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 **2**

2 Les polynômes symétriques **3**
2.1 Introduction aux polynômes symétriques 3
2.2 Le théorème fondamental des polynômes symétriques 4

Références **5**

1 Rappels sur les Corps Finis

Dans la suite de ce rapport, K désignera un

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 1. 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,

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

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 $\sigma_1, \sigma_2, ..., \sigma_n$.

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