Université Paul Sabatier **Toulouse**
L2 Mathématiques: groupes et géométrie **8 mars 2012**

Examen partiel

Ce sujet comporte un exercice et un problème. Les documents et appareils électroniques de toutes sortes ne sont pas acceptés. Une attention toute particulière sera accordée à la qualité de la rédaction, et toute affirmation devra être argumentée.

Exercice

Soit G un groupe ; on désigne par e son élément neutre. Pour $a \in G$, on note

$$ord(a) = \inf\{n \in \mathbb{N}^* \mid a^n = e\}$$

l'ordre de a.

1. Montrer que, pour tout élément a de G, on a
$$ord(a) = ord(a^{-1}) .$$
2. Montrer que pour tous a et b dans G, on a
$$ord(ab) = ord(ba) .$$
3. Montrer que pour tous $a, b, c \in G$, on a
$$ord(abc) = ord(bca) .$$
4. On suppose à présent que $G = S_3$ est le groupe des permutations sur l'ensemble à trois éléments. Trouver trois éléments $a, b, c \in S_3$ tels que
$$ord(abc) \neq ord(bac) .$$
5. Soit $a \in G$ un élément d'ordre fini. Montrer que l'application
$$\begin{aligned} \varphi : \mathbb{Z} &\to G \\ k &\mapsto a^k \end{aligned}$$
est un morphisme de groupes. Décrire l'image de φ ainsi que $\ker(\varphi)$. En déduire que φ induit un isomorphisme de groupes
$$\mathbb{Z}/m\mathbb{Z} \simeq \langle a \rangle$$
où $m = ord(a)$.

Problème

Les parties I, II et III sont indépendantes les unes des autres. Cependant, la partie IV utilise les résultats de celles qui la précèdent.

Partie I

Pour un ensemble fini E, on notera $|E|$ le nombre d'éléments de E. Soit G un groupe fini tel que, pour tout $x \in G$, on ait
$$x^2 = e .$$

a) Montrer que G est commutatif.
b) Soit $x \in G \setminus \{e\}$. On note $H = \langle x \rangle$ le sous-groupe de G engendré par x. Expliquer pourquoi le quotient G/H est naturellement muni d'une structure de groupe. Calculer $|G|$ en fonction de $|G/H|$. En déduire que l'existence d'un élément $x \neq e$ implique que $|G|$ est un nombre pair. Montrer que, pour tout $y \in G/H$, on a $y^2 = e$.

c) Soit m le plus grand entier positif ou nul tel que 2^m divise $|G|$. Montrer par récurrence sur l'entier m que $|G| = 2^m$.

Partie II

a) Soit $n \geqslant 2$ un entier. Montrer qu'une permutation $\sigma \in S_n$ est un cycle de longueur n si et seulement si σ est un élément d'ordre n.
b) Soit E un ensemble fini de cardinal n. On se donne une bijection

$$\alpha : E \to E$$

telle que $\alpha^n = id_E$ et telle que $\alpha^i \neq id_E$ pour $0 < i < n$. Montrer que, pour tout couple $(x, y) \in E^2$, il existe un entier $k \geqslant 1$ tel que $\alpha^k(x) = y$.

Partie III

a) Soit n un entier positif ou nul, et soit E un ensemble de cardinal $2n + 1$. On suppose donnée bijection $\sigma : E \to E$ telle que $\sigma \circ \sigma = id_E$. Montrer que, pour tout $x \in E$ tel que $\sigma(x) \neq x$, si on pose $F = E \setminus \{x, \sigma(x)\}$, l'application

$$\begin{aligned} F &\to F \\ y &\mapsto \sigma(y) \end{aligned}$$

est bien définie et bijective. En déduire, par un raisonnement par récurrence sur n, qu'il existe $x \in E$ tel que $\sigma(x) = x$.
b) Soit G un groupe fini non trivial d'ordre pair. Déduire de la question précédente qu'il existe un élément $x \in G \setminus \{e\}$ tel que $x^2 = e$.

Partie IV

Soit p un nombre premier impair. On considère un groupe fini G d'ordre $p + 1$. On suppose donné un automorphisme

$$\alpha : G \to G$$

tel que $\alpha^p = id_G$ et $\alpha \neq id_G$.
a) Montrer que $\alpha^i \neq id_G$ pour $0 < i < p$.
b) On pose $E = G \setminus \{e\}$. Montrer que l'application

$$\begin{aligned} E &\to E \\ x &\mapsto \alpha(x) \end{aligned}$$

est bijective.
c) En déduire que $p = 2^m - 1$ pour un certain nombre entier positif m.

Remarque heuristique : les nombres de Mersenne sont précisément les nombres premiers p de la forme $p = 2^m - 1$ (par exemple $p = 3$, $p = 7$, $p = 31$, $p = 127$). Il est possible de prouver une réciproque au résultat obtenu dans la partie IV : pour tout nombre de Mersenne p, il existe un groupe fini G d'ordre $p + 1$ muni d'un automorphisme $\alpha : G \to G$ d'ordre p. La question de savoir s'il y a une infinité de nombres de Mersenne est un problème encore ouvert.