Master CSI 1 — 2009-2010

Arithmétique : DS du 2 novembre 2009

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

– Exercice 1.

a) Que pouvez-vous dire de la factorisation du polynôme $X^{25} - X$ sur $\mathbb{F}_5[X]$? En déduire le nombre de polynômes unitaires irréductibles de degré 2 dans $\mathbb{F}_5[X]$.

b) Combien de générateurs admet le groupe multiplicatif du corps $\mathbb{F}_{25}$ à 25 éléments ? En déduire le nombre de polynômes unitaires irréductibles primitifs de degré 2 sur $\mathbb{F}_5[X]$.

c) Calculer l'ordre de X dans $K = \mathbb{F}_5[X]/(X^2 + X + 2)$. En déduire que K est un corps et que $X^2 + X + 2$ est irréductible sur $\mathbb{F}_5$.

d) Soit α une racine de $X^2 + X + 2$ dans K. Trouver le polynôme minimal de α^2. Est-il primitif ?

– **Solution.**

a) Le polynôme $X^{25} - X$ est égal au produit de tous les polynômes unitaires irréductibles de degré 1 et de tous les polynômes unitaires irréductibles de degré 2 de $\mathbb{F}_5[X]$. Comme il y a 5 polynômes unitaires irréductibles de degré 1 (soit X, $X-1, \ldots, X-4$), il y a donc $20/2 = 10$ polynômes irréductibles unitaires de degré 2.

b) Le groupe multiplicatif de $\mathbb{F}_{25}$ est cyclique à 24 éléments. Il admet donc $\phi(24)$ générateurs, soit 8 éléments. Chaque polynôme unitaire irréductible primitif de degré 2 admet deux de ces éléments comme racines. Il y a donc 4 tels polynômes.

c) On remarque que dans K on a $X^2 = -X + 3, X^3 = -X + 2, X^4 = 3X + 2, X^5 = -X - 1, X^6 = 2$. On en déduit que $X^{24} = 2^4 = 1$ et que $X^i \neq 1$ pour $1 \leqslant i < 24$. L'ordre de X est donc 24, ce qui veut dire qu'il y a 24 puissances de X distinctes et qu'elles sont toutes inversibles, i.e. dans le groupe multiplicatif de K. Tous les 24 éléments non nuls de K sont donc inversibles, et K est un corps. Or K est un corps si et seulement si $X^2 + X + 2$ est irréductible.

d) Le polynôme minimal de α^2 est le polynôme $P_{\alpha^2}(X) = (X - \alpha^2)(X - \alpha^{10})$. Or $\alpha^2 = -\alpha - 2$ et $\alpha^{10} = (-\alpha - 2)^5 = -\alpha^5 - 2^5 = \alpha - 1$. Par ailleurs nous avons déjà vu que $\alpha^{12} = (\alpha^6)^2 = 4$. Nous avons donc

$$P_{\alpha^2}(X) = X^2 + 3X - 1.$$

Enfin nous avons $(\alpha^2)^{12} = \alpha^{24} = 1$ donc α^2 n'est pas primitif.

– Exercice 2.

a) Trouver les facteurs irréductibles du polynôme X^4+X^3+X+1 dans $\mathbb{F}_2[X]$.

b) Soit A l'anneau $A = \mathbb{F}_2[X]/(X^4 + X^3 + X + 1)$. Combien le groupe multiplicatif A^* contient-il d'éléments ? Montrer qu'il est cyclique et en exhiber un générateur.

– **Solution.**

a) $X^4 + X^3 + X + 1 = (X^2 + X + 1)(X + 1)^2$.

b) Il s'agit de trouver le nombre de polynômes de degré au plus 3 qui ne sont ni multiples de $(X + 1)$ (c'est-à-dire qui ont un nombre impair de coefficients), ni multiples de $X^2 + X + 1$. Au 8 polynômes non multiples de $X + 1$ il faut donc enlever $X^2 + X + 1$ et $X(X^2 + X + 1)$. Il reste 6 éléments et $A^* = 6$.

On a $X \in A^*$ et manifestement $X^2 \neq 1$ et $X^3 \neq 1$. Or l'ordre de X doit être un diviseur de 6, et comme ce n'est ni 1 ni 2 ni 3, ce ne peut être que 6. Le groupe A^* est donc cyclique et X en est un générateur.

– Exercice 3. Soient dans $\mathbb{F}_3[X]$ les deux polynômes $P_1(X) = X^3 - X - 1$ et $P_2(X) = X^3 + X^2 - 1$.

a) Montrer que $P_1(X)$ et $P_2(X)$ sont irréductibles.

b) Calculer les ordres de X dans $\mathbb{F}_3[X]/(P_1)$ et dans $\mathbb{F}_3[X]/(P_2)$.

c) Soit α la classe de X dans $K_1 = \mathbb{F}_3[X]/(P_1)$. Montrer sans calculs qu'il existe une puissance α^i de α qui est une racine du polynôme $P_2(X)$ dans K_1. On pourra utiliser le théorème de l'élément primitif.

d) Montrer que α^4 est bien une racine de $P_2(X)$ dans K_1. Quelles sont les autres racines de $P_2(X)$ dans K_1 ?

e) Exhiber un isomorphisme de corps entre K_1 et $\mathbb{F}_3[X]/(P_2)$.

f) Combien y a-t-il d'autres polynômes unitaires irréductibles de degré 3 dans $\mathbb{F}_3[X]$ dont les racines dans K_1 sont du même ordre que α ?

g) Trouver le polynôme minimal de α^2.

– **Solution.**

a) Si $P_1(X)$ ou $P_2(X)$ étaient réductibles il auraient un facteur de degré 1, et auraient donc une racine dans $\mathbb{F}_3$. On vérifie que ce n'est pas le cas : les polynômes sont donc irréductibles.

b) On sait que $\mathbb{F}_3[X]/(P_1)$ et $\mathbb{F}_3[X]/(P_2)$ ont un groupe multiplicatif à $3^3-1 = 26$ éléments. Or $26 = 2 \times 13$, et X n'a pas pour ordre 2, donc son ordre est soit 13 soit 26.

Il s'agit donc de calculer $X^{13} \bmod P_1$ et $X^{13} \bmod P_2$. Dans le premier cas on a $X^3 = X + 1$ donc $X^9 = (X + 1)^3 = X^3 + 1 = X + 2$. Puis $X^4 = X^2 + X$ donc $X^{13} = (X + 2)(X^2 + X) = X^3 + 2X = 1$.

Par un calcul analogue on trouve $X^{13} = 1 \bmod P_2$ également. Dans les deux cas l'ordre de X est donc 13.

c) On sait (théorème de l'élément primitif) qu'il existe dans K_1 un élément γ primitif, c'est-à-dire générateur de K_1^*. On sait également que P_2, diviseur de $X^{27}-X$, a une racine β dans K_1, donc de la forme $\beta=\gamma^i$. Or $\alpha^{13}=\beta^{13}=1$ donc α et β sont des puissances paires de γ. Or le sous-groupe de K_1^* des puissances paires de γ est d'ordre 13 qui est premier, donc tout élément de ce sous-groupe est une puissance de n'importe quel autre élément.

d) On vérifie $(\alpha^4)^3+(\alpha^4)^2-1=(\alpha^2+2)+(2\alpha^2+2)-1=0$. Les autres racines de $P_2(X)$ sont $(\alpha^4)^3=\alpha^{12}=\alpha^2+2$ et $(\alpha^4)^9=\alpha^{36}=\alpha^{10}=\alpha(\alpha^9)=\alpha^2+2\alpha$.

e) Il suffit de s'assurer que X est l'image d'une racine de $P_2(X)$. L'application suivante est bien un isomorphisme de corps :

$$\begin{array}{rcl} K_1 & \to & \mathbb{F}_3[X]/(P_2) \\ a+b\alpha^4+c\alpha^8+d\alpha^{12} & \mapsto & a+bX+cX^2+dX^3 \end{array}$$

f) Comme nous l'avons vu, les éléments de K_1^* d'ordre 13 sont toutes les puissances de α différentes de 1. Il y en a donc 12. Si leur ordre est 13 ils ne sont pas dans $\mathbb{F}_3$ et leur polynôme minimal est donc de degré 3. Il y a donc $12/3=4$ tels polynômes.

g) On a :

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

D'où l'on déduit $(\alpha^2)^3+(\alpha^2)^2+\alpha^2+2=0$. Le polynôme minimal de α^2 est donc :

$$P_{\alpha^2}(X)=X^3+X^2+X+2.$$