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 de ce morphisme 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 $\mathbb{Z}/n\mathbb{Z}$, $n = 0$ ou 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 $\mathbb{Z}/p\mathbb{Z}$.

□

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 le résultat suivant :

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

$$\begin{aligned} P : \quad K &\longrightarrow K \\ X &\longmapsto \sum_{i=0}^{n} a_i X^i, a_i \in K. \end{aligned}$$

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

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

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

$$P: \begin{array}{ccc} \mathbb{F}_5 & \longrightarrow & \mathbb{F}_5 \\ X & \longmapsto & X^3 \end{array}$$

   est clairement bijective.

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

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

   Il faut montrer que cette application n'est pas bijective.