Université Claude Bernard - Lyon 1 Semestre d'automne 2011-2012
Math III - PMI

Feuille d'exercices n° 8
GROUPES

---

1 Sous-groupes. Théorème de Lagrange

Exercice 1. Montrer que les matrices $\pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \pm\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, où i est le nombre complexe tel que $i^2 = -1$, forment un groupe pour la multiplication des matrices. (On montrera que c'est un sous-groupe du groupe $GL_2(\mathbb{C})$. On remarquera que démontrer directement que cet ensemble de matrices est un groupe impose des calculs long et fastidieux, en particulier pour vérifier l'associativité, d'où l'intéret de la méthode proposée, qui est fréquemment utilisée). On note ce groupe $\mathcal{H}$ et on l'appelle *groupe quaternionique*.

Rappels. Soit G un groupe et e son élément neutre. Une loi de groupe est en général notée multiplicativement. La notation additive est réservée aux groupes abéliens.
L'ordre du groupe G est son nombre d'éléments (cardinal) si ce groupe est fini, et l'infini sinon.
L'ordre (ou la période) d'un élément $a \in G$ est le plus petit nombre entier positif m tel que $a^m = e$ (où a^m désigne le produit de m éléments égaux à a, dans le cas des groupes abéliens l'équation $a^m = e$ est remplacée par $ma = 0$.) Si aucun m de la sorte n'existe, a est dit d'ordre infini.
Si m est l'ordre de a, un *sous-groupe engendré par a* est le sous-groupe de cardinal m, ses éléments sont $\{a, a^2, \cdots, a^{m-1}, a^m = e\}$. L'ordre d'un élément a d'un groupe fini peut se définir comme le cardinal du sous-groupe qu'il engendre. Par le théorème de Lagrange, cet ordre divise l'ordre du groupe :
Théorème de Lagrange - pour un groupe G fini, et pour tout sous-groupe H de G, le cardinal de H divise le cardinal de G.
Un groupe G d'ordre premier p est cyclique et simple (=pas de sous-groupes). En effet, tout élément non neutre x de G est d'ordre strictement supérieur à 1 et par ce qui précède un diviseur de p. Comme p est premier, l'ordre de x est p ; autrement dit, x engendre un groupe cyclique d'ordre p, nécessairement égal à G.
Ce théorème peut servir à démontrer le petit théorème de Fermat et sa généralisation, le théorème d'Euler.

Exercice 2.

1. Quel est l'ordre du groupe multiplicatif $(\mathbb{Z}/13\mathbb{Z})^\times$?
2. Quels sont les éléments α du groupe $\mathbb{Z}/13\mathbb{Z}$ tels que : $\alpha^2 = 1,\ \alpha^3 = 1,\ \alpha^4 = 1,\ \alpha^5 = 1$.
3. Soit $(\mathbb{Z}/15\mathbb{Z})^\times$ le groupe multiplicatif des éléments inversibles de $\mathbb{Z}/15\mathbb{Z}$. Quels sont les éléments de $(\mathbb{Z}/15\mathbb{Z})^\times$? Quels sont les ordres des éléments de $(\mathbb{Z}/15\mathbb{Z})^\times$?

Exercice 3. Calculer la valeur $\varphi(m)$ de l'indicatrice d'Euler pour : a) $m = 27$, b) $m = 13$, c) $m = p^k$ (p premier), d) $m = 12$, e) $m = m_1 \times m_2$ tel que $\mathrm{PGCD}(m_1, m_2) = 1$, f) $m = 60$.

Exercice 4.

1. Montrer que si a est premier avec n, alors : $a^{\varphi(n)} \equiv 1 \pmod{n}$. Que devient cette relation si n est un nombre premier ? En déduire que pour tout entier a et tout nombre premier p, on a : $a^p \equiv a \pmod{p}$.
2. Soient $a, n \geq 1$ deux entier tels que : $a^{n-1} \equiv 1 \pmod{n}$ et $a^l \not\equiv 1 \pmod{n}$ pour tout l diviseur strict de $n-1$. Montrer que n est premier.

Exercice 5. Enoncer l'analogue du petit théorème de Fermat (appelé le théorème d'Euler) pour $n = 12$.

Exercice 6. Calculer le dernier chiffre de 7^{25}. Même question avec $7^{100!}$.

Exercice 7. Trouver tous les éléments du groupe engendré par la matrice : $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$. Quel est l'ordre de ce groupe ?

Exercice 8. Soit E un ensemble. On note S_E le groupe des applications bijectives de E dans E (ou permutations de E) pour la loi de composition interne définie par la composition des applications. Si $E = \{1, 2, 3\}$ les éléments sont

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Ce groupe est noté S_3 - le groupe de permutations de 3 éléments, aussi appelé le groupe symétrique. Dresser la table de ce groupe. Pour chaque élément preciser son ordre. Ecrire une partie génératrice de S_3 à deux éléments.

2 Morphismes de groupes

Exercice 9. Le but de cet exercice est de démontrer que le groupe multiplicatif des éléments inversibles de $\mathbb{Z}/5\mathbb{Z}$, noté $\mathbb{F}_5^*$, est isomorphe au groupe additif $\mathbb{Z}/4\mathbb{Z}$.

1. Dresser la table d'addition de $\mathbb{Z}/4\mathbb{Z}$ et la table de multiplication de $\mathbb{F}_5^*$. Préciser le neutre et les ordres des éléments de chaque groupe.
2. Construire un isomorphisme entre $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{F}_5^*$.

Exercice 10. Montrer qu'un isomorphisme de groupes préserve l'ordre.
En déduire que les groupes $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes.

Exercice 11.

1. Soit $\phi : G \to H$ un morphisme de groupes. Montrer que
   (a) $\phi(1_G) = \phi(1_H)$ où $1_G, 1_H$ sont des éléments neutres respectifs de G et H.
   (b) $\phi(x^{-1}) = \phi(x)^{-1}$ pour tout $x \in G$.
2. On considère le groupe additive $\mathbb{Z}$. Définir la loi du groupe additive sur le produit $\mathbb{Z} \times \mathbb{Z}$. Montrer que $\mathbb{Z}$ et $\mathbb{Z} \times \mathbb{Z}$ sont deux groupes non isomorphes.