Travaux Dirigés de MT10

Corps finis de caractéristique 2 : Construction de F4

Corrigé

Ce TD a pour objectif de se familiariser avec les corps finis de caractéristique 2 et traite du corps F4 à 4 éléments.

Dans l'anneau Euclidien Z/2Z[X] (ou F2[X]), on se propose de commencer à déterminer les polynômes irréductibles divisibles seulement par 1 et eux-mêmes en s'inspirant du crible d'Erathostène (un polynôme irréductible étant identifié, tous ses produits par un autre polynôme ne sont donc pas irréductibles).

1) Donner les polynômes irréductibles de degré 1

   Reponse : X et X+1 sont les deux seuls polynômes de degré 1 et sont irréductibles.
2) Trouver un critère simple de divisibilité d'un polynôme quelconque par X et un autre critère de divisibilité par X+1, en déduire un critère permettant d'affirmer rapidement d'un polynôme qu'il n'est divisible ni par X ni par X+1

Réponse : un polynôme divisible par X s'annule en 0 donc son terme de degré 0 vaut 0, un polynôme divisible par X+1 s'annule en X=1 (rappel 1=-1), donc la somme de ses coefficients vaut 0, donc les coefficients non nuls doivent être en nombre pair. Un polynôme est donc divisible ni par X ni par X+1 si et seulement si son terme de degré 0 vaut 1 et si son nombre de termes est impair.

3) Utilisant le critère précédent, montrer que X^2+X+1 est le seul polynôme irréductible de degré 2 de F2[X]

Réponse : le seul polynôme de degré 2 dont le terme de degré 0 ne vaut pas 0 (et vaut donc 1) et dont le nombre de monômes soit impair est X^2+X+1

4) Utilisant le fait qu'un polynôme de degré 3 non irréductible est forcément divisible par un polynôme de degré 1, donner tous les polynômes irréductibles de degré 3

Réponse : Le coefficient de X^3 vaut 1 (par hypothèse) et le terme de degré 0 vaut 1 (sinon le polynôme serait divisible par X). Il faut rajouter un monôme pour avoir un nombre de termes impair et on a deux possibilités pour le faire. Les deux polynômes ainsi obtenus sont donc irréductibles et ce sont les seuls : X^3+X+1 et X^3+X^2+1

5) Trouver les polynômes irréductibles de degré 4 (attention cette fois à enlever le carré du polynôme irréductible de degré 2).

*Réponse : Les termes d'ordre 4 et 0 sont imposés et valent respectivement X^4 et 1. Restent **3** termes qui doivent être en nombre impair, on peut donc rajouter à X^4+1, soit 1 seul monôme (**3** possibilités) soit 3 monômes (**1** possibilité), soit **4** possibilités dont il convient d'enlever les polynômes divisibles par l'un des polynômes irréductibles déjà identifiés hors ceux de degré 1 (déjà pris en compte) : reste un polynôme à enlever qui est le carré du degré 2 soit X^4+X^2+1, reste donc au degré 4 : X^4+X+1, X^4+X^3+1 et $X^4+X^3+X^2+X+1$*

6) Trouver les polynômes irréductibles de degré 5 (il faut utiliser le critère de non divisibilité par X et par X+1 puis enlever les produits des irréductibles de degré 3 par l'irréductible de degré 2).

Réponse : Reste donc au degré 5 : X^5+X^2+1, X^5+X^3+1, $X^5+X^4+X^3+X^2+1$, $X^5+X^4+X^3+X+1$, $X^5+X^4+X^2+X+1$, $X^5+X^3+X^2+X+1$

7) Dresser les tables de Pythagore de l'addition de la multiplication de F4 considérés comme classes d'équivalence de $F2[X]/(X^2+X+1)$, on utilisera la même notation pour les polynômes de degré maximal 1 et leur classe d'équivalence.

Réponse : Les 4 éléments de F4 sont donc 0, 1, X et 1+X

Table de Pythagore de l'addition

	0	*1*	*X*	*X+1*
0	*0*	*1*	*X*	*X+1*
1	*1*	*0*	*X+1*	*X*
X	*X*	*X+1*	*0*	*1*
X+1	*X+1*	*X*	*1*	*0*

Table de Pythagore de la multiplication

	0	*1*	*X*	*X+1*
0	*0*	*0*	*0*	*0*
1	*0*	*1*	*X*	*X+1*
X	*0*	*X*	*X+1*	*1*
X+1	*0*	*X+1*	*1*	*X*

8) On note désormais α et β les deux racines de X^2+X+1 dans F4. Prenant α^0 et α^1 comme base de F4 considéré comme F2 espace vectoriel, lister les 4 éléments de F4 et montrer que les calculs sont exactement les mêmes, que l'on utilise pour les éléments de F4 la vision « classe d'équivalence des polynômes de F2[X] modulo le polynôme générateur » ou « combinaison linéaire des puissances inférieures au degré du polynôme générateur d'une racine quelconque de ce polynôme générateur ».

Réponse : Les 4 éléments de F4 sont donc 0, 1, α et $1+\alpha$. Les calculs des sommes et produits de ces éléments en utilisant le fait que $\alpha^2=\alpha+1$ redonnent bien les tables de Pythagore de la question précédente, il s'agit de deux points de vue totalement équivalents.

9) Donner, en justifiant, une expression de β en fonction de α

Réponse : Puisque β appartient à F4 et ne vaut ni 1 ni α, et $\beta=1+\alpha$ et bien évidemment $\alpha=1+\beta$ les deux racines ayant un rôle tout à fait symétrique

10) Pour tout z de F4 que vaut z^4 ?

Réponse : F4 peut être aussi vu comme le corps des racines (et constitué exactement des racines) du polynôme X^4-X (identique à X^4+X) polynôme égal à $X(X-1)(X^2+X+1)$ identique à $X(X+1)(X^2+X+1)$. Par conséquent pour tout z de F4 $z^4=z$

11) Pour tout z de F4* que vaut z^3 ?

Réponse : $X^4-X = X(X^3-X)$ donc F4 est constitué de 0 et des 3 racines cubiques de l'unité (dont 1, les deux autres étant donc α et $\beta=1+\alpha$), par conséquent pour tout z de F4 $z^3=1$*

12) Le groupe multiplicatif F4* est il cyclique ? Dans l'affirmative donner tous ses générateurs

Réponse : On sait d'après le cours que le sous-groupe multiplicatif d'un corps fini est toujours cyclique. Ici de plus il l'est nécessairement car d'ordre 3 donc tous les éléments sauf 1 sont générateurs (donc α et $\beta=1+\alpha$ sont générateurs) donc $\alpha^2=\beta=1+\alpha$ et bien sûr $\beta^2=\alpha=1+\beta$ ce que l'on peut vérifier aisément sur les tables de multiplication.

13) Calculer les puissances (entre 0 et 3) de l'un de ces générateurs et son inverse qui est la table de logarithmes en base ce générateur. Bien indiquer dans quoi ces fonctions sont définies et dans quoi elles prennent leur valeur. Calculer le carré de α et le carré de $\alpha+1$ en utilisant la table de logarithmes.

Réponse : on détermine facilement la table des puissances de α :

n	α^n
0	*1*
1	α
2	$\alpha+1$
3	*1*

Ainsi la fonction α^n est une fonction définie dans Z/3Z à valeurs dans F4 dont on peut facilement dresser la table inverse (qui est le log à base α) défini sur F4* et à valeur dans Z/3Z*

Table des $\log_\alpha(P)$

z	$\log_\alpha(P)$
0	
1	*0*
α	*1*
$\alpha+1$	*2*

$\log_X(n)$ est une fonction définie sur F4 à valeurs dans Z/3Z*

Les logarithmes s'additionnent donc modulo 3.

Exemple, le carré de α a donc pour logarithme 1+1[3]=2 et en effet dans la table des puissances on vérifie que ce carré est bien $\alpha+1$

De même, le carré de $\alpha+1$ a pour logarithme 2+2[3]=1 et vaut donc α

Travaux Dirigés de MT10

Corps finis : Construction de F8

Ce TD a pour objectif de continuer à se familiariser avec les corps finis de caractéristique 2 et traite du corps F8 à 8 éléments

14) En utilisant le TD précédent, montrer qu'il y a deux constructions possibles de F8 en tant qu'extension de degré 3 de F2

Réponse : d'après le TD précédent, il y a deux polynômes irréductibles de degré 2 de F2[X] qui sont X^3+X+1 et X^3+X^2+1. On peut donc construire F8 comme $F2[X]/(X^3+X+1)$ ou comme $F2[X]/(X^3+X^2+1)$

15) On note γ est l'une quelconque des racines de X^3+X+1, lister en fonction de γ les 8 éléments de F8

Réponse : Une base de F8 vu comme F2 espace vectoriel est d'après le cours (γ^0, γ^1, γ^2) *donc* $F_8=\{0, 1, \gamma, \gamma+1, \gamma^2, \gamma^2+1, \gamma^2+\gamma, \gamma^2+\gamma+1\}$

16) Lister en fonction de γ les 3 racines X^3+X+1

Réponse : Par hypothèse on en connaît déjà une qui est γ, donc $\gamma^3+\gamma+1=0$. Pour trouver les autres on utilise le morphisme de Frobenius (pour tout élément ξ du corps $\xi->\xi^2$) qui conserve l'addition et la multiplication puisque $(\xi.\psi)^2=\xi^2.\psi^2$ et du fait de la caractéristique 2 on a également $(\xi+\psi)^2=\xi^2+\psi^2$ (le double produit est nul). Le morphisme de Frobenius est donc un automorphisme de corps. Par conséquent $\gamma^6+\gamma^2+1=0$ donc γ^2 est une autre racine (différente de γ) et comme $\gamma^{12}+\gamma^4+1=0$, γ^4 est la troisième (différente des deux autres car comme $\gamma^3=\gamma+1$, $\gamma^4=\gamma^2+\gamma$). Les trois racines de X^3+X+1 sont donc γ, γ^2 et $\gamma^4=\gamma^2+\gamma$

17) Montrer que γ est générateur du groupe multiplicatif F8* et montrer que par conséquent on connaît déjà trois générateurs de ce groupe

Réponse : d'après le cours on sait que ce groupe a des générateurs et comme dans ce cas particulier c'est un groupe d'ordre 7 (premier) il a donc 6 générateurs (tous les éléments différents de 1). Mais on le vérifie directement en déterminant le groupe cyclique : γ, γ^2, $\gamma^3=\gamma+1$, $\gamma^4=\gamma^2+\gamma$, $\gamma^5=\gamma^3+\gamma^2=\gamma^2+\gamma+1$, $\gamma^6=\gamma^3+\gamma^2+\gamma=\gamma^2=\gamma^2+1$, $\gamma^7=\gamma^3+\gamma=1$. Le choix de γ étant arbitraire (γ^2 et $\gamma^4=\gamma^2+\gamma$ jouent exactement le même rôle), on a donc déjà trois générateurs de F8 qui sont γ, γ^2 et $\gamma^4=\gamma^2+\gamma$. On a donc également :*

$F8=\{0, \gamma^0(=1), \gamma^1(=\gamma), \gamma^2(=\gamma^2), \gamma^3(=\gamma+1), \gamma^4(=\gamma^2+\gamma), \gamma^5(=\gamma^2+\gamma+1), \gamma^6(=\gamma^2+1)\}$ (ou de manière tout à fait semblable comme puissances de γ^2 ou $\gamma^4=\gamma^2+\gamma$)

18) On note δ est l'une quelconque des racines de X^3+X^2+1, lister en fonction de δ les 8 éléments de F8

Réponse : Une base de F8 vu comme F2 espace vectoriel est d'après le cours (δ^0, δ^1, δ^2) *donc* $F_8=\{0, 1, \delta, \delta+1, \delta^2, \delta^2+1, \delta^2+\delta, \delta^2+\delta+1\}$

19) Lister en fonction de δ les 3 racines X^3+X^2+1

Réponse : Par hypothèse on en connaît déjà une qui est δ, donc $\delta^3+\delta^2+1=0$. Pour trouver les autres on utilise le morphisme de Frobenius (pour tout élément ξ du corps $\xi->\xi^2$) qui conserve l'addition et la multiplication puisque $(\xi.\psi)^2=\xi^2.\psi^2$ et du fait de la caractéristique 2 on a également $(\xi+\psi)^2=\xi^2+\psi^2$ (le double produit est nul). Le morphisme de Frobenius est donc un automorphisme de corps. Par conséquent $\delta^6+\delta^4+1=0$ donc δ^2 est une autre racine (différente de δ) et comme $\delta^{12}+\delta^4+1=0$, δ^4 est la troisième (différente des deux autres car

comme $\delta^3=\delta^2+1$, $\delta^4=\delta^3+\delta=\delta^2+\delta+1$). Les trois racines de X^3+X+1 sont donc δ, δ^2 et $\delta^4=\delta^3+\delta=\delta^2+\delta+1$

20) Montrer que δ est générateur du groupe multiplicatif F8* et montrer que par conséquent cela nous donne trois autres générateurs du groupe

Réponse : d'après le cours on sait que ce groupe a des générateurs et comme dans ce cas particulier c'est un groupe d'ordre 7 (premier) il a donc 6 générateurs (tous les éléments différents de 1). Mais on le vérifie directement en déterminant le groupe cyclique : δ, δ^2, $\delta^3=\delta^2+1$, $\delta^4=\delta^3+\delta=\delta^2+\delta$, $\delta^5=\delta^3+\delta^2=\delta+1$, $\delta^6=\delta^2+\delta$, $\delta^7=\delta^3\delta^2=1$. Le choix de δ étant arbitraire (δ^2 et $\delta^4=\delta^2+\delta+1$ jouent exactement le même rôle) on a les trois autres générateurs de F8 qui sont δ, δ^2 et $\delta^4=\delta^2+\delta+1$).*

On a donc également :

F8={0, δ^0(=1), δ^1 (=γ), δ^2 (=δ^2), δ^3 (=δ^2+1), δ^4(=$\delta^2+\delta$), δ^5(=$\delta+1$), δ^6(=$\delta^2+\delta$)} (ou de manière tout à fait semblable comme puissances de δ^2 ou $\delta^4=\delta^2+\delta$)

21) Calculer le polynôme $X(X+1)(X^3+X+1)(X^3+X^2+1)$, qu'en concluez vous ?

Réponse : Après calcul $X(X+1)(X^3+X+1)(X^3+X^2+1)=X^8+X$, par conséquent : 0, 1, les trois racines de X^3+X+1, les trois racines de X^3+X^2+1 sont les 8 éléments de F8 et vérifient $X^8+X=0$, les racines de ce polynôme sont toutes distinctes car le polynôme dérivé vaut 1 et n'a donc pas de racines

9) Pour tout z de F8 que vaut z^8 ?

Réponse : F8 peut être aussi vu comme le corps des racines (et constitué exactement des racines) du polynôme X^8-X (identique à X^8+X), par conséquent pour tout z de F8 que vaut $z^8=z$

10) Pour tout z de F8* que vaut z^7 ?

Réponse : $X^8-X = X(X^7-X)$ donc F8 est constitué de 0 et des 7 racines septièmes de l'unité (donc 1, les six autres étant les éléments de F8 différents de 0 et 1), par conséquent pour tout z de F8 $z^7=1$*

11) F4 est il inclus dans F8 ?

Réponse : non car 0 et 1 appartiennent bien au deux en revanche les éléments différents de 0 et de 1 dans F4 sont racines cubiques de l'unité donc $\alpha^3=\beta^3=1$ donc $\alpha^7=\alpha$ et $\beta^7=\beta$ tous deux différents de 1. F8 n'est donc pas une extension de F4 ce qui est normal (8 n'est pas une puissance de 4).

12) Exprimer en fonction de γ les trois racines de X^3+X^2+1, le vérifier explicitement avec une d'entre elles

Réponse : les trois racines de X^3+X+1 étant γ, γ^2 γ^4, les trois racines de X^3+X^2+1 sont donc nécessairement les éléments restants de F8 qui ne valent ni 0 ni 1 donc γ^3 (=$\gamma+1$), γ^5(=$\gamma^2+\gamma+1$), γ^6(=γ^2+1). On vérifie bien par exemple que $\gamma^9+\gamma^6+1=\gamma^2+\gamma^2+1+1=0$ le calcul pour les trois autres étant inutile (Frobenius).

13) Exprimer en fonction de δ les trois racines de X^3+X+1, le vérifier explicitement avec une d'entre elles

Réponse : les trois racines de X^3+X^2+1 étant δ, δ, δ^4, les trois racines de X^3+X+1 sont donc nécessairement les éléments restants de F8 qui ne valent ni 0 ni 1 donc δ^3 (=δ^2+1), δ^5(=$\delta+1$), δ^6(=$\delta^2+\delta$). On vérifie bien par exemple que $\delta^9+\delta^3+1=\delta^2+\delta^2+1+1=0$, le calcul pour les trois autres étant inutile (Frobenius).

14) En utilisant les résultats précédents mettre en évidence trois isomorphismes possibles (bijection entre les éléments exprimés en fonction de δ et ceux exprimés en fonction de γ et réciproquement)

Réponse : Fonction de ce qui précède on a donc bien trois isomorphismes possibles :

$\delta \to \gamma^3=\gamma+1$, donc $\delta^2 \to \gamma^6=\gamma^2+1$ et $\delta^4 \to \gamma^{12}=\gamma^5=\gamma^2+\gamma+1$

$\delta \to \gamma^5=\gamma^2+\gamma+1$, donc $\delta^2 \to \gamma^{10}=\gamma^3=\gamma+1$ et $\delta^4 \to \gamma^{20}=\gamma^6=\gamma^2+1$

$\delta \to \gamma^6=\gamma^2+1$, donc $\delta^2 \to \gamma^{12}=\gamma^5=\gamma^2+\gamma+1$ et $\delta^4 \to \gamma^{24}=\gamma^3=\gamma+1$

La correspondance peut aussi être exprimée dans l'autre sens :
$\gamma \to \delta^3 = \delta^2 + 1$, donc $\gamma^2 \to \delta^6 = \delta^2 + \delta$ et $\gamma^4 \to \delta^{12} = \delta^5 = \delta + 1$
$\gamma \to \delta^5 = \delta + 1$, donc $\gamma^2 \to \delta^{10} = \delta^3 = \delta^2 + 1$ et $\gamma^4 \to \delta^{20} = \delta^6 = \delta^2 + \delta$
$\gamma \to \delta^6 = \delta^2 + \delta$, donc $\gamma^2 \to \delta^{12} = \delta^5 = \delta + 1$ et $\gamma^4 \to \delta^{24} = \delta^3 = \delta^2 + 1$

15) A quels automorphismes correspondent les trois isomorphismes identifiés entre les deux constructions ?

Réponse : Parmi ces trois isomorphismes l'un est Frobenius, l'autre Frobenius au carré, le dernier (Frobenius à la puissance 4 donc élévation à la puissance 8) est donc l'identité. Savoir lequel est lequel n'a pas de sens car cela est tout à fait arbitraire (correspond à l'arbitraire dans le choix des racines appelées respectivement γ et δ)