Université Grenoble Alpes

Rapport de Travail d'étude et de recherche

Algèbre des polynômes invariants sous l'action d'un groupe fini

Auteur :
Mallaury Guebey

Enseignant référent :
Mme Odile Garotta

Janvier 2018 - Mai 2018

Table des matières

ALGÈBRE DES POLYNÔMES INVARIANTS SOUS L'ACTION D'UN GROUPE FINI

GUEBEY MALLAURY

1. Motivation et résumé du sujet

Soient K un corps de caractéristique nulle, V un K-espace vectoriel de dimension n, un entier strictement positif.
Notons $GL(V)$ l'ensemble des endomorphismes inversibles de V, $K[X_1, ..., X_n]$ l'ensemble des polynômes en n variables à coefficients dans K.

Le but de ce travail d'étude et de recherches est de décrire explicitement l'algèbre $\mathcal{I}$ des polynômes invariants sous l'action linéaire d'un groupe fini G.
Nous savons par exemple, que le théorème fondamental des polynômes symétriques affirme que l'algèbre des polynômes symétriques de $K[X_1, \ldots, X_n]$ (c'est-à-dire l'algèbre des polynômes invariants sous S_n, le groupe des permutations, qui agit par permutations de $X_1, \ldots, X_n$) est engendrée par les n polynômes symétriques élémentaires.
Nous pouvons donc légitimement nous demander s'il existe d'autres résultats de ce type, plus généraux, qui nous permettraient d'appréhender plus facilement les polynômes invariants sous l'action d'autres groupes finis G.

Une fois définies les notions de base de notre étude que sont les fonctions polynomiales sur V et les polynômes invariants sous G sous-groupe fini de $GL(V)$, nous présenterons deux résultats majeurs sur ce sujet :
Nous montrerons d'abord (théorème de Noether) que l'algèbre $\mathcal{I}$ est engendrée par un nombre fini de polynômes homogènes (de degrés $\leq |G|$), et comment obtenir une telle famille génératrice (pas forcément minimale).

Puis notre objectif principal sera d'établir les deux implications du théorème de Chevalley-Shephard-Todd :
Soient K un corps de caractéristique nulle, V un K-espace vectoriel de dimension $n \geq 1$ et $G \subset GL(V)$ un groupe fini. Alors G est engendré par des pseudo-réflexions si et seulement si l'algèbre $\mathcal{I}$ des invariants de G est isomorphe à $K[X_1, ..., X_n]$.

Nous définirons à cette occasion la "série de Molien" de l'algèbre $\mathcal{I}$, qui code les dimensions de ses composantes homogènes, et nous verrons que le théorème de Molien exprime cette série formelle comme une fraction rationnelle associée à la représentation de G dans V. Nous illustrerons l'intérêt de la série et du théorème de Molien en obtenant une famille de deux générateurs homogènes du groupe diédral D_m.

Nous terminerons en discutant sur des familles de générateurs homogènes de l'algèbre des invariants de deux groupes engendrés par des pseudo-réflexions : le groupe diédral D_m et le groupe des isométries du cube.

Enfin, notre annexe présente les notions de base et de degré de transcendance d'une extension de corps, et elle en donne certaines propriétés fondamentales qui sont utilisées dans le cœur du mémoire.

2. Les fonctions polynomiales sur un espace vectoriel

On désigne par K un corps de caractéristique nulle.
Soit V un K-espace vectoriel muni d'une base $B = (e_1, ..., e_n)$ et de sa base duale $B^* = (e_1^*, ..., e_n^*)$. On note $F = F(V)$ l'ensemble des fonctions $f : V \to K$. Muni de l'addition et de la multiplication par un scalaire habituelles, F est une algèbre sur K.
On définit les fonctions $x_i \in F$, pour tout $1 \leq i \leq n$ par $x_i(v) =< e_i^*, v >$, pour tout $v \in V$ et on définit $\mathcal{P} = \mathcal{P}(V)$ la sous-algèbre de F engendrée par 1 (la fonction constante égale à 1), $x_1, x_2..., x_n$. Ainsi les éléments de $\mathcal{P}$ sont des fonctions f de la forme : $f = \sum_{\alpha=(\alpha_1,...,\alpha_n)} a_\alpha x_1^{\alpha_1} x_2^{\alpha_2} ... x_n^{\alpha_n}$, où $a_\alpha \in K$ et les $\alpha \in \mathbf{N}^n$ sont presque tous nuls.

Remarque 2.1. $\mathcal{P}$ ne dépend pas du choix de B. En effet, si $B' = (x_1', ..., x_n')$ est une autre base de V, alors il existe une matrice inversible $P \in M_n(K)$ telle que si l'on note $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ et $X' = \begin{pmatrix} x_1' \\ x_2' \\ \vdots \\ x_n' \end{pmatrix}$, $X' = P^{-1}X$. C'est-à-dire, chacun des x_i' est combinaison K-linéaire des x_i et donc fonction polynomiale en les x_i. Donc les éléments de $\mathcal{P}$ sont toujours les fonctions f de la forme : $f = \sum_{\alpha=(\alpha_1,...,\alpha_n)} a_\alpha x_1^{\alpha_1} x_2^{\alpha_2} ... x_n^{\alpha_n}$, où $a_\alpha \in K$ et les $\alpha \in \mathbf{N}^n$.

Définition 2.2. Les fonctions $f \in \mathcal{P}$ sont appelées fonctions polynomiales sur V.

L'application

$$\begin{array}{ccc} \phi : K[X_1, ..., X_n] & \to & \mathcal{P} \\ X_i & \mapsto & x_i \\ k \in K & \mapsto & (v \mapsto k, \text{ pour tout } v \in V) \end{array}$$

est un isomorphisme de K-algèbres.
En effet, ϕ est bien définie et est un morphisme de K-algèbres par la propriété universelle (on a bien défini ϕ sur les X_i et sur K). ϕ est surjective par définition de $\mathcal{P}$, de plus, K étant de caractéristique nulle, il est infini et dans ce cas, on sait que ϕ est injective. C'est pourquoi pour la suite, nous confondrons les fonctions polynomiales et les polynômes.

Définition 2.3. (i) La fonction $a_\alpha x_1^{\alpha_1} x_2^{\alpha_2} ... x_n^{\alpha_n}$ est appelée monôme de degré $d = \sum_{i=1}^n \alpha_i$.
(ii) Une fonction polynomiale $f \in \mathcal{P}$ est dite homogène de degré d si elle est somme finie de monômes de degré d. On note $\mathcal{P}_d$ l'ensemble des fonctions polynomiales homogène de degré d. On considère que $0 \in \mathcal{P}_d$ pour tout d.

Remarque 2.4. On a clairement que $\forall d \in \mathbf{N}$, $\mathcal{P}_d$ est un sous-espace vectoriel de $\mathcal{P}$ de dimension finie $\binom{n+d-1}{d}$ et $\mathcal{P}$ est la somme directe : $\mathcal{P} = \bigoplus_{d \in \mathbf{N}} \mathcal{P}_d$. De plus, d'après la remarque (2.1), $\mathcal{P}_d$ ne dépend pas du choix de la base B.

Définition 2.5. Si $T \in GL(V)$, on définit, pour tout $f \in \mathcal{P}$ l'application Tf par :

$$\begin{array}{rccc} Tf & : & V & \to & K \\ & & v & \mapsto & f(T^{-1}v) \end{array}$$

Proposition 2.6. Si $S, T \in GL(V)$ et $f \in \mathcal{P}$ alors $(ST)f = S(Tf)$ et si $S = id_V$, $Sf = f$.
De plus, pour tout $S \in GL(V)$, pour tout $f, g \in \mathcal{P}$, pour tout $\lambda \in K$,
$S(\lambda f) = \lambda S(f)$,
$S(f + g) = S(f) + S(g)$ et
$S(fg) = S(f)S(g)$.
Enfin, $S(1) = 1$.

Ainsi, $(T, f) \mapsto Tf$ définit bien une action du groupe $GL(V)$ sur $\mathcal{P}$ et $f \mapsto Tf$ est un automorphisme d'algèbre de $\mathcal{P}$.

Démonstration. Si $v \in V$, alors $((ST)f)(v) = f((ST)^{-1}v) = f(T^{-1}S^{-1}v) = (Tf)(S^{-1}v) = (S(Tf))(v)$. Donc $(ST)(f) = S(Tf)$. □

Proposition 2.7. Si $f \in \mathcal{P}$, alors $Tf \in \mathcal{P}$. Précisément, on a : pour tout $i \in \{1, ..., n\}$, $Tx_i = \sum_{k=1}^{n} a_{ik}x_k$ où $(a_{ij})_{1 \le i,j \le n}$ sont les coefficients de $N = (mat_B T)^{-1}$.
De plus, $T\mathcal{P}_d = \mathcal{P}_d$ pour chaque degré d.

Démonstration. Soit $i \in \{1, ..., n\}$.
Soit $v \in V$. Notons $M = mat_B T$. Alors M est inversible (car $T \in GL(V)$). Notons $(a_{ij})_{1 \le i,j \le n}$ les coefficients de M^{-1}.
$Tx_i(v) = x_i(T^{-1}(v)) = x_i M^{-1} v = x_i((\sum_{k=1}^{n} a_{jk}v_k)_{1 \le j \le n}) = \sum_{k=1}^{n} a_{ik}v_k$
$= \sum_{k=1}^{n} a_{ik}x_k(v) \in \mathcal{P}_1$.
Donc $T\mathcal{P}_1 \subset \mathcal{P}_1$ ce qui permet de conclure car T agit par automorphisme d'algèbres d'après la proposition précédente. □

Si G est un sous-groupe fini de $GL(V)$, on obtient donc des représentations linéaires de G : $\mathcal{P}$ qui est de dimension infinie et les $\mathcal{P}_d$, pour tout entier d (cf (2.7)) qui sont de dimension finie.

Proposition 2.8. Soit $S \in GL(V)$ telle que $S - id_V$ est de rang 1. Alors son polynôme caractéristique χ_S est scindé sur K, et S est diagonalisable si et seulement si $\zeta = \det S \neq 1$.
De plus, si S est d'ordre fini, et si $car(K) = 0$ (ou $car(K)$ première avec $ord(S)$), alors S est diagonalisable, i.e. $\zeta \neq 1$.

Démonstration. Par hypothèse, $H = Ker(S - id_V)$ est un hyperplan. Si on complète une base de H en une base de V, la matrice de S dans cette base est triangulaire, et $\det(S)$ est son coefficient (n, n), noté ζ.
Ainsi, $\chi_S(X) = (X - 1)^{n-1}(X - \zeta)$ est scindé sur K.
S est diagonalisable si et seulement si V est somme directe de ses sous-espaces propres. Or, $E_1 = Ker(S - id_V)$ est l'hyperplan ; donc S est diagonalisable si et seulement si il admet une autre valeur propre que 1, i.e. si et seulement si $\zeta \neq 1$.

Supposons maintenant que S est d'ordre fini m dans $GL(V)$. Notons $D(X) = pgcd(\chi_S(X), X^m - 1) \in K[X]$. Alors par Bézout, $D(X)$ annule S ; $D(X)$ est scindé sur K car il divise $\chi_S(X)$ qui est scindé ; et enfin, $D(X)$ a ses racines simples car $X^m - 1$ a ses racines simples dès que $car(K)$ est nulle ou première avec m. □

Définition 2.9. Un endomorphisme S de $GL(V)$ est une pseudo-réflexion si $S-id_V$ est de rang 1 et si S est diagonalisable sur K (si S est d'ordre fini et $car(K) = 0$, cette dernière condition est réalisée).

Remarque 2.10. Par la proposition (2.8), si $S \in GL(V)$ vérifie $S - id_V$ est de rang 1, S est d'ordre fini et si $car(K) = 0$ ou est première avec $ord(S)$, alors S est une pseudo réflexion.

Soit S une pseudo-réflexion de V. Alors $H = \ker(S - Id)$ est de dimension $n-1$. Soit $(e_2, ...e_n)$ une base de H. Si $w \in V$ est un vecteur propre de S qui n'est pas dans H, alors $(w, e_2, ...e_n)$ est une base de V et la valeur propre associée à w est ζ, différent de 1.
Donc pour tout $v \in V$, si $v = v_1 w + \sum_{i=2}^{n} v_i e_i$,

$$S(v) = \zeta v_1 w + \sum_{i=2}^{n} v_i e_i \text{ et donc } S(v) - v = (\zeta - 1)v_1 w$$

Ainsi, pour tout $v \in V$, $S(v) = v + L_S(v)w$ où L_S est la forme linéaire $v \mapsto (\zeta - 1)v_1$.

Remarque 2.11. (i) L_S n'est déterminée qu'à un facteur près car si l'on remplace w par λw où $\lambda \neq 0$, L_S devient $\lambda^{-1} L_S$.
(ii) S^{-1} est une pseudo-réflexion et $L_{S^{-1}}(v) = (\zeta^{-1} - 1)v_1$.
(iii) $L_S \in V^* \subset \mathcal{P}$.

Proposition 2.12. L'élément L_S de $\mathcal{P}$ construit ci-dessus est un diviseur de $Sf - f$, pour tout $f \in \mathcal{P}$.

Démonstration. Sans perte de généralité, on pose $e_1 = w$ et on se place dans la base $B = (e_1, ..., e_n)$ comme ci-dessus qui diagonalise S.

Lemme. Si P est le polynôme associé à $Sf - f$, X_1 divise P si et seulement si $P(0, X_2, ..., X_n) = 0$. Donc par l'isomorphisme ϕ, x_1 divise $Sf - f$ si et seulement si pour tout $v \in H = Vect(e_2, ..., e_n)$, $(Sf - f)(v) = 0$.

Or, pour tout $v \in H$, $(Sf - f)(v) = f(S^{-1}(v)) - f(v) = f(v + L_{S^{-1}}(v)e_1) - f(v) = f(v + (\zeta^{-1} - 1)v_1) - f(v) = f(v) - f(v) = 0$ car $v \in H$ donc $v_1 = 0$. □

En conséquence de cette proposition, on peut écrire, pour tout $f \in \mathcal{P}$,

$$Sf = f + (\delta_S f) L_S$$

où $\delta_S f$ est une fonction de $\mathcal{P}$ déterminée à un facteur multiplicatif près qui est soit 0 soit de degré strictement inférieur à celui de f. δ_S est ainsi un endomorphisme de $\mathcal{P}$ qui vérifie

$$\delta_S \mathcal{P}_d \subset \mathcal{P}_{d-1}, \text{ pour tout } d \in \mathbf{N}^*.$$

Remarque 2.13. Si on a $K = \mathbf{R}$ (resp. $\mathbf{C}$), on peut munir V d'un produit scalaire (resp. hermitien) qui soit G-invariant et alors en imposant $\|v_1\|_2 = 1$, L_S est bien déterminée.

3. L'algèbre des invariants, théorèmes de Noether et Chevalley-Shephard-Todd(I)

Soit G un sous-groupe fini de $GL(V)$.

Définition 3.1. Si $f \in \mathcal{P}$ et $Tf = f$ pour tout $T \in G$, alors f est appelé un invariant de G. On notera $\mathcal{I} = \mathcal{I}(G)$ l'ensemble des invariants de G.

Remarque 3.2. $\mathcal{I}$ est une sous-algèbre de $\mathcal{P}$. De plus, si on pose $\mathcal{I}_d = \mathcal{I} \cap \mathcal{P}_d$ pour chaque d, alors $\mathcal{I}_d$ est un sous espace de $\mathcal{I}$ composé d'homogènes de degré d et $\mathcal{I}$ est la somme directe $\bigoplus_{d\in\mathbf{N}} \mathcal{I}_d$.

Définition 3.3. On définit

$$\begin{array}{rccccc} M_G = M & : & \mathcal{P} & \to & \mathcal{P} \\ & & f & \mapsto & \frac{1}{|G|}\sum\limits_{T\in G} Tf \end{array}$$

M effectue une moyenne des G-transformations de f. On a clairement que M est linéaire et pour tout entier d positif ou nul, $M(\mathcal{P}_d) \subset \mathcal{P}_d$ (par la proposition (2.7)).

Proposition 3.4. (i) Si $f \in \mathcal{P}$ alors $M(f) \in \mathcal{I}$.
(ii) $\forall f \in \mathcal{I}$, $M(f) = f$.
(iii) On a $M^2 = M$.
Donc M est une projection de $\mathcal{P}$ sur $\mathcal{I}$ et de chaque $\mathcal{P}_d$ sur $\mathcal{I}_d$.
(iv) Pour tout $f \in \mathcal{I}$, pour tout $g \in \mathcal{P}$, $M(fg) = fM(g)$. Donc M est $\mathcal{I}$-linéaire et $\mathcal{P}$ est un $\mathcal{I}$-module.

Démonstration. (i) Soient $f \in \mathcal{P}$ et $S \in G$.
$SM(f) = S(\frac{1}{|G|}\sum\limits_{T\in G} Tf) = \frac{1}{|G|}\sum\limits_{T\in G} STf$.
Or, $\{ST : T \in G\} = \{T : T \in G\}$.
Donc $SM(f) = \frac{1}{|G|}\sum\limits_{T\in G} Tf = M(f)$.
C'est-à-dire $M(f) \in \mathcal{I}$.

(ii) On a : $\forall f \in \mathcal{I}$, $M(f) = \frac{1}{|G|}\sum\limits_{T\in G} Tf = \frac{1}{|G|}\sum\limits_{T\in G} f = \frac{1}{|G|}|G|f = f$.

(iii) Comme $M(f) \in \mathcal{I}$, on a que $M(M(f)) = M(f)$.
Donc $M^2 = M$.

(iv) Soient $f \in \mathcal{I}$ et $g \in \mathcal{P}$. $M(fg) = \frac{1}{|G|}\sum_{T\in G} T(fg) = \frac{1}{|G|}\sum_{T\in G} T(f)T(g) = \frac{1}{|G|}\sum_{T\in G} fT(g) = f\frac{1}{|G|}\sum_{T\in G} T(g) = fM(g)$. □

Exemple 3.5. On considère le groupe cyclique $C_4 \subset GL_2(K)$ engendré par

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Dans cet exemple, l'ensemble des invariants sous l'action de C_4 est
$\mathcal{I} = \{f \in K[X,Y], f(X,Y) = f(A\begin{pmatrix} X \\ Y \end{pmatrix}) = f(-Y,X)\}$.
On a : $A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $A^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $A^4 = I_2$. Donc l'opérateur M est

donné par : $M(f)(X,Y) = \frac{1}{4}(f(X,Y) + f(-Y,X) + f(-X,-Y) + f(Y,-X))$.
Par la proposition (3.4), on peut facilement calculer des invariants :
$M(X^2) = \frac{1}{4}(X^2 + (-Y)^2 + (-X)^2 + Y^2) = \frac{1}{2}(X^2 + Y^2)$
$M(XY) = \frac{1}{4}(XY + (-Y)X + (-X)(-Y) + Y(-X)) = 0$
$M(X^3Y) = \frac{1}{4}(X^3Y + (-Y)^3X + (-X)^3(-Y) + Y^3(-X)) = \frac{1}{2}(X^3Y - XY^3)$
$M(X^2Y^2) = \frac{1}{4}(X^2Y^2 + (-Y)^2X^2 + (-X)^2(-Y)^2 + Y^2(-X)^2) = X^2Y^2$
Ainsi, $X^2 + Y^2$, $X^3Y - XY^3$ et $X^2Y^2 \in \mathcal{I}$.

Nous verrons en (3.10) que $\mathcal{I} = K[X^2+Y^2, X^3Y - XY^3, X^2Y^2]$. Pour cela, nous utiliserons le théorème crucial suivant, établi par Emmy Noether en 1916 :

Théorème 3.6 (Noether)**.** *Soit N l'ordre de G. L'algèbre $\mathcal{I}$ des invariants de G est de type fini, engendrée par les invariants homogènes de degré au plus N.*

Pour la preuve de ce théorème, nous aurons recours au lemme (3.7) suivant, qui exprime chaque monôme de $\mathcal{P}$ comme une combinaison linéaire de puissances de formes linéaires sur V. D'où il suit que le K-espace vectoriel $\mathcal{P}$ est engendré par les puissances des formes linéaires sur V (3.8).

Lemme 3.7. En caractéristique nulle, pour tout entier $n \geq 1$, on a dans $\mathcal{P}$

$$x_1 ... x_n = \frac{1}{n!} \sum_{p=1}^{n} (-1)^{n-p} \sum_{I \subset \{1,...,n\}, |I|=p} x_I^n$$

où $x_I = \sum_{i \in I} x_i$.

Démonstration. Supposons pour commencer que $x_n = 0$. Dans ce cas, on va montrer que le terme de droite est nul.
On a

$$\begin{aligned} &\sum_{p=1}^{n} (-1)^{n-p} \Big(\sum_{I \subset \{1,...,n\}, |I|=p} x_I^n \Big) \\ =&\sum_{p=1}^{n} (-1)^{n-p} \Big(\sum_{I \subset \{1,...,n-1\}, |I|=p} x_I^n + \sum_{I \subset \{1,...,n\}, n \in I, |I|=p} x_I^n \Big) \end{aligned}$$

Notons

$$a_p = \sum_{I \subset \{1,...,n-1\}, |I|=p} x_I^n \text{ et } b_p = \sum_{I \subset \{1,...,n\}, n \in I, |I|=p} x_I^n$$

On remarque que $a_n = 0$ et $b_1 = 0$. De plus, si $p = n$, alors $|\mathcal{I}| = n \Leftrightarrow \mathcal{I} = \{1, ..., n\}$.
Or, pour tout $1 \leq p \leq n-1$,

$$\sum_{I \subset \{1,...,n-1\}, |I|=p} x_I^n = \sum_{I \subset \{1,...,n\}, n \in I, |I|=p+1} x_I^n$$

C'est-à-dire

$$a_p = b_{p+1}$$

(par exemple, $x_1 + x_2 + x_3$ apparaît dans $\sum_{I \subset \{1,...,n-1\}, |I|=3} x_I^n$ et $x_1 + x_2 + x_3 + x_n$ apparaît dans $\sum_{I \subset \{1,...,n\}, n \in I, |I|=4} x_I^n$ et on a bien $x_1 + x_2 + x_3 = x_1 + x_2 + x_3 + x_n$).

On obtient alors des compensations grâce aux $(-1)^{n-p}$:

$$\begin{aligned}
&\sum_{p=1}^{n}(-1)^{n-p}\left(\sum_{I\subset\{1,\dots,n\},|I|=p} x_I^n\right)\\
=&\sum_{p=1}^{n-1}(-1)^{n-p}(b_p+b_{p+1})+b_n+a_n\\
=&\sum_{p=1}^{n-1}(-1)^{n-p}b_p+\sum_{p=1}^{n-1}(-1)^{n-p}b_{p+1}+b_n\\
=&\sum_{p=1}^{n-1}(-1)^{n-p}b_p-\sum_{q=2}^{n}(-1)^{n-q}b_q+b_n\\
=&(-1)^{n-1}b_1-b_n+b_n\\
=&0
\end{aligned}$$

Ce raisonnement est également valable si on suppose $x_1 = 0$, $x_2 = 0$,... ou $x_{n-1} = 0$. Par conséquent, le polynôme de droite est multiple de $x_1...x_n$. De plus, chaque monôme est homogène de degré n. Donc il existe $\lambda \in K$ tel que

$$\sum_{p=1}^{n}(-1)^{n-p}\sum_{I\subset\{1,\dots,n\},|I|=p} x_I^n = \lambda\prod_{i=1}^{n} x_i$$

Enfin, en développant $(\sum_{i=1}^{n} x_i)^n$, le terme $\prod_{i=1}^{n} x_i$ apparaît $n!$ fois.
Donc $\lambda = n!$.

□

Conséquence 3.8. Chaque monôme de $\mathcal{P}$ s'exprime comme une combinaison linéaire de puissances de formes linéaires sur V et donc le K-espace vectoriel $\mathcal{P}$ est engendré par les puissances des formes linéaires sur V.

Démonstration. (théorème de Noether)
Soit $\mathcal{J}$ la sous-algèbre de $\mathcal{I}$ engendrée par les invariants homogènes de degré au plus N. Soit $\mathcal{P}_{<N} = \mathcal{P}_1 \oplus ... \oplus \mathcal{P}_{N-1}$ le sous-espace vectoriel de $\mathcal{P}$ formé des fonctions polynomiales de degré au plus $N-1$.
On a : $\mathcal{I} = vect(\oplus_{d=0}^{N}\mathcal{I}_d) = M(vect(\oplus_{d=0}^{N}\mathcal{I}_d))$ et une base de $\mathcal{I}$ est l'ensemble des monôme de degré $\leq N$.
Montrons que le produit $\mathcal{J}\cdot\mathcal{P}_{<N}$ est égal à $\mathcal{P}$.
Puisque l'espace vectoriel $\mathcal{P}$ est engendré par les puissances des formes linéaires (3.8), il suffit de montrer que $l^n \in \mathcal{J}\cdot\mathcal{P}_{<N}$ pour toute forme linéaire l sur V, et pour tout entier $n \geq 0$.
Ceci est clair si $n < N$ (parce qu'alors $l^n \in \mathcal{P}_{<N}$). Si $n = N$, alors on a dans $\mathcal{P}[t]$:

$$\prod_{T\in G}(t - Tl) = t^N + a_1t^{N-1} + ... + a_N$$

où les a_i sont dans $\mathcal{J}$. En évaluant en $t = l$, puisque $id_V \in G$, on a donc

$$l^N \in \mathcal{J} + \mathcal{J}l + ... + \mathcal{J}l^{N-1}$$

Par récurrence supposons que pour $n \geq N$, $l^n \in \mathcal{J} + \mathcal{J}l + ... + \mathcal{J}l^{N-1}$. Alors $l^{n+1} = l^n l \in \mathcal{J}l + \mathcal{J}l^2 + ... + \mathcal{J}l^N$. Mais puisque $l^N \in \mathcal{J} + \mathcal{J}l + ... + \mathcal{J}l^{N-1}$, on a donc bien que $l^{n+1} \in \mathcal{J} + \mathcal{J}l + ... + \mathcal{J}l^{N-1}$.
Donc pour tout $n \geq 0$, $l^n \in \mathcal{J} \cdot \mathcal{P}_{<N}$. Ainsi, $\mathcal{P} \subset \mathcal{J} \cdot \mathcal{P}_{<N}$ et puisque l'inclusion inverse est évidente, on a égalité entre ces deux ensembles.
Montrons maintenant que $\mathcal{J} = \mathcal{I}$. Soit $f \in \mathcal{I}$. Par ce que l'on vient de montrer, on peut écrire

$$f = \sum_{i=1}^{s} a_i f_i \text{ pour } s \geq 1$$

avec des a_i dans $\mathcal{J}$ et des f_i dans $\mathcal{P}_{<N}$.
En appliquant l'opérateur M (cf (3.3)) à f, on obtient par (3.4) :

$$f = M(f) = \sum a_i M(f_i)$$

avec des a_i dans $\mathcal{J}$ et des $M(f_i)$ dans $\mathcal{I}_{<N} \subset \mathcal{J}$.
Donc $f \in \mathcal{J}$ et puisque l'inclusion inverse est évidente, $\mathcal{J} = \mathcal{I}$.
Enfin, $\dim \oplus_{n=1}^{N} \mathcal{I}_n < \infty$ donc une base de cet espace fournit une famille finie de générateurs de l'algèbre $\mathcal{I}$. □

Remarque 3.9. Il résulte de plus de (3.4) (iii) que chaque $\mathcal{I}_d$ est égal à $M(\mathcal{P}_d)$, et donc on obtient que : les $M(\prod_{i=1}^{n} X_i^{a_i})$ où $1 \leq \sum_{i=1}^{n} a_i \leq |G|$ forment une famille de générateurs homogènes de l'algèbre $\mathcal{I}$.

Exemple 3.10. Reprenons l'exemple (3.5) où $G = C_4$. Pour obtenir une famille de générateurs homogènes de l'algèbre $\mathcal{I}$, il nous suffit donc de calculer $M(X^iY^j)$ pour chaque $1 \leq i + j \leq 4$.
On a :

X^iY^j	$M(X^iY^j)$	X^iY^j	$M(X^iY^j)$
X	0	XY^2	0
Y	0	Y^3	0
X^2	$\frac{1}{2}(X^2+Y^2)$	X^4	$\frac{1}{2}(X^4+Y^4)$
XY	0	X^3Y	$\frac{1}{2}(X^3Y-XY^3)$
Y^2	$\frac{1}{2}(X^2+Y^2)$	X^2Y^2	X^2Y^2
X^3	0	XY^3	$-\frac{1}{2}(X^3Y-XY^3)$
X^2Y	0	Y^4	$\frac{1}{2}(X^4+Y^4)$

Donc $\mathcal{I}$ est engendré par les polynômes homogènes suivants : X^2+Y^2, X^4+Y^4, $X^3Y - XY^3$ et X^2Y^2.
Cependant, nous n'avons pas besoin de X^4+Y^4 car $X^4+Y^4 = (X^2+Y^2)^2 - 2X^2Y^2$.
Donc

$$\mathcal{I} = K[X^2+Y^2, X^3Y - XY^3, X^2Y^2]$$

Nous ne savons pas à ce stade si nous pouvons faire mieux, c'est-à-dire si tous les polynômes sont indispensables dans cette écriture de $\mathcal{I}$.

Remarque 3.11. L'inconvénient avec ce théorème est que si $|G|$ est grand, il est difficile de chercher les générateurs de $\mathcal{I}$ à la main comme nous venons de le faire. La liste fournie par le théorème de Noether (cf remarque (3.9)), n'est en général pas minimale et il est difficile d'en extraire une sous-famille minimale.

Notations 3.12. • On note $\mathcal{I}_h^+$ l'ensemble des polynômes invariants homogènes de degré strictement positif, i.e., $\mathcal{I}_h^+ = \{P \in \mathcal{I} : P \text{ est homogène de degré } d \text{ strictement positif }\}$.
• On note $\mathcal{A}$ l'idéal de $K[X_1, ..., X_n]$ engendré par $\mathcal{I}_h^+$.
Ainsi $\mathcal{A} = \{\sum_{i=1}^n P_i Q_i : n \in \mathbb{N}^*, Q_i \in \mathcal{I}_h^+, P_i \in K[X_1, ..., X_n]\}$.

Si $T \in G$, alors $T\mathcal{A} \subset \mathcal{A}$.
En effet, si $\sum_{i=1}^n P_i Q_i \in \mathcal{A}$ où $Q_i \in \mathcal{I}_h^+$, pour tout i, alors
$T(\sum_{i=1}^n P_i Q_i) = \sum_{i=1}^n T(P_i)T(Q_i) = \sum_{i=1}^n T(P_i)Q_i \in \mathcal{A}$ car $T(P_i) \in K[X_1, ..., X_n]$.

Proposition 3.13. Soit $P \in K[X_1, ..., X_n]$ tel que $P(0) = 0$.
Alors $M(P) \in \mathcal{A}$.

Démonstration. Supposons de plus que P est homogène. Notons $d > 0$ son degré. Alors $T(P)$ est également homogène de degré d quelque soit T appartenant à G (cf (2.7)).
Ainsi $M(P) = \frac{1}{|G|} \sum_{T \in G} T(P)$ est homogène de degré $d > 0$.
Comme $M(P) \in \mathcal{I}$, on a donc $M(P) \in \mathcal{I}_h^+ \subset \mathcal{A}$.

Si P n'est pas homogène, P s'écrit $P = \sum_{i=1}^m P_i$ où les P_i sont homogènes de degré $i > 0$. On applique alors ce qu'on vient de faire aux P_i et on trouve : $M(P) = \sum_{i=1}^m M(P_i) \in \mathcal{A}$.
□

Nous allons voir deux résultats qui s'appliquent dans le cas où G est un groupe fini quelconque. Ils nous serviront par la suite pour démontrer le théorème de Chevalley-Sheppard-Todd.

Proposition 3.14. Si $(f_1, ..., f_m)$ est une famille de $\mathcal{I}_h^+$ qui engendre l'idéal $\mathcal{A}$, on a $\mathcal{I} = K[f_1, ..., f_m]$.

Démonstration. On a clairement : $K[f_1, ..., f_m] \subset \mathcal{I}$ car $f_1, ..., f_m \in \mathcal{I}$.
Par récurrence forte sur d, montrons que $\mathcal{I}_d \subset K[f_1, ..., f_m]$:
Initialisation : Pour tout $P \in \mathcal{I}_0$, P est une constante et est donc un élément de $K[f_1, ..., f_m]$.
Hérédité : Soit $d > 0$. Supposons que $\mathcal{I}_k \subset K[f_1, ..., f_m]$ pour tout $k < d$.
Soit $P \in \mathcal{I}_d$. Alors $P \in \mathcal{A}$. Donc P peut s'écrire : $P = \sum_{i=1}^m P_i f_i$ où $P_i \in \mathcal{P}$.
Comme P et tous les f_i sont homogènes, on peut supposer que tous les P_i sont homogènes et alors, si $P_i \neq 0$, $\deg P_i = \deg P - \deg f_i = d - \deg f_i < d$.
En appliquant M à P, on a : $P = MP = \sum_{i=1}^m (MP_i) f_i$. Or chaque MP_i appartient à $\mathcal{I}$ et est homogène de degré $< d$. Donc par hypothèse, $MP_i \in K[f_1, ..., f_m]$ et enfin, $P \in K[f_1, ..., f_m]$. □

Théorème 3.15. *Le corps $Frac(\mathcal{I})$ a pour degré de transcendance n sur K.*

Démonstration. Voir l'annexe (paragraphe 6) pour la définition du degré de transcendance d'une extension. Pour chaque $i \in \{1, ..., n\}$, on définit $P_i = \prod_{T \in G}(TX_i - t) \in K[X_1, ..., X_n][t] \cong \mathcal{P}[t]$. Avec la propriété universelle de l'algèbre $\mathcal{P}[t]$, on prolonge l'action de G sur $\mathcal{P}$ en une action sur $\mathcal{P}[t]$ en posant $T.t = t$ pour $T \in G$.
Ainsi, P_i est invariant sous l'action de G, donc ses coefficients sont également invariants sous l'action de G. Autrement dit, $P_i \in \mathcal{I}[t]$.
De plus $P_i \neq 0$ et on remarque que $t = X_i$ est une racine de $P_i(t)$ (car $id \in G$). Cela signifie que le corps $K(X_1, ..., X_n)$ est une extension algébrique du corps $Frac(\mathcal{I})$. De plus, $Frac(\mathcal{I})$ possède des bases de transcendance sur K (6.2). Soit $\mathcal{B}$ l'une d'elles. $Frac(\mathcal{I}) \supset K(\mathcal{B})$ est algébrique.
Alors par transitivité, $K(X_1, ..., X_n) \supset K(\mathcal{B})$ est algébrique et comme $\mathcal{B}$ est une famille algébriquement indépendante sur K, $\mathcal{B}$ est une base de transcendance de $K(X_1, ..., X_n) \supset K$.
Ainsi, $card(\mathcal{B}) = n$. □

Remarque 3.16. Ce théorème entraîne notamment que $Frac(\mathcal{I})$ n'est pas réduit à K (les constantes) dès que $\dim V \geq 1$, et cela pour tout sous-groupe fini de $GL(V)$. On a que $Frac(\mathcal{I})$ est "gros", aussi gros que $K(X_1, ..., X_n)$ qui le contient.

Dans la fin de ce paragraphe 3, nous allons décrire $\mathcal{I}(G)$ quand G est fini et engendré par des pseudo-réflexions de V.

Proposition 3.17. On suppose que G est fini et engendré par des pseudo-réflexions de V.
Soient $Q_1, ..., Q_k \in \mathcal{I}$, $P_1, ..., P_k \in K[X_1, ..., X_n]$ homogènes tels que $P_1Q_1 + ... + P_kQ_k = 0$.
Alors soit $P_1 \in \mathcal{A}$, soit Q_1 appartient à l'idéal $\mathcal{B}$ de $\mathcal{I}$ engendré par $Q_2, ..., Q_k$.

Démonstration. Si $P_1 = 0$, alors $P_1 \in \mathcal{A}$.
Si $P_1 \neq 0$, nous raisonnons par récurrence forte sur le degré de P_1 :
Initialisation : Supposons que $\deg P_1 = 0$. Alors $Q_1 = -\frac{P_2}{P_1}Q_2 - ... - \frac{P_k}{P_1}Q_k$ et donc $Q_1 = M(Q_1) = -M(\frac{P_2}{P_1})Q_2 - ... - M(\frac{P_k}{P_1})Q_k \in \mathcal{B}$.
Hérédité : Soit $m \in \mathbb{N}^*$. Supposons la propriété vraie si $\deg P_1 = k$, $\forall k \leq m$. Alors si $\deg P_1 = m$, supposons que $Q_1 \notin \mathcal{B}$ et montrons que $P_1 \in \mathcal{A}$.
Soit S une pseudo-réflexion de G.
Alors $0 = S(\sum_{i=1}^k Q_iP_i) = \sum_{i=1}^k Q_iS(P_i) = \sum_{i=1}^k Q_i(P_i + (\delta_S P_i)L_S) = \sum_{i=1}^k Q_iP_i + L_S \sum_{i=1}^k Q_i\delta_S(P_i) = L_S \sum_{i=1}^k Q_i\delta_S(P_i)$.
Ainsi, par intégrité de $\mathcal{P}$, $\sum_{i=1}^k Q_i\delta_S(P_i) = 0$ et comme $\deg \delta_S(P_1) < \deg P_1$ et les $\delta_S(P_i)$ sont homogènes, par hypothèse de récurrence, $\delta_S(P_1) \in \mathcal{A}$. Donc $SP_1 - P_1 = (\delta_S P_1)L_S \in \mathcal{A}$.
Si S' est une autre pseudo-réflexion de G, alors $S'SP_1 - P_1 = S'(SP_1 - P_1) + (S'(P_1) - P_1) \in \mathcal{A}$. En répétant cette opération, on montre que $TP_1 - P_1 \in \mathcal{A}$ pour tout $T \in G$. En effet, G est engendré par des pseudo-réflexions et l'inverse de toute pseudo réflexion en est une donc tout élément de G est un produit fini de pseudo-réflexions. Ainsi, $MP_1 - P_1 = \frac{1}{|G|} \sum_{T \in G} (TP_1 - P_1)$ est également dans $\mathcal{A}$ et donc $P_1 = MP_1 - (MP_1 - P_1) \in \mathcal{A}$ par la proposition précédente. □

On sait que $\mathcal{P}$ est isomorphe à $K[X_1, ..., X_n]$ qui est noethérien par le théorème de Hilbert. En conséquence, tout idéal de $\mathcal{P}$ est engendré par un nombre fini

d'éléments, notamment $\mathcal{A} = (\mathcal{I}_h^+)$.

Il existe une famille finie $f_1, ..., f_m$ dans $\mathcal{I}_h^+$ que l'on suppose de cardinal minimal telle que $\mathcal{A} = (f_1, ..., f_m)$.

Définition 3.18. Une telle famille $f_1, ..., f_m$ est appelée une famille de générateurs basiques de $\mathcal{A}$.

Théorème 3.19. *Si G est fini et engendré par des pseudo-réflexions de V, les générateurs basiques $f_1, ..., f_m$ de $\mathcal{A}$ sont algébriquement indépendants sur K.*

Démonstration. Par l'absurde, supposons qu'il existe $g = g(Y_1, ..., Y_m) \in K[Y_1, ..., Y_m]$ non nul tel que $g(f_1, ..., f_m) = 0$. Prenons g de degré minimal.
Les f_i étant des polynômes homogènes en $X_1, ..., X_n$, chaque monôme en les f_i l'est aussi, et $g(f_1, ..., f_m)$ comme polynôme en les X_i est la somme de tels monômes qui s'annulent entre eux.
Toutes les composantes homogènes de chaque degré doivent disparaitre. Donc en considérant dans $g(f_1, ..., f_m)$ le plus petit degré en les X_i des monômes en les f_i que l'on note d, on peut supposer que $g(f_i, ..., f_m)$ se développe (avant annulation) en une somme de monômes de degré d en $X_1, ..., X_n$.
Pour $1 \leq i \leq m$, on pose $g_i = g_i(f_1, ..., f_m) = \frac{\partial g}{\partial f_i} \in \mathcal{I}$ car g est un polynôme en les f_i qui sont invariants.
Chaque g_i est soit 0, soit homogène de degré $d - \deg f_i$ en $X_1, ..., X_n$. Les g_i sont non tous nuls car g n'est pas constant.
Soit τ l'idéal de $\mathcal{I}$ engendré par $\{g_1, ..., g_m\}$. Quitte à renommer si nécessaire les g_i (i.e. quitte à renommer les f_i), on peut supposer que τ est engendré par $\{g_1, ..., g_k\}$ mais par aucun sous-ensemble strict de $\{g_1, ..., g_k\}$. Donc pour $k < i \leq m$, il existe $h_{ij} \in \mathcal{I}$ tel que $g_i = \sum_{j=1}^{k} h_{ij} g_j$.
Encore une fois, puisque l'on peut considérer les monômes de chaque degré séparément, on peut supposer que h_{ij} est homogène de degré $\deg g_i - \deg g_j$ et alors, $\deg h_{ij} = (d - \deg f_i) - (d - \deg f_j) = \deg f_j - \deg f_i$.
Puisque g (vu comme polynôme en $X_1, ..., X_n$) est nul, on a : $\frac{\partial g}{\partial X_s} = 0$ pour tout $1 \leq s \leq n$. Et alors,

$$\begin{aligned}
0 &= \sum_{i=1}^{m} \frac{\partial g}{\partial f_i} \frac{\partial f_i}{\partial X_s} = \sum_{i=1}^{m} g_i \frac{\partial f_i}{\partial X_s} \\
&= \sum_{i=1}^{k} g_i \frac{\partial f_i}{\partial X_s} + \sum_{i=k+1}^{m} (\sum_{j=1}^{k} h_{ij} g_j) \frac{\partial f_i}{\partial X_s} \\
&= \sum_{i=1}^{k} g_i \frac{\partial f_i}{\partial X_s} + \sum_{i=1}^{k} \sum_{j=k+1}^{m} h_{ji} g_i \frac{\partial f_j}{\partial X_s} \\
&= \sum_{i=1}^{k} g_i \left(\frac{\partial f_i}{\partial X_s} + \sum_{j=k+1}^{m} h_{ji} \frac{\partial f_j}{\partial X_s} \right)
\end{aligned}$$

Comme $g_1 \notin (g_2, ..., g_k)$, d'après (3.17), $\frac{\partial f_1}{\partial Y_s} + \sum_{j=k+1}^{m} h_{j1} \frac{\partial f_j}{\partial Y_s} \in \mathcal{A}$, pour tout $1 \leq s \leq n$.

Comme $\mathcal{A} = (f_1, ..., f_m)$, on peut écrire : $\frac{\partial f_1}{\partial X_s} + \sum_{j=k+1}^{m} h_{j1} \frac{\partial f_j}{\partial X_s} = \sum_{i=1}^{m} r_{is} f_i$ avec $r_{is} \in \mathcal{P}$, pour tout s et pour tout i. De plus, la fonction polynomiale de la partie gauche de l'égalité étant homogène de degré $\deg f_1 - 1$, on peut supposer que les r_{is} sont homogènes et tels que $\deg r_{is} + \deg f_i = \deg f_1 - 1$ ou $r_{is} = 0$.
On remarque alors que nécessairement $r_{1s} = 0$ (l'égalité sur les degrés ne peut être vérifiée).

En multipliant par X_s et en sommant sur tous les s, on obtient :

$$\sum_{s=1}^{n} X_s \frac{\partial f_1}{\partial X_s} + \sum_{j=k+1}^{m} h_{j1} \sum_{s=1}^{n} X_s \frac{\partial f_j}{\partial X_s} = \sum_{i=1}^{m} (\sum_{s=1}^{n} r_{is} X_s) f_i$$

Or, d'après la formule d'Euler pour les polynômes homogènes, $\sum_{s=1}^{n} X_s \frac{\partial f_j}{\partial X_s} = (\deg f_j) f_j$, donc on a :

$$(\deg f_1) f_1 + \sum_{j=k+1}^{m} h_{j1} (\deg f_j) f_j = \sum_{i=1}^{m} (\sum_{s=1}^{n} r_{is} X_s) f_i$$

Dans la partie droite de l'égalité, on a clairement que chaque coefficient $\sum_{s=1}^{n} r_{is} X_s$ est soit 0, soit de degré supérieur ou égal à 1.
Or on a : $\sum_{s=1}^{n} r_{1s} X_s = 0$.
Donc comme $f_1 \in \mathcal{I}_h^+$, $\deg f_1 \neq 0$ et $f_1 \in (f_2, ..., f_m)$ ce qui contredit le fait que m devait être minimal. □

Proposition 3.20. Si $(f_1, ..., f_m)$ est une famille de générateurs basiques de $\mathcal{A}$, on a : $\mathcal{I} = K[f_1, ..., f_m]$.

Démonstration. On applique la proposition (3.14). □

Théorème 3.21. *Le cardinal m d'une famille de générateurs basiques est égal à la dimension de V.*

Démonstration. Soit $(f_1, ..., f_m)$ une famille de $\mathcal{I}_h^+$ qui engendre l'idéal $\mathcal{A}$.
Posons $\mathcal{E} = K(X_1, ..., X_n)$ et $\mathcal{F} = K(f_1, ..., f_m)$.
Alors $K \subset \mathcal{F} \subset \mathcal{E}$ et $\mathcal{E}$ a pour degré de transcendance n sur K (une base de transcendance de $K(X_1, ..., X_n)$ sur K est $(X_1, ..., X_n)$).
Par ailleurs, le degré de transcendance de $\mathcal{F}$ sur K est m (par le théorème (3.19), la proposition (3.20) et la définition (6.1), $(f_1, ..., f_m)$ est une base de transcendance de $K(f_1, ..., f_m)$ sur K).
Montrons que $\mathcal{E}$ est une extension algébrique de $\mathcal{F}$:
pour tout $1 \leq i \leq n$, on définit $F_i \in K[X_1, ..., X_n]|X] : F_i(X) = \prod_{T \in G} (X - TX_i)$.
On a clairement que $F_i(X_i) = 0$ (facteur nul pour $T = id$). De plus, pour tout $S \in G$, on a : $(SF_i)(X) = \prod_{T \in G} (X - (ST)X_i) = F_i(X)$ car $\{ST : T \in G\} = G$.
Ainsi, les coefficients de $F_i(X)$ sont des polynômes en $X_1, ..., X_n$ qui sont invariants sous l'action de G ; autrement dit, $F_i(X) \in \mathcal{I}[X] \subset \mathcal{F}[X]$.
Donc $\mathcal{E}$ est engendré par $(X_1, ..., X_n)$ qui sont algébriques sur $\mathcal{F}$. Ceci implique que $\mathcal{E} \supset \mathcal{F}$ est une extension algébrique.
De plus, $\mathcal{F} = K(f_1, ..., f_m)$ donc par (3.19) et (6.3), $n = DegTr(\mathcal{E} : K) = m$. □

Bilan 3.22. Si $car(K) = 0$, V est un K-espace vectoriel de dimension $n \geq 1$ et $G \subset GL(V)$ est un groupe fini engendré par des pseudo-réflexions,
alors l'algèbre $\mathcal{I}$ des invariants de G est engendrée par n polynômes homogènes algébriquement indépendants, de sorte qu'elle est isomorphe à $\mathcal{P}$, et donc à $K[X_1, ..., X_n]$.
Ceci constitue l'une des implications du théorème de Chevalley-Shephard-Todd (1954-1955) :

Théorème 3.23 (CST)**.** *Soient K un corps de caractéristique nulle, V un K-espace vectoriel de dimension $n \geq 1$ et $G \subset GL(V)$ un groupe fini. Alors G est engendré par des pseudo-réflexions si et seulement si l'algèbre $\mathcal{I}$ des invariants de G est isomorphe à $K[X_1, ..., X_n]$.*

4. Séries de Molien

Dans cette section, on utilisera l'anneau $K[[t]]$ des séries formelles en t à coefficients dans K.
Pour $T \in GL(V)$, on notera $tr_d T$ la trace de $T_{|\mathcal{P}_d}$ qui est également, si $T \in G$ un sous-groupe fini de $GL(V)$, la valeur en T du caractère χ_d de la représentation de G sur $\mathcal{P}_d$.

Proposition 4.1. Si $T \in GL(V)$, alors

$$\sum_{d=0}^{\infty}(tr_d T)t^d = \det(id_V - tT^{-1})^{-1} \in K(t)$$

.

Démonstration. Notons d'abord que tous les calculs peuvent se faire matriciellement, le choix d'une base B de V fournissant une base naturelle B_d de chaque $\mathcal{P}_d$ (les monômes $\prod_{i=1}^n X_i^{a_i}, (a_1, ..., a_n) \in \mathbf{N}^n, \sum_i a_i = d$ ordonnés lexicographiquement).
On peut alors se placer sur la clôture algébrique Ω de K ; là, il existe $Q \in GL_n(\Omega)$ telle que $QAQ^{-1} = A' \in GL_n(\Omega)$ soit triangulaire (où $A = mat_B(T)$).
Il suffit alors de prouver la proposition dans le cas où $V = \Omega^n$, $K = \Omega$ et la matrice de T dans la base canonique B est triangulaire (on vérifie en effet que pour tout $d \geq 0$, A' et A induisent des endomorphismes semblables de $\mathcal{P}_d$, via (2.7)).
Si $\lambda_1, ..., \lambda_n$ sont les valeurs propres de T, alors par (2.7), $T_{|\mathcal{P}_d}$ a également une matrice triangulaire dans B_d, avec pour coefficients diagonaux $\{\prod_{i=1}^n \lambda_i^{-a_i}, (a_1, ..., a_n) \in \mathbf{N}^n, \sum_i a_i = d\}$.
En effet, pour tout $i \in \{1, ..., n\}$, $Tx_i = \lambda_i^{-1}x_i + \sum_{j<i} \mu_{ij}x_j$ où $\mu_{ij} \in K$ d'après (2.7) ($mat_B(T)^{-1}$ est triangulaire). Donc $\prod_{i=1}^n (Tx_i)^{a_i} = \prod_{i=1}^n (\lambda_i^{-1}x_i + \sum_{j<i} \mu_{ij}x_j)^{a_i} = \prod_{i=1}^n \lambda_i^{-a_i}x_i^{a_i} + S$ où S est un polynôme en les $x_1, ..., x_n$ ne contenant pas le monôme $\prod_{i=1}^n x_i^{a_i}$.
Ainsi,

$$\begin{aligned}(tr_d T)t^d &= \sum\{(\prod_{i=1}^n \lambda_i^{-a_i})t^d, (a_1, ..., a_n) \in \mathbf{N}^n, \sum_i a_i = d\} \\ &= \sum\{\prod_{i=1}^n (\lambda_i^{-1}t)^{a_i}, (a_1, ..., a_n) \in \mathbf{N}^n, \sum_i a_i = d\}\end{aligned}$$

et $\sum_{d=0}^{\infty}(tr_d T)t^d = \sum\{\prod_{i=1}^n (\lambda_i^{-1}t)^{a_i}, (a_1, ..., a_n) \in \mathbf{N}^n\}$.
Notons maintenant que $1 - \lambda_i^{-1}t$ a pour coefficient constant $1 \neq 0$. Il est donc inversible dans $K[[t]]$ d'inverse : $(1 - \lambda_i^{-1}t)^{-1} = \sum_{a=0}^{\infty}(\lambda_i^{-1}t)^a$. Donc

$$\begin{aligned}\prod_{i=1}^n (1 - \lambda_i^{-1}t)^{-1} &= \prod_{i=1}^n (\sum_{a_i=0}^{\infty} (\lambda_i^{-1}t)^{a_i}) \\ &= \sum\{\prod_{i=1}^n (\lambda_i^{-1}t)^{a_i}, (a_1, ..., a_n) \in \mathbf{N}^n\} \\ &= \sum_{d=0}^{\infty}(tr_d T)t^d\end{aligned}$$

Enfin, on remarque que $\prod_{i=1}^{n}(1-\lambda_i^{-1}t)^{-1} = \prod_{i=1}^{n}\frac{1}{1-\frac{1}{\lambda_i}t} = \prod_{i=1}^{n}\frac{\lambda_i}{\lambda_i - t} = \frac{\det T}{\det(T-t1)} = \frac{\det T}{\det(T(id_V - tT^{-1}))} = \frac{1}{\det(id_V - tT^{-1})}$. □

Corollaire 4.2. $\sum_{d=0}^{\infty}(\dim \mathcal{P}_d)t^d = (1-t)^{-n}$

Démonstration. On applique la proposition précédente avec $T = 1$. □

Corollaire 4.3. La dimension de $\mathcal{P}_d$ est $\binom{n+d-1}{d}$, pour tout d.

Démonstration. Par récurrence sur n :
Initialisation : si $n = 1$, par la proposition précédente, $\sum_{d=0}^{\infty}(\dim \mathcal{P}_d)t^d = (1-t)^{-1}$. Or $(1-t)^{-1} = \sum_{d\geq 0} t^d$. Donc en identifiant les coefficients devant t^d, pour tout $d \geq 0$, on a : $\dim \mathcal{P}_d = 1 = \binom{d}{d}$.
Hérédité : Supposons la proposition vraie pour un certain $n \geq 1$. En dérivant formellement n fois l'expression $(1-t)^{-1} = \sum_{d\geq 0} t^d$, on obtient :

$$\frac{n!}{(1-t)^{n+1}} = \sum_{k\geq 0}(k+n)(k+n-1)...(k+1)t^k$$

$$\frac{1}{(1-t)^{n+1}} = \sum_{k\geq 0}\frac{1}{n!}(k+n)...(k+1)t^k$$

Donc par la proposition précédente, $\dim \mathcal{P}_d = \frac{(d+n)...(d+1)}{n!} = \frac{(n+d)!}{d!n!} = \binom{n+d}{d}$. □

Lemme 4.4. Soit W un sous-espace de V et p une projection de V sur W (i.e. $p(V) = W$ et $p^2 = p$).
Alors $\dim W = tr(p)$.

Démonstration. On a : $p_{|W} = id_W$. De plus, si on pose $W' = (id-p)(V) = \{v - p(v), v \in V\}$, alors W' est un complémentaire de W.
Donc $V = W \bigoplus W'$ et $p_{|W'} = 0$.
Soient $B = (w_1, ..., w_r)$ une base de W et $B' = (w'_1, ..., w'_s)$ une base de W'. Soit $\mathcal{B}$ la concaténation de ces deux bases ($\mathcal{B}$ est une base de V).
Alors $mat(p, \mathcal{B}) = \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & \cdots & 0 \\ 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}$ et $\dim W = tr(p)$. □

Définition 4.5. Soient G un sous-groupe fini de $GL(V)$ et $\mathcal{I}$ l'algèbre des invariants de G. On définit la série de Molien de G par :

$$\phi(t) = \phi_G(t) = \sum_{d=0}^{\infty}(\dim \mathcal{I}_d)t^d$$

Exemple 4.6. Pour le groupe trivial $G = \{1_G\}$, on a : $\phi(t) = (1-t)^{-n} = \sum_{d=0}^{\infty} \binom{n+d-1}{d} t^d$

Proposition 4.7. Si G est un sous-groupe fini de $GL(V)$, alors

$$\dim \mathcal{I}_d = \frac{1}{|G|} \sum_{T \in G} tr_d T = \frac{1}{|G|} \sum_{T \in G} \chi_d(T)$$

.

Démonstration. On a vu que l'opérateur M est une projection de $\mathcal{P}_d$ sur $\mathcal{I}_d$, pour chaque degré d. Donc par la proposition précédente, on a :
$\dim \mathcal{I}_d = tr(M_{|\mathcal{P}_d}) = tr(\frac{1}{|G|} \sum_{T \in G} T_{|\mathcal{P}_d}) = \frac{1}{|G|} \sum_{T \in G} tr_d T = \frac{1}{|G|} \sum_{T \in G} \chi_d(T)$. □

Théorème 4.8 (Molien, 1897)**.** *Si G est un sous-groupe fini de $GL(V)$, alors sa série de Molien est $\phi(t) = \frac{1}{|G|} \sum_{T \in G} \det(1-tT)^{-1}$.*
La "formule de Molien" est la suivante :

$$\sum_{d=0}^{\infty} (\dim \mathcal{I}_d) t^d = \frac{1}{|G|} \sum_{T \in G} \det(1-tT)^{-1}$$

.

Démonstration. En appliquant les propositions (4.1) et (4.7),
$\phi(t) = \sum_{d=0}^{\infty} (\dim \mathcal{I}_d) t^d = \sum_{d=0}^{\infty} \frac{1}{|G|} (\sum_{T \in G} tr_d T) t^d = \frac{1}{|G|} \sum_{T \in G} (\sum_{d=0}^{\infty} (tr_d T) t^d) = \frac{1}{|G|} \sum_{T \in G} \det(1-tT^{-1})^{-1} = \frac{1}{|G|} \sum_{T \in G} \det(1-tT)^{-1}$ (car $\{T^{-1} : T \in G\} = G$). □

Exemple 4.9. Le groupe diédral D_3
On pose $G = D_3 = \{id, r, r^2, s, sr, sr^2\}$ où r est la rotation d'angle $2\pi/3$ centrée en O et s est la symétrie orthogonale par rapport à l'axe (Ox).
On prend ici $K = \mathbf{R}$ et $V = \mathbf{R}^2$.
On identifie chaque élément de D_3 à sa matrice dans $GL_2(\mathbf{R})$.
On a 3 classes de conjugaison : $\{id\}$, $\{s, sr, sr^2\}$ et $\{r, r^2\}$. De plus, on sait que la trace et le déterminant d'une matrice sont invariants par changement de base donc constants sur les classes de conjugaison.
Si $T = id_V$, $\det(id_V - tT)^{-1} = \frac{1}{(1-t)^2}$.
Si $T = s$, $mat(id_V - tT) = \begin{pmatrix} 1-t & 0 \\ 0 & 1+t \end{pmatrix}$. Donc $\det(id - tT)^{-1} = \frac{1}{(1-t)(1+t)} = \frac{1}{1-t^2}$.
Si $T = r$, $mat(id_V - tT) = \begin{pmatrix} 1 - t\cos(2\pi/3) & t\sin(2\pi/3) \\ -t\sin(2\pi/3) & 1 - t\cos(2\pi/3) \end{pmatrix} = \begin{pmatrix} 1+t/2 & t\sqrt{3}/2 \\ -t\sqrt{3}/2 & 1+t/2 \end{pmatrix}$.
Donc $\det(id - tT)^{-1} = \frac{1}{(1+t/2)^2 + 3t^2/4} = \frac{1}{1+t+t^2/4+3t^2/4} = \frac{1}{1+t+t^2}$.
Ainsi, $\phi(t) = \frac{1}{6}(\frac{1}{(1-t)^2} + \frac{3}{1-t^2} + \frac{2}{1+t+t^2})$.
En développant en série formelle, on obtient pour coefficients :
1 0 1 1 1 1 2 1 2 2 2 2 3 2 3 3 3 3 ... (les coefficients forment des paquets de 6 du type : n $n-1$ n n n n).

Exemple 4.10. Soit m un entier supérieur ou égal à 3.
Nous allons dans cet exemple calculer la série de Molien du groupe cyclique $G = C_m$ qui agit diagonalement sur $\mathbf{C}^2$ via le morphisme :

$$\begin{array}{rccc} \psi & : & \mathbf{Z}/m\mathbf{Z} & \to & GL_2(\mathbf{C}) \\ & & \bar{k} & \mapsto & A^k \end{array}$$

où $A = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$ et $\zeta = \exp(2i\pi/m)$.
(Cette formule nous servira pour le calcul de la série de Molien du groupe diédral D_m de l'exemple suivant).
Alors $S \in \mathbf{C}[X,Y]$ est dans $\mathcal{I}(C_m)$ si et seulement si $S(A\begin{pmatrix} X \\ Y \end{pmatrix}) = S$ si et seulement si $S(\zeta X, \zeta^{-1}Y) = S(X,Y)$.
Notons $S = \sum_{i=0}^{r_1}\sum_{j=0}^{r_2} a_{ij}X^iY^j$ avec $a_{ij} \in \mathbf{C}$.
Alors S est invariant si et seulement si

$$\sum_{i=0}^{r_1}\sum_{j=0}^{r_2} a_{ij}\zeta^{i-j}X^iY^j = \sum_{i=0}^{r_1}\sum_{j=0}^{r_2} a_{ij}X^iY^j$$

En identifiant les coefficients des deux côtés, la condition devient : $\zeta^{i-j} = 1$ pour tout i,j.
C'est-à-dire, $i - j \equiv 0[m]$ pour tout i,j tels que $a_{ij} \neq 0$.
Donc S n'est formé que de monômes de la forme : $a_{ij}X^iY^j$ où $i-j \equiv 0[m]$. De tels monômes appartiennent à $\mathbf{C}[XY, X^m, Y^m]$. Et on a XY, X^m et Y^m appartiennent à $\mathcal{I}(C_m)$.
D'où $\mathcal{I}(C_m) = \mathbf{C}[XY, X^m, Y^m]$.
On a alors pour tout $d \in \mathbf{N}$, $\mathcal{I}_d = \oplus_{k=0}^{m-1}\mathbf{C}[X^m,Y^m]_{d-k}(XY)^k$ (il s'agit de faire une partition des monômes X^iY^j de degré d en X,Y, dont les exposants i,j ont même reste mod m, en fonction de ce reste "k").
Alors la série de Molien associée est la somme de $k=0$ à $m-1$ des séries $S_k(t) = \sum_{d\geq 0} m_{k,d}t^d$, où $m_{k,d}$ désigne la dimension de $\mathcal{P}_d \cap C[X^m,Y^m](XY)^k$.
Alors il vient que $m_{k,d}$ est la dimension du sous-espace vectoriel des polynômes homogènes de degré $d-2k$ dans $\mathbf{C}[X^m,Y^m]$, qui vaut soit 0 , soit $1+(d-2k)/m$ dans le cas où m divise $d-2k$ (cf (4.3) avec $n=2$).
On obtient ainsi que $S_k(t) = \sum_{j\geq 0}(j+1)t^{mj+2k} = t^{2k}/((1-t^m)^2)$.
Alors la série de Molien de C_m est :

$$\begin{aligned} S(t) &= \sum_{k=0}^{m-1} S_k(t) = \sum_{k=0}^{m-1} \frac{t^{2k}}{(1-t^m)^2} \\ &= \frac{1-t^{2m}}{(1-t^2)(1-t^m)^2} \\ &= \frac{1+t^m}{(1-t^2)(1-t^m)} \end{aligned}$$

Exemple 4.11. Soit m un entier supérieur ou égal à 3. Prenons, $K = \mathbf{C}$ et $G = D_m$ le groupe diédral d'ordre $2m$.
Considérons la représentation naturelle ρ de G dans $\mathbf{C}^2$, qui est fidèle et identifions D_m à cette image. Ce qui revient à prendre G le sous-groupe de $GL_2(\mathbf{C})$ engendré par les matrices :

$$S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ et } T = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} \text{ où } \zeta = e^{2i\pi/m}$$

Notons que cette représentation de D_m est équivalente à sa représentation usuelle définie sur $\mathbf{R}$ comme groupe d'isométrie de $\mathbf{R}^2$.

On a en effet en utilisant la matrice $C = \frac{1}{\sqrt{2}}\begin{pmatrix} -i & 1 \\ -i & -1 \end{pmatrix}$ comme matrice de changement de base, que $CTC^{-1} = \begin{pmatrix} \cos(2\pi/m) & -\sin(2\pi/m) \\ \sin(2\pi/m) & \cos(2\pi/m) \end{pmatrix}$ et $CSC^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.
Les $2m$ éléments de G sont : les matrices T^j pour $0 \leq j \leq m-1$ et $\begin{pmatrix} 0 & \zeta^j \\ \zeta^{-j} & 0 \end{pmatrix}$ pour $0 \leq j \leq m-1$.
La série de Molien de G est :

$$\phi(t) = \frac{1}{2m}\left(\frac{m}{1-t^2} + \sum_{j=0}^{m-1} \frac{1}{1-2t\cos(2\pi j/m)+t^2}\right)$$

Par (4.8), on reconnaît que $\frac{1}{m}\left(\sum_{j=0}^{m-1} \frac{1}{1-2t\cos(2\pi j/m)+t^2}\right)$ est la série de Molien du sous-groupe $< T >$, calculée en (4.10).
On a donc :

$$\phi(t) = \frac{1}{2}\left(\frac{1}{1-t^2} + \frac{1+t^m}{(1-t^2)(1-t^m)}\right) = \frac{1}{(1-t^2)(1-t^m)} = \sum_{d\geq 0} a(d)t^d$$

où pour tout $d \geq 0$, $a(d) = card\{(x,y) \in \mathbf{N}^2, 2x+my = d\}$.
Un polynôme P appartient à $\mathcal{I}$ si et seulement si

$$P(X,Y) = P(Y,X) = P(\zeta X, \zeta^{-1}Y)$$

Ainsi, les polynômes $P = XY$ et $Q = X^m + Y^m$ appartiennent à $\mathcal{I}$.
On voit facilement que les polynômes P et Q sont algébriquement indépendants sur $\mathbf{C}$ (donc sur tout sous-corps de $\mathbf{C}$). $(*)$
En effet, $U = X^m$ et $V = Y^m$ le sont. Donc $UV = P^m$ et $U + V = Q$ le sont aussi. Si $\Phi \in \mathbf{C}[Z,T]$ non nul vérifiait $\Phi(P,Q) = 0$, le polynôme $\Psi = \prod_{j=0}^{m-1} \Phi(\zeta^j Z, T)$ appartiendrait à $\mathbf{C}[Z,T]$ et serait de la forme $\Omega(Z^m, T)$ avec $\Omega \in \mathbf{C}[X_1, X_2]$ non nul, et on aurait $0 = \Psi(P,Q) = \Omega(P^N, Q)$, ce qui est impossible (voir remarque (6.7) pour un autre argument).
L'ensemble $\mathcal{J} = \mathbf{C}[P,Q]$ est une sous-algèbre de $\mathbf{C}[X_1, X_2]$. En notant $\mathcal{J}_d$, $d \in \mathbf{N}$ les composantes homogènes de $\mathcal{J}$, le fait $(*)$ et l'homogénéité de P et Q montrent que pour tout d, $\dim(\mathcal{J}_d) = card\{(x,y) \in \mathbf{N}^2, \deg(P^xQ^y) = d\} = card\{(x,y) \in \mathbf{N}^2, 2x+my = d\} = a(d)$, et comme $\mathcal{J}_d \subset \mathcal{I}_d$, on en déduit que $\mathcal{J}_d = \mathcal{I}_d$ pour tout $d \geq 0$.
En conclusion, $\mathcal{I} = \mathbf{C}[P,Q]$ et $P = XY$ et $Q = X^m + Y^m$ sont algébriquement indépendants sur $\mathbf{C}$.

Remarque 4.12. Notons que le fait que $\mathcal{I}$ possède deux générateurs homogènes algébriquement indépendants résulte aussi de (3.22), puisque :
Le groupe D_m est engendré par des réflexions de $\mathbf{C}^2$.

En effet, S et $TS = \begin{pmatrix} 0 & \zeta \\ \zeta^{-1} & 0 \end{pmatrix}$ sont des matrices de réflexions de $\mathbf{C}^2$, et on a $< S, TS >=< S, T >$. En fait, le groupe D_m possède exactement m réflexions, de matrices les $T^jS = \begin{pmatrix} 0 & \zeta^j \\ \zeta^{-j} & 0 \end{pmatrix}$, pour $1 \leq j \leq m$.

5. Fin de la preuve du théorème de Chevalley-Shephard-Todd

Nous allons à présent montrer l'autre implication du théorème de Chevalley-Shephard-Todd. On suppose donc désormais que :

(H) : G est un sous-groupe fini de $GL(V)$ satisfaisant : $\mathcal{I} = K[f_1, ..., f_n]$ où $f_1, ..., f_n$ sont des générateurs basiques (cf (3.18)) et algébriquement indépendants sur K.

Notons que le nombre de générateurs basiques n est égal à la dimension de V (en effet, la preuve de (3.21) ne dépend que des conclusions des résultats (3.19) et (3.20) que nous supposons ici vérifiées).
On peut supposer que $\deg f_i = d_i$, avec $1 \leq d_1 \leq d_2 \leq ... \leq d_n$.
On remarque alors que pour chaque dimension d,
$\{\prod_{i=1}^n f_i^{a_i} : (a_1, ..., a_n) \in \mathbf{N}^n, \sum_i a_i d_i = d\}$ est une base du K-espace vectoriel $\mathcal{I}_d$.

Proposition 5.1. Sous l'hypothèse (H), la série de Molien de G est donnée par :

$$\phi(t) = \prod_{i=1}^{n} (1 - t^{d_i})^{-1}$$

Démonstration. $\prod_{i=1}^n (1 - t^{d_i})^{-1} = \prod_{i=1}^n (1 + t^{d_i} + t^{2d_i} + ...) = \sum_{d=0}^{\infty} \alpha_d t^d$
où $\alpha_d = |\{(a_1, ..., a_n) \in \mathbf{N}^n, \sum_i a_i d_i = d\}| = \dim(\mathcal{I}_d)$ par la remarque précédant la proposition. □

Remarque 5.2. Les générateurs basiques $f_1, ..., f_n$ ne sont en général pas uniques. C'est pourquoi la proposition suivante peut paraître surprenante.

Proposition 5.3. Les degrés $d_1, ..., d_n$ des générateurs basiques sont uniquement déterminés par G.

Démonstration. En plus des hypothèses déjà faites sur $\mathcal{I}$, supposons que $\mathcal{I} = K[f'_1, ..., f'_n]$ où $\{f'_1, ..., f'_n\}$ sont homogènes, algébriquement indépendants et $\deg f'_i = d'_i$ avec $d'_1 \leq d'_2 \leq ... \leq d'_n$.
On a : $\prod_{i=1}^n (1 - t^{d_i})^{-1} = \prod_{i=1}^n (1 - t^{d'_i})^{-1}$ (cf (5.1)). Alors d_1 et d'_1 sont tous les deux le degré du premier terme non constant dans la série de Molien de G. Donc $d_1 = d'_1$.
Ensuite, en multipliant les deux membres de l'égalité ci-dessus par $(1 - t^{d_1})$, on obtient : $\prod_{i=2}^n (1 - t^{d_i})^{-1} = \prod_{i=2}^n (1 - t^{d'_i})^{-1}$. On conclut par récurrence. □

Si $T \in GL(V)$ a pour valeurs propres $\lambda_1, ..., \lambda_n$, alors $\det(id_V - tT) = \prod_{i=1}^n (1 - \lambda_i t) \in K[t]$.
En particulier, si T est une pseudo-réflexion, $\det(id_V - tT) = (1 - \zeta t)(1 - t)^{n-1}$ où $\zeta \neq 1$, $\zeta \in K$.
De plus, on a bien sûr que : si $T = id_V$, $\det(id_V - tT) = (1 - t)^n$.
Inversement, si $T \in GL(V)$ est tel que $\det(id_V - tT)$ a $(1 - t)^{n-1}$ pour diviseur, alors $\frac{\det(id_V - tT)}{(1-t)^{n-1}} = (1 - \zeta t)$ où ζ est une valeur propre de T. Donc T a pour valeur propre 1 avec multiplicité $\geq n - 1$ et ζ. Donc $T = id_V$ (si $\zeta = 1$) ou T est une pseudo-réflexion (si $\zeta \neq 1$).

Proposition 5.4. Sous l'hypothèse (H), on a :

$$|G| = \prod_{i=1}^{n} d_i$$

Démonstration. Pour chaque $T \neq id_V$ dans G, on définit $h_T(t) = \frac{(1-t)^{n-1}}{\det(id_V - tT)} \in K[[t]]$. On utilise les facteurs $(1-t)$ pour compenser tous les facteurs de $\det(id_V - tT)^{-1}$ résultant de la valeur propre 1.
Alors, si T n'est pas une pseudo-réflexion, $h_T(1) = 0$ et si T est une pseudo-réflexion, $h_T(t) = \frac{1}{(1-\zeta t)}$ où $\zeta \neq 1$. Donc $h_T(1) = \frac{1}{(1-\zeta)}$.
Ensuite, $(1+t+t^2+...+t^{d_i-1})(1-t) = 1-t^{d_i}$. D'où $\frac{1-t}{1-t^{d_i}} = \frac{1}{1+t+t^2+...+t^{d_i-1}}$. Par le théorème de Molien (4.8) et la proposition (5.1), on a :

$$\prod_{i=1}^{n}(1-t^{d_i})^{-1} = \frac{1}{|G|}\sum_{T\in G}\det(1-tT)^{-1}$$

En multipliant les deux côtés de cette égalité par $(1-t)^n$, on obtient :

$$\prod_{i=1}^{n}(1+t+t^2+...+t^{d_i-1})^{-1} = \frac{1}{|G|}(1+\sum_{T\in G, T\neq id_V}(1-t)h_T(t))$$

En évaluant en $t=1$, on a : $\prod_{i=1}^{n} d_i^{-1} = |G|^{-1}$. □

Proposition 5.5. Sous l'hypothèse (H), le nombre r de pseudo-réflexions appartenant à G est

$$r = \sum_{i=1}^{n}(d_i - 1)$$

.

Démonstration. Pour chaque $T \in G$ qui n'est ni id_V, ni une pseudo-réflexion, on définit $g_T(t) = (1-t)^{n-2}\det(id_V - tT)^{-1} \in K[[t]]$. Le numérateur de cette fraction permet de compenser chaque facteur de la forme $(1-t)$ résultant de la valeur propre 1 de T.
Ainsi, $g_T(1)$ est bien défini.
Notons que si $S \in G$ est une pseudo-réflexion, $\det S = \zeta$ est sa valeur propre différente de 1 et on a $(1-t)^n \det(id_V - tS)^{-1} = \frac{1-t}{1-\zeta t}$.
Pour le calcul suivant, j'abrège "pseudo-réflexion" par "pr" et je note ζ_T la valeur propre de T différente de 1 lorsque T est une pseudo-réflexion. D'après la preuve

précédente,

$$\begin{aligned}\prod_{i=1}^{n}(1+t+t^2+...+t^{d_i-1})^{-1} &= \frac{1}{|G|}\left(1+\sum_{T\in G,T\neq id_V}(1-t)h_T(t)\right)\\ &= \frac{1}{|G|}\left(1+\sum_{T\in G,T\neq id_V}(1-t)\frac{(1-t)^{n-1}}{\det(id_V-tT)}\right)\\ &= \frac{1}{|G|}\left(1+\sum_{T\in G,T\neq id_V}\frac{(1-t)^{n}}{\det(id_V-tT)}\right)\\ &= \frac{1}{|G|}\left(1+\sum_{T\in G,Tpr,\zeta_T=-1}\frac{1-t}{1+t}+\sum_{T\in G,Tpr,\zeta_T\neq -1}\frac{1-t}{1-\zeta_T t}\right.\\ &\left.+\sum(1-t)^2 g_T(t) : T\in G, T\neq id_V \text{ et T n'est pas une pr}\right)\end{aligned}$$

Pour les pseudo-réflexions telles que $\zeta_T \neq -1$, on a également $\zeta_T^{-1} \neq -1$ donc :

$$\sum_{T\in G,Tpr,\zeta_T\neq -1}\frac{1-t}{1-\zeta_T t}=\frac{1}{2}\sum_{T\in G,Tpr,\zeta_T\neq -1}\left(\frac{1-t}{1-\zeta_T t}+\frac{1-t}{1-\zeta_T^{-1}t}\right)$$

On dérive les deux membres de l'équation précédente par rapport à t.

Il est facile de montrer par récurrence sur $n \geq 1$ que

$$(\prod_{i=1}^{n} f_i)' = \sum_{i=1}^{n} f_{i'}(\prod_{j=1,j\neq i}^{n} f_j)$$

A gauche, on obtient :

$$\left(\sum_{i=1}^{n}-\frac{1+2t+...+(d_i-1)t^{d_i-2}}{(1+t+...+t^{d_i-1})^2}\prod_{j=1,j\neq i}^{n}(1+t+...+t^{d_j-1})^{-1}\right)$$

Ensuite, à droite on obtient :

$$\frac{1}{|G|}\left(\sum_{T\in G,Tpr,\zeta_T=-1}\frac{-(1+t)-(1-t)}{(1+t)^2}\right.$$

$$+\frac{1}{2}\left(\sum_{T\in G,Tpr,\zeta_T\neq -1}\frac{-(1-\zeta_T t)+\zeta_T(1-t)}{(1-\zeta_T t)^2}+\frac{-(1-\zeta_T^{-1}t)+\zeta_T^{-1}(1-t)}{(1-\zeta_T^{-1}t)^2}\right)$$

$$\left.+(1-t)\sum(1-t)g_T'(t)-2g_T(t) : T\in G, T\neq id_V \text{ et T n'est pas une pr}\right)$$

Pour $t = 1$, on a pour la partie gauche :

$$\sum_{i=1}^{n} -\frac{(d_i-1)d_i}{2d_i^2} \prod_{j=1, j\neq i}^{n} d_j^{-1} = \sum_{i=1}^{n} -\frac{d_i-1}{2d_i} \prod_{j=1, j\neq i}^{n} d_j^{-1} = \sum_{i=1}^{n} -\frac{d_i-1}{2} \prod_{j=1}^{n} d_j^{-1}$$

$$= \frac{1}{|G|} \sum_{i=1}^{n} -\frac{d_i-1}{2} \text{ (cf (5.4))}$$

et pour la partie droite :

$$\frac{1}{|G|}\Big(\sum_{T\in G, Tpr, \zeta_T=-1} \frac{-1}{2} + \frac{1}{2}\Big(\sum_{T\in G, Tpr, \zeta_T\neq -1} (-1)\Big)\Big) = \frac{-r}{2|G|}$$

.

Donc en simplifiant par $-\frac{1}{2|G|}$, on obtient :

$$r = \sum_{i=1}^{n} (d_i - 1)$$

□

Corollaire 5.6. Sous l'hypothèse (H), si $G \neq \{id_V\}$, G contient au moins une pseudo-réflexion.

Démonstration. Si $G \neq \{id_V\}$, G contient au moins deux éléments. Donc par (5.4), $|G| = \prod_{i=1}^{n} d_i \geq 2$. Donc un des d_i est supérieur ou égal à 2 et donc $r = \sum_{i=1}^{n}(d_i - 1) \geq 1$. □

On peut finalement prouver la seconde implication du théorème CST :

Théorème 5.7. *Supposons que G est un sous-groupe fini de $GL(V)$ tel que $\mathcal{I}$ soit isomorphe à une algèbre de polynômes : $\mathcal{I} = K[f_1, ..., f_n]$, où les polynômes $f_1, ..., f_n$ sont homogènes et algébriquement indépendants. Alors G est engendré par des pseudo-réflexions.*

Démonstration. On note $d_i = \deg f_i$ pour chaque $1 \leq i \leq n$.
Soit H le sous-groupe de G engendré par toutes les pseudo-réflexions de G. Notons $\mathcal{I}_H$ l'ensemble des éléments invariants sous l'action de H.
Alors d'après le bilan que nous avons dressé en fin de partie 3., il existe $g_1, ..., g_n \in \mathcal{P}$ homogènes, invariants sous l'action de H et algébriquement indépendants tels que :

$$\mathcal{I}_H = K[g_1, ..., g_n]$$

Notons $d'_j = \deg g_j$ pour chaque $1 \leq j \leq n$.
On a clairement $\mathcal{I} \subset \mathcal{I}_H$ donc chaque f_i est un polynôme en les g_j.
Puisque les f_i et les g_j sont algébriquement indépendants, le déterminant Jacobien $\det(\partial f_i/\partial g_j)$ est non nul (cf (6.6)). Par conséquent, il existe π une permutation de $\{1, ..., n\}$ telle que :

$$\frac{\partial f_{\pi(1)}}{\partial g_1} \frac{\partial f_{\pi(2)}}{\partial g_2} ... \frac{\partial f_{\pi(n)}}{\partial g_n} \neq 0$$

Cela signifie que pour chaque $i \in \{1, ..., n\}$, g_i apparaît dans $f_{\pi(i)}(g_1, ..., g_n)$ (sinon l'expression ci-dessus serait nulle). En conséquence, $d'_i = \deg g_i \leq d_{\pi(i)} = \deg f_{\pi(i)}$. Notons r le nombre de pseudo-réflexions dans G et a fortiori dans H. Par la proposition (5.5), on a

$$r = \sum_{i=1}^{n}(d_i - 1) = \sum_{i=1}^{n}(d_{\pi(i)} - 1)$$

et aussi :

$$r = \sum_{i=1}^{n}(d'_i - 1)$$

Puisque $d'_i \leq d_{\pi(i)}$, on a $d'_i = d_{\pi(i)}$ pour chaque entier i.
Donc par la proposition (5.4), $|G| = \prod_{i=1}^{n} d_i = \prod_{i=1}^{n} d'_i = |H|$.
Ainsi $G = H$.

□

Exemple 5.8. Reprenons l'exemple présenté en (3.5) et (3.10) où nous avions laissé en suspens la question suivante : est-ce que les trois polynômes sont indispensables pour engendrer l'algèbre $\mathcal{I}$: $\mathcal{I} = K[X^2 + Y^2, X^3Y - XY^3, X^2Y^2]$?
Notons $f_1 = X^2 + Y^2$, $f_2 = X^3Y - XY^3$ et $f_3 = X^2Y^2$.
Le théorème CST nous fournit désormais une réponse :
Si on note f'_1 et f'_2 deux polynômes quelconques parmi ces trois polynômes, s'ils engendraient $\mathcal{I}$, alors par (6.4), on pourrait en extraire une base de transcendance de $Frac(\mathcal{I})$ sur K. Or, par (3.15), une telle base a pour cardinal $2 = \dim V$. Donc ce serait $\{f'_1, f'_2\}$ qui du coup, serait algébriquement libre d'une part et vérifierait $\mathcal{I} = K[f'_1, f'_2]$ d'autre part. Et ainsi, $\mathcal{I}$ serait une algèbre de polynôme et par CST, G serait engendré par des pseudo-réflexions. Ce n'est pas le cas car le déterminant de A vaut 1.
En conclusion, la famille des trois générateurs est minimale et de cardinal minimal.
D'après Grove-Benson, *Finite Reflection Groups* - Second Edition, exercice 7.14 page 122, on a : $f_1^2 f_3 - 4f_3^2 - f_2^3 = 0$.
Ainsi, on a f'_3 est algébrique sur $K[f'_1, f'_2]$, pour toute numérotation des trois.

Définition 5.9. Un sous-groupe G de $GL(V)$ est dit effectif si $V^G = \{0\}$ où $V^G = \{v \in V, \forall T \in G, Tv = v\}$.

Proposition 5.10. Si $V^G = \{0\}$, G n'a pas d'invariant de degré 1.

Démonstration. En effet, si χ désigne le caractère de la représentation de G dans V, on sait que celui de la représentation $\mathcal{I}_1 = V^*$ est $\bar{\chi}$, et que $\dim \mathcal{I}_1 =< \bar{\chi}, 1 >= \dim V^G = 0$. □

Proposition 5.11. Si $K = \mathbf{R}$, $G \subset \mathcal{O}(V)$ et $V^G = \{0\}$, alors $\mathcal{I}_2 \neq \{0\}$ et G possède un générateur basique de degré 2 : on a $d_1 = 2$ et on peut choisir $f_1 : v \mapsto < v, v >$ (carré de la norme euclidienne sur V).

Démonstration. En se plaçant dans une base orthonormée de V, le polynôme $Q = \sum_{i=1}^{n} X_i^2$ est un invariant puisque $G \subset \mathcal{O}(V)$ et une isométrie préserve la distance à l'origine.
Si $f_1, ..., f_r$ sont des générateurs basiques de $\mathcal{I}$, alors Q s'écrit comme polynôme

en ces générateurs. En prenant les composantes homogènes de cette expression, on peut ne garder que celle de degré 2 ; or on sait que $d_1 > 1$ (proposition précédente), donc les monômes de degré 2 en les f_i sont forcément juste des $a_i f_i$ où $a_i \in \mathbf{R}$. On ne garde que ceux tels que a_i est non nul (il y en a au moins un car $Q \neq 0$). Alors Q est la somme de ces $a_i f_i$, avec f_i homogène de degré 2. On peut alors décider de remplacer l'un de ces f_i par Q dans la famille $\{f_1, ..., f_r\}$ car un tel f_i est combinaison linéaire de Q et des autres f_j. □

Conséquence 5.12. Si $m \geq 3$ et G est le groupe diédral D_m vu comme groupe d'isométrie de $\mathbf{R}^2$, G est un groupe effectif, puisque 1 n'est pas valeur propre des rotations d'ordre m. On a donc :

$$d_1 = 2 \text{ et on peut prendre } f_1 = X^2 + Y^2$$

Si G est le groupe des isométries du cube, G est un groupe effectif puisque la représentation associée est irréductible non triviale (on calcule ainsi que $< \chi, 1 >= 0 = \dim V^G$). On a donc :

$$d_1 = 2 \text{ et on peut prendre } f_1 = X^2 + Y^2 + Z^2$$

Nous allons à présent traiter plus précisément ces deux exemples.

Exemple 5.13. Reprenons l'exemple du groupe diédral d'ordre $2m$ agissant sur $\mathbf{C}^2$ (4.11). On rappelle que les matrices :

$$S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ et } T = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} \text{ où } \zeta = e^{2i\pi/m}$$

engendrent D_m. Et à l'exemple (4.11), nous avions établi que $\mathcal{I} = \mathbf{C}[P, Q]$ où $P = X_1 X_2$ et $Q = X_1^m + X_2^m$. Nous allons ici faire un changement de base de $V = \mathbf{C}^2$. On obtiendra une expression P_1 et Q_1 de P et Q dans les nouvelles coordonnées $(Y_i)_i$. Ce changement de variable nous ramène au plongement usuel de D_m comme groupe des isométries de $\mathbf{R}^2$: en effet, si C^{-1} est notre matrice de changement de base, la matrice $S' = CSC^{-1}$ est la matrice réelle dans $B' = (e'_1, e'_2)$, base orthonormée de $\mathbf{R}^2$, de la symétrie orthogonale par rapport à e'_1, et la nouvelle matrice $T' = CTC^{-1}$ est celle de la rotation d'angle $2\pi/m$.

On utilise la matrice $C = \frac{1}{\sqrt{2}} \begin{pmatrix} -i & 1 \\ -i & -1 \end{pmatrix}$ pour effectuer un changement de variable :

$$C \begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix} = \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}$$

Ce qui équivaut à :

$$\begin{cases} X_1 &= (1/\sqrt{2})(-iY_1 + Y_2) \\ X_2 &= (1/\sqrt{2})(-iY_1 - Y_2) \end{cases}$$

Donc

$$\begin{aligned} P &= X_1 X_2 \\ &= (1/\sqrt{2})(-iY_1 + Y_2)(1/\sqrt{2})(-iY_1 - Y_2) \\ &= -\frac{1}{2}(Y_1^2 + Y_2^2) \end{aligned}$$

et

$$\begin{aligned}Q &= (1/\sqrt{2}^m)(-iY_1+Y_2)^m + (1/\sqrt{2}^m)(-iY_1-Y_2)^m \\ &= (1/\sqrt{2}^m)\Big(\sum_{j=0}^{m}\binom{m}{j}Y_2^j(-iY_1)^{m-j} + (-1)^m\sum_{j=0}^{m}\binom{m}{j}Y_2^j(iY_1)^{m-j}\Big) \\ &= (1/\sqrt{2}^m)(-1)^m\Big(\sum_{j=0}^{m}(1+(-1)^j)\binom{m}{j}Y_2^j(iY_1)^{m-j}\Big)\end{aligned}$$

Donc si m est pair : $m = 2p$, alors

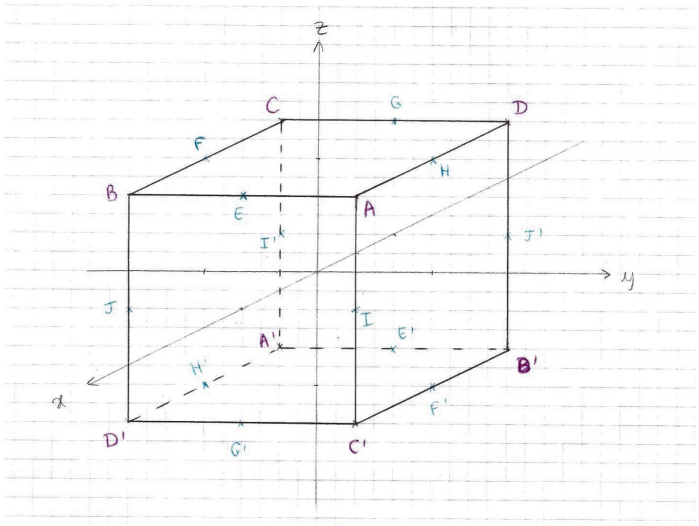
$$\begin{aligned}Q &= (2/\sqrt{2}^m)\Big(\sum_{j=0}^{m/2}\binom{m}{2j}Y_2^{2j}(-i)^{2(p-j)}Y_1^{m-2j}\Big) \\ &= (2/\sqrt{2}^m)\Big(\sum_{j=0}^{m/2}\binom{m}{2j}Y_2^{2j}(-1)^{p-j}Y_1^{m-2j}\Big)\end{aligned}$$

et si m est impair : $m = 2p+1$, alors

$$\begin{aligned}Q &= (2/\sqrt{2}^m)\Big(-\sum_{j=0}^{(m-1)/2}\binom{m}{2j}Y_2^{2j}(i)^{m-2j}Y_1^{m-2j}\Big) \\ &= (2/\sqrt{2}^m)\Big(\sum_{j=0}^{(m-1)/2}\binom{m}{2j}Y_2^{2j}(-1)^{p-j+1}iY_1^{m-2j}\Big)\end{aligned}$$

En posant $P_1 = Y_1^2 + Y_2^2$ et $Q_1 = \sum_{j=0}^{m/2}\binom{m}{2j}Y_2^{2j}(-1)^jY_1^{m-2j}$ si $m = 2p$ ou $Q_1 = \sum_{j=0}^{(m-1)/2}\binom{m}{2j}Y_2^{2j}(-1)^jY_1^{m-2j}$ si $m = 2p+1$, alors les nouveaux polynômes P_1 et Q_1 ainsi trouvés sont des générateurs basiques de $\mathcal{I}$, où $\mathcal{I} \subset \mathbf{C}[Y_1, Y_2]$.
Pour D_3, on obtient pour générateurs : $P_1 = Y_1^2 + Y_2^2$ et $Q_1 = Y_1 - 3Y_2^2Y_1$.
Pour D_4, on obtient pour générateurs : $P_1 = Y_1^2 + Y_2^2$ et $Q_1 = Y_1^4 - 6Y_2^2Y_1^2 + Y_2^4$.

Exemple 5.14. On note $A = (1,1,1)$, $B = (1,-1,1)$, $C = (-1,-1,1)$, $D = (-1,1,1)$ et A', B', C', D' leurs symétriques respectifs par la symétrie de centre O. On note E le milieu de $[AB]$, F le milieu de $[BC]$, G le milieu de $[CD]$, H le milieu de $[AD]$, I le milieu de $[AC']$, J le milieu de $[DB']$ et E', F', G', H', I', J' leurs symétriques respectifs par la symétrie de centre O.
On considère $\mathcal{C}$ le cube de $\mathbf{R}^3$ centré en l'origine : $ABCDA'B'C'D'$.



Il y a un nombre fini de rotations de $\mathbf{R}^3$ centrées à l'origine laissant le cube invariant :
- l'identité,
- les rotations ayant pour axe de symétrie la droite passant par les milieux de deux faces opposées et d'angle $\pi/2$, π ou $3\pi/2$ (par exemple, en notant $r(\pi/2, (Ox))$ la rotation d'angle $\pi/2$ et d'axe de rotation (Ox), celle-ci est l'une d'entre elles),
- les rotations ayant pour axe de symétrie la droite passant par les milieux de deux arrêtes opposées et d'angle π (par exemple, $r(\pi, (EE'))$),
- les rotations ayant pour axe de symétrie la droite passant par deux sommets opposées et d'angle $2\pi/3$ ou $4\pi/3$ (par exemple, $r(2\pi/3, (AA'))$),

on compte ainsi 24 rotations laissant le cube invariant.

De plus, $-id$ composée avec chacune de ces 24 rotations laisse également $\mathcal{C}$ invariant.
On peut ainsi décomposer le groupe des isométries du cube :

$$G =< G^+, -id >= G^+ \sqcup \{-id \circ T, T \in G^+\} = G^+ \sqcup (-id)G^+$$

où G^+ est le sous-groupe des rotations laissant invariant $\mathcal{C}$ (les isométries positives de G).

Proposition 5.15. Le groupe G^+ est engendré par $r_1 = r(2\pi/3, (AA'))$ et $r_2 = r(\pi/2, (Oz))$.
Le groupe G des isométries du cube est un sous-groupe d'ordre 48 de $\mathcal{O}(\mathbf{R}^3)$ engendré par des réflexions.

Démonstration. Montrons que $G^+ =< r(2\pi/3, (AA')), r(\pi/2, (Oz)) >=< r_1, r_2 >$.
On sait que G^+ est isomorphe par ϕ au groupe de permutations S_4 (où $\phi : G \to S_4$ est le morphisme qui définit l'action de G sur les 4 grandes diagonales du cube).
Cet isomorphisme nous ramène à justifier que si σ est un 3-cycle et η un 4-cycle de S_4, alors on a $S_4 =< \sigma, \eta >$. En effet, par Lagrange, $H =< \sigma, \eta >$ est d'ordre multiple de $3 \times 4 = 12$. De plus, η est une permutation impaire dons $H \neq A_4$. Or on sait que A_4 est l'unique sous-groupe d'indice 2 de S_4. Ainsi $H = S_4$.

On vient de voir ci-dessus que G^+ est d'ordre 24 et d'indice 2 dans G, donc G est d'ordre 48. De plus nous avons que G est engendré par $-id$, r_1 et r_2 ($G =< G^+, -id >$), donc pour conclure que G est engendré par des réflexions, il suffit de montrer que les deux rotations r_1 et r_2 et $-id$ sont produit de réflexions de G.
Pour montrer cela, nous allons travailler matriciellement :
$-id$ est la composée de 3 réflexions de G, par rapport aux plans (xOy), (yOz) et (xOz) :

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&-1\end{pmatrix}\begin{pmatrix}-1&0&0\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&-1&0\\0&0&1\end{pmatrix} = -I_3$$

r_1 est la composée de la symétrie par rapport au plan d'équation $x = z$ et celle par rapport au plan d'équation $y = z$: $r_1 = s_{(x=z)} \circ s_{(y=z)}$. En effet :

$$\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix} = \begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix} = \text{mat } r(2\pi/3, (AA')) = \text{mat } r_1$$

Et enfin r_2 est la composée de la symétrie par rapport au plan xOz et celle par rapport au plan d'équation $x + y = 0$: $r_2 = s_{xOy} \circ s_{(x+y=0)}$. En effet :

$$\begin{pmatrix}1&0&0\\0&-1&0\\0&0&1\end{pmatrix}\begin{pmatrix}0&-1&0\\-1&0&0\\0&0&1\end{pmatrix} = \begin{pmatrix}0&-1&0\\1&0&0\\0&0&1\end{pmatrix} = \text{mat } r(\pi/2, (Oz)) = \text{mat } r_2$$

Donc G est engendré par des réflexions. □

Nous sommes sur le corps $\mathbf{R}$ donc ici les pseudo-réflexions sont en fait des réflexions. Donc par le théorème CST, $\mathcal{I}(G)$ est isomorphe à $\mathbf{R}[X, Y, Z]$.

On cherche à déterminer f_1, f_2 et f_3 des générateurs homogènes algébriquement indépendants de $\mathcal{I}$.
On obtient des invariants par une approche géométrique :

1) Tout d'abord, $X^2 + Y^2 + Z^2 \in \mathcal{I}(G)$. En effet, les éléments de G sont des isométries vectorielles. Elles conservent donc la distance à l'origine, et donc le polynôme $X^2 + Y^2 + Z^2$.
On peut donc fixer l'un des f_i égal à $f_1 = X^2 + Y^2 + Z^2$ (par (6.4)).

2) On définit $f = XYZ$. On note $V(XYZ) = \{(x, y, z) \in \mathbf{R}^3, xyz = 0\}$. Comme les éléments de G permutent les faces du cube, ils conservent l'union des trois plans de coordonnées, c'est-à-dire $V(XYZ)$.

On note $I(V(XYZ)) = \{P \in K[X, Y, Z], \forall (x, y, z) \in V(XYZ), P(x, y, z) = 0\}$. Soit $P \in I(V(XYZ))$. En faisant la division euclidienne de P par X en tant que polynôme en X (ce qui est possible car le coefficient dominant de X est inversible dans $K[Y, Z]$),on écrit $P(X, Y, Z) = XQ(X, Y, Z)+R(Y, Z)$. Comme $P(0, Y, Z) = 0$, on a $R = 0$. En faisant de même avec les variables Y et Z, on trouve que $P \in (XYZ)$ et si $\deg P = 3$, $P = \lambda XYZ$ avec $\lambda \in \mathbf{R}$.

Soit $T \in G+$. Comme $V(XYZ)$ est stable par T, on a, pour $(x, y, z) \in V(XYZ)$, l'égalité : $f(T \cdot (x, y, z)) = 0$, c'est-à-dire $f(T \cdot (X, Y, Z)) \in I(V(XYZ))$.

On obtient donc $f(T \cdot (X,Y,Z)) = \lambda f$. Et comme $T^n = Id$ pour un certain n, on a nécessairement $\lambda = \pm 1$.
On en conclut que $(XYZ)^2 \in \mathcal{I}_G$.

3) On considère $g = (X+Y+Z)(X+Y-Z)(X-Y+Z)(X-Y-Z)$. Cette fois-ci, on définit $V(g)$ comme l'union des 4 plans vectoriels orthogonaux aux 4 grandes diagonales.
$A' = (-1,-1,-1)$ donc $\overrightarrow{AA'} = (-2,-2,-2)$. Un vecteur directeur de (AA') est donc $\vec{u} = (1,1,1)$. Donc le plan orthogonal à (AA') est $\{(x,y,z) \in \mathbf{R}^3, x+y+z = 0\}$.
On trouve de même que
- le plan orthogonal à (BB') est : $\{(x,y,z) \in \mathbf{R}^3, x-y+z = 0\}$.
- le plan orthogonal à (CC') est : $\{(x,y,z) \in \mathbf{R}^3, x+y-z = 0\}$.
- le plan orthogonal à (DD') est : $\{(x,y,z) \in \mathbf{R}^3, x-y-z = 0\}$.

Donc $V(g) = \{(x,y,z) \in \mathbf{R}^3, x+y+z = 0\} \cup \{(x,y,z) \in \mathbf{R}^3, x-y+z = 0\} \cup \{(x,y,z) \in \mathbf{R}^3, x+y-z = 0\} \cup \{(x,y,z) \in \mathbf{R}^3, x-y-z = 0\}$.

Comme l'ensemble des 4 grandes diagonales est stable par G, on en déduit que $V(g)$ est stable par G.
On note $I(V(g)) = \{P \in K[X,Y,Z], \forall (x,y,z) \in V(g), P(x,y,z) = 0\}$.
Soit $P \in I(V(g))$. On effectue la division euclidienne de P par $(X+Y+Z)$: $P(X,Y,Z) = (X+Y+Z)Q(X,Y,Z) + R(X,Y,Z)$ avec $\deg_X R < 1$, $\deg_Y R < 1$ et $\deg_Z R < 1$. C'est-à-dire $R(X,Y,Z) = c \in \mathbf{R}$ et comme $P(1,1,-2) = 0$, $R = 0$. En continuant avec les divisions par $X+Y-Z, X-Y+Z$ et $X-Y-Z$, on obtient que $P = \lambda(X+Y+Z)(X+Y-Z)(X-Y+Z)(X-Y-Z)$ où $\lambda \in \mathbf{R}$ si $\deg P = 4$.
Soit $T \in G$.
On obtient donc une nouvelle fois $g(T \cdot (X,Y,Z)) = \lambda g$ et par le même argument que ci-dessus, $\lambda = \pm 1$. Donc $g^2 \in \mathcal{I}_G$.

4) Enfin pour $h = (X^2-Y^2)(X^2-Z^2)(Y^2-Z^2)$, on utilise $V(h)$ l'union des 6 plans vectoriels orthogonaux aux paires de diagonales opposées inscrites dans les faces du cube.
$\overrightarrow{AD'} = (0,-2,-2)$ donc un vecteur directeur de (AD') est $\vec{v} = (0,1,1)$. Donc le plan orthogonal à (AD') est $\{(x,y,z) \in \mathbf{R}^3, y+z = 0\}$.
De même,
- le plan orthogonal à (BC') est : $\{(x,y,z) \in \mathbf{R}^3, y-z = 0\}$.
- le plan orthogonal à (AB') est : $\{(x,y,z) \in \mathbf{R}^3, x+z = 0\}$.
- le plan orthogonal à (DC') est : $\{(x,y,z) \in \mathbf{R}^3, x-z = 0\}$.
- le plan orthogonal à (AC) est : $\{(x,y,z) \in \mathbf{R}^3, x+y = 0\}$.
- le plan orthogonal à (CC') est : $\{(x,y,z) \in \mathbf{R}^3, x-y = 0\}$.

Donc $V(h) = \{(x,y,z) \in \mathbf{R}^3, y+z = 0\} \cup \{(x,y,z) \in \mathbf{R}^3, y-z = 0\} \cup \{(x,y,z) \in \mathbf{R}^3, x+z = 0\} \cup \{(x,y,z) \in \mathbf{R}^3, x-z = 0\} \cup \{(x,y,z) \in \mathbf{R}^3, x+y = 0\} \cup \{(x,y,z) \in \mathbf{R}^3, x-y = 0\}$.
Une fois de plus $V(h)$ est stable par G et on obtient par le même raisonnement que $h^2 \in \mathcal{I}_G$.

Ensuite, le nombre de réflexions contenues dans G est égal au nombre de rotations d'angle π contenus dans G^+ (en effet, une réflexion est une rotation d'angle

π composée avec $-id$). Donc par (5.4) et (5.5),

$$\begin{cases} 48 &= d_1d_2d_3 \\ 9 &= d_1+d_2+d_3-3 \end{cases}$$

Or d_1 vaut 2 (5.11). Donc

$$\begin{cases} 24 &= d_2d_3 \\ 10 &= d_2+d_3 \end{cases}$$

Ensuite, $d_2 = 10-d_3$ implique que $24 = (10-d_3)d_3$. Et en résolvant cette dernière équation, on trouve que $d_3 = 4$ ou $d_3 = 6$.
Donc $d_1 = 2$, $d_2 = 4$ et $d_3 = 6$ (on les ordonne par ordre croissant).
De plus, $g(X,Y,Z) = g(Y,Z,X) = g(-Y,X,Z)$ et $g(-X,-Y,-Z) = g(X,Y,Z)$ donc $g \in \mathcal{I}$.
Et $\deg f^2 = 6$ et $\deg g = 4$.

En complément, dans le livre de Kane, *Reflection groups and invariant theory*, Springer, 2001, pages 172-173, ils énoncent que $f_1 = X^2+Y^2+Z^2$, $f_2 = X^2Y^2 + X^2Z^2 + Y^2Z^2$ et $f_3 = (XYZ)^2$ forment des générateurs basiques de $\mathcal{I}(G)$. Donc $\mathcal{I}(G) = \mathbf{R}[f_1,f_2,f_3]$.
Et donc puisque $g(X,Y,Z) = (X+Y+Z)(X+Y-Z)(X-Y+Z)(X-Y-Z) = (X^2+Y^2+Z^2)^2 - 4(X^2Y^2+X^2Z^2+Y^2Z^2) = (f_1(X,Y,Z))^2 - 4f_2(X,Y,Z)$, on a $f_2 = 1/4(f_1^2 - g)$. C'est pourquoi on a également :

$$\begin{aligned}\mathcal{I} &= \mathbf{R}[X^2+Y^2+Z^2, X^2Y^2Z^2, (X+Y+Z)(X+Y-Z)(X-Y+Z)(X-Y-Z)] \\ &= \mathbf{R}[f_1,f_3,g]\ .\end{aligned}$$

6. Annexe

Une référence pour la notion de base de transcendance et ses premières propriétés est le début du livre : *Groupes, Algèbres et géométrie* - Tome 3, d'Arnaudiès-Bertin.

Définition 6.1. Soient $K \supset k$ une extension de corps. On dit qu'une partie B de K est une base de transcendance sur k si elle vérifie les deux conditions suivantes :
(i) les éléments de B sont algébriquement indépendants sur k ;
(ii) le corps K est une extension algébrique du sous-corps $k(B)$.

Théorème 6.2. *(i) Si $K \supset k$ une extension de corps, alors K possède une base de transcendance sur k.*
(ii) Le cardinal d'une base de transcendance de K sur k est indépendant de la base.

Définition 6.3. On appelle degré de transcendance de K sur k le cardinal d'une base de transcendance de K sur k et on le note $DegTr(K : k)$.

Théorème 6.4. *Soient $K \supset k$ une extension de corps. Si $S \subset K$ est telle que $K \supset k(S)$ est algébrique et si $S_0 \subset S$ est une famille algébriquement indépendante, alors il existe B une base de transcendance de K sur k telle que $S_0 \subset B \subset S$.*
En particulier, $DegTr(K : k)$ est le plus grand cardinal d'une famille algébriquement indépendante de K sur k.
(Une preuve de ce théorème se trouve dans Algèbre *de Lang.)*

Définition 6.5. Soient $g_1, ..., g_n \in \mathcal{P}$ homogènes et algébriquement indépendants et $f_1, ..., f_n$ dans $K[g_1, ..., g_n]$.
Le Jacobien de $(f_1, ..., f_n)$ relativement à $(g_1, ..., g_n)$ est le polynôme de $K[g_1, ..., g_n]$ défini par :

$$Jac((f_1, ..., f_n)/(g_1, ..., g_n)) = \det(\partial f_i/\partial g_j)_{i,j}$$

Lemme 6.6. Avec les notations de la définition précédente, la famille $(f_1, ..., f_n)$ est algébriquement indépendante si et seulement si $Jac((f_1, ..., f_n)/(g_1, ..., g_n)) \neq 0$.

Démonstration. Supposons que la famille $(f_1, ..., f_n)$ est algébriquement indépendante.
Pour chaque $1 \leq i \leq n$, soit $P_i(X_0, ..., X_n) \in K[X_0, ..., X_n]$ un polynôme non nul de degré minimal vérifiant : $P_i(g_i, f_1, ..., f_n) = 0$ (P_i existe par le théorème (6.4) : on ne peut avoir $n + 1$ éléments algébriquement indépendants).
Dérivons cette égalité par rapport à g_j :

$$\delta_{ij} \frac{\partial P_i}{\partial X_0}(g_i, f_1, ..., f_n) + \sum_{l=1}^{n} \frac{\partial P_i}{\partial X_l}(g_i, f_1, ..., f_n) \frac{\partial f_l}{\partial g_j} = 0 \ .$$

En réécrivant en terme de matrices $n \times n$, on obtient :

$$\left(\frac{\partial P_i}{\partial X_l}(g_i, f_1, ..., f_n) \right)_{i,l} \left(\frac{\partial f_l}{\partial g_j} \right)_{l,j} = -D\left(\left(\frac{\partial P_i}{\partial X_0}(g_i, f_1, ..., f_n) \right)_i \right)$$

où $D((\lambda_i)_i)$ désigne la matrice diagonale ayant $(\lambda_i)_i$ pour diagonale.
Puisque pour chaque i, on a : $\frac{\partial P_i}{\partial X_0}(g_i, f_1, ..., f_n) \neq 0$ (par minimalité de P_i et puisque

$car(K) = 0$), on voit que la matrice $\left(\frac{\partial f_l}{\partial g_j}\right)_{l,j}$ est inversible.
Ce qui signifie que $Jac((f_1, ..., f_n)/(g_1, ..., g_n)) \neq 0$.

Réciproquement, si la famille $(f_1, ..., f_n)$ n'est pas algébriquement indépendante, soit $P(X_1, ...X_n) \in K[X_1, ..., X_n]$ de degré minimal tel que $P(f_1, ..., f_n) = 0$.
En différentiant par rapport à g_j,

$$\sum_{i=1}^{n} \frac{\partial P}{\partial X_i}(f_1, ..., f_n)\frac{\partial f_i}{\partial g_j} = 0 \ (*)$$

Or, $carK = 0$, donc il existe i tel que $\frac{\partial P}{\partial X_i} \neq 0$, et alors, par minimalité du degré de P, $\frac{\partial P}{\partial X_i}(f_1, ..., f_n) \neq 0$.
Et donc $(*)$ montre que la matrice $\left(\frac{\partial f_i}{\partial g_j}\right)_{ij}$ n'est pas inversible ; par suite,
$Jac((f_1, ..., f_n)/(g_1, ..., g_n)) = 0$. □

Remarque 6.7. Ce lemme permet de prouver d'une autre manière que XY et $X^m + Y^m$ sont algébriquement indépendants (preuve établie en (4.11)).

7. Bibliographie

— Grove-Benson, *Finite Reflection Groups* - Second Edition, Springer, 2010.

— Cox-Little-O'Shea, *Ideals, Varieties, and Algorithms* - Third Edition, Springer, 2007.

— Arnaudiès-Bertin, *Groupes, Algèbres et géométrie* - Tome 3, Ellipses, 2001.

— Broué, *Introduction to complex reflection groups and their braid groups*, Springer, 2010.

— Peyré, *L'algèbre discrète de la transformée de Fourier*, Ellipses, 2004.

— Sturmfels, *Algorithms in Invariant Theory* - Second edition, Springer, 2008.

— Lang, *Algebra*, Springer, 2002.

— Brion, *Invariants et covariants des groupes algébriques réductifs, Notes de l'école d'été CIMPA à Monastir*, 1996.

— Kane, *Reflection groups and invariant theory*, Springer, 2001.