Projet de Recherche . 2020-2021

Faculté des Sciences et Techniques
Master 1 - Maths. CRYPTIS

Polynômes de Permutations

A l'attention de :
M. NECER

Rédigé par :
PIARD A.
JACQUET R.
CARVAILLO T.

Table des matières

Introduction

1 Construction des Corps Finis

1.1 Existence et unicité

Soit $\mathbb{K}$ un corps quelconque et soit φ le morphisme suivant :

$$\varphi : \left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{K} \\ n & \longmapsto & n \cdot 1_{\mathbb{K}} \end{array} \right.$$

Définition 1. Soit $\mathbb{K}$ un corps quelconque. Toute partie $\mathcal{P}$ de $\mathbb{K}$ vérifiant :

- $\mathcal{P}$ est non vide et est une partie stable pour $+$ et $\times$ de $\mathbb{K}$ et $\mathcal{P}$ muni des lois induites par celles de $\mathbb{K}$ est lui-même un corps.
- $\mathcal{P}$ est un sous anneau de $\mathbb{K}$, $1 \in \mathcal{P}$ et $(p \in \mathcal{P}^* = \mathcal{P} - \{0\} \Rightarrow p^{-1} \in \mathcal{P}^*)$.
- $\mathcal{P}$ est un sous groupe de $(\mathbb{K}, +)$ et $\mathcal{P}^*$ muni de la loi $\times$ est un sous groupe multiplicatif $(\mathbb{K}^*, \times)$.

est appelée sous-corps de $\mathbb{K}$.

Définition 2. Soit $\mathbb{K}$ un corps quelconque.

- $\mathbb{K}$ est dit premier s'il ne contient aucun sous-corps strict.
- Si $\mathbb{K}$ est un corps, le sous-corps de $\mathbb{K}$ engendré par 1_K est un corps premier, c'est le sous-corps premier de $\mathbb{K}$.

Le noyau du morphisme φ est un idéal de $\mathbb{Z}$ et donc de la forme $k\mathbb{Z}$ pour $k \in \mathbb{Z}$. Par le premier théorème d'isomorphisme on a $\mathrm{Im}(\varphi) \cong \mathbb{Z}/n\mathbb{Z}$. Par intégrité de $\mathbb{Z}/n\mathbb{Z}$, $n = 0$ où n est un nombre premier. Si $n = 0$ alors φ est injective et donc le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Q}$. Si $n \neq 0$ alors le sous-corps premier est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et n s'appelle la **caractéristique** de $\mathbb{K}$.

Définition 3. Soient L et $\mathbb{K}$ deux corps. Si L/K est une extension de corps alors L est un espace vectoriel sur K, où l'addition vectorielle est l'addition dans L et la multiplication par un scalaire $K \times L$ est la restriction à $K \times L$ de la multiplication dans L. La dimension du K-espace vectoriel L est appelée le degré de l'extension et est notée $[L : K]$.

Définition 4. Soit P un polynôme sur un corps K. On appelle corps de décomposition de P sur K une extension L de K telle que :

- dans $L[X]$, P est produit de facteurs de degré 1,
- les racines de P engendrent L.

Proposition 1. *Soit P un polynôme sur un corps K. Alors P admet un corps de décomposition, unique à K-isomorphisme près.*

Proposition 2.

- *Le cardinal de* $\mathbb{K}$ *est une puissance de* p.
- *Réciproquement, pour tout* $n \in \mathbb{N}^*$, *il existe un corps* $\mathbb{K}$ *de cardinal* p^n. *En outre* $\mathbb{K}$ *est unique à isomorphisme près.*

Démonstration.

- Puisque le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ alors $\mathbb{K}$ est naturellement muni d'une structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. On note $n = [\mathbb{K} : \mathbb{Z}/p\mathbb{Z}]$ alors $\#\mathbb{K} = \#(\mathbb{Z}/p\mathbb{Z})^n = p^n$.
- Soit $n \in \mathbb{N}^*$. Si $\mathbb{K}$ est un corps fini de cardinal p^n alors $\mathbb{K}$ est le corps de décomposition de $X^{p^n} - X$ sur $\mathbb{Z}/p\mathbb{Z}$: en effet, puisque pour tout $x \in \mathbb{K}$, x est racine de $X^{p^n} - X$ donc $X^{p^n} - X$ possède ses p^n racines dans $\mathbb{K}$.
  Réciproquement, soit K le corps de décomposition de X^{p^n} sur $\mathbb{Z}/p\mathbb{Z}$. Soit $\mathcal{K}$ l'ensemble des éléments de K qui sont racines de $X^{p^n} - X$. On vérifie que $\mathcal{K}$ est un sous-corps de K. Puisque $1_K \in \mathcal{K}$, et si $x, y \in \mathcal{K}$ alors $x^{p^n} = x$ et $y^{p^n} = y$, donc $(x+y)^{p^n} x + y$ et $(xy^{-1})^{p^n} = xy^{-1}$, si bien que $x+y, xy^{-1} \in \mathcal{K}$. Par ailleurs la dérivée formelle, $(X^{p^n} - X)' = -1$ est premier avec $X^{p^n} - X$ donc les racines de $X^{p^n} - X$ sont simples. On en déduit alors que $\#\mathcal{K} = p^n$. Finalement $K = \mathcal{K}$ est un corps à p^n éléments et il est unique à isomorphisme près en vertu de l'unicité du corps de décomposition de $X^{p^n} - X$ sur $\mathbb{Z}/p\mathbb{Z}$.

$\square$

On notera dorénavant $\mathbb{F}_q$ **le** corps fini à $q = p^n$ éléments.

1.2 Construction

Soit $P \in \mathbb{F}_p[X]$ un polynôme irréductible sur $\mathbb{F}_p$. On note $n = \deg(P)$. Puisque P est irréductible, l'idéal (P) est donc maximal. Le quotient $\mathbb{F}_p[X]/(P)$ est le corps de rupture de P sur $\mathbb{F}_p$ de cardinal p^n. Afin de montrer que l'on peut toujours construire les corps finis nous allons montrer que pour tout $n \in \mathbb{N}^*$ il existe un polynôme irréductible sur $\mathbb{F}_p$ de degré n.

Proposition 3. *Soit* $n \in \mathbb{N}^*$, *on définit par*

$$\mathcal{P}(n,p) = \{P \in \mathbb{F}_p[X],\ P \text{ unitaire , irréductible de degré } n\}.$$

alors pour tout $n \in \mathbb{N}^*$ *on a,*

$$X^{p^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}(n,p)} P.$$

Démonstration. — Soit P un facteur irréductible de $X^{p^n} - X$ sur $\mathbb{F}_p$ de degré d. Le corps de rupture de P sur $\mathbb{F}_p$ est de cardinal p^d du corps de décomposition $X^{p^n} - X$ sur $\mathbb{F}_p$, c'est-à-dire F_{p^n}, donc d divise n.

- Réciproquement, on suppose que d divise n et soit $P \in \mathcal{P}(n,p)$. Soit α une racine de P dans le corps de rupture de P sur $\mathbb{F}_p$. Alors par le théorème ? on a $\mathbb{F}_p(\alpha) \simeq \mathbb{F}_{p^d}$. D'où α est racine de $X^{p^n} - X$. Or puisque P est irréductible, alors P est le polynôme minimal de α sur $\mathbb{F}_p$ donc P divise $X^{p^n} - X$. En outre les facteurs irréductible de$X^{p^n} - X$ sur $\mathbb{F}_p$ sont simple puisque P étant le polynôme minimal de α et que P divise $X^{p^n} - X$.

□

Corollaire 1. Soit $n \in \mathbb{N}^*$, il existe un polynôme irréductible sur $\mathbb{F}_p$ de degré n.

Démonstration. En conservant les notations de la proposition précédente, il s'agit de montrer que $\#\mathcal{P}(n,p) > 0$. Pour ce faire on évalue le degré de l'égalité

$$X^{p^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}(n,p)} P.$$

on a alors

$$p^n = \sum_{d|n} d \cdot \#\mathcal{P}(n,p)$$

On en déduit alors que pour tout $d \in \mathbb{N}^*$ on a $p^d \geq d \cdot \#\mathcal{P}(n,p)$, puis,

$$\begin{aligned} n \cdot \#\mathcal{P}(n,p) &= p^n - \sum_{d|n, d\neq n} d \cdot \#\mathcal{P}(n,p) \\ &\geq p^n - \sum_{d|n, d\neq n} p^d \\ &\geq p^n - \sum_{d=1}^{n-1} p^d \\ &\geq p^n - p\frac{p^{n-1}-1}{p-1} > 0 \end{aligned}$$

Puisque n est positif alors $\mathcal{P}(n,p) > 0$. □

2 Polynômes de permutations

Rappelons d'abord ce qu'est un polynôme dans le cas général.

Définition 5. Soit K un ensemble non vide. On appelle polynôme en l'indéterminée X, toute application

$$P : \left| \begin{array}{ccc} K & \longrightarrow & K \\ X & \longmapsto & \sum_{i=0}^{n} a_i X^i, a_i \in K. \end{array} \right.$$

Définition 6. Soit K un ensemble fini de cardinal $n \in \mathbb{N}^*$. Une permutation de K est une bijection de K dans K.

Définition 7. Soit P un polynôme de $\mathbb{F}_q[X]$. P est appelé **polynôme de permutation** de $\mathbb{F}_q$ si et seulement si la fonction associée

$$P : \left| \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ x & \longmapsto & P(x) \end{array} \right.$$

est une permutation, c'est-à-dire est bijective.

Exemples. On se place dans $\mathbb{F}_5$.

1. Le polynôme X^3 est un polynôme de permutation. En effet, l'application

$$P : \left| \begin{array}{ccc} \mathbb{F}_5 & \longrightarrow & \mathbb{F}_5 \\ x & \longmapsto & X^3 \end{array} \right.$$

est clairement bijective.

2. Le polynôme X^2 n'est pas un polynôme de permutation. Considérons l'application

$$P : \left| \begin{array}{ccc} \mathbb{F}_5 & \longrightarrow & \mathbb{F}_5 \\ x & \longmapsto & X^2 \end{array} \right.$$

En effet cette application n'est pas injective. Soient $(X, Y) \in (\mathbb{F}_5 \times \mathbb{F}_5)$. On a $P(X) = P(Y)$ si et seulement si $X^2 = Y^2$. En prenant $X = 2$ et $Y = 3$ on fausse l'injectivité.

De manière plus générale, nous avons pour $k \in \mathbb{N}$

Proposition 4. *X^k est un polynôme de permutation de $\mathbb{F}_q$ si et seulement si $pgcd(k, q-1) = 1$.*

Démonstration. $\Leftarrow$ Supposons que $pcgd(k, q-1) = 1$. Soit

$$P : \left| \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ x & \longmapsto & P(x) \end{array} \right.$$

Si $pcgd(k, q-1)$, i.e. si $k \nmid q-1$ ou $q-1 \nmid k$, il est évident que $x^k \neq 0 \; \forall x \in \mathbb{F}_q \backslash \{0\}$. Donc 0 est le seul antécédent de 0. $\mathbb{F}_q$ étant un corps, on a $\mathbb{F}_q^* = \mathbb{F}_q^{\times}$, donc $|\mathbb{F}_q^*| = q-1$. Soit α un générateur de $\mathbb{F}_q^*$. La théorie élémentaire des groupes nous donne $| < \alpha^k > | = \frac{q-1}{pcgd(k,q-1)}$. Et donc par hypothèse, $| < \alpha^k > | = q-1$. Donc $P(\alpha)$ engendre $P(\mathbb{F}_q^*)$ et par cardinalité nous obtenons la conclusion voulue.
$\Rightarrow$ Nous allons raisonner par contraposée, i.e. montrer que $pcgd(k, q-1) \neq 1 \Rightarrow X^k$ n'est pas un polynôme de permutation.
Supposons donc $pcgd(k, q-1) = m$, où $m \in \mathbb{N}$, on obtient donc

$$\begin{cases} k = k'.m \\ q-1 = q'.m \end{cases}$$

Et par suite, $k = k'.\frac{q-1}{q}$.
Donc, $X^k = X^{k'.\frac{q-1}{q}} = (X^{(q-1)})^{\frac{k'}{q'}} = 1$. Donc, $\forall x \in \mathbb{F}_q^{\times}$, $P(x) = 1$, l'application associé n'est donc pas bijective, par suite P n'est pas un polynôme de permutation. On obtient donc l'équivalence souhaitée. $\square$

3 Histoire de groupes...

3.1 Préliminaires, l'interpolation de Lagrange

Les motivations et descriptions analytiques détaillées de cette notion n'entrent pas dans le cadre de ce projet. Nous nous contenterons donc de rappeler, dans notre cadre, la :

Définition 8. Soit

$$\phi : \left| \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ x & \longmapsto & \phi(x) \end{array} \right.$$

Le problème est de trouver un polynôme P, de degré minimal $\leq q$, tel que

$$P(x) = \phi(x) \ \forall \in x \in \mathbb{F}_q.$$

Proposition 5 (Admise). *L'unique solution au problème présenté ci-dessus est donnée par*

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

Proposition 6. *De manière plus élégante, nous avons*

$$P(x) := \sum_{d \in \mathbb{F}_q} \phi(d)(1 - (x - d)^{q-1})$$

Démonstration. De manière générale, nous avons que $X^q - X = \displaystyle\prod_{c \in \mathbb{F}_q} (X - c)$, donc

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

En appliquant l'égalité précédente pour $x = d$, on obtient que

$$\prod_{c \in \mathbb{F}_q, c \neq d} (d - c) = -1$$

Finalement, on obtient que

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

et la proposition est ainsi prouvée. □

Remarque 1. Il est facile de voir que si ϕ est un polynôme, alors l'interpolation de Lagrange est une simple application du lemme chinois des restes.
Il suffit de considérer la solution P du système

$$\begin{cases}\phi\equiv 1 \pmod{X-c_1}\\ \phi\equiv 1 \pmod{X-c_2}\\ \ldots\\ \phi\equiv 1 \pmod{X-c_q}\end{cases}$$

pour s'en convaincre.

De cette remarque découle le fait que pour travailler sur des polynômes de permutation, il suffit de les regarder modulo X^q-X. Nous allons dès lors obtenir une structure intéressante, celle de groupe.

3.2 Un groupe, enfin !

Proposition 7. *L'ensemble* $\mathbb{P}\mathbb{o}\mathbb{l}\mathbb{y}$ *des polynômes de permutation sur* $\mathbb{F}_q$ *muni de la loi de composition* $\circ$ *est un groupe, i.e,* $(\mathbb{P}\mathbb{o}\mathbb{l}\mathbb{y},\circ)$ *est un groupe.*

Démonstration. Soient $P=\sum_{i\in[\![0,q]\!]}A_iX^i$, $Q=\sum_{j\in[\![0,q]\!]}B_jX^j$ et $R=\sum_{k\in[\![0,q]\!]}C_kX^k$ des polynômes à coefficients dans $\mathbb{F}_q$.

- ♣ La composée de deux polynômes est encore un polynôme. Il est de plus facile de remarquer que si l'on permute un ensemble deux foix, cela reste un ensemble permuté. La composition de deux polynôme de permutation est donc un polynôme de permutation. Nous avons donc notre loi interne.
- ♣ Montrons son assiocativité :
  D'une part, on a

$$(P\circ Q)\circ R$$

$$=\sum_{i\in[\![0,q]\!]}A_i\left(\sum_{j\in[\![0,q]\!]}B_jX^j\right)^i\circ\left(\sum_{k\in[\![0,q]\!]}C_kX^k\right)$$

$$=\sum_{i\in[\![0,q]\!]}A_i\left(\sum_{j\in[\![0,q]\!]}B_j\left(\left(\sum_{k\in[\![0,q]\!]}C_kX^k\right)\right)^j\right)^i$$

puis,

$$
\begin{aligned}
& P \circ (Q \circ R) \\
&= \left(\sum_{i\in[\![0,q]\!]} A_i X^i\right) \circ \left(\sum_{j\in[\![0,q]\!]} B_j \left(\left(\sum_{k\in[\![0,q]\!]} C_k X^k\right)\right)^j\right) \\
&= \sum_{i\in[\![0,q]\!]} A_i \left(\sum_{j\in[\![0,q]\!]} B_j \left(\left(\sum_{k\in[\![0,q]\!]} C_k X^k\right)\right)^j\right)^i
\end{aligned}
$$

donc la loi $\circ$ est associative.

- ♣ Le neutre est évidemment le polynôme constant égal à 1.
- ♣ Rappelons que, par définition, un polynôme de permutation est une application bijective de $\mathbb{F}_q$. Il suffit donc de considérer son application récipoque P^{-1} pour obtenir Q tel que $P \circ Q = 1$. Ceci nous donne l'élément neutre. Ceci marche toujours modulo $X^q - X$ car

$$
\Pi : \left| \begin{array}{rcl} \mathbb{F}_q[X] & \longrightarrow & \mathbb{F}_q[X]\backslash(X^q - X) \\ P & \longmapsto & [P]_{X^q-X} \end{array} \right.
$$

est un morphisme d'anneaux.

Il s'ensuit que $(\mathbb{P}\mathbb{o}\mathbb{l}\mathbb{y}, \circ)$ est un groupe. □

Proposition 8. *On a l'isomorphisme suivant,* $(\mathbb{P}\mathbb{o}\mathbb{l}\mathbb{y}, \circ) \cong \mathbb{S}_q$*, où* $\mathbb{S}_q$ *est le groupe des permutations de l'ensemble* $[\![1, ..., q]\!]$*.*

Démonstration. La difficulté de cette preuve réside dans le fait qu'un polynôme de $\mathbb{F}_q$ peut être représenté par une permutation très complexe et inversement. On rappelle que dans $\mathbb{S}_q$, toute permutation τ peut être représentée comme produit de transpositions. Dans notre cas il est suffisant de considérer les transpositions échangeant uniquement les éléments 0 et $a \in \mathbb{F}_q$ que l'on note $\tau_{0,a}$. Il vient alors que pour toutes transpositions de $\mathbb{S}_q$ échangeant deux éléments a et b de $\mathbb{F}_q$ on a,

$$\tau_{0,a} \cdot \tau_{0,b} \cdot \tau_{0,a} = \tau_{a,b}$$

si bien que l'on exhibe le polynôme associé à la transposition

$$\tau_{0,a} : \mathbb{t}(x) = -a^2\left[\left((x-a)^{q-2} + a^{-1})\right)^{q-2} - a\right]^{q-2}$$

Il est facile de le vérifier dans le cas où $a = 1$. On considère le corps $\mathbb{F}_p$. On remarque que

$$
\mathrm{g}_1(x) - x = \begin{cases} 1 & \text{si } x = 0 \\ -1 & \text{si } x = 1 \\ 0 & \text{sinon.} \end{cases}
$$

On en déduit alors que $\mathrm{g}_0(x) - x = (ax+b) + \prod_{k=2}^{p-1}(x-k)$

En appliquant notre égalité pour $x = 1$ et $x = 0$ on obtient le système suivant,

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

Or puisque dans $\mathbb{F}_p$ on a $(p-1)! = -1$ et $(p-2)! = 1$ alors on en déduit que $(a,b) = (0,1)$ et donc $\mathrm{g}_1(x) = x + \prod_{k=2}^{p-1}(x-k)$. $\square$