Feuille 2 : Ordre et Generateurs

Exercice 17 (♡ Ordre d'un élément).
Soient G, H deux groupes.

(1) Soit $f \in \mathrm{Hom}(G, H)$ et $x \in G$. Comparer l'ordre de x et de $f(x)$.
(2) Soient $x, g \in G$. Comparer l'ordre de x et de gxg^{-1}.
(3) Soient $x, y \in G$. Comparer l'ordre de xy et de yx.
(4) Dans le cas où $xy = yx$, déterminer l'ordre de xy en fonction des ordres de x et de y, en supposant que les ordres sont premiers entre eux. Peut-on déterminer l'ordre de xy en général, seulement à partir des ordres de x et y ?

Exercice 18 (Générateurs des groupes cycliques).
Soient $n \geq 2$ et $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$. Montrer que les propriétés suivantes sont équivalentes

(1) $\overline{k}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$.
(2) $\overline{k}$ est inversible (pour la multiplication) dans $\mathbb{Z}/n\mathbb{Z}$
(3) n et k sont premiers entre eux.

Exercice 19 (Sous-groupes d'un groupe cyclique).
Soit $n \in \mathbb{N}^*$ et $G = \mathbb{Z}/n\mathbb{Z}$. Soit $k \in \mathbb{Z}$ et $d = \mathrm{pgcd}(k, n)$.

(1) Déterminer l'ordre de k dans G.
(2) Montrer que k et d engendrent le même sous-groupe de G.
(3) En déduire que pour tout diviseur d de n, il existe un unique sous-groupe C_d qui soit d'ordre d.
(4) Quels sont tous les sous-groupes de G ?

Exercice 20 (♠ Groupes de cardinal premier).
Soit p un nombre premier et G un groupe de cardinal p.

(1) Montrer que G est cyclique.
(2) En déduire que tous les groupes de cardinal p sont isomorphes.

Exercice 21 (Pas de sous-groupe).
Soit G un groupe n'ayant pas de sous-groupe non-trivial.

(1) Montrer que G est monogène.
(2) Montrer que G est fini.
(3) Montrer que $|G|$ est un nombre premier.

Exercice 22 (★ Groupe d'ordre pair et impair).

(1) Soit G un groupe fini de cardinal pair. Montrer qu'il existe un élément d'ordre 2.
(2) Soit G un groupe fini de cardinal impair. Montrer que $\forall x \in G, \exists! y \in G, x = y^2$

Exercice 23 (Groupe de similitude).
Pour $\alpha \in \mathbb{C}^*$ et $\beta \in \mathbb{C}$, on note $f_{\alpha,\beta} : \mathbb{C} \to \mathbb{C}$ définie par $f(z) = \alpha z + \beta$.

(1) Montrer que l'ensemble des fonctions $f_{a,b}$ est un groupe pour la loi $\circ$.
(2) Ce groupe est-il commutatif
(3) A quelle(s) condition(s) sur α et β, l'élément $f_{\alpha,\beta}$ est-il d'ordre fini.

Exercice 24 (Groupe d'ordre ab)**.**
Soit G un groupe commutatif fini d'ordre ab avec $a \wedge b = 1$.
On pose $A = \{x \in G | x^a = e\}$ et $B = \{x \in G | x^b = e\}$.

(1) Montrer que A et B sont des sous-groupes de G.
(2) Montrer que $A \cap B = \{e\}$ et $AB = G$.

Exercice 25 (Groupes d'ordre 4)**.**
Montrer qu'il n'existe que deux groupes d'ordre 4 à isomorphisme près. (Raisonner sur l'exposant du groupe)

Exercice 26 (Groupe d'exposant 2)**.**
Soit G un groupe fini tel que $\forall x \in G, x^2 = e$

(1) Montrer que G est commutatif.
(2) Soit H un sous-groupe strict de G et $x \notin H$. On note K le sous-groupe engendré par $H \cup \{x\}$. Montrer que $|K| = 2|H|$.
(3) En déduire que $|G|$ est une puissance de 2.

Exercice 27 (Groupes d'ordre 6)**.**
Le but de l'exercice est de trouver tous les groupes d'ordre 6, à isomorphisme près. Soit G un groupe d'ordre 6.

(1) Montrer que G ne peut pas être constitué uniquement d'éléments d'ordre 2. (utiliser l'exercice précédent.)
(2) Supposons que G est commutatif.
    (a) Montrer que G ne peut pas être constitué uniquement d'éléments d'ordre 3.
    (b) En déduire que G possède un élément d'ordre 6. (donc G est cyclique)
(3) Supposons que G n'est pas commutatif
    (a) Montrer que G n'a pas d'éléments d'ordre 6.
    (b) En déduire qu'il existe x d'ordre 2 et y d'ordre 3 tels que $G = \{e, y, y^2, x, xy, xy^2\}$.
    (c) Montrer que $xyx = y^2$, puis Etablir la table de G dans ce cas
(4) En déduire qu'il n'y a que deux groupes d'ordre 6 à isomorphisme près.

Exercice 28 (♠ Petit théorème de Fermat)**.**
Soit p un nombre premier.

(1) Montrer que tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles pour la multiplication.
(2) En déduire que pour tout $a \in \mathbb{Z}$, le nombre p divise $a^p - a$. (petit théorème de Fermat)

Exercice 29 (♠ Théorème de Cayley)**.**
Soit $G = \{g_1, \dots, g_n\}$ un groupe fini d'ordre n. On note $\mathrm{Bij}(G)$ le groupe des bijections de G dans lui-même (Ce groupe est isomorphe au groupe $\mathcal{S}_n$ des permutations sur n éléments).

(1) Soit $g \in G$. Soit l'application suivante
$$\begin{aligned} \varphi_g : G &\longrightarrow G \\ x &\longmapsto gx \end{aligned}$$
Montrer que φ_g est bijective.
(2) Considérons maintenant l'application suivante
$$\begin{aligned} \Phi : G &\longrightarrow \mathrm{Bij}(G) \\ g &\longmapsto \varphi_g \end{aligned}$$
Montrer que Φ est un morphisme de groupes.
(3) Montrer que Φ est injective et en déduire que tout groupe fini est isomorphe à un sous-groupe de $\mathcal{S}_n$.

Exercice 30 (♠ Groupes distingués)**.**
Soit H et K deux sous-groupes distingués du groupe G.

(1) Montrer que $H \cap K$ est un sous-groupe distingué de G.
(2) Montrer que $HK = \{hk | h \in H, k \in K\}$ est un sous-groupe de G, puis montrer qu'il est distingué dans G.

Exercice 31 (Isométries du Carré)**.**
On considère le groupe G des rotations et réflexions qui préservent un carré.

(1) Donner la liste des 8 éléments de G. (Il doit y avoir 4 rotations et 4 symétries).
(2) Donner la liste des sous-groupes de G. (Commencer par les sous-groupes engendrés par 1 élément, puis par 2 éléments, etc ...)
(3) Parmi ces sous-groupes, lesquels sont distingués dans G?

Exercice 32 (♠ Exemples)**.**

(1) Montrer que le quotient $\mathbb{C}/\mathbb{R}$ est isomorphe à $\mathbb{R}$. (avec l'addition comme loi)
(2) Montrer que le quotient $\mathbb{R}/\mathbb{Z}$ est isomorphe à $\mathbb{U}$ le groupe des nombres complexes de module 1.
(3) Soit $G = (\mathbb{R}^*, \times)$ et $H = \mathbb{R}_+^*$. Montrer que G/H est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.
(4) Soit $G = \mathrm{GL}_2(\mathbb{C})$ et $H = \{k \cdot \mathrm{I}_2 \mid k \in \mathbb{C}^*\}$. Montrer que H est bien un sous-groupe distingué, et montrer que G/H est isomorphe à $\mathrm{SL}_2(\mathbb{C})$.

Exercice 33 (Groupe Affine)**.**
Soit G l'ensemble des fonctions affine de $\mathbb{C}$ dans $\mathbb{C}$. C'est à dire :

$$G = \left\{ \begin{array}{ll} f : \mathbb{C} & \to \mathbb{C} \\ \quad z & \mapsto az + b \end{array} \;\middle|\; a \in \mathbb{C}^*, b \in \mathbb{C} \right\}$$

On rappelle que G, muni de la loi $\circ$ est un groupe (exercice 23).

(1) Montrer que G est un groupe pour la loi $\circ$.
(2) Montrer que l'ensemble T des translations
$$T = \left\{ z \mapsto z + b \;\middle|\; b \in \mathbb{C} \right\}$$
est un sous-groupe distingué de G, isomorphe à $\mathbb{C}$.
(3) Montrer que l'ensemble H des homothéties :
$$H = \left\{ z \mapsto az \;\middle|\; a \in \mathbb{C}^* \right\}$$
est un sous-groupe de G isomorphe à $\mathbb{C}^*$. Montrer qu'il n'est pas distingué dans G.
(4) En déduire que le quotient G/T est isomorphe à $\mathbb{C}^*$.
(5) Est-ce que G est isomorphe au groupe produit $\mathbb{C} \times \mathbb{C}^*$?

Exercice 34.
Soit $(G, +)$ le groupe quotient $(\mathbb{Q}, +)$ par $\mathbb{Z}$. Pour $x \in \mathbb{Q}$, on note $\overline{x} \in G$ la classe de x dans $\mathbb{Q}/\mathbb{Z}$.

(1) Soit $x = \frac{p}{q} \in \mathbb{Q}$ avec p et q premiers entre eux. Déterminer l'ordre de $\overline{x}$.
(2) En déduire que tout élément de G est d'ordre fini.
(3) Montrer que G n'est pas d'exposant fini.

Exercice 35 (Groupes simples)**.**
Soit G un groupe tel que G ne contient aucun sous-groupe distingué à part $\{e\}$ et G. (Un tel groupe est appelé groupe *simple*)

(1) Soit H un autre groupe quelconque et $f \in \mathrm{Hom}(G, H)$. Montrer que si f n'est pas le morphisme trivial (tel que $f(g) = e$ pour tout $x \in G$), alors f est injectif.
(2) On suppose que G est un groupe fini et abélien (en plus d'être simple). Montrer que G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ avec p premier.

Exercice 36. ★ Montrer que si $G/Z(G)$ est engendré par un seul élément, alors G est abélien.

Exercice 37 (Groupes d'ordre pq)**.**
Soient p, q deux nombres premiers et G un groupe abélien tel que $|G| = pq$. Montrer que G est cyclique.

Exercice 38 (Groupes abéliens d'ordre 600)**.**

(1) ♡ Montrer que si n et m sont premiers entre eux, alors $\mathbb{Z}_n \times \mathbb{Z}_m$ est isomorphe à $\mathbb{Z}_{mn}$.

(2) Dans la liste suivante, déterminer quels groupes sont isomorphes entre eux :

$$\mathbb{Z}_{600} \; ; \; \mathbb{Z}_2 \times \mathbb{Z}_{300} \; ; \; \mathbb{Z}_3 \times \mathbb{Z}_{200} \; ; \; \mathbb{Z}_4 \times \mathbb{Z}_{150} \; ; \; \mathbb{Z}_5 \times \mathbb{Z}_{120} \; ; \; \mathbb{Z}_6 \times \mathbb{Z}_{100}$$

$$\mathbb{Z}_8 \times \mathbb{Z}_{75} \; ; \; \mathbb{Z}_{10} \times \mathbb{Z}_{60} \; ; \; \mathbb{Z}_{12} \times \mathbb{Z}_{50} \; ; \; \mathbb{Z}_{15} \times \mathbb{Z}_{40} \; ; \; \mathbb{Z}_{20} \times \mathbb{Z}_{30} \; ; \; \mathbb{Z}_{24} \times \mathbb{Z}_{25}$$

(3) Existe t'il d'autres groupes abéliens d'ordre 600 que ceux de la liste ?

Exercice 39. ♠
Déterminer le nombre de groupes abéliens d'ordre 32, d'ordre 72, et d'ordre 210. (les trois questions sont indépendantes).