Groupe de permutations-105

Tagline : Le groupe des permutations $\mathfrak{S}_n$ d'un ensemble fini prend une place particulière parmi les groupes finis. En effet, tout groupe agissant sur un ensemble fini s'envoie dans le groupe $\mathfrak{S}_n$. En particulier, en faisant agir à gauche un groupe G d'ordre n sur lui-même, on obtient une injection de G dans $\mathfrak{S}_n$.

1 Etude du groupe

Constatation de départ : un algébriste ne fait pas la difference entre $\mathfrak{S}(E)$ et $\mathfrak{S}_n$, mais c'est moins pire qu'un topologue qui ne fait pas la différence entre un beignet et une tasse de café ! Pire au quotidien, j'entends.

Ordre du groupe $\mathfrak{S}_n$: $n!$

• Formule de conjugaison

On écrit les cycles sous la forme $(i_1 \cdots i_k)$. Attention, il y a k écritures différentes pour le même cycle.

$$\sigma(i_1 \cdots i_k)\sigma^{-1} = (\sigma(i_1) \cdots \sigma(i_k)).$$

• Décomposition en cycles à supports disjoints. Exposant, Générateurs

On a existence et unicité à permutation près de la décomposition en cycles. On en déduit que l'exposant du groupe est le ppcm de $\{1, 2, \cdots, n\}$. Il en décole également que les cycles constituent un système de générateurs, puis, les transpositions, grâce à la formule

$$(i_1 i_2 \cdots i_k) = (i_1 i_2) \cdots (i_{k-1} i_k)$$

Les transpositions de type $(kk+1)$ forment un système de générateurs (avec relations de tresses*). Pour finir, il faut noter le système de générateurs le plus petit possible (mais dont les relations sont compliquées) donné par (12) et $(12 \cdots n)$.

• Classes de conjugaison-paramétrisation, cardinal

Grâce à la décomposition (unique) en cycles, on peut paramétrer les classes de conjugaison via les longueurs de cycles. On peut supposer les longueurs λ_i des cycles décroissantes, de sorte que $\lambda = (\lambda_1, \cdots, \lambda_s)$ est la partition associée à la classe de conjugaison de σ. Le nombre de classes de conjugaison de $\mathfrak{S}_n$ est donc égal au nombre $p(n)$ de partitions de n, donné par la série génératrice

$$\sum_{n\geq 0} p(n) z^n = \prod_{k\geq 1} \frac{1}{1-z^k}.$$

Le cardinal d'une classe est donnée par

Proposition* Soit σ une permutation de $\mathfrak{S}_n$ associée à une partition $\lambda := (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_s)$ de n. Soit $a_j(\lambda)$ le nombre de fois où j apparaît dans la partition λ, c'est-à-dire, le nombre de supports de cycles C_i de cardinal j. Alors, le cardinal de la classe de conjugaison de σ est égal à

$$|\mathcal{C}_\sigma| = \frac{n!}{\prod_j a_j(\lambda)! j^{a_j(\lambda)}}.$$

• Caractères (morphismes) de $\mathfrak{S}_n$ dans le groupe multiplicatif $\mathbb{C}^*$.

En utilisant le système de générateurs donné par les transpositions, on montre qu'il y a au plus deux tels morphismes (dont un trivial). On peut ensuite exhiber le morphisme

$$\epsilon(\sigma) = \prod_{1\leq i<j\leq n} \frac{\sigma(j)-\sigma(i)}{j-i} = \prod_{\{i,j\}\in\mathcal{P}_{2,n}} \frac{\sigma(j)-\sigma(i)}{j-i},$$

où $\mathcal{P}_{2,n}$ désigne l'ensemble des parties de $\{1, \cdots, n\}$ à 2 éléments. On doit noter au passage que $\frac{\sigma(j)-\sigma(i)}{j-i}$ est bien défini pour $\{i,j\} \in \mathcal{P}_{2,n}$, car il ne dépend pas de l'ordre dans lequel on a choisi i et j.

Du coup, on introduit le groupe alterné $\mathfrak{A}_n := \ker \epsilon$.

• Automorphismes de $\mathfrak{S}_n$

En utilisant le cardinal des classes de conjugaison d'éléments d'ordre 2, on obtient que tout automorphisme est intérieur (en montrant que toute transposition s'envoie sur une transposition, voir le Perrin), sauf pour $n = 6$ où l'on a une exception numérique entre transpositions et 3-transpositions.

$$\frac{6!}{4!2^1} = \frac{6!}{3!2^3}$$

2 Sous-groupes de $\mathfrak{S}_n$

• Le centre

Le centre de $\mathfrak{S}_n$ est trivial pour $n \neq 2$. C'est juste une application de la formule de conjugaison.

• Le groupe dérivé=le groupe alterné, qui est engendré par les 3-cycles. Moralité, c'est toujours ceux qui en bougent le moins qui engendrent le plus. $D(\mathfrak{S}_n) = \mathfrak{A}_n$. L'inclusion directe est évidente. Pour l'inclusion inverse, on le fait en deux temps : d'une part les 3-cycles engendrent $\mathfrak{A}_n$ et d'autre part on vérifie qu'ils sont bien dans $D(\mathfrak{S}_n)$.

C'est très utile : on obtient souvent des morphismes qui partent de $\mathfrak{S}_n$ (par des actions de groupes), puis, que l'on dérive.

• Le seul sous-groupe d'indice 2 de $\mathfrak{S}_n$ est $\mathfrak{A}_n$.

• Simplicité du groupe alterné.

On montre qu'un sous-groupe distingué contient un 3-cycle, puis, il les contient tous. C'est historique dans la non résolution par radicaux d'une équation de degré 5.

• Tout sous-groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$ (mais pour $n = 6$ il peut ne pas être le stabilisateur d'un élément). Bien connaître la preuve qui passe par l'action d'un groupe G sur ses classes G/H.

• Groupe dérivé du groupe alterné. C'est toujours lui-même sauf pour $n = 3$ (groupe trivial) et $n = 4$ (le groupe de Klein).

3 Applications

3.1 Actions du groupe symétrique

Il faut remarquer que $\mathfrak{S}_n$, à l'instar de $\mathrm{GL}_n(\mathbb{K})$, arrive avec une action naturelle. Elle est n-transitive, ce qui constitue un record absolu, quand on sait à quel point la triple-transitivité est rare dans la nature.

• Théorème de Cayley

• Polynômes symétriques

On a une action par automorphismes de $\mathfrak{S}_n$ sur l'algèbre des polynômes à n indéterminées. La sous-algèbre des invariants est l'algèbre des polynômes symétriques. Parmi eux, il y a les polynômes symétriques élémentaires et les polynômes de Newton. Les premiers sont importants car ils engendrent la sous-algèbre des invariants (en toute caractéristique, et même sur $\mathbb{Z}$!) De

plus, les fonctions symétriques élémentaires en les racines d'un polynôme unitaire sont les coefficients du polynôme.

• Représentations du groupe symétrique : la triviale, la signature, la naturelle (matrices de permutation), la standard (liée à la double transitivité de l'action naturelle de $\mathfrak{S}_n$, ce qui consitute un joli développement, voir [H2G2, tome 2]).

Au programme de l'agrégation, on n'est pas censé connaître les représentations de $\mathfrak{S}_n$, mais seulement quelques unes. Il est bon de savoir calculer la table de caractères pour $n \leq 5$.

• La table des caractères de $\mathfrak{S}_n$ est à coefficients dans $\mathbb{Z}$.

3.2 Autres applications

• Le déterminant.

Sans signature pas de déterminant. Ce serait dommage ! En fait, l'unicité d'une forme n-linéaire alternée à constante près sur un espace vectoriel de dimension n est assez claire, mais l'existence, pas du tout. Cela provient essentiellement de l'existence de la signature.

• Représentation du groupe du tétraèdre ou du groupe de l'icosaèdre.

• Le problème des prisonniers*

En gros, on itère une bijection d'un ensemble à $2m$ éléments et on veut retomber sur l'élément de départ au bout de m itérations.

Développements possibles :

• $\mathfrak{A}_5$ est le seul groupe simple d'ordre 60.

On fait agir G sur ses six 5-Sylow. On obtient alors un morphisme non trivial de G dans $\mathfrak{S}_5$, que l'on dérive.

• $\mathfrak{A}_n$ est simple pour $n \neq 4$.

• Représentation de $\mathfrak{S}_4$ via le groupe du tétraèdre.

Le groupe G des isométries du tétraèdre régulier agit sur les quatre sommets. Cela fournit donc un morphisme de G dans $\mathfrak{S}_4$ qui se trouve être iso. L'action de $\mathfrak{S}_4 \simeq G$ sur les sommets-paires d'arêtes-faces fournissent de jolies représentations.

• Les caractères du groupe $\mathfrak{S}_n$ sont à coefficients entiers.

• Frobenius-Zolotarev

On calcule la signature d'un automorphisme de l'espace $\mathbb{F}_p^n$, pour p impair. Il est égal au symbole de Legendre du déterminant.

• Formes de Hankel

On peut placer ici ce développement en raison de la présence de fonctions symétriques élémentaires.

• Automorphismes de $\mathfrak{S}_n$.

• Isomorphisme exceptionnel $\mathrm{PSL}_2(\mathbb{F}_5) \simeq \mathfrak{A}_5$.

4 Questions du jury

Exercice classique : La formule de Wilson avec les p-Sylow de $\mathfrak{S}_p$, p premier.
Exercice classique : Peut-on voir $\mathfrak{S}_n$ comme produit semi-direct de $\mathfrak{A}_n$

5 Preuves

5.1 Signature

La signature est bien un morphisme de $\mathfrak{S}_n$ dans $\mathbb{C}^*$ puisque, pour $\sigma, \tau \in \mathfrak{S}_n$:

$$\begin{aligned}
\epsilon(\sigma \circ \tau) &= \prod_{\{i,j\} \in \mathcal{P}_{2,n}} \frac{\sigma\big(\tau(j)\big) - \sigma\big(\tau(i)\big)}{j - i} \\
&= \prod_{\{i,j\} \in \mathcal{P}_{2,n}} \frac{\sigma\big(\tau(j)\big) - \sigma\big(\tau(i)\big)}{\tau(j) - \tau(i)} \prod_{\{i,j\} \in \mathcal{P}_{2,n}} \frac{\tau(j) - \tau(i)}{j - i} \\
&= \prod_{\{k,l\} \in \mathcal{P}_{2,n}} \frac{\sigma(k) - \sigma(l)}{k - l} \prod_{\{i,j\} \in \mathcal{P}_{2,n}} \frac{\tau(j) - \tau(i)}{j - i} = \epsilon(\sigma)\epsilon(\tau).
\end{aligned}$$

5.2 Automorphisme extérieur de $\mathfrak{S}_6$

Il n'est pas très difficile de prouver la présence d'un automorphisme extérieur de $\mathfrak{S}_6$: on fait par exemple agir $\mathfrak{S}_5$ sur ses six 5-Sylow. L'image de l'action est un sous-groupe transitif H de $\mathfrak{S}_6$. On fait ensuite agir $\mathfrak{S}_6$ sur $\mathfrak{S}_6/H$ qui possède 6 éléments (comme dans la preuve de H d'indice n implique $H \simeq \mathfrak{S}_{n-1}$), et on obtient, par cette action, un morphisme de $\mathfrak{S}_6$ dans lui-même qui en fait est un automorphisme de $\mathfrak{S}_6$ et qui envoie H, qui est transitif, sur le stabilisateur de $\overline{e}$, qui ne l'est pas.

5.3 Cardinal d'une classe de conjugaison

Proposition. On fixe σ dans $\mathfrak{S}_n$. On note C_i les supports des cycles de la décomposition de σ et on fixe un représentant x_i de C_i pour tout i.

1. Soit τ dans le commutant Z_σ de σ. Alors, τ permute les supports C_i ayant même cardinal.
2. Réciproquement, on fixe une permutation ϕ des C_i de même cardinaux qui envoie C_i sur $C_{\phi(i)}$, et, pour tout i, on se donne un z_i dans chaque C_i. Alors, il existe une unique permutation τ dans Z_σ telle que $\tau(x_i) = z_{\phi(i)}$.

Démonstration. On veut montrer tout d'abord que τ passe aux classes de conjugaison : *i. e.* si $\tau(x_i)$ est dans C_j, alors, pour tout y_i dans C_i, $\tau(y_i)$ est dans C_j. Effectivement, comme $x_i, y_i \in C_i$, il existe k_i tel que $\sigma^{k_i}(x_i) = y_i$. On en déduit que

$$\tau(y_i) = \tau(\sigma^{k_i}(x_i)) = \sigma^{k_i}(\tau(x_i)) \in C_j.$$

Comme la bijection τ envoie C_i sur C_j, ils ont même cardinaux.

Montrons maintenant la seconde assertion.

Unicité Le support C_i est l'orbite de x_i pour l'action naturelle du sous-groupe $\langle\sigma\rangle$ de $\mathfrak{S}_n$. C'est-à-dire que pour y_i dans C_i, il existe k_i tel que $\sigma^{k_i}(x_i) = y_i$. On a alors :

$$\tau(y_i) = \sigma^{k_i}(\tau(x_i)) = \sigma^{k_i}(z_{\phi(i)}).$$

Comme les C_i forment une partition de E et que tout $\tau(y_i)$ est entièrement déterminé, pour tout y_i et pour tout i, τ est unique.

Existence Pour tout y_i dans C_i, on définit k_i (minimal positif) tel que $y_i = \sigma^{k_i}(x_i)$ et on pose $\tau(y_i) = \sigma^{k_i}(z_{\phi(i)})$. Alors, comme C_i et $C_{\phi(i)}$ sont de même cardinal, τ fournit bien une bijection entre C_i et $C_{\phi(i)}$ pour tout i, et donc, τ est bien une permutation. De plus, comme τ est construite à l'aide de puissances de σ, τ commute à σ. Conclusion, on a bien $\tau \in Z_\sigma$.

Exemple 5.1. Si σ est comme dans l'exemple **??**, la proposition nous dit que l'on construit un élément du commutant de σ en permutant C_1 et C_2, et en fixant C_3, et C_4. Soit, par exemple, $\tau(1) = 8$, $\tau(2) = 5$, $\tau(3) = 7$, $\tau(4) = 4$. Regardons combien nous avons de choix : 2! permutations possibles, pour chaque permutation, 3 possibilité pour l'image de $x_1 = 1$, et trois pour l'image de $x_2 = 2$, puis 2 choix pour l'image de 3 et un seul choix pour l'image de 4. Soit, en tout $2! \times 3^2 \times 2^1 \times 1^1 = 36$ possibilités.

Corollaire 5.2. Soit σ une permutation de $\mathfrak{S}_n$ associée à une partition $\lambda := (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_s)$ de n. Soit $a_j(\lambda)$ le nombre de fois où j apparaît dans la partition λ, c'est-à-dire, le nombre de supports de cycles C_i de cardinal j. Alors, le cardinal de la classe de conjugaison de σ est égal à

$$|\mathcal{C}_\sigma| = \frac{n!}{\prod_j a_j(\lambda)! j^{a_j(\lambda)}}.$$

Démonstration. Il suffit pour cela de montrer que $|Z_\sigma| = \prod_j a_j(\lambda)! j^{a_j(\lambda)}$. Mais ceci est clair par la proposition, voir l'exemple ci-dessus, puisqu'un élément de Z_σ est entièrement déterminé par les données suivantes, pour chaque j de 1 à n :

1. d'une permutation ϕ de l'ensemble des supports C_i de cardinal j
2. d'un élément $y_{\phi(i)}$, pour chaque i tel que C_i est de cardinal j, choisi dans $C_{\phi(i)}$.

5.4 Intégralité de la table de caractères de $\mathfrak{S}_n$

Exercice 5.3 (Un préliminaire sur les extensions cyclotomiques)**.**

Pour n entier naturel, soit $\mathcal{P}_n$ l'ensemble des entiers de 1 à n premiers avec n, et $\omega \in \mathbb{C}$ une racine primitive n-ième de l'unité. On rappelle que le polynôme cyclotomique ϕ_n est irréductible (et unitaire) sur $\mathbb{Q}$, donc sur $\mathbb{Z}$.

1. Montrer que l'évaluation en ω fournit un isomorphisme de corps $\mathbb{Q}[X]/(\phi_n) \to \mathbb{Q}(\omega)$. En déduire l'existence, et l'unicité, d'un automorphisme ζ_k sur $\mathbb{Q}[\omega]$, pour tout k de $\mathcal{P}_n$, qui fixe $\mathbb{Q}$ et envoie ω sur ω^k.
2. Montrer que $\overline{k} \cdot P(\omega) = P(\omega^k)$ définit une action du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ sur $\mathbb{Q}(\omega)$, resp. $\mathbb{Z}[\omega]$, par automorphismes de corps, resp. d'anneau.
3. Soit α dans $\mathbb{Q}(\omega)$, resp. dans $\mathbb{Z}[\omega]$. Montrer que $\zeta_k(\alpha) = \alpha$ pour tout k de $\mathcal{P}_n$ si et seulement si $\alpha \in \mathbb{Q}$, resp. $\alpha \in \mathbb{Z}$.

   On pourra écrire la condition sous la forme d'un système et reconnaître une matrice de Vandermonde.

Soluce

1. Comme $\phi_n(\omega) = 0$, ϕ_n est dans le noyau de l'évaluation, et comme, de plus, ϕ_n est irréductible dans $\mathbb{Q}[X]$, qui est principal, ϕ_n engendre le

noyau. Comme ω est un nombre algébrique, on a $\mathbb{Q}[\omega] = \mathbb{Q}(\omega)$, ce qui implique la surjectivité de l'évaluation. L'isomorphisme d'anneaux en résulte, par passage au quotient, et un isomorphisme d'anneaux entre deux corps est un isomorphisme de corps.

L'unicité de ζ_k est claire car ω engendre $\mathbb{Q}[\omega]$. Pour l'existence, on remarque juste que ω^k est aussi une racine primitive n-ième de l'unité, donc $\mathbb{Q}[\omega^k]$ est encore isomorphe à $\mathbb{Q}[X]/(\phi_n)$, d'où un isomorphisme ζ_k de $\mathbb{Q}[\omega]$ sur $\mathbb{Q}[\omega^k]$. On a clairement $\mathbb{Q}[\omega^k] \subset \mathbb{Q}[\omega]$, et on déduit l'inclusion inverse par égalité des dimensions, ce qui implique que ζ_k est bien un automorphisme.

2. L'assertion portant sur $\mathbb{Q}[\omega]$ est claire en utilisant l'unicité de ζ_k et $(\omega^k)^{k'} = \omega^{kk'}$. Comme ci-dessus, une double inégalité prouve que $\mathbb{Z}[\omega^k] = \mathbb{Z}[\omega]$, et il en résulte l'assertion sur $\mathbb{Z}[\omega]$.

3. La partie « si » est claire, puisque si α est dans $\mathbb{Q}$, on peut le voir comme un polynôme constant (en ω) ; il est donc invariant par ζ_k.

   Montrons la réciproque dans le cas où $\alpha \in \mathbb{Q}[\omega]$. On sait que l'on peut écrire $\alpha = \sum_{i=0}^{\varphi(n)-1} a_i\omega^i$, $a_i \in \mathbb{Q}$, puisque le polynôme ϕ_n est de degré $\varphi(n)$. Le système d'équations $\zeta_k(\alpha) = \alpha$, pour tout k de $\mathcal{P}_n$ s'écrit sous la forme

   $$\alpha e = Va,$$

   où $e = (1, \cdots, 1)$, $a = (a_0, \cdots, a_{\varphi(n)-1})$, tous deux écrits en colonnes, et V la matrice de Vandermonde $V = \left((\omega^j)^i\right)_{i,j}$, avec $0 \leq i \leq \varphi(n) - 1$ et $j \in \mathcal{P}_n$. Soit $e_1 = (1, 0, \cdots, 0)$, le premier vecteur de la base canonique. On a $Ve_1 = e$, d'où

   $$Va = \alpha e = \alpha V e_1 = V(\alpha e_1).$$

   Comme V est la matrice de Vandermonde des ω^k, $k \in \mathcal{P}_n$, qui sont deux à deux distincts, V est inversible et donc, $a = \alpha e_1$, ce qui entraîne que tout a_i, $i \neq 0$ est nul. Il vient $\alpha \in \mathbb{Q}$.

   Maintenant, si α est dans $\mathbb{Z}[\omega]$, alors, on peut écrire $\alpha = \sum_{i=0}^{\varphi(n)-1} a_i\omega^i$, $a_i \in \mathbb{Z}$, en utilisant la division euclidienne dans $\mathbb{Z}[X]$ par ϕ_n, qui est unitaire [1]. Donc, l'assertion sur $\mathbb{Z}$ est analogue.

Remarque. Le résultat sur $\mathbb{Q}$ provient d'un résultat classique de théorie de Galois : le groupe de Galois de $\mathbb{Q}(\omega)$ sur $\mathbb{Q}$ est le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$, et donc, les $(\mathbb{Z}/n\mathbb{Z})^*$-invariants de $\mathbb{Q}(\omega)$ sont réduits à $\mathbb{Q}$. Pour l'assertion sur $\mathbb{Z}$, on peut remarquer que les éléments de $\mathbb{Z}[\omega]$ sont des entiers algébriques, et qu'un entier algébrique dans $\mathbb{Q}$ est forcément dans $\mathbb{Z}$.

1. Attention ! L'anneau $\mathbb{Z}[X]$ n'est pas euclidien. Toutefois, la division euclidienne de $\mathbb{Q}[X]$ d'un polynôme de $\mathbb{Z}[X]$ par un polynôme unitaire, reste dans $\mathbb{Z}[X]$.

Exercice 5.4 (Condition pour que la table d'un groupe soit dans $\mathbb{Z}$)**.**
Soit G un groupe de cardinal n. On fait agir le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ sur G par $\overline{k} \cdot g = g^k$.

1. Montrer que l'on définit une action de $(\mathbb{Z}/n\mathbb{Z})^*$ sur l'espace des fonctions centrales par
$$\overline{k} \cdot f : g \mapsto f(g^k),\ \overline{k} \in (\mathbb{Z}/n\mathbb{Z})^*,\ g \in G.$$
2. Soit χ un caractère de G. Montrer, avec les notations de l'exercice **??**, que $\chi(g^k) = \zeta_k\big(\chi(g)\big)$, puis, que χ est invariant par $(\mathbb{Z}/n\mathbb{Z})^*$ si et seulement si χ est à valeurs dans $\mathbb{Z}$.
3. Montrer que la table de caractères de G est à valeurs dans $\mathbb{Z}$ si et seulement si pour tout $\overline{k}$ dans $(\mathbb{Z}/n\mathbb{Z})^*$, et pour tout g dans G, g^k et g sont dans la même classe de conjugaison.
Pour la partie « seulement si », on pourra noter δ_h la fonction caractéristique de la classe de conjugaison de h, et montrer l'égalité $\overline{k} \cdot \delta_{g^k} = \delta_g$.

Soluce

1. Tout d'abord, g^k est bien défini puisque, par Lagrange, $g^n = e$. Si g et h sont dans la même classe de conjugaison, alors il en est de même de g^k et h^k. Donc, si f est une fonction centrale (*i. e.* passe aux classes de conjugaison), alors $\overline{k} \cdot f$ est également une fonction centrale.
Reste à montrer les axiomes de l'action. L'élément neutre $\overline{1}$ fixe effectivement f. De plus,
$$\overline{kk'} \cdot f(g) = f(g^{kk'}) = f\big((g^{k'})^k\big) = \overline{k} \cdot f(g^{k'}) = \overline{k} \cdot \big(\overline{k'} \cdot f(g)\big).$$
2. Tout d'abord, $\chi(g)$ est une somme de valeurs propres λ_i pour l'action de G, donc, une somme de puissances de ω, où ω est une racine primitive n-ième de l'unité. On a, en particulier, $\chi(g) \in \mathbb{Z}[\omega]$. De plus, $\chi(g^k)$ est la somme des λ_i^k. On a donc $\chi(g^k) = \zeta_k\big(\chi(g)\big)$, pour l'automorphisme ζ_k construit dans l'exercice **??**.
Il est donc clair que si χ est invariant par $(\mathbb{Z}/n\mathbb{Z})^*$, alors $\chi(g)$ est invariant pour l'action de $(\mathbb{Z}/n\mathbb{Z})^*$; il est donc entier, par l'exercice **??** 3), et la réciproque est claire.
3. Si, pour tout k dans $(\mathbb{Z}/n\mathbb{Z})^*$, g^k et g sont dans la même classe de conjugaison pour tout g, alors, comme χ est une fonction centrale, on a $\overline{k} \cdot \chi = \chi$. Ainsi, par la question qui précède, χ est à valeurs dans $\mathbb{Z}$.

Montrons la réciproque. Tout d'abord, nous allons montrer, selon l'indication proposée, que $\overline{k} \cdot \delta_{g^k} = \delta_g$. On a vu que $(\mathbb{Z}/n\mathbb{Z})^*$ agissait sur G et que cette action passait aux classes de conjugaison. Si h est dans la même classe de conjugaison que g, alors $\overline{k} \cdot \delta_{g^k}(h) = \delta_{g^k}(h^k) = 1$, puisque h^k est dans la même classe de conjugaison que g^k. De plus, si h^k est dans la même classe que g^k, alors, $(h^k)^{k'} = h$ est dans la même classe que $(g^k)^{k'} = g$, où $\overline{k}'$ est l'inverse de $\overline{k}$ dans $(\mathbb{Z}/n\mathbb{Z})^*$. Donc, par la contraposée, si h et g ne sont pas dans la même classe de conjugaison, h^k n'est pas dans la même classe que g^k, et donc $\overline{k} \cdot \delta_{g^k}(h) = \delta_{g^k}(h^k) = 0$, ce qui prouve bien l'égalité $\overline{k} \cdot \delta_{g^k} = \delta_g$.

On suppose (par la contraposée), que g^k et g ne sont pas dans la même classe de conjugaison. Or, $\overline{k} \cdot \delta_{g^k} = \delta_g$, ce qui prouve que l'action de $(\mathbb{Z}/n\mathbb{Z})^*$ sur les fonctions centrales n'est pas triviale. Comme les caractères irréductibles engendrent l'espace des fonctions centrales, on obtient qu'il existe un caractère irréductible χ tel que $\overline{k} \cdot \chi \neq \chi$. Encore par l'exercice **??**, ce caractère ne peut avoir toutes ses valeurs dans $\mathbb{Q}$, et en particulier, il ne peut pas avoir toutes ses valeurs entières.

Exercice 5.5 (Intégralité des caractères de $\mathfrak{S}_n$)**.**
Montrer, à l'aide de l'exercice **??**, que la table des caractères de $\mathfrak{S}_n$ est à coefficients entiers pour tout n.

Soluce D'après l'exercice **??**, il suffit de montrer que, si k est premier avec $n!$, alors g^k est dans la même classe de conjugaison que g, c'est-à-dire, que g^k et g ont même partition associée pour la décomposition en cycles disjoints. Or, si g se décompose en $\prod_i \sigma_i$, g^k se décompose en $\prod_i \sigma_i^k$, puisque ces cycles commutent. Il suffit donc de montrer l'assertion pour chaque cycle.

Soit donc $\sigma = (i_1 \cdots i_m)$ un m-cycle. Comme $m \leq n$, on voit que m divise $n!$, et qu'il est donc premier avec k. On suppose $(\sigma^k)^{m'}(i_1) = i_1$ pour un m'. Alors, $\sigma^{km'}$ fixe i_1, ce qui implique que m divise km', puisque les seules puissance de σ qui fixent i_1 sont les multiples de m. Par le lemme de Gauss, m divise m'. On voit alors que σ^k est encore un m-cycle, et qu'il est ainsi dans la même classe de conjugaison que σ.

5.5 L'enigme des prisonniers

Exercice 5.6 (L'énigme des prisonniers)**.**
Afin de régler le problème de surpopulation des prisons, on décide de jouer avec le sort de 100 prisonniers [a]. On fournit aux prisonniers un matricule allant de 1 à 100. On leur indique une pièce, où se trouvent 100 boîtes numérotées de 1 à 100, contenant chacune le matricule d'un prisonnier, de sorte que chaque prisonnier soit représenté.
Lorsqu'un prisonnier rentre dans cette pièce, il va choisir 50 boîtes. Tous les prisonniers vont passer chacun à leur tour, et si un seul des prisonniers ne trouve pas son matricule dans une des boîtes, alors, tous les prisonniers sont fusillés [b].
Heureusement, un des prisonniers est mathématicien ; il va proposer à ses codétenus une stratégie pour améliorer leurs chances de survie [c]. Voici sa stratégie :
Chacun commence par ouvrir la boîte portant son numéro, tire le matricule qui est à l'intérieur, puis ouvre la boîte ayant ce matricule pour numéro, tire le matricule qui est à l'intérieur, et ainsi de suite jusqu'à ce qu'il trouve son matricule ou qu'il ait ouvert 50 boîtes.
Voici deux questions bien naturelles. Quelle est la probabilité pour que le groupe survive si on laisse chaque prisonnier agir au hasard ? Quelle est la probabilité pour que le groupe survive si l'on suit le conseil du mathématicien ?

a. Inutile de rappeler que l'histoire se déroule sous un régime totalitaire, et dans un pays totalement imaginaire.

b. Ce détail n'est pas vraiment utilisé dans la preuve. Il permet juste de créer de l'adrénaline et une motivation supplémentaire pour le candidat au concours.

c. Cette partie de l'énoncé a pour but non dissimulé de réintégrer une image positive du mathématicien dans la population carcérale. Ceci dit, on ne saura jamais pourquoi le mathématicien est sous les verrous. A cette question du jury, suggérez une erreur judiciaire.

Soluce. On est maintenant entre gens sérieux et nous allons remplacer le nombre 100 par un nombre n quelconque, que l'on peut supposer pair, le nombre 50 sera donc remplacé par $\frac{n}{2}$.

• Premier cas. Les risques du hasard.

Pour un prisonnier donné, la probabilité que son matricule apparaisse dans les tirages successifs est de $\frac{n/2}{n} = \frac{1}{2}$. L'indépendance de chaque prisonnier (l'anarchie, quoi !) fait que la chance de survie du groupe est de $(1/2)^n$.

• Second cas. Le risque sous contrôle.

Soit E_n l'ensemble des nombres entiers de 1 à n, P l'ensemble des prisonniers (ou si l'on préfère, l'ensemble de leurs matricules), et B l'ensemble des

boîtes.

L'ensemble E_n est alors identifié à la fois à P, via les matricules, et à B, via la numérotation des boîtes. On pourra dire, sans ambiguïté, le prisonnier p, ou la boîte k, .

Le fait d'avoir placé un matricule dans chaque boîte fournit une bijection σ de E_n dans lui-même, telle que la boîte p contient le matricule $\sigma(p)$. L'identification fait donc de σ une permutation.

Tout le suspense réside maintenant dans cet élément σ de $\mathfrak{S}_n$.

La procédure du choix des boîtes proposée par le mathématicien se traduit de la façon suivante : soit p un prisonnier, il va tout d'abord se diriger vers la boîte p. Il va donc tirer le matricule $\sigma(p)$. La procédure consiste maintenant à ouvrir la boîte $\sigma(p)$, dont il tirera le matricule $\sigma\big(\sigma(p)\big) = \sigma^2(p)$. S'il suit convenablement la procédure, la k-ième boîte qu'il ouvrira contiendra le matricule $\sigma^k(p)$.

Il est primordial que le prisonnier p retrouve son propre matricule au bout de $\frac{n}{2}$ essais. Cela signifie que l'on veut $\sigma^k(p) = p$ pour $1 \leq k \leq \frac{n}{2}$. Et ceci doit être valable pour tout p.

On a donc résumé le problème en une propriété de la permutation σ. Etudions de plus près cette propriété.

Décomposons σ en cycles disjoints : $\sigma = c_1 c_2 \cdots c_m$. Soit p dans E_n. Si $\sigma(p) = p$, alors, le prisonnier p trouve son matricule dans la première boîte. On suppose $\sigma(p) \neq p$, alors p appartient à un seul des cycles c_l, puisque les cycles sont disjoints. De plus, $\sigma(p) = c_l(p)$. L'élément $c_l(p)$ appartient encore au cycle c_l par construction, et donc $\sigma^2(p) = c_l^2(p)$. Par récurrence, $\sigma^k(p) = c_l^k(p)$.

Supposons que tous les cycles de la décomposition de σ soient de longueur inférieure à $\frac{n}{2}$. Dans ce cas, chaque c_l est d'ordre $l \leq \frac{n}{2}$, et ainsi, $\sigma^k(p) = p$ pour un $k \leq \frac{n}{2}$. On a gagné (la vie, et l'agreg. Wouah, la chance !).

En revanche, supposons que σ contienne un cycle de longueur l, $l > \frac{n}{2}$, alors tout prisonnier p appartenant à ce cycle ne pourra trouver son matricule au bout de la procédure.

Reste à calculer la probabilité pour que σ soit une permutation dont les longueurs des cycles, dans la décomposition en cycles disjoints, soient toutes inférieures à $\frac{n}{2}$. Il vaut mieux calculer la probabilité de l'évènement complémentaire. Effectivement, s'il existe un cycle de longueur l, $l > \frac{n}{2}$, alors, celui-ci est unique (dans le sens où il ne peut pas y en avoir deux de longueur l, $l > \frac{n}{2}$, dans la décomposition de σ).

On fixe donc l, $l > \frac{n}{2}$, et on cherche le nombre de σ de $\mathfrak{S}_n$ telles que σ possède un cycle de longueur l dans sa décomposition. Pour une partie fixée de E_n de cardinal l, il y a $\frac{l!}{l} = (l-1)!$ l-cycles qui permutent cette partie. Effectivement, un cycle peut s'écrire exactement de l façons distinctes. Il ne

reste plus qu'à permuter (de façon quelconque) les $n-l$ éléments restants. Il y a en tout, par unicité de la décomposition en cycles disjoints

$$\binom{n}{l} \times (n-l)!(l-1)! = \frac{n!}{l}$$

permutations possédant un cycle de longueur l.

Par les unicités indiquées ci-dessus, cela nous fait en tout

$$\sum_{l=\frac{n}{2}+1}^{n} \frac{n!}{l}$$

possibilités. C'est-à-dire que la probabilité de l'évènement complémentaire est

$$\frac{1}{n!} \sum_{l=\frac{n}{2}+1}^{n} \frac{n!}{l} = \sum_{l=\frac{n}{2}+1}^{n} \frac{1}{l} = \frac{1}{n} \sum_{l=\frac{n}{2}+1}^{n} \frac{1}{\frac{l}{n}}.$$

Quand n tend vers l'infini, cette probabilité tend donc vers

$$\int_{\frac{1}{2}}^{1} \frac{1}{t} \mathrm{d}t = \ln(2).$$

La probabilité cherchée est donc, pour n grand, proche de $1-\ln(2) \simeq 0,3068$.

Par exemple pour $n = 100$, on a

$$(\frac{1}{2})^{100} = 7,888 \times 10^{-31}, \;\; 1 - \sum_{l=51}^{100} \frac{1}{l} = 0,312$$

Y a pas photo !

Remarque. Si σ possède un cycle (forcément unique) de longueur $l > \frac{n}{2}$, alors les prisonniers du cycle correspondant n'auront aucune chance de retrouver leur matricule dans les boîtes.

6 Tables de caractères et addendum

La table de caractères de $\mathfrak{S}_4$ est donnée par :

$\lvert C_g \rvert$	1	6	3	8	6
$\mathfrak{S}_4$	Id	(12)	(12)(34)	(123)	(1234)
χ_{triv}	1	1	1	1	1
χ_ϵ	1	-1	1	1	-1
χ_{std}	3	1	-1	0	-1
$\epsilon\chi_{\text{std}}$	3	-1	-1	0	1
ϕ	2	0	2	-1	0

La table de caractères de $\mathfrak{A}_5$ est la suivante

$\lvert C_g\rvert$	1	15	20	12	12
$\mathfrak{A}_5$	Id	(12)(34)	(123)	(12345)	(12354)
χ_{triv}	1	1	1	1	1
χ_{std}	4	0	1	-1	-1
γ	5	1	-1	0	0
ψ_1	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
ψ_2	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$

Relations de tresses avec $t_k := (kk+1)$:

$$t_i t_j = t_j t_i, |j-i| \geq 2,\ t_i t_{i+1} t_i = t_{i+1} t_i t_{i+1},\ t_i^2 = e.$$

Références

Daniel Perrin : Cours d'algèbre. Collection CAPES/agrégation. Editions Ellipses, Paris, 1997.
Les preuves peuvent être trouvées sur :
Philippe Caldero et Jérôme Germoni. Nouvelles histoires hédonistes de groupes et de géométries-2 (A venir)