DM d'octobre ; corrigé

1. Chaque classe de conjugaison de $\mathfrak{S}_n$ est caractérisée par les longueurs $\lambda = (\lambda_1, \lambda_2, \ldots)$, avec $\lambda_1 \geq \lambda_2 \geq \cdots$, des cycles disjoints dont ses éléments sont produits. Un tel λ est une partition de n.
2. On a $\mathfrak{S}_n = \mathfrak{A}_n \cup \mathfrak{A}_n\tau$. Un conjugué de σ dans $\mathfrak{S}_n$ est donc soit de la forme $\rho\sigma\rho^{-1}$ avec $\rho \in \mathfrak{A}_n$ (auquel cas il est dans $\mathcal{CA}(\sigma)$), soit $(\rho\tau)\sigma(\rho\tau)^{-1} = \rho\tau\sigma\tau^{-1}\rho^{-1}$ (et alors il est dans $\mathcal{CA}(\tau\sigma\tau^{-1})$).
3. Ce sont des classes d'équivalence (pour la conjugaison), donc elles sont égales ou disjointes. De plus $\mathcal{CA}(\tau\sigma\tau^{-1}) = \tau\mathcal{CA}(\sigma)\tau^{-1}$, parce que $\tau\mathfrak{A}_n = \mathfrak{A}_n\tau$ (qui est $\mathfrak{S}_n \setminus \mathfrak{A}_n$).
4. On a donc $\mathcal{CA}(\sigma) = \mathcal{CS}(\sigma)$ si et seulement si σ (qui appartient à $\mathcal{CA}(\sigma)$) est dans $\mathcal{CA}(\tau\sigma\tau^{-1})$. Cela signifie $\sigma = \mu\tau\sigma\tau^{-1}\mu^{-1}$ pour un certain $\mu \in \mathfrak{A}_n$, c'est-à-dire $\sigma = \rho\sigma\rho^{-1}$ pour un certain $\rho \in \mathfrak{S}_n \setminus \mathfrak{A}_n$.
5. (a) Soit $\sigma = cc_1 \cdots$ cette décomposition, avec c de longueur paire. On a $c \in \mathfrak{S}_n \setminus \mathfrak{A}_n$. Comme c commute avec les c_i (supports disjoints) et $ccc^{-1} = c$, on a $c\sigma c^{-1} = \sigma$. D'après la question précédente, on a $\mathcal{CA}(\sigma) = \mathcal{CS}(\sigma)$.

   (b) Soit $\sigma = c\,c' \cdots$ cette décomposition, avec c et c' de même longueur impaire. On peut procéder de deux façons. La première : $c = (i_1\, i_2\, \ldots\, i_r)$ et $c' = (j_1\, j_2\, \ldots\, j_r)$. On choisit $\rho = (i_1\, j_1) \cdots (i_r\, j_r)$, qui est une permutation impaire. On a $\rho^{-1} = \rho$ et $\rho cc'\rho^{-1} = cc'$ tandis que ρ commute avec les autres cycles (supports disjoints). Donc $\rho\sigma\rho^{-1} = \sigma$ pour $\rho \in \mathfrak{S}_n \setminus \mathfrak{A}_n$ et on conclut grâce à la question 4. La deuxième : cc' est le carré du cycle $\rho = (i_1\, j_1\, i_2 \cdots j_r)$, qui est lui-même une permutation impaire, qui commute aux autres cycles. Alors $\rho cc'\rho^{-1} = \rho\rho^2\rho^{-1} = \rho^2 = cc'$, donc $\rho\sigma\rho^{-1} = \sigma$ et on conclut de la même façon.

   Attention ! On ne peut pas appliquer la question 5, car l'écriture $\sigma = \rho\,\rho \cdots$ n'est pas une factorisation en cycles disjoints.

   (c) Soit $c = (i_1 \cdots i_r)$ un cycle de support I, et ρ commutant avec c. On a $\rho c = c\rho$. Si $i \notin I$, alors $\rho(i) = c(\rho(i))$ donc $\rho(i) \notin I$. Ainsi ρ préserve le complémentaire de I, donc I lui-même. Puis $\rho(i_{k+1}) = c(\rho(i_k))$ montre que si $\rho(i_k) = i_\ell$, alors $\rho(i_{k+1}) = i_{\ell+1}$. Ceci implique l'existence d'un $0 \leq s \leq r-1$ tel que $\rho(i_k) = i_{k+s}$, modulo r. C'est-à-dire que la restriction de ρ à I est égale à celle de c^s.

   Supposons maintenant que dans la décomposition en cycles disjoints $\sigma = c_1\, c_2 \cdots$, chaque c_j soit de longueur impaire, ces longueurs étant deux à deux distinctes (en particulier, il y a au plus un point fixe, car c'est un cycle de longueur 1). Si $\mathcal{CA}(\sigma) = \mathcal{CS}(\sigma)$, alors $\sigma = \rho\sigma\rho^{-1}$ pour un certain $\rho \in \mathfrak{S}_n \setminus \mathfrak{A}_n$. On a donc $\sigma = c'_1 c'_2 \cdots$,

avec $c'_j = \rho c_j \rho^{-1}$. C'est une décomposition en cycles disjoints, donc identique à celle d'origine, à permutation près des facteurs. Mais comme la longueur de c'_j est égale à celle de c_j, et les longueurs sont uniques, on a en fait $c'_j = c_j$, c'est-à-dire que ρ commute avec chaque c_j. D'après le paragraphe précédent, ρ préserve chacun des supports des c_j, et coïncide avec une puissance de c_j sur son support. On a donc $\rho = c_1^{s_1} c_2^{s_2} \cdots$, et c'est donc une permutation paire car chaque c_j est paire. Cette contradiction montre qu'en fait $\mathcal{CA}(\sigma) \neq \mathcal{CS}(\sigma)$.

6. On part des classes de conjugaison de $\mathfrak{S}_5$ (question 1). Ce sont $\{id\}$, la classe des transpositions, celle des 3-cycles, celles des doubles transpositions, celle des 4-cycles, celle des 5-cycles et enfin celle des produits d'une transposition et d'un 3-cycle (étant entendu que les produits sont à supports disjoints). On ne conserve que les permutations paires : $\{id\}$, les 3-cycles, les doubles transpositions et les 5-cycles. On applique alors la question 4 : seule la $\mathfrak{S}_5$-classe des 5-cycles se casse en deux $\mathfrak{A}_5$-classes (de cardinal moitié). On a donc 5 classes dans $\mathfrak{A}_5$. Leurs cardinaux respectifs sont 1, 20 (pour chacun des $\binom{5}{3} = 10$ choix de trois éléments a, b, c, il y a deux cycles $(a\,b\,c)$ et $(a\,c\,b)$), 15 (5 manières de choisir le point fixe, puis trois de scinder en deux paires les quatre autres), 12 et 12 (le nombre de n-cycles dans $\mathfrak{S}_n$ est $(n-1)!$).

7. Soit H un sous-groupe de $\mathfrak{A}_5$. L'ordre de celui-ci est 60 et c'est un multiple de $|H|$. Donc l'ordre de H ne peut valoir que $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$. Si H est distingué, c'est une réunion de classes de conjugaison, et il contient au moins $\{id\}$. Son cardinal est donc de la forme $1 + 20a + 15b + 12c + 12d$ avec a, b, c, d valant 0 ou 1. Comme $13, 16, 21, 25, 27, 33, 36, \ldots$ ne sont pas dans la liste ci-dessus, les seules possibilités restent 1 ($H = \{id\}$) et 60 ($H = \mathfrak{A}_5$).

8. On a plusieurs points fixes, appliquer la question 5b. Si H contient un 3-cycle, il les contient tous (il est distingué et ils sont conjugués entre eux). Mais ceux-ci engendrent $\mathfrak{A}_n$, donc $H = \mathfrak{A}_n$.

9. Soit $\rho \in H$, ayant au moins $n-5$ points fixes. Quitte à renommer les entiers, on peut supposer que $k \geq 6$ implique $\rho(k) = k$. L'ensemble K des $\sigma \in H$ qui ont cette même propriété est un sous-groupe de H. Par restriction à $\{1, \ldots, 5\}$, K définit un sous-groupe $\hat{K}$ de $\mathfrak{A}_5$.

   On ne peut pas affirmer que K est distingué dans $\mathfrak{A}_n$. En revanche $\hat{K}$ l'est dans $\mathfrak{A}_5$. En effet, si $\sigma \in K$ et $\mu \in \mathfrak{A}_5$, alors μ est la restriction d'un $\theta \in \mathfrak{A}_n$ qui fixe $6, \ldots, n$. On a $\theta\sigma\theta^{-1} \in H$ car ce sous-groupe est distingué dans $\mathfrak{A}_n$. Comme ce produit fixe encore $6, \ldots, n$, il est dans K. Par restriction, on en déduit bien que $\mu\hat{\sigma}\mu^{-1} \in \hat{K}$.

   Comme $\mathfrak{A}_5$ est simple et $\hat{K}$ a au moins un élément non trivial ($\hat{\rho}$), on a $\hat{K} = \mathfrak{A}_5$. Mais alors K (et donc aussi H) contient un 3-cycle. Finalement H est égal à $\mathfrak{A}_n$.

10. Comme σ est non trivial, il existe a et b distincts tels que $\sigma(a) = b$. Soit alors $c \neq b$ tel que $\sigma(c) \neq a$ (il y a de la place, avec $n \geq 5$). L'ensemble $\gamma = \{a, b, c\} \cup \sigma^{-1}\{a, b, c\}$ a au plus 5 éléments (car $\sigma^{-1}(b) = a$). Son complémentaire Γ en a au moins $n-5$. Soit $\tau := (a\,c\,b)$. Si $x \in \Gamma$, on a

$$\tau\sigma\tau^{-1}\sigma^{-1}(x) = \tau\sigma\sigma^{-1}(x) = \tau(x) = x.$$

Donc $\tau\sigma\tau^{-1}\sigma^{-1}$ a au moins $n-5$ points fixes. Par ailleurs,

$$\tau\sigma\tau^{-1}\sigma^{-1}(\sigma(c)) = \tau\sigma\tau^{-1}(c) = \tau\sigma(a) = \tau(b) = a \neq \sigma(c).$$

Ainsi $\tau\sigma\tau^{-1}\sigma^{-1} \neq \mathrm{id}$. Enfin, $\tau\sigma\tau^{-1} \in H$ car H est distingué, donc $\tau\sigma\tau^{-1}\sigma^{-1} \in H$.

11. Puisque $\mathfrak{A}_3$ a trois éléments, il est isomorphe à $\mathbb{Z}/3\mathbb{Z}$, qui est simple car 3 est premier. Le groupe $\mathfrak{A}_4$ n'est pas simple parce que le sous-groupe réunion des classes $\{id\}$ et des doubles transpositions est distingué ; c'est bien un groupe car $(a\,b)(c\,d)\cdot(a\,c)(b\,d) = (a\,d)(b\,c)$.

12. Soit $n \geq 5$ et G un sous-groupe distingué de $\mathfrak{S}_n$. Soit $H = G \cap \mathfrak{A}_n$. C'est un sous-groupe distingué de $\mathfrak{A}_n$, qui est donc égal à $\{id\}$ ou à $\mathfrak{A}_n$. Dans le premier cas, soit $\tau \in G$. Alors $\tau^2 \in G \cap \mathfrak{A}_n$ entraine $\tau^2 = id$. Soit τ' une permutation conjuguée à τ. Comme G est distingué, on a $\tau' \in G$. Comme $\epsilon(\tau') = \epsilon(\tau)$, on obtient $\tau\tau' \in G \cap \mathfrak{A}_n$. Ainsi $\tau\tau' = id$, mais alors $\tau' = \tau^{-1} = \tau$. Puisque τ est son unique conjugué, c'est l'identité, et G est réduit à $\{id\}$. Dans le second cas, G contient $\mathfrak{A}_n$. L'indice $(\mathfrak{S}_n : G)$ divise $(\mathfrak{S}_n : \mathfrak{A}_n) = 2$, donc vaut 1 ou 2, ce qui ne permet que $G = \mathfrak{S}_n$ et $G = \mathfrak{A}_n$.

13. Le nombre de 5-Sylow divise l'ordre 60 et est congru à 1 modulo 5 (Thm de Sylow, complété en exercice). Les seules possibilités sont 1 et 6. Si c'était 1, l'unique 5-Sylow serait distingué, ce qui est impossible car G est simple. Il y en a donc 6.

14. Dans l'action par conjugaison, G permute les 5-Sylow entre eux. En les numérotant de 1 à 6, on obtient donc un morphisme de G dans $\mathfrak{S}_6$, qui à $g \in G$ associe la permutation $\sigma_g(i) = j$ si $gS_ig^{-1} = S_j$. Notons que cette action sur les 5-Sylow est transitive (Thm de Sylow).

    Le noyau de ce morphisme est distingué dans G, donc est égal à $\{1\}$ ou à G lui-même. Le second cas signifierait que $\sigma_g = id$ pour tout g, ce qui contredit la transitivité de l'action. Le noyau est donc égal à $\{1\}$: le morphisme est injectif.

    Le groupe G est donc isomorphe à son image H. En particulier, l'ordre de H est 60.

    Comme $\mathfrak{A}_6$ est distingué dans $\mathfrak{S}_6$, son image réciproque par le morphisme est distinguée dans G, donc est égale à $\{1\}$ ou à G. Ce n'est pas $\{1\}$, car alors H serait un sous-groupe de $\mathfrak{S}_6$ ne rencontrant $\mathfrak{A}_6$ qu'en $\{id\}$, et on a vu que H serait $\{1\}$, alors qu'il a 60 éléments. Donc cette image réciproque est G. Comme le morphisme est injectif, cela signifie que son image H est incluse dans $\mathfrak{A}_6$.

    L'ordre de $\mathfrak{A}_6$ est $\frac{1}{2}6! = 360$ et celui de H est 60. Son indice dans $\mathfrak{A}_6$ est donc $360/60 = 6$.

15. À nouveau, $\ker\Psi$ est distingué dans $\mathfrak{A}_6$ qui est simple. Donc Ψ est injectif ou trivial. Mais il n'est pas trivial car l'action de multiplication à gauche sur les classes est transitive. Donc il est injectif. Son image est donc de même ordre, 360, que $\mathfrak{A}_6$.

    L'ensemble $\mathfrak{A}_6/H$ est de cardinal 6 (l'indice calculé plus haut).

    Le groupe $\mathrm{Bij}(\mathfrak{A}_6/H)$ est donc isomorphe à $\mathfrak{S}_6$, et $\Psi(\mathfrak{A}_6)$ est donc isomorphe à un de ses sous-groupes. Ce sous-groupe est d'indice $720/360 = 2$. Comme le seul sous-groupe de $\mathfrak{S}_n$ d'indice 2 est $\mathfrak{A}_n$, on en déduit que l'action de $\mathfrak{A}_6$ sur $\mathfrak{A}_6/H$ se fait par permutation paires.

16. Le sous-groupe $\Psi(H)$ fixe un élément, à savoir la classe $1H = H$. Donc $\Psi(H)$ est réellement un sous-groupe du groupe qui permute les 5 autres classes g_iH, et qui le fait par permutation paires. Ce dernier groupe est isomorphe à $\mathfrak{A}_5$, d'ordre 60. Comme $\Psi(H)$ en est un sous-groupe de même ordre, il lui est égal.

    Comme Ψ est injectif, H est isomorphe à son image, donc à $\mathfrak{A}_5$. Par suite G est aussi isomorphe à $\mathfrak{A}_5$.

17. Dans une B.O.N. dont l'un des éléments est l'axe de rotation de ρ, la matrice s'écrit

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & \sin\theta \\ 0 & -\sin\theta & \cos\theta \end{pmatrix},$$

    θ étant l'angle de cette rotation. Les valeurs propres de ρ sont $\lambda = 1$ et celles du bloc 2×2, à savoir $e^{\pm i\theta}$. Par hypothèse, -1 est valeur propre, donc $e^{\pm i\theta} = -1$. La matrice ci-dessus est alors $\mathrm{diag}\{1, -1, -1\}$, ρ est un renversement.

18. Dans le plan $\mathbb{R}^2$, soit S une symétrie orthogonale (réflexion), par exemple celle par rapport à l'axe horizontal. Si $R \in \mathbf{SO}_2$ est une rotation, alors $S' = RS$ est une isométrie de déterminant $(+1)(-1) = -1$, donc une réflexion. On a alors $R = S'S$, et on trouve que toute rotation plane est produit de deux réflexions.

    Passons au cas d'une rotation ρ dans $\mathbb{R}^3$. Soit Π le plan de rotation (orthogonal à l'axe de la rotation $\mathbb{R}\vec{e}$). La restriction $R = \rho|_\Pi$ est une rotation plane, c'est donc le produit de deux réflexions $S'S$. On étend S' et S par linéarité à $\mathbb{R}^3$ en σ' et σ, en posant $\sigma'\vec{e} = \sigma\vec{e} = -\vec{e}$. Comme $\mathbb{R}\vec{e}$ et Π sont orthogonaux, que les restrictions de σ, σ' à ces deux sous-espaces sont des isométries, σ et σ' sont des isométries de $\mathbb{R}^3$. Ce sont des renversements (isométries de valeurs propres $1, -1, -1$). Le produit $\sigma'\sigma$ coïncide avec ρ sur Π (c'est $S'S$) et aussi sur $\mathbb{R}\vec{e}$ car $\sigma'\sigma\vec{e} = -\sigma'\vec{e} = \vec{e}$. Par linéarité, on a donc $\sigma'\sigma = \rho$.

    Tout élément de $\mathbf{SO}_3$ est un produit de (deux) renversements, donc ceux-ci engendrent le groupe.

19. Deux renversements ρ_1 et ρ (d'axes $\vec{e}_1, \vec{e}$) sont conjugués dans $\mathbf{SO}_3$, car il existe une rotation λ telle que $\lambda\vec{e} = \vec{e}_1$. Le renversement $\lambda\rho\lambda^{-1}$ fixe $\vec{e}_1$, donc est égal à ρ_1.

    Si le sous-groupe distingué H contient un renversement, il les contient donc tous, et comme ils engendrent $\mathbf{SO}_3$, on obtient $H = \mathbf{SO}_3$.

20. Cet ensemble est l'image d'un compact connexe (S^2) par une application continue. C'est donc un compact connexe de $\mathbb{R}^+$, c'est-à-dire un intervalle fermé borné. Comme ρ a des points fixes (les points de son axe de rotation), cet intervalle est de la forme $[0, d(\rho)]$. Comme ρ n'est pas triviale, $d(\rho)$ est > 0.

    Tout point de S^2 s'écrit sous la forme $x = \cos\theta\vec{e} + \sin\theta y$ avec $\vec{e}$ l'un des points fixes de ρ et y dans le cercle unité $C_\rho = S^2 \cap \vec{e}^{\perp}$. Par Pythagore, on a $\|\rho(x) - x\|^2 = \sin^2\theta\|\rho(y) - y\|^2$, dont le maximum est atteint sur C_ρ. Pour $x \in C_\rho$, on a

$$\|\rho(x) - x\| = \sqrt{(1 - \cos\alpha)^2 + \sin^2\alpha} = 2\sin\frac{\alpha}{2},$$

    où $\alpha \in]0, \pi[$ est l'angle de la rotation. Cette expression est donc le carré de $d(\rho)$.

21. Tout d'abord, il existe une rotation envoyant x_2 sur x_1. Comme $\mathbf{SO}_3$ est un groupe, on l'utilise pour se ramener au cas où $x_2 = x_1$. Le groupe des rotations d'axe $\mathbb{R}x_1$ agit sur S^2, et ses orbites sont les cercles obtenus par intersection de S^2 avec les plans orthogonaux à x_1. Comme $\|x_1 - y_1\| = \|x_1 - y_2\|$, y_1 et y_2 sont dans l'un de ces cercles. Il existe donc une telle rotation qui envoie y_1 sur y_2. Comme $\rho(x_1) = x_1$, ρ convient.

22. Par définition de $d(\rho)$ et par la question 20, il existe $z \in S^2$ tel que $\|\rho(z) - z\| = \|x - y\|$. D'après la question 21, il existe une rotation σ telle que $\sigma(x) = z$ et $\sigma(y) = \rho(z)$. Alors $(\sigma^{-1}\rho\sigma)(x) = y$. Comme H est distingué, $\sigma^{-1}\rho\sigma \in H$ convient.

23. Soit ρ comme à la question 22. On a $d(\rho) > 0$. Il existe donc une suite finie $x_0, \ldots, x_k$ telle que d'une part $x_k = -x_0$ et d'autre part $\|x_j - x_{j-1}\| \leq d(\rho)$ pour tout $j = 1, \ldots, k$ (prendre $k = 1 + [\pi/d(\rho)]$ et les x_j sur un demi-cercle de diamètre $[x_0, -x_0]$). Par la question 22, le groupe H contient des éléments $\rho_1, \ldots, \rho_k$ tels que $\rho_j(x_{j-1}) = x_j$. Le produit $\rho_k \cdots \rho_1 \in H$ envoie donc x_0 sur $x_k = -x_0$.Par la question 17, ce produit est un renversement. Par la question 19, $H = \mathbf{SO}_3$.

    On a montré que si H est distingué dans $\mathbf{SO}_3$ et ne se réduit pas à l'identité, alors $H = \mathbf{SO}_3$. Ce dernier est donc un groupe simple.