Devoir surveillé de Mathématiques n^{0}8 — 4 mars 2017

➤ *La durée du devoir est de 4h, les calculatrices sont interdites. Le sujet est rédigé sur 4 pages, et est constitué de 2 problèmes.*

➤ *N'oubliez pas de numéroter vos copies, d'encadrer ou de souligner les résultats à la fin de chaque question, d'accorder du soin à la présentation, et à votre rédaction (phrases, quantificateurs, liens logiques).*
Enfin, en cas de besoin, vous avez le droit d'admettre le résultat d'une question pour passer à la suivante.

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

Ce problème a deux objectifs principaux : un théorème de Lagrange (1736-1813) concernant les groupes finis, et un résultat concernant le groupe alterné A_5 dû à Galois (1811-1832, Evariste de son prénom). Le premier permet de démontrer en particulier que tout groupe de cardinal 5 est abélien, résultat qui complète celui que nous avons établi en cours (sur les groupes de cardinal $\leqslant 4$). Le second, établi en toute fin de devoir, est l'ingrédient essentiel pour prouver que l'équation générique de degré 5 n'est pas résoluble par radicaux, ce qui signifie très grossièrement qu'il n'existe pas de formule générale donnant les racines d'une équation polynomiale de degré 5.

Notations et rappels. Soit $(G, *)$ un groupe. Pour tout élément g de G, on note $g^2 = g * g$; $g^3 = g * g * g$ et plus généralement pour tout entier $n \in \mathbb{N}$: $g^n = \underbrace{g * g * \cdots * g}_{n \text{ termes}}$.

Cette définition est étendue à un exposant entier relatif, en posant pour tout $n \in \mathbb{Z}_-$: $g^n = \left(g^{-1}\right)^{-n}$.
On note par ailleurs : $\langle g \rangle = \left\{g^k \ / \ k \in \mathbb{Z}\right\}$.
On rappelle que pour tout entier n supérieur ou égal à 2, S_n désigne le groupe symétrique d'ordre n, et A_n le groupe alterné d'ordre n, respectivement constitués des permutations et des permutations paires de $\mathbb{N}_n$.

Enfin deux transpositions (ij) et (kl) sont dites à supports disjoints lorsque $\{i, j\} \cap \{k, l\} = \emptyset$.

➤ Partie A - Générateurs du groupe alterné.

1) Donner la liste des éléments de S_3, puis celle des éléments de A_3. Quels sont les sous-groupes de A_3 ?
2) Soit $n \geqslant 5$ un entier naturel. Un résultat du cours affirme que S_n est engendré par les transpositions. Le but de cette question est d'établir que A_n est engendré par les 3-cycles.
   a) Montrer que le produit de deux transpositions (non nécessairement à supports disjoints) de S_n est soit un 3-cycle, soit le produit de deux 3-cycles.
   b) En déduire que les 3-cycles engendrent A_n, càd que tout élément de A_n s'écrit comme produit de 3-cycles.

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

Soient $(G, *)$ un groupe, d'élément neutre e, et g un élément de G.

3) Montrer que $\langle g \rangle$ est un sous-groupe de G. *Par la suite, $\langle g \rangle$ sera appelé le **sous-groupe engendré par** g.*
4) **Deux exemples**.
   a) Dans $(S_3, \circ)$, quel est le sous groupe engendré par le 3-cycle (132) ?
   b) Dans $(\mathbb{Z}, +)$, quel est le sous-groupe engendré par 2 ?
5) On revient au cas général. On dit qu'un élément g de G est **d'ordre fini** s'il existe un entier naturel N non nul tel que $g^N = \mathrm{e}$. Lorsque tel est le cas, on appelle **ordre de** g le plus petit N non nul tel que $g^N = \mathrm{e}$.
   a) Exemple 1 : dans $(S_4, \circ)$, quel est l'ordre du 4-cycle $\sigma = (1234)$?
   b) Exemple 2 : dans $(\mathrm{GL}_2(\mathbb{R}), \times)$, donner un exemple d'élément qui n'est pas d'ordre fini.
   c) Montrer que si G est fini, tout élément g de G est d'ordre fini.
   d) Soit g un élément de G d'ordre N, et soit m un entier. Etablir que $g^m = \mathrm{e}$ si et seulement si N 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.

Soient donc G un groupe fini, et H un sous-groupe de G.

Pour tout élément g de G, on note : $gH = \{g * h \,/\, h \in H\}$.

6) Etablir que pour tout élément g de G, on a : $\text{Card}\,(gH) = \text{Card}\,(H)$.

7) Soient g et g' deux éléments de G. Montrer que les ensembles gH et $g'H$ sont soit égaux, soit disjoints.

8) En déduire que le cardinal de H divise celui de G.

9) Application : établir que l'ordre d'un élément g de G divise le cardinal de G.

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

Un groupe G fini est appelé **cyclique** s'il existe un élément g de G tel que $G = \langle g \rangle$.

10) Le groupe S_3 est-il cyclique ? Le groupe A_3 est-il cyclique ?

11) Etablir que si G est un groupe cyclique, alors G est abélien.

12) Montrer que si G est de cardinal 5, alors G est cyclique (donc 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) Montrer que la relation de conjugaison définie ci-dessus est une relation d'équivalence sur S_n.

14) Un sous-groupe H de S_n est dit **distingué** s'il est stable par conjugaison dans le sens suivant :

$$\forall\, h \in H,\ \forall\, \sigma \in S_n \ \ \sigma h \sigma^{-1} \in H$$

a) Etablir que $\langle (12) \rangle$ n'est pas un sous-groupe distingué de S_3.

b) Montrer que (pour tout entier $n \geqslant 2$) A_n est un sous-groupe distingué de S_n.

➤ **PARTIE F - Simplicité de A_5**.

15) Quel est le cardinal de A_5 ?

16) Montrer que tout élément de A_5 distinct de l'identité est soit un 3-cycle, soit un 5-cycle, soit une composée de deux transpositions à supports disjoints.

17) Intermède : un peu de dénombrement.

a) Combien existe t-il de 5-cycles dans A_5 ?

b) Combien existe t-il de 3-cycles dans A_5 ?

c) Combien existe t-il de produits de deux transpositions à supports disjoints dans A_5 ?

---

*. Ce qui évite la très rébarbative rédaction de toutes les tables de multiplication possibles pour un groupe de cardinal 5. Plus généralement, la méthode utilisée dans ce problème permet d'affirmer que tout groupe dont le cardinal est un nombre premier est abélien.

18) Temporairement, on se replace dans le cas général de S_n, avec $n \geqslant 5$.

  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.
  Montrer qu'il existe une permutation paire σ telle que :
  $$\forall\, i \in [\![1, n-2]\!],\ \sigma(a_i) = b_i$$
  On pourra éventuellement utiliser une composition par une certaine transposition pour obtenir la bonne parité.

  b) Soit $\sigma \in S_n$. On suppose que $\tau_1 = (i_1 \cdots i_k)$ est un k-cycle (avec $k \in [\![2, n]\!]$), et on pose $\tau_2 = \sigma \tau_1 \sigma^{-1}$. Etablir que :
  $$\tau_2 = (\sigma(i_1) \cdots \sigma(i_k))$$

19) Déduire de la question précédente que les 3-cycles sont deux à deux conjugués dans A_5, càd que si c_1 et c_2 sont deux 3-cycles, il existe $\sigma \in A_5$ telle que : $c_2 = \sigma c_1 \sigma^{-1}$.

20) Montrer de même que les composées de deux transpositions à supports disjoints sont conjuguées dans A_5 .

21) Un sous-groupe H de A_5 est dit **distingué** si
$$\forall\, h \in H,\ \forall\, \sigma \in A_5,\ \sigma h \sigma^{-1} \in H$$
Soit H un sous-groupe distingué (donc stable par conjugaison) de A_5.

  a) Montrer que si H contient un 3-cycle, alors il les contient tous. De même, montrer que si H contient un produit de deux transpositions à supports disjoints, alors il contient tous les produits de deux transpositions à supports disjoints.
  On pourra admettre par la suite qu'il en va de même pour les 5-cycles : si H contient un 5-cycle, alors il les contient tous.

  b) Etablir que $H = \{\mathrm{id}\}$ ou $H = A_5$.
  *Commentaire. Cet ultime résultat signifie que le groupe A_5 ne possède pas de sous-groupe distingué non trivial (c'est-à-dire distinct de lui-même et de $\{id\}$) ; un tel groupe est appelé un groupe **simple**. Comme indiqué dans le préambule du problème, c'est cette simplicité qui implique qu'une équation polynomiale de degré 5 n'est pas résoluble par radicaux, càd qu'il n'existe pas (contrairement au cas du second degré) de formule "avec des racines" donnant les solutions d'une équation de degré 5 en général. Ce résultat peut être généralisé (Galois l'a fait) à $n \geqslant 5$; en effet, pour tout entier $n \geqslant 5$, le groupe A_n est également simple.*

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

On rappelle que les fonctions cosinus hyperbolique (ch), sinus hyperbolique (sh) et tangente hyperbolique (th) sont respectivement définies sur $\mathbb{R}$ par :
$$\forall\, x \in \mathbb{R},\ \mathrm{ch}(x) = \frac{\mathrm{e}^x + \mathrm{e}^{-x}}{2}\ ; \qquad \forall\, x \in \mathbb{R},\ \mathrm{sh}(x) = \frac{\mathrm{e}^x - \mathrm{e}^{-x}}{2}\ ; \qquad \forall\, x \in \mathbb{R},\ \mathrm{th}(x) = \frac{\mathrm{sh}(x)}{\mathrm{ch}(x)}$$

➤ Partie A - Etude d'une bijection réciproque.

1) Justifier brièvement que th réalise une bijection de $\mathbb{R}$ vers I, où I est un intervalle à préciser.
Dans la suite de ce problème, on note argth la bijection réciproque de th ; la fonction argth est donc définie sur I et est à valeurs dans $\mathbb{R}$.

2) Etudier l'éventuelle parité de la fonction argth, puis son sens de variation.

3) Justifier que argth est dérivable sur $\mathbb{R}$, et calculer sa dérivée.

4) Pour conclure, exprimer argth à l'aide des fonctions usuelles.
Il s'agit ici de résoudre, pour un réel y quelconque dans I, l'équation $\mathrm{th}(x) = y$.

➤ 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 :

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

5) Déterminer les fonctions constantes solutions du problème posé.

6) Déterminer les valeurs possibles de $f(0)$ si f est solution.

7) Montrer que si f est solution, on a : $\forall x \in \mathbb{R},\ -1 \leqslant f(x) \leqslant 1$ *(exprimer $f(x)$ en fonction de $f(x/2)$).*

8) Montrer que si f est solution, alors $(-f)$ est également solution. Puis vérifier que th est 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 : $\forall n \in \mathbb{N},\ u_n = f\left(\frac{x_0}{2^n}\right)$.

9) Montrer que la suite (u_n) est convergente, et préciser sa limite.

10) Etablir une relation entre u_n et u_{n+1} ; en déduire que la suite (u_n) garde un signe constant, puis étudier sa monotonie suivant le signe de u_0.

11) En utilisant les résultats des questions 9 et 10, aboutir à une contradiction.

12) Que peut-on dire si l'hypothèse "$f(0) = 1$" est remplacée par l'hypothèse "$f(0) = -1$" ?

13) Conclure.

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

14) En raisonnant par l'absurde et en considérant une suite du même type que celle des questions 9 à 13, montrer que : $\forall x \in \mathbb{R},\ f(x) \neq -1$ et $f(x) \neq 1$.

On définit alors une fonction g en posant : $\forall x \in \mathbb{R},\ g(x) = \operatorname{argth}(f(x))$.

15) Montrer que : $\forall x \in \mathbb{R},\ g(2x) = 2g(x)$.

16) Montrer que g est dérivable en 0.

17) Soit $x \in \mathbb{R}^*$. On définit une suite (v_n) en posant : $\forall n \in \mathbb{N},\ v_n = \dfrac{g\left(\frac{x}{2^n}\right)}{\left(\frac{x}{2^n}\right)}$.

Justifier que la suite (v_n) est convergente et préciser sa limite.

18) En déduire que g est linéaire.

19) Déterminer toutes les fonctions solutions du problème posé.