UNIVERSITE MOHAMED BOUDIAF M'SILA

FACULTE DES MATHEMATIQUES ET DE L'INFORMATIQUE

Département de Mathématiques

MEMOIRE DE FIN D'ETUDE

Présenté pour l'obtention du diplôme de **Master**

Domaine : Mathématiques et Informatique

Filière : Mathématiques

Option : Mathématiques discrètes

Par

OUADAH KHOUKHA

Sujet

Polynômes cyclotomiques sur un corps fini (un cas particulier sur F_2)

Devant le jury composé de :

Président :	A. Amroune	Prof	Univ M'sila
Rapporteur :	C. Mihoubi	MC /B	Univ M'sila
Examinateur :	L .Ladjlat	MA/A	Univ M'sila

Promotion: 2014/2015

Résumé

Dans ce mémoire on considère les polynômes sur un corps fini qui ont beaucoup d'application notamment dans la théorie algébrique du codage. Le plus important pour les polynômes dans $F_2[x]$, où F_2 est un corps fini à 2 élémemts, sont les polynômes cyclotomiques. Pour l'instant la seule chose que nous sachions sur le polynôme cyclotomique est de la forme : (pour n un entier supérieur à 1, et α une racine primitive $n - ième$ de l'unité)

$$\Phi_n = (x - \alpha_1)(x - \alpha_2)...(x - \alpha_{\varphi(n)}) \in F(\alpha)[x] \text{ et } \alpha_1, \alpha_2, ..., \alpha_{\varphi(n)} \text{ dans } F(\alpha).$$

Et essayé d'écrire un polynôme cyclotomique sous forme d'un polynôme irréductible

Mots clefs : Corps fini, polynômes irréductibles, polynômes cyclotomiques.

ABSTRACT

In this memory we consider the polynomials on a finished field which have much application in particular in the algebraic theory of coding.The most important for the polynomials dans$F_2[x]$, where F_2 is finished body of 2 elements, are polynomials cyclotomic . For the instar the only thing that we know about the cyclotomic polynomial which has the following form: (for n an entirety higher than 1, and α a nth primitive root of the unit)

$$\Phi_n = (x - \alpha_1)(x - \alpha_2)...(x - \alpha_{\varphi(n)}) \in F(\alpha)[x] \text{ et } \alpha_1, \alpha_2, ..., \alpha_{\varphi(n)} \text{ dans } F(\alpha).$$

And tried to write a cyclotomic polynomial in the form of an irreducible polynomial

Key words : field finished, irreducible polynomials, cyclotomic polynomials.

Table des matières

Introduction

en 1801, les polynômes cyclotomiques sont utilisé par Carl Friedrich Gauss dans ses Disquisitiones arithmeticae. Il apporte une contribution majeure à un problème ouvert depuis l'Antiquité : celui de la construction à la règle et au compas de polygones réguliers. Ces travaux servent de référence durant tout le siècle. Dans ce texte, Gauss détermine avec exactitude la liste des polygones constructibles, et donne une méthode effective pour leur construction jusqu'au polygone à 256 côtés. Ce problème de construction reçoit une réponse définitive en (1837) par Pierre-Laurent Wantzel.

Gauss met en évidence de tels ensembles et utilise le transport de structure par morphisme entre deux anneaux pour montrer le caractère irréductible des polynômes cyclotomiques. Dans le même livre, il utilise ces mêmes structures pour résoudre un autre problème pressenti par Fermat (1601 – 1685) et formalisé par Euler (1707 – 1783) : celui de la loi de réciprocité quadratique.

Dès cette époque, de nombreuses applications sont proposées tel que Le polynôme cyclotomique d'indice quatre permet la construction d'un nouvel ensemble de nombres algébriques celui des entiers de Gauss.

D'autre parte Joseph-Louis Lagrange (1736 – 1813) comprend que la résolution de ce problème général est intimement liée aux propriétés des permutations des racines. Le cas particulier des polynômes cyclotomiques l'illustre.

En mathématiques, plus précisément en algèbre commutative, le polynôme cyclotomique usuel associé à un entier naturel n est le polynôme sont les racines primitives $n - ièmes$ de l'unité. Son degré vaut $\varphi(n)$, où φ désigne la fonction indicatrice d'Euler. Il est à coefficients entiers et irréductible sur $\mathbb{Q}$. Lorsqu'on réduit ses coefficients modulo un nombre premier p ne divisant pas n, on obtient un polynôme unitaire (également appelé polynôme cyclo-

tomique) à coefficients dans le corps fini F_p, et dont les racines sont les racines primitives $n - ièmes$ de l'unité dans la clôture algébrique de ce corps, mais qui n'est plus nécessairement irréductible. Pour tout entier m, le polynôme X^{m-1} est le produit des polynômes cyclotomiques associés aux diviseurs de m.

Notre travail comporte trois chapitres :

Dans le premier chapitre, nous évoquons les principales propriétés des corps finis.

Dans le deuxième chapitre nous parlerons sur les polynômes irréductibles sur corps finis

Et Dans le dernier chapitre nous présentons "Les polynômes cyclotomiques en général sur Z et en particulier sur F_2".

Bibliographie

[1] **F. Butin**. *Algèbre polynômes, théorie de Galois et applications informatiques.* Hermann éditeurs 6 rue de la sorbonne 75005, Paris.

[2] **N. Bruyère**. Eléments de théorie des corps finis. Agrégation de mathématiques. Université de Rouen. (2005-2006).

[3] **S. Caruso**. Polynômes cyclotomiques. La plupart des livres d'algèbre par exemple Demazure.

[4] **A. Doneddu**. *Polynômes et algébre linéaire.* Librairie vuibert, 63, boulevard saint-Germain, 75005 paris, (1979).

[5] **D. Guin, T. Hausberger**. *Algèbre I(groupes, corps et théorie de Galois).* Parc d'activittesnde courtabeuf, BP112, France.

[6] **A. kraus**. corps finis. Cours de cryptographie MM067. Université Pierre et Marie Curie. (2012/2013).

[7] **C. Mihoubi**. Etude sur l'irréductibilité d'un polynôme sur un corps fini.Thèse de Magistére. Université Mohamed boudiaf M'sila, (2001).

[8] **C. Mihoubi**. Cours de corps fini et polynôme. 1^{ere} anneé Master. *Université Mohamed boudiaf M'sila*, (2013-2014).

[9] **J . Onillon** . L'incroyable histoire des polynômes cyclotomiques (Décembre 1994/Juillet 2001). free cyclo. pdf/application /pdf objects.

[10] **L. Pierre**. *Polynômes irréductibles corps de rupture. Exemples et application*s (2010).

[11] **F. Ulmer**. Théorie des groupes. Edition Marekting S.A, rue Bargue 75740 Paris, (2012).

[12] Corps finis Licence de mathématiques (L3)Compléments d'algèbre et arithmétique *Université de Nice* (2005-06) . www-math. unice. Fr/∼ merbe/complement/corps-fini. pdf.