UJF, L3 mathématiques — Septembre 2015

Mat35b Algèbre A, groupe 2

Feuille d'exercices n°2

1. a) Justifier que la table de la loi de multiplication dans un groupe fini est un carré latin, i.e. un tableau carré dans lequel chaque élément apparaît une et une seule fois dans chaque ligne et chaque colonne.

b) Donner la liste de toutes les tables de multiplication possibles pour les groupes d'ordre 2 ou 3, et en déduire qu'un tel groupe est commutatif.

c)* Montrer que dans un groupe d'ordre pair, il existe un nombre pair, non nul, d'éléments égaux à leur inverse.

d) Reprendre la question b) pour les groupes d'ordre 4. Donner des exemples de groupes pour chaque table possible.

2. Si E est un ensemble, on note $S(E)$ l'ensemble des bijections de E sur lui-même. Si $E = \{1, \ldots, n\}$, on le note S_n (ou $\mathfrak{S}_n$). Lister les éléments de S_3, et écrire la table de la loi de groupe. Ce groupe est-il commutatif ?

3. Dans le plan euclidien, on considère le carré de sommets $A = (-1, 1), B = (-1, -1), C = (1, -1), D = (1, 1)$.

a) Montrer que l'ensemble des isométries vectorielles qui préservent globalement le carré $ABCD$ est un groupe à 8 éléments. On le note D_4.

b) Écrire les matrices représentatives des éléments de D_4 dans la base canonique $(\vec{i}, \vec{j})$ de $\mathbb{R}^2$, (puis dans la base $((\vec{i}+\vec{j})/\sqrt{2}, (\vec{i}-\vec{j})/\sqrt{2})$).

c) Décrire les éléments de D_4 comme des permutations de l'ensemble $\mathcal{S} = \{A, B, C, D\}$.

On obtient ainsi trois réalisations concrètes du même groupe.

d) Reprendre ces questions en remplaçant le carré par un triangle équilatéral centré en l'origine; puis par un polygone régulier à n côtés ($n \geq 3$) centré en l'origine et dont un sommet est $(1, 0)$.

4. Soit $n \geq 1$ un entier. On rappelle que $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes d'équivalence de $\mathbb{Z}$ pour la relation de congruence modulo n. C'est un ensemble à n éléments, et chaque classe est représentée par un unique entier compris entre 0 et $n-1$. On rappelle que les lois binaires $\overline{x} + \overline{y} = \overline{x+y}$ et $\overline{x} \cdot \overline{y} = \overline{xy}$ sur $\mathbb{Z}/n\mathbb{Z}$ sont bien définies (pourquoi?)

a) Soit $x \in \mathbb{Z}$. Que signifie $\overline{x} = \overline{0}$?

b) Étudier les propriétés des deux lois $+$ et $\cdot$: associativité, commutativité, distributivité de l'une par rapport à l'autre, existence d'un élément neutre, d'un inverse ...

c) L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est-il un groupe pour la loi $+$? pour la loi $\cdot$?

d) On suppose que $n = 17$.

i) En calculant dans $\mathbb{Z}/17\mathbb{Z}$, calculer le reste de la division euclidienne de $16 \times 15 \times 14$ par 17.

ii) Calculer $\overline{2}^m$ pour $m = 1, \dots, 8$. Déterminer le reste de la division euclidienne de 2^{2014} par 17.

e) Vrai ou faux: si $\overline{x} \cdot \overline{y} = \overline{0}$ dans $\mathbb{Z}/n\mathbb{Z}$, on a $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$.

f) Soit $m \in \mathbb{Z}$. Trouver une condition nécessaire et suffisante sur m pour que $\overline{m}$ soit inversible pour la multiplication.

g)* On note $(\mathbb{Z}/n\mathbb{Z})^\times$ l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ inversibles pour la multiplication. Montrer que $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ est un groupe.

5. Soit I un intervalle de $\mathbb{R}$ et $f : I \to \mathbb{R}$ une bijection. On définit une loi $*$ sur I par

$$x * y = f^{-1}(f(x) + f(y)) \quad \text{pour tous } x, y \in I.$$

a)* Montrer que $(I, *)$ est un groupe commutatif. Expliciter le neutre, et l'inverse de $x \in I$ pour la loi $*$. Que dire de l'application f?

b) Donner la loi $*$ dans les cas suivants :

i)* $I =]0, +\infty[, f(x) = \ln(x)$;

ii) $I = \mathbb{R}, f(x) = 1 + x$;

iii) $I =]-1, 1[, f(x) = \ln(\frac{1+x}{1-x})$.

6. Soient $(G, \cdot)$ un groupe, H un ensemble et $f\colon G \to H$ une bijection.

a) Montrer qu'il existe une unique loi interne $*$ sur H telle que $(H, *)$ soit un groupe et f soit un isomorphisme de groupes.

b) Vérifier que $f\colon \mathbb{R}^{+*} \to]0, 1[$ définie par $x \mapsto \frac{1}{1+x}$ est une bijection. Déterminer la loi sur $]0, 1[$ induite par f et le groupe $(\mathbb{R}^{+*}, \cdot)$.

7. Les applications suivantes sont-elles des morphismes de groupes ?

$f\colon x \mapsto 2x$ de $\mathbb{R}$ dans $\mathbb{R}$, resp. de $\mathbb{R}^\times$ dans $\mathbb{R}^\times$, $f\colon x \mapsto x^2$ de $\mathbb{C}^\times$ dans $\mathbb{C}^\times$, resp. de G dans G ($(G, \cdot)$ un groupe); $f\colon \mathbb{R} \to \mathrm{GL}_2(\mathbb{R})$ définie par $t \mapsto \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$.

8. Soient G et G' deux groupes. On suppose que G' est abélien.

a) Montrer que l'ensemble $\mathrm{Hom}(G, G')$ des morphismes de groupes $G \to G'$ est un groupe pour la loi $\cdot$

$$(f_1 \cdot f_2)(g) = f_1(g) \cdot f_2(g), \quad \text{pour tout } g \in G.$$

b) Soit $g \in G$. On rappelle que l'application $\varphi_g\colon \mathbb{Z} \to G$ définie par $m \mapsto g^m$ est un morphisme de groupes. Montrer que l'application $\varphi\colon G \to \mathrm{Hom}(\mathbb{Z}, G)$ définie par $g \mapsto \varphi_g$ est une bijection, i.e. que tout morphisme de groupes $\mathbb{Z} \to G$ est de la forme φ_g pour un unique $g \in G$.

d) Si G est abélien, montrer que φ est un isomorphisme de groupes.