2[X]/(P_1)$. Quels sont les sous-corps de K_1 ? En déduire que le polynôme minimal de n'importe quel élément de K_1 a pour degré 1 ou 7.

– **Solution.** Les sous-corps de K_1 sont de cardinal 2^m avec m diviseur de 7. Comme 7 est premier les sous-corps de K_1 sont $\mathbb{F}_2$ et K_1. Comme tout élément γ de K_1 engendre un sous-corps $\mathbb{F}_2[\gamma]$ de K_1, le degré de l'extension $\mathbb{F}_2[\gamma]/\mathbb{F}_2$ et donc du polynôme minimal de γ est 1 ou 7.

f) Quelle est la décomposition en facteurs irréductibles de $X^{128}+X$ dans $K_1[X]$? On considère maintenant la décomposition en facteurs irréductibles de $X^{128}+X$ dans $\mathbb{F}_2[X]$. Quels sont les différents degrés des facteurs intervenant dans la décomposition ? En déduire le nombre de polynômes irréductibles de degré 7 sur $\mathbb{F}_2$.

– **Solution.** On a :

$$X^{128} + X = \prod_{\gamma \in K_1} (X + \gamma)$$

et par ailleurs $X^{128}+X$ est égal au produit de X, $X+1$, et tous les polynômes irréductibles de $\mathbb{F}_2[X]$ de degré 7. Dans $\mathbb{F}_2[X]$ le nombre de polynômes irréductibles de degré 7 est donc $126/7 = 18$.

g) On note par α la classe de X dans K_1. Trouver le polynôme minimal de $\alpha^5+\alpha^4$. En déduire un isomorphisme de $K_3 = \mathbb{F}_2[X]/(P_3)$ sur $K_1 = \mathbb{F}_2[X]/(P_1)$.

– **Solution.** Le calcul montre que $\alpha^5+\alpha^4$ est une racine de $P_3(X)$. On en déduit que l'application

$$\sum_{i=0}^{6} a_i X^i \mapsto \sum_{i=0}^{6} a_i (\alpha^5+\alpha^4)^i$$

définit un isomorphisme de K_3 sur K_1.

– EXERCICE 3. Soit $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$ le corps à quatre éléments.

a) Montrer que le polynôme $P_1(X) = X^2+\alpha X+1$ est irréductible dans $\mathbb{F}_4[X]$. Combien y a-t-il de polynômes unitaires irréductibles de $\mathbb{F}_4[X]$ de degré 2 ?

– **Solution.** On constate que $P_1(0) = 1 \neq 0$, $P_1(1) = \alpha \neq 0$, $P_1(\alpha) = 1 \neq 0$ et $P_1(\alpha+1) = \alpha \neq 0$. Le polynôme $P_1(X)$ n'a donc pas de diviseur de degré 1 et est irréductible.

Il y a 16 polynômes unitaires de degré 2. Parmi ceux-ci quatre sont de la forme $(X+a)^2$ et six sont de la forme $(X+a)(X+b)$ avec a et b distincts (car $6 = 4 \times 3/2$). Il reste donc 6 polynômes unitaires irréductibles de degré 2.

b) Soit K le corps quotient $\mathbb{F}_4[X]/(P_1)$ et soit ω la classe de X dans ce quotient. Quel est l'ordre multiplicatif de ω ?

– **Solution.** Comme $|K| = 16$, l'ordre de ω divise 15. Les possibilités a priori sont donc $3, 5, 15$. Le calcul montre que $\omega^3 = \alpha\omega + \alpha \neq 1$ mais par contre $\omega^5 = 1$. L'ordre de ω égale 5.

c) Montrer que pour tout $k \in K$, on a $k^5 \in \mathbb{F}_4$.

– **Solution.** Pour tout $k \neq 0$ on a $(k^5)^3 = k^{15} = 1$. L'élément k^5 est donc racine de $X^4 + X$ et est par conséquent dans $\mathbb{F}_4$.

d) Soient $P_1, P_2, \ldots, P_m$ les différents polynômes unitaires irréductibles de degré 2. Montrer que chaque P_i a deux racines dans K et les donner sous la forme $a\omega + b$, avec $a, b \in \mathbb{F}_4$.

– **Solution.** Si P_i est irréductible sur $\mathbb{F}_4$ et de degré 2, il définit un corps $\mathbb{F}_4[X]/(P_i)$ à 16 éléments dans lequel P_i se factorise en produit de termes de degré 1, par construction. Comme tous les corps à 16 éléments sont isomorphes, en particulier à K, chaque P_i doit avoir deux racines dans K. Ainsi, les racines des 6 polynômes unitaires irréductibles de degré 2 constituent les 12 éléments de K qui ne sont pas dans $\mathbb{F}_4$. Par ailleurs, si k est une racine d'un tel polynôme, k^4 doit l'être aussi. On en déduit que les paires de racines associées à des polynômes irréductibles sont :

$$\begin{aligned}
\{\omega, \omega^4\} &= \{\omega, \omega+\alpha\} \\
\{\omega+1, \omega^4+1\} &= \{\omega+1, \omega+\alpha+1\} \\
\{\alpha\omega, (\alpha\omega)^4\} &= \{\alpha\omega, \alpha\omega+\alpha+1\} \\
\{\alpha\omega+1, (\alpha\omega+1)^4\} &= \{\alpha\omega+1, \alpha\omega+\alpha\} \\
\{(\alpha+1)\omega, ((\alpha+1)\omega)^4\} &= \{(\alpha+1)\omega, (\alpha+1)\omega+1\} \\
\{(\alpha+1)\omega+\alpha, ((\alpha+1)\omega+\alpha)^4\} &= \{(\alpha+1)\omega+\alpha, (\alpha+1)\omega+1+\alpha\}
\end{aligned}$$

e) Pourquoi les racines de chaque $P_i(X)$ ont-elles le même ordre multiplicatif ?

– **Solution.** Comme 4 est premier avec 15, k et k^4 on toujours le même ordre.

f) Donner la décomposition de $X^{15}+1$ en facteurs unitaires irréductibles sur $\mathbb{F}_4$.

– **Solution.**

$$X^{15}+1 = (X+1)(X+\alpha)(X+\alpha^2)(X^2+X+\alpha)(X^2+X+\alpha^2)(X^2+\alpha X+1) \times (X^2+\alpha X+\alpha)(X^2+\alpha^2 X+1)(X^2+\alpha X+\alpha^2).$$

g) Combien de polynômes P_i ont leurs racines d'ordre $|K^*|$?

– **Solution.** Quatre, car il y a $8=\phi(15)$ éléments primitifs dans K.