№ 13/2016 - M / MT

REPUBLIQUE ALGÉRIENNE DEMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEURE ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE
HOUARI BOUMEDIENE-ALGER
Faculté de Mathématiques

MÉMOIRE

Présenté pour l'obtention du diplôme de MAGISTER

En: MATHÉMATIQUES

Spécialité : Arithmétique, Codage et Combinatoire : Théorie des Nombres

par

REZIG Boualem

Sujet

Polynômes de Dickson de première espèce involutifs sur un corps de caractéristique 2

Soutenu publiquement le ,**07/05/2016 ,** devant le jury composé de :

Mme.C. SELMANE	MCA USTHB/FMT	Présidente
Mme L. BENFERHAT	MCA USTHB/FMT	Directrice de Mémoire
M. B. BENSEBAA	MCA USTHB /FMT	Examinateur

Remerciements

Je remercie mon Professeur et ma directrice de mémoire, madame BENFERHAT Leila,pour le sujet de mémoire intéressant qu'elle m'a proposé et pour son aide.

Je remercie Madame la présidente, Professeur SELMANE Scheherazad, pour avoir bien voulu présider ce Jury.

Je remercie également, Monsieur BENSEBA Boualem, pour avoir accepté d'examiner mon mémoire de Magister.

Table des matières

Résumé

L'un des concepts fondamentaux de la cryptographie symétrique est une clé qui permet à la fois de chiffrer et de déchiffrer un message.

Etant donné un chiffrement basé sur une permutation $E : X \to X$, où X est l'ensemble des signes d'un message avec la propriété $E(E(x)) = x, \forall x \in X$, c'est à dire que E est une involution. Alors E permet de chiffrer et déchiffrer le message.

Ce mémoire consiste en l'étude d'un article de P. Charpin, S. Mesnager et S. Sarkar sur les polynômes de Dickson de première espèce qui induisent des involutions.

Dans le premier chapitre, nous rappelons les résultats fondamentaux sur les corps finis utiles aux chapitres suivants.

Dans le chapitre suivant, nous donnons la définition de polynôme de permutation ainsi que les critères qui donnent les conditions pour lesquelles un polynôme est de permutation avec des démonstrations élaborées et plusieurs exemples.

Le dernier chapitre est réservée à l'étude détaillée de l'article de P. Charpin, S. Mesnager et S. Sarkar. Nous déterminons donc l'ensemble des involutions de Dickson et son cardinal.

Introduction

Nous commençons par la question suivante liée à la cryptographie : peut-on avoir un algorithme qui permet à la fois de chiffrer et déchiffrer un message. La réponse est oui, l'exemple classique pour ce genre de cryptosystème est Enigma. L'avantage d'avoir le même algorithme est que l'implementation de l'algorithme de chiffrement est utilisée pour le déchiffrement, ce qui réduit le coût de l'implementation.

Etant donné un chiffrement basé sur une permutation $E : X \to X$, où X est l'espace message avec la propriété $E(E(x)) = x, \forall x \in X$, c'est à dire que E est une involution. Alors E permet de chiffrer et déchiffrer le message.

Ce mémoire consiste en l'étude d'un article de P. Charpin, S. Mesnager et S. Sarkar (2015) sur les polynômes de Dickson de première espèce qui induisent des involutions. Il est composé de trois chapitres.

Dans le premier chapitre, nous rappelons les notions fondamentales sur les corps finis telles que la cardinalité, l'existence et l'unicité ainsi que la norme et la trace. Nons donnons la définition du caractère additif d'un corps fini et quelques propriétés. Enfin, pour mieux comprendre, nous donnons des exemples de corps finis.

Dans le deuxième chapitre, nous rappelons la définition de polynôme de permutation sur un corps fini ainsi que le critère d'Hermite qui permet de montrer qu'un polynôme est de permutation. Nous donnons quelques exemples de polynômes de permutation tels que les monômes, les polynômes de Dickson et les polynômes linéarisés.

Le dernier chapitre est consacré à l'étude détaillée de l'article de P. Charpin, S. Mesnager et S. Sarkar. Nous exposons donc les résultats avec des démonstrations détaillées sur les polynômes de Dickson de premère espèce dans $\mathbb{F}_2[x]$ en précisant l'ensemble des involutions de Dickson et son cardinal.

Chapitre 1

Rappels sur les corps finis

1.1 Introduction

Dans ce chapitre, nous rappelons les notions fondamentales sur les corps finis telles que la cardinalité, l'existence et l'unicité ainsi que la norme et la trace. Nons donnons la définition de caractère additif d'un corps fini et quelques propriétés. Enfin, pour mieux comprendre, nous donnons des exemples de corps finis.

Les références utilisées sont : [1], [3] et [4].

1.2 Rappels élémentaires

Définition 1.2.1 *Un corps fini est un corps ayant un nombre fini d'éléments.*

Théoréme 1.2.1 (Théorème de Wedderburn) *Tout corps fini est commutatif.*

Théoréme 1.2.2 $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ *est un corps fini si, et seulement si, n est premier.*

Démonstration. Supposons que n n'est pas premier, alors on peut écrire $n = qk$, où $1 < k < n$ et $1 < q < n$. On a alors $\overline{0} = \overline{n} = \overline{pq} = \overline{pq}$ avec $\overline{p} \neq \overline{0}$ et $\overline{q} \neq \overline{0}$, donc $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ n'est pas intègre, d'où $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ n'est pas un corps, puisque tout corps est intègre. Supposons maintenant que n est premier. Montrons alors que tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ est inversible. Soit $\overline{x} \in \dfrac{\mathbb{Z}}{n\mathbb{Z}}$, $\overline{x} \neq \overline{0}$. Comme n est premier, alors $\mathrm{PGCD}(x, n) = 1$. Il existe donc $k, s \in \mathbb{Z}$ tels que $kn + sx = 1$, donc $\overline{an + bx} = \overline{1}$, d'où $\overline{an} + \overline{b}\overline{x} = \overline{1}$, et comme $\overline{n} = \overline{0}$, alors $\overline{b}\overline{x} = \overline{1}$, c'est-à-dire que $\overline{x}$ est inversible, d'où $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est un corps. ■

Théoréme 1.2.3 *$\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est intègre si, et seulement si, n est premier.*

1.3 Cardinalité

Théoréme 1.3.1 *Tout corps fini $\mathbb{K}$ contient une copie de $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$, où p est un nombre premier.*

Démonstration. Soit $\mathbb{K}$ un corps fini. Soit l'application

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{K} \\ n &\longrightarrow n.1 \end{aligned}$$

où

$$n.1 = \begin{cases} 1+1+\cdots+1 & (n \text{ fois }) \quad si \;\; n > 0, \\ 0 & si \quad n = 0, \\ (-1)+(-1)+\cdots+(-1) & (-n \text{ fois }) \quad si \;\; n < 0. \end{cases}$$

L'application f est un morphisme d'anneaux. Nous savons que

$$\frac{\mathbb{Z}}{\ker f} \simeq f(\mathbb{Z}).$$

Nous avons

$$\ker f \; = \{m \in \mathbb{Z} \; : m.1 = 0\}.$$

Comme $\ker f$ est un idéal de $\mathbb{Z}$, il est donc de la forme $n\mathbb{Z}$, $n \in \mathbb{N}$, d'où $\dfrac{\mathbb{Z}}{\ker f} = \dfrac{\mathbb{Z}}{n\mathbb{Z}} \simeq f(\mathbb{Z})$. Comme $\mathbb{K}$ est un corps fini, il est donc intègre et tout sous-anneau de $\mathbb{K}$ est intègre, d'où $f(\mathbb{Z}) \simeq \dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est intègre. C'est à dire que n est premier. Autrement dit, $\mathbb{K}$ est une extension de $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$, où p est premier. ■

Remarque 1.3.1 *Le nombre premier p est la caractéristique du corps $\mathbb{K}$, c'est à dire., le plus petit entier strictement positif tel que $p.1 = 0$.*

Définition 1.3.1 *Le corps $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$, noté $\mathbb{F}_p$, est appelé corps premier de $\mathbb{K}$.*

Théoréme 1.3.2 *Soit p un nombre premier et $\mathbb{K}$ un corps fini de caractéristique p et de cardinal q. Alors il existe un entier n tel que*

$$q = p^n.$$

Démonstration. Considérons $\mathbb{F}_q$ comme un espace vectoriel sur $\mathbb{F}_p$. Posons $\dim_{\mathbb{F}_p}(\mathbb{F}_q) = n$ et soit $\beta = \{\zeta_1, \ldots, \zeta_n\}$ une base de $\mathbb{F}_q$ sur $\mathbb{F}_p$, alors chaque élèment $a \in \mathbb{F}_q$ peut s'écrire comme combinaison linéaire des élèments de la base β avec des coefficients dans $\mathbb{F}_p$. Donc il existe $c_1, \ldots, c_n \in \mathbb{F}_p$ qui satisfont $a = c_1\zeta_1 + \ldots + c_n\zeta_n$, d'où, en considérant toutes les combinaisons linéaires des éléments de la base β, on obtient p^n élèments dans $\mathbb{F}_q$ qui sont distincts. Par conséquent

$$q = p^n.$$

■

1.3.1 Existence et unicité

Dans la suite, nous noterons un corps fini à q éléments F_q.

Théoréme 1.3.3 .

1- *Pour tout nombre premier p et pour tout $n \in \mathbb{N}^*$, il existe un corps fini à p^n éléments.*

2- *Deux corps finis ayant le même nombre d'éléments sont isomorphes.*

Démonstration.

1- Posons $q = p^n$ et soit $f(x) = x^q - x \in \mathbb{F}_p[x]$. Alors l'ensemble

$$R = \left\{\alpha \in \overline{\mathbb{F}}_p \ : f(\alpha) = 0\right\},$$

des racines de $f(x)$ forme un corps à q élément. En effet, on a $0 \in R$ et $1 \in R$. Soit $a, b \in R$, alors $(a+b)^q = a^q + b^q = a + b$, donc $a + b \in R$. De plus $(ab)^q = a^q b^q = ab$, donc $ab \in R$. On a par ailleurs que $(a^{-1})^q = (1/a)^q = 1/a^q$. On en déduit que R est un sous-corps de $\overline{\mathbb{F}}_p$ à q éléments.

2- Soit $\mathbb{F}_q$ un corps fini à q éléments et soit $a \in \mathbb{F}_q$. On a $a^q = a$. En effet, si $a = 0$, c'est vérifié. Sinon, comme le groupe multiplicatif $\mathbb{K}^*$ est d'ordre $q - 1$, alors $a^{q-1} = 1$, et en multipliant par a les deux membres de l'égalité, on obtient le résultat. Donc, pour tout $a \in \mathbb{F}_q$, $x - a$ divise $x^q - x$. On a alors,

$$x^q - x = \prod_{a \in \mathbb{F}_q} (x - a).$$

Donc, tout corps fini à q éléments est le corps de décomposition de $x^q - x$ sur $\mathbb{F}_p$. Le corps de décomposition étant unique à isomorphisme près, on a le résultat voulu.

■

1.4 Exemples de corps finis

Soit $f(x) \in \mathbb{F}_p[x]$ un polynôme unitaire irréductible, de degré n. Soit $(f(x))$ l'idéal de $\mathbb{F}_p[x]$ engendré par le polynôme $f(x)$. Nous savons que $\mathbb{F}_p[x]/(f(x))$ est un corps à p^n éléments et que l'on a l'isomorphisme de corps

$$\mathbb{F}_p[x]/(f(x)) \backsimeq \mathbb{F}_p[\alpha],$$

où α est une racine de $f(x)$ dans une clôture algébrique de $\mathbb{F}_p$. Dans la suite, après avoir choisi un polynôme unitaire et irréductible de degré n, on écrira simplement

$$\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha].$$

Exemples 1.4.1 *Le corps* $\mathbb{F}_4$.
Soit $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. *On a* $f(0) = f(1) = 1$, *donc* $f(x)$ *n'a pas de racine dans* $\mathbb{F}_2$, *et comme il est de degré* 2, *alors il est irréductible sur* $\mathbb{F}_2$, *d'où*

$$\mathbb{F}_4 = \mathbb{F}_2[\alpha] = \{a + \alpha b : a, b \in \mathbb{F}_2 \text{ et } \alpha^2 = \alpha + 1\}.$$

Remarquons que $\alpha^3 = \alpha^2\alpha = \alpha(\alpha+1) = \alpha^2 + \alpha = \alpha + 1 + \alpha = 1$. *On obtient alors les tables d'addition et de multiplication dans* $\mathbb{F}_4 = \{0, 1, \alpha, 1+\alpha\}$.

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

.

Le polynôme $x^2 + x + 1$ est l'unique polynôme irréductible sur $\mathbb{F}_2$ de degré 2.

Exemples 1.4.2 *Le corps* $\mathbb{F}_8$.
Le polynôme $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ *est irréductible car il est de degré* 3 *et n'admet pas de racine dans* $\mathbb{F}_2$ *puisque* $f(0) = f(1) = 1$. *On a donc*

$$\mathbb{F}_8 = \mathbb{F}_2[\alpha] = \{a\alpha^2 + b\alpha + c : a, b, c \in \mathbb{F}_2 \text{ et } \alpha^3 + \alpha + 1 = 0\}.$$

Exemples 1.4.3 *Le corps* $\mathbb{F}_{16}$.
Le polynôme $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ *est irréductible. En effet,* $f(0) = f(1) = 1 \neq 0$, *donc* $f(x)$ *n'a pas de racine dans* $\mathbb{F}_2$ *; de plus* $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq f(x)$, *et* $x^2 + x + 1$ *est le seul polynôme irréductible de degré* 2 *sur* $\mathbb{F}_2$. *On a donc*

$$\mathbb{F}_{16} = \mathbb{F}_2[\alpha] = \{a\alpha^3 + b\alpha^2 + c\alpha + d : a, b, c, d \in \mathbb{F}_2\}.$$

Exemples 1.4.4 *Le corps* $\mathbb{F}_9$
Le polynôme $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$ *est irréductible car il est de degré* 2 *et n'admet pas de racine dans* $\mathbb{F}_3$ *puisque* $f(0) = 1$ *et* $f(1) = f(2) = 2$. *On obtient alors la représentation*

$$\mathbb{F}_9 = \{a + \alpha b : a, b \in \mathbb{F}_3 \text{ et } \alpha^2 = 2\}.$$

1.5 Groupe multiplicatif

Théoréme 1.5.1 *Soit* $\mathbb{F}_q$ *le corps fini à* q *éléments, et soit* $\mathbb{F}_q^*$ *son groupe multiplicatif. Alors* $\mathbb{F}_q^*$ *est un groupe cyclique.*

Le groupe $\mathbb{F}_q^*$ étant cyclique, il admet un générateur.

Définition 1.5.1 *Un générateur de groupe cyclique* $\mathbb{F}_q^*$ *est appelé élément primitif du corps* $\mathbb{F}_q$.

Exemples 1.5.1 *Le polynôme* $f(x) = x^4 + x^3 + 1 \in \mathbb{F}_2[x]$ *est irréductible. Soit* $\beta \in \overline{\mathbb{F}}_2$ *une racine de* $f(x)$ *et soit* $\mathbb{F}_{16} = \mathbb{F}_2[\beta]$. *On a* $\beta^4 = \beta^3 + 1, \beta^5 = \beta^4\beta = \beta^3 + \beta + 1$. *Comme l'ordre de* β *dans le groupe* $\mathbb{F}_{16}^*$ *divise l'ordre du groupe, qui est égal à* 15, *on en déduit que l'ordre de* β *est égal à* 15, *d'où* β *est primitif.*

1.6 Sous-corps d'un corps fini.

Proposition 1.6.1 *Soit K un corps fini et soit L un sous corps de K, alors K et L ont même caractéristique.*

Démonstration. Comme K est un corps fini à p^n éléments avec p premier et n entier positif, et $L \subset K$ alors L est un corps fini, donc de cardinal q^m, où q désigne un nombre premier et m un entier positif. D'autre part, on a $L \subset K$ alors $(L,+)$ est un sous groupe de $(K,+)$, donc d'aprés le théorème de Lagrange q^m divise p^n. Comme p et q sont des nombres premiers, alors $p = q$. ■

Théoréme 1.6.1 *Soit $m,n \in \mathbb{N}$ et p un nombre premier, alors*

$$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \Leftrightarrow m \text{ divise } n.$$

Démonstration. On suppose que $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$. Posons $k = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]$, on a $p^n = p^m \times p^m \times ... \times p^m$ (k fois), donc $p^n = p^{mk}$, d'où $n = mk$ et m divise n. Réciproquement, si m divise n, alors il existe k tel que $n = mk$. Soit $x \in \mathbb{F}_{p^m}$. On a

$$x^{p^n} = x^{p^{mk}} \implies x^{p^n} = \left(\left(\left(x^{p^m}\right)^{p^m}\right)^{\cdots}\right)^{p^m} (k \text{ fois}).$$

On en déduit que $x^{p^n} = \left((x)^{p^{m\cdots}}\right)^{p^m} = x$, car $x^{p^m} = x$ du fait que $x \in \mathbb{F}_{p^m}$, d'où $x \in \mathbb{F}_{p^n}$, alors $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$. ■

Exemples 1.6.1 *1-* $\mathbb{F}_8 = \mathbb{F}_{2^3}$ *n'est pas un sous-corps de* $\mathbb{F}_{16} = \mathbb{F}_{2^4}$ *car* $3 \nmid 4$.

2- $\mathbb{F}_8 = \mathbb{F}_{2^3}$ *est un sous-corps de* $\mathbb{F}_{64} = \mathbb{F}_{2^6}$ *car* $3 \mid 6$.

3-$\mathbb{F}_4$ *est un sous-corps de* $\mathbb{F}_{16} = \mathbb{F}_{2^4}$ *car* $2 \mid 4$.

4-$\mathbb{F}_9$ *est un sous-corps de* $\mathbb{F}_{81} = \mathbb{F}_{3^4}$ *car* $2 \mid 4$.

1.7 Automorphismes d'un corps fini

Théoréme 1.7.1 *Soit $\alpha \in \mathbb{F}_{p^n}$.Alors il existe un unique polynôme unitaire et irréductible $P_\alpha(X) \in \mathbb{F}_p[X]$ tel que $P_\alpha(\alpha) = 0$ et $P_\alpha(X)$ divise tout polynôme $f(X)$ de $\mathbb{F}_p[X]$ ayant α comme zéro. De plus* $\deg(P_\alpha) \leq n$.

Démonstration. Il suffit de remarquer que l'ensemble $\Pi = \{f \in \mathbb{F}_p[X], f(\alpha) = 0\}$ est un idéal principal distinct de $\{0\}$. Il est alors égal à $P_\alpha(X)\mathbb{F}_p[X]$ où $P_\alpha(X)$ est le polynôme recherché. ■

Définissions les conjugués d'un élément α comme suit.

Définition 1.7.1 *Soit $\alpha \in \mathbb{F}_{p^n}$. Les conjugués de α sont les racines dans $\mathbb{F}_{p^n}$ de $P_\alpha(X)$.*

Grâce au lemme suivant, il n'est pas difficile de prouver que α^p,α^{p^2},...,$\alpha^{p^{n-1}}$ sont racines de $P_\alpha(X)$.

Lemma 1.7.1 *Soient $\alpha_1, ..., \alpha_k$, k éléments d'un corps de caractéristique p. Alors*

$$\forall i \in \mathbb{N}, (\alpha_1 + ... + \alpha_k)^{p^i} = \alpha_1^{p^i} + ... + \alpha_k^{p^i}.$$

Démonstration. Il suffit de remarquer que les coefficients de la somme

$$(\alpha_1 + ... + \alpha_k)^{p^i} = \sum_{j_1+...+j_k=p^i} \frac{p^i!}{j_1!...j_k!} \alpha_1^{j_1}...\alpha_k^{j_k}$$

sont des multiples de p excepté pour $j_l = p^i$ $(0 \leq l \leq k)$. ■

Le degré de P_α ou encore le nombre de conjugués associés à α est alors donné après une démonstration purement technique par le théorème suivant.

Théoréme 1.7.2 *Soit $\alpha \in \mathbb{F}_{p^n}$. Le nombre de conjugés de α divise n. C'est le petit entier d tel que $p^d \equiv 1 \bmod ord(\alpha)$.*

Enfin, le groupe des automorphismes d'un corps fini est lui aussi cyclique.

Proposition 1.7.1 *Les automorphismes d'un corps fini $\mathbb{F}_{p^n}$ sont Id, ϕ, ϕ^2, ..., ϕ^{n-1} où l'automorphisme ϕ est donné par*

$$\begin{aligned} \mathbb{F}_{p^n} &\to \mathbb{F}_{p^n}, \\ x &\mapsto x^p. \end{aligned}$$

Démonstration. On vérifie facilement que , ϕ et ses composés ϕ^i sont des automorphismes, distincts si $i < n$. Réciproquement, soit f un morphisme et α une racine primitive de $\mathbb{F}_q$ de polynôme minimal $P_\alpha(X)$. Nous avons $P_\alpha(f(\alpha)) = f(P_\alpha(\alpha)) = 0$, et donc il existe un indice $i < n$ tel que $f(\alpha) = \alpha^{p^i}$ d'où on conclut facilement que $f = \phi^i$. ■

1.8 Trace et norme sur un corps fini

Théoréme 1.8.1 *Soit $f \in \mathbb{F}_q[x]$ un polynôme irréductible de degré m. Si α est une racine de f dans $\mathbb{F}_{q^m}$ alors toutes les racines de f sont distinctes dans $\mathbb{F}_{q^m}$ et sont données par*

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}} \in \mathbb{F}_{q^m}$$

Démonstration. On sait que f est un polynôme qui admet au plus m racines dans $\mathbb{F}_{q^m}$. Soit β une racine de f dans $\mathbb{F}_{q^m}$. Montrons que $f(\beta^q) = 0$.

Posons

$$f(x) = \sum_{i=0}^{m} a_i x^i, a_i \in \mathbb{F}_q.$$

On a

$$\begin{aligned} f(\beta^q) &= a_0 + a_1\beta^q + a_2(\beta^q)^2 + \ldots + a_m(\beta^q)^m \\ &= a_0^q + a_1^q\beta^q + a_2^q(\beta^q)^2 + \ldots + a_m^q(\beta^q)^m, \ (a_i \in \mathbb{F}_q \Rightarrow a_i^q = a_i) \\ &= (a_0 + a_1\beta^q + a_2(\beta^q)^2 + \ldots + a_m(\beta^q)^m)^q \\ &= (f(\beta))^q = 0^q = 0. \end{aligned}$$

Ceci montre que α et α^q sont des racines de f dans $\mathbb{F}_{q^m}$ et que $\alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ sont aussi des racines de f. Si $\alpha^{q^i} = \alpha^{q^j} pour\ 0 \leq i < j \leq m-1$, alors on aura

$$\begin{aligned} \alpha^{q^{i-j}} &= 1 \\ i.e\ )\ \alpha^{q^m}\alpha^{q^{i-j}} &= \alpha^{q^m} \\ \alpha^{q^{m+i-j}} &= \alpha^{q^m} = \alpha. \end{aligned}$$

Donc α est une racine d'un autre polynôme de degré $m+i-j$. Cependant $0 < m+i-j < m$, ce qui contredit le fait que α est une racine d'un polynôme irréductible de degré m. ■

Corollaire 1.8.1 *Soit f un polynôme irréductible dans $\mathbb{F}_q[x]$ de degré m. Alors le corps de décomposition de f sur $\mathbb{F}_q$ est $\mathbb{F}_{q^m}$.*

Démonstration. D'après le théorème (1.8.1), f se décompose complètement dans $\mathbb{F}_{q^m}$. donc $\mathbb{F}_q(\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}) = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$, α étant une racine de f dans $\mathbb{F}_{q^m}$. ■

Définition 1.8.1 *Soit $\alpha \in \mathbb{F}_{q^m}$. La Trace de α sur $\mathbb{F}_q$ notée par $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ est donnée par*

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

Si $\mathbb{F}_q = \mathbb{F}_p$ est un corps premier, alors $Tr_{\mathbb{F}_{p^m}/\mathbb{F}_p}$ est appelée Trace absolue ou tout simplement Trace.

Définition 1.8.2 *Soit $\alpha \in L = \mathbb{F}_{q^m}$ et $K = \mathbb{F}_q$. La Norme de α sur K, notée $N_{L/K}(\alpha)$ est donnée par*

$$N_{L/K}(\alpha) = \alpha.\cdots.\alpha^q.\alpha^{q^{m-1}}$$

Lemma 1.8.1 *Soit $\alpha \in \mathbb{F}_{q^m}$. Alors $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$ et $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$.*

Démonstration. Soit $m_\alpha(x) \in \mathbb{F}_q[x]$ le polynôme minimal de α sur $\mathbb{F}_q$ et soit $m_\alpha(x) = \sum_{i=0}^{r} a_i x^i$ tel que $r = [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$. On a bien que $r \mid m$ et m_α définit une extension du corps $\mathbb{F}_{q^r}$ de $\mathbb{F}_q$. D'après le théorème 13, on a

$$\begin{aligned}
\prod_{i=0}^{m-1}(x-\alpha^{q^i}) &= \prod_{i=0}^{r-1}(x-\alpha^{q^i}).\prod_{i=0}^{r-1}(x-\alpha^{q^{i+r}}).\cdots.\prod_{i=0}^{r-1}(x-\alpha^{q^{i+r(\frac{m}{r}-1)}}) \\
&= \underbrace{\prod_{i=0}^{r-1}(x-\alpha^{q^i}).\cdots.\prod_{i=0}^{r-1}(x-\alpha^{q^i}).}_{\frac{m}{r}\ fois} \\
&= m_\alpha(x)^{\frac{m}{r}}.
\end{aligned}$$

Comme $m_\alpha(x) \in \mathbb{F}_q[x]$, alors $m_\alpha(x)^{\frac{m}{r}}$admet des coefficients dans $\mathbb{F}_q$. Le coefficient du deuxième terme est donné par

$$-(\alpha + \alpha^q + \ldots + \alpha^{q^{m-1}}) = -Tr(\alpha),$$

et le coefficient constant est la Norme de α. Par comparaison on a

$$\begin{aligned}
rTr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) &= -ma_{m-1} \in \mathbb{F}_q \\
\text{et } N_{L/K}(\alpha) &= a_0^{\frac{m}{r}} \in \mathbb{F}_q.
\end{aligned}$$

■

1.8.1 Propriétés de la trace et de la norme

Soit L une extension finie de K, avec $[L : K] = m$ et soit $\alpha, \beta \in L, c \in K$. On a :

$$\begin{aligned}
Tr_{L/K}(\alpha+\beta) &= Tr_{L/K}(\alpha) + Tr_{L/K}(\beta) \\
Tr_{L/K}(c.\alpha) &= c.Tr_{L/K}(\alpha) \\
Tr_{L/K}(c) &= m.c \\
Tr_{L/K}(\alpha^q) &= Tr_{L/K}(\alpha)
\end{aligned}$$

$$\begin{aligned} N_{L/K}(\alpha.\beta) &= N_{L/K}(\alpha).N_{L/K}(\beta) \\ N_{L/K}(c) &= c^m \\ N_{L/K}(\alpha^q) &= N_{L/K}(\alpha). \end{aligned}$$

1.9 Caractère additif d'un corps fini

Définition 1.9.1 *Soit G un groupe multiplicatif abélien fini, d'ordre n, et d'élément neutre 1. Un caractère χ de G est un homomorphisme de G dans le groupe multiplicatif U des nombres complexes de modules* 1.

Donc

$$\chi : (G, .) \longrightarrow (U, .)$$

est une application qui vérifie :

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

Définition 1.9.2 *Soit χ un caractère de G. On définit le caractère conjugué $\overline{\chi}$ de G par :*

$$\overline{\chi}(g) = \overline{\chi(g)}, \forall g \in G.$$

Soit $\mathbb{F}_q$ un corps fini de caractéristique p. Considérons le groupe additif $\mathbb{F}_q$. Soit Tr : $\mathbb{F}_q \to \mathbb{F}_p$ la trace de $\mathbb{F}_q$, alors la fonction χ_1 défini par

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

est un caractère du groupe additif de $\mathbb{F}_q$, puisque nous avons

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

et donc

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

Le caractère χ_1 est appelé caractère additif canonique de $\mathbb{F}_q$ et tous les caractères additifs de $\mathbb{F}_q$ peuvent être exprimés en fonction de χ_1, d'après le théorème suivant :

Théoréme 1.9.1 *Pour $b \in \mathbb{F}_q$, la fonction χ_b avec $\chi_b(c) = \chi_1(bc)$, $\forall c \in \mathbb{F}_q$ est un caractère additif de $\mathbb{F}_q$ et tout caractère de $\mathbb{F}_q$ est obtenu ainsi.*

Démonstration. $\forall c_1, c_2 \in \mathbb{F}_q$ on a

$$\begin{aligned}\chi_b(c_1+c_2) &= \chi_1(bc_1+bc_2)\\ &= \chi_1(bc_1)\chi_1(bc_2)\\ &= \chi_b(c_1)\chi_b(c_2).\end{aligned}$$

Comme la trace absolue est une application de $\mathbb{F}_q$ dans $\mathbb{F}_p$, χ_1 est un caractère non trivial. Donc, si $a, b \in \mathbb{F}_q$ avec $a \neq b$, alors

$$\frac{\chi_a(c)}{\chi_b(c)} = \frac{\chi_1(ac)}{\chi_1(bc)} = \chi_1((a-b)c) \neq 1, \text{ pour un certain } c \in \mathbb{F}_q.$$

Ainsi χ_a et χ_b sont des caractères distincts. Par conséquent, si b parcourt $\mathbb{F}_q$, nous obtenons q caractères additifs distincts χ_b. D'autre part, $\mathbb{F}_q$ a exactement q caractères additifs, et ainsi nous obtenons tous les caractères additifs de $\mathbb{F}_q$. ■

Pour $b = 0$, dans le théorème précédent, nous obtenons le caractère additif trivial χ_0, pour lequel $\chi_0(c) = 1$ pour tout $c \in \mathbb{F}_q$.

Soit E une extension finie de $\mathbb{F}_q$ et χ_1 le caractère additif canonique de $\mathbb{F}_q$, et soit μ_1 le caractère additif canonique de E. Alors χ_1 et μ_1 sont reliés par l'identité

$$\chi_1(Tr_{E/\mathbb{F}_q}(\beta)) = \mu_1(\beta), \ \forall \beta \in E.$$

On a la relation de transitivité

$$Tr_{E/\mathbb{F}_p}(\beta) = Tr_{\mathbb{F}_q/\mathbb{F}_p}(Tr_{E/F_q}(\beta)), \quad \forall \beta \in E.$$

1.9.1 Relations d'orthogonalité des caractères additifs d'un corps fini

Proposition 1.9.1 *Soient χ_a, χ_b deux caractères additifs de $\mathbb{F}_q$, alors*

$$\sum_{c \in \mathbb{F}_q} \chi_a(c)\overline{\chi_b(c)} = \begin{cases} 0 \text{ pour } a \neq b \\ q \text{ pour } a = b \end{cases}. \tag{1.1}$$

En particulier

$$\sum_{c \in \mathbb{F}_q} \chi_a(c) = 0 \text{ pour } a \neq 0. \tag{1.2}$$

De plus $\forall c, d \in \mathbb{F}_q$, *On a*

$$\sum_{b \in \mathbb{F}_q} \chi_a(c)\overline{\chi_b(c)} = \begin{cases} 0 \text{ pour } c \neq d \\ q \text{ pour } c = d \end{cases} . \tag{1.3}$$

Chapitre 2

Polynômes de permutation et exemples

2.1 Introduction

Dans ce chapitre, nous rappelons la définition d'un polynôme de permutation sur un corps fini ainsi que le critère d'Hermite qui permet de montrer qu'un polynôme est de permutation. Nous donnons quelques exemples de polynômes de permutation tels que les monômes, les polynômes de Dickson et les polynômes linéarisés.

Les référence utilisées sont : [1] et [2] et [6].

2.2 Rappels sur les polynômes de permutation

Définition 2.2.1 *Soit $\mathbb{F}_q$ un corps fini, où $q = p^n$, p étant un nombre premier. Soit $f \in \mathbb{F}_q[x]$, f est dit polynôme de permutation de $\mathbb{F}_q$ si l'équation $f(x) = a$ admet une solution unique dans $\mathbb{F}_q, \forall a \in \mathbb{F}_q$.*

Lemma 2.2.1 *Soit $f \in \mathbb{F}_q[x]$, f est un polynôme de permutation de $\mathbb{F}_q$ si et seulement si*

1. *L'application $f : \mathbb{F}_q \to \mathbb{F}_q$ est surjective ;*
2. *L'application $f : \mathbb{F}_q \to \mathbb{F}_q$ est injective ;*
3. *$f(x) = a$ admet au moins une solution dans $\mathbb{F}_q, \forall a \in \mathbb{F}_q$.*

Démonstration. Comme $\mathbb{F}_q$ est fini alors f injective $\Leftrightarrow$ f surjective $\Leftrightarrow$ f bijective ■

Théoréme 2.2.1 *Soit $\phi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ une application de $\mathbb{F}_q$ dans $\mathbb{F}_q$. Alors, il existe un unique polynôme $g \in \mathbb{F}_q[x]$ de degré $\leq q-1$ tel que $g(c) = \phi(c)$, $\forall c \in \mathbb{F}_q$ et*

$$g(x) = \sum_{c \in \mathbb{F}_q} \phi(c)(1 - (x-c)^{q-1}).$$

Démonstration. En effet, ce polynôme est donné par la formule d'interpolation de Lagrange.

Soit $a_0, \ldots, a_{q-1}$, q points distincts de $\mathbb{F}_q$ et $b_0, \ldots, b_{q-1}$, q points arbitraires de $\mathbb{F}_q$ avec $\phi(a_i) = b_i$, $i = \overline{0, q-1}$. Alors, il existe un unique polynôme $g \in \mathbb{F}_q[x]$, degré $g \leq q-1$, tel que

$$g(x) = \sum_{i=0}^{n} b_i \prod_{k=0, k \neq i}^{n} \frac{(x-a_k)}{(a_i - a_k)}.$$

Donc on peut écrire

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

or

$$\prod_{\substack{d \in \mathbb{F}_q \\ d \neq c}} (c-d) = (c-d_1).(c-d_2).\ldots.(c-d_{q-1}) = -1$$

et

$$\prod_{\substack{d \in \mathbb{F}_q \\ d \neq c}} (x-d) = \frac{\prod\limits_{d \in \mathbb{F}_q} (x-d)}{(x-c)} = \frac{x^q - x}{x-c} = \frac{x^q - c^q - (x-c)}{(x-c)} = \frac{(x-c)^q - (x-c)}{(x-c)} = (x-c)^{q-1} - 1,$$

d'où la relation. ■

Lemma 2.2.2 *Soient f, $g \in \mathbb{F}_q[x]$. On a $f(c) = g(c)$ pour tout $c \in \mathbb{F}_q$ si et seulement si $f(x) \equiv g(x) \bmod (x^q - x)$.*

Démonstration. En effectuant la division euclidienne de $f(x) - g(x)$ par $x^q - x$, on peut écrire $f(x) - g(x) = h(x)(x^q - x) + r(x)$ avec h, $r \in \mathbb{F}_q[x]$ et $\deg r < q$. Donc $f(c) = g(c)$ $\forall c \in \mathbb{F}_q$ si et seulement $r(c) = 0$ $\forall c \in \mathbb{F}_q$, ce qui est équivalent à $r = 0$. ■

2.2.1 Critère d'Hermite

Pour la démonstration du critère d'Hermite, nous utiliserons le lemme suivant :

Lemma 2.2.3 *Soient $a_0, \ldots, a_{q-1}$ des éléments de $\mathbb{F}_q$. Les deux conditions suivantes sont équivalentes :*

1. *$a_0, \ldots, a_{q-1}$ sont distincts*
2. $\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0 \text{ pour } t = 0, \ldots, q-1 \\ -1 \qquad \text{pour } t = q-1 \end{cases}$

Démonstration. Soit $0 \leq i \leq q-1$. Considérons le polynôme

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

On a

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

et

$$\begin{aligned} g_i(b) &= 1 - \sum_{j=0}^{q-1} a_i^{q-1-j} b^j = 1 - a_i^{q-1} \sum_{a_i \neq b}^{q-1} a_i^{-j} b^j, \ b \in \mathbb{F}_q, \ b \neq a_i \\ &= 1 - a_i^{q-1} \sum_{a_i \neq b}^{q-1} (\frac{b}{a_i})^j. \end{aligned}$$

Posons

$$X = \frac{b}{a_i}.$$

Donc

$$\begin{aligned} g_i(b) &= 1 - a_i^{q-1} \sum_{a_i \neq b}^{q-1} (X)^j = 1 - a_i^{q-1}(1 + X + \ldots + X^{q-1}) = 1 - a_i^{q-1}(\frac{1 - X^q}{1 - X}), \text{où } b \neq a_i \text{ et } \frac{b}{a_i} \neq 1 \\ &= 1 - 1 = 0, \end{aligned}$$

donc

$$g_i(b) = 0.$$

Alors le polynôme

$$g(x) = \sum_{i=0}^{q-1} g_i(x) = -\sum_{j=0}^{q-1} \left(\sum_{j=0}^{q-1} a_i^{q-1-j} \right) x^j.$$

On a

$$g(x) = 1, \forall x \in \mathbb{F}_q \Leftrightarrow \{a_0, \cdots, a_{q-1}\} = \mathbb{F}_q.$$

Comme $\deg(g) < q$, alors

$$g(x) = 1, \forall x \in \mathbb{F}_q \Leftrightarrow g(x) = 1.$$

■

Théoréme 2.2.2 (Critère d'Hermite) *Soit $\mathbb{F}_q$ un corps fini de caractéristique p et $f \in \mathbb{F}_q[x]$. Alors f est un polynôme de permutation si et seulement si les conditions suivantes sont vérifées :*

1. *f a exactement une racine dans $\mathbb{F}_q$.*
2. *Soit t un entier avec $1 \leq t \leq q-2$ et $t \neq 0 \bmod p$, la réduction de $(f(x))^t \bmod (x^q - x)$ est de degré $\leq q-2$.*

Démonstration. Supposons que f est un polynôme de permutation.

1. L'application $f : \mathbb{F}_q \to \mathbb{F}_q$ est bijective.
2. Ecrivons la réduction de $(f(x))^t \bmod (x^q - x)$ sous la forme :

$$\sum_{j=0}^{q-1} b_j^{(t)} x^j,$$

où

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

D'après le lemme 2.2.3, on a

$$b_{q-1}^{(t)} = 0, \ 1 \leq t \leq q-2,$$

ce qui implique (1).

Réciproquement ; supposons que (1) et (2) soient vérifiées alors (1) implique que

$$\sum_{c \in \mathbb{F}_q} f(c)^{q-1} \neq 0 = -1$$

et (2) implique que

$$\sum_{c \in \mathbb{F}_q} f(c)^t = 0 \ \text{ pour } 1 \leq t \leq q-2 \ \text{ et } t \neq 0 \bmod p.$$

En utilisant que

$$\sum_{c \in \mathbb{F}_q} f(c)^{tp^j} = \left(\sum_{c \in \mathbb{F}_q} f(c)^t \right)^{p^j},$$

on a

$$\sum_{c \in \mathbb{F}_q} f(c)^t = 0 \text{ pour } 0 \leq t \leq q-2,$$

et cette égalité est vérifiée pour $t = 0$.

Par le lemme 2.2.3, f est un polynôme de permutation de $\mathbb{F}_q$.

■

Corollaire 2.2.1 *Si $d > 1$ est un diviseur de $q-1$, alors il n'existe pas de polynôme de permutation de $\mathbb{F}_q$ de degré d.*

Démonstration. Si $f \in \mathbb{F}_q[x]$ avec $\deg(f) = d$ et $d \mid q-1$, alors $\deg(f^{\frac{q-1}{d}}) = q-1$ pour

$$1 \leq t = \frac{q-1}{d} \leq q-2.$$

Or la condition (2) du critère d'Hermite n'est pas vérifiée pour $t = \frac{q-1}{d}$. ■

Théoréme 2.2.3 *$f \in \mathbb{F}_q[x]$ est un polynôme de permutation de $\mathbb{F}_q$ si et seulement si les deux conditions suivantes sont vérifées :*

1. *La réduction de $f(x)^{q-1} \bmod (x^q - x)$ est de degré $q-1$.*
2. *Pour chaque entier t avec $1 \leqslant t \leqslant q-2$ et $t \neq 0 \bmod p$, la réduction de $f(x)^t \bmod (x^q - x)$ est de degré $\leqslant q-2$.*

Démonstration. La nécessité de 2 vient du théorème 2.2.2. Dans les notations de la preuve de ce théorème. On a

$$b_{q-1}^{(q-1)} = -\sum_{c \in F_q} f(c)^{q-1}.$$

Ainsi si f est un polynôme de permutation de $\mathbb{F}_q$, alors $b_{q-1}^{(q-1)} = 1$, d'après le lemme 2.2.3, et 1 est vérifiée.

Réciproquement, supposons 1 et 2 satisfaites. Alors comme dans la preuve du théorème 2.2.3, 2 implique que $\sum_{c \in F_q} f(x)^t = 0$ pour $0 \leqslant t \leqslant q-2$, et 1 implique que $\sum_{c \in F_q} f(x)^{q-1} \neq 0$. Ainsi le polynôme

$$g(x) = -\sum_{j=0}^{q-1} \left(\sum_{c \in F_q} f(c)^{q-1-j} \right) x^j,$$

est une constante non nulle. Si f n'était pas un polynôme de permutation de $\mathbb{F}_q$, alors l'argument dans la preuve de lemme 2.2.3 montrerait que $g(b) = 0$ pour un certain $b \in \mathbb{F}_q$, qui est une contradiction. ■

Théoréme 2.2.4 *Le polynôme $f \in \mathbb{F}_q[x]$ est un polynôme de permutation de $\mathbb{F}_q$ si et seulement si*

$$\sum_{c \in F_q} \chi(f(c)) = 0,$$

pour tous les caractères additifs non triviaux χ de $\mathbb{F}_q$.

Démonstration. Si f est un polynôme de permutation de $\mathbb{F}_q$ et χ un caractère additif non trivial de $\mathbb{F}_q$, alors

$$\sum_{c\in\mathbb{F}_q}\chi(f(c)) = \sum_{c\in\mathbb{F}_q}\chi(c) = 0,$$

d'après (2.9).

Réciproquement, si χ_0 désigne le caractère additif trivial de $\mathbb{F}_q$ et $\sum\limits_{c\in\mathbb{F}_q}\chi(f(c)) = 0$ pour tout $\chi \neq \chi_0$, alors pour tout $a \in \mathbb{F}_q$ le nombre N de solutions de $f(x) = a$ dans $\mathbb{F}_q$ est donné par

$$N = \frac{1}{q}\sum_{c\in\mathbb{F}_q}\sum_{\chi}\chi(f(c))\overline{\chi(a)} = 1 + \frac{1}{q}\sum_{\chi\neq\chi_0}\overline{\chi(a)}\sum_{c\in\mathbb{F}_q}\chi(f(c)) = 1.$$

Donc f est un polynôme de permutation de $\mathbb{F}_q$. ■

2.3 Exemples de polynômes de permutation

Théoréme 2.3.1 *Pour tout $(a, b) \in \mathbb{F}_q^* \times \mathbb{F}_q$,le polynôme linéaire $f = ax+b$ est un polynôme de permutation de $\mathbb{F}_q$.*

Démonstration. La fonction associée $f : x \to f(x)$ est bijective : $\forall y \in \mathbb{F}_q$, $\exists! x \in \mathbb{F}_q$ tel que $f(x) = y$.

On a $ax + b = y \Leftrightarrow x = (y - b)/a$. ■

Théoréme 2.3.2 *Soient $f(x), g(x) \in \mathbb{F}_q[x]$, alors $f(g(x))$ est un polynôme de permutation si et seulement si f et g sont des polynômes de permutation.*

Démonstration. La composée de deux applications bijectives est bijective. ■

Théoréme 2.3.3 *Soit n un entier naturel positif. Alors x^n est un polynôme de permutation de $\mathbb{F}_q$ si et seulement si* $\gcd(n, q - 1) = 1$;

Démonstration. Soit l'application $\varphi : \mathbb{F}_q \to \mathbb{F}_q$ telle que $\varphi(g) = g^n$.

On a $\varphi(0) = 0$.

On sait que $\mathbb{F}_q^*$ est un groupe cyclique d'ordre $q - 1$. Soit g un générateur de $\mathbb{F}_q^*$, c'est à dire que $\mathbb{F}_q^* = \{g, g^2, \ldots g^{q-1} = 1\}$.

L'application φ est un morphisme du groupe multiplicatif $\mathbb{F}_q^*$ dans $\mathbb{F}_q^*$. On a

$$\begin{aligned} \varphi \text{ bijective} &\Leftrightarrow \varphi(g^i) = \varphi(g)^i \ 1 \leq i \leq q-1 \text{ sont tous distincts} \\ g \text{ générateur de } \mathbb{F}_q^* &\Leftrightarrow \varphi(g) \text{ générateur de } \mathbb{F}_q^* \\ &\Leftrightarrow g^n \text{ générateur de } \mathbb{F}_q^* \\ &\Leftrightarrow \gcd(n, q-1) = 1 \end{aligned}$$

■

Théoréme 2.3.4 *Soit $r \in \mathbb{N}$ tel que $\gcd(r, q-1) = 1$. Soit un entier $s > 0$, $s \mid q-1$. Soit $g \in \mathbb{F}_q[x]$. Si $g(x^s)$ admet 0 comme racine unique dans $\mathbb{F}_q$, alors*

$$f(x) = x^r (g(x^s))^{(q-1)/s}$$

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

Démonstration. Montrons que f satisfait le critère d'Hermite.

1. $f(x) = 0$ admet une seule racine qui est égale à 0.

2. Soit $t \in \mathbb{Z}$, $1 \leq t \leq q-2$. Supposons que : $s \nmid t$

$$\begin{aligned} f(x)^t &= (x^r (g(x^s))^{q-1/s})^t \\ &= x^{rt} g(x^s)^{(q-1)t/s}. \end{aligned}$$

   On a $f(x)^t$ de degré $rt + ms$, avec $m \in \mathbb{Z}$.
   Comme $(r, q-1) = 1$ et $s \mid q-1$, alors $(r, s) = 1$. Donc $s \nmid rt+ms$. D'où $q-1 \nmid rt+ms$.
   Par conséquent, $f(x)^t \bmod x^q - x$ est de degré $\leq q-2$.
   Supposons que $s \mid t$. Posons $t = ks$ avec $k \in \mathbb{N}$. Alors

$$f(x)^t = x^{rt} (g(x^s))^{(q-1)k}.$$

   Posons $h(x) = x^{rt}$. On a $f(c)^t = h(c), \forall c \in \mathbb{F}_q^*$ car $g(c^s)^{(q-1)k} = 1$ et donc $f(c)^t = h(c), \forall c \in \mathbb{F}_q$. D'où

$$f(x)^t \equiv x^{rt} \bmod (x^q - x),$$

   et ceci d'après le lemme 2.2.2. Comme $q-1 \nmid rt$, alors la reduction de $f(x)^t \bmod (x^q - x)$ est de degré $\leq q-2$.

■

2.3.1 Les polynômes linéarisés

Les polynômes linéarisés jouent un rôle important, que ce soit en théorie ou en pratique. C'est une classe de polynômes très spéciale.

Définition 2.3.1 *Soit q une puissance d'un nombre premier, et n un entier. Un polynôme de la forme* :

$$L(X) = \sum_{i=0}^{n} \alpha_i X^{q^i} \quad \in \mathbb{F}_{q^n}[X]$$

est appelé polynôme linéarisé.

On peut parfois trouver dans la littérature la notation q-polynôme pour désigner un tel polynôme.

La proposition suivante est un cas particulier du critère d'Hermite appliqué aux q-polynômes.

Lemma 2.3.1 *Un q-polynôme L (dont on peut supposer le degré inférieur à q^n) induit une permutation de $\mathbb{F}_{q^n}$ si, et seulement si 0 est l'unique racine de F dans $\mathbb{F}_{q^n}$.*

Démonstration. On peut vérifier que l'opérateur $L : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ est linéaire. Il vérifie donc les propriétés suivantes :

$$\begin{aligned} L(\beta+\gamma) &= L(\beta)+L(\gamma),\ \forall \beta,\gamma \in \mathbb{F}_{p^r}, \\ L(c\beta) &= cL(\beta),\ \forall c \in \mathbb{F}_p,\ \forall \beta \in \mathbb{F}_{p^r}, \end{aligned}$$

On a $\ker(L) = \{0\}$, d'où l'application est injective. Donc L est un polynôme de permutation. ■

Définition 2.3.2 *Deux polynômes P et Q sont dits linéairement équivalents lorsqu'il existe deux polynômes linéarisés L_1 et L_2 tels que*:

$$Q = L_1 \circ P \circ L_2$$

Si on reprend la définition 2.3.2, on remarque que si P et Q sont des permutations, alors L_1 et L_2 le sont aussi. Sinon la composée $L_1 \circ P \circ L_2$ n'est pas bijective. On a donc la proposition suivante:

Proposition 2.3.1 *Deux polynômes de permutations P et Q sont dits linéairement équivalents lorsqu'il existe deux polynômes de permutations linéarisés L_1 et L_2 tels que* :

$$Q = L_1 \circ P \circ L_2$$

La proposition suivante permet de construire un polynôme linéaire de permutation sur $\mathbb{F}_{q^n}$.

Proposition 2.3.2 *Pour toute famille d'éléments $c_i \in F_{2^n}$, $i \in \{1, ..., n-1\}$ non tous nuls, il existe $c_0 \in \mathbb{F}_{2^n}$ tel que le polynôme linéarisé*

$$P(X) = c_0X + c_1X^2 + ... + c_{n-1}X^{2^{n-1}} = \sum_{i=0}^{n-1} c_iX^{2^i}$$

soit un polynôme de permutation de $\mathbb{F}_{2^n}$.

Démonstration. On sait qu'un polynôme linéaire de permutation n'admet que zéro comme racine dans son corps de coefficients. On peut réécrire $P(X)$ comme suit,

$$P(X) = X(c_0 + c_1X + c_2X^{2^2-1} + ... + c_{n-1}X^{2^{n-1}-1})$$

Or on sait d'après ([6], Théorème 6) que le polynôme

$$c_1X + c_2X^{2^2-1} + ... + c_{n-1}X^{2^{n-1}-1} \tag{2.1}$$

ne peut être de permutation, indépendamment de ces coefficients. Il existe donc bien un élément $c_0 \in F_{2^n}$ qui n'est pas dans l'image de (2.1) tel que

$$c_0 + c_1X + c_2X^{2^2-1} + ... + c_{n-1}X^{2^{n-1}-1}$$

n'ait pas de racine dans F_{2^n}. ■

2.3.2 Polynômes de Dickson

Les polynômes de Dickson sont des suites de polynômes à une indeterminée et dépendant d'un paramètre (qu'on notera respectivement X et a) ,

On notera respectivement D_n et E_n les polynômes de première et deuxième espèces.

Les polynômes de Dickson de deuxième espèce sont traditionnellement indexés par leur degré, mais il est commode d'introduire un polynôme de deuxième espèce réduit par $\overline{E}_n = E_{n-1}$, en posant $\overline{E}_0 = 0$.

Polynômes de Dickson de première espèce

Formule de Waring

Définition 2.3.3 *Soit $\Re$ un anneau commutatif. Un polynôme $f \in \Re[x_1, \ldots x_n]$ est dit symétrique si*

$$f(x_{i_1}, \ldots x_{i_n}) = f(x_1, \ldots, x_n)$$

pour toute permutation $i_1, \ldots, i_n$ des entiers $1, \ldots, n$.

Posons $\Re[x_1, \ldots, x_n] = A$ et soit $g \in A$ tel que

$$g(z) = (z - x_1)(z - x_2) \cdots (z - x_n),$$

alors

$$g(z) = z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} + \cdots + (-1)^n \sigma_n$$

avec

$$\begin{aligned}
\sigma_k &= \sigma_k(x_1, \ldots, x_n) \\
&= \sum_{1 \le i_1 \le \ldots \le i_k \le n} x_{i_1} \ldots x_{i_k} \ (k = 1, 2, \ldots, n), \\
\sigma_1 &= x_1 + x_2 + \ldots + x_n \\
&\vdots \\
\sigma_2 &= x_1x_2 + x_1x_3 + \cdots + x_2x_3 + \cdots + x_2x_n + \cdots + x_{n-1}x_n \\
\sigma_n &= x_1x_2 \cdots x_n.
\end{aligned}$$

Le polynôme $\sigma_k = \sigma_k(x_1, \ldots, x_n) \in \Re[x_1, \ldots x_n]$ est appelé $k - ième$ polynôme élémentaire symétrique sur $\Re$.

Soit

$$S_k = S_k(x_1, \ldots x_n) = x_1^k + \cdots + x_n^k \in \Re[x_1, \ldots x_n] \text{ pour } k \ge 1.$$

Théoréme 2.3.5 *On a*

$$S_k = \sum_{\substack{i_1, \ldots, i_n \\ i_1 + 2i_2 + \cdots + ni_n = k}} (-1)^{i_2 + i_4 + i_6} \frac{(i_1 + i_2 + \cdots + i_n - 1)!k}{i_1! i_2! \ldots i_n!} \sigma_1^{i_1} \sigma_2^{i_2} \ldots \sigma_n^{i_n} \ \textit{pour } k \ge 1$$

Quand la somme parcourt tous les $n - uplets$ $(i_1, \ldots, i_n)$ d'entiers positifs avec $i_1 + 2i_2 + \cdots + ni_n = k$, le coefficient de $\sigma_1^{i_1} \sigma_2^{i_2} \ldots \sigma_n^{i_n}$ est toujours un entier.

Pour deux inconnues x_1, x_2 et $k \in \mathbb{N}$, nous avons

$$\begin{aligned} S_k &= x_1^k + x_2^k = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} (-1)^{i_2} \frac{(i_1+i_2-1)!}{i_1!_{2!}} \sigma_1^{i_1} \sigma_2^{i_2} \\ &= \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} (-1)^{i_2} \frac{(i_1+i_2-1)!}{i_1! i_2!} (x_1+x_2)^{i_1} (x_1 x_2)^{i_2}. \end{aligned}$$

Posons $i_1 = k-2j$ et $i_2 = j$. On a

$$\begin{aligned} x_1^k + x_2^k &= \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} (-1)^j \frac{(k-2j+j-1)!k}{(k-2j)!j!} (x_1+x_2)^{k-2j} (x_1x_2)^j \qquad (2.2) \\ &= \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} (-1)^j \frac{(k-j-1)!k}{(k-2j)!j!} (x_1+x_2)^{k-2j} (x_1x_2)^j \\ &= \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \begin{pmatrix} k-j \\ j \end{pmatrix} (-x_1x_2)^j (x_1+x_2)^{k-2j}. \end{aligned}$$

Définition 2.3.4 *Soit $a \in \mathbb{F}_q$. On définit le polynôme de Dickson de première espèce par*

$$D_n(x,a) = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-j} \begin{pmatrix} n-j \\ j \end{pmatrix} (-a)^j (x)^{n-2j}, \qquad (2.3)$$

en posant $D_0(x,a) = 2$.

Si nous travaillons dans le corps des nombres complexes, alors ces polynômes sont étroitement liés aux polynômes bien connus de Chebyshev de première espèce $T_n(x) = \cos(n \arccos x)$. En effet, si nous posons $x_1 = e^{i\theta}$ et $x_2 = e^{-i\theta}$ dans la formule (2.2), alors

$$x_1^k + x_2^k = e^{ki\theta} + e^{-ki\theta} = 2\cos(k\theta) = \sum_{j=0}^{\lfloor k|2 \rfloor} (-1)^j \frac{k}{k-j} \binom{k-j}{j} (2\cos\theta)^{k-2j},$$

d'où

$$\begin{aligned} D_n(2x,1) &= \sum_{j=0}^{\lfloor n|2 \rfloor} \frac{n}{n-j} \binom{n-j}{j} (-1)^j (2x)^{k-2j} \qquad (2.4) \\ &= \sum_{j=0}^{\lfloor k|2 \rfloor} (-1)^j \frac{n}{n-j} \binom{n-j}{j} 2^{n-2j} x^{n-2j} \qquad (\ x = cos\theta \text{ et } \theta = \arccos x) \\ &= 2T_n(x). \end{aligned}$$

Pour ces raisons, les polynômes de Dickson s'appellent parfois polynômes de Chebyshev. L'identité (2.4) peut être utilisée pour définir les polynômes de Chebyshev de première espèce sur tout corps de caractéristique différente de 2.

Si nous considérons un polynôme de Dickson $D_n(x,a)$ sur un corps F, alors dans le corps des fonctions rationnelles sur F, d'indéterminée y, nous avons l'identité

$$D_n(y+\frac{a}{y},a)=y^n+\frac{a^n}{y^n}, \tag{2.5}$$

en posant $x_1=y$ et $x_2=a\mid y$ dans la formule (2.2).

Nous avons également

$$D_n(x,ab^2)=\sum_{j=0}^{\lfloor n|2\rfloor}\frac{n}{n-j}\binom{n-j}{j}(-a)^j b^n b^{-(n-2j)}x^{n-2j}=b^n\ D_n(b^{-1}x,a),\ \forall a,b\in F,\ b\neq 0. \tag{2.6}$$

Théoréme 2.3.6 *Le polynôme de Dickson $D_n(x,a), a\in\mathbb{F}_q^*$ est un polynôme de permutation de $\mathbb{F}_q$ si et seulement si* $\gcd(n,q^2-1)=1$.

Démonstration. *Supposons que $D_n(b,a)=D_n(c,a)$ pour $b,c\in\mathbb{F}_q$. Nous pouvons trouver deux éléments $\alpha,\beta\in\mathbb{F}_{q^2}^*$ tels que $\beta+a\beta^{-1}=b$ et $\gamma+a\gamma^{-1}=c$. D'après , $\beta^n+a^n\beta^{-n}=\gamma^n+a^n\gamma^{-n}$, donc $(\beta^n-\gamma^n)(\beta^n\gamma^n-a^n)=0$, d'où donc $\beta^n=\gamma^n$ ou $\beta^n=(a\gamma^{-1})^n$.*
Si $\gcd(n,q^2-1)=1$, *alors x^n est un polynôme de permutation de $\mathbb{F}_{q^2}$ d'après l'exemple 2.3.3, ce qui implique que $\beta=\gamma$ ou $\beta=a\gamma^{-1}$. Dans les deux cas, on a $b=c$, et ainsi le polynôme $D_n(x,a)$ est un polynôme de permutation de $\mathbb{F}_q$.*
Supposons maintenant que $\gcd(n,q^2-1)=d>1$.*Si d est pair , alors q est impair et n est pair. Puisque $D_n(x,a)$ contient seulement des puissances paires de x, nous avons $D_n(c,a)=D_n(-c,a)$ pour $c\in\mathbb{F}_q$, mais pour $c\neq -c$, par conséquent $D_n(x,a)$ n'est pas un polynôme de permutation de $\mathbb{F}_q$. Si d est impair, alors il existe un nombre premier impair r divisant d. Donc r divise n, et $q-1$ ou $q+1$ est divisible par r. Nous distinguons donc deux cas. Dans le premier cas, $x^r=1$ admet r solutions dans $\mathbb{F}_q$, ainsi il existe $b\in\mathbb{F}_q, b\neq 1,a$ avec $b^r=1$. Donc $b^n=1$, et ainsi d'après (2.5), nous avons*

$$D_n(b+ab^{-1},a)=1+a^n=D_n(1+a,a).$$

Puisque $b+ab^{-1}=1+a$ impliquerait $b=1$ ou $b=a$, nous avons $b+ab^{-1}\neq 1+a$. Par conséquent $D_n(x,a)$ n'est pas un polynôme de permutation de $\mathbb{F}_q$. Dans le deuxième cas,

soit $\gamma \in \mathbb{F}_{q^2}$ un solution de $x^{q+1} = a$; Puisque $x^r = 1$ admet r solutions dans $\mathbb{F}_{q^2}$, il existe $\beta \in \mathbb{F}_{q^2}$, $\beta \neq 1, a\gamma^{-2}$ avec $\beta^r = 1$. Nous avons donc $\beta^{q+1} = 1$ et $\beta^n = 1$, par conséquent d'après (2.5),

$$D_n(\gamma + a\gamma^{-1}, a) = D_n(\beta\gamma + a(\beta\gamma)^{-1}, a).$$

Nous avons $\gamma + a\gamma^{-1} = \gamma + \gamma^q \in \mathbb{F}_q$, et $\beta\gamma + a(\beta\gamma)^{-1} = \beta\gamma + (\beta\gamma)^q \in \mathbb{F}_q$. Nous avons également $\beta\gamma + a(\beta\gamma)^{-1} \neq \gamma + a\gamma^{-1}$ car sinon, $\beta = 1$ ou $\beta = a\gamma^{-2}$, ainsi $D_n(x, a)$ n'est pas un polynôme de permutation de $\mathbb{F}_q$. ■

Définition 2.3.5 *Soit $a \in \mathbb{F}_q$, pour tous entiers positifs n et k, on définit le $n^{ème}$ polynôme de Dickson de $(k+1) - ième$ espèce $D_{n,k}(x, a)$ sur $\mathbb{F}_q$ par*

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

On note les polynômes de Dickson de première espèce par $D_n(x, a)$.

Pour $n = 0$, on pose $D_{0,k}(x, a) = 2 - k$.

2.4 Formulaire (Polynômes de Dickson de première et deuxième espèces)

2.4.1 Expression des coefficients

$$\begin{aligned}
D_0(X, a) &= 2, \\
D_n(X, a) &= \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{n}{n-k} \begin{pmatrix} n-k \\ k \end{pmatrix} (-a)^k X^{n-2k} \text{ si } n > 0, && (2.7) \\
E_0(X, a) &= 1, && (2.8) \\
E_n(X, a) &= \sum_{k=0}^{\lfloor n/2 \rfloor} \begin{pmatrix} n-k \\ k \end{pmatrix} (-a)^k X^{n-2k} sin > 0. && (2.9)
\end{aligned}$$

2.4.2 Relations de récurrence

$$D_n(X,a) = XD_{n-1}(X,a) - aD_{n-2}(X,a), \tag{2.10}$$

$$E_n(X,a) = XE_{n-1}(X,a) - aE_{n-2}(X,a). \tag{2.11}$$

$$\begin{pmatrix} D_{n+1}(X,a) \\ D_n(X,a) \end{pmatrix} = \begin{pmatrix} X & -a \\ 1 & 0 \end{pmatrix} \begin{pmatrix} D_n(X,a) \\ D_{n-1}(X,a) \end{pmatrix} \tag{2.12}$$

$$\begin{pmatrix} E_{n+1}(X,a) \\ E_n(X,a) \end{pmatrix} = \begin{pmatrix} X & -a \\ 1 & 0 \end{pmatrix} \begin{pmatrix} E_n(X,a) \\ E_{n-1}(X,a) \end{pmatrix} \tag{2.13}$$

2.4.3 Équations fonctionnelles

$$D_n\left(U + \frac{a}{U}, a\right) = U^n + \left(\frac{a}{U}\right)^n.$$

$$E_n\left(U + \frac{a}{U}, a\right) = \frac{U^{n+1} - \left(\frac{a}{U}\right)^{n+1}}{U - \frac{a}{U}}. \tag{2.14}$$

$$\overline{E}_n\left(U + \frac{a}{U}, a\right) = \frac{U^n - \left(\frac{a}{U}\right)^n}{U - \frac{a}{U}}. \tag{2.15}$$

2.4.4 Séries génératrices

$$\sum_{n\geq 0} D_n(X,a)Z^n = \frac{2 - XZ}{1 - XZ - aZ^2}, \tag{2.16}$$

$$\sum_{n\geq 0} E_n(X,a)Z^n = \frac{1}{1 - XZ - aZ^2}. \tag{2.17}$$

$$\sum_{n\geq 0} \overline{E}_n(X,a)Z^n = \frac{Z}{1 - XZ - aZ^2}. \tag{2.18}$$

2.4.5 Équations différentielles

D_n et E_n et $\overline{E}_n$ sont respectivement solutions de

$$\left(x^2 - 4a\right) y" + xy' - n^2 y = 0, \tag{2.19}$$

$$\left(x^2 - 4a\right) y" + 3xy' - n\left(n+2\right) y = 0 \tag{2.20}$$

$$\left(x^2 - 4a\right) y" + 3xy' - \left(n^2 - 1\right) y = 0. \tag{2.21}$$

2.4.6 Premiers termes

n	D_n	E_n
0	2	1
1	X	X
2	$X^2 - 2a$	$X^2 - a$
3	$X^3 - 3aX$	$X^3 - 2aX$
4	$X^4 - 4aX^2 + 2a^2$	$X^4 - 3aX^2 + a^2$
5	$X^5 - 5aX^3 + 5a^2X$	$X^5 - 4aX^3 + 3a^2X$
6	$X^6 - 6aX^4 + 9a^2X^2 - 2a^3$	$X^6 - 5aX^4 + 6a^2X^2 - a^3$
7	$X^7 - 7aX^5 + 14a^2X^3 - 7a^3X$	$X^7 - 6aX^5 + 10a^2X^3 - 4a^3X$

2.4.7 Relations mutuelles

$$\begin{cases} D_n(X,a) = 2E_n(X,a) - XE_{n-1}(X,a). \\ (X^2-4a)\,\overline{E}_n(X,a) = 2D_{n+1}(X,a) - XD_n(X,a). \end{cases}$$

$$E_n(X,a) - D_n(X,a) = aE_{n-2}(X,a).$$

2.4.8 Formules de duplication

$$\begin{cases} D_{2n}(X,a) = D_n^2(X,a) - 2a^n \\ \bar{E}_{2n}(X,a) = D_n(X,a)\bar{E}_n(X,a) \end{cases}$$

$$\begin{cases} D_{2n+1}(X,a) = D_{n+1}(X,a)D_n(X,a) - a^nX \\ \overline{E}_{2n+1}(X,a) = \overline{E}_{n+1}^2(X,a) - \alpha\overline{E}_n^2(X,a) \end{cases}$$

2.4.9 Propriétés multiplicatives

$$\begin{cases} D_{mn}(X,a) = D_m\left(D_n(X,a), a^n\right) \\ \bar{E}_{mn}(X,a) = \overline{E}_m\left(D_n(X,a), a^n\right)\overline{E}_n(X,a) \end{cases}$$

2.4.10 Propriétés additives

$$\begin{cases} D_{n+m}(X,a) = D_n(X,a)D_m(X,a) - a^m D_{n-m}(X,a) \\ E_{n+m}(X,a) = E_n(X,a)E_m(X,a) - aE_{n-1}(X,a)E_{m-1}(X,a) \\ E_{n+m}(X,a) = \overline{E}_n(X,a)\overline{E}_{m+1}(X,a) - a\overline{E}_{n-1}(X,a)\overline{E}_m(X,a) \end{cases}$$

2.4.11 Équation de Pell-Fermat

$$D_n^2(X,a) - \left(X^2 - 4a\right)\overline{E}_n^2(X,a) = 4a^n.$$

2.4.12 Lien avec d'autres suites et polynômes

Nombres de Lucas : $D_n(1,-1)$

Nombres de Fibonacci : $\overline{E}_n(1,-1)$

Nombres de Mersenne : $\overline{E}_n(3,2)$

Nombres de Fermat : $D_{2^n}(3,2)$

2.4.13 Polynômes de Tchebychev

$$\begin{cases} D_n(2aX, a^2) = 2a^n T_n(X). \\ E_n(2aX, a^2) = a^n U_n(X). \end{cases}$$

Chapitre 3

Polynômes de Dickson involutifs sur un corps de caractéristique 2

3.1 Introduction

Un polynôme de permutation $F(x)$ sur un corps fini est appelé involution si $F \circ F(x) = x$. La notion d'involution est importante en cryptographie symétrique. Dans ce chapitre, Nous exposons les résultats d'un article de "Pascale Charpin, Sihem Mesnager et Sumanta Sarkar" (2015) sur les polynômes de Dickson de première espèce dans $\mathbb{F}_2[x]$ qui sont des involutions. Nous donnons donc quelques propriétés des polynômes de Dickson de première espèce sur $\mathbb{F}_2$ ainsi que plusieurs résultats avec des démonstrations détaillées.

Pour plus de détails se référer à [5].

3.2 Rappels sur les polynômes de Dickson de première espèce

Définition 3.2.1 *Un polynôme de Dickson de* $1^{ère}$ *espèce de degré* k *à une indéterminée* x*, de paramètre* $a \in \mathbb{F}_{2^n}^*$ *est défini par*:

$$D_k(x,a) = \sum_{i=0}^{[k/2]} \frac{k}{k-i}\binom{k-i}{i} a^i x^{k-2i},\ k \geq 2,$$

où $[k/2]$ *désigne la partie entière de* $k/2$.

On pose $a = 1$. Dans la suite, les polynômes $D_k(x,1)$ seront notés $D_k(x)$.

Le polynôme de Dickson $D_k \in \mathbb{F}_2[x]$ est défini par la relation de récurrence

$$D_0(x) = 0 \text{ et } D_1(x) = x.$$
$$D_{i+2}(x) = xD_{i+1}(x) + D_i(x).$$

En utilisant cette définition, on peut montrer les propriétés suivantes

Proposition 3.2.1 *1.* $deg(D_i) = i$,

2. $D_{2i}(x) = (D_i(x))^2$,

3. $D_{ij}(x) = D_i(D_j(x))$,

4. $D_i(x + x^{-1}) = x^i + x^{-i}$,

$\forall x$, et $\forall\ i, j$ entiers positifs.

Théoréme 3.2.1 *Le polynôme de Dickson* $D_k \in \mathbb{F}_2[x]$ *est un polynôme de permutation sur* $\mathbb{F}_{2^n}$ *si, et seulement si,*

$$\gcd\left(k, 2^{2n} - 1\right) = 1.$$

3.3 Symboles de Legendre et Jacobi

On rappelle qu'un entier a est dit résidu quadratique modulo un nombre premier p si, et seulement si, il existe un entier u tel que $a \equiv u^2 \pmod{p}$.

Définition 3.3.1 *Soit* P *un entier impair,* $P > 2$ *, et* $P = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$*, la décompsition de* P *en facteurs premiers . Soit* a *un entier. Le symbole de Jacobi de* a *est*

$$Jac(a, P) = \left(\frac{a}{p}\right) = \left(\frac{a}{p_1}\right)^{a_1} ... \left(\frac{a}{p_k}\right)^{a_k},$$

où $\left(\frac{a}{p_i}\right)$*, appelé symbole de Legendre, est défini comme suit*:

$$\left(\frac{a}{p_i}\right) = \begin{cases} 0 \text{ si } p_i \text{ divise } a \\ 1 \text{ si } a \text{ est résidu quadratique } \pmod{p_i} \\ \text{ie, } \exists k > 0 \text{ tel que } a \equiv k^2 \pmod{p_i} \\ -1 \text{ si } a \text{ n'est pas résidu quadratique} \pmod{p_i} \end{cases}$$

Soient $a, b \in \mathbb{Z}$, nous avons les propriétés suivantes :

$$\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right) \tag{3.1}$$

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}} \; et \left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}. \tag{3.2}$$

$$a \equiv b \,(\mathrm{mod}\, P) \Rightarrow \left(\frac{a}{P}\right) = \left(\frac{b}{P}\right). \tag{3.3}$$

Remarquons que si $Jac\,(a, b) = -1$, alors a n'est pas résidu quadratique $(\mathrm{mod}\, P)$.

3.4 Polynômes de Dickson induisant des involutions

Posons $n = 2m$ et k un entier tel que $pgcd\,(k, 2^n - 1) = 1$. Alors D_k permute $\mathbb{F}_{2^m}$.

Dans cette partie nous allons décrire l'ensemble des k tels que D_k soit une involution de $\mathbb{F}_{2^m}$, pour m fixé.

Lemma 3.4.1 *On pose $n = 2m$, alors $\forall x \in \mathbb{F}_{2^m}$, $\exists \gamma \subset \mathbb{F}_{2^n}^*$, tel que $x = \gamma + \gamma^{-1}$. L'élément γ vérifie $\gamma^{2^m-1} = 1$ ou $\gamma^{2^m+1} = 1$.*

Démonstration. Pour tout $x \in \mathbb{F}_{2^m}$, il existe γ tel que : $x = \gamma + \gamma^{-1}$ si, et seulement si, $\gamma^2 + \gamma x + 1 = 0$ admet une solution dans $\mathbb{F}_{2^n}^*$.
On a : $\gamma + \gamma^{-1} \in \mathbb{F}_{2^m}$ si, et seulement si , $\left(\gamma + \frac{1}{\gamma}\right)^{2^m} = \gamma + \frac{1}{\gamma}$, c'est à dire

$$\left(\gamma^{2^m} + \gamma\right)\left(\gamma^{2^m+1} + 1\right) = 0.$$

■

Théoréme 3.4.1 *Soit k et l deux entiers non nuls. Alors*

$$D_k\,(x) \equiv D_l\,(x) \left(\mathrm{mod}\, x^{2^m} + x\right)$$

si, et seulement si,

$$k \equiv l \,(\mathrm{mod}\, 2^m - 1) \;\; ou \; k \equiv -l \,(\mathrm{mod}\, 2^m - 1)$$

$$et$$

$$k \equiv l \,(\mathrm{mod}\, 2^m + 1) \;\; ou \; k \equiv -l \,(\mathrm{mod}\, 2^m + 1).$$

Démonstration. Supposons que $D_k(x) \equiv D_l(x)\ \forall x \in \mathbb{F}_{2^m}$. Par le lemme, en posant $x = \gamma + \gamma^{-1}$ et en appliquant la proposition

$$D_k(x) = \gamma^k + \left(\frac{1}{\gamma}\right)^k \equiv D_l(x) = \gamma^l + \left(\frac{1}{\gamma}\right)^l,$$

où $\gamma \in \mathbb{F}_{2^n}^*$ tel que $\gamma^{2^m-1} = 1$ ou $\gamma^{2^m+1} = 1$.

Donc

$$D_k(x) = \gamma^k + \left(\frac{1}{\gamma}\right)^k \equiv D_l(x) = \gamma^l + \left(\frac{1}{\gamma}\right)^l$$

devient

$$\gamma^l\left(\gamma^{2k}+1\right) + \gamma^k\left(\gamma^{2l}+1\right) = 0 \Leftrightarrow \left(\gamma^l + \gamma^k\right)\left(\gamma^{l+k}+1\right) = 0.$$

D'où

$$D_k(x) = \gamma^k + \left(\frac{1}{\gamma}\right)^k \equiv D_l(x) = \gamma^l + \left(\frac{1}{\gamma}\right)^l$$

est équivalent à $\gamma^{l+k} = 1$ ou $\gamma^{k-l} = 1$.

Soit α une racine primitive de $\mathbb{F}_{2^n}$. On peut donc considérer deux formes pour γ : $\gamma = \alpha^{s(2^m-1)}$ et $\gamma = \alpha^{t(2^m+1)}$, pour s, t entiers.

Donc

$$D_k(x) = \gamma^k + \left(\frac{1}{\gamma}\right)^k \equiv D_l(x) = \gamma^l + \left(\frac{1}{\gamma}\right)^l$$

est vérifié pour γ si, et seulement si, on a les deux conditions suivantes :

- si $\gamma = \alpha^{s(2^m-1)}$ alors $k \pm l \equiv 0 \pmod{2^m+1}$;
- si $\gamma = \alpha^{t(2^m+1)}$ alors $k \pm l \equiv 0 \pmod{2^m-1}$.

■

On peut décrire maintenant les cas où

$$D_k(x) \equiv x \bmod \left(x^{2^m} + x\right).$$

Corollaire 3.4.1 *Soit $n = 2m$. On définit*

$$K_n = \left\{k \mid 1 \le k \le 2^n - 1,\ D_k(x) \equiv x \pmod{x^{2^m} + x}\right\}.$$

Alors

$$K_n = \{1, 2^m, 2^n - 2^m - 1, 2^n - 2\}.$$

Démonstration. En appliquant le théorème précédent au cas $l = 1$, k est une solution des quatres congruences modulo $(2^n - 1)$:

1. $k \equiv 1 \pmod{2^m - 1}$ et $k \equiv 1 \pmod{2^m + 1}$.
2. $k \equiv 1 \pmod{2^m - 1}$ et $k \equiv -1 \pmod{2^m + 1}$.
3. $k \equiv -1 \pmod{2^m - 1}$ et $k \equiv 1 \pmod{2^m + 1}$.
4. $k \equiv -1 \pmod{2^m - 1}$ et $k \equiv -1 \pmod{2^m + 1}$.

   Si $k < 2^m - 1$, alors $k = 1$, d'après (1).

   $k = 2^m$ est une solution de (2) .

   On suppose donc $k > 2^m$. (1) implique que $(2^m - 1)$ et $(2^m + 1)$ divise $k - 1$. Comme $2^m - 1$ et $2^m + 1$ sont impairs et premiers entre eux, donc l'unique solution de (1) est 2^n on a $2^n \equiv 1$ modulo $(2^n - 1)$.

   Nous avons également, (4) implique que $2^n - 1$ divise $(k + 1)$ donc $k = 2^n - 2$ est une solution de (4).

   La congruence (2) implique que $(2^m - 1)$ divise $k - 1$ donc $k = 2^n - 2$ est l'unique solution de (4).

   La congruence (2) entraine que $(2^m - 1)$ divise $k - 1$ et $(2^m + 1)$ divise $(k + 1)$. Donc il existe b tel que

$$k = b\,(2^m - 1) + 1 = b\,(2^m + 1) - 2b + 1,$$

   c'est à dire que

$$k + 1 = -2b + 2mod\,(2^m + 1)\,.$$

   Ce qui implique que $b \equiv 1 \bmod (2^m + 1)$, d'où $b = 1$. Par conséquent $k = 2^m$.

   La congruence (3) implique que $(2^m - 1)$ divise $(k + 1)$ et $(2^m + 1)$ divise $(k - 1)$. Donc il existe b telque

$$k = b\,(2^m + 1) + 1 = b\,(2^m - 1) + 2b + 1,$$

   c'est à dire que

$$k + 1 \equiv 2b + 2 \bmod (2^m - 1)\,,$$

   d'où $b \equiv -1 \bmod (2^m - 1)$ et donc $b = 2^m - 2$. Par conséquent

$$k = (2^m - 2)\,(2^m + 1) + 1 = 2^{2m} - 2^m - 1.$$

■

Lemma 3.4.2 *Soit $n = 2m$. Alors*

1. $2^n - 2^m - 1$ *et* $2^n - 2$ *sont non résidus quadratiques modulo* $2^n - 1$.

2. 2^m *est un résidu quadratique modulo* $2^n - 1$ *si, et seulement si,* m *est pair et les racines carrées sont* $2^{m/2}S_n$*, où les* S_n *sont les racines carrées de* 1 *modulo* $2^n - 1$.

Démonstration. Comme $2^n - 1 \equiv 3 (\mathrm{mod}\, 4)$, $2^{n-1} - 1$ est un entier impair. Alors on a

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

Par ailleurs, on a $2^n - 1 \equiv 7 (\mathrm{mod}\, 8), \forall\ n \geq 3$, ce qui implique que $\dfrac{(2^n-1)^2 - 1}{8}$ est un entier pair. D'où

$$\left(\frac{2}{2^n - 1}\right) = (-1)^{\dfrac{(2^n-1)^2-1}{8}} = 1,$$

en appliquant .

Donc $2^n - 2$ est non résidu quadratique modulo $(2^n - 1)$, en utilisant , puisque $-1 \equiv 2^m - 2 (\mathrm{mod}\, 2^n - 1)$.Ce qui implique aussi que

$$\left(\frac{2^n - 2^m - 1}{2^n - 1}\right) = \left(\frac{-2^m}{2^n - 1}\right) = \left(\frac{-1}{2^n - 1}\right)\left(\frac{2}{2^n - 1}\right)^m = -1,$$

puisque

$$-2^m \equiv 2^n - 2^m - 1 (\mathrm{mod}\, 2^n - 1).$$

Alors $2^n - 2^m - 1$ est non résidu quadratique modulo $2^n - 1$.

Par ailleurs, puisque n est pair, 3 divise $2^n - 1$. Comme 2 est non résidu quadratique modulo 3, c'est à dire que $\left(\frac{2}{3}\right) = -1$ donc $\left(\frac{2^m}{3}\right) = (-1)^m = 1$ si, et seulement si, m est pair. D'où, si m est impair, 2^m est non résidu quadratique modulo $2^n - 1$. Si m est pair, 2^m est un résidu quadratique modulo $2^n - 1$ puisque $\left(2^{m/2}\right)^2 \equiv 2^m \,\mathrm{mod}\, 2^n - 1$. Posons

$$S_n = \left\{u \mid 1 \leq u \leq 2^n - 2,\ u^2 \equiv 1 (\mathrm{mod}\, 2^n - 1)\right\}. \tag{3.4}$$

L'application $k \to 2^{m/2}k$ est bijective sur l'ensemble S_n des racines carrées de 1 modulo $2^n - 1$ avec l'ensemble des racines carrées de 2^m modulo $(2^n - 1)$. ■

Théoréme 3.4.2 *Soit* D_k *un polynôme de Dickson,* $1 \leq k \leq 2^n - 1$, $n = 2m$, $m \geq 2$. *Soit* S_n *défini précédemment, alors* D_k *est une involution sur* F_{2^m} *si, et seulement si,*

1. $k \in S_n$*, où* m *est impair.*

2. $k \in S_n \cup 2^{m/2}S_n$ *si* m *est pair.*

Démonstration. On considère $D_k(x) \bmod (x^{2^m} + x)$. Comme $\gcd(k, 2^n - 1) = 1$, D_k est une permutation de F_{2^m}. C'est une involution si, et seulement si,

$$D_k \circ D_k(x) = D_{k^2}(x) = x, \forall x \in F_{2^m}.$$

D'aprés le corollaire précédent, $k^2 \in \{1, 2^m\ ,\ 2^n - 2^m - 1, 2^n - 2\}$ où k^2 est calculé modulo $(2^n - 1)$. D'aprés le lemme, c'est équivalent à $k \in S_n$ si m est impair et $k \in S_n \cup 2^{m/2} S_n$, si m est pair. ■

3.5 L'ensemble des involutions de Dickson

Dans cette partie, nous considérons les involutions sur $\mathbb{F}_{2^n}$ et $n = 2m$.

Soit S_n comme défini précedemment et.

$$K_n = \{1, 2^m, 2^n - 2^m - 1, 2^n - 2\} \equiv \{\pm 1, \pm 2^m\} \pmod{2^n - 1}.$$

L'ensemble K_n est un sous-groupe multiplicatif de S_n. On Définit une relation d'équivalence sur S_n

$$s_1 \sim s_2 \text{ si et seulement si } \frac{s_1}{s_2} \in K_n.$$

Lemma 3.5.1 *On note $\sigma(s)$ la classe de $s \in S_n$. Alors $\sigma(s) = \{s, -s, 2^m s, -2^m s\}$ et nous avons*

$$D_t(x) \equiv D_s(x) \quad \left(\bmod x^{2^m} + x\right), \text{ pour } t \in \sigma(s).$$

Démonstration. Si s et t appartiennent à la même classe alors D_s et D_t induisent la même permutation sur $\mathbb{F}_{2^n}$. Par conséquent, il existe $k \in K_n$ tel que $t = ks$. Alors, d'aprés le corollaire 8 et la proposition 2,on a pour $x \in \mathbb{F}_{2^n}$,

$$D_t(x) = D_{sk}(x) = D_s \circ D_k(x) = D_s(x) \bmod \left(x^{2^m} + x\right).$$

■

Donc toute classe distincte de la classe de 1 entraîne une involution non triviale. La composition des polynômes de Dickson est stable et la commutativité des entiers entraine la commutativité de la loi de composition. Donc, si D_s et D_t sont deux involutions non triviales sur $\mathbb{F}_{2^m}$ alors :

$$(D_s \circ D_t)^{-1} = D_t^{-1} \circ D_s^{-1} = D_t \circ D_s = D_{ts} = D_{st}.$$

Montrons que D_{st} est une involution. Si s et t sont dans la même classe alors $D_{st} = D_{s^2}$, d'après le lemme, où s est une racine carrée de 1, alors $D_{st}(x) \equiv x \left(\mathrm{mod}\, x^{2^m} + x\right)$.
Nous supposons que $t \notin \sigma(s)$. Si $t \in \sigma\left(2^{m/2}s\right)$ alors $D_{st} = \left(D_{s^2}\right)^{2^{m/2}}$ donc $D_{st}(x) \equiv x^{m/2} \left(\mathrm{mod}\, x^{2^m} + x\right)$.Dans d'autres cas, il y a plus de 4 classes et $st \pmod{2^n - 1} = r$, où r n'est pas dans les classes $\left\{s, t, 2^{m/2}, 2^{m/2}s\right\}$.

Lemma 3.5.2 *Si D_s et D_t sont deux involutions de Dickson de $\mathbb{F}_{2^m}$ alors $D_s \circ D_t = D_{st}$ est une involution. Par ailleurs, on a*

1. *Si $t \in \sigma(s)$ alors $st \bmod (2^n - 1) \in \sigma(1)$.*
2. *Si $t = 2^{m/2}$ (m pair) alors $st \in \sigma\left(2^{m/2}s\right)$.*
3. *Si $t \in \sigma\left(2^{m/2}s\right)$ (m pair) alors $st \bmod (2^n - 1) \in \sigma\left(2^{m/2}\right)$.*
4. *Si s et t sont des représentants de classes non triviales alors $st \bmod (2^n - 1) = r$, où r est un représentent d'une classe non triviale.*

Remarque 3.5.1 *Notons que les trois premières propositions sont des équivalences*:
$st \in \sigma(u)$ est équivalent à $t \in \sigma(us^{-1}) \pmod{2^n - 1} = \sigma(us)$ (s est un résidu quadratique de 1 modulo $2^n - 1$, son inverse modulo $2^n - 1$ est le même).

Exemples 3.5.1 $n = 6, m = 3$:

$$k_6 = \{1, 8, 55, 62\} = S_6.$$

Pour $k \in K_6$, $D_k(x) \equiv x \bmod (x^8 + x)$. Par exemple

$$D_{55}(x) = x + x^{33} + x^9 + x^{41} + x^{49} + x^5 + x^{37} + x^{53} + x^7 + x^{39} + x^{55} \equiv x \bmod \left(x^8 + x\right).$$

Exemples 3.5.2 $n = 8, m = 4$:

$$K_8 = \{1, 16, 239, 254\} \text{ et } S_8 = \{1, 16, 86, 101, 154, 169, 239, 254\}.$$

Notons que $-86 = 169$, $86 \times 16 = 101$et $86 \times (-16) = 154$, nous remarquons aussi que $D_k(x) \pmod{x^{16} + x}$ où $k \in (S_8 \cup 4S_8) \setminus K_8$. Nous obtenons trois D_k qui sont les représentants des trois classes :

$$k \in \{4, 64, 191, 251\} \cup \{86, 101, 154, 169\} \cup \{89, 149, 106, 166\}.$$

Par exemple

$$D_4(x) = x^4 \left(\mathrm{mod}\, x^{16} + x\right)$$

$$\begin{aligned} D_{86}(x) &= x^2 + x^6 + x^{10} + x^{18} + x^{22} + x^{34} + x^{38} + x^{42} + x^{86} + x^{74} + x^{82} + x^{66} + x^{70} \\ &= x^2 + x^3 + x^4 + x^8 + x^{12} + x^{11} + x^{14} \quad \left(\mathrm{mod}\, x^{16} + x\right). \end{aligned}$$

Et avec $89 \equiv 86 * 4 \,(\mathrm{mod}\, 255)$

$$\begin{aligned} D_{89}(x) &= (D_{86})^4 \\ &= x^2 + x^3 + x^{12} + x^8 + x^{11} + x + x^{14} \left(\mathrm{mod}\, x^{16} + x\right). \end{aligned}$$

Exemples 3.5.3 $n = 10, m = 5$:

$$K_{10} = \{1, 32, 991, 1022\},$$

et

$$S_{10} = \{1, 32, 340, 373, 650, 683, 991, 1022\}.$$

Nous avons une involution non triviale unique avec $\mathbb{F}_{2^5} : D_{340}$.

3.5.1 Le nombre d'involutions de Dickson

Nous calculons maintenant le nombre de polynôme de Dickson qui induisent des involutions sur $\mathbb{F}_{2^m}$, nous commençons par un résultat technique.

Lemma 3.5.3 *Le nombre de résidus quadratiques de* 1 *modulo* $2^n - 1$ *est égal à* 2^τ *où* τ *est le nombre de facteurs premiers dans la décomposition de* $2^n - 1$.

Démonstration. Soit p un nombre entier positif et notons $\rho(p)$ le nombre de racines carrées de l'unité modulo p, c.-à-d., le nombre de solutions de l'équation de congruence :

$$x^2 \equiv 1 \,(\mathrm{mod}\, p).$$

Nous allons montrer que

$$\rho(pq) = \rho(p)\,\rho(q), \text{ où } p \text{ et } q \text{ sont copremiers.}$$

Notons que selon le théorème Chinois, $\mathbb{Z}/(pq)\mathbb{Z}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ par l'isomorphisme

$$\psi : \; x \in \mathbb{Z}/(pq)\mathbb{Z} \mapsto (x \pmod p, x \pmod q).$$

Par la construction, dans $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, $(a,b)^2 = (c,d)$ est équivalent à $a^2 = c$ et $b^2 = d$, tel que

$$\psi\left(x^2\right) = \left(x^2 \left(\mathrm{mod}\, p\right), x^2 \left(\mathrm{mod}\, q\right)\right).$$

On a $\rho\left(p^\alpha\right) = 2$ pour tout nombre premier p et nombre entier positif α. En effet, supposons que $x^2 \equiv 1 \left(\mathrm{mod}\, p^\alpha\right)$. Alors

$$x^2 - 1 = (x+1)(x-1) \equiv 0 \pmod{p^\alpha},$$

Ce qui est équivalent à

$$x + 1 \equiv 0 \pmod{p^\alpha} \qquad \text{ou} \qquad x - 1 \equiv 0 \pmod{p^\alpha},$$

alors $x \equiv \pm 1$ *mod* p^α. Puisque $2^n - 1$ est un nombre impair, nous pouvons écrire

$$2^n - 1 = \prod_{i=1}^{\tau} p_i^{\alpha_i},$$

où p_i est un facteur premier et les α_i sont des nombres entiers positifs. Donc

$$\rho\left(2^n - 1\right) = \prod_{i=1}^{\tau} \rho\left(p_i^{\alpha_i}\right) = 2^\tau.$$

■

Théoréme 3.5.1 *Soit m un nombre entier positif tel que $m > 1$ et $n = 2m$. Soit τ le nombre de facteurs premiers dans la décomposition de $2^n - 1$. Alors le nombre (non trivial) de polynômes de Dickson sur $\mathbb{F}_{2^m}$ qui sont des involutions est égal à*

$$2^{\tau-2} - 1 \text{ } \textit{si } m \textit{ est impair et } 2^{\tau-1} - 1 \text{ } \textit{si } m \textit{ est pair.}$$

Démonstration. Supposons que m est impair, d'après le théorème, D_k est une involution si, et seulement si, $k \in S_n$, où k est un résidu quadratique de 1 modulo $2^n - 1$. Le nombre k est égal à 2^τ d'après le Lemme. Maintenant, d'après le lemme, le nombre de polynômes de Dickson est égal à $2^\tau/4 = 2^{\tau-2}$ où K_n est de la cardinal 4. Supposons que m est pair. L'étude est la même que dans le cas impair sauf que, dans le cas pair, D_k est une involution si, et seulement, $k \in S \cup 2^{m/2}S$. Cela signifie que nous devons remplacer 2^τ par $2^{\tau+1}$ dans les calculs précédents. Nous concluons en excluant la classe de 1. ■

Exemples 3.5.4 $n = 6$, $m = 3$, $2^n - 1 = 63 = 3^2 \times 7$, $\tau = 2$. *Le nombre de polynômes non triviaux de Dickson qui sont des involutions est égal à $2^{\tau-2} - 1 = 0$, c'est-à-dire qu'il n'y a aucun polynôme de Dickson qui soit une involution, excepté $D_1(x) = x$.*

$n = 8$, $m = 4$, $2^n - 1 = 255 = 17 \times 5 \times 3$, $\tau = 3$.Le nombre de polynôme non triviaux de Dickson qui sont des involutions est égal à $2^{\tau-1} - 1 = 3$.

$n = 10,\ m = 5$, $2^n - 1 = 1023 = 31 \times 11 \times 3$, $\tau = 3$.Le nombre de polynôme non triviaux de Dickson qui sont des involutions est égal à $2^{\tau-2} - 1 = 1$.

$n = 12$, $m = 6$, $2^n - 1 = 4095 = 3^2 \times 5 \times 7 \times 13$, $\tau = 4$.Le nombre de polynôme non triviaux de Dickson qui sont des involutions est égal à $2^{\tau-1} = 8$.
Un ensemble de représententents de ces classes est :

$$\{1, 181, 1574, 1756\} \cup \{8, 1448, 307, 1763\} \subset S_{12} \cup 8 * S_{12}.$$

Notons que $181 * 1574 = -1756 \bmod 4095$.

Bibliographie

[1] R. Lidl et H. Niedderreiter, Finite Fields, Encyclopedia of Mathematics and its Apllications 20, Addison-Wesley.

[2] Mullen, Dickson polynomials over finite fields, Adv. Math. (China) 20 (1991) 24–32.

[3] A. Cherchem, Cours Master, 2014.

[4] M. Waldschmidt, Introduction à la théorie des corps finis, 6, 7, 11, 14 Janvier 2015, Université Houari Boumediene, Alger.

[5] P. Charpin, S. Mesnager et S. Sarkar, Cryptology ePrint Archive : Report 2015/434.

[6] T. Berger, A. Canteaut, P. Charpin et Y. Laigle-Chapuy, Almost perfect nonlinear functions. Rapport de recherche INRIA, 5774, 2005.