Groupe symétrique

Marc SAGE

5 juillet 2006

Table des matières

1 Conjugaison dans $\mathfrak{S}_n$

Soit $(a_1, ..., a_l)$ un cycle et σ une permutation. Montrer que

$$\sigma \circ (a_1, ..., a_l) \circ \sigma^{-1} = (\sigma(a_1), ..., \sigma(a_l)).$$

En déduire que deux permutations sont conjuguées ssi elles ont le même nombres d'orbites de longueur l pour tout $l \geq 1$.

Solution proposée.

• Distinguons deux cas. Si k est un entier distinct des $\sigma(a_i)$, alors $\sigma^{-1}(k)$ n'est pas un a_i, donc est fixe par le cycle $(a_1, ..., a_l)$, d'où

$$\begin{aligned} \sigma \circ (a_1, ..., a_l) \circ \sigma^{-1}(k) &= \sigma \circ (a_1, ..., a_l)\left(\sigma^{-1}(k)\right) \\ &= \sigma\left(\sigma^{-1}(k)\right) \\ &= k \\ &= (\sigma(a_1), ..., \sigma(a_l))(k). \end{aligned}$$

Si maintenant k vaut un $\sigma(a_i)$, alors

$$\begin{aligned} \sigma \circ (a_1, ..., a_l) \circ \sigma^{-1}(k) &= \sigma \circ (a_1, ..., a_l) \circ \sigma^{-1}(\sigma(a_i)) \\ &= \sigma \circ (a_1, ..., a_l)(a_i) \\ &= \sigma(a_{i+1}), \end{aligned}$$

les indices étant évidemment pris modulo l. Dans les deux cas, on a l'égalité annoncée.

• Soit σ et σ' conjuguées dans $\mathfrak{S}_n$, mettons $\sigma' = \varphi\sigma\varphi^{-1}$. En décomposant $\sigma = \prod \gamma_i$ en produit de cycles à supports disjoints, on obtient

$$\sigma' = \varphi\left(\prod \gamma_i\right)\varphi^{-1} = \prod \varphi\gamma_i\varphi^{-1} = \prod \gamma_i'$$

où $\gamma_i' := \varphi\gamma_i\varphi^{-1}$ est un cycle de longueur celle de γ_i par ce qui précède, et tous les γ_i' sont à supports disjoints : en effet, si $\gamma_i = \left(a_1^i, ..., a_{l_i}^i\right)$, alors $\gamma_i' = \left(\varphi\left(a_1^i\right), ..., \varphi\left(a_{l_i}^i\right)\right)$, et il suffit d'invoquer l'injectivité de φ. On a donc obtenu la décomposition de σ' en produit de cycles à supports disjoints, d'où le premier sens.

Supposons à présent que $\begin{cases} \sigma = \prod \gamma_i \\ \sigma' = \prod \gamma_i' \end{cases}$ sont des décompositions en produit de cycles à supports disjoints avec γ_i et γ_i' ayant même longueur pour tout i. Définissons une permutation φ comme suit : si $\begin{cases} \gamma_i = (a_1, ..., a_l) \\ \gamma_i' = (a_1', ..., a_l') \end{cases}$, on pose $\varphi(a_i) = a_i'$, et on complète φ en dehors des supports des γ_i par n'importe quoi d'injectif (l'hypothèse d'égalité des longueurs des orbites assure que cela est possible). Intérêt de la chose ? Pouvoir écrire

$$\varphi\gamma_i\varphi^{-1} = \varphi(a_1, ..., a_l)\varphi^{-1} = (\varphi(a_1), ..., \varphi(a_l)) = (a_1', ..., a_l') = \gamma_i',$$

d'où

$$\varphi\sigma\varphi^{-1} = \varphi\left(\prod \gamma_i\right)\varphi^{-1} = \prod \varphi\gamma_i\varphi^{-1} = \prod \gamma_i' = \sigma',$$

ce qui montre que σ et σ sont conjuguées.

Remarque. L'identité de conjugaison est extrèmement pratique, il vaut mieux donc la retenir :

$$\sigma \circ (a_1, ..., a_l) \circ \sigma^{-1} = (\sigma(a_1), ..., \sigma(a_l)).$$

La cns obtenue pour que deux permutations soient conjuguées est *elle aussi* à connaître.

2 Dual de $\mathfrak{S}_n$

Soit $n \geq 2$: déterminer tous les morphismes de groupes de $\mathfrak{S}_n$ dans $\mathbb{C}^*$.

Solution proposée.

Soit f un tel morphisme. Pour connaitre f, il suffit de le connaitre sur des générateurs de $\mathfrak{S}_n$; prenons par exemple les transpositions. Un transposition étant d'ordre 2, toutes les transpositions sont envoyées sur 1 ou -1. Montrons qu'en fait les transpositions ont même image par f, ce qui ne laissera que deux possibilités pour f : la signature (cas où les transpositions sont envoyées sur -1) et l'identité.

Remarquons tout d'abord que deux éléments conjugués ont même image par f, vu que le groupe d'arrivée est abélien :

$$f\left(\varphi\sigma\varphi^{-1}\right) = f(\varphi) f(\sigma) f\left(\varphi^{-1}\right) = f(\varphi) f(\varphi)^{-1} f(\sigma) = f(\sigma).$$

Ensuite, pour i, j, k distincts, on a

$$(k,j)(i,j)(k,j)^{-1} = (i,k)$$

(utiliser par exemple l'identité de conjugaison), ce qui montre d'après la remarque que $f(i,j)$ est indépendant de $j \neq i$; soit ε_i cette valeur commune. Or, par symétrie, on a pour tout $i \neq j$

$$\varepsilon_i = f(i,j) = f(j,i) = \varepsilon_j.$$

Finalement, $f(i,j)$ ne dépend ni de i ni de j, donc est constant, *CQFD.*

3 Signature du Frobenius

• *Soit E et F deux ensembles avec $|E| \geq 2$. À une permutation $\sigma \in \mathfrak{S}(E)$ on associe la permutation $\widetilde{\sigma} \in \mathfrak{S}\left(F^E\right)$ qui envoie u sur $u \circ \sigma^{-1}$. Montrer que*

$$\varepsilon(\widetilde{\sigma}) = \varepsilon(\sigma)^{\frac{|F|(|F|-1)}{2}|F|^{|E|-2}}.$$

• *En déduire la signature du Frobenius défini par*

$$\mathrm{Fr} : \left\{ \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ x & \longmapsto & x^p \end{array} \right.$$

où $\mathbb{F}_q$ est un corps à $q = p^n$ éléments avec p la caractéristique de $\mathbb{F}_q$. On admettra l'existence d'une $\mathbb{F}_p$-base de $\mathbb{F}_q$ qui est une orbite sous l'action de Fr.

Solution proposée.

• On regarde l'image $\widetilde{\tau}$ d'une transposition $\tau = (i,j)$. Via la bijection

$$\left\{ \begin{array}{ccc} F^E & \longrightarrow & F^{E\setminus\{i,j\}} \times F \times F \\ u & \longmapsto & \left(u_{|E\setminus\{i,j\}}, u(i), u(j)\right) \end{array} \right. ,$$

on regarde $\widetilde{\tau}$ comme une permutation de $F^{E\setminus\{i,j\}} \times F \times F$. Soit $u \in F^E$, que l'on représente par (v,a,b) via la bijection ci-dessus. $\widetilde{\tau}$ envoie alors u sur

$$u \circ \tau^{-1} : \left\{ \begin{array}{c} i \mapsto u(j) = b \\ j \mapsto u(i) = a \\ \text{le reste est fixe} \end{array} \right. ,$$

d'où $\widetilde{\tau}(v,a,b) = (v,b,a)$. À v fixé, on a donc $|F|$ orbites triviales pour les (a,a) et $\frac{|F|(|F|-1)}{2}$ orbites à 2 éléments pour $(a,b) \mapsto (b,a)$. Faire varier v multiplie le nombre d'orbites par $|F|^{|E|-2}$, d'où le résultat.

• Notons $B = \left(a, a^p, a^{p^2}, ..., a^{p^{n-1}}\right)$ la base donnée par l'énoncé. On a donc une bijection $\mathbb{F}_q \simeq \mathbb{F}_p^B$, et dans $\mathbb{F}_p^B$ le Frobenius a pour action

$$(\lambda_1, ..., \lambda_n) \mapsto (\lambda_n, \lambda_1, ..., \lambda_{n-1}) :$$

en effet, en observant que Fr est un morphisme additif (développer le binôme, les coefficients binomiaux son presque tous multiples de p), on a

$$\mathrm{Fr}\left(\sum_{i=1}^n \lambda_i a^{p^{i-1}}\right) = \left(\sum_{i=1}^n \lambda_i a^{p^{i-1}}\right)^p = \sum_{i=1}^n \left(\lambda_i a^{p^{i-1}}\right)^p = \sum_{i=1}^n \lambda_i^p a^{p^{i-1}p} = \sum_{i=1}^n \lambda_i a^{p^i}.$$

En notant γ le n-cycle $(1,2,...,n)$ l'application du premier point

$$\left\{\begin{array}{ccc}\mathfrak{S}(B) & \longrightarrow & \mathfrak{S}\left(\mathbb{F}_p^B\right)\\ \sigma & \longmapsto & \widetilde{\sigma}\end{array}\right.$$

envoie par conséquent γ sur Fr, d'où pour $n \geq 2$

$$\varepsilon(\mathrm{Fr}) = \varepsilon(\gamma)^{\frac{p(p-1)}{2}p^{n-2}} = (-1)^{(n-1)\frac{p(p-1)}{2}p^{n-2}}.$$

Pour $n = 1$, Fr vaut l'identité, donc la formule reste valide.

4 Les automorphismes de $\mathfrak{S}_n$ sont intérieurs pour $n \neq 6$

Rappelons qu'un automorphisme *intérieur* d'un groupe est un morphisme du type $i_a : g \mapsto aga^{-1}$ où a est un élément du groupe. On se propose de montrer que les automorphismes du groupe symétrique $\mathfrak{S}_n$ sont tous intérieurs si $n \neq 6$.

Soit $\varphi \in \mathrm{Aut}\,\mathfrak{S}_n$ où $n \geq 2$ et $n \neq 6$.

• *Montrer que si φ stabilise les transpositions, alors φ est intérieur.*

• *On se donne une permutation $\sigma \in \mathfrak{S}_n$, dont on note c_l le nombre d'orbites de longueur l pour $l = 1,...,n$. Soit* $\mathrm{Comm}\,\sigma$ *l'ensemble des permutations qui commutent avec σ – on l'appelle le* commutant *de σ. Montrer que son cardinal est donné par la formule*

$$\#\,\mathrm{Comm}\,\sigma = \prod_{l=1}^{n} c_l! l^{c_l}.$$

• *Conclure en regardant l'action de φ sur le commutant d'une transposition.*

Solution proposée.

• Pour déterminer φ, on regarde son action sur des générateurs de $\mathfrak{S}_n$. Comme on a déjà des informations sur les transpositions (système de générateurs standard), on raffine en ne regardant que les $(1,i)$.

Le point à remarquer est que, puisque $(1,2)$ et $(1,3)$ ne commutent pas, leur image par φ ne commutent pas non plus ; or, ces dernières étant par hypothèse des transpositions, leurs supports doivent se rencontrer, et ne peuvent coïncider par injectivité de φ. On peut donc écrire

$$\left\{\begin{array}{l}\varphi(1,2) = (\alpha_1,\alpha_2)\\ \varphi(1,3) = (\alpha_1,\alpha_3)\end{array}\right. \text{ où } \alpha_1,\alpha_2,\alpha_3 \text{ sont distincts.}$$

Pour les même raisons que précédemment, le support de $\varphi(1,i)$ pour $i \geq 4$ doit rencontrer ceux de $\varphi(1,2)$ et $\varphi(1,3)$ en un point chacun. On va éliminer trois des quatre cas possibles, pour ne garder que α_1 comme point en commun, ce afin de pouvoir écrire

$$\varphi(1,i) = (\alpha_1,\alpha_i) \text{ où } \alpha_i \neq \alpha_1,\alpha_2.$$

Déjà, l'un des points en commun doit être α_1, sinon le support de $\varphi(1,i)$ contiendrait $\{\alpha_2,\alpha_3\}$ et $\varphi(1,i)$ vaudrait (en utilisant l'identité de conjugaison)

$$(\alpha_2,\alpha_3) = (\alpha_1,\alpha_3)(\alpha_1,\alpha_2)(\alpha_1,\alpha_3) = \varphi[(1,3)(1,2)(1,3)] = \varphi(2,3),\ \textit{absurde}$$

par injectivité de φ. Pour éliminer les deux autres cas, on peut par exemple supposer que le support de $\varphi(1,i)$ rencontre celui de $\varphi(1,2)$ en α_1 et celui de $\varphi(1,3)$ en α_3. On en déduirait de le même façon

$$\varphi(1,i) = (\alpha_1,\alpha_3) = \varphi(1,3),\ \textit{absurde car } i \geq 4.$$

On obtient ainsi une permutation α de $\{1,...,n\}$, toujours par l'injectivité de φ. α étant la seule permutation qui se soit naturellement distinguée dans ce raisonnement, nous sommes moralement obliger de vérifier si φ est intérieur relativement à α :

$$\alpha \circ (1,i) \circ \alpha^{-1} = (\alpha(1),\alpha(i)) = (\alpha_1,\alpha_i) = \varphi(1,i)\ ;$$

les $(1,i)$ engendrant $\mathfrak{S}_n$, on a gagné.

• Cassons σ en produit de cycles à supports disjoints :

$$\sigma = \prod_{l=1}^{n} \prod_{i=1}^{c_l} \gamma_i^l.$$

On doit donc avoir, pour $c \in \operatorname{Comm} \sigma$:

$$\sigma = c\sigma c^{-1} = \prod_{l=1}^{n} \prod_{i=1}^{c_l} c\gamma_i^l c^{-1}.$$

En invoquant l'unicité de la décomposition de σ, on voit que, à l fixé, d'une part c permute les supports des γ_i^l, ce pour garder les mêmes longueurs (d'où $c_l!$ choix), d'autre part le cycle $c\gamma_i^l c^{-1}$ est entièrement déterminé par l'image par c d'un seul élément du support de γ_i^l, l'ordre imposé par le cycle γ_i^l imposant le reste par l'identité de conjugaison (d'où l choix pour chaque cycle, *i.e.* l^{c_l} pour tous les cycles). Ploum.

• Considérons une transposition τ. Montrons que $\varphi(\tau)$ est une transposition, ce qui concluera par le premier point. Déjà, $\varphi(\tau)$ est d'ordre 2, donc se casse en un produit de disons $p \leq \frac{n}{2}$ transpositions à supports disjoints. On veut $p = 1$. Par ailleurs, on vérifie aisément que

$$\varphi(\operatorname{Comm} \tau) = \operatorname{Comm} \varphi(\tau),$$

ce qui nous incite à prendre les cardinaux (φ est bijective !) afin d'appliquer le second point :

$$\begin{aligned}
\#\operatorname{Comm} \tau &= \#\operatorname{Comm} \varphi(\tau) \\
(n-2)! \times 2 &= (n-2p)! \times p! \times 2^p \\
2^{p-1} &= \frac{(n-2)!}{(n-2p)!p!} = \frac{(n-2)!}{(n-2p)!\,(2p-2)!} \frac{(2p-2)!}{p!} \\
&= \binom{n-2}{2p-2} (2p-2)(2p-3)...(p+1).
\end{aligned}$$

Pour $p \geq 4$, *i.e.* $2p-2 > p-1$, le produit $(2p-2)(2p-3)...(p+1)$ contient au moins deux termes consécutifs, donc un terme impair, ce qui est impossible vu le membre de gauche.

Pour $p = 3$, on obtient

$$4 = \binom{n-2}{4} 4 \implies n = 6 \text{ ou } 2,$$

mais on doit avoir $p \leq \frac{n}{2}$ et $n \neq 6$, d'où contradiction.

Pour $p = 2$, on obtient

$$2 = \binom{n-2}{2} = \frac{(n-2)(n-3)}{2},$$

ce qui est absurde par des arguments de parité.

Le seul cas possible est donc $p = 1$, *CQFD.*

Remarque. L'hypothèse $n \neq 6$ est cruciale, puisque $(n,p) = (6,3)$ satisfait à l'équation ci-dessus, et surtout parce que l'on peut trouver des automorphismes de $\mathfrak{S}_6$ qui ne soient pas intérieurs – voir la construction de Pierre-Loïc Méliot sur sa page web.

5 Matrices de permutation et théorème de Brauer

Soit $n \geq 1$ un entier. À une permutation $\sigma \in \mathfrak{S}_n$ on associe la matrice $P_\sigma \in \mathcal{M}_n(K)$ qui permute les vecteurs $e_1, ..., e_n$ de la base canonique de K^n selon l'action de σ :

$$P_\sigma e_i = e_{\sigma(i)}.$$

Noter que le corps de base n'intervient pas vraiment, puisque P_σ ne contient que des 0 et 1. Par exemple, la matrice associé au n-cyle $\gamma = (1, 2, ..., n)$ est

$$P_\gamma = \begin{pmatrix} 0 & & & 1 \\ 1 & \ddots & & 0 \\ & \ddots & 0 & \vdots \\ & & 1 & 0 \end{pmatrix}$$

(qui est une matrice cyclique, comme quoi les terminologie se retrouvent...) et son polynôme caractéristique vaut $X^n - 1$. On vérifie par ailleurs aisément que $P : \mathfrak{S}_n \longrightarrow GL_n(K)$ est un morphisme de groupes :

$$\begin{cases} P_{\sigma\sigma'} = P_\sigma P_{\sigma'} \\ P_{\sigma^{-1}} = P_\sigma^{-1} \end{cases}.$$

Notre but est de donner deux démonstrations du théorème suivant.

Théorème (Brauer).
Soit K un corps quelconque. Deux permutations σ et σ' de $\mathfrak{S}_n$ sont conjuguées ssi les matrices de permutation associées P_σ et $P_{\sigma'}$ sont conjuguées dans $GL_n(K)$.

Première démonstration.
On suppose ici que K est de caractéristique nulle.
• *Trivialiser l'un des sens.*
• *Décrire le polynôme caractéristique de P_σ en fonction de la décomposition de σ en produit de cycles à supports disjoints.*
• *On considère L un corps de décomposition de $\prod_{l=1}^n (X^l - 1)$ sur K. Montrer que le groupe μ_l des racines l-ièmes de l'unité est cyclique pour tout l. On pourra admettre (ou redémontrer) que le ppcm des ordres des éléments d'un groupe fini est atteint par un élément du groupe.*
• *Conclure en raisonnant sur l'ordre des racines des polynômes caractérisitiques des P_σ dans L.*

Deuxième démonstration.
On laissera un sens aux bons soins du lecteur...
• *Soit $r \geq 1$ un entier. Si γ est un cyle de longueur l, déterminer la décomposition de γ^r à conjugaison près (*i.e. *le nombre d'orbites et leur longueur). En déduire le nombre d'orbites de σ^r où σ est une permutation quelconque.*
• *En regardant les points fixes des itérées de P_σ, montrer que*

$$\forall r \geq 1,\ \sum_{l=1}^n (l \wedge r)\, c_l = \sum_{l=1}^n (l \wedge r)\, c'_l$$

avec les notations évidentes de l'exercice précédent.
• *Conclure en interprétant la relation ci-dessus matriciellement. On pourra utiliser la formule $n = \sum_{d|n} \varphi(d)$ où φ est l'indicatrice d'Euler.*

Solution proposée.
• P étant un morphisme, le sens direct est trivial :

$$\sigma' = \varphi\sigma\varphi^{-1} \implies P_{\sigma'} = P_{\varphi\sigma\varphi^{-1}} = P_\varphi P_\sigma P_\varphi^{-1}.$$

• Cassons $\sigma = \prod_{l=1}^n \prod_{i=1}^{c_l} \gamma_i^l$ en produit de cycles à supports disjoints. Quitte à conjuguer par une bonne permutation, ce qui ne change pas le polynôme caractéristique, on peut ordonner les supports des cycles selon la longueur de ces derniers. Matriciellement, cela revient à dire que P_σ est diagonale par blocs avec c_1 blocs (1), c_2 blocs $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$, ..., c_l blocs $\begin{pmatrix} 0 & & & 1 \\ 1 & \ddots & & 0 \\ & \ddots & 0 & \vdots \\ & & 1 & 0 \end{pmatrix}$ de taille l, et ainsi de suite. Il est alors immédiat que

$$\chi_{P_\sigma} = \prod_{l=1}^n \left(X^l - 1\right)^{c_l}.$$

• Déjà, μ_l est de cardinal l. En effet, μ_l est exactement l'ensemble des racines de X^l-1 sur L, donc $\#\mu_l \leq n$, l'inégalité inverse s'obtenant en remarquant que les racines de X^l-1 sont toutes simples (sinon la dérivée de X^l-1 s'annulerait en un $\xi \in \mu_l$, *i.e.* $l\xi^{l-1}=0$, ce qui est *absurde* vu que K est de caractéristique nulle).

Ensuite, si par l'absurde μ_l n'était pas cyclique, tous ses élément seraient d'un ordre $< l$, donc le ppcm m de ces ordres également puisqu'il est atteint. Mais alors X^m-1 s'annulerait sur μ_l, d'où $l > m$ racines pour ce polynôme qui hurlerait à la contradiction.

• P_σ et $P_{\sigma'}$ étant semblables, elles ont même polynôme caractéritique. D'après le point qui précède, on obtient

$$\prod_{l=1}^{n} \left(X^l-1\right)^{c_l} = \prod_{l=1}^{n} \left(X^l-1\right)^{c'_l}.$$

Pour montrer que σ et σ' sont conjuguées, on doit montrer que $c_l = c'_l$ pour tout l. Soit $1 \leq \lambda \leq n$ fixé et $\xi \in \mu_\lambda$ un élément d'ordre λ (on parle de racine *primitive* λ-ième de l'unité, *i.e.* qui engendre μ_λ). Regardons comme suggéré l'ordre de la racine ξ dans les polynômes ci-dessus. Puisqu'on a les équivalences

$$\xi \text{ racine de } X^l-1 \iff \xi^l = 1 \iff \text{l'ordre de } \xi \text{ divise } l \iff \lambda \mid l,$$

on en déduit l'ordre recherché :

$$\sum_{\lambda|l} c_l = \sum_{\lambda|l} c'_l$$

(on a déjà dit pourquoi les racines des X^l-1 étaient simples). Ceci tenant pour tout $1 \leq l \leq n$, on en déduit l'égalité recherchée $c_l = c'_l$ pour tout l : considérer sinon le plus petit l tel que $c_l \neq c'_l$ pour obtenir une absurdité.

• Le premier sens se traite comme précédemment.

• Soit γ un cycle de longueur l, que l'on peut supposer (quitte à conjuguer par une bonne permutation, ce qui ne change pas la longueur des cycles dans la décomposition de γ) être $(1, 2, ..., l)$.

Si $r \mid l$, disons $l = kr$, il est facile d'expliciter γ^r :

$$\begin{aligned} \gamma^r &= (r+1, 2r+1..., kr+1)\,(r+2, 2r+2, ..., kr+2)\,...\,(r+(k-1), 2r+(k-1), ..., kr+(k-1)) \\ &\sim (1, ..., k)\,(k+1, ..., 2k)\,...\,((r-1)k+1, ..., rk), \end{aligned}$$

d'où r orbites de longueur k.

Dans le cas général, on introduit le pgcd $\delta = l \wedge r$ pour se ramener au cas précédent. Bézout nous donne deux entiers a et b tels que $al + br = \delta$. On en déduit

$$\begin{cases} \gamma^r = \left(\gamma^\delta\right)^{\frac{r}{\delta}} \\ \gamma^\delta = \left(\gamma^l\right)^a \left(\gamma^r\right)^b = \left(\gamma^r\right)^b \end{cases},$$

de sorte que les sous-groupes $\langle \gamma^r \rangle$ et $\left\langle \gamma^\delta \right\rangle$ de $\mathfrak{S}_n$ sont identiques. Or, les orbites d'une permutations $\sigma \in \mathfrak{S}_n$ peuvent être décrites comme les parties de $\{1, ..., n\}$ stables par $\langle \sigma \rangle$ et minimales pour cette propriété. On en déduit que γ^r et γ^δ ont mêmes orbites. Puisque $\delta \mid l$, γ^δ (et donc γ^r) se décompose par ce qui précède en δ orbites de longueur $\frac{l}{\delta}$.

Soit maintenant $\sigma = \prod_{l=1}^{n} \prod_{i=1}^{c_l} \gamma_i^l$ une permutation quelconque (avec les notations évidentes). Puisque les γ_i^l commutent (ils sont à supports disjoints), le calcul de σ^r est aisé :

$$\sigma^r = \prod_{l=1}^{n} \prod_{i=1}^{c_l} \left(\gamma_i^l\right)^r.$$

En appliquant ce qui précède, on voit que chaque $\left(\gamma_i^l\right)^r$ fournit $l \wedge r$ orbites de longueur $\frac{l}{l \wedge r}$ chacune, d'où le nombre d'orbites de σ^r :

$$\#\left\{\text{orbites de } \sigma^r\right\} = \sum_{l=1}^{n} c_l\,(l \wedge r).$$

• Supposons P_σ et $P_{\sigma'}$ conjuguées, disons $P_{\sigma'} = PP_\sigma P^{-1}$. En itérant, il vient $P_{\sigma'}^r = PP_\sigma^r P^{-1}$ pour tout $r \geq 1$, d'où en prenant les points fixes

$$\operatorname{Fix} P_{\sigma'}^r = P\left(\operatorname{Fix} P_\sigma^r\right).$$

En fait, on va considérer les points fixes sur un corps fini, mettons $\mathbb{F}_2$, ce afin de faire du dénombrement. Ceci étant dit, un vecteur de $\mathbb{F}_2^n$ est fixe par P_σ ssi ses coordonnées sont constantes sur les orbites de σ, ce qui montre que

$$\#\operatorname{Fix} P_\sigma = 2^{\{\text{orbites de } \sigma\}}.$$

En prenant les cardinaux dans la relation ci-dessus (P est bijective !), on obtient que σ^r et σ'^r ont le même nombre d'orbites pour tout r. En utilisant le point précédant, il vient

$$\sum_{l=1}^{n} c_l \,(l \wedge r) = \sum_{l=1}^{n} c'_l \,(l \wedge r) \ \text{ pour tout } r \geq 1.$$

• On introduit les matrices $\left\{ \begin{array}{l} C_{i,j} = c_j \\ C'_{i,j} = c'_j \end{array} \right.$ et la matrice $[A]_{i,j} = i \wedge j$, de sorte que le nombre d'orbites de σ^r s'exprime par la formule matricielle

$$\sum_{j=1}^{n} c_j \,(j \wedge k) = \sum_{j=1}^{n} [C]_{i,j} \,[A]_{j,k} = [AC]_{i,k} \ \text{ pour tout } \ (i,k)\,.$$

On en déduit $AC = AC'$. Pour conclure, il suffit d'inverser A. Or, en cherchant à écrire A comme le produit de deux matrices gentilles (par exemple triangulaires), on est amené à utiliser l'identité donnée dans l'énoncé comme suit :

$$i \wedge j = \sum_{d \mid i \wedge j} \varphi\,(d) = \sum_{d \mid i \text{ et } d \mid j} \varphi\,(d) = \sum_{d=1}^{n} \Phi_{d,i} \Phi_{d,j}$$

où Φ est triangulaire supérieure définie par $[\Phi]_{p,q} = \left\{ \begin{array}{l} \varphi\,(p) \ \text{ si } p \mid q \\ 0 \text{ sinon} \end{array} \right.$. Ceci s'écrit encore $[A]_{i,j} = [{}^t\Phi\Phi]_{i,j}$ pour tout (i,j), d'où

$$\det A = \det \Phi^2 = \prod_{i=1}^{n} \varphi\,(i)^2 \neq 0, \ \textit{CQFD.}$$

Remarque. Pour montrer que le ppcm des ordres des éléments d'un groupe (appelé *exposant*) fini G est atteint par un élément de G, on peut raisonner comme suit.

On casse $\#G = \prod_{i=1}^{r} p_i^{\alpha_i}$ en produit de facteurs premiers, et on considère G_i l'ensemble des éléments de G dont l'ordre est une puissance de p_i. G_i est non vide car contient toujours le neutre, donc on peut considérer $g_i \in G_i$ d'ordre maximal $p_i^{\gamma_i}$. Le produit $g_0 = \prod g_i$ est alors d'ordre $\prod p_i^{\gamma_i}$ puisque les p_i sont premiers entre eux.

Soit maintenant un $g \in G$, d'ordre disons $\prod p_i^{\beta_i}$. Alors g élevé à la puissance $\prod_{j \neq i} p_j^{\beta_j}$ est d'ordre $p_i^{\beta_i}$, d'où $\beta_i \leq \gamma_i$ par maximalité de γ_i. Ceci tenant pour tout i, l'ordre de g divise celui de g_0, ce qui montre que l'exposant de G est exactement l'ordre de g_0.

Remarque. On peut se demander si la finitude de l'exposant entraine celle de l'ordre du groupe (*problème de Burnside*). La réponse est non dans le cas général, bien que les contre-exemples soient loin d'être triviaux, mais est positive pour les sous-groupes de $GL_n\,(\mathbb{C})$ (cf. feuille sur la réduction).