Projet de Systèmes Polynomiaux.
2020-2021

Faculté des Sciences et Techniques
Master 1 - Maths. CRYPTIS

Théorème fondamental des polynômes symétriques

A l'attention de :
M. LICKTEIG

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

Table des matières

1 Rappels sur les Corps Finis

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 $1_{\mathbb{K}}$ 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 $\mathbb{Z}/n\mathbb{Z}$, $n = 0$ 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 $L[X]$, $P(X)$ est produit de facteurs de degré 1,

— les racines de $P(X)$ 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 $X^{p^n} - X$ alors $X^{p^n} - X$ 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.

1.1 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 $\mathcal{P}(n,p)$ 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 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 simples puisque P est 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 de degré n sur $\mathbb{F}_p$.

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 $\mathcal{P}(n, p) > 0$. □

1.2 Polynômes multivariés

2 Les polynômes symétriques

2.1 Introduction aux polynômes symétriques

Les polynômes symétriques prennent forme à partir de l'étude des racines de n'importe quel polynôme. Considérons le polynôme $P = X^3 + bX^2 + cX + d$. C'est un polynôme cubique donc il a 3 racines, non nécessairement distinctes. On notera ces racines α_1, α_2 et α_3. Le polynôme P peut alors se factoriser ainsi :

$$X^3 + bX^2 + cX + d = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3),$$

ce qui nous donne :

$$\begin{aligned} X^3 + bX^2 + cX + d &= (X - \alpha_1)(X - \alpha_2)(X - \alpha_3) \\ X^3 + bX^2 + cX + d &= X^3 - X^2(\alpha_3 + \alpha_2 + \alpha_1) + X(\alpha_2\alpha_3 + \alpha_1\alpha_3 + \alpha_1\alpha_2) - \alpha_1\alpha_2\alpha_3 \end{aligned}$$

Par identification, on obtient

$$\begin{aligned} b &= -(\alpha_3 + \alpha_2 + \alpha_1) \\ c &= \alpha_2\alpha_3 + \alpha_1\alpha_3 + \alpha_1\alpha_2 \\ d &= -\alpha_1\alpha_2\alpha_3. \end{aligned}$$

On observe donc que les coefficients de P sont polynomiaux en ses racines. Par ailleurs, comme modifier l'ordre des termes de P ne le change pas, il s'ensuit que les polynômes définissant b, c et d par rapport à α_1, α_2 et α_3 restent les mêmes si on permute α_1, α_2 et α_3.
Les polynômes respectant ce fait sont dits *polynômes symétriques*. Cela nous amène à la définition générale suivante.

Définition 5. Un polynôme $P \in K[X_1, X_2, \ldots, X_n]$ est dit symétrique si

$$P(X_{i_1}, X_{i_2}, \ldots, X_{i_n}) = P(X_1, X_2, \ldots, X_n),$$

pour toute permutation $X_{i_1}, X_{i_2}, \ldots, X_{i_n}$ de $X_1, X_2, \ldots, X_n$.

Exemples.

1. Soit $P = X^{n_1} + Y^{n_2} + Z^{n_3} \in K[X, Y, Z]$, avec $n_1, n_2, n_3 \in \mathbb{N}$. Alors P est un polynôme symétrique. En effet,

$$\begin{aligned} P &= X^{n_1} + Z^{n_3} + Y^{n_2} \\ P &= Y^{n_2} + X^{n_1} + Z^{n_3} \\ P &= Y^{n_2} + Z^{n_3} + X^{n_1} \\ P &= ... \end{aligned}$$

2. Soit $P = XYZ \in K[X, Y, Z]$. Ce polynôme est symétrique car $P = XYZ = YZX = ZYX = \ldots$.

2.2 Le théorème fondamental des polynômes symétriques

En considérant tous les rappels faits à précédemment, nous pouvons introduire le fameux théorème fondamental des polynômes symétriques.

Théorème 1. Tout polynôme symétrique de $K[X_1, X_2, ..., X_n]$ peut s'écrire de façon unique comme une expression polynomiale en les polynômes symétriques élémentaires $\sigma_1, \sigma_2, ..., \sigma_n$.

Démonstration. CLO 331 □

Corollaire 1.

Références

[1] COX David, LITTLE John, O'SHEA Donal
Ideal, Varieties, and Algorithms - An Introduction To Computational Algebraic Geometry and Commutative Algebra,
Third Edition, 7.1, p.317- ?

[2] https://math.unice.fr/~walter/L3_Alg_Arith/cours2.pdf