HAL open science

Sur l'algèbre et la combinatoire des sous-graphes d'un graphe.

Xavier Buchwalder

To cite this version:

Xavier Buchwalder. Sur l'algèbre et la combinatoire des sous-graphes d'un graphe.. Mathématiques [math]. Université Claude Bernard - Lyon I, 2009. Français. NNT : . tel-00441324v1

HAL Id: tel-00441324

https://theses.hal.science/tel-00441324v1

Submitted on 15 Dec 2009 (v1), last revised 27 Jun 2011 (v3)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

253 -2009 Année 2009

THÈSE DE L'UNIVERSITÉ DE LYON
Délivrée par
l'UNIVERSITÉ CLAUDE BERNARD LYON 1

ÉCOLE DOCTORALE MATHÉMATIQUES ET INFORMATIQUE

DIPLÔME DE DOCTORAT
(arrêté du 7 août 2006)

soutenue publiquement le 30 Novembre 2009
par
Xavier BUCHWALDER

TITRE : SUR L'ALGÈBRE ET LA COMBINATOIRE DES SOUS-GRAPHES D'UN GRAPHE

Directeur de thèse : Pr J.A. BONDY

RAPPORTEURS : Pr P.J. CAMERON
Pr A. SCHRIJVER

JURY : Pr J.A. BONDY
Pr P.J. CAMERON
Pr S. ELIAHOU
Pr M. POUZET
Pr J. RAMÍREZ-ALFONSÍN
Pr N. THIÉRY

Résumé
On introduit une nouvelle structure algébrique qui formalise bien les problèmes de reconstruction, assortie d'une conjecture qui permettrait de traiter directement des symétries. Le cadre fournit par cette étude permet de plus d'engendrer des relations qui ont lieu entre les nombres de sous-structures, et d'une certaine façon, la conjecture formulée affirme qu'on les obtient toutes. De plus, la généralisation des résultats précédemment obtenus pour la reconstruction permet de chercher à en apprécier les limites en recherchant des cas où ces relations sont optimales. Ainsi, on montre que les théorèmes de V.Müller et de L.Lovász sont les meilleurs possibles en exhibant des cas limites. Cette généralisation aux algèbres d'invariants, déjà effectuée par P.J.Cameron et V.B.Mnukhin, permet de placer les problèmes de reconstruction en tenaille entre d'une part des relations (fournies) que l'on veut exploiter, et des exemples qui établissent l'optimalité du résultat. Ainsi, sans aucune donnée sur le groupe, le résultat de L.Lovász est le meilleur possible, et si l'on considère l'ordre du groupe, le résultat de V.Müller est le meilleur possible.

Mots clés
reconstruction, graphes, conjecture d'Ulam, sous-ensembles, algèbre d'invariants, ensemble partiellement ordonné, groupe agissant sur un ensemble partiellement ordonné, coefficients binomiaux

Institut Camille Jordan
Université Claude Bernard Lyon1
43 bvd du 11 Novembre 1918
69622 Villeurbanne cedex
France

Titre en Anglais

On algebraic and combinatorial aspects of the subgraphs of a graph.

Résumé en Anglais

A new algebraic structure is described, that is a useful framework in which reconstruction problems and results can be expressed. A conjecture is made which would, provided it is true, help to address the problem of symmetries. A consequence of the abstract language in which the theory is formulated is the expression of relations between the numbers of substructures of a structure (for example, the number of subgraphs of a given type in a graph). Moreover, a generalisation similar to the one achieved by P.J.Cameron and V.B.Mnukhin of the results of edge reconstruction to invariant algebras is stated. Examples are then provided to show that the result of L.Lovász is best possible if one knows nothing about the underlying group, and that the result of V.Müller is best possible if one knows only the order of the group. Thus, reconstruction problems are set in a theory that generates relations to address them, and at the same time, provides examples establishing the sharpness of the theorems.

Mots clés en Anglais

reconstruction, graphs, Ulam's conjecture, subsets, invariant algebras, posets, groups acting on posets, binomial coefficients

Table des matières

1 Digèbres **13**

1.1 Algèbre d'incidence, fonctions polynomiales, et actions de groupes 13

1.1.1 Algèbre d'incidence 13

1.1.2 Caractères et sous-algèbres de $\mathcal{S}_n$ 14

1.1.3 Actions de groupes 16

1.2 Digèbres 16

1.2.1 Définition 16

1.2.2 Premières propriétés 20

1.2.3 Système de blocs d'une digèbre 26

1.2.4 Exemple emblématique 29

1.3 Commutants 30

1.3.1 Structures d'incidence 31

1.3.2 Commutant 34

1.3.3 Commutants d'ordres supérieurs 39

1.3.4 Une conjecture équivalente sur les commutants 44

2 Coefficients des digèbres, Relations polynomiales **47**

2.1 Coefficients des digèbres 47

2.2 ε-algèbres 51

2.3 Relations connues 53

2.4 De nouvelles relations ? 60

2.4.1 Relations d'ordre 0 60

2.4.2 Relations d'ordre 1 61

2.4.3 Relations d'ordre 2 62

2.4.4 Relations d'ordre quelconque, tests 63

3 Digèbres engendrées par un élément, application aux problèmes de reconstruction **66**

3.1 Une conjecture de reconstruction générale 67

3.2 Graphes non orientés 70

3.2.1 Reconstruction par les sommets 70

3.2.2 Reconstruction par les arêtes 73
3.3 Graphes orientés 73
3.3.1 Reconstruction par les sommets 73
3.4 Digèbres engendrées par un élément 74

A Digèbres de petits ordres **81**
A.1 Digèbres simples 81
A.2 Algèbres d'invariants d'ordre 1 82
A.3 Algèbres d'invariants d'ordre 2 82
A.4 Algèbres d'invariants d'ordre 3 83
A.5 Algèbres d'invariants d'ordre 4 83
A.6 Algèbres d'invariants d'ordre 5 84
A.7 Algèbres d'invariants d'ordre 6 86
A.8 Algèbres d'invariants d'ordre 7 87
A.9 Algèbres d'invariants d'ordre 8 88

Remerciements

Tout d'abord, une pensée reconnaissante pour les personnes qui, si elles ne publient jamais d'article, contribuent néanmoins par leur travail irréprochable à celui des chercheurs. Je garderai toujours en mémoire l'aide précieuse et désintéressée que certaines personnes ont pu m'apporter, leur gentillesse, et leur conscience professionnelle.

Sur le plan personnel, j'aimerais remercier mes proches, pour leur soutien indéfectible, leurs conseils avisés, et surtout pour avoir su porter avec moi les affres de la recherche mathématique.

J'aimerais aussi remercier les membres du jury pour l'intérêt qu'ils ont bien voulu porter à mon travail, leurs questions et remarques aussi nombreuses que précises, et surtout pour les point de vues élevés et distincts qu'ils ont donnés sur celui-ci. Parmi eux, j'aimerais tout spécialement remercier le Professeur Alexander Schrijver pour le temps qu'il m'a consacré, le Professeur Maurice Pouzet pour m'avoir fait profiter de sa grande expertise du sujet, ainsi que le Professeur Peter Cameron pour toutes ses remarques, et une question très intéressante.

Ce travail n'aurait pas été possible sans Adrian Bondy, qui a su diriger cette thèse tout en laissant à son élève une très grande liberté. Il a également beaucoup apporté à ce texte par une relecture très rigoureuse. Je tiens tout particulièrement à lui exprimer ma gratitude pour les efforts considérables qu'il a déployé afin de rendre possible mon insertion professionnelle dans la communauté mathématique.

Introduction

Étant donné une structure quelconque, on peut se demander si elle peut être identifiée à partir de ses composants. Pour que ce problème ait un sens, il faut naturellement que les composants soient utiles à plusieurs structures. Ainsi on est amené à formuler un problème de reconstruction, en définissant une classe de structures, dotée d'une notion de sous-structure. Pour alimenter le coté générique des briques de base, on dote l'ensemble des structures d'une action de groupe compatible avec la notion de sous-structure. C'est donc naturellement vers la notion de groupe agissant sur un ensemble partiellement ordonné (poset) que l'on va se tourner en suivant cette approche.

Ainsi, on est amené a définir un problème de reconstruction générique de façon formelle :

Problème 1. *Étant donné un ensemble partiellement ordonné fini P, muni de l'action d'un groupe G, compatible avec la structure de poset, c'est à dire : si $A \subseteq B$ et $\sigma \in G$, alors $\sigma(A) \subseteq \sigma(B)$, et un ensemble d'orbites $\mathcal{O}_1, \ldots, \mathcal{O}_r$ de P sous l'action de G, peut-on identifier l'orbite à laquelle appartient un élément A de P par le nombre d'éléments de chacune des $\mathcal{O}_i$ inclus dans A ?*

En théorie des graphes, ce cadre générique est motivé par la conjecture de reconstruction formulée par S.M.Ulam et P.J.Kelly ([6], [26]). On rappelle ici l'énoncé de cette conjecture, ainsi que quelques résultats. On pourra se reporter à [2] pour un excellent aperçu de la théorie des graphes, ainsi qu'à [1] pour le détail des résultats déjà obtenus sur les conjectures de reconstruction.

Si G est un graphe sur l'ensemble de sommets $\{1, \ldots, n\}$, on peut, pour chaque sommet i, considérer le graphe obtenu en retirant de G toutes les arêtes incidentes à i. L'ensemble de tous les types de graphes obtenus de cette façon à partir de G, comptés avec multiplicités, est appelé le *deck* de G.

Conjecture 1 (Ulam)**.** *Si G est un graphe sur au moins trois sommets, alors le type de G est uniquement déterminé par son deck.*

Une autre conjecture plus faible concernant les arêtes est due à F.Harary ([5]). Si G est un graphe, on peut, pour chaque arête a de G, considérer le graphe obtenu en retirant a de G. L'ensemble de tous les types de graphes obtenus de cette façon à partir de G, comptés avec multiplicités est appelé le *deck-arête* de G.

Conjecture 2 (Harary)**.** *Si G est un graphe ayant au moins quatre arêtes, alors le type de G est uniquement déterminé par son deck-arête.*

Pour la Conjecture 2, divers résultats ont été obtenus, notamment :

Proposition 1 (Lovász)**.** *Un graphe sur n sommets est arête-reconstructible si il a strictement plus de $\frac{n(n-1)}{4}$ arêtes.*

Proposition 2 (Müller)**.** *Un graphe sur n sommets est arête-reconstructible si il a plus de $1 + log_2 n!$ arêtes.*

En revanche, pour la reconstructibilité associée à la Conjecture 1 on sait qu'un graphe est reconstructible si et seulement si son complémentaire l'est. On sait aussi que les graphes non connexes sont reconstructibles [7], que le nombre de cycles hamiltoniens est reconstructible, et donc aussi le polynôme caractéristique.

Enfin, on sait que la conjecture de Ulam-Kelly implique celle de Harary.

Au titre des généralisations, on peut noter que la conjecture de sommet-reconstruction pour les digraphes est fausse (Stockmeyer [22]).

On développe ici l'approche mentionnée plus haut qui met en avant le groupe de permutations agissant sur un poset P qui est ici celui des parties d'un ensemble. Il est probable que des résultats et méthodes soient généralisables à un poset quelconque, mais la complexité du problème dans le seul cas du poset booléen impose la plus grande humilité pour ce qui est du cas général.

On remarque que l'ensemble des fonctions à valeurs réelles définies sur P est en bijection avec l'espace vectoriel réel formel défini sur P grâce à la relation d'inclusion (une base de cet espace est formée par les applications $p_B \ : \ A \mapsto \ 1$ si $A \subseteq B, \ 0$ sinon) et que cet espace est naturellement muni d'une structure d'algèbre grâce à la multiplication dans $\mathbb{R}$, correspondant à l'opération union.

On pose donc S_n l'algèbre formée par l'espace vectoriel réel P muni de l'opération bilinéaire union, qui est en bijection avec $\mathcal{L}(P, \mathbb{R})$. Cette algèbre à déjà fait l'objet de travaux importants et une partie des résultats présentés ici (celle qui traite du calcul et des premières propriétés) n'est qu'une reformulation de considérations effectuées par d'autres (voir par exemple [9], [4],[12], et [14]).

Il est ainsi possible d'exprimer les fonctions qui, à un ensemble A, associent le nombre d'éléments d'une orbite $\mathcal{O}_i$ inclus dans A, comme des éléments de S_n : ce sont en fait les $p_{\mathcal{O}_i}$, sommes des applications p_B pour B parcourant $\mathcal{O}_i$.

La structure d'algèbre de $\mathcal{S}_n$ définie de cette manière traduit le problème de reconstruction générique (Problème 1) en ce sens qu'un problème de reconstruction par les O_i est vrai si et seulement si les $p_{\mathcal{O}_i}$ engendrent l'algèbre des invariants $\mathcal{S}_n^G$ du groupe G.

Il est clair que l'ensemble des polynômes reconstructibles est contenu dans $\mathcal{S}_n^G$, et s'il existe un groupe H plus grand que G qui stabilise les $\mathcal{O}_i$, contenu dans $\mathcal{S}_n^H$. Deux cas sont possibles : soit l'algèbre engendrée par les $p_{\mathcal{O}_i}$ est l'algèbre des invariants d'un certain groupe, auquel cas on obtient le meilleur résultat possible de reconstruction, soit ce n'est pas le cas. Ainsi, on est naturellement amené à se demander sous quels critères une sous-algèbre de $\mathcal{S}_n$ est l'algèbre des invariants d'un certain groupe G. Une réponse à cette question ramènerait l'étude d'un problème de reconstruction au fait de savoir si l'algèbre engendrée par les $p_{\mathcal{O}_i}$ vérifie ces critères.

Il est clair que toute algèbre d'invariants vérifie certaines propriétés, comme par exemple :

- étant donné deux orbites $\mathcal{O}_1$ et $\mathcal{O}_2$, le nombre d'éléments de $\mathcal{O}_1$ qui contiennent un représentant de $\mathcal{O}_2$ est indépendant du représentant choisi. On peut traduire ceci par la stabilité des algèbres d'invariants sous l'opération :
$$\partial\left(\prod_{i\in S} x_i\right) = \sum_{i\in S}\prod_{j\in S\setminus i} x_j$$
- étant donné une orbite $\mathcal{O}_1$ l'ensemble des complémentaires des éléments de $\mathcal{O}_1$ est aussi une orbite. On peut traduire ceci par la stabilité des algèbres d'invariants sous l'opération :
$$\complement\left(\prod_{i\in S} x_i\right) = \prod_{j\notin S} x_j$$

On conjecture ici que, réciproquement, toute sous-algèbre de S_n invariante par ∂ et $\complement$ est l'algèbre des invariants d'un certain groupe H.

L'essentiel de ce travail est le résultat de tentatives infructueuses de démonstration de cette conjecture qui reste à ce jour irrésolue.

Il est intéressant de remarquer que les objets introduits dans ce but permettent d'expliciter très convenablement les résultats de L.Lovász et V.Müller, et de proposer des pistes pour de nouveaux résultats.

En effet, on peut remarquer qu'une sous-algèbre de $\mathcal{S}_n$ est une algèbre d'invariants, si et seulement si elle est stable par les applications des $\mathrm{Com}_k(\mathfrak{S}_n)$, espaces vectoriels des applications linéaires h de $\mathcal{S}_n^{\otimes k}$ dans $\mathcal{S}_n$ telles que

$$\forall \sigma \in \mathfrak{S}_n,\ \sigma \circ h = h \circ (\underbrace{\sigma \otimes \sigma \otimes \ldots \otimes \sigma}_{k})$$

c'est à dire qu'une sous algèbre $\mathcal{A}$ de $\mathcal{S}_n$ est une algèbre d'invariants si et seulement si

$$\mathrm{Com}_k(\mathfrak{S}_n)(\mathcal{A}^{\otimes k}) \subseteq \mathcal{A}$$

On cherchera donc à exprimer les applications de $\mathrm{Com}_k(\mathfrak{S}_n)$ grâce aux trois opérations dont on dispose, c'est à dire ∂, $\complement$, et la multiplication.

Si l'on s'intéresse aux nombres $\binom{\mathcal{O}_1}{\mathcal{O}_2}$ d'éléments d'une orbite $\mathcal{O}_2$ inclus dans un représentant quelconque d'une orbite $\mathcal{O}_1$ on peut remarquer que les matrices de ces trois opérations peuvent s'exprimer grâce au nombres $\binom{\mathcal{O}_1}{\mathcal{O}_2}$. Il est donc clair que les relations de dépendance qui existent entre ces opérateurs fournissent immédiatement des relations entre ces coefficients. Ces relations sont d'un intérêt évident pour les problèmes de reconstruction, en effet, on peut traduire tous les résultats existants en termes de relations polynomiales, valables dans toute algèbre d'invariants. Un problème de reconstruction est facilement traduisible par la possibilité d'égalité entre certaines lignes de coefficients. On s'intéresse également à la généralisation aux algèbres stables par ∂ et $\complement$ (*digèbres*), pour lesquelles on généralise les résultats de Lovász et Müller sur la reconstruction. Comme on l'a déjà remarqué, cette approche met en valeur le groupe sous-jacent aux problèmes de reconstruction, aspect qui a déjà fait l'objet de travaux par P.J. Cameron, V.B. Mnukhin, ce qui permet de donner des limites à ces résultats, et on montre ici que sous leurs hypothèses, ils sont les meilleurs possibles.

Ce travail se termine par la description de cas particuliers intéressants comme ceux des graphes et des digraphes, et l'on remarquera que le cas des graphes présente une particularité intéressante : en effet dans ce cas on peut montrer que le groupe de symétries sous-jacent est celui d'un seul élément. Dans, ce cadre, la conjecture sur les algèbres stables par ∂ et $\complement$ présente des liens très intéressants avec la Conjecture 1. On s'intéresse donc aux digèbres

engendrées par un seul élément, cas particulier qui s'avère toutefois difficile et pour lequel la conjecture reste indémontrée.

Dans le cadre plus général d'une action de groupe sur l'ensemble partiellement ordonné des sous-ensembles d'un ensemble, de nombreux résultats ont été obtenus, dont le fameux théorème de Livingstone et Wagner([10]). On pourra par exemple citer [17], [21], [3]. Des travaux présentant des similarités ont aussi été effectués, par exemple [24], [25], [19], et enfin [20] qui présente un théorème dont l'énoncé ressemble fort à la conjecture originale présentée ci-dessus.

Le chapitre 1 concerne la théorie générale associée aux algèbres stables par ∂ et C, elle met en place une structure de blocs qui correspond à celle d'orbites dans le cas des algèbres d'invariants, et détaille diverses règles de calculs et outils relatifs aux digèbres. Ce cadre algébrique abstrait a été forgé pour donner une rigueur nécessaire aux résultats naturels, et s'il est intéressant du point de vue esthétique, et fonctionnel (en ce sens qu'il engendre *ex-nihilo* des relations), son intérêt principal réside dans le fait qu'il fut à maintes reprises un langage de validation performant.

Le chapitre 2 concerne les coefficients $\binom{\mathcal{O}_1}{\mathcal{O}_2}$, et les relations qui les relient, on y fait le lien avec les travaux et résultats précédents qui sont intégrés dans la théorie des digèbres par le biais des relations polynomiales entre coefficients. L'aspect reconstructif de ces résultats y est volontairement sous-représenté, en effet il s'agit surtout de mettre en évidence les relations polynomiales, et d'intégrer les travaux précédents dans un traitement plus systématique et élaboré de l'ensemble des relations polynomiales entre les $\binom{\mathcal{O}_1}{\mathcal{O}_2}$. On y établi également une petite classification de ces relations, dans le but de mettre en évidence ce que chaque résultat apporte d'un point de vue strictement formel. Contrairement à celui de L. Lovász, le résultat de V. Müller ne figure toutefois pas dans cette étude, en effet il repose plus sur une interprétation que sur une nouvelle relation. Son expression est reportée dans le chapitre 3, le lecteur intéressé pourra sans peine imaginer que ce résultat s'intègre bien dans le cadre proposé.

On exprime dans le chapitre 3 des problèmes de reconstruction généraux comme indiqué ci-dessus, pour lesquels les résultats de V.Müller et de L.Lovász sont valides, et l'on montre des cas ou ces résultats sont les meilleurs possibles. On présente ensuite les cas particuliers des graphes et des digraphes, et l'on montre les liens qui existent entre la conjecture de Ulam, la conjecture présentée ci-dessus sur les algèbres stables par ∂ et C, et en particulier

le cas intéressant des digèbres engendrées par un élément, dans lequel la reconstruction par les sommets trouve sa place.

Une annexe présente les caractéristiques des algèbres d'invariants de petits ordres, dont on a vérifié qu'elles sont les digèbres pour les très petits cas. On y pioche au fil de l'eau quelques digèbres remarquables, notamment des exemples de digèbres non équivalentes ayant pourtant le même jeu de coefficients. Les exemples limites des résultats de L.Lovász et V.Müller y sont aussi représentés. Ils peuvent servir d'exemple à tout moment au lecteur qui pourra y vérifier les résultats présentés, ou quelque autre intuition personnelle. On y montre aussi les cardinalités non reconstructibles pour un problème de reconstruction par les arêtes généralisé au sens de P.J. Cameron et V.B Mnukhin.

Chapitre 1

Digèbres

Dans toute cette partie, n est un nombre entier fixé supérieur où égal à un. On considère l'ensemble $\{1, \ldots, n\}$ des nombres entiers de 1 à n, ainsi que l'ensemble de ses parties : $\mathcal{P}(\{1, \ldots, n\})$.

1.1 Algèbre d'incidence, fonctions polynomiales, et actions de groupes

1.1.1 Algèbre d'incidence

Définition 1. *On note $\mathcal{S}_n$ l'algèbre résultant du quotient de l'algèbre de polynômes sur n indéterminées $\mathbb{R}[x_1, \ldots, x_n]$ par l'idéal engendré par les polynômes $x_1^2 - x_1, x_2^2 - x_2, \ldots, x_n^2 - x_n$.*

Pour mettre l'accent sur le produit dans $\mathcal{S}_n$ on le notera parfois $p \cdot q$ en lieu et place de pq.

Il est clair que $\mathcal{S}_n$ est un $\mathbb{R}$-espace vectoriel de dimension 2^n dont une base est formée par les

$$p_S = \prod_{i \in S} x_i, \text{ où } S \in \mathcal{P}(\{1, \ldots, n\})$$

On a donc par convention $p_\emptyset = 1$, et pour tout couple de sous-ensembles

A et B de $\{1,\ldots,n\}$, $p_A \cdot p_B = p_{A\cup B}$. On notera dans toute la suite $|S|$ le cardinal de S.

Définition 2. *Si A et B sont des sous-ensembles de $\{1,\ldots,n\}$, on définit $p_A(B)$ comme étant égal à 1 si A est contenu dans B, et à 0 sinon. On obtient ainsi un isomorphisme d'algèbre entre $\mathcal{S}_n$ et l'ensemble des fonctions à valeurs réelles sur $\mathcal{P}(\{1,\ldots,n\})$.*

Proposition 3. *Soit $p \in \mathcal{S}_n$, alors*

$$p(S) = 0,\ \forall S \subseteq \{1,\ldots,n\} \ \Leftrightarrow\ p = 0$$

Preuve : Soit

$$p = \sum_{A\subseteq\{1,\ldots,n\}} \alpha_A p_A \ \in \mathcal{S}_n$$

si $p \neq 0$, il existe $C \subseteq \{1,\ldots,n\}$ tel que

$$\alpha_C \neq 0 \text{ et } \forall D \ t.q.\ D \subseteq C,\ \alpha_D = 0$$

On a alors $p(C) = \alpha_C \neq 0$, la réciproque est évidente. □

1.1.2 Caractères et sous-algèbres de $\mathcal{S}_n$

Proposition 4. *Si ϕ est un morphisme d'algèbre non nul de $\mathcal{S}_n$ dans $\mathbb{R}$, alors il existe $S \subseteq \{1,\ldots,n\}$ tel que*

$$\phi(p) = p(S), \quad \forall\ p \in \mathcal{S}_n$$

Preuve : On a pour toute partie A de $\{1,\ldots,n\}$: $\phi(p_A) = \phi({p_A}^2) = \phi(p_A)^2$ donc $\phi(p_A)$ vaut soit 0 soit 1. De plus pour toutes les parties A et B de $\{1,\ldots,n\}$, on a $\phi(p_A)\phi(p_B) = \phi(p_A p_B) = \phi(p_{A\cup B})$. Donc l'ensemble des parties A telles que $\phi(p_A) = 1$ est stable par union et on a :

$$\text{si } A \subseteq B \text{ alors } \phi(p_B) = 1 \Rightarrow \phi(p_A) = 1$$

On en déduit que l'ensemble des parties A telles que $\phi(p_A) = 1$ est l'ensemble des parties d'un certain sous-ensemble S de $\{1,\ldots,n\}$.

Réciproquement, pour toute partie S de $\{1,\ldots,n\}$, l'application de $\mathcal{S}_n$ dans $\mathbb{R}$ qui à p associe $p(S)$ est un morphisme d'algèbre. □

Proposition 5. *Si $\mathcal{A}$ est une sous-algèbre de $\mathcal{S}_n$ contenant 1, alors il existe une partition P de $\mathcal{P}(\{1,\ldots,n\})$ telle que*

$$\mathcal{A} = \left\{p \ \in \mathcal{S}_n \quad t.q. \quad \forall P_i \in P \quad \forall (A,B) \in P_i^2 \quad p(A) = p(B)\right\}$$

Remarque 1. *On peut donc dire que les caractères de $\mathcal{S}_n$ (i.e. les morphismes d'algèbre de $\mathcal{S}_n$ dans $\mathbb{R}$) trient les sous-algèbres.*

Preuve : On définit une relation d'équivalence sur $\mathcal{P}(\{1,\ldots,n\})$ par :

$$A\mathcal{R}B \Leftrightarrow p(A) = p(B),\ \forall p \ \in \mathcal{A}$$

Cette relation partitionne $\mathcal{P}(\{1,\ldots,n\})$ en blocs $P_1,\ldots,P_n$. On va montrer que pour tout bloc P_i, il existe un polynôme q_i de $\mathcal{A}$ tel que $q_i(A) = 1$ si $A \in P_i$ et $q_i(A) = 0$ sinon.

Supposons tout d'abord que $\mathcal{A}$ soit engendrée par un seul polynôme p. Alors si A est un élément de P_i on prend

$$q_i = \frac{\prod_{T \notin P_i}(p - p(T))}{\prod_{T \notin P_i}(p(A) - p(T))}$$

Dans le cas général, comme $\mathcal{A}$ est de dimension finie, il existe $p_1,\ldots,p_s$ des générateurs de $\mathcal{A}$, et alors les blocs de $\mathcal{A}$ sont les intersections de ceux des algèbres engendrées par p_1, par p_2, par ..., par p_s. Il suffit ensuite de considérer le produit des q_i obtenus. □

Remarque 2. *La construction qui précède est une interpolation de Lagrange. On verra dans la suite l'usage qu'on en fait pour construire les idempotents de l'algèbre $\mathcal{S}_n$. L'usage de cette construction dans ce but est bien connue en algèbre commutative, le lecteur interressé pourra se reporter à [14] comme première référence bibliographique.*

Remarque 3. *Réciproquement, toute partition de $\mathcal{P}(\{1,\ldots,n\})$ définit une unique sous-algèbre de $\mathcal{S}_n$, d'où le corollaire suivant :*

Corollaire 1. *Il y a un nombre fini de sous-algèbres de $\mathcal{S}_n$.*

Preuve : Elles sont en bijection avec les partitions de $\mathcal{P}(\{1,\ldots,n\})$. □

1.1.3 Actions de groupes

Le groupe des permutations $\mathfrak{S}_n$ de $1, \ldots, n$ agit de manière naturelle sur $\mathcal{S}_n$ comme un groupe d'isomorphismes d'algèbre défini par :

$$\sigma \cdot x_i = x_{\sigma(i)} \ , \ \sigma \ \in \ \mathfrak{S}_n$$

En effet, on obtient pour tout sous-ensemble A de $\{1, \ldots, n\}$, $\sigma(p_A) = p_{\sigma(A)}$ avec $\sigma(A) = \{\sigma(a), \quad a \in A\}$. On a donc bien, pour tout couple de sous-ensembles A et B de $\{1, \ldots, n\}$, $\sigma(p_A \cdot p_B) = \sigma(p_{A \cup B}) = p_{\sigma(A \cup B)} = \sigma(p_A) \cdot \sigma(p_B)$.

Définition 3. *Étant donné un sous-groupe G de $\mathfrak{S}_n$, l'ensemble :*

$$\mathcal{S}_n^G = \{p \in \mathcal{S}_n \quad t.q. \quad \sigma \cdot p = p \quad \forall \sigma \in G\}$$

est une sous-algèbre de $\mathcal{S}_n$. On l'appelle sous-algèbre d'invariants *de G. Les éléments de $\mathcal{S}_n^G$ sont appelés* invariants *de G, et on parlera donc parfois d'ensemble des invariants de G pour désigner $\mathcal{S}_n^G$.*

L'objet de ce chapitre est une tentative de caractérisation des sous-algèbres de $\mathcal{S}_n$ qui sont des sous-algèbres d'invariants.

1.2 Digèbres

1.2.1 Définition

Définition 4.

- *On appelle* dérivation *et on note ∂ l'application linéaire de $\mathcal{S}_n$ dans $\mathcal{S}_n$ définie par :*

$$\partial\left(\prod_{i \in S} x_i\right) = \sum_{i \in S} \prod_{j \in S \setminus i} x_j$$

c'est à dire :

$$\partial(p_S) = \sum_{i \in S} p_{S \setminus i}$$

- *On appelle* complémentation *et on note* $\complement$ *l'application linéaire de* $\mathcal{S}_n$ *dans* $\mathcal{S}_n$ *définie par :*

$$\complement\left(\prod_{i\in S} x_i\right) = \prod_{j\notin S} x_j$$

c'est à dire :

$$\complement\left(p_S\right) = p_{S^c}$$

On a alors par convention $\partial(p_\emptyset) = \partial(1) = 0$ et $\complement(p_\emptyset) = \complement(1) = p_{\{1,\ldots,n\}}$.

Remarque 4. *Le complémentaire de l'ensemble* S *dans* $\{1,\ldots,n\}$ *sera noté* S^c *dans toute la suite.*

Proposition 6. $\complement$ *est un isomorphisme et* $\complement^2 = Id$.

Preuve : A partir de la définition et du fait que la complémentation est d'ordre 2. □

Proposition 7. *Soit* $S \subseteq \{1,\ldots,n\}$, *on a :*

$$\partial^k(p_S) = \sum_{\substack{A\subseteq S \\ |A|=|S|-k}} k!p_A \quad \forall k \geq 0$$

Il s'agit tout simplement de compter combien il y a de façons d'enlever successivement k éléments de l'ensemble S pour obtenir un certain ensemble $A \subseteq S$.

Preuve : par récurrence sur k :

- si $k = 0$ les deux membres de l'équation valent p_S.

- On a

$$\begin{aligned}
\partial^{k+1}(p_S) &= \partial \circ \partial^k(p_S) \\
&= \sum_{\substack{A\subseteq S \\ |A|=|S|-k}} k!\partial(p_A) \\
&= \sum_{\substack{B\subseteq S \\ |B|=|S|-k-1}} \left(\sum_{\substack{B\subseteq A\subseteq S \\ |A|=|S|-k}} 1 \right) k!p_B \\
&= \sum_{\substack{B\subseteq S \\ |B|=|S|-k-1}} (|S|-|B|)\, k!p_B \\
&= \sum_{\substack{B\subseteq S \\ |B|=|S|-k-1}} (k+1)!p_B
\end{aligned}$$

□

Corollaire 2. *∂ est un endomorphisme nilpotent d'indice n+1.*

Définition 5. *On appelle* digèbre *une sous-algèbre non vide, non réduite à $\{0\}$ de $\mathcal{S}_n$, qui est stable par dérivation et par complémentation.*

Remarque 5. *Pour être précis, on devrait parler de n-digèbre, ou de digèbre d'ordre n. On omettra néanmoins de préciser le n lorsque le contexte l'indique clairement. Dans tout ce chapitre, n est un entier fixé. Les trois opérations de dérivation, complémentation, et multiplication sont indispensables à la définition, comme on le verra p37.*

Exemples :

- Il est clair que $\mathcal{S}_n$ est une digèbre.
- si n=3, l'algèbre $\mathcal{S}_3$ est formée par les combinaisons linéaires sur les vecteurs

$$1,\ x_1,\ x_2,\ x_3,\ x_1x_2, x_1x_3,\ x_2x_3,\ x_1x_2x_3$$

  Soit $\mathcal{D}$ l'ensemble des combinaisons linéaires sur les vecteurs

$$1,\ x_1+x_2,\ x_3,\ x_1x_2,\ x_1x_3+x_2x_3,\ x_1x_2x_3$$

on a la table de multiplication :

$* \nearrow$	1	x_1+x_2	x_3	x_1x_2	$x_3x_1+x_2x_3$	$x_1x_2x_3$
1	1	x_1+x_2	x_3	x_1x_2	$x_3x_1+x_2x_3$	$x_1x_2x_3$
x_1+x_2	x_1+x_2	$x_1+x_2+2x_1x_2$	$x_1x_3+x_2x_3$	$2x_1x_2$	$x_1x_3+x_2x_3+2x_1x_2x_3$	$2x_1x_2x_3$
x_3	x_3	$x_1x_3+x_2x_3$	x_3	$x_1x_2x_3$	$x_1x_3+x_2x_3$	$x_1x_2x_3$
x_1x_2	x_1x_2	$2x_1x_2$	$x_1x_2x_3$	x_1x_2	$2x_1x_2x_3$	$x_1x_2x_3$
$x_3x_1+x_2x_3$	$x_3x_1+x_2x_3$	$x_1x_3+x_2x_3+2x_1x_2x_3$	$x_1x_3+x_2x_3$	$2x_1x_2x_3$	$x_1x_3+x_2x_3+2x_1x_2x_3$	$x_1x_2x_3$
$x_1x_2x_3$	$x_1x_2x_3$	$2x_1x_2x_3$	$x_1x_2x_3$	$x_1x_2x_3$	$2x_1x_2x_3$	$x_1x_2x_3$

Donc $\mathcal{D}$ est une sous-algèbre de $\mathcal{S}_3$. On a de plus :

$$\begin{aligned}
\partial(1) &= 0\\
\partial(x_1+x_2) &= 2\\
\partial(x_3) &= 1\\
\partial(x_1x_2) &= x_1+x_2\\
\partial(x_1x_3+x_2x_3) &= x_1+x_2+2x_3\\
\partial(x_1x_2x_3) &= x_1x_2+x_1x_3+x_2x_3
\end{aligned}$$

et :

$$\begin{aligned}
\complement(1) &= x_1x_2x_3\\
\complement(x_1+x_2) &= x_1x_3+x_2x_3\\
\complement(x_3) &= x_1x_2\\
\complement(x_1x_2) &= x_3\\
\complement(x_1x_3+x_2x_3) &= x_1+x_2\\
\complement(x_1x_2x_3) &= 1
\end{aligned}$$

Donc $\mathcal{D}$ est en plus stable par dérivation et par complémentation : c'est une digèbre.

1.2.2 Premières propriétés

Définition 6. *On note l l'endomorphisme de $\mathcal{S}_n$ défini par*

$$l(x) = \sum_{k=0}^{n} \frac{\partial^k(x)}{k!}$$

Proposition 8. *$\forall S \subseteq \{1, \ldots, n\}$, on a :*

$$l(p_S) = \sum_{A \subseteq S} p_A$$

Preuve : D'après la Proposition 7 p17,

$$\sum_{k=0}^{n} \frac{\partial^k(p_S)}{k!} = \sum_{k=0}^{n} \sum_{\substack{A \subseteq S \\ |A| = |S| - k}} p_A = \sum_{A \subseteq S} p_A$$

□

Proposition 9. *Pour tout entier r non nul, on a :*

$$l^r = \sum_{k=0}^{n} \frac{r^k}{k!} \partial^k$$

Preuve : Si $r \neq 0$ et $s \neq 0$, alors

$$\begin{aligned}
\left(\sum_{k=0}^{n} \frac{r^k}{k!} \partial^k\right) \circ \left(\sum_{i=0}^{n} \frac{s^i}{i!} \partial^i\right) &= \sum_{k=0}^{n} \sum_{i=0}^{n} \frac{r^k s^i}{k! i!} \partial^{k+i} \\
&= \sum_{m=0}^{2n} \partial^m \sum_{k=0}^{m} \frac{r^k s^{m-k}}{k!(m-k)!} \\
&= \sum_{m=0}^{n} \frac{\partial^m}{m!} \sum_{k=0}^{m} \frac{m!}{k!(m-k)!} r^k s^{m-k} \\
&= \sum_{m=0}^{n} \frac{(r+s)^m}{m!} \partial^m
\end{aligned}$$

La proposition est vraie pour $r = 1$, donc par récurrence pour tout $r \geq 1$ grâce au calcul ci-dessus. Ce même calcul montre que

$$\left(\sum_{k=0}^{n} \frac{(-1)^k}{k!} \partial^k\right) \circ l = Id$$

La proposition est donc vraie pour $r = -1$, et par suite pour tout $r \leq -1$ par récurrence. $\square$

Corollaire 3. *l est un isomorphisme de $\mathcal{S}_n$.*

Preuve : on a d'après la Proposition 9 p20 :

$$l^{-1} = \sum_{k=0}^{n} \frac{(-1)^k}{k!} \partial^k$$

$\square$

Proposition 10. *Il existe des nombres rationnels $a_1, \ldots, a_{n+1}$ tels que :*

$$\partial = \sum_{r=1}^{n+1} a_r l^r$$

Preuve : D'après la Proposition 9 p20, si $r \geq 1$:

$$l^r = \sum_{k=0}^{n} \frac{r^k}{k!} \partial^k$$

Il faut donc choisir les $a_1, \ldots, a_{n+1}$ de telle façon que :

$$\sum_{r=1}^{n+1} a_r r^k = \begin{cases} 1 \ si \ k = 1 \\ 0 \ sinon \end{cases}$$

C'est à dire :

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & n+1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 2^n & \cdots & (n+1)^n \end{bmatrix} \cdot \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_{n+1} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}$$

Ceci est toujours possible grâce à l'inversion de la matrice de Vandermonde considérée. $\square$

Corollaire 4. *Si V est un sous-espace vectoriel de $\mathcal{S}_n$ alors V est stable par ∂ si et seulement si V est stable par l.*

Corollaire 5. *Une digèbre est une sous-algèbre non vide, non réduite à* $\{0\}$ *de* $\mathcal{S}_n$ *qui est stable par* l *et par* $\complement$.

Définition 7. *On note* ε *l'endomorphisme de* $\mathcal{S}_n$ *défini par*

$$\varepsilon(x) = \complement \circ l^{-1} \circ \complement(x)$$

De plus, si $x = p_S$*, on notera* $\varepsilon_S = \varepsilon\left(p_S\right)$.

Proposition 11. *Une digèbre est une sous-algèbre non vide, non réduite à* $\{0\}$ *de* $\mathcal{S}_n$ *qui est stable par* ε *et par* $\complement$.

Preuve : D'après le Corollaire 5 p22, $\mathcal{D}$ est une digèbre si, et seulement si $\mathcal{D}$ est stable par l et par $\complement$. Comme l est un isomorphisme, il est clair que $\mathcal{D}$ est stable par l si et seulement si $\mathcal{D}$ est stable par l^{-1}. □

Proposition 12. *L'ensemble* $\{\varepsilon_S \ : \ S \subseteq \{1, \ldots, n\}\}$ *est une base de* $\mathcal{S}_n$.

Preuve : ε est un isomorphisme, comme composé d'isomorphismes. □

Proposition 13.

$$\varepsilon_S = \sum_{A \supseteq S} (-1)^{|A|-|S|} p_A$$

Preuve : Par définition :

$$\begin{aligned}
\varepsilon_S &= \sum_{k=0}^{n} \frac{(-1)^k}{k!} \complement \circ \partial^k(p_{S^c}) \\
&= \sum_{k=0}^{n} (-1)^k \sum_{\substack{A \subseteq S^c \\ |A| = |S^c| - k}} p_{A^c} \\
&= \sum_{k=0}^{n} (-1)^k \sum_{\substack{B \supseteq S \\ |B| = |S| + k}} p_B \\
&= \sum_{B \supseteq S} (-1)^{|B|-|S|} p_B
\end{aligned}$$

□

Proposition 14. $\varepsilon_S(T) = 1$ *si* $S = T$ *et* 0 *sinon.*

Preuve :

$$\begin{aligned}
\varepsilon_S(T) &= \sum_{A \supseteq S} (-1)^{|A|-|S|} p_A(T) \\
&= (-1)^{|S|} \sum_{A \ t.q. \ S \subseteq A \subseteq T} (-1)^{|A|} \\
&= \begin{cases} 1 \ si \ S = T \\ 0 \ si \ S \neq T \end{cases}
\end{aligned}$$

□

Proposition 15. *Pour tout polynôme p de $\mathcal{S}_n$, on a :*

$$p \cdot \varepsilon_T = p(T)\varepsilon_T$$

Preuve : D'après la Proposition 3 p14, il suffit de vérifier que :

$$\forall S \subseteq \{1, \ldots, n\}, \ p(S)\varepsilon_T(S) = p(T)\varepsilon_T(S)$$

D'après la Proposition 14 p22, on a :

$$p(S)\varepsilon_T(S) = \begin{cases} p(T) & si \ S = T \\ 0 & sinon \end{cases} = p(T)\varepsilon_T(S)$$

□

Proposition 16. *Si S et T sont deux parties de $\{1, \ldots, n\}$, on a :*

$$\varepsilon_S \cdot \varepsilon_T = \begin{cases} \varepsilon_S & si \ S = T \\ 0 & sinon \end{cases}$$

Preuve : D'après la Proposition 15 p23

$$\varepsilon_S \cdot \varepsilon_T = \varepsilon_S(T)\varepsilon_T$$

On conclut grâce à la Proposition 14 p22. □

Remarque 6. *La définition des ε rentre dans le cadre des algèbres de Möbius, telles que définies par V.B.Mnukhin ([14]). Ils représentent une base de l'algèbre $\mathcal{S}_n$ dans laquelle le produit correspond au produit de Kronecker, ce qui facilite grandement les calculs.*

Corollaire 6. *Si B_1 et B_2 sont deux ensembles de sous-ensembles de $\{1, \ldots, n\}$, alors :*

$$\left(\sum_{S \in B_1} \varepsilon_S\right) \cdot \left(\sum_{T \in B_2} \varepsilon_T\right) = \sum_{U \in B_1 \cap B_2} \varepsilon_U$$

Proposition 17.

$$p_S = \sum_{A \supseteq S} \varepsilon_A$$

On remarque que ceci n'est qu'une inversion de Möbius de la Proposition 13 p22.

Preuve : On sait que les ε_A forment une base de $\mathcal{S}_n$, donc il existe des coefficients α_A^S tels que

$$p_S = \sum_{A \subseteq \{1,\ldots,n\}} \alpha_A^S \varepsilon_A$$

On doit alors avoir

$$p_S \cdot \varepsilon_T = \sum_{A \subseteq \{1,\ldots,n\}} \alpha_A^S \varepsilon_A \varepsilon_T = \alpha_T^S \, \varepsilon_T$$

d'après la Proposition 16 p23, et

$$p_S \cdot \varepsilon_T = p_S(T)\varepsilon_T = \begin{cases} \varepsilon(T) & si \ S \subseteq T \\ 0 & sinon \end{cases}$$

d'après la Proposition 15 p23. On a donc

$$\alpha_T^S = \begin{cases} 1 & si \ S \subseteq T \\ 0 & sinon \end{cases}, \quad p_S = \sum_{T \ t.q. \ S \subseteq T} \varepsilon_T$$

□

Proposition 18. *Si $\mathcal{D}$ est une digèbre, alors $\mathcal{D}$ contient les polynômes*

$$\sum_{A \ t.q. \ |A|=k} p_A, \quad k \in \{0 \ldots n\}$$

Remarque 7. *On obtient ainsi le fait que toute digèbre contient l'algèbre des invariants du groupe symétrique, c'est à dire $\mathcal{S}^{\mathfrak{S}_n}$.*

Preuve : $\mathcal{D}$ est une digèbre, donc il existe

$$p = \sum_{A \subseteq \{1,\dots,n\}} \alpha_A \varepsilon_A \neq 0 \ \in \mathcal{D}$$

D'après la Proposition 16 p23 :

$$p^2 = \sum_{A \subseteq \{1,\dots,n\}} \alpha_A^2 \varepsilon_A \in \mathcal{D}$$

donc :

$$\varepsilon^{-1}(p^2) = \sum_{A \subseteq \{1,\dots,n\}} \alpha_A^2 p_A \in \mathcal{D}$$

Posons $k = max\,\{r \ t.q. \ \exists A \subseteq \{1,\dots,n\} \ t.q. \ |A| = r \ et \ \alpha_A \neq 0\}$. Alors

$$\partial^k \circ \varepsilon^{-1}(p^2) = \left(\sum_{A \subseteq \{1,\dots,n\} \ t.q. \ |A|=k} k! \alpha_A^2 \right) p_\emptyset \in \mathcal{D}$$

Donc $1 = p_\emptyset \in \mathcal{D}$ qui est stable par $\complement$ donc $p_{\{1,\dots,n\}} \in \mathcal{D}$. Il ne reste plus qu'à remarquer que :

$$\frac{1}{s!} \partial^s (p_{\{1,\dots,n\}}) = \sum_{A \ t.q. \ |A|=n-s} p_A, \quad s \in \{1 \dots n\}$$

□

Définition 8. *Il est clair que l'intersection de deux digèbres est une digèbre non réduite à* $\{0\}$ *d'après la Proposition 18 p24. On peut donc parler de digèbre engendrée : si* S *est un sous-ensemble de* $\mathcal{S}_n$*, on définit la* digèbre engendrée *par* S *comme étant la plus petite digèbre (au sens de l'inclusion) contenant* S*.*

Exemple : si $n = 3$, la digèbre engendrée par $x_1 x_2 x_3$ est formée par les combinaisons linéaires des vecteurs

$$1, x_1 + x_2 + x_3, x_1 x_2 + x_2 x_3 + x_1 x_3, x_1 x_2 x_3$$

1.2.3 Système de blocs d'une digèbre

Définition 9. *On appelle* bloc *d'une digèbre $\mathcal{D}$ une partie B non vide de $\mathcal{P}(\{1,\dots,n\})$ telle que :*

1. $$\sum_{S\in B} p_S \in \mathcal{D}$$
2. *B est minimal pour cette propriété :*
$$\forall\ C \subseteq B,\ C \neq \emptyset \quad \sum_{S\in C} p_S \ \notin\ \mathcal{D}$$

Proposition 19.

1. *L'ensemble des blocs d'une digèbre $\mathcal{D}$ forme une partition de $\mathcal{P}(\{1,\dots,n\})$.*
2. *L'ensemble des polynômes $\varepsilon_B = \sum_{S\in B} \varepsilon_S$, ou B parcourt l'ensemble des blocs de $\mathcal{D}$, est une base de $\mathcal{D}$ comme $\mathbb{R}$-espace vectoriel.*
3. *L'ensemble des polynômes $p_B = \sum_{S\in B} p_S$, ou B parcourt l'ensemble des blocs de $\mathcal{D}$, est une base de $\mathcal{D}$ comme $\mathbb{R}$-espace vectoriel.*

Preuve :

1. Soient B_1 et B_2 deux blocs de $\mathcal{D}$. Alors $B_1 \cap B_2 = \emptyset$. En effet sinon, on a $\sum_{S\in B_1} \varepsilon_S \in \mathcal{D}$ et $\sum_{S\in B_2} \varepsilon_S \in \mathcal{D}$ car $\mathcal{D}$ est stable par ε. Donc d'après le Corollaire 6 p24 :
$$\left(\sum_{S\in B_1} \varepsilon_S\right)\left(\sum_{T\in B_2} \varepsilon_T\right) = \sum_{U\in B_1\cap B_2} \varepsilon_U$$
Comme $\mathcal{D}$ est stable par ε^{-1}, on a $\sum_{U\in B_1\cap B_2} p_U \in \mathcal{D}$, c'est à dire que B_1 et B_2 ne sont pas minimaux.
On remarque finalement que pour tout sous ensemble S de $\{1,\dots,n\}$, il existe un bloc de $\mathcal{D}$ qui contient S, d'après la Proposition 18 p24.
2. D'après la Proposition 5 p15 on sait qu'il existe une partition $P = (P_1,\dots,P_s)$ de $\mathcal{P}(\{1,\dots,n\})$ telle que
$$\mathcal{D} = \left\{p \ \in \mathcal{S}_n \quad t.q. \quad \forall P_i \in P \quad \forall (A,B) \in P_i^2 \quad p(A) = p(B)\right\}$$
Pour chacun des P_i, on pose $q_i = \sum_{B\in P_i} \varepsilon_B$. Alors d'après la Proposition 15 p23 on a :
$$\mathcal{D} = \{p \ \in \mathcal{S}_n \quad t.q. \quad \forall i\ \exists t_i \in \mathbb{R} \quad t.q. \quad p\cdot q_i = t_i q_i\}$$

En effet, d'après la Proposition 15 p23, pour tout polynôme p, on a $p \cdot q_i = \sum_{B \in P_i} p(B)\varepsilon_B$. On en déduit donc que p a la même valeur t_i sur tous les éléments du bloc P_i si et seulement si le polynôme $p \cdot q_i$ est un multiple du polynôme q_i, et plus précisément $t_i q_i$.

Comme $q_i^2 = q_i$ on a $q_i \in \mathcal{D}$. Il ne reste plus qu'à remarquer par évaluation que, pour tout polynôme p appartenant à $\mathcal{D}$, p s'écrit comme une combinaison linéaire réelle des polynômes q_i :

$$\sum_{i=1}^{s} p \cdot q_i = \sum_{i=1}^{s} p(B_i) q_i = p$$

Comme les ε_S sont indépendants (Proposition 12), et les P_i disjoints, les q_i sont indépendants. On remarque au passage que les P_i sont exactement les blocs de $\mathcal{D}$.

3. On vient de voir que l'ensemble des polynômes $\varepsilon_B = \sum_{S \in B} \varepsilon_S$, ou B parcours l'ensemble des blocs de $\mathcal{D}$, engendre $\mathcal{D}$ comme $\mathbb{R}$-espace vectoriel. Comme ε^{-1} est un isomorphisme qui stabilise $\mathcal{D}$, il envoie une base de $\mathcal{D}$ vers une base de $\mathcal{D}$.

□

Définition 10. *On parlera de* système de blocs *de $\mathcal{D}$ pour désigner l'ensemble des blocs de $\mathcal{D}$. De plus, si B est un bloc, on note $p_B = \sum_{A \in B} p_A$ et $\varepsilon_B = \sum_{A \in B} \varepsilon_A$.*

Proposition 20. *Si $\mathcal{D}_1$ et $\mathcal{D}_2$ sont deux digèbres telles que $\mathcal{D}_1 \subseteq \mathcal{D}_2$, alors les blocs de $\mathcal{D}_2$ sont contenus dans ceux de $\mathcal{D}_1$.*

Preuve : Si B est un bloc de $\mathcal{D}_1$, alors

$$\sum_{A \in B} p_A \in \mathcal{D}_1 \subseteq \mathcal{D}_2$$

Donc B est une réunion de blocs de $\mathcal{D}_2$. □

Corollaire 7. *Tous les sous-ensembles de $\{1, \ldots, n\}$ contenus dans un bloc B d'une digèbre $\mathcal{D}$ sont de même cardinalité.*

Preuve : D'après la Proposition 18 p24, si $\mathcal{D}$ est une digèbre, alors $\mathcal{D}$ contient la digèbre dont les blocs sont les :

$$\{A, \quad t.q.\ |A| = k\}, \quad k \in \{1 \ldots n\}$$

□

Exemple : Si A est un sous-ensemble de $\{1,\dots,n\}$, alors on va montrer que les blocs de la digèbre engendrée par le polynôme p_A sont les

$$B_{r,l} = \{U \subseteq \{1,\dots,n\}\ t.q.\ |U| = r\ et\ |A \cap U| = l\}$$

Pour tout $r \in \{1\dots,n\}$ et tout $l \in \{1,\dots|A|\}$,on pose $q_{r,l} = \sum_{S\in B_{r,l}} p_S$. Alors :

- $\complement(q_{r,l}) = q_{n-r,|A|-l}$
- $\partial(q_{r,l}) = (n - |A| - r + l + 1)\, q_{r-1,l} + (|A| - l + 1)\, q_{r-1,l-1}$
- $$q_{u,v} \cdot q_{r,l} = \sum_{\substack{i=1\dots n\\ j=1\dots|A|}} \binom{j}{v,l}\binom{i-j}{u-v, r-l} q_{i,j}$$

  où $\binom{j}{v,l}$ est le nombre de façons d'exprimer un ensemble à j éléments comme l'union d'un de ses sous-ensembles à v éléments et d'un de ses sous-ensembles à l éléments, c'est à dire :

$$\binom{j}{v,l} = \binom{j}{v}\binom{v}{j-l} = \binom{j}{l}\binom{l}{j-v}$$

Donc l'espace vectoriel engendré par les $q_{r,l}$ est une digèbre.

Réciproquement,

$$q_{l,l} = \sum_{U\in B_{l,l}} p_U = \sum_{\substack{U\subseteq A\\ |U|=l}} p_U = \frac{1}{(|A|-l)!}\partial^{|A|-l}(p_A)$$

d'après la Proposition 7 p17, donc $q_{l,l}$ appartient à la digèbre engendrée par p_A.

De la même façon,

$$q_{l,0} = \sum_{U\in B_{l,0}} p_U = \sum_{\substack{U\subseteq A^c\\ |U|=l}} p_U = \frac{1}{(|A|-l)!}\partial^{|A^c|-l}\complement(p_A)$$

appartient à la digèbre engendrée par p_A.

Il ne reste plus qu'à remarquer que

$$q_{r,l} = \sum_{U\in B_{r,l}} p_U = q_{l,l}\cdot q_{r-l,0} \quad \forall r \geq l$$

appartient à la digèbre engendrée par p_A.

Remarque 8. *La digèbre engendrée par p_A est l'algèbre des invariants du stabilisateur de A.*

1.2.4 Exemple emblématique

On a vu précédemment (1.1.3 p16) que le groupe des permutations $\mathfrak{S}_n$ de $\{1, \ldots, n\}$ agit de manière naturelle sur $\mathcal{S}_n$ comme un groupe d'isomorphismes d'algèbre définis par :

$$\sigma \cdot x_i = x_{\sigma(i)} \ , \ \sigma \ \in \ \mathfrak{S}_n$$

Proposition 21. *Les $\sigma \ \in \ \mathfrak{S}_n$ définis en 1.1.3 p16 sont des homomorphismes de digèbre, au sens où :*

1. *ce sont des homomorphismes d'algèbre de $\mathcal{S}_n$ dans $\mathcal{S}_n$.*
2. *on a $\sigma \circ \partial = \partial \circ \sigma$*
3. *et $\sigma \circ \mathsf{C} = \mathsf{C} \circ \sigma$*

Preuve :

1. Par définition de l'action de $\mathfrak{S}_n$ sur $\mathcal{S}_n$.
2.

$$\begin{aligned} \sigma \circ \partial(p_S) &= \sigma \left(\sum_{i \in S} \prod_{j \in S \setminus i} x_j \right) \\ &= \sum_{i \in S} \prod_{j \in S \setminus i} x_{\sigma(j)} \\ &= \partial \circ \sigma(p_S) \end{aligned}$$

3.

$$\begin{aligned} \sigma \circ \mathsf{C}(p_S) &= \sigma \left(\prod_{j \notin S} x_j \right) \\ &= \prod_{j \notin S} x_{\sigma(j)} \\ &= \mathsf{C} \circ \sigma(p_S) \end{aligned}$$

□

Proposition 22. *Tout homomorphisme de digèbre est soit nul, soit injectif.*

Preuve : Le noyau d'un homomorphisme de digèbre est soit réduit à $\{0\}$, soit une digèbre, auquel cas il contient $1 = p_\emptyset$ (d'après la Proposition 18 p24) et est en plus un idéal de $\mathcal{S}_n$, c'est donc tout $\mathcal{S}_n$. $\square$

Proposition 23. *Tout isomorphisme de digèbre est l'un des σ définis à la Proposition 21 p29.*

Preuve : Soit ϕ un isomorphisme de digèbre. On a alors

$$\phi(\varepsilon_S \varepsilon_T) = \phi(\varepsilon_S)\phi(\varepsilon_T) \ \forall S, T$$

donc si l'on pose $\phi(\varepsilon_S) = \sum_A \alpha_A^S \varepsilon_A$, on a : $\alpha_A^S \in \{0, 1\}$ et $\alpha_A^S \alpha_A^T = 0 \ \forall S \neq T$. Comme ϕ est un isomorphisme ϕ permute les ε_S, en effet si $\alpha_A^S \neq 0$ et $\alpha_B^S \neq 0$ avec $A \neq B$ alors on aurait $\alpha_A^T = 0$ et $\alpha_B^T = 0$ pour tout T différent de S, ce qui contredit le fait que ϕ est un isomorphisme. De la même façon ϕ permute les p_S car $\phi \circ \varepsilon = \varepsilon \circ \phi$. On doit de plus avoir $\phi(p_{S \cup T}) = \phi(p_S)\phi(p_T)$ donc $\phi(p_\emptyset) = p_\emptyset$. On a enfin

$$\partial \circ \phi \left(p_{\{x_i\}}\right) = \phi \circ \partial \left(p_{\{x_i\}}\right) = \phi(p_\emptyset) = p_\emptyset$$

Donc $\phi \left(p_{\{x_i\}}\right) = p_{\{x_k\}}$, pour un certain k. On a ainsi ϕ qui permute les x_i, et donc ϕ est l'un des σ ci-dessus. $\square$

Proposition 24. *L'ensemble des invariants de G est une digèbre notée $\mathcal{D}(G)$. Le système de blocs de cette digèbre est l'ensemble des orbites de l'action naturelle de G sur $\mathcal{P}(\{1, \ldots, n\})$.*

Preuve : Le fait que $\mathcal{D}(G)$ soit une digèbre résulte immédiatement de la Proposition 21 p29. $\square$

L'intérêt des digèbres réside dans la réciproque de cette proposition, c'est à dire :

Conjecture 3. *Si $\mathcal{D}$ est une digèbre, alors $\mathcal{D}$ est une algèbre d'invariants.*

1.3 Commutants

Dans cette partie, on développe des outils de calcul dans le but d'attaquer la conjecture ci-dessus.

1.3.1 Structures d'incidence

Dans cette section, on décrit les orbites de $\mathfrak{S}_n$ sur $\mathcal{P}(\{1,\ldots,n\})^k$, c'est à dire la façon dont le groupe des permutations d'un ensemble agit sur les k-uplets de ses sous-ensembles. Il est clair que, par exemple, pour que deux paires d'ensembles soient dans la même orbite, il faut que les cardinaux des ensembles correspondent deux à deux, mais aussi que les cardinaux des intersections correspondent. Ceci se généralise facilement de la façon suivante :

Définition 11. *On dit que deux éléments $S = (S_1, \ldots, S_k)$ et $T = (T_1, \ldots, T_k)$ de $\mathcal{P}(\{1,\ldots,n\})^k$ ont la même structure d'incidence si pour toute partie J de $\{1,\ldots,k\}$, on a :*

$$\left|\bigcap_{j\in J} S_j\right| = \left|\bigcap_{j\in J} T_j\right|$$

Cette relation partitionne $\mathcal{P}(\{1,\ldots,n\})^k$ en classes d'équivalence qu'on appelle structures d'incidence *de $\mathcal{P}(\{1,\ldots,n\})^k$.*

Alternativement, le terme structure d'incidence d'ordre k désignera la fonction μ de $\mathcal{P}(\{1,\ldots,k\})$ dans $\mathbb{N}$, telle que

$$\forall J, \quad \mu(J) = \left|\bigcap_{j\in J} S_j\right|$$

pour un représentant S de la structure d'incidence. Par convention, on pose $\mu(\emptyset) = n$. Ainsi on pourra dire que la structure d'incidence d'ordre 2 de (A_1, A_2) est

$$\mu : \begin{cases} \{1\} \mapsto |A_1| \\ \{2\} \mapsto |A_2| \\ \{1,2\} \mapsto |A_1 \cap A_2| \end{cases}$$

Si (A_1, A_2) appartient à la structure d'incidence μ, on note $(A_1, A_2) \vdash \mu$.

Proposition 25. *Les structures d'incidences d'ordre k sont les fonctions μ de $\mathcal{P}(\{1,\ldots,k\})$ dans $\mathbb{N}$ telles que :*

$$\forall J \subseteq \{1,\ldots,k\}, \sum_{\substack{L\subseteq\{1,\ldots,k\} \\ L\supseteq J}} (-1)^{|L|-|J|}\mu(L) \geq 0$$

Si de plus on note

$$\hat{\mu} \ : \ J \mapsto \sum_{\substack{L\subseteq\{1,\ldots,k\} \\ L\supseteq J}} (-1)^{|L|-|J|}\mu(L)$$

alors $\hat{\mu}(J)$ est le cardinal de $\bigcap_{j\in J} S_j \cap \bigcap_{i\notin J} S_i^c$ pour tout représentant S de la structure d'incidence μ d'ordre k, et pour toute sous-partie J de $\{1,\ldots,k\}$.

Preuve : Soit S un représentant d'une structure d'incidence d'ordre k, et posons pour toute partie J de $\{1,\ldots,k\}$, $f(J) = |\bigcap_{j\in J} S_j \cap \bigcap_{i\notin J} S_i^c|$. Alors il est clair que pour tout J,

$$\mu(J) = \sum_{J\subseteq L\subseteq\{1,\ldots,k\}} f(L)$$

Par inversion de Möbius, on obtient :

$$f(J) = \sum_{J\subseteq L\subseteq\{1,\ldots,k\}} (-1)^{|L|-|J|}\mu(L)$$

Comme $f(J)$ est toujours positif, on a nécessairement

$$\sum_{J\subseteq L\subseteq\{1,\ldots,k\}} (-1)^{|L|-|J|}\mu(L) \geq 0$$

pour toute structure d'incidence μ, et cette quantité représente bien le cardinal de l'ensemble mentionné. Réciproquement, si g est une fonction de $\mathcal{P}(\{1,\ldots,k\})$ dans $\mathbb{N}$ telle que :

$$\forall J \subseteq \{1,\ldots,k\}, h(J) = \sum_{J\subseteq L\subseteq\{1,\ldots,k\}} (-1)^{|L|-|J|} g(L) \geq 0$$

alors on peut trouver une famille de 2^k ensembles disjoints $A_J,\ J \subseteq \{1,\ldots,k\}$ telle que $|A_J| = h(J),\ \forall J$. En effet on a vu que $n = \mu(\emptyset) = \sum_L h(L)$. En posant $T_i = \bigcup_{i\in J\subseteq\{1,\ldots,k\}} A_J$ pour tout i, alors la famille T a la structure d'incidence μ ($T \vdash \mu$). □

Proposition 26. *Les structures d'incidence de $\mathcal{P}(\{1,\ldots,n\})^k$ sont les orbites de l'action naturelle de $\mathfrak{S}_n$ sur $\mathcal{P}(\{1,\ldots,n\})^k$.*

Preuve : Soient deux éléments $S = (S_1,\ldots,S_k)$ et $T = (T_1,\ldots,T_k)$ de $\mathcal{P}(\{1,\ldots,n\})^k$ ayant la même structure d'incidence. Alors

$$\left|\bigcap_{i=1}^{n} S_i\right| = \left|\bigcap_{i=1}^{n} T_i\right|$$

Supposons que $S_t = \bigcap_{i=1}^n S_i \neq \emptyset$: alors $T_t = \bigcap_{i=1}^n T_i \neq \emptyset$ et les deux éléments $S' = (S_t, S_1 \setminus S_t, \ldots, S_k \setminus S_t)$ et $T' = (T_t, T_1 \setminus T_t, \ldots, T_k \setminus T_t)$ de $\mathcal{P}(\{1, \ldots, n\})^{k+1}$ ont la même structure d'incidence.

Donc il suffit de prouver que quelque soit k, si deux éléments $S = (S_1, \ldots, S_k)$ et $T = (T_1, \ldots, T_k)$ de $\mathcal{P}(\{1, \ldots, n\})^k$ ont la même structure d'incidence avec $S_t = \emptyset$, alors il existe une permutation σ de $\mathfrak{S}_n$ telle que $\sigma(S_i) = T_i,\ i = 1 \ldots k$.

On appelle profondeur de $S = (S_1, \ldots, S_k)$ le nombre

$$p = min \left\{ r \geq 1 \, t.q. \, \forall J \subseteq \{1 \ldots k\} \, t.q. \, |J| = r, \, |\bigcap_{j \in J} S_j| = 0 \right\}$$

On procède pour tout k par récurrence sur p :

- Si $p = 1$ alors $S = T = (\emptyset, \ldots, \emptyset)$.
- Supposons le résultat vrai pour tout k et pour tout $p \leq f$, et soit $S = (S_1, \ldots, S_k)$ et $T = (T_1, \ldots, T_k)$ deux éléments de $\mathcal{P}(\{1, \ldots, n\})^k$ ayant la même structure d'incidence et une profondeur $f + 1$.
  On pose :

$$\tilde{S} = (S_i \cap S_j, 1 \leq i < j \leq k, S_i \setminus \bigcup_{\substack{j=1 \ldots k \\ j \neq i}} S_j, i = 1 \ldots k)$$

  et

$$\tilde{T} = (T_i \cap T_j, 1 \leq i < j \leq k, T_i \setminus \bigcup_{\substack{j=1 \ldots k \\ j \neq i}} T_j, i = 1 \ldots k)$$

  Alors $\tilde{S}$ et $\tilde{T}$ ont la même structure d'incidence et une profondeur f. Donc il existe une permutation σ de $\mathfrak{S}_n$ telle que $\sigma(\tilde{S}_u) = \tilde{T}_u, \forall u$. Il ne reste plus qu'à remarquer que $\sigma(S) = T$.

□

Proposition 27. *Il y a* $\binom{n+2^k-1}{2^k-1}$ *structures d'incidence d'ordre* k *sur* $\{1, \ldots, n\}$.

Preuve : On a vu dans la Proposition 25 p31 que les structures d'incidence sont en bijection avec les fonctions $\hat{\mu}$ de $\mathcal{P}(\{A, \ldots, k\})$ dans $\mathbb{N}$ telles que $\sum_{J \subseteq \{1, \ldots, k\}} \hat{\mu}(J) = n$ c'est à dire avec les compositions de n en 2^k entiers. Le nombre de compositions de n en l entiers est connu pour être $\binom{n+l-1}{l-1}$, ce qui clôt la preuve. □

1.3.2 Commutant

On a déjà défini quelques opérations supplémentaires sur les digèbres, par exemple l et ε, et remarqué qu'on pouvait s'en servir pour reformuler la définition de celles-ci. On s'attache dans cette section à définir la sous-algèbre d'endomorphismes de $\mathcal{S}_n$ engendrée par ∂ et $\complement$, qui se trouve, et ce n'est pas un hasard, être l'ensemble des applications qui commutent avec tous les éléments de $\mathfrak{S}_n$.

Définition 12. *On note Com($\mathfrak{S}_n$) l'ensemble des applications linéaires h de $\mathcal{S}_n$ dans $\mathcal{S}_n$ telles que*

$$\forall \sigma \in \mathfrak{S}_n,\ h \circ \sigma = \sigma \circ h$$

Définition 13. *Si A_1 et A_2 sont deux sous-ensembles de $\{1, \ldots, n\}$, on pose $E_{A_1 \to A_2}$ l'application linéaire de $\mathcal{S}_n$ dans lui même qui envoie p_{A_1} sur p_{A_2} et p_S sur 0 si $S \neq A_1$.*

La famille de fonctions ainsi définie forme une base de l'espace vectoriel $\mathcal{L}(\mathcal{S}_n)$ des applications linéaires de $\mathcal{S}_n$ dans lui même.

Proposition 28. *Les*

$$E_\mu = \sum_{(A_1, A_2) \vdash \mu} E_{A_1 \to A_2}$$

où μ parcours l'ensemble des structures d'incidences d'ordre 2, forment une base de Com($\mathfrak{S}_n$).

Preuve : Étant donné un couple (A_1, A_2) de sous ensembles de $\{1, \ldots, n\}$, et une permutation $\sigma \in \mathfrak{S}_n$, on remarque que $\sigma \circ E_{A_1 \to A_2} \circ \sigma^{-1} = E_{\sigma(A_1) \to \sigma(A_2)}$. Donc si

$$\sum_{(A_1, A_2)} \lambda_{(A_1, A_2)} E_{A_1 \to A_2}$$

est un élément de Com($\mathfrak{S}_n$), alors on a $\lambda_{(\sigma(A_1), \sigma(A_2))} = \lambda_{(A_1, A_2)}$ pour tout couple (A_1, A_2). D'après la Proposition 26 p32, l'ensemble des couples (C, D) tels qu'il existe un élément σ de $\mathfrak{S}_n$ tel que $\sigma(A_1) = C$ et $\sigma(A_2) = D$ est exactement la structure d'incidence de (A_1, A_2), ce qui montre la Proposition. □

Remarque 9. *Dans les calculs, on notera parfois $E_{k,l,r}$ l'application E_μ lorsque μ est d'ordre 2, et*

- $k = \mu(\{1\})$

- $l = \mu(\{2\})$
- $r = \mu(\{1,2\})$

On note $id = \complement \circ \complement$ l'identité de $\mathcal{S}_n$, et id_k l'application de $\mathcal{S}_n$ dans lui-même qui envoie p_S sur lui-même si $|S| = k$ et sur zéro sinon. Il est clair que toutes ces applications sont dans $\mathrm{Com}(\mathfrak{S}_n)$. De plus, d'après le Corollaire 7 p27, elles stabilisent toute digèbre.

Proposition 29. *$Com(\mathfrak{S}_n)$ est le plus petit sous-espace vectoriel (au sens de l'inclusion) de $\mathcal{L}(\mathcal{S}_n, \mathcal{S}_n)$ contenant ∂, $\complement$ et les id_k qui soit stable par $\circ$. De plus, si $\mathcal{D}$ est une digèbre, alors :*

$$Com(\mathfrak{S}_n)(\mathcal{D}) \subseteq \mathcal{D}$$

Preuve : Soit $\mathcal{H}$ l'espace engendré par ∂, $\complement$ et les id_k (par combinaisons linéaires et par $\circ$). Il est clair que $\mathcal{H} \subseteq \mathrm{Com}(\mathfrak{S}_n)$ car ce dernier contient ∂, $\complement$ et les id_k, et est stable par combinaisons linéaires et par $\circ$.

D'après la Proposition 28 p34, il s'agit de montrer que les applications E_μ sont dans $\mathcal{H}$. En effet les applications de $\mathcal{H}$ stabilisent toute digèbre $\mathcal{D}$.

D'après la Proposition 7 p17, on a :

$$\partial^l(p_S) = \begin{cases} 0 & si\ |S| < l \\ \sum\limits_{\substack{A \subseteq S \\ |A| = |S| - l}} l!\, p_A & si\ |S| \geq l \end{cases}$$

Donc $\partial^l \circ id_k = l!\, E_{k,k-l,k-l}$, c'est à dire que les $E_{k,s,s}$ où s est plus petit que k sont dans $\mathcal{H}$.

On a $A^c \cap B^c = (A \cup B)^c$, donc $\complement \circ E_{k,l,r} \circ \complement$ envoie un ensemble A de taille $n-k$ sur les ensembles B de taille $n-l$ tels que $r = |A^c \cap B^c| = |(A \cup B)^c| = n - |(A \cup B)| = n - |A| - |B| + |A \cap B|$ c'est à dire que $\complement \circ E_{k,l,r} \circ \complement = E_{n-k,n-l,n-k-l+r}$. Donc grâce à ce qui précède, les $E_{k,s,k}$ où s est plus grand que k sont dans $\mathcal{H}$.
Finalement, si r est plus petit que k et que l, on a :

$$E_{r,l,r} \circ E_{k,r,r} = \sum_{s \geq r} \binom{s}{r} E_{k,l,s}$$

Donc quels que soient k, l, et r, $E_{k,l,r} \in \mathcal{H}$ et $E_{k,l,r}$ stabilise toute digèbre $\mathcal{D}$. $\square$

On peut en fait obtenir mieux :

Proposition 30. *Com*$(\mathfrak{S}_n)$ *est le plus petit sous-espace vectoriel (au sens de l'inclusion) de* $\mathcal{L}(\mathcal{S}_n, \mathcal{S}_n)$ *contenant* ∂ *et* $\complement$ *qui soit stable par* $\circ$.

Preuve : Il s'agit de montrer que les $E_{k,l,r}$ peuvent être obtenus grâce à ∂ et $\complement$, au moyen de compositions et de combinaisons linéaires. On se propose de le démontrer par récurrence sur k, pour k variant de 0 à n.

- Si $k = 0$, alors $r = 0$, et on a

$$\partial^{n-l} \circ \complement \circ \partial^n \circ \complement = \frac{n!^2}{(n-l)!} E_{0,l,0}$$

- Supposons le résultat vrai pour tout k strictement inférieur à j. Alors pour tout u strictement inférieur à j, on sait engendrer les

$$E_{u,j,u} \circ \partial^{j-u} = \sum_{r=u}^{j} \binom{r}{u} E_{j,j,r}$$

  En particulier, pour $u = j - 1$, l'application

$$w = E_{j,j,j-1} + jE_{j,j,j} = E_{j,j,j-1} + jid_j$$

  On remarque que $w^2 = (n-2)E_{j,j,j-1} + j(n-j)id_j + 4E_{j,j,j-2}$.
  D'autre part, on sait aussi engendrer, dans le cas $u = j-2$, l'application $x = E_{j,j,j-2} + (j-1)E_{j,j,j-1} + \binom{j}{2} id_j$.
  Comme la matrice $\begin{bmatrix} 0 & 4 & 1 \\ 1 & n-2 & j-1 \\ j & j(n-j) & \frac{j(j-1)}{2} \end{bmatrix}$ est de déterminant j^2, on en conclut que l'on peut retrouver l'application id_j lorsque $j > 0$.
  Il ne reste plus qu'à remarquer pour conclure que

$$\complement \circ \partial^{l-r} \circ \complement \circ \partial^{j-r} \circ id_j = \sum_{s=r}^{\min(j,l)} \binom{s}{r} E_{j,l,s}$$

□

Com$(\mathfrak{S}_n)$ étant stable par transposition, il est légitime de chercher à appliquer la théorie des $*$-algèbres afin de profiter de sa semi-simplicité. Ceci est aussi l'occasion de revenir sur la définition des digèbres en montrant que

les trois opérateurs sont nécessaires : on a défini les digèbres à l'aide de trois opérations : $\partial, \complement$ et la multiplication. On se propose ici de montrer que chacune d'elle est nécessaire, c'est à dire que les deux autres ne suffisent pas à définir la structure de digèbre.

multiplication et ∂

On peut considérer les polynômes engendrés par p_A si A est un sous-ensemble strict de $S = \{1, \ldots, n\}$: ce sont les $\sum_{\substack{U \subseteq A \\ |U|=k}} p_U$, pour k variant de 0 à $|A|$.

multiplication et $\complement$

Comme contre exemples, on peut citer $\{p_\emptyset, p_S\}$ pour $S \geq 2$, ou encore $\{p_\emptyset, p_A, p_{A^c}, p_S\}$ pour un ensemble A de cardinal strictement compris entre 1 et $|S| \geq 3$, ou même généraliser ceci avec plusieurs ensembles : si $A_1, \ldots, A_r$ sont des sous-ensembles de S, alors les p_B où B est l'un des :

$$\left\{ \bigcap_{j \in J} A_j \cap \bigcap_{j \notin J} A_j^c, \quad J \subset S \right\}$$

forment une algèbre stable par $\complement$.

$\complement$ et ∂

On a vu que ∂ et $\complement$ engendrent $\mathrm{Com}\,(\mathfrak{S}_n)$ en tant que sous-algèbre de $\mathcal{L}\,(\mathcal{S}_n)$. $\mathrm{Com}\,(\mathfrak{S}_n)$ est stable par transposition (dans la base formée des p_S par exemple), c'est donc une *-algèbre, et on a les deux propriétés suivantes :

- Tout sous-espace stable par ∂ et $\complement$ admet un supplémentaire stable : son orthogonal. Autrement dit $\mathrm{Com}\,(\mathfrak{S}_n)$ est semi-simple.
- $\mathrm{Com}\,(\mathfrak{S}_n)$ est égal à son bicommutant, autrement dit toute application linéaire qui commute avec ∂ et $\complement$ appartient à la sous-algèbre de $\mathcal{L}\,(\mathcal{S}_n)$ engendrée par les permutations de $\mathfrak{S}_n$. On peut peut-être avoir ceci en considérant que l'algèbre de groupe est semi-simple.

Il est donc envisageable de décomposer $\mathcal{S}_n$ en sous-espaces vectoriels stables par ∂ et $\complement$. Cette décomposition n'est en rien unique, on exhibe ici une décomposition qui n'est pas totale.

Pour tout entier k compris entre 0 et n, on pose :

$$\mathcal{V}_k = \bigcap_{i,j} \ker E_{i,k,j}$$

Proposition 31. *On a alors :*

- *si* $k \geq \frac{n}{2}$, *alors* $\mathcal{V}_k = \mathcal{V}_{n-k}$
- *si* $k \leq l \leq \frac{n}{2}$, *alors* $\mathcal{V}_l \subsetneq \mathcal{V}_k$

Preuve :

- On a $\complement \circ E_{i,k,j} = E_{i,n-k,i-j}$, de plus $\complement$ est inversible, donc $E_{i,k,j}(p) = 0$ si et seulement si $E_{i,n-k,i-j}(p) = 0$.
- $E_{l,k,k} \circ E_{i,l,v} = \sum_{u=\max(0,i+l-n)}^{v} \binom{i-u}{v-u}\binom{n-i-k+u}{l-k-v+u} E_{i,k,u}$, donc on obtient facilement les $E_{i,k,j}$ en fonction des $E_{l,k,k} \circ E_{i,l,v}$ par un système triangulaire, pourvu que $l < n - i$. Si $l < i$, alors les $E_{n-i,k,j}$ s'expriment en fonction des $E_{l,k,k} \circ E_{n-i,l,v}$, donc on peut conclure en considérant que $E_{i,k,j} = E_{n-i,k,j} \circ \complement$. Finalement, si $l > n - i$ et $l > i$, alors $l > n/2$.

$\square$

On remarque aussi que l'orthogonal $\mathcal{V}_0^{\perp}$ de $\mathcal{V}_0$ est $\mathcal{S}_n^{\mathfrak{S}_n}$, l'algèbre des invariants du groupe symétrique. En effet pour tout polynôme p de $\mathcal{S}_n$, et tout entier k compris entre 0 et n, on a $E_{k,0,0}(p) = \langle p_k, p\rangle\ p_{\emptyset}$, avec $p_k = \sum_{U\ t.q.\ |U|=k} p_U$.

On peut donc établir une décomposition stable de $\mathcal{S}_n$:

$$\mathcal{S}_n = \mathcal{S}_n^{\mathfrak{S}_n} \oplus \bigoplus_{k=0}^{\frac{n}{2}-1} \mathcal{W}_k, \quad \text{avec } \mathcal{W}_k = \mathcal{V}_{k+1} \setminus \mathcal{V}_k$$

Il est clair que $\mathcal{S}_n^{\mathfrak{S}_n}$ est irréductible pour $\mathrm{Com}\,(\mathfrak{S}_n)$, en effet quel que soit p vecteur non nul de $\mathcal{S}_n^{\mathfrak{S}_n}$, $\mathrm{Com}\,(\mathfrak{S}_n) \cdot p = \mathcal{S}_n^{\mathfrak{S}_n}$.

Il n'en est pas de même pour les $\mathcal{V}_k$, par exemple si l'on considère la digèbre $\mathcal{D}_3$ d'ordre 3 qui est l'algèbre des invariants pour une transposition, on obtient :

$$\mathcal{D}_3 = \mathcal{S}_3^{\mathfrak{S}_3} \oplus < p_{\{1\}} + p_{\{2\}} - 2p_{\{3\}}, p_{\{1,2\}} + p_{\{2,3\}} - 2p_{\{1,2\}} >$$

Ainsi, $\mathcal{D}_3$ se décompose en deux sous espaces simple pour $\mathrm{Com}\,(\mathfrak{S}_n)$, dont le deuxième est inclus strictement dans $\mathcal{W}_1$.

On voit donc que les $\mathcal{W}_k$ sont des espaces stables par $\complement$ et ∂, mais pas par multiplication. Finalement, il est clair que la décomposition partielle ci-

dessus vaut pour toutes les digèbres $\mathcal{D}$, c'est à dire que :

$$\mathcal{D} = \mathcal{S}_n^{\mathfrak{S}_n} \oplus \bigoplus_{k=0}^{\frac{n}{2}-1} (\mathcal{W}_k \cap \mathcal{D})$$

Remarque 10. *Cette décomposition des digèbres en somme directe de noyaux est très librement inspirée des travaux autour du théorème de Livingstone et Wagner ([10]), entre autres le travail de Maurice Pouzet [17] (voir aussi [21]).*

1.3.3 Commutants d'ordres supérieurs

Il s'agit dans cette section de prendre en compte la multiplication, qui est un opérateur binaire sur $\mathcal{S}_n$, comme on l'a fait pour ∂ et $\complement$ dans la section précédente. On remarque là encore, que la multiplication a de bonnes propriétés par rapport aux éléments de $\mathfrak{S}_n$, et le principal résultat de cette section est la Proposition 33 p40, qui donne un nouveau résultat de génération par ∂, $\complement$, et la multiplication. Il s'agit ici d'une attaque de la conjecture 3 p30 à travers une version qui met en jeu les applications qui commutent avec les éléments de $\mathfrak{S}_n$, cette démarche sera détaillée dans la prochaine section.

Étant donné un entier strictement positif k, on considère

$$\mathcal{S}_n^{\otimes k} = \underbrace{\mathcal{S}_n \otimes \ldots \otimes \mathcal{S}_n}_{k}$$

le produit tensoriel de k copies de $\mathcal{S}_n$.

C'est un $\mathbb{R}$-espace vectoriel de dimension 2^{kn} dont une base est formée par les

$$p_S = p_{S_1} \otimes \ldots \otimes p_{S_k}, \text{ où } S \in \mathcal{P}(\{1, \ldots, n\})^k$$

Étant donné deux entiers positifs k et l, on peut définir l'ensemble $\mathcal{L}\left(\mathcal{S}_n^{\otimes k}, \mathcal{S}_n^{\otimes l}\right)$ des applications linéaires de $\mathcal{S}_n^{\otimes k}$ dans $\mathcal{S}_n^{\otimes l}$, qui est un espace vectoriel, et à l'intérieur de ce dernier $\mathrm{Com}_k^l(\mathfrak{S}_n)$ le sous-espace vectoriel des applications linéaires h de $\mathcal{S}_n^{\otimes k}$ dans $\mathcal{S}_n^{\otimes l}$ telles que

$$\forall \sigma \in \mathfrak{S}_n,\ (\underbrace{\sigma \otimes \sigma \otimes \ldots \otimes \sigma}_{l}) \circ h = h \circ (\underbrace{\sigma \otimes \sigma \otimes \ldots \otimes \sigma}_{k})$$

Définition 14. *On pose $E_{(A_1\ldots,A_k)\to(B_1,\ldots,B_l)}$ l'application linéaire de $\mathcal{S}_n^{\otimes k}$ dans $\mathcal{S}_n^{\otimes l}$ qui envoie $p_{A_1}\otimes\ldots\otimes p_{A_k}$ sur $p_{B_1}\otimes\ldots\otimes p_{B_l}$ et $p_{S_1}\otimes\ldots\otimes p_{S_k}$ sur 0 si $S\neq A$.*

La famille ainsi définie forme une base de l'espace vectoriel $\mathcal{L}\left(\mathcal{S}_n^{\otimes k},\mathcal{S}_n^{\otimes l}\right)$ des applications linéaires de $\mathcal{S}_n^{\otimes k}$ dans $\mathcal{S}_n^{\otimes l}$.

Proposition 32. *Les*

$$E_\mu=\sum_{(A_1,\ldots,A_k,B_1,\ldots,B_l)\vdash\mu}E_{(A_1\ldots,A_k)\to(B_1,\ldots,B_l)}$$

où μ parcourt l'ensemble des structures d'incidence d'ordre $k+l$, forment une base de $Com_k^l(\mathfrak{S}_n)$.

Preuve : de la même façon que pour la Proposition 28 p34, étant donné un k-uplet A et un l-uplet B de sous ensembles de $\{1,\ldots,n\}$, on remarque que $\sigma\circ E_{A\to B}\circ\sigma^{-1}=E_{\sigma(A)\to\sigma(B)}$. Donc si $\sum_{(A,B)}\ \lambda_{(A,B)}E_{A\to B}$ est un élément de $\mathrm{Com}(\mathfrak{S}_n)$, alors on a $\lambda_{(\sigma(A),\sigma(B))}=\lambda_{(A,B)}$ pour tout couple (A,B). D'après la Proposition 26 p32, l'ensemble des couples (C,D) tels qu'il existe un élément σ de $\mathfrak{S}_n$ tel que $\sigma(A)=C$ et $\sigma(B)=D$ est exactement la structure d'incidence de (A,B), ce qui montre la Proposition. □

La section précédente décrit donc $\mathrm{Com}_1^1(\mathfrak{S}_n)=\mathrm{Com}(\mathfrak{S}_n)$ et montre que ce dernier est engendré par ∂, $\complement$, et les id_k.

$\mathbf{Com}_2^1(\mathfrak{S}_n)$ et $\mathbf{Com}_1^2(\mathfrak{S}_n)$

Définition 15. *On note m la multiplication de $\mathcal{S}_n$. Il est clair que c'est un élément de $Com_2^1(\mathfrak{S}_n)$.*

De plus, quelque soit h une application de $\mathrm{Com}_2^1(\mathfrak{S}_n)$ et j,k,l trois applications de $\mathrm{Com}(\mathfrak{S}_n)$ il est clair que $j\circ h\circ(k\otimes l)$ est aussi une application de $\mathrm{Com}_2^1(\mathfrak{S}_n)$.

Proposition 33. *$Com_2^1(\mathfrak{S}_n)$ est le sous-espace vectoriel de $\mathcal{L}\left(\mathcal{S}_n^{\otimes k},\mathcal{S}_n^{\otimes l}\right)$ engendré par les*

$$j\circ m\circ(k\otimes l),\quad \text{avec } j,k,l\ \in Com(\mathfrak{S}_n)$$

Preuve : On peut considérer que j, k, et l sont des applications du type

$$e_{k,l,r} : \begin{cases} \varepsilon_S \mapsto \sum\limits_{\substack{T \ t.q. \\ |T|=l \\ |T\cap S|=r}} \varepsilon_T \text{ si } |S| = k \\ \varepsilon_S \mapsto 0 \text{ sinon.} \end{cases}$$

on a alors :

$$e_{k,a_3,r_3} \circ m \circ (e_{a_1,k,r_1} \otimes e_{a_2,k,r_2}) (\varepsilon_{A_1} \otimes \varepsilon_{A_2}) = \sum_{A_3} Z^{a_1,a_2,a_3}_{k,r_1,r_2,r_3} (A_1, A_2, A_3) \, \varepsilon_{A_3}$$

où

$$Z^{a_1,a_2,a_3}_{k,r_1,r_2,r_3} (A_1, A_2, A_3) = \begin{cases} 0 \text{ si } |A_i| \neq a_i \text{ pour l'un des } i = 1,2,3 \\ |\{U \in \{1,\ldots,n\} \ t.q. \ |U| = k, |U \cap A_i| = r_i, i = 1,2,3\}| \text{ sinon} \end{cases}$$

Il s'agit donc de montrer que la fonction indicatrice d'une structure d'incidence quelconque s'exprime comme une combinaison linéaire des Z.

Soit U tel que :

$$\begin{array}{lcl} |U| & = & k \\ |U \cap A_1| & = & r_1 \\ |U \cap A_2| & = & r_2 \\ |U \cap A_3| & = & r_3 \end{array}$$

On a alors :

$$\begin{array}{lcl} r_1 + r_2 - k & \leq & |U \cap A_1 \cap A_2| \\ r_1 + r_3 - k & \leq & |U \cap A_1 \cap A_3| \\ r_2 + r_3 - k & \leq & |U \cap A_2 \cap A_3| \\ r_1 + r_2 + r_3 - k & \leq & |U \cap A_1 \cap A_2 \cap A_3^c| + |U \cap A_1 \cap A_2^c \cap A_3| \\ & & +|U \cap A_1^c \cap A_2 \cap A_3| + 2|U \cap A_1 \cap A_2 \cap A_3| \end{array}$$

On a donc $Z^{a_1,a_2,a_3}_{k,r_1,r_2,r_3} (A_1, A_2, A_3) \neq 0$ seulement si :

$$\begin{array}{lcl} r_1 + r_2 - k & \leq & |A_1 \cap A_2| \\ r_1 + r_3 - k & \leq & |A_1 \cap A_3| \\ r_2 + r_3 - k & \leq & |A_2 \cap A_3| \\ r_1 + r_2 + r_3 - k & \leq & |A_1 \cap A_2 \cap A_3^c| + |A_1 \cap A_2^c \cap A_3| \\ & & +|A_1^c \cap A_2 \cap A_3| + 2|A_1 \cap A_2 \cap A_3| \end{array}$$

De plus, le cas d'égalité est valide, c'est à dire que si (A_1, A_2, A_3) sont trois ensembles de cardinaux respectifs a_1, a_2, et a_3 tels que :

$$\begin{array}{lcl} r_1 + r_2 - k & = & |A_1 \cap A_2| \\ r_1 + r_3 - k & = & |A_1 \cap A_3| \\ r_2 + r_3 - k & = & |A_2 \cap A_3| \\ r_1 + r_2 + r_3 - k & = & |A_1 \cap A_2 \cap A_3^c| + |A_1 \cap A_2^c \cap A_3| \\ & & +|A_1^c \cap A_2 \cap A_3| + 2|A_1 \cap A_2 \cap A_3| \end{array}$$

alors on a $Z_{k,r_1,r_2,r_3}^{a_1,a_2,a_3}(A_1, A_2, A_3) \neq 0$.

En effet si on pose $V = (A_1 \cap A_2) \cup (A_2 \cap A_3) \cup (A_1 \cap A_3)$, alors :

$$|V| = 2(r_1 + r_2 + r_3 - k) - (r_1 + r_2 - k) - (r_1 + r_3 - k) - (r_2 + r_3 - k) = k$$
$$|V \cap A_1| = (r_1 + r_2 + r_3 - k) - (r_2 + r_3 - k) = r_1$$
$$|V \cap A_2| = (r_1 + r_2 + r_3 - k) - (r_1 + r_3 - k) = r_2$$
$$|V \cap A_3| = (r_1 + r_2 + r_3 - k) - (r_1 + r_2 - k) = r_3$$

Donc en ordonnant les structures d'incidence d'ordre 3 telles que $|A_1| = a_1, |A_2| = a_2, |A_3| = a_3$, et les fonctions $Z_{k,r_1,r_2,r_3}^{a_1,a_2,a_3}$ dans un ordre convenable, on obtient un système triangulaire bien défini qui donne les indicatrices recherchées. □

Corollaire 8. *Pour toute digèbre $\mathcal{D}$:*

$$Com_2^1(\mathfrak{S}_n)\,(\mathcal{D} \otimes \mathcal{D}) = \mathcal{D}$$

Preuve : D'après ce qui précède, $\mathrm{Com}_2^1(\mathfrak{S}_n)\,(\mathcal{D} \otimes \mathcal{D}) \subseteq \mathcal{D}$. Pour l'inclusion dans l'autre sens, il suffit de remarquer que pour tout bloc B de $\mathcal{D}$, on a $m(\varepsilon_B \otimes \varepsilon_B) = \varepsilon_B$.

□

Le cas de $\mathrm{Com}_1^2(\mathfrak{S}_n)$ est entièrement symétrique, et on montrera ainsi facilement que ce dernier est l'espace vectoriel engendré par les

$$(k \otimes l) \circ \Delta \circ j, \quad \text{avec } j, k, l \ \in \mathrm{Com}(\mathfrak{S}_n)$$

où Δ est l'application symétrique de m, c'est à dire l'application qui envoie ε_S sur $\varepsilon_S \otimes \varepsilon_S$ pour toute partie S de $\{1, \ldots, n\}$.

$\mathbf{Com}_2^2(\mathfrak{S}_n)$, $\mathbf{Com}_3^1(\mathfrak{S}_n)$, et $\mathbf{Com}_1^3(\mathfrak{S}_n)$

On pourrait imaginer obtenir ces trois espaces vectoriels de fonctions de façon naturelle à partir de la dérivation, de la complémentation, et de la multiplication grâce au trois espaces suivants :

- Le sous-espace vectoriel $\mathcal{H}_2^2$ de $\mathrm{Com}_2^2(\mathfrak{S}_n)$ engendré par les composées d'une fonction de $\mathrm{Com}_2^1(\mathfrak{S}_n)$ puis d'une fonction de $\mathrm{Com}_1^2(\mathfrak{S}_n)$.
- Le sous-espace vectoriel $\mathcal{H}_3^1$ de $\mathrm{Com}_3^1(\mathfrak{S}_n)$ engendré par les composées d'une fonction de $id \otimes \mathrm{Com}_2^1(\mathfrak{S}_n)$ puis d'une fonction de $\mathrm{Com}_2^1(\mathfrak{S}_n)$.
- Le sous-espace vectoriel $\mathcal{H}_1^3$ de $\mathrm{Com}_1^3(\mathfrak{S}_n)$ engendré par les composées d'une fonction de $\mathrm{Com}_1^2(\mathfrak{S}_n)$ puis d'une fonction de $id \otimes \mathrm{Com}_1^2(\mathfrak{S}_n)$.

Les égalités d'un de ces espaces avec son commutant associé sont équivalentes, cela ne fait que traduire le fait que certaines fonctions engendrent $\mathrm{Com}_4^0(\mathfrak{S}_n)$. La Proposition suivante montre que c'est faux en général :

Proposition 34. *Si $n \geq 20$, $\mathcal{H}_2^2$ est strictement inclus dans $Com_2^2(\mathfrak{S}_n)$.*

Preuve : L'identité de $\mathcal{S}_n \otimes \mathcal{S}_n$ est bien une application de $\mathrm{Com}_2^2(\mathfrak{S}_n)$, mais elle n'est pas incluse dans $\mathcal{H}_2^2$. En effet si l'on pose $id = \sum_t h_t l_t$ avec pour tout t, $h_t \in \mathrm{Com}_1^2(\mathfrak{S}_n)$ et $l_t \in \mathrm{Com}_2^1(\mathfrak{S}_n)$, alors pour tout couple d'ensembles B_1 et B_2 :

$$p_{B_1} \otimes p_{B_2} = \sum_t h_t \circ l_t \left(p_{B_1} \otimes p_{B_2}\right)$$

autrement dit pour tout couple B_1, B_2, il existe des éléments x_t de $\mathcal{S}_n$, et des fonctions h_t de $\mathrm{Com}_1^2(\mathfrak{S}_n)$, telles que

$$p_{B_1} \otimes p_{B_2} = \sum_t h_t \left(x_t\right)$$

Ceci est impossible, en effet $\mathcal{S}_n$ est, on l'a vu, de dimension 2^n et $\mathrm{Com}_1^2(\mathfrak{S}_n)$ a pour dimension le nombre de structures d'incidence d'ordre 3 (d'après la Proposition 32 p40), c'est à dire $\binom{n+7}{7}$ d'après la Proposition 27 p33. On en déduit que l'image de $\mathcal{S}_n$ par $\mathrm{Com}_1^2(\mathfrak{S}_n)$ est de dimension inférieure ou égale à $\binom{n+7}{7}2^n$, ce qui est strictement inférieur à la dimension de $\mathcal{S}_n \times \mathcal{S}_n$ (i.e. 4^n)

si n est supérieur ou égal à 20, en effet dans ce cas :

$$\begin{aligned}
\ln\left(\frac{\binom{n+7}{7}}{2^n}\right) &= \sum_{i=1}^{7}\ln(n+i) - n\ln(2) - \ln(7!) \\
&= \sum_{i=1}^{7}\ln(20+i) + \sum_{i=1}^{7}\ln\left(1+\frac{n-20}{20+i}\right) - n\ln(2) - \ln(7!) \\
&\leq \sum_{i=1}^{7}\ln(20+i) + \sum_{i=1}^{7}\frac{n-20}{20+i} - (n-20)\ln(2) - 20\ln(2) - \ln(7!) \\
&\leq (n-20)\underbrace{\left(\sum_{i=1}^{7}\frac{1}{20+i} - \ln(2)\right)}_{<0} + \underbrace{\sum_{i=1}^{7}\ln(20+i) - 20\ln(2) - \ln(7!)}_{<0}
\end{aligned}$$

□

1.3.4 Une conjecture équivalente sur les commutants

On a vu que les $\mathrm{Com}_k^l(\mathfrak{S}_n)$ sont partie prenante de la structure de digèbre, en effet les trois opérations de dérivation, complémentation, et multiplication engendrent notamment Com_1^1 et Com_2^1, mais pas les commutants d'ordre supérieur. On se doute bien que cette idée de génération est au coeur de la Conjecture 3 p30, on peut en fait la reformuler totalement en terme de commutants :

Conjecture 4. *Si $\mathcal{D}$ est une digèbre, alors pour tout entier k supérieur ou égal à 1 :*

$$Com_k(\mathfrak{S}_n)(\mathcal{D}^{\otimes k}) \subseteq \mathcal{D}$$

Proposition 35. *Les Conjectures 3 p30 et 4 p44 sont équivalentes.*

Remarque 11. *L'étude de la section précédente montre que la propriété de la Conjecture 4 p44 est vraie si $k = 1$ ou $k = 2$.*

Preuve : Il est clair que la Conjecture 3 p30 implique la Conjecture 4 p44.

Il s'agit donc de prouver que si pour tout entier k supérieur ou égal à 1

$$\mathrm{Com}_k(\mathfrak{S}_n)(\mathcal{D}^{\otimes k}) \subseteq \mathcal{D}$$

alors $\mathcal{D}$ est une algèbre d'invariants.

Soient C et D deux parties de $\{1, \ldots, n\}$. On veut montrer que l'une des deux conditions suivantes est vérifiée :

- C et D ne sont pas dans un même bloc de $\mathcal{D}$
- il existe $\sigma \in \mathfrak{S}_n$ tel que $\sigma(C) = D$ et σ stabilise tous les blocs de $\mathcal{D}$.

Soit $A_i, i \in \{1, \ldots, 2^n\}$ la famille des sous-ensembles de $\{1, \ldots, n\}$, pour tout i, B_i le bloc de $\mathcal{D}$ qui contient A_i, et r l'entier tel que $A_r = C$. On pose

$$P = \bigotimes_{i=1}^{2^n} A_i \ \in \mathcal{S}_n^{\otimes 2^n}$$

On définit ensuite c l'application de $\mathcal{S}^{\otimes 2^n}$ dans $\mathcal{S}_n$ qui à $p_{A_1} \otimes \ldots \otimes p_{A_{2^n}}$ associe p_{A_r} si $(A_1, \ldots, A_{2^n})$ à la même structure d'incidence que P, et 0 sinon. Il est clair que cette application est un élément de $\mathrm{Com}^1_{2^n}(\mathfrak{S}_n)$.

Donc si la Conjecture 4 p44 est vraie, $c\,(p_{B_1} \otimes \ldots \otimes p_{B_{2^n}})$ est un élément de $\mathcal{D}$. De plus :

$$c\left(\sum_{S_i \in B_i} p_{S_1} \otimes \ldots \otimes p_{S_k}\right) = p_C + \ldots$$

Comme ceci est contenu dans $\mathcal{D}$, le deuxième membre contient p_D.

On en déduit qu'il existe une famille $C_i, i \in \{1 \ldots 2^n\}$ de sous-ensembles de $\{1, \ldots, n\}$ telle que

- les familles A et C ont la même structure d'incidence,
- quel que soit i, les ensembles A_i et C_i sont dans un même bloc de $\mathcal{D}$,
- $C_r = D$.

Finalement, le passage de A à C est une permutation de $\{1, \ldots, n\}$, car on a vu que les structures d'incidence sont les orbites de l'action naturelle de $\mathfrak{S}_n$ (Proposition 26 p32). □

Au vu de la preuve, on ne se sert que du cas $k = 2^n$, c'est à dire du fait que si $\mathcal{D}$ est une digèbre, alors :

$$\mathrm{Com}_{2^n}(\mathfrak{S}_n)(\mathcal{D}^{\otimes 2^n}) \subseteq \mathcal{D}$$

Il est clair que ceci implique la même propriété pour les k plus petits, en effet on peut toujours "oublier" un argument, c'est à dire sommer sur tous les paramètres le concernant. En revanche on peut se demander ce qui se passe lorsque k est plus grand que 2^n : il est clair que $\mathcal{D}$ est alors une digèbre, mais est-il possible de "rebâtir" $\mathrm{Com}_k(\mathfrak{S}_n)$ $(k > 2^n)$ à partir de $\mathrm{Com}_{2^n}(\mathfrak{S}_n)$?

En fait, $\mathrm{Com}_k(\mathfrak{S}_n)$ n'existe pas vraiment si $k > 2^n$, car d'une certaine façon il y a au plus 2^n arguments distincts : on sait qu'une base de $\mathrm{Com}^k(\mathfrak{S}_n)$ est indexée par les structures d'incidence de taille $k+1$. Pour toute structure d'incidence μ d'ordre 2^n sur $\{1, \ldots, n\}$, et tout représentant $(S_1, \ldots, S_k)$ de μ, il existe des sous-ensembles $A_1, \ldots, A_r$ de $\{1, \ldots, k\}$ tels que $\forall i, j \in A_k,\ S_i = S_j$. Il est facile de voir que les $A_1, \ldots, A_r$ sont indépendants du représentant de μ choisi. On peut donc engendrer $\mathrm{Com}_k(\mathfrak{S}_n)$ avec $\mathrm{Com}_{2^n}(\mathfrak{S}_n)$ et quelques multiplications.

Chapitre 2

Coefficients des digèbres, Relations polynomiales

Dans toute cette partie, on utiliseras la notation Ω pour désigner l'ensemble $\{1, \ldots, n\}$. On notera $|A|$ le nombre d'éléments de A si A est un sous-ensemble de Ω, ou le nombre d'éléments d'un de ses représentants si A est un bloc d'une digèbre $\mathcal{D}$. Le nombre de sous-ensembles de Ω formant le bloc A sera quant à lui noté $\sharp A$.

2.1 Coefficients des digèbres

On a vu que chaque digèbre est munie d'un système de blocs, qui en supposant que la Conjecture 3 p30 soit vraie, représente les orbites de son groupe d'automorphismes sur $\mathcal{P}(\Omega)$. Il existe une notion d'incidence entre ces blocs, qui transmet la notion d'inclusion dans $\mathcal{S}_n$ au quotient que représente une digèbre, plus précisément :

Proposition 36. *Si B_1 et B_2 sont deux blocs d'une digèbre $\mathcal{D}$, et A un élément de B_1 donné, alors le nombre d'éléments de B_2 qui sont inclus dans A est indépendant du représentant A choisi. On note $\binom{B_1}{B_2}_{\mathcal{D}}$ ce nombre, ou plus simplement $\binom{B_1}{B_2}$ lorsque le contexte indique clairement dans quelle digèbre on se trouve.*

Remarque 12. *Jusqu'ici, on a noté $\binom{n}{k}$ le coefficient binomial qui représente le nombre de façons de choisir k éléments dans un ensemble à n éléments. La*

similarité des notations est voulue, en effet les deux interprétations coïncident dans la digèbre des invariants du groupe symétrique $\mathcal{S}_n^{\mathfrak{S}_n}$ dont les blocs (c'est à dire les orbites) sont constitués par les ensembles de même cardinalité, et où par conséquent un nombre suffit pour décrire un bloc.

Preuve : Soient B_1 et B_2 deux blocs d'une digèbre $\mathcal{D}$, de cardinalités respectives k_1 et k_2 avec $k_2 \leq k_1$. Considérons l'application E, de $\mathcal{S}_n$ dans lui-même, qui envoie pour tout sous-ensemble S de Ω, p_S sur $\sum_{A \ t.q. \ S \subseteq A} p_A$. Cette application est un élément de $\mathrm{Com}\,(\mathfrak{S}_n)$, donc on a $E(p_{B_2}) \in \mathcal{D}$, et donc quel que soit l'élément A du bloc B_1, le nombre d'éléments de B_2 qui sont inclus dans A est indépendant du représentant A choisi. □

Proposition 37. *Soit $(B_1, \ldots, B_k)$ une liste des blocs d'une digèbre $\mathcal{D}$, et $\mathcal{M}$ la matrice $k \times k$ dont le coefficient (i, j) est $\binom{B_i}{B_j}$. Alors $\mathcal{M}$ est la matrice de $\complement \circ l \circ \complement$ (voir la définition 6 p20 pour l) dans la base $(p_{B_1}, \ldots, p_{B_k})$.*

Preuve : On a vu à la Proposition 8 p20 que pour tout S contenu dans Ω, on a :

$$l(p_S) = \sum_{A \subseteq S} p_A$$

donc :

$$\complement \circ l \circ \complement(p_S) = \sum_{A \ t.q. \ S \subseteq A} p_A$$

On en déduit donc que si B_j est un bloc de $\mathcal{D}$,

$$\complement \circ l \circ \complement\left(p_{B_j}\right) = \sum_{S \in B_j} \sum_{A \ t.q. \ S \subseteq A} p_A = \sum_{i=1}^{k} \binom{B_i}{B_j} p_{B_i}$$

□

Pour toute digèbre $\mathcal{D}$ sur n éléments, on peut ordonner ses s blocs par cardinalité croissante, de façon à ce que le bloc en position i soit le complémentaire du bloc en position s-i. Dans la base de $\mathcal{D}$ ainsi formée, la matrice de $\complement$ s'exprime très simplement comme une antidiagonale de 1, et la matrice de $\complement \circ l \circ \complement$ examinée ci-dessus est triangulaire inférieure, avec des 1 sur la diagonale. Ce genre de base n'est évidemment pas unique en général, mais reste fort sympathique. En effet si on suppose donné la matrice de $\complement \circ l \circ \complement$ dans une telle base, alors on dispose évidement de la matrice de $\complement$, et par conséquent de toutes les

matrices des applications de $\mathrm{Com}\,(\mathfrak{S}_n)$ que l'on peut obtenir par composition comme on a vu à la Proposition 29 p35. De plus, la multiplication des blocs est facilement accessible, en effet :

Proposition 38. *Si $(B_1, \ldots, B_s)$ sont les blocs d'une digèbre $\mathcal{D}$, alors pour tout i, j, on a :*

$$p_{B_i} \cdot p_{B_j} = \sum_{k=1}^{s} \binom{B_k}{B_i, B_j} p_{B_k}$$

avec

$$\binom{B_k}{B_i, B_j} = \sum_{l=1}^{s} (-1)^{|B_k|-|B_l|} \binom{B_k}{B_l} \binom{B_l}{B_i} \binom{B_l}{B_j}$$

Preuve : D'après la Proposition 17 p24 on a :

$$p_{B_i} = \sum_A \binom{A}{B_i} \varepsilon_A \quad p_{B_j} = \sum_A \binom{A}{B_j} \varepsilon_A$$

Donc

$$p_{B_i} p_{B_j} = \sum_A \binom{A}{B_i} \binom{A}{B_j} \varepsilon_A$$

Comme de plus

$$\varepsilon_A = \sum_B (-1)^{|B|-|A|} \binom{B}{A} p_B$$

On a

$$p_{B_i} p_{B_j} = \sum_B \left(\sum_A (-1)^{|B|-|A|} \binom{B}{A} \binom{A}{B_i} \binom{A}{B_j} \right) p_B$$

□

Remarque 13. *La proposition ci-dessus définit implicitement $\binom{B_k}{B_i, B_j}$ comme le nombre de façons d'écrire un élément du bloc B_k comme une réunion d'un élément du bloc B_i et d'un élément du bloc B_j, et affirme qu'il est indépendant du représentant choisi. Ceci a déjà été mis en évidence par W.L.Kocay [8] dans le cadre de la reconstruction des graphes.*

L'ensemble de la structure d'une digèbre se trouve donc résumé dans cette matrice de coefficients qui représente $\mathsf{C} \circ l \circ \mathsf{C}$ dans une bonne base. En effet on vient de voir qu'elle fournit les trois opérations nécessaires à établir la structure de digèbre. Il est donc naturel de penser que la donnée de cette matrice décrit uniquement une digèbre, c'est à dire qu'elle définit une sous-algèbre

de $\mathbb{R}[x_1, \ldots, x_n]/ < x_1^2 - x_1, x_2^2 - x_2, \ldots, x_n^2 - x_n >$, stable par ∂ et par $\complement$, à isomorphisme près. On peut déjà se demander si les autres opérations que représentent les applications linéaires des $\mathrm{Com}_k(\mathfrak{S}_n)$ peuvent être reconstruites à partir des coefficients comme on l'a fait pour la multiplication. Pour cela, il faut bien sûr supposer qu'elle stabilisent toute digèbre, c'est à dire que la Conjecture 4 p44 est vraie. La proposition suivante traduit ce que l'on sait déjà sur $\mathrm{Com}(\mathfrak{S}_n)$ et $\mathrm{Com}_2(\mathfrak{S}_n)$:

Proposition 39. *Si $\mathcal{D}$ est une digèbre et k vaut 1 ou 2, alors*

$$Com_k(\mathfrak{S}_n)(\mathcal{D}^{\otimes k}) \subseteq \mathcal{D}$$

et on peut calculer les matrices des applications linéaires de $Com_k(\mathfrak{S}_n)$ restreintes à $\mathcal{D}^{\otimes k}$ à partir de la matrice des coefficients mentionnée ci-dessus.

Il est intéressant de constater que la seule preuve dont on dispose pour prouver que $\mathrm{Com}_2(\mathfrak{S}_n)(\mathcal{D}^{\otimes 2}) \subseteq \mathcal{D}$ fournit directement le calcul des matrices associées. Par ailleurs, la généralisation de cette proposition à tous les k implique la Conjecture 4 p44, et se trouve être en même temps équivalente au fait que la donnée de la matrice de coefficients décrit uniquement une digèbre à isomorphisme près. En effet il n'est pas difficile de voir que le calcul d'une application de $\mathrm{Com}^0_{2^n}(\mathfrak{S}_n)$ bien choisie dans une base de $\mathcal{D}^{2^n}$ décrit explicitement la façon dont 2^n ensembles forment $\mathcal{D}$.

Une question plus faible que de savoir quelles sont toutes les digèbres (les algèbres d'invariants ?) est donc de savoir quels sont les jeux de coefficients possibles. Il est clair que certaines relations doivent exister entre les trois opérations de dérivation, complémentation, et de multiplication, tout simplement parce que ces relations existent dans $\mathcal{S}_n$, et doivent donc se transmettre à ses sous-algèbres. Ces relations auront bien évidemment lieu dans les $\mathrm{Com}^l_k(\mathfrak{S}_n)$ étudiés plus haut, et fourniront ainsi les générateurs d'un idéal de relations polynomiales qui doivent être vérifiées par les coefficients d'une digèbre tels que décrit ci-dessus.

Avant de procéder plus avant vers ses relations, on peut remarquer que la stabilité par les deux opérations ∂, $\complement$ n'est pas nécessaire à la définition de coefficients. D'après les Proposition 5 p15 et 19 p26, on sait que la structure d'algèbre de $\mathcal{S}_n$ définit une structure de blocs qui correspond aux ensembles sur lesquels une sous-algèbre prend toujours une valeur constante. On détaille dans la section suivante les conditions à réunir pour définir une matrice de coefficients raisonnable.

2.2 ε-algèbres

Soit $\mathcal{D}$ une digèbre d'ordre n, et A un sous-ensemble de $\Omega = \{1, \ldots, n\}$. $\mathcal{D}$ est alors une sous-algèbre de $\mathcal{S}_n$, l'algèbre des polynômes sur les variables $x_1, \ldots, x_n$. Il est possible de définir des digèbres d'ordre $|A|$ avec comme ensemble de base A, en prenant une variable pour chaque élément de A, ce qui engendre une algèbre de polynômes que l'on note $\mathcal{S}_A$. On pose alors h_A l'application de $\mathcal{S}_n$ dans $\mathcal{S}_A$ qui envoie p_S sur lui-même si S est contenu dans A, et sur 0 sinon. Alors $h_A(\mathcal{D})$ est stable par ε_A et par la multiplication dans $\mathcal{S}_A$, mais n'est pas toujours une digèbre :

- $h_A(\mathcal{D})$ est stable par multiplication, en effet $h_A(p \cdot q) = h_A(p) \cdot h_A(q)$, car pour tous ensembles S, T, $S \cup T$ est inclus dans A si, et seulement si S et T sont inclus dans A. On a donc $h_A(p_S \cdot p_T) = h_A(p_S) \cdot h_A(p_T)$ pour tout couple S, T, et on peut conclure par linéarité.
- On a vu qu'une base de $\mathcal{D}$ en tant qu'espace vectoriel est donnée par les $p_{\mathcal{B}_i}$ où les $\mathcal{B}_i$ sont les blocs de $\mathcal{D}$. Pour montrer que $h_A(\mathcal{D})$ est stable par ε, il suffit donc de montrer que pour tout bloc $\mathcal{B}_i$ de $\mathcal{D}$, $\varepsilon_A \circ h_A\left(\sum_{B \in \mathcal{B}_i} p_B\right)$ appartient à $h_A(\mathcal{D})$.
  On a :

$$\begin{aligned}
\varepsilon_A \circ h_A\left(\sum_{B \in \mathcal{B}_i} p_B\right) &= \varepsilon_A\left(\sum_{\substack{B \in \mathcal{B}_i \\ B \subseteq A}} p_B\right) \\
&= \sum_{\substack{B \in \mathcal{B}_i \\ B \subseteq A}} \sum_{\substack{U \\ B \subseteq U \subseteq A}} (-1)^{|U|-|B|} p_U \\
&= \sum_{U \subseteq A} (-1)^{|U|-|B|} p_U \left|\{B \in \mathcal{B}_i \ t.q. \ B \subseteq U\}\right|
\end{aligned}$$

  Comme $\mathcal{D}$ est une digèbre, tous les éléments d'un bloc $\mathcal{B}_j$ contiennent le même nombre d'éléments de $\mathcal{B}_i$, donc

$$\begin{aligned}
\varepsilon_A \circ h_A\left(\sum_{B \in \mathcal{B}_i} p_B\right) &= \sum_j (-1)^{|\mathcal{B}_j|-|\mathcal{B}_i|} \binom{\mathcal{B}_j}{\mathcal{B}_i} \sum_{\substack{U \subseteq A \\ U \in \mathcal{B}_j}} p_u \\
&= \sum_j (-1)^{|\mathcal{B}_j|-|\mathcal{B}_i|} \binom{\mathcal{B}_j}{\mathcal{B}_i} h_A\left(p_{\mathcal{B}_j}\right)
\end{aligned}$$

- Dire que $h_A(\mathcal{D})$ est une digèbre équivaut à dire que c'est un espace stable par complémentation. A supposer que la conjecture soit vraie, ceci équivaut au fait que pour tout couple U_1, U_2 de sous-ensembles de A inclus dans un même bloc de $\mathcal{D}$, il existe une permutation des éléments de A qui stabilise tous les polynômes de $h_A(\mathcal{D})$, et qui envoie U_1 sur U_2. Ceci peut arriver, par exemple lorsque $\mathcal{D}$ est l'algèbre des invariants de $\mathfrak{S}_n$.
  Mais ce n'est pas toujours le cas, ceci suppose en effet que les complémentaires de U_1 et U_2 dans A soient isomorphes dans $h_A(\mathcal{D})$. Il est clair que ces derniers peuvent ne pas être isomorphes dans $\mathcal{D}$.
  Par exemple, si $\mathcal{D}$ est l'algèbre des invariants du groupe de permutations $\{\mathrm{id}, (1,2)(3,4)\}$ sur quatre éléments, et A est le sous-ensemble $\{1,2,3\}$, alors on a $h_A(\mathcal{D}) = \left\{p_\emptyset,\ p_{\{1\}} + p_{\{2\}},\ p_{\{3\}},\ p_{\{1,2\}},\ p_{\{1,3\}},\ p_{\{2,3\}},\ p_{\{1,2,3\}}\right\}$.

En revanche, en supposant que $\mathcal{D}$ est une algèbre d'invariants, et que A est stable par le groupe, $h_A(\mathcal{D})$ est une digèbre. Dans tous les cas, on peut toujours définir une matrice de coefficients pour $h_A(\mathcal{D})$: ce n'est autre que la sous-matrice de celle de $\mathcal{D}$ dont les lignes et les colones correspondent aux blocs de $\mathcal{D}$ qui contiennent au moins un élément inclus dans A.

Définition 16. *On appelle* ε-algèbre *une sous-algèbre non vide, non réduite à* $\{0\}$ *de* $\mathcal{S}_n$ *qui est stable par* ε.

On vient de voir que les ε-algèbres ne sont pas forcément des digèbres, en effet pour qu'une ε-algèbre soit une digèbre, il faut et il suffit qu'elle soit stable par complémentation. On peut également considérer comme contre exemple l'algèbre formée par les multiples de p_A pour un certain ensemble A.

De la même façon que pour les digèbres, on peut définir une structure de blocs, ainsi que les coefficients associés. Il faut toutefois noter que si les blocs d'une ε-algèbre sont toujours disjoints, il ne partitionnent plus forcément $\mathcal{P}(\Omega)$.

Proposition 40. *Étant donné deux blocs* $\mathcal{B}_1$ *et* $\mathcal{B}_2$ *d'une* ε*-algèbre* $\mathcal{E}$*, et* A *un élément de* B_1 *donné, alors le nombre d'éléments de* B_2 *qui sont inclus dans* A *est indépendant du représentant* A *choisi. On note toujours* $\binom{B_1}{B_2}_{\mathcal{E}}$ *ce nombre, ou plus simplement* $\binom{B_1}{B_2}$ *lorsque le contexte indique clairement dans quelle* ε*-algèbre on se trouve.*

Preuve : Il suffit de remarquer que l'application E utilisée dans la preuve de

la Proposition 36 p47 n'est autre que l'inverse de ε, en effet :

$$\begin{aligned} E \circ \varepsilon(p_S) &= \sum_{A \ t.q. \ S \subseteq A} (-1)^{|A|-|S|} E(p_A) \\ &= \sum_{A \ t.q. \ S \subseteq A} (-1)^{|A|-|S|} \sum_{B \ t.q. \ A \subseteq B} p_B \\ &= \sum_{B} (-1)^{|S|} p_B \sum_{A \ t.q. \ S \subseteq A \subseteq B} (-1)^{|A|} \\ &= p_S \end{aligned}$$

□

Proposition 41. *Réciproquement, si $\mathfrak{p}$ est une partition de $\mathcal{P}(\{1, \ldots, n\})$ telle que tous les éléments A d'un bloc B_1 contiennent le même nombre d'éléments d'un bloc B_2, alors les $\left\{\sum_{A \in \mathfrak{p}_i} p_A, \ \mathfrak{p}_i \in \mathfrak{p}\right\}$ forment une ε-algèbre.*

Preuve : Il est clair que les $\left\{\sum_{A \in \mathfrak{p}_i} \varepsilon_A, \ \mathfrak{p}_i \in \mathfrak{p}\right\}$ forment une algèbre. Il suffit de montrer que c'est un espace stable par ε^{-1} : soit $\mathfrak{p}_i \in \mathfrak{p}$, alors

$$\begin{aligned} \sum_{A \in \mathfrak{p}_i} p_A &= \sum_{A \in \mathfrak{p}_i} \sum_{B \ t.q. \ A \subseteq B} \varepsilon_B \\ &= \sum_{B} \binom{B}{\mathfrak{p}_i} \varepsilon_B \end{aligned}$$

□

On peut montrer que si $\mathfrak{m}$ est une ε-algèbre, alors $h_A(\mathfrak{m})$ aussi. Ceci ouvre la voie à l'énumération des ε-algèbres à permutation près, ainsi que de leurs matrices de coefficients. Malheureusement, le problème reste doublement exponentiel.

Avant de passer à l'étude systématique des relations que l'on peut obtenir, on peut déjà s'intéresser aux relations, plus ou moins évidentes, qui peuvent être établies entre les coefficients, intégrant de fait toute l'étude précédente dans une série de résultats relatifs aux problèmes de reconstruction.

2.3 Relations connues

Certaines relations sont immédiates, par exemple :

- Si $H_1, \ldots, H_p$ sont tous les blocs de cardinalité k, alors

$$\sum_{i=1}^{p} \binom{G}{H_i} = \binom{|G|}{k}$$

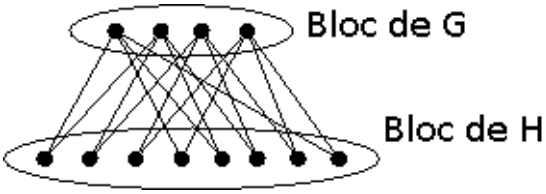
- Si $|G| \geq |H|$ on a $\binom{B_1}{B_2} = 1$ si $B_1 = B_2$, et 0 sinon.

En regardant ce qui se passe avec le complémentaire, on peut aussi trouver certaines relations, par exemple, il est clair que $\binom{\Omega}{G} = \binom{\Omega}{G^c}$.

Proposition 42. *Plus généralement, pour tout couple d'éléments G et H, on a*

$$\binom{\Omega}{H}\binom{H^c}{G^c} = \binom{\Omega}{G}\binom{G}{H}$$

Preuve : Considérons le graphe biparti dont les sommets sont formés par les éléments du bloc de G et ceux du bloc de H, un élément H étant relié à un élément de G si le premier est inclus dans le second.



Alors les éléments du bloc de G ont tous le même nombre de voisins $\binom{G}{H}$. Deux ensembles sont dans le même bloc si et seulement si leurs complémentaires le sont, et on a de plus $H \subseteq G$ si et seulement si $G^c \subseteq H^c$, donc les éléments du bloc de H ont tous le même nombre de voisins $\binom{H^c}{G^c}$. Le nombre d'arêtes de ce graphe est donc :

$$\binom{\Omega}{H}\binom{H^c}{G^c} = \binom{\Omega}{G}\binom{G}{H}$$

□

Diverses relations supplémentaires entre les coefficients sont déjà connues, elles proviennent de l'étude du problème de reconstruction, mais s'appliquent au cas général. Un des premiers résultats des travaux sur la reconstruction est le suivant :

Proposition 43 (Lemme de Kelly)**.** *Si $H_1, \ldots, H_p$ sont les blocs de cardinalité $|G|-1$, on a*

$$\binom{G}{H} = \frac{1}{|G|-|H|} \sum_{i=1}^{p} \binom{G}{H_i}\binom{H_i}{H}$$

pour tout bloc H tel que $|H| < |G|$.

On peut généraliser facilement :

Proposition 44. *Si $H_1, \ldots, H_p$ sont les blocs de cardinalité k, on a*

$$\binom{|G|-|H|}{k-|H|}\binom{G}{H} = \sum_{i=1}^{p} \binom{G}{H_i}\binom{H_i}{H}$$

pour tout H tel que $|H| \leq k$.

Pour démontrer cette proposition, il suffit de considérer qu'un élément du bloc de H inclus dans G est inclus dans exactement $\binom{|G|-|H|}{k-|H|}$ sous-ensembles à k éléments de G.

Une jolie propriété de la matrice des coefficients d'une digèbre a été mise en évidence par V.B.Mnukhin [12] :

Proposition 45. *Si $\mathcal{M}$ est une matrice de coefficients d'une digèbre $\mathcal{D}$, on a, pour tout k dans $\mathbb{Z}$ et tout couple (G, H) de blocs de $\mathcal{D}$:*

$$\mathcal{M}^k_{G,H} = k^{|G|-|H|}\binom{G}{H}$$

avec la convention $0^0 = 1$

Preuve : Soit M_k la matrice dont le coefficient G, H est $k^{|G|-|H|}\binom{G}{H}$. Alors on a avec la convention considérée, $M_0 = Id$ l'identité de l'algèbre des matrices, et pour tout k différent de 0, $M_k A = M_{k+1}$. En effet le coefficient G, H du produit $M_k A$ est

$$(M_k A)_{G,H} = \sum_U k^{|G|-|U|}\binom{G}{U}\binom{U}{H}$$

où la somme porte sur tous les blocs U de $\mathcal{D}$, ce qui en fixant un représentant g du bloc G donne

$$(M_k A)_{G,H} = \sum_{U \subseteq g} k^{|g|-|U|} \binom{U}{H}$$

où la somme porte sur tous les sous-ensembles U de g.

$$\begin{aligned}
(M_k A)_{G,H} &= \sum_{U \subseteq g} k^{|g|-|U|} \sum_{V \subseteq U} \mathbb{1}_{\{V \simeq H\}} \\
&= \sum_{V \subseteq g} k^{|g|} \mathbb{1}_{\{V \simeq H\}} \sum_{V \subseteq U \subseteq g} k^{-|U|} \\
&= \sum_{V \subseteq g} k^{|g|} \mathbb{1}_{\{V \simeq H\}} \sum_{r=0}^{|g|-|V|} \binom{|g|-|V|}{r} k^{-r-|V|} \\
&= \sum_{V \subseteq g} k^{|g|-|V|} \mathbb{1}_{\{V \simeq H\}} \left(1 + \frac{1}{k}\right)^{|g|-|V|} && (2.1) \\
&= \sum_{V \subseteq g} \mathbb{1}_{\{V \simeq H\}} (k+1)^{|g|-|V|} && (2.2) \\
&= (k+1)^{|G|-|H|} \binom{G}{H} && (2.3)
\end{aligned}$$

En considérant qu'avec la convention $0^0 = 1$, les équations 2.1 p56, 2.2 p56, et 2.3 p56 restent valables.

Comme on a $M_1 = A$ et $M_k A = M_{k+1}$ pour tout k, c'est facilement vrai pour $k = 0$, et la proposition résulte d'une induction dans les deux sens. □

Proposition 46. *Les relations (entre les coefficients d'une digèbre) fournies par les Propositions 43 p55, 44 p55, et 45 p55 sont équivalentes.*

Preuve :

- Il est clair que la Proposition 44 p55 implique la Proposition 43 p55, il suffit de prendre $k = |G| - 1$. Pour la réciproque, on procède par récurrence sur $r = |G| - k$. Lorsque $r = 1$, on retrouve le cas de la Proposition 43 p55, donc la récurrence est initialisée. Supposons les relations vérifiées jusqu'à r, alors :

$$\binom{G}{H} \binom{|G|-|H|}{|G|-|H|-r} = \sum_{i=1}^{p} \binom{G}{H_i} \binom{H_i}{H}$$

où les H_i sont les blocs de cardinalité $|G| - r$. D'après la Proposition 43 p55, on a alors

$$\binom{H_i}{H} = \frac{1}{|H_i| - |H|} \sum_{j=1}^{q} \binom{H_i}{F_j} \binom{F_j}{H}$$

si les F_j sont les blocs de cardinalité $|G| - r - 1$. En regroupant les deux équations, on obtient :

$$\binom{G}{H} \binom{|G| - |H|}{|G| - |H| - r} = \sum_{i=1}^{p} \frac{1}{|H_i| - |H|} \sum_{j=1}^{q} \binom{H_i}{F_j} \binom{F_j}{H} \binom{G}{H_i}$$

$$\binom{G}{H} \binom{|G| - |H|}{|G| - |H| - r} (|G| - r - |H|) = \sum_{j=1}^{q} \binom{F_j}{H} \sum_{i=1}^{p} \binom{G}{H_i} \binom{H_i}{F_j}$$

C'est à dire, par application de l'hypothèse de récurrence au rang r pour les $\binom{G}{F_j}$:

$$\binom{G}{H} \binom{|G| - |H|}{|G| - |H| - r} (|G| - r - |H|) = \sum_{j=1}^{q} \binom{F_j}{H} (r + 1) \binom{G}{F_j}$$

Soit au final :

$$\binom{G}{H} \binom{|G| - |H|}{|G| - |H| - r - 1} = \sum_{j=1}^{q} \binom{G}{F_j} \binom{F_j}{H}$$

Ce qui achève la preuve de l'équivalence de la Proposition 44 p55 et de la Proposition 43 p55.

- Supposons vérifiées les relations de la Proposition 44 p55. Alors avec

M_k la matrice dont le coefficient G, H est $k^{|G|-|H|}\binom{G}{H}$, on a

$$\begin{aligned}
(M_k \cdot M)_{G,H} &= \sum_U k^{|G|-|U|}\binom{G}{U}\binom{U}{H} \\
&= \sum_{l=|H|}^{|G|} k^{|G|-l} \sum_{\substack{E \\ |E|=l}} \binom{G}{E}\binom{E}{H} \\
&= \binom{G}{H} \sum_{l=|H|}^{|G|} k^{|G|-l}\binom{|G|-|H|}{l-|H|} \\
&= \binom{G}{H} \sum_{i=0}^{|G|-|H|} k^{(|G|-|H|)-i}\binom{|G|-|H|}{i} \\
&= (k+1)^{|G|-|H|}\binom{G}{H}
\end{aligned}$$

- Dans l'autre sens, on se propose de montrer que pour tout k, si $H_1, \ldots, H_p$ sont les blocs de cardinalité k, on a

  $$\binom{|G|-|H|}{k-|H|}\binom{G}{H} = \sum_{i=1}^{p}\binom{G}{H_i}\binom{H_i}{H}$$

  pour tout H tel que $|H| \leq k$.
  Si les relations de la Proposition 45 p55 sont vérifiées, alors quel que soit l, on a

  $$(l+1)^{|G|-|H|}\binom{G}{H} = \sum_U l^{|G|-|U|}\binom{G}{U}\binom{U}{H}$$

  C'est à dire :

  $$\sum_{i=0}^{|G|-|H|}\binom{|G|-|H|}{i} l^{|G|-|H|-i}\binom{G}{H} = \sum_{i=0}^{|G|-|H|-i} l^{|G|-|H|-i} \sum_{\substack{E \\ |E|=i+|H|}} \binom{G}{E}\binom{E}{H}$$

  Comme ceci est valable pour tout l, l'identification des deux polynômes fournit le résultat souhaité.

□

Finalement, on peut examiner un résultat très connu sur les problèmes de reconstruction : la preuve par Lovász [11] que les graphes sur n sommets possédant strictement plus de $\frac{n(n-1)}{4}$ arêtes sont arêtes-reconstructibles

(voir aussi [18], [17]). Il est de prouver ce résultat en utilisant seulement les relations ci-dessus, et une nouvelle relation facile :

Proposition 47. *Si A et B sont deux blocs d'une digèbre $\mathcal{D}$, alors le nombre de façons d'écrire l'ensemble total Ω comme union d'un élément de A et d'un élément de B est :*

$$\binom{\Omega}{A, B} = \binom{\Omega}{A}\binom{A}{B^c}$$

On peut alors reformuler le résultat de Lovász, qui est valable dans toutes les digèbres :

Proposition 48. *Si $\mathcal{D}$ est une digèbre sur n éléments dont les blocs sont $B_1, \ldots, B_s$ et A, B sont deux sous-ensembles de Ω de cardinalité $k > \frac{n}{2}$, tels que pour tout bloc B_i de cardinalité strictement inférieure à k on ait $\binom{A}{B_i} = \binom{B}{B_i}$, alors A et B sont inclus dans un même bloc.*

Preuve : Elle repose sur le lemme suivant, que l'on pourrait appeler "relation de Lovász".

Lemme 1. *Si $\mathcal{D}$ est une digèbre sur n éléments dont les blocs sont $B_1, \ldots, B_s$, alors quels que soient U et V deux sous-ensembles de Ω :*

$$\sum_{i=1}^{s} (-1)^{e(B_i)} \frac{\binom{U}{B_i}\binom{V}{B_i}}{\binom{\Omega}{B_i}} = \frac{\binom{U^c}{V}}{\binom{\Omega}{V}}$$

En posant $U = V = A$ puis $U = A$ et $V = B$ dans le lemme ci-dessus, on obtient la Proposition. □

Preuve du lemme : On a

$$\begin{aligned}
\sum_{i=1}^{s} (-1)^{e(B_i)} \frac{\binom{U}{B_i}\binom{V}{B_i}}{\binom{\Omega}{B_i}} &= \sum_{i=1}^{s} \frac{(-1)^{e(B_i)}}{\binom{\Omega}{B_i}} \frac{\binom{\Omega}{B_i}}{\binom{\Omega}{U}} \binom{B_i^c}{U^c} \frac{\binom{\Omega}{B_i}}{\binom{\Omega}{V}} \binom{B_i^c}{V^c} \\
&= \frac{1}{\binom{\Omega}{U}\binom{\Omega}{V}} \sum_{i=1}^{s} (-1)^{e(B_i)} \binom{\Omega}{B_i} \binom{B_i^c}{U^c} \binom{B_i^c}{V^c} \\
&= \frac{1}{\binom{\Omega}{U}\binom{\Omega}{V}} \sum_{i=1}^{s} (-1)^{e(K_n)-e(B_i^c)} \binom{\Omega}{B_i^c} \binom{B_i^c}{U^c} \binom{B_i^c}{V^c} \\
&= \frac{1}{\binom{\Omega}{U}\binom{\Omega}{V}} \binom{\Omega}{U^c, V^c} = \frac{\binom{U^c}{V}}{\binom{\Omega}{V}}
\end{aligned}$$

$\square$

De plus, on a déjà vu des relations à l'intérieur de $\mathrm{Com}\,(\mathfrak{S}_n)$ lorsqu'on a étudié les digèbres, la liste n'a pas d'importance, puisque l'on peut écrire toutes les matrices de ses éléments.

2.4 De nouvelles relations ?

2.4.1 Relations d'ordre 0

On a vu à la Proposition 28 p34 que les :

$$E_\mu = \sum_{(A,B)\vdash\mu} E_{A\to B}$$

où μ parcours l'ensemble des structures d'incidences d'ordre 2, forment une base de $\mathrm{Com}(\mathfrak{S}_n)$.

Il est facile de voir que les matrices de ces derniers s'expriment en fonction des coefficients, en effet on a vu à la Proposition 29 p35 que $\mathrm{Com}(\mathfrak{S}_n)$ est engendré par ∂, $\complement$ et les id_k et la loi de composition $\circ$. Plus précisément, si $|G| = l$ et $|H| = k$, alors :

$$\sum_s \binom{s}{r} E_{k,l,s_{[G,H]}} = \sum_{\substack{U \\ |U|=r}} \binom{G}{U}\binom{U^c}{H^c}$$

On a donc

$$E_{k,l,r_{[G,H]}} = \sum_U (-1)^{|U|-r}\binom{|U|}{r}\binom{G}{U}\binom{U^c}{H^c}$$

Il est clair que $E_{k,l,r}$ est nulle si $k+l-r > n$ ou si $r > k$ ou encore si $r > l$. Ces deux derniers cas sont inclus dans l'équation ci-dessus, on obtient donc les relations polynomiales :

$$\text{si } \ k+l-r > n, \quad \sum_U (-1)^{|U|-r}\binom{|U|}{r}\binom{G}{U}\binom{U^c}{H^c} = 0$$

2.4.2 Relations d'ordre 1

On peut établir une loi de composition entre les E_μ facilement grâce à $\mathrm{Com}_2^1(\mathfrak{S}_n)$. En effet si on pose :

$$E_{k,l,r} \circ E_{i,k,j} = \sum_t Y_{i,j,k,l,t,r} E_{i,l,t}$$

où $Y_{i,j,k,l,t,r}$ est le nombre de sous-ensembles C de Ω, de cardinalité k, qui forment la structure d'incidence suivante :

- $|A \cap C| = j$
- $|B \cap C| = r$

avec un couple A, B de sous-ensembles donnés de Ω, de cardinalités respectives i et l tels que $|A \cap B| = t$, alors ce nombre peut être calculé de la façon suivante : si (A, B, C) vérifie les conditions ci-dessus, alors on a :

- $|A| = i$
- $|B| = l$
- $|C| = k$
- $|A \cap C| = j$
- $|B \cap C| = r$
- $|A \cap B| = t$

si on suppose de plus que $|A \cap B \cap C| = s$, alors on doit avoir :

- $C \cap A^c \cap B^c$ est un sous-ensemble de cardinalité $k - j - r + s$ de $A^c \cap B^c$
- $C \cap A \cap B^c$ est un sous-ensemble de cardinalité $j - s$ de $A \cap B^c$
- $C \cap A^c \cap B$ est un sous-ensemble de cardinalité $r - s$ de $A^c \cap B$
- $C \cap A \cap B$ est un sous-ensemble de cardinalité s de $A \cap B$

Les quatre ensembles $A^c \cap B^c$, $A \cap B^c$, $A^c \cap B$, et $A \cap B$ forment une partition de Ω de cardinalités respectives $n-i-l+t$, $i-t$, $l-t$, et t, donc réciproquement, étant donné A et B de cardinalités respectives i et l et d'intersection de taille t, tout ensemble C vérifiant les quatre conditions ci-dessus convient. On en déduit donc que

$$Y_{i,j,k,l,t,r} = \sum_{s=0}^{t} \binom{n-i-l+t}{k-j-r+s} \binom{i-t}{j-s} \binom{l-t}{r-s} \binom{t}{s}$$

2.4.3 Relations d'ordre 2

De la même façon, on peut chercher les relations qui ont lieu pour les fonctions de $\mathrm{Com}_2^1(\mathfrak{S}_n)$. On a vu qu'une base de cet espace vectoriel est formée par les E_μ, où μ est une structure d'incidence d'ordre trois. De plus, on sait que la famille

$$\left\{ E_{k,a_3,r_3} \circ m \circ (E_{a_1,k,r_1} \times E_{a_2,k,r_2}) \right\}$$

est génératrice de l'espace vectoriel $\mathrm{Com}_2^1(\mathfrak{S}_n)$ (voir Proposition 33 p40). On n'a besoin, pour exprimer les E_μ, que des fonctions paramétrées par $a_1, a_2, a_3, r_1, r_2, r_3$ et k, tels que :

- $\mu(\emptyset) = n$
- $\mu(\{1\}) = a_1$
- $\mu(\{2\}) = a_2$
- $\mu(\{3\}) = a_3$
- $\mu(\{1,2\}) = r_1 + r_2 - k$
- $\mu(\{1,3\}) = r_1 + r_3 - k$
- $\mu(\{2,3\}) = r_2 + r_3 - k$
- $\mu(\{1,2,3\}) = r_1 + r_2 + r_3 - 2k$

est une structure d'incidence, c'est à dire que d'après la Proposition 25 p31 , elle vérifie :

$$\forall J \subseteq \{1,\ldots,k\}, \sum_{J \subseteq L \subseteq \{1,\ldots,k\}} (-1)^{|L|-|J|} \mu(L) \geq 0$$

On obtient donc :

- $\mu(\{1,2,3\}) = r_1 + r_2 + r_3 - 2k \geq 0$
- $\mu(\{2,3\}) - \mu(\{1,2,3\}) = k - r_1 \geq 0$
- $\mu(\{1,3\}) - \mu(\{1,2,3\}) = k - r_2 \geq 0$
- $\mu(\{1,2\}) - \mu(\{1,2,3\}) = k - r_3 \geq 0$
- $\mu(\{3\}) - \mu(\{1,3\}) - \mu(\{2,3\}) + \mu(\{1,2,3\}) = a_3 - r_3 \geq 0$
- $\mu(\{2\}) - \mu(\{1,2\}) - \mu(\{2,3\}) + \mu(\{1,2,3\}) = a_2 - r_2 \geq 0$
- $\mu(\{1\}) - \mu(\{1,3\}) - \mu(\{1,2\}) + \mu(\{1,2,3\}) = a_1 - r_1 \geq 0$
- $\mu(\emptyset) - \mu(\{1\}) - \mu(\{2\}) - \mu(\{3\}) + \mu(\{1,2\}) + \mu(\{1,3\}) + \mu(\{2,3\}) - \mu(\{1,2,3\}) = n - a_1 - a_2 - a_3 - k + r_1 + r_2 + r_3 \geq 0$

Remarquons que l'on sait déjà que pour tout $i = 1, 2, 3$, on doit évidement avoir, $n \geq k \geq r_i \leq a_i \leq n$, c'est à dire que les E_{k,a_i,r_i} ne sont pas nulles. On obtient donc deux relations supplémentaires :

$$\begin{aligned} r_1 + r_2 + r_3 &\geq 2k \\ n - k &\geq a_1 + a_2 + a_3 - r_1 - r_2 - r_3 \end{aligned}$$

La première équation traduit le fait qu'on s'intéresse uniquement aux intersections d'au moins deux ensembles, alors que la deuxième concerne le fait que les sous-ensembles qu'on laisse ne s'intersectent pas.

Comme on s'y attend, ces dernières relations sont plus faibles, en effet on doit avoir $n - k \geq a_1 - r_1 + a_2 - r_2 + a_3 - r_3 \geq 0$, et pour tout $i = 1, 2, 3$, $n - a_i \geq k - r_i + \sum_{j \neq i} (a_j - r_j) \geq 0$.

Donc les fonctions en $n, a_1, a_2, a_3, r_1, r_2, r_3, k$ qui violent au moins l'une des inégalités de la liste tout en vérifiant celles ci-dessus sont inutiles : elles s'expriment comme combinaisons linéaires des autres. Remarquons que cela implique d'avoir des relations entre les fonctions Z de la preuve de la Proposition 33 p40, ce sont celles qui ont lieu dans l'algèbre symétrique.

2.4.4 Relations d'ordre quelconque, tests

On a vu dans la première partie qu'il est impossible d'utiliser la même technique pour exprimer tous les E_μ lorsque l'ordre de la structure d'incidence μ est au moins quatre. Néanmoins, on peut penser qu'il existe des relations de dépendance linéaire entre les fonctions de $\mathrm{Com}_k^l(\mathfrak{S}_n)$ que l'on sait exprimer grâce aux coefficients.

Se pose alors la question de savoir si ce processus peut-être stoppé, c'est à dire si l'on peut espérer obtenir un ensemble fini de relations polynomiales entre les coefficients. Étant donné une matrice de coefficients, ces derniers étant en nombre fini, il est clair que tout idéal de relations polynomiales qui les relient est noethérien donc admet un nombre fini de générateurs. Dans l'absolu, si l'on pouvait exprimer toutes les applications des $\mathrm{Com}_k(\mathfrak{S}_n)$ en fonction des coefficients, on aurait probablement une preuve de la Conjecture 4 p44, mais on serait aussi assuré d'obtenir un système complet de relations. Ceci n'est malheureusement pas possible, en effet il existe des digèbres ayant la même matrice de coefficients, mais qui ne sont pas isomorphes par permutation. Or les applications de $\mathrm{Com}_{2^n}(\mathfrak{S}_n)$ permettent, on l'a vu sans la

preuve de la Proposition 35 p44, de retrouver l'incidence des éléments des blocs, et donc d'identifier une digèbre a permutation près.

Le plus petit exemple, parmi les algèbres d'invariants est d'ordre 8, il y en a deux couples présentés en annexe.

Remarque 14. *A priori, ceci ne remet pas en cause la Conjecture 4 p44, en effet ce n'est pas parce qu'on ne peut exprimer un opérateur en fonction d'opérateurs stabilisants connus, que cet opérateur ne stabilise pas. A titre d'exemple simple, on pourra considérer les sous espaces vectoriels de* $\mathbb{R}^2$ *stables par* $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ *: ils sont stables par* $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ *qui n'est pourtant pas dans l'algèbre engendrée par* $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$*. On trouve ici un lien intéressant avec le théorème du bicommutant de von Neumann, qu'on à déjà aperçu à travers les* $*$*-algèbres p36.*

Finalement, a-t-on vraiment obtenu de nouvelles relations ? Pour le savoir, il suffit de chercher des exemples de matrices vérifiant certaines relations mais pas d'autres, ce qui étaie une classification dont une bonne partie a déjà été effectuée dans la Proposition 46 p56.

La matrice suivante vérifie les relations de complément, et de Kelly, Mnukhin, mais pas celle de Lovász :

$$\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 3 & 3 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 3 & 3 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 3 & 3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 4 & 6 & 0 & 0 & 4 & 0 & 1 & 0 & 0 & 0 \\
1 & 4 & 6 & 0 & 0 & 4 & 0 & 0 & 1 & 0 & 0 \\
1 & 5 & 10 & 0 & 0 & 10 & 0 & 0 & 5 & 1 & 0 \\
1 & 6 & 15 & 0 & 0 & 20 & 0 & 0 & 15 & 6 & 1
\end{bmatrix}$$

contrairement à, par exemple :

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 3 & 0 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 3 & 1 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 3 & 0 & 3 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 4 & 1 & 5 & 1 & 2 & 1 & 1 & 0 & 0 & 0 \\ 1 & 4 & 2 & 4 & 0 & 4 & 0 & 0 & 1 & 0 & 0 \\ 1 & 5 & 2 & 8 & 2 & 6 & 2 & 4 & 1 & 1 & 0 \\ 1 & 6 & 3 & 12 & 4 & 12 & 4 & 12 & 3 & 6 & 1 \end{bmatrix}$$

La matrice suivante vérifie les relations de Kelly, Mnukhin, Lovász (sous une forme dépourvue de division), pourtant elle ne ressemble pas à une matrice de coefficients de digèbre :

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 3 & 0 & 3 & 1 & 0 & 0 & 0 \\ 1 & 3 & 1 & 2 & 0 & 1 & 0 & 0 \\ 1 & 4 & 0 & 6 & 4 & 0 & 1 & 0 \\ 1 & 5 & 0 & 10 & 10 & 0 & 5 & 1 \end{bmatrix}$$

On peut vérifier que par exemple, les coefficients de $E_{2,5,2}$ sur la troisième colonne sont tous nuls, ce qui contredit le fait que $E_{5,2,2} \circ E_{2,5,2}$ contient des termes de la forme $E_{2,2,r}$ qui ne sont pas tous nuls sur la troisième colonne.

Chapitre 3

Digèbres engendrées par un élément, application aux problèmes de reconstruction

On formalise un problème de reconstruction de la manière suivante : Étant donné un ensemble partiellement ordonné S muni de l'action d'un groupe G respectant l'ordre, et un ensemble de fonctions $f_1, \ldots, f_p$ définies sur les orbites de S pour G, peut-on identifier une orbite $\mathcal{O}$ à partir des valeurs prises par les fonctions $f_1, \ldots, f_p$ sur $\mathcal{O}$?

Dans ce travail, l'ensemble S est restreint aux parties d'un ensemble $\Omega = \{1, \ldots, n\}$, et par conséquent le groupe G sera donc un sous-groupe de $\mathfrak{S}_n$. L'ensemble d'arrivée des fonctions $f_1, \ldots, f_p$ n'a pas d'importance, ce qui importe ce sont les points qu'elles séparent. Comme l'ensemble de définition que l'on considère est fini, on pourra toujours se ramener à un ensemble d'arrivée de taille suffisante, on choisit le corps $\mathbb{R}$ des nombres réels.

On a vu dans la première partie que les fonctions

$$p_A \ : \ S \mapsto \begin{cases} 1 \text{ si } A \subseteq S \\ 0 \ \text{ sinon} \end{cases}$$

forment une base de l'ensemble $\mathcal{L}$ des applications de $\mathcal{P}(\Omega)$ dans $\mathbb{R}$. On peut donc ramener les fonctions $f_1, \ldots, f_p$ à des éléments de $\mathcal{S}_n$ c'est à dire de la digèbre $\mathbb{R}[x_1, \ldots, x_n]/ < x_1^2 - x_1, x_2^2 - x_2, \ldots, x_n^2 - x_n >$.

Le problème de reconstruction se ramène alors à celui de savoir si l'algèbre

engendrée par les éléments $f_1, \ldots, f_p$ de $\mathcal{S}_n$, c'est à dire l'algèbre des fonctions qui séparent les même points que $f_1, \ldots, f_p$, est une algèbre d'invariants. En effet il est clair que tout sous-groupe G de $\mathfrak{S}_n$ qui laisse invariant les fonctions $f_1, \ldots, f_p$ laissera invariante l'algèbre qu'ils engendrent. Il s'agit donc de savoir si les $f_1, \ldots, f_p$ engendrent $\mathcal{S}_n^G$.

Une réponse positive à la Conjecture 3 p30 ramènerait la question à celle de savoir si l'algèbre engendrée par les $f_1, \ldots, f_p$ est une digèbre. On peut donc considérer un sous-problème de reconstruction :

Étant donné un ensemble d'éléments $f_1, \ldots, f_p$ de $\mathcal{S}_n$, à quelle(s) condition(s) engendrent-t-ils une algèbre qui est une digèbre ?

3.1 Une conjecture de reconstruction générale

P.J.Cameron [4] a proposé une généralisation de la conjecture de reconstruction par les arêtes à l'ensemble des algèbres d'invariants, que l'on étend facilement aux digèbres :

Définition 17.

- *Etant donné un groupe G agissant sur un ensemble Ω, on dit que deux sous-ensembles A et B de Ω sont G-isomorphes si il existe un élément σ de G tel que $\sigma(A) = B$.*
- *On dit que deux sous-ensembles U et V sont G-hypomorphes si il existe une bijection ϕ de U vers V telle que pour tout élément u de U, $U \setminus \{u\}$ et $V \setminus \{\phi(u)\}$ sont G-isomorphes.*
- *On dit qu'un sous ensemble S de Ω est G-reconstructible si tout sous-ensemble G-hypomorphe à S est G-isomorphe à S.*

Le problème de reconstruction généralisé est donc de savoir quelles peuvent être les cardinaux des ensembles non reconstructibles.

Le résultat de Müller se généralise, de même que celui de Lovász comme on l'a déjà vu plus haut :

Proposition 49. *Si $\mathcal{D}$ est une digèbre sur n éléments dont les blocs sont $B_1, \ldots, B_s$, et si A, B sont deux sous-ensembles de Ω de même cardinalité k, tels que pour tout bloc B_i de cardinalité strictement inférieure à k on ait : $\binom{A}{B_i} = \binom{B}{B_i}$, et tels que $k > 1 + \log_2 \binom{\Omega}{A}$, alors A et B sont contenus dans un même bloc.*

Preuve : Pour tout couple d'ensembles U et V, et tout nombre entier r, on pose :

$$G^r_{U,V} = \sum_{i=1}^{s} (-1)^{e(B_i)-r} \binom{e(B_i)}{r} \frac{\binom{U}{B_i}\binom{V}{B_i}}{\binom{\Omega}{B_i}}$$

On a alors $\sum_r G^r_{U,V} = 1$. De plus, sous les hypothèses du théorème,

$$G^r_{A,A} - G^r_{B,A} = (-1)^{e(H)-r} \frac{\binom{e(A)}{r}}{\binom{\Omega}{A}}$$

On obtient donc

$$\frac{2^{e(A)}}{\binom{\Omega}{A}} = \sum_r |G^r_{A,A} - G^r_{B,A}| \leq \sum_r G^r_{A,A} + \sum_r G^r_{A,B} = 2$$

□

Remarque 15. *On remarque la réapparition de la quantité* $\sum_{B_i e(B_i)=r} \frac{\binom{U}{B_i}\binom{V}{B_i}}{\binom{\Omega}{B_i}}$ *qui apparaissait déjà dans le preuve de Lovász. A ce sujet, il est intéressant de noter que les* $G^r_{U,V}$ *sont exactement les* $E_{k,k,r\ [U,V]}$ *définis plus haut, et que les quantités précédentes leur correspondent par inversion de Möbius.*

Dans le cas des algèbres d'invariants, ce résultat est connu sous la forme suivante : les ensembles de cardinal $k > 1 + \log_2 |G|$ sont reconstructibles, ou $|G|$ est l'ordre du groupe sous-jacent, qui est une conséquence directe de la formulation précédente. Il est amusant de noter que pour le groupe symétrique de Ω, la borne obtenue est $1+\log_2 n!$, ce qui est asymptotiquement moins bonne que celle de Lovász.

Il existe des digèbres d'ordre $2p$ avec des ensembles de cardinal p non reconstructibles. Par exemple, on peut considérer l'algèbre des invariants du groupe de permutations dont les générateurs sont les :

$$\{(1,2)(2i+1,2i+2) \quad i = 1..p-1\}$$

Les deux ensembles $A = \{1,3,5,\ldots,2p-1\}$ et $B = \{2,4,6,\ldots,2p\}$ des nombres impairs et pairs ne sont pas dans la même orbite (donc pas dans le même bloc). En effet il suffit de considérer pour chaque ensemble S de taille p le nombre $r(S)$: résidu modulo 2 du nombre d'éléments impairs supérieurs ou égaux à trois. On remarque que les ensembles :

- U contient 1 et $r(U) = 0$ ou U contient 2 et $r(U) = 1$

- U contient 1 et $r(U) = 1$ ou U contient 2 et $r(U) = 0$

sont disjoints et stables par tous les générateurs du groupe, de plus ils séparent A et B.

Malgré cela, A et B ont les mêmes types de sous-ensembles, en effet, si U est un sous-ensemble de A de cardinal $q < p$, on associe à U un unique sous-ensemble V de B de la manière suivante : pour chaque élément i de U, on ajoute $i + 1$ à V. Il est clair que chaque sous-ensemble V ainsi obtenu provient d'un seul et unique antécédent U. Il suffit donc de montrer que dans tout les cas, U et V sont dans une même orbite. On applique successivement à U toutes les permutations de la forme $(1, 2)(u, u + 1)$ pour chaque élément u de U différent de 1 (elles commutent). On obtient ainsi un ensemble qui est soit V, soit $(1, 2)(V)$. Dans ce dernier cas, comme $q < p$, il existe un nombre impair j n'appartenant pas à U (donc $j + 1$ n'appartient pas à V), donc il suffit d'appliquer la permutation $(1, 2)(j, j + 1)$ pour obtenir V.

Cet exemple est facilement adaptable en digèbre d'ordre $2p+1$ contenant des ensembles de cardinal p non reconstructibles, en effet il suffit de considérer le même groupe agissant sur l'ensemble des nombres compris entre 1 et $2p+1$. (On ne peut pas considérer des ensembles de cardinal $p + 1$, car les orbites de cardinal p sont déjà séparées).

On peut remarquer que l'ordre du groupe est $2^{\frac{n-2}{2}}$. En effet on a déjà vu qu'il était commutatif, engendré par $\frac{n-2}{2}$ générateurs d'ordre 2. On a donc $1 + \log_2(G) = \frac{n}{2}$. Le même groupe est donc aussi un cas limite du théorème de Müller.

On peut même ajouter que ceci permet de générer tous les cas limites du théorème de Müller, il suffit d'ajouter un certain nombre d'éléments "fictifs", sur lequel le groupe n'a aucun effet.

On peut alors se demander quels sont les paramètres du groupe, autre que son ordre, qui peuvent avoir une influence. Il est très facile d'établir un résultat complet de non 2-reconstructibilité, en effet :

Proposition 50. *Les orbites de taille 2 pour G sont reconstructibles si et seulement si $n_2 = \frac{n_1(n_1+1)}{2}$, ou n_1 et n_2 représentent respectivement les nombres d'orbites de G sur les ensembles ayant 1 ou 2 éléments.*

Cette trivialité est bien un résultat sur le groupe au sens où, d'après la formule de Pólya, si $\mathrm{Fix}(g)$ est le nombre d'éléments de Ω fixés par la

permutation g :

$$n_1 = \frac{1}{|G|} \sum_{g \in G} \mathrm{Fix}(g)$$

$$n_2 = \frac{1}{|G|} \sum_{g \in G} \left(\binom{\mathrm{Fix}(g)}{2} + \frac{\mathrm{Fix}(g^2) - \mathrm{Fix}(g)}{2} \right)$$

Pour ce genre de problème, il y a donc deux façons de profiter de la structure de digèbre :

- Vouloir montrer qu'une algèbre engendrée est une digèbre, alors en supposant que la conjecture 3 soit vraie, c'est une algèbre d'invariants.
- Profiter des relations obtenues pour obtenir de meilleurs résultats.

3.2 Graphes non orientés

3.2.1 Reconstruction par les sommets

On ne considérera que des graphes simples, qui seront de plus vus comme des sous-graphes de K_n, le graphe complet sur n sommets, dont on a numéroté les sommets de 1 à n. C'est à dire qu'on considère un graphe comme une partie des arêtes de K_n. De même, un sous-graphe d'un graphe G est une partie de l'ensemble des arêtes de G. On utilisera donc la notation $\varnothing$ pour désigner le graphe sans arête.

Si G est un graphe, on peut pour chaque sommet i de $\{1, \ldots, n\}$ considérer le graphe obtenu en retirant de G toutes les arêtes incidentes à i. L'ensemble de tous les types de graphes obtenus de cette façon à partir de G, comptés avec multiplicités est appelé le deck de G.

Conjecture 5 (Ulam)**.** *Si G est un graphe sur au moins trois sommets, alors le type de G est uniquement déterminé par son deck.*

On associe a chaque arête $\{u, v\}$ de K_n une variable $x_{\{u,v\}}$. On peut alors considérer $\mathcal{G}_n$ l'algèbre résultant du quotient de l'algèbre de polynômes sur $\binom{n}{2}$ indéterminées $\mathbb{R}[x_{\{1,2\}}, \ldots, x_{\{n-1,n\}}]$ par l'idéal engendré par les polynômes $x^2_{\{1,2\}} - x_{\{1,2\}}, x^2_{\{1,3\}} - x_{\{1,3\}}, \ldots, x^2_{\{n-1,n\}} - x_{\{n-1,n\}}$.

Il est clair que $\mathcal{G}_n$ est un $\mathbb{R}$-espace vectoriel de dimension $2^{\binom{n}{2}}$ dont une base est formée par les

$$p_G = \prod_{\{u,v\} \in E(G)} x_{\{u,v\}}, \text{ où G est un graphe}$$

.

Le groupe symétrique $\mathfrak{S}_n$ agit naturellement sur les sommets de K_n par renumérotation. Ceci induit une action sur les arêtes de K_n par $\sigma \cdot \{u, v\} = \{\sigma(u), \sigma(v)\}$. On a donc une inclusion de $\mathfrak{S}_n$ dans le groupe des permutations des arêtes, et donc une sous-digèbre $\mathcal{T}_n$ associée dans $\mathcal{G}_n$, dont les blocs sont les types de graphe à isomorphisme près.

Définition 18. *On note $\mathcal{E}_n$ l'algèbre engendrée par les polynômes correspondant aux types de graphes ayant au moins un sommet isolé.*

Proposition 51. *Les blocs de $\mathcal{E}_n$ sont formés par les graphes ayant le même deck.*

Corollaire 9. *La Conjecture 1 p7 est équivalente à $\mathcal{T}_n = \mathcal{E}_n$.*

En effet si $\mathcal{T}_n = \mathcal{E}_n$, alors tout polynôme $p_{[G]}$ correspondant à un type de graphe $[G]$ s'exprime algébriquement en fonction des polynômes correspondant aux types de graphes ayant au moins un sommet isolé. Donc si un graphe a un deck de type $[G]$, il contient le même nombre de sous-graphes isomorphes à $[G]$ qu'un élément de $[G]$, comme il a en particulier le même nombre d'arêtes, c'est donc un élément de $[G]$.

Réciproquement, si la Conjecture 1 p7 est vraie, alors la valeur $p_{[G]}(A)$ est uniquement déterminée par les valeurs $p_{[T]}(A)$, où T est un type de graphe ayant au moins un sommet isolé. On en déduit que $p_{[G]}$ s'exprime algébriquement en fonction des $p_{[T]}$, où T est un type de graphe ayant au moins un sommet isolé.

Corollaire 10. *Le type $[G]$ est reconstructible si, et seulement si $\varepsilon(p_{[G]})$ appartient à $\mathcal{E}_n$.*

Définition 19. *On note*

$$g = \sum_{i=1}^{n} \prod_{\substack{j=1 \\ j \neq i}}^{n} x_{\{i,j\}}$$

Proposition 52. *Si σ est une permutation des arêtes de K_n, alors σ est induite par une permutation des sommets si et seulement si $\sigma \cdot g = g$*

Preuve : Il est clair que si σ est induite par une permutation des sommets, alors $\sigma \cdot g = g$. Réciproquement, si $\sigma \cdot g = g$ alors σ permute les

$$e_i = \prod_{\substack{j=1 \\ j \neq i}}^{n} x_{\{i,j\}}$$

On note τ la permutation de $\{1, \ldots, n\}$ telle que $\sigma \cdot e_i = e_{\tau \cdot i}$. Alors σ est induite par τ. $\square$

Si la Conjecture 3 p30 est vraie, alors il suffirait de montrer que $\mathcal{E}_n$ est une digèbre pour prouver la conjecture d'Ulam (1 p7) : en effet il est clair que $\mathcal{E}_n$ est incluse dans $\mathcal{T}_n$. On aurait alors que $\mathcal{E}_n$ est une algèbre d'invariants. Son groupe d'automorphismes associé contient évidemment $\mathfrak{S}_n$, de plus comme g est dans $\mathcal{E}_n$, on aurait égalité.

On peut déjà dire que $\mathcal{E}_n$ est une algèbre, de plus le fait qu'un graphe et son complémentaire aient le même deck fournit la stabilité par $\varepsilon \circ \complement \circ \varepsilon^{-1}$.

On n'aurait en fait pas besoin de la Conjecture 3 p30, il suffirait de la démontrer dans ce cas particulier, c'est à dire :

Conjecture 6. *La digèbre engendrée par g est $\mathcal{T}_n$.*

Proposition 53. *La conjecture d'Ulam (1 p7) pour tout n implique la Conjecture 6 p72 pour tout n.*

Preuve : D'après la Proposition 18 p24, 1 et $\sum_{\{u,v\} \in E(G)} x_{\{u,v\}}$ sont inclus dans la digèbre engendrée par g. On va montrer par récurrence sur le nombre de sommets non-isolés de G que p_G est dans la digèbre engendrée par g.

Supposons que tous les p_G soient engendrés par g si G a au plus t-1 sommets non-isolés, et soit H un graphe ayant t sommets non-isolés. D'après la conjecture d'Ulam au rang t, dans $\mathcal{T}_t$, les p_G où G a au plus t-1 sommets non-isolés, engendrent p_H. C'est à dire que, dans $\mathcal{T}_t$, p_H s'exprime comme un polynôme en fonction des p_G, où G a au plus t-1 sommets non-isolés. La même combinaison polynomiale c des p_G où G a au plus t-1 sommets non-isolés dans $\mathcal{T}_n$ donne p_H plus une combinaison linéaire de p_U où U a plus de t sommets non-isolés. (En effet le coefficient sur p_A du produit des p_{B_i} est le même dans toute algèbre contenant ces derniers : il s'agit du nombre de façons d'écrire A comme une réunion des B_i).

Il ne reste plus qu'à constater qu'on peut "filtrer" les termes supplémentaires en :

- fabriquant le polynôme p_t correspondant au cliques de taille t grâce à des intersections,
- multipliant $\varepsilon(c)$ par $\varepsilon \circ l(p_t)$,
- appliquant ε^{-1}.

□

3.2.2 Reconstruction par les arêtes

Si G est un graphe, on peut pour chaque arête a de G considérer le graphe obtenu en retirant a de G. L'ensemble de tous les types de graphes obtenus de cette façon à partir de G, comptés avec multiplicités est appelé le deck-arête de G.

Conjecture 7 (Harary)**.** *Si G est un graphe ayant au moins quatre arêtes, alors le type de G est uniquement déterminé par son deck-arête.*

Avec les notations employées ci-dessus, il est équivalent de dire que $\partial p_G = \partial p_H$ si et seulement si H et G sont de même type, autrement dit dans un même bloc de $\mathcal{T}_n$. Ce problème s'inscrivant naturellement dans le problème général de la Définition 17, et ses résultats ayant déjà été traités, on ne le détaille pas plus.

3.3 Graphes orientés

3.3.1 Reconstruction par les sommets

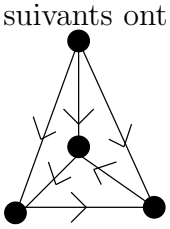
Les digraphes ne sont pas reconstructibles par les sommets : Stockmeyer [22] a exhibé une suite de contre-exemples qui montrent que les tournois ne sont pas reconstructibles par les sommets.

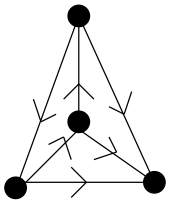
On peut regarder ce qui se passe pour les petits cas :

1. sur trois sommets : le groupe d'automorphismes est clair : il s'agit des permutations des arêtes qui préservent les paires opposées. L'algèbre

engendrée par les polynômes correspondants aux graphes sur deux sommets est donc une digèbre, mais le groupe des symétries est plus grand que celui attendu.

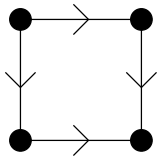
2. sur quatre sommets : l'ensemble de polynômes formé par les digraphes ayant le même deck n'est pas une digèbre, en effet s'il est bien stable par complémentaire, il ne l'est pas par dérivation. Les deux digraphes suivants ont le même deck :

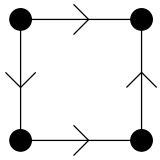




On peut vérifier qu'ils sont les seuls à avoir ce deck.

Ils ne contiennent pas de copie du premier graphe ci-dessous, mais ils contiennent tous les deux une copie du deuxième





Ces deux graphes ont pourtant aussi le même deck. Donc en dérivant le polynôme somme des deux premiers graphes, on obtient un polynôme qui contient le quatrième graphe, mais pas le troisième. On n'obtient donc pas une digèbre.

Remarque : le groupe d'automorphismes des types de digraphes sur quatre sommets dont un isolé est réduit au groupe des permutations des quatre sommets.

3.4 Digèbres engendrées par un élément

Le problème de reconstruction des graphes par les sommets présente un cas intéressant de la conjecture sur les digèbres dans le cas ou le groupe stabilisateur est celui d'un seul polynôme. On a vu que dans ce cas, la conjecture implique que la digèbre est engendrée par un élément : l'un de ses blocs. On s'intéresse dans cette section à ce cas particulier de la conjecture, c'est à dire :

Conjecture 8. *Si $\mathcal{D}$ est une digèbre engendrée par un de ses blocs, alors $\mathcal{D}$*

est une algèbre d'invariants.

On a déjà vu que la digèbre engendrée par p_A, où A est un ensemble, est bien l'algèbre des invariants pour le groupe de permutations qui stabilise A. Il est clair que cette propriété est aussi vérifiée pour deux ensembles, c'est à dire : si A et B sont deux ensembles de même cardinalité, alors la digèbre engendrée par $p_A + p_B$ est l'algèbre des invariants pour le groupe de permutations qui stabilise la paire A, B, c'est à dire la digèbre dont les blocs sont constituées d'ensembles formant une structure d'incidence donnée avec A et B ou avec B et A. En effet, ces blocs sont tout simplement les $E_\mu(p_A, p_B) + E_\mu(p_B, p_A)$ lorsque μ parcourt l'ensemble des structures d'incidence d'ordre 3. En d'autres termes, la digèbre engendrée par $p_A + p_B$ est tout simplement $\mathrm{Com}_2^1(\mathfrak{S}_n)(p_A + p_B, p_A + p_B)$.

Que se passe-t-il si A et B n'ont pas la même cardinalité ? Dans ce cas on peut facilement obtenir p_A et p_B, et le même raisonnement que ci-dessus s'applique pour donner cette fois ci l'algèbre des invariants pour le groupe de permutations qui stabilise A et B, c'est à dire la digèbre dont les blocs sont constituées d'ensemble formant une structure d'incidence donnée avec A et B.

Le cas de trois ensembles est intéressant, en effet on a vu que dans ce cas, on ne sait pas si $\mathrm{Com}_3^1(\mathfrak{S}_n)$ "stabilise" toute digèbre. On met en lumière ici la possibilité, jusqu'à maintenant ignorée, d'utiliser plusieurs fois le même élément de $\mathcal{D}$: étant donné une application h de $\mathrm{Com}_3^1(\mathfrak{S}_n)$, et trois éléments p_1, p_2, p_3 de $\mathcal{D}$, on aurait voulu montrer que $h(p_1, p_2, p_3)$ est un élément de $\mathcal{D}$.

On peut penser à construire, grâce à ∂, $\mathfrak{C}$ (c'est à dire $\mathrm{Com}(\mathfrak{S}_n)$), et la multiplication (donc au total, tout $\mathrm{Com}_2(\mathfrak{S}_n)$), une application $\hat{h}$ de $\mathrm{Com}_k(\mathfrak{S}_n)$, avec k plus grand que 3, telle que, par exemple

$$\hat{h}(p_1, p_1, p_1, p_2, p_2, p_2, p_3, p_3) = h(p_1, p_2, p_3)$$

On se place ici dans un cadre différent, mais cette idée y transparait, et vient apporter quelques arguments en faveur de la conjecture 3.

Soit donc trois ensembles A_1, A_2, et A_3 qui forment un seul bloc d'une digèbre, c'est à dire que pour toute partie J de $\{1, 2, 3\}$, le nombre

$$\left| \bigcap_{j \in J} A_j \cap \bigcap_{j \notin J} A_j^c \right|$$

ne dépend que du nombre d'éléments de J.

On pose $q = p_{A_1} + p_{A_2} + p_{A_3}$. On veut montrer que la digèbre $< q >$ engendrée par q est la sous algèbre des polynômes invariants par les permutations qui stabilisent le triplet (A_1, A_2, A_3). On peut décrire cette sous-algèbre par ses blocs qui sont formés par les sous-ensembles U de Ω qui forment une structure d'incidence donnée avec un triplet d'ensembles composé de A_1, A_2 et A_3.

Lemme 2. *$< q >$ contient les*

1. $p_{A_1 \cap A_2} + p_{A_1 \cap A_3} + p_{A_2 \cap A_3}$
2. $p_{A_1 \cap A_2^c} + p_{A_1 \cap A_3^c} + p_{A_2 \cap A_1^c} + p_{A_2 \cap A_3^c} + p_{A_3 \cap A_1^c} + p_{A_3 \cap A_2 c}$
3. $p_{A_1^c \cap A_2^c} + p_{A_1^c \cap A_3^c} + p_{A_2^c \cap A_3^c}$

Preuve :

1. $q \cap q - q = 2\left(p_{A_1 \cap A_2} + p_{A_1 \cap A_3} + p_{A_2 \cap A_3}\right)$
2. $q^c \cap q = 3 + p_{A_1 \cap A_2^c} + p_{A_1 \cap A_3^c} + p_{A_2 \cap A_1^c} + p_{A_2 \cap A_3^c} + p_{A_3 \cap A_1^c} + p_{A_3 \cap A_2 c}$
3. $q^c \cap q^c - q^c = 2\left(p_{A_1^c \cap A_2^c} + p_{A_1^c \cap A_3^c} + p_{A_2^c \cap A_3^c}\right)$

□

Lemme 3. *$< q >$ contient les*

1. $p_{A_1 \cap A_2 \cap A_3}$
2. $p_{A_1^c \cap A_2 \cap A_3} + p_{A_1 \cap A_2^c \cap A_3} + p_{A_1 \cap A_2 \cap A_3^c}$
3. $p_{A_1 \cap A_2^c \cap A_3^c} + p_{A_1^c \cap A_2 \cap A_3^c} + p_{A_1^c \cap A_2^c \cap A_3}$
4. $p_{A_1^c \cap A_2^c \cap A_3^c}$

Preuve :

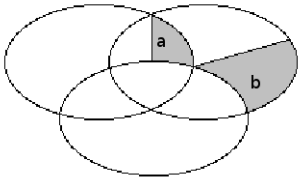
1. $q \cap q \cap q = q + 6\ p_{A_1 \cap A_2 \cap A_3} + 6\left(p_{A_1 \cap A_2} + p_{A_1 \cap A_3} + p_{A_2 \cap A_3}\right)$
2. $q^c \cap q \cap q = 4\ q + 2\left(p_{A_1^c \cap A_2 \cap A_3} + p_{A_1 \cap A_2^c \cap A_3} + p_{A_1 \cap A_2 \cap A_3^c}\right) + p_{A_1 \cap A_2^c} + p_{A_1 \cap A_3^c} + p_{A_2 \cap A_1^c} + p_{A_2 \cap A_3^c} + p_{A_3 \cap A_1^c} + p_{A_3 \cap A_2 c} + 3$
3. $q^c \cap q^c \cap q = 3 + 4\ q^c + 2\left(p_{A_1 \cap A_2^c \cap A_3^c} + p_{A_1^c \cap A_2 \cap A_3^c} + p_{A_1^c \cap A_2^c \cap A_3}\right) + p_{A_1 \cap A_2^c} + p_{A_1 \cap A_3^c} + p_{A_2 \cap A_1^c} + p_{A_2 \cap A_3^c} + p_{A_3 \cap A_1^c} + p_{A_3 \cap A_2^c}$
4. $q^c \cap q^c \cap q^c = 6\ p_{A_1^c \cap A_2^c \cap A_3^c} + 6\left(p_{A_1 \cap A_2} + p_{A_1 \cap A_3} + p_{A_2 \cap A_3}\right) + q$

□

Lemme 4. *$< q >$ contient les $r_{a,b} = \sum_U p_U$ ou la somme porte sur les U tels que :*

- $|U \cap A_{\sigma(1)}| = 0$
- $|U \cap A_{\sigma(2)} \cap A_{\sigma(3)}| = a$
- $|U \cap A_{\sigma(2)}| = b$
- $|U \cap A^c_{\sigma(2)} \cap A_{\sigma(3)}| = 0$

pour une permutation σ de $\{1, 2, 3\}$, et un entier strictement positif a.



Preuve : Un tel U est de cardinalité b. Soit h l'élément de $\mathrm{Com}_2^1(\mathfrak{S}_n)$ qui envoie une paire d'ensembles distincts X, Y de même cardinalité que les A_i et dont l'intersection est de même cardinalité que les $A_i \cap A_j$ vers la somme des ε_Z pour les ensembles Z de cardinal b tels que :

- $|U \cap X \cap Y| = a$
- $|U \cap X^c \cap Y| = b$
- $|U \cap X \cap Y^c| = 0$

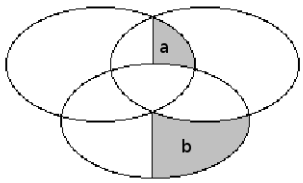
Soit l l'élément de $\mathrm{Com}(\mathfrak{S}_n)$ qui envoie un ensemble X de même cardinalité que les A_i vers la somme des ε_Z pour les ensembles Z de cardinalité b dont l'intersection avec X est vide.

Alors $\varepsilon^{-1}(l(q) \cdot h(q, q))$ fournit le polynôme recherché. $\square$

Lemme 5. *$< q >$ contient les $s_{a,b} = \sum_U p_U$ ou la somme porte sur les U tels que :*

- $|U \cap A_{\sigma(1)} \cap A_{\sigma(2)}| = 0$
- $|U \cap A_{\sigma(1)} \cap A_{\sigma(3)})| = 0$
- $|U \cap A_{\sigma(1)} \cap A^c_{\sigma(2)} \cap A^c_{\sigma(3)}| = 0$
- $|U \cap A_{\sigma(2)} \cap A^c_{\sigma(1)} \cap A^c_{\sigma(3)}| = 0$
- $|U \cap A^c_{\sigma(1)} \cap A^c_{\sigma(1)} \cap A_{\sigma(3)}| = b$
- $|U \cap A_{\sigma(1)} \cap A_{\sigma(2)} \cap A^c_{\sigma(3)}| = a$

pour une permutation σ de $\{1, 2, 3\}$.



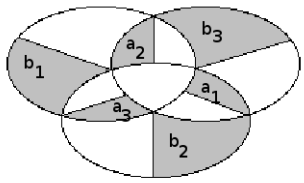
Preuve : D'après le Lemme 3 p76, $< q >$ contient $p_1 = p_{A_1^c \cap A_2 \cap A_3} + p_{A_1 \cap A_2^c \cap A_3} + p_{A_1 \cap A_2 \cap A_3^c}$ et $p_2 = p_{A_1 \cap A_2^c \cap A_3^c} + p_{A_1^c \cap A_2 \cap A_3^c} + p_{A_1^c \cap A_2^c \cap A_3}$.

Soit l_1 l'application de $\mathrm{Com}\,(\mathfrak{S}_n)$ qui envoie un ensemble X de même cardinalité que $A_1^c \cap A_2 \cap A_3$ vers la somme des p_Z pour les ensembles Z de cardinalité a inclus dans X, et l_2 l'application de $\mathrm{Com}\,(\mathfrak{S}_n)$ qui envoie un ensemble X de même cardinalité que $A_1^c \cap A_2^c \cap A_3$ vers la somme des p_Z pour les ensembles Z de cardinalité b inclus dans X. Alors $l_1(p_1) \cap l_2(p_2) = r_{a,b} + s_{a,b}$. □

Lemme 6. *$< q >$ contient les $w_{a_1,a_2,a_3,b_1,b_2,b_3} = \sum_U p_U$ ou la somme porte sur les U tels que :*

- $|U \cap A_1 \cap A_2 \cap A_3| = 0$
- $|U \cap A_{\sigma(1)}^c \cap A_{\sigma(2)} \cap A_{\sigma(3)}| = a_1$
- $|U \cap A_{\sigma(1)} \cap A_{\sigma(2)}^c \cap A_{\sigma(3)}| = a_2$
- $|U \cap A_{\sigma(1)} \cap A_{\sigma(2)} \cap A_{\sigma(3)}^c| = a_3$
- $|U \cap A_{\sigma(1)} \cap A_{\sigma(2)}^c \cap A_{\sigma(3)}^c| = b_1$
- $|U \cap A_{\sigma(1)}^c \cap A_{\sigma(2)} \cap A_{\sigma(3)}^c| = b_2$
- $|U \cap A_{\sigma(1)}^c \cap A_{\sigma(2)}^c \cap A_{\sigma(3)}| = b_3$
- $|U \cap A_1^c \cap A_2^c \cap A_3^c| = 0$

pour une permutation σ de $\{1, 2, 3\}$.



Preuve : On a

$$s_{a_1,b_1} \cdot s_{a_2,b_2} = \sum_{i,j} \binom{i}{a_1, a_2} \binom{j}{b_1, b_2} q_{i,j} + w_{a_1,a_2,0,b_1,b_2,0}$$

Ou $\binom{s}{t,u}$ est le nombre de façon de décomposer un ensemble à s éléments en union d'un ensemble à t élément et d'un ensemble à u éléments.
De la même façon :

$$\begin{aligned} s_{a_1,b_1} \cdot s_{a_2,b_2} \cdot s_{a_3,b_3} &= \sum_{i,j} \binom{i}{a_1, a_2, a_3} \binom{j}{b_1, b_2, b_3} q_{i,j} \\ &+ \sum_{i,j} \binom{i}{a_1, a_2} \binom{j}{b_1, b_2} w_{i,a_3,0,j,b_3,0} \\ &+ \sum_{i,j} \binom{i}{a_1, a_3} \binom{j}{b_1, b_3} w_{i,a_2,0,j,b_2,0} \\ &+ \sum_{i,j} \binom{i}{a_2, a_3} \binom{j}{b_2, b_3} w_{i,a_1,0,j,b_1,0} \\ &+ w_{a_1,a_2,a_3,b_1,b_2,b_3} \end{aligned}$$

□

Proposition 54. *La digèbre $< q >$ engendrée par q est la sous algèbre des polynômes invariants par les permutations qui stabilisent le triplet (A_1, A_2, A_3), c'est à dire $< q >$ contient les $\sum_U p_U$ ou la somme porte sur les U tels que :*

- $|U \cap A_1 \cap A_2 \cap A_3| = a_0$
- $|U \cap A^c_{\sigma(1)} \cap A_{\sigma(2)} \cap A_{\sigma(3)}| = a_1$
- $|U \cap A_{\sigma(1)} \cap A^c_{\sigma(2)} \cap A_{\sigma(3)}| = a_2$
- $|U \cap A_{\sigma(1)} \cap A_{\sigma(2)} \cap A^c_{\sigma(3)}| = a_3$
- $|U \cap A_{\sigma(1)} \cap A^c_{\sigma(2)} \cap A^c_{\sigma(3)}| = b_1$
- $|U \cap A^c_{\sigma(1)} \cap A_{\sigma(2)} \cap A^c_{\sigma(3)}| = b_2$
- $|U \cap A^c_{\sigma(1)} \cap A^c_{\sigma(2)} \cap A_{\sigma(3)}| = b_3$
- $|U \cap A^c_1 \cap A^c_2 \cap A^c_3| = b_0$

pour une permutation σ de $\{1, 2, 3\}$.

Preuve : Soit l_0 l'application de $\mathrm{Com}\,(\mathfrak{S}_n)$ qui envoie un ensemble X de même cardinalité que $A_1 \cap A_2 \cap A_3$ vers la somme des p_Z pour les ensembles Z de cardinalité a_0 inclus dans X, et m_0 l'application de $\mathrm{Com}\,(\mathfrak{S}_n)$ qui envoie un ensemble X de même cardinalité que $A^c_1 \cap A^c_2 \cap A^c_3$ vers la somme des p_Z pour les ensembles Z de cardinalité b_0 inclus dans X. Alors

$$l_0\left(p_{A_1 \cap A_2 \cap A_3}\right) \cdot m_0\left(p_{A^c_1 \cap A^c_2 \cap A^c_3}\right) \cdot w_{a_1,a_2,a_3,b_1,b_2,b_3}$$

est le polynôme recherché. On remarquera pour conclure qu'on a utilisé au total 36 fois q pour pouvoir obtenir un élément quelconque de la digèbre engendrée. □

Remarque 16. *Dans le cas des graphes, on veut montrer que la digèbre est engendrée par un élément, lequel provient d'un bloc dont trois éléments distincts ont toujours une intersection nulle. Cette propriété remarquable n'aide pourtant pas vraiment à la simplification du calcul.*

FIN

Annexe A

Digèbres de petits ordres

A.1 Digèbres simples

Il est facile de produire des digèbres par produit direct :

Proposition 55. *Si $\mathcal{D}$ et $\mathcal{E}$ sont deux digèbres d'ordres respectifs n et m, on définit la digèbre produit d'ordre $n+m$ en posant :*

$$\mathcal{D} \otimes \mathcal{E} = \langle \nu(p) \cdot \tau(q), \quad p \in \mathcal{E}, \;\; q \in \mathcal{F} \rangle_{\mathbb{R}}$$

ou

- *ν est l'unique homomorphisme de digèbre de $\mathcal{S}_n$ dans $\mathcal{S}_{m+n}$ qui envoie x_i sur x_i.*
- *τ est l'unique homomorphisme de digèbre de $\mathcal{S}_m$ dans $\mathcal{S}_{m+n}$ qui envoie x_i sur x_{n+i}.*

Preuve : En procédant de cette manière, on obtient bien une digèbre, en effet, pour tout élément p de $\mathcal{E}$ et tout élément q de $\mathcal{F}$,

- $\partial\left(\nu(p) \cdot \tau(q)\right) = \nu \circ \partial(p) \cdot \tau(q) + \nu(p) \cdot \tau \circ \partial(q)$
- $\mathsf{C}\left(\nu(p) \cdot \tau(q)\right) = \nu \circ \mathsf{C}(p) \cdot \tau \circ \mathsf{C}(q)$

□

Il est facile d'obtenir la matrice de coefficients de $\mathcal{D} \otimes \mathcal{E}$ en fonction de celles de $\mathcal{D}$ et $\mathcal{E}$, en effet les blocs de $\mathcal{D} \otimes \mathcal{E}$ sont en bijection évidente avec les éléments du produit cartésien de ceux de $\mathcal{D}$ et de $\mathcal{E}$. Dans le cas ou $\mathcal{D}$ et $\mathcal{E}$

sont des algèbres d'invariants, $\mathcal{D} \otimes \mathcal{E}$ est l'algèbre des invariants du "produit cartésien" de $Aut(\mathcal{D})$ par $Aut(\mathcal{E})$.

Les digèbres produit se décomposant facilement, on est donc amené a ne considérer que les digèbres indécomposables, qui seront naturellement affublées de l'attribut simple.

Définition 20. *Une digèbre $\mathcal{D}$ d'ordre n est dite* décomposable *s'il existe une partition non triviale (V_1, V_2) de $\{1, \ldots, n\}$ telle que*

- *V_1 (donc V_2) est le seul élément de son bloc (il est "stable").*
- *Si $\mathcal{B}_{V_1}$ est l'ensemble des blocs de $\mathcal{D}$ dont tous les éléments sont inclus dans V_1 (et respectivement pour $\mathcal{B}_{V_2}$), alors les blocs de $\mathcal{D}$ sont les :*

$$\{U \cup V, \quad U \in B_1,\ V \in B_2\}, \quad B_1 \in \mathcal{B}_{V_1},\ B_2 \in \mathcal{B}_{V_2}$$

dans le cas contraire, elle est dite simple.

Proposition 56. *L'indice de reconstructibilté de $\mathcal{D} \otimes \mathcal{E}$ est égal au maximum des indices de reconstructibilité de $\mathcal{D}$ et de $\mathcal{E}$.*

Pour clore ce travail, on présente la liste des algèbres d'invariants de petits ordres accompagnées de leurs matrices de coefficients, ainsi que des cardinaux des orbites non reconstructibles. Cette liste a été construite facilement grâce au logiciel gap.

A.2 Algèbres d'invariants d'ordre 1

Il n'y en a qu'une seule : celle du groupe trivial, dont la matrice est [1].

A.3 Algèbres d'invariants d'ordre 2

Il y en a deux :

- celle du groupe trivial, dont la matrice est $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$, qui n'est pas simple.

- celle du groupe symétrique à deux éléments, dont la matrice est $\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 2 & 1 \end{bmatrix}$ qui est simple.

A.4 Algèbres d'invariants d'ordre 3

Il y a trois algèbres d'invariants, dont une est simple :

Group([(1,2,3)])
Group([(1,3,2), (1,2)]) [1]

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{bmatrix}$$

{}
{1},{2},{3}
{1,2},{2,3},{1,3}
{1,2,3}

A.5 Algèbres d'invariants d'ordre 4

Il y a huit algèbres d'invariants, dont quatre sont simples :

Group([(1,3)(2,4)]) [1, 2]

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 2 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 2 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 2 & 2 & 2 & 1 & 2 & 1 & 2 & 2 & 1 \end{bmatrix}$$

{}
{1},{3}
{2},{4}
{1,2},{3,4}
{1,3}
{1,4},{2,3}
{2,4}
{1,2,3},{1,3,4}
{1,2,4},{2,3,4}
{1,2,3,4}

Group([(1,4)(2,3), (1,3)(2,4)]) [1, 2]

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 1 & 0 & 0 \\ 1 & 3 & 1 & 1 & 1 & 1 & 0 \\ 1 & 4 & 2 & 2 & 2 & 4 & 1 \end{bmatrix}$$

{}
{1},{4},{3},{2}
{1,2},{3,4}
{1,3},{2,4}
{1,4},{2,3}
{1,2,3},{2,3,4},{1,3,4},{1,2,4}
{1,2,3,4}

Group([(1,2)(3,4), (1,3,2,4)])
Group([(1,3)(2,4), (1,4)(2,3), (1,2)]) [1, 2]

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 & 0 \\ 1 & 3 & 1 & 2 & 1 & 0 \\ 1 & 4 & 2 & 4 & 4 & 1 \end{bmatrix}$$

{}
{1},{2},{3},{4}
{1,2},{3,4}
{1,3},{2,4},{2,3},{1,4}
{1,2,3},{1,2,4},{2,3,4},{1,3,4}
{1,2,3,4}

Group([(1,3)(2,4), (1,4)(2,3), (2,4,3)])
Group([(1,3)(2,4), (1,4)(2,3), (2,4,3), (1,2)]) [1]

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 \\ 1 & 3 & 3 & 1 & 0 \\ 1 & 4 & 6 & 4 & 1 \end{bmatrix}$$

{}
{1},{3},{2},{4}
{1,2},{3,4},{1,4},{2,3},{1,3},{2,4}
{1,2,3},{1,3,4},{1,2,4},{2,3,4}
{1,2,3,4}

A.6 Algèbres d'invariants d'ordre 5

Il y a onze algèbres d'invariants, dont deux sont simples :

Group([(1,2,3,4,5)])
Group([(1,2,3,4,5), (2,5)(3,4)]) [1, 2]

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 3 & 2 & 1 & 1 & 0 & 0 & 0 \\ 1 & 3 & 1 & 2 & 0 & 1 & 0 & 0 \\ 1 & 4 & 3 & 3 & 2 & 2 & 1 & 0 \\ 1 & 5 & 5 & 5 & 5 & 5 & 5 & 1 \end{bmatrix}$$

{}
{1},{2},{3},{4},{5}
{1,2},{2,3},{3,4},{4,5},{1,5}
{1,3},{2,4},{3,5},{1,4},{2,5}
{1,2,3},{2,3,4},{3,4,5},{1,4,5},{1,2,5}
{1,2,4},{2,3,5},{1,3,4},{2,4,5},{1,3,5}
{1,2,3,4},{2,3,4,5},{1,3,4,5},{1,2,4,5},{1,2,3,5}
{1,2,3,4,5}

Group([(1,2,3,4,5), (2,5)(3,4), (2,3,5,4)])
Group([(1,2,3,4,5), (3,4,5)])
SymmetricGroup([1 .. 5]) [1]

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 \\ 1 & 3 & 3 & 1 & 0 & 0 \\ 1 & 4 & 6 & 4 & 1 & 0 \\ 1 & 5 & 10 & 10 & 5 & 1 \end{bmatrix}$$

{}
{1},{2},{3},{5},{4}
{1,2},{2,3},{1,5},{1,3},{3,4},{4,5},{3,5},{1,4},{2,4},{2,5}
{1,2,3},{2,3,4},{1,4,5},{1,3,5},{3,4,5},{2,3,5},{1,2,5},{1,2,4},{2,4,5},{1,3,4}
{1,2,3,4},{2,3,4,5},{1,3,4,5},{1,2,3,5},{1,2,4,5}
{1,2,3,4,5}

A.7 Algèbres d'invariants d'ordre 6

Il y a trente cinq algèbres d'invariants, dont dix neuf sont simples :

Group([(1,2)(3,4)(5,6)])	[1, 2]
Group([(1,2,3)(4,5,6)])	[1, 2]
Group([(3,4)(5,6), (1,2)(5,6)])	[1, 3]
Group([(3,4)(5,6), (1,2)(3,5,4,6)])	[1, 2, 3]
Group([(3,4)(5,6), (1,2)(3,5)(4,6)])	[1, 2]
Group([(5,6), (1,2)(3,4)])	[1, 2]
Group([(1,2,3)(4,5,6), (1, 4)(2, 6)(3, 5)])	[1, 2]
Group([(1,2,3)(4,5,6), (2,3)(5,6)])	[1, 2]
Group([(1,2)(3,4)(5,6), (1,3,5)(2,4,6)])	[1, 2, 3]
Group([(5,6), (3,4), (1,2)(3,5)(4,6)])	[1, 2]
Group([(3,4)(5,6), (3,5)(4,6), (1,2)(5,6)])	[1, 2, 3]
Group([(3,4)(5,6), (1,2)(5,6), (1,3,5)(2,4,6)])	[1, 2, 3]
Group([(1,2)(3,4)(5,6), (1,3,5)(2,4,6), (3,5)(4,6)])	[1, 2]
Group([(4,5,6), (1,2,3), (1, 4)(2, 5)(3, 6)]) Group([(4,5,6), (1,2,3), (2,3)(5,6), (1, 4)(2, 5)(3, 6)]) Group([(4,5,6), (1,2,3), (2,3)(5,6), (1,4)(2,5,3,6)]) Group([(4,5,6), (4,6), (1,2,3), (2,3), (1, 4)(2, 5)(3, 6)])	[1, 2]
Group([(5,6), (3,4), (1,2), (1,3,5)(2,4,6)])	[1, 2, 3]

Group([(3,4)(5,6), (1,2)(5,6), (1,3,5)(2,4,6), (3,5)(4,6)])	[1, 2, 3]
Group([(3,4)(5,6), (1,2)(5,6), (1,3,5)(2,4,6), (3,5,4,6)]) Group([(5,6), (3,4), (1,2), (1,4,5)(2,3,6), (3,5)(4,6)])	[1, 2]
Group([(1,2,3,4,6), (1,4)(5,6)])	[1, 3]
Group([(1,5,3,6,4), (1,6)(2,4), (3,4,6,5)]) Group([(1,2,3,4,5), (4,5,6)]) SymmetricGroup([1 .. 6])	[1]

A.8 Algèbres d'invariants d'ordre 7

Il y a cinquante et une algèbres d'invariants, dont dix sont simples :

Group([(5,6,7), (1,2)(3,4)]) Group([(5,6,7), (1, 2)(3, 4)(6, 7)]) Group([(5,7,6), (6,7), (1,2)(3,4)])	[1, 2]
Group([(1,2,3,4,5,6,7)])	[1, 2, 3]
Group([(4,5)(6,7), (4,6)(5,7), (1,2,3)(5,6,7)])	[1, 3]
Group([(1,2,3,4,5,6,7), (2, 7)(3, 6)(4, 5)])	[1, 2]
Group([(3,4,5,6,7), (4,7)(5,6), (1,2)(4,5,7,6)])	[1, 3]
Group([(1,2,3,4,5,6,7), (2,3,5)(4,7,6)])	[1, 3]
Group([(4,5)(6,7), (4,6)(5,7), (1,2,3)(5,6,7), (2,3)(6,7)])	[1, 3]
Group([(1,2,3,4,5,6,7), (2,3,5)(4,7,6), (2, 7)(3, 6)(4, 5)])	[1, 3]
Group([(1,2,3,4,5,6,7), (1,2)(3,6)])	[1, 3]

Group([(1,2,3,4,5,6,7), (5,6,7)])
SymmetricGroup([1 .. 7]) [1]

A.9 Algèbres d'invariants d'ordre 8

Il y a 168 algèbres d'invariants, dont 86 sont simples. Parmi elles, on trouve :

Group([(5,6)(7,8), (3,4)(7,8), (3,5,7)(4,6,8), (5,7)(6,8), (1,2)(7,8)]) [1,2,4]

Group([(7,8), (5,6), (3,4), (3,6,7)(4,5,8), (1, 2)(5, 7)(6, 8)]) [1,2,4]

et

Group([(7,8), (5,6), (3,4), (3,6,7)(4,5,8), (1,2)]) [1,2,3]

Group([(7,8), (3,4)(5,6), (1,2)(5,6), (1,3,5)(2,4,6), (3,5)(4,6)]) [1,2,3]

qui sont les deux seuls couples d'algèbres d'invariants non isomorphes par une permutation de $\mathfrak{S}_8$ ayant même matrice de coefficients.

On remarque aussi par exemple, pour son manque de reconstructibilité :

Group([(5,6)(7,8), (1,2)(3,4), (1, 3, 2, 4)(5, 7, 6, 8)]) [1,2,3,4]

Index

$*$-algèbre, 37
G-hypomorphes, 67
G-isomorphes, 67
G-reconstructible, 67
$\mathcal{S}_n$, 13
ε-algèbre, 52

bicommutant, 37
bloc, 26

Cameron, 67
complémentation, 17

dérivation, 16
digèbre, 18
digèbre décomposable, 82
digèbre engendrée, 25
digèbre simple, 82

ensemble des invariants, 16

homomorphisme de digèbre, 29

invariants, 16

Lovász, 59

Müller, 67

sous-algèbre d'invariants, 16
structure d'incidence, 31
système de blocs, 27

Bibliographie

[1] J.A.Bondy, A graph reconstructor's manual. *Surveys in Combinatorics* (1991) **166** 221-252

[2] J.A.Bondy U.S.R.Murty, Graph Theory. *Graduate Texts in Mathematics* **244** Springer (2007)

[3] P.J.Cameron, Transitivity of finite permutation groups on unordered sets.*Mathematische Zeitschrift* **148** (1976) 127-139

[4] P.J.Cameron, Stories from the age of reconstruction.*Congressus Numerantium* **113** (1996) 31-41

[5] F.Harary, On the reconstruction of a graph from a collection of subgraphs. *Theory of graphs and its applications* (1964)

[6] P.J.Kelly, On isometric Transformations. *Ph.D. thesis, University of Wisconsin*, (1942)

[7] P.J.Kelly, A congruence theorem for trees, *Pacific J. Math.* **7** (1957) 961-968

[8] W.L.Kocay, On reconstructing spanning subgraphs. *Ars Combin.*, **11** (1981) 301-313

[9] W.L.Kocay, Some new methods in reconstruction theory. *Combin. Math.* **IX** (Brisbane 1981) 89-114

[10] D.Livingstone A.Wagner, Transitivity of finite permutation groups on unordered sets. *Mathematische Zeitschrift* **90** (1965) 393-403

[11] L.Lovász, A note on the line reconstruction problem. *J. Combin. Theory Ser. B* **13** (1972) 309-310

[12] V.B.Mnukhin, The k-orbit reconstruction and the orbit algebra. *Acta Applic. Math.* **29** (1992) 83-117

[13] V.B.Mnukhin, The k-orbit reconstruction for Abelian and Hamiltonian Groups. *Acta Applic. Math.* **52** (1998) 149-162

[14] V.B.Mnukhin, An introduction to Möbius algebras. *Tempus Lecture notes* **11**

[15] V.B.Mnukhin I.J.Siemons, On the Livingstone-Wagner Theorem. *Electronic Journal of Combinatorics*, **11** (2004) R29

[16] V.Müller, The edge reconstruction hypothesis is true for graphs with more then $n \log_2 n$ edges. *J. Combin. Theory Ser. B* **22** (1977) 281-283

[17] M.Pouzet, Application d'une propriété combinatoire des parties d'un ensemble aux groupes et aux relations.*Mathematische Zeitschrift* **150** (1976) 117-134

[18] M.Pouzet R.Fraïssé, Cours de logique mathématique t.1. Paris : Gauthier-Villars (1971)

[19] A.Schrijver L.Lovász M.H.Freedman, Reflection positivity, rank connectivity, and homomorphisms of graphs. *Journal of the AMS* **20** (2007) 37-51

[20] A.Schrijver, Tensor subalgebras and first fundamental theorems in invariant theory. *Journal of Algebra* **319** (2008) 11305-1319

[21] J.Siemons, On partitions and permutation groups on unordered sets. *Archiv der Mathematik* **38** (1982) 391-403

[22] P.K.Stockmeyer, A census of nonreconstructible digraphs.I. Six related families. *J.Combin.theory Ser. B* (1981) **31** 232-239

[23] B.D.Thatte, Kocay's Lemma, Whitney's Theorem, and some Polynomial Invariant Reconstruction Problems. *Electronic Journal of Combinatorics*, **12** (2005) R63

[24] N.Thiéry, Invariants algébriques de graphes et reconstruction. Une étude expérimentale. *Thèse numero 167-99*, 15 juin 1999

[25] N.Thiéry M.Pouzet, Invariants algébriques de graphes et reconstruction. *C. R. Acad. Sci. Paris Sér. I Math.* **333**(**9**) (2001) 821-826

[26] S.M.Ulam, A Collection of Mathematical Problems. Wiley (Interscience), New York (1960) **29**