Corrigé du DS de Mathématiques n°8 — 4 mars 2017

Problème 1 — (A la mémoire d'Evariste...)

➤ Partie A - Générateurs du groupe alterné.

1) $S_3 = \{\mathrm{id}, (12), (13), (23), (123), (132)\}$ et $A_3 = \{\mathrm{id}, (123), (132)\}$.

Le groupe A_3 a exactement deux sous-groupes : $\{\mathrm{id}\}$ et A_3.

2) a) Soient τ_1 et τ_2 deux transpositions de S_n. Leurs supports (de cardinal 2) peuvent avoir une intersection constituée de 0, 1 ou 2 éléments.

1er cas — Si $\mathrm{Card}\,(\mathrm{supp}\,(\tau_1) \cap \mathrm{supp}\,(\tau_2)) = 0$: alors il existe quatre entiers distincts i, j, k et l tels que $\tau_1 = (ij)$ et $\tau_2 = (kl)$.

Dans ce cas on a : $\tau_1\tau_2 = (ij)(kl) = (kjl)(ikj)$.

2ème cas — Si $\mathrm{Card}\,(\mathrm{supp}\,(\tau_1) \cap \mathrm{supp}\,(\tau_2)) = 1$: alors il existe trois entiers distincts i, j et k tels que $\tau_1 = (ij)$ et $\tau_2 = (ik)$.

Dans ce cas on a : $\tau_1\tau_2 = (ij)(ik) = (ikj)$.

3ème cas — Si $\mathrm{Card}\,(\mathrm{supp}\,(\tau_1) \cap \mathrm{supp}\,(\tau_2)) = 2$: alors il existe deux entiers distincts i et j tels que $\tau_1 = (ij)$ et $\tau_2 = (ij)$.

Dans ce cas on a : $\tau_1\tau_2 = (ij)(ij) = \mathrm{id} = (123)\,(132)$ (par exemple).

Bilan : dans tous les cas, on a pu écrire $\tau_1\tau_2$ soit comme un 3-cycle, soit comme un produit de deux 3-cycles.

Conclusion. Le produit de deux transpositions de S_n est soit un 3-cycle, soit le produit de deux 3-cycles.

b) Soit σ un élément de A_n. Puisque S_n est engendré par les transpositions, il existe m transpositions $\tau_1, \ldots, \tau_m$ telles que : $\sigma = \prod_{k=1}^{m} \tau_k$. Or, σ étant un élément de A_n, l'entier m est nécessairement pair ; ainsi il existe un entier m' tel que $m = 2m'$. On a donc :

$$\sigma = \prod_{k=1}^{2m'} \tau_k \qquad \text{soit}^{*} : \qquad \sigma = \prod_{k=1}^{m'} (\tau_{2k-1}\tau_{2k})$$

Or d'après la question précédente, chacun des termes $\tau_{2k-1}\tau_{2k}$ est un 3-cycle, ou un produit de 3-cycles. Il s'ensuit que σ est un produit de 3-cycles.

Conclusion. Tout élément de A_n peut s'écrire comme un produit de 3-cycles. En d'autres termes, le groupe alterné A_n est engendré par les 3-cycles.

➤ Partie B - Ordre d'un élément dans un groupe.

3) Soit g un élément de G. Montrons que $\langle g\rangle$ est un sous-groupe de G.

SG1 : $\langle g\rangle \subset G$ par définition.

SG2 : $\mathrm{id} = g^0 \in \langle g\rangle$.

SG3 : soient γ et γ' deux éléments de $\langle g\rangle$. Par définition de $\langle g\rangle$, il existe deux entiers k et k' tels que : $\gamma = g^k$ et $\gamma' = g^{k'}$. Il s'ensuit que : $\gamma * \gamma' = g^{k+k'}$, d'où en particulier $\gamma * \gamma' \in \langle g\rangle$.

En résumé : $\left[(\gamma, \gamma') \in \langle g\rangle^2\right] \Longrightarrow [(\gamma * \gamma') \in \langle g\rangle]$

SG4 : soit γ un élément de $\langle g\rangle$. Par définition de $\langle g\rangle$, il existe un entier k tel que : $\gamma = g^k$. Il s'ensuit que : $\gamma^{-1} = g^{-k}$, d'où en particulier $\gamma^{-1} \in \langle g\rangle$. En résumé : $[\gamma \in \langle g\rangle] \Longrightarrow \left[\gamma^{-1} \in \langle g\rangle\right]$

Conclusion. Pour tout élément g de G, $\langle g\rangle$ est un sous-groupe de G.

4) a) On a : $(123)^0 = \mathrm{id}$; $(123)^1 = (123)$; $(123)^2 = (132)$ et $(123)^3 = \mathrm{id}$. Il s'ensuit que $\langle(123)\rangle = A_3$.

b) Dans $(\mathbb{Z}, +)$, le sous-groupe engendré par 2 est $2\mathbb{Z}$, le sous-groupe des entiers pairs.

∗. En "faisant des paquets de deux".

5) a) On a : $(1234)^1 = (1234)$; $(1234)^2 = (13)(24)$; $(1234)^3 = (1432)$ et $(1234)^4 = \mathrm{id}$.

Il s'ensuit que le 4-cycle (1234) est d'ordre 4.

b) Dans $(\mathrm{GL}_2(\mathbb{R}), \times)$, on considère $g = 2\mathrm{I}_2$. La matrice g est telle que : $\forall n \in \mathbb{N},\ g^n = 2^n \mathrm{I}_2$. Par conséquent : $\forall n \in \mathbb{N}^*,\ g^n \neq \mathrm{I}_2$. Il s'ensuit que la matrice g n'est pas d'ordre fini dans $\mathrm{GL}_2(\mathbb{R})$.

c) Soient G un groupe fini, et g un élément de G. Notons $n = \mathrm{Card}(G)$. On considère l'ensemble : $\{g^k \,/\, k \in [\![\, 0, n \,]\!]\}$. Si tous les éléments de cet ensemble étaient distincts, alors son cardinal serait $(n+1)$; ceci est absurde, puisqu'il s'agit d'une partie de G, qui est de cardinal n par hypothèse.

Il existe donc deux entiers k et k' distincts dans $[\![\, 0, n \,]\!]$ tels que : $g^k = g^{k'}$. Sans nuire à la généralité on peut supposer que $k < k'$ (si ce n'est pas le cas, on permute les rôles de k et k'). On a alors : $g^0 = g^{k'-k}$, c'est à dire : $g^{k'-k} = \mathrm{e}$.
En observant que $k' - k$ est un entier naturel non nul (puisque $k < k'$), on a établi l'existence d'un élément N de $\mathbb{N}^*$ tel que $g^N = \mathrm{e}$. Ce qui signifie que g est d'ordre fini.

Conclusion. Tout élément d'un groupe fini est d'ordre fini.

d) Soit g un élément de G d'ordre N, et soit m un entier.

Supposons que N divise m : alors il existe un entier k tel que $m = kN$. Il s'ensuit que : $g^m = g^{kN} = \left(g^N\right)^k = \mathrm{e}^k = \mathrm{e}$. D'où : $[N \text{ divise } m] \Longrightarrow [g^m = \mathrm{e}]$.

Réciproquement, supposons que $g^m = \mathrm{e}$. D'après le théorème de la division euclidienne, il existe un (unique) couple (q, r) tel que $m = Nq + r$ avec $q \in \mathbb{Z}$ et $r \in [\![\, 0, N-1 \,]\!]$. On a alors : $g^{Nq+r} = g^{Nq} * g^r = \mathrm{e} * g^r = g^r$; et donc $g^r = \mathrm{e}$.

Si r était non nul, on aurait alors prouvé l'existence d'un élément r de $\mathbb{N}^*$ tel que $g^r = \mathrm{e}$, avec r strictement inférieur à l'ordre de g : contradiction.

On en déduit que $r = 0$, ce qui implique que $m = Nq$, et donc que N divise m. D'où : $[g^m = \mathrm{e}] \Longrightarrow [N \text{ divise } m]$.

Conclusion. Pour g un élément d'ordre N on a : $[g^m = \mathrm{e}] \Longleftrightarrow [N \text{ divise } m]$.

➤ **Partie C - Un théorème de Lagrange**. Le but de cette partie est d'établir que le cardinal de tout sous-groupe d'un groupe fini divise le cardinal de G.

6) Soit H un sous-groupe d'un groupe fini G. Observons que H est de cardinal fini, en tant que partie d'un ensemble fini.

Soit g un élément arbitraire de G.
Les applications $\varphi : H \longrightarrow gH$ et $\psi : gH \longrightarrow H$ sont clairement réciproques l'une de l'autre.
$h \longmapsto g * h$ $\quad$ $x \longmapsto g^{-1} * x$

En particulier φ et ψ sont bijectives ; les ensembles H et gH sont donc équipotents. D'où : $\mathrm{Card}(H) = \mathrm{Card}(gH)$.

Conclusion. Pour tout élément g de G on a : $\mathrm{Card}(H) = \mathrm{Card}(gH)$.

7) Soient g et g' deux éléments de G. Supposons que gH et $g'H$ ne sont pas disjoints. Alors il existe deux éléments h et k dans H tels que : $g * h = g' * k$. En particulier : $g^{-1} * g' = h * k^{-1} \in H$.†

Soit alors γ un élément quelconque de $g'H$. Il existe un élément h_0 de H tel que : $\gamma = g' * h_0$. On écrit alors judicieusement : $\gamma = g * g^{-1} * g' * h_0$. On en déduit que : $\gamma = g * \underbrace{h * k^{-1} * h_0}_{\in H}$. Par suite : $\gamma \in gH$.

On a ainsi établi que : $g'H \subset gH$.

En réécrivant le même raisonnement en permutant g et g', ou en observant que g et g' jouent des rôles symétriques dans le raisonnement précédent, on obtient l'autre inclusion : $gH \subset g'H$. Finalement, lorsque gH et $g'H$ ne sont pas disjoints, ils sont égaux.

Conclusion. Pour tout couple (g, g') d'éléments de G, on a $[gH = g'H]$ ou $[gh \cap g'H = \emptyset]$.

†. En effet, k est un élément de H. Puisque H est un sous-groupe, k^{-1} est un élément de H. Par ailleurs, h est un autre élément de H. En utilisant une nouvelle fois le fait que H est un sous-groupe, on en déduit que : $h * k^{-1} \in H$.

8) Le groupe G est fini par hypothèse. On peut donc noter : $G = \{g_1, \dots, g_n\}$ (avec $n = \text{Card}(G)$). On a alors : $G = \bigcup_{i=1}^{n} \{g_i\}$ et donc $G = \bigcup_{i=1}^{n} g_i H$. La première égalité provient de l'observation puissante selon laquelle un ensemble fini est la réunion des singletons qui le composent ; la seconde découle de la première et du fait que pour tout entier i on a : $\{g_i\} \subset g_i H \subset G$.

D'après la question précédente, il peut exister parmi les $g_i H$ des ensembles égaux. Notons alors k le nombre de parties disjointes parmi ces $g_i H$. Quitte à renuméroter les g_i, on peut supposer qu'il s'agit des k premières parties, et on alors : $G = \bigcup_{i=1}^{k} g_i H$. Cette union étant disjointe, on a donc : $\text{Card}(G) = \sum_{i=1}^{k} \text{Card}\,(g_i H)$. Or d'après la question 6, on a : $\text{Card}(g_i H) = \text{Card}(H)$ (pour tout g_i).

On en déduit que : $\text{Card}(G) = \sum_{i=1}^{k} \text{Card}\,(H)$ d'où : $\text{Card}(G) = k\text{Card}\,(H)$. Finalement, le cardinal de G est multiple de celui de H. **Conclusion**. Si G est un groupe fini, le cardinal de tout sous-groupe de G divise le cardinal de G.

9) Soit g un élément d'un groupe fini G. Alors g est d'ordre fini (d'après la question 5-c), et son ordre est le cardinal de $\langle g \rangle$. Or $\langle g \rangle$ est un sous-groupe de G (d'après la question 3), donc son ordre divise celui de G (d'après la question précédente).

Conclusion. Dans un groupe fini G, tout élément g est d'ordre fini, et l'ordre de g divise le cardinal de G.

➤ **Partie D - Abélianité des groupes de cardinal 5**.

10) D'après la définition, il est équivalent de dire que G est cyclique ou qu'il existe un élément g de G dont l'ordre est égal au cardinal de G.

Or dans le groupe S_3, les éléments peuvent être d'ordre 1 (l'identité), d'ordre 2 (les trois transpositions) ou d'ordre 3 (les deux 3-cycles). Aucun élément n'a donc un ordre égal au cardinal de S_3, qui vaut 6. Donc S_3 n'est pas cyclique.

En revanche le groupe A_3 est cyclique, puisque $A_3 = \langle (123) \rangle$ (ou $A_3 = \langle (132) \rangle$).

11) Si G est un groupe cyclique, alors il existe un élément g de G tel que $G = \left\{g^k \,/ k \in \mathbb{Z}\right\}$. Il est alors clair que G est abélien (essentiellement car $g^k * g^{k'} = g^{k+k'} = g^{k'} * g^k$). **Conclusion**. $[G \text{ cyclique}] \Longrightarrow [G \text{ abélien}]$.

12) Soit G un groupe de cardinal 5. Soit g un élément de G, distinct de l'élément neutre. On sait que g est d'ordre fini, et que cet ordre divise 5 (d'après la question 9). Ainsi l'ordre de g pourrait valoir 1 ou 5 ; mais $g \neq e$, donc g n'est pas d'ordre 1. Il s'ensuit que g est d'ordre 5, ce qui signifie que : $G = \langle g \rangle$. D'où le groupe G est cyclique, donc abélien d'après la question précédente.

Conclusion. Tout groupe fini de cardinal 5 est abélien.

Complément. Tout groupe fini de cardinal p premier est abélien.

➤ **Partie E - Conjugaison dans un groupe**.

Soit n un entier supérieur ou égal à 2. On dit que deux permutations τ_1 et τ_2 de S_n sont **conjuguées** s'il existe une permutation σ de S_n telle que : $\tau_2 = \sigma \tau_1 \sigma^{-1}$.

13) Soit $\tau \in S_n$. Alors : $\tau = \text{id}\tau\text{id}^{-1}$. Donc τ est conjuguée à elle-même, ce qui prouve la **réflexivité** de la relation de conjugaison.

Soient τ_1 et τ_2 deux permutations (dans S_n) conjuguées. Par définition, il existe une permutation σ de S_n telle que : $\tau_2 = \sigma \tau_1 \sigma^{-1}$. On a donc : $\tau_1 = \sigma^{-1} \tau_2 \sigma$ d'où $\tau_1 = \sigma' \tau_2 \sigma'^{-1}$ (en ayant posé $\sigma' = \sigma^{-1}$). Il s'ensuit que la relation de conjugaison est **symétrique**.

Soient enfin τ_1, τ_2 et τ_3 trois permutations (dans S_n) telles que τ_1 et τ_2 d'une part, τ_2 et τ_3 d'autre part sont conjuguées. Par définition, il existe deux permutations σ et ρ de S_n telles que : $\tau_2 = \sigma \tau_1 \sigma^{-1}$ et $\tau_3 = \rho \tau_2 \rho^{-1}$. On en déduit que :

$$\tau_3 = \rho\sigma\tau_1\sigma^{-1}\rho^{-1} = \rho\sigma\tau_1\,(\rho\sigma)^{-1} \quad \text{d'où : } \tau_3 = \zeta\tau_1\zeta^{-1} \text{ (en ayant posé : } \zeta = \rho\sigma).$$

On en déduit que τ_1 et τ_3 sont conjuguées ; ce qui établit la **transitivité** de la relation de conjugaison.

Conclusion. La relation de conjugaison dans S_n est réflexive, symétrique et transitive. C'est donc une relation d'équivalence sur S_n.

14) a) On a : $(13)(12)(13)^{-1} = (13)(12)(13) = (23)$. Or : $(23) \notin \langle(12)\rangle$.
Il s'ensuit que : $\langle(12)\rangle$ n'est pas un sous-groupe distingué de S_3.

b) Soit τ un élément arbitraire de A_n. Pour tout élément σ de S_n, on a : $\varepsilon\left(\sigma\tau\sigma^{-1}\right) = \varepsilon(\sigma)\,\varepsilon(\tau)\,\varepsilon\left(\sigma^{-1}\right)$.
Puisque $\varepsilon\left(\sigma^{-1}\right) = \varepsilon(\sigma)$, on en déduit que : $\varepsilon\left(\sigma\tau\sigma^{-1}\right) = \varepsilon(\tau)$ d'où : $\varepsilon\left(\sigma\tau\sigma^{-1}\right) = 1$ puisque τ est paire par hypothèse.

On en déduit que pour toute permutation σ de S_n, la permutation $\sigma\tau\sigma^{-1}$ est encore un élément de A_n. Le sous-groupe A_n est donc stable par conjugaison. Ainsi, A_n est un sous-groupe distingué de S_n.

➤ **Partie F - Simplicité de A_5.**

15) D'après le cours : $\text{Card}\,(A_5) = \dfrac{5!}{2}$ d'où : $\text{Card}\,(A_5) = 60$.

16) Une première idée. Soit $\sigma \in A_n$, avec $\sigma \neq \text{id}$. On sait que σ s'écrit comme un produit de 2 ou 4 transpositions. En effet, tout élément de S_5 s'écrit comme un produit d'au plus 5 transpositions (résultat général du cours) ; pour une permutation paire de S_5, le nombre de transpositions intervenant dans ce produit peut donc être égal à 0, 2 ou 4. Mais la valeur 0 est exclue, puisque l'on suppose que $\sigma \neq \text{id}$.

Supposons que σ soit produit de deux transpositions : alors d'après la discussion faite dans la question 2-a, σ est soit égale au produit de deux transpositions à supports disjoints (1er cas), soit égale à un 3-cycle (2ème cas).‡ Jusque-là tout va bien.
Supposons que σ soit produit de 4 transpositions : aïe ! Même avec la discussion faite dans la question 2-a, et même en décidant par exemple de regrouper deux par deux les transpositions, le nombre de cas à étudier suivant les supports des transpositions est ici très dissuasif !

Une seconde idée. Une autre stratégie consiste à observer que toute permutation peut s'écrire comme un produit de cycles à supports disjoints ; c'est en tout cas clair sur les exemples vus précédemment dans ce devoir (et en exercices). On pose donc pour tout entier naturel $n \geqslant 2$:

$$\text{P}(n) : \text{“Toute permutation de } S_n \text{ peut s'écrire comme un produit de cycles à supports disjoints.”}$$

Prouvons $\text{P}(n)$ par récurrence sur n.

➤ **Initialisation**. Pour $n = 2$, le groupe S_2 est constitué de id (produit de 0 cycle), et de (12) (produit d'un cycle). La propriété $\text{P}(2)$ est donc vraie.

➤ **Hérédité**. Supposons $\text{P}(n)$ vraie pour un certain entier $n \geqslant 2$, et montrons que $\text{P}(n+1)$ l'est.

Soit $\sigma \in S_{n+1}$. On distingue deux cas :

☞ Si $\sigma(n+1) = n+1$. Alors $\sigma_{|\mathbb{N}_n}$ est un élément de S_n. D'après l'hypothèse de récurrence, il existe alors k cycles à supports disjoints $c_1, \ldots, c_k$ (dans S_n) tels que : $\sigma_{|\mathbb{N}_n} = \prod_{i=1}^{k} c_i$. Or un cycle de S_n induit naturellement un cycle de S_{n+1}, et la relation précédente implique que σ est le produit des k cycles c_i vus comme éléments de S_{n+1}.

☞ Si $\sigma(n+1) \neq n+1$. Il existe alors un entier naturel non nul p tel que les entiers $n+1, \sigma(n+1), \ldots, \sigma^{p-1}(n+1)$ sont distincts, et $\sigma^p(n+1) = n+1$. On définit alors un cycle c en posant :

$$c = \left((n+1)\,\sigma(n+1)\cdots\sigma^{p-1}(n+1)\right)$$

Par construction, la permutation $c^{-1}\sigma$ laisse invariants les entiers : $n+1, \sigma(n+1), \ldots, \sigma^{p-1}(n+1)$.
En particulier, puisque $c^{-1}\sigma$ laisse invariant $n+1$, on peut (d'après l'étude faite dans le premier cas) affirmer que $c^{-1}\sigma = \prod_{i=1}^{k} c_i$ où les c_i sont k cycles à supports disjoints. En outre, les supports des c_i sont disjoints de $\left\{n+1, \sigma(n+1), \ldots, \sigma^{p-1}(n+1)\right\}$ puisque le produit des c_i laisse invariants ces éléments.

‡. Le 3ème cas est exclu puisque $\sigma \neq \text{id}$.

Par suite : $\sigma = c\prod_{i=1}^{k} c_i$, et on a écrit σ comme produit de cycles à supports disjoints.

Dans les deux cas, on a montré que $\mathrm{P}(n+1)$ est vraie.

➤ **Conclusion**. Toute permutation de S_n peut s'écrire comme un produit de cycles à supports disjoints.

En particulier, tout élément de A_5 peut s'écrire comme un produit de cycles à supports disjoints. Mais le nombre de décompositions est alors limité ! En effet, pour des raisons de parité, un élément de A_5 ne pourra être que l'identité, ou un produit de deux transpositions à supports disjoints, ou un 3-cycle ou un 5-cycle.

Conclusion. Tout élément de A_5 distinct de l'identité est soit un 3-cycle, soit un 5-cycle, soit un produit de deux transpositions à supports disjoints.

17) a) Pour définir un 5-cycle $(a_1a_2a_3a_4a_5)$ dans A_5, on peut toujours convenir de commencer par $a_1 = 1$. En d'autres termes, tout 5-cycle admet une écriture de la forme : $(1a_2a_3a_4a_5)$. Pour créer un tel cycle, on a 4 choix pour a_2 ; 3 choix pour a_3 ; 2 choix pour a_4 et plus de choix du tout pour a_5.

Conclusion. Il existe 24 5-cycles dans A_5.

b) Pour définir un 3-cycle, on commence par choisir trois éléments de $[\![\, 1,5 \,]\!]$. Il y a $\binom{5}{3} = 10$ façons de le faire. On observe alors que chaque combinaison $\{a_1, a_2, a_3\}$ donne naissance à exactement deux 3-cycles : $(a_1a_2a_3)$ et $(a_1a_3a_2)$.

Conclusion. Il existe 20 3-cycles dans A_5.

c) D'après la question 16, le groupe A_5 est constitué de l'identité, des 5-cycles, des 3-cycles et des produits de deux transpositions à supports disjoints dans A_5. On en déduit, d'après les questions 15, 17-a et 17-b qu'il existe :
$60 - (1 - 24 - 20) = 15$ produits de deux transpositions à supports disjoints dans A_5.

18) a) Soient $a_1, \ldots, a_{n-2}$ (n-2) éléments de $[\![\, 1,n \,]\!]$; on note a_{n-1} et a_n les deux éléments restants. Et soient de même $b_1, \ldots, b_{n-2}$ (n-2) éléments de $[\![\, 1,n \,]\!]$; on note b_{n-1} et b_n les deux éléments restants.

On définit un élément τ de S_n en posant : $\forall\, i \in [\![\, 1,n \,]\!],\ \tau(a_i) = b_i$.

Si τ est paire, on pose $\sigma = \tau$. Sinon, on pose $\sigma = (a_{n-1}a_n)\,\tau$.

Dans les deux cas, σ est paire et vérifie : $\forall\, i \in [\![\, 1,n-2 \,]\!],\ \sigma(a_i) = b_i$.

b) Etablir l'égalité $\tau_2 = (\sigma(i_1)\cdots\sigma(i_k))$, c'est établir que pour tout $\sigma(i_j)$ on a $\tau_2(\sigma(i_j)) = \sigma(i_{j+1})$ (avec la convention que $\sigma(i_{k+1}) = i_1$) ; et que tout les autres entiers de $\mathbb{N}_n$ ne sont pas dans le support de τ_2.

On sépare donc les entiers de $\mathbb{N}_n$ en deux parties disjointes : ceux qui appartiennent à l'ensemble $\{\sigma(i_1), \ldots, \sigma(i_k)\}$ et les autres.

➤ Soit m un entier dans $\{\sigma(i_1), \ldots, \sigma(i_k)\}$. Alors il existe un entier j compris entre 1 et k tel que : $m = \sigma(i_j)$.

D'une part on a alors : $\tau_2(m) = \sigma\tau_1\sigma^{-1}(\sigma(i_j)) = \sigma\tau_1(i_j) = \sigma(i_{j+1})$

Et d'autre part : $(\sigma(i_1)\cdots\sigma(i_k))(m) = (\sigma(i_1)\cdots\sigma(i_k))(\sigma(i_j)) = \sigma(i_{j+1})$

On en déduit que pour tout m un entier dans $\{\sigma(i_1), \ldots, \sigma(i_k)\}$ on a : $\tau_2(m) = (\sigma(i_1)\cdots\sigma(i_k))(m)$.

➤ Soit m un entier dans $\mathbb{N}_n \setminus \{\sigma(i_1), \ldots, \sigma(i_k)\}$. Alors il est déjà clair que : $(\sigma(i_1)\cdots\sigma(i_k))(m) = m$.

Par ailleurs, l'hypothèse faite sur m impose que $\sigma^{-1}(m) \notin \{i_1, \ldots, i_k\}$. En effet, dans le cas contraire, m serait égal à un $\sigma(i_j)$ pour un certain entier j, ce qui contredirait notre hypothèse. Il s'ensuit que $\sigma^{-1}(m)$ est laissé invariant par τ_1, d'où :

$$\tau_2(m) = \sigma\tau_1\sigma^{-1}(m) = \sigma\tau_1\left(\sigma^{-1}(m)\right) = \sigma\left(\sigma^{-1}(m)\right) = m$$

On en déduit que pour tout m un entier dans $\mathbb{N}_n \setminus \{\sigma(i_1), \ldots, \sigma(i_k)\}$ on a : $\tau_2(m) = (\sigma(i_1)\cdots\sigma(i_k))(m)$.

➤ En conclusion, on a établi que : $\forall\, m \in \mathbb{N}_n,\ \tau_2(m) = (\sigma(i_1)\cdots\sigma(i_k))(m)$. D'où : $\tau_2 = (\sigma(i_1)\cdots\sigma(i_k))$

19) Soient c_1 et c_2 deux 3-cycles de A_5. Il existe trois entiers a_1, a_2 et a_3 (*resp.* b_1, b_2 et b_3) dans $\mathbb{N}_5$ tels que $c_1 = (a_1a_2a_3)$ (*resp.* $c_2 = (b_1b_2b_3)$). D'après la question 18-a, il existe une permutation paire $\sigma \in A_5$ telle que : $\forall\, i \in [\![\, 1,3 \,]\!],\ \sigma(a_i) = b_i$. D'après la question 18-b, on a alors $c_2 = \sigma c_1 \sigma^{-1}$ ce qui signifie que c_1 et c_2 sont conjugués.

Conclusion. Les 3-cycles sont deux à deux conjugués dans A_5.

20) Soient $\sigma_1 = (i_1 j_1)(k_1 l_1)$ et $\sigma_2 = (i_2 j_2)(k_2 l_2)$ deux produits de transpositions à supports disjoints. On note m_1 (*resp.* m_2) l'unique entier de $\mathbb{N}_5$ tel que $\mathbb{N}_5 = \{i_1, j_1, k_1, l_1, m_1\}$ (*resp.* ...). On définit une permutation α dans S_5 en posant : $\alpha(i_1) = i_2$, $\alpha(j_1) = j_2$,...

Si α est paire, on pose $\rho = \alpha$ et on a alors : $\rho\sigma_1\rho^{-1} = (\rho(i_1)\rho(j_1))(\rho(k_1)\rho(l_1)) = (i_2 j_2)(k_2 l_2) = \sigma_2$

Si α est impaire, on pose $\rho = \alpha(i_1 j_1)$ et on a alors : $\rho\sigma_1\rho^{-1} = (\rho(j_1)\rho(i_1))(\rho(k_1)\rho(l_1)) = (j_2 i_2)(k_2 l_2) = \sigma_2$

Dans les deux cas, on a établi l'existence d'une permutation $\rho \in A_5$ telle que : $\rho\sigma_1\rho^{-1} = \sigma_2$.

Conclusion. Les produits de deux transpositions à supports disjoints sont deux à deux conjugués dans A_5.

21) a) Soit H un sous-groupe distingué de A_5. Si H contient un 3-cycle c, alors H contient tout élément conjugué à c (puisque H est stable par conjugaison). Or d'après la question 19, les 3-cycles sont deux à deux conjugués dans A_5 ; donc H contient tous les 3-cycles.

Le même raisonnement s'applique aux permutations qui sont produits de deux transpositions à supports disjoints, en vertu de la question 20 cette fois-ci.

Conclusion. Lorsque H est un sous-groupe distingué (càd stable par conjugaison) de H_5, il contient tous les 3-cycles dès lors qu'il en contient un. De même, si H contient un produit de deux transpositions à supports disjoints, alors il contient tous les produits de deux transpositions à supports disjoints.

b) Il est clair que $\{\mathrm{id}\}$ et A_5 sont des sous-groupes distngués de A_5. Le but est de prouver qu'il n'existe que ceux-là.

Soit H un sous-groupe distingué de A_5. Si H n'est pas réduit à l'identité, alors H contient au moins un 3-cycle (ou un 5-cycle, ou un produit de deux transpositions à supports disjoints). Mais alors, d'après la question précédente, H contient tous les 3-cycles (ou tous les 5-cycles, ou...), qui sont au nombre de 20 (ou 24 ou 15).
Or H ne peut contenir (en plus de l'identité évidemment) que les 3-cycles, sinon il serait de cardinal 21 ; or son cardinal doit diviser celui de A_5 (égal à 60) d'après le théorème de Lagrange (question 8). Il doit donc contenir au moins un 5-cycle ou un produit de deux transpositions à supports disjoints ; mais alors il contient toutes les permutations de ce type et on obtient donc : $\mathrm{Card}(H) > 30$. Une nouvelle application du théorème de Lagrange implique que $\mathrm{Card}(H) = 60$, càd $H = A_5$.

De même H ne peut contenir que les 5-cycles, sinon il serait de cardinal 25 ; et H ne peut contenir que les produits de deux transpositions à supports disjoints, sinon il serait de cardinal 16. Dans ces deux cas, on raisonne comme précédemment pour conclure finalement que $H = A_5$.

Conclusion. Le groupe A_5 ne possède aucun sous-groupe non trivial stable par conjugaison (les seuls sous-groupes distingués de A_5 sont $\{\mathrm{id}\}$ et A_5).

Problème 2 — (Résolution d'une équation fonctionnelle).

1) La fonction th est continue et strictement croissante sur $\mathbb{R}$. A ce titre elle réalise une bijection de $\mathbb{R}$ vers $\mathrm{th}(\mathbb{R})$, càd de $\mathbb{R}$ vers $]-1,1[$.

2) D'après la question précédente, la fonction th admet une bijection réciproque, notée argth. On peut alors affirmer que la fonction argth est impaire et strictement croissante, car th l'est et que la bijection réciproque d'une fonction impaire (*resp.* strictement croissante) est impaire (*resp.* strictement croissante).

3) La bijection réciproque f^{-1} d'une fonction f est dérivable en $f(x_0)$ dès lors que f est dérivable en x_0 et que $f'(x_0) \neq 0$; et dans ce cas $\left(f^{-1}\right)'(f(x_0)) = 1/f'(x_0)$.

La fonction th est dérivable sur $\mathbb{R}$, et sa dérivée $(1 - \mathrm{th}^2)$ ne s'annule pas. Il s'ensuit que pour tout réel x_0, la fonction argth est dérivable en $\mathrm{th}(x_0)$, et $\mathrm{argth}'(\mathrm{th}(x_0)) = \dfrac{1}{1 - \mathrm{th}^2(x_0)}$.

Par conséquent, la fonction argth est dérivable sur $]-1,1[$, et : $\forall x \in]-1,1[$, $\mathrm{argth}'(x) = \dfrac{1}{1-x^2}$.

4) Soit y un réel strictement compris entre -1 et 1, et résolvons dans $\mathbb{R}$ l'équation $\text{th}(x) = y$ (afin de déterminer $\text{argth}(y)$). On a :

$$[\text{th}(x) = y] \iff \left[\frac{\mathrm{e}^x - \mathrm{e}^{-x}}{\mathrm{e}^x + \mathrm{e}^{-x}} = y\right] \iff [\mathrm{e}^x - \mathrm{e}^{-x} = y\mathrm{e}^x + y\mathrm{e}^{-x}] \iff \left[(1-y)\,\mathrm{e}^{2x} = 1 + y\right]$$

$$\left[\mathrm{e}^{2x} = \frac{1+y}{1-y}\right] \iff \left[x = \frac{1}{2}\ln\left(\frac{1+y}{1-y}\right)\right]$$

Conclusion. $\forall x \in\ ]-1,1[\ ,\ \text{argth}(x) = \ln\left(\sqrt{\dfrac{1+x}{1-x}}\right)$

➤ **Partie B - Une équation fonctionnelle**.

Le but de cette partie est de résoudre le problème suivant :
"Déterminer les fonctions f définies sur $\mathbb{R}$, à valeurs réelles et dérivables en 0 qui vérifient :

$$\forall x \in \mathbb{R},\ f(2x) = \frac{2f(x)}{1 + (f(x))^2}.\ "$$

5) Soit f constante égale à k. La fonction f est alors solution du problème posé si et seulement si : $k = \dfrac{2k}{1+k^2}$, càd SSI $k = 0$ ou $1 + k^2 = 2$.
Finalement, les fonctions constantes solutions du problème sont celles égales à 0, à 1 ou à -1.

6) Si f est solution du problème, alors $f(0) = \dfrac{2f(0)}{1+f(0)^2}$. Les calculs de la question précédente permettent alors d'affirmer que $f(0) \in \{-1, 0, 1\}$.

7) Soit x un réel. On a d'après l'énoncé : $f(x) = \dfrac{2f(x/2)}{1+f(x/2)^2}$. Posons alors pour tout y réel : $g(y) = \dfrac{2y}{1+y^2}$. La fonction g est définie sur $\mathbb{R}$, impaire, et de classe $\mathscr{C}^\infty$ sur $\mathbb{R}$ (d'après les théorèmes généraux). On peut en particulier calculer sa dérivée sur $\mathbb{R}$:

$$\forall y \in \mathbb{R},\ g'(y) = \frac{2 + 2y^2 - 4y^2}{(1+y^2)^2} = \frac{2}{(1+y^2)^2}\left(1 - y^2\right)$$

La fonction g étant impaire, il suffit d'étudier ses variations sur $\mathbb{R}_+$ pour les connaître sur $\mathbb{R}$. D'après le calcul précédent, la fonction g' est positive sur $[0,1]$, négative sur $[1, +\infty[$. On en déduit le tableau de variation de g ci-contre.

x	$-\infty$		-1		0		1		$+\infty$
$f(x)$	0	↘	-1	↗	0	↗	1	↘	0

On en déduit que : $\forall x \in \mathbb{R},\ -1 \leqslant f(x) \leqslant 1$

8) Supposons que f soit solution du problème posé. Alors pour tout réel x : $(-f)(2x) = \dfrac{2 \times (-f)(x)}{1 + ((-f)(x))^2}$. Donc $-f$ est également solution.

Dans les questions 9 à 13, on suppose que f est une solution du problème posé, que $f(0) = 1$ et que f n'est pas constante.

On considère $x_0 \in \mathbb{R}$, tel que $f(x_0) \neq f(0)$, et on définit la suite (u_n) en posant : $\forall n \in \mathbb{N},\ u_n = f\left(\dfrac{x_0}{2^n}\right)$.

9) La suite de terme général $\dfrac{x_0}{2^n}$ converge évidemment vers 0. Puisque f est continue (car dérivable) en 0, la propriété de continuité séquentielle implique que : $\lim\limits_{n\to+\infty} f\left(\dfrac{x_0}{2^n}\right) = f(0)$. D'où : $\lim\limits_{n\to+\infty} u_n = 1$.

10) Soit n un entier naturel. On a : $u_n = f\left(\frac{x_0}{2^n}\right) = f\left(2\,\frac{x_0}{2^{n+1}}\right) = \dfrac{2f\left(\frac{x_0}{2^{n+1}}\right)}{1+\left(f\left(\frac{x_0}{2^{n+1}}\right)\right)^2} = \dfrac{2u_{n+1}}{1+u_{n+1}^2}$.

En résumé : $\boxed{\forall n \in \mathbb{N},\ u_n = \dfrac{2u_{n+1}}{1+u_{n+1}^2}}$. Puisque $1+u_{n+1}^2 > 0$, on en déduit que la suite $\boxed{(u_n) \text{ est de signe constant}}$.

Par ailleurs, pour tout entier naturel n on a : $u_{n+1} - u_n = u_{n+1} - \dfrac{2u_{n+1}}{1+u_{n+1}^2} = \dfrac{u_{n+1}^3 - u_{n+1}}{1+u_{n+1}^2} = \dfrac{u_{n+1}^2-1}{1+u_{n+1}^2}\,u_{n+1}$.

En résumé : $\forall n \in \mathbb{N},\ u_{n+1} - u_n = \dfrac{u_{n+1}^2-1}{1+u_{n+1}^2}\,u_{n+1}$. Puisque la fonction f est à valeurs dans $[-1,1]$, on en déduit que : $\dfrac{u_{n+1}^2-1}{1+u_{n+1}^2} \leqslant 0$. Il s'ensuit que $u_{n+1}-u_n$ est du signe opposé à u_{n+1}, càd du signe opposé à u_0 puisque la suite (u_n) est de signe constant.

Conclusion. Si $u_0 \geqslant 0$, alors la suite (u_n) est décroissante ; sinon la suite (u_n) est croissante.

11) La fonction f étant à valeurs dans $[-1,1]$, et puisque l'on fait l'hypothèse que $u_0 \neq 1$, on a donc $u_0 \in [-1,1[$. Distinguons deux cas.

➤ 1er cas : si $u_0 \in [-1,0[$. Alors la suite (u_n) est à termes négatifs (d'après la question 10), donc ne peut converger vers 1 (question 9) : contradiction.

➤ 2ème cas : si $u_0 \in [0,1[$. Alors la suite (u_n) est décroissante (question 10) et majorée par u_0, qui est strictement inférieur à 1. Donc (u_n) ne peut converger vers 1 (question 9) : contradiction.

Puisque les deux cas conduisent à une contradiction : il n'existe pas de solution f du problème telle que $f(0)=1$.

12) & 13) Par ailleurs, s'il existait une solution f du problème telle que $f(0)=-1$, alors la fonction $(-f)$ serait également solution du problème (question 8) et vérifierait $(-f)(0) = 1$; ce qui ne peut se produire d'après la question précédente.

Conclusion. Il n'existe pas de solution f du problème telle que $f(0)=1$, ou telle que $f(0)=-1$.

Dans les questions 14 à 18, on suppose que f est une solution du problème posé, que $f(0)=0$.

14) Raisonnons par l'absurde, et supposons qu'il existe un réel x_0 tel que $f(x_0)=1$. On pose alors pour tout entier naturel n : $u_n = f\left(\frac{x_0}{2^n}\right)$. Alors la suite (u_n) converge vers $f(0)=0$ (même raisonnement que dans la question 9). Or le calcul effectué dans la question 10 montre que la suite (u_n) est constante égale à 1 (puisque $u_0=1$) : contradiction.

Il n'existe donc pas de réel x_0 tel que $f(x_0)=1$. En utilisant le résultat de la question 8, on peut également affirmer qu'il n'existe pas de réel x_0 tel que $f(x_0)=-1$.

Conclusion. La fonction f est à valeurs dans $]-1,1[$.

15) Soit x un réel. On a :

$$g(2x) = \text{argth}(f(2x)) = \frac{1}{2}\ln\left(\frac{1+f(2x)}{1-f(2x)}\right) = \frac{1}{2}\ln\left(\left(\frac{1+f(x)}{1-f(x)}\right)^2\right) = \ln\left(\frac{1+f(x)}{1-f(x)}\right) = 2\text{argth}(f(x)) = 2g(x)$$

Conclusion. $\forall x \in \mathbb{R},\ g(2x) = 2g(x)$.

16) La fonction f est dérivable en 0 (par hypothèse), et la fonction argth est dérivable en $0 = f(0)$ (question 3). Donc $g = \text{argth} \circ f$ est dérivable en 0 (et $g'(0) = f'(0)$).

17) La suite de terme général $\dfrac{x}{2^n}$ converge vers 0. D'après la propriété de continuité séquentielle, la suite de terme général $g\left(\dfrac{x}{2^n}\right)$ converge vers $g(0)$. D'où par limite séquentielle : $\boxed{\lim\limits_{n\to+\infty} \dfrac{g\left(\frac{x}{2^n}\right)}{\left(\frac{x}{2^n}\right)} = g'(0)}$.

18) Soit x un réel. Pour tout entier n on a : $v_n = \dfrac{g\left(\dfrac{x}{2^n}\right)}{\left(\dfrac{x}{2^n}\right)} = \dfrac{g\left(2\times\dfrac{x}{2^{n+1}}\right)}{\left(2\times\dfrac{x}{2^{n+1}}\right)} = \dfrac{g\left(\dfrac{x}{2^{n+1}}\right)}{\left(\dfrac{x}{2^{n+1}}\right)} = v_{n+1}$.

Ainsi la suite (v_n) est constante. Or, d'après la question précédente elle converge vers $g'(0)$. Donc la suite (v_n) est constante égale à $g'(0)$ (et en particulier $v_0 = g(x)/x = g'(0)$). Or cette relation est valable pour tout réel x. Autrement dit : $\forall x \in \mathbb{R},\ \dfrac{g(x)}{x} = g'(0)$, d'où : $\forall x \in \mathbb{R},\ g(x) = g'(0)x$. **Conclusion**. g est linéaire.

19) Les fonctions f solutions du problème posé sont exactement les suivantes :

- Si $f(0) = 1$: seule la fonction constante égale à 1 est solution (questions 5 et 13).
- Si $f(0) = -1$: seule la fonction constante égale à -1 est solution (questions 5 et 13).
- Si $f(0) = 0$: alors les fonctions solutions sont exactement les fonctions

$$f_k : x \in \mathbb{R} \longmapsto \mathrm{th}(kx) \ (k \text{ parcourant } \mathbb{R}).$$