# Sous-algèbre des invariants de l'algèbre d'un monoïde

Marc SAGE

26 janvier 2012

## Table des matières



**Résumé**

Savez-vous ce que sont un groupe et un espace vectoriel ? Connaissez-vous les caractérisation d'un projecteur ? Alors bienvenu dans ce modeste texte tranversant les contrées des Dirac, du produit de convolution, des plongements de structures, de contructions algébriques générales, des actions de groupes, des classes de conjugaison, des algèbre des invariants, des projecteurs sur les invariants, des fixateurs, du lemme du berger, des représentations de groupes finis, des coefficients de structure, des partitions ensemblistes, de l'ordre de raffinement, des factorisations transitives... Nous espérons que ce court texte permettra à son lecteur d'apercevoir la variété de la faune mathématique que sa simple machette linéaire lui rendra accessible. Je remercie Jérôme Dégot de m'avoir permis d'intervenir deux heures dans sa HX3 à la Toussiure pendant qu'il profitait des pistes enneigées.

Considérons un monoïde $M$ et un corps $K$. Comment former des polynômes en des éléments de $M$ à coefficients dans $K$ ?

Une idée est de plonger le monoïde $M$ dans une $K$-algèbre (dont la structure monoïdale est donnée par la multiplication) où le calcul $K$-polynomial fera alors sens.

# 1 Prolongement d'un monoïde dans une algèbre de convolution *via* les Dirac

**Définitions.**
*Pour tous ensembles $a$ et $b$, on définit un* ***symbole de Kronecker***

$$\delta_a^b := \begin{cases} 1 \text{ si } a = b \\ 0 \text{ si } a \neq b \end{cases}.$$

*Pour tout $m \in M$, on définit le* ***Dirac*** *en $m$ par la fonction*

$$\delta_m : \begin{cases} M & \longrightarrow & \{0,1\} \\ a & \longmapsto & \delta_m^a \end{cases}.$$

Puisque tout corps contient $\{0,1\}$, les Diracs $\delta_m$ peuvent être vus comme des fonctions à valeurs dans $K$, *i. e.* comme des éléments de $K^M$. Mieux : les Diracs tombent tous dans l'ensemble $K^{(M)}$ des fonctions à support *fini*. On rappelle que le ***support*** d'une famille $(\lambda_m)_{m\in M} \in K^M$ est l'ensemble $\{m \in M \ ; \ \lambda_m \neq 0\}$.

**Propriété.** *L'application* $\begin{cases} M & \hookrightarrow & K^{(M)} \\ m & \longmapsto & \delta_m \end{cases}$ *est injective.*

**Démonstration.** À $m$ et $n$ fixés dans $M$, on a les implications

$$\delta_m = \delta_n \Longrightarrow 1 = \delta_m^m = \delta_m(m) = \delta_n(m) = \delta_n^m \Longrightarrow m = n.$$

**Définition.** *Pour $f$ et $g$ applications de $M$ dans $K$, on définit leur* ***convolée*** *par*

$$f * g : \begin{cases} M & \longrightarrow & K \\ m & \longmapsto & \sum_{ab=m} f(a)\, g(b) \end{cases}$$

(qui sera bien définie si l'équation $ab = m$ en les inconnues $a$ et $b$ admet un nombre *fini* de solutions pour tout $m \in M$).

La loi $*$ (appelée ***produit de convolution*** ou ***produit de Cauchy***) est bien définie sur $K^{(M)}$ et stabilise ce dernier (exercice). Elle est de plus clairement $K$-bilinéaire (comme forme bilinéaire en des évaluations). Elle possède également un neutre $\delta_{1_M}$ et est associative : on vérifiera (exercice !) les identités

$$\forall^3 f,g,h \in K^M, \quad \begin{cases} f * \delta_1 = \delta_1 * f = f \\ [f*g*h](m) = \sum_{abc=m} f(a)\, g(b)\, h(c) \end{cases}.$$
$$\forall m \in M,$$

Ainsi, *le $K$-espace vectoriel $K^{(M)} = \bigoplus_{m\in M} K$ est une $K$-algèbre pour le produit de convolution.*

**Proposition.** *L'application* $\begin{cases} M & \hookrightarrow & K^{(M)} \\ m & \longmapsto & \delta_m \end{cases}$ *est un monomorphisme de monoïdes multiplicatifs.*

On pourra donc identifier le monoïde $M$ à son image (son ***plongé***) dans l'algèbre $K^{(M)}$.

**Démonstration.** Le lecteur a déjà été invité à vérifier que le neutre $1_M$ était envoyé sur le neutre $1_{K^M} = \delta_{1_M}$.

Par ailleurs, à $m, n, x$ fixés dans $M$, on a

$$[\delta_m * \delta_n](x) = \sum_{ab=x} \delta_m(a)\, \delta_n(b) = \sum_{ab=x} \delta_m^a \delta_n^b = \sum_{\substack{ab=x \\ a=m \\ b=n}} 1 \cdot 1 = \begin{cases} 1 \text{ si } x = mn \\ 0 \text{ sinon} \end{cases} = \delta_{mn}^x = \delta_{mn}(x),$$

d'où l'égalité $\delta_m * \delta_n = \delta_{mn}$ en faisant varier $x$ dans $M$.

On note $K[M]$ l'ensemble des polynômes en les éléments de $M$ (dans l'algèbre $K^{(M)}$). On l'appelle la ***$K$-algèbre engendrée par*** $M$.

Ensemblistement, c'est *toute* la sous-algèbre $K^{(M)} = \bigoplus_{m\in M} K$, ce qui montre que

*les éléments de $M$ forment une base de l'algèbre $K[M]$.*

Cette dernière est donc de dimension le cardinal de $M$ :

$$\dim K[M] = \operatorname{Card} M.$$

**Exemple.** Considérons le monoïde libre à un générateur $M := \{1, X, X^2, X^3, ...\}$. Alors l'algèbre $K[M]$ vaut celle des polynômes $K[X] = K^{(\mathbb{N})}$ avec le produit de Cauchy usuel. Elle est de dimension dénombrable $\aleph_0 = \operatorname{Card}\mathbb{N}$ (premier cardinal infini).

# 2 Et si l'on fait agir un groupe, qui restera dans l'ombre ?

On va maintenant faire agir un groupe fini sur l'algèbre $\mathcal{A} := K[M]$ et étudier les éléments « invisibles » par cette action.

Soit $G$ un groupe fini

1. qui ***agit*** sur $M$ – *i. e.* on se donne pour tout $g \in G$ une application $\left\{ \begin{array}{ccc} M & \longrightarrow & M \\ m & \longmapsto & g\cdot m \end{array} \right.$ ;
2. avec un ***neutre*** – *i. e.* $\forall m \in m,\ 1\cdot m = m$ ;
3. de manière ***associative*** – *i. e.* $\left\{ \begin{array}{c} \forall g,h \in G, \\ \forall m \in M, \end{array} \right. \quad g\cdot(h\cdot m) = (gh)\cdot m$ ;
4. et de façon ***distributive*** – *i. e.* $\left\{ \begin{array}{c} \forall g \in G, \\ \forall m,n \in M, \end{array} \right. \quad g\cdot(mn) = (g\cdot m)(g\cdot n).$

**Exemple.** On prend $G := M$ et l'on le fait agir sur lui-même par ***conjugaison intérieure*** :

$$g\cdot m := gmg^{-1}.$$

Lorsque les trois premiers axiomes ci-dessus sont vérifiés, on parle plus simplement d'***action de groupe*** (sur un ensemble). Le dernier axiome exprime la compatibilité des actions avec la structure monoïdale : il exprime en effet que toutes les actions $m \mapsto g\cdot m$ sont des (auto)morphismes de monoïdes.

L'action de $G$ sur $M$ peut par linéarité se prolonger à tout $\operatorname{Vect} M = \mathcal{A}$ :

$$\text{poser } g\cdot\left(\sum \lambda_m m\right) := \sum \lambda_m (g\cdot m).$$

**Propriété.** *Cette action est algébrique, au sens où toutes les applications $g\cdot$ sont des (auto)-morphismes d'algèbres :*

$$\begin{array}{c} \forall^3 m,n,o \in M, \\ \forall g \in G, \end{array} \quad , \ g\cdot(\lambda m + no) = \lambda(g\cdot m) + (g\cdot n)(g\cdot o).$$

*Pour préserver l'unité, on supposera de plus que le monoïde $M$ est* ***réduit****,* i. e. *que son seul idempotent est* $1$ *:*

$$\left.\begin{array}{c} \forall m \in M, \\ m^2 = m \Longrightarrow m = 1 \end{array}\right\} \Longrightarrow \forall g \in G,\ g\cdot 1 = 1.$$

**Démonstration.** La linéarité découle trivialement de la définition. Fixons un $g \in G$.

Montrons que $g\cdot(ab) = (g\cdot a)(g\cdot b)$ pour tout $a,b \in \mathcal{A}$. Puisque le produit de $M$ est bilinaire et l'action de $G$ linéaire, les deux membres de l'égalité souhaitée sont bilinéaires en $(a,b)$. Ils coïncideront donc pour tous $a,b$ ssi ils coïncident lorsque $a$ et $b$ décrivent indépendamment une base de $\mathcal{A}$, par exemple $M$, ce qui devient évident par hypothèse de distributivité.

Enfin, puisque $g\cdot$ préserve le produit, il préserve les puissances, *a fortiori* les idempotents, de sorte que $g\cdot 1$ est un idempotent de $\mathcal{A}$ : puisqu'il réside dans $M$, il vaut 1 par hypohtèse, ce qui conclut.

**Définitions.**
*Deux éléments $a$ et $b$ dans $\mathcal{A}$ sont dits* ***conjugués*** *(sous l'action de $G$) si* $\exists g \in G,\ b = g\cdot a$.

*La conjugaison est une relation d'équivalence (exercice !) dont les classes d'équivalences sont appelées* ***classes de conjugaison*** *et l'ensemble quotient noté* $\mathcal{A}/_G$.

*On notera la classe de conjugaison d'un élément* $a \in \mathcal{A}$ *par*

$$C_a = G \cdot a := \{g \cdot a\}_{g \in G}$$

*et on l'identifie abusivement à la somme de ses éléments dans l'algèbre* $\mathcal{A}$ *:*

$$C_a := \sum_{c \in C_a} c \qquad \begin{array}{c}\text{(attention : plusieurs } g \in F \text{ peuvent} \\ \text{donner le même élément } g \cdot a)\end{array} .$$

*La projection canonique* $\left\{ \begin{array}{ccc} \mathcal{A} & \longrightarrow & \mathcal{A}/_G \\ a & \longmapsto & C_a \end{array} \right.$ *induit,* modulo *l'abus d'écriture et la mise en garde ci-dessus, un endomorphisme de* $K$*-espaces vectoriels*

$$\pi : \left\{ \begin{array}{ccc} \mathcal{A} & \longrightarrow & \mathcal{A} \\ a & \longmapsto & \sum_{g \in G} g \cdot a \end{array} \right. .$$

*Un élément* $a \in \mathcal{A}$ *est dit* ***invariant*** *(sous l'action de* $G$*) s'il est fixé par tous les* $g \in G$*,* i. e. *si* $\forall g \in G,\ g \cdot a = a$.

*L'****algèbre des invariants*** *de* $\mathcal{A}$ *sera notée* $\mathcal{A}^G$ *(exercice : c'est bien une sous-algèbre de* $\mathcal{A}$*).*

**Exemple.** Quand $G$ agit sur lui-même par conjugaison intérieure, un élément $m \in G$ est invariant ssi il commute avec tous les $g \in G$ : on a effet à $g \in G$ fixé les équivalences

$$g \cdot m = m \iff gmg^{-1} = g \iff gm = mg.$$

**Proposition.** *L'endomorphisme* $p := \frac{\pi}{|G|}$ *est un projecteur sur les invariants et linéaire par rapport à ces derniers :*

$$p : \left\{ \begin{array}{ccc} \mathcal{A} & \twoheadrightarrow & \mathcal{A}^G \\ a & \longmapsto & \frac{1}{|G|} \sum_{g \in G} g \cdot a \end{array} \right. \qquad \textit{est } \mathcal{A}^G\textit{-linéaire.}$$

**Démonstration.** Rappelons à $a \in G$ fixé que la translation $g \mapsto ag$ dans $G$ est injective (car $a$ est simplifiable) et d'image $aG \subset G$ ; puisque les cardinaux sont finis et égaux, on a l'égalité[1] $aG = G$.

$\mathcal{A}^G$-linéarité Soit $i$ invariant et $a \in \mathcal{A}$. On a

$$\begin{aligned} \pi(ia) &= \sum_{g \in G} g \cdot (ia) \overset{\text{action}}{\underset{\text{distributive}}{=}} \sum_{g \in G} (g \cdot i)(g \cdot a) \overset{i \text{ invariant}}{=} \sum_{g \in G} i(g \cdot a) \\ &\overset{\text{produit de } \mathcal{A}}{\underset{\text{distributif}}{=}} i \sum_{g \in G} (g \cdot a) = i\,\pi(a)\,, \text{ d'où } p(ia) = ip(a)\,. \end{aligned}$$

$\operatorname{Im} p \subset \mathcal{A}^G$ Soit $a \in A$ et $g_0 \in G$. Alors

$$\begin{aligned} g_0 \cdot p(a) &= g_0 \cdot \left( \frac{1}{|G|} \sum_{g \in G} g \cdot a \right) \overset{\text{action}}{\underset{\text{linéaire}}{=}} \frac{1}{|G|} \sum_{g \in G} g_0 \cdot (g \cdot a) \\ &\overset{\text{action}}{\underset{\text{associative}}{=}} \frac{1}{|G|} \sum_{g \in G} (g_0 g) \cdot a \overset{g \leftarrow g_0^{-1} h}{=} \frac{1}{|G|} \sum_{h \in g_0 G} h \cdot a \overset{g_0 G = G}{=} \frac{1}{|G|} \sum_{h \in G} h \cdot a = p(a)\,. \end{aligned}$$

$\mathcal{A}^G \subset \operatorname{Im} p$ Soit $i$ invariant. Alors

$$i = \frac{1}{|G|} |G|\, i = \frac{1}{|G|} \sum_{g \in G} i \overset{i \text{ invariant}}{=} \frac{1}{|G|} \sum_{g \in G} g \cdot i = p(i) \in \operatorname{Im} p.$$

$p(1) = 1$ On calcule directement

$$p(1) = \frac{1}{|G|} \sum_{g \in G} g \cdot 1 \overset{\text{action}}{\underset{\text{neutre}}{=}} \frac{1}{|G|} \sum_{g \in G} 1 = \frac{1}{|G|} |G| = 1.$$

$p^2 = p$ Soit $a \in A$. L'élément $i := p(a)$ est dans $\operatorname{Im} p = \mathcal{A}^G$, d'où

$$p^2(a) = p(i) = p(i1) \overset{\mathcal{A}^G\text{-linéarité}}{=} ip(1) = i1 = i = p(a)\,.$$

[1] Cet argument peut être utilisé pour démontrer un cas particulier du théorème de Lagrange dans les groupes finis abéliens : fixant de même un $a \in G$, le produit de tous les éléments de $G$ vaut celui de éléments de $aG$, à savoir $\prod_{g \in G} ag \overset{G \text{ abélien}}{=} a^{|G|} \prod_{g \in G} g$, d'où en simplifiant par $\prod_{g \in G} g$ l'égalité $a^{|G|} = 1$.

# 3 Les classes de conjugaison sont des invariants basiques

**Proposition.** *Pour tout $m \in M$, on a $p(m) = \frac{C_m}{|C_m|}$.*

**Démonstration.** Pour tenir compte des multiplicités des éléments dans la somme $\sum_{g\in G} g\cdot m$, on introduit le ***fixateur***[2] de $m$, défini par

$$\operatorname{Fix} m := \{g \in G \ ; \ g\cdot m = m\}.$$

Regardons les antécédents par la surjection $\left\{ \begin{array}{ccc} G & \twoheadrightarrow & C_m \\ g & \longmapsto & g\cdot m \end{array} \right.$ d'un $g_0\cdot m$ fixé. Un élement $g\in G$ en sera un antécédent ssi

$$\begin{aligned} g\cdot m \overset{?}{=} g_0\cdot m &\iff g_0^{-1}\cdot(g\cdot m) \overset{?}{=} g_0^{-1}\cdot(g_0\cdot m) \\ &\iff \left(g_0^{-1}g\right)\cdot m \overset{?}{=} \left(g_0^{-1}g_0\right)\cdot m = 1\cdot m = m \\ &\iff g_0^{-1}g \overset{?}{\in} \operatorname{Fix} m \\ &\iff g \overset{?}{\in} g_0\left(\operatorname{Fix} m\right). \end{aligned}$$

On en déduit que la ***fibre*** (*i. e.* l'ensemble des antécédents) de $g_0\cdot m$ est précisément $g_0(\operatorname{Fix} m)$. Puisque $g_0$ est injective, le cardinal de $g_0(\operatorname{Fix} m)$ vaut celui de $\operatorname{Fix} m$ et en particulier ne dépend pas de $g_0$. Par le lemme du berger, on en déduit $|G| = |C_m|\,|\operatorname{Fix} m|$.

(Une remarque linéaire : si notre groupe $G$ était noté additivement, les équivalences ci-dessus rappeleraient furieusement celles entre l'injectivité d'une application linéaire et la nullité de son noyau. Et nous aurions redémontré que l'ensemble des antécédents d'un $g_0$ fixé est le translaté par ce dernier du noyau. Le fixateur est donc déjà connu en additif.)

Concluons. On regroupe dans la somme $p(m) = \frac{1}{|G|}\sum_{g\in G} \underbrace{g\cdot m}_{\in C_m}$ les termes selon leur valeur dans $C_m$ ; autrement dit, on partionne $G$ en $\bigsqcup_{c\in C_m} \{g\in G\}_{g\cdot m = c}$ selon les fibres de la surjection précédente, lesquelles sont toutes de cardinal $|\operatorname{Fix} m|$ :

$$\begin{aligned} \frac{1}{|G|}\sum_{g\in G} g\cdot m &= \frac{1}{|G|}\sum_{c\in C_m}\sum_{\substack{g\in G\\ g\cdot m = c}} g\cdot m = \frac{1}{|G|}\sum_{c\in C_m}\sum_{\substack{g\in G\\ g\cdot m = c}} c = \frac{1}{|G|}\sum_{c\in C_m} c \sum_{\substack{g\in G\\ g\cdot m = c}} 1 \\ &= \frac{1}{|G|}\sum_{c\in C_m} c \underbrace{\#\{g\in G \ ; \ g\cdot m = c\}}_{=|\operatorname{Fix} m|} = \frac{|\operatorname{Fix} m|}{|G|}\sum_{c\in C_m} c = \frac{C_m}{|C_m|}. \end{aligned}$$

**Corollaire.** *Les classes de conjugaison de $M$ forment une base de l'algèbre des invariants $K[M]^G$.*

**Démonstration.** Un élément $i = \sum \lambda_m m$ invariant vaut son projeté $p(i) = \sum \lambda_m p(m) = \sum \lambda_m \frac{C_m}{|C_m|}$ et est donc engendré par les classes $C_m$.

Supposons maintenant donnée une relation de liaison $\sum_{m\in T}\lambda_m C_m = 0$ où $T$ est une ***tranversale*** de $M$ pour l'action de $G$ (*i. e.* une partie de $M$ contenant exactement un représentant de chaque classe). Fixons un $m_0\in M$. L'élément $m_0 = 1\cdot m_0$ est dans la classe $C_{m_0}$ et dans aucune autre (par disjonction des classes d'équivalence), d'où l'évaluation

$$C_m(m_0) = \left[\sum_{c\in C_m} c\right](m_0) = \left[\sum_{c\in C_m}\delta_c\right](m_0) = \sum_{c\in C_m}\delta_c(m_0) = \sum_{c\in C_m}\delta_c^{m_0} = \sum_{\substack{c\in C_m\\ c=m_0}} 1 = \left\{ \begin{array}{l} 1 \text{ si } m_0\in C_m \\ 0 \text{ sinon} \end{array} \right. .$$

On en déduit

$$0 = \left[\sum_{m\in T}\lambda_m C_m\right](m_0) = \sum_{m\in T}\lambda_m\ C_m(m_0) = \sum_{m\in T}\lambda_m \left\{ \begin{array}{l} 1 \text{ si } m_0\in C_m \\ 0 \text{ sinon} \end{array} \right. = \sum_{\substack{m\in T\\ C_m\ni m_0}} \lambda_m = \lambda_{m_0},$$

d'où la nullité de tous les scalaires $\lambda_m$.

[2] Parfois noté $G_m$ . Noter la cohérence avec la notation $M^G$ : dans les deux cas le $G$ est *au-dessus* des éléments de $M$, lesquels sont *sous* l'action de $G$.

# 4 Une application : toute représentation de dimension finie est somme directe de représentations irréductibles

Les idées qui précèdent sont à l'œuvre dans un lemme qui apparaît naturellement dans la théorie des représentations des groupes en dimension finie.

**Définitions.**
*Une **représentation** d'un groupe $G$ est un morphisme $\rho$ de groupes de $G$ vers un groupe linéaire $GL(V)$. Elle induit une action sur l'espace vectoriel $V$ (auquel on identifiera abusivement et volontiers le morphisme $\rho$) par*

$$g \cdot v := [\rho(g)](v)$$

(on représente les éléments de $G$ comme automorphismes linéaires).
*Un sous-espace vectoriel $W \subset V$ stable par cette action induit par restriction une **sous-représentation***

$$\rho_W : \left\{ \begin{array}{ccc} G & \longrightarrow & GL(W) \\ g & \longmapsto & \rho(g)_{|W} \end{array} \right. .$$

*Une représentation $V$ est dite **irréductible** si elle n'admet aucun sous-représentation propre, i. e. de sous-représentation $W$ telle que $\{0\} \subsetneq W \subsetneq V$.*

On notera une analogie avec la définition des nombres premiers :

| représentation de dimension finie | somme directe | sous-représentation | supplémentaire | représentation irréductible |
|---|---|---|---|---|
| nombre entier naturel | produit | diviseur | diviseur complémentaire | nombre premier |

Il est donc naturel d'essayer d'obtenir un théorème de décomposition en « facteurs » irréductibles.

**Théorème.** *Toute représentation d'un groupe fini de dimension finie est somme directe de représentations irréductibles.*

**Démonstration.** On raisonne comme pour la décomposition en facteurs premiers par récurrence – sur la dimension.

En dimension 0, il n'y qu'une seule sous-représentation (tout comme l'entier 1 n'admet qu'un seul diviseur dans $\mathbb{N}$), donc aucune sous-représentation propre : on est irréductible.

Supposons ensuite le théorème montré pour les représentations de dimensions $< n$ où $n$ est un entier $\geq 1$ fixé et considérons une représentation $V$ de dimension $n$. Si $V$ est irréductible, on a terminé, sinon $V$ admet une sous-représentation propre $0 \subsetneq W \subsetneq V$. Afin de pouvoir récurrer, il nous suffirait de montrer que $V$ est somme directe de $W$ et d'une autre sous-représentation propre (chez les entiers, c'est automatique : si $d$ est un diviseur propre de $n$, alors $\frac{n}{d}$ aussi et leur produit fait $n$). Ce qui fait l'objet du lemme suivant.

**Lemme (Maschke).** *Soit $E$ un espace vectoriel, $G$ un sous-groupe fini de $GL(E)$ et $F$ un sous-espace vectoriel stable par (tous les éléments de) $G$. Montrer que $F$ admet un supplémentaire stable par $G$.*

Idée 1 : si deux endomorphismes commutent, alors l'image et le noyau de l'un sont stables par l'autre (lemme très classique *et* très utile) :

$$\forall u, v \in L(E),\ uv = vu \Longrightarrow \operatorname{Ker} u \text{ et } \operatorname{Im} u \text{ stables par } v.$$

On va donc chercher un endomorphisme commutant avec $G$ dont les noyau et image soient $F$ et un supplémentaire de $F$, par exemple un projecteur sur $F$ qui commuterait avec $G$ (son noyau répondrait alors au problème).

Idée 2 : commuter, c'est être invariant par conjugaison intérieure. On part donc d'un projecteur $p$ sur $F$ et on le « commutativise » en posant $\widetilde{p} := \frac{1}{|G|} \sum_{g \in G} gpg^{-1}$. On vérifie ensuite que $\widetilde{p}$ est bien un projecteur sur $F$. La démonstration est la même que pour notre projection $\mathcal{A}^G$-linéaire plus haut : on montre par double inclusion l'égalité $L(E)^G = \operatorname{Im} \widetilde{p}$.

# 5 Une autre application : factorisation de l'identité et coefficients de structures

Dans une algèbre $A$ dont on connaît une base linéaire $(a_i)$, la structure de $A$ sera déterminée par son *produit*. Par linéarité, ce dernier est déterminé par les produits des éléments de bases $a_i a_j = \sum_k \lambda_{i,j}^k a_k$. Les coefficients $\lambda_{i,j}^k$ qui apparaisent sont ainsi baptisés ***coefficients de structure*** (de l'algèbre $A$).

**Problème.** *On se donne $C_1, ..., C_k$ des classes de conjugaison (intérieure) dans un groupe fini $G$ : de combien de façons peut-on factoriser l'élément neutre sous la forme $g_1 \cdots g_k = 1$ avec $g_i \in C_i$ pour tout $i$ ?*

Idée : on se place dans l'algèbre du groupe $\mathbb{Q}[G]$ et on développe le produit des classes de conjugaison

$$\begin{aligned} C_1 C_2 \cdots C_k &= \left(\sum_{g_1 \in C_1} g_1\right)\left(\sum_{g_2 \in C_2} g_2\right) \cdots \left(\sum_{g_k \in C_k} g_k\right) = \sum_{\substack{g_1 \in C_1 \\ g_2 \in C_2 \\ \cdots \\ g_k \in C_k}} \underbrace{g_1 g_2 \cdots g_k}_{\substack{\text{appartient à une} \\ \text{certaine classe} \\ \text{de conjugaison}}} \\ &= \sum_{\substack{g_1 \in C_1 \\ \cdots \\ g_k \in C_k}} \sum_{\substack{C \text{ classe de} \\ \text{conjugaison}}} \sum_{g_1 g_2 \cdots g_k \in C} g_1 g_2 \cdots g_k. \end{aligned}$$

En projetant cette relation sur les invariants à l'aide du projecteur $p$, on obtient

$$\begin{aligned} C_1 \cdots C_k &= p(C_1 \cdots C_k) = \sum_{\substack{g_1 \in C_1 \\ \cdots \\ g_k \in C_k}} \sum_{\substack{C \text{ classe de} \\ \text{conjugaison}}} \sum_{g_1 \cdots g_k \in C} \underbrace{p(g_1 \cdots g_k)}_{= \frac{C}{|C|}} = \sum_{\substack{C \text{ classe de} \\ \text{conjugaison}}} \frac{C}{|C|} \sum_{\substack{g_1 \in C_1 \\ \cdots \\ g_k \in C_k}} \sum_{g_1 \cdots g_k \in C} 1 \\ &= \sum_{\substack{C \text{ classe de} \\ \text{conjugaison}}} \frac{C}{|C|} \# \left\{ \begin{array}{c} \overrightarrow{g} \in C_1 \times \cdots \times C_k \ ; \\ g_1 \cdots g_k \in C \end{array} \right\}. \end{aligned}$$

Ainsi, la réponse cherchée est un coefficient de structure : la coordonnée dans $\mathbb{Q}[G] = \bigoplus_C \mathbb{Q}C$ de la classe $C_1 = \{1\}$.

Le problème est loin d'être résolu, mais cette idée donne au moins un point de départ.

Illustrons par un exemple tirée de la recherche des années 2000.

On s'intéresse aux factorisations de l'identité comme ci-dessus en rajoutant une condition : la *transitivité* du groupe engendré par $g_1, ..., g_k$. On va pouvoir encoder cette dernière dans une structure monoïdale et obtenir ainsi les nombres cherchés comme coefficients de structure de l'algèbre du monoïde considéré.

Soit $G$ un groupe fini agissant sur un ensemble $E$ fini – par exemple le groupe symétrique $\mathsf{S}_n$ sur l'ensemble $\{1, ..., n\}$.

Appelons ***partition ensembliste*** (et on oubliera « ensembliste » pour alléger) de $E$ tout ensemble $\pi = \{\pi_i\}$ de parties de $E$ dont les éléments $\pi^i$ (appelés ***parts*** de $\pi$) sont non vides, deux à deux disjoints et recouvrent $E$. Une partition $\pi$ est dite ***plus fine*** (ou ***moins grossière***) qu'une partition $\varpi$ si toute part de $\pi$ est incluse dans une part de $\varpi$ (on note alors $\pi \leq \varpi$). Par exemple, la partition $\{\{e\}\}_{e \in E}$ dont toutes les parts sont des singletons est la plus fine et la partition $\{E\}$ à une part est la plus grossière.

On montre que l'***ordre de grossièreté*** (ou son opposé l'***ordre de raffinement***) est ***achevé***, au sens où toute partie admet une borne supérieure (et inférieure), avec la description suivante des parts du *supremum* d'une famille de partitions $(\pi^i)$ : *deux éléments $a, b \in E$ sont dans une même part de* $\sup\{\pi^i\}$ *si et seulement s'il y a une suite finie de parts de certains $\pi^i$ telle que la première contienne $a$, la dernière contienne $b$ et telle que deux successives se rencontrent.* Par exemple, les partitions $\{\{1,2,3\},\{4,5\},\{6\}\}$ et $\{\{1,2\},\{3,4\},\{5,6\}\}$ ont pour borne supérieure la partition la plus grossière. On peut aller de 1 à 6 en suivant les parts $\{1,2,3\}$, $\{3,4\}$, $\{4,5\}$, $\{5,6\}$.

Des exemples de partitions sont données pour chaque $g \in G$ par les classes de conjugaison (alors appelées ***orbites)*** du sous-groupe monogène $\langle g \rangle$. On parle alors de ***partition orbitale*** et on la note

$$\mathrm{Orb}\, g := \{\text{classes de conjugaison sous l'action de } \langle g \rangle\}.$$

La transitivité se code bien en terme de partitions orbitales (exercice !) :

*le groupe engendré par une famille $(g_i)$ de $G$ agit transitivement*
*ssi le* supremum *des* $\mathrm{Orb}\, g_i$ *est la partition maximale* $\{E\}$.

On définit alors un ensemble $\mathbb{G}$ de couples $\binom{g}{\pi}$ où $\pi$ est une partition de $E$ et où $g \in G$ agit sur chaque part de $\pi$, ce qui se résume en $\operatorname{Orb} g \leq \pi$. On met un produit sur $\mathbb{G}$ en composant les éléments de $G$ et en prenant le *supremum* $\vee$ des partitions. On laisse au lecteur le soin de vérifier que cette loi produit

$$\binom{g}{\pi}\binom{h}{\varpi} := \binom{gh}{\pi \vee \varpi}$$

munit bien $\mathbb{G}$ d'une structure de monoïde sur lequel $G$ agit de manière distributive par

$$\varphi \cdot \binom{g}{\{\pi_i\}} := \binom{\varphi g \varphi^{-1}}{\{\varphi(\pi_i)\}}.$$

On peut alors coder notre problème en termes de coefficients de structure.

On commencer par remarquer que l'égalité $g_1 \cdots g_k = 1$ et la transitivité de $\langle g_1, ..., g_k \rangle$ se codent en une seule égalité dans le monoïde $\mathbb{G}$ :

$$\binom{g_1}{\operatorname{Orb} g_1} \cdots \binom{g_k}{\operatorname{Orb} g_k} = \binom{1}{\{E\}}.$$

En reprenant le développement du produit ci-dessus des classes de conjugaison, on parvient sans effort (exercice !) à notre destination.

**Proposition.** *Étant données des classes de conjugaison (intérieure) $C_1, ..., C_k$ dans le groupe $G$, le nombre de factorisations $g_1 \cdots g_k = 1$ avec $g_i \in C_i$ pour tout $i$ et où le groupe $\langle g_1, ..., g_k \rangle$ agit transitivement vaut le coefficient de structure de la classe normalisée $\frac{C_{\binom{1}{\{E\}}}}{\left|C_{\binom{1}{\{E\}}}\right|}$ dans le produit $C_{\binom{g_1}{\operatorname{Orb} g_1}} \cdots C_{\binom{g_k}{\operatorname{Orb} g_k}}$ de l'algèbre des invariants $\mathbb{Q}[\mathbb{G}]^G$.*