DM n° 14 : Groupes, anneaux

Problème 1 –

- *Un pseudo-anneau A est un ensemble muni de deux lois de composition interne notées $+$ et $\times$, telles que $(A,+)$ soit un groupe abélien, et telle que $\times$ soit associative et distributive sur $+$. En revanche, il n'existe pas nécessairement d'élément neutre pour la loi $\times$.*
- *Un anneau est donc un pseudo-anneau admettant un élément neutre 1_A pour la loi $\times$.*
- *Une partie I de A est appelée* idéal bilatère *de A si I est un sous-groupe additif de $(A,+)$, et si pour tout $x \in I$ et $y \in A$, $xy \in I$ et $yx \in I$.*
- *Le centre $C(A)$ d'un pseudo-anneau A est : $C(A) = \{x \in A \mid \forall y \in A,\ xy = yx\}$.*
- *On dit qu'un pseudo-anneau A est commutatif si la loi $\times$ est commutative, ce qui revient à dire que $C(A) = A$.*

1. Soit A un pseudo-anneau
   (a) Montrer que $C(A)$ est un sous-groupe additif de $(A,+)$.
   (b) Montrer que tout idéal bilatère I de A est un pseudo-anneau.
2. Soit A un pseudo-anneau vérifiant : $\forall x \in A, \quad x^2 - x \in C(A)$.
   (a) En considérant $x+y$, montrer que pour tout $(x,y) \in A^2$, $xy + yx \in C(A)$.
   (b) En déduire que A est commutatif.

Dans la suite, A désigne un anneau *tel que pour tout $x \in A$, $x^3 = x$. On veut prouver que A est commutatif.*

3. Prouver l'égalité $6 = 0$, où 6 désigne $6 \cdot 1_A$.
4. On note $2A = \{2 \cdot a \mid a \in A\}$ et $3A = \{3 \cdot a \mid a \in A\}$. Prouver les assertions suivantes :
   (a) $3A \cap 2A = \{0\}$
   (b) $3A$ et $2A$ sont des idéaux bilatères de A
   (c) Tout élément de A s'écrit de façon unique comme somme d'un élément de $3A$ et d'un élément de $2A$.
   (d) $\forall x \in 3A, \ \forall y \in 2A, \ xy = yx = 0$.
5. (a) Prouver que pour tout $x \in 3A$, $2x = 0$ et $x^2 = x$.
   (b) En déduire que pour tout $(x,y) \in (3A)^2$, $xy = yx$
6. Soit x et y dans $2A$. En développant $(x+y)^3$ et $(x-y)^3$, montrer que $xy = yx$.
7. Montrer que A est commutatif.

Problème 2 – Simplicité de $\mathfrak{A}_n$

Le but du problème est de prouver la simplicité de $\mathfrak{A}_n$ lorsque $n \geqslant 5$, ce qui signifie que $\mathfrak{A}_n$ n'a pas d'autre sous-groupe distingué que $\{\mathrm{id}\}$ et lui-même. Ce résultat est à la base de la preuve de Galois de la non-résolubilité des équations de degré $n \geqslant 5$ par radicaux. Soit $n \geqslant 5$.

Préliminaire

1. Montrer que le produit de deux transpositions (non nécessairement à supports disjoints) de $\mathfrak{S}_n$ est soit un 3-cycle, soit la composée de deux 3-cycles.
2. En déduire que les 3-cycles engendrent $\mathfrak{A}_n$, c'est-à-dire que tout élément de $\mathfrak{A}_n$ s'écrit comme produit de 3-cycles.

Partie I – Conjugaison

On dit que deux permutations τ_1 et τ_2 de $\mathfrak{S}_n$ sont conjuguées s'il existe $\sigma \in \mathfrak{S}_n$ tel que $\tau_2 = \sigma \circ \tau_1 \circ \sigma^{-1}$.

1. Montrer que la relation de conjugaison est une relation d'équivalence.
2. Soit, avec les notations précédentes, $\tau_1 = (i_1\ i_2\ \cdots\ i_k)$ un cycle, et τ_2 conjugué (par s) à τ_1. Montrer que τ_2 est égal au cycle :
$$\tau_2 = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k)).$$
3. Montrer que deux permutations sont conjuguées dans $\mathfrak{S}_n$ si et seulement si elles ont même type cyclique.

Partie II – Simplicité de $\mathfrak{A}_5$

1. Soit $a_1, \dots, a_{n-2}$ des éléments 2 à 2 distincts de $[\![1, n]\!]$, et a_{n-1}, a_n les deux éléments de $[\![1, n]\!]$ n'étant pas dans cette liste. On se donne de même $b_1, \dots, b_{n-2}$ des éléments distincts de $[\![1, n]\!]$, complétés par les 2 éléments manquant b_{n-1} et b_n. Montrer qu'il existe une permutation paire σ telle que
$$\forall i \in [\![1, n-2]\!], \quad \sigma(a_i) = b_i.$$
On pourra éventuellement utiliser une composition par une certaine transposition pour obtenir la bonne parité.
2. En déduire que les 3-cycles (a_1, a_2, a_3) sont conjugués dans $\mathfrak{A}_5$, c'est-à-dire que si c_1 et c_2 sont deux 3-cycles, il existe $\sigma \in \mathfrak{A}_5$ tel que $c_2 = \sigma c_2 \sigma^{-1}$.
3. Montrer de même que les composées de deux transpositions à supports disjoints sont conjuguées dans $\mathfrak{A}_5$.
4. Soit $c_0 = (1\ 2\ 3\ 4\ 5)$, et $c = (a_1\ a_2\ a_3\ a_4\ a_5)$ un 5-cycle, et $\sigma \in \mathfrak{S}_5$ définie par $\sigma(k) = a_k$. Expliciter un élément τ de $\mathfrak{S}_5$ tel que $c^2 = (\sigma \circ \tau) \circ c_0 \circ (\sigma \circ \tau)^{-1}$.
5. En déduire que pour tout 5-cycle c, soit c, soit c^2 est conjugué dans $\mathfrak{A}_5$ au cycle c_0.
6. Soit H un sous-groupe distingué de $\mathfrak{A}_5$ (donc stable par conjugaison). Montrer que si H contient un 3-cycle, il les contient tous, et de même pour les produits de 2 transpositions à supports disjoints, ainsi que pour les 5-cycles.
7. En comptant le nombre de 3-cycles, le nombre de 5-cycles et le nombre de produits de 2 transpositions à supports disjoints, en déduire que $H = \{\mathrm{id}\}$ ou $H = \mathfrak{A}_5$. Conclure.

Partie III – Simplicité de $\mathfrak{A}_n$, $n > 5$

Soit $n > 5$, et soit H un sous-groupe distingué de $\mathfrak{A}_n$, différent de $\{\mathrm{id}\}$. Soit $\sigma \neq \mathrm{id}$ dans H

1. Soit a tel que $\sigma(a) \neq a$. On pose $b = \sigma(a)$, et on considère c différent de a, b et $\sigma(b)$. Soit τ le 3-cycle $(a\ b\ c)$. Quel est le type cyclique de $\sigma\tau^{-1}\sigma^{-1}$? Montrer que $\tau\sigma\tau^{-1}\sigma^{-1}$ admet au moins $n-5$ points fixes.
2. Soit F un sous-ensemble de $[\![1, n]\!]$ de cardinal 5, contenant l'ensemble des points non fixes de $\tau\sigma\tau^{-1}\sigma^{-1}$. Soit $\mathfrak{A}(F)$ l'ensemble des permutations de $\mathfrak{A}_n$ laissant tous les points extérieurs à F fixes. Montrer que $\mathfrak{A}(F)$ est isomorphe, en tant que groupe, à $\mathfrak{A}_5$, et en déduire que $\mathfrak{A}(F)$ est simple.
3. Montrer que $H \cap \mathfrak{A}(F)$ est distingué dans $\mathfrak{A}(F)$, et en déduire que H contient au moins un 3-cycle.
4. En déduire que $\mathfrak{A}_n$ est simple.