GROUPE DES PERMUTATIONS D'UN ENSEMBLE FINI : APPLICATIONS

par

Pascal Boyer

Table des matières

1. Le groupe symétrique

Prérequis : action d'un groupe sur un ensemble

1.1. Définition et premières propriétés. —

Définition 1.1. — L'ensemble des bijections de l'ensemble $\{1, \cdots, n\}$ muni de la loi de composition est un groupe noté $\mathfrak{S}_n$ appelé le groupe symétrique d'ordre n ; ses éléments sont appelés des permutations.

Remarque : pour E un ensemble fini de cardinal, toute bijection de E sur $\{1, \cdots, n\}$, induit un isomorphisme du groupe $\mathfrak{S}(E)$ des bijections de E dans E, sur $\mathfrak{S}_n$.

Lemme 1.2. — *Le cardinal de $\mathfrak{S}_n$ est égal à $n!$.*

Remarque : il n'est pas raisonnable d'espérer comprendre « parfaitement » le groupe $\mathfrak{S}_n$; en effet d'après le théorème de Cayley, en faisant opérer tout groupe G sur lui-même par translation à gauche, G s'identifie à un sous groupe de $\mathfrak{S}_{|G|}$. Un argument plus convaincant pour justifier l'étude plus précise des $\mathfrak{S}_n$ est l'heuristique suivante : pour comprendre un groupe G, il est en général très instructif de le faire agir sur un ensemble E, i.e. de construire un morphisme $G \to \mathfrak{S}(E)$ c'est même parfois seulement comme cela que le groupe G est défini.

Définition 1.3. — Les orbites de l'action du groupe engendré par σ sur $\{1, \cdots, n\}$, sont appelés ses cycles ; si $1 \leq k \leq n$ appartient à un cycle de longueur > 1, on dit qu'il appartient au support de σ. Si le support de σ est constitué d'un unique cycle de cardinal m, on dit que σ est un m-cycle.

Remarque : autrement dit le support d'une permutation σ est l'ensemble des k tels que $\sigma(k) \neq k$. Les dérangements sont les permutations de support maximal, i.e. $\{1, \cdots, n\}$; ce sont en quelque sorte les permutations les plus compliquées celles que l'on ne peut pas identifier avec une permutation d'ordre strictement plus petit. A l'opposé, les permutations les plus simples sont les 2-cycles que l'on appelle les transpositions.

Théorème 1.4. — *Toute permutation $\sigma \in \mathfrak{S}_n$ peut s'écrire comme la composée de cycles à supports disjoints. Cette décomposition est unique au sens où l'ordre de composition de ces cycles est indifférent. Les supports de ces cycles correspondent aux orbites de σ.*

Remarque : le résultat précédent s'appelle *la décomposition à supports disjoints* d'une permutation. En particulier en utilisant que l'ordre d'un m-cycle est m et la commutation de deux cycles à supports disjoints, on en déduit que l'ordre de σ est égal au ppcm des cardinaux de ses orbites.

Proposition 1.5. — *(cf.* [**5**]*) Notons D_n le nombre de dérangements de $\mathfrak{S}_n$; on a alors les propriétés suivantes :*
(i) $\sum_{k=0}^{n} \binom{k}{n} D_{n-k} = n!$;
(ii) $D_n = n! \Big(\sum_{k=0}^{n} \frac{(-1)^k}{k!} \Big)$;
(iii) la série génératrice $\sum_{k \geq 0} \frac{D_k z^k}{k!}$ *est égale à* $\frac{e^{-z}}{1-z}$*, son rayon de convergence est e ;*
(iv) $D_k = \lfloor \frac{k!}{e} + \frac{1}{2} \rfloor$;
(v) $D_{n+1} = n(D_n + D_{n-1})$;
(vi) $D_n = nD_{n-1} + (-1)^n$.

Preuve : La première relation découle directement de la partition de $\mathfrak{S}_n$ selon le cardinal du support ; la relation (ii) en découle alors directement ou se prouve en utilisant la formule du crible à l'égalité
$$D_n = n! - \sharp\Big(\bigcup_{i=1}^n U_i\Big)$$
où U_i désigne le sous-ensemble de $\mathfrak{S}_n$ des permutations fixant i.

La relation (iii) se prouve en utilisant (i) ou alors directement par une preuve purement de combinatoire algébrique. L'égalité (iv) découle de
$$\frac{k!}{e} + \frac{1}{2} = D_k + \frac{1}{2} + k!R_k, \qquad R_k = \sum_{n=k+1}^{+\infty} \frac{(-1)^n}{n!}$$
et de la minoration des séries alternées $|R_k| \leq \frac{1}{(k+1)!}$.

La relation de récurrence (v) se prouve comme suit : soit l'orbite de $n+1$ est de cardinal 2 ce qui donne nD_{n-1} possibilité pour un tel dérangement et sinon nD_n. La dernière relation se prouve à partir de (v) par récurrence ou peut se montrer purement combinatoirement mais de manière détournée pour l'instant. □

Exercice 1.1. — *Un paysan a $2n+1$ vaches telles, l'une quelconque de ses vaches étant mises de côté, il peut répartir les $2n$ restantes en deux sous-troupeaux de même poids total. Montrez que toutes les vaches ont le même poids.*

Proposition 1.6. — *Soit $c \in \mathfrak{S}_n$ un m-cycle ; pour tout $r \in \mathbb{N}$, la décomposition à support disjoints de c^r admet $m \wedge r$-cycles tous de longueur $\frac{m}{m\wedge r}$. Une permutation $\sigma \in \mathfrak{S}_n$ commute avec c si et seulement elle s'écrit sous la forme $c^r \circ \sigma'$ où le support de σ' est disjoints de celui de c.*

Remarque : le commutant de c en tant que sous-groupe de $\mathfrak{S}_n$ est ainsi isomorphe à $\mathbb{Z}/m\mathbb{Z} \times \mathfrak{S}_{n-m}$.

Proposition 1.7. — *(cf. [**10**]) Pour $n \neq 6$, les automorphismes de $\mathfrak{S}_n$ sont intérieurs.*

1.2. Générateurs. — Si on cherche les générateurs les plus simples possibles, on se tourne vers les transpositions et on peut montrer les résultats suivants :

(i) les transpositions engendrent $\mathfrak{S}_n$;

(ii) les transpositions $(i\ i+1)$ engendrent $\mathfrak{S}_n$;

(iii) les transpositions $(1\ i)$ engendrent $\mathfrak{S}_n$.

Dans les deux derniers cas, on remarque qu'on ne peut pas enlever des transpositions : si (iii) on enlève $(1\ k)$ alors toute permutation dans le groupe engendré par les autres laisse k invariant ; dans (ii) ce sont les sous-ensembles $[1,k]$ et $[k+1,n]$ qui sont stables. On peut en fait montrer le résultat suivant.

Proposition 1.8. — *(cf. [**3**]) Soit $\{\tau_1, \cdots, \tau_r\}$ un ensemble de transpositions qui engendrent $\mathfrak{S}_n$, alors $r \geq n-1$.*

Remarque : si on s'autorise à prendre d'autres permutations, on note que $(1\ 2)$ et $(1\ 2 \cdots n)$ engendrent $\mathfrak{S}_n$; évidemment comme $\mathfrak{S}_n$ n'est pas commutatif pour $n \geq 3$, on ne peut pas trouver un seul générateur.

Présentation par générateurs et relations : soit G_n le groupe engendré $x_1, \cdots, x_{n-1}$ et soumis aux relations :

$$\begin{aligned} x_i^2 = 1 & \qquad 1 \leq i \leq n-1 \\ (x_i x_{i+1})^3 = 1 & \qquad 2 \leq i \leq n-2 \\ (x_i x_j)^2 = 1 & \qquad |i-j| > 1. \end{aligned}$$

Proposition 1.9. — *(cf. [**13**]) Pour tout $1 \leq i \leq n-1$, soit $a_i = (i, i+1)$ la transposition de $\mathfrak{S}_n$. Alors l'application $< x_1, \cdots, x_{n-1} > \to \mathfrak{S}_n$ qui à x_i associe a_i, induit une bijection de G sur $\mathfrak{S}_n$.*

Remarque : autrement dit dans un language plus savant, $\mathfrak{S}_n$ est un *Groupes de Coxeter*, i.e. un groupe ayant une présentation du type $< r_1, \cdots, r_n \mid (r_i r_j)^{m_{i,j}} >$ où $(m_{i,j})_{1 \leq i,j \leq n}$ est une matrice symétrique à valeurs dans $\mathbb{N} \cup \{\infty\}$ avec $m_{i,i} = 1$ (i.e. les générateurs sont d'ordre 2) et $m_{i,j} \geq 2$ pour $i \neq j$: la condition $(r_i r_j)^\infty$ signifie par convention qu'aucune relation n'est imposée entre r_i et r_j.

1.3. Classes de conjugaisons. — Une question usuelle dans l'étude d'un groupe est de comprendre ses classes de conjugaison, autrement dit en language savant, les orbites de l'action du groupe sur lui-même par conjugaison. Dans le cas du groupe symétrique la question est réglée par la décomposition en cycles à support disjoints via la formule

$$\sigma \circ (a_1 \ \cdots \ a_r) \circ \sigma^{-1} = (\sigma(a_1) \ \cdots \ \sigma(a_r)).$$

Proposition 1.10. — *Deux permutations de $\mathfrak{S}_n$ sont conjuguées si et seulement si elles ont le même nombre de cycles de longueur donnée, dans l'écriture de leur décomposition en cycles à supports disjoints*

Remarque : la formule précédente permet de montrer aisément que, pour $n \geq 3$, le centre de $\mathfrak{S}_n$ est réduit à l'identité. Selon le même principe si f est un morphisme de groupes de $\mathfrak{S}_n$ dans $\mathbb{C}^\times$ alors toutes les transpositions ont même image car elles sont toutes conjuguées, ainsi il y a au plus un caractère non trivial, i.e. une représentation de dimension 1, $\mathfrak{S}_n \to GL_1(\mathbb{C})$. Il reste alors à la construire.
Construction de la signature : il y a essentiellement trois façons de la définir.

- la première en imposant $\epsilon(\tau) = -1$ pour toute transposition τ puis $\epsilon(\sigma) = (-1)^r$ où σ peut s'écrire en produit de r transpositions. Il s'agit alors de vérifier que la parité de r ne dépend que de σ, par contre ainsi définie ϵ est clairement un morphisme.
- La deuxième est d'utiliser la décomposition en cycles à supports disjoints et d'imposer $\epsilon(\sigma) = (-1)^{n-L(\sigma)}$ où $L(\sigma)$ est le nombre d'orbites : cette fois ci ϵ est bien définie par contre il faut vérifier que c'est bien un morphisme.
- Enfin la troisième et la meilleure est de poser $\epsilon(\sigma) = \prod_{i<j} \frac{\sigma(j)-\sigma(i)}{j-i}$ (parfois on dit que $\epsilon(\sigma) = (-1)^s$ où s est le nombre d'inversions i.e. de couples $i < j$ tels que $\sigma(i) > \sigma(j)$) : ϵ est bien définie et clairement un morphisme.

Définition 1.11. — Le noyau de la signature est un sous-groupe distingué $\mathcal{A}_n$ dit alterné ; il est de cardinal $\frac{n!}{2}$.

Proposition 1.12. — *La classe de conjugaison dans $\mathfrak{S}_n$ d'un élément $\sigma \in \mathcal{A}_n$ donne deux classes de conjugaison de $\mathcal{A}_n$ (resp. une unique classe de conjugaison) si et seulement si le commutateur de σ est contenu dans $\mathcal{A}_n$ (resp. sinon).*

Preuve : Tout repose sur la remarque triviale suivante : soient $\tau \in \mathfrak{S}_n - \mathcal{A}_n$ avec $\sigma' = \tau \circ \sigma \circ \tau^{-1}$. Alors il existe $\rho \in \mathcal{A}_n$ tel que $\sigma' = \rho \circ \sigma \circ \rho^{-1}$ si et seulement si $\tau^{-1} \circ \rho$ appartient au commutant de σ ; on conclut alors aisément. □

Remarque : le commutateur de $\sigma \in \mathcal{A}_n$ est contenu dans $\mathcal{A}_n$ si et seulement si les longueurs des cycles dans la décomposition en cycles à supports disjoints sont tous impairs sans multiplicité. En effet si c est un tel cycle de longueur paire alors il appartient au commutant et n'appartient pas à $\mathcal{A}_n$; si $c_1 = (a_1 \cdots a_{2r+1})$ et $c_2 = (b_1 \cdots b_{2r+1})$ sont deux tels cycles distincts alors $(a_1 b_1) \circ \cdots \circ (a_{2r+1} b_{2r+1})$ appartient au commutant et pas à $\mathcal{A}_n$.

1.4. Quelques propriétés sur le groupe alterné. — Commençons par les générateurs.

Proposition 1.13. — *Pour $n \geq 3$, $\mathcal{A}_n$ est engendré par les 3-cycles.*

Corollaire 1.14. — *Le centre de $\mathcal{A}_n$ est réduit à l'identité pour $n \geq 3$.*

Exercice 1.2. — *Pour $n \geq 5$, quels sont les caractères de $\mathcal{A}_n$?*

En ce qui concerne une présentation par générateurs et relations, soit G'_n le groupe engendré par les générateurs $x_1, \cdots x_{n-2}$ soumis aux relations :

$$x_1^3 = x_i^2 = 1 \qquad 2 \leq i \leq n-2$$

$$(x_i x_{i+1})^3 = 1 \qquad 1 \leq i \leq n-3$$

$$(x_i x_j)^2 = 1 \qquad |i-j| > 1.$$

Pour $n = 3$, on a déjà vu que $G'_3 \simeq \mathbb{Z}/3\mathbb{Z} \simeq \mathcal{A}_3$. Supposons donc $n \geq 4$.

Proposition 1.15. — *Soient $a_1 = (1,2,3)$ et $a_i = (1,2)(i+1, i+2)$ pour $2 \leq i \leq n-2$ les permutations de $\mathcal{A}_n$. L'application $< x_1, \cdots, x_{n-2} > \longrightarrow \mathcal{A}_n$ qui à x_i associe a_i, induit un isomorphisme $G'_n \simeq \mathcal{A}_n$.*

Théorème 1.16. — *Pour $n \geq 5$, $\mathcal{A}_n$ est simple.*

Remarque : il y a plusieurs preuves possibles : soit on se ramène au cas $n = 5$ comme dans [**10**], soit en considérant le nombre minimal d'éléments « dérangés ». Dans tous les cas, il s'agit, étant donné un sous-groupe distingué H non trivial de $\mathcal{A}_n$, de construire un 3-cycle dans H de sorte que comme les 3-cycles sont conjugués dans $\mathcal{A}_n$, il les contient tous et est donc égal à $\mathcal{A}_n$. La technique comme d'habitude en théorie des groupes consiste à étudier des commutateurs.

Remarque : via les théorèmes de Sylow, on peut aussi montrer que $\mathcal{A}_5$ est le seul groupe simple d'ordre 60.

Corollaire 1.17. — *Le groupe dérivée de $\mathcal{A}_n$ est égal à $\mathcal{A}_n$ pour $n \geq 5$.*

Remarque : $\mathcal{A}_n$ n'est donc pas résoluble, fait qui à une application spectaculaire sur la non résolution par radicaux des équations polynomiales de degré ≥ 5 ;

1.5. Quelques sous-groupes. — De la simplicité de $\mathcal{A}_n$ pour $n \geq 5$, on montre que $\mathcal{A}_n$ est le seul sous-groupe distingué non trivial de $\mathfrak{S}_n$. Le théorème de Sylow nous apprend que $\mathfrak{S}_n$ contient tous les groupes d'ordre n qui sont donc d'indice $(n-1)!$ ce qui est très gros. En ce qui concerne les gros sous-groupes citons le résultat suivant :

Proposition 1.18. — *Si G est un sous-groupe d'indice $1 \leq k \leq n$ de $\mathfrak{S}_n$ avec $n \geq 5$, alors $k = 1, 2, n$ et G est isomorphe à $\mathfrak{S}_n$, $\mathcal{A}_n$ ou $\mathfrak{S}_{n-1}$.*

Définition 1.19. — Soient G un groupe, k un entier strictement positif et Z un sous-groupe de $\mathfrak{S}_k$. On appelle produit en couronne de G avec Z que l'on note $G \int Z$, le produit semi-direct $G^k \rtimes Z$ où Z agit sur G^k par permutations des facteurs : $z.(g_1, \cdots, g_k) = (g_{z^{-1}(1)}, \cdots, g_{z^{-1}(k)})$.

Remarque : si G agit fidèlement sur un ensemble S, la formule $(g_1, \cdots, g_k, z).(s, i) = (g_{z(i)}.s, z(i))$ définie bien un action fidèle de $G \int Z$ sur $S \times \{1, \cdots, k\}$, et que celle-ci est fidèle.

Soit p un nombre premier. On note Z_p le sous-groupe de $\mathfrak{S}_p$ engendré par la permutation cyclique $(1, 2, \cdots, p)$. On désigne par $Z_p^{\int r}$ la puissance r-ème de Z_p pour le produit en couronne,

$$Z^{\int 0} = \{1\} \text{ et } Z_p^{\int r+1} = Z_p^{\int r} \int Z_p.$$

Par récurrence $Z_p^{\int r+1}$ agit fidèlement sur $\{1, \cdots, p^r\} \times \{1, \cdots, p\} \simeq \{1, \cdots, p^{r+1}\}$ de sorte que l'ordre de $Z_p^{\int r}$ plongé dans $\mathfrak{S}_{p^r}$ est $p^{1+p+\cdots+p^{r-1}}$.

Proposition 1.20. — *Soit $n = a_0 + a_1 p + \cdots + a_k p^k$ écrit en base p ; tout p-Sylow de $\mathfrak{S}_n$ est isomorphe*

$$(Z_p^{\int 1})^{a_1} \times (Z_p^{\int 2})^{a_2} \times \cdots \times (Z_p^{\int k})^{a_k} \hookrightarrow \mathfrak{S}_p^{a_1} \times \cdots \mathfrak{S}_{p^k}^{a_k}.$$

Remarque : rappelons que $v_p(n!) = \sum_{k=1}^{\infty} \lfloor n/p^k \rfloor$ qui est encore égal à $(a_1 + a_2 p + \cdots + a_k p^{k-1}) + (a_2 + \cdots + a_k p^{k-2}) + \cdots + (a_{k-1} + a_k p) + a_k$.

En ce qui concerne les petits groupes symétriques, notons les coïncidences suivantes que l'on montrera plus ou moins aisément via une action sur un ensemble bien choisi :
- $GL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$;
- $PSL_2(\mathbb{F}_3) \simeq \mathcal{A}_4$;
- $PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$;
- $\mathcal{A}_8 \simeq GL_4(\mathbb{F}_2)$.

1.6. Groupe de Galois comme groupe de permutation des racines. — Etant donné un polynôme $P \in K[X]$, on note L son corps de décomposition, i.e. $L = K(x_1, \cdots, x_n)$ où les x_i sont les racines de P dans $\bar{K}$. Le groupe des automorphismes G de L laissant K fixe, est appelé les groupes de Galois : celui-ci permute les racines de P et peut donc ainsi être vu comme un sous-groupe de $\mathfrak{S}_n$ (un élément de G est complètement déterminé par son action sur les x_i).

Génériquement le groupe de Galois G d'un polynôme de degré n est isomorphe à $\mathfrak{S}_n$: il est contenu dans $\mathcal{A}_n$ si et seulement si le discriminant de P est un carré de K. Pour le calculer on utilise pour p ne divisant pas son discriminant, la factorisation de P modulo p : si celle-ci est le produit de facteurs irréductibles de degré $n_1, \cdots, n_r$ avec donc $\sum_i n_i = n$, on en déduit que G contient une permutation dont la décomposition en cycles à support disjoints est de type $(n_1, \cdots, n_r)$.

Par exemple si P est irréductible modulo 2, et s'il possède exactement $n-2$ racines modulo 3, alors G vu comme un sous-groupe de $\mathfrak{S}_n$ contient un n-cycle et une transposition : ces derniers engendrent $\mathfrak{S}_n$ de sorte que $G \simeq \mathfrak{S}_n$.

2. Applications au polynômes

On considère l'action de $\mathfrak{S}_n$ sur les polynômes de $K[X_1, \cdots, X_n]$ par permutation des indéterminées.

2.1. Polynômes symétriques. — Pour $\underline{i} = (i_1, \cdots, i_n)$, on note $X^{\underline{i}} = X_{i_1} \cdots X_{i_n}$; ce monôme est dit *de degré n* et *de poids* $i_1 + 2i_2 + \cdots + ni_n$; le degré (resp. le poids) d'un polynôme est le maximum du degré (resp. du poids) de ses monômes. Le résultat fondamental est le suivant.

Théorème 2.1. — *(cf.* [**1**] *p.58 ou* [**6**] *p.133)*

(i) La sous-algèbre $\mathbb{Z}[X_1, \cdots, X_n]^{\Sigma_n}$ des polynômes symétriques, est engendrée sur $\mathbb{Z}$ par les polynômes symétriques élémentaires

$$\sigma_1 = X_1 + \cdots + X_n, \qquad \sigma_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} X_{i_1} \cdots X_{i_k}, \quad \sigma_n = X_1 \cdots X_n.$$

(ii) Les $\sigma_1, \cdots, \sigma_n$ son algébriquement indépendants sur $\mathbb{Z}$ de sorte que tout $P \in K[X_1, \cdots, X_n]^{\Sigma_n}$ s'écrit de façon unique comme un polynôme $Q(\sigma_1, \cdots, \sigma_n)$; le poids de Q est inférieur ou égal au degré de P.

(iii) La famille des monômes $X^{\underline{m}} = X_1^{m_1} \cdots X_n^{m_n}$ tels que $0 \leq m_i < i$ pour $1 \leq i \leq n$, est une base de $\mathbb{Z}[X_1, \cdots, X_n]$ comme module sur le sous-anneau $\mathbb{Z}[X_1, \cdots, X_n]^{\Sigma_n}$; c'est donc un $\mathbb{Z}[X_1, \cdots, X_n]^{\Sigma_n}$-module libre de rang $n!$.

Remarque : en ce qui concerne les fractions rationnelles, pour K, un corps on a encore

$$K(X_1, \cdots, X_n)^{\mathfrak{S}_n} = K(\sigma_1, \cdots, \sigma_n).$$

Comme conséquence important, on obtient que $\mathfrak{S}_n$ est le groupe de Galois de l'équation générale d'ordre n, i.e. si L désigne le corps de décomposition sur $K = k(a_1, \cdots, a_n)$ du polynôme $X^n - a_1 X^{n-1} + \cdots + (-1)^n a_n$ alors L/K est galoisienne de groupe de Galois $\mathfrak{S}_n$ vu comme le groupe des permutations des solutions $x_1, \cdots, x_n$ du polynôme ci-dessus.

Exercice 2.1. — ***Transcendance de*** π *(cf. le poly de Chambert-Loir)*

(i) Soit f un polynôme à coefficients réels de degré m. Montrez que pour tout nombre complexe z, l'intégrale complexe

$$I(f; z) = \int_0^1 z e^{z(1-u)} f(zu) dz$$

vérifie

$$I(f; z) = e^z \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(z)$$

ainsi que la majoration

$$|I(f; z)| \leq |z| e^{|z|} \sup_{u \in [0,1]} |f(zu)|$$

(ii) Soit f un polynôme à coefficients entiers. Montrez que pour tout $n \geq 0$, il existe un polynôme f_n à coefficients entiers tel que $f^{(n)} = n! f_n$.

(iii) Pour un polynôme f et $g : \mathbb{C} \to \mathbb{C}$ une fonction, on note $\sum_{f(\alpha)=0} g(\alpha)$ la somme $g(\alpha_1) + \cdots + g(\alpha_n)$ où les α_i sont les racines de f répétées autant de fois que leur multiplicité. Montrez que si f est à coefficients entiers de coefficient a, alors pour tout $n \geq 0$, $a^n \sum_{f(\alpha)=0} \alpha^n$ appartient à $\mathbb{Z}$.
Indication : on pourra introduire une matrice dont la trace est $a^n \sum_{f(\alpha)=0} \alpha^n$.

(iv) Soit f un polynôme à coefficients entiers tel que $f(0) \neq 0$ et de coefficient dominant a. Pour p un nombre premier, soit $g(x) = x^{p-1} f^p(x)$ et $J_p = \sum_{f(\alpha)=0} I(g; \alpha)$. Montrez qu'il existe un entier M tel que

$$\frac{a^{m-p}}{(p-1)!} J_p = a^{m-p} N f(0)^p + pM$$

où $N = \sum_{f(\alpha)=0} e^{\alpha}$. En déduire que N n'est pas un entier non nul.

(v) On veut montrer que π est transcendant. On raisonne par l'absurde : soit f un polynôme irréductible à coefficients entiers tel que $f(i\pi) = 0$ dont on note $\alpha_1, \cdots, \alpha_n$ les racines.

(a) En développant l'égalité $\prod_{f(\alpha)=0}(1 + e^{\alpha})$ montrez que

$$\sum_{\epsilon \in \{0,1\}^n} exp(\sum \epsilon_j \alpha_j) = 0.$$

(b) Soit $Q(X) = \prod_{\epsilon \in \{0,1\}^n}(X - \sum \epsilon_j \alpha_j)$. Montrer que $Q(X) \in \mathbb{Q}[X]$.

(c) En utilisant la question (4), aboutissez à une contradiction.

Remarque : les polynômes semi-symétriques i.e. invariant sous $\mathcal{A}_n$ est $K[\sigma_1, \cdots, \sigma_n, V_n]$ où K est de caractéristique distincte de 2 et $V_n = \prod_{i<j}(X_i - X_j)$.

2.2. Algorithme de calcul. — La procédure est récursive comme suit : $P(X_1, \cdots, X_{n-1}, 0) = Q_1(\sigma_1^0, \cdots, \sigma_{n-1}^0)$ où $\sigma_i^0 = \sigma_i(X_1, \cdots, X_{n-1}, 0)$. On pose alors

$$P_1(X_1, \cdots, X_n) = P(X_1, \cdots, X_n) - Q_1(\sigma_1, \cdots, \sigma_{n-1})$$

de sorte que comme $P_1(X_1, \cdots, X_{n-1}, 0) = 0$, $P_1(X_1, \cdots, X_n)$ est divisible par σ_n égal à $\sigma_n P_2$ avec $\deg P_2 \leq \deg P - n$.

2.3. Relations de Newton et de Waring. — Notons $s_d = X_1^d + \cdots + X_n^d$ et soit dans $\mathbb{Z}[X_1, \cdots, X_n, T]$, $F(T) = \prod_{i=1}^n (1 - TX_i) = 1 - \sigma_1 T + \sigma_2 T^2 - \cdots + (-1)^n \sigma_n T^n$. On a

$$\frac{-TF'(T)}{F(T)} = \frac{TX_1}{1 - TX_1} + \cdots + \frac{TX_n}{1 - TX_n} = \sum_{m \geq 1} T^m s_m$$

où la dernière égalité découle du développement en série formelle $(1-Z)^{-1} = \sum_{m \geq 0} Z^m$ pour $Z = TX_i$. Après simplification par T, on obtient la relation de Newton

$$F(T)\Big(\sum_{m \geq 1} T^{m-1} s_m\Big) + F'(T) = 0$$

qui est une égalité dans $\mathbb{Z}[X_1, \cdots, X_n][[T]]$. En considérant le coefficient de T^k, on trouve :

$$k \geq n : \ s_k - \sigma_1 s_{k-1} + \cdots + (-1)^n \sigma_n s_{k-n} = 0$$

$$1 \leq k \leq n : \ s_k - \sigma_1 s_{k-1} + \cdots + (-1)^{k-1} \sigma_{k-1} s_1 + (-1)^k k s_k = 0.$$

Dans $\mathbb{Q}[X_1, \cdots, X_n][[T]]$, la relation de Newton s'écrit $\frac{F'(T)}{F(T)} = -P'(T)$, où $P(T) = \sum_{m\geq 1} \frac{s_m}{m} T^m$. Par « intégration » on obtient

$$F(T) = \exp\Big(-P(T)\Big) = 1 - P(T) + \frac{1}{2}P(T)^2 - \frac{1}{3!}P(T)^3 + \cdots$$

ce qui a bien un sens puisque $P(T)$ commence par T et donc $P(T)^k$ par T^k de sorte que le coefficient de T^k ne fait intervenir que les $P(T)^j$ pour $j \leq k$ et est donc fini. En particulier, on note que cette expression permet de calculer le polynôme G_k tel que $\sigma_k = G_k(s_1, \cdots, s_n)$.

Si inversement on cherche à exprimer les s_i en fonction des $\sigma_1, \cdots, \sigma_n$, on utilise l'expression $P(T) = -\log\Big(F(T)\Big)$ où $F(T) = 1 - TG(T)$ avec $G(T) = \sigma_1 - \sigma_2 T + \sigma_3 T^2 + \cdots$ et donc

$$P(T) = TG + \frac{T^2G^2}{2} + \frac{T^3G^3}{3} + \cdots$$

Remarque : ainsi si K est de caractéristique nulle alors la famille $(s_1, \cdots, s_n)$ de $K[X_1, \cdots, X_n]$ est algébriquement libre sur K et engendre l'algèbre $K[X_1, \cdots, X_n]^{\Sigma_n}$.

Remarque : il est au moins un cas non anecdotique, où l'on cherche à inverser les relations de Newton en caractéristique non nulle : lorsque l'on cherche à décrypter un code BCH. La situation est celle où on a accès à tous les S_k et on cherche à obtenir le degré n du polynôme ainsi que les fonctions symétriques élémentaires σ_i. On peut alors procéder ainsi : notons

$$H_t = \begin{pmatrix} S_1 & S_2 & \cdots & S_t \\ S_2 & S_3 & \cdots & S_{t+1} \\ \vdots & \vdots & & \vdots \\ S_t & S_{t+1} & \cdots & S_{2t-1} \end{pmatrix} \qquad V = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

de sorte que $H_n = V \mathrm{diag}(\alpha_1, \cdots, \alpha_n)^t V$ où les α_i sont les racines distinctes non nulles du polynôme cherché. Ainsi H_n est inversible et donc pour tout $t \geq n$, le rang de H_t est $\geq n$. En outre les formules de Newton montrent que chaque colonne de numéro $\geq n+1$ de H_t est combinaison linéaires n précédentes. Ainsi l'entier n est égal au rang de H_t pour tout $t \geq n$ et on obtient les σ_i en résolvant le système de Cramer donné par les formules de Newton

$$H_n \begin{pmatrix} \sigma_n \\ \vdots \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} -S_{n+1} \\ \vdots \\ -S_{2n} \end{pmatrix}.$$

2.4. Théorème de Sylvester. — Lorsque l'on veut compter le nombre de racines distinctes réelles d'un polynôme réel, on dispose de l'algorithme de Sturm : en fait celui-ci peut compter les racines distinctes sur n'importe quel intervalle. Ce calcul est plutôt laborieux, Sylvester a alors suggéré la méthode suivante pour compter les racines réelles d'un polynôme réel unitaire $P(X)$ de degré n : notons $V = \mathbb{R}[X]/(P)$ et pour $a \in V$ on note $\mathrm{tr}(a)$ la trace de l'application linéaire $v \in V \mapsto av \in V$. Soit alors ϕ la forme bilinéaire symétrique définie par $\phi(v, w) = \mathrm{tr}(vw)$.

Théorème 2.2. — ***(Sylvester), cf.*** [**7**] *Pour $P(X) = \prod_{i=1}^{n}(X - \alpha_i) \in \mathbb{R}[X]$, on note $s_k = \sum_{i=1}^{n} \alpha_i^k$ les sommes de Newton. La matrice de ϕ dans la base $1, X, \cdots, X^{n-1}$ est*

$$\begin{pmatrix} s_0 & s_1 & \cdots & s_{n-1} \\ s_1 & s_2 & \cdots & s_n \\ \vdots & \vdots & \ddots & \vdots \\ s_{n-1} & s_n & \cdots & s_{2n} \end{pmatrix}$$

dont la signature est égal au nombre de racines réelles distinctes de P.

Corollaire 2.3. — *Pour $1 \leq k \leq n-1$, il existe des polynômes $P_{k,n} \in \mathbb{R}[X_1, \cdots, X_n]$ à n variables tels que pour tout $P(X) = X^n - a_{n-1}X^{n-1} + \cdots + (-1)^n a_0 \in \mathbb{R}[X]$, P est scindé à racines simples réelles si et seulement si $P_{k,n}(a_0, \cdots, a_{n-1}) > 0$, $\forall k = 1, \cdots, n-1$.*

Remarque : pour $n = 2$, $P(X) = X^2 - \sigma_1 X - \sigma_2$, on obtient $P_{1,2} = s_0 s_2 - s_1^2$ avec $s_0 = 2, s_1 = \sigma_1$ et $s_2 = \sigma_1^2 - 2\sigma_2$ soit $P_{1,2} = \sigma_1^2 - 4\sigma_1\sigma_2$ qui est le discriminant bien connu.

2.5. Inégalités de Muirhead. — Soit $\lambda = (\lambda_1, \cdots, \lambda_n)$ tel que $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq 0$ *une partition* ; on pose $|\lambda| = \lambda_1 + \cdots + \lambda_n$. On dit que $\lambda \geq \mu$ si pour tout $k = 1, \cdots, n$ on a $\lambda_1 + \cdots + \lambda_k \geq \mu_1 + \cdots + \mu_k$. A toute partition λ on associe le polynôme homogène symétrique de degré $|\lambda|$:

$$M_\lambda(x_1, \cdots, x_n) = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} x_1^{\lambda_{\sigma(1)}} \cdots x_n^{\lambda_{\sigma(n)}}.$$

Théorème 2.4. — *(**Muirhead** cf.* [**11**] *p.82) L'inégalité*

$$M_\lambda(x) \geq M_\mu(x)$$

est vérifiée pour tout vecteur $x = (x_1, \cdots, x_n)$ à coordonnées positives, si et seulement si $|\lambda| = |\mu|$ et $\lambda \geq \mu$. Les cas d'égalités sont $\lambda = \mu$ ou $x_1 = \cdots = x_n$.

Remarque : pour $\mu = (1, \cdots, 1)$ et $\lambda = (n, 0, \cdots, 0)$ on retrouve l'inégalité bien connue entre les moyennes géométrique et arithmétique :

$$M_\lambda(x) = \frac{x_1^n + \cdots + x_n^n}{n} \geq M_\mu(x) = x_1 \cdots x_n$$

Preuve : Supposons tout d'abord que l'inégalité de l'énoncé soit vérifiée pour tout $x > 0$: pour $x_1 = \cdots = x_k = a$ et $x_{k+1} = \cdots = x_n = 1$ on a

$$1 \leq \lim_{a \to +\infty} \frac{M_\lambda(x)}{M_\mu(x)} = \lim_{a \to \infty} \frac{a^{\lambda_1 + \cdots + \lambda_k}}{a^{\mu_1 + \cdots + \mu_k}}$$

et donc $\lambda_1 + \cdots + \lambda_k \geq \mu_1 + \cdots + \mu_k$; pour $k = n$ et $a > 1$ (resp. $0 < a < 1$) on obtient $|\lambda| \geq |\mu|$ et $|\lambda| \leq |\mu|$.

Réciproquement considérons pour $i < j$ tel que $\mu_j > 0$ la partition $\mu' = R_{i,j}\mu$ définie par $\mu'_i = \mu_i + 1$, $\mu'_j = \mu_j - 1$ et $\mu'_k = \mu_k$ pour tout $k \neq i, j$: on a $\mu' > \mu$ et $|\mu'| = |\mu|$. Le résultat découle alors directement des deux lemmes suivants. $\square$

Lemme 2.5. — *Si $\lambda = R_{i,j}\mu$ alors pour tout $x > 0$ on a $M_\lambda(x) \geq M_\mu(x)$ avec égalité si et seulement si $x_1 = \cdots = x_n$.*

Preuve : Pour toute paire d'indices $1 \leq p < q \leq n$, la différence $M_\lambda(x) - M_\mu(x)$ contient une composante de la forme

$$A.(x_p^{\lambda_i} x_q^{\lambda_j} + x_q^{\lambda_i} x_p^{\lambda_j} - x_p^{\mu_i} x_q^{\mu_j} - x_q^{\mu_i} x_p^{\mu_j}) \qquad A > 0,$$

où $\lambda_i = \mu_i + 1$ et $\lambda_j = \mu_j - 1$ avec $\mu_i \geq \mu_j$. Oubliant le coefficient A, l'expression se factorise

$$(x_p x_q)^{\mu_j - 1}(x_p - x_q)(x_p^{\mu_i + 1 - \mu_j} - x_q^{\mu_i + 1 - \mu_j}) \geq 0$$

avec égalité si et seulement si $x_p = x_q$. Ainsi $M_\lambda(x) - M_\mu(x) \geq 0$ avec inégalité stricte si tous les x_i ne sont pas égaux. □

Lemme 2.6. — *Soit $\lambda \geq \mu$ avec $\lambda \neq \mu$ et $|\lambda| = |\mu|$; alors λ s'obtient à partir de μ après un nombre fini de transformation du type $R_{i,j}$.*

Preuve : Soit i le plus petit indice tel que $\lambda_i \neq \mu_i$: la condition $\lambda \geq \mu$ impose alors $\lambda_i > \mu_i$. De l'égalité $|\lambda| = |\mu|$, on en déduit qu'il existe $i < j$ tel que $\lambda_j < \mu_j > 0$. On peut alors appliquer $R_{i,j}$ à μ et pour $\nu = R_{i,j}\mu \leq \lambda$ on obtient :

$$|\lambda_i - \mu_i| = |\lambda_i - \nu_i| + 1, \qquad |\lambda_j - \mu_j| = |\lambda_j - \nu_j| + 1$$

et donc $\sum_k |\lambda_j - \nu_k| = \sum_k |\lambda_k - \mu_k| - 2$ de sorte qu'après un nombre fini de telles étapes on obtient une partition $\lambda' \leq \lambda$ telle que $\sum_k |\lambda_k - \lambda'_k| = 0$ et donc $\lambda' = \lambda$. □

3. Applications à l'algèbre linéaire

3.1. Déterminant et permanent. — On rappelle que $\det A = \sum_{\sigma \in \mathfrak{S}_n} \epsilon(\sigma) \prod_{i=1}^n a_{\sigma(i),i}$ qui se calcule aussi en développant selon une ligne

$$\det A = \sum_{i=1}^n (-1)^{i+j} a_{i,j} \det A_{i,j}.$$

Le calcul du déterminant permet en particulier de calculer le polynôme caractéristique d'une matrice et donc ensuite de localiser les valeurs propres.
L'algorithme de Faddeev-Leverrier, cf. [**4**], pour le calcul du polynôme caractéristique d'une matrice $M \in \mathbb{M}_n(K)$: on définit la suite $(M_k)_{0 \leq k \leq n-1}$ par récurrence : $M_0 = M$ et pour $1 \leq k \leq n-1$:

$$M_k = M\Big(M_{k-1} - \frac{1}{k}\mathrm{tr}(M_{k-1} I_n)\Big).$$

On a alors

$$\det(XI_n - M) = X^n - \sum_{k=1}^n \frac{1}{k}\mathrm{tr}(M_{k-1})X^{n-k}.$$

Le permanent de A est défini par $perA = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^n a_{\sigma(i),i}$; c'est une forme n-linéaire symétriques des n lignes (ou colonnes), il est donc invariant par toute permutations de celles-ci. On peut développer le permanent par rapport à une ligne ou une colonne : $perA = \sum_{i=1}^n a_{i,j} perA_{i,j}$. On a aussi $\mathrm{per}({}^tA) = \mathrm{per}(A)$ mais par contre en général $\mathrm{per}(AB) \neq \mathrm{per}(BA)$ ce qui annihile toute velléité de calcul par manipulations des lignes et des colonnes.

Théorème 3.1. — *(**Frobenius-König**, cf.* [**9**] *l'exercice 1.4.19 p34 dans le volume Exercices corrigés) Soit A à coefficients positifs alors $perA = 0$ ssi il existe une sous-matrice nulle de A de taille $(r, n+1-r)$. Par ailleurs $perA > 0$ si et seulement s'il existe $\sigma \in \mathfrak{S}_n$ telle que $a_{\sigma(i),i} > 0$ pour tout $1 \leq i \leq n$.*

Preuve : Notons $\mathcal{M}_n^+$ l'ensemble des matrices carrées d'ordre n à coefficients positifs ou nuls. Dans le sens direct, soit $1 \leq s \leq n$ tel qu'il existe une matrice extraite nulle de A de taille $s \times (n+1-s)$. Par des permutations des lignes et colonnes, on transforme A en une matrice $A' = \begin{pmatrix} A_1 & 0_{s,n-s} \\ A_2 & A_3 \end{pmatrix}$ avec A_1 carrée d'ordre s ayant sa dernière colonne nulle de sorte que $\mathrm{per}(A_1) = 0$ et donc $\mathrm{per}(A) = \mathrm{per}(A') = \mathrm{per}(A_1)\mathrm{per}(A_3) = 0$.

Réciproquement, on raisonne par récurrence sur $n > 0$; le cas $n = 1$ étant trivial supposons le résultat acquis jusqu'au rang n et traitons le cas de $A \in \mathcal{M}_{n+1}^+$ tel que $\mathrm{per}(A) = 0$ avec $A \neq 0$. Soit $a_{i,j} > 0$ de sorte que $\mathrm{per}(A_{i,j}) = 0$. D'après l'hypothèse de récurrence, on peut extraire de $A_{i,j}$ une matrice nulle de format $s \times (n+1-s)$ avec $1 \leq s \leq n$ et des permutations sur les lignes et colonnes permettent de transformer A en une matrice $A' = \begin{pmatrix} A_1 & 0_{s,n+1-s} \\ A_2 & A_3 \end{pmatrix}$ avec donc $\mathrm{per}A_1 = 0$ ou $\mathrm{per}A_3 = 0$. Supposons $\mathrm{per}(A_1) = 0$; d'après l'hypothèse de récurrence, on peut extraire de A_1 une matrice nulle de format $t \times (s+1-t)$ de sorte que l'on peut extraire de A un bloc nul de format $t \times \Big((s+1-t) + (n+1-s)\Big)$ i.e. $t \times (n+2-t)$ ce qui est bien le résultat escompté. $\square$

Corollaire 3.2. — **(lemme des mariages)** *Soient F, G des ensembles finis et $\Phi : G \rightarrow \mathcal{P}(F)$; les assertions suivantes sont alors équivalentes :*

(i) il existe une injection $\phi : G \rightarrow F$ telle que $\forall g \in G$, $\phi(g) \in \Phi(g)$;

(ii) $\forall G' \in \mathcal{P}(G)$, $\sharp \bigcup_{g \in G'} \Phi(g) \geq \sharp G'$.

Remarque : pour interpréter le corollaire, G (resp. F) est l'ensemble des garçons (resp. filles) et $\Phi(g)$ représente l'ensemble des filles que g connait. L'application ϕ est un mariage. On peut prouver ce résultat simplement en posant la bonne hypothèse de récurrence.

Preuve : L'existence de ϕ est injective, implique clairement la propriété (ii). En ce qui concerne l'implication réciproque, on construit $A \in \mathcal{M}_n^+$ comme suit, où $n = \sharp F$:

– sur les $m = \sharp G$ premières lignes, $a_{i,j} = 1$ si la j-ème fille $f_j \in \Phi(g_i)$ et 0 sinon ;

– les coefficients des $n - m$ dernières lignes sont tous égaux à 1.

Si on avait $\mathrm{per}(A) = 0$, il existerait une matrice nulle de format $s \times (n+1-s)$ extraite des m premières lignes dont on note $i_1 < i_1 < \cdots < i_s$ (resp. $j_1 < \cdots < j_{n+1-s}$) les indices des lignes (resp. colonnes). On aurait alors

$$\bigcup_{k=1}^{s} \Phi(g_{i_k}) \subset F \backslash \{f_{j_1}, \cdots, f_{j_{n+1-s}}\}$$

de sorte que $\sharp \bigcup_{k=1}^{s} \Phi(g_{i_k}) \leq n - (n+1-s) = s-1 < s$ ce qui contredit (ii). Ainsi donc $\mathrm{per}A = \sum_{\sigma \in \mathfrak{S}_n} a_{\sigma(1),1} \cdots a_{\sigma(n),n} \neq 0$ et donc par positivité des termes, il existe une permutation σ telle que $a_{\sigma(i),i} \neq 0$ pour tout $i = 1, \cdots, n$. Ainsi pour tout $i = 1, \cdots, m$, ona $a_{i,\sigma^{-1}(i)} \neq 0$ et $f_{\sigma^{-1}(i)} \in \Phi(g_i)$ et l'application ϕ définie par $\phi(g_i) = f_{\sigma^{-1}(i)}$ vérifie les conditions de (i). $\square$

3.2. Matrices de permutation. — Etant donnée une base $(e_1, \cdots, e_n)$ du K-espace vectoriel E, on fait agir le groupe symétrique $\mathfrak{S}_n$ par permutations des vecteurs de base, i.e. $\sigma \in \mathfrak{S}_n \mapsto P_\sigma \in GL_n(E)$ tel que $P_\sigma(e_i) = e_{\sigma(i)}$.

Théorème 3.3. — *(**Brauer**, cf. RMS97 ou [**2**]) Les matrices de permutation P_σ et P_τ sont conjuguées dans $GL_n(\mathbb{R})$ si et seulement si σ et τ sont conjuguées dans $\mathfrak{S}_n$*

Preuve : Nous présentons rapidement plusieurs preuves, les deux premières étant seulement valables en caractéristique nulle. Notons déjà que si $\sigma = s\tau s^{-1}$ alors $P_\sigma = P_s P_\tau P_s^{-1}$ et donc P_σ et P_τ sont conjuguées. Réciproquement, il s'agit de montrer que le nombre $c_k(\sigma)$ de cycles de longueur k dans la décomposition en cycles à supports disjoints de σ est égal à $c_k(\tau)$ pour tout $k \geq 1$.
Première preuve : la décomposition en cycles à support disjoints de σ donne une décomposition en espaces cycliques de E avec $c_k(\sigma)$ sous-espaces cycliques pour le polynôme $X^k - 1 = \prod_{d|k} \Phi_d(X)$, où les Φ_d sont les polynômes cyclotomiques qui sont irréductibles sur $\mathbb{Z}$. Ainsi les facteurs irréductibles des invariants de similitude de P_σ sont les Φ_d où d divise un k tel que $c_k(\sigma) > 0$. L'espace associé à un de ces Φ_d est la somme directe de n_d facteurs où $n_d = \sum_{d|k} c_k(\sigma)$ qui est donc égal à $\sum_{d|k} c_k(\tau)$. Ainsi pour k_0 maximal tel que $c_k(\sigma) \neq 0$, on en déduit que $n_{k_0} = c_{k_0}(\sigma) = c_{k_0}(\tau)$ et par récurrence évidente de k_0 à 1, on en déduit que pour tous $k > 0$, $c_k(\sigma) = c_k(\tau)$.
Remarque : dans le même genre, sans utiliser les invariants de similitude, on peut raisonner sur le polynôme caractéristique et la multiplicité des racines.

Deuxième preuve : on utilise les égalités $\mathrm{tr}\sigma^m = \mathrm{tr}\tau^m$ pour tout $m \geq 0$. On rappelle que la décomposition en cycles à supports disjoints de la puissance m-ème d'un k-cycle consiste en $k \wedge m$ cycles de longueur $k/k \wedge m$ et donc $\mathrm{tr}\sigma^m = \sum_{k|m} kc_k(\sigma)$ et on conclut comme précédemment.

Troisième preuve, valable donc en toute caractéristique : on utilise les égalités $\dim E^{\sigma^m} = \dim E^{\tau^m}$, ces dimensions étant égales au nombre d'orbite de σ^m ce qui donne $\sum_k k \wedge mc_k(\sigma) = \sum_k k \wedge mc_k(\tau)$. On utilise alors l'inversibilité de la matrice des pgcd.

□

Théorème 3.4. — *(**Décomposition de Bruhat**, cf.* [**8**]*) : $T(n,K)\backslash GL(n,K)/T(n,K) \simeq \mathfrak{S}_n$ où $T(n,K)$ désigne l'ensemble des matrices triangulaires supérieures.*

Remarque : on peut ainsi associer à toute matrice inversible une unique matrice de permutation.

Corollaire 3.5. — *Soit $\mathcal{D}$ l'ensemble des drapeaux maximaux : chaque orbite de $\mathcal{D} \times \mathcal{D}$ sous l'action de $GL(n,K)$ contient exactement un couple (I_n, P_σ).*

Preuve : L'action de $GL(n,K)$ sur $\mathcal{D}$ donne une bijection du quotient $GL(n,K)/T(n,K)$ avec $\mathcal{D}$; le couple $(A,B) \in GL(n,K)/T(n,K) \times GL(n,K)/T(n,K)$ est dans la classe de $(I_n, A^{-1}B)$. On écrit la décomposition de Bruhat de $A^{-1}B = TP_\sigma T'$ et donc $(A,B) \sim (I_n, TP_\sigma T') = (I_n, TP_\sigma)$ soit $(A,B) \sim (T^{-1}, P_\sigma) = (I_n, P_\sigma)$. Reste alors à voir que si $(I_n, P_\sigma) \sim (I_n, P_\tau)$ alors $\sigma = \tau$. Il existe donc $T \in T(n,K)$ telle que $TP_\sigma = P_\tau$ dans $GL(n,K)/T(n,K)$ et donc $P_\sigma = T^{-1} P_\tau T'$ pour $T' \in T(n,K)$ et donc $\sigma = \tau$ d'après l'unicité dans la décomposition de Bruhat. □
Remarque : ainsi l'ensemble des classes de paires de drapeaux complets sous l'action de $GL(n,\mathbb{C})$, est en bijection avec $\mathfrak{S}_n$.

Théorème 3.6. — *(Birkhoff, cf.* [**12**] *8.7.1)L'ensemble des matrices bistochastiques est compact convexe et ses points extrémaux sont les matrices de permutations.*

Preuve : La condition est clairement suffisante, montrons donc sa nécessité. Si $P = \alpha A + \beta B$ est une matrice de permutation et α, β des réels positifs de somme 1 avec A, B bi-stochastiques. Ainsi pour tout i,j tel que $p_{i,j} = 0$ on doit avoir $a_{i,j} = b_{i,j} = 0$ de sorte que P, A, B ont pour chaque colonne et ligne exactement un seul de leur coefficient non nul. Etant bi-stochastique on en déduit que ce coefficient est égal à 1 et donc $P = A = B$. On en déduit donc que les matrices de permutation sont des points extrémaux.

Soit désormais une matrice bistochastique A qui ne soit pas une matrice de permutation. Il existe alors une ligne i_1 qui contienne au moins deux coefficients non nuls compris strictement entre 0 et 1. Soit donc $0 < a_{i_1,i_2} < 1$. Il existe alors $i_3 \neq i_2$ tel que $0 < a_{i_3,i_2} < 1$, puis i_4 tel que $0 < a_{i_3,i_4} < 1$ et ainsi de suite. En continuant ainsi ce procédé il existe un indice où l'on considère un $a_{i,j}$ déjà pris précédemment. Considérons alors la suite des $(a_{i_k,j_k})_{k=1,\cdots,r}$ de la première occurence de $a_{i,j}$ à la position précédant la deuxième occurence : pour tout k impair (resp. pair) on a $i_{k+1} = i_k$ (resp. $j_{k+1} = j_k$). Soit $a_{i',j'}$ minimal parmi cette suite. On construit alors la matrice $B = [b_{i,j}]$ avec $b_{i_{2k+1},j_{2k+1}} = 1$ pour $1 \leq 2k+1 \leq r$ et $b_{i_{2k},j_{2k}} = -1$ les autres coefficients étant nuls. Les matrices $A_+ = A + a_{i',j'}B$ et $A_- = A - a_{i',j'}B$ sont positive par minimalité de $a_{i',j'}$ et bistochastique car la somme des colonnes et des lignes de B est toujours nulle. De l'égalité $A = \frac{A_+ + A_-}{2}$ on en déduit que A n'est pas un point extrémal. □

Remarque : d'après le théorème de Krein-Millman, on en déduit qu'une matrice A est bistochastique si et seulement s'il existe des matrices de permutations $P_1, \cdots, P_N$, avec $N \leq n!$, et des scalaires positifs $\alpha_1, \cdots, \alpha_N \in \mathbb{R}$ tels que $\alpha_1 + \cdots + \alpha_N = 1$ et $A = \alpha_1 P_1 + \cdots + \alpha_N P_N$. On peut en fait montrer que l'on peut prendre $N \leq n^2 - 2n + 2$.

Application : Conditionnement des valeurs propres : les valeurs propres varient continument, on aimerait cependant une estimation quantitative. Par exemple pour $D = \mathrm{diag}(\lambda_1, \cdots, \lambda_n)$, les valeurs propres de $D + E$ sont contenues dans la réunion des disques de Gersgorin $\{z \in \mathbb{C} : |z - \lambda_i - e_{i,i}| \leq R'_i(E)\}$ pour $i = 1, \ldots, n$. Autrement dit si λ' est une racine de $D + E$, il existe i tel que $|\lambda' - \lambda_i| \leq |||E|||_\infty$. Plus généralement, on en déduit directement que si A est diagonalisable, $A = PDP^{-1}$ et si λ est une valeur propre de $A + E$, il existe i tel que

$$|\lambda - \lambda_i| \leq \kappa_\infty(P)|||E|||$$

où $\kappa_\infty(E) := |||P|||_\infty . |||P^{-1}|||_\infty$ est le facteur de conditionnement introduit au §**??**. On peut en fait généraliser ce résultat à toutes les normes matricielles subordonnées à une norme monotone (i.e. pour tout $x = [x_i]$, $y = [y_i] \in \mathbb{C}^n$, $|x| \leq |y| \Rightarrow ||x|| \leq ||y||$) ou absolue (i.e. $||x|| = || \, |x| \, ||$) (cf. [**12**] 6.3.2) ; les normes $||| \bullet |||_2$, $||| \bullet |||_\infty$ et $||| \bullet |||_1$ sont de telles normes. En particulier pour $||| \bullet |||_2$, l'interprétation géométrique donnée au théorème **??**, on en déduit que si A possède deux vecteurs propres « presque »] colinéaires alors le problème de déterminer les valeurs propres risque d'être mal conditionné. Au contraire si A est normal ce qui est équivalent à dire que ses vecteurs propres forment une base orthonormale alors $\kappa(P) = 1$ car P sera unitaire et le problème de détermination des valeurs propres est parfaitement conditionné i.e. pour toute valeur propre λ de $A + E$ il existe i tel que $|\lambda - \lambda_i| \leq |||E|||_2$. Dans le cas où A **et** $A + E$ sont normaux, on peut améliorer les résulats précédents.

Théorème 3.7. — *(Hoffman et Wielandt) (cf.* [**12**] *6.3.5) Soient $A, E \in \mathbb{M}_n(\mathbb{C})$ telles que A et $A + E$ sont normales dont on note $\{\lambda_1, \cdots, \lambda_n\}$ et $\{\lambda'_1, \cdots, \lambda'_n\}$ l'ensemble des valeurs propres. Il existe alors une permutation $\sigma \in \mathfrak{S}_n$ telle que*

$$\Big[\sum_{i=1}^n |\lambda'_{\sigma(i)} - \lambda_i|^2\Big]^{1/2} \leq ||E||_2$$

Preuve : Commençons par diagonaliser $A = VDV^*$ et $A + E = WD'W^*$. On a alors

$$\begin{aligned}||E||_2^2 &= ||(A+E) - A||_2^2 = ||WD'W^* - VDV^*||_2^2 = ||ZD'Z^* - D||_2^2\\ &\mathrm{tr}(ZD'Z^* - D)(ZD'Z^* - D)^* = \mathrm{tr}(D'(D')^* + DD^*) - \mathrm{tr}(ZD'Z^*D^* + DZ(D')^*Z^*)\\ &= \textstyle\sum_{i=1}^n (|\lambda_i'|^2 + |\lambda_i|^2) - 2\mathrm{Re}\ \mathrm{tr}(ZD'Z^*D^*)\end{aligned}$$

où $Z = V^*W$ de sorte que $||E||_2^2$ est plus grand que

$$a = \sum_{i=1}^n (|\lambda_i'|^2 + |\lambda_i|^2) - 2\max\{\mathrm{Re}\ \mathrm{tr}(UD'U^*D^*) :\ U \text{ est unitaire}\}$$

Pour $U = [u_{i,j}]$, on a Re $\mathrm{tr}(UD'U^*D^*) = \sum_{i,j=1}^n |u_{i,j}|^2 \mathrm{Re}\ (\bar\lambda_i\lambda_j')$ où $C = [c_{i,j} = |u_{i,j}|^2]$ est une matrice doublement stochastique. On en déduit donc que

$$\max\{\mathrm{Re}\ \mathrm{tr}(UD'U^*D^*) :\ U \text{ est unitaire}\} \leq max\{\sum_{i,j=1}^n c_{i,j}\mathrm{Re}\ (\bar\lambda_i\lambda_j') :\ C \text{ est doublement stochastique}\}$$

Or la fonction à maximiser est une fonction linéaire sur un compact convexe dont les points extrémaux sont d'après le théorème de Birkhoff les matrices de permutations qui sont des matrices unitaires de sorte que

$$\max\{\mathrm{Re}\ \mathrm{tr}(UD'U^*D^*) :\ U \text{ est unitaire}\} = \mathrm{Re}\ \mathrm{tr}(PD'{}^tPD^*)$$

où P est une matrice de permutation i.e. $Pe_i = e_{\sigma(i)}$ pour une permutation $\sigma \in \mathfrak{S}_n$. De l'égalité Re $\mathrm{tr}(PD'{}^tPD^*) = \sum_{i=1}^n \mathrm{Re}\ (\lambda'_{\sigma(i)}\bar\lambda_i)$ on obtient

$$||E||_2^2 \geq \sum_{i=1}^n \Big[|\lambda'_{\sigma(i)}|^2 + |\lambda_i|^2 - 2\mathrm{Re}\ (\lambda'_{\sigma(i)}\bar\lambda_i)\Big] = \sum_{i=1}^n |\lambda'_{\sigma(i)} - \lambda_i|^2$$

□

Remarque : en reprenant les mêmes arguments mais en considérant

$$\min\{\sum_{i,j=1}^n c_{i,j}\mathrm{Re}\ (\lambda_i'\bar\lambda_j) :\ C = [c_{i,j}] \text{ est doublement stochastique}\},$$

on obtient qu'il existe une permutation τ pour laquelle

$$\Big[\sum_{i=1}^n |\lambda'_{\tau(i)} - \lambda_i|^2\Big]^{1/2} \geq ||E||_2$$

Dans le cas où A est hermitienne et $A+E$ normale, on peut prendre les arrangements suivants : $\lambda_1 \leq \cdots \leq \lambda_n$ et Re $\lambda_1' \leq \cdots \leq$ Re λ_n' ; cf. [**12**] 6.3.8.

3.3. Théorème de Frobenius-Zolotarev. — Soit $p \geq 3$ premier et V un espace vectoriel de dimension finie sur $\mathbb{F}_p$ alors pour tout $u \in GL(V)$, la signature de u est égale à $(\frac{\det u}{p})$. En particulier pour $V = \mathbb{F}_p$, on peut prouver la loi de réciprocité quadratique ; on renvoie à [**2**].

4. Applications à la géométrie

4.1. Polyèdres réguliers et sous-groupe finis de $SO(3,\mathbb{R})$. — En faisant agir un sous-groupe fini G de $SO(3)$ sur la sphère unité, l'étude de ses pôles permet de déterminer G, à savoir de montrer le résultat suivant.

Théorème 4.1. — *Les seuls sous-groupes finis de $SO(3)$ sont $\mathbb{Z}/n\mathbb{Z}$, D_n, $\mathcal{A}_4$, $\mathfrak{S}_4$ ou $\mathcal{A}_5$.*

Application : à un polyèdre régulier de l'espace est associé le sous-groupe de $SO(3)$ qui le stabilise ; il est donc fini et l'étude précédente permet de montrer qu'il n'y a que 5 possibilités.
Remarque : une autre façon d'interpréter le résultat précédent est de dire que $\mathfrak{S}_5$ admet une représentation de dimension 3 ; elle est même irréductible. L'étude systématique des représentations irréductibles de $\mathfrak{S}_n$ met un jeu une combinatoire très élégante en lien avec les tableaux de Young.

4.2. n-butterfly. — Soit $n \geq 1$ et n cercles concentriques $\mathcal{C}_1, \cdots, \mathcal{C}_n$; on considère une droite PQ et M le milieu des points d'intersection de cette droite avec un quelconque de ces cercles. On considère alors deux droites D_1 et D_2 passant par M dont les points d'intersection avec les cercles $\mathcal{C}_1, \cdots, \mathcal{C}_n$ sont notés $A_n, A_{n-1} \cdots, A_1, B_1, \cdots, B_n$ et $C_n, \cdots, C_1, D_1, \cdots, D_n$. Soit alors une permutation $\sigma \in \mathfrak{S}_n$; pour tout $i = 1, \cdots, n$ on note $X_i = A_i D_{\sigma(i)} \cap PQ$ et $Y_i = C_i B_{\sigma(i)} \cap PQ$, cf. la figure 1.

L'énoncé du théorème qu'il s'agit de prouver est que

$$\frac{1}{MX_1} + \cdots + \frac{1}{MX_n} = \frac{1}{MY_1} + \cdots + \frac{1}{MY_n}.$$

(i) Soit ABC un triangle et $M \in [BC]$; on note $\alpha = \widehat{BAM}$ et $\beta = \widehat{MAC}$, alors

$$\frac{\sin(\alpha+\beta)}{AM} = \frac{\sin(\alpha)}{AC} + \frac{\sin(\beta)}{AB}.$$

(ii) La configuration est celle de la figure 2 : trois demi-droites issues d'un point M sur lesquelles sont portées des points $C_1, \cdots, C_n$ et $B_1, \cdots, B_n$. Pour une permutation $\sigma \in \mathfrak{S}_n$, on note $Y_i = C_i B_{\sigma(i)} \cap D$; alors $\frac{1}{MY_1} + \cdots + \frac{1}{MY_n}$ ne dépend pas de σ.

(iii) Démontrez le théorème.

Preuve : (i) Cela découle simplement du fait que l'aire de ABC est la somme de l'aire de ABM et ACM.

(ii) On applique (i) aux triangles $MC_iB_{\sigma(i)}$: $\frac{\sin(\beta+\gamma)}{MY_i} = \frac{\sin\gamma}{MB_{\sigma(i)}} + \frac{\sin\beta}{MC_i}$ où $\gamma = \widehat{CMY}$ et $\beta = \widehat{YMB}$. En additionnant ces égalités, on obtient

$$\sin(\beta+\gamma)\Big(\frac{1}{MY_1} + \cdots + \frac{1}{MY_n}\Big) = \sin\gamma\Big(\frac{1}{MB_1} + \cdots + \frac{1}{MB_n}\Big) + \sin\beta\Big(\frac{1}{MC_1} + \cdots + \frac{1}{MC_n}\Big)$$

où le membre de droite de dépend visiblement pas de σ.

(iii) Considérons $\sigma = \mathrm{Id}$; d'après le théorème du papillon « simple », on a $MX_i = MY_i$ ce qui donne le résultat. Par ailleurs d'après (ii) les sommes de l'énoncé sont indépendantes de la permutation d'où le résultat. □

5. Développements

– simplicité de $\mathcal{A}_N$ pour $n \neq 4$ [**10**]
– tout groupe simple d'ordre 60 est isomorphe à $\mathcal{A}_5$;

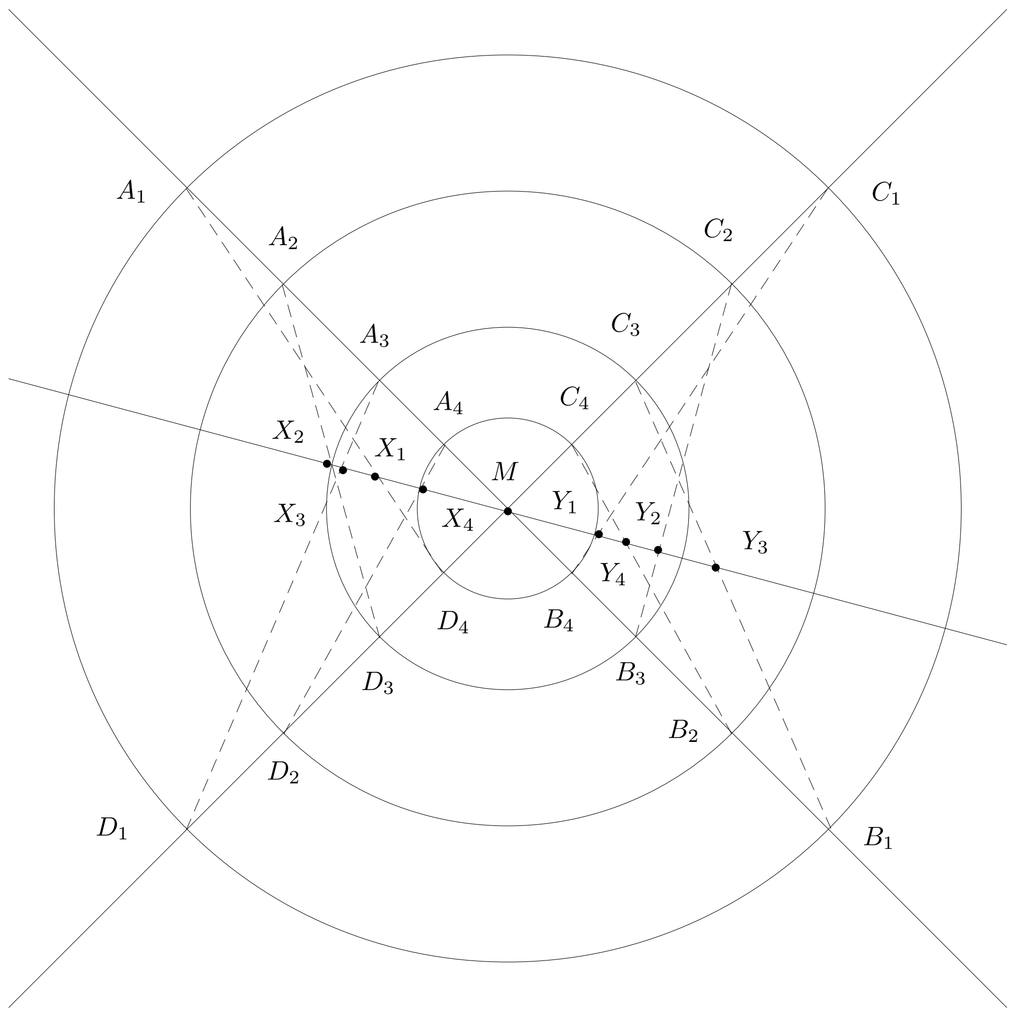

FIGURE 1.

- le groupe du cube
- les automorphisme de $\mathfrak{S}_n$ sont intérieurs lorsque $n \neq 6$ [**10**]
- théorème sur les polynômes symétriques
- deux matrices de permutations sont conjuguées si et seulement si les permutations sont conjuguées
- une présentation de $\mathfrak{S}_5$
- inégalités de Muirhead
- permanent et lemme des mariages
- transcendance de π

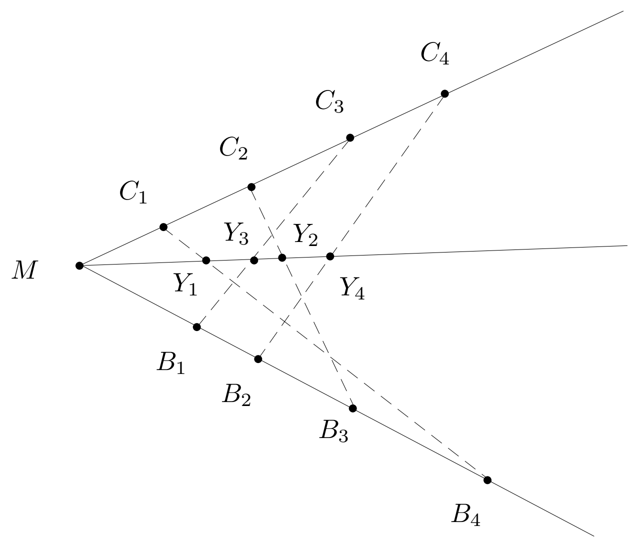

FIGURE 2.

6. Questions

- Trouvez n minimal tel que $\mathbb{Z}/p\mathbb{Z}$ (resp. $\mathbb{Z}/pq\mathbb{Z}$) est un sous-groupe de $\mathfrak{S}_n$.
- Soit G un sous-groupe résoluble de $\mathfrak{S}_n$; existe-t-il un entier k indépendant de n tel que $\sharp G \leq n^k$ (regardez les sous-groupes de Sylow de $\mathfrak{S}_n$).

7. Solutions des exercices

1.1 L'énoncé se traduit matriciellement comme suit : il existe une matrice $A \in \mathbb{M}_{2n+1}(\mathbb{R})$ telle que

- $a_{i,i} = 0$ (on met la i-ème vache de côté) ;
- $a_{i,j} = \pm 1$ si $j \neq i$ (le signe dépend dans quel sous-troupeau on met la j-ème vache quand la i-ème est de côté) ;
- $\sum_{j=1}^{2n+1} a_{i,j} = 0$ (les deux sous-troupeaux sont de même cardinal) ;
- $\sum_{j=1}^{2n+1} a_{i,j}p_j = 0$, où p_j est le poids de la j-ème vache (les deux sous-troupeaux ont même poids total).

Le résultat découle alors directement du fait suivant : toute matrice $A \in \mathbb{M}_{2n+1}(\mathbb{R})$ à coefficients diagonaux nuls, les autres étant égaux à ± 1 est de rang $2n$. En effet comme le vecteur n'ayant que des 1 est dans le noyau, le vecteur des p_i qui est aussi dans le noyau lui sera proportionnel et donc tous les p_i seront égaux. Considérons la matrice extraite B obtenue en ôtant la dernière ligne et colonne et montrons qu'elle est inversible. Son déterminant est

$$\delta = \sum_{\sigma \in \mathfrak{S}_{2n}} \epsilon(\sigma) a_{1,\sigma(1)} \cdots a_{2n,\sigma(2n)}.$$

Les termes diagonaux étant nuls, les seuls termes non nuls sont ceux pour lesquels σ est un dérangement. Par ailleurs chacun de ces termes étant égal à ± 1, il suffit de montrer que $D_n \equiv 1 \mod 2$. Comme $D_{2n-1} = (2n-2)(D_{2n-2}+D_{2n-3})$ il est pair et $D_{2n} = (2n-1)(D_{2n-1}+D_{2n-2})$ est de la même parité que D_{2n-2} ; on conclut par récurrence.

1.2 On procède comme dans le cas de $\mathfrak{S}_n$; comme $\mathcal{A}_n$ est engendré par les 3 cycles et que, pour $n \geq 5$, les 3-cycles sont tous conjugués dans $\mathcal{A}_n$, l'image d'un 3-cycle est égale à $1, j$ ou j^2 et ne dépend pas du choix du 3-cycle. Or comme le carré d'un 3-cycle est un 3-cycle, on en déduit que le seul caractère est le caractère trivial.

2.1 (1) On intègre par partie soit

$$\begin{aligned} I(f;z) &= [-e^{z(1-u)}f(zu)]_0^1 + \textstyle\int_0^1 e^{z(1-u)}zf'(zu)du \\ &= -f(z) + e^z f(0) + I(f';z); \end{aligned}$$

d'où le résultat par récurrence sur le degré de f. Pour obtenir la majoration de $|I(f;z)|$, il suffit d'intégrer sur $[0,1]$, l'inégalité

$$|ze^{z(1-u)}f(zu)| \leq |z|e^{|z|} \sum_{u\in[0,1]} |f(zu)|,$$

valable pour tout $u \in [0,1]$.

(2) Par linéarité, il suffit de considérer le cas de $f = X^m$; $f^{(m)} = m(m-1)\cdots(m-n+1)X^{m-n}$. Le polynôme $f_n := C_n^m X^{m-n}$ est à coefficients entiers et vérifie $f^{(n)} = n!f_n$.

(3) Soit m le degré de f et notons A la matrice compagnon du polynôme f/a. Par construction $aA \in \mathbb{M}_m(\mathbb{Z})$ de sorte que a^nA^n est aussi à coefficients entiers ainsi que sa trace. Or les valeurs propres de a^nA^n sont les $(a\alpha)^n$, α parcourant les racines de f avec multiplicités.

(4) On a

$$J_p = N\Big(\sum_n g^{(n)}(0)\Big) - \sum_n\Big(\sum_{f(\alpha)=0} g^{(n)}(\alpha)\Big).$$

Si $f(\alpha)=0$, α est un zéro d'ordre p de g et donc $g^{(n)}(\alpha) = 0$ pour tout $n < p$. D'autre part si $n \geq p$, d'après ce qui précède, $g_n = g^{(n)}/p!$ est un polynôme à coefficients entiers de degré $m-n$ et

$$a^{m-n} \sum_{f(\alpha)=0} g^{(n)}(\alpha)$$

est entier, multiple de $p!$. En 0, on a $g^{(n)}(0) = 0$ pour $n < p-1$ et pour $n \geq p$ alors que

$$g^{(p-1)}(0) = (p-1)!f(0)^p$$

Ainsi, il existe un entier M tel que

$$\frac{a^{m-p}}{(p-1)!}J_p = a^{m-p}Nf(0)^p + pM$$

Le second membre de cette égalité est entier et si p ne divise pas $aNf(0)$, il n'est pas multiple de p ; il est en particulier non nul et donc au moins égal à 1 en valeur absolue. Ainsi

$$|J_p| \geq (p-1)!a^{p-m} = (p-1)!p^{1-p\deg f}$$

Or la majoration de l'intégrale I dans (1) implique qu'il existe un réel $c > 0$ tel que $|J_p| \leq c^p$ pour tout p. Quand p tend vers l'infini, la formule de Stirling rend ces deux inégalités incompatibles, d'où le résultat.

(5) (a) c'est clair

(b) Les $\sum \epsilon_j \alpha_j = 0$ sont les racines du polynôme

$$P_0 = \prod_{\epsilon \in [0,1]^n} (X - \sum_j \epsilon_j \alpha_j)$$

dont les coefficients s'expriment comme des polynômes symétriques en les α_j : ce sont donc des polynômes en les fonctions symétriques élémentaires des α_j, donc en les coefficients de f. Ce sont donc des nombres rationnels.

(c) Soit un entier N tel que $NP_0 \in \mathbb{Z}[X]$ et soit $q \geq 1$ la multiplicité del a racine 0 dans P_0. On pose $P := NF_0/X^q$: c'est un polynôme à coefficients entiers avec $P(0) \neq 0$. De plus on a

$$0 \sum_{\epsilon \in [0,1]^n} \exp(\sum_j \epsilon_j \alpha_j) = q + \sum_{P(\beta)=0} e^\beta$$

ce qui contredit (4).

Références

[1] N. Bourbaki. *Groupes et algèbres de Lie : chapitres 4,5 et 6*. Masson, 1981.

[2] D. Ferrand. *Polycopié*. Université de Rennes I, 2001.

[3] S. Francinou and Gianella H. *Exercices de mathématiques pour l'agrégation algèbre 1*. Masson, 1994.

[4] F.R. Gantmacher. *Théorie des matrices tome 1*. Dunod, 1966.

[5] R. Graham, D. Knuth, and O Patashnik. *Concrete Mathematics : A Foundation for Computer Science*. Addison-Wesley, 1994.

[6] N. Jacobson. *Basic algebra I*. W H Freeman (Sd), 1974.

[7] E. Leichtnam and X. Schauer. *Algèbre 2*. Ellipses, 1998.

[8] R. Mneimné and Testard. *Introduction à la théorie des groupes de Lie classique*. Hermann.

[9] Monier. *Algèbre et géométrie, tome 2*.

[10] D. Perrin. *Cours d'algèbre*. Ellipses, 1998.

[11] V. Prasolov. *Polynomials*. Springer, 2004.

[12] Horn R. and C. Johnson. *Matrix analysis*. Cambridge University Press, 1985.

[13] Tsuzuku. *Finite groups and finite geometries*.

Pascal Boyer