Master CSI 1 — 2018-2019

Arithmétique : DS du 6 novembre 2018

Master Sciences et Technologies, mention Mathématiques ou Informatique, parcours Cryptologie et Sécurité informatique

Responsable : Gilles Zémor

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

– Exercice 1. On considère l'anneau $A = \mathbb{F}_2[X]/(X^4+1)$.

a) Combien le groupe $(A^*, \times)$ contient-il d'éléments ?

b) Quel est l'ordre maximal d'un élément du groupe ? Montrer que ce groupe n'est pas cyclique.

– **Solution.**

a) Les inversibles de A s'écrivent comme des polynômes de degré au plus 3 premiers avec $X^4+1 = (X+1)^4$, c'est-à-dire qui ne sont pas multiples de $X+1$. Il y a huit multiples de $X+1$ qu'il faut ôter aux seize éléments de A pour avoir l'ensemble A^* des inversibles. D'où $|A^*| = 8$.

b) On a $P(X)^4 = P(X^4) = P(1)$ dans A. Donc $P(X)^4 = 0$ ou $P(X)^4 = 1$ dans A. Dans A^* on a $P(X)^4 = 1$ sinon $P(X)$ ne serait pas inversible. Donc tout élément de A^* est d'ordre au plus 4. Par ailleurs X est clairement d'ordre 4 donc l'ordre maximal d'un élément de A^* est 4. Le groupe n'est donc pas cyclique sinon il y aurait un élément d'ordre 8.

– Exercice 2.

a) Calculer X^{64} dans $\mathbb{F}_2[X]/(X^6+X+1)$.

b) En déduire que X^6+X+1 est irréductible sur $\mathbb{F}_2$.

c) Donner un exemple de polynôme $P(X)$ de $\mathbb{F}_2[X]$ de degré 6, *non irréductible*, tel que $X^{64} = X$ dans $\mathbb{F}_2[X]/(P)$. Combien y a-t-il de tels polynômes ?

d) Le polynôme X^6+X+1 est-il primitif ?

e) Combien y a-t-il de polynômes irréductibles sur $\mathbb{F}_2$ de degré 6 ? De polynômes irréductibles primitifs ?

– **Solution.**

a) Dans $A = \mathbb{F}_2[X]/(X^6+X+1)$ on a $X^8 = X^3+X^2$, $X^{16} = X^4+X+1$, $X^{32} = X^3+1$ et $X^{64} = X$.

b) Comme $64 = 2^6$, on sait que $X^{64}+X$ est le produit des polynômes irréductibles de degrés $1, 2, 3$ et 6 (les diviseurs de 6. Comme X^6+X+1 n'est pas divisible par X ou $X+1$, il ne peut qu'être produit de deux irréductibles de degré 3, ou lui-même irréductible. Il n'est pas produit des deux irréductibles de degré 3 sinon il diviserait X^8+X, mais on a vu à la question précédente que X^8 n'est pas égal à X modulo X^6+X+1. Il est donc irréductible.

c) Il y a le produit des deux irréductibles de degré 3 mentionné à la question précédente, soit $(X^3+X+1)(X^3+X^2+1) = X^6+X^5+X^4+X^3+X^2+X+1$. Pour en construire d'autres, il faut faire un produit d'irréductibles de degré 1, 2, ou 3, sans prendre deux fois le même polynôme. Comme il n'y a que deux polynômes de degré 1 et un polynôme irréductible de degré 2, la seule manière restante de procéder est de prendre un produit constitué d'un polynôme de degré 1, du polynôme irréductible de degré 2, et d'un polynôme irréductible de degré 3. Comme il y a deux polynômes irréductibles, respectivement de degrés 1 et de degrés 3, on trouve quatre tels produits. En tout il y a donc cinq diviseurs de degré 6 non irréductibles de $X^{64}+X$.

d) Le polynôme X^6+X+1 est primitif si l'ordre de X modulo X^6+X+1 est égal à 63. Il s'agit donc de tester X^d pour les diviseurs d de 63, car l'ordre de X ne peut être qu'un tel d (Lagrange).
Dans $\mathbb{F}_2[X]/(X^6+X+1)$ on a :

$$\begin{aligned} X^7 &= X^2+X \\ X^9 &= X^4+X^3 \\ X^{21} = X^3(X^9)^2 = X^3(X^8+X^6) &= X^3(X^3+X^2+X+1) \\ &= X^6+X^5+X^4+X^3 \\ &= X^5+X^4+X^3+X+1 \end{aligned}$$

L'ordre de X est donc 63 et X^6+X+1 est donc primitif.

e) Une fois qu'on a supprimé les deux polynômes de degré 1, le polynôme irréductible de degré 2 et les deux polynômes irréductibles de degré 3, les seuls diviseurs irrédutibles de $X^{64}+X$ restants sont les irréductibles de degré 6. Il y en a donc $(64-1-1-2-3-3)/6 = 9$.
Le nombre d'éléments primitifs du corps $\mathbb{F}_{64}$ est le nombre de générateurs de son groupe multiplicatif, soit $\phi(63) = \phi(7)\phi(9) = 6\times 6 = 36$. Toutes les six racines d'un polynôme primitif sont des éléments primitifs de $\mathbb{F}_{64}$, il y a donc $36/6 = 6$ polynômes primitifs de degré 6.

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

a) Combien y a-t-il de polynômes de $\mathbb{F}_4[X]$ unitaires de degré 2 irréductibles ?

b) Montrer qu'un polynôme de $\mathbb{F}_2[X]$ irréductible de degré 3 est aussi irréductible dans $\mathbb{F}_4[X]$.

c) Montrer que dans le corps $\mathbb{F}_{16}$ à 16 éléments il existe un élément β tel que $\beta^4 = \beta+1$.

d) Trouver un élément γ de $\mathbb{F}_{16}$, exprimé en fonction de β, tel que $\{0, 1, \gamma, \gamma+1\}$ constitue un sous-corps de $\mathbb{F}_{16}$.

e) Quel est, dans $\mathbb{F}_2[X]$, le polynôme minimal de β^2+1 ? De β^3+1 ?

– **Solution.**

a) Il y a $4^2 = 16$ polynômes unitaires de degré 2. Ce qui ne sont pas irréductibles s'écrivent $(X+x)(X+y)$, $x, y \in \mathbb{F}_4$, il y en a donc $4+\binom{4}{2} = 10$. Il y a donc six polynômes unitaires irréductibles de degré 2.

b) Si un polynôme $P \in \mathbb{F}_2[X]$ de irréductible de degré 3 n'est pas irréductible dans $\mathbb{F}_4[X]$ c'est qu'il a une racine x dans $\mathbb{F}_4$. Mais une telle racine doit vérifier $x^3 = 1$, donc $X + x$ doit diviser $X^3 + 1$ dans $\mathbb{F}_4[X]$. Mais comme P divise $X^7 + 1$ dans $\mathbb{F}_2[X]$, on aurait aussi que $X + x$ divise $X^7 + 1$ dans $\mathbb{F}_4[X]$. Donc $X^3 + 1$ et $X^7 + 1$ auraient un pgcd différent de $X + 1$. Rappelons que le pgcd de deux polynômes de $\mathbb{F}_2[X]$ est le même, qu'il soit calculé dans $\mathbb{F}_2[X]$ ou dans $\mathbb{F}_4[X]$.

c) Le polynôme X^4+X+1 est irréductible sur $\mathbb{F}_2$, le quotient $\mathbb{F}_2[X]/(X^4+X+1)$ est une des représentations du corps $\mathbb{F}_{16}$, dans laquelle X^4+X+1 a une racine β par construction.

d) L'élément β est primitif dans $\mathbb{F}_{16}$ car $\beta^5 = \beta^2 + \beta \neq 1$. On peut justement prendre $\gamma = \beta^5 = \beta^2 + \beta$ qui vérifie $\gamma^3 = \beta^{15} = 1$. On a $\gamma^3 + 1 = (\gamma + 1)(\gamma^2 + \gamma + 1) = 0$ et $\gamma \neq 1$, donc $\gamma^2 + \gamma + 1 = 0$, ce qui permet d'affirmer que γ engendre un corps à quatre éléments.

e) On remarque $(\beta^2 + 1) = (\beta + 1)^2 = (\beta^4)^2 = \beta^8$. L'élément $\beta^2 + 1$ est donc conjugué de β et a le même polynôme minimal. Or par construction, le polynôme minimal de β est $X^4 + X + 1$.
On calcule

$$\begin{aligned}(\beta^3+1)^2 &= \beta^6 + 1 = \beta^3 + \beta^2 + 1\\ (\beta^3+1)^3 &= (\beta^3+1)(\beta^3+\beta^2+1) = \beta^6 + \beta^5 + \beta^2 + 1\\ &= \beta^3 + \beta^2 + \beta + 1\\ (\beta^3+1)^4 &= (\beta^3+\beta^2+1)^2 = \beta^3 + \beta^2 + \beta\end{aligned}$$

ce qui permet de constater que $(\beta^3 + 1)^4 + (\beta^3 + 1)^3 + 1 = 0$. Le polynôme minimal de $\beta^3 + 1$ est donc $X^4 + X^3 + 1$.

– Exercice 4.

a) Montrer que le polynôme $P(X) = X^3 - X - 1$ est irréductible sur $\mathbb{F}_3$. Est-il primitif ?

b) Soit α une racine de $P(X)$ dans le corps à 27 éléments $\mathbb{F}_{27}$. Quel est le polynôme minimal de α^3 ?

c) Quelles sont les racines du polynôme minimal de α^2 dans $\mathbb{F}_3[X]$? Expliciter ce polynôme de $\mathbb{F}_3[X]$.

– **Solution.**

a) Si $P(X)$ était réductible il aurait un facteur de degré 1, autrement dit il aurait une racine dans $\mathbb{F}_3$ ce qui n'est pas le cas. Le quotient $\mathbb{F}_3[X]/(X^3 - X - 1)$ a un groupe multiplicatif de cardinal $3^3 - 1 = 26$ éléments. Il s'agit donc de tester si $13 = 26/2$ est ou non l'ordre de X. On calcule

$$\begin{aligned}X^9 &= (X+1)^3 = X^3 + 1 = X - 1\\ X^4 &= X(X+1) = X^2 + X\\ X^{13} &= X^9 X^4 = (X-1)(X^2+X) = X^3 - X = 1.\end{aligned}$$

L'ordre multiplicatif de X est 13, et $X^3 - X - 1$ n'est donc pas primitif.

b) Le polynôme minimal de α^3 est le même que le polynôme minimal de α, soit $X^3 - X - 1$.

c) Les autres racines sont

$$\begin{aligned}(\alpha^2)^3 = (\alpha^3)^2 = (\alpha+1)^2 &= \alpha^2 - \alpha + 1\\ (\alpha^2)^9 = (\alpha^2 - \alpha + 1)^3 &= \alpha^6 - \alpha^3 + 1 = \alpha^2 - \alpha + 1 - (\alpha+1) + 1\\ &= \alpha^2 + \alpha + 1\end{aligned}$$

Le polynôme minimal de α^2 est donc

$$m(X) = (X - \alpha^2)(X - \alpha^2 + \alpha - 1)(X - \alpha^2 - \alpha - 1).$$

On pourrait l'expliciter en développant, mais il probablement plus simple d'écrire

$$\begin{aligned}(\alpha^2)^2 &= \alpha(\alpha+1) = \alpha^2 + \alpha\\ (\alpha^2)^3 &= \alpha^2 - \alpha + 1\end{aligned}$$

et de constater que $\alpha^2 + (\alpha^2)^2 + (\alpha^2)^3 = 1$. Le polynôme minimal de α^2 est donc $X^3 + X^2 + X - 1$ (qui est bien irréductible car de degré 3 et sans racine dans $\mathbb{F}_3$).