Stage de recherche de M1

Avril - juin 2023

Gael Druez

Symmetries in computationnal algebra

Sous la direction de Cordian Riener

UiT The Arctic University of Norway

Avec le soutien financier de :

ENS rennes | Université de Rennes

Centre Henri Lebesgue
Centre de Mathématiques

gael.druez@ens-rennes.fr

Table des matières

 gael.druez@ens-rennes.fr

1 Présentation et objectifs

Ce stage vise à généraliser un résultat connu sur des polynômes symétriques.

En effet, [N P09] et [Lau16] étudient une factorisation du discriminant pour des polynômes symétriques. On cherche à généraliser ce résultat pour des polynômes invariants sous l'action d'un groupe plus général, à savoir un groupe de réflexion.

Dans une première partie, on étudiera le résultat de factorisation du discriminant pour des polynômes symétriques. On introduira les outils importants et on expliquera rapidement les idées importantes de la preuve.

Ensuite, on étudiera les groupes de réflexion et comment certaines de leurs propriétés laissent penser qu'ils généraliseront le résultat. On suivra les exemples des groupes $\mathcal{S}_n$ et $\mathcal{D}_n$, le groupe symétrique et le groupe diédral, tous deux des groupes de réflexions qui nous permettront de mettre en avant les propriétés importantes.

Enfin, on regardera en détail la généralisation en question : on détaillera comment les notions particulières à $\mathcal{S}_n$ peuvent se généraliser à un groupe de réflexion quelconque, en utilisant les propriétés particulières de ces groupes.

 gael.druez@ens-rennes.fr

2 Discriminant et polynômes symétriques

2.1 Discriminant, motivation et définitions

La notion de *résultant* de deux polynômes est assez classique en algèbre : le résultant de deux polynômes en une variable est un scalaire (dans l'anneau des coefficients des polynômes), qui est nul si et seulement si les deux polynômes ont au moins une racine commune. On parle alors de *discriminant* d'un polynôme pour parler du résultant de ce polynôme et de son polynôme dérivé.

On peut généraliser ces notions à un plus grand nombre de polynômes. Considérons un système de n équations polynomiales homogènes (c'est-à-dire que tous les monômes d'un polynôme sont de même degré). Alors ce système possède des solution non triviales si et seulement si les polynômes ont un résultant non nul, où le résultant est un polynôme en les coefficients des polynômes du système. On peut ensuite regarder un système formé des n dérivées partielles d'un polynôme en n variables, et le resultant de ses dérivées partielles sera appelé *discriminant*.

Cette notion est importante, par exemple lorsqu'on recherche les points critique d'un polynôme homogène. Cela arrive en physique lorsqu'on cherche des minima. On recherche alors des points d'annulation du polynôme et de toutes ses dérivées, et donc le discriminant est important pour avoir des informations sur l'existence de tels points critiques. (*cf.* [N P09])

Ainsi, si l'on considère un polynôme en $n \geqslant 2$ variables, homogène de degré $d \geqslant 2$: $F(x_1, \dots, x_n) = \sum_{|\alpha|=d} u_\alpha x^\alpha$; le discriminant de F est, à un multiple scalaire près, le résultant suivant : $\mathrm{Res}\left(\frac{\partial F}{\partial x_1}, \dots, \frac{\partial F}{\partial x_n}\right)$.

Si on regarde un système constitué de n polynômes en n variables $F^{\{1\}}, \dots, F^{\{n\}}$, alors on dit que le système est *équivariant* sous l'action canonique de $\mathcal{S}_n$ s'il vérifie :

$$\forall i \in [\![1, n]\!],\ \forall \sigma \in \mathcal{S}_n,\ \forall x \in \mathbb{C}^n,\ F^{\{i\}}(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = F^{\{\sigma(i)\}}(x_1, \dots, x_n) \tag{1}$$

D'un autre point de vue, les polynômes $F^{\{1\}}, \dots, F^{\{n\}}$ sont équivariants si la fonction

$$F : \begin{array}{ccc} \mathbb{C}^n & \longrightarrow & \mathbb{C}^n \\ (x_1, \dots, x_n) & \longmapsto & (F^{\{1\}}(x_1, \dots, x_n), \dots, F^{\{n\}}(x_1, \dots, x_n)) \end{array}$$

est symétrique, c'est-à-dire qu'appliquer une permutation $\sigma \in \mathcal{S}_n$ au départ ou à l'arrivée a le même effet :

$$F(\sigma(x)) = \sigma(F(x_1, \dots, x_n))$$

$$F \circ \sigma = \sigma \circ F$$

> *On considère ici l'action canonique de $\mathcal{S}_n$ sur $\mathbb{C}^n$ qui consiste à permuter les coordonnées : si $u = (u_1, \dots, u_n)$ est un élément de $\mathbb{C}^n$, alors pour toute permutation $\sigma \in \mathcal{S}_n$, on a $\sigma(u) := (u_{\sigma(1)}, \dots, u_{\sigma(n)})$.*

Le résultat principal de cette partie est la factorisation du résultant de polynômes symétriques en des résultants d'un nombre inférieur de polynômes (ce qui accélère grandement le calcul). Ce théorème sera énoncé en fin de partie, mais avant cela il faut présenter deux outils qui seront utiles dans la preuve et dans la suite.

2.2 Les différences divisées

Une majorité de ce qui suit, jusqu'à la fin de la partie, suit les travaux de Laurent Busé et Anna Karasoulou dans [Lau16].

On étudie un système $F^{\{1\}}, \dots, F^{\{n\}} \in \mathbb{K}[x_1, \dots, x_n]$ de polynômes homogènes, de degré d, vérifiant (1).

Alors ces polynômes vérifient également une autre propriété :

Proposition :

Un système $F^{\{1\}}, \dots, F^{\{n\}}$ de polynômes vérifiant (1) vérifie également

$$\forall i, j \in [\![1, n]\!],\ F^{\{i\}} - F^{\{j\}} \in \langle x_i - x_j \rangle \tag{2}$$

En particulier, si les variables x_i et x_j sont égales, alors les polynômes $F^{\{i\}}$ et $F^{\{j\}}$ sont égaux.

Preuve :

Soient $i < j$ fixés entre 1 et n. On note $\sigma \in \mathcal{S}_n$ la transposition $(i\ j)$.
D'après (1) appliquée avec notre i et notre σ :

$$\forall x \in \mathbb{C}^n,\ F^{\{i\}}(x_1, \dots, x_j, \dots, x_i, \dots, x_n) = F^{\{j\}}(x_1, \dots, x_i, \dots, x_j, \dots, x_n)$$

Donc pour tout $x \in \mathbb{C}^n$ vérifiant $x_i = x_j$, $F^{\{i\}}(x) = F^{\{j\}}(x)$.
Les zéros du polynôme $x_i - x_j$ sont donc inclus dans les zéros du polynôme $F^{\{i\}} - F^{\{j\}}$, ce qui nous donne l'inclusion suivante : $V(x_i - x_j) \subset V(F^{\{i\}} - F^{\{j\}})$. On a alors $I(V(F^{\{i\}} - F^{\{j\}})) \subset I(V(x_i - x_j))$.
Or $V(x_i - x_j)$ est un sous-espace affine avec $x_i - x_j$ un polynôme de degré 1, donc on a $I(V(x_i - x_j)) = \langle x_i - x_j \rangle$. De plus, on a évidemment $F^{\{i\}} - F^{\{j\}} \in I(V(F^{\{i\}} - F^{\{j\}}))$.
Finalement, on a bien $F^{\{i\}} - F^{\{j\}} \in \langle x_i - x_j \rangle$.

□

On note $V(x_{i_1}, \dots, x_{i_k}) := \prod_{1 \leqslant r < s \leqslant k} (x_{i_r} - x_{i_s}) = \det \begin{vmatrix} 1 & x_{i_1} & \dots & x_{i_1}^{k-1} \\ 1 & x_{i_2} & \dots & x_{i_2}^{k-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_{i_k} & \dots & x_{i_k}^{k-1} \end{vmatrix}$ le déterminant de Vandermonde associé à $x_{i_1}, \dots, x_{i_k}$.

Proposition - Existence des différences divisées :

Pour tout ensemble $\{i_1, \dots, i_k\} \subset [\![1, n]\!]$, il existe un unique polynôme homogène $F^{\{i_1,\dots,i_k\}} \in \mathbb{K}[x_1, \dots, x_n]$ de degré $d - k + 1$ vérifiant :

$$V(x_{i_1}, \dots, x_{i_k}) \cdot F^{\{i_1,\dots,i_k\}}(x_1, \dots, x_n) = \det \begin{vmatrix} 1 & x_{i_1} & \dots & x_{i_1}^{k-2} & F^{\{i_1\}}(x_1, \dots, x_n) \\ 1 & x_{i_2} & \dots & x_{i_2}^{k-2} & F^{\{i_2\}}(x_1, \dots, x_n) \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_{i_k} & \dots & x_{i_k}^{k-2} & F^{\{i_k\}}(x_1, \dots, x_n) \end{vmatrix}$$

gael.druez@ens-rennes.fr

Preuve :

Il suffit pour cela de montrer que $V(x_{i_1},\dots,x_{i_k})$ divise le déterminant de droite. Pour cela, on montre que $\forall\ 1 \leqslant r < s \leqslant k,\ x_{i_r} - x_{i_s}$ divise ce déterminant.
C'est relativement immédiat, car si on choisit $1 \leqslant r < s \leqslant k$, alors en soustrayant la ligne s à la ligne k dans le déterminant, on obtient le déterminant suivant :

$$\det\begin{vmatrix} 1 & x_{i_1} & \dots & x_{i_1}^{k-2} & F^{\{i_1\}}(x_1,\dots,x_n) \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & x_{i_r} - x_{i_s} & \dots & x_{i_r}^{k-2} - x_{i_s}^{k-2} & F^{\{i_r\}}(x_1,\dots,x_n) - F^{\{i_s\}}(x_1,\dots,x_n) \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_{i_k} & \dots & x_{i_k}^{k-2} & F^{\{i_k\}}(x_1,\dots,x_n) \end{vmatrix}$$

On sait alors que, dans la ligne du milieu, tous les termes sont divisibles par $x_{i_r} - x_{i_s}$ (d'après la propriété (2) pour la dernière colonne, et d'après la propriété connue disant que $a - b \mid a^n - b^n$ pour les autres).

$\square$

Définition - Différences divisées :

> Avec les notations précédentes, pour tout entier $0 \leqslant k \leqslant n$, on appelle **différences divisées d'ordre k-1** les polynômes $F^{\{i_1,\dots,i_k\}}$, où $\{i_1,\dots,i_k\} \subset [\![1,n]\!]$.

On remarque que pour $k-1 > d$, on a $F^{\{i_1,\dots,i_k\}} = 0$

Le cas simple où $k = 2$ montre rapidement que les premières différences divisées vérifient $(x_i - x_j)\cdot F^{\{i,j\}} = F^{\{i\}} - F^{\{j\}}$, ou encore $F^{\{i,j\}} = \dfrac{F^{\{i\}} - F^{\{j\}}}{x_i - x_j}$. Cette expression justifie l'appellation de différence divisée.

Une formule similaire s'obtient pour les différences divisées d'ordres supérieurs :

Proposition - Différences divisées d'ordre supérieur :

> Soit $\{i_1,\dots,i_k\} \subset [\![1,n]\!]$ contenant au moins 2 éléments. La différence divisée F^I, qui est d'ordre $k-1$, vérifie :
>
> $$\forall p < q \in [\![1,k]\!],\ (x_{i_q} - x_{i_p})F^{\{i_1,\dots,i_k\}} := F^{\{i_1,\dots,i_k\}\backslash\{i_p\}} - F^{\{i_1,\dots,i_k\}\backslash\{i_q\}}$$

Preuve :

Pour prouver cela, on remarque tout d'abord que pour $k = 2$ c'est déjà fait, et que comme ça ne dépend pas de l'ordre des indices, on peut se contenter de le prouver pour $p = 1$ et $q = 2$. On part alors de l'égalité qu'on a montré plus tôt :

$$V(x_{i_1}, x_{i_2}, \ldots, x_{i_k}) \cdot P^{\{i_1,\ldots,i_k\}}(x_1,\ldots,x_n) = \begin{vmatrix} 1 & x_{i_1} & \ldots & x_{i_1}^{k-2} & P^{\{i_1\}}(x_1,\ldots,x_n) \\ 1 & x_{i_2} & \ldots & x_{i_2}^{k-2} & P^{\{i_2\}}(x_1,\ldots,x_n) \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_{i_k} & \ldots & x_{i_k}^{k-2} & P^{\{i_k\}}(x_1,\ldots,x_n) \end{vmatrix}$$

et on élimine les variables par récurrence, en faisant des manipulations sur le déterminant à droite, que l'on note Δ. En effet, en soustrayant à chaque ligne la dernière, on obtient :

$$\Delta = \begin{vmatrix} 0 & x_{i_1} - x_{i_k} & x_{i_1}^2 - x_{i_k}^2 & \ldots & x_{i_1}^{k-2} - x_{i_k}^{k-2} & P^{\{i_1\}} - P^{\{i_k\}} \\ 0 & x_{i_2} - x_{i_k} & x_{i_2}^2 - x_{i_k}^2 & \ldots & x_{i_2}^{k-2} - x_{i_k}^{k-2} & P^{\{i_2\}} - P^{\{i_k\}} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & x_{i_{k-1}} - x_{i_k} & x_{i_{k-1}}^2 - x_{i_k}^2 & \ldots & x_{i_{k-1}}^{k-2} - x_{i_k}^{k-2} & P^{\{i_{k-1}\}} - P^{\{i_k\}} \\ 1 & x_{i_k} & x_{i_k}^2 & \ldots & x_{i_k}^{k-2} & P^{\{i_k\}} \end{vmatrix}$$

$$= \begin{vmatrix} 0 & x_{i_1} - x_{i_k} & (x_{i_1} - x_{i_k})(x_{i_1} + x_{i_k}) & \ldots & (x_{i_1} - x_{i_k})\sum_{r=0}^{k-3} x_{i_1}^r x_{i_k}^{k-3-r} & (x_{i_1} - x_{i_k})P^{\{i_1,i_k\}} \\ 0 & x_{i_2} - x_{i_k} & (x_{i_2} - x_{i_k})(x_{i_2} + x_{i_k}) & \ldots & (x_{i_2} - x_{i_k})\sum_{r=0}^{k-3} x_{i_2}^r x_{i_k}^{k-3-r} & (x_{i_2} - x_{i_k})P^{\{i_2,i_k\}} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & x_{i_{k-1}} - x_{i_k} & (x_{i_{k-1}} - x_{i_k})(x_{i_{k-1}} + x_{i_k}) & \ldots & (x_{i_{k-1}} - x_{i_k})\sum_{r=0}^{k-3} x_{i_{k-1}}^r x_{i_k}^{k-3-r} & (x_{i_{k-1}} - x_{i_k})P^{\{i_{k-1},i_k\}} \\ 1 & x_{i_k} & x_{i_k}^2 & \ldots & x_{i_k}^{k-2} & P^{\{i_k\}} \end{vmatrix}$$

$$= (x_{i_1} - x_{i_k})(x_{i_2} - x_{i_k})\ldots(x_{i_{k-1}} - x_{i_k}) \begin{vmatrix} 0 & 1 & x_{i_1} + x_{i_k} & \ldots & \sum_{r=0}^{k-3} x_{i_1}^r x_{i_k}^{k-3-r} & P^{\{i_1,i_k\}} \\ 0 & 1 & x_{i_2} + x_{i_k} & \ldots & \sum_{r=0}^{k-3} x_{i_2}^r x_{i_k}^{k-3-r} & P^{\{i_2,i_k\}} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 1 & x_{i_{k-1}} + x_{i_k} & \ldots & \sum_{r=0}^{k-3} x_{i_{k-1}}^r x_{i_k}^{k-3-r} & P^{\{i_{k-1},i_k\}} \\ 1 & x_{i_k} & x_{i_k}^2 & \ldots & x_{i_k}^{k-2} & P^{\{i_k\}} \end{vmatrix}$$

$$= (x_{i_k} - x_{i_1})(x_{i_k} - x_{i_2})\ldots(x_{i_k} - x_{i_{k-1}}) \begin{vmatrix} 1 & x_{i_1} + x_{i_k} & \ldots & \sum_{r=0}^{k-3} x_{i_1}^r x_{i_k}^{k-3-r} & P^{\{i_1,i_k\}} \\ 1 & x_{i_2} + x_{i_k} & \ldots & \sum_{r=0}^{k-3} x_{i_2}^r x_{i_k}^{k-3-r} & P^{\{i_2,i_k\}} \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_{i_{k-1}} + x_{i_k} & \ldots & \sum_{r=0}^{k-3} x_{i_{k-1}}^r x_{i_k}^{k-3-r} & P^{\{i_{k-1},i_k\}} \end{vmatrix}$$

(Le $(-1)^{k-1}$ dû au développement du déterminant a été absorbé par l'inversion des $k-1$ différences.)
Notons $\tilde{\Delta}$ ce dernier déterminant. En multipliant sa colonne $j-1$ (qui contient, sur la ligne 1 par exemple, $\sum_{r=0}^{j-2} x_{i_1}^r x_{i_k}^{j-2-r}$) par x_{i_k}, on obtient $\sum_{r=0}^{j-2} x_{i_1}^r x_{i_k}^{j-1-r}$, que l'on soustrait au terme de la colonne j : $\sum_{r=0}^{j-1} x_{i_1}^r x_{i_k}^{j-1-r} - \sum_{r=0}^{j-2} x_{i_1}^r x_{i_k}^{j-1-r} = x_{i_1}^{j-1}$. On obtient finalement :

$$\Delta = (x_{i_k} - x_{i_1})(x_{i_k} - x_{i_2})\dots(x_{i_k} - x_{i_{k-1}}) \begin{vmatrix} 1 & x_{i_1} & \dots & x_{i_1}^{k-3} & P^{\{i_1,i_k\}} \\ 1 & x_{i_2} & \dots & x_{i_2}^{k-3} & P^{\{i_2,i_k\}} \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_{i_{k-1}} & \dots & x_{i_{k-1}}^{k-3} & P^{\{i_{k-1},i_k\}} \end{vmatrix}$$

et donc finalement :

$$V(x_{i_1}, x_{i_2}, \dots, x_{i_k}) \cdot P^{\{i_1,\dots,i_k\}} = \prod_{j=1}^{k-1} (x_{i_k} - x_{i_j}) \begin{vmatrix} 1 & x_{i_1} & \dots & x_{i_1}^{k-3} & P^{\{i_1,i_k\}} \\ 1 & x_{i_2} & \dots & x_{i_2}^{k-3} & P^{\{i_2,i_k\}} \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_{i_{k-1}} & \dots & x_{i_{k-1}}^{k-3} & P^{\{i_{k-1},i_k\}} \end{vmatrix}$$

On remarque qu'on a réduit notre déterminant d'une taille, mais qu'en contrepartie on a augmenté de 1 le rang de nos différences divisées.
On peut alors conclure cette hérédité, $\mathbb{K}[x_1, \dots, x_n]$ étant intègre et $\prod_{j=1}^{k-1} (x_{i_k} - x_{i_j})$ étant non nul :

$$V(x_{i_1}, \dots, x_{i_{k-1}}) \cdot P^{\{i_1,\dots,i_k\}} = \begin{vmatrix} 1 & x_{i_1} & \dots & x_{i_1}^{k-3} & P^{\{i_1,i_k\}} \\ 1 & x_{i_2} & \dots & x_{i_2}^{k-3} & P^{\{i_2,i_k\}} \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_{i_{k-1}} & \dots & x_{i_{k-1}}^{k-3} & P^{\{i_{k-1},i_k\}} \end{vmatrix} \qquad \text{(déterminant } k-1 \times k-1\text{)}$$

Si on l'applique sur une étape supplémentaire, on obtient :

$$V(x_{i_1}, \dots, x_{i_{k-2}}) \cdot P^{\{i_1,\dots,i_k\}} = \begin{vmatrix} 1 & x_{i_1} & \dots & x_{i_1}^{k-4} & P^{\{i_1,i_{k-1},i_k\}} \\ 1 & x_{i_2} & \dots & x_{i_2}^{k-4} & P^{\{i_2,i_{k-1},i_k\}} \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_{i_{k-2}} & \dots & x_{i_{k-2}}^{k-4} & P^{\{i_{k-2},i_{k-1},i_k\}} \end{vmatrix} \qquad \text{(déterminant } k-2 \times k-2\text{)}$$

Et ainsi de suite jusqu'à obtenir :

$$V(x_{i_1}, x_{i_2}) \cdot P^{\{i_1,\dots,i_k\}} = \begin{vmatrix} 1 & P^{\{i_1,i_3,\dots,i_{k-1},i_k\}} \\ 1 & P^{\{i_2,i_3,\dots,i_{k-1},i_k\}} \end{vmatrix}$$

Soit finalement

$$(x_{i_1} - x_{i_2}) \cdot P^{\{i_1,\dots,i_k\}} = P^{\{i_2,i_3,\dots,i_{k-1},i_k\}} - P^{\{i_1,i_3,\dots,i_{k-1},i_k\}}$$

Le résultat reste valide pour des indices i_p, i_q quelconques car l'ordre des éléments de I n'a pas d'importance.

□

On peut en conclure une propriété plus générale :

Proposition :

Si on fixe I et J deux sous-ensembles stricts de $[\![1,n]\!]$ de cardinal commun r, alors le polynôme $P^I - P^J$ est dans l'idéal engendré par les $(r+1)^{\text{èmes}}$ différences divisées, c'est-à-dire : $P^I - P^J \in \langle \{P^K \; ; \; K \subset [\![1,n]\!], \; |K| = r+1\} \rangle$.

Preuve :

Pour montrer cela, on élimine progressivement les éléments différents entre I et J.
Si $I = J$, $P^I - P^J = 0$ et c'est gagné.
Si I et J ont un seul élément qui n'est pas commun, alors par ce qui précède, $P^I - P^J \in \langle P^{I\cup J} \rangle$.
Si I et J ont au moins 2 éléments qui ne sont pas en commun, alors en notant $i \in I \backslash J$ et $j \in J \backslash I$, on intercale un polynôme judicieux : $P^I - P^J = \left(P^I - P^{(I\backslash\{i\})\cup\{j\}}\right) + \left(P^{(I\backslash\{i\})\cup\{j\}} - P^J\right)$
On a alors, dans la première différence, seulement un élément qui n'est pas en commun, et dans la deuxième on a strictement réduit le nombre d'éléments qui ne sont pas en commun.
Par récurrence, on aboutit finalement au résultat.

□

2.3 Partitions et réduction du nombre de variables

Définition - Partition :

Soit $p \in \mathbb{N}$ un entier.
On appelle **partition** de l'entier p tout suite finie décroissante $\lambda_1 \geqslant \cdots \geqslant \lambda_k \geqslant 0$ telle que $\sum_{i=1}^k \lambda_i = p$.
On note alors $\lambda \vdash p$.

L'entier k sera souvent noté $\ell(\lambda)$ pour rappeler qu'il dépend de la partition λ choisie.

Étant donnée une partition $\lambda = (\lambda_1, \dots, \lambda_k) \vdash n$, on définit :

$$\rho_\lambda : \begin{array}{ccc} \mathbb{C}[x_1,\dots,x_n] & \longrightarrow & \mathbb{C}[y_1,\dots,y_k] \\ F(x_1,\dots,x_n) & \longmapsto & F(\underbrace{y_1,\dots,y_1}_{\lambda_1}, \underbrace{y_2,\dots,y_2}_{\lambda_2}, \dots, \underbrace{y_k,\dots,y_k}_{\lambda_k}) \end{array}$$

L'application ainsi définie est un morphisme d'algèbres de polynômes. Concrètement, ce morphisme "réduit le nombre de variables" des polynômes, en en fixant certaines égales selon la partition considérée.

Cette réduction du nombre de variables va être importante dans la suite, mais on va vouloir préserver certaines propriétés.

Remarquons d'abord que d'après la Proposition **??** (la formule qui définit les différences divisées) et d'après la Propriété 1, on a :

$$\forall\ I = \{i_1, \ldots, i_k\} \subset [\![1, n]\!],\ \forall \sigma \in \mathcal{S}_n,\ \ \sigma(F^{\{i_1,\ldots,i_k\}}) = F^{\{\sigma(i_1),\ldots,\sigma(i_k)\}}$$

Maintenant, si $\rho_\lambda(x_i) = \rho_\lambda(x_j)$, alors $\rho_\lambda(F^{\{i\}}) = \rho_\lambda(F^{\{j\}})$, par les propriété de morphisme d'algèbres. En effet, on a vu que $(x_i - x_j) \cdot F^{\{i,j\}} = F^{\{i\}} - F^{\{j\}}$, donc $\rho_\lambda\left((x_i - x_j) \cdot F^{\{i,j\}}\right) = \rho_\lambda(x_i - x_j) \cdot \rho_\lambda(F^{\{i,j\}}) = \rho_\lambda\left(F^{\{i\}} - F^{\{j\}}\right)$. Donc si $\rho_\lambda(x_i) = \rho_\lambda(x_j)$, on a $\rho_\lambda(x_i - x_j) = 0$ et donc $\rho_\lambda\left(F^{\{i\}} - F\{j\}\right) = 0$, ce qui donne bien $\rho_\lambda(F^{\{i\}}) = \rho_\lambda(F^{\{j\}})$.

On peut alors définir sans ambiguité, avec toujours notre partition quelconque λ fixée et pour tout $i \in [\![1, \ell(\lambda)]\!]$, le polynôme en $\ell(\lambda)$ variables :

$$F_\lambda^{\{i\}}(y_1, \ldots, y_{\ell(\lambda)}) \coloneqq \rho_\lambda\left(F^{\{j\}}(x_1, \ldots, x_n)\right) \in \mathbb{K}[y_1, \ldots, y_{\ell(\lambda)}]$$

où $j \in [\![1, n]\!]$ vérifie $\rho_\lambda(x_j) = y_i$. La vérification ci-dessus permet de vérifier que cette définition ne dépend pas du j choisi.

> *Que fait concrètement cette manipulation ? Voyons cela avec un exemple et un tableau. On travaille avec* $n = 4$*, on a donc* 4 *polynômes en autant de variables. On se fixe une partition de* 4*, par exemple* $\lambda = (3, 1)$*, de longueur* $\ell(\lambda) = 2$*.*
> *L'application* ρ_λ *permet de réduire le nombre de polynômes et leur nombre de variable (de* 4 *à* $\ell(\lambda) = 2$*) en les regroupant selon la partition choisie :*

1	$F^{\{1\}}(x_1, x_2, x_3, x_4)$			
2	$F^{\{2\}}(x_1, x_2, x_3, x_4)$	$\to \rho_\lambda \to$	$F_\lambda^{\{1\}}(y_1, y_2) \quad (\lambda_1 = 3)$	1
3	$F^{\{3\}}(x_1, x_2, x_3, x_4)$			
4	$F^{\{4\}}(x_1, x_2, x_3, x_4)$		$F_\lambda^{\{2\}}(y_1, y_2) \quad (\lambda_2 = 1)$	2

Remarquons que les polynômes obtenus vérifient toujours la propriété de symétrie 1, ils admettent donc des différences divisées. On les note $F_\lambda^{\{i_1,\ldots,i_r\}}(y_1, \ldots, y_{\ell(\lambda)})$, avec $\{i_1, \ldots, i_r\} \subset [\![1, \ell(\lambda)]\!]$. La Proposition **??** s'applique alors, et on montre que pour tout $I = \{i_1, \ldots, i_k\} \subset [\![1, n]\!]$, on peut définir $J = \{j_1, \ldots, j_k\} \subset [\![1, \ell(\lambda)]\!]$ tel que $\forall r \in [\![1, k]\!]$, $\rho_\lambda(x_{i_r}) = y_{j_r}$. Alors, sous réserve que $|I| = |J|$, c'est-à-dire que chaque x_{i_r} est envoyé sur un y_{j_r} distinct, on a $\rho_\lambda\left(F^I(x_1, \ldots, x_n)\right) = F_\lambda^J(y_1, \ldots, y_{\ell(\lambda)})$.

gael.druez@ens-rennes.fr

2.4 Énoncé du théorème de factorisation

Théorème - Factorisation du déterminant:

> Soient $F^{\{1\}}, \dots, F^{\{n\}} \in \mathbb{K}[x_1, \dots, x_n]$ des polynômes homgènes de degré d, vérifiant la propriété d'équivariance 1. On a alors :
>
> - Si $d \geqslant n$, alors
>
> $$Res\left(F^{\{1\}}, \dots, F^{\{n\}}\right) = \prod_{\lambda \vdash n} Res\left(F_\lambda^{\{1\}}, F_\lambda^{\{1,2\}}, \dots, F_\lambda^{\{1,2,\dots,k\}}\right)^{m_\lambda}$$
>
> - Si $d < n$, alors
>
> $$Res\left(F^{\{1\}}, \dots, F^{\{n\}}\right) = \left(F^{\{1,2,\dots,d\}}\right)^{m_0} \times \prod_{\substack{\lambda \vdash n \\ \ell(\lambda) \leqslant d}} Res\left(F_\lambda^{\{1\}}, F_\lambda^{\{1,2\}}, \dots, F_\lambda^{\{1,2,\dots,\ell(\lambda)\}}\right)^{m_\lambda}$$

Ce théorème est particulièrement intéressant car il décompose le calcul d'un résultant en plusieurs calculs de résultants plus petits. Sachant que la complexité de calcul d'un résultant croit très rapidement avec n, c'est un progrès considérable.

Remarquons d'ailleurs que les nouveaux résultants à calculer sont, non plus en n mais en $\ell(\lambda)$. Ceci est d'autant plus intéressant car il y a "plus" de partitions avec une longueur faible que de partitions avec une grande longueur.

On peut enfin évoquer le fait qu'il n'est pas nécéssaire de calculer un par un tous les résultants du produit : pour une longueur de partition fixée, on peut calculer les terme général associé à une partition quelconque de cette longueur, ce qui nous laisse un faible nombre de résultants à calculer (un pour chaque longueur possible de partition, donc au plus $\min(n, d)$).

2.5 Éléments de preuve et commentaires

L'idée principale de la preuve va être d'utiliser les propriétés du résultant et celles des différences divisées pour remplacer chaque $F^{\{i\}}$ par une expressin faisant intervenir une différence divisée.

Détaillons la première étape :

$$\begin{aligned} Res\left(F^{\{1\}}, F^{\{2\}}, \dots, F^{\{n\}}\right) &= \pm Res\left(F^{\{1\}}, F^{\{1\}} - F^{\{2\}}, \dots, F^{\{1\}} - F^{\{n\}}\right) \\ &= \pm Res\left(F^{\{1\}}, (x_1 - x_2) \cdot F^{\{1,2\}}, \dots, (x_1 - x_n) \cdot F^{\{1,n\}}\right) \end{aligned}$$

On utilise ensuite la propriété de multiplicativité du résultant, qui décompose cette dernière ligne en un produit de 2^{n-1} termes : pour chaque $(x_1 - x_i) \cdot F^{\{1,i\}}$, on a le choix entre prendre $(x_1 - x_2)$ ou $F^{\{1,2\}}$. Alors, si on a fait le premier choix pour les indices $I_1 := \{i_1, \dots, i_{n-k}\} \subset [\![2, n]\!]$ et le second choix pour les autres indices $J_1 := \{j_1, \dots, j_{k-1}\} = [\![2, n]\!] \backslash I_1$, on obtient le facteur suivant :

$$\pm Res\left(F^{\{1\}}, F^{\{1,j_1\}}, \dots, F^{\{1,j_{k-1}\}}, x_1 - x_{i_1}, \dots, x_1 - x_{i_{n-k}}\right)$$

On applique ensuite $\rho_1 : \left| \begin{array}{ccc} \mathbb{K}[x_1, \dots, x_n] & \longrightarrow & \mathbb{K}[y_1, \dots, y_k] \\ x_i,\ i \in I_1 & \longmapsto & y_1 \\ x_{j_r},\ r \in [\![1, k-1]\!] & \longmapsto & y_{r+1} \end{array} \right.$, qui est un morphisme d'algèbre qui préserve le degré, et donc qui ne change pas le résultant.

Concrètement, cela revient à mettre toutes les variables $x_1, x_{i_1}, \dots, x_{i_{n-k}}$ dans la "même boîte" y_1, et de renommer les autres de y_2 à y_k. Intuitivement, cela fonctionne car dans un résultant, ce sont les zéros des polynômes qui nous intéressent, et les zéros communs des $x_1 - x_i$ sont les points où les coordonnées $x_1, x_{i_1}, \dots, x_{i_{n-k}}$ sont toutes égales.

On obtient alors le facteur suivant, en notant $F_1^{\{1,r\}} := \rho_1\left(F^{\{1,j_{r-1}\}}\right)$:

$$\pm Res\left(F_1^{\{1\}}, F_1^{\{1,2\}}, \dots, F_1^{\{1,k\}}\right)$$

On réitère ces étapes en séparant les différences diviées d'ordre 1 en un produit faisant intervenir des différences divisées d'ordre 2, et en séparant les facteurs. Cet algorithme s'arrête soit quand il n'y a plus de différences divisées à augmenter d'un ordre (si on a "supprimé" un grand nombre de variables en peu d'étapes), soit quand on atteint des différences divisées d'ordre trop grand et que donc elles s'annulent.

Pour obtenir la forme voulue, il reste un petit travail à mener sur les sous-ensemble de $[\![1,n]\!]$ qui peuvent aboutir à un facteur dans le produit final, notamment en les réunissant en classes d'une relation d'équivalence bien choisie (classes d'équivalence qui s'avèrent être en correspondance avec les partitions de n), et en déterminant le cardinal de ces classes (l'exposant m_λ apparaissant dans la formule).

 gael.druez@ens-rennes.fr

3 Groupes de réflexions

3.1 Représentation de groupes et définition

Une grande majorité des informations sur les groupes de réflexions est inspirée de [Hum94]. Certaines idées viennent de [Mic23]. Quelques éclairages différents sur certaines preuves ont également été apportés par [Fla78].

Définition - Représentation de groupe :

> Une **représentation** d'un groupe G est un morphisme de groupes $\rho : G \longrightarrow GL(V)$ de G dans l'espace des automorphismes de V. Si V est de dimension finie (ce qui sera le cas pour nous), il est isomorphe à $\mathbb{K}^n$ et donc $GL(V)$ s'apparente à un groupe de matrices inversibles.

On se fixe $(V, \langle .,. \rangle)$ un espace euclidien réel.

Définition - Réflexion :

> Une **réflection** de V est une application linéaire qui envoie un certain vecteur α sur son opposé et qui fixe l'hyperplan orthogonal à α. On notera s_α une réflexion qui envoie α sur $-\alpha$ (attention, le α n'est pas unique).
> On a la formule suivante :
>
> $$\forall \lambda \in V,\ s_\alpha(\lambda) = \lambda - \frac{2\langle \lambda, \alpha \rangle}{\langle \alpha, \alpha \rangle}\alpha$$

Définition - Groupe de réflexion :

> Un **groupe de réflexion** est un sous-groupe fini de $\mathcal{O}(V)$ engendré par un nombre fini de réflexions.
> Par extension, on appellera groupe de réflexion tout groupe dont la représentation est un sous-groupe fini de $\mathcal{O}(V)$ engendré par un nombre fini de réflexions.

"Être un groupe de réflexion" est donc, dans le cas d'un groupe quelconque, une propriété de la représentation de ce groupe (ou encore de son action sur l'espace euclidien) et non une propriété intrinsèque.

> *On va étudier deux exemples en particulier :*
>
> 1. $\mathcal{S}_n$, *qui agit sur* $V := \mathbb{R}^n$ *en permutant les vecteurs de la base canonique (c'est-à-dire les coordonnées dans cette base) :* $\forall x \in V,\ \forall \sigma \in \mathcal{S}_n,\ \sigma(x) = (x_{\sigma(1)}, \dots, x_{\sigma(n)})$.
>   *C'est un groupe de réflexion car les transpositions sont des réflexions (pour* $i \neq j$, $(i\ j)$ *envoie* $e_i - e_j$ *sur son opposé et laisse fixe l'hyperplan orthogonal) et* $\mathcal{S}_n$ *est engendré par les transpositions.*
> 2. $\mathcal{D}_m$, *qui agit sur* $V = \mathbb{R}^2$ *par les transformations laissant fixe un polygone régulier à* m *côtés centré sur l'origine.*
>   *Ce groupe est habituellement engendré par une rotation d'angle* $\frac{2\pi}{m}$ *et une réflection par rapport à une diagonale, mais dans notre cas on peut remarquer que la rotation peut s'exprimer comme une succession de deux réflexions, donc* $\mathcal{D}_m$ *est bien engendré par des réflexions.*

gael.druez@ens-rennes.fr

3.2 Racines

Certaines réflexions jouent un rôle particulier, ainsi que les vecteurs qu'elles envoient sur leur opposé. On va donner un nom à ces réflexions et aux vecteurs associés.

Définition - Système de racines :

On appelle **système de racines** tout ensemble $\Phi \subset V$, ensemble fini de vecteurs non nuls de V, vérifiant :

$$\textbf{(R1)}\ \forall \alpha \in \Phi,\ \Phi \cap \mathbb{R}\alpha = \{\alpha,\ -\alpha\} \qquad \text{et} \qquad \textbf{(R2)}\ \forall \alpha \in \Phi,\ s_\alpha(\Phi) = \Phi$$

Si W est un groupe de rélfexion engendré par les $\alpha \in \Phi$, alors ces α sont appelés les **racines** de W.

(R1) signifie que seuls α et $-\alpha$ appartiennent à Φ parmi les vecteurs sur la droite engendrée par α. **(R2)** signifie que l'image de tout élément de Φ par la réflexion associée à un autre élément de Φ reste dans Φ : Φ est stable par les réflexions associées à ses éléments.

La construction qu'on a fait semble partir des racines pour aller vers le groupe qu'elles engendrent, mais l'inverse est vrai aussi : si W est un groupe de réflexion engendré par les réflexions s_α, alors l'union des $\{\alpha, -\alpha\}$ est un système de racines associé à W.

Il n'y a pas de contraintes sur les racines en dehors de **(R1)** et **(R2)**. Les racines peuvent être de norme 1 ou non, elles peuvent couvrir toutes les réflexions de W ou non.

Définition - Système de racines positif :

On fixe un ordre total sur V. Un sous-sensemble Π d'un système de racines Φ est dit **positif** pour cet ordre s'il contient exactement les $\alpha \in \Phi,\ \alpha > 0$.

On a alors évidemment $\Phi = \Pi \cup -\Pi$, car $0 \notin \Phi$. Un ordre total sur V, et donc un tel système positif, existe bien (par exemple, l'ordre lexicographique dans une base choisie). Il n'y a pas unicité de l'ordre, mais une fois l'ordre fixé le système positif est défini de manière unique comme l'ensemble des racines positives.

Définition - Système de racines simple :

Un sous-sensemble Δ d'un système de racines Φ est dit **simple** si Δ est une base de $\mathrm{Vect}(\Phi)$, et si de plus chaque $\alpha \in \Phi$ se décompose comme une combinaison linéaire d'éléments de Δ avec des coefficients tous de même signes.

Théorème - Existences et unicités de systèmes simples et positifs :

1. Pour tout système simple Δ, il existe un unique système positif contenant Δ.
2. Tout système positif contient un unique système simple ; en particulier, les système simples existent.

gael.druez@ens-rennes.fr

Preuve :

La preuve est assez fastidieuse et ne semble pas faire apparaître d'outil utile dans la suite, on la passe donc sous silence.
Une propriété qui peut être intéressante à noter et qui intervient dans la preuve est la suivante :

$$\forall \alpha \neq \beta \in \Delta,\ \langle \alpha, \beta \rangle \leqslant 0$$

Cette propriété peut par exemple être vérifiée sur la Figure 1 ci-dessous.

□

Explicitons les ensembles Φ, Π et Δ pour nos deux exemples.

1. *Pour $\mathcal{S}_n$, l'ensemble $\Phi := \{e_i - e_j \mid i \neq j\}$ convient (on vérifie aisément **(R1)** et **(R2)**).*
   Si on choisit l'ordre lexicographique par rapport à la base canonique, on a alors $\Pi = \{e_i - e_j \mid i < j\}$.
   Enfin, $\Delta := \{e_i - e_{i+1}\ ;\ i \in [\![1, n-1]\!]$ convient . Pour montrer cela, on remarque d'abord que Vect(Φ) est l'hyperplan noyau de $(x_1, \dots, x_n) \mapsto x_1 + \dots + x_n$, puis que la famille Δ est libre et possède $n-1$ éléments, donc c'en est une base. Ensuite, pour $i < j$, $e_i - e_j = \sum_{k=i}^{j-1} e_k - e_{k+1}$, et pour $i > j$, $e_i - e_j = \sum_{k=j}^{i-1} -(e_k - e_{k+1})$.
2. *Pour $\mathcal{D}_m$, en assimilant $\mathbb{R}^2$ avec $\mathbb{C}$, $\Phi := \{e^{\frac{ik\pi}{m}}\ ;\ k \in [\![0, m-1]\!]\}$ convient.*
   Si on prend l'ordre lexicographique par rapport à la base canonique (on compare d'abord les abscisses, puis les ordonnées), les complexes strictement positifs sont ceux dont l'a bscisse est strictement positive, ainsi que ceux donc l'abscisse est nulle et l'ordonnée strictement positive. D'où $\Pi = \{e^{\frac{ik\pi}{m}}\ ;\ k \in]\!] - \lfloor \frac{m+1}{2} \rfloor, \lfloor \frac{m}{2} \rfloor]\!]\}$
   Enfin, $\Delta = \left\{e^{\frac{ik\pi}{3}}\ ;\ k \in \{-\lfloor \frac{m-1}{2} \rfloor, \lfloor \frac{m}{2} \rfloor\}\right\}$ rassemble les deux racines positives les plus "éloignées" sur le cercle. (cf. Figure 1)

Proposition - Action des réflexions simples sur le système positif :

Soit Δ un système simple contenu dans un système positif Π.
Si $\alpha \in \Delta$, alors $s_\alpha(\Pi \backslash \{\alpha\}) = \Pi \backslash \{\alpha\}$.

Preuve :

Soit $\alpha \in \Delta$ fixée. Soit $\beta \in \Pi$, $\beta \neq \alpha$. Par définition d'un système simple, on peut écrire $\beta = \sum_{\gamma \in \Delta} c_\gamma \gamma$ avec tous les $c_\gamma \geqslant 0$.
Maintenant, les seuls multiples de α dans Φ sont $\{\pm\alpha\}$, donc uniquement α dans Π. Donc, comme β n'est pas un multiple de α, il existe $\gamma \neq \alpha$ tel que $c_\gamma > 0$.
On regarde maintenant $s_\alpha(\beta) = \beta - c\alpha \in \Phi$. Par propriété des systèmes simples, les coefficients de cette combinaison linéaire sont tous de même signe, et notre c_γ strictement positif apparaît dedans. On en conclut que $s_\alpha(\beta) \in \Pi$. Or $s_\alpha(\beta)$ ne peut pas être α car sinon $\beta = -\alpha < 0$.
Finalement, s_α envoie toute racine positive distincte de α sur une racine positive distincte de α. s_α envoie donc $\Pi \backslash \{\alpha\}$ dans lui-même injectivement (si $s_\alpha(\beta) = s_\alpha(\gamma)$, on applique s_α pour obtenir $\beta = \gamma$), donc bijectivement. □

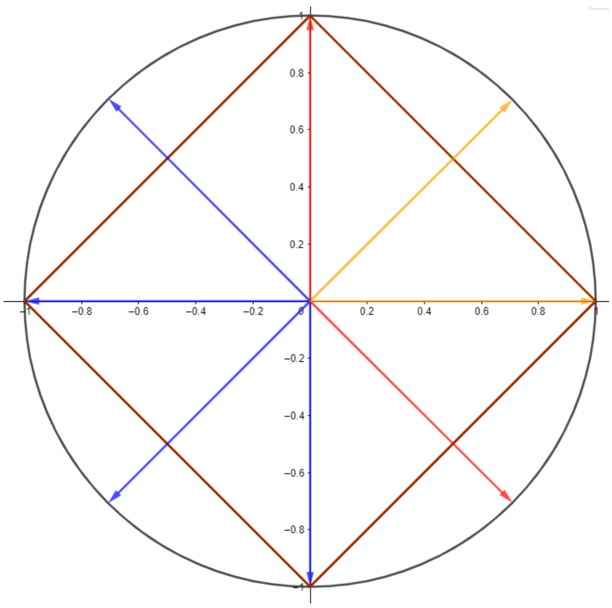

FIGURE 1 – Les racines de $\mathcal{D}_4$, avec en jaune/orange les racines positives (en orange les racines simples) et en bleu les racines négatives

Théorème :

> Deux système positifs (resp. simples) de Φ sont cojugués sous W.

Preuve :

Par récurrence, si on a deux systèmes positifs Π et Π', on applique successivement des s_α bien choisis (α appartenant à Π et à $-\Pi'$) à Π pour obtenir Π' (en utilisant la propriété précédente).

□

On va avoir besoin d'une caractéristique des éléments de W qu'on introduit ici :

Définition - la fonction ℓ :

> Soit $w \in W$. On note $\ell(w)$ le plus petit entier r tel qu'il existe une décomposition de la forme $w = s_{\alpha_1} \dots s_{\alpha_r}$, $\alpha_i \in \Delta$.

Proposition :

> Une réflexion envoie une unique racine positive sur une racine négative.

Preuve :

On a vu que s_α permute les racines positives distinctes de α, donc la seule racine positive potentiellement envoyée sur une racine négative est α, et comme elle est envoyée sur $-\alpha < 0$, il y en a bien une.

□

Conséquance : composer $w \in W$ par une réflexion ne peut faire varier que de ± 1 la valeur de $\ell(w)$.

gael.druez@ens-rennes.fr

3.3 Propriétés avancées

On va maintenant balayer des propriétés de certains objets en lien avec les groupes de réflexions, qui auront potentiellement des implications dans la généralisation qu'on va faire ensuite.

Précisons que cette étude a été faite *avant* de commencer la généralisation qui sera décrite en partie suivante, l'objectif étant d'avoir des outils pour apréhender les groupes de réflexions. Tous ces outils ne serviront peut-être pas.

Sous-groupes paraboliques

Cette notion va permettre de mieux comprendre les sous-espaces de V relativement aux racines simples.

On note, pour Δ fixé, $S := \{s_\alpha \ ; \ \alpha \in \Delta\}$ l'ensemble des "réflexions simples".
Ensuite, pour tout sous-ensemble $I \subset S$, on note $W_I = \langle s_\alpha \ ; \ s_\alpha \in I\rangle$ le sous-groupe de W engendré par les réflexions de I. On note également $\Delta_I := \{\alpha \in \Delta \mid s_\alpha \in I\} \subset \Delta$ l'ensemble des racines simples qui correspondent. (On a alors par exemple $W_\varnothing = \{1\}$ et $W_S = W$.)

Proposition :

Soit Δ fixé et soit S l'ensemble des rélexions correspondant.
Soit $I \subset S$, on définit $\Phi_I := \Phi \cap \mathrm{Vect}\Delta_I$, où $V_I := \mathrm{Vect}\Delta_I$ est un sous-espace vectoriel de l'espace ambiant $V \simeq \mathbb{K}^n$.

1. Φ_I est un système de racines dans V (resp. V_I) ayant pour système simple associé Δ_I et pour groupe de réflexions associé W_I (resp. W_I restreint à V_I)
2. En regardant W_I comme un groupe de réflexion, de fonction taille associée ℓ_I au système simple Δ_I, on a $\ell = \ell_I$ sur W_I.
3. On définit $W^I := \{w \in W \mid \forall s \in I, \ \ell(ws) > \ell(w)\}$. Alors, pour $w \in W$ fixé, il existe un unique $u \in W^I$ et un unique $v \in W_I$ tels que $w = uv$. Leur taille vérifie $\ell(w) = \ell(u) + \ell(v)$. De plus, u est l'unique élément de taille minimale dans le coset wW_I.

Preuve :

On prouve uniquement 3.
Soit $w \in W$ fixé. On choisit un élément $u \in wW_I$ de taille minimale, et on note v l'élément de W_I vérifiant $w = uv$. On remarque que $\forall s \in I$, $us \in wW_I$ car $us = wv^{-1}s$ avec $v, s \in W_I$ et W_I est un sous-groupe. Alors $u \in W^I$ car $\forall s \in I$, $\ell(us) > \ell(u)$ (car u est de taille minimale dans wW_I, et $\ell(us) \neq \ell(u)$ car s est une réflexion donc $\ell(us) = \ell(u) \pm 1$).
On écrit $u = s_1 \dots s_q$ ($s_i \in S$) et $v = s'_1 \dots s'_r$ ($s'_i \in I$ d'après 2.) sous leur forme réduite. Alors $\ell(w) \leqslant \ell(u) + \ell(v) = q + r$. D'après une condition vue précédemment dans l'ouvrage, on pourrait alors omettre deux facteurs s_i ou s'_i sans modifier w. Or omettre un facteur s_i de u fournirait un élément de wW_I de taille strictement inférieure à celle de u, ce qui contredirait le minimalité de u. Donc les deux facteurs s'_i, s'_j sont dans l'expression de v, absurde car on a pris un expression réduite. On a donc bien $\ell(w) = \ell(u) + \ell(v)$.
$u = wv^{-1}$ avec $v \in W_I$ donc on a bien $u \in wW_I$. Supposons maintenant qu'il existe $u' \in wW_I \cap W^I$ tel que $\ell(u') \leqslant \ell(u)$, avec $u' \neq u$. On écrit alors $u' = uv$ avec $\ell(v) = r > 0$, sous forme réduite $v = s_1 \dots s_r$. Mais alors $\ell(u's_r) < \ell(u')$, ce qui contredit $u' \in W^I$.

□

gael.druez@ens-rennes.fr

En Résumé :

- W_I est le groupe de réflexion engendré par les réflexions de $I \subset S$.
- W^I est l'ensemble des réflexions "qui ne peuvent pas être raccourcies par des rélfexions de I", c'est-à-dire que tout réflexion $w \in W$ se factorise de manière unique dans $W^I \oplus W_I$.
- wW_I est l'ensemble des éléments de la forme $ws_1 \dots s_q$, avec $s_i \in I$. Il possède un unique élément de taille minimale, et cet élément appartient à W^I.

Polynômes de Poincaré

L'utilité de cette notion n'est pas certaine, mais comme on va parler de polynômes il est préférable de l'inclure.

On veut quantifier à quel point W "grossit" par rapport à l'ensemble générateur S. Pour cela, on définit la suite $a_n := \mathrm{Card}\{w \in W \mid \ell(w) = n\}$. Comme les valeurs de la fonction ℓ sont bornées par le nombre de racines positives, cela définit un polynôme :

Définition - Polynôme de Poincaré :

On appelle **polynôme de Poincaré** de W le polynôme suivant :

$$W(t) := \sum_{n \geqslant 0} a_n t^n = \sum_{w \in W} t^{\ell(w)}$$

On peut définir ce polynôme pour n'importe quel sous-ensemble X de W en faisant la somme sur les $w \in X$.

Proposition :

Soit $I \subset S$, alors :

1. $W_I(t)$ coïncide avec le polynôme de Poincaré du groupe de réflexion W_I
2. $W(t) = W_I(t) W^I(t)$

Preuve :

1. Immédiat en considérant le fait que ℓ coïncide avec ℓ_I sur W_I
2. D'après la proposition précédente, toute réflexion $w \in W$ se décompose de manière unique comme produit uv avec $u \in W^I$ et $v \in W_I$. Ainsi,

$$\begin{aligned} W_I(t) W^I(t) &= \left(\sum_{v \in W_I} t^{\ell(v)} \right) \times \left(\sum_{u \in W^I} t^{\ell(u)} \right) \\ &= \sum_{(u,v) \in W^I \times W_I} t^{\ell(v)} t^{\ell(u)} \\ &= \sum_{(u,v) \in W^I \times W_I} t^{\ell(v) + \ell(u)} \\ &= \sum_{w \in W} t^{\ell(w)} = W(t) \qquad \text{en utilisant l'unicité de la décomposition} \end{aligned}$$

□

Dans la suite, on note $(-1)^I$ au lieu de $(-1)^{|I|}$ pour simplifier. Rappelons que W possède un unique élément w_0 de taille maximale $\ell(w_0) = N := |\Pi|$.

Proposition :

$$\sum_{I\subset S}(-1)^I \frac{W(t)}{W_I(t)} = \sum_{I\subset S}(-1)^I W^I(t) = t^N$$

Preuve :

La première égalité est immédiate avec la proposition précédente.
Pour la seconde, soit $w \in W$ fixé, regardons combien de fois il apparaît dans la somme $\sum_{I\subset S}(-1)^I W^I(t) = \sum_{I\subset S}\sum_{u\in W^I}(-1)^I t^{\ell(u)}$. Notons $K := \{s \in S \mid \ell(ws) > \ell(w)\}$. Alors, $\forall s \in S, [\ \ell(ws) > \ell(w) \Leftrightarrow s \in K]$, donc $[\forall s \in I, \ell(ws) > \ell(w)] \Leftrightarrow [\forall s \in I,\ s \in K] \Leftrightarrow I \subset K$, et donc finalement $w \in W^I \Leftrightarrow I \subset K$.
Le coefficient devant $t^{\ell(w)}$ est donc $\sum_{I\subset K}(-1)^I$. Dès que K est non vide, on montre que cette somme s'annule (calculer le développement de $0 = (1 + (-1))^{|K|}$ et reconnaître la somme recherchée). Le seul terme restant est donc pour $K = \varnothing$, mais alors un seul w convient : $w = w_0$, avec $\ell(w_0) = N$.

□

Domaine fondamental

Cette notion a une explicitation accessible dans le cas de $\mathcal{S}_n$: on va regarder l'application π : $\begin{array}{ccc} \mathbb{C}^n & \to & \mathbb{C}^n \\ x & \mapsto & (\pi_1(x), \ldots, \pi_n(x)) \end{array}$.

Remarquons tout d'abord qu'elle est surjective, car les polynômes π_i sont indépendants car G est un groupe de réflexion.

En revanche, elle n'est pas nécessairement injective : par exemple, dans le cas où $G = S_n$, comme les π_i sont symétriques, une permutation des coordonnées de x ne change pas l'image. D'une manière générale, comme les π_i sont invariants sous l'action de G, tout élément dans l'orbite de x a la même image que x par π.

En revanche, si on quotiente par G, c'est-à-dire qu'on regarde l'application π comme partant des orbites au lieu des points, alors elle devient injective : $\tilde{\pi}$: $\begin{array}{ccc} \mathbb{C}^n/G & \to & \mathbb{C}^n \\ \mathcal{O}(x) & \mapsto & (\pi_1(x), \ldots, \pi_n(x)) \end{array}$ est donc une bijection.
Dans le but d'éventuellement étudier cette application π plus en détail dans la suite, on évoque ici les domaines fondamentaux.

On fixe Π et Δ.
À chaque hyperplan H_α, on associe les demi-espaces ouverts $A_\alpha := \{\lambda \in V \mid \langle\lambda, \alpha\rangle > 0\}$ et $A'_\alpha := -A_\alpha$. On définit également le cône ouvert $C := \bigcap_{\alpha\in\Delta} A_\alpha$ et le cône fermé $D := \bar{C} = \bigcap_{\alpha\in\Delta} A_\alpha \cup H_\alpha$. On a alors $D = \{\lambda \in V \mid \forall \alpha \in \Delta,\ \langle\lambda, \alpha\rangle \geqslant 0\}$. On veut montrer que D est un **domaine fondamental** de l'action

gael.druez@ens-rennes.fr

de W sur V, c'est-à-dire que tout $\lambda \in V$ est conjugué (sous l'action de W) [1] à un unique élément de D.

Proposition :

Tout $\lambda \in V$ est conjugué à un $\mu \in D$. De plus, $\mu - \lambda$ est une combinaison linéaire de racines simples (ie d'éléments de Δ) à coefficients positifs ou nuls.

Preuve :

On considère l'ordre partiel défini sur V par $\lambda \leqslant \mu \Leftrightarrow \mu - \lambda$ est une combinaison linéaire à coefficients positifs ou nuls de Δ.
Soit $\lambda \in V$ fixé. On regarde l'ensemble des conjugués μ de λ vérifiant $\lambda \leqslant \mu$. Cet ensemble est non vide (il contient λ), on en choisit un élément maximal μ, ie vérifiant $\mu \leqslant \nu \Rightarrow \mu = \nu$.
Maintenant, pour tout $\alpha \in \Delta$, $\nu := s_\alpha(\mu)$ est un conjugué de μ donc de λ.
Si $\nu = \mu$, alors $\mu \in H_\alpha$ et donc $\langle \mu, \alpha \rangle = 0$.
Sinon, $\nu \neq \mu$, donc par maximalité de μ, on obtient que $\nu - \mu$ n'est pas une combinaison linéaire à coefficients positifs ou nuls de Δ. Or $\nu - \mu = s_\alpha(\mu) - \mu = -2\frac{\langle \mu, \alpha \rangle}{\langle \alpha, \alpha \rangle}\alpha$ est une combinaison linéaire de Δ, donc son unique coefficient éventuellement non nul doit être strictement négatif, ie $\langle \mu, \alpha \rangle > 0$.
Dans tous les cas, $\langle \mu, \alpha \rangle \geqslant 0$ et donc $\mu \in D$.

$\square$

On a montré l'existence d'un conjugué dans D, il reste à montre l'unicite. Pour cela, il suffit de montrer qu'aucun élément de D n'est conjugué à un autre élément de D.

On travaille toujours avec Π, et donc Δ, et donc D, fixés.

Théorème :

1. Si $w\lambda = \mu$ pour $\lambda, \mu \in D$ et $w \in W$, alors $\lambda = \mu$ et w est un produit de réflexions simples ($\in S$) qui fixent λ.
   En particulier, si $\lambda \in C = \mathring{D}$, alors le stabilisateur de λ est trivial.
2. D est un domaine fondamental pour l'action de W sur V
3. Le stabilisateur de $\lambda \in V$ est engendré par les rélfexions s_α, $\alpha \in \Phi$ qui laissent fixe λ, ie les réflexions s_α pour lesquelles $\lambda \in H_\alpha$
4. Si $U \subset V$ est un sous-ensemble quelconque, alors le sous-groupe de W qui fixe U est engendré par les réflexions qui fixent U

1. implicitement, on ne parlera de conjugaison que sous cette action (sauf mention contraire)

Preuve :

1. Raisonnons par récurrence sur $\ell(w)$ = le nombre de racines positives envoyées sur des racines négatives par w.
   $\boxed{I}$ Si $\ell(w) = 0$, alors $w = 1$ est bien un produit (vide) de réflexions simples qui fixent λ.
   $\boxed{H}$ Si $\ell(w) = n > 0$, alors notons $\alpha \in \Delta$ une racine positive envoyée sur une racine négative (on peut choisir une racine simple, car si toutes les racines simples étaient envoyées sur des racines positives, comme $w\Delta$ est un système simple, par unicité on aurait $w\Pi \subset \Pi$). Alors ws_α envoie $n-1$ racines positives sur des racines négatives : $\ell(ws_\alpha) = n-1$ (d'après un lemme précédent). De plus, comme $\lambda, \mu \in D$ et $w\alpha < 0$, on a :
   $$0 \geqslant \langle \mu, w\alpha \rangle = \langle w^{-1}\mu, w^{-1}w\alpha \rangle = \langle \lambda, \alpha \rangle \geqslant 0$$
   donc $\langle \lambda, \alpha \rangle = 0$. Ainsi, s_α fixe λ, d'où $\mu = w\lambda = ws_\alpha\lambda$ avec $\ell(ws_\alpha) = n-1$. Par hypothèse de récurrence, $\lambda = \mu$ et ws_α est un produit de réflexions simples qui fixent λ, et donc w aussi.
2. D'après le premier point et la proposition précédente.
3. Soit $\lambda \in V$, alors d'après la proposition précédente, il existe $w \in W$ tel que $\mu := w\lambda \in D$. Alors le stabilisateur W_μ de μ est engendré par les réflexions qui laissent fixe μ, d'après le premier point. Or les stabilisateurs d'éléments qui sont conjugués sont eux-mêmes conjugués, la formule générale $G_{gx} = gG_xG^{-1}$ donnant dans notre cas
   $W_\lambda = W_{w^{-1}\mu} = w^{-1}W_\mu w$.
   Ainsi, W_λ est engendré par les réflexions de la forme $w^{-1}s_\alpha w$, avec s_α qui fixe $\mu = w\lambda$. Or $w^{-1}s_\alpha w = s_{w^{-1}\alpha}$ par propriété des réflexions, et car $w \in \mathcal{O}(V)$. Enfin,
   $s_\alpha\mu = \mu \Leftrightarrow s_\alpha w\lambda = w\lambda \Leftrightarrow w^{-1}s_\alpha w\lambda = \lambda \Leftrightarrow s_{w^{-1}\alpha}\lambda = \lambda$ donc W_λ est exactement engendré par les réflexions simples qui fixent λ.
4. Le stabilisateur de U est clairement le stabilisateur de Vect$U$, et donc également le stabilisateur d'une base $\lambda_1, \dots, \lambda_t$ de Vect$U$. On travaille par récurrence sur t, la propriété à prouver étant : "Pour tout groupe de réflexion W et tout sous-ensemble $U \subset W$ dont le Vect est de dimension $t \in \mathbb{N}$, le sous-groupe de W qui fixe U est engendré par les réflexions qui fixent U".

   $\boxed{I}$ Le cas $t = 1$ a été traité dans le point précédent.
   $\boxed{H}$ Si $\lambda_1, \dots, \lambda_t$ est une base de Vect$U$, on sait que le stabilisateur W_{λ_1} de λ_1 est généré par les réflexions s_α qui fixent λ_1. Notons Φ' l'ensemble des tels α et de leurs opposés $-\alpha$. On a alors $\forall w \in W_{\lambda_1},\ ws_\alpha w^{-1} = s_{w\alpha}$, et donc $\forall w \in W_{\lambda_1},\ ws_\alpha = s_{w\alpha}w$, ie $ws_\alpha\lambda_1 = s_{w\alpha}w\lambda_1$. Comme $w,\ s_\alpha \in W_{\lambda_1}$, LHS $= ws_\alpha\lambda_1 = \lambda_1$ et RHS $= s_{w\alpha}w\lambda_1 = s_{w\alpha}\lambda_1$. Donc $w\alpha \in \Phi'$ car $s_{w\alpha}$ fixe λ_1.
   On en déduit que $\forall w \in W_{\lambda_1},\ w\alpha \in \Phi'$, c'est-à-dire que W_{λ_1} stabilise Φ'.
   Ainsi, W_{λ_1} est un groupe de réflexions, avec pour ensemble de racines Φ'. On peut appliquer l'hypothèse de récurrence à ce groupe de réflexions et à son sous-groupe qui fixe $\{\lambda_2, \dots, \lambda_t\}$. Or ce sous-groupe est précisément le stabilisateur de U.

$\square$

Le treillis des sous-groupes paraboliques

Cette notion est la notion principale pour laquelle on a vu ce que précède. Elle établit un lien entre les sous-ensembles de Δ et les spus-groupes paraboliques, lien qui peut s'avérer intéressant pour la généralisation des différences divisées.

On se sert du dernier point du théorème précédent pour obtenir une description plus précise de l'ensemble des sous-groupes paraboliques de la forme W_I, pour un sous-ensemble $I \subset S$ des reflexions simples (relativement à un Δ fixé).

Définition - Treillis :

> Un **treillis** est un ensemble partiellement ordonné tel que toute paire d'élément admet une borne supérieure et une borne inférieure.

Exemple :

- Tout ensemble muni d'un ordre total est un treillis (la borne supérieure d'une paire est le plus grand élément de la paire, la borne inférieure est le plus petit).
- Pour un ensemble E, $(\mathcal{P}(E), \subset)$ est un treillis, avec $\sup(A, B) = A \cup B$ et $\inf(A, B) = A \cap B$.
- L'ensemble des sous-groupes d'un groupe G, muni de $\inf(H_1, H_2) = H_1 \cap H_2$ et $\sup(H_1, H_2) = \langle H_1 \cup H_2 \rangle$, est un treillis.
- $(\mathbb{N}, \mid)$ est un treillis, avec $\inf(a, b) = a \wedge b$ et $\sup(a, b) = a \vee b$.

Définition - morphisme de treillis :

> Un **morphisme de treillis** est une application $\varphi : (E, \wedge, \vee) \longrightarrow (F, \cap, \cup)$ telle que :
>
> $$\forall x, y \in E,\ \varphi(x \wedge y) = \varphi(x) \cap \varphi(y) \text{ et } \varphi(x \vee y) = \varphi(x) \cup \varphi(y)$$

Proposition :

> La correspondance $I \mapsto W_I$ fournit un isomorphisme de treillis entre d'un côté, les sous-ensembles I de S, et de l'autre l'ensemble des sous-groupes paraboliques.

Preuve :

Pour montrer cette proposition, il faut :

1. montrer que l'ensemble des sous-groupes paraboliques est bien un treillis
2. montrer que la correspondance définir est bien compatible avec les bornes supérieures et inférieures
3. montrer qu'elle est bijective

On va en fait se contenter de montrer deux choses, pour $I, J \subset S$:

a. $W_{I \cup J} = \langle W_I, W_J \rangle$ (le groupe engndré par W_I et W_J)

b. $W_{I \cap J} = W_I \cap W_J$

On aura alors montré 1. car l'ensemble des sous-groupes paraboliques est alors stable par bornes sup et inf, donc c'est un sous-treillis du treillis des sous-groupes de W. 2. sera une conséquence immédiate de a. et b.. Enfin, la surjectivité est claire par définition des sous-groupes paraboliques, et l'injectivité viendra du fait que si $W_I = W_J$, alors $W_I \cap W_J = \langle W_I, W_J \rangle$ $(= W_I = W_J)$ donc $W_{I \cap J} = W_{I \cup J}$.

a. immédiat car $\langle\ \langle \{i_1, \dots, i_p\} \rangle, \langle \{j_1, \dots, j_q\} \rangle\ \rangle\ =\ \langle \{i_1, \dots, i_p, j_1, \dots, j_q\} \rangle$

b. Montrons que $W_{I \cap J} = W_I \cap W_J$.

$\boxed{\subset}$ ok

$\boxed{\supset}$ On va se servir des ensembles $V_I = \mathrm{Vect}\Delta_I$ qu'on a évoqué lorsqu'on a parlé des sous-groupes paraboliques. On a évidemment $V_I \cap V_J = V_{I \cap J}$. D'après une formule connue d'algèbre linéaire, pour deux sous-espaces A, $B \subset V$, on a $(A \cap B)^\perp = A^\perp + B^\perp$. Ce qui nous donne $V_I^\perp + V_J^\perp = (V_I \cap V_J)^\perp = v_{I \cap J}^\perp$.
Soit alors $w \in W_I \cap W_J$. w fixe donc tous les vecteurs de $V_I^\perp + V_J^\perp = v_{I \cap J}^\perp$. D'après le point 4. du théorème précédent, w est un produit de s_α qui fixent également chaque vecteur de cet ensemble. Mais alors chaque α est orthogonal à cet espace, et donc appartient à $\Phi \cap V_{I \cap J}$. Il s'ensuit que $w \in W_{I \cap J}$

□

Critère d'indépendence algébrique grâce au Jacobien

Ce critère va nous permettre de savoir quand diviser par le Jacobien, ce qui va être utile pour généraliser les différences divisées.

Proposition :

> Les polynômes $f_1, \dots, f_n \in \mathbb{K}[x_1, \dots, x_n]$ sont algébriquement indépendants si et seulement si $\det \mathcal{J}(f_1, \dots, f_n) \neq 0$.

gael.druez@ens-rennes.fr

Preuve :

$\boxed{\Leftarrow}$ Soit $h \in \mathbb{K}[y_1, \dots, y_n]$ non nul tel que $h(f_1, \dots, f_n) = 0$, de degré minimal. En utilisant la règle de la chaîne pour dériver cette relation par rapport à x_j, on obtient :

$$\begin{aligned}
\forall j \in [\![1, n]\!], \frac{\partial h}{\partial x_j} = 0 \quad &\Leftrightarrow \begin{bmatrix} \dfrac{\partial h}{\partial x_1} \\ \vdots \\ \dfrac{\partial h}{\partial x_n} \end{bmatrix} = 0_{\mathbb{K}^n} \Leftrightarrow \begin{bmatrix} \sum_{i=1}^{n} \dfrac{\partial h}{\partial y_i}(f_1, \dots, f_n) \dfrac{\partial f_i}{\partial x_1} \\ \vdots \\ \sum_{i=1}^{n} \dfrac{\partial h}{\partial y_i}(f_1, \dots, f_n) \dfrac{\partial f_i}{\partial x_n} \end{bmatrix} = 0_{\mathbb{K}^n} \\
&\Leftrightarrow \begin{bmatrix} \dfrac{\partial f_1}{\partial x_1} & \cdots & \dfrac{\partial f_n}{\partial x_1} \\ \vdots & \ddots & \vdots \\ \dfrac{\partial f_1}{\partial x_n} & \cdots & \dfrac{\partial f_n}{\partial x_n} \end{bmatrix} \times \begin{bmatrix} \dfrac{\partial h}{\partial y_1}(f_1, \dots, f_n) \\ \vdots \\ \dfrac{\partial h}{\partial y_n}(f_1, \dots, f_n) \end{bmatrix} = 0_{\mathbb{K}^n} \\
&\Leftrightarrow \begin{bmatrix} \dfrac{\partial h}{\partial y_1}(f_1, \dots, f_n) \\ \vdots \\ \dfrac{\partial h}{\partial y_n}(f_1, \dots, f_n) \end{bmatrix} \in \operatorname{Ker}\left(\begin{bmatrix} \dfrac{\partial f_1}{\partial x_1} & \cdots & \dfrac{\partial f_n}{\partial x_1} \\ \vdots & \ddots & \vdots \\ \dfrac{\partial f_1}{\partial x_n} & \cdots & \dfrac{\partial f_n}{\partial x_n} \end{bmatrix} \right) \\
&\Rightarrow \det \begin{bmatrix} \dfrac{\partial f_1}{\partial x_1} & \cdots & \dfrac{\partial f_n}{\partial x_1} \\ \vdots & \ddots & \vdots \\ \dfrac{\partial f_1}{\partial x_n} & \cdots & \dfrac{\partial f_n}{\partial x_n} \end{bmatrix} = \det \mathcal{J}(f_1, \dots, f_n) = 0
\end{aligned}$$

car le gradient de h est non nul car h est supposé non nul, donc au moins une des dérivées partielles est non nulle, et comme elles sont de degré strictement inférieur au degré de h, celles-ci ne peuvent annuler $(f_1, \dots, f_n)$ par minimalité du degré de h.

$\boxed{\Rightarrow}$ Si $f_1, \dots, f_n$ sont algébriquement indépendants, on utilise le fait que pour tout i, la famille $(x_i, f_1, \dots, f_n)$ est algébriquement liée (car le degré de transcendance de l'extension est n). On peut donc trouver un polynôme h_i en $n+1$ variables tel que $h_i(x_i, f_1, \dots, f_n) = 0$, avec un degré non nul en la première variable. On différentie cette égalité par rapport à x_k et on met les systèmes obtenus sous forme du produit matriciel suivant :

$$\left[\frac{\partial h_i}{\partial y_j}\right]_{i,j} \times \left[\frac{\partial f_i}{\partial x_j}\right]_{i,j} = \left[-\delta_{i,j} \frac{\partial h_i}{\partial x_j}\right]_{i,j}$$

La matrice (diagonale) de droite a un déterminant non nul d'après ce qui précède, donc c'est aussi le cas pour les matrices de gauche, en particulier pour $\mathcal{J}(f_1, \dots, f_n)$.

□

Corollaire :

Si $f_1, \dots, f_n$ sont algébriquement indépendants et homogènes de degrés $d_1, \dots, d_n$, alors $\det \mathcal{J}(f_1, \dots, f_n)$ est homogène de degré $\sum(d_i - 1) = N$.

Preuve :

det $\mathcal{J}(f_1, \dots, f_n) = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \frac{\partial f_1}{\partial x_{\sigma(1)}} \dots \frac{\partial f_n}{\partial x_{\sigma(n)}}$, chaque terme de la somme étant un polynôme nul ou un produit de polynômes homogènes de degrés $d_1 - 1, \dots, d_n - 1$.

□

Factorisation du Jacobien

Ce résultat nous donne une expression du Jacobien en fonction des formes linéaires associées aux racines.

Définition :

Un polynôme $f \in \mathbb{K}[x_1, \dots, x_n]$ est dit *antivariant* si $\forall w \in W,\ w \cdot f = (\det w)\, f$

On définit, pour $\alpha \in \Phi$, ℓ_α comme étant la forme linéaire (ie le polynôme de degré au plus 1 en toutes les variables) dont le noyau est l'hyperplan H_α orthogonal à α.
À un multiple scalaire près, $\ell_\alpha : \lambda \mapsto \langle \alpha, \lambda \rangle$.
Remarquons que pour des racines $\alpha, \beta \in \Phi$, on a $s_\beta \cdot \ell_\alpha = \ell_{s_\beta(\alpha)}$. On a aussi $\ell_{-\alpha} = -\ell_\alpha$.
(On rappelle que W agit sur $\mathbb{K}[x_1, \dots, x_n]$ de la manière suivante : $\forall w \in W,\ w \cdot f : x \mapsto f(w^{-1}(x))$.)

Proposition :

Soient $f_1, \dots, f_n$ des polynômes invariants fixés comme générateurs de W, et soit $\mathcal{J}$ le déterminant de la matrice jacobienne associée. Alors :

1. $\mathcal{J} = c \prod_{\alpha \in \Phi^+} \ell_\alpha$ (pour un certain $c \in \mathbb{K}$ qui dépend du choix de f_i)
2. Un polynôme est antivariant si et seulement si il peut s'écrire comme le produit de $\mathcal{J}$ et d'un polynôme invariant
3. Pour tout k, l'espace vectoriel des polynômes antivariants homogènes de degré k est de même dimension que celui des polynômes invariants homogènes de degré
$k - N = k - \deg \mathcal{J}$

gael.druez@ens-rennes.fr

Preuve :

1. Par le théorème d'inversion locale, $\mathcal{J}$ s'annule sur tous les hyperplans H_α, $\alpha \in \Phi$. Ainsi, $\forall \alpha \in \Phi^+$, $\ell_\alpha | \mathcal{J}$. Or les ℓ_α sont irréductibles et non proportionnelles, donc $\prod_{\alpha \in \Phi^+} \ell_\alpha \mid \mathcal{J}$. On conclut par égalité des degrés.
2. Tout d'abord, $\mathcal{J}$ est antivariant. En effet, si β est une racine simple, alors s_β envoie β sur $-\beta$ et permute les autres racines positives, donc $s_\beta \cdot \prod_{\alpha \in \Phi^+} \ell_\alpha = -\prod_{\alpha \in \Phi^+} \ell_\alpha$. En décomposant $w \in W$ en produit de racines simples et itérant ce calcul, on trouve bien que $w \cdot \mathcal{J} = (\det w)\mathcal{J}$.
   Il vient alors immédiatement que le produit d'un polynôme invariant par $\mathcal{J}$ est antivariant.
   Maintenant, si f est antivariant, alors en particulier, $\forall \alpha \in \Phi^+$, $s_\alpha \cdot f = -f$. Donc, si $a \in H_\alpha$, on a $-f(a) = (s_\alpha \cdot f)(a) = f(s_\alpha(a)) = f(a)$ donc $f(a) = 0$. f s'annule ainsi sur les zéros de ℓ_α pour toute racine α, donc comme précédemment on montre que $\mathcal{J} \mid f$, ie $f = g\mathcal{J}$.
   On applique alors un $w \in W$ quelconque : $w \cdot f = w \cdot g\mathcal{J}$. Or $w \cdot f = (\det w)f$ et $w \cdot g\mathcal{J} = (w \cdot g)(w \cdot \mathcal{J}) = (\det w)(w \cdot g)\mathcal{J}$, d'ou l'égalité $g = w \cdot g$.
3. Immédiat avec le point précédent.

$\square$

gael.druez@ens-rennes.fr

4 Généralisation

<table>
<tr><th>Groupe symétrique S_n</th><th>Groupe de réflexion G</th></tr>
<tr><td>$$\rho : \begin{array}{ccc} S_n & \to & \mathrm{GL}_n(\mathbb{K}) \\ \sigma & \mapsto & \left[\rho_\sigma : x \mapsto (x_{\sigma(1)}, \ldots, x_{\sigma(n)})\right] \end{array}$$</td><td>$$\phi : \begin{array}{ccc} G & \to & \mathrm{GL}_n(\mathbb{K}) \\ g & \mapsto & \begin{cases} M_g : x \mapsto M_g x \\ \phi(g) : x \mapsto \phi(g)(x) \end{cases} \end{array}$$</td></tr>
<tr><td colspan="2">$$f : \begin{array}{ccc} \mathbb{K}^n & \to & \mathbb{K}^n \\ x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} & \mapsto & \begin{bmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{bmatrix} \end{array}$$ polynomiale (chaque f_i est un polynôme en $x_1, \ldots, x_n$)</td></tr>
<tr><td colspan="2">Propriété d'équivariance :</td></tr>
<tr><td>$\forall \sigma \in S_n,\ \forall x \in \mathbb{K}^n,\ f(\rho_\sigma(x)) = \rho_\sigma(f(x))$</td><td>$\forall g \in G,\ \forall x \in \mathbb{K}^n,\ f(\phi_g(x)) = \phi_g(f(x))$</td></tr>
<tr><td>On note $\Phi = \{e_i - e_j\ ;\ i \neq j\}$, $\Pi = \{e_i - e_j\ ;\ i < j\}$ et $\Delta = \{e_i - e_{i+1}\ ;\ i \in [\![1, n]\!]\}$</td><td>Notons Φ un système de racines de G, Π un système positif et Δ un système simple.</td></tr>
<tr><td>Comme $S_n = \langle (ij)\ ;\ i < j \rangle$ et que $\rho((ij)) = s_{e_i - e_j}$, on peut restreindre la propriété d'équivariance aux permutations issues de Π : $\forall \alpha \in \Pi,\ \forall x \in \mathbb{K}^n,\ f(s_\alpha(x)) = s_\alpha(f(x))$</td><td>Comme G est supposé être un groupe de réflexion, il est engendré par un ensemble $\{g_i\ ;\ i\}$ tel que tout ϕ_{g_i} est une réflexion dont un vecteur normal α_i est dans Π. On peut donc restreindre la propriété d'équivariance : $\forall \alpha \in \Pi,\ \forall x \in \mathbb{K}^n,\ f(s_\alpha(x)) = s_\alpha(f(x))$</td></tr>
<tr><td colspan="2">Base d'invariants :</td></tr>
<tr><td>On a deux ensemble de polynômes invariants générateurs usuels : $$p_k : x \mapsto \sum_{i=1}^{n} x_i^k$$ $$e_k : x \mapsto \sum_{I \subset [\![1,n]\!],\ |I| = k} \prod_{i \in I} x_i$$</td><td>On sait qu'il existe des polynômes $\sigma_1, \ldots, \sigma_n$ algébriquement indépendants qui engendrent l'espace des invariants</td></tr>
<tr><td>Les p_k vérifient $\frac{\partial p_k}{\partial x_i} = k x_i^{k-1}$ et donc leur jacobien est proportionnel à un déterminant de Vandermonde</td><td>Comme les σ_k sont algébriquement indépendants, leur jacobien est non nul (d'après le critère vu précédemment)</td></tr>
<tr><td colspan="2">Définition des différences divisées :</td></tr>
<tr><td>Pour $I := \{i_1, \ldots, i_k\} \subset [\![1, n]\!]$, on définit $$F^I = \frac{\mathcal{J}(p_{i_1}, p_{i_2}, \ldots, p_{i_{k-1}}, F)}{\mathcal{J}(p_{i_1}, p_{i_2}, \ldots, p_{i_{k-1}}, p_{i_k})}$$</td><td>Pour $I := \{i_1, \ldots, i_k\} \subset [\![1, n]\!]$, on définit $$F^I = \frac{\mathcal{J}(\sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_{k-1}}, F)}{\mathcal{J}(\sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_{k-1}}, \sigma_{i_k})}$$</td></tr>
</table>

Tout d'abord, on définit l'action de notre groupe de réflexion sur $V = \mathbb{K}^n$. On choisit une application polynomiale f dont on va regarder les composantes, et on traduit la propriété d'équivariance de f avec l'action de G : ça reste la même idée, à savoir qu'appliquer un élément de G avant ou après f a le même résultat. On a également, comme pour tout groupe de réflexion, les systèmes de racines Φ, Π et Δ.

Pour ce qui est de la généralisation des différences divisées, après pas mal de recherches sur les liens entre racines, formes linéaires associées et zéros de polynômes, c'est finalement d'un point de

 gael.druez@ens-rennes.fr

vue plutôt géométrique qu'il fallait le voir :

Théorème :

> Soit G un groupe de réflexion agissant sur V de dimension finie n. Soient $p_1, \ldots, p_n$ des polynômes invariants générateurs de l'ensemble des polynômes invariants :
> $\mathbb{K}[x_1, \ldots, x_n]^G = \mathbb{K}[p_1, \ldots, p_n]$. Soit f un application polynomiale $V \longrightarrow V$ équivariante sous l'action de G.
> Alors, en notant $\mathcal{J}$ le déterminant de la matrice Jacobienne, on a :
>
> $$\mathcal{J}(p_1, \ldots, p_{n-1}, p_n) \text{ divise } \mathcal{J}(p_1, \ldots, p_{n-1}, f)$$

Preuve :

Comme les p_k engendrent l'espace des polynômes invariants, il existe un polynôme $g \in \mathbb{K}[y_1, \ldots, y_n]$ tel que $f = g(p_1, \ldots, p_n)$.
En utilisant la règle de la chaîne, on obtient l'égalité suivante sur les gradients :

$$\nabla f = \underbrace{[\nabla p_1 \mid \ldots \mid \nabla p_n]}_{\text{matrice Jacobienne des } p_k} \times \nabla g = \sum_{k=1}^{n} \frac{\partial g}{\partial p_k} \nabla p_k$$

On peut alors exprimer le jacobien qui nous intéresse :

$$\begin{aligned}
\mathcal{J}(p_1, \ldots, p_{n-1}, f) &= \det \left| \nabla p_1 \ \ldots \ \nabla p_{n-1} \ \nabla f \right| \\
&= \det \left| \nabla p_1 \ \ldots \ \nabla p_{n-1} \ \sum_{k=1}^{n} \frac{\partial g}{\partial p_k} \nabla p_k \right| \\
&= \sum_{k=1}^{n} \frac{\partial g}{\partial p_k} \det \left| \nabla p_1 \ \ldots \ \nabla p_{n-1} \ \nabla p_k \right| \\
&= \sum_{k=1}^{n} \frac{\partial g}{\partial p_k} \mathcal{J}(p_1, \ldots, p_{n-1}, p_k) \\
&= \frac{\partial g}{\partial p_n} \cdot \mathcal{J}(p_1, \ldots, p_{n-1}, p_n)
\end{aligned}$$

car si $k \in [\![1, n-1]\!]$, on a un déterminant avec deux colonnes égales, celui-ci est donc nul.
Ceci conclut la preuve.

□

gael.druez@ens-rennes.fr

Conclusion

Malheureusement, mon stage a duré trop peu de temps et je n'ai pas pu avancer autant que je voulais. Bien que le début semble prometteur, il reste beaucoup à faire, notamment des manipulation à généraliser.

J'ai passé beaucoup de temps à analyser le résultat de la première partie dans un premier temps, et ensuite j'ai fait l'erreur de ma lancer dans une recherche en ne maîtrisant que sommairement les groupes de réflexions. Je suis alors revenu à mon étude des groupes de réflexions, et j'ai eu l'esprit plus clair là-dessus, mais la fin du stage est arrivée rapidement ensuite.

Néanmoins, nous allons continuer à avancer sur cette piste avec les 3 autres personnes dans le projet.

De mon côté, je suis satisfait de ce stage car il m'a permis de faire le lien entre les connaissances académiques et le monde de la recherche. En effet, j'ai principalement étudié pour accumuler des connaissances nouvelles, mais j'ai aussi expérimenté la recherche : à partir d'une idée de mon maître de stage, j'ai cherché à généraliser une notion dont on n'avait pas trouvé de travaux avant ça. Il y a eu beaucoup d'échecs (que je n'ai pas rapportés dans ce rapport), mais quelques réussites quand même (par exemple quand une preuve dans le cas général est beaucoup plus rapide que dans le cas particulier en utilisant les outils généraux). Je suis content d'avoir pu expérimenter ce monde particulier de la recherche et je pense en avoir eu un aperçu représentatif.

Bibliographie et remerciements

Références

[Fla78] Leopold FLATTO. "Invariant of finite reflection groups". In : *L'enseignement mathématique, Band 24* (1978).

[Hum94] James E. HUMPHREYS. *Reflection groups and Coxeter groups*. Cambridge University Press, 1994. ISBN : 0 521 43613 3.

[N P09] Sh. Shakirov N. PERMINOV. "Discriminant of symmetric polynomials (unpublished)". In : (2009).

[Lau16] Anna Karasoulou LAURENT BUSÉ. "Resultant of an equivariant polynomial system with respect to the symmetric group". In : *Journal of Symbolic Computation* (2016). DOI : 76:142-157.

[Mic23] Cordian Riener MICHAL KOCVARA Bernard Mourrain (Editors). *Polynomial Optimisation, Moments and Applications*. Springer, 2023. ISBN : 978-3-031-38658-9.

Remerciements

Je tiens à remercier toutes les personnes qui ont rendu ce stage possible. Ça a été une expérience très enrichissante culturellement, humainement et mathématiquement.

Merci en particulier à Cordian RIENER de m'avoir donné cette opportunité et de m'avoir accueilli dans l'équipe. Merci également au Centre Henri LEBESGUE et à l'ENS Rennes pour l'aide financière.

gael.druez@ens-rennes.fr