Action de groupes finis sur les algèbres de polynômes

Marc SAGE

Table des matières

1 Préliminaires

Soit k un corps (bientôt $k = \mathbb{R}$) et V un k-ev de dimension n de base $(e_1, ..., e_n)$.

1.1 Algèbre symétrique du dual et fonctions polynomiales

On considère l'algèbre symétrique $S(V^*)$ du dual V^*.

On sait, via la correspondance $X_i \longmapsto e_i^*$, que

$$S(V^*) \simeq k[X_1, ..., X_n].$$

Les éléments $P(e_1^*, ..., e_n^*)$ de $S(V^*)$ peuvent alors être vus comme des fonctions polynomiales sur V via

$$[P(e_1^*, ..., e_n^*)](x) = P(e_1^*(x), ..., e_n^*(x))$$

où x est un vecteur de V.

Montrons que ceci ne dépend pas du choix d'une base de V. On dispose en effet, à $x \in V$ fixé, d'une application linéaire

$$\Phi_x : \left\{ \begin{array}{ccc} V^* & \longrightarrow & k \\ \varphi & \longmapsto & \varphi(x) \end{array} \right.$$

que l'on peut prolonger dans $S(V^*)$ en

$$\overline{\Phi_x} : \left\{ \begin{array}{ccc} S(V^*) & \longrightarrow & k \\ \varphi_1 \cdot ... \cdot \varphi_r & \longmapsto & \varphi_1(x) ... \varphi_r(x) \end{array} \right. .$$

Si $f \in S(V^*)$, il suffit de poser $f(x) = \overline{\Phi_x}(f)$, qui est clairement indépendant du choix de la base $(e_1, ..., e_n)$.

En écrivant $f = P(e_1^*, ..., e_n^*)$, on a bien

$$[P(e_1^*, ..., e_n^*)](x) = P(e_1^*(x), ..., e_n^*(x))$$

comme voulu, ce qui montre par ailleurs que f est bien polynomiale en les coordonéees $e_i^*(x)$ de x dans la base $(e_1, ..., e_n)$.

Réciproquement, toute fonction polynomiale sur V (en les coordonéees x_i de $x \in V$ dans une base $(e_1, ..., e_n)$ fixée) peut s'écrire $f(x) = P(x_1, ..., x_n)$, donc correspond à un $P(e_1^*, ..., e_n^*)$ dans $S(V^*)$.

On identifiera donc $S(V^*)$ à l'algèbre des fonctions polynomiales sur V modulo le choix arbitraire d'une base.

1.2 Action de groupe sur $S(V^*)$

Soit maintenant G un sous-groupe de $GL(V)$. Il agit à droite dans $S(V^*)$ via

$$\sigma \cdot f(x) = f\left(\sigma^{-1}(x)\right)$$

où $\sigma \in G$ et $f \in S(V^*)$, ou encore, après choix d'une base $(e_1, ..., e_n)$, par

$$\sigma \cdot P(e_1^*, ..., e_n^*) = P\left(e_1^* \circ \sigma^{-1}, ..., e_n^* \circ \sigma^{-1}\right).$$

Propriété.
L'action de G sur $S(V^*)$ est algébrique.

Démonstration.

On montre cela en se donnant une base $(e_1, ..., e_n)$ de V :

$$\begin{aligned}\sigma \cdot (P + \lambda Q) &= \sigma \cdot (P(e_1^*, ..., e_n^*) + \lambda Q(e_1^*, ..., e_n^*)) \\ &= P\left(e_1^* \circ \sigma^{-1}, ..., e_n^* \circ \sigma^{-1}\right) + \lambda Q\left(e_1^* \circ \sigma^{-1}, ..., e_n^* \circ \sigma^{-1}\right) \\ &= \sigma \cdot P + \lambda \sigma \cdot Q\end{aligned}$$

et

$$\begin{aligned}\sigma \cdot (PQ) &= \sigma \cdot (P(e_1^*, ..., e_n^*) Q(e_1^*, ..., e_n^*)) \\ &= P\left(e_1^* \circ \sigma^{-1}, ..., e_n^* \circ \sigma^{-1}\right) Q\left(e_1^* \circ \sigma^{-1}, ..., e_n^* \circ \sigma^{-1}\right) \\ &= (\sigma \cdot P)(\sigma \cdot Q)\end{aligned}$$

Propriété.
L'action de G préserve le degré : pour tout $\left\{ \begin{array}{l} \sigma \in G \\ f \in S \end{array} \right.$ *, on a*

$$\deg(\sigma \cdot f) = \deg f.$$

Démonstration.
σ^{-1} étant linéaire, les $e_i^* \circ \sigma^{-1}$ sont des polynômes linéaires l_i en les e_j^*, donc si $f = P(e_1^*, ..., e_n^*)$ on a

$$\begin{aligned}\deg(\sigma \cdot f) &= \deg(\sigma \cdot P(e_1^*, ..., e_n^*)) = \deg\left(P\left(e_1^* \circ \sigma^{-1}, ..., e_n^* \circ \sigma^{-1}\right)\right) \\ &= \deg(P(l_1, ..., l_n)) \leq \deg(P(e_1^*, ..., e_n^*)) \leq \deg f.\end{aligned}$$

L'égalité s'obtient alors par un argument de symétrie :

$$\deg f = \deg\left(\sigma^{-1}\sigma \cdot f\right) \leq \deg(\sigma \cdot f) \leq \deg f.$$

On notera désormais l'action de G de manière fonctionnelle, *i.e.*

$$\sigma(f) := \sigma \cdot f,$$

de sorte que G peut être considéré comme un groupe d'automorphismes d'algèbres de $S(V^*)$.

On s'intéresse par la suite à l'algèbre des invariants $S(V^*)^G$, *i.e.* aux fonctions polynomiales $f \in S(V^*)$ vérifiant

$$\forall \sigma \in G,\ \sigma(f) = f,$$

ou encore qui vérifient

$$\forall (\sigma, x) \in G \times V,\ f(\sigma(x)) = f(x).$$

1.3 Projecteur sur $S(V^*)^G$

Dans le cas où G est fini, on dispose d'un élément $p = \frac{1}{|G|} \sum_{\sigma \in G} \sigma$ vérifiant les propriétés suivantes :
- $\forall g \in G, gp = p$;
- p agit linéairement sur $S(V^*)$ via $p(f) = \frac{1}{|G|} \sum_{\sigma \in G} \sigma(f)$;
- p est un projecteur d'image $S(V^*)^G$;
- p est $S(V^*)^G$-linéaire, au sens où $\left\{ \begin{array}{l} \forall s \in S(V^*) \\ \forall r \in S(V^*)^G \end{array} \right.$, $p(sr) = p(s) r$

Démonstration.
- Le premier point est immédiat par construction de p.
- L'action linéaire de p est bien définie car l'action de G sur $S(V^*)$ est algébrique – *a fortiori* linéaire.

• Il est classique que $p^2 = p$:

$$\begin{aligned} p^2(f) &= p(p(f)) = p\left(\frac{1}{|G|}\sum_{\sigma\in G}\sigma(f)\right) = \frac{1}{|G|}\sum_{\tau\in G}\tau\left(\frac{1}{|G|}\sum_{\sigma\in G}\sigma(f)\right) = \frac{1}{|G|}\sum_{\tau\in G}\left(\frac{1}{|G|}\sum_{\sigma\in G}\tau\sigma(f)\right) \\ &= \frac{1}{|G|}\sum_{\tau\in G}\left(\frac{1}{|G|}\sum_{\sigma\in G}\sigma(f)\right) = \frac{1}{|G|}|G|\left(\frac{1}{|G|}\sum_{\sigma\in G}\sigma(f)\right) = p(f). \end{aligned}$$

Montrons que $\operatorname{Im} p = S(V^*)^G$. On a d'une part :

$$g((p(f))) = g\left(\frac{1}{|G|}\sum_{\sigma\in G}\sigma(f)\right) = \frac{1}{|G|}\sum_{\sigma\in G}g(\sigma(f)) = \frac{1}{|G|}\sum_{\sigma\in G}g\sigma(f) = \frac{1}{|G|}\sum_{\sigma\in G}\sigma(f) = p(f),$$

donc $\operatorname{Im} p \subset S(V^*)^G$, d'autre part si $f \in S(V^*)^G$, alors

$$f = \frac{1}{|G|}\sum_{\sigma\in G}f = \frac{1}{|G|}\sum_{\sigma\in G}\sigma(f) = p(f) \in \operatorname{Im} p.$$

• La $S(V^*)^G$-linéarité s'obtient par un calcul direct :

$$p(sr) = \frac{1}{|G|}\sum_{\sigma\in G}\sigma(sr) = \frac{1}{|G|}\sum_{\sigma\in G}\sigma(s)\sigma(r) = \frac{1}{|G|}\sum_{\sigma\in G}\sigma(s)r = p(s)r.$$

On sera souvent amené à projeter à l'aide du projecteur p pour envoyer $S(V^*)$ dans $S(V^*)^G$.

1.4 Notations pour la suite

Dans tout ce qui suit, on pose

$$\begin{gathered} k \text{ un corps de caractéristique nulle,} \\ V \text{ un } k\text{-espace vectoriel de dimension } n \geq 1, \\ G \text{ un sous-groupe fini de } GL(V), \\ S = S(V^*) \text{ l'algèbre des fonctions polynomiales sur } V, \\ R = S^G = S(V^*)^G \text{ l'algèbre des invariants de } S \text{ sous } G, \\ R^+ = \{f \in R \ ; \ \deg f \geq 1\} \text{ les invariants non constants.} \end{gathered}$$

2 Transcendance

2.1 Base de transcendance

Définition.
Soit $k \subset K$ une extension de corps.
On appelle base de transcendance *de K sur k (ou k-base de transcendance) toute famille d'éléments de K k-algébriquement indépendants maximale.*
Par convention, la famille vide est une base de transcendance de toute extension.

On fera évidemment le parallèle avec la notion de base dans les espaces vectoriels, une base pouvant être définie comme une famille libre de cardinal maximal.
En particulier, Zorn assure de la même manière l'existence d'une base de transcendance.

Propriété.
Toute extension $k \subset K$ admet une k-base de transcendance. Pour un telle base $\mathcal{B}$, K est algébrique sur $k(\mathcal{B})$.

Démonstration.
Soit X l'ensemble des familles d'éléments de K k-algébriquement indépendants ordonné par l'inclusion. X est non vide car il contient $\emptyset$, et est faiblement inductif (si $\mathcal{C}$ est une chaine de X, $\bigcup_{\mathcal{F}\in\mathcal{C}} \mathcal{F}$ est encore dans X), donc admet un élément maximal $\mathcal{B}$.

S'il y a un $x \in K$ transcendant sur $k(\mathcal{B})$, alors d'une part $x \notin \mathcal{B}$, d'autre part $\mathcal{B} \cup \{x\}$ est encore une famille d'éléments algébriquement indépendants, *absurde* par maximalité.

Pour mieux marquer l'analogie avec l'algèbre linéaire, on omettra par la suite le terme "algébrique" concernant la liberté ou l'indépendance des familles considérées, et de même on parlera de "k-base" ou de "base" au lieu de "base de transcendance sur k".

2.2 Lemme de l'échange – Théorème de la base imcomplète

Comme avec l'algèbre linéaire, on dispose d'un lemme de l'échange ainsi que d'un théorème de la base incomplète.

Proposition (lemme de l'échange).
Soit $(x_1, ..., x_{n\geq 1})$ une base de K et $\xi \in K$ tel que $(x_1, ..., x_r, \xi)$ soit libre (avec $0 \leq r < n$)
Alors on peut remplacer dans $(x_1, ..., x_n)$ un des $x_{i>r}$ par ξ de sorte que la nouvelle famille reste une base de K.
En d'autres termes, il y a un $i > r$ tel que

$$\left(x_1, ..., x_r, \xi, x_{\tau(r+2)}, ..., x_{\tau(n)}\right)$$

soit une base de K, où l'on a noté τ la transposition $(r+1, i)$ de $\mathfrak{S}_n$.

Démonstration.
K est algébrique sur $k(x_1, ..., x_n)$. En particulier, ξ est algébrique sur $k(x_1, ..., x_n)$, d'où un polynôme $P \in K[X_0, X_1 ..., X_n]$ non nul tel que $P(\xi, x_1, ..., x_n) = 0$. Nécessairement, ξ intervient vraiment dans P (car les $x_1, ..., x_n$ sont libres), et l'un des $x_{i>r}$ aussi (car $\xi, x_1, ..., x_r$ sont libres), mettons x_n, d'où x_n algébrique sur $k[\xi, x_1, ..., x_{n-1}]$. En posant

$$\kappa = k[x_1, ..., x_{n-1}] = k(x_1, ..., x_{n-1}),$$

on a x_n algébrique sur $\kappa[\xi]$, ce qui se traduit en termes de degrés d'extension par $[\kappa[\xi, x_n] : \kappa[\xi]] < \infty$.
On a alors

$$\underbrace{[\kappa[\xi, x_n] : \kappa[\xi]]}_{<\infty} \times [\kappa[\xi] : \kappa] = [\kappa[\xi, x_n] : \kappa] = [\kappa[\xi, x_n] : \kappa[x_n]] \times \underbrace{[\kappa[x_n] : \kappa]}_{=\infty} = \infty,$$

d'où $[\kappa[\xi] : \kappa] = \infty$; par conséquent, la famille $(\xi, x_1, ..., x_{n-1})$ est libre, et c'est même une base par maximalité de son cardinal.

Corollaire.
Supposons que K admette une base finie $(x_1, ..., x_d)$ de cardinal d. Alors toute famille libre $(y_i)_{i\in I}$ d'éléments de K a un cardinal $|I| \leq d$.

Démonstration.
Quitte à extraire de (y_i) une sous-famille libre $(y_1, ..., y_n)$, on supposera I fini de cardinal n.
Supposons par récurrence que, pour $r \in \{0, ..., d-1\}$, il y a une permutation $\sigma \in \mathfrak{S}_d$ telle que

$$\left(y_{\sigma(1)}, ..., y_{\sigma(r)}, x_{\sigma(r+1)}, ..., x_{\sigma(d)}\right) \text{ soit une base de } K.$$

Le cas $r = 0$ correspond à l'hypothèse $(x_1, ..., x_d)$ base de K et amorce ainsi la récurence. Alors

$$y_{\sigma(1)}, ..., y_{\sigma(r)}, y_{\sigma(r+1)} \text{ sont libres,}$$

donc le lemme de l'échange s'applique : on peut remplacer un des $x_{\sigma(i>r)}$ par $y_{\sigma(r+1)}$ de sorte que, en notant τ la transposition $(\sigma(r+1), \sigma(i)) \in \mathfrak{S}_d$, la famille

$$\left(y_{\sigma(1)}, ..., y_{\sigma(r)}, y_{\sigma(r+1)}, x_{\tau\sigma(r+2)}, ..., x_{\tau\sigma(d)}\right) \text{ reste une base de } K \ ;$$

or $\sigma = \tau\sigma$ sur $\{1, ..., r\}$, donc la même famille

$$\left(y_{\tau\sigma(1)}, ..., y_{\tau\sigma(r)}, y_{\tau\sigma(r+1)} x_{\tau\sigma(r+2)}, ..., x_{\tau\sigma(d)}\right) \text{ est une base de } K,$$

d'où l'hypothèse de récurrence au rang $r+1$.

On en déduit l'hyphothèse au rang d :

$$(y_1, ..., y_d) \text{ est une base de } K,$$

d'où $n \leq d$ par maximalité du cardinal d'une base.

Ce corollaire correspond à l'énoncé linéaire "si un espace vectoriel E admet une base finie de cardinal n, alors toute famille libre est de cardinal $\leq n$".

On peut donc en déduire un théorème de la base incomplète ainsi qu'un équivalent de la dimension

Corollaire 1 (théorème de la base incomplète).
Soit $(x_1, ..., x_d)$ une base de K. Alors toute famille libre $(y_1, ..., y_p)$ peut se compléter en une base.

Démonstration.
Si $(y_1, ..., y_p)$ est maximale, c'est gagné. Sinon, on peut trouver un $y_{p+1} \in K$ tel que $(y_1, ..., y_p, y_{p+1})$ soit libre. On réitère jusce qu'à que l'on ne puisse plus trouver de famille libre strictement plus grande, ce qui arrive nécessairement car une famille de cardinal $> n$ ne peut être libre d'après le corollaire.

2.3 Degré de transcendance

Corollaire 2 (cardinal des bases de transcendance).
Supposons que K admette une base finie $(x_1, ..., x_d)$ de cardinal d. Alors toute autre base de K a pour cardinal d.

Démonstration.
Soient $(y_i)_{i \in I}$ une autre base. Par le corollaire précédent, et puisque (y_i) est libre, on a $|I| \leq d$, d'où $|I|$ fini. On réapplique le corollaire en intervertissant les deux bases, ce qui donne $d \leq |I|$. Il en résulte $|I| = d$.

Définition.
Si K admet une k-base de transcendance ***finie****, le cardinal commun des bases de transcendance de $k \subset K$ est appelé* degré de transcendance *de K sur k et est noté*

$$d = \deg \mathrm{tr}_k K.$$

Ainsi, une extension quelconque comporte une première partie transcendante pure et une seconde partie algébrique :

$$\underbrace{\overbrace{k \subset k(x_1, ..., x_d)}^{transcendante\ pure} = \overbrace{k(x_1, ..., x_d) \subset K}^{algébrique}}_{extension\ quelconque}.$$

Exemple.
$(X_1, ..., X_n)$ est une base de transcendance de $k(X_1, ..., X_n)$, d'où

$$\deg \mathrm{tr}_k\, k(X_1, ..., X_n) = n.$$

Démonstration.
$(X_1, ..., X_n)$ est clairement libre, et est en outre maximale. En effet, soit $F \in k(X_1, ..., X_n)$, mettons $F = \frac{P}{Q}$. Alors le polynôme

$$A(X_0, X_1, ..., X_n) = X_0 Q(X_1, ..., X_n) - P(X_1, ..., X_n)$$

s'annule en $(F, X_1, ..., X_n)$ et est non nul car $Q \neq 0$, donc $(F, X_1, ..., X_n)$ est liée.

2.4 Lien avec $S(V^*)$, $S(V^*)^G$, et $k(X_1, ..., X_n)$

Les deux propositions qui suivent s'intuitent bien en remplaçant "algébriquement engendré" par "linéairement engendré" et "degré de transcendance" par "dimension".

Proposition.
Si $k(x_1, .., x_n) \subset K$ est algébrique, alors $\deg \mathrm{tr}_k K \leq n$. *En d'autres termes :*

$$k \subset \underbrace{k(x_1, ..., x_n) \subset K}_{\text{algébrique}} \implies \deg \mathrm{tr}_k K \leq n.$$

Démonstration.
Supposons dans un premier temps $(x_1, .., x_n)$ libre. On la complète en une base $(x_1, ..., x_n, x_{n+1}, ..., x_d)$ où $d = \deg \mathrm{tr}_k K$. Si $d > n$, alors $x_d \in K$ est algébrique sur $k(x_1, .., x_n)$, *absurde* par liberté de $(x_1, ..., x_d)$.
Maintenant, on peut toujours extraire de $(x_1, .., x_n)$ une sous-famille libre maximale $\left(x_{i_1}, .., x_{i_p}\right)$ où $p \leq n$, et alors

$$k\left(x_{i_1}, .., x_{i_p}\right) \subset k(x_1, .., x_n) \text{ est algébrique.}$$

En effet, chaque x_i est ou bien dans $\left\{x_{i_1}, .., x_{i_p}\right\}$ et est alors clairement algébrique sur $k\left(x_{i_1}, .., x_{i_p}\right)$, ou bien dans $\{x_1, .., x_n\} \setminus \left\{x_{i_1}, .., x_{i_p}\right\}$ donc liée avec $\left\{x_{i_1}, .., x_{i_p}\right\}$ par maximalité et par conséquent algébrique sur $k\left(x_{i_1}, .., x_{i_p}\right)$. Alors K est algébrique sur $k\left(x_{i_1}, .., x_{i_p}\right)$ et on peut appliquer le premier cas :

$$\deg \mathrm{tr}_k K \leq p \leq n.$$

Proposition.
Soit $K \subset L \subset M$ une tour d'extensions. Si M est algébrique sur L, alors $\deg \mathrm{tr}_K L = \deg \mathrm{tr}_K M$.
En d'autres termes :

$$K \subset \underbrace{L \subset M}_{\text{algébrique}} \implies \deg \mathrm{tr}_K L = \deg \mathrm{tr}_K M.$$

Démonstration.
Notons n le degré de transcendance de M sur K.
Premier point : $n + 1$ éléments de L sont nécessairement K-liés, car ils sont dans M qui est de degré de transcendance n sur K .
Deuxième point : si $x_1, ..., x_p$ sont $p < n$ éléments libres de L, alors il existe un $x \in L$ qui n'est pas dans $K[x_1, ..., x_p]$. En effet, sinon L serait algébrique sur $K[x_1, ..., x_p]$, donc sur $K(x_1, ..., x_p)$, et comme $L \subset M$ est algébrique par hypothèse, $K(x_1, ..., x_p) \subset M$ serait algébrique par transivité de l'algébraïcité. Par la propriété précédente, on devrait avoir $n = \deg \mathrm{tr}_K M \leq p$, *absurde.*
Ainsi, toute famille libre à $p < n$ éléments de L peut se compléter en une famille libre à n éléments, qui est alors maximale par le premier point, d'où $\deg \mathrm{tr}_K L = n$.

Corollaire.
Soit E une extension intermédiaire de $k \subset k(X_1, ..., X_n)$. Si $k(X_1, ..., X_n)$ est algébrique sur E, alors $\deg \mathrm{tr}_k E = n$.
En d'autres termes :

$$k \subset \underbrace{E \subset k(X_1, ..., X_n)}_{\text{algébrique}} \implies \deg \mathrm{tr}_k E = n.$$

Démonstration.
Immédiat car $\deg \mathrm{tr}_k k(X_1, ..., X_n) = n$.

Application.
On regarde le cas particulier où $E = \mathrm{Frac}\, R$ vu dans $k(X_1, ..., X_n)$.

Lemme.
Soit G agissant algébriquement sur A un anneau intègre unitaire. Alors A^G est un sous-anneau intègre de A (on peut donc plonger le corps des fractions $\mathrm{Frac}\left(A^G\right)$ *dans* $\mathrm{Frac}\, A$*), et dans* $\mathrm{Frac}\, A$ *on a*

$$\mathrm{Frac}\left(A^G\right) = (\mathrm{Frac}\, A)^G$$

où l'action algébrique de G dans $\mathrm{Frac}\, A$ *est (nécessairement) définie par*

$$\sigma\left(\frac{a}{b}\right) = \frac{\sigma(a)}{\sigma(b)}.$$

Démonstration.
A^G est un sous-anneau de A car l'action de G est linéaire, intègre car A est intègre.
Si l'on veut prolonger l'action de G sur $\mathrm{Frac}\, A$ de manière à ce qu'elle reste algébrique, on doit avoir

$$1 = \sigma(1) = \sigma\left(b\frac{1}{b}\right) = \sigma(b)\,\sigma\left(\frac{1}{b}\right) \implies \sigma\left(\frac{1}{b}\right) = \frac{1}{\sigma(1)}$$

et

$$\sigma\left(\frac{a}{b}\right) = \sigma\left(a\frac{1}{b}\right) = \sigma(a)\,\sigma\left(\frac{1}{b}\right) = \sigma(a)\,\frac{1}{\sigma(b)} = \frac{\sigma(a)}{\sigma(b)}.$$

Il est alors immédiat que $\mathrm{Frac}\left(A^G\right) \subset (\mathrm{Frac}\, A)^G$.
Soit d'autre part $r = \frac{p}{q} \in (\mathrm{Frac}\, A)^G$. On écrit subtilement

$$r = \frac{p\prod_{\sigma\neq \mathrm{Id}}\sigma(q)}{q\prod_{\sigma\neq \mathrm{Id}}\sigma(q)};$$

la fraction et le dénominateur sont G-invariants, donc le numérateur aussi, d'où $r \in \mathrm{Frac}\left(A^G\right)$.

Proposition.
On considère R et S dans $k[X_1, ..., X_n]$. Alors

$$\deg \mathrm{tr}_k\,(\mathrm{Frac}\, R) = n.$$

Démonstration.
On applique le lemme aux anneaux $R \subset S$ vus dans $k[X_1, ..., X_n]$, en remarquant que l'action de G est bien algébrique. Il en résulte

$$\mathrm{Frac}\, R = \mathrm{Frac}\left(k[X_1, ..., X_n]^G\right) \simeq \mathrm{Frac}\,(k[X_1, ..., X_n])^G = k(X_1, ..., X_n)^G.$$

Par ailleurs, G peut être vu comme un sous-groupe fini d'automorphismes de $k(X_1, ..., X_n)$, et Artin nous dit alors que l'extension

$$k(X_1, ..., X_n)^G \subset k(X_1, ..., X_n)$$

est galoisienne de groupe de Galois G. Elle est en particulier finie, donc algébrique, par conséquent le dernier corollaire s'applique.

3 Théorème de Chevalley

3.1 $S(V^*)^G$ est une algèbre de type fini

Proposition.
R est une algèbre de type fini, i.e.

$$R = k[f_1, ..., f_m]$$

où les f_i peuvent être supposés homogènes de degré ≥ 1.

Démonstration.
L'idéal (R^+) de S engendré par R^+ est de type fini car $S \simeq k[X_1, ..., X_n]$ est noethérien, donc s'écrit

$$\left(R^+\right) = (f_1) + ... + (f_m)$$

où $f_i \in S$.

Montrons qu'on peut supposer les f_i dans R, en les remplaçant par $f - p(f_i)$ où p est le projecteur sur R. On montre pour cela que

$$(f_1 - p(f_1)) + ... + (f_m - p(f_m)) = (f_1) + ... + (f_m).$$

Chaque $f_i \in (R^+)$ s'écrit $f_i = s_i r_i^+$, donc $p(f_i) = p(s_i) r_i^+$ est soit nul soit non constant, *i.e.* $p(f_i) \in R^+ \cup \{0\}$. Si $p(f_i) = 0$, alors

$$(f_i - p(f_i)) = (f_i) \subset (f_1) + ... + (f_m) = (R^+),$$

et si $p(f_i) \in R^+$, alors

$$(f_i - p(f_i)) \subset (f_i) + (p(f_i)) \subset (f_i) + (R^+) = (R^+),$$

donc dans tous les cas on a

$$(f_1 - p(f_1)) + ... + (f_m - p(f_m)) \subset (R^+) + ... + (R^+) = (R^+).$$

Pour avoir l'inclusion inverse, ? ? ? ? ?

On peut par ailleurs supposer les f_i homogènes (non nuls) quitte à les décomposer selon leur composantes homogènes, et non constants (sinon $(R^+) = S$ et $1 \in R \subset S = (R^+)$, *absurde* à cause des degrés). Finalement :

$$(R^+) = (f_1) + ... + (f_m)$$

où les f_i peuvent être supposés homogènes et dans R^+.

Montrons dans ces conditions que $R = k[f_1, ..., f_m]$.

• Il est tout d'abord clair que

$$k[f_1, ..., f_m] \subset k\left[R^+\right] = R^+.$$

• Soit maintenant $f \in R$; on montre par récurrence sur $\deg f$ que $f \in k[f_1, ..., f_m]$.

Si f est constant, ok.

Si $f \in R^+$, on peut déjà supposer que f est homogène quitte à récurrer sur les composantes homogènes de degré $< \deg f$. Alors $f \in (R^+) = (f_1) + ... + (f_m)$, donc $\exists s_1, ..., s_m \in S$ tels que $f = \sum_{i=1}^m s_i f_i$. D'autre part, chaque f_i est dans $(R^+) = SR^+$, donc s'écrit $f_i = s_i' r_i^+$ où $r_i^+ \in R^+$ est homogène (car f_i homogène), d'où

$$f = \sum_{i=1}^m s_i s_i' r_i^+ = \sum_{i=1}^m s_i'' r_i^+ \text{ en posant } s_i'' = s_i s_i'.$$

On peut toujours supposer les $s_i'' r_i^+$ homogènes quitte à décomposer les s_i'' et à compter plusieurs fois les r_i^+, et de même degré que f (les autres termes de degré strictement inférieur devant s'entretuer), d'où

$$\deg s_i'' = \deg f - \deg r_i^+ < \deg f.$$

On aimerait récurrer sur les s_i'', mais ils n'ont pas de raison d'être dans R. Qu'à cela ne tienne, on projette :

$$f = p(f) = \sum_{i=1}^m p(s_i'') r_i^+$$

avec $p(s_i'') \in R$ et

$$\deg p(s_i'') \leq \deg s_i'' < \deg f,$$

d'où $p(s_i'') \in k[f_1, ..., f_m]$ par récurrence et

$$f = \sum_{i=1}^m p(s_i'') r_i^+ \in k[f_1, ..., f_m] \text{ ? ? ? ? ?}$$

comme voulu.

Remarque. Notons une certaine correspondance entre les générateurs (linéaires) de l'idéal $I = (R^+)$ et les générateurs (algébriques) de l'algèbre R.

• On vient de montrer que si $f_1, ..., f_m$ homogènes dans R^+ engendrent linéairement l'idéal (R^+), alors ils engendrent algébriquement l'algèbre des invariants $R = k[f_1, ..., f_m]$, *i.e.*

$$(R^+) = (f_1) + ... + (f_m) \implies R = k[f_1, ..., f_m].$$

• Réciproquement, supposons que $R = k[f_1, ..., f_m]$ est engendrée par $f_1, ..., f_m$ homogènes dans R^+. Alors tout élément r^+ homogène de R^+ est un polynôme non constant, donc tombe dans $(f_1) + ... + (f_m)$, d'où

$$\left(R^+\right) \subset (f_1) + ... + (f_m).$$

L'inclusion réciproque est immédiate vu que chaque f_i est dans R^+. On a finalement l'implication

$$R = k[f_1, ..., f_m] \implies \left(R^+\right) = (f_1) + ... + (f_m).$$

Conclusion.
Si $f_1, ..., f_m$ sont homogènes dans R^+, on a l'équivalence

$$R = k[f_1, ..., f_m] \iff \left(R^+\right) = (f_1) + ... + (f_m).$$

On aimerait maintenant raffiner la famille de générateurs de R, par exemple montrer qu'on peut la choisir libre. Cela fait l'objet du théorème de Chevalley.

3.2 Lemmes préparatoires

Considérons un système de générateurs minimal de R. Tentons de montrer qu'il sont algébriquement indépendants. C'est faux dans le cas général. Cela est vrai dans le cas où G est engendré par des réflexions, au sens suivant.

Définition.
On dira que G est engendré par les réflexions *si $k = \mathbb{R}$ (V est ainsi un espace euclidien) et G engendré par les réflexions orthogonales qu'il contient.*
(Puisque $\mathcal{O}(V)$ est engendré par les réflexions orthogonales, G est alors un sous-groupe fini de $\mathcal{O}(V)$)

Noter que le groupe trivial {Id} est engendré par les refléxions (au nombre de 0).

On supposera par la suite que G est engendré par les réflexions.

Lemme 0.
Soit $f \in S$, H un hyperplan et l une forme linéaire de noyau H. Pour que l divise f, il suffit que f s'annule sur H. En d'autres termes :

$$f(H) = 0 \implies l \mid f.$$

Démonstration.
Soit $(e_1, ..., e_{n-1})$ une base de H et e_n qui la complète de façon à ce que $l = e_n^*$. Dans la base $(e_1, ..., e_n)$, f est un polynôme $P(e_1^*, ..., e_n^*)$ et $l = e_n^*$. On écrit alors P en isolant le terme sans X_n : $P = AX_n + B$ où $B \in \mathbb{R}[X_1, ..., X_{n-1}]$. On en déduit

$$\begin{aligned} P(e_1^*, ..., e_n^*) &= A(e_1^*, ..., e_n^*)\, e_n^* + B\left(e_1^*, ..., e_{n-1}^*\right) \\ f &= \alpha l + B\left(e_1^*, ..., e_{n-1}^*\right) \text{ où } \alpha \in S. \end{aligned}$$

En évaluant la précédente égalité sur un élément $x = \sum_{i=1}^{n-1} \lambda_i e_i$ de H, on obtient

$$0 = f(x) = \alpha(x) \underbrace{e_n^*(x)}_{=0} + B\left(e_1^*(x), ..., e_{n-1}^*(x)\right) = B(\lambda_1, ..., \lambda_{n-1}),$$

donc B est nul sur $\mathbb{R}^{n-1}$, *i.e.* nul tout court, d'où $f = \alpha l$ comme voulu.

Lemme 1.
Soit $f \in S$. Si s est une réflexion par rapport à H et l une forme linéaire de noyau H, alors l divise $s(f) - f$.

Démonstration.
Soit $g = s(f) - f$. D'après le lemme 0, il suffit de montrer que g est nul sur H. Soit donc $x \in H$, *i.e.* x fixe par s. On vérifie :

$$g(x) = [s(f) - f](x) = f \circ s^{-1}\left(\underbrace{x}_{=s(x)}\right) - f(x) = f(x) - f(x) = 0.$$

Lemme 2.
Soit $f \in S$ de degré $\deg f \geq 1$. Si $\sigma(f) - f \in (R^+)$ pour toute réflexion $\sigma \in G$, alors $f \in (R^+)$.

Démonstration.
Remarquons tout d'abord sur G stabilise (R^+) : si $(s, r) \in S \times R^+$ et $g \in G$, alors

$$g(sr) = g(s)\, g(r) = \underbrace{g(s)}_{\in S}\underbrace{r}_{\in R^+} \in \left(R^+\right).$$

Montrons maintenant que

$$\sigma(f) - f \in \left(R^+\right)$$

pour tout élément σ de G, par récurrence sur le nombre p de réflexions composant σ.
Pour $p = 0$, $\sigma = \mathrm{Id}$, d'où $\sigma(f) - f = 0 \in (R^+)$.
Pour $p = 1$, c'est l'hypothèse.
Pour $p \geq 2$, soit $\sigma = \prod_{i=1}^{p} \sigma_i$ où les σ_i sont des réflexions. En notant $\tau = \prod_{i=2}^{p} \sigma_i$ et en utilisant la remarque ainsi que les hypothèses de récurrence pour 1 et $p-1$, on a

$$\sigma(f) - f = \sigma_1\tau(f) - f = \underbrace{\sigma_1\left(\underbrace{\tau(f) - f}_{\in(R^+)}\right)}_{\in(R^+)} + \underbrace{\sigma_1(f) - f}_{\in(R^+)} \in \left(R^+\right).$$

Pour conclure, on somme sur tous les éléments du groupe afin de projeter :

$$\sum_{\sigma \in G} \frac{1}{|G|}\left(\sigma(f) - f\right) \in \left(R^+\right) \implies \underbrace{p(f)}_{\in R} - f \in \left(R^+\right);$$

or $p(f)$ n'est pas constant ? ? ? ? ?, donc se trouve dans $R^+ \cup \{0\}$, d'où $f \in (R^+)$ comme voulu.

Lemme clef.
Soit $f_1, ..., f_{m\geq 1} \in R^+$ tels que $f_1 \notin (f_2) + ... + (f_m)$ (traduit l'hypothèse de minimalité). Alors

$$\forall s_1, ..., s_m \in S,\ \sum_{i=1}^{m} s_i f_i = 0 \implies s_1 \in \left(R^+\right).$$

Démonstration.
On fait une récurrence sur $d = \deg s_1$.
• Si $d = 0$, alors $s_1 = 0 \in (R^+)$, sinon $s_1 \in k$ serait inversible et on aurait $f_1 = \sum_{i=2}^{m} \frac{s_i}{s_1} f_i$, d'où (en projetant)

$$f_1 = \sum_{i=2}^{m} \underbrace{p\left(\frac{s_i}{s_1}\right)}_{\in R} f_i,$$

absurde par hypothèse.

• Pour $d \geq 1$, on applique un $\sigma \in G$ à l'égalité $\sum_{i=1}^{m} s_i f_i = 0$: $\sum_{i=1}^{m} \sigma(s_i) f_i = 0$, d'où (par soustraction)

$$\sum_{i=1}^{m} (\sigma(s_i) - s_i) f_i = 0.$$

Fixons $\sigma \in G$ une réflexion et $l \in V^*$ telle que $\operatorname{Ker} l = \operatorname{Fix} \sigma$. D'après le lemme 1, l divise $\sigma(s_i) - s_i$, *i.e.*

$$\sigma(s_i) - s_i = l s_i'$$

où $s_i' \in S$ et

$$\begin{aligned} \deg s_i' &= \deg(\sigma(s_i) - s_i) - \deg l \\ &\leq \max(\deg \sigma(s_i), \deg s_i) - \deg l \\ &= \max(\deg s_i, \deg s_i) - 1 \\ &= \deg s_i - 1. \end{aligned}$$

On en déduit $\sum_{i=1}^{m} l s_i' f_i = 0$,d'où (en simplifiant par l vu dans $k[X_1, ..., X_n]$) $\sum_{i=1}^{m} s_i' f_i = 0$ avec $\deg s_i' < \deg s_i$. Par hypothèse de récurrence, on a $s_1' \in (R^+)$, d'où

$$\sigma(s_1) - s_1 = l s_1' \in \left(R^+\right),$$

ceci tenant pour tout réflexion $\sigma \in G$. On conclut alors par le lemme 2 : $s_1 \in (R^+)$.

3.3 Théorème de Chevalley

Définiton.
Soit A une sous-algèbre de $\mathbb{R}[X_1, ..., X_r]$. On dit que $(f_1, ..., f_r)$ forme un ensemble basique *de A si*
• *$A = \mathbb{R}[f_1, ..., f_r]$ est engendrée par les $f_1, ..., f_r$;*
• *les f_i sont homogènes et algébriquement indépendants.*

Il s'agit de l'analogue d'une base d'un espace vectoriel.

Remarque.
Si R admet un ensemble basique $(f_1, ..., f_r)$, alors nécessairement il est de cardinal $r = n = \dim V$.
En effet, si $R = k[f_1, ..., f_r]$, alors

$$\operatorname{Frac} R \simeq \operatorname{Frac} k[f_1, ..., f_r] \simeq k(f_1, ..., f_r) \simeq k(X_1, ..., X_r),$$

d'où $\deg \operatorname{tr}_k(\operatorname{Frac} R) = r$, mais on sait par ailleurs que $\deg \operatorname{tr}_k(\operatorname{Frac} R) = n$.

Théorème (Chevalley).
Soit G un groupe fini engendré par les réflexions Alors R admet un ensemble basique.

Démonstration.
On prend $(f_1, ..., f_r)$ une famille minimale de générateurs homogènes de R (un tel système existe par la proposition préliminaire). Il suffit de montrer qu'ils sont libres pour qu'ils forment un ensemble basique de R.
Supposons par l'absurde que les $f_1, ..., f_r$ sont liés, *i.e.* $P(f_1, ..., f_r) = 0$ où $P \neq 0$. Posons $d_i = \deg f_i$.
On dérive $P(f_1, ..., f_r) = 0$ selon x_k :

$$\sum_{i=1}^{r} \underbrace{\frac{\partial P}{\partial X_i}(f_1, ..., f_r)}_{\in R} \underbrace{\frac{\partial f_i}{\partial x_k}}_{\in S} = 0 \text{ pour tout } k = 1, ..., n.$$

On a presque les conditions du lemme clef : en posant

$$F_i = \frac{\partial P}{\partial X_i}(f_1, ..., f_r)$$

(remarquer que $\deg F_i = d - d_i$), on a

$$\sum_{i=1}^{r} \underbrace{\frac{\partial f_i}{\partial x_k}}_{\in S} \underbrace{F_i}_{\in R} = 0$$

pour tout $k = 1, ..., n$, donc il suffirait de prendre les F_i minimaux.

Regardons pour cela l'idéal

$$J = RF_1 + ...RF_r.$$

Quitte à réindexer, supposons que $F_1, ..., F_{s \leq r}$ l'engendrent minimalement, avec

$$F_1 \notin RF_2 + ... + RF_s.$$

Ainsi, pour $i > s$, $F_i \in J$ se décompose selon $F_1, ..., F_s$, mettons en

$$F_i = \sum_{j=1}^{s} g_{i,j} F_j$$

où $g_{i,j} \in R$. On réécrit maintenant

$$\sum_{i=1}^{r} \frac{\partial f_i}{\partial x_k} F_i = 0$$

sous la forme

$$\sum_{i=1}^{s} \frac{\partial f_i}{\partial x_k} F_i + \sum_{i>s} \left(\sum_{j=1}^{s} g_{i,j} F_j \right) \frac{\partial f_i}{\partial x_k} = 0,$$

i.e.

$$\sum_{j=1}^{s} \frac{\partial f_j}{\partial x_k} F_i + \sum_{j=1}^{s} \left(\sum_{i>s} g_{i,j} \frac{\partial f_i}{\partial x_k} \right) F_j = 0,$$

ou encore

$$\sum_{j=1}^{s} \underbrace{\left(\frac{\partial f_j}{\partial x_k} + \sum_{i>s} g_{i,j} \frac{\partial f_i}{\partial x_k} \right)}_{\in S} F_i = 0.$$

On peut maintenant appliquer le lemme clef à $F_1, ...F_s$:

$$\frac{\partial f_1}{\partial x_k} + \sum_{i>s} g_{i,1} \frac{\partial f_i}{\partial x_k} \in (R^+).$$

D'après la correspondance entre (R^+) et R, on sait que

$$(R^+) = (f_1) + ... + (f_r)$$

puisqu'aucun des f_i ne saurait être constant (par minimalité des générateurs) (et donc les f_i sont dans R^+), d'où

$$\frac{\partial f_1}{\partial x_k} + \sum_{i>s} g_{i,1} \frac{\partial f_i}{\partial x_k} = \sum_{j=1}^{r} s_{j,k} f_j$$

où $s_{j,k} \in S$. Ceci tenant pour tout $k = 1, ..., r$, il reste à appliquer l'identité d'Euler : pour f polynomiale homogène de degré $\deg f$:

$$\sum_{k=1}^{r} X_k \frac{\partial f}{\partial X_k} = (\deg f)\, f.$$

On somme donc sur k après multiplication par X_k :

$$\left(\sum_{k=1}^{r} X_k \frac{\partial f_1}{\partial x_k} \right) + \sum_{i>s} g_{i,1} \left(\sum_{k=1}^{r} X_k \frac{\partial f_i}{\partial x_k} \right) = \sum_{j=1}^{r} \left(\sum_{k=1}^{r} X_k s_{j,k} \right) f_j.$$

Ainsi,

$$d_1 \times f_1 + \sum_{i>s} g_{i,1} \left(d_i \times f_i \right) = \sum_{j=1}^{r} \underbrace{S_j}_{\in S,\ \deg S_j \geq 1} f_j.$$

Il reste à faire des considérations sur les degrés de chaque terme pour pouvoir conclure. Il nous faut déjà les $\deg g_{i,1}$.

En reprenant la décomposition

$$F_i = \sum_{j=1}^{s} g_{i,j} F_j,$$

il raisonnable de croire que l'on puisse supposer les $g_{i,j}F_j$ inférieurs à F_i en degré, *i.e.*

$$\deg g_{i,j} \leq \deg F_i - \deg F_j.$$

Pour le montrer, supposons dans un premier temps les $F_1, ..., F_s$ et les $g_{i,j}$ homogènes. Alors les termes $g_{i,j}F_j$ de degré strictement plus grand que $\deg F_i$ doivent s'entretuer, donc on peut les supposer nuls, d'où le résultat. Dans le cas général, on décompose les $F_1, ..., F_s$ et les $g_{i,j}$ selon leur composantes homogènes, et on retrouve le résultat en considérant les composantes de plus haut degré ? ? ? ? ?.

Concluons. Dans l'expression

$$d_1 \times f_1 + \sum_{i>s} g_{i,1} \left(d_i \times f_i\right) = \sum_{j=1}^{r} \underbrace{S_j}_{\in S,\ \deg S_j \geq 1} f_j,$$

le degré à gauche est borné par $\deg f_1$, puisque

$$\deg\left(g_{i,1} f_i\right) = \deg g_{i,1} + \deg f_i \leq \left(\deg F_i - \deg F_1\right) + \left(d - \deg F_i\right) = d - \deg F_1 = \deg f_1,$$

donc le $S_1 f_1$ dans le membre de droite doit disparaître car

$$\deg S_1 f_1 = \deg S_1 \deg f_1 \geq 1 + \deg f_1.$$

En faisant tout passer à droite sauf f_1, il reste alors

$$f_1 = \sum_{j>1} \lambda_j f_j,$$

absurde par minimalité de r.

Exemple.

Soit $\varepsilon_1, ..., \varepsilon_n$ une bon de $\mathbb{R}^n$, $G = \mathfrak{S}_n$ vu comme matrices de permutations. Les tranpositions (i, j) sont des réflexions de vecteurs normal $\varepsilon_i - \varepsilon_j$, et elles engendrent bien G. On est donc dans les conditions du théorème :

$$\mathbb{R}\left[X_1, ..., X_n\right]^{\mathfrak{S}_n} = \mathbb{R}\left[f_1, ..., f_n\right].$$

Par exemple, on sait que les *fonctions symétriques élémentaires*

$$f_i = \sum_{1 \leq k_1 < ... < k_i \leq n} X_{k_1} ... X_{k_i}$$

conviennent, ou bien les *sommes de Newton*

$$f_i = X_1^i + ... + X_n^i.$$

On notera dans cet exemple que les degrés d_i des f_i sont les mêmes à permutation près, et vérifient

$$\begin{aligned} \prod d_i &= |G| \\ \sum \left(d_i - 1\right) &= \#\left\{\text{réflexions de } G\right\}. \end{aligned}$$

C'est général, et montré dans la suite.

4 Critère d'indépendance algébrique

Soient $f_1, ..., f_n$ dans $S(k^n)$ homogènes. On appelle *Jacobien* de $f_1, ..., f_n$ le polynôme dans $k[X_1, ..., X_n]$

$$J(f_1, ..., f_n) = \det\left(\frac{\partial f_i}{\partial X_j}\right).$$

Théorème.
$(f_1, ..., f_n)$ est libre ssi $J(f_1, ..., f_n) \neq 0$.

Démonstration.
• Supposons $(f_1, ..., f_n)$ liée. Soit P non nul dans $k[Y_1, ..., Y_n]$ de degré minimal telle que $P(f_1, ..., f_n) = 0$. On dérive par rapport à X_k :

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

ce qui s'écrit encore

$$\begin{pmatrix} \frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_n}{\partial X_1} \\ \vdots & & \vdots \\ \frac{\partial f_1}{\partial X_n} & \cdots & \frac{\partial f_n}{\partial X_n} \end{pmatrix} \begin{pmatrix} \frac{\partial P}{\partial X_1}(f_1, ..., f_n) \\ \vdots \\ \frac{\partial P}{\partial X_n}(f_1, ..., f_n) \end{pmatrix} = 0$$

On a $\deg \frac{\partial P}{\partial X_k} < \deg P$, donc les $\frac{\partial P}{\partial X_k}(f_1, ..., f_n)$ ne sont pas nuls (car $\deg P$ minimal et k est de caractéristique nulle), donc on a un vecteur non nul annulé par la matrice $\left(\frac{\partial f_i}{\partial X_j}\right)$ sur le corps $k(Y_1, ..., Y_n)$, donc le déterminant de cette matrice est nul.

• Supposons $(f_1, ..., f_n)$ algébriquement indépendants. Puisque $\deg \mathrm{tr}_k\, k(X_1, ..., X_n) = n$, la famille $(X_i, f_1, ..., f_n)$ est liée pour tout $i = 1, ...n$; il existe donc P_i dans $k[Y_0, Y_1, ..., Y_n]$ telle que

$$P_i(X_i, f_1, ..., f_n) = 0$$

avec $\deg_{Y_0} P_i > 0$. On choisit P_i non nul annulateur de $(X_i, f_1, ..., f_n)$ de degré en Y_0 minimal.

En dérivant par rapport à X_k, il vient :

$$\frac{\partial P_i}{\partial Y_0}(X_i, f_1, ..., f_n)\, \delta_i^k + \sum_{j=1}^{n} \frac{\partial P_i}{\partial Y_j}(X_i, f_1, ..., f_n) \frac{\partial f_j}{\partial X_k} = 0$$

$$\sum_{j=1}^{n} \frac{\partial P_i}{\partial Y_j}(X_i, f_1, ..., f_n) \frac{\partial f_j}{\partial X_k} = -\frac{\partial P_i}{\partial Y_0}(X_i, f_1, ..., f_n)\, \delta_i^k.$$

En posant $\begin{cases} A = \left(\frac{\partial P_i}{\partial Y_j}(X_i, f_1, ..., f_n)\right)_{1 \leq i,j \leq n} \\ B = \left(\frac{\partial f_j}{\partial x_k}\right)_{1 \leq j,k \leq n} \end{cases}$ dans $\mathcal{M}_n(k(X_1, ..., X_n))$, on obtient

$$\begin{aligned} \sum_{j=1}^{n} A_{i,j} B_{j,k} &= -\frac{\partial P_i}{\partial Y_0}(X_i, f_1, ..., f_n)\, \delta_i^k \\ [AB]_{i,k} &= -\frac{\partial P_i}{\partial Y_0}(X_i, f_1, ..., f_n)\, \delta_i^k \\ AB &= -\operatorname{Diag}\left(\frac{\partial P_i}{\partial Y_0}(X_i, f_1, ..., f_n)\right). \end{aligned}$$

Or les $\frac{\partial P_i}{\partial Y_0}(X_i, f_1, ..., f_n)$ sont tous non nuls, sinon ou bien $\frac{\partial P_i}{\partial Y_0} = 0$, *i.e.* P_i s'écrit

$$P_i(Y_0, ..., Y_n) = Q_i(X_1, ..., X_n),$$

d'où $Q_i(f_1, ..., f_n) = P_i(X_i, f_1 ..., f_n) = 0$, donc $Q_i = 0$ (par liberté des f_j) et $P_i = 0$, *absurde*, ou bien $\frac{\partial P_i}{\partial Y_0}$ est un polynôme non nul annulateur de $(X_i, f_1, ..., f_n)$, *absurde* par minimalité de $\deg_{Y_0} P_i$. Ainsi $\det AB \neq 0$, d'où $J(f_1, ..., f_n) = \det B \neq 0$.

5 Degrés des générateurs de $\mathbb{R}[x_1, ..., x_n]^G$

Dans cette section, G est toujours un sous-groupe fini de $GL(V)$, mais G n'est plus supposé engendré par les réflexions et on ne suppose plus que $k = \mathbb{R}$.

5.1 Egalités des degrés

Proposition.
Si $(f_1, \ldots, f_n)$ et $(g_1, \ldots, g_n)$ sont deux ensembles basiques de R, alors

$$\{\deg f_i\} = \{\deg g_i\}.$$

Démonstration.
On écrit g_i comme un polynôme en les f_j et vice-versa :

$$\begin{cases} g_i(x_1, ..., x_n) = G_i(f_1(x_1, ..., x_n), ..., f_n(x_1, ..., x_n)) \\ f_i(x_1, ..., x_n) = F_i(g_1(x_1, ..., x_n), ..., g_n(x_1, ..., x_n)) \end{cases}.$$

On a donc

$$f_i = F_i(g_1, ..., g_n) = F_i(G_1(f_1, ..., f_n), ..., G_n(f_1, ..., f_n)).$$

On dérive formellement par rapport à f_k :

$$\delta_i^k = \sum_{j=1}^{n} \frac{\partial F_i}{\partial X_j} \frac{\partial G_j}{\partial X_k}.$$

On traduit cela matriciellement en posant $\begin{cases} A = \left(\frac{\partial F_i}{\partial X_j}\right)_{1 \leq i,j \leq n} \\ B = \left(\frac{\partial G_j}{\partial X_k}\right)_{1 \leq j,k \leq n} \end{cases}$ et en réécrivant

$$[\mathrm{Id}]_{i,k} = \sum_{j=1}^{n} A_{i,j} B_{j,k} = [AB]_{i,k}.$$

On en déduit $AB = \mathrm{Id}$ et $\det\left(\frac{\partial F_i}{\partial X_j}\right) = \det A \neq 0$. Il existe donc une permutation σ telle que

$$\varepsilon(\sigma)\left(\frac{\partial F_1}{\partial X_{\sigma(1)}} ... \frac{\partial F_n}{\partial X_{\sigma(n)}}\right) \neq 0.$$

On a donc $\frac{\partial F_i}{\partial X_{\sigma(i)}} \neq 0$ pour tout $i = 1, ..., n$, *i.e.* $\deg_{X_{\sigma(i)}} F_i > 0$, donc $g_{\sigma(i)}$ apparaît explicitement lorsqu'on écrit $f_i = F_i(g_1, ..., g_n)$, d'où $\deg f_i \leq \deg g_{\sigma(i)}$.On en déduit

$$\sum_{i=1}^{n} \deg f_i \leq \sum_{i=1}^{n} \deg g_{\sigma(i)} = \sum_{i=1}^{n} \deg g_i,$$

d'où par symétrie $\sum_{i=1}^{n} \deg f_i = \sum_{i=1}^{n} \deg g_i$. Puisque $\deg f_i \leq \deg g_{\sigma(i)}$, on a nécessairement $\deg f_i = \deg g_{\sigma(i)}$ pour tout i.

5.2 Une identité remarquable

Lemme.
Soit E un k-espace vectoriel et $\rho : G \longrightarrow GL(E)$ un morphisme de groupes. Alors l'endomorphisme

$$p = \frac{1}{|G|} \sum_{g \in G} \rho(g)$$

est le projecteur sur les vecteurs de E invariants par $\rho(G)$, i.e.

$$\operatorname{Im} p = E^{\rho(G)}.$$

Démonstration
D'une part, on a

$$x \in \operatorname{Fix} \rho(G) \implies p(x) = \frac{1}{|G|} \sum_{g \in G} \rho(g)(x)$$

$$\implies p(x) = \frac{1}{|G|} \sum_{g \in G} x \implies p(x) = x \implies x \in \operatorname{Im} p,$$

d'autre part, on a

$$\begin{aligned}
& y \in \operatorname{Im} p \\
\implies \quad & \exists x \in E \text{ tel que } y = p(x) \\
\implies \quad & \forall g \in G,\ \rho(g)(y) = \rho(g)\left(\frac{1}{|G|} \sum_{h \in G} \rho(h)(x)\right) \\
\implies \quad & \rho(g)(y) = \frac{1}{|G|} \sum_{h \in G} \rho(g)\rho(h)(x) \\
\implies \quad & \rho(g)(y) = \frac{1}{|G|} \sum_{h \in G} \rho(h)(x) \\
\implies \quad & \rho(g)(y) = y \\
\implies \quad & y \in \operatorname{Fix} \rho(G).
\end{aligned}$$

Par ailleurs, un calcul déjà fait en 1.3 montre que $p^2 = p$, *i.e.* p projecteur.

Proposition.
Supposons que $(f_1, ..., f_n)$ soit un ensemble basique de R, avec $d_i = \deg f_i$. On a alors, dans $k((X))$:

$$\frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(\mathrm{Id} - Xg)} = \prod_{i=1}^{n} \frac{1}{(1 - X^{d_i})}.$$

Plus précisément, ces deux quantités sont une même expression de la série génératrice

$$\sum_{i \geq 0} (\dim R_i) X^i$$

où R_i désigne la composante homogène de R de degré i.

Démonstration.
• Travaillons le membre du gauche.
Soit $g \in G$. On a $g^{|G|} = \mathrm{Id}$, d'où un polynôme annulateur scindé simple (dans un corps de dissociation K de $X^{|G|} - 1$) de g, qui est par conséquent diagonalisable (dans K) de valeurs propres $\lambda_1, \ldots, \lambda_n$. On a donc

$$\det(\mathrm{Id} - Xg) = \prod_{i=1}^{n} (1 - X\lambda_i),$$

d'où (en développant dans $K((X))$)

$$\begin{aligned}\frac{1}{\det(\mathrm{Id}-Xg)} &= \frac{1}{1-X\lambda_1}...\frac{1}{1-X\lambda_n}\\ &= \left(1+\lambda_1 X+\lambda_1^2X^2+...\right)...\left(1+\lambda_n X+\lambda_n^2X^2+...\right)\\ &= \sum_{i_1,...,i_n\geq 0}\left(X\lambda_1\right)^{i_1}...\left(X\lambda_n\right)^{i_n}\\ &= \sum_{i_1,...,i_n\geq 0}X^{i_1+...+i_n}\lambda_1^{i_1}...\lambda_n^{i_n}\\ &= \sum_{i\geq 0}\left(\sum_{i_1+...+i_n=i}\lambda_1^{i_1}...\lambda_n^{i_n}\right)X^i.\end{aligned}$$

Montrons que $\sum_{i_1+...+i_n=i}\lambda_1^{i_1}...\lambda_n^{i_n}=\mathrm{tr}\,S^i(g)$ en utilisant l'identité

$$\text{trace} = \text{sommes des valeurs propres}$$

sur l'endomorphisme $S^i\left(g^{-1}\right)$.

Soit $e_1,...,e_n$ une base de V qui diagonalise g (existence ? ? ? ? ? on tensorise V par une extension k où $X^{|G|}-1$ se scinde), et posons $l_i=e_i^*$.Alors $l_1,...,l_n$ est une base de V^*, donc la partie homogène S_i de degré total i a pour base

$$\left\{\left(l_1^{i_1}\cdot...\cdot l_n^{i_n}\right)\ \text{tels que}\ i_1+...+i_n=i\right\}.$$

On considère comme annoncé l'endomorphisme

$$S^i\left(g^{-1}\right):\left\{\begin{array}{ccc}S_i & \longrightarrow & S_i\\ f_1\cdot...\cdot f_i & \longmapsto & (f_1\circ g)\cdot...\cdot(f_i\circ g)\end{array}\right.,$$

et on remarque que la base

$$\left\{\left(l_1^{i_1}\cdot...\cdot l_n^{i_n}\right)\ \text{tels que}\ i_1+...+i_n=i\right\}$$

diagonalise $S^i(g)$ selon les valeurs propres $\lambda_1^{i_1}...\lambda_n^{i_n}$:

$$S^i(g)\left(l_1^{i_1}\cdot...\cdot l_n^{i_n}\right)=(l_1\circ g)^{i_1}\cdot...\cdot(l_n\circ g)^{i_n}=\left(\lambda_1 l_1\right)^{i_1}\cdot...\cdot\left(\lambda_n l_n\right)^{i_n}=\lambda_1^{i_1}...\lambda_n^{i_n}\left(l_1^{i_1}\cdot...\cdot l_n^{i_n}\right).$$

On en déduit

$$\sum_{i_1+...+i_n=i}\lambda_1^{i_1}...\lambda_n^{i_n}=\sum_{\lambda\in\mathrm{Sp}\,S^i(g^{-1})}\lambda=\mathrm{tr}\,S^i\left(g^{-1}\right)$$

$$\frac{1}{\det(\mathrm{Id}-Xg)}=\sum_{i\geq 0}\mathrm{tr}\,S^i\left(g^{-1}\right)X^i$$

$$\frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(\mathrm{Id}-Xg)}=\frac{1}{|G|}\sum_{g\in G}\sum_{i\geq 0}\mathrm{tr}\,S^i\left(g^{-1}\right)X^i$$

$$=\sum_{i\geq 0}\mathrm{tr}\left(\frac{1}{|G|}\sum_{g\in G}S^i\left(g^{-1}\right)\right)X^i=\sum_{i\geq 0}\mathrm{tr}\left(\frac{1}{|G|}\sum_{g\in G}S^i(g)\right)X^i.$$

D'après le lemme, $\frac{1}{|G|}\sum_{g\in G}S^i(g)$ est le projecteur sur les vecteurs de $S^i(V^*)$ invariants par $S^i(G)$. Par conséquent

$$\mathrm{tr}\left(\frac{1}{|G|}\sum_{g\in G}S^i(g)\right)=\mathrm{rg}\left(\frac{1}{|G|}\sum_{g\in G}S^i(g)\right)=\dim\left(S^i\left(V^*\right)^G\right)=\dim R_i,$$

et donc

$$\frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(\mathrm{Id}-Xg)}=\sum_{i\geq 0}\left(\dim R_i\right)X^i.$$

• On part maintenant du membre de droite, qu'on plonge dans $k((X))$:

$$\begin{aligned}\frac{1}{1-X^{d_1}}...\frac{1}{1-X^{d_n}} &= \left(1+X^{d_1}+\left(X^{d_1}\right)^2+...\right)...\left(1+X^{d_n}+\left(X^{d_n}\right)^2+...\right)\\ &= \sum_{i_1,...,i_n\geq 0}\left(X^{d_1}\right)^{i_1}...\left(X^{d_n}\right)^{i_n}=\sum_{i_1,...,i_n\geq 0}X^{i_1d_1+...+i_nd_n}=\sum_{i\geq 0}\left(\sum_{i_1d_1+...+i_nd_n=i}1\right)X^i\\ &= \sum_{i\geq 0}\#\left\{(i_1,...,i_n)\in\mathbb{N}^n\ ;\ \sum_{i=1}^n i_id_i=i\right\}X^i.\end{aligned}$$

Or, si $f_1,...,f_n$ est un système basisque de R, alors $\deg f_i=d_i$ et

$$\left\{\left(f_1^{i_1}\cdot...\cdot f_n^{i_n}\right)\ ;\ i_1d_1+...+i_nd_n=i\right\}$$

est une base de R_i. On a donc

$$\dim R_i=\#\left\{(i_1,...,i_n)\in\mathbb{N}^n\ ;\ \sum_{i=1}^n i_id_i=i\right\},$$

d'où

$$\frac{1}{1-X^{d_1}}...\frac{1}{1-X^{d_n}}=\sum_{i\geq 0}\#\left\{(i_1,...,i_n)\in\mathbb{N}^n\ ;\ \sum_{i=1}^n i_id_i=i\right\}X^i=\sum_{i\geq 0}\left(\dim R_i\right)X^i,\ \textit{CQFD.}$$

5.3 Somme et produit des degrés

On suppose maintenant que V est euclidien ($k=\mathbb{R}$), mais on n'impose pas que G soit engendré par les réflexions.

Lemme.
Soit $g\in G$ tel que $g\neq \mathrm{Id}$. On a l'équivalence (dans $\mathbb{C}[X]$)

$$(1-X)^{n-1}\mid\det(\mathrm{Id}-Xg)\iff g\textit{ est une réflexion.}$$

Démonstration
Si $(1-X)^{n-1}\mid\det(\mathrm{Id}-Xg)$, alors $\det(\mathrm{Id}-Xg)$ est scindé simple sur $\mathbb{C}$. Or,

$$\det(\mathrm{Id}-Xg)=(-1)^n(\det g)\det\left(X\,\mathrm{Id}-g^{-1}\right),$$

donc le polynôme caractéristique $\chi_h=\det(X\,\mathrm{Id}-h)$ de $h=g^{-1}$ est scindé simple sur $\mathbb{C}$. Puisque la somme des racines de χ_h doit être réelle, la dernière racine est réelle. Comme elle est de module 1 dans $\mathbb{R}$ et ne peut valoir 1 (sinon $h=\mathrm{Id}$), elle vaut -1. h est donc bien une réflexion, donc $g=h^{-1}$ aussi.
La réciproque est immédiate.

Théorème.
Soit G un sous-groupe fini de $GL(V)$ (non nécessairement engendré par les réflexions). On note N le nombre de réflexions dans G. Supposons que $(f_1,...,f_n)$ soit un ensemble basique de R, avec $d_i=\deg f_i$. Alors

$$\begin{cases}\prod_{i=1}^n d_i=|G|\\ \sum_{i=1}^n(d_i-1)=N\end{cases}.$$

Démonstration .
On part de l'identité remarquable établie tantôt :

$$\frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(\mathrm{Id}-Xg)}=\prod_{i=1}^n\frac{1}{(1-X^{d_i})}.$$

En séparant (à l'aide du lemme) les trois cas $\begin{cases} g = \mathrm{Id} \\ g \text{ réflexion} \\ g \text{ autre chose} \end{cases}$ pour le membre de gauche, en écrivant

$$\left(1 + X + ... + X^{d_i - 1}\right)(1 - X) = 1 - X^{d_i}$$

pour le membre de droite, on obtient en multipliant l'égalité par $(1-X)^n$:

$$\frac{1}{|G|}\left(1 + N\frac{1-X}{1+X} + (1-X)^2 f(X)\right) = \prod_{i=1}^{n} \frac{1}{1 + X + ... + X^{d_i - 1}}$$

où f est une fraction rationnelle dont 1 n'est pas un pôle.

On évalue en $X = 1$: $\frac{1}{|G|} = \prod_{i=1}^{n} \frac{1}{d_i}$, d'où la première relation.

Pour obtenir l'autre relation, on dérive. En notant que $\frac{1-X}{1+X} = \frac{2}{1+X} - 1$,on obtient en dérivant

$$\begin{aligned} \frac{1}{|G|}\left(1 + 2N\frac{1}{1+X} - N + (1-X)^2 f(X)\right)' &= \prod_{i=1}^{n}\left(\frac{1}{1 + X + ... + X^{d_i - 1}}\right) \sum_{i=1}^{n} \frac{\left(\frac{1}{1+X+...+X^{d_i-1}}\right)'}{\left(\frac{1}{1+X+...+X^{d_i-1}}\right)} \\ \frac{1}{|G|}\left(-2N\frac{1}{(1+X)^2} + (1-X)\, g(X)\right) &= \prod_{i=1}^{n} \frac{1}{1 + X + ... + X^{d_i - 1}} \sum_{i=1}^{n} \frac{-\frac{1+2X+...+(d_i-1)X^{d_i-2}}{\left(1+X+...+X^{d_i-1}\right)^2}}{\frac{1}{1+X+...+X^{d_i-1}}}, \end{aligned}$$

puis on évalue en $X = 1$:

$$\begin{aligned} \frac{1}{|G|}\left(-2N\frac{1}{4}\right) &= \prod_{i=1}^{n} \frac{1}{d_i} \sum_{i=1}^{n} \frac{-\left(\frac{(d_i-1)d_i}{\frac{2}{(d_i)^2}}\right)}{\frac{1}{d_i}} \\ \frac{-N}{2|G|} &= \frac{1}{|G|} \sum_{i=1}^{n} \left(-\frac{1}{2}\right) \frac{(d_i - 1)\, d_i}{\frac{1}{d_i} d_i^2} \\ N &= \sum_{i=1}^{n} (d_i - 1). \end{aligned}$$

6 Théorème de Shepard - Todd

On étudie la réciproque du théorème de Chevalley. On se place donc dans un cadre euclidien ($k = \mathbb{R}$).

Théorème (Shepard - Todd)
Soit G sous-groupe fini de $GL(V)$. Si R admet un ensemble basique, alors G est engendré par les réflexions qu'il contient.

Démonstration
Si R admet un ensemble basique, on peut écrire

$$R \simeq \mathbb{R}[f_1, ..., f_n]$$

où les f_i sont libres homogènes.

Soit H le sous-groupe de G engendré par les réflexions de G. On va montrer que $H = G$.

On applique Chevalley à H : il y a des invariants h_i homogènes libres tels que

$$S(V^*)^H \simeq \mathbb{R}[h_1, ..., h_n].$$

Puisque $R = S(V^*)^G \subset S(V^*)^H$, les $f_i \in R$ de décomposent dans $S(V^*)^H$:

$$f_i = F_i(h_1, ..., h_n)$$

où $F_i \in \mathbb{R}[Y_1, ..., Y_n]$. En dérivant selon X_k, on obtient

$$\frac{\partial f_i}{\partial X_k} = \sum_{j=1}^{n} \frac{\partial F_i}{\partial Y_j} \frac{\partial h_j}{\partial X_k}.$$

En posant $\begin{cases} A = \left(\frac{\partial F_i}{\partial Y_j}\right)_{1 \leq i,j \leq n} \\ B = \left(\frac{\partial h_j}{\partial X_k}\right)_{1 \leq j,k \leq n} \end{cases}$, cela se met sous la forme $\left(\frac{\partial f_i}{\partial X_k}\right)_{1 \leq i,k \leq n} = AB$, d'où

$$J(f_1, ..., f_n) = \det A \det B = J(F_1, ..., F_n) J(h_1, ..., h_n).$$

Puisque les f_i sont libres, $J(f_1, ..., f_n)$ est non nul, donc $J(F_1, ..., F_n)$ est aussi non nul, d'où un $\sigma \in \mathfrak{S}_n$ tel que $\frac{\partial F_1}{\partial Y_{\sigma(1)}} ... \frac{\partial F_n}{\partial Y_{\sigma(n)}} \neq 0$. Ainsi, $\frac{\partial F_i}{\partial Y_{\sigma(i)}} \neq 0$ pour tout $i = 1, ..., n$, *i.e.* $\deg_{Y_{\sigma(i)}} F_i > 0$,donc $h_{\sigma(i)}$ apparaît vraiment dans $f_i = F_i(h_1, ..., h_n)$, d'où

$$\deg f_i \geq \deg h_{\sigma(i)}.$$

D'autre part,

$$N = \#\{\text{réflexions de } H\} = \#\{\text{réflexions de } G\},$$

donc en appliquant le théorème portant sur la somme et le produit des degrés, on a obtient

$$\sum_{i=1}^{n} (\deg f_i - 1) = N = \sum_{i=1}^{n} (\deg h_i - 1) = \sum_{i=1}^{n} \left(\deg h_{\sigma(i)} - 1\right),$$

d'où l'égalité des degrés $\deg f_i = \deg h_{\sigma(i)}$. En appliquant la seconde relation du théorème, on en déduit :

$$|H| = \prod_{i=1}^{n} \deg h_i = \prod_{i=1}^{n} \deg h_{\sigma(i)} = \prod_{i=1}^{n} \deg f_i = |G|,$$

et comme $H \subset G$, on a bien $H = G$.

Exemples.

• Soit $\varepsilon_1, ..., \varepsilon_n$ une bon de $\mathbb{R}^n$, $G = \mathfrak{S}_n$ vu comme matrices de permutations engendré par les réflexions (i, j) de vecteurs normal $\varepsilon_i - \varepsilon_j$.

Considérons les sommes de Newton

$$S_i = x_1^i + ... + x_n^i$$

pour $i = 1, ..., n$. On sait que

$$\mathbb{R}[X_1, ..., X_n]^{\mathfrak{S}_n} = \mathbb{R}[S_1, ..., S_n]$$

via les relations entre fonctions symétriques élémentaires et sommes de Newton.

D'autre part, $\frac{\partial S_i}{\partial X_j} = i X_j^{i-1}$, donc

$$J(S_i) = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ 2X_1 & 2X_2 & \cdots & 2X_n \\ \vdots & \vdots & \ddots & \vdots \\ nX_1 & nX_2 & \cdots & nX_n \end{vmatrix} = n! \operatorname{Vand}(X_1, ..., X_n) \neq 0,$$

donc les S_i sont algèbriquement indépendants.

• On reste dans le même cadre. On considère les n réflexions s_i par rapport aux $(\mathbb{R}\varepsilon_i)^{\perp}$. Les s_i commutent et engendrent un sous-groupe $S \simeq \left(\mathbb{Z}/2\mathbb{Z}\right)^n$.

Soit $G = \langle \mathfrak{S}_n, S \rangle$. Pour $\sigma \in \mathfrak{S}_n$, on a

$$\sigma s_i = \sigma s_{\sigma(i)}.$$

En effet,

$$\sigma s_i \sigma^{-1}(\varepsilon_k) = \sigma\left(s_i\left(\varepsilon_{\sigma^{-1}(k)}\right)\right) = \sigma\left((-1)^{\delta_i^{\sigma^{-1}(k)}} \varepsilon_{\sigma^{-1}(k)}\right) = (-1)^{\delta_i^{\sigma^{-1}(k)}} \sigma\left(\varepsilon_{\sigma^{-1}(k)}\right) = (-1)^{\delta_{\sigma(i)}^{k}} \varepsilon_k = s_{\sigma(i)}(\varepsilon_k).$$

Ainsi, dans l'écriture d'un élément de G, on peut regrouper d'un côté les termes de $\mathfrak{S}_n$ de l'autre ceux de S, *i.e.* $\mathfrak{S}_n S = G$. De plus $S \lhd G$ (car S abélien) et $\mathfrak{S}_n \cap S = \{1\}$, par conséquent

$$G \simeq S \rtimes \mathfrak{S}_n \simeq \left(\mathbb{Z}/2\mathbb{Z}\right)^n \rtimes \mathfrak{S}_n.$$

Cherchons un ensemble basique pour R. On veut des gens invariant par toutes les symétries, donc par changement de signe. Par exemple,

$$f_i = x_1^{2i} + ... + x_n^{2i}.$$

On a déjà la condition

$$\prod_{i=1}^{n} d_i = \prod_{i=1}^{n} 2i = 2^n n! = |G|\,.$$

Peut-on en conclure que les f_i forment bien un ensemble basique de R ?

7 Critère pour déterminer un ensemble basique

Proposition.
Soit G sous-groupe fini de $GL(V)$ engendré par les réflexions. Soient $g_1, ..., g_n$ libres homogènes dans R tels que

$$\prod_{i=1}^{n} \deg g_i = |G|\,.$$

Alors $(g_1, ..., g_n)$ est un ensemble basique de R.

Démonstration
Notons $R' = \mathbb{R}[g_1, ..., g_n] \subset R$. On veut $R' = R$.

Chevalley nous donne un ensemble basique $(f_1, ..., f_n)$ pour R. En posant $\begin{cases} d_i = \deg f_i \\ e_i = \deg g_i \end{cases}$, supposons (quitte à réordonner) les degré triés par ordre croissant :

$$\begin{cases} e_1 \leq e_2 \leq ... \leq e_n \\ d_1 \leq d_2 \leq ... \leq d_n \end{cases}.$$

Montrons que

$$\forall i,\ e_i \geq d_i.$$

Si ceci n'était pas le cas, considérons k le premier indice où $e_k < d_k$. On aurait alors

$$\begin{gathered} e_1 \leq ... \leq e_k < d_k \leq ... \leq d_n \\ \forall i \in \{1, ..., k\},\ e_i < \min\{d_k, ..., d_n\} \\ \forall i \in \{1, ..., k\},\ g_i \in \mathbb{R}[f_1, ..., f_{k-1}] \\ \mathbb{R}[g_1, ..., g_k] \subset \mathbb{R}[f_1, ..., f_{k-1}], \end{gathered}$$

et en prenant le corps des fractions et le degré de transcendance sur k, on obtiendrait

$$\begin{aligned} \mathbb{R}(g_1, ..., g_k) &\subset \mathbb{R}(f_1, ..., f_{k-1}) \\ \deg \mathrm{tr}_k\, \mathbb{R}(g_1, ..., g_k) &\leq \deg \mathrm{tr}_k\, \mathbb{R}(f_1, ..., f_{k-1}) \\ k &\leq k-1,\ \textit{absurde.} \end{aligned}$$

Puisque $\prod_{i=1}^n d_i = |G| = \prod_{i=1}^n e_i$ par hypothèse, on a donc l'égalité des degrés

$$e_i = d_i\ \forall i.$$

On se souvient alors d'un résultat (identité remarquable) :

$$\prod_{i=1}^{n} \frac{1}{1-t^{d_i}} = \sum_{k \geq 0} (\dim R_k)\, t^k.$$

On en déduit $\dim R_k = \dim R'_k$, et comme on a $R'_k \subset R_k$, on a égalité de toutes les composantes homogènes de R' et R, donc de R' et R.

8 Factorisation du jacobien

On suppose à nouveau que G est un sous-groupe fini de $GL(V)$ engendré par les réflexions.

Définition.
On dira que $f \in S$ est anti-invariant *par G si*

$$\forall \sigma \in G,\ \sigma(f) = (\det \sigma) f.$$

Pour chaque réflexion s, soit $\alpha_s \in V$ qui complète une base orthogonale de l'hyperplan stable H, et notons $l_s = \langle \alpha_s, \cdot \rangle$.

Théorème.
Soit $(f_1, ..., f_n)$ *un ensemble basique d'invariants et J leur Jacobien. Alors il y a un réel non nul λ tel que :*

$$J = \lambda \prod_{s \text{ réflexion}} l_s.$$

Démonstration
• Montrons en premier lieu que $\prod_{s \text{ réflexion}} l_s$ divise J.
En remarquant que les l_s sont des polynômes homogènes de degré 1, donc des irréductibles de $\mathbb{R}[X_1, ..., X_n]$, et deux à deux non associés (car $s \neq s' \implies \alpha_s \nparallel \alpha_{s'}$), il suffit par conséquent de montrer que chaque l_s divise J pour que leur produit divise J.
Soit s une réflexion, H son hyperplan associé et l sa forme linéaire associé. Pour avoir $l \mid J$, il suffit (d'après le lemme 0) que J soit nul sur H.
Soit donc $a \in H$, et supposons $J(a) \neq 0$. En remaquant que J est le jacobien de l'application polynomiale

$$f : \left\{ \begin{array}{ccc} \mathbb{R}^n & \longrightarrow & \mathbb{R}^n \\ (x_1, ..., x_n) & \longmapsto & (f_1(x_1, ..., x_n), ..., f_n(x_1, ..., x_n)) \end{array} \right. ,$$

le théorème d'inversion locale affirme l'existence d'une boule ouverte B autour de a sur laquelle $f_{|B}$ est injective (car $f_{|B}$ est un difféomorphisme). Or f est invariante par G, en particulier par la réflexion s, donc pour α dans B mais hors de H, on a

$$f_{|B}(\alpha) = f_{|B}(s_\alpha(\alpha)) = f_{|B}(-\alpha),$$

absurde par injectivité de $f_{|B}$.
• Maintenant que l'on a montré que $\prod_{s \text{ réflexion}} l_s$ divise J, comparons les degrés pour conclure à l'égalité :

$$\begin{aligned} \deg J &= \deg\left(\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \frac{\partial f_1}{\partial X_{\sigma(1)}} ... \frac{\partial f_n}{\partial X_{\sigma(n)}}\right) \leq \max_{\sigma \in \mathfrak{S}_n} \deg\left(\varepsilon(\sigma) \frac{\partial f_1}{\partial X_{\sigma(1)}} ... \frac{\partial f_n}{\partial X_{\sigma(n)}}\right) \\ &= \max_{\sigma \in \mathfrak{S}_n} \deg\left(\frac{\partial f_1}{\partial X_{\sigma(1)}} ... \frac{\partial f_n}{\partial X_{\sigma(n)}}\right) = \max_{\sigma \in \mathfrak{S}_n}\left(\deg\left(\frac{\partial f_1}{\partial X_{\sigma(1)}}\right) + ... + \deg\left(\frac{\partial f_n}{\partial X_{\sigma(n)}}\right)\right) \\ &\leq \max_{\sigma \in \mathfrak{S}_n}((d_1 - 1) + ... + (d_n - 1)) = (d_1 - 1) + ... + (d_n - 1) = N \\ &= \sum_{s \text{ réflexion}} 1 = \sum_{s \text{ réflexion}} \deg l_s = \deg\left(\prod_{s \text{ réflexion}} l_s\right). \end{aligned}$$

Corollaire.
Les anti-invariants de S forment un $S(V^*)^G$-module de rang 1 engendré par J.

Démonstration.
• Montrons déjà que J est anti-invariant.
Vu que G est engendré par les réflexions, il suffit de montrer que pour σ réflexion, $\sigma(J) = (\det \sigma) J$, *i.e.*

$$\sigma(J) = -J.$$

On calcule par conséquent

$$\sigma(J) = \sigma\left(\lambda \prod_{s \text{ réflexion}} ls\right) = \lambda \prod_{s \text{ réflexion}} \sigma(l_s)$$

et on s'intéresse donc à $\sigma(l_s)$.

Remarquons tout d'abord que, si s_H est la réflexion orthogonale par rapport à l'hyperplan H, alors le conjugué de s_H par un élément σ du groupe orthogonal (donc de G) n'est autre que $s_{\sigma(H)}$, *i.e.*

$$\sigma s_H \sigma^{-1} = s_{\sigma(H)}.$$

En particulier, si s_H et σ sont dans G, alors $s_{\sigma(H)}$ aussi.

On peut donc regarder l'action de $\{\mathrm{Id}, \sigma\}$ sur $\{s_H \in G\}$ par conjugaison définie par

$$\sigma * s_H = s_{\sigma(H)}.$$

Les orbites $\left\{s_H, s_{\sigma(H)}\right\}$ de $s_H \in G$ sont de cardinal 1 ou 2 selon que $\sigma = s_H$ ou pas. En notant les orbites $\Omega_0 = \{\sigma\}, \Omega_1, ..., \Omega_r$, on a donc

$$\sigma(J) = \lambda \prod_{s \text{ réflexion}} \sigma(l_s) = \lambda \prod_{i=0}^{r} \prod_{s \in \Omega_i} \sigma(l_s) = \lambda\sigma(l_\sigma) \prod_{i=1}^{r} \prod_{s \in \Omega_i} \sigma(l_s) = \lambda(-l_\sigma) \prod_{i=1}^{r} \prod_{s \in \Omega_i} \sigma(l_s).$$

On s'intéresse donc au produit $\sigma(l_s)\sigma(l_{s'})$ où $\{s, s'\}$ est une orbite non triviale

En notant $\begin{cases} s = s_H \\ s' = s_{\sigma(H)} \end{cases}$, on remarque que $\sigma(l_s)$ et $l_{s'}$ sont liées car ont même noyau

$$\operatorname{Ker}\sigma(l_s) = \operatorname{Ker}\sigma(l_{s_H}) = \operatorname{Ker}\left(l_{s_H} \circ \sigma^{-1}\right) = \sigma(\operatorname{Ker} l_{s_H}) = \sigma(H) = \operatorname{Ker} l_{s_{\sigma(H)}} = \operatorname{Ker} l_{s'},$$

ce qui s'écrit $\sigma(l_s) = a l_{s'}$ où $a \in \mathbb{R}^*$. De même,

$$\operatorname{Ker}\sigma(l_{s'}) = \operatorname{Ker}\sigma\left(l_{s_{\sigma(H)}}\right) = \operatorname{Ker} l_{s_{\sigma\sigma(H)}} = \operatorname{Ker} l_{s_H} = \operatorname{Ker} l_{s'},$$

donc $\sigma(l_{s'})$ et $l_s = l_{s_{\sigma(H)}}$ sont liées, ce qui donne $\sigma(l_{s'}) = b l_s$ avec $b \in \mathbb{R}^*$. On en déduit

$$(ab) l_s = a(b l_s) = a\sigma(l_{s'}) = \sigma(a l_{s'}) = \sigma(\sigma(l_s)) = l_s,$$

d'où $ab = 1$. Le produit recherché vaut donc

$$\sigma(l_s)\sigma(l_{s'}) = ab l_s l_{s'} = l_s l_{s'}.$$

On peut maintenant finir le calcul :

$$\sigma(J) = \lambda(-l_\sigma) \prod_{i=1}^{r} \prod_{s \in \Omega_i} \sigma(l_s) = -\lambda l_\sigma \prod_{i=1}^{r} \prod_{s \in \Omega_i} l_s = -\lambda \prod_{i=0}^{r} \prod_{s \in \Omega_i} l_s = -\lambda \prod_{s \text{ réflexion}} l_s = -J.$$

• Soit maintenant $P \in S$ anti-invariant, et montrons que J divise P dans S. Il suffit pour cela de montrer que chaque l_s (irréductible) divise P, *i.e.* que P s'annule sur les $\operatorname{Ker} l_s$ (toujours par le lemme 0).

Soit donc s_H une réflexion de G. P anti-invariant, d'où $s_H(P) = -P$. Pour $x \in H$, en explicitant P sur une base $(e_1^*, ..., e_n^*)$, on a

$$\begin{aligned}
-P(x) &= [s_H(P)](x) \\
&= [s_H(P(e_1^*, ..., e_n^*))](x) \\
&= \left[P\left(e_1^* \circ s_H^{-1}, ..., e_n^* \circ s_H^{-1}\right)\right](x) \\
&= [P(e_1^* \circ s_H, ..., e_n^* \circ s_H)](x) \\
&= P(e_1^* \circ s_H(x), ..., e_n^* \circ s_H(x)) \\
&= P(e_1^*(x), ..., e_n^*(x)) \\
&= P(x),
\end{aligned}$$

d'où $P(x) = 0$ comme voulu

Par conséquent, $\exists Q \in S$ tel que $P = JQ$. Pour $g \in G$, on a alors $g(P) = g(J)\, g(Q)$, *i.e.* (puisque P et J sont anti-invariants)

$$\begin{aligned}
(\det g) P &= (\det g) Jg(Q) \\
(\det g) JQ &= (\det g) Jg(Q) \\
Q &= g(Q).
\end{aligned}$$

Ceci tenant pour tout $g \in G$, Q est dans R comme voulu.