Théorème fondamental des polynômes symétriques : une démonstration combinatoire

Salim Rostam

9 janvier 2019

Références : Ramis-Deschamps-Odoux, *Algèbre 1* ; Macdonald, *Symmetric functions and Hall polynomials*.

Le but de cette note est de présenter une démonstration du « théorème fondamental des polynômes symétriques », assez combinatoire et qui consiste à faire un changement de base. On peut tout à fait s'en servir de développement pour les leçons suivantes [1] (liste 2019) :

101* Groupe opérant sur un ensemble. Exemples et applications.

105* Groupe des permutations d'un ensemble fini.

108* Exemples de parties génératrices d'un groupe. Applications.

144 Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.

151* Dimension d'un espace vectoriel. Rang. Exemples et applications.

190 Méthodes combinatoires, problèmes de dénombrement.

Soit k un corps. On considère l'anneau de polynômes à n indéterminées $k[x_1, \dots, x_n]$. Si $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ est un monôme, on définit deux types de degrés.

— Le degré *lexicographique*, donné par le n-uplet $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, qui détermine entièrement le monôme. On écrira parfois x^α pour désigner $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

— Le degré *total*, donné par $\alpha_1 + \cdots + \alpha_n \in \mathbb{N}$. Un polynôme est dit *homogène* de degré $d \in \mathbb{N}$ si tous ses monômes sont de degré total d.

Rappelons que le groupe symétrique $\mathfrak{S}_n$ agit sur $k[x_1, \dots, x_n]$ par permutation des variables.

Exercice. L'action donnée par $(\sigma, x_i) \mapsto x_{\sigma(i)}$ est-elle une action à gauche ou une action à droite ?

Définition. Un polynôme $P \in k[x_1, \dots, x_n]$ est dit *symétrique* s'il est un point fixe pour cette action. On note $\Lambda_n \coloneqq k[x_1, \dots, x_n]^{\mathfrak{S}_n}$ la sous-algèbre fixée.

Un exemple de fonction symétrique est le *d-ième polynôme symétrique élémentaire*

$$\sigma_d(x_1, \dots, x_n) \coloneqq \sum_{1 \le i_1 < \cdots < i_d \le n} x_{i_1} \cdots x_{i_d} \in \Lambda_n,$$

pour $d \in \{1, \dots, n\}$. C'est un polynôme (symétrique) homogène de degré d. On a la « relation coefficients-racines » :

$$\prod_{d=1}^{n} (x - x_r) = x^n + \sum_{d=0}^{n-1} (-1)^{n-d} \sigma_{n-d}(x_1, \dots, x_n) x^d.$$

1. Pour les leçons étoilées, préférer si possible un autre développement.

Théorème. *Tout polynôme symétrique en n variables s'écrit de façon unique sous la forme $Q(\sigma_1, \dots, \sigma_n)$ avec $Q \in k[y_1, \dots, y_n]$.*

Remarque. Le Théorème reste vrai si k est un anneau commutatif. Il suffit dans la suite de penser « k-module libre » au lieu de « k-espace vectoriel ».

Il faut connaitre, bien sûr ce théorème, mais également une façon de trouver le polynôme Q ! Si P est un polynôme symétrique, on regarde le monôme de plus grand degré lexicographique (pour l'ordre lexicographique), de coefficient $a \in k^*$. Si ce degré est $\alpha = (\alpha_1, \dots, \alpha_n)$, on considère alors $\widetilde{P} \coloneqq P - a\sigma_1^{\alpha_1 - \alpha_2} \cdots \sigma_{n-1}^{\alpha_{n-1} - \alpha_n} \sigma_n^{\alpha_n}$. Le monôme de degré α a bien disparu dans $\widetilde{P}$, et comme il n'y a pas de monôme de plus grand degré qui puisse apparaître (exercice !) on peut réappliquer la procédure à $\widetilde{P}$.

Une démonstration classique du théorème est, étant donnée un polynôme $P \in k[x_1, \dots, x_n]$ symétrique, considérer le polynôme symétrique $P(x_1, \dots, x_{n-1}, 0)$ et raisonner par récurrence (voir par exemple RDO 1). On va présenter ici une preuve moins constructive mais peut-être plus conceptuelle, que l'on peut trouver dans le livre de I. G. Macdonald « *Symmetric Functions and Hall Polynomials* ».

Rappelons qu'une *partition* d'un entier N est une suite finie $\lambda = (\lambda_1 \geq \cdots \geq \lambda_h > 0)$ décroissante (au sens large) d'entiers naturels non nuls de somme $N =: |\lambda|$. La *hauteur* de λ est l'entier $h =: h(\lambda)$. Si $\lambda = (\lambda_1, \dots, \lambda_h)$ est une partition de hauteur $h \leq n$, que l'on complète en un n-uplet en posant $\lambda_i \coloneqq 0$ pour $i \in \{h+1, \dots, n\}$, on définit

$$m_\lambda(x_1, \dots, x_n) \coloneqq \sum_{\alpha \in \mathfrak{S}_n \cdot \lambda} x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in \Lambda_n,$$

où $\mathfrak{S}_n \cdot \lambda$ désigne l'orbite de $(\lambda_1, \dots, \lambda_n) \in \mathbb{N}^n$ pour l'action de $\mathfrak{S}_n$ sur les n-uplets.

Remarque.
— Soit $d \in \{1, \dots, n\}$. Si (1^d) désigne la partition $(\underbrace{1, \dots, 1}_{d \text{ fois}})$ alors $m_{(1^d)}(x_1, \dots, x_n) = \sigma_d(x_1, \dots, x_n)$.
— Le polynôme m_λ est (symétrique) homogène de degré $|\lambda|$.

Lemme. *La famille $\{m_\lambda\}_{h(\lambda) \leq n}$ est une k-base de Λ_n.*

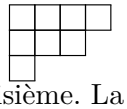
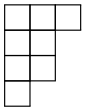
Démonstration. Tout d'abord, la famille est bien libre car la sous-famille constituée des termes dominants pour l'ordre lexicographique (les $x_1^{\lambda_1} \cdots x_n^{\lambda_n}$) est échelonnée. Si maintenant $P \in \Lambda_n$ est un polynôme symétrique, si $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ est un monôme de P avec coefficient $a \in k^*$ alors il existe une partition λ de hauteur au plus n telle que $\alpha \in \mathfrak{S}_n \cdot \lambda$ (on trie !). Exactement tous les termes de am_λ apparaissent dans P, puisque P est symétrique, et $P - am_\lambda$ est un polynôme symétrique avec strictement moins de termes que P. On récurre. □

Si λ est une partition vérifiant $\lambda_1 \leq n$, on définit

$$\sigma_\lambda \coloneqq \sigma_{\lambda_1} \cdots \sigma_{\lambda_h} \in \Lambda_n.$$

C'est un polynôme (symétrique) homogène de degré $|\lambda|$. On veut exprimer σ_λ sur la base des m_μ pour $h(\mu) \leq n$.

Définition. Soit $\lambda = (\lambda_1 \geq \dots)$ une partition. On définit la partition *conjuguée* λ' par $\lambda'_i \coloneqq \#\{j : \lambda_j \geq i\}$.

Graphiquement, on peut représenter λ par un *diagramme de Young*, c'est-à-dire, une série de boîtes justifiées à gauche représentant les parts de λ. Par exemple, la partition $\lambda \coloneqq (4,3,1)$ se représente par  : on a $\lambda_1 = 4$ cases sur la première ligne, $\lambda_2 = 3$ sur la deuxième et $\lambda_3 = 1$ sur la troisième. La partition conjuguée s'obtient en regardant le nombre de boîtes sur les colonnes (ou en renversant le diagramme par rapport à la diagonale), ici $\lambda' = (3,2,2,1)$ est  .

Remarque.
— On a $h(\lambda') = \lambda_1$. En particulier, la conjugaison réalise une bijection entre les partitions de première part n (resp. $\leq n$) et les partitions de hauteur n (resp. $\leq n$).
— On a $\lambda'' = \lambda$, en particulier $h(\lambda) = \lambda'_1$.

Proposition. *Soit λ une partition vérifiant $h(\lambda) \leq n$. Il existe des (uniques) scalaires $a_{\lambda,\mu} \in k$ tels que*

$$\sigma_{\lambda'}(x_1, \ldots, x_n) = m_\lambda(x_1, \ldots, x_n) + \sum_{\substack{h(\mu) \leq n \\ \mu < \lambda}} a_{\lambda,\mu} m_\mu(x_1, \ldots, x_n).$$

Remarque. On a $\lambda'_1 = h(\lambda) \leq n$ donc $\sigma_{\lambda'}(x_1, \ldots, x_n)$ est bien définie.

L'ordre dont il est question sur les partitions est l'ordre lexicographique. On a en fait un résultat plus fort puisque la proposition reste vraie avec l'ordre (partiel) $\lhd$ de *dominance* sur les partitions, plus fin que l'ordre lexicographique (autrement dit $\lambda \lhd \mu \implies \lambda < \mu$).

Démonstration. L'unicité est claire par le Lemme. Pour l'existence, on va simplement regarder quels monômes apparaissent lorsque l'on développe $\sigma_{\lambda'}(x_1, \ldots, x_n)$. Ce sont les

$$\left(x_{i_1^{(1)}} \cdots x_{i_{\lambda'_1}^{(1)}}\right) \cdots \left(x_{i_1^{(h)}} \cdots x_{i_{\lambda'_h}^{(h)}}\right),$$

où h est la hauteur de λ' et $1 \leq i_1^{(j)} < \cdots < i_{\lambda'_j}^{(j)} \leq n$ pour tout $j \in \{1, \ldots, n\}$. Soit $\alpha \in \mathbb{N}^n$ tel que le monôme précédent s'écrive $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. On désire montrer que $\alpha \leq \lambda$ pour l'ordre lexicographique. Pour cela, remplissons le diagramme de Young de λ de la façon suivante : pour $j \in \{1, \ldots, h(\lambda')\}$ (rappelons que $h(\lambda') = \lambda_1$), on remplit la colonne j de haut en bas par les $i_k^{(j)}$ pour k allant de 1 à λ'_j. Sur l'exemple précédent de la partition $\lambda = (4,3,1)$, cela donne

$i_1^{(1)}$	$i_1^{(2)}$	$i_1^{(3)}$	$i_1^{(4)}$
$i_2^{(1)}$	$i_2^{(2)}$	$i_2^{(3)}$	
$i_3^{(1)}$			

Comptons maintenant le nombre de 1 parmi les $i_k^{(j)}$. Par définition de α ils sont exactement α_1, de plus ils apparaissent nécessairement dans la première ligne du tableau (car les entiers sont strictement croissants de haut en bas dans chaque colonne, par définition). Puisqu'il y a exactement λ_1 cases dans la première ligne du tableau, on en déduit qu'il y a au plus λ_1 fois l'entier 1 dans la première ligne et donc dans tout le tableau, d'où

$$\alpha_1 \leq \lambda_1.$$

Comptons maintenant le nombre de 1 et 2. Pour la même raison de stricte croissance que précédemment, ils ne peuvent apparaître que dans les deux premières lignes du tableau, qui

contient exactement $\lambda_1 + \lambda_2$ cases. Mais on sait que les entiers 1 et 2 apparaissent en tout exactement $\alpha_1 + \alpha_2$ fois, par définition de α (il y a α_1 fois 1 et α_2 fois 2). On a donc

$$\alpha_1 + \alpha_2 \leq \lambda_1 + \lambda_2.$$

On continue jusqu'à la dernière ligne du tableau, éventuellement vide (on a complété λ en un n-uplet par des parts nulles) pour laquelle on trouve

$$\alpha_1 + \cdots + \alpha_n \leq \lambda_1 + \cdots + \lambda_n.$$

Remarque. L'*ensemble* des inégalités précédentes définit exactement la relation de dominance $\alpha \trianglelefteq \lambda$. Cependant, on voit qu'elles impliquent bien $\alpha \leq \lambda$ pour l'ordre lexicographique.

Puisque $\sigma_{\lambda'}(x_1, \ldots, x_n)$ est symétrique, le monôme $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ y apparait si et seulement si $x^{\sigma\cdot\alpha}$ y apparait, pour chaque $\sigma \in \mathfrak{S}_n$. De plus, le raisonnement précédent assure que l'on a encore $\sigma \cdot \alpha \leq \lambda$. Finalement, si μ désigne le n-uplet α trié dans l'ordre décroissant alors μ est une partition et $\mu \leq \lambda$.

On obtient donc l'égalité annoncée. On a bien $a_{\lambda,\lambda} = 1$ puisque le monôme x^λ, et donc m_λ, est atteint une unique fois : lorsque $i_k^{(j)} = k$ pour tout j, k (sur l'exemple, cela donne $\begin{array}{|c|c|c|}\hline 1&1&1\\\hline 2&2&2\\\hline 3\\\cline{1-1}\end{array}$).

□

Remarque. Les partitions de la forme (1^d) étant minimales pour l'ordre lexicographique, on retrouve bien le résultat remarqué auparavant $\sigma_d(x_1, \ldots, x_n) = m_{(1^d)}(x_1, \ldots, x_n)$ (les partitions $(1^{d'})$ avec $d' < d$ n'apparaissent pas pour des raisons de degré total). En effet, la partition conjuguée de (1^d) est (d), qui est partition constituée d'une seule part, égale à d.

Par la Proposition, la famille $(\sigma_{\lambda'})_{h(\lambda)\leq n} = (\sigma_\lambda)_{\lambda_1 \leq n}$ s'exprime via une matrice triangulaire inversible en fonction de la famille $(m_\lambda)_{h(\lambda)\leq n}$, où l'on a pris soin de ranger les partitions dans l'ordre lexicographique. Par le Lemme, la famille $(\sigma_\lambda)_{\lambda_1 \leq n}$ est donc également une k-base de Λ_n. On en déduit donc le Théorème. En effet, si $P \in \Lambda_n$ est un polynôme symétrique alors il s'écrit $P = \sum_{\lambda_1 \leq n} p_\lambda \sigma_\lambda$ qui est bien de la forme voulue. Réciproquement, soit $P = Q(\sigma_1, \ldots, \sigma_n)$ avec $Q(y) = \sum_{\alpha \in \mathbb{N}^n} q_\alpha y^\alpha$. On veut écrire

$$P = Q(\sigma_1, \ldots, \sigma_n) = \sum_{\alpha \in \mathbb{N}^n} q_\alpha \sigma_1^{\alpha_1} \cdots \sigma_n^{\alpha_n},$$

en fonction des σ_λ. On va faire un changement de variable : soit $\phi : \{\lambda\}_{\lambda_1 \leq n} \to \mathbb{N}^n$ l'application qui à une partition λ vérifiant $\lambda_1 \leq n$ associe le vecteur $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ des multiplicités : l'entier i apparait exactement α_i fois dans λ (remarquons que la hauteur de λ devient la somme des composantes de α). L'application ϕ est bijective, d'inverse l'application qui à $\alpha \in \mathbb{N}^n$ associe la partition où chaque $i \in \{1, \ldots, n\}$ apparait exactement α_i fois. Remarquons que si $\alpha = \phi(\lambda)$ avec λ de hauteur h alors

$$\sigma_1^{\alpha_1} \cdots \sigma_n^{\alpha_n} = \sigma_{\lambda_1} \ldots \sigma_{\lambda_h} = \sigma_\lambda,$$

chaque polynôme σ_d apparaissant exactement α_d fois. Ainsi, on obtient

$$P = Q(\sigma_1, \ldots, \sigma_n) = \sum_{\alpha \in \mathbb{N}^n} q_\alpha \sigma_1^{\alpha_1} \cdots \sigma_n^{\alpha_n} = \sum_{\lambda_1 \leq n} q_{\phi(\lambda)} \sigma_\lambda,$$

donc par le Lemme les $q_{\phi(\lambda)}$ sont uniquement déterminés par P donc Q est entièrement déterminé par P.