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 $\text{Im}(\varphi) \cong \mathbb{Z}/n\mathbb{Z}$. 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 $\mathbb{Z}/p\mathbb{Z}$.

$\square$

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

Définition 5 (Ordre)**.** Soit E un ensemble quelconque, on appelle *ordre partiel* sur E toute relation vérifiant les propriétés suivantes pour $(x,y) \in E^2$:

1. $x \preccurlyeq x$ (réflexivité)
2. $x \preccurlyeq y$ et $y \preccurlyeq x \Rightarrow x = y$ (antisymétrie)
3. $x \preccurlyeq y$ et $y \preccurlyeq z \Rightarrow x \preccurlyeq z$ (transitivité)

En d'autres terme, $\preccurlyeq$ est une relation d'équivalence sur E.

Définition 6 (Ordre total, ordonné)**.** Sous les mêmes notations, on dit que $\preccurlyeq$ est un *ordre total* si deux éléments quelconques sont toujours comparable, i.e. si

$$\forall (x,y) \in E^2, x \preccurlyeq y \text{ ou } y \preccurlyeq x$$

De plus, $\preccurlyeq$ est dit *bien ordonné* si

$$\forall\ F \subseteq E, \exists\ f_{min} \in F \text{ tel que } \forall f \in F,\ f_{min} \preccurlyeq f$$

Définition 7 (Monoïde)**.** On appelle monoïde tout ensemble muni d'une loi de composition interne et d'un élément neutre.

Définition 8. Soient $n \in \mathbb{N}$ et $\{X_1, ..., X_n\}$ un ensemble fini d'indéterminées. On définit le monoïde $\mathbb{M}_n$ comme suit :

$$\mathbb{M}_n := \{X^\alpha := X_1^{\alpha_1} \dots X_n^{\alpha_n}\}$$

Proposition 4.

$$\phi : \left| \begin{array}{rcl} \mathbb{M}_n & \longrightarrow & \mathbb{N}^n \\ X^\alpha := X_1^{\alpha_1} \dots X_n^{\alpha_n} & \longmapsto & \alpha := (\alpha_1, \dots, \alpha_n) \end{array} \right.$$

est un isomorphisme de monoïde.

Définition 9 (Ordre monomial)**.** On dit que $\preccurlyeq$ est un ordre monomial sur $\mathbb{M}_n$ si

1. $\preccurlyeq$ est un ordre total
2. $\preccurlyeq$ est compatible avec la multiplication, i.e. si pour tout
   $$X = X_1 \dots X_n\ ,\ \alpha = (\alpha_1, \dots, \alpha_n)\ ,\ \beta = (\beta_1, \dots, \beta_n) \text{ et } \gamma = (\gamma_1, \dots, \gamma_n)$$
   on a
   $$X^\alpha \preccurlyeq X^\beta \Rightarrow X^\alpha.X^\gamma \preccurlyeq X^\beta.X^\gamma$$
3. $\mathbb{M}_n$ est bien ordonné par $\preccurlyeq$

Définition 10 (Ordre lexicographique)**.** Pour deux vecteurs exposant $\alpha = (\alpha_1, \dots, \alpha_n)$ et $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$, on peut spécifier ordre, appellé *ordre lexicographique* définit comme suit :

$$\alpha \preccurlyeq_{lex} \beta$$

si

$$\exists\ m \in [\![1, n]\!] \text{ tel que } \forall\ i < m\ ,\ \alpha_i - \beta_i = 0 \text{ et } \alpha_m < \beta_m$$

Nous allons dès à présent travailler dans $\mathbb{K}[X_1, \dots, X_n]$, et $\preccurlyeq$ désignera toujours un ordre monomial sur $\mathbb{M}_n \subseteq \mathbb{K}[X_1, \dots, X_n]$.

Définition 11 (Leading Term)**.** On appelle *terme* tout éléments de $\mathbb{M}_n$ multiplié par un élément non nul c du corps de base.
On appelle *Leading Term*(LT) de $P \in \mathbb{K}[X_1, \dots, X_n]$, son monôme de plus haut degré par rapport à l'ordre $\preccurlyeq$.
La constante c sera appelée *Leading Coefficient*(LC), et $X_1^{\alpha_1} \dots X_n^{\alpha_n}$ le *Leading Monomial*, de sorte que :

$$P = \underbrace{\underbrace{c}_{\text{LC(P)}} . \underbrace{X_1^{\alpha_1} \dots X_n^{\alpha_n}}_{\text{LM(P)}}}_{\text{LT(P)}} + \text{Q}$$

où $Q \in \mathbb{K}[X_1, \dots, X_n]$ est constitué des termes de la forme X^β , $\beta \preccurlyeq_{lex} \alpha$ et $X \in \mathbb{K}[X_1, \dots, X_n]$.

Définition 12 (Multi degré)**.** Le vecteur d'exposant $\alpha := (\alpha_1, \ldots, \alpha_n)$ est appellé le multi degré de P et est noté $mdeg(P)$.

Proposition 5. Soient $P, Q \in \mathbb{K}[X_1, \ldots, X_n]$, on a $mdeg(P.Q) = mdeg(P)+mdeg(Q)$.

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 13. 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 $P = X^n + Y^n + Z^n \in K[X, Y, Z]$, avec $n \in \mathbb{N}$. Alors P est un polynôme symétrique. Comme le prouve la fonction *symmfunc* de Maple :

```
> P := X^n + Y^n + Z^n;
  type(P, symmfunc(X, Y, Z));
```

$$P := X^n + Y^n + Z^n$$
$$true$$

   Où la fonction renvoie un booléen : *true* si le polynôme est symétrique, *false* si non.

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

2.2 Polynômes symétriques élémentaires

Voir CLO page 318, def 2

2.3 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 $K\left[X_1, X_2, ..., X_n\right]$ peut s'écrire de façon unique comme une expression polynomiale en les polynômes symétriques élémentaires $\sigma_1, \sigma_2, ..., \sigma_n$.

Démonstration. Pour cette démonstration nous allons utiliser l'ordre lexicographique suivant, $x_1 > x_2 > \ldots > x_n$. Soit $f \in K[x_1, \ldots, x_n]$ un polynôme symétrique non nul, et on définit l'application LT par $LT(f) = ax^{\alpha}$, où $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ et $a \in K$. On peut supposer sans perte de généralité que les α_i, $i \in \{1, \ldots, n\}$ sont ordonnés comme tel : $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_n$. En effet, supposons que l'on ait $\alpha_i < \alpha_{i+1}$ pour un certain $i \in \{1, \ldots, n\}$. Il suffit alors de considérer le vecteur d'exposants β, obtenu à partir de α en permutant α_i et α_{i+1}. On écrit $\beta = (\alpha_1, \ldots, \alpha_{i+1}, \alpha_i, \ldots, \alpha_n)$. Puisque ax^{α} est un terme de f, on en déduit que ax^{β} est un terme de $f(x_1, \ldots, x_{i+1}, x_i, \ldots, x_n)$. Or, f est symétrique donc $f(x_1, \ldots, x_{i+1}, x_i, \ldots, x_n) = f$, et par conséquent, ax^{β} est un terme de f. Ceci est impossible puisque $\beta > \alpha$ selon l'ordre lexicographique.

Posons maintenant,

$$h = \sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\ldots\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\sigma_n^{\alpha_n}$$

Pour trouver le *Leading Term* de h, on a besoin de $LT(\sigma_r) = x_1x_2\cdots x_r$ avec $r \in \{1, \ldots, r\}$. On en déduit alors que,

$$\begin{aligned} LT(h) &= LT(\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\ldots\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\sigma_n^{\alpha_n}) \\ &= LT(\sigma_1)^{\alpha_1-\alpha_2}LT(\sigma_2)^{\alpha_2-\alpha_3}\ldots LT(\sigma_n)^{\alpha_n} \\ &= x_1^{\alpha_1-\alpha_2}(x_1x_2)^{\alpha_2-\alpha_3}\ldots(x_1x_2\ldots x_n)^{\alpha_n} \\ &= x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n} = x^{\alpha}. \end{aligned}$$

Il s'ensuit donc que f et ah ont le même *Leading Term*, et par conséquent,

$$\text{mdeg}(f - ah) < \text{mdeg}(f), \text{ lorsque } f - ah \neq 0.$$

Posons maintenant $f_1 = f - ah$. On remarque que f_1 est symétrique puisque f et ah le sont. Donc, si $f_1 \neq 0$, on peut répéter l'étape précédente pour construire $f_2 = f_1 - a_1h_1$, où a_1 est une constante et $h_1 = \displaystyle\prod_{i=1}^{n}\sigma_i^{\gamma_i}$, $\gamma_i \in \mathbb{N}$. On sait aussi que $LT(f_2) < LT(f_1)$ lorsque $f_2 \neq 0$. En continuant ainsi on obtient une suite de polynômes $f, f_1, f_2, \ldots$ avec

$$\text{mdeg}(f\ )> \text{mdeg}(f_1) > \text{mdeg}(f_2) \dots .$$

Comme l'ordre lexicographique est bien ordonné, la suite est finie. Mais le processus se termine seulement lorsque $f_{t+1} = 0$ pour un certain $t \in \mathbb{N}$. On voit alors assez naturellement que

$$f = ah + a_1h_1 + \ldots + a_th_t$$

ce qui montre que f est polynomiale en les polynômes symétriques élémentaires.

Il nous reste à montrer l'unicité. Supposons qu'on a un polynôme symétrique f pouvant s'écrire

$$f = g_1(\sigma_1, \ldots, \sigma_n) = g_2(\sigma_1, \ldots, \sigma_n).$$

Notons $y_1, \ldots, y_n$ les n variables des polynômes à n indéterminées g_1 et g_2. On doit montrer que $g_1 = g_2$ dans $K[y_1, \ldots, y_n]$.
Si on pose $g = g_1 - g_2$, alors $g(\sigma_1, \ldots, \sigma_n) = 0$ dans $K[x_1, \ldots, x_n]$. La preuve revient alors à montrer que $g = 0$ dans $K[x_1, \ldots, x_n]$.

Par l'absurde, supposons que $g \neq 0$. Si on écrit $g = \sum_\beta a_\beta y^\beta$, alors $g(\sigma_1, \ldots, \sigma_n)$ est la somme des polynômes $g_\beta = a_\beta \sigma_1^{\beta_1}\sigma_2^{\beta_2}\ldots\sigma_n^{\beta^n}$, où $\beta = (\beta_1, \ldots, \beta_n)$. De plus, par le calcul de $LT(h)$, on déduit que

$$LT(g_\beta) = a_\beta x_1^{\beta_1+\ldots+\beta_n} x_2^{\beta_2+\ldots+\beta_n}\ldots x_n^{\beta_n}.$$

Montrons maintenant que l'application,

$$\iota : \Big|\ (\beta_1, \ldots, \beta_n) \longmapsto (\beta_1 + \ldots + \beta_n, \beta_2 + \ldots + \beta_n, \ldots, \beta_n)$$

est injective. Soient $\beta = (\beta_1, \ldots, \beta_n)$ et $\beta' = (\beta'_1, \ldots, \beta'_n)$,

$$\begin{aligned}
\iota(\beta) = \iota(\beta') &\Leftrightarrow (\beta_1 + \ldots + \beta_n, \beta_2 + \ldots + \beta_n, \ldots, \beta_n) = (\beta'_1 + \ldots + \beta'_n, \beta'_2 + \ldots + \beta'_n, \ldots, \beta'_n) \\
&\Leftrightarrow \left\{ \begin{array}{rcl} \beta_1 + \ldots + \beta_n &=& \beta'_1 + \ldots + \beta'_n \\ \beta_2 + \ldots + \beta_n &=& \beta'_2 + \ldots + \beta'_n \\ & \ldots & \\ \beta_n &=& \beta'_n \end{array} \right. \\
&\Leftrightarrow \beta_i = \beta'_i\ ,\ \forall i \in \{1, \ldots, n\},\ \text{ en remontant les égalités de chaque ligne}
\end{aligned}$$

Donc ι est une application injective. Par conséquent, les g_β ont des Leading Term distincts. En particulier, en choisissant β tel que $LT(g_\beta) > LT(g_\gamma)$, quelques soient $\gamma \neq \beta$, alors $LT(g_\beta)$ sera plus grand que tous les termes des g_γ. Finalement il n'y a rien pour annuler $LT(g_\beta)$, et par conséquent, $g(\sigma_1, \ldots, \sigma_n)$ ne peut être nul, l'unicité en découle. □

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