Travaux Dirigés de MT10

Corps finis de caractéristique 2 : Construction de F4

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
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
3) Utilisant le critère précédent, montrer que X^2+X+1 est le seul polynôme irréductible de degré 2 de Z/2Z[X]
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
5) Trouver les polynômes irréductibles de degré 4 (attention cette fois à enlever le carré du polynôme irréductible de degré 2).
6) 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.
7) 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
8) Donner, en justifiant, une expression de β en fonction de α
9) Pour tout z de F4 que vaut z^4 ?
10) Pour tout z de F4* que vaut z^3 ?
11) Le groupe multiplicatif F4* est il cyclique ? Dans l'affirmative donner tous ses générateurs
12) Calculer les puissances (entre 0 et 3) de l'un de ces générateurs et en déduire la fonction 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 X et le carré de X+1 en utilisant la table de logarithmes.

Travaux Dirigés de MT10

Corps finis de caractéristique 2 : 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

1) En utilisant le TD précédent, montrer qu'il y a deux constructions possibles de F8 en tant qu'extension de degré 3 de F2
2) On note γ est l'une quelconque des racines de X^3+X+1, lister en fonction de γ les 8 éléments de F8
3) Lister en fonction de γ les 3 racines X^3+X+1
4) Montrer que γ est générateur du groupe multiplicatif F8* et montrer que par conséquent on connaît déjà trois générateurs de ce groupe
5) 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
6) Lister en fonction de δ les 3 racines X^3+X^2+1
7) Montrer que δ est générateur du groupe multiplicatif F8* et montrer que par conséquent cela nous donne trois autres générateurs du groupe
8) Calculer le polynôme $X(X+1)(X^3+X+1)(X^3+X^2+1)$, qu'en concluez vous ?
9) Pour tout z de F8 que vaut z^8 ?
10) Pour tout z de F8* que vaut z^7 ?
11) F4 est il inclus dans F8 ?
12) Exprimer en fonction de γ les trois racines de X^3+X^2+1, le vérifier explicitement avec une d'entre elles
13) Exprimer en fonction de δ les trois racines de X^3+X+1, le vérifier explicitement avec une d'entre elles
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)
15) A quels automorphismes correspondent les trois isomorphismes identifiés entre les deux constructions ?