TD 5 – Groupes, morphismes de groupes

Énoncés

Exercice 1 – Vrai ou faux : $(\mathbf{N}, +)$ (resp. $(\mathbf{Z}, +)$, resp. $(\mathbf{Z}, \cdot)$, resp. $(\mathbf{Z} \smallsetminus \{0\}, \cdot)$, resp. $(\mathbf{R} \smallsetminus \{0\}, \cdot)$) est un groupe.

Exercice 2 – Montrer que $2\mathbf{Z}$ est un sous-groupe de $\mathbf{Z} = (\mathbf{Z}, +)$ et que l'application $f : \mathbf{Z} \longrightarrow 2\mathbf{Z}$, $f(x) = 2x$ est un isomorphisme de groupes.

Exercice 3 – Montrer que $H = \{(a, b) \in \mathbf{Z}^2 \mid a \equiv b \pmod 2\}$ est un sous-groupe de $\mathbf{Z}^2 = (\mathbf{Z}^2, +)$ et que l'application $f : \mathbf{Z}^2 \longrightarrow H$, $f(u, v) = u(2, 0) + v(1, 1) = (2u + v, v)$ est un isomorphisme de groupes.

Exercice 4 – Soit $(G, *)$ un groupe. Décrire tous les morphismes de groupes $\mathbf{Z} \longrightarrow (G, *)$ (resp. $\mathbf{Z}^2 \longrightarrow (G, *)$).

Exercice 5 – Montrer : une application $f : \mathbf{Z} \longrightarrow \mathbf{Z}$ est un morphisme de groupes si et seulement si il existe $a \in \mathbf{Z}$ tel que $f(x) = ax$, pour tout $x \in \mathbf{Z}$. Déterminer le noyau et l'image de f. Quand est-ce que f est un isomorphisme de groupes ?

Exercice 6 – Montrer : une application $f : \mathbf{Z}^2 \longrightarrow \mathbf{Z}^2$ est un morphisme de groupes si et seulement si il existe $a, b, c, d \in \mathbf{Z}$ tels que $f(x, y) = (ax + by, cx + dy)$, pour tout $(x, y) \in \mathbf{Z}^2$. Déterminer le noyau de f. Quand est-ce que f est un isomorphisme de groupes ?

Exercice 7 – Les groupes suivants, sont-ils isomorphes ? Pourquoi ?

1. $(\mathbf{R}, +)$ et $(\mathbf{R}_{>0}, \cdot)$;
2. $(\mathbf{Z}/4\mathbf{Z}, +)$ et $(\mathbf{Z}/2\mathbf{Z}, +) \times (\mathbf{Z}/2\mathbf{Z}, +)$;
3. $(\mathbf{Z}/6\mathbf{Z}, +)$ et $(\mathbf{Z}/2\mathbf{Z}, +) \times (\mathbf{Z}/3\mathbf{Z}, +)$;
4. $(\mathbf{Z}/mn\mathbf{Z}, +)$ et $(\mathbf{Z}/m\mathbf{Z}, +) \times (\mathbf{Z}/n\mathbf{Z}, +) \quad (m, n \geq 1)$;
5. $(\mathbf{Z}/4\mathbf{Z}, +)$ et $(\mathbf{Z}/5\mathbf{Z} \smallsetminus \{0\}, \cdot)$;
6. $(\mathbf{R} \smallsetminus \{0\}, \cdot)$ et $(\mathbf{C} \smallsetminus \{0\}, \cdot)$;
7. $(\mathbf{R}, +)$ et $(\mathbf{C}, +)$.

Exercice 8 – (Automorphismes intérieurs) Soit G un groupe. Montrer que, pour tout $g \in G$, l'application $f : G \longrightarrow G$, $f(h) = ghg^{-1}$ est un automorphisme de G. Déterminer son inverse $f^{-1} : G \longrightarrow G$.

Exercice 9 – Soit G un groupe tel que $g^2 = e$ pour tout $g \in G$ (ici, e désigne l'élément neutre de G). Montrer que G est abélien.

Exercice 10 – Soit G un groupe. Montrer que l'application $g \mapsto g^{-1}$ est un morphisme de groupes $G \longrightarrow G$ si et seulement si G est abélien.

Exercice 11 – L'application $f_1 : (\mathbf{C} \smallsetminus \{0\}, \cdot) \longrightarrow (\mathbf{R} \smallsetminus \{0\}, \cdot)$, $f_1(z) = |z|$, est-elle un morphisme de groupes ? Si c'est le cas, déterminer son noyau et son image. Idem pour :

$$f_2 : (\mathbf{Z}^2, +) \longrightarrow (\mathbf{Z}, +), \quad f_2(a,b) = a - b; \quad f_3 : (\mathbf{Z}^2, +) \longrightarrow (\mathbf{Z}/2\mathbf{Z}, +), \quad f_3(a,b) = a - b \pmod 2;$$
$$f_4 : (\mathbf{Z}^2, +) \longrightarrow (\mathbf{Z}, +) \times (\mathbf{Z}/2\mathbf{Z}, +), \quad f_4(a,b) = (a - b, b \pmod 2));$$
$$f_5 : (\mathbf{Z}^3, +) \longrightarrow (\mathbf{Q}_{>0}, \cdot), \quad f_5(a,b,c) = 2^a 3^b 5^c; \quad f_6 : (\mathbf{Z}^3, +) \longrightarrow (\mathbf{Q}_{>0}, \cdot), \quad f_6(a,b,c) = 2^a 3^b 6^c.$$

Exercice 12 – Soit $g \in G$ d'ordre fini et soit $f : G \longrightarrow H$ un morphisme de groupes. Montrer que l'ordre de $f(g)$ divise l'ordre de g. Si f est injectif, montrer que l'ordre de $f(g)$ est égal a l'ordre de g.

Exercice 13 – Soit $n \geq 1$ un entier. Montrer que $\mu_n = (\{z \in \mathbf{C} \mid z^n = 1\}, \cdot)$ est un groupe cyclique d'ordre n. Définir un isomorphisme de groupes explicite $(\mathbf{Z}/n\mathbf{Z}, +) \xrightarrow{\sim} \mu_n$. Pour tout diviseur positif $d \mid n$, montrer que $\mu_d \subset \mu_n$ est un sous-groupe de μ_n (cyclique d'ordre d). Y a-t-il d'autres sous-groupes ?

Exercice 14 – Définir un isomorphisme de groupes $(\mathbf{Z}, +) \xrightarrow{\sim} (\mathbf{Z}^2, +)/\mathbf{Z}(1,1)$, où $\mathbf{Z}(1,1) = \{m(1,1) = (m,m) \mid m \in \mathbf{Z}\} \subset \mathbf{Z}^2$. Idem pour $(\mathbf{Z}, +) \times (\mathbf{Z}/2\mathbf{Z}, +) \xrightarrow{\sim} (\mathbf{Z}^2, +)/\mathbf{Z}(2,2)$.

Exercice 15 – Notons G le groupe $((\mathbf{Z}/16\mathbf{Z})^*, \cdot)$ des éléments inversibles de $\mathbf{Z}/16\mathbf{Z}$.

1. Quel est l'ordre de G ?
2. Énumérer les éléments de G et déterminer leurs ordres respectifs.
3. Le groupe G est-il cyclique ?
4. Montrer que l'application $f : \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \longrightarrow (\mathbf{Z}/16\mathbf{Z})^*$ qui est donnée par la formule $f(a \pmod 2, b \pmod 4) = (-1)^a 5^b \pmod{16}$ est bien définie. Que peut-on dire de f ?

Exercice 16 – Soit $(G, *)$ un groupe, soient $H, H' \subset G$ des sous-groupes de G. Montrer :

1. $H \cap H'$ est un sous-groupe de G.
2. Si $H \not\subset H'$ et $H' \not\subset H$, alors $H \cup H'$ n'est pas un sous-groupe de G. [Indication : étudier le cas $(G, *) = (\mathbf{Z}, +)$, $H = 4\mathbf{Z}$ et $H' = 6\mathbf{Z}$.]

3. Si $(G,+)$ est un groupe abélien, alors $H+H' := \{h+h' \mid h \in H,\, h' \in H'\}$ est un sous-groupe de G contenant $H \cup H'$. Réciproquement, si K est un sous-groupe de G contenant $H \cup H'$, alors $H + H' \subset K$. [Par exemple, $4\mathbf{Z} + 6\mathbf{Z} = 2\mathbf{Z}$.]

4. Si $(G,+)$ est un groupe abélien et si $g,h \in G$, alors $\{mg + nh \mid m,n \in \mathbf{Z}\} \subset G$ est un sous-groupe de G contenant g et h. Réciproquement, si K est un sous-groupe de G contenant g et h, alors $\{mg + nh \mid m,n \in \mathbf{Z}\} \subset K$.

5. Y a-t-il un analogue du point précédent lorsque $(G,*)$ n'est pas abélien ?

Exercice 17 – (Pour enthousiastes) Soit G un groupe abélien fini, soient $g,h \in G$. On note m (resp. n) l'ordre de g (resp. l'ordre de h). Montrer que :

1. pour tout $k \geq 1$, l'ordre de g^k est égal à $m/\mathrm{pgcd}(m,k)$ (en particulier, il divise m);

2. si $\mathrm{pgcd}(m,n) = 1$, alors il existe $k,l \geq 1$ tels que $(gh)^k = g$ et $(gh)^l = h$; en déduire que l'ordre de gh est égal à mn;

3. si $G = \langle g \rangle$ est le groupe cyclique d'ordre m engendré par g, alors le nombre d'éléments de G d'ordre d est égal à $\varphi(d)$ (resp. à 0) si d divise (resp. ne divise pas) m;

4. $\sum_{d|m} \varphi(d) = m$;

5. il existe $a,b \geq 1$ tels que $a \mid m$, $b \mid n$, $\mathrm{pgcd}(a,b) = 1$ et $ab = \mathrm{ppcm}(m,n)$;

6. l'ordre de $g^{m/a}h^{n/b} = \mathrm{ppcm}(m,n)$;

7. il existe $g_{max} \in G$ dont l'ordre est égal au ppcm des ordres de tous les éléments de G;

8. si le groupe G satisfait à la propriété $|\{x \in G \mid x^k = e\}| \leq k$ pour tout $k \geq 1$, alors G est cyclique.