Algèbre – Interrogation I

*Vous disposez de **45 minutes** pour résoudre les quatre exercices suivants qui sont tous indépendants. Vous pouvez admettre le résultat d'une question pour résoudre une question ultérieure même sans l'avoir traitée. Vous pouvez utiliser librement tous les résultats du cours. Ce qui a été vu uniquement en TD est à redémontrer. En cas de questions ou si vous repérez ce qui vous semble être une erreur d'énoncé, n'hésitez pas à me solliciter. On prendra soin de rédiger de façon propre et rigoureuse.*

Exercice 1. Énoncer et démontrer le théorème de factorisation pour un morphisme de groupes finis $f : G \to G'$. Rappeler le lien entre $|\mathrm{Ker}(f)|$ et celui de $|\mathrm{Im}(f)|$.

Exercice 2. Soient p un nombre premier et n un entier naturel tels que $p > n$. On considère G un groupe d'ordre pn et H un sous-groupe de G d'ordre p.

1. Justifier que H est un p-Sylow de G.
2. Démontrer que H est un sous-groupe distingué de G.

Exercice 3.

1. Soient n un entier naturel plus grand que 2 et $\varphi : \mathfrak{S}_n \longrightarrow \{\pm 1\}$ un morphisme de groupes. Montrer que toutes les transpositions ont la même image et décrire tous les morphismes φ possibles.
2. Rappeler ce que vaut $Z(\mathfrak{S}_3)$ et donner une partie génératrice de $\mathfrak{S}_3$. Montrer que

$$f : \left\{ \begin{array}{ccc} \mathfrak{S}_3 & \longrightarrow & \mathtt{Aut}(\mathfrak{S}_3) \\ \sigma & \longmapsto & [\mu \mapsto \sigma\mu\sigma^{-1}] \end{array} \right.$$

   est un isomorphisme de groupes.
3. Décrire toutes les actions de groupes de $\mathbb{Z}/7\mathbb{Z}$ sur $\mathfrak{S}_3$ par automorphismes.
   On rappelle que si G et X sont deux groupes et que G agit sur X, on dit que G agit sur X *par automorphismes* si pour tout $g \in G$, $x \mapsto g \cdot x$ est un automorphisme de X.
4. Soient n un entier naturel supérieur ou égal à 2 et $n_1, \ldots, n_k$ des entiers naturels non nuls tels que $n = n_1 + n_2 + \cdots + n_k$. En utilisant le théorème de Lagrange pour un sous-groupe bien choisi, montrer que

$$\prod_{i=1}^{k} (n_i)! \,\Big|\, n!.$$

Exercice 4.

1. Soient p un nombre premier, G un p-groupe et X un ensemble fini sur lequel G agit. On note

$$X^G := \{x \in X \,:\, \forall g \in G,\, g \cdot x = x\}.$$

   Montrer que $\left|X^G\right| \equiv |X| \pmod p$.
2. Que pouvez-vous en déduire si $|X|$ n'est pas divisible par p ?

La suite de l'exercice est un **bonus** à traiter *uniquement* si vous avez terminé le reste ! On considère p un nombre premier congru à 1 modulo 4 et on souhaite montrer que p est somme de deux carrés. On note

$$X = \left\{(x, y, z) \in \mathbb{N}^3 \,:\, x^2 + 4yz = p\right\}.$$

On pose alors $i : X \longrightarrow X$ définie par

$$(x, y, z) \longmapsto \left\{ \begin{array}{l} (x + 2z, z, y - x - z) \text{ si } x < y - z \\ (2y - x, y, x - y + z) \text{ si } y - z < x < 2y \\ (x - 2y, x - y + z, y) \text{ si } x > 2y. \end{array} \right.$$

3. Vérifier que i est bien définie et est une involution, c'est-à-dire que $i \circ i = \mathrm{Id}_X$. En déduire une action de $\mathbb{Z}/2\mathbb{Z}$ sur X.
4. Montrer que i a un unique point fixe.
5. Établir que $|X|$ est impair.
6. Montrer que l'application $j : X \longrightarrow X$ définie par $j(x, y, z) = (x, z, y)$ est une involution et en déduire qu'elle admet un point fixe. Conclure !