2M220 – Arithmétique, 2014-2015 François Lê
Université Pierre et Marie Curie francois.le@imj-prg.fr

TD n° 3 – Groupes

Exercice 1
Munis des lois proposées, lesquels des ensembles suivants sont des groupes ?

$(\mathbf{N},+)$; $(\mathbf{Z},+)$; $(\mathbf{Z},\times)$; $(\mathbf{Z}\setminus\{0\},\times)$; $(\mathbf{R},\times)$; $(\mathbf{R}\setminus\{0\},\times)$; $(\mathscr{M}_n(\mathbf{R}),\times)$

Exercice 2
Soit $(G,*)$ un groupe.

1. Rappeler la définition d'un sous-groupe de G.
2. Soient H, H' deux sous-groupes de G. Montrer que $H\cap H'$ est un sous-groupe de G.
3. De façon générale, la réunion de deux sous-groupes de G est-elle un sous-groupe de G ? *Indication : regarder $G=(\mathbf{Z},+)$, $H=2\mathbf{Z}$ et $H'=3\mathbf{Z}$.*

Exercice 3

1. Soit $S=\{z\in\mathbf{C},\ |z|=1\}$. Montrer que S est un sous-groupe de $\mathbf{C}^*$.
2. Soit n un entier $\geqslant 1$ et soit $\mathbf{U}_n=\{z\in\mathbf{C}\mid z^n=1\}$. Montrer que $\mathbf{U}_n$ est un sous-groupe de S.

Exercice 4
Soit $(G,+)$ un groupe commutatif et soient A,B deux sous-groupes de G.

1. Montrer que l'ensemble $C=\{a+b\mid(a,b)\in A\times B\}$ est un sous-groupe de G.
2. Montrer que $A\subset C$ et que $B\subset C$.
3. Soit D un sous-groupe de G tel que $A\subset D$ et $B\subset D$. Montrer que $C\subset D$. *Le sous-groupe C s'appelle le sous-groupe engendré par A et B. On le note $A+B$.*
4. Soient $a,b\in\mathbf{Z}$. Montrer que $a\mathbf{Z}+b\mathbf{Z}=(a\wedge b)\mathbf{Z}$.

Exercice 5

1. Écrire la table d'addition des groupes $(\mathbf{Z}/5\mathbf{Z},+)$ et $(\mathbf{Z}/6\mathbf{Z},+)$.
2. Montrer que $\{\overline{0},\overline{3},\overline{6},\overline{9}\}$ est un sous-groupe de $\mathbf{Z}/12\mathbf{Z}$..

Exercice 6

1. Soit $n\in\mathbf{N}^*$. Montrer que tout élément de $\mathbf{Z}/n\mathbf{Z}$ est peut être écrit comme une somme itérée de $\overline{1}$.
2. Avec $n=7$, montrer que le même énoncé est encore vrai en remplaçant $\overline{1}$ par $\overline{2}$.
3. Dans le cas $n=14$, montrer que $\overline{1}$ ne peut pas être écrit comme une somme itérée de $\overline{2}$.
4. Toujours avec $n=14$, calculer les ordres respectifs de $\overline{2}$, $\overline{3}$, $\overline{7}$.

François Lê
francois.le@imj-prg.fr

Exercice 7

1. Rappeler la formule (du cours) donnant l'ordre de $\overline{k}$ dans $(\mathbf{Z}/n\mathbf{Z}, +)$.
2. Calculer le nombre d'éléments d'ordre 28 dans $\mathbf{Z}/28\mathbf{Z}$.

Exercice 8

Parmi les applications suivantes, lesquelles sont des morphismes de groupes ?

$$\begin{array}{ccc} \mathbf{R}_+^* & \to & \mathbf{R} \\ x & \mapsto & \ln x \end{array} \; ; \quad \begin{array}{ccc} \mathbf{C}^* & \to & \mathbf{R}_+^* \\ z & \mapsto & |z| \end{array} \; ; \quad \begin{array}{ccc} \mathbf{Z} & \to & \mathbf{Z} \\ n & \mapsto & 2n \end{array} \; ; \quad \begin{array}{ccc} \mathbf{Z} & \to & \mathbf{Z} \\ n & \mapsto & n+1 \end{array} \; ;$$

$$\begin{array}{ccc} \mathscr{M}_n(\mathbf{R}) & \to & \mathbf{R} \\ M & \mapsto & \mathrm{tr} A \end{array} \; ; \quad \begin{array}{ccc} \mathrm{GL}_n(\mathbf{R}) & \to & \mathbf{R}^* \\ M & \mapsto & \det A \end{array}$$

Exercice 9

Soit $\mathbf{U}_n = \{z \in \mathbf{C} \mid z^n = 1\}$. Le but de l'exercice est de montrer que $\mathbf{U}_n$ est isomorphe à $\mathbf{Z}/n\mathbf{Z}$.

1. On note $\omega = e^{2i\pi/n}$. Montrer que l'application φ définie par

$$\varphi : \begin{array}{ccc} \mathbf{Z}/n\mathbf{Z} & \to & \mathbf{U}_n \\ \overline{k} & \mapsto & \omega^k \end{array}$$

   est bien définie, c'est-à-dire qu'elle est bien à valeurs dans $\mathbf{U}_n$ et la valeur de $\varphi(\overline{k})$ ne dépend pas du choix du représentant de la classe $\overline{k}$.
2. Montrer que φ est surjective.
3. Montrer que φ est injective.

Exercice 10

S'inspirer de l'exercice précédent pour montrer que :

1. $\mathbf{R}/\mathbf{Z}$ est isomorphe à $S = \{z \in \mathbf{C},\ |z| = 1\}$.
2. Si un groupe G de cardinal n possède un élément d'ordre n, alors G est isomorphe à $\mathbf{Z}/n\mathbf{Z}$.

Exercice 11

Soit $(G, \cdot)$ un groupe dont le cardinal est un nombre premier p. En utilisant le théorème de Lagrange, montrer que G est isomorphe à $\mathbf{Z}/p\mathbf{Z}$.