SUR L'ARITÉ DES FONCTIONS

ANNICK VALIBOUZE *

Introduction

Par référence à la notion d'arité sur les arbres nous avons une notion d'arité sur les fonctions : une fonction de n variables est d'*arité* m $(m \leq n)$ si elle est de degré nul en exactement $n-m$ variables. Nous étudions l'action naturelle du groupe symétrique de degré n sur les anneaux des polynômes en n variables. Si un polynôme de n variables est d'arité m alors l'action du groupe symétrique de degré m sur f suffit alors à effectuer certains calculs (Théorème 1.3). La réduction du groupe symétrique de degré n à celui de degré m peut être étendue à des groupes plus généraux que le groupe symétrique moyennant deux hypothèses restrictives (Théorème 3.3). Nous terminons sur le cas de produits directs de groupes (Théorème 4.2).

Les Théorèmes 1.3 et 4.2 permettent en particulier d'obtenir des gains notables dans les calculs des résolvantes et des multi-résolvantes intervenant dans les recherche de groupes de Galois ou de polynômes minimaux d'extensions de corps. Cette application est déjà implantée et sera disponible dans la prochaine version du système de calcul formel Macsyma.

1. Cas du groupe symétrique

Nous adoptons les conventions de Macdonald ([7]).

Soit $n \in \mathbb{N}^*$. On désigne par $\mathcal{P}_n$ l'ensemble des partitions en n parts au plus : ce sont les éléments $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ tels que $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$. Si $\alpha = (\alpha_i) \in \mathcal{P}_n$, on appelle *longueur* de α l'entier $max\{i \mid \alpha_i \geq 1\}$, noté $l(\alpha)$, et le *poids* de α, noté $|\,\alpha\,|$, est la somme $\alpha_1 + \cdots + \alpha_n$ de ses parts. Nous adopterons également la notation exponentielle, c'est-à-dire que la partition (4 4 1 1 1 0 0) sera aussi notée $1^3 4^2$. Une *transversale* de l'action d'un groupe sur un ensemble est un sous-ensemble qui contient un et un seul élément de chaque orbite.

On a une action naturelle à droite de $\mathfrak{S}_n$, le groupe symétrique de degré n, sur $\mathbb{N}^n$, donnée par

$$\begin{array}{ccc} \mathbb{N}^n \times \mathfrak{S}_n & \longrightarrow & \mathbb{N}^n \\ ((\beta_1, \ldots, \beta_n), \sigma) & \longmapsto & (\beta_{\sigma(1)}, \ldots, \beta_{\sigma(n)}) \end{array} \quad .$$

La proposition qui suit est évidente :

Date:

* Avec le soutien du GDR de Calcul Formel MEDICIS et du GDR-PRC Math-Info.

Proposition 1.1. *L'ensemble $\mathcal{P}_n$ est une transversale de l'action à droite naturelle de $\mathfrak{S}_n$ sur $\mathbb{N}^n$.*

Soient $x_1, \dots, x_n$ des indéterminées sur $\mathbb{C}$. L'action à droite ci-dessus induit une action naturelle à gauche de $\mathfrak{S}_n$ sur $\mathbb{C}[x_1, \dots, x_n]$, définie par

$$\begin{array}{rcl} \mathfrak{S}_n \times \mathbb{C}[x_1, \dots, x_n] & \longrightarrow & \mathbb{C}[x_1, \dots, x_n] \\ (\sigma, f) & \longmapsto & \sigma * f = \sigma * f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \end{array} \quad .$$

L'action à droite de $\mathfrak{S}_n$ sur $\mathbb{N}^n$ se prolonge de façon évidente à $\mathbb{C}^n$ avec la formule analogue :

$$\begin{array}{rcl} \mathbb{C}^n \times \mathfrak{S}_n & \longrightarrow & \mathbb{C}^n \\ ((\lambda_1, \dots, \lambda_n), \sigma) & \longmapsto & \lambda \natural \sigma = (\lambda_{\sigma(1)}, \dots, \lambda_{\sigma(n)}) \end{array} \quad ; \tag{1}$$

avec (1), il est bien clair que pour tout $f \in \mathbb{C}[x_1, \dots, x_n]$:

$$\forall \sigma \in \mathfrak{S}_n,\ \forall \lambda \in \mathbb{C}^n \qquad (\sigma * f)(\lambda) = f(\lambda \natural \sigma) \qquad . \tag{2}$$

Pour $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathcal{P}_n$, on note $M_{\alpha,n}$ la *fonction monomiale* associée à α ; c'est-à-dire

$$M_{\alpha,n} = \sum_{\beta \in Orb(\alpha)} x_1^{\beta_1} \dots x_n^{\beta_n} \qquad , \tag{3}$$

où $Orb(\alpha)$ est la $\mathfrak{S}_n$-orbite de α. On voit facilement que si $\mathcal{T}'_\alpha$ désigne une transversale quelconque de l'action de $\mathfrak{S}_n$ sur les classes latérales à gauche de $Stab(\alpha)$, alors :

$$M_{\alpha,n} = \sum_{t \in \mathcal{T}'_\alpha} x_{t(1)}^{\alpha_1} \dots x_{t(n)}^{\alpha_n} \qquad ; \tag{4}$$

Par exemple, sur l'anneau $\mathbb{C}[x, y, z, t]$ on a $M_{\alpha,4} = x^2y + x^2z + y^2x + y^2z + z^2x + z^2y + x^2t + t^2x + y^2t + t^2y + z^2t + t^2z$.

Soit $Sym(x_1, \dots, x_n)$ l'anneau des polynômes symétriques à coefficients dans $\mathbb{C}$. Il est bien connu (voir [7]) que l'ensemble des $(M_{\alpha,n})_{\alpha \in \mathcal{P}_n}$ est une base vectorielle de $Sym(x_1, \dots, x_n)$.

Il est intéressant pour la suite d'introduire une transversale $\mathcal{T}'_\alpha$ particulière. Supposons $\alpha = (a_1^{m_1} \dots a_r^{m_r}) \in \mathcal{P}_n$ avec $m_i \neq 0$ et $a_i > 0$. On voit alors que le groupe $Stab(\alpha)$ n'est autre que le sous-groupe de Young $\mathfrak{S}_{\underline{m}}$ de $\mathfrak{S}_n$ formé des $\sigma \in \mathfrak{S}_n$ laissant stable chacun des intervalles suivants :

$$\begin{array}{c} J_1 = [1, m_1] \qquad , \qquad J_2 = [m_1 + 1, m_1 + m_2] \qquad , \dots , \\ J_r = [m_1 + \dots + m_{r-1} + 1, l(\alpha) = m_1 + \dots + m_r] \qquad . \end{array} \tag{5}$$

On déduit immédiatement de là :

Proposition 1.2. *L'ensemble des $\sigma \in \mathfrak{S}_n$ dont la restriction à chacun des intervalles de* (5) *est strictement croissante est une transversale du groupe $Stab(\alpha)$.*

La transversale définie dans la Proposition 1.2 sera notée $\mathcal{T}_\alpha$ dans toute la suite. De (4) on déduit donc l'expression de $M_{\alpha,n}$:

$$M_{\alpha,n} = \sum_{t\in\mathcal{T}_\alpha} x_{t(1)}^{\alpha_1}\dots x_{t(n)}^{\alpha_n} \qquad ; \tag{6}$$

la formule (6) donne immédiatement les formules que l'on trouve déjà dans Lagrange : $card(Stab(\alpha)) = m_1!\dots m_r!(n-l(\alpha))!$ et $card(\mathcal{T}_\alpha) = \frac{n!}{m_1!\dots m_r!(n-l(\alpha))!}$.

Soit $f \in \mathbb{C}[x_1,\dots,x_n]\backslash\{0\}$; notons $Stab(f)$ le stabilisateur de f dans $\mathfrak{S}_n$, i.e. $Stab(f) = \{\sigma \in \mathfrak{S}_n \mid \sigma * f = f\}$, et $Orb(f)$ la $\mathfrak{S}_n$-orbite de f. Nous définissons le *symétrisé réduit* de f, noté $\mathcal{O}_n(f)$, par $\mathcal{O}_n(f) = \sum_{h\in Orb(f)} h$. On a donc pour toute transversale $\mathcal{T}$ de $\mathfrak{S}_n$ modulo $Stab(f)$:

$$\mathcal{O}_n(f) = \sum_{t\in\mathcal{T}} t * f \qquad . \tag{7}$$

Par définition, $Tr_n(f) = [Stab(f)].\mathcal{O}_n(f)$ sera appelé le *symétrisé de f*. Ainsi pour un monôme f, $\mathcal{O}_n(f)$ est la fonction monomiale associée à f et $Tr_n(f)$ est la fonction monomiale augmentée.

Considérons l'extension galoisienne $\mathcal{L}/\mathcal{K}$, où $\mathcal{L} = \mathbb{C}(x_1,\dots,x_n)$ et où $\mathcal{K}$ est le corps des fractions de $Sym(x_1,\dots,x_n)$ ($\mathcal{K}$ est le corps des fractions rationnelles symétriques en n variables sur $\mathbb{C}$). Il est clair que :

$$Tr_n = Tr_{\mathcal{L}/\mathcal{K}}|_{\mathbb{C}[x_1,\dots,x_n]} \qquad . \tag{8}$$

La fonction $\mathcal{O}_n$ s'interprète de façon analogue : soit $\mathcal{K}(f)$ l'extension de $\mathcal{K}$ engendrée par f dans $\mathcal{L}$, alors :

$$\mathcal{O}_n(f) = Tr_{\mathcal{K}(f)/\mathcal{K}}(f) \qquad . \tag{9}$$

Fixons un entier m, $1 \le m < n$. Pour toute la suite nous posons $Tr = Tr_n$, $\mathcal{O} = \mathcal{O}_n$ et $M_\alpha = M_{\alpha,n}$. On utilise le plongement canonique de $\mathfrak{S}_m$ dans $\mathfrak{S}_m \times \mathfrak{S}_1 \cdots \times \mathfrak{S}_1 \subset \mathfrak{S}_n$.

Notons $\mathcal{A}_m = Tr(\mathbb{C}[x_1,\dots,x_m])$ et $\mathcal{A}_{m,k} = Tr((\mathbb{C}[x_1,\dots,x_m])_k)$ la composante de degré k ; alors $\mathcal{A}_m = \bigoplus_{k\in\mathbb{N}^*}\mathcal{A}_{m,k}$. Remarquons que si $\alpha \in \mathcal{P}_m$, alors $M_{\alpha,m} \in \mathcal{A}_m$, comme il résulte aussitôt des définitions ; donc $\mathcal{A}_m$ contient le sous $\mathbb{C}$-espace vectoriel $\mathcal{A}'_m$ de $Sym(x_1,\dots,x_n)$ engendré par les $(M_{\alpha,m})_{\alpha\in\mathcal{P}_m}$; ci-dessous, nous verrons notamment que $\mathcal{A}'_m = \mathcal{A}_m$.

Fixons $\alpha \in \mathcal{P}_m$. Nous cherchons un lien simple entre $\mathcal{O}(M_{\alpha,m})$ et $M_\alpha = M_{\alpha,n}$. Pour cela nous allons traiter un exemple avec $n = 4$ et les variables x, y, z, t. Choisissons la partition $\alpha = (2,1)$, avec $m = 3$. Nous avons donc

$$\begin{aligned} M_{\alpha,m} &= x^2y + x^2z + y^2x + y^2z + z^2x + z^2y = f(x,y,z) \qquad \text{et} \\ \mathcal{O}(M_{\alpha,m}) &= f(x,y,z) + f(x,y,t) + f(x,z,t) + f(y,z,t) = 2M_\alpha \qquad . \end{aligned}$$

On vérifie aisément que le facteur de proportionnalité est donné par

$$\mathcal{O}(M_{\alpha,m}) = \binom{n-l(\alpha)}{m-l(\alpha)} M_\alpha \qquad (\alpha \in \mathcal{P}_m\backslash(\underline{0})) \qquad . \tag{10}$$

Cette relation sera démontrée dans le paragraphe 3 en utilisant la Proposition 3.2 qui donne une formule équivalente pour des groupes plus généraux (voir la remarque 4).

Remarque 1. On a $\mathcal{O}(M_{\underline{0},m}) = 1 = M_{\underline{0}}$. Ainsi pour $\alpha = \underline{0}$ la relation (10) n'est vraie que si $m = 0$. Il est facile de constater que tous les résultats de cet article restent vrais pour des arités nulles ($m = 0$). Mais ce cas a été exclu (puisque m est supposé supérieur à 1) par souci de clarté et manque d'intérêt.

Bien que la relation (10) soit en défaut pour $\alpha = \underline{0}$, nous avons tout de même le résultat suivant pour tout $\alpha \in \mathcal{P}_m$:

$$Tr(M_{\alpha,m}) = m!(n-m)!\binom{n-l(\alpha)}{m-l(\alpha)} M_\alpha \qquad . \tag{11}$$

En effet, si $\alpha \neq \underline{0}$ on applique (10) :

$$Tr(M_{\alpha,m}) = [Stab_{\mathfrak{S}_n}(M_{\alpha,m})]\,\mathcal{O}(M_{\alpha,m}) = m!\,(n-m)!\binom{n-l(\alpha)}{m-l(\alpha)} M_\alpha \qquad ,$$

puisque $[Stab_{\mathfrak{S}_n}(M_{\alpha,m})] = [\mathfrak{S}_m \times \mathfrak{S}_{n-m}]$ et pour $\alpha = \underline{0}$

$$Tr(M_{\underline{0},m}) = n! = m!\,(n-m)!\binom{n}{m} M_{\underline{0}} \qquad .$$

Nous pouvons désormais passer aux fonctions :

Théorème 1.3. *Soit $g \in \mathbb{C}[x_1, \dots, x_m]$, d'arité m. Soit $\mathcal{O}_m(g)$ le symétrisé réduit de g dans $\mathbb{C}[x_1, \dots, x_m]$. Supposons que :*

$$\mathcal{O}_m(g) = \sum_{\alpha \in \mathcal{P}_m} \lambda_\alpha\, M_{\alpha,m} \qquad ,$$

où $(\lambda_\alpha)_{\alpha \in \mathcal{P}_m}$ est une famille de support fini. Alors

$$\mathcal{O}(g) = \sum_{\alpha \in \mathcal{P}_m} \lambda_\alpha \binom{n-l(\alpha)}{m-l(\alpha)} M_\alpha \qquad , \tag{12}$$

et les $\mathbb{C}$-espaces vectoriels $\mathcal{A}_m$ et $\mathcal{A}'_m$ sont égaux.

Démonstration. D'abord,

$$Tr(Tr_m(g)) = \sum_{\sigma \in \mathfrak{S}_n} \sigma * (\sum_{\tau \in \mathfrak{S}_m} \tau * g) = \sum_{\tau \in \mathfrak{S}_m} \sum_{\sigma \in \mathfrak{S}_n} (\sigma\tau) * g = \sum_{\tau \in \mathfrak{S}_m} Tr(g)$$

(car pour τ fixé, $\sigma \mapsto \sigma\tau$ est une bijection de $\mathfrak{S}_n$ sur $\mathfrak{S}_n$), donc

$$Tr(Tr_m(g)) = m!\,Tr(g) = [Stab_{\mathfrak{S}_n}(g)]\,m!\,\mathcal{O}(g) \qquad .$$

Puis du fait que g est d'arité m, $Stab_{\mathfrak{S}_n}(g)$ est isomorphe à $Stab_{\mathfrak{S}_m}(g) \times \mathfrak{S}_{n-m}$, donc $[Stab_{\mathfrak{S}_n}(g)] = (n-m)!\,[Stab_{\mathfrak{S}_m}(g)]$. Et ainsi en posant $C = [Stab_{\mathfrak{S}_m}(g)]$ on obtient finalement cette première formule :

$$Tr(Tr_m(g)) = C\,(n-m)!\,m!\,\mathcal{O}(g) \qquad .$$

Par ailleurs on a : $Tr_m(g) = [Stab_{\mathfrak{S}_m}(g)]\, \mathcal{O}_m(g) = \sum_{\alpha\in\mathcal{P}_m} C\,\lambda_\alpha\, M_{\alpha,m}$, par hypothèse sur $\mathcal{O}_m(g)$, ce qui par la linéarité de la trace nous donne :

$$\begin{aligned} Tr(Tr_m(g)) &= \sum_{\alpha\in\mathcal{P}_m} C\,\lambda_\alpha\, Tr(M_{\alpha,m}) \\ &= \sum_{\alpha\in\mathcal{P}_m} C\,\lambda_\alpha\,(n-m)!\,m!\binom{n-l(\alpha)}{m-l(\alpha)} M_\alpha \qquad , \end{aligned}$$

d'après (11). On obtient donc, en comparant les deux formulations obtenues pour $Tr(Tr_m(g))$:

$$C\,(n-m)!\,m!\,\mathcal{O}(g) = \sum_{\alpha\in\mathcal{P}_m} C\,\lambda_\alpha\, m!\,(n-m)!\binom{n-l(\alpha)}{m-l(\alpha)} M_\alpha \qquad ,$$

$$\text{d'où en simplifiant : } \mathcal{O}(g) = \sum_{\alpha\in\mathcal{P}_m} \lambda_\alpha \binom{n-l(\alpha)}{m-l(\alpha)} M_\alpha \qquad \square$$

Remarque 2. Il est essentiel, dans (12), que g soit d'arité m. Supposons, en effet qu'on ait $g \in \mathbb{C}[x_1,\dots,x_{m'}]$ avec $1 \le m' < m$, g sans terme constant et d'arité m'. Si l'arité n'intervenait pas, pour obtenir $\mathcal{O}(g)$ on pourrait appliquer le Théorème 1.3 de m' à m puis de m à n ou bien directement de m' à m. Ce qui impliquerait que pour tout $\alpha \in \mathcal{P}_m$ on ait $\binom{n-l(\alpha)}{m'-l(\alpha)} = \binom{m-l(\alpha)}{m'-l(\alpha)}\binom{n-l(\alpha)}{m-l(\alpha)}$, ce qui est faux. Puisque $\mathcal{O}_m(g)$ est d'arité m, on peut même constater en développant $\binom{m-l(\alpha)}{m'-l(\alpha)}\binom{n-l(\alpha)}{m-l(\alpha)}$ que

$$\mathcal{O}(\mathcal{O}_m(g)) = \binom{n-m'}{n-m}\mathcal{O}(g) \qquad ,$$

alors que si g est d'arité m on a : $\mathcal{O}(\mathcal{O}_m(g)) = \mathcal{O}(g)$.

2. Application au calcul rapide des résolvantes

Cette application s'inscrit dans un travail en cours avec J.M. Arnaudiès (voir [1]) et il existe déjà quelques exemples dans [11].

Avec les notations et hypothèses ci-dessus, fixons $g \in \mathbb{C}[x_1,\dots,x_m]\backslash\{0\}$, d'arité m. Soient $g_1 = g,\dots,g_s$ les conjugués distincts de g dans l'extension $\mathcal{L}/\mathcal{K}$. Le polynôme élément de $\mathcal{K}[T]$:

$$g_*(T) = \prod_{i=1}^{s}(T-g_i) \tag{13}$$

est appelé *résolvante de Lagrange* (voir [4, tome IV]) définie par g dans $\mathbb{C}[x_1,\dots,x_n]$. En fait, on a $g_*(T) \in Sym(x_1,\dots,x_n)[T]$. Développons $g_*(T)$:

$$g_*(T) = T^s - C_1T^{s-1} + \cdots + (-1)^s C_s,\ \ C_i \in Sym(x_1,\dots,x_n) \qquad . \tag{14}$$

Nous nous proposons de décrire un calcul des C_i qui ramène tout à des manipulations dans $\mathbb{C}[x_1,\dots,x_m]$. Lorsque m/n est “ petit ”, on obtient ainsi d'excellentes simplifications dans le calcul des C_i. Pour cela nous allons procéder par le passage des fonctions puissances comme le faisait déjà Lagrange (voir [5, tome VIII]) dans des cas particuliers et nous utiliserons de plus le théorème de l'arité.

Soient $g'_1 = g, \dots, g'_t$ les conjugués distincts de g dans l'extension $\mathcal{L}_m/\mathcal{K}_m$. Considérons le polynôme $\mathcal{P}(T) \in \mathcal{K}_m[T]$ défini par :

$$\mathcal{P}(T) = \prod_{i=1}^{t}(T - g'_i) \qquad . \tag{15}$$

On a $\mathcal{P}(T) \in Sym(x_1, \dots, x_m)[T]$; développant $\mathcal{P}(T)$:

$$\mathcal{P}(T) = T^t - D_1 T^{t-1} + \dots + (-1)^t D_t \ \ , D_i \in Sym(x_1, \dots, x_m) \qquad . \tag{16}$$

Nous supposerons $\mathcal{P}(T)$ déjà connu ; à cause des formules de Girard-Newton ou bien celles de Waring (voir [2, 7]), cette hypothèse signifie que pour tout entier $j \in \mathbb{N}$, on connait les *fonctions puissances* :

$$p_j = \sum_{i=1}^{t}(g'_i)^j \qquad . \tag{17}$$

Pour calculer $g_*(T)$, il s'agit de calculer en fonction des p_j les fonctions puissances

$$P_j = \sum_{i=1}^{s} g_i^j \qquad , \text{pour } 1 \leq j \leq s \qquad . \tag{18}$$

Fixons $j \in \mathbb{N}$. On a $Stab_{\mathfrak{S}_r}(g) \subset Stab_{\mathfrak{S}_r}(g^j)$ pour $r = m$ ou $r = n$ (par exemple : $g = x_1 - x_2$ et g^2 ont respectivement $\mathcal{A}_2$ et $\mathfrak{S}_2$ comme stabilisateur dans $\mathfrak{S}_2$) ; de plus, puisque g^k est d'arité m, pour tout $k \in \mathbb{N}^*$:

$$Stab_{\mathfrak{S}_n}(g^k) \cong Stab_{\mathfrak{S}_m}(g^k) \times \mathfrak{S}_{n-m} \qquad .$$

Donc, si on pose :

$$f_j = [Stab_{\mathfrak{S}_m}(g^j) : Stab_{\mathfrak{S}_m}(g)] \qquad ,$$

on a aussi $f_j = [Stab_{\mathfrak{S}_n}(g^j) : Stab_{\mathfrak{S}_n}(g)]$. Un calcul direct facile montre que

$$\begin{array}{lrcl} & Tr_m(g^j) & = & [Stab_{\mathfrak{S}_m}(g)]\, p_j \qquad , \\ \text{et d'autre part} & Tr_m(g^j) & = & [Stab_{\mathfrak{S}_m}(g^j)]\, \mathcal{O}_m(g^j) = f_j\, [Stab_{\mathcal{S}_m}(g)]\, \mathcal{O}_m(g^j) \qquad . \end{array}$$

Par suite $p_j = f_j\, \mathcal{O}_m(g^j)$ et de même $P_j = f_j \mathcal{O}\,(g^j)$ ce qui avec le Théorème 1.3 entraîne :

Théorème 2.1. *Soit $g \in \mathbb{C}[x_1, \dots, x_m]$ d'arité m. Pour $j \in [1, s]$, supposons que les p_j définis en* (17) *s'écrivent sous la forme :*

$$p_j = \sum_{\alpha \in \mathcal{P}_m} \lambda_{\alpha,j} M_{\alpha,m} \qquad ;$$

alors les P_j associés définis en (18) *satisfont*

$$P_j = \sum_{\alpha \in \mathcal{P}_m} \lambda_{\alpha,j} \binom{n-l(\alpha)}{m-l(\alpha)} M_\alpha \quad . \tag{19}$$

En réutilisant les formules de Girard-Newton dans $\mathbb{C}[x_1, \dots, x_n]$, la formule (19) permet de calculer les coefficients C_i de (14). Notons que l'entier s est connu comme fonction de l'entier t car : $m! = t\,[Stab_{\mathfrak{S}_m}(g)]$; $n! = s\,[Stab_{\mathfrak{S}_n}(g)]$ et $[Stab_{\mathfrak{S}_n}(g)] = (n-m)!\,[Stab_{\mathfrak{S}_m}(g)]$ donc on a immédiatement :

$$s = \binom{n}{m} t \quad . \tag{20}$$

Exemple 1. La transformation de Tchirnhaus. C'est le cas où g est un polynôme d'une variable x_1 ($m = 1$). On a $p_j = g^j = \sum_{i \in \mathbb{N}} \lambda_i x_1^i$ où $(\lambda_i)_{i \in \mathbb{N}})$ est une famille de support fini. Donc ou bien $\alpha = (i)$ avec $i \neq 0$ et donc $\binom{n-l(\alpha)}{m-l(\alpha)} = 1$ et M_α est la i-ième fonction puissance sur $\{x_1, \dots, x_n\}$, ou bien $\alpha = (0)$ et $\binom{n-l(\alpha)}{m-l(\alpha)} = n$ qui est la fonction puissance d'ordre 0 sur $\{x_1, \dots, x_n\}$. On obtient donc P_j en remplaçant dans p_j le terme x_1^i par la i-ième fonction puissance sur $\{x_1, \dots, x_n\}$. Ceci donne également un algorithme pour calculer le résultant.

Exemple 2. Les résolvantes symétriques. Soit $g = s$ une fonction symétrique en m variables ($1 \leq m \leq n$). On a $p_j = \mathcal{O}_m(s^j) = s^j$ (ici $f_j = 1$). Il suffit donc de calculer s^j sur la base des fonctions monomiales en $x_1, \dots, x_m$ pour obtenir $P_j = \mathcal{O}(s^j)$. Le cas trivial (et extrèmement rapide à calculer) est celui de $s = x_1 x_2 \dots x_m$ puisque les P_j s'obtiennent simplement à partir des fonctions puissances sur $\{x_1, \dots, x_n\}$. Avec la formule multinomiale, il est facile de constater qu'avec $s = x_1^r + \dots + x_m^r$ on obtient :

$$P_j = \sum \binom{j}{\alpha} \binom{n-l(\alpha)}{m-l(\alpha)} M_\alpha$$

où la somme est étendue aux partition $\alpha \in \mathcal{P}_m$ de poids j et où $\binom{j}{\alpha}$ est le coefficient multinomial associé à α et j.

En résumé, le Théorème 2.1 ramène le calcul de $g_*(T)$ à celui de $\mathcal{P}(T)$, ce qui, dans des cas concrets, se révèle d'une efficacité remarquable.[1]

Afin de calculer des groupes de Galois, L. Soicher (voir [9] ou bien [8]) calcule des résolvantes linéaires (i.e. g est linéaire) par la méthode des résultants (donnée par Lagrange, dans [4]) en l'optimisant avec l'interpolation

[1] Par exemple, la résolvante $(x_1 - x_2)_*(x^9 + 7x^5 - 3x^2 - 5x + 1)$ de degré 72 se calcule en 18 secondes sur un IBM RS/6000 modèle 550 sous AIX 3.1.5 avec 64 Mo de mémoire. Ces calculs, actuellement implantés dans Macsyma, sont réalisable dans tout système de Calcul Formel dès lors qu'il possède des fonctions manipulant les polynômes symétriques (par exemple le système Symmetrica (voir [10]) spécialement conçu pour de telles manipulations).

par rapport à la variable T et avec le théorème des restes chinois sur les entiers. La méthode des résultants efficace (dans le même ordre de temps que par les fonctions symétriques) pour les résolvantes linéaires, mais trop coûteuse pour d'autres types de résolvantes, devient difficilement applicable.

3. Cas d'un sous-groupe de $\mathfrak{S}_n$

Soit $n \in \mathbb{N}^*$; donnons-nous un sous-groupe Γ de $\mathfrak{S}_n$. Nous gardons les mêmes notations qu'en (1) et (2) pour la restriction à Γ des actions $\natural$ à droite et $*$ à gauche. Il est très facile de trouver des bases linéaires de $C(x_1, \dots, x_n)^\Gamma$, la $\mathbb{C}$-algèbre des polynômes Γ-invariants ; pour cela, remarquons que le sous-ensemble $\mathbb{N}^n$ de $\mathbb{C}^n$ est Γ-stable. On a alors le résultat connu :

Proposition 3.1. *Soit A un sous-anneau de $\mathbb{C}$. Soit Ω l'ensemble des Γ-orbites de $\mathbb{N}^n$ pour l'action $\natural$. Pour chaque $\omega \in \Omega$, posons :*

$$B_\omega = \sum_{\alpha=(\alpha_1,\dots,\alpha_n)\in\omega} x^\alpha \qquad \text{où } x^\alpha = x_1^{\alpha_1}\dots x_n^{\alpha_n} \qquad ;$$

alors $(B_\omega)_{\omega\in\Omega}$ est une base du A-module $A[x_1, \dots, x_n] \bigcap C(x_1, \dots, x_n)^\Gamma$. En particulier, c'est une base du $\mathbb{C}$-espace vectoriel $C(x_1, \dots, x_n)^\Gamma$.

Dans le cas où $\Gamma = \mathfrak{S}_n$ on a $B_\omega = M_\alpha$ avec $\alpha \in \omega \bigcap \mathcal{P}_n$.

Notons $\mathcal{K}_\Gamma$ le corps des fractions de $\mathbb{C}(x_1, \dots, x_n)^\Gamma$. Fixons maintenant $f \in \mathbb{C}[x_1, \dots, x_n]$. La *trace* de f, notée $Tr_{\mathcal{L}/\mathcal{K}_\Gamma}(f)$, est donnée par :

$$Tr_{\mathcal{L}/\mathcal{K}_\Gamma}(f) = \sum_{\sigma\in\Gamma} \sigma * f \qquad . \tag{21}$$

Le polynôme minimal de f sur $\mathcal{K}_\Gamma$ est $\prod_{g\in Orb_\Gamma(f)}(T - g)$ et ses coefficients appartiennent à $\mathcal{K}_\Gamma \bigcap \mathbb{C}[x_1, \dots, x_n] = \mathbb{C}(x_1, \dots, x_n)^\Gamma$. En particulier, l'élément $\sum_{g\in Orb_\Gamma(f)} g$, que nous noterons $\mathcal{O}(f)$, appartient à $\mathbb{C}(x_1, \dots, x_n)^\Gamma$. Nous dirons que $\mathcal{O}(f)$ est une *trace réduite de f*. Il est clair que $\mathcal{O}(f) = Tr_{\mathcal{K}_\Gamma(f)/\mathcal{K}_\Gamma}(f)$ et comme de plus

$$Tr_{\mathcal{L}/\mathcal{K}_\Gamma}(f) = \sum_{\sigma\in\Gamma} \sigma * f = \sum_{g\in Orb_\Gamma(f)} [Stab_\Gamma(g)]\, g = [Stab_\Gamma(f)] \sum_{g\in Orb_\Gamma(f)} g$$

on obtient pour tout $f \in \mathbb{C}[x_1, \dots, x_n]$:

$$Tr_{\mathcal{L}/\mathcal{K}_\Gamma}(f) = [Stab_\Gamma(f)]\, \mathcal{O}(f) \qquad . \tag{22}$$

Pour un monôme $f = x^\alpha$ cette formule s'écrit :

$$\forall \alpha \in \mathbb{N} \qquad Tr_{\mathcal{L}/\mathcal{K}_\Gamma}(x^\alpha) = [Stab_\Gamma(x^\alpha)]\, \mathcal{O}(x^\alpha) \qquad . \tag{23}$$

Comme $[Stab_\Gamma(x^\alpha)] = [Stab_\Gamma(\alpha)]$, si on note $\omega = Orb_\Gamma(\alpha)$ on a $\mathcal{O}(x^\alpha) = B_\omega$ et on trouve cette expression de B_ω :

$$\forall \alpha \in \omega \qquad \sum_{\sigma\in\Gamma} \sigma * x^\alpha = [Stab_\Gamma(\alpha)]\, B_\omega = \frac{[\Gamma]}{card(\omega)} B_\omega \qquad . \tag{24}$$

Comme pour le cas du groupe symétrique, donnons-nous un entier m, $1 \leq m < n$, et considérons l'action naturelle de Γ sur $[1,n]$. Soit $\mathcal{G}_m$ le stabilisateur de $[1,m]$ pour cette action naturelle, i.e. $\mathcal{G}_m = \{\sigma \in \Gamma \mid \sigma([1,m]) = [1,m]\}$.

On a un morphisme naturel de groupes

$$\begin{array}{rcccl} \theta & : & \mathcal{G}_m & \longrightarrow & \mathfrak{S}_m \\ & & \sigma & \longmapsto & \sigma|_{[1,m]} \end{array} \quad ,$$

dont l'image sera notée Γ_m.

Comme dans le paragraphe 1, $\mathfrak{S}_m$ sera ci-dessous identifié à un sous-groupe de $\mathfrak{S}_n$ par le plongement canonique $\mathfrak{S}_m \mapsto \mathfrak{S}_n$. Fixons $\alpha \in \mathbb{N}^m$; notons $\omega_m = Orb_{\Gamma_m}(x^\alpha)$, $\omega = Orb_\Gamma(x^\alpha)$, $P_\alpha = B_\omega = \sum_{h\in\omega} h$ et $P_{\alpha,m} = B_{\omega_m} = \sum_{h\in\omega_m} h$. Les fonctions Tr et $\mathcal{O}$ relatives aux sous-groupe Γ_m de $\mathfrak{S}_m$ seront notées Tr_m et $\mathcal{O}_m$. Donc $P_\alpha = \mathcal{O}(x^\alpha)$ et $P_{\alpha,m} = \mathcal{O}_m(x^\alpha)$.

Pour la suite, il est intéressant de remarquer le résultat suivant :

Lemme 1. *Avec les notations décrites ci-dessus, si* Γ_m *opère transitivement sur* $[1,m]$ *alors* $Stab_\Gamma(B_{\omega_m}) = \mathcal{G}_m$.

Démonstration. (a) Soit d'abord $\sigma \in \mathcal{G}_m$ et notons $\overline{\sigma} = \sigma|_{[1,m]}$. Puisque $\overline{\sigma} \in \Gamma_m$, l'application $h \mapsto \overline{\sigma} * h$ est une bijection de ω_m sur ω_m. On a donc :

$$\sigma * B_{\omega_m} = \sum_{h\in\omega_m} \sigma * h = \sum_{h\in\omega_m} \overline{\sigma} * h$$

(car, du fait que $\alpha \in \mathbb{N}^m$, on a $\overline{\sigma} * h = \sigma * h$ pour tout $h \in \omega_m$) d'où $\sigma * B_{\omega_m} = B_{\omega_m}$. Cela prouve que $\mathcal{G}_m \subset Stab_\Gamma(B_{\omega_m})$.

(b) Remarquons ensuite que, du fait que $\alpha \neq \underline{0}$ et que Γ_m opère transitivement sur $[1,m]$, on a un même entier $d \geq 1$ tel que $deg_{X_i}(B_{\omega_m}) = d$ pour tout $i \in [1,m]$. En effet, soit $i_0 \in [1,m]$ tel que $deg_{X_{i_0}}(B_{\omega_m}) \geq 1$: un tel i_0 existe car $\alpha \neq \underline{0}$ (la formule $B_{\omega_m} = \sum_{\beta\in Orb_{\Gamma_m}(\alpha)} x^\beta$ le montre clairement). Pour tout $\tau \in \Gamma_m$, on vient de voir que $\tau * B_{\omega_m} = B_{\omega_m}$, mais $deg_{X_{i_0}}(\tau * B_{\omega_m}) = deg_{X_{\tau^{-1}(i_0)}}(B_{\omega_m})$, donc $deg_{X_{\tau^{-1}(i_0)}}(B_{\omega_m}) = deg_{X_{i_0}}(B_{\omega_m}) \geq 1$. Lorsque τ parcourt Γ_m, $\tau^{-1}(i_0)$ parcours $[1,m]$ car, par hypothèse, Γ_m opère transitivement sur $[1,m]$. Donc l'assertion en découle.

(c) Soient maintenant $i \in [1,m]$ et $\sigma \in \mathfrak{S}_n$ tel que $\sigma * B_{\omega_m} = B_{\omega_m}$. On a $deg_{X_i}(B_{\omega_m}) = d = deg_{X_i}(\sigma * B_{\omega_m}) = deg_{X_{\sigma^{-1}(i)}}(B_{\omega_m})$; donc $deg_{X_{\sigma^{-1}(i)}}(B_{\omega_m}) = d \geq 1$. Mais par construction, B_{ω_m} ne dépend que de $x_1, \ldots, x_m$. D'où forcément : $\sigma^{-1}(i) \leq m$. Cela est vrai pour tout $i \in [1,m]$. Donc $\sigma \in \mathcal{G}_m$, et le lemme est ainsi prouvé. □

La proposition suivante donne l'extension de la formule (11) à un sous-groupe du groupe symétrique :

Proposition 3.2. *Avec les notations ci-dessus, si* Γ_m *est un sous-groupe de* Γ *qui opère transitivement sur* $[1,m]$ *et si* $\alpha \in \mathbb{N}^m$ *alors :*

$$Tr(B_{\omega_m}) = [\mathcal{G}_m]\, F_{\omega,m}\, B_\omega \tag{25}$$

ou, de manière équivalente,

$$Tr(P_{\alpha,m}) = [\mathcal{G}_m]\, f_\alpha\, P_\alpha \qquad , \textit{ avec} \tag{26}$$

$$F_{\omega,m} = f_\alpha = [Stab_\Gamma(x^\alpha) : Stab_{\mathcal{G}_m}(x^\alpha)] \qquad . \tag{27}$$

Démonstration. Supposons tout d'abord $\alpha \neq \underline{0}$. On a $Tr_m(x^\alpha) = [Stab_{\Gamma_m}(x^\alpha)]\, \mathcal{O}_m(x^\alpha) = [Stab_{\Gamma_m}(x^\alpha)]\, B_{\omega_m}$. Donc on a d'une part

$$Tr(Tr_m(x^\alpha)) = [Stab_{\Gamma_m}(x^\alpha)]\, Tr(B_{\omega_m}) \qquad .$$

D'autre part $Tr_m(x^\alpha) = \sum_{\tau\in\Gamma_m} \tau * x^\alpha$, d'où

$$\begin{aligned} Tr(Tr_m(x^\alpha)) &= \sum_{\sigma\in\Gamma} \sigma * \sum_{\tau\in\Gamma_m} \tau * x^\alpha = \sum_{\tau\in\Gamma_m} (\sum_{\sigma\in\Gamma} (\sigma\tau) * x^\alpha) \\ &= \sum_{\tau\in\Gamma_m} Tr(x^\alpha) = [\Gamma_m]\, Tr(x^\alpha) \qquad , \end{aligned}$$

car pour τ fixé, $\sigma \mapsto \sigma\tau$ est une bijection de Γ sur lui-même (puisque $\tau \in \Gamma_m \subset \Gamma$ par hypothèse). Mais comme $Tr(x^\alpha) = [Stab_\Gamma(x^\alpha)]\, \mathcal{O}(x^\alpha) = [Stab_\Gamma(x^\alpha)]\, B_\omega$ les deux expressions de $Tr(Tr_m(x^\alpha))$ aboutissent à

$$[Stab_{\Gamma_m}(x^\alpha)]\, Tr(B_{\omega_m}) = [\Gamma_m]\, [Stab_\Gamma(x^\alpha)]\, B_\omega \qquad . \tag{28}$$

Notons $\mathcal{N}_m$ le noyau du morphisme naturel $\mathcal{G}_m \xrightarrow{\theta} \mathfrak{S}_m$ et considérons le groupe $Stab_{\mathcal{G}_m}(x^\alpha) = Stab_\Gamma(x^\alpha) \bigcap \mathcal{G}_m$. Il contient $\mathcal{N}_m$, et son image par le morphisme naturel θ n'est autre que $Stab_{\Gamma_m}(x^\alpha)$. On a donc

$$\mathcal{N}_m = Ker(\theta|_{Stab_{\mathcal{G}_m}(x^\alpha)}) \qquad ,$$

d'où $[Stab_{\mathcal{G}_m}(x^\alpha)] = [Stab_{\Gamma_m}(x^\alpha)]\, [\mathcal{N}_m]$. Puisque $Stab_{\mathcal{G}_m}(x^\alpha)$ est un sous-groupe de $Stab_\Gamma(x^\alpha)$, on en déduit que $[Stab_{\Gamma_m}(x^\alpha)]\, [\mathcal{N}_m]$ divise $[Stab_\Gamma(x^\alpha)] = \frac{[\Gamma]}{card(\omega)}$. On a alors un entier $f_\alpha \in \mathbb{N}^*$, ne dépendant en fait que de ω et de m, donc que nous pouvons également noter $F_{\omega,m}$, et tel que :

$$[Stab_\Gamma(x^\alpha)] = f_\alpha\, [Stab_{\Gamma_m}(x^\alpha)]\, [\mathcal{N}_m] = F_{\omega,m}\, [Stab_{\Gamma_m}(x^\alpha)]\, [\mathcal{N}_m] \qquad .$$

En reportant cette relation dans (28) et en remarquant que $[\mathcal{G}_m] = [\mathcal{N}_m]\, [\Gamma_m]$, on obtient la relation (25) de la proposition.

Maintenant si $\alpha = \underline{0}$ alors on a $f_{\underline{0}} = [\Gamma]/[\mathcal{G}_m]$. Ce qui permet de constater que :

$$Tr(P_{\underline{0},m}) = [\Gamma] = [\mathcal{G}_m]\, f_{\underline{0}}\, P_{\underline{0}} \qquad ,$$

et la relation (26) est encore satisfaite. □

Remarque 3. Le calcul de $F_{\omega,m}$ n'est pas immédiat, en effet

$$F_{\omega,m} = \frac{card(\omega_m)[\Gamma]}{card(\omega)[\mathcal{G}_m]} \qquad .$$

Remarque 4. Dans le cas du groupe symétrique on trouve bien la relation (10). On se place dans le cas où $\Gamma = \mathfrak{S}_m$. On voit que l'hypothèse de la Proposition 3.2 est satisfaite puisque $\Gamma_m = \mathfrak{S}_m$ et $\mathcal{G}_m \cong \mathfrak{S}_m \times \mathfrak{S}_{n-m}$. Reprenant les notations de la formule (5) du paragraphe 1, il vient :

$$Stab_\Gamma(x^\alpha) = Stab_{\mathfrak{S}_n}(\alpha) = \{\sigma \in \mathfrak{S}_n \mid \sigma(J_1) = J_1, \cdots, \sigma(J_r) = J_r\} \qquad ,$$

donc $[Stab_\Gamma(x^\alpha)] = m_1!m_2!\dots m_r!(n-l(\alpha))!$, et de même

$$Stab_{\mathcal{G}_m}(x^\alpha) = \{\sigma \in \mathfrak{S}_m \times \mathfrak{S}_{n-m} \mid \sigma(J_1) = J_1, \cdots, \sigma(J_r) = J_r\}$$

d'où $[Stab_{\mathcal{G}_m}(x^\alpha] = m_1!m_2!\dots m_r!(m-l(\alpha))!(n-m)!$, ce qui donne bien la formule (10) :

$$f_\alpha = \frac{[Stab_\Gamma(x^\alpha]}{[Stab_{\mathcal{G}_m}(x^\alpha]} = \frac{(n-l(\alpha))!}{(m-l(\alpha))!\,(n-m)!} = \binom{n-l(\alpha)}{m-l(\alpha)} \qquad .$$

Notons $\mathcal{T}_m$ une transversale pour l'action $\natural$ de Γ_m sur $\mathbb{N}^m$. D'après la Proposition 3.1, la famille $(P_{\alpha,m})_{\alpha\in\mathcal{T}_m}$ est une base du $\mathbb{C}$-espace vectoriel $\mathbb{C}(x_1,\dots,x_m)^{\Gamma_m}$. On peut maintenant donner le résultat suivant sur les fonctions d'arité m :

Théorème 3.3. (Arité) *Soit $g \in \mathbb{C}[x_1,\dots,x_m]$ d'arité m. Ecrivons $\mathcal{O}_m(g)$ sous la forme :*

$$\mathcal{O}_m(g) = \sum_{\alpha\in\mathcal{T}_m} \lambda_\alpha\, P_{\alpha,m} \qquad , \tag{29}$$

où (λ_α) est une famille de support fini. Alors si Γ_m est un sous-groupe de Γ qui opère transititivement sur $[1,m]$ il vient

$$\mathcal{O}(g) = \sum_{\alpha\in\mathcal{T}_m} \lambda_\alpha\, f_\alpha\, P_\alpha \qquad , \tag{30}$$

où les f_α sont donnés par la relation (27) de la Proposition 3.2.

Démonstration. Notons d'abord que (29) a un sens, parce que $\mathcal{O}_m(g)$ est Γ_m invariant. On a :

$$Tr_m(g) = [Stab_{\Gamma_m}(g)]\,\mathcal{O}_m(g) = \sum_{\alpha\in\mathcal{T}_m} C\,\lambda_\alpha\, P_{\alpha,m} \qquad ,$$

avec $C = [Stab_{\Gamma_m}(g)]$. D'où

$$Tr(Tr_m(g)) = \sum_{\alpha\in\mathcal{T}_m} C\,\lambda_\alpha\, Tr(P_{\alpha,m}) \qquad .$$

En appliquant la relation (26) de la Proposition 3.2, on obtient :

$$Tr(Tr_m(g)) = \sum_{\alpha\in\mathcal{T}_m} C\,\lambda_\alpha\,[\mathcal{G}_m]\, f_\alpha\, P_\alpha \qquad .$$

D'autre part

$$Tr(Tr_m(g)) = \sum_{\sigma\in\Gamma} \sigma * (\sum_{\tau\in\Gamma_m} \tau * g) = \sum_{\tau\in\Gamma_m}\sum_{\sigma\in\Gamma} (\sigma\tau) * g = [\Gamma_m]\, Tr(g) \qquad ,$$

car pour τ fixé, et du fait que $\tau \in \Gamma_m \subset \Gamma$, $\sigma \mapsto \sigma\tau$ est une bijection de Γ sur Γ. De plus, comme $Tr(g) = [Stab_\Gamma(g)]\, \mathcal{O}(g)$ on obtient, en identifiant les deux expression de $Tr(Tr_m(g))$, :

$$[\Gamma_m]\,[Stab_\Gamma(g)]\,\mathcal{O}(g) = \sum_{\alpha \in \mathcal{T}_m} C\,\lambda_\alpha\,[\mathcal{G}_m]\,f_\alpha\,P_\alpha \qquad . \tag{31}$$

Du fait que l'arité de g est m, le raisonnement fait pour prouver le Lemme 1 prouve que $Stab_\Gamma(g) \subset \mathcal{G}_m$; il est clair que $\mathcal{N}_m \subset Stab_\Gamma(g)$, et que la restriction à $Stab_\Gamma(g)$ du morphisme naturel $\mathcal{G}_m \mapsto \mathfrak{S}_m$ a pour noyau $\mathcal{N}_m$ et pour image $Stab_{\Gamma_m}(g)$. Donc

$$[Stab_\Gamma(g)] = [\mathcal{N}_m]\,[Stab_{\Gamma_m}(g)] \qquad ,$$

tandis que $[\mathcal{G}_m] = [\mathcal{N}_m]\,[\Gamma_m]$. En reportant ces relations dans (31), et en simplifiant, on obtient :

$$\mathcal{O}(g) = \sum_{\alpha \in \mathcal{T}_m} \lambda_\alpha\,f_\alpha\,P_\alpha \qquad \square$$

Définition 3.4. Un triplet (I, J, G) sera appelé un *triplet transitif* s'il remplit les conditions suivantes :

(i) I est un ensemble fini non vide;

(ii) J une partie non vide de I;

(iii) G est un sous-groupe de $\mathfrak{S}_I$ tel que $Stab_G(J)$ opère transitivement sur J;

(iv) pour tout $\sigma \in Stab_G(J)$, le prolongement à I de $\mathfrak{S}|_J$ par l'identité sur $I \backslash J$ appartient à G.

Remarque 5. La condition (iv) de cette définition signifie que si l'on identifie $\mathfrak{S}_J$ à un sous-groupe de $\mathfrak{S}_I$, alors l'image naturelle de $Stab_G(J)$ par $\sigma \mapsto \sigma|_J$ est contenue dans G. Autrement dit, un système transitif est la donnée d'un groupe de permutations G d'un ensemble fini I, et d'un sous-ensemble J de I, tels que (I, J, G) remplissent les hypothèses du Théorème 3.3.

Remarque 6. Un tel système peut se construire aisément en prenant pour G le produit direct d'un sous-groupe transitif de $\mathfrak{S}_m$ et d'un sous-groupe quelconque de $\mathfrak{S}_{n-m}$.

4. Cas d'un produit direct de groupes de permutations

Nous allons voir que le théorème de l'arité se généralise naturellement à des produits de groupes.

Donnons-nous maintenant $d \in \mathbb{N}^*$. Soient des entiers $n_1 \geq 1, \ldots, n_d \geq 1$ et $\mathfrak{S}_{n_1} \times \cdots \times \mathfrak{S}_{n_d}$ le sous-groupe de Young de $\mathfrak{S}_n$ ($n = n_1 + \cdots + n_d$). Pour chaque i on se donne un sous-groupe Γ_i de $\mathfrak{S}_{n_i}$ et un entier m_i ($1 \leq m_i \leq n_i$) définissant un sous-groupe noté Γ_{i,m_i} induit par le stabilisateur de $[1, m_i]$ dans Γ_i (voir paragraphe 3). Nous noterons $\mathcal{G}^{(i)}_{m_i}$ ce stabilisateur.

Nous noterons $\mathcal{T}_{m_i}$ une transversale pour l'action $\natural$ de Γ_{i,m_i} sur $\mathbb{N}^{m_i}$; comme d'habitude, $\mathbb{N}^{m_i}$ sera identifié, par le plongement naturel, à un sous-ensemble de $\mathbb{N}^{n_i}$.

Soient Γ le produit direct $\Gamma_1 \times \cdots \times \Gamma_d$ et $\Gamma_{(m)}$ le produit direct $\Gamma_{1,m_1} \times \cdots \times \Gamma_{d,m_d}$. Naturellement $\Gamma_{(m)}$ sera identifié à un sous-groupe de Γ. Il est clair que l'ensemble $\mathcal{T} = \mathcal{T}_{m_1} \times \cdots \times \mathcal{T}_{m_d}$ est une transversale pour l'action produit $\natural$ de $\Gamma_{(m)}$ sur l'ensemble $\mathcal{E} = \mathbb{N}^{m_1} \times \cdots \times \mathbb{N}^{m_d}$ (i.e action produit de celles des Γ_i sur les $\mathbb{N}^{m_i}$).

Enfin nous nous donnons n interminées sur $\mathbb{C}$:

$$X = (X_1^{(1)}, \ldots, X_{n_1}^{(1)}, \ldots, X_1^{(d)}, \ldots, X_{n_d}^{(d)}) \qquad .$$

Pour i fixé ($1 \leq i \leq d$), on notera $X^{(i)}$ le sous-ensemble $(X_1^{(i)}, \ldots, X_{n_i}^{(i)})$. L'action à gauche $*$ de Γ sur X est l'action produit de celles des Γ_i sur les $X^{(i)}$.

Nous ferons l'hypothèse fondamentale que, pour chaque i, Γ_{i,m_i} est un sous-groupe de Γ_i agissant transitivement sur $[1, m_i]$ (i.e. $([1, n_i], [1, m_i], \Gamma_i)$ est un système transitif).

Nous allons étudier quelques propriétés des fonctions suivantes :

- fonction $Tr = Tr_{\mathbb{C}(X)/\mathcal{K}_\Gamma}|_{\mathbb{C}[X]}$, où $\mathcal{K}_\Gamma$ est le corps des Γ-invariants de $\mathbb{C}(X)$;
- fonction $\mathcal{O} : \mathbb{C}[X] \to C(X)^\Gamma$, $f \mapsto$ trace réduite de f ;
- fonctions Tr_m et $\mathcal{O}_m$: analogues à Tr et $\mathcal{O}$, mais avec $\Gamma_{(m)}$ à la place de Γ, et Y à la place X, où Y désigne le sous-ensemble de variables $((X_j^{(i)}, 1 \leq j \leq m_i), 1 \leq i \leq d)$;
- fonctions $Tr^{(i)}$ et $\mathcal{O}^{(i)}$, $Tr_{m_i}^{(i)}$ et $\mathcal{O}_{m_i}^{(i)}$, analogues à Tr, $\mathcal{O}$, Tr_m et $\mathcal{O}_m$, mais associées au système transitif $([1, n_i], [1, m_i], \Gamma_i)$.

Soit $\alpha = (\alpha^{(1)}, \ldots, \alpha^{(d)}) \in \mathbb{N}^n$ avec $\alpha^{(i)} \in \mathbb{N}^{n_i}$ pour tout i.

Nous poserons, si $\alpha^{(i)} \in \mathbb{N}^{m_i}$ pour tout i :

$$P_{\alpha,m} = \sum_{h \in Orb_{\Gamma_{(m)}}(x^\alpha)} h \quad ; \quad P^{(i)}_{\alpha^{(i)},m_i} = \sum_{h \in Orb_{\Gamma_{i,m_i}}(x^{\alpha^{(i)}})} h \quad ; \tag{32}$$

et pour α quelconque :

$$P_\alpha = \sum_{h \in Orb_\Gamma(x^\alpha)} h \quad ; \quad P^{(i)}_{\alpha^{(i)}} = \sum_{h \in Orb_{\Gamma_i}(x^{\alpha^{(i)}})} h \quad . \tag{33}$$

Lemme 2. *Soit $\alpha = (\alpha^{(1)}, \ldots, \alpha^{(d)}) \in \mathcal{E}$, alors on a $P_\alpha = \prod_{i=1}^d P^{(i)}_{\alpha^{(i)}}$.*

Démonstration. Il est clair que $Orb_\Gamma(\alpha) = Orb_{\Gamma_1}(\alpha^{(1)}) \times \cdots \times Orb_{\Gamma_d}(\alpha^{(d)})$, d'où :

$$\begin{aligned} P_\alpha &= \sum_{\beta \in Orb_\Gamma(\alpha)} x^\beta = \sum_{\beta \in Orb_\Gamma(\alpha)} x^{\beta^{(1)}} \cdots x^{\beta^{(d)}} \\ &= \prod_{i=1}^d \Big(\sum_{\beta \in Orb_{\Gamma_i}(\alpha^{(i)})} x^{\beta^{(i)}} \Big) = \prod_{i=1}^d P^{(i)}_{\alpha^{(i)}} \qquad \square \end{aligned}$$

Lemme 3. *Soit* $\alpha = (\alpha^{(1)}, \dots, \alpha^{(d)}) \in \mathcal{E}$ *alors*

$$Tr(P_{\alpha,m}) = \prod_{i=1}^{d} Tr^{(i)}(P^{(i)}_{\alpha^{(i)},m_i}) \qquad .$$

Démonstration. En appliquant le Lemme 2 à $P_{\alpha,m}$ on a

$$\begin{aligned} Tr(P_{\alpha,m}) &= \sum_{\substack{\sigma\in\Gamma \\ \sigma=(\sigma_1,\dots,\sigma_d)}} \sigma * P_{\alpha,m} = \sum_{\substack{\sigma\in\Gamma \\ \sigma=(\sigma_1,\dots,\sigma_d)}} (\sigma * P^{(1)}_{\alpha^{(1)},m_1}) \cdots (\sigma * P^{(d)}_{\alpha^{(d)},m_d}) \\ &= \prod_{i=1}^{d} \Big(\sum_{\sigma_i\in\Gamma_i} \sigma_i * P^{(i)}_{\alpha^{(i)},m_i} \Big) = \prod_{i=1}^{d} Tr^{(i)}(P^{(i)}_{\alpha^{(i)},m_i}) \qquad \square \end{aligned}$$

Une conséquence immédiate de ces lemmes est l'extension suivante de la relation (*26*) de la Proposition *3.2*.

Proposition 4.1. *Soit* $\alpha = (\alpha^{(1)}, \dots, \alpha^{(d)}) \in \mathcal{E}$, *alors*

$$Tr(P_{\alpha,m}) = [\mathcal{G}_{(m)}] f_\alpha \, P_\alpha \qquad \text{, avec} \tag{34}$$

$$f_\alpha = \prod_{i=1}^{d} [Stab_{\Gamma_i}(x^{\alpha^{(i)}}) : Stab_{\mathcal{G}^{(i)}_{m_i}}(x^{\alpha^{(i)}})] \qquad , \tag{35}$$

où $\mathcal{G}^{(i)}_{m_i}$ *est le stabilisateur de* $[1, m_i]$ *dans* Γ_i *et* $\mathcal{G}_{(m)} = \mathcal{G}^{(1)}_{m_1} \times \cdots \times \mathcal{G}^{(d)}_{m_d}$.

Démonstration. Avec le Lemme 3, il suffit, pour obtenir cette proposition, d'appliquer (26) à chaque $P^{(i)}_{\alpha^{(i)},m_i}$, ce qui est possible puisque pour tout i le triplet $([1, n_i], [1, m_i], \Gamma_i)$ est un système transitif. $\square$

Le théorème qui suit montre que tout ce qui précède débouche sur un outil de calcul :

Théorème 4.2. *Les notations étant celles qui précèdent, soit g un élément de $\mathbb{C}[X]$ non nul, tel que pour tout i, g soit d'arité m_i par rapport à $X^{(i)}$, et ne dépende que de $X^{(i)}_1, \dots, X^{(i)}_{m_i}$. Alors $\mathcal{O}_m(g)$ s'écrit :*

$$\mathcal{O}_m(g) = \sum_{\alpha\in\mathcal{T}} \lambda_\alpha \, P_{\alpha,m} \qquad , \tag{36}$$

avec (λ_α) famille à support fini dans $\mathbb{C}$; et si pour chaque i le triplet $([1, n_i], [1, m_i], \Gamma_i)$ est un système transitif

$$\mathcal{O}(g) = \sum_{\alpha\in\mathcal{T}} \lambda_\alpha \, f_\alpha \, P_{\alpha,m} \qquad , \tag{37}$$

où les f_α sont définis par (35).

Démonstration. Montrons tout d'abord que (36) a un sens. Soit $\mathcal{T}_{m_i}$ une transversale pour l'action $\natural$ de Γ_{i,m_i} sur $\mathbb{N}^{m_i}$. Soit $\mathcal{T} = \mathcal{T}_{m_1} \times \cdots \times \mathcal{T}_{m_d}$; on sait que

$$(P_{\alpha,m})_{\alpha\in\mathcal{T}} = \Big(\prod_{i=1}^{d} P^{(i)}_{\alpha^{(i)},m_i}\Big)_{\alpha\in\mathcal{T}}$$

est une base du $\mathbb{C}$-espace vectoriel des $f \in \mathbb{C}[Y]$ qui sont $\Gamma_{(m)}$-invariants (voir Proposition 3.1 et Lemme 2). On a donc bien une décomposition de $\mathcal{O}_m(g)$ comme dans l'assertion (36) du théorème puisque $\mathcal{O}_m(g)$ est $\Gamma_{(m)}$-invariant.

Démontrons maintenant la relation (37) du Théorème 4.2. Soit $\mathcal{G}_{(m)}$ le groupe produit $\mathcal{G}_{m_1}^{(1)} \times \cdots \times \mathcal{G}_{m_d}^{(d)}$. Notons $\mathfrak{S}_{\underline{m}}$ le sous-groupe $\mathfrak{S}_{m_1} \times \ldots \times \mathfrak{S}_{m_d}$ de $\mathfrak{S}_n$.

Soit $\mathcal{N}_m$ le noyau du morphisme $\theta : \mathcal{G}_{(m)} \to \mathfrak{S}_{\underline{m}}$. Notant $\mathcal{N}_{m_i}^{(i)}$ le noyau de $\theta_i : \mathcal{G}_{m_i}^{(i)} \to \mathfrak{S}_{m_i}$, on a : $\mathcal{N}_m = \mathcal{N}_{m_1}^{(1)} \times \cdots \times \mathcal{N}_{m_d}^{(d)}$. Du fait que g est d'arité m_i en $X^{(i)}$, on déduit que $Stab_\Gamma(g) \subset \mathcal{G}_{(m)}$. Comme $\mathcal{N}_m \subset Stab_\Gamma(g)$, on voit que $\mathcal{N}_m$ est le noyau $\theta|_{Stab_\Gamma(g)}$; l'image $\theta(Stab_\Gamma(g))$ est $Stab_{\Gamma_{(m)}}(g)$, d'où :

$$[Stab_\Gamma(g)] = [\mathcal{N}_m]\,[Stab_{\Gamma_{(m)}}(g)] \qquad . \tag{38}$$

Par ailleurs, en considérant le morphisme θ, on a $[\mathcal{G}_{(m)}] = [\mathcal{N}_m]\,[\Gamma_{(m)}]$.

Maintenant, par analogie à la preuve du Théorème 3.3 de l'arité, on a d'une part $Tr(Tr_m(g)) = [\Gamma_{(m)}]\,Tr(g) = [\Gamma_{(m)}]\,[Stab_\Gamma(g)]\mathcal{O}(g) = [\mathcal{G}_{(m)}][Stab_{\Gamma_{(m)}}(g)]\mathcal{O}(g)$, en utilisant (38), et d'autre part

$$\begin{aligned}
Tr_m(g) &= [Stab_{\Gamma_{(m)}}(g)]\,\mathcal{O}_m(g) = [Stab_{\Gamma_{(m)}}(g)] \sum_{\alpha\in\mathcal{T}} \lambda_\alpha\, P_{\alpha,m} \qquad , \\
\text{donc :} \qquad Tr(Tr_m(g)) &= \sum_{\alpha\in\mathcal{T}} [Stab_{\Gamma_{(m)}}(g)]\,\lambda_\alpha\, Tr(P_{\alpha,m}) \\
&= \sum_{\alpha\in\mathcal{T}} [Stab_{\Gamma_{(m)}}(g)]\,\lambda_\alpha\,[\mathcal{G}_{(m)}]\,f_\alpha\, P_\alpha \qquad ,
\end{aligned}$$

en appliquant la Proposition 4.1. En identifiant nos deux expressions de $Tr(Tr_m(g))$, on obtient :

$$[\mathcal{G}_{(m)}]\,[Stab_{\Gamma_{(m)}}(g)]\,\mathcal{O}(g) = \sum_{\alpha\in\mathcal{T}} [\mathcal{G}_{(m)}]\,[\Gamma_{(m)}]\,\lambda_\alpha\, f_\alpha\, P_\alpha \qquad ,$$

ce qui, après simplification, donne la formule (37) du théorème. □

Remarque 7. Pour la clarté de la présentation, nous avons supposé $m_i \neq 0$ pour tout i, mais le Theorème 4.2 reste valable si certains m_i sont nuls.

L'exemple fondamental où tout ce qui précède s'applique est celui où l'on prend $\Gamma_i = \mathfrak{S}_{n_i}$ pour tout i (cas des polynômes *multisymétriques*). Alors les $P^{(i)}_{\alpha^{(i)},m_i}$ et les $P^{(i)}_{\alpha^{(i)}}$ sont les fonctions monomiales sur $X^{(i)}$; on peut prendre $\mathcal{T}_{m_i} = \mathcal{P}_{m_i}$. L'entier f_α de (35) est évidemment donné par :

$$f_\alpha = \prod_{i=1}^{d} \binom{n_i - l(\alpha^{(i)})}{m_i - l(\alpha^{(i)})} \qquad . \tag{39}$$

Conclusion. Avec le Théorème 4.2 nous avons un théorème général utile aux calculs des résolvantes de plusieurs polynômes (définies et appelées *images directes* dans [3]), dont une application est de chercher des polynômes minimaux d'extensions algébriques obtenues à partir de combinaisons d'extensions algébriques définies elles mêmes par des polynômes minimaux (ce problème avait été posé par Loos dans [6]). Dans le cas d'un seul polynôme nous avons vu dans le paragraphe 2 que les calculs de résolvantes, introduites par Lagrange pour la résolution des équations, pouvaient alors devenir très rapides.

Remerciements. Jean-Marie Arnaudiès qui s'est intéressé à ce travail a permis qu'il aboutisse sous la forme actuelle. Je le remercie vivement de son investissement généreux et constructif. Je remercie aussi le rapporteur pour les nombreuses remarques et suggestions qu'il a faites sur la première version de ce papier.

References

[1] Arnaudiès,J-M, A. Valibouze, (1992), *Résolvantes de Lagrange*, manuscrit.
[2] Girard, 1629, Invention Nouvelle en Algèbre, Amsterdam.
[3] M.Giusti, D.Lazard, A.Valibouze, (1988). *Algebraic transformations of polynomial equations, symmetric polynomials and elimination,* Symbolic and Algebraic Computation, International Symposium ISSAC '88 (P. Gianni, ed.), Lect. Notes in Comp. Sc. **358**, 309-314.
[4] Lagrange, J.L., Reflexions sur la résolution algébrique des équations, Prussian Academy, 1770 (Mémoires, Tome IV p.205-421).
[5] Lagrange, J.L., Traité de la résolution des équations numériques : Notes sur la théorie des équations algébriques, Mémoires, Tome VIII, p133-367.
[6] Loos, R., *Computing in Algébraic Extension*, Computer Algebra, Symbolic and Algebraic Computation, Springer-Verlag, 173-187.
[7] Macdonald, I.G., Symmetric functions and Hall polynomials, Clarendon Press, Oxford 1979.
[8] John McKay and Leonard Soicher, (1985), *Computing Galois Groups over the rationals*, Journal of number theory **20**, 273-281.
[9] Leonard Soicher, *The computation of the Galois groups*, Thesis in departement of computer science, Concordia University, Montreal, Quebec, Canada, (1981).
[10] Symmetrica, A computer algebra system for finite symmetric groups , A. Kohnert, A.Kerber (Lehrstuhl II fur Math. Bayreuth, Postfach 10 12 51, 8580 Bayreuth).
[11] A. Valibouze, (1988), *Manipulations de fonctions symétriques*, Thèse de l'Université Paris VI.

L.I.T.P., Université Paris VI, 4 place Jussieu, F-75252 Paris Cedex 05
E-mail address: avb@litp.ibp.fr