REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère De L'Enseignement Supérieur et De la Recherche Scientifique

UNIVERSITÉ D'ORAN1 AHMED BEN BELLA
Faculté des Sciences Exactes et Appliquées
Département de mathématiques

Thèse

Présentée par

KEBLI SALIMA

Pour Obtenir

LE DIPLÔME DE Doctorat en sciences

Spécialité : Mathématiques

Option : Algèbre et cryptographie

Intitulée :

Polynômes de permutation sur des corps finis et équations diophantiennes

Soutenue le 29-06-2017 à 13h devant le jury composé de

TERBECHE M. Professeur, Université d'Oran 1 Ahmed Benbella	Président
KIHEL O. Professeur, Brock Université - Canada	Directeur de thèse
BELGHABA K. Professeur, Université d'Oran 1 Ahmed Benbella	Co-directeur
MORTAD M.H. Professeur, Université d'Oran 1 Ahmed Benbella	Examinateur
BENCHERIF F. Professeur, USTHB – Alger	Examinateur
TLEMCANI M. Professeur, USTO - Oran	Examinateur
BENSEBAA B. MCA, USTHB – Alger	Membre invité

Année universitaire : 2016/2017

Polynômes de permutation sur des corps finis et équations diophantiennes

Dédicaces

Mes pensées à ma mère qui aurait été fiere de voir cet instant.

A ma famille, ma belle famille.

A mes enfants Achraf et Fatima Bouchra.

Remerciements

J'adresse mes vifs remerciements aux personnes qui ont contribués à l'effort de ce travail, par leur riche collaboration et leur disponibilité.

Je témoigne ma gratitude et reconnaissance particulière à **Mr O.KIHEL**, encadreur principal et Professeur de Brock university, Ontario (Canada), pour ses contributions approfondies, ainsi que son orientation dans mon processus de recherche.

L'attention témoignée et son professionnalisme ont grandement contribué à l'aboutissement de cette thèse. Je citerai également son hospitalité d'accueil pour mon stage pratique au sein de Brock university.

Je remercie vivement **Mr M. TERBECHE**, Professeur de l'université d'Oran 1, d'avoir accepté de présider le jury de soutenance. Je lui en suis très reconnaissante.

J'adresse de sincères remerciements à **Mr K. BELGHABA**, co-encadreur local et Professeur de l'université d'Oran 1, pour ses conseils avisés et son ecoute qui ont été prépondérants pour la bonne réussite de cette thèse.

Je remercie également **Mr F. BENCHERIF**, **Mr B. BENSEBAA**, Professeurs de l'USTHB (Alger) et **Mr M. TLEMCANI**, Professeur de l'USTO (Oran), qui nous honnorent de leur présence pour l'évaluation et l'appréciation du travail proposé.

Un grand remerciement revient à **Mr M.H. MORTAD**, Professeur de l'université d'Oran 1, pour avoir accepté d'examiner ce travail. Je lui en suis reconnaissante d'avoir porté son regard d'expert à ce manuscrit.

L'intervention dans mes recherches de **Mr M. AYAD**, Professeur de l'université de Littoral, Calais (France), m'a permis d'enrichir ma documentation, compte tenu de la particularité du sujet traité ; je le remercie.

Table des matières

Notations et Abréviations

$\mathbb{F}_q$	Corps de *Galois* d'ordre q
$\mathbb{F}_q^*$	Groupe multiplicatif cyclique
$\mathbb{F}_p[x]$	L'anneau des polynômes à une indéterminée à coefficients dans $\mathbb{F}_p$
$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}$	L'application trace de $\mathbb{F}_{q^m}$ dans $\mathbb{F}_q$
$N_{\mathbb{F}_{q^m}/\mathbb{F}_q}$	L'application norme de $\mathbb{F}_{q^m}$ dans $\mathbb{F}_q$
$\varphi(n)$	La fonction indicatrice d'*Euler*
$\mu(n)$	La fonction arithmétique de *Möbius*
$K(\alpha)$	Corps d'extension simple de K
$N_p(d)$	Nombre de polynômes irréductibles unitaires de degré d dans $\mathbb{F}_p[x]$
$deg(f)$	Degré du polynôme f
$[\mathbb{F}_{p^m} : \mathbb{F}_p]$	Dimension de $\mathbb{F}_{p^m}$ en tant que $\mathbb{F}_p-$espace vectoriel
$Gal(\mathbb{F}_{q^m} : \mathbb{F}_q)$	Groupe de *Galois* de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$
$pgcd(n, m)$	Plus grand diviseur commun de n et m
$Ind_b(a)$	Logarithme discret de a en base b

Introduction

L'étude des polynômes de permutation est un sujet qui a été initié par *Hermite* en 1863 concernant les corps premiers. D'autres résultats ont été énoncés par *Dickson* en 1897 sur les polynômes de permutation définis sur des corps généraux. Il s'agit d'un domaine vaste d'un intérêt considérable en raison de son lien à des systèmes cryptographiques et de l'analyse combinatoire [15] [16] [3] [4] et [21].

De nombreux auteurs ont travaillé sur ce sujet , *Carlitz, Dickson, Zur gathen, Lidl, Niederreiter*. Cependant il reste encore des questions ouvertes.

Le problème réccurent qui se pose est celui de trouver de bons algorithmes pour tester si un polynôme défini sur un corps fini est de permutation.

En 1991, *Von Zur Gathen* [25] a montré qu'il est facile d'obtenir des algorithmes probabilistes efficaces de complexité polynomiale et même linéaire à partir de critères simples. Cet algorithme consiste soit à remplacer des relations polynomiales par leur évaluation dans une extension du corps de base, soit à tester sur un échantillon réduit une propriété qui doit être vraie pour tous les éléments du corps. Nous donnerons les détails dans le deuxième chapitre.

En 1988, les travaux de *Lidl et Mullen* [14] s'orientaient vers la détermination d'un algorithme déterministe de complexité inférieure à $O(nq)$ où n est le degré du polynôme, et q est le cardinal du corps de base. Une solution à ce problème a été énoncée par *Shparlinski* [22] en utilisant la relation avec les polynômes exeptionnels [17]. Mais la complexité obtenue restait toujours exponentielle. Par la suite, en 2005, *Kayal* [11] a proposé un algorithme polynomial déterministe en utilisant les avancées dans le domaine de la factorisation des polynômes.

En 1993, *Lidl et Mullen* [16] ont proposé une liste des problèmes ouverts concernant les polynômes de permutation. Les propriétés, les constructions et les applications des polynômes de permutation sont répertoriés et définis dans l'ouvrage de *Lidl* et *Neiderreiter* [17].

Une équation diophantienne est une équation polynomiale de la forme $f(x_1, ..., x_n) = 0$ dont les coefficients sont des entiers et dont on cherche les solutions entières i.e dans $\mathbb{Z}^n$, ou rationnelles i.e dans $\mathbb{Q}^n$.
L'exemple le plus fascinant est l'équation de *Fermat* dont la forme est

$$x^n + y^n = z^n, \quad n \geq 3$$

Au XVIIème siècle, *P. Fermat* conjecture que l'équation ci-dessus n'admet pas de solutions non triviales, la résolution complète de ce problème a occupé les plus grands mathématiciens pendant plus de trois siècles, et a contribué à developper de nombreuses théorie. Par exemple en cherchant à résoudre les équations connu sous le nom de *Pell-Fermat* et dont la forme est $x^2 - Ny^2 = \pm 1$, on est amené à introduire le corps de nombres $\mathbb{Q}(\sqrt{N})$ et les solutions de l'équation sont les unités de ce corps de nombres.
Dans un sens plus large, on appelle un problème diophantien, la recherche des points entiers ou rationnels sur les courbes algébriques que définissent ces équations. Dans cette direction, le théorème de *Siegel* nous offre un point de départ permettant de décider la finitude ou l'infinitude du nombre de solutions. Lorsque le théorème de *Siegel* assure la finitude du nombre de solutions, on s'intérèsse à la recherche de ces solutions.
En 1970, *Yu. Matiiassevitch* a répondu au dixième problème de *Hilbert*, et a démontré l'impossibilité de trouver un algorithme permettant de trouver explicitement les solutions d'une équation diophantienne. Ce théorème ne permet pas de faire une étude généralisée, mais laisse la possibilité d'une étude particulière à chaque situation.

Cette thèse est consacrée à l'étude des polynômes de permutation, ainsi qu'à la recherche de solutions d'une équation diophantienne, a savoir l'équation pyramidale carrée de *Lucas*. Elle est organisée en cinq chapitres.

Dans le premier chapitre, nous mettons en place des objets mathématiques qui serviront par la suite. Il s'agit des corps finis, et des notions indispensables comme la caractéristique et sa relation avec les sous corps et les extensions de corps, le groupe multiplicatif cyclique $\mathbb{F}_q^*$, et le groupe de *Galois* de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$.

Le deuxième chapitre est consacré aux polynômes de permutation. Nous donnons d'abord la définition formelle, ainsi que les critères simples permettant de tester si un polynôme induit une permutation sur un corps fini. Nous présentons aussi une liste assez exhaustive de classes de polynômes de permutation, telles que les polynômes linéarisés, les polynômes quadratiques, les polynômes binomiaux, les polynômes exceptionnels, ainsi que les polynômes de *Dickson*.

Dans le troisième chapitre, nous portons un intérêt particulier aux polynômes dits de troisième espèce de la forme $x^r f(x^{\frac{q-1}{d}})$, où d est un diviseur de $q-1$, selon le travail de *Wan* et *Lidl* [27]. A cette occasion, nous discutons le critère de *Wan* et *Lidl* [27] qui donne des conditions nécessaires et suffisantes pour que cette classe de polynômes soit de permutation. Les outils mathématiques utilisés à cet effet sont les notions de caractères multiplicatifs définis sur le groupe multiplicatif $\mathbb{F}_q^*$ et de racine primitive. Une partie de ce chapitre est consacrée au travail de *Ayad* et *Kihel* [5] qui ont établi des conditions suffisantes sur les entiers u et q pour que les polynômes de la forme $h(x) = x^u(1+x^{\frac{q-1}{4}}+x^{\frac{q-1}{2}})$ soient des permutations, en utilisant des méthodes élémentaires.

Dans le quatrième chapitre, nous présentons le contenu de notre publication intitulée "On a familly of permutation polynomials" [7]. Nous nous intéressons spécialement aux polynômes de la forme

$$h(x) = x^u(1 \pm x^{\frac{q-1}{4}} \pm x^{\frac{q-1}{2}}).$$

Nous donnons des conditions nécessaires et suffisantes telles que $h(x)$ soit une permutation, en se basant sur l'application du théorème de *Wan* et *Lidl* [27].

Enfin dans le cinquième chapitre, nous étudions un problème diophantien qui concerne la recherche de solutions de l'équation diophantienne de *Lucas* et dont la forme est

$$n^3 + (n+1)^3 + ... + (n+k-1)^3 = y^2$$

La réponse à cette question donne naissance à notre seconde publication intitulée "On a variant of the Lucas' square pyramid problem"[12]. Nous donnons ainsi une majoration à l'entier k en fonction de n et nous listons toutes les solutions possibles, en se reposant seulement sur des méthodes élémentaires.

Chapitre 1

Corps finis

La théorie des corps finis est née au $XVIII^e$ siècle avec les travaux de *Gauss* et ceux de *Galois*, dans le contexte de la résolution d'équations dans le corps des entiers modulo le nombre premier p, noté $\mathbb{F}_p$. Un corps fini est entièrement déterminé par son ordre, qui est une puissance d'un nombre premier. Ce nombre étant appelé sa caractéristique.
Avec le développement de l'informatique, les corps finis ont trouvé de nombreuses applications. Ils interviennent par exemple en cryptographie, dans la conception des chiffrements à clés secrète et publique, en théorie des codes pour déterminer des codes correcteurs efficaces et pour le problème du logarithme discret.
Dans ce chapitre nous présentons les aspets principaux des corps finis avec des preuves dans la plupart des cas. Pour d'autres, des justifications sont disponibles dans *Lidl* et *Neiderreiter* [17].

1.1 Caractérisation des corps finis

1.1.1 Caractéristique et cardinal

Soit K un corps. L'application

$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \longrightarrow & K \\ & & n & \longmapsto & n1_K \end{array}$$

est un homomorphisme d'anneaux dont l'image $Im\varphi$ est le sous groupe additif engendré par l'unité 1_K et dont le noyau est un idéal de $\mathbb{Z}$. Par décomposition canonique, on obtient un isomorphisme d'anneaux ψ qui rend le diagramme suivant commutatif :

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi} & K \\ \downarrow & & \uparrow \\ \mathbb{Z}/m\mathbb{Z} & \xrightarrow[\psi]{} & Im\varphi \end{array}$$

$m\mathbb{Z}$ n'est autre que le noyau de φ. S'il est réduit à $\{0\}$, on dit que le corps K est de caractéristique nulle. Sinon c'est un idéal premier puisque K n'admet pas de diviseurs de zéro, ainsi on a nécessairement $m = p$ (premier). Le nombre p est appelé la caractéristique du corps K.

Pour tout nombre premier p, l'ensemble des éléments de l'anneau $\mathbb{Z}/p\mathbb{Z}$ forme un corps fini d'ordre p, qui peut être identifié avec le corps de *Galois* d'ordre p noté $\mathbb{F}_p$.
Les corps premiers $\mathbb{F}_p$ jouent un role trés important dans la théorie des nombres. En effet tout corps K de caractéristique p contient un sous-corps isomorphe à $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, et donc peut être considéré comme une extension de $\mathbb{F}_p$. Cette observation avec le fait que tout corps fini est de caractéristique p premier, est fondamentale pour la construction des corps finis.
Nous présentons dans ce qui suit, une série de résultats concernant les corps finis.

Lemme 1.1 *Soit K un corps fini contenant un sous corps L de cardinal q. Alors K est de cardinal q^m, où $m = [K : L]$ est la dimension de K en tant que L-espace vectoriel.*

Preuve : Comme K est fini et $L \subseteq K$, alors il peut être muni d'une structure de L-espace vectoriel de dimension finie $m = [K : L]$. Ainsi tout élément $v \in K$ s'écrit de manière unique

$$v = \alpha_1 v_1 + ... + \alpha_m v_m$$

où les $(v_i)_{i=1,...,m}$ forment une base du corps K et les $(\alpha_i)_{i=1,...,m}$ sont dans K. Il vient que $K \simeq L^m$. Il y a alors une relation entre les cardinaux de ces corps et la dimension m donnée par

$$\mid K \mid = \mid L \mid^{m=[K:L]} \text{ i.e } \mid K \mid = q^m . \square$$

Proposition 1.1 *Soit K un corps fini de caractéristique p premier, alors K possède p^n éléments avec $n \in \mathbb{N}^*$.*

Preuve : En effet, le nombre n est égal à la dimension de K considéré comme espace vectoriel sur $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ i.e $(K \supset \mathbb{F}_p)$ et $n = [K : \mathbb{F}_p]$ alors

$$K \simeq (\mathbb{F}_p)^n \implies \mid K \mid = p^n . \square$$

On constate que $\mathbb{F}_p$ est le plus petit sous corps de K, puisque tout corps fini de caractéristique p premier contient nécessairement $\mathbb{F}_p$.

On va voir par la suite qu'on peut construire des corps finis à $q = p^n$ éléments à partir des polynômes irréductibles sur $\mathbb{F}_p$, et ceci par adjonction de α (racine d'un polynôme irréductible de degré n dans une extension de $\mathbb{F}_p$) à $\mathbb{F}_p$. Mais jusqu'à présent rien ne justifie l'existence d'un tel polynôme pour toute valeur de p premier et $n \in \mathbb{N}^*$. On ne peut donc pas en déduire pour l'instant qu'un corps à $q = p^n$ éléments existe toujours. Nous allons considérer les résultats suivants :

Proposition 1.2 *Si K est un corps fini de cardinal q, (nécessairement commutatif d'après le théorème de Wedderburn) alors pour tout $a \in K$, $a^q = a$.*

Preuve : S'il existe un corps K à q éléments, alors tout élément a non nul de K vérifie $a^{q-1} = 1$ d'après le théorème de *Lagrange*[1] appliqué au groupe multiplicatif K^* de K,

1. Si G est un groupe fini, alors pour tout sous groupe H de G, $\mid H \mid$ divise $\mid G \mid$.

ainsi $a^q = a$ pour tout $a \in K$. $\square$

Ici, K est le corps de décomposition du polynôme $f(x) = x^q - x \in \mathbb{F}_p[x]$ alors $f(x) = x^q - x$ peut être factoriser sur K comme

$$x^q - x = \prod_{a \in K} (x - a)$$

Lemme 1.2 *Si K est un corps de caractéristique p, alors*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n},\ \forall a, b \in K \text{ et } n \in \mathbb{N}^*$$

Preuve : On raisonne par récurrence sur n.

Pour $n = 1$, la formule du binôme de *Newton* s'écrit

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} \tag{1.1}$$

et l'on vérifie que tout les coefficients binomiaux $\binom{p}{i}$ sont divisible par p dès que $0 < i < p$. En effet,

$$\begin{aligned} \binom{p}{i} = \frac{p!}{(p-i)!i!} &\Rightarrow p! = (p-i)!i!\binom{p}{i} \\ &\Rightarrow p(p-1)...(p-i+1) = i!\binom{p}{i} \end{aligned}$$

On en déduit que p divise $i!\binom{p}{i}$, et comme p est premier alors il est premier avec chacun des facteurs du produit $i!$, alors $pgcd(p, i!) = 1$. Et comme p divise $i!\binom{p}{i}$ alors d'après le théorème de *Gauss*[2], p divise $\binom{p}{i}$ ce qui implique que

$$\binom{p}{i} \equiv 0 \pmod{p}, \quad 0 < i < p,$$

on aura donc

$$(a+b)^p = a^p + b^p.$$

Enfin, si la propriété est vraie pour n, alors elle est vraie pour $n+1$

$$(a+b)^{p^{n+1}} = [(a+b)^{p^n}]^p = [a^{p^n} + b^{p^n}]^p = a^{p^{n+1}} + b^{p^{n+1}} \ \square$$

2. Si un entier a divise le produit de deux entiers b et c et tel que $(a, b) = 1$, alors a divise c.

Proposition 1.3 *Existence et unicité des corps finis*
Pour tout nombre premier p et tout entier positif n, il existe un corps fini à $q = p^n$ éléments isomorphe au corps de décomposition de $x^q - x$ sur $\mathbb{F}_p$.

Preuve :
Existence : Pour $q = p^n$. Considérons $x^q - x$ sur $\mathbb{F}_p[x]$ et K le corps de décomposition du polynôme $x^q - x$ sur $\mathbb{F}_p$. Le polynôme $f(x) = x^q - x$ admet q racines distinctes dans K i.e qu'il est séparable puisque $f'(x) = qx^{q-1} - 1 = -1$ sur $\mathbb{F}_p$.
L'ensemble $S = \{a \in K : a^q - a = 0\}$ est un sous-corps de K, en effet

— 0 et 1 sont bien dans S,
— si $a, b \in S$ d'après le lemme (1.2) on a $(a-b)^q = a^q - b^q = a - b$, d'où $a - b \in S$,
— si $a, b \in S$ et $b \neq 0$, $(ab^{-1})^q = a^q b^{-q} = ab^{-1} \in S$

ainsi S est de cardinal $q = p^n$ dont ses éléments sont les racines de $x^q - x$ i.e $S = K$.
Unicité : l'unicité provient du résultat général sur l'existence et l'unicité du corps de décomposition d'un polynôme donné f sur le corps $\mathbb{F}_p$.□

Le corps fini à q éléments est le corps de *Galois* d'ordre q noté $\mathbb{F}_q$ désignant une extension du corps premier $\mathbb{F}_p$. Une conséquence est qu'il ne peut pas exister de corps finis à q éléments si q n'est pas une puissance d'un nombre premier p.

Proposition 1.4 *Soient $n, m \in \mathbb{N}^*$, on a $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ si et seulement si $m \mid n$.*

Preuve :
Supposons que $\mathbb{F}_{p^m}$ est un sous corps de $\mathbb{F}_{p^n}$, alors on peut considérer $\mathbb{F}_{p^n}$ comme un espace vectoriel sur $\mathbb{F}_{p^m}$ de dimension $k = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]$, ceci donne la relation

$$| \mathbb{F}_{p^n} | = | \mathbb{F}_{p^m} |^k \Longrightarrow p^n = p^{mk} \Longrightarrow m \mid n.$$

Réciproquement, si $m \mid n$ alors il existe un certain $k \geq 1$ tel que $n = km$, et d'après la Proposition 1.3, le polynôme $x^{p^n} - x$ est scindé dans $\mathbb{F}_{p^n}$. Et ses racines, deux à deux

distinctes sont exactement les éléments de $\mathbb{F}_{p^n}$. D'autre part,

$$\begin{aligned} x^{p^n} - x &= x^{p^{mk}} - x \\ &= (x^{p^m} - x) + (x^{(p^m)^2} - x^{p^m}) + ... + (x^{(p^m)^k} - x^{(p^m)^{k-1}}) \\ &= (x^{p^m} - x) + (x^{p^m} - x)^{p^m} + ... + (x^{p^m} - x)^{p^{m(k-1)}} \end{aligned}$$

Donc $x^{p^m} - x$ divise $x^{p^n} - x$ et aussi toutes ses racines dans $\mathbb{F}_{p^n}$. Ces racines sont exactement les points fixes dans $\mathbb{F}_{p^n}$ de l'endomorphisme de *Frobenius* de $\mathbb{F}_{p^m}$, donc ils forment un sous corps de cardinal p^m ainsi on a bien $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$. $\square$

Cette proposition montre que l'unique sous corps de $\mathbb{F}_{p^n}$ d'ordre p^m (où $m \mid n$) consiste précisément en les racines du polynôme $x^{p^m} - x$ sur $\mathbb{F}_{p^n}$, ce qui donne un moyen de tester si un élément de $\mathbb{F}_{p^n}$ appartient bien à un de ses sous corps.

Exemple 1.1 *Les sous corps du corps fini* $\mathbb{F}_{3^{48}}$ *peuvent être déterminer à partir des diviseurs du nombre* 48 *comme l'indique la Figure 1.1*

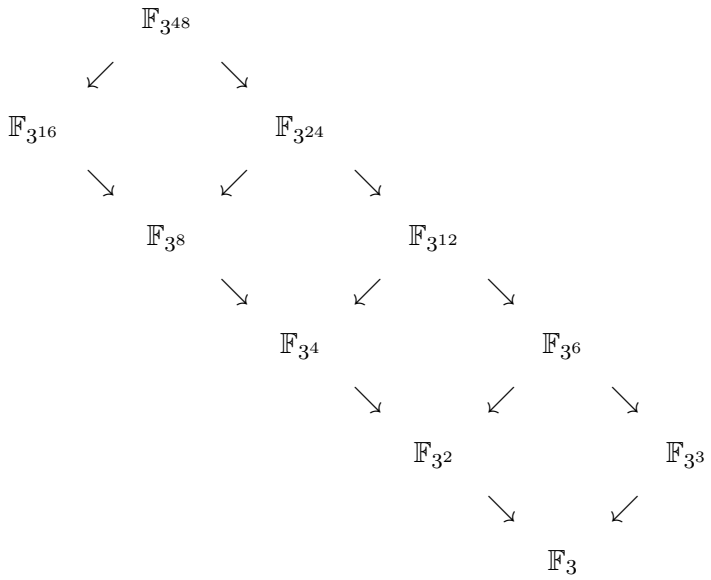

FIGURE 1.1 – Sous-corps du corps $\mathbb{F}_{3^{48}}$

Théorème 1.1 *[17] Pour tout corps fini $\mathbb{F}_q$, le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique.*

Preuve : Supposons que $q \geq 3$ et soit $h = p_1^{\alpha_1} p_2^{\alpha_2} .... p_m^{\alpha_m}$, avec $\alpha_i \in \mathbb{N}^*$ la décomposition en produit de facteurs premiers de $h = q - 1$ (l'ordre de $\mathbb{F}_q^*$).

Pour tout $i, 1 \leq i \leq m$, le polynôme $x^{\frac{h}{p_i}} - 1$ admet au plus $\frac{h}{p_i}$ racines dans $\mathbb{F}_q$, et comme $\frac{h}{p_i} < h$, alors il existe $a_i \in \mathbb{F}_q^*$ tel que $a_i^{\frac{h}{p_i}} \neq 1$.

Soit $b_i = a_i^{\frac{h}{p_i^{\alpha_i}}} \Longrightarrow b_i^{p_i^{\alpha_i}} = a_i^h = 1$ alors l'ordre de b_i divise $p_i^{\alpha_i}$ cela veut dire qu'il est de la forme $p_i^{s_i}$ avec $0 \leq s_i \leq \alpha_i$.

Si $s_i < \alpha_i$, on pourrait écrire

$$b_i^{p_i^{s_i}} = 1 \Longrightarrow a_i^{hp_i^{s_i - \alpha_i}} = 1 \Longrightarrow a_i^{\frac{h}{p_i}} = 1$$

ce qui est absurde, donc b_i est d'ordre $p_i^{\alpha_i}$.

Montrons alors que l'élément $b = b_1 b_2 .....b_m$ est d'ordre $h = q - 1$.

Supposons que l'ordre de b divise h alors $|< b >|$ divise $\frac{h}{p_i}$ pour un certain $i, 1 \leq i \leq m$, on suppose que $i = 1$ alors

$$|< b >| \quad \text{divise} \quad \frac{h}{p_1} \Longrightarrow 1 = b^{\frac{h}{p_1}} = b_1^{\frac{h}{p_1}} b_2^{\frac{h}{p_1}} .... b_m^{\frac{h}{p_1}}$$

mais

$$p_i^{\alpha_i} \text{ divise } \frac{h}{p_i}, 2 \leq i \leq m \Longrightarrow b_i^{\frac{h}{p_1}} = 1 \Longrightarrow b_1^{\frac{h}{p_1}} = 1 \Longrightarrow |< b_1 >| \text{ divise } \frac{h}{p_1}$$

ce qui est impossible puisque $|< b_1 >| = p_1^{\alpha_1}$, ainsi $\mathbb{F}_q^*$ est cyclique de génerateur b. □

Définition 1.1 *On appelle élément primitif de $\mathbb{F}_q$ tout générateur du groupe multiplicatif $\mathbb{F}_q^*$.*

On remarque par ailleurs que $\mathbb{F}_q$ admet exactement $\varphi(q-1)$ éléments primitifs où φ désigne la fonction indicatrice d'*Euler*[3]. De plus si α est un élément primitif de $\mathbb{F}_q^*$ alors l'ensemble des générateurs de $\mathbb{F}_q^*$ est

$$\{\alpha^k / 1 \leq k \leq q-1 \quad \text{et} \quad pgcd(k, q-1) = 1\}$$

3. L'indicatrice d'*Euler* est une fonction arithmétique, qui à tout entier $n > 0$ associe le nombre d'entiers compris entre 1 et n et premiers avec n.

1.2 Extension de corps

Soit K un sous corps du corps F (pas nécessairement fini), et M un ensemble de F, alors le corps $K(M) = \bigcap_{i \in I} F_i, \quad F_i \leq F$ et $K \subseteq F_i$ et $M \subseteq F_i$ pour $i \in I$ est un corps d'extension de K obtenu par adjonction les éléments de M à K. Pour $M = \{\theta_1, ..., \theta_n\}$ on écrit $K(M) = K(\theta_1, ..., \theta_n)$ et si $M = \{\theta\}$ alors $L = K(\theta)$ est dite extension simple de K et θ est un élément primitif de L sur K.

Définition 1.2 *Soit K un sous corps de F et $\theta \in F$, si θ satisfait un polynôme non trivial à coefficients dans K i.e si $a_n\theta^n + ... + a_1\theta + a_0 = 0, \quad a_i \in K$ non tous nuls alors θ est dit algébrique sur K.*
Une extension L de K est dite algébrique sur K si tout élément de L est algébrique.

Supposons que $\theta \in F$ est algébrique sur K et considérons l'ensemble $J = \{f \in K[x] \ / \ f(\theta) = 0\}$. J est un idéal de $K[x]$ différent de (0) puisque θ est algébrique. Il existe alors un polynôme irréductible unitaire $g \in K[x]$ tel que J soit un idéal principal engendré par g, le polynôme g est alors appelé polynôme minimal de θ sur K. Le degré de θ sur K est le degré du polynôme g.

Note 1.1 *On note qu'une extension simple $K(\alpha)$ est finie si et seulement si α est algébrique sur K. Un exemple d'une extension simple infinie de K (à isomorphisme près) est le corps de fractions rationnelles $K(x)$, où x est considérée comme étant variable.*

1.3 Existence de polynômes irréductibles

La construction explicite du corps $\mathbb{F}_{p^n}$ est basée sur l'existence d'un polynôme irréductible unitaire $f(x) \in \mathbb{F}_p[x]$ de degré n. On note qu'il est facile de montrer que pour tout $n \in \mathbb{N}^*$, il existe un polynôme irréductible de degré n dans $\mathbb{F}_p[x]$, mais l'expression explicite d'un tel polynôme s'avère difficile.

Notons $N_p(d)$ le nombre de polynômes irréductibles unitaires de degré d dans $\mathbb{F}_p[x]$. On a alors la propriété suivante

$$p^n = \sum_{d/n} dN_p(d), \quad \forall n \in \mathbb{N}^* \tag{1.2}$$

Pour l'étude de cette dernière équation, on considère le polynôme $f(x) = x^{p^n} - x \ \in \mathbb{F}_p[x]$ et sa décomposition en facteurs irréductibles unitaires

$$f(x) = p_1(x)...p_r(x)$$

On sait déja que ce polynôme n'admet pas de facteurs multiples puisque $f'(x) = -1$. Les polynômes $p_i(x),\ i = 1, ..., r$ sont exactement les polynômes irréductibles de $\mathbb{F}_p[x]$ dont le degré divise n.

En effet, Si $p(x)$ est irréductible de degré d, et α une racine de p dans une extension de $\mathbb{F}_p$. cette extension est alors de degré d sur $\mathbb{F}_p$ isomorphe à $\mathbb{F}_{p^d}$. On a donc

$$x^{p^d} = x \ \Rightarrow x^{p^n} = x \text{ puisque } d \text{ divise } n.$$

Il en resulte que $p(x)$ divise $f(x)$.

Réciproquement si $p(x)$ est irréductible de degré d et divise $f(x)$, alors toute racine α de $p(x)$ annule $f(x)$ donc $\mathbb{F}_{p^n}$ contient $\mathbb{F}_{p^d} = \mathbb{F}_p(\alpha)$ d'où d divise n.

En comparant le degré de f avec le produit $\prod_{i=1}^{r} p_i(x)$, on obtient l'équation (1.2).

Définissons maintenant la fonction arithmétique de *Möbius* qui va de $\mathbb{N}^*$ vers l'ensemble $\{0, 1, -1\}$ par

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^k & \text{si } n \text{ est produit de } k \text{ facteurs premiers distincts} \\ 0 & \text{si } n \text{ admet un facteur carré} \end{cases}$$

cette fonction satisfait pour $n \in \mathbb{N}^*$ la propriété suivante

$$\sum_{d/n} \mu(d) = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si } n > 1 \end{cases}$$

Pour dériver une formule explicite qui détermine le nombre de polynômes irréductibles unitaires dans $\mathbb{F}_p[x]$ d'un degré fixe, on a besoin de la formule d'inversion de *Möbius* Soient h et H deux fonctions de $\mathbb{N}^*$ vers le groupe additif G. On pose $H(n) = \sum_{d/n} h(d)$ alors $h(n) = \sum_{d/n} \mu(\frac{n}{d})H(d)$. En utilisant la propriété ci-dessus, on obtient

$$\begin{aligned}\sum_{d/n} \mu(d) &= \sum_{d/n} \mu(d)H(\frac{n}{d}) \\ &= \sum_{d/n} \mu(d) \sum_{c/\frac{n}{d}} h(c) \\ &= \sum_{c/n} \sum_{d/\frac{n}{c}} \mu(d)h(c) \\ &= \sum_{c/n} h(c) \sum_{d/\frac{n}{c}} \mu(d) = h(n)\end{aligned}$$

Le nombre $N_p(n)$ de polynômes irréductibles unitaires de $\mathbb{F}_p[x]$ de degré n est donné par

$$N_p(n) = \frac{1}{n} \sum_{d/n} \mu(\frac{n}{d})p^d = \frac{1}{n} \sum_{d/n} \mu(d)p^{\frac{n}{d}} \tag{1.3}$$

On applique la formule d'inversion de *Möbius* sur le groupe $\mathbb{Z}$.
Soient $h(n) = nN_p(n)$ et $H(n) = p^n,\ n \in \mathbb{N}^*$, alors d'après les formules ci-dessus, il vient

$$\begin{aligned}H(n) &= \sum_{d/n} nN_p(n) \\ &= \sum_{d/n} h(n) \\ &= \sum_{d/n} \sum_{d/n} \mu(d)H(\frac{n}{d}) \\ &= \sum_{d/n} \sum_{d/n} \mu(d)p^{\frac{n}{d}}\end{aligned}$$

$$\implies nN_p(n) = \sum_{d/n} \mu(d)p^{\frac{n}{d}} \implies N_p(n) = \frac{1}{n} \sum_{d/n} \mu(d)p^{\frac{n}{d}}$$

Exemple 1.2 *Soit $p = 5$, alors le nombre de polynômes irréductibles unitaires dans $\mathbb{F}_5[x]$ de degré 20 est donné par $N_5(20) = \frac{1}{20} \sum_{d/20} \mu(d)5^{\frac{n}{d}}$. Les diviseurs de 20 sont*

1, 2, 4, 5, 10 *et* 20.

$$\begin{aligned} N_5(20) &= \frac{1}{20}[\mu(1)5^{20} + \mu(2)5^{10} + \mu(4)5^5 + \mu(5)5^4 + \mu(10)5^2 + \mu(20)5] \\ &= \frac{1}{20}[5^{20} - 5^{10} - 5^4 + 5^2] \\ &= 4768371093720 \end{aligned}$$

1.4 Construction de corps finis

Soient $f(x) \in \mathbb{F}_p[x]$ un polynôme irréductible de degré n, et α une racine de $f(x)$ dans une extension de $\mathbb{F}_p$. Soit $\mathbb{F}_p(\alpha)$ une extension simple de $\mathbb{F}_p$ engendrée par α alors on a :

— $\mathbb{F}_p(\alpha) \simeq \mathbb{F}_p[x]/ < f(x) >$

— $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = n$ et $\{1, \alpha, ..., \alpha^{n-1}\}$ est une base de $\mathbb{F}_p(\alpha)$ sur $\mathbb{F}_p$

— Si $\theta \in \mathbb{F}_p(\alpha)$, alors θ est algébrique sur $\mathbb{F}_p$ est son degré divise n

Soit l'application

$$\begin{array}{rccc} \tau & : & \mathbb{F}_p[x] & \longrightarrow & \mathbb{F}_p(\alpha) \\ & & g & \longmapsto & \tau(g(x)) = g(\alpha) \end{array}$$

τ est un homomorphisme d'anneaux dont le noyau $Ker\ \tau$ est un idéal principal de $\mathbb{F}_p[x]$, engendré par le polynôme minimal de α i.e $ker\ \tau =< f(x) >$. Alors d'après le 1^{er} théorème d'isomorphisme on a $Im\ \tau \simeq \mathbb{F}_p[x]/ < f(x) >$, mais $\mathbb{F}_p[x]/ < f(x) >$ est un corps puisque f est irréductible ainsi $Im\ \tau$ est un corps avec $(\mathbb{F}_p \subseteq Im\ \tau \subseteq \mathbb{F}_p(\alpha))$ et $\alpha \in Im\ \tau$. Et comme $\mathbb{F}_p(\alpha)$ est le plus petit corps contenant $\mathbb{F}_p$ et α alors $Im\ \tau = \mathbb{F}_p(\alpha)$ ainsi

$$\mathbb{F}_p(\alpha) \simeq \mathbb{F}_p[x]/ < f(x) >$$

Si de plus $\mu(x) \in \mathbb{F}_p[x]$ et $\mu(\alpha) \neq 0$ alors le $pgcd(f(x), \mu(x)) = 1$. Par l'identité de *Bezout*, ils existent $a(x),\ b(x) \in \mathbb{F}_p[x]$ tels que

$$a(x)f(x) + b(x)\mu(x) = 1$$

En conséquence $b(\alpha)\mu(\alpha) = 1$. Ce qui implique que $\frac{1}{\mu(\alpha)} = b(\alpha) \in \mathbb{F}_p(\alpha)$.
Maintenant qu'on sait que $Im\,\tau = \mathbb{F}_p(\alpha)$ alors $\forall\,\theta \in \mathbb{F}_p(\alpha)$, $\exists\, g \in \mathbb{F}_p[x]$ tel que $\theta = g(\alpha)$. Par la division Euclidienne par f, il vient $g = qf + r$ avec $deg(r(x)) < deg(f(x)) = n$, d'où $\theta = g(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha)$. θ est donc une combinaison lineaire de $1, \alpha, ..., \alpha^{n-1}$ à coefficients dans $\mathbb{F}_p$.
Si $a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} = 0$, $a_i \in \mathbb{F}_p$ alors le polynôme $h(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$ admet α comme racine. Ce qui contredit la minimalité du polynôme f. Ainsi $h(x) = 0$ i.e $a_i = 0,\ i = 0, .., n-1$.
$\mathbb{F}_p(\alpha)$ est une extension finie de $\mathbb{F}_p$, d'après la section précédente tout élément $\theta \in \mathbb{F}_p(\alpha)$ est algébrique.
Soit à présent θ de degré d sur $\mathbb{F}_p$. Les relations entre les cardinaux sont les suivantes :

- $[\mathbb{F}_p(\theta) : \mathbb{F}_p] = d$,
- $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = n$,
- $[\mathbb{F}_p(\alpha) : \mathbb{F}_p(\theta)][\mathbb{F}_p(\theta) : \mathbb{F}_p] = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$

Il vient

$$[\mathbb{F}_p(\alpha) : \mathbb{F}_p(\theta)]d = n$$

Ainsi d divise n.
On constate que les éléments d'une extension algébrique simple $\mathbb{F}_p(\alpha)$ de $\mathbb{F}_p$ sont les polynômes en α

$$\mathbb{F}_p(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{n-1}\alpha^{n-1}/a_i \in \mathbb{F}_p\}$$
$$i.e\ |\mathbb{F}_p(\alpha)| = p^n$$

et par isomorphisme on aura $\mathbb{F}_q = \mathbb{F}_p(\alpha) = \mathbb{F}_p + \mathbb{F}_p\alpha + ... + \mathbb{F}_p\alpha^{n-1}$

Théorème 1.2 *Toute extension finie $\mathbb{F}_r$ d'un corps fini $\mathbb{F}_q$ est une extension simple i.e de la forme $\mathbb{F}_q(\alpha)$.*

Preuve : Si ξ est un élément primitif de $\mathbb{F}_r$, alors $\mathbb{F}_r^* = \{1, \xi, \xi^2, \xi^3, ..., \xi^{r-2}\}$ donc $\mathbb{F}_r = \mathbb{F}_q(\xi)$. □

Sachant maintenant que $\mathbb{F}_q$ avec $q = p^n$ existe. Un polynôme irréductible $f(x) \in \mathbb{F}_p[x]$ de degré $n \geq 1$ existe aussi. Alors on peut construire $\mathbb{F}_q$, comme le montre l'exemple suivant :

Exemple 1.3 *Construction pratique de* $\mathbb{F}_q$

On souhaite construire le corps $\mathbb{F}_{3^3}$ possédant $3^3 = 27$ éléments. Pour cela on considère g un polynôme unitaire irréductible de $\mathbb{F}_3[x]$ de degré 3, α une racine de g, ξ un élément primitif et x un élément de $\mathbb{F}_{3^3}$. Cet élément x admettera donc deux représentations :

- Une représentation exponentielle : si $x \neq 0$, $\exists\, i \in \{0, 1, ..., 3^3 - 2\}$ tel que $x = \xi^i$, dans ce cas x est représenté par la valeur de l'exposant i. Dans cette écriture la multiplication est facile à implémenter.
- Une représentation polynomiale : $\exists\, a_0, a_1, a_2 \in \mathbb{F}_3$ tels que $x = a_0 + a_1\alpha + a_2\alpha^2$. Dans ce cas, on représente x par la séquence $[a_2a_1a_0]$. Dans cette écriture c'est plutôt l'addition qui est facile à implémenter.

Les éléments du corps $\mathbb{F}_{27}$ sont présentés dans le tableau suivant :

$0 = [000]$	$\xi^8 = [120]$	$\xi^{17} = [211]$
$1 = [001]$	$\xi^9 = [222]$	$\xi^{18} = [011]$
$\xi = [010]$	$\xi^{10} = [121]$	$\xi^{19} = [110]$
$\xi^2 = [100]$	$\xi^{11} = [012]$	$\xi^{20} = [202]$
$\xi^3 = [102]$	$\xi^{12} = [112]$	$\xi^{21} = [221]$
$\xi^4 = [122]$	$\xi^{13} = [002]$	$\xi^{22} = [111]$
$\xi^5 = [022]$	$\xi^{14} = [020]$	$\xi^{23} = [212]$
$\xi^6 = [220]$	$\xi^{15} = [200]$	$\xi^{24} = [021]$
$\xi^7 = [101]$	$\xi^{16} = [201]$	$\xi^{25} = [210]$

TABLE 1.1 – Représentation des éléments du corps $\mathbb{F}_{3^3}$

1.5 Polynômes irréductibles et éléments conjugués

Rappelons le résultat suivant

Lemme 1.3 *soit $f \in \mathbb{F}_q[x]$ un polynôme irréductible sur $\mathbb{F}_q$ et α une racine de f dans une extension de $\mathbb{F}_q$, alors pour tout polynôme*

$$h \in \mathbb{F}_q[x],\ h(\alpha) = 0 \iff f \text{ divise } h$$

Lemme 1.4 *Soit $f \in \mathbb{F}_q[x]$ un polynôme irréductible de degré m sur $\mathbb{F}_q$. Alors*

$$f(x) \text{ divise } x^{q^n} - x \text{ ssi } m \text{ divise } n$$

Preuve : Supposons que $f(x)$ divise $x^{q^n} - x$.
Soit α une racine de f dans le corps de décomposition de f sur $\mathbb{F}_q$ alors

$$\alpha^{q^n} = \alpha \Longrightarrow \alpha \in \mathbb{F}_{q^n}$$

Cela signifie que $\mathbb{F}_q(\alpha)$ est un sous corps de $\mathbb{F}_{q^n}$ et comme

$$[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m \text{ et } [\mathbb{F}_{q^n} : \mathbb{F}_q] = n \text{ et } \mathbb{F}_q \subset \mathbb{F}_q(\alpha) \subset \mathbb{F}_{q^n}$$

il vient

$$[\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)].[\mathbb{F}_q(\alpha) : \mathbb{F}_q] \Longrightarrow n = km$$

ainsi m divise n.
Réciproquement, si m divise n ; d'après la Proposition 1.4 $\mathbb{F}_{q^n}$ est une extension de $\mathbb{F}_{q^m}$ et si α est une racine de f dans le corps de décomposition sur $\mathbb{F}_q$, alors $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ et $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$.
Par conséquent, $\alpha \in \mathbb{F}_{q^n}$ i.e $\alpha^{q^n} = \alpha$. Ainsi α est une racine de $x^{q^n} - x \in \mathbb{F}_q[x]$. Comme f est le polynôme minimal s'annulant en α, alors $f(x)$ divise $x^{q^n} - x$.□

Proposition 1.5 *Tout polynôme irréductible f de $\mathbb{F}_q[x]$ de degré m possède exactement m racines distinctes dans $\mathbb{F}_{q^m}$. Si α est l'une de ses racines, toutes les autres racines de f sont de la forme $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$*

Preuve : Soit α une racine de $f(x) = a_m x^m + a_{m-1}x^{m-1} + ... + a_1 x + a_0, a_i \in \mathbb{F}_q$ dans le corps de décomposition de f, alors $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ et $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Ainsi $\alpha \in \mathbb{F}_{q^m}$. Montrons maintenant que α^q est une racine de f. Le Lemme 1.2 et la Proposition 1.2 permettent d'écrire

$$\begin{aligned} f(\alpha^q) &= a_m\alpha^{qm} + ... + a_1\alpha^q + a_0 \\ &= a_m^q\alpha^{qm} + ... + a_1^q\alpha^q + a_0^q \\ &= (a_m\alpha^m + ... + a_1\alpha + a_0)^q \\ &= f(\alpha)^q = 0 \end{aligned}$$

Ainsi les éléments $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ sont bien les racines de f dans $\mathbb{F}_{q^m}$. Il reste seulement à vérifier qu'elles sont toutes distinctes.
Supposons $\alpha^{q^i} = \alpha^{q^j}$ avec $0 \leq i < j \leq m$, $(\alpha^{q^i})^{q^{m-j}} = (\alpha^{q^j})^{q^{m-j}} = \alpha$, $\alpha^{q^{m-j+i}} = \alpha$. Par le Lemme 1.3 $f(x)$ divise $x^{q^{m-j+i}} - x$, mais ceci est possible si seulement si m divise $m - j + i$ mais $0 < m - j + i < m$ ce qui est absurde et par suite $i = j$.□
On constate que $\mathbb{F}_{q^m}$ est bien le corps de décomposition de f puisque

$$\mathbb{F}_q(\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}) = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}.$$

On introduit à présent une définition très commode pour les éléments figurant dans la Proposition 1.5 et ceci indépendamment du fait que $\alpha \in \mathbb{F}_{q^m}$ soit une racine du polynôme irréductible de degré m dans $\mathbb{F}_q[x]$.

Définition 1.3 *Soit $\mathbb{F}_{q^m}$ une extension de $\mathbb{F}_q$ et $\alpha \in \mathbb{F}_{q^m}$ alors les éléments $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ sont appelés les conjugués de α par rapport à $\mathbb{F}_q$.*

Théorème 1.3 *Les conjugués d'un élément $\alpha \in \mathbb{F}_{q^m}^*$ ont le même ordre dans le groupe multiplicatif $\mathbb{F}_{q^m}^*$.*

Preuve : Comme $\mathbb{F}_{q^m}^*$ est un groupe multiplicatif cyclique par le Théorème 1.1, alors il existe un élément $\xi \in \mathbb{F}_{q^m}^*$ tel que $\mathbb{F}_{q^m}^* =< \xi >$. Il vient que tout sous groupe engendré par ξ^k est d'ordre $\frac{q^m-1}{pgcd(k,q^m-1)}$.
Soit $\{\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}\}$ l'ensemble des conjugués de $\alpha \in \mathbb{F}_{q^m}^*$ par rapport à $\mathbb{F}_q$.

Alors il exite un entier i tel que $\alpha = \xi^i$. Il vient que tout sous groupe engendré par $\alpha^{q^j},\ 0 \leq j \leq m-1$ est d'ordre $\frac{q^m-1}{pgcd(iq^j, q^m-1)},\ 0 \leq j \leq m-1$. Comme toute puissance de la caractéristique de $\mathbb{F}_{q^m}$ est relativement premiere avec $q^m - 1$ il découle

$$|< \alpha^{q^j} >| = \frac{q^m - 1}{pgcd(i, q^m - 1)},\ 0 \leq j \leq m-1$$

Exemple 1.4 *Soit $\alpha \in \mathbb{F}_{16=2^4}$ une racine de $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Les conjugués de α sur $\mathbb{F}_2$ sont $\alpha, \alpha^2, \alpha^4 = \alpha + 1, \alpha^8 = \alpha^2 + 1$ qui sont tous des primitifs de $\mathbb{F}_{16}$.*

1.5.1 Groupe de Galois de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$

Il y a une relation très importante entre les conjugués d'un élément et les automorphismes d'un corps fini. On définit le groupe de *Galois* de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$ par le groupe des automorphismes du corps $\mathbb{F}_{q^m}$, qui fixent les éléments de $\mathbb{F}_q$. On le note $Gal(\mathbb{F}_{q^m}, \mathbb{F}_q)$. Un élément σ de cet ensemble est une application bijective de $\mathbb{F}_{q^m}$ dans lui même vérifiant

$$\sigma(x+y) = \sigma(x) + \sigma(y)$$
$$\sigma(xy) = \sigma(x)\sigma(y), \forall x, y \in \mathbb{F}_{q^m}$$
$$\sigma(a) = a, \forall a \in \mathbb{F}_q$$

On connait déja un élément de $Gal(\mathbb{F}_{q^m}, \mathbb{F}_q)$. Il s'agit de l'automorphisme de *Frobenius*

$$\begin{array}{rccc} \sigma & : & \mathbb{F}_{q^m} & \longrightarrow & \mathbb{F}_{q^m} \\ & & x & \longmapsto & x^q \end{array}$$

et on remarque que $\sigma_j(x) = x^{q^j}$ est un élément de $Gal(\mathbb{F}_{q^m}, \mathbb{F}_q)$ pour tout entier naturel j.

Proposition 1.6 *Les automorphismes de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$ sont exactement les applications $\sigma_0, \sigma_1, ..., \sigma_{m-1}$ définies par $\sigma_j(x) = x^{q^j}, x \in \mathbb{F}_{q^m}$ et $0 \leq j \leq m-1$*

Preuve : On sait déja que $\forall x, y \in \mathbb{F}_{q^m}$

$$\sigma_j(x+y) = \sigma_j(x) + \sigma_j(y)$$
$$\sigma_j(xy) = \sigma_j(x)\sigma_j(y),$$

donc σ_j est un endomorphisme de $\mathbb{F}_{q^m}$.
De plus $\sigma_j(x) = 0$ ssi $x = 0$ ce qui implique que σ_j est injective.
D'après la Proposition 1.2, $\sigma_j(a) = a^{q^j} = a$ et donc σ_j est un automorphisme de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$. Les applications $\sigma_j, (0 \leq j \leq m-1)$ sont distinctes deux à deux car elles transforment un élément primitif α de $\mathbb{F}_{q^m}$ à des éléments α^{q^j} distincts.
On suppose maintenant que σ est un automorphisme arbitraire de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$, α un élément primitif de $\mathbb{F}_{q^m}$ et $f(x) = x^m + a_{m-1}x^{m-1} + ... + a_0 \in \mathbb{F}_q[x]$ le polynôme minimal de α sur $\mathbb{F}_q$. Alors

$$\begin{aligned}\sigma(f(\alpha)) &= \sigma(\alpha^m + a_{m-1}\alpha^{m-1} + ... + a_0) \\ &= \sigma(\alpha^m) + a_{m-1}\sigma(\alpha^{m-1}) + ... + a_1\sigma(\alpha) + a_0 \\ &= \sigma(\alpha)^m + a_{m-1}\sigma(\alpha)^{m-1} + ... + a_1\sigma(\alpha) + a_0 = 0\end{aligned}$$

Ceci montre que $\sigma(\alpha)$ est une racine de f dans $\mathbb{F}_{q^m}$. Comme les racines de f sont les conjugués $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ de α, donc $\sigma(\alpha) = \alpha^{q^j}$ pour un certain $j \in \{0, 1, ..., m-1\}$.□

On remarque ainsi que les conjugués d'un élément primitif $\alpha \in \mathbb{F}_{q^m}$ sont obtenus en appliquant toutes les applications (automorphisme de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$) $\sigma_j, 0 \leq j \leq m-1$ à α. L'ensemble des automorphismes de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$ muni de la loi de composition forme un groupe cyclique isomorphe à $\mathbb{Z}/m\mathbb{Z}$ engendré par σ_1. C'est bien le groupe de *Galois* $Gal(F_{q^m}/\mathbb{F}_q) = \{Id, \sigma, \sigma_2, ..., \sigma_{m-1}\}$

1.6 Traces, Normes et Bases

On présente ici quelques théorèmes concernant la trace et la norme d'un élément $\alpha \in \mathbb{F}_{q^m}$, qui restent valables pour toute extension finie $\mathbb{F}_{q^m}$ d'un corps $\mathbb{F}_q$. On considère ainsi $\mathbb{F}_{q^m}$ en tant que $\mathbb{F}_q$-espace vectoriel de dimension m, admettant $\{\alpha_1, \alpha_2, ..., \alpha_m\}$ comme base. Alors tout élément $\alpha \in \mathbb{F}_{q^m}$ peut être écrit d'une façon unique

$$\alpha = c_1\alpha_1 + ... + c_m\alpha_m, \quad c_i \in \mathbb{F}_q, 1 \leq i \leq m$$

Définition 1.4 *Soit $\alpha \in \mathbb{F}_{q^m}$. Alors*

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + ... + \alpha^{q^{m-1}} \in \mathbb{F}_q$$

Les propriétés du Théorème 1.4 se démontrent par un simple raisonnement, en utilisant le fait que $\mathbb{F}_q$ est de caractéristique p premier et le Lemme 1.2.

Théorème 1.4 *Soit la fonction $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$, alors les propriétés suivantes sont satisfaites*

- $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha+\beta) = Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) + Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta), \quad \forall \alpha, \beta \in \mathbb{F}_{q^m}$
- $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c\alpha) = cTr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha), \quad \forall c \in \mathbb{F}_q, \alpha \in \mathbb{F}_{q^m}$
- *La fonction trace $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ est une forme linéaire de $\mathbb{F}_{q^m}$ dans $\mathbb{F}_q$*
- $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a) = ma, \quad \forall a \in \mathbb{F}_q$;
- $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^q) = Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha), \quad \forall \alpha \in \mathbb{F}_{q^m}$

Le résultat suivant donne une déscription de toutes les formes linéaires existant de $\mathbb{F}_{q^m}$ dans $\mathbb{F}_q$ en fonction de la trace.

Théorème 1.5 *Soit $\mathbb{F}_{q^m}$ une extension finie du corps $\mathbb{F}_q$, alors les formes linéaires de $\mathbb{F}_{q^m}$ dans $\mathbb{F}_q$ sont exactement les applications $\mathrm{L}_\beta, \beta \in \mathbb{F}_{q^m}$ où*

$$\mathrm{L}_\beta(\alpha) = Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta\alpha), \forall \alpha \in \mathbb{F}_{q^m}$$

En particulier si $\beta \neq \gamma$, on a $\mathrm{L}_\beta \neq \mathrm{L}_\gamma$

Preuve : D'après la propriété 3 du Théorème 1.4 L_β est bien une forme linéaire de $\mathbb{F}_{q^m}$ dans $\mathbb{F}_q$. Il reste à démontrer que $L_\beta \neq L_\gamma$ pour tous α, β, γ de $\mathbb{F}_{q^m}$ avec $\alpha \neq 0$ et $\beta \neq \gamma$.

$$\begin{aligned} L_\beta(\alpha) - L_\gamma(\alpha) &= Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta\alpha) - Tr(\gamma\alpha) \\ &= Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}((\beta-\gamma)\alpha) \\ &\neq 0, \text{puisque } \alpha \text{ est supposé non nul} \end{aligned}$$

Et comme $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\mathbb{F}_{q^m}) = \mathbb{F}_q$ alors $L_\beta \neq L_\gamma$.
On constate qu'il y a q^m formes linéaires de $\mathbb{F}_{q^m}$ dans $\mathbb{F}_q$.

Théorème 1.6 *Soit $\mathbb{F}_{q^m}$ une extension finie du corps $\mathbb{F}_q$, alors pour $\alpha \in \mathbb{F}_{q^m}$, $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = 0$ si et seulement si $\alpha = \beta^q - \beta$ pour un certain $\beta \in \mathbb{F}_{q^m}$*

Preuve : Supposons $\alpha \in \mathbb{F}_{q^m}$ avec $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = 0$. Et β une racine du polynôme $x^q - x - \alpha$ dans un corps d'extension de $\mathbb{F}_{q^m}$ alors $\beta^q - \beta = \alpha$ et

$$\begin{aligned} Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) &= \alpha + \alpha^q + ... + \alpha^{q^{m-1}} \\ &= (\beta^q - \beta) + (\beta^q - \beta)^q + ... + (\beta^q - \beta)^{q^{m-1}} \\ &= (\beta^q - \beta) + (\beta^{q^2} - \beta^q) + ... + (\beta^{q^m} - \beta^{q^{m-1}}) \\ &= \beta^{q^m} - \beta = 0 \quad \Longrightarrow \quad \beta \in \mathbb{F}_{q^m}.\square \end{aligned}$$

Définissons maintenant la norme d'un élément $\alpha \in \mathbb{F}_{q^m}$

Définition 1.5 *Soit $\alpha \in \mathbb{F}_{q^m}$. Alors*

$$N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \alpha\alpha^q....\alpha^{q^{m-1}} = \alpha^{\frac{q^m-1}{q-1}} \ \in \mathbb{F}_q$$

Les propriétés de cette fonction sont citées dans le Théorème 1.7

Théorème 1.7 *La fonction norme $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ satisfait les propriétés suivantes :*

- $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha\beta) = N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta), \quad \forall\alpha, \beta \in \mathbb{F}_{q^m}$
- $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ *est une fonction surjective de $\mathbb{F}_{q^m}$ dans $\mathbb{F}_q$, et de $\mathbb{F}_{q^m}^*$ dans $\mathbb{F}_q^*$*
- $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a) = a^m, \quad \forall a \in \mathbb{F}_q$
- $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^q) = N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha), \quad \forall\alpha \in \mathbb{F}_{q^m}$

Si l'on se donne $\{\alpha_1, \alpha_2, ..., \alpha_m\}$ une $\mathbb{F}_q-$ base de $\mathbb{F}_{q^m}$, un élément $\alpha \in \mathbb{F}_{q^m}$ peut être représenté par ses coordonnées $c_j(\alpha) \in \mathbb{F}_q$ par $\alpha = c_1(\alpha)\alpha_1 + c_2(\alpha)\alpha_2 + ... + c_m(\alpha)\alpha_m$. Nous avons donc un large choix pour la représentation du corps $\mathbb{F}_{q^m}$, chaque $\mathbb{F}_q-$ base induit une représentation possible du corps.

En effet, c_j est une forme linéaire de $\mathbb{F}_{q^m}$ dans $\mathbb{F}_q$ et selon le Théorème 1.5, $\exists\ \beta_j \in \mathbb{F}_{q^m}$ tel que $c_j(\alpha) = Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta_j\alpha),\ \forall\alpha \in \mathbb{F}_{q^m}$ et si $\alpha = \alpha_i,\ 1 \leq i \leq m$

$$c_j(\alpha_i) = Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta_j\alpha_i) = \begin{cases} 0 & \text{si } \ i \neq j \\ 1 & \text{si } \ i = j \end{cases} \tag{1.4}$$

et $\{\beta_1, \beta_2, ..., \beta_m\}$ devient une base de $\mathbb{F}_{q^m}$.

En effet, si $d_1\beta_1 + d_2\beta_2 + ... + d_m\beta_m = 0, \quad d_i \in \mathbb{F}_q, \quad 1 \leq i \leq m$, alors en multipliant par un fixe α_i, et en appliquant la fonction $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}$, on peut montrer que $d_i = 0$ pour $i = 1, .., m$.

Une base $\{\beta_1, \beta_2, ..., \beta_m\}$ qui satisfait la relation (1.4) est appelée base duale, elle est unique, puisque les coefficients $c_j(\alpha),\ 0 \leq j \leq m$ sont donnés par

$$c_j(\alpha) = Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta_j\alpha),\ \forall\alpha \in \mathbb{F}_{q^m}$$

Et selon le Théorème 1.5, les éléments $\beta_j,\ 0 \leq j \leq m$ sont déterminés de façon unique par les formes linéaires $c_j,\ 0 \leq j \leq m$.

De ce qui précède, on peut distinguer deux type de base d'une importance particulière. La première est la base polynomiale $\{1, \alpha, \alpha^2, .., \alpha^{m-1}\}$, où α est un élément primitif de $\mathbb{F}_{q^m}$. Et la deuxième est la base normale de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$, $\{\alpha, \alpha^q, ..., \alpha^{q^{m-1}}\}$, cette dernière comporte l'élément $\alpha \in \mathbb{F}_{q^m}$ et ses conjugués.

Exemple 1.5 *Soit $\alpha \in \mathbb{F}_8$ une racine du polynôme irréductible $x^3 + x^2 + 1$ dans $\mathbb{F}_2[x]$, alors la base normale du corps $\mathbb{F}_8$ est $\{\alpha, \alpha^2, 1 + \alpha + \alpha^2\}$ puisque $\alpha^4 = 1 + \alpha + \alpha^2$.*

Chapitre 2

Polynômes de permutation

Les polynômes de permutation ont une importance considérable en raison de leurs liens avec la cryptographie moderne utilisée dans la transmission et le stockage securisé des données. Nous allons l'illustrer avec un exemple simplifié. Soit $\mathbf{M}$ un message qu'un expéditeur veut envoyer à son destinataire en toute sécurité, où $\mathbf{M}$ est un élément de $\mathbb{F}_q$. Si $P(x)$ est un polynôme de permutation de $\mathbb{F}_q$, le message transmis est un élément du corps fini $\mathbf{M}_c = P(\mathbf{M})$, et comme P est une permutation de $\mathbb{F}_q$, $P(x)$ est une bijection. Ce qui veut dire que le destinataire peut obtenir le message original $\mathbf{M}$ en calculant $P^{-1}(\mathbf{M}_c) = P^{-1}(P(\mathbf{M})) = \mathbf{M}$. Afin d'éviter les attaques malveillantes, la permutation doit posséder plusieurs propriétés supplémentaires.

Dans ce chapitre, nous allons présenter des résultats importants sur les polynômes de permutation, et expliquer leur détermination. Nous allons également étudier diverses classifications de ces polynômes, ainsi que les conditions pour qu'un polynôme arbitraire soit une permutation.

2.1 Permutations

Définition 2.1 *Soit X un ensemble fini, de cardinal n, $n \in \mathbb{N}^*$. On appelle permutation de X toute bijection de X dans lui même.*

On note S_n l'ensemble de toutes les permutations de X, et comme le nombre de permutations de n éléments est $n!$, nous avons alors $\mid S_n \mid = n!$.
Si $X = \{1, 2, ..., n\}$, un élément $\sigma \in S_n$ se note généralement sous la forme

$$\sigma = \begin{pmatrix} 1 & 2 & . & . & . & n \\ \sigma(1) & \sigma(2) & . & . & . & \sigma(n) \end{pmatrix}$$

L'ensemble S_n des permutations de X est un groupe pour la loi de composition interne $\circ$, appelé groupe symétrique de X.

2.2 Polynômes de permutation

Un polynôme $f \in \mathbb{F}_q[x]$ est dit polynôme de permutation de $\mathbb{F}_q$ si la fonction associée

$$\begin{cases} f & : & \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ & & x & \longmapsto & f(x) \end{cases}$$

est une permutation c'est-à-dire bijective. Il est clair que si f est un polynôme de permutation alors l'équation $f(x) = a$ admet une solution unique dans $\mathbb{F}_q, \forall a \in \mathbb{F}_q$.

Exemple 2.1 *Les polynômes de permutation de degré au plus* 3 *et vérifiant* $p(0) = 0$ *du corps* $\mathbb{F}_5$ *sont :*
$x,\ x^3,\ 2x + x^2 + x^3,\ 3x + 2x^2 + x^3,\ 3x + 3x^2 + x^3$ *et finalement* $2x + 4x^2 + x^3$

Si ϕ est une fonction arbitraire de $\mathbb{F}_q$ dans $\mathbb{F}_q$ alors il existe un polynôme unique $f(x) \in \mathbb{F}_q[x]$ de degré $\leq q - 1$ tel que $f(x) = \phi(x), \forall x \in \mathbb{F}_q$ et

$$f(x) = \sum_{d \in F_q} \phi(d)(1 - (x - d)^{q-1})$$

Le polynôme $f(x)$ peut être identifié avec le polynôme d'interpolation de *Lagrange* pour la fonction donnée ϕ, en effet

$$f(x) = \sum_{d\in\mathbb{F}_q} \phi(d)\frac{\prod_{c\in\mathbb{F}_q, c\neq d}(x-c)}{\prod_{c\neq d}(d-c)}$$

$$\text{or } \prod_{c\neq d}(d-c) = (d-c_1).(d-c_2)...(d-c_{q-1}) = -1$$

$$\begin{aligned}\prod_{c\in\mathbb{F}_q, c\neq d}(x-c) &= \frac{\prod_{c\in\mathbb{F}_q}(x-c)}{x-d}\\ &= \frac{x^q - x}{x-d}\\ &= \frac{x^q - d^q - (x-d)}{x-d}\\ &= \frac{(x-d)^q - (x-d)}{x-d}\\ &= (x-d)^{q-1} - 1\end{aligned}$$

d'où la relation.

Et si ϕ est déja un polynôme de $\mathbb{F}_q[x]$, alors $\phi(x)$ définit la même fonction que $r(x)$, où $r(x)$ est le reste de la division euclidienne de $\phi(x)$ par le polynôme $x^q - x$ i.e

$$\phi(x) \equiv r(x) \mod (x^q - x)$$

On constate que les polynômes identiquement nuls sur $\mathbb{F}_q$, sont les multiples du polynôme $x^q - x$.

Exemples 2.1

1. *Soient* $f(x),\ g(x)\ \in \mathbb{F}_q[x]$, *alors l'application composée* $f(g(x))$ *est un polynôme de permutation si et seulement si* f *et* g *sont des polynômes de permutation.*
2. *Tout polynôme linéaire sur* $\mathbb{F}_q$ *est de permutation.*
3. *Le polynôme* $f(x) = a\ x^n,\ a \neq 0$ *est de permutation si et seulement si* n *et* $q-1$ *sont relativement premiers.*
4. *Le polynôme* $f(x) = \sum_{i=0}^{r} a_i x^{p^i} \in \mathbb{F}_q[x]$ *est de permutation si et seulement si* $f(0) = 0$.

5. *Le polynôme* $f(x) = ax^i + bx^j + c,\ a \neq 0, i > j \geq 1,$ *et* $pgcd(i-j, q-1) = 1$ *est de permutation si et seulement si* ($b = 0$ *et* $pgcd(i, q-1) = 1$)

Preuves :

1. $f \circ g$ est bijective implique que g est injective sur le domaine fini $\mathbb{F}_q$ et f est surjective sur $\mathbb{F}_q$ alors f et g sont bijectives.

2. Trivial, l'application f est clairement bijective.

3. Supposons que$f(x) = f(y)$ et $y \neq 0$ alors $x^n = y^n \Longrightarrow (\frac{x}{y})^n = 1$ alors l'ordre de l'élément $\frac{x}{y}$ dans le groupe multiplicatif cyclique $\mathbb{F}_q^*$ divise n, et il divise $q-1$ puisque le cardinal de $\mathbb{F}_q^*$ est égal à $q-1$, alors il divise ainsi $pgcd(n, q-1)$ ceci implique que

$$| < \frac{x}{y} > | = 1$$

Supposons maintenant que $pgcd(n, q-1) = d > 1$ alors $n = dn'$ avec d divisant $q-1$ Soit $\alpha \in \mathbb{F}_q^*$ un élément d'ordre d alors

$$\alpha^d = 1^d = 1 \Longrightarrow \alpha^{dn'} = 1^{dn'} \Longrightarrow \alpha^n = 1^n$$

ainsi $a\alpha^n = a1^n$ cela veut dire que f n'est pas surjective.

4. Le polynôme $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ est $\mathbb{F}_p-$ linéaire,

$$f(x+y) = f(x) + f(y)$$
$$\text{et } f(ax) = af(x),\ a \in \mathbb{F}_p$$

ainsi on obtient l'équivalence puisque le noyau de f est nul.

5. Supposons que $f(x) = ax^i + bx^j + c$ est un polynôme de permutation avec $a \neq 0, i > j \geq 1$, et $pgcd(i-j, q-1) = 1$ alors $x^i + \frac{b}{a}x^j + \frac{c}{a}$ est un polynôme de permutation, impliquant que $x^i - \alpha x^j = x^j(x^{i-j} - \alpha)$ avec $\alpha = -\frac{b}{a}$ est un polynôme de permutation. On suppose maintenant que $b \neq 0$ i.e $\alpha \neq 0$ et $pgcd(i-j, q-1) = 1$ alors il existe d'après le théorème de *Bezout* $u, v\ \in \mathbb{Z}$ tels que $u(i-j) + v(q-1) = 1$ alors

$$\alpha^1 = (\alpha^u)^{i-j}.\alpha^{v(q-1)} = (\alpha^u)^{i-j} = \beta^{i-j}$$

$f(\beta) = 0$ alors que $\beta \neq 0,\ \beta = \alpha^u$ contradiction.

L'implication inverse est un cas particuler du troisième point.

2.3 Critères simples

Afin de pouvoir étudier ces polynômes, il est important de disposer de moyens théoriques aussi bien qu'algorithmiques pour tester si un polynôme est de permutation. On expose au préalable des critères simples bien qu'inefficaces du point de vue algorithmique permettant d'obtenir de nombreux résultats théoriques.

2.3.1 Critère d'Hermite-Dickson

Le premier critère est celui d'*Hermite-Dickson* qui est très utilisé pour prouver que des familles de polynômes sont des permutations. L'application directe de ce test est de complexité [1] $O(q^2)$, ce qui est beaucoup trés élevé en pratique.
Soit $f(x) \in \mathbb{F}_q[x]$. On note $\overline{(f(x))^k}$ l'unique polynôme de $\mathbb{F}_q[x]$ tel que $(f(x))^k \equiv \overline{(f(x))^k} \mod (x^q - x)$ et $deg(\overline{(f(x))^k}) \leq q-1$. Autrement dit, $\overline{(f(x))^k}$ est le reste de la division euclidienne du polynôme $(f(x))^k$ par $x^q - x$ dans $\mathbb{F}_q[x]$.

Théorème 2.1 *Soient $\mathbb{F}_q$ un corps de caractéristique p et $f(x) \in \mathbb{F}_q[x]$, alors f est un polynôme de permutation si et seulement si les conditions suivantes sont vérifiées*
(i) *$f(x) = 0$ admet une racine unique dans $\mathbb{F}_q$*
(ii) *Pour tout k compris entre 1 et $q-2$ tel que $k \neq 0 \pmod p$, $\overline{(f(x))^k} \mod (x^q - x)$ est de degré inférieur ou égal à $q-2$*

La démonstration du théorème d'*Hermite-Dickson* repose sur le lemme suivant

Lemme 2.1 *Soient $a_0, a_1, ..., a_{q-1}$ des éléments du corps $\mathbb{F}_q$, alors les conditions suivantes sont équivalentes*

1. *$a_0, a_1, ..., a_{q-1}$ sont distincts*
2. $$\sum_{i=0}^{q-1} a_i^k = \begin{cases} 0 & pour\ k = 0, 1, ..., q-2, \\ -1 & pour\ k = q-1 \end{cases}$$

1. La complexité mesure la quantité d'opérations nécessaires pour la résolution d'un problème en fonction de la taille des données.

Preuve : Soit i un entier fixe appartenant à l'ensemble $\{0, 1, ..., q-1\}$. Considérons le polynôme

$$g_i(x) = 1 - \sum_{j=0}^{q-1} a_i^{q-1-j} x^j$$

On peut remarquer facilemnt que pour $i \neq s$ on a

$$g_i(x) = \begin{cases} 1 & \text{si } x = a_i, \\ 0 & \text{si } x = a_s \end{cases}$$

En effet, $g_i(a_i) = 1 - \sum_{j=0}^{q-1} a_i^{q-1} = 1 - q a_i^{q-1} = 1$ car p est la caractéristique de $\mathbb{F}_q$ et q est une puissance de p. Et

$$\begin{aligned} g_i(a_s) &= 1 - \sum_{j=0}^{q-1} a_i^{q-1-j} a_s^j \\ &= 1 - [1 + \frac{a_s}{a_i} + (\frac{a_s}{a_i})^2 + ... + (\frac{a_s}{a_i})^{q-1}] \\ &= 0 \end{aligned}$$

Soit le polynôme

$$\begin{aligned} g(x) &= \sum_{i=0}^{q-1} g_i(x) \\ &= -\sum_{j=0}^{q-1} (\sum_{i=0}^{q-1} a_i^{q-1-j}) x^j \\ &= g_0(x) + g_1(x) + ... + g_{q-1}(x) \end{aligned}$$

$g(x) = 1$ si et seulement si $x \in \mathbb{F}_q = \{a_0, a_1, ..., a_{q-1}\}$. Et comme g est de degré inférieur ou égal à $q-1$, alors $g(x) = 1$ sur $\mathbb{F}_q$ si et seulement si g est congru à 1. Ainsi on peut écrire

$$g(x) = -\sum_{i=0}^{q-1} a_i^{q-1} - \sum_{i=0}^{q-1} a_i^{q-2} x - \sum_{i=0}^{q-1} a_i^{q-3} x^2 - ... - \sum_{i=0}^{q-1} a_i^0 x^{q-1} = 1$$

ce qui implique que

$$\sum_{i=0}^{q-1} a_i^k = \begin{cases} 0 & \text{pour } k = 0, 1, ..., q-2, \\ -1 & \text{pour } k = q-1 \end{cases}$$

Démonstration du théorème d'*Hermite-Dickson* :

Supposons que f est un polynôme de permutation de $\mathbb{F}_q$, alors il est clair que $f(x) = 0$ admet une racine unique puisque f est bijective, et la réduction du polynôme $f(x)^k$ modulo $x^q - x$ est un polynôme de degré inférieur à q de la forme $\sum_{j=0}^{q-1} b_j^{(k)} x^j$, où $b_{q-1}^k = -\sum_{i=0}^{q-1} f(a_i)^k$ (par le polynôme de *Lagrange*), et selon le Lemme 2.1, on a $b_{q-1}^k = 0$, pour $k = 1, 2, ..., q-2$ ainsi $\overline{f(x)^k} \mod (x^q - x)$ est de degré inférieur ou égal à $q-2$.

Réciproquement, supposons les deux conditions sont vérifiées. Alors on a d'après le *(i)* $\sum_{i=0}^{q-1} f(a_i)^{q-1} = -1$ et d'après *(ii)* $\sum_{i=0}^{q-1} f(a_i)^k = 0$, $1 \leq k \leq q-2$, $t \neq 0 \pmod p$.

Comme $\mathbb{F}_q$ est fini de caractéristique p, alors on peut utiliser la formule

$$\sum_{i=0}^{q-1} f(a_i)^{kp^j} = (\sum_{i=0}^{q-1} f(a_i)^k)^{p^j},$$

on obtient

$$\sum_{i=0}^{q-1} f(a_i)^k = 0 \text{ pour } 0 \leq k \leq q-2.$$

Ainsi les $f(a_i)$, $i = 0, 1, ..., q-2$ sont tous distincts, ce qui implique d'après le Lemme 2.1 que f est un polynôme de permutation.□

Nous proposons dans ce qui suit un exemple d'application du critère d'*Hermite-Dickson* ;

Corollaire 2.1 *Si d est un diviseur de $q-1$, alors il n'existe pas de polynôme de permutation de $\mathbb{F}_q$ de degré d.*

En effet, Si $f \in \mathbb{F}_q[x]$ sachant que $\deg f = d$ et que $d/q-1$ alors $\deg(f^{\frac{q-1}{d}}) = q-1$ pour $1 \leq k = \frac{q-1}{d} \leq q-2$, ainsi la condition (ii) du théorème d'*Hermite-Dickson* n'est pas satisfaite pour $k = \frac{q-1}{d}$.

2.3.2 Critère de Lutz-Carlitz

Lutz-Carlitz présentaient une nouvelle forme du théorème d'*Hermite-Dickson* et montraient le théorème suivant

Théorème 2.2 *Soit $f(x)$ un polynôme à coefficients dans $\mathbb{F}_q$. Supposons que*
(i) $(f(x))^k \mod (x^q - x)$, $1 \leq k \leq q-2$ *est de degré inférieur ou égal à* $q-2$, *et*
(ii) $(f(x))^{q-1} \mod (x^q - x)$ *est de degré* $q-1$
alors $f(x)$ est un polynôme de permutation.

Dans cette thèse, nous utilisons une méthode différente pour démontrer le théorème de *Lutz-Carlitz*. En fait, nous étendons ce dernier et nous prouvons le suivant

Théorème 2.3 *Soient $\mathbb{F}_q$ un corps de caractéristique p et $f(x)$ un polynôme de $\mathbb{F}_q[x]$, alors les conditions suivantes sont équivalentes*
(i) *f est un polynôme de permutation*
(ii) $(f(x))^k \mod (x^q - x)$, $1 \leq k \leq q-2$ *est de degré inférieur ou égal à* $q-2$, *et* $(f(x))^{q-1} \mod (x^q - x)$ *est de degré* $q-1$
(iii) *identique à* ***(ii)*** *en ajoutant la condition* $k \neq 0 \pmod p$

Avant toute chose, nous fixons quelques notations et faits qui feront objet de la démonstration.
Fixons un corps K, un polynôme en $x_1, x_2, ..., x_n$ à coefficients dans K est une somme

$$P(x_1, ..., x_n) = \sum a_{i_1,...,i_n} x_1^{i_1} x_2^{i_2} ... x_n^{i_n}, \quad i_1, ..., i_n \in \mathbb{N}$$

avec $a_{i_1,...,i_n} \in K$ et tous sauf un nombre fini des $a_{i_1,...,i_n}$ égaux à 0. L'ensemble des polynômes en $x_1, x_2, ..., x_n$ à coefficients dans K forme un anneau commutatif noté $K[x_1, x_2, ..., x_n]$. Les produits $a_{i_1,...,i_n} x_1^{i_1} x_2^{i_2} ... x_n^{i_n}$ avec $a_{i_1,...,i_n} \neq 0$ sont des termes de degré $i_1 + ... + i_n$ et le degré de P est le maximum des degrés des termes de P.
La démonstration du Théorème 2.3 repose sur les 3 faits suivants :
Fait 1 : Soient $K[x_1, x_2, ..., x_n]$ un anneau commutatif sur le corps K et k un entier positif compris entre 1 et n.
Le $k-$ième polynôme élémentaire symétrique en n variables est

$$s_k(x_1, x_2, ..., x_n) = \sum x_{i_1} x_{i_2} ... x_{i_k}, \quad 1 \leq i_1 < ... < i_k \leq n$$

Le $k-$ième polynôme symétrique homogène est

$$\sigma_k(x_1, x_2, ..., x_n) = \ x_1^k + x_2^k + ... + x_n^k$$

Et les formules de *Newton* en fonction des polynômes s_k et σ_k sont données par

$$\sigma_k - s_1\sigma_{k-1} + ... + (-1)^k k s_k = 0 \text{ pour } 1 \leq k \leq n-1$$
$$\text{et } \sigma_k - s_1\sigma_{k-1} + ... + (-1)^{n-1}\sigma_{k-(n-1)} = 0 \text{ pour } k \geq 1$$

Fait 2 : Soit $\mathbb{F}_q = \{c_1, c_2, ..., c_q\}$, alors $f(x)$ est un polynôme de permutation si et seulement si

$$x^q - x = \prod_{c\in\mathbb{F}_q}(x - f(c)) = \prod_{c\in\mathbb{F}_q}(x - c)$$
et
$$s_k(f(c_1), ..., f(c_q)) = \begin{cases} 0 & \text{pour } k = 1, ..., q-2, \\ -1 & \text{pour } k = q-1, \\ 0 & \text{pour } k = q \end{cases}$$

Fait 3 : Soit σ une application de $\mathbb{F}_q$ dans lui même, alors il existe un polynôme unique $g(x) \in \mathbb{F}_q[x]$ de degré strictement inférieur à q tel que $g(x) = \sigma(x),\ \forall x \in \mathbb{F}_q$ et $g(x) = \sum_{c\in\mathbb{F}_q} \sigma(c)(1-(x-c)^{q-1})$ et

$$\begin{aligned} \deg g(x) \leq q-2 &\Longleftrightarrow \sum_{c\in\mathbb{F}_q} \sigma(c) = 0 \\ &\Longleftrightarrow \sum_{c\in\mathbb{F}_q} g(c) = 0 \end{aligned}$$

Démonstration du théorème de *Lutz-Carlitz* :

(i)$\Longrightarrow$ (ii) On suppose que f est un polynôme de permutation alors d'après le fait 2, on a pour k compris entre 1 et $q-2$, le $k-$ième polynôme symétrique élémentaire,

$$s_k(f(c_1), ..., f(c_q)) = 0,$$

ceci conduit d'après la formule de *Newton* à

$$\sigma_k(f(c_1), ..., f(c_q)) = f^k(c_1) + f^k(c_2) + ... + f^k(c_q) = 0.$$

Or le fait 3 implique que la réduction de $(f(x))^k \mathrm{mod}(x^q - x)$ est de degré inférieur ou égal à $q-2$ si et seulement si $\sum_{c\in\mathbb{F}_q} f^k(c) = 0$.
Pour $k = q-1$, le polynôme symétrique élémentaire de degré $q-1$,

$$s_{q-1}(f(c_1), ..., f(c_q)) = -1$$

et la formule de *Newton* donnent

$$\sigma_{q-1}(f(c_1), ..., f(c_q)) = q - 1 \neq 0$$

ainsi

$$\sum_{c\in\mathbb{F}_q} f^{q-1}(c) = q - 1$$

ceci implique que $\deg f^{q-1}(x)$ est supérieur à $q-2$, et par réduction modulo $x^q - x$ on obtient un polynôme de degré $q-1$.
(ii)$\Longrightarrow$(iii)évidente.
(iii)$\Longrightarrow$(i) Supposons que

- $pgcd(k, p) = 1$ pour $1 \leq k \leq q-2$
- $deg(f^k(x)) \leq q-1$ pour $(1 \leq k \leq q-2)$ et
- $deg(f^{q-1}(x)) = q-1$

Alors d'après le fait 3, on a

- $\sum_{c\in\mathbb{F}_q} f^k(c) = 0$ pour $1 \leq k \leq q-2$
- $\sum_{c\in F_q} f^{q-1}(c) = a \neq 0$ i.e $\sigma_k(f(c_1), ..., f(c_q)) = 0$ pour $1 \leq k \leq q-2$ et
- $\sigma_{q-1}(f(c_1), ..., f(c_q)) = a \neq 0$

Ainsi on peut montrer en raisonnant par récurrence que

$$s_k(f(c_1), ..., f(c_q)) = 0 \text{ pour } (1 \leq k \leq q-2)$$

$$\text{et } s_{q-1}(f(c_1), ..., f(c_q)) \neq 0$$

Il reste à montrer que le polynôme $h(x) = \prod_{c\in F_q}(x - f(c))$ est séparable sachant que le $pgcd(k, p) = 1$.
En effet $h(x) = x^q + \sum_{p/i} a_i x^i + bx + c$, $b \neq 0$ alors $h'(x) = b \neq 0$ c'est à dire que toutes

les racines de h sont distinctes.
Ainsi h est séparable ce qui veut dire d'après le fait 2 que f est un polynôme de permutation.□

2.3.3 Calculer les images

L'algorithme le plus simple consiste à calculer les images d'un polynôme donné $P \in \mathbb{F}_q[x]$, et voir si elles sont distinctes. Le nombre d'opérations qui doivent être effectuées augmente selon la croissance du degré du polynôme P ainsi que l'ordre q du corps en question. Ce test nous permet de s'arrêter à la première image rencontrée deux fois, sinon on continue jusqu'à la dernière image du polynôme P.

Autrement, on peut dire que $P \in \mathbb{F}_q[x]$ est un polynôme de permutation si et seulement si la propriété suivante $\prod_{c\in\mathbb{F}_q}(x - P(c)) = x^q - x$ est vérifiée.

Pour un polynôme de degré n, ce test nécessite $O(qn)$ opérations puisque une évaluation seule est effectuée en $O(n)$ opérations, plus $O(q)$ pour voir si les valeurs sont distinctes. La complexité moyenne de ce test est de $O(n\sqrt{q})$, puisque il ya possibilité de s'arrêter à la premiere valeur rencontrée deux fois.

2.3.4 Caractères additifs

Un autre résultat sur les polynômes de permutation peut être donné en fonction des caractères additifs définis sur le corps fini $\mathbb{F}_q$.

Soit alors G un groupe abélien multiplicatif fini, de cardinal $|G|$. On appelle caractère χ du groupe G, un morphisme de G dans le groupe multiplicatif des racines complexes de l'unité, noté U avec

$$\chi(g_1g_2) = \chi(g_1)\chi(g_2), \quad \forall\ g_1, g_2 \in G$$

$$\chi(1_G) = 1 \text{ en particulier } \chi(g)^{|G|} = \chi(g^{|G|}) = 1$$

On note aussi $\chi(g)\chi(g^{-1}) = \chi(gg^{-1}) = \chi(1_G) = 1$ alors $\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$, $\forall g \in G$ où $\overline{\chi(g)}$ désigne le conjugué complexe de $\chi(g)$ dans U.

Pour tout groupe G, on a un caractère trivial $\chi_0 : g \to 1$. Tout les autres caractères sur G sont non-triviaux. Etant donnés deux caractères de G, notés χ et $\chi^{'}$, on en déduit un autre caractère, noté $\chi.\chi^{'}$ (ou simplement $\chi\chi^{'}$), défini par la formule $\chi\chi^{'}(g) = \chi(g)\chi^{'}(g)$. Si χ est un caractère, alors $\frac{1}{\chi(g)} = \overline{\chi(g)} = \overline{\chi}(g),\ \forall g \in G$, et $\overline{\chi}$ est clairement un caractère, donc tout caractère de G admet un inverse multiplicatif dans $\widehat{G}$ (l'ensemble de caractères de G), alors $(\widehat{G}, .)$ est un groupe fini d'élément neutre χ_0.

Dans un corps fini $\mathbb{F}_q$ il y a deux groupes abéliens. Le groupe additif et le groupe multiplicatif. Etablissons la différence entre les caractères associés à ces deux structures de groupe.

Considérons en premier le groupe additif $\mathbb{F}_q$. Soit alors p la caractéristique de $\mathbb{F}_q$, le corps premier associé à $\mathbb{F}_q$ est bien le corps $\mathbb{F}_p$.

Soit $Tr : \mathbb{F}_q \to \mathbb{F}_p$ la fonction trace. La fonction χ_1 définie par

$$\chi_1(c) = e^{2\pi i Tr(c)/p},\ \forall c \in \mathbb{F}_q$$

est un caractère du groupe additif $\mathbb{F}_q$. En effet d'après les propriétés de la fonction trace, nous avons

$$Tr(c_1 + c_2) = Tr(c_1) + tr(c_2),\ \forall c_1, c_2 \in \mathbb{F}_q$$

alors

$$\chi_1(c_1 + c_2) = \chi_1(c_1)\chi_1(c_2).$$

On appelle χ_1 le caractère additif canonique de $\mathbb{F}_q$ et tout les autres caractères additifs χ_b existant sur $\mathbb{F}_q$ peuvent être exprimés en fonction de χ_1 tels que

$$\chi_b(c) = \chi_1(bc),\ \forall b, c \in \mathbb{F}_q.$$

Considérons maintenant le groupe multiplicatif $\mathbb{F}_q^*$. Selon le Théorème 1.1, $\mathbb{F}_q^*$ est un groupe cyclique d'ordre $q-1$. Soit alors g un élément primitif de $\mathbb{F}_q$. Pour tout $j = 0, 1, ..., q-2$, la fonction ψ_j définit par

$$\psi_j(g^k) = e^{2\pi i jk/q-1},\quad k = 0, 1, ..., q-2$$

est un caractère multiplicatif de $\mathbb{F}_q^*$, où ψ_0 représente le caractère trivial i.e

$$\psi_0(c) = 1,\ \forall c \in \mathbb{F}_q^*.$$

ψ_0 représente aussi l'identité du groupe cyclique d'ordre $q-1$ de caractères multiplicatifs de $\mathbb{F}_q^*$ contenant les éléments $\psi_j,\ j = 0, 1, ..., q-2$.

Nous énonçons ainsi un critère qui donne la relation entre les polynômes de permutation de $\mathbb{F}_q[x]$ et les caractères additifs de $\mathbb{F}_q$

Théorème 2.4 *Soit f un polynôme de $\mathbb{F}_q[x]$, alors f est un polynôme de permutation si et seulement si $\sum_{c\in\mathbb{F}_q}\chi(f(c)) = 0$, pour tout caractère additif non-trivial*

Preuve : Supposons que f est un polynôme de permutation de $\mathbb{F}_q$ et χ un caractère additif non-trivial. Alors l'équation $f(x) = a$ admet une solution unique dans $\mathbb{F}_q$, $\forall a \in \mathbb{F}_q$ i.e $\sum_{c\in\mathbb{F}_q}\chi(f(c)) = \sum_{c\in\mathbb{F}_q}\chi(c)$ et comme χ est un caractère non trivial alors il existe $c_0 \in \mathbb{F}_q$ tel que $\chi(c_0) \neq 1$

$$\chi(c_0)\sum_{c\in\mathbb{F}_q}\chi(c) = \sum_{c\in\mathbb{F}_q}\chi(c_0)\chi(c) = \sum_{c\in\mathbb{F}_q}\chi(c_0c) = \sum_{c\in\mathbb{F}_q}\chi(c)$$
$$(\chi(c_0)-1)\sum_{c\in\mathbb{F}_q}\chi(c) = 0 \ \Rightarrow \sum_{c\in\mathbb{F}_q}\chi(c) = 0$$

Inversement, supposons que $\sum_{c\in\mathbb{F}_q}\chi(f(c)) = 0$, $\forall\chi$ caractère additif non trivial. Utilisons l'identité suivante

$$\sum_{b\in\mathbb{F}_q}\chi_b(c)\overline{\chi_b(d)} = \begin{cases} 0 & c \neq d \\ q & c = d \end{cases} \quad c, d \in \mathbb{F}_q \tag{2.1}$$

Sachant que q est l'ordre de $\mathbb{F}_q$.

Posons N le nombre de solutions de l'équation $f(x) = a$ dans $\mathbb{F}_q$ pour $a \in \mathbb{F}_q$. Alors d'après l'identité (2.1)

$$\begin{aligned} N &= \frac{1}{q}\sum_{c\in\mathbb{F}_q}\sum_{\chi}\chi(f(c))\overline{\chi(a)} \\ &= \frac{1}{q}\sum_{\chi}\sum_{c\in\mathbb{F}_q}\chi(f(c))\overline{\chi(a)} \\ &= 1 + \frac{1}{q}\sum_{\chi\neq\chi_0}\overline{\chi(a)}\sum_{c\in\mathbb{F}_q}\chi(f(c)) \\ &= 1 \quad \text{car} \sum_{c\in\mathbb{F}_q}\chi(f(c)) = 0 \end{aligned}$$

ceci implique que le nombre de solutions de l'équation $f(x) = a$ est égal à 1, ainsi f est un polynôme de permutation.

2.4 Groupe de polynômes de permutation

Comme cité précédemment tout polynôme sur $\mathbb{F}_q$ est de degré inférieur à q que l'on peut aussi obtenir par réduction modulo $x^q - x$. De plus, deux polynômes f et g peuvent être combiné par l'opération de composition et par réduction modulo $x^q - x$. Alors il est commode d'écrire $< g(x) >< f(x) >=< h(x) >$ si on a bien $(f \circ g)(x) \equiv h(x) \mathrm{mod}(x^q - x)$.

Sous cette opération de composition de polynômes, l'ensemble des polynômes de permutation sur $\mathbb{F}_q$ forme un groupe isomorphe au groupe des permutations S_q. Ainsi à tout polynôme de permutation de $\mathbb{F}_q$, on peut associer une unique permutation $\sigma \in S_q$.

Une des difficultés provenant de cet isomorphisme et qu'un polynôme trés simple conduit à une permutation complexe et réciproquement.

En effet, toute permutation du groupe S_q peut être représentée par un produit de transpositions, il est alors suffisant de considérer les transpositions qui échangent les éléments 0 et a du corps $\mathbb{F}_q$, qu'on note $\tau_{0,a}$.

On peut constater que $\tau_{0,a}\tau_{0,b}\tau_{0,a} = \tau_{a,b}$ pour toute transposition echangeant (a et b de $\mathbb{F}_q$) de S_q. Alors le polynôme

$$f_a(x) = -a^2[((x-a)^{q-2} + a^{-1})^{q-2} - a]^{q-2}$$

est associé à la transposition $\tau_{0,a}$.

Considérons le corps premier $\mathbb{F}_p$, alors l'unique polynôme de degré inférieur ou égal à $p-1$ dans $\mathbb{F}_p[x]$ qui représente la transposition $\tau_{0,1}$ est $f(x) = x + \prod_{k=2}^{p-1}(x-k)$.

En effet,

$$f(x) - x = \begin{cases} 1 & \text{si } x = 0 \\ -1 & \text{si } x = 1 \\ 0 & \text{si } x \neq 0, 1 \end{cases} \tag{2.2}$$

Donc $f(x) - x = (ax+b)\prod_{k=2}^{p-1}(x-k)$, pour $x = 0$ et 1, on obtient le système d'inconnues a et b suivant

$$\begin{cases} 1 = b(-1)^{p-2}(p-1)! = -b(p-1)! \\ -1 = (a+b)(-1)^{p-1}(p-2)! = -(a+b)(p-2)! \end{cases} \tag{2.3}$$

Or dans $\mathbb{F}_p$, $(p-1)! = -1$ et $(p-2)! = 1$, ainsi $(a,b) = (0,1)$ et donc $f(x) = x + \prod_{k=2}^{p-1}(x-k)$

2.4.1 Générateurs du groupe des polynômes de permutation

Théorème 2.5 *Si $q > 2$ et c est un élément primitif de $\mathbb{F}_q$, alors le groupe des polynômes de permutation S_q est engendré par $cx, x+1$ et x^{q-2}.*

La démonstration de ce théorème provient de la forme générale du polynôme correspondant à la transposition $\tau_{0,a},\ a \in \mathbb{F}_q^*$ et les identités suivantes

$$< ax >=< c^s x >=< cx >^s \text{ et } < ax+b >=< cx >^{s-t} < x+1 >< cx >^t$$

tels que $a, b \in \mathbb{F}_q^*$, $a = c^s$ et $b = c^t$ avec $s > t \geq 1$.
L'intérêt de ces générateurs est la simplicité de leur forme polynomiale.

On trouve également des générateurs du sous groupe de S_q comportant toutes les permutations paires, appelé groupe alterné et noté A_q. Nous appelons ainsi polynôme de permutation sur $\mathbb{F}_q$ paire si la permutation qui lui ait associée est paire.

2.5 Classes de polynômes de permutation

Wan et Lidl ont parlé dans leur article [27] de trois classes majeures de polynômes de permutation.

- polynômes de permutation de *Dickson*.
- polynômes de permutation linéarisés.
- polynômes de permutation de la forme $x^r f(x^{\frac{q-1}{d}})$, où d est un diviseur de $q-1$. Cette classe aborde le troisième chapitre.

Une liste aussi exhaustive que possible des résultats connus suit ci-après

2.5.1 Les polynômes de petit degré

Comme cité précédemment, l'ensemble des polynômes de permutation de $\mathbb{F}_q$ forme un groupe sous l'opération de composition de polynômes i.e si $f_1(x)$ et $f_2(x)$ sont des

polynômes de permutation de $\mathbb{F}_q$, alors le polynôme composé $f_1(f_2(x))$ est aussi un polynôme de permutation de $\mathbb{F}_q$. Ainsi, on peut simplifier la classification en utilisant cette observation et en définissant le polynôme normalisé.

En effet, si $f \in \mathbb{F}_q[x]$ est un polynôme de permutation de $\mathbb{F}_q$, alors $f_1(x) = c\, f(x+b) + d, \quad c \neq 0$ est encore un polynôme de permutation de $\mathbb{F}_q$. En choisissant b, c et d convenablement, on obtient un polynôme de permutation qui satisfait les conditions suivantes ;

Définition 2.2 *Un polynôme $f \in \mathbb{F}_q[x]$ est dit normalisé si*

- *f est unitaire*
- *$f(x) = 0$ admet 0 comme solution unique*
- *Si le degré de f n'est pas divisible par la caractéristique de $\mathbb{F}_q$, alors le coefficient de x^{n-1} est 0*

Lorsque le degré d'un polynôme satisfait certaines conditions, une utilisation directe du critère d'*Hermite-Dickson* permet de trouver des polynômes de permutation normalisés de $\mathbb{F}_q$. Le Tableau 2.1, décrit tous les polynômes normalisés de degré inférieur ou égal à 5.

Il est clair que lorsque le degré des polynômes augmente, une telle classification devient beaucoup plus difficile à établir. L'Exemple 2.2 donne des conditions suffisantes et nécessaires pour que les polynômes de la forme $x^8 + ax^j$ avec $j < 8$ soient des permutations.

Exemple 2.2 *Le polynôme $x^8 + ax^j$ avec $1 \leq j \leq 7$ et $a \neq 0$ est une permutation de $\mathbb{F}_q$ si et seulement si une des conditions suivantes est satisfaite*

1. $j = 1,\ q = 2^{3r}$ *et* $a^{(q-1)/7} \neq 1$;
2. $j = 1,\ q = 29$ *et* $a \in \{-4, 4, -10, 10\}$;
3. $j = 2,\ q = 2^{2r}$ *et* $a^{(q-1)/3} \neq 1$;
4. $j = 3,\ q = 11$ *et* $a \in \{-2, 2, -4, 4\}$;
5. $j = 5,\ q = 4$ *et* $a \in \{-1, 1\}$;
6. $j = 5,\ q = 7$ *et* $a \in \{-3, 3\}$

Polynôme	condition sur les coefficients	Condition sur q
x		
x^2		$q = 0 \mod 2$
x^3		$q \neq 1 \mod 3$
$x^3 - ax$	a non carré	$q = 0 \mod 3$
$x^4 \pm 3x$		$q = 7$
$x^4 + a_1x^2 + a_2x$	0 est une racine unique	$q = 0 \mod 2$
x^5		$q \neq 1 \mod 5$
$x^5 - ax$	$\forall b \in \mathbb{F}_q, b^4 \neq a$	$q \neq 0 \mod 5$
$x^5 + ax$	$a^2 = 2$	$q = 9$
$x^5 \pm 2x$		$q = 7$
$x^5 + ax^3 \pm x^2 + 3a^2x$	a non carré	$q = 7$
$x^5 + ax^3 + 5^{-1}a^2x$		$q = \pm 2 \mod 5$
$x^5 + ax^3 + 3a^2x$	a non carré	$q = 13$
$x^5 - 2ax^3 + a^2x$	a non carré	$q = 0 \mod 5$

TABLE 2.1 – Polynômes de permutation normalisés de degré inférieur à 5

Pour q impair, on peut caractériser les polynômes de permutation de $\mathbb{F}_q$ qui sont de la forme $x^{(q+1)/2} + ax$. Soit alors η un caractère quadratique de $\mathbb{F}_q$ sachant que $\eta(0) = 0$;

Théorème 2.6 *Pour q impair, le polynôme $x^{(q+1)/2} + ax \in \mathbb{F}_q[x]$ est de permutation si et seulement si $\eta(a^2 - 1) = 1$*

Preuve : Soit le polynôme $f(x) = x^{(q+1)/2} + ax$. Nous allons montrer que f n'est pas injectif si et seulement si $\eta(a^2 - 1) \neq 1$
Si $f(c) = f(0) = 0$ pour $c \in \mathbb{F}_q^*$ alors $a = -c^{(q-1)/2}$, ainsi $\eta(a^2 - 1) = 0$
Si $f(b) = f(c) \neq 0$ pour $b,\ c \in \mathbb{F}_q^*, b \neq c$ alors $bc^{-1} = (a + c^{(q-1)/2})(a + b^{(q-1)/2})^{-1}$ et on distingue les deux cas suivants

- Si $\eta(b) = \eta(c)$ alors on aura $b^{(q-1)/2} = c^{(q-1)/2}$ et $b = c$ qui est une contradiction.
- Si $\eta(b) \neq \eta(c)$ alors on peut dire sans perte de généralités que $\eta(b) = -1$ et $\eta(c) = 1$, ce qui implique $b^{(q-1)/2} = -1$ et $c^{(q-1)/2} = 1$, ainsi

$$\begin{aligned} -1 = \eta(bc^{-1}) &= \eta((a+1)(a-1)^{-1}) \\ &= \eta((a+1)(a-1)) = \eta(a^2 - 1) \end{aligned}$$

Inversement, supposons que $\eta(a^2 - 1) \neq 1$, alors soit $a^2 - 1 = 0$ soit $\eta(a^2 - 1) = -1$.
Si $a^2 - 1 = 0$ on a $a = \pm 1$, il existe alors un certain $c \in \mathbb{F}_q^*$ tel que $c^{(q-1)/2} = -a$, où $f(c) = f(0)$. Et si $\eta(a^2 - 1) = -1$, $b = (a+1)(a-1)^{-1}$ alors $\eta(b) = -1$, et $b^{(q-1)/2} = -1$, ainsi

$$\begin{aligned} f(b)(a + b^{(q-1)/2})b &= (a-1)b \\ &= (a+1) = f(1), \text{ avec } b \neq 1 \end{aligned}$$

Remarquons que dans les deux cas f n'est pas injectif, impliquant que f n'est pas un polynôme de permutation.□

2.5.2 Polynômes linéarisés

Un polynôme de la forme $f(x) = \sum_{i=0}^{k} a_i x^{p^i} \in \mathbb{F}_{p^n}[x]$ est de permutation si et seulement s'il admet 0 comme racine unique dans $\mathbb{F}_q$. C'est en fait un polynôme linéarisé

qui correspond à une application linéaire de $\mathbb{F}_q$ dans lui même.

Beaucoup d'exemples peuvent être générés à partir de ce type de polynôme, soit en les composant avec d'autres polynômes de $\mathbb{F}_q$ soit en les additionnant des polynômes de la forme ax de $\mathbb{F}_q$ comme le montre les résultats suivants ;

Théorème 2.7 *Un polynôme de permutation de $\mathbb{F}_q$ est de permutation sur toutes les extensions finies de $\mathbb{F}_q$ si et seulement s'il est de la forme $ax^{p^h} + b$ avec $a \neq 0$ et $h \geq 0$.*

Théorème 2.8 *Si $f \in \mathbb{F}_q[x]$ n'est pas de la forme $ax^{p^h} + b$, il existe une infinité d'extensions finies $\mathbb{F}_{q^r}$ de $\mathbb{F}_q$ telles que f ne soit pas un polynôme de permutation de $\mathbb{F}_{q^r}$.*

Théorème 2.9 *Pour tout polynôme linéarisé $L \in \mathbb{F}_q[x]$, il existe $a \in \mathbb{F}_q$ tel que $L(x) - ax$ soit un polynôme de permutation.*

La vérification pratique du caractère bijectif de ces polynômes est finalement simple puisque il s'agit de résoudre un système linéaire. Les preuves associées à ces résultats se trouvent dans [17].

2.5.3 Polynômes quadratiques

On peut trouver des exemples parmi les classes que nous avons déja rencontrées. En utilisant des résultats élémentaires de divisibilité et le fait que x^n permute $\mathbb{F}_q$ si et seulement si $pgcd(n, q-1) = 1$. Alors le monôme x^{2^k+1} permute $\mathbb{F}_{2^n}$ si et seulement si $\frac{n}{pgcd(n,k)}$ est impair.

Les polynômes purement quadratiques, sont ceux qui n'admettent pas de termes linéaires. Si alors $\mathbb{F}_q$ est un corps de caractéristique différente de 2, tous les exposants sont pairs ainsi tous les polynômes sont pairs i.e $f(x) = f(-x)$. Les seuls polynômes satisfaisant cette propriété sont obtenus dans des corps de caractéristique 2.
Un moyen pour obtenir un polynôme de degré algébrique 2 [2] est de prendre le produit de deux polynômes linéarisés pour obtenir un polynôme dit bilinéaire qui est de la forme

2. On appelle degré algébrique du polynôme $f \in \mathbb{F}_{p^n}[x]$ le poids maximal de l'écriture en base p des degrés de ses monômes.

$f(x) = L_1(x)L_2(x) \mod (x^q - x)$ où $L_1[x],\ L_2[x] \in \mathbb{F}_q[x]$ sont linéarisés.
Si un polynôme f est produit de deux polynômes linéarisés $f(x) = L_1(x)L_2(x)$, en le composant avec l'inverse de L_1 qui existe et qui est linéaire, on obtient la conséquence suivante, $f(x)$ est linéairement équivalent à un polynôme du type $xL_1(x)$.
Mais d'un point de vue applicatif, cela n'est pas satisfaisant puisqu'on reste avec des polynômes linéairement équivalents à des fonctions puissances. Plusieurs exemples de polynômes non équivalents d'une efficacité satisfaisante sont donnés par *Blokhuis* et *al* [8].

2.5.4 Polynômes exceptionnels

Dans cette section, on introduit quelques idées géométriques à l'étude des polynômes de permutation. Cette relation permet en particulier l'utilisation des résultats de *Weil* pour estimer le nombre de points rationnels sur une courbe absolument irréductible définie toujours sur un corps fini.
Soit $f \in \mathbb{F}_q[x]$ un polynôme de degré $d \geq 1$, on forme un polynôme à deux indéterminées de degré $d-1$,

$$\phi(x,y) = \frac{f(x) - f(y)}{x - y}, \quad \phi \in \mathbb{F}_q[x,y]$$

et on définit une courbe algébrique C_ϕ par

$$C_\phi = \{(a,b) \in \mathbb{F}_q \times \mathbb{F}_q : \phi(a,b) = 0\}$$

Les points $(a,b) \in \mathbb{F}_q$ sont dits rationnels.
Le polynôme f est un polynôme de permutation si et seulement si la courbe C_ϕ n'admet aucun point rationnel en dehors de la ligne $x = y$.

On rappelle qu'un polynôme à coefficients dans un corps K est dit absolument irréductible s'il est irréductible sur toute extension algébrique de K. Ou de façon équivalente sur une clôture algébrique du corps K.
Considérons par exemple le polynôme $\phi(x,y) = y^2 + x^2 \in \mathbb{F}_7[x,y],\quad \phi$ est irréductible sur $\mathbb{F}_7$ mais n'est pas irréductible sur l'extension $\mathbb{F}_{7^2} \simeq \mathbb{F}_7[x]/ < x^2 + 1 > \simeq \mathbb{F}_7(\alpha)$, où α est racine du polynôme $x^2 + 1$. Car il se décompose en $(y + \alpha x)(y - \alpha x)$ sur $\mathbb{F}_{7^2}$.

Définition 2.3 *Un polynôme $f \in \mathbb{F}_q[x]$ de degré supérieur ou égal à 2 est dit exceptionnel sur $\mathbb{F}_q$ si aucun des facteurs irréductibles de*

$$\phi(x,y) = \frac{f(x)-f(y)}{x-y}$$

n'est absolument irréductible.

Autrement dit, f est exceptionnel sur $\mathbb{F}_q$ si tout facteur irréductible du polynôme $\phi(x,y) \in \mathbb{F}_q[x,\ y]$ admet une factorisation sur une certaine extension algébrique de $\mathbb{F}_q$.

Théorème 2.10 *Tout Polynôme exceptionnel sur $\mathbb{F}_q$ est un polynôme de permutation.*

Exemple 2.3 *Soit $f(x) = x^3 + 3x^2 + 3x$ un polynôme de $\mathbb{F}_q[x]$, où $\mathbb{F}_q$ est un corps fini de caractéristique p premier différent de 2. Nous formons le polynôme $\phi(x,y)$*

$$\begin{aligned}\phi(x,y) = \frac{f(x)-f(y)}{x-y} &= \frac{x^3-y^3}{x-y} + 3\frac{x^2-y^2}{x-y} + 3\frac{x-y}{x-y} \\ &= x^2 + xy + y^2 + 3(x+y) + 3 \\ &= x^2 + (3+y)x + y^2 + 3y + 3 \quad \in \mathbb{F}_q(y)[x]\end{aligned}$$

c'est un polynôme de degré 2 dont le discriminant est égal à $-3(y+1)^2$. On a donc deux cas à distinguer

— *Si -3 est un carré dans $\mathbb{F}_q$ i.e il existe $a \in \mathbb{F}_q$ tel que $-3 = a^2$ alors le polynôme $\phi(x,y)$ admet deux racines $x_1 = \frac{-y-3+a(y+1)}{2}$ et $x_2 = \frac{-y-3-a(y+1)}{2}$ et s'écrit donc comme*

$$\phi(x,y) = (x - \frac{-y-3+a(y+1)}{2})(x - \frac{-y-3-a(y+1)}{2})$$

Ces deux facteurs sont absolument irréductibles dans $\mathbb{F}_q[x,y]$, ce qui implique d'après le Théorème 2.10 que f n'est pas un polynôme de permutation de $\mathbb{F}_q$.

— *Si -3 n'est pas un carré dans $\mathbb{F}_q$, alors $\phi(x,y)$ est irréductible dans $\mathbb{F}_q[x,y]$. Dans une clôture algébrique de $\mathbb{F}_q$, $x^2+3=0$ est décomposable, on revient alors au premier cas, ce qui implique d'après le Théorème 2.10 que f est un polynôme de permutation de $\mathbb{F}_q$.*

La réciproque du Théorème 2.10 est fausse. En effet, soit $q=p^r$ et $f(x)=x^p$, alors f permute $\mathbb{F}_q$ puisque $pgcd(p,q-1)=1$. Alors

$$\phi(x,y)=\frac{x^p-y^p}{x-y}=\frac{(x-y)^p}{x-y}=(x-y)^{p-1}$$

Or $x-y$ est absolument irréductible, donc f n'est pas un polynôme exceptionnel.
Le résultat suivant donne une condition nécéssaire pour que la réciproque du Théorème 2.10 soit vraie.

Théorème 2.11 *Il existe une suite d'entiers $c_1, c_2, ...$ tels que pour tout corps fini $\mathbb{F}_q$ d'ordre $q > c_n$ avec $pgcd(n,q)=1$ alors la proposition suivante a lieu :*
Si $f(x) \in \mathbb{F}_q[x]$ est un polynôme de permutation de degré n alors f est exceptionnel sur $\mathbb{F}_q$.

2.5.5 Les polynômes de Dickson

Introduisons maintenant une classe spéciale de polynômes, appelés polynômes de *Dickson*. Cette classe possède de nombreuses propriétés et donne de nombreux exemples de polynômes de permutation.
Nous nous donnerons ici des résultats en relation directe avec les polynômes de permutation. Le reste est répertorié dans [27].

Définition 2.4 *Le $n-$ième polynômes de Dickson de paramètre a est définit par :*

$$D_n(x,a)=\sum_{i=0}^{\lfloor n/2\rfloor}\frac{n}{n-i}\binom{n-i}{i}(-a)^i x^{n-2i}$$

Les premiers polynômes de cette séquence sont
$D_0(x,a)=2$

$D_1(x,a) = x$

$D_2(x,a) = x^2 - 2a$

$D_3(x,a) = x^3 - 3xa$

$D_4(x,a) = x^4 - 4x^2a + 2a^2$

Théorème 2.12 *Le polynôme* $D_n(x,a),\ a \in \mathbb{F}_q^*$ *est de permutation sur* $\mathbb{F}_q$ *si et seulement si* $pgcd(n, q^2-1) = 1$

Il est à noter que l'ensemble de polynômes de *Dickson* $D_n(x,a)$ avec $pgcd(n,q^2-1)=1$ est stable par composition si et seulement si a prend ses valeurs dans l'ensemble $\{0,1,-1\}$

2.5.6 Les binômes

Une autre voie de classement de polynômes est de considérer le nombre de termes. Le cas des monômes est simple. Cependant dès que l'on passe aux binômes, la classification devient trés compliquée. Il s'agit en fait de l'un des problèmes proposés par *Lidl* et *Mullen* [16].
Les résultats énoncés dans cette section sont liés au problème de polynômes binomiaux et aux conditions d'existence de binôme de permutation sur un corps fini. Les auteurs dans [20] ont démontré le résultat suivant

Théorème 2.13 *Soit* n *un entier positif, alors il existe une constante* $C(n)$ *telle que pour* $q > C(n)$, *il n'existe pas de polynôme de permutation de* $\mathbb{F}_q$ *de la forme* $ax^n + bx^m + c\ \in \mathbb{F}_q[x]$, *avec* $n > m > 1$, $pgcd(n,m) = 1$ *et* $ab \neq 0$

Par la suite, *Turnwald* [24] a amélioré le théorème ci-dessus. Et a démontré en utilisant les polynômes exceptionnels, le résultat suivant :

Théorème 2.14 *Si* $f(x) = ax^n + x^m$ *permute* $\mathbb{F}_q$, *où* $n > m > 0$ *et* $a \in \mathbb{F}_q^*$, *alors soit* $q \leq (n-2)^4 + 4n - 4$, *soit* $n = mp^i$

Pour q impair, *Turnwald* [24] a aussi énoncé le résultat suivant :

Théorème 2.15 *Si* $f(x) = ax^n + x^m$ *permute* $\mathbb{F}_p$, *où* $n > m > 0$ *et* $a \in \mathbb{F}_p^*$, *alors* $p < n\ max(m, n-m)$

Le cas $m = 1$ a été démontré par *Wan* [28]

Théorème 2.16 *Si* $f(x) = ax^n + x$ *permute* $\mathbb{F}_p$, *où* $n > 1$ *et* $a \in \mathbb{F}_p^*$, *alors* $p - 1 < (n-1)pgcd(n-1, p-1)$

Les majorations dans les deux théorèmes précedents ne sont pas du même type. La borne du Théorème 2.15 est donnée en fonction de $max(m, n-m)$, et celle du théorème 2.16 en fonction du $pgcd(n-1, p-1)$. Ces deux théorèmes ont été améliorés par *Masuda* et *Zieve* [19], où p a été majoré seulement par $d = pgcd(n-m, p-1)$

Théorème 2.17 *Si* $f(x) = ax^n + x^m$ *permute* $\mathbb{F}_p$, *où* $n > m > 0$, *et* $a \in \mathbb{F}_q^*$, *et alors* $p - 1 < d(d+1)$.

Ayad et *al* [3], ont montré comment on peut obtenir dans certains cas, un polynôme de permutation binomial d'un sous corps de $\mathbb{F}_q$ à partir d'un polynôme binomial $f(x) \in \mathbb{F}_q[x]$, et ont déduit une majoration de p en fonction de $d = pgcd(n-m, p-1)$.

Théorème 2.18 *Soit* $f(x) = ax^n + x^m$ *un polynôme de permutation binomial de* $\mathbb{F}_q$, *avec* $q = p^r$, *et* s *un diviseur positif de* r. *Soit* $d = pgcd(n-m, p-1)$, *alors*

1. *Il existe un binôme* $g(x) = bx^n + x^m \in \mathbb{F}_{p^s}[x]$, $d-$*equivalent à* $f(x)$ *si et seulement si l'ordre de* a *dans* $\mathbb{F}_q^*$ *divise* $ppcm(p^s - 1, (q-1)/d)$
2. *Si les conditions d'équivalence dans (1) sont satisfaites, alors le nombre de* $g(x) = bx^n + x^m \in \mathbb{F}_{p^s}[x]$, $d-$*equivalent à* $f(x)$ *est égal à* $pgcd(p^s - 1, (q-1)/d)$, *et ils sont tous distincts comme permutations de* $\mathbb{F}_{p^s}$. *De plus, nous avons* $g(x) \equiv bx^{n_1} + x^{m_1} \mod (x^{p^s} - x)$ *si* $p^s - 1$ *ne divise pas* d *et* $g(x) \equiv (b+1)x^k \mod (x^{p^s} - x)$ *si* $p^s - 1$ *divise* d, *où* k, m_1, n_1 *sont des entiers positifs inférieur à* $p_s - 1$, $m_1 \neq n_1$ *et* $pgcd(p^s - 1, k) = 1$.
3. *Soit* t *un entier positif. Il existe un binôme* $g(x) = bx^n + x^m \in (\mathbb{F}_{p^t} \cap \mathbb{F}_q)[x]$, $d-$*equivalent à* $f(x)$ *si et seulement si l'ordre de* a *dans* $\mathbb{F}_q^*$ *divise* $ppcm(p^t - 1, (q-1)/d)$.

On note que les polynômes f et g sont dits $d-$équivalents ($f \sim g$), s'il existe $\xi \in (\mathbb{F}_q)^d$ tel que $b = \xi a$.

Corollaire 2.2 *Supposons qu'il existe un polynôme de permutation binomial* $f(x) = ax^n + x^m$ *de* $\mathbb{F}_q$ *avec* $q = p^r$ *tel que pour tout nombre premier* l *divisant* d, *le* $pgcd(l(l-1), r) = 1$. *Alors* $d = p - 1$ *ou bien il existe un polynôme de permutation binomial de* $\mathbb{F}_q$, $g_1(x) = cx^{n_1} + x^{m_1}$ *tel que* $n \equiv kn_1 \mod (p-1)$, $m \equiv km_1 \mod (p-1)$, *et* $0 < km_1 < kn_1 < p - 1$, *où* k *est un entier positif relativement premier avec* $p - 1$ *et* $p - 1 \leq d(d-1)$

Chapitre 3

Polynômes de la forme $x^r f(x^{(q-1)/d})$

3.1 Introduction

La caractérisation des polynômes de permutation n'est pas toujours facile. Les polynômes du type $x^r f(x^{(q-1)/d})$, où $r \geq 1$, $d \geq 1$ et d est un diviseur de $q-1$, ont été considérés pendant longtemps comme classe de polynômes de permutation dit de troisième espèce. Il s'est avèré qu'au fil du temps tous les résultats obtenus se sont trouvés être des cas particuliers de ce type de polynômes. Par exemple *Akbary* et *Wang* [1] ont observé que tout polynôme $h(x) \in \mathbb{F}_q[x]$ peut être mis sous la forme $a(x^r f(x^{(q-1)/d})) + b$, pour un certain $r \geq 1$ et d diviseur de $q-1$.
En effet, On peut écrire sans perte de généralités

$$h(x) = a(x^n + a_{n-i_1}x^{n-i_1} + ... + a_{n-i_k}x^{n-i_k}) + b$$

où a, $a_{n-i_j} \neq 0$, $j = 1, ..., k$. Supposons que $j \geq 1$ et $n - i_k = r$, alors $h(x) = ax^r f(x^{(q-1)/d}) + b$, où $f(x) = x^{e_0} + a_{n-i_1}x^{e_1} + ... + a_{n-i_{k-1}}x^{e_{k-1}} + a_r$, avec

$$d = \frac{q-1}{pgcd(n-r, n-r-i_1, ..., n-r-i_{k-1}, q-1)},$$

et $pgcd(e_0, e_1, ..., e_{k-1}, d) = 1$.

En raison de l'importance des polynômes de la forme $x^r f(x^{(q-1)/d})$, il est intéressant de donner un critère pour les polynômes de permutation de ce type. Ce critère a été donné par *Wan* et *Lidl* en 1991 dans leur article de repère intitulé "Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure" [27]. Le critère donné par *Wan* et *Lidl* généralise les résultats précédents sur ce type de polynômes. Si par exemple une racine primitive de $\mathbb{F}_q$ est connue, et d est petit, leur critère donne un moyen suffisant pour construire des polynômes de permutation de $\mathbb{F}_q$.

Soit b un élément primitif de $\mathbb{F}_q$, alors pour tout élément a de $\mathbb{F}_q^*$, il existe un entier positif r avec $0 \leq r \leq q-2$ tel que $a = b^r$. L'entier r est appelé le logarithme discret de a en base b, ou simplement index, noté $r = Ind_b(a)$. Cette fonction satisfait modulo le cardinal de $\mathbb{F}_q^*$ les propriétés suivantes :

$$Ind(ac) = [Ind(a) + ind(c)] \mathrm{mod}(q-1)$$
$$Ind(ac^{-1}) = [Ind(a) - Ind(c)] \mathrm{mod}(q-1)$$

Une application directe de ces propriétés permet de ramener le calcul de la loi de groupe à une addition ou une soustraction. Obtenir le produit de deux éléments d'un corps fini par cette technique n'est pas toujours approprié quand il s'agit de corps de grandes tailles. En fait, calculer a à partir de r d'un point de vue algorithmique est facile, en particulier en utilisant la fonction inverse de la fonction index ou bien ce qu'on appelle exponentiation binaire, l'inverse est aujourd'hui considéré comme difficile pour certains groupes.

3.2 Critère de *Wan* et *Lidl*

Etablissons le critère de *Wan* et *Lidl*, qui donne des conditions nécessaires et suffisantes pour que les polynômes de la forme $x^r f(x^{(q-1)/d})$ soient des permutations de $\mathbb{F}_q$, où d et r sont deux entiers positifs tels que d divise $q-1$.

Définition 3.1 *Soit d un diviseur de $q-1$, et g un élément primitif de $\mathbb{F}_q$. Et soit*

$\omega = g^{(q-1)/d}$ la $d-$ième racine primitive de l'unité dans $\mathbb{F}_q$. On définit un caractère multiplicatif à valeurs dans $\mathbb{Z}/d\mathbb{Z}$ par :

$$\begin{array}{rccc} \psi & : & \mathbb{F}_q^* & \longrightarrow & \mathbb{Z}/d\mathbb{Z} \\ & & a & \longmapsto & \psi(a) \equiv Ind_g(a) \mod d \end{array}$$

où $Ind_g(a)$ est la classe d'équivalence de $b \mod (q-1)$, telle que $a = g^b$.

On remarque que

$$a^{(q-1)/d} = g^{b(q-1)/d} = \omega^{\psi(a)}$$

Avec cette définition, *Wan* et *Lidl* ont introduit le critère suivant

Théorème 3.1 *Soient d et r deux entiers positifs tels que d divise $q-1$ et $f(x) \in \mathbb{F}_q[x]$. Alors le polynôme $h(x) = x^r f(x^{(q-1)/d})$ est un polynôme de permutation de $\mathbb{F}_q$ si et seulement si les trois conditions suivantes sont satisfaites :*
(i) *$pgcd(r, \frac{q-1}{d}) = 1$*
(ii) *Pour tout $0 \leq i < d$, $f(\omega^i) \neq 0$*
(iii) *Pour $0 \leq i < j < d$, $\psi(\frac{f(\omega^i)}{f(\omega^j)}) \not\equiv r(j-i) \mod d$*

Preuve : Si h est un polynôme de permutation de $\mathbb{F}_q$, alors $h(x) = 0$ admet la solution nulle $x = 0$ comme solution unique, ce qui montre que la condition *(ii)* est nécessaire. En effet, comme $h(x) = x^r f(x^{(q-1)/d})$, on peut conclure que

$$f(x^{(q-1)/d}) = f(\omega^{\psi(x)}) = f(\omega^i) \neq 0 \text{ pour tout } 0 \leq i < d.$$

Supposons maintenant que la condition *(ii)* est vraie, pour démontrer le théorème, il est suffisant de montrer que $h(x)$ est un polynôme de permutation de $\mathbb{F}_q$ si et seulement si les conditions *(i)* et *(iii)* sont satisfaites.
Comme $f(\omega^i) \neq 0$, et tout élément $x \in \mathbb{F}_q^*$, s'écrit sous la forme g^k, pour un certain entier positif k, il est clair que h représente une permutation de $\mathbb{F}_q$ si et seulement si les éléments de l'ensemble $\{Ind_g(h(g^k)) \mod (q-1),\ 0 \leq k \leq q-2\}$ sont distincts, ce qui forme l'ensemble de classes d'équivalence de l'anneau quotient $\mathbb{Z}/(q-1)\mathbb{Z}$.

Soit k un entier tel que

$$k = i + dj, \quad 0 \leq i \leq d-1, \quad 0 \leq j < \tfrac{q-1}{d}$$

alors on peut simplifier l'écriture de $Ind_g(h(g^k)) \mod (q-1)$ comme suit

$$\begin{aligned}
Ind_g(h(g^k)) &= Ind_g((g^k)^r f((g^k)^{(q-1)/d})) \\
&= Ind_g((g^k)^r) + Ind_g(f((g^k)^{(q-1)/d}) \\
&= Ind_g(g^{kr}) + Ind_g(f(g^{k(q-1)/d})) \\
&= kr + Ind_g(f(g^{k(q-1)/d})) \\
&= (i+dj)r + Ind_g(f(g^{(i+dj)(q-1)/d})) \\
&= (dr)j + ri + Ind_g(f(g^{i(q-1)/d} g^{j(q-1)})) \\
&= (dr)j + ri + Ind_g(f(\omega^i)) \\
&= (dr)j + Ing_g(g^{ri}) + Ind_g(f(\omega^i)) \\
&= (dr)j + Ind_g(g^{ri} f(\omega^i))
\end{aligned}$$

$\{Ind_g(h(g^k)) \mod (q-1),\ 0 \leq k \leq q-2\} = \mathbb{Z}/(q-1)\mathbb{Z}$ si et seulement si $\{rj,\ 0 \leq j < \frac{q-1}{d}\} = \mathbb{Z}/(\frac{q-1}{d})\mathbb{Z}$ et $\{Ind_g(g^{ri} f(\omega^i)),\ 0 \leq i \leq d-1\} = \mathbb{Z}/d\mathbb{Z}$.
On a donc h un polynôme de permutation si et seulement si :

- Pour $0 \leq j_1 < j_2 < \frac{q-1}{d}$, $rj_1 \neq rj_2 \mod (\frac{q-1}{d})$ ce qui est équivalent à ce que le $pgcd(r, \frac{q-1}{d}) = 1$
- Pour $0 \leq i_1 < i_2 \leq d-1$, $\psi(\frac{f(\omega^{i_1})}{f(\omega^{i_2})}) \neq r(i_2 - i_1) \mod d$

  En effet, supposons le contraire et prenons i_1 et i_2 tels que

  $$\begin{aligned}
  \psi(\tfrac{f(\omega^{i_1})}{f(\omega^{i_2})}) &\equiv r(i_2 - i_1) \mod d \\
  \text{alors } \tfrac{f(\omega^{i_1})}{f(\omega^{i_2})} &\equiv g^{r(i_2-i_1)} = g^{ri_1 - ri_2} = \tfrac{g^{ri_1}}{g^{ri_2}} \\
  \Rightarrow \quad g^{ri_1} f(\omega^{i_1}) &= g^{ri_2} f(\omega^{i_2})
  \end{aligned}$$

  Traduisant que les éléments de l'ensemble $\{Ind_g(g^{ri} f(\omega^i)),\ 0 \leq i \leq d-1\}$ ne sont pas distincts.

Ainsi la condition (iii) est nécessaire pour que l'ensemble

$$\{Ind_g(h(g^k)) \mod (q-1),\ 0 \leq k \leq q-2\}$$

soit égal à $\mathbb{Z}/(q-1)\mathbb{Z}$, et le théorème est démontré.
Une traduction du critère de *Wan* et *Lidl* est donnée par le théorème suivant :

Théorème 3.2 *Soient d un diviseur de $q-1$ et $r \in \mathbb{N}$ tels que $pgcd(r, \frac{q-1}{d}) = 1$. Soit $f(x) \in \mathbb{F}_q[x]$ tel que $f(\omega^i) \neq 0,\ \forall i \in \{0, 1, ..., d-1\}$. On définit $\pi(i)$ et $t(i)$ par la relation suivante :*

$$Ind_g(f(\omega^i)) = \pi(i) - ri + dt(i),\ \pi(i) \in \mathbb{Z}/d\mathbb{Z} \text{ et } t(i) \in \mathbb{Z}/(\tfrac{q-1}{d})\mathbb{Z},$$

alors le polynôme $h(x) = x^r f(x^{\frac{q-1}{d}})$ permute $\mathbb{F}_q$ si et seulement si $\pi(i)$ permute $\mathbb{Z}/d\mathbb{Z}$

A partir de ce résultat, on peut construire des polynômes de permutation de $\mathbb{F}_q$ de la forme $x^r f(x^{\frac{q-1}{d}})$ en résolvant simplement un système d'équations linéaires.
Soient g une racine primitive de $\mathbb{F}_q$, $\pi \in S_d$ une permutation et t une application de $\mathbb{Z}/d\mathbb{Z}$ dans $\mathbb{Z}/(\frac{q-1}{d})\mathbb{Z}$. Choisissons un entier r tel que $pgcd(r, \frac{q-1}{d}) = 1$.
Notons $\omega = g^{\frac{q-1}{d}}$, alors le système

$$\sum_{j=0}^{d-1} a_j \omega^{ij} = g^{\pi(i)-ri+dt(i)}$$

a une solution unique $a_j \in \mathbb{F}_q,\ j \in \{0, ..., d-1\}$ puisque il s'agit bien du système de *Vandermonde*.
Selon le Théorème 3.1, $h(x) = x^r f(x^{\frac{q-1}{d}})$ représente un polynôme de permutation de $\mathbb{F}_q$, avec $f(x) = a_{d-1}x^{d-1} + ... + a_1 x + a_0$.

3.3 Applications du critère de *Wan* et *Lidl*

Citons dans cette section quelques applications du critère de *Wan* et *Lidl* sous forme de corollaires, qui généralisent les résultats précédents sur les polynômes de permutation de la forme $x^r f(x^s)$.

Corollaire 3.1 *Soient d un diviseur de $q-1$, et $r \in \mathbb{N}$ tels que $pgcd(r, \frac{q-1}{d}) = 1$, alors le polynôme $h(x) = x^r f(x^{\frac{q-1}{d}})^d$ est un polynôme de permutation si et seulement si $f(x^{\frac{q-1}{d}})$ n'admet pas de racine non nulle dans $\mathbb{F}_q$.*

Corollaire 3.2 *Soient d un diviseur de $q-1$, $r \in \mathbb{N}$, et $\alpha \in \mathbb{F}_q$. Alors le polynôme $x^r(x^{\frac{q-1}{d}} - \alpha)$ est une permutation de $\mathbb{F}_q$ si et seulement si $pgcd(r, \frac{q-1}{d}) = 1$, $\alpha^d \neq 1$ et pour tout $0 \leq i < j < d$*

$$\psi(\tfrac{\omega^i - \alpha}{\omega^j - \alpha}) \equiv 0 \mod d$$

Corollaire 3.3 *Soient d un diviseur de $q-1$, et $f(x)$ un polynôme de $\mathbb{F}_q[x]$, alors pour q suffisamment grand, il existe $a \in \mathbb{F}_q$ tel que $x^r(f(x^{\frac{q-1}{d}}) + a)^k$ soit un polynôme de permutation de $\mathbb{F}_q$ pour tout $k \in \mathbb{N}^*$ et pour tout $r \in \mathbb{N}$ tel que $pgcd(r, q-1) = 1$*

3.4 Nouvelle famille de polynômes de permutation

Nous établissons dans cette section une nouvelle famille de polynômes de permutation présentée par *Ayad* et *Kihel* [5]. Les auteurs dans [5] ont utilisé des méthodes élémentaires pour prouver que cette dernière représente une famille de polynômes de permutation. Nous allons donner la preuve du théorème suivant

Théorème 3.3 *Soit u un entier positif et $f(x)$ un polynôme de $\mathbb{F}_q$ tel que*

$$f(x) = x^u(x^{\frac{q-1}{2}} + x^{\frac{q-1}{4}} + 1).$$

Supposons que les conditions suivantes soient satisfaites

(i) $pgcd(u, q-1) = 1$

(ii) $q \equiv 1 \mod 8$

(iii) $3^{\frac{q-1}{4}} \equiv 1 \pmod p$

alors f est un polynôme de permutation de $\mathbb{F}_q$

Preuve : Montrons qu'avec les conditions indiquées ci dessus, le polynôme

$$f(x) = x^u(x^{\frac{q-1}{2}} + x^{\frac{q-1}{4}} + 1) \tag{3.1}$$

représente une application injective sur $\mathbb{F}_q$.

Supposons que $f(a) = f(b), \quad a, b \in \mathbb{F}_q$.

Si $a = 0$ nous aurons $f(a) = f(0) = 0$ alors

$$0 = f(a) = f(b) = b^u(b^{\frac{q-1}{2}} + b^{\frac{q-1}{4}} + 1)$$

supposons que $b \neq 0$, cela veut dire que $b^u \neq 0$ et $b^{\frac{q-1}{2}} + b^{\frac{q-1}{4}} + 1 = 0$.

Posons $c = b^{\frac{q-1}{4}}$ alors l'équation $b^{\frac{q-1}{2}} + b^{\frac{q-1}{4}} + 1 = 0$ devient $c^2 + c + 1 = 0$, or $(c-1)(c^2+c+1) = 0$ implique que $c^3 - 1 = 0$, il en résulte que c est une racine cubique de l'unité.

Nous avons $c = c.1 = c.c^3 = c^4 = (b^{\frac{q-1}{4}})^4 = 1$ dans $\mathbb{F}_q$, mais la condition *(iii)* implique que $c \neq 1$ qui est une contradiction. Ainsi nous aurons nécessairement $b = 0 = a$

Supposons dés maintenant que $ab \neq 0$.

D'après le critère d'Euler, nous avons

$$a^{\frac{q-1}{2}} = \begin{cases} 1 & \text{si } a \text{ est résidu quadratique modulo } p \\ -1 & \text{sinon} \end{cases} \tag{3.2}$$

et

$$b^{\frac{q-1}{2}} = \begin{cases} 1 & \text{si } b \text{ est résidu quadratique modulo } p \\ -1 & \text{sinon} \end{cases} \tag{3.3}$$

Par symmetrie, nous allons considérer seulement les trois cas suivants

1er cas) : Si $a^{\frac{q-1}{2}} = b^{\frac{q-1}{2}} = 1$ alors $a^{\frac{q-1}{4}} = \varepsilon_1$ et $b^{\frac{q-1}{4}} = \varepsilon_2$ avec $\varepsilon_1, \varepsilon_2 \in \{-1, 1\}$

Si $a^{\frac{q-1}{4}} = b^{\frac{q-1}{4}} = 1$ alors L'équation (3.1) donne

$$\begin{aligned} f(a) = f(b) &\Longrightarrow a^u(a^{\frac{q-1}{2}} + a^{\frac{q-1}{4}} + 1) = b^u(b^{\frac{q-1}{2}} + b^{\frac{q-1}{4}} + 1) \\ &\Longrightarrow a^u(1+1+1) = b^u(1+1+1) \\ &\Longrightarrow a^u 3 = b^u 3 \\ &\Longrightarrow a^u = b^u \\ &\Longrightarrow (\frac{a}{b})^u = 1 \Longrightarrow a = b \text{ puisque } pgcd(u, q-1) = 1 \text{ d'après la condition } (i) \end{aligned}$$

qui est une contradiction.

Si $a^{\frac{q-1}{4}} = 1$ et $b^{\frac{q-1}{4}} = -1$ alors L'équation (3.1) donne

$$\begin{aligned}
f(a) = f(b) &\Longrightarrow a^u(a^{\frac{q-1}{2}} + a^{\frac{q-1}{4}} + 1) = b^u(b^{\frac{q-1}{2}} + b^{\frac{q-1}{4}} + 1) \\
&\Longrightarrow a^u(1 + 1 + 1) = b^u(1 - 1 + 1) \\
&\Longrightarrow a^u 3 = b^u \\
&\Longrightarrow \frac{b^u}{a^u} = 3 \\
&\Longrightarrow (\frac{b}{a})^u = 3 \Longrightarrow ((\frac{b}{a})^u)^{\frac{q-1}{4}} = 3^{\frac{q-1}{4}} \\
&\Longrightarrow ((\frac{b}{a})^{\frac{q-1}{4}})^u = 3^{\frac{q-1}{4}} \\
&\Longrightarrow (\frac{b^{\frac{q-1}{4}}}{a^{\frac{q-1}{4}}})^u = 3^{\frac{q-1}{4}} \Longrightarrow (\frac{-1}{1})^u = 3^{\frac{q-1}{4}} \\
&\Longrightarrow (-1)^u = 3^{\frac{q-1}{4}} = 1 \text{ puisque on a } 3^{\frac{q-1}{4}} \equiv 1 \pmod{p} \text{ d'après la condition } \textit{(iii)}
\end{aligned}$$

ce qui montre que u est pair, mais d'après la condition *(i)* nous avons $pgcd(u, q-1) = 1$ i.e u ne peut être pair puisque $q-1$ est pair. Ce qui est encore une contradiction.

2ème cas) : Si $a^{\frac{q-1}{2}} = b^{\frac{q-1}{2}} = -1$, alors

$$\begin{aligned}
f(a) = f(b) &\Longrightarrow a^u(a^{\frac{q-1}{2}} + a^{\frac{q-1}{4}} + 1) = b^u(b^{\frac{q-1}{2}} + b^{\frac{q-1}{4}} + 1) \\
&\Longrightarrow a^u(-1 + a^{\frac{q-1}{4}} + 1) = b^u(-1 + b^{\frac{q-1}{4}} + 1) \\
&\Longrightarrow a^u(a^{\frac{q-1}{4}}) = b^u(b^{\frac{q-1}{4}}) \\
&\Longrightarrow a^{u+\frac{q-1}{4}} = b^{u+\frac{q-1}{4}} \\
&\Longrightarrow (\frac{b}{a})^{(u+\frac{q-1}{4})} = 1
\end{aligned}$$

Soit δ l'ordre de l'élément $\frac{b}{a}$ dans $\mathbb{F}_q$. Comme $(\frac{b}{a})^{u+\frac{q-1}{4}} = 1$ et $(\frac{b}{a})^{q-1} = 1$, alors δ divise $u + \frac{q-1}{4}$ et $q-1$. Soit l un nombre premier diviseur de δ et $pgcd(u, q-1) = 1$, alors u ne peut être pair puisque $q-1$ l'est, ce qui donne l premier impair. Et puisque on peut ecrire $q - 1 = 4(\frac{q-1}{4})$, et l ne peut diviser 4, alors l doit être un diviseur de $\frac{q-1}{4}$. Et comme δ divise $u + \frac{q-1}{4}$ alors on peut conclure que l divise u, ce qui est impossible puisque $pgcd(u,\ q-1) = 1$

3ème cas) : Si $a^{\frac{q-1}{2}} = -b^{\frac{q-1}{2}} = 1$. On a $a^{\frac{q-1}{4}} = \pm 1$ et $b^{\frac{q-1}{4}} = \xi$, où ξ est une racine primitive quadratique de l'unité.

(a) Si $a^{\frac{q-1}{4}} = 1$ et $b^{\frac{q-1}{4}} = \xi$ alors L'équation (3.1) donne

$$\begin{aligned} f(a) = f(b) &\Longrightarrow a^u(a^{\frac{q-1}{2}} + a^{\frac{q-1}{4}} + 1) = b^u(b^{\frac{q-1}{2}} + b^{\frac{q-1}{4}} + 1) \\ &\Longrightarrow a^u(1+1+1) = b^u(-1+\xi+1) \\ &\Longrightarrow a^u 3 = \xi b^u \\ &\Longrightarrow (\frac{a}{b})^u = \frac{\xi}{3} \text{ puisque la caractéristique de } \mathbb{F}_q \text{ est differente de 3} \\ &\Longrightarrow ((\frac{a}{b})^u)^{\frac{q-1}{2}} = (\frac{\xi}{3})^{\frac{q-1}{2}} \Longrightarrow (\frac{a^{\frac{q-1}{2}}}{b^{\frac{q-1}{2}}})^u = (\frac{\xi}{3})^{\frac{q-1}{2}} \\ &\Longrightarrow (-1)^u = \frac{\xi^{\frac{q-1}{2}}}{3^{\frac{q-1}{2}}} \Longrightarrow 3^{\frac{q-1}{2}} = -1 \text{puisque } \xi \text{ est une racine quadratique de l'unité} \end{aligned}$$

ceci contredit la condition *(iii)*, ainsi $f(a) \neq f(b)$

(b) Si $a^{\frac{q-1}{4}} = -1$ et $b^{\frac{q-1}{4}} = \xi$ alors L'équation (3.1) donne

$$\begin{aligned} f(a) = f(b) &\Longrightarrow a^u(a^{\frac{q-1}{2}} + a^{\frac{q-1}{4}} + 1) = b^u(b^{\frac{q-1}{2}} + b^{\frac{q-1}{4}} + 1) \\ &\Longrightarrow a^u(1-1+1) = b^u(-1+\xi+1) \\ &\Longrightarrow a^u = \xi b^u \\ &\Longrightarrow (\frac{a}{b})^u = \xi \Longrightarrow ((\frac{a}{b})^u)^4 = (\xi)^4 \Longrightarrow (\frac{a}{b})^{4u} = 1 \Longrightarrow (\frac{a}{b})^4 = 1 \end{aligned}$$

Si $\frac{a}{b} = -1$ alors $a^{\frac{q-1}{2}} = (-1)^{\frac{q-1}{2}} b^{\frac{q-1}{2}} = b^{\frac{q-1}{2}}$ qui est une contradiction puisque a et b sont supposés différents.

Si $\frac{a}{b} = \pm\xi$ alors $a^{\frac{q-1}{2}} = (\pm\xi)^{\frac{q-1}{2}} b^{\frac{q-1}{2}}$, ce qui donne $1 = (\xi 4)^{\frac{q-1}{8}}(-1)$, ce qui est encore impossible.

Ainsi on a nécessairement $a = b$, et le théorème est prouvé.

Chapitre 4

Famille de polynômes de permutation de $\mathbb{F}_q$

4.1 Introduction

L'interêt croissant pour les polynômes de permutation réside en partie dans leur application à la cryptographie et à la théorie des codages. Un des problèmes ouverts proposé par *Lidl* et *Mullen* [16], est celui de trouver une nouvelle classe de polynômes de permutation de $\mathbb{F}_q$. Malgré l'intérêt suscité par le sujet, la caractérisation des polynômes de permutation et celle de la recherche de nouvelles familles de polynômes à caractère bijectif demeurent des questions ouvertes. *Ayad* et *Kihel* [5] ont utilisé des techniques élémentaires, et ont établi des conditions suffisantes sur les entiers u et q pour que le polynôme $x^u(1 + x^{\frac{q-1}{4}} + x^{\frac{q-1}{2}})$ représente un polynôme de permutation de $\mathbb{F}_q$.
Dans ce chapitre, nous généralisons le Théorème 3.3 présenté au chapitre 3, à la famille des polynômes $h(x) = x^u(1 \pm x^{\frac{q-1}{4}} \pm x^{\frac{q-1}{2}})$ et nous donnons des conditions nécessaires et suffisantes pour que $h(x)$ soit un polynôme de permutation de $\mathbb{F}_q$. Les preuves que nous allons présenter reposent en grande partie sur le Théorème 3.1 de *Wan* et *Lidl* [27] presenté au chapitre 3.

4.2 Polynômes de la forme $h(x) = x^u(1 \pm x^{\frac{q-1}{4}} \pm x^{\frac{q-1}{2}})$

Soit $\mathbb{F}_q$ un corps fini de caractéristique p contenant $q = p^r$ éléments. Nous rappellons qu'un polynôme $f(x) \in \mathbb{F}_q[x]$ est appelé polynôme de permutation de $\mathbb{F}_q$ si l'application induite $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ est bijective. Dans la première partie de cette section, nous construisons une nouvelle famille de polynômes de permutation sur $\mathbb{F}_q$, et nous démontrons le théorème suivant

Théorème 4.1 *Soit $p \neq 5$ un nombre premier, et $q = p^r$, où r est un entier positif tel que $q \equiv 1 \bmod 4$. Soit g un élément primitif de $\mathbb{F}_q$ et $\omega = g^{\frac{q-1}{4}}$ la 4-racine primitive de l'unité dans $\mathbb{F}_q$. Alors le polynôme*

$$h(x) = x^u(1 + x^{\frac{q-1}{4}} - x^{\frac{q-1}{2}})$$

est un polynôme de permutation de $\mathbb{F}_q$ si et seulement si une des conditions suivantes est satisfaite.

(1) $q \equiv 1 \bmod 8$, $pgcd(u, \frac{q-1}{4}) = 1$, *$u$ impair et* $(2+\omega)^{\frac{q-1}{4}} = \pm 1$

(2) $q \not\equiv 1 \bmod 8$, $pgcd(u, \frac{q-1}{4}) = 1$, *$u$ pair et* $(2+\omega)^{\frac{q-1}{4}} \neq \pm 1$.

Preuve : Supposons que $h(x) = x^u(1 + x^{\frac{q-1}{4}} - x^{\frac{q-1}{2}})$ est un polynôme de permutation de $\mathbb{F}_q$, où $q \equiv 1 \bmod 4$.

Soit

$$f(x) = -x^2 + x + 1$$

alors $h(x)$ est bien de la forme $x^u f(x^{\frac{q-1}{4}})$.

Par le Théorème 3.1 de *Wan* et *Lidl*, nous avons

(i) $pgcd(u, \frac{q-1}{4}) = 1$

(ii) Pour tout $0 \leq i < 4$, $f(\omega^i) \neq 0$

(iii) Pour $0 \leq i < j < 4$, $\psi(\frac{f(\omega^i)}{f(\omega^j)}) \not\equiv u(j-i) \bmod 4$

Nous avons donc deux cas à discuter.

1er cas) : $q \equiv 1 \bmod 8$.

alors d'après la condition *(iii)* du Théorème 3.1 nous avons

$$\psi(\frac{f(\omega^i)}{f(\omega^j)}) \not\equiv u(j-i) \bmod 4 \quad \text{pour} \quad 0 \leq i < j < 4.$$

avec

$$\frac{f(\omega^i)}{f(\omega^j)} = g^e \quad \text{dans } \mathbb{F}_q \text{ où } \quad e = Ind_g(\frac{f(\omega^i)}{f(\omega^j)})$$

Ainsi en prenant toutes les valeurs possibles pour i et j telles que $0 \leq i < j < 4$, et en utilisant les formules de la somme et du produit des racines $n-$ième de l'unité

$$\sum_{k=0}^{n-1} \omega_k = 0 \qquad \text{et} \quad (-1)^{n-1} \prod_{k=0}^{n-1} \omega_k = 1 \tag{4.1}$$

nous aurons,

- Si $i = 0$ et $j = 1$,

  $$\frac{f(1)}{f(\omega)} = \frac{1}{2+\omega} = g^e \;\Rightarrow\; (2+\omega)^{\frac{q-1}{4}} \omega^e = 1$$

  La condition *(iii)* implique que $e \not\equiv u \bmod 4$. Et la condition $pgcd(u, \frac{q-1}{4}) = 1$ implique que u est impair.

- Si $i = 0, j = 2$,

  $$\frac{f(1)}{f(\omega^2)} = -1 = g^e \;\Rightarrow\; (-1)^{\frac{q-1}{4}} = \omega^e \;\Rightarrow\; \omega^e = 1,$$

  En conséquence, $e \equiv 0 \bmod 4$. La condition *(iii)* implique que $e \not\equiv 2u \bmod 4$, et cela veut encore dire que u est impair

- Si $i = 0, j = 3$,

  $$\frac{f(1)}{f(\omega^3)} = \frac{1}{2-\omega} = g^e \;\Rightarrow\; (2-\omega)^{\frac{q-1}{4}} \omega^e = 1$$

  La condition *(iii)* implique que $e \not\equiv 3u \bmod 4$.

- Si $i = 1, j = 2$,

  $$\frac{f(\omega)}{f(\omega^2)} = -(2+\omega) = g^e \;\Rightarrow\; (2+\omega)^{\frac{q-1}{4}} = \omega^e$$

  La condition *(iii)* implique que $e \not\equiv u \bmod 4$

- Si $i = 1, j = 3$,

  $$\frac{f(\omega)}{f(\omega^3)} = \frac{2+\omega}{2-\omega} = g^e \;\Rightarrow\; (2+\omega)^{\frac{q-1}{4}} = (2-\omega)^{\frac{q-1}{4}} \omega^e$$

  La condition *(iii)* implique que $e \not\equiv 2u \bmod 4$

- Si $i = 2, j = 3$,

$$\frac{f(\omega^2)}{f(\omega^3)} = (2-\omega) = g^e \;\Rightarrow\; (2-\omega)^{\frac{q-1}{4}} = \omega^e$$

La condition *(iii)* implique que $e \not\equiv u \bmod 4$.

Dans tous les cas possibles, nous avons u impair alors

$$u \equiv 1 \bmod 4, \text{ ou bien } \; u \equiv 3 \bmod 4$$

Si $u \equiv 1 \bmod 4$, les résultats seront les suivants

$$\begin{cases} (2+\omega)^{\frac{q-1}{4}}\omega^e = 1 \\ e \not\equiv u \bmod 4 \end{cases} \quad \Rightarrow \quad (2+\omega)^{\frac{q-1}{4}} \neq \omega^3 \tag{4.2}$$

et

$$\begin{cases} (2+\omega)^{\frac{q-1}{4}} = \omega^e \\ e \not\equiv u \bmod 4 \end{cases} \quad \Rightarrow \quad (2+\omega)^{\frac{q-1}{4}} \neq \omega \tag{4.3}$$

Ainsi,

$$(2+\omega)^{\frac{q-1}{4}} = \pm 1$$

Si $u \equiv 3 \bmod 4$, les systèmes (4.2) et (4.3) impliquent que

$$(2+\omega)^{\frac{q-1}{4}} = \pm 1$$

2ème cas) : $q \not\equiv 1 \bmod 8$.

Nous avons donc d'après la condition *(iii)* du Théorème 3.1

$$\psi(\frac{f(\omega^i)}{f(\omega^j)}) \not\equiv u(j-i) \bmod 4 \;\text{ pour }\; 0 \leq i < j < 4.$$

avec

$$\tfrac{f(\omega^i)}{f(\omega^j)} = g^e \quad \text{dans } \mathbb{F}_q \text{ où } \quad e = Ind_g(\tfrac{f(\omega^i)}{f(\omega^j)})$$

Ainsi, en faisant varier les valeurs i et j telles que $0 \leq i < j < 4$, et en utilisant les formules (4.1), nous aurons

- Pour $i=0,\ j=1$ on a : $\begin{cases} (2+\omega)^{\frac{q-1}{4}}\omega^e = 1 \\ e \not\equiv u \bmod 4 \end{cases}$
- Pour $i=0,\ j=2$ on a : $\begin{cases} \omega^e = 1 \text{ i.e } e \equiv 0 \bmod 4 \\ e \not\equiv 2u \bmod 4 \end{cases}$
- Pour $i=0,\ j=3$ on a : $\begin{cases} (2-\omega)^{\frac{q-1}{4}}\omega^e = 1 \\ e \not\equiv 3u \bmod 4 \end{cases}$
- Pour $i=1,\ j=2$ on a : $\begin{cases} (2+\omega)^{\frac{q-1}{4}} = \omega^e \\ e \not\equiv u \bmod 4 \end{cases}$
- Pour $i=1,\ j=3$ on a : $\begin{cases} (2+\omega)^{\frac{q-1}{4}} = (2-\omega)^{\frac{q-1}{4}}\omega^e \\ e \not\equiv 2u \bmod 4 \end{cases}$
- Pour $i=2,\ j=3$ on a : $\begin{cases} (2-\omega)^{\frac{q-1}{4}} = \omega^e \\ e \not\equiv u \bmod 4 \end{cases}$

Sachant que le $pgcd(u, \frac{q-1}{4}) = 1$, alors tous les cas ci-dessus impliquent que l'entier u est pair. Dans ce cas

$$u \equiv 0 \bmod 4 \quad \text{ou bien } u \equiv 2 \bmod 4$$

Si $u \equiv 0 \bmod 4$, les résultats seront

$$\begin{cases} (2+\omega)^{\frac{q-1}{4}}\omega^e = 1 \\ e \not\equiv u \bmod 4 \end{cases} \quad \Rightarrow \quad (2+\omega)^{\frac{q-1}{4}} \neq 1 \tag{4.4}$$

et

$$\begin{cases} (2+\omega)^{\frac{q-1}{4}} = \omega^e \\ e \not\equiv u \bmod 4 \end{cases} \quad \Rightarrow \quad (2+\omega)^{\frac{q-1}{4}} \neq 1 \tag{4.5}$$

Et si $u \equiv 2 \bmod 4$, nous aurons $(2+\omega)^{\frac{q-1}{4}} \neq \omega^2 = -1$

Ce qui implique que

$$(2+\omega)^{\frac{q-1}{4}} \neq \pm 1.$$

Réciproquement, supposons que la condition (1) du Théorème 4.1 est satisfaite. Alors la condition *(i)* du Théorème 3.1 l'est également.

Vérifions la condition *(ii)* du Théorème 3.1

— $f(\omega^0 = 1) = 1 \neq 0$

— $f(\omega^1) = 1 + \omega - \omega^2 = 2 + \omega \neq 0$ parce que $p \neq 5$

— $f(\omega^2) = 1 + \omega^2 - \omega^4 = -1 \neq 0$

— $f(\omega^3) = 1 + \omega^3 - \omega^6 = 2 - \omega \neq 0$ parce que $p \neq 5$

Alors $f(\omega^i) \neq 0$ pour chaque i tel que $0 \leq i < 4$.

Vérifions la condition *(iii)* du Théorème 3.1. Selon les cas des entiers i et j tels que $0 \leq i < j < 4$,

- Pour $i = 0, j = 1$,

$$\frac{f(1)}{f(\omega)} = \frac{1}{2+\omega} = g^e \quad \Rightarrow \quad (2+\omega)^{\frac{q-1}{4}}\omega^e = 1.$$

  Nous avons $(2+\omega)^{\frac{q-1}{4}} = \pm 1$, ce qui implique que e est pair. Mais u est impair, alors $e \not\equiv u \bmod 4$.

- Pour $i = 0, j = 2$,

$$\frac{f(1)}{f(\omega^2)} = \frac{1}{1+\omega^2-\omega^4} = -1 = g^e \quad \Rightarrow \quad (-1)^{\frac{q-1}{4}} = 1 = \omega^e$$

  En conséquence $e \equiv 0 \bmod 4$. Alors $e \not\equiv 2u \bmod 4$ puisque u est impair.

- Pour $i = 0, j = 3$,

$$\frac{f(1)}{f(\omega^3)} = \frac{1}{1+\omega^3-\omega^6} = \frac{1}{2-\omega} = g^e \quad \Rightarrow \quad (2-\omega)^{\frac{q-1}{4}}\omega^e = 1$$

  Nous avons $(2+\omega)^{\frac{q-1}{4}} = \pm 1$, conduisant à $(2-\omega)^{\frac{q-1}{4}} = \pm 1$. Par suite $\omega^e = \pm 1$, alors, e est pair. Par conséquent $e \not\equiv 3u \bmod 4$.

- Pour $i = 1, j = 2$,

$$\frac{f(\omega)}{f(\omega^2)} = \frac{1+\omega-\omega^2}{1+\omega^2-\omega^4} = -(2+\omega) = g^e \quad \Rightarrow \quad (2+\omega)^{\frac{q-1}{4}} = \omega^e$$

  Et comme $(2+\omega)^{\frac{q-1}{4}} = \pm 1$, alors $\omega^e = \pm 1 \Rightarrow e$ est pair. Par conséquent $e \not\equiv u \bmod 4$

- Pour $i = 1, j = 3$,

$$\frac{f(\omega)}{f(\omega^3)} = \frac{1+\omega-\omega^2}{1+\omega^3-\omega^6} = \frac{2+\omega}{2-\omega} = g^e,$$

implique que

$$(2+\omega)^{\frac{q-1}{4}} = (2-\omega)^{\frac{q-1}{4}}\omega^e$$

donc $\omega^e = 1$. Ainsi $e \equiv 0 \bmod 4$. En conséquence $e \not\equiv 2u \mod 4$

- Pour $i = 2, j = 3$, alors l'égalité

$$\frac{f(\omega^2)}{f(\omega^3)} = \frac{1+\omega^2-\omega^4}{1+\omega^3-\omega^6} = \frac{-1}{2-\omega} = g^e$$

implique que

$$(-1)^{\frac{q-1}{4}} = (2-\omega)^{\frac{q-1}{4}}\omega^e,$$

i.e $(2-\omega)^{\frac{q-1}{4}}\omega^e = 1$. Mais comme $(2-\omega)^{\frac{q-1}{4}} = \pm 1$, alors $\omega^e = \pm 1$. Ce qui implique que e est pair. Ainsi, $e \not\equiv u \bmod 4$

Nous constatons alors que $e \not\equiv u(j-i) \bmod 4$ pour $0 \leq i < j < 4$. Ce qui veut dire d'après le théorème de *Wan* et *Lidl* que h est un polynôme de permutation de $\mathbb{F}_q$.

Supposons maintenant que la condition (2) du théorème est satisfaite. Nous avons donc $pgcd(u, \frac{q-1}{4}) = 1$. Il reste à vérifier les conditions *(ii)* et *(iii)* du Théorème 3.1. En effet, comme $p \neq 5$, nous avons

- $f(\omega^0) = 1 \neq 0$
- $f(\omega^1) = 1+\omega-\omega^2 = 2+\omega \neq 0$
- $f(\omega^2) = 1+\omega^2-\omega^4 = -1 \neq 0$
- $f(\omega^3) = 1+\omega^3-\omega^6 = 2-\omega \neq 0$

Alors $f(\omega^i) \neq 0$ pour tout i avec $0 \leq i < 4$.

Vérifions la condition *(iii)* i.e

$$\psi(\frac{f(\omega^i)}{f(\omega^j)}) \neq u(j-i) \bmod 4 \quad \text{pour } 0 \leq i < j < 4$$

- Pour $i = 0, j = 1$. Nous obtenons $(2+\omega)^{\frac{q-1}{4}}\omega^e = 1$. Et comme $(2+\omega)^{\frac{q-1}{4}} = \pm\omega$ alors $\omega^e = \pm\omega$. Ce qui implique que e est impair. Mais u est pair, alors $e \not\equiv u \bmod 4$.

- Pour $i = 0,\ j = 2.$ nous aurons $(-1)^{\frac{q-1}{4}} = -1 = \omega^e$ ce qui implique que $e \equiv 2 \bmod 4$. Alors $e \not\equiv 2u \bmod 4$ puisque u est pair.
- Pour $i = 0,\ j = 3$. L'égalité sers $(2-\omega)^{\frac{q-1}{4}}\omega^e = 1$. Or nous avons $(2+\omega)^{\frac{q-1}{4}} = \pm\omega$, ce qui conduit à $(2-\omega)^{\frac{q-1}{4}} = \pm\omega$, impliquant que e est impair. Par conséquent $e \not\equiv 3u \bmod 4$
- Pour $i = 1,\ j = 2$. L'égalité est

$$-(2+w) = g^e \Rightarrow (-1)^{\frac{q-1}{4}}(2+w)^{\frac{q-1}{4}} = w^e \Rightarrow -(2+w)^{\frac{q-1}{4}} = w^e.$$

  Et comme $(2+w)^{\frac{q-1}{4}} = \pm w$ alors $w^e = \pm w$ ce qui implique que e est impair. Alors $e \not\equiv u \bmod 4$ puisque u est pair.
- Pour $i = 1,\ j = 3.$ nous aurons $(2+w)^{\frac{q-1}{4}} = (2-w)^{\frac{q-1}{4}}w^e$. Et comme $(2+w)^{\frac{q-1}{4}} = \pm w$ et $(2-w)^{\frac{q-1}{4}} = \pm w$, alors $w^e = -1$ ce qui implique $e \equiv 2 \bmod 4$. Et comme u est pair, alors $2u \equiv 0 \bmod 4$. Ainsi $e \not\equiv 2u \bmod 4$.
- Pour $i = 2,\ j = 3$. Nous obtenons $\frac{-1}{2-w} = g^e \Rightarrow (-1)^{\frac{q-1}{4}} = (2-w)^{\frac{q-1}{4}}w^e = -1$. Et comme $(2+w)^{\frac{q-1}{4}} = \pm w$, alors e est impair ce qui donne $e \not\equiv u \bmod 4$ puisque u est pair.

Nous constatons que dans tous les cas possibles pour i et j

$$e \not\equiv u(j-i) \bmod 4$$

Ainsi le théorème est démontré.

Ayad et *Kihel* [5] ont montré ci dessus le Théorème 3.3.
Nous allons généraliser ce dernier et montrer le suivant ;

Théorème 4.2 *Soit p un nombre premier, et $q = p^r$ où r est un entier positif tel que $q \equiv 1 \mod 4$. Soit $h(x) = x^u(x^{\frac{q-1}{2}} + x^{\frac{q-1}{4}} + 1)$ un polynôme sur $\mathbb{F}_q$. Alors h est un polynôme de permutation de $\mathbb{F}_q$, si et seulement si une des conditions suivantes est satisfaite.*

(1) $q \equiv 1 \mod 8$, $pgcd(u, \frac{q-1}{4}) = 1$ *et* $3^{\frac{q-1}{4}} \equiv 1 \pmod p$.

(2) $q \not\equiv 1 \mod 8$, $pgcd(u, \frac{q-1}{4}) = 1$, u *pair et* $3^{\frac{q-1}{4}} \equiv -1 \pmod p$.

Preuve : Supposons que $q \equiv 1 \mod 8$, $f(x) = x^2 + x + 1$, et $s = \frac{q-1}{4}$. Alors

$$h(x) = x^u f(x^s).$$

Si $h(x)$ est un polynôme de permutation sur $\mathbb{F}_q$, alors la condition *(iii)* du Théorème 3.1 est bien satisfaite i.e :

$$Ind_g \frac{f(\omega^i)}{f(\omega^j)} \not\equiv u(j-i) \mod 4, \quad \text{pour} \quad 0 \leq i < j < 4$$

Soit $\frac{f(\omega^i)}{f(\omega^j)} = g^e$, les résultats pour les différentes valeurs de i et de j seront les suivants.

- Si $i = 0$, $j = 1$,

$$\frac{f(1)}{f(w)} = \frac{3}{w^2 + w + 1} = \frac{3}{w} = g^e \Rightarrow \left(\frac{3}{w}\right)^{\frac{q-1}{4}} = (g^e)^{\frac{q-1}{4}}$$

  Alors $3^{\frac{q-1}{4}} = w^{\frac{q-1}{4}} w^e$, ce qui donne,

$$3^{\frac{q-1}{4}} = \begin{cases} w^e & \text{si } q \equiv 1 \bmod 16 \\ -w^e & \text{si } q \not\equiv 1 \bmod 16 \end{cases} \quad \text{avec} \quad e \not\equiv u \bmod 4 \tag{4.6}$$

- Si $i = 0$, $j = 2$,

$$\frac{f(1)}{f(\omega^2)} = \frac{3}{w^4 + w^2 + 1} = 3 = g^e$$

  Il en résulte

$$3^{\frac{q-1}{4}} = (g^e)^{\frac{q-1}{4}} = w^e, \quad \text{avec } e \not\equiv 2u \bmod 4.$$

- Si $i = 0$, $j = 3$,

$$\frac{f(1)}{f(\omega^3)} = \frac{3}{w^6 + w^3 + 1} = \frac{3}{w^3} = \frac{-3}{w} = g^e$$

  Ce qui implique que $(-3)^{\frac{q-1}{4}} = w^{\frac{q-1}{4}} w^e$. Ainsi

$$3^{\frac{q-1}{4}} = \begin{cases} w^e & \text{si } q \equiv 1 \bmod 16 \\ -w^e & \text{si } q \not\equiv 1 \bmod 16 \end{cases} \quad \text{avec} \quad e \not\equiv 3u \bmod 4 \tag{4.7}$$

Nous obtenons les résultats suivants

$$3^{\frac{q-1}{4}} = \begin{cases} w^e & \text{si } q \equiv 1 \bmod 16 \\ -w^e & \text{si } q \not\equiv 1 \bmod 16 \end{cases} \quad \text{avec} \quad \begin{cases} e \not\equiv u \bmod 4 \\ \text{et} \\ e \not\equiv 3u \bmod 4 \end{cases} \tag{4.8}$$

Et $3^{\frac{q-1}{4}} = w^e$ avec $e \not\equiv 2u \bmod 4$.

Nous savons déja que $pgcd(u, \frac{q-1}{4}) = 1$, ce qui implique que u est impair et $\frac{q-1}{4}$ est pair. Et d'après les résultats ci dessus $e \not\equiv ku \bmod 4$ pour $k = 1, 2, 3$, alors e est pair avec $e \not\equiv 2 \bmod 4$. Impliquant que $3^{\frac{q-1}{4}} = w^e \not\equiv -1 \pmod p$ et $3^{\frac{q-1}{4}} \equiv \pm 1 \pmod p \Rightarrow 3^{\frac{q-1}{4}} \equiv 1 \pmod p$.

Réciproquement, supposons que la condition (1) du théorème est satisfaite i.e $q \equiv 1 \mod 8$, $pgcd(u, \frac{q-1}{4}) = 1$ et $3^{\frac{q-1}{4}} \equiv 1 \pmod p$.
Si $pgcd(u, \frac{q-1}{4}) = 1$, alors $pgcd(u, q-1) = 1$. Il découle que

$$3^{\frac{q-1}{4}} = \begin{cases} \pm 1 \\ \text{ou} \\ \pm w \end{cases} \tag{4.9}$$

Mais comme $3^{\frac{q-1}{4}} \equiv 1 \pmod p$, alors le Théorème 3.3 implique que le polynôme $h(x) = x^u(x^{\frac{q-1}{2}} + x^{\frac{q-1}{4}} + 1)$ permute $\mathbb{F}_q$.

Supposons maintenant que $q \not\equiv 1 \bmod 8$, démontrons alors que le polynôme $h(x) = x^u(x^{\frac{q-1}{2}} + x^{\frac{q-1}{4}} + 1)$ permute $\mathbb{F}_q$ si et seulement si $pgcd(u, \frac{q-1}{4}) = 1$, u est pair, et $3^{\frac{q-1}{4}} \equiv -1 \pmod p$.

Si $q \not\equiv 1 \mod 8$ alors $q \equiv 5 \mod 8$. Ainsi,

$$\frac{q-1}{4} \equiv \begin{cases} 1 \mod 4 \\ \text{ou} \\ 3 \mod 4. \end{cases}$$

Nous avons donc deux cas à distinguer :

1er cas) : Si $\frac{q-1}{4} \equiv 1 \mod 4$,

Si h est polynôme de permutation alors d'après le théorème *Wan* et *Lidl*, la condition suivante est vérifiée

$$Ind_g \frac{f(\omega^i)}{f(\omega^j)} \not\equiv u(j-i) \mod 4, \quad \text{pour} \quad 0 \leq i < j < 4$$

- Si $i = 1$ et $j = 2$,

$$\frac{f(w)}{f(w^2)} = \frac{w^2+w+1}{w^4+w^2+1} = w = g^e \quad \Rightarrow \quad w^{\frac{q-1}{4}} = w^e$$

  Ce qui implique que $e \equiv \frac{q-1}{4} \mod 4$. Alors d'après la condition *(iii)* du Théorème 3.1 $u \not\equiv 1 \mod 4$

- Si $i = 1$ et $j = 3$,

$$\frac{f(w)}{f(w^3)} = \frac{w^2+w+1}{w^6+w^3+1} = \frac{w}{w^3} = w^2 = g^e \quad \Rightarrow \quad (-1)^{\frac{q-1}{4}} = w^e$$

  Ce qui implique que $e \equiv 2 \mod 4$. Alors la condition *(iii)* du Théorème 3.1 implique $e \not\equiv 2u \mod 4$

A partir de ces deux premiers cas, nous constatons que u est pair. Alors

$$u \equiv 0 \mod 4 \quad \text{ou} \quad u \equiv 2 \mod 4$$

Etudions le cas $u \equiv 2 \mod 4$,

- Si $i = 0$ et $j = 1$,

$$\frac{f(1)}{f(w)} = \frac{3}{w^2+w+1} = \frac{3}{w} = g^e.$$

Nous obtenons $3^{\frac{q-1}{4}} = w^{\frac{q-1}{4}} w^e$, i.e $3^{\frac{q-1}{4}} = w^{e+1}$. Le Théorème 3.1 *(iii)* implique que $e \not\equiv u \equiv \text{mod}4$, il en résulte $3^{\frac{q-1}{4}} \neq w^3$

- Si $i = 0$ et $j = 2$,

$$\frac{f(1)}{f(w^2)} = \frac{3}{w^4 + w^2 + 1} = 3 = g^e \quad \Rightarrow \quad 3^{\frac{q-1}{4}} = w^e$$

Le Théorème 3.1 *(iii)* implique que $e \not\equiv 2u \equiv 0 \mod 4$. Le résultat sera $3^{\frac{q-1}{4}} \neq 1 \mod 4$.

- Si $i = 0$ et $j = 3$,

$$\frac{f(1)}{f(w^3)} = \frac{3}{w^6 + w^3 + 1} = \frac{3}{w^3} = g^e \implies 3^{\frac{q-1}{4}} = -w^3 {}^{\frac{q-1}{4}} w^e$$

Voulant dire que $3^{\frac{q-1}{4}} = w^{e+3}$. Le Théorème 3.1 *(iii)* implique que $e \not\equiv 3u \equiv 2 \text{ mod } 4$. Par conséquent $3^{\frac{q-1}{4}} \neq w$.

Ainsi

$$\begin{cases} 3^{\frac{q-1}{4}} \neq w^3 \\ 3^{\frac{q-1}{4}} \neq 1 \mod 4 \\ 3^{\frac{q-1}{4}} \neq w \end{cases} \implies 3^{\frac{q-1}{4}} \equiv -1 \pmod{p}$$

Si $u \equiv 0 \mod 4$, nous avons les résultats suivants

- Si $i = 0, j = 1$,

$$\frac{f(1)}{f(w)} = \frac{3}{w^2 + w + 1} = \frac{3}{w} = g^e \implies 3^{\frac{q-1}{4}} = w^{\frac{q-1}{4}} w^e$$

Ce qui veut dire que $3^{\frac{q-1}{4}} = w^{e+1} \pmod{p}$. Le Théorème 3.1 *(iii)* implique que $e \not\equiv u \equiv 0 \mod 4$. Alors $3^{\frac{q-1}{4}} \neq w$.

- Si $i = 0$ et $j = 2$,

$$\frac{f(1)}{f(w^2)} = \frac{3}{w^4 + w^2 + 1} = 3 = g^e \implies 3^{\frac{q-1}{4}} = w^e$$

Le Théorème 3.1 *(iii)* implique que $e \not\equiv 2u \equiv 0 \mod 4$. Nous aurons comme résultat $3^{\frac{q-1}{4}} \neq 1 \mod 4$.

- Si $i = 0$ et $j = 3$,

$$\frac{f(1)}{f(w^3)} = \frac{3}{w^6 + w^3 + 1} = \frac{3}{w^3} = g^e \implies 3^{\frac{q-1}{4}} = -w^3 3^{\frac{q-1}{4}} w^e$$

Voulant dire que $3^{\frac{q-1}{4}} = w^{e+3}$. Le Théorème 3.1 *(iii)* implique que $e \not\equiv 3u \equiv 0 \bmod 4$. Alors $3^{\frac{q-1}{4}} \neq w^3$.

Ainsi

$$3^{\frac{q-1}{4}} = -1 \pmod p.$$

2ème cas) : Si $\frac{q-1}{4} \equiv 3 \mod 4$.

- Si $i = 1$ et $j = 2$,

$$\frac{f(w)}{f(w^2)} = \frac{w^2 + w + 1}{w^4 + w^2 + 1} = w = g^e \Rightarrow w^{\frac{q-1}{4}} = w^e$$

Ce qui implique que $e \equiv \frac{q-1}{4} \equiv 3 \mod 4$. Le Théorème 3.1(*iii*) implique que $u \not\equiv 3 \mod 4$.

- Si $i = 1$ et $j = 3$,

$$\frac{f(w)}{f(w^3)} = \frac{w^2 + w + 1}{w^6 + w^3 + 1} = \frac{w}{w^3} = w^2 = g^e \Rightarrow (-1)^{\frac{q-1}{4}} = w^e$$

Ce qui implique que $e \equiv 2 \mod 4$. Le Théorème 3.1(*iii*) implique que $e \not\equiv 2u \mod 4$.

Ainsi, nous avons

$$\begin{cases} u \not\equiv 1 \mod 4 \\ u \not\equiv 3 \mod 4 \end{cases} \implies u \equiv 2 \mod 4$$

- Si $i = 0$ et $j = 2$,

$$\frac{f(1)}{f(w^2)} = \frac{3}{w^4 + w^2 + 1} = 3 = g^e \Rightarrow 3^{\frac{q-1}{4}} \equiv w^e$$

Le Théorème 3.1(*iii*) implique que $e \not\equiv 2u \equiv 0 \mod 4$. Alors $3^{\frac{q-1}{4}} \not\equiv 1 \mod 4$.

- Si $i = 0$ et $j = 1$,

$$\frac{f(1)}{f(w)} = \frac{3}{w^2+w+1} = \frac{3}{w} = g^e.$$

En conséquence $3^{\frac{q-1}{4}} = w^{\frac{q-1}{4}} w^e$, i.e $3^{\frac{q-1}{4}} = w^{e+1}$. Le Théorème 3.1(iii) implique que $e \not\equiv u \equiv 2 \mod 4$. Et nous obtenons comme résultat $3^{\frac{q-1}{4}} \neq w^3$.

- Si $i = 0$ et $j = 3$,

$$\frac{f(1)}{f(w^3)} = \frac{3}{w^6+w^3+1} = \frac{3}{w^3} = g^e \implies 3^{\frac{q-1}{4}} = w^{3\frac{q-1}{4}} w^e$$

Ce qui donne $3^{\frac{q-1}{4}} = w^{e+3}$.

Le Théorème 3.1(iii) implique que $e \not\equiv 3u \equiv 2 \mod 4$ et que $3^{\frac{q-1}{4}} \neq w$.

Nous avons ainsi

$$\begin{cases} 3^{\frac{q-1}{4}} \not\equiv 1 \mod 4 \\ 3^{\frac{q-1}{4}} \neq w^3 \\ 3^{\frac{q-1}{4}} \neq w \end{cases} \implies 3^{\frac{q-1}{4}} \equiv -1 \pmod p$$

Si $u \equiv 0 \mod 4$, nous avons ci après :

- Si $i = 0$ et $j = 2$,

$$\frac{f(1)}{f(w^2)} = \frac{3}{w^4+w^2+1} = 3 = g^e \Rightarrow 3^{\frac{q-1}{4}} = w^e,$$

Le Théorème 3.1(iii) implique que $e \not\equiv 2u \equiv 0 \mod 4$. Alors $3^{\frac{q-1}{4}} \not\equiv 1 \pmod p$.

- Si $i = 0$ et $j = 1$,

$$\frac{f(1)}{f(w)} = \frac{3}{w^2+w+1} = \frac{3}{w} = g^e \implies 3^{\frac{q-1}{4}} = w^{\frac{q-1}{4}} w^e$$

Par consequent $3^{\frac{q-1}{4}} = w^{e+3}$. Le Théorème 3.1(iii) implique que $e \not\equiv u \equiv 0 \mod 4$. Donc $3^{\frac{q-1}{4}} \neq w^3$.

- Si $i = 0$ et $j = 3$,

$$\frac{f(1)}{f(w^3)} = \frac{3}{w^6+w^3+1} = \frac{3}{w^3} = g^e \implies 3^{\frac{q-1}{4}} = w^{3\frac{q-1}{4}} w^e$$

i.e $3^{\frac{q-1}{4}} = w^{e+1}$. Le Théorème 3.1($iii$) implique que $e \not\equiv 3u \equiv 0 \mod 4$. Alors $3^{\frac{q-1}{4}} \neq w$.

Ainsi, nous avons

$$3^{\frac{q-1}{4}} \equiv -1 \pmod{p}.$$

Réciproquement, supposons que $q \not\equiv 1 \mod 8$, $pgcd(u, \frac{q-1}{4}) = 1$, u est pair et $3^{\frac{q-1}{4}} \equiv -1 \pmod{p}$.

Pour prouver que $h(x)$ est un polynôme de permutation, nous avons seulement à vérifier que

— $f(w^i) \neq 0$ pour $0 \leq i < 4$, et

— $ind_g \frac{f(w^i)}{f(w^j)} \not\equiv u(j-i) \mod 4$, Pour tout $0 \leq i < j < 4$.

Nous avons $f(w^i) = w^{2i} + w^i + 1$,

$$f(w^i) = \begin{cases} 3 & \text{si } i = 0 \\ w & \text{si } i = 1 \\ 1 & \text{si } i = 2 \\ w^3 & \text{si } i = 3 \end{cases}$$

Alors $f(w^i) \neq 0$ pour tout $0 \leq i < 4$.

Et nous avons,

$$\frac{f(w^i)}{f(w^j)} = \frac{w^{2i} + w^i + 1}{w^{2j} + w^j + 1}.$$

- Si $i = 0$ et $j = 1$,

$$\frac{f(1)}{f(w)} = \frac{3}{w} = g^e \text{ où } e = Ind_g(\frac{1}{w})$$

Alors,

$$3^{\frac{q-1}{4}} = w^{\frac{q-1}{4}} (g^e)^{\frac{q-1}{4}} \implies 3^{\frac{q-1}{4}} = w^{\frac{q-1}{4}} w^e = -1.$$

ce qui implique $\frac{q-1}{4} + e \equiv 2 \mod 4$.

Nous avons $q \not\equiv 1 \mod 8$, alors soit $\frac{q-1}{4} \equiv 1 \mod 4$ soit $\frac{q-1}{4} \equiv 3 \mod 4$. Nous aurons alors,

$$e \equiv 2 - \frac{q-1}{4} \equiv \pm 1 \mod 4.$$

- Si $i = 0$ et $j = 2$,

$$\frac{f(1)}{f(w^2)} = \frac{3}{w^4+w^2+1} = 3 = g^e \implies 3^{\frac{q-1}{4}} = w^e$$

Et comme $3^{\frac{q-1}{4}} \equiv -1 \pmod{p}$ alors $e \equiv 2 \bmod 4 \Rightarrow e \not\equiv 2u \equiv 0 \mod 4$.

- Si $i = 0$ et $j = 3$,

$$\frac{f(1)}{f(w^3)} = \frac{3}{w^6+w^3+1} = \frac{-3}{w} = g^e.$$

Nous obtenons $3^{\frac{q-1}{4}} = -w^{\frac{q-1}{4}}w^e$ impliquant $w^{\frac{q-1}{4}}w^e = 1$. Nous aurons donc

$$e + \frac{q-1}{4} \equiv 0 \bmod 4 \Leftrightarrow e \equiv 3 \bmod 4 \text{ ou } e \equiv 1 \bmod 4$$

alors $e \not\equiv 3u \bmod 4$ puisque u est pair.

- Si $i = 1$ et $j = 2$,

$$\frac{f(w)}{f(w^2)} = \frac{w^2+w+1}{w^4+w^2+1} = w = g^e \implies w^{\frac{q-1}{4}} = w^e$$

ceci implique que $e \equiv \frac{q-1}{4} \mod 4$. Mais comme u est pair alors $u \not\equiv 1 \mod 4$ et $e \not\equiv u \mod 4$.

- Si $i = 1$ et $j = 3$,

$$\frac{f(w)}{f(w^3)} = \frac{w^2+w+1}{w^6+w^3+1} = \frac{w}{w^3} = w^2 = g^e \implies (-1)^{\frac{q-1}{4}} = w^e$$

impliquant $e \equiv 2 \mod 4$. Alors $e \not\equiv 2u \mod 4$ puisque u est pair.

- Si $i = 2$ et $j = 3$,

$$\frac{f(w^2)}{f(w^3)} = \frac{w^4+w^2+1}{w^6+w^3+1} = \frac{1}{w} = g^e \implies w^{\frac{q-1}{4}}w^e = 1$$

obtenant $e + \frac{q-1}{4} \equiv 0 \bmod 4 \Leftrightarrow e \equiv 3$ ou à $1 \bmod 4$. Alors $e \not\equiv u$ puisque u est supposé pair.

Ainsi toutes les conditions du théorème de *Wan* et *Lidl* sont vérifiées, alors h est bien un polynôme de permutation. Et le théorème est prouvé.□

Chapitre 5

Equations Diophantiennes

5.1 Introduction

La recherche d'une méthode permettant de trouver explicitement les solutions d'une équation diophantienne représente le dixième problème de *Hilbert*. En 1970, *Yu. Matiiassevitch* a répondu à ce problème et a démontré l'impossibilité de trouver un algorithme permettant de résoudre toutes les équations diophantiennes. Ce théorème ferme la porte à une étude des équations diophantiennes en toute généralité, mais laisse la possibilité d'une étude spécifique à chaque situation.
Dans ce chapitre, nous étudions un problème diophantien relatif à l'équation de *Lucas*. Nous présentons une méthode algorithmique, permettant de trouver toutes les solutions possibles de l'équation pyramidale carrée de *Lucas*. La méthode que nous avons développé, nous a d'ores et déja, permis de traiter les cas $1 < n \leq 300$.

5.2 Sur une variante de l'équation pyramidale carrée de *Lucas*

Le problème de recherche d'entiers k tels que la somme des k carrés consécutifs représente un carré a été initié par *Lucas* [18], qui a formulé le problème comme suit :

quand est ce qu'une pyramide carrée de boulets de canon contient-elle un nombre de ces boulets, qui soit un carré parfait ? Ceci est équivalent à l'équation diophantienne suivante

$$1^2 + 2^2 + 3^2 + ... + k^2 = y^2. \tag{5.1}$$

Ce ne fut qu'en 1918 qu'une solution complète du problème de *Lucas* été donné par *Watson* [29] qui a montré que l'équation 5.1 possède seulement deux solutions, à savoir $(k, y) = (1, 1)$ et $(24, 70)$.

Il est naturel de se demander si ce phénomène continue à se produire lorsque le carré initial est shifté. Ceci est en fait equivalent à la résolution de l'équation diophantienne suivante :

$$n^2 + (n+1)^2 + ... + (n+k-1)^2 = y^2 \tag{5.2}$$

Ce problème a été considéré par de nombreux auteurs de différents points de vue. Par exemple, *Beeckmans* [6] a déterminé toutes les valeurs $1 \leq k \leq 1000$ pour lesquelles l'équation 5.2 admet des solutions (n, y). En utilisant la théorie des courbes élliptiques, *Bremner et al* [9] ont trouvé toutes les solutions (k, y) de l'équation 5.2 quand $1 < n \leq 100$. *Stroeker* [23] considérait la question suivante : quand est ce que la somme de k cubes consécutifs en commençant par n^3 est égale un carré parfait ? Ce dernier a considéré le cas ou k est un entier fixé.

Dans ce travail, nous fixons un entier $n > 1$ et nous considérons la question précitée. Nous donnons par le Théorème 5.1 une borne supèrieure à l'entier k en fonction de n, puis nous utilisons cette borne pour faire quelques calculs et ainsi nous listons tous les k possible quand $1 \leq n \leq 300$. Notre méthode s'appuie sur des techniques élémentaires. Soit l'équation diophantienne suivante :

$$n^3 + (n+1)^3 + (n+2)^3 + ... + (n+k-1)^3 = y^2. \tag{5.3}$$

Ce problème est intéressant seulement quand n est supèrieur à 1.

En effet, lorsque $n = 1$, à cause de l'égalité bien connue

$$1^3 + 2^3 + ... + k^3 = \Big(\frac{k(k+1)}{2}\Big)^2 \tag{5.4}$$

l'équation 5.3 est toujours vraie pour n'importe quelle valeur de l'entier k.

Lorsque $n > 1$, *Stroeker* [23] a résolu l'équation 5.3 pour $2 \leq k \leq 50$ et pour $k = 98$.

Ainsi donc, nous prouvons,

Théorème 5.1 *Si $n > 1$ est un entier fixé, il existe seulement un nombre fini de k tel que la somme des k cubes consécutifs à partir de n^3 est un carré parfait. De plus $k \leq \lfloor \frac{n^2}{\sqrt{2}} - n + 1 \rfloor$*

Preuve :

L'égalité $1^3 + 2^3 + 3^3 + ... + (n-1)^3 = \left(\frac{(n-1)n}{2}\right)^2$ donne

$$n^3 + (n+1)^3 + ... + (n+k-1)^3 = \left(\frac{(n+k)(n+k-1)}{2}\right)^2 - \left(\frac{n(n-1)}{2}\right)^2$$

par conséquent l'équation 5.3 donne

$$\left(\frac{(n+k)(n+k-1)}{2}\right)^2 - \left(\frac{n(n-1)}{2}\right)^2 = y^2$$

Il est bien connu que les solutions positives de cette équation sont données par

$$\begin{cases} \frac{(n+k)(n+k-1)}{2} = \alpha(a^2+b^2) \\ \frac{n(n-1)}{2} = \alpha(a^2-b^2) \qquad \alpha \in \mathbb{N} \\ y = \alpha(2ab), \end{cases} \tag{5.5}$$

ou

$$\begin{cases} \frac{(n+k)(n+k-1)}{2} = \alpha(a^2+b^2) \\ \frac{n(n-1)}{2} = \alpha(2ab) \qquad \alpha \in \mathbb{N} \\ y = \alpha(a^2-b^2), \end{cases} \tag{5.6}$$

où $a, b \in \mathbb{N}$, avec $pgcd(a,b) = 1$, $a > b$ et $a \not\equiv b(\mod 2)$.

La première équation du système 5.5 implique que

$$(n+k-1)^2 < 2\alpha(a^2+b^2). \tag{5.7}$$

La seconde équation du même système implique que

$$\frac{n^2}{2} > \frac{n(n-1)}{2} = \alpha(a^2-b^2) \geq \alpha(a+b)$$

et donc

$$\Big(\frac{n^2}{2}\Big)^2 > (\alpha(a+b))^2 \geq \alpha(a^2+b^2). \tag{5.8}$$

Nous obtenanons par les inégalités 5.7 et 5.8 le suivant

$$(n+k-1)^2 < 2\alpha(a^2+b^2) \leq 2\Big(\frac{n^2}{2}\Big)^2$$

par conséquent nous obtenons l'inégalité

$$n+k-1 \leq \frac{n^2}{\sqrt{2}}$$

impliquant que,

$$k \leq \frac{n^2}{\sqrt{2}} - n + 1$$

La seconde équation du système 5.6 implique que,

$$\frac{n(n-1)}{2} = 2\alpha(ab)$$

alors

$$\frac{n^2}{4} > \alpha ab$$

En rassemblant la première et la dernière équation du système 5.6, nous obtenons

$$2\Big(\frac{n^2}{4}\Big)^2 > 2\alpha^2 a^2 b^2 > \alpha(a^2+b^2) > \Big(\frac{n+k-1}{2}\Big)^2$$

ce qui implique que,

$$k \leq \frac{n^2}{\sqrt{2}} - n + 1.$$

Dans les deux situations possibles, nous nous sommes conduit à la même majoration de l'entier k ainsi

$$k \leq \lfloor \frac{n^2}{\sqrt{2}} - n + 1 \rfloor$$

5.2.1 Quelques calculs

En se reposant sur le Théorème 5.1, nous écrivons un programme sur MAPLE et nous obtenons les solutions de l'équation 5.3 pour $1 < n \leq 300$. Les solutions trouvées sont listées dans le Tableau suivant

n	k	y^2
4	1	64
9	1	729
	17	104329
14	12	97344
	21	345744
16	1	4096
21	128	121528576
23	3	41616
25	1	15625
	5	99225
	15	518400
	98	56205009
28	8	254016
33	33	4322241
36	1	46656
49	1	117649
	291	3319833924
64	1	262144
	42	26904969
	48	34574400
69	32	19998784
78	105	268304400
81	1	531441
	28	24147396
	69	114383025
	644	68869504900
88	203	1765764441
96	5	4708900
97	98	336098889
100	1	1000000
105	64	171714816
111	39	87609600
118	5	8643600
	60	200505600

n	k	y^2
120	17	35808256
	722	125308212121
121	1	1771561
	1205	771665618025
133	32	106007616
144	1	2985984
	13	43956900
	21	77053284
	77	484968484
	82	540423009
	175	2466612225
	246	5647973409
153	18	76055841
	305	10817040025
165	287	10205848576
168	243	6902120241
169	1	4826809
	2022	5755695204609
176	45	353816100
	195	4473603225
189	423	34640654400
196	1	7529536
216	98	1875669481
	784	248961081600
217	63	976437505
	242	10499076225
	434	44214734529
221	936	446630236416
225	1	11390625
	35	498628900
	280	15560067600
	3143	32148582480784
232	87	1854594225
	175	6108204025
256	1	16777216
	169	7052640400
	336	29537234496

n	k	y^2
	1190	1090405850625
265	54	1349019441
	2209	9356875327801
289	1	24137569
	4616	144648440352144
295	76	2830240000
298	560	133210400400

TABLE 5.1 – Solutions de l'équation pyramidale carrée de *Lucas* pour $1 < n \leq 300$

Soit $C_n = |\{(k, y)$ solutions de l'équation 5.3$\}|$, où $|.|$ représente le cardinal de l'ensemble C_n, nous remarquons à partir du Théorème 5.1, que pour tout n, l'ensemble C_n est fini, et à partir du Tableau 5.1, que pour $1 \leq n \leq 300$, $C_n \leq 7$. Les valeurs manquantes de l'entier n sans celles pour lesquelles les solutions n'exitent pas.

Conclusion

Les outils mathématiques concernant les corps finis, et leurs notions relationnelles nous ont permis d'assoir les éléments de base pour aborder nos travaux.

Il s'ensuit une définition formelle des polynômes de permutation et des critères pour tester qu'un polynôme induit une permutation sur un corps fini, tel que défini dans les différentes classes des polynômes précitées.

L'intêret particulier accordé aux polynômes de la forme $x^r f(x^{(q-1)/d})$, où $r \geq 1$, $d \geq 1$ et d est un diviseur de $q-1$, ainsi que les travaux de *Ayad* et *Kihel*, qui ont établi des conditions suffisantes sur les entiers u et q relatifs aux polynômes $h(x) = x^u(1 + x^{\frac{q-1}{4}} + x^{\frac{q-1}{2}})$; nous ont permis d'aborder le contenu de nos travaux qui se réfèrent particulièrement aux polynômes de la forme $h(x) = x^u(1 \pm x^{\frac{q-1}{4}} \pm x^{\frac{q-1}{2}})$, sur la base de l'application du théorème de *Wan* et *Lidl*.

Considérer les permutations sous une forme polynomiale permet de représenter de façon simple et surtout concise des permutations complexes des éléments d'un corps fini.

Cette représentation a été utilisée par exemple pour définir des systèmes de chiffrement à clé publique ; comme il suit :

Soient p et q deux nombres premiers. Notons $N = pq$ leur produit et choisissons e un nombre premier avec $\varphi(N) = (p-1)(q-1)$. et $d = e^{-1} \pmod{\varphi(N)}$. Le couple (N, e) va constituer la clé publique, et d est la clé privée.

Le chiffrement est alors simplement défini par

$$c = m^e \pmod{N};$$

et le déchiffrment par

$$m = c^d \pmod{N}.$$

Le polynôme de permutation intervenant est donc le polynôme $X^e \in (\mathbb{Z}/N\mathbb{Z})[X]$. Il possède les propriétés suivantes :

— Spécification efficace

— Evaluation efficace

— Inversion difficile.

Il est également très courant de voir intervenir des familles de polynômes de permutation en géométrie, précisément pour la recherche d'obtention des caractéristiques extrémales.

Comme précité, dans ce travail, nous avons présenté une nouvelle famille de polynômes de permutation de la forme $h(x) = x^u(1 \pm x^{\frac{q-1}{4}} \pm x^{\frac{q-1}{2}})$, trés adaptée aux besoins de l'informatique.

L'étude de ces derniers est donnée par les Théorèmes 4.1 et Théorème 3.3. En effectuant un changement de variable $x \to -x$ dans l'expression $h(x)$ du Théorème 4.1 et le Théorème 4.2, nous obtenons toutes les possibilités pour $h(x)$. Leurs démonstrations reposent en grande partie sur l'application du théorème de *Wan* et *Lidl*, puisqu'il est bien question des polynômes du type $x^r f(x^{(q-1)/d})$, où $r \geq 1,\ d \geq 1$ et d est un diviseur de $q-1$.

Les résultats que nous avons developpé sont valables pour toute valeur de p premier, sauf pour $p = 5$. Il s'agit d'une condition nécessaire du Théorème 4.1. En effet si $p = 5$ dans le Théorème 4.1, nous aurons $f(w) = 0$ ou $f(w^3) = 0$. Traduisant qu'une condition du critère de *Wan* et *Lidl* n'est pas satisfaite, impliquant que $h(x)$ n'est pas un polynôme de permutation de $\mathbb{F}_q$.

Il est à mentionner que les corps constitués d'un grand nombre d'éléments ou d'expressions polynomiales complexes, ne facilitent pas l'application de certains systèmes cryptographiques.

Les différentes familles d'attaques reposent sur la facilité d'acces aux propriétés de ces polynômes.

La recherche de nouvelles familles de polynômes moins complexes et plus élaborées à

caractère bijectif compliqueront d'avantage le déchiffrement du système ; selon les critères de spécificité, d'évaluation et de la difficulté d'inversion précités.

La méthode que nous avons developpé par le Theorème 5.1 nous a permis de constater la finitude du nombre de solutions de l'équation pyramidale carré de *Lucas*, et ce en majorant l'entier k.

En règle générale, et pour un entier n très grand, on obtient systématiquement des majorations très grandes qui laissent un nombre très élevé de cas à traiter, rendant impossible l'énumération de tous les cas possibles. Il est donc intéréssant de voir s'il existe une constante C telle que le cardinal de l'ensemble des solutions de l'équation pyramidale carré de *Lucas*, soit majorée par C i.e

$$C_n \leq C, \quad \forall n \text{ entier.}$$

Table des figures

Liste des tableaux

Bibliographie

[1] A. Akbaray and Q. Wang. On polynomials of the form $x^r f(x^{(q-1)/l})$. *International Journal of Mathematics and Mathematical sciences*, 2007(ID 23408) :7 pages, October 2007.

[2] S. Akhtari. The diophantine equation $ax^4 - by^2 = 1$. *J. Reine Angew. Math*, 630 :33–57, 2009.

[3] M. Ayad, K. Belghaba, and O. Kihel. On permutation binomials over finite fields. *Bulletin of the Australian Mathematical Society*, 89 :112–124, 2014.

[4] M. Ayad, K. Belghaba, and O. Kihel. On permutation binomials. *To appear in Rocky Mountain Journal of Mathematics*, 19 March 2015.

[5] M. Ayad and O. Kihel. A new class of permutation polynomials of $\mathbb{F}_q$. *Elemt. Math*, 68(2) :53–55, 22 September 2013.

[6] L. Beeckmans. Squares expressible as sum of consecutive squares. *The American Mathematical Monthly*, 101(5) :437–442, 1994.

[7] K. Belghaba and S. Kebli. On a family of permutation polynomials of $\mathbb{F}_q$. *South Pacific Journal of Pure and Applied Mathematics*, 2 :17–29, November 2013.

[8] A. Blokhuis, R.S. Coulter, M. Henderson, and C.M O'Keef. Permutations amongst the dembowski-ostorm polynomials. *In Dieter Jungnickel and Harald Niederreiter, editors, Fifth International Conference on Finite Fields and Applications.*, Springer 1999.

[9] A. Bremner, R. J. Stroeker, and N. Tzanakis. On sums of consecutive squares. *journal of number theory*, 62(1) :39–70, 1997.

[10] L. Carlitz and J Lutz. A characterization of permutation polynomials over a finite field. *The American Mathematical Monthly*, 85(9) :746–748, 1978.

[11] N. Kayal. Recognizing permutation functions in polynomial time. *Electronic Colloquium on Computational Complexity*, 8, December 2005.

[12] S. Kebli and O. Kihel. On a variant of the lucas' square pyramid problem. *Annales Mathematicae et Informaticae*, 46 :245–250, 2016.

[13] Y. Laigle-Chapuy. *Polynômes de permutation et application en cryptographie*. PhD thesis, Université de Pierre et Marie Curie, Juin 2009.

[14] R. Lidl and G.L Mullen. When does a polynomial over a finite field permute the elements of the field ? *Amer. Math. Month*, 95 :243–246, 1988.

[15] R. Lidl and G.L Mullen. Cycle structure of dickson permutation polynomials. *Mathematical Journal of Okayama University*, 1(33), January 1991.

[16] R. Lidl and G.L Mullen. When does a polynomial over a finite field permute the elements of the field ? *Amer. Math. Month.*, 100 :71–74, 1993.

[17] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of Encyclopedia of Mathematics and its applications. Cambridge University Press, second edition edition, 1997.

[18] E. Lucas. Question 1180. *Nouvelles Annales de Mathématiques*, 2(14) :336, 1875.

[19] A. Masuda and M. Zieve. Permutation binomials over finite fields. *Trans. Amer. Math Soc*, 361 :4169–4180, 2009.

[20] H. Neiderreiter and K. H. Robinson. Complete mappings of finite fields. *J. Austral. Math. Soc*, 3(33) :197–212, 1982.

[21] R. Pieper. Cryptanalysis of rédei and dickson permutations on arbitrary finite rings. *Appl. Algebra Engry. Comm. Comput*, 1(4) :59–76, 1993.

[22] I. E. Shparlinski. A deterministic test for permutation polynomials. *Comput. Complexity*, 2(2) :129–132, 1992.

[23] R. J. Stroeker. On the sum of consecutive cubes being a perfect square. *Compositio Mathematica*, 97(1-2) :295–307, 1995.

[24] G. Turnwald. Permutation polynomials of binomial type in contributions to general algebra 6. *Holder-Pichler-Tempsky, Vienna*, pages 281–286, 1988.

[25] J. von zur Gathen. Tests for permutation polynomials. *SIAM J. Comut*, 20(3) :591–602, 1991.

[26] J. von zur Gathen. Values of polynomials over finite fields. *Bull. Austral. Math. Soc*, 1(43) :141–146, 1991.

[27] D. Wan and R. Lidl. Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure. *Mh. Math*, 112 :149–163, may 1991.

[28] Q. Wan. Permutation polynomials over finite field. *Acta Math Sinica (N. S)*, 3 :1–5, 1987.

[29] G. N. Watson. The problem of the square pyramid. *Messenger of Mathematics*, 48 :1–22, 1918-19.

Résumé

Dans cette thèse, nous présentons le contenu de notre publication intitulée On a familly of permutation polynomials. Nous nous intéressons spécialement aux polynômes de la forme précitée. Nous donnons des conditions nécessaires et suffisantes telle qu'une famille de polynômes soit des permutations, en se basant sut l'application du théorème de Wan et Lidl. Nous étudions un problème diophantien qui concerne la recherche de solutions de l'équation pyramidale carrée de Lucas. La réponse a cette question donne naissance a notre seconde publication. Nous donnons ainsi une majoration d un entier k en fonction de n et nous listons toutes les solutions possibles, en se reposant seulement sur des méthodes élémentaires.

Mots clés :

Corps finis; Groupe cyclique; Racine primitive; Critère d Hermite Dickson; Théorème de Wan et Lidl; Polynômes exceptionnels; Polynômes quadratiques; Polynômes de permutation; Equation diophantiennes; Problème de Lucas.