TD N° 2 - **Groupes, sous-groupes, morphismes, ordre.**

Exo 1. Est-ce un groupe ? Si oui, est-il abélien ?

1) $(\mathbb{R}^{+\times}, \cdot)$, $(\mathbb{C}^\times, +)$, $(\mathbb{C}, \cdot)$, $(\mathbb{U}, +)$, $(\mathbb{U}, \cdot)$, $(\mathbb{U}_n, \cdot)$, $(\{z \in \mathbb{C} \mid |z| = 2\}, \cdot)$, où $\mathbb{U}$ est l'ensemble des nombres complexes de module 1 et $\mathbb{U}_n$ l'ensemble des racines n-ièmes de l'unité dans $\mathbb{C}$.

2) L'ensemble des applications affines de $\mathbb{R}$ dans $\mathbb{R}$ muni de l'addition (resp. multiplication, composition) des fonctions.

3) L'ensemble des endomorphismes d'un espace vectoriel muni de l'addition (resp. composition) des applications.

4) L'ensemble des rotations du plan muni de la composition des applications.

5) L'ensemble des rotations du plan de centre O fixé muni de la composition des applications.

6) L'intervalle $]-1, 1[$ muni de la loi définie par $x \star y = \frac{x+y}{1+xy}$.

Exo 2. 1) Montrer que la table de la loi de composition d'un groupe fini est un carré latin, c'est-à-dire un tableau carré dans lequel chaque élément apparaît une et une seule fois dans chaque ligne et chaque colonne.

2) Donner la liste des tables possibles pour les groupes à $2, 3$ ou 4 éléments. On cherchera en particulier des exemples de groupes pour chacune d'entre elles. Montrer qu'un groupe à $2, 3$ ou 4 éléments est commutatif.

Exo 3. 1) Montrer que l'ensemble $\mathfrak{S}(E)$ des bijections d'un ensemble non vide E sur lui-même muni de la composition des applications est un groupe.

2) Si E possède n éléments, quel est le cardinal de $\mathfrak{S}(E)$?

3) On note $\mathfrak{S}_n = \mathfrak{S}(\{1, \ldots, n\})$. Lister les éléments de $\mathfrak{S}_3$, et expliciter la table de ce groupe. Est-il commutatif ?

Exo 4. 1) Soit X un sous-ensemble non vide du plan euclidien $E = \mathbb{R}^2$. Montrer que $\mathrm{Is}(X) = \{f \in \mathrm{O}(E) \mid f(X) = X\}$ est un sous-groupe de $\mathrm{O}(E)$.

2) Déterminer $\mathrm{Is}(X)$ lorsque X est un polygone régulier à n côtés centré en l'origine. On parle du groupe diédral D_n (également noté D_{2n}).

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

$$x * y = f^{-1}(f(x) + f(y)).$$

1) Montrer que $(I, *)$ est un groupe commutatif.

2) Expliciter la loi $*$ dans les cas suivants :

2.a) $I =]0, +\infty[, f(x) = \ln(x)$;

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

2.c) $I = \mathbb{R}, f(x) = \lambda x$ avec $\lambda \in \mathbb{R}^\times$ fixé ;

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

Exo 6. Soient G_1 et G_2 deux groupes.

1) Montrer que $G_1 \times G_2$ est un groupe pour la loi

$$(g_1, g_2)\cdot(g_1', g_2') = (g_1 g_1', g_2 g_2').$$

On parle du produit direct de G_1 et G_2.

2) Soit H_i un sous-groupe de G_i pour $i \in \{1, 2\}$. Montrer que $H_1 \times H_2$ est un sous-groupe de $G_1 \times G_2$. Réciproque ?

Exo 7. Pour tous $n, m \in \mathbb{N}$, de développements 2-adiques donnés par

$$n = \sum_{j \geq 0} x_j 2^j \text{ et } m = \sum_{j \geq 0} y_j 2^j,$$

on note

$$n \oplus m = \sum_{j \geq 0} z_j 2^j,$$

où z_j est l'unique élément de $\{0, 1\}$ tel que $z_j \equiv x_j + y_j \mod 2$.

1) Calculer $5 \oplus 0, 3 \oplus 3, 4 \oplus 8, 31 \oplus 26$.

2) Montrer que $(\mathbb{N}, \oplus)$ est un groupe commutatif.

Soient $n_1, \ldots, n_p \in \mathbb{N}$.

3) On suppose que $n_1 \oplus \cdots \oplus n_p = 0$. Montrer que, pour tout $k \in \{1, ..., p\}$ et tout entier $m_k \neq n_k$, on a

$$n_1 \oplus \cdots \oplus n_{k-1} \oplus m_k \oplus n_{k+1} \oplus \cdots \oplus n_p \neq 0.$$

4) On suppose que $n_1 \oplus \cdots \oplus n_p \neq 0$. Montrer qu'il existe $k \in \{1, ..., p\}$, et un entier $m_k < n_k$ tel que

$$n_1 \oplus \cdots \oplus n_{k-1} \oplus m_k \oplus n_{k+1} \oplus \cdots \oplus n_p = 0.$$

Indication. Soit 2^d la plus grand puissance de 2 intervenant dans le développement 2-adique de $n_1 \oplus \cdots \oplus n_p$. Justifier qu'il existe $k \in \{1, ..., p\}$ tel que le d-ème digit de n_k soit 1. Montrer alors que l'entier $m_k = (n_1 \oplus \cdots \oplus n_p) \oplus n_k$ convient.

5) On considère le jeu à deux joueurs suivant. On se donne un certain nombre de tas d'allumettes. A tour de rôle, chaque joueur choisit un tas, et prend autant d'allumettes qu'il souhaite. Le joueur qui prend la dernière allumette a perdu.

Montrer qu'un des deux joueurs a une stratégie gagnante, et que cela ne dépend que de la configuration de départ.

Exo 8. On note $Z(G)$, et on appelle centre de G, l'ensemble des éléments d'un groupe G qui commutent à tous les éléments de G. Montrer que $Z(G)$ est un sous-groupe de G.

Exo 9. Les applications suivantes sont-elles des morphismes de groupes ?

$$\begin{aligned} \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto 2x \end{aligned} \qquad \begin{aligned} \mathbb{R}^\times &\longrightarrow \mathbb{R}^\times \\ x &\longmapsto 2x \end{aligned} \qquad \begin{aligned} \mathbb{C}^\times &\longrightarrow \mathbb{C}^\times \\ x &\longmapsto x^2 \end{aligned}$$

$$\begin{aligned} G &\longrightarrow G \\ x &\longmapsto x^2 \end{aligned} \quad , G \text{ groupe} \qquad \begin{aligned} \mathbb{R} &\longrightarrow \mathrm{GL}_2(\mathbb{R}) \\ t &\longmapsto \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Exo 10. Soient G un groupe et G' un groupe commutatif. Montrer que l'ensemble $\mathrm{Hom}(G, G')$ des morphismes de groupes de G dans G' est un groupe pour la loi

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

Exo 11. 1) Déterminer l'ensemble des endomorphismes de groupes de $\mathbb{Z}$. Lesquels sont injectifs ? surjectifs ?

2) Plus généralement, considérons un groupe G.

2.a) Décrire l'ensemble $\mathrm{Hom}(\mathbb{Z}, G)$, et montrer qu'il est en bijection avec G.

2.b) Si G est commutatif, montrer que les groupes $\mathrm{Hom}(\mathbb{Z}, G)$ et G sont isomorphes.

Exo 12. Soit G un groupe.

1) Montrer que l'ensemble $\mathrm{Aut}(G)$ des automorphismes de G est un groupe pour la composition.

2) Soit $g \in G$. Montrer que l'application

$$\mathrm{Int}_g : \begin{aligned} G &\longrightarrow G \\ x &\longmapsto gxg^{-1} \end{aligned}$$

est un élément de $\mathrm{Aut}(G)$. Un tel automorphisme est appelé un automorphisme intérieur de G.

3) Montrer que l'application

$$\mathrm{Int}\colon \begin{array}{rcl} G & \longrightarrow & \mathrm{Aut}(G) \\ g & \longmapsto & \mathrm{Int}_g \end{array}$$

est un morphisme de groupes. Expliciter son noyau.

Exo 13. 1) Déterminer les $a \in \mathbb{Z}$ tels que $\langle a \rangle = \mathbb{Z}$.

2) Déterminer les $a, b \in \mathbb{Z}$ tels que $\langle a, b \rangle = \mathbb{Z}$.

Exo 14. Soit $n \in \mathbb{Z}$. Déterminer les $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ tels que $\langle \overline{a} \rangle = \mathbb{Z}/n\mathbb{Z}$.

Exo 15. Quel est le sous-groupe de $\mathrm{O}(\mathbb{R}^2)$ engendré par une rotation ? une réflexion orthogonale ? deux réflexions orthogonales ? une réflexion orthogonale et une rotation ?

Exo 16. Pour tout $n \in \{1, ..., 10\}$, déterminer si $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique, et en donner une partie génératrice minimale.

Exo 17. Soit $f : G \longrightarrow G'$ un morphisme de groupes. Soit $\mathcal{P}$ une partie de G.

1) Montrer que $f(\langle \mathcal{P} \rangle) = \langle f(\mathcal{P}) \rangle$.

2) Montrer que si $\mathcal{P}$ engendre G, $f(\mathcal{P})$ engendre $\mathrm{im}(f)$.

3) On suppose que f est un isomorphisme de groupes. Montrer que $\mathcal{P}$ engendre G si et seulement si $f(\mathcal{P})$ engendre G'.

Exo 18. Le groupe $\mathfrak{S}_3$ est-il cyclique ? En donner une partie génératrice de cardinal minimal.

Exo 19. Soit E un espace euclidien de dimension $n \geq 1$. Le but de cet exercice est de montrer le résultat suivant.

Théorème. *Toute isométrie $u \in \mathrm{O}(E)$ est la composée de $n - \dim_{\mathbb{R}}(\ker(u - \mathrm{Id}_E))$ réflexions orthogonales. De plus, si $u \in \mathrm{O}(E)$ est la composée de p réflexions orthogonales, alors $p \geq n - \dim_{\mathbb{R}}(\ker(u - \mathrm{Id}_E))$.*

Corollaire. *Le groupe $\mathrm{O}(E)$ est engendré par les réflexions orthogonales.*

1) Soit u une isométrie de E, distincte de Id_E.

1.a) Montrer qu'il existe $x_1 \in \ker(u - \mathrm{Id}_E)^\perp$ non nul. Justifier que $x_1 \neq u(x_1)$.

1.b) On note τ_1 l'unique réflexion orthogonale de E envoyant x_1 sur $u(x_1)$. Montrer que $\ker(u - \mathrm{Id}_E) \subsetneq \ker(\tau_1 \circ u - \mathrm{Id}_E)$.

1.c) Montrer que u est la composée d'au plus $n - \dim_{\mathbb{R}}(\ker(u - \mathrm{Id}_E))$ réflexions orthogonales.

2) Considérons une isométrie $u \in \mathrm{O}(E)$ telle que $u = \tau_1 \circ \cdots \circ \tau_p$, pour des réflexions orthogonales $\tau_1, ..., \tau_p$. Montrer que $\dim_{\mathbb{R}}(\ker(u - \mathrm{Id}_E)) \geq n - p$. On pourra commencer par remarquer que $\cap_{i=1}^{p} \ker(\tau_i - \mathrm{Id}_E) \subset \ker(u - \mathrm{Id}_E)$.

Exo 20. Soit E un espace euclidien.

1) Soient τ, τ' deux réflexions orthogonales de E. Montrer qu'il existe $f \in \mathrm{O}(E)$ telle que $\tau' = f \circ \tau \circ f^{-1}$.

2) Donner un morphisme de groupes $\mathrm{O}(E) \longrightarrow \mathbb{C}^{\times}$ non trivial.

3) Soit $\varphi : \mathrm{O}(E) \longrightarrow \mathbb{C}^{\times}$ un morphisme de groupes non trivial. Montrer que $\varphi(\tau) = -1$ pour toute réflexion orthogonale τ. En déduire qu'il existe un unique morphisme de groupes $\mathrm{O}(E) \longrightarrow \mathbb{C}^{\times}$ non trivial.

Exo 21. Calculer l'ordre des éléments du groupe G, et lister ses sous-groupes, dans les cas suivants : $G = \mathbb{Z}/4\mathbb{Z}, \{\pm 1\} \times \{\pm 1\}, D_4, \mathfrak{S}_3$.

Exo 22. Déterminer l'ensemble des éléments d'ordre fini du groupe des isométries vectorielles du plan. S'agit-il d'un sous-groupe ?

Exo 23. On suppose que $f : G \longrightarrow G'$ est un morphisme de groupes injectif. Montrer que $o(x) = o(f(x))$. Que peut-on dire si f n'est plus supposé injectif ?

Exo 24. Parmi les groupes $\mathbb{R}, \mathbb{R}^{\times},]0, +\infty[, \mathbb{C}^{\times}, \mathbb{U}_6, D_3, \mathfrak{S}_3, \mathbb{Z}/6\mathbb{Z}$ et $\mathbb{U}_2 \times \mathbb{U}_6$, lesquels sont isomorphes ?

Exo 25. 1) Montrer qu'un groupe dont les éléments sont d'ordre ≤ 2 est commutatif et, s'il est fini, isomorphe à $(\mathbb{Z}/2\mathbb{Z})^n$ pour un certain entier $n \geq 0$.

2) Soit G l'ensemble des matrices triangulaires supérieures de $\mathrm{GL}_3(\mathbb{Z}/3\mathbb{Z})$ dont les termes diagonaux sont tous égaux à $\overline{1}$. Montrer que G est un sous-groupe de $\mathrm{GL}_3(\mathbb{Z}/3\mathbb{Z})$, et que l'on a $M^3 = I_3$ pour tout $M \in G$. Ce groupe est-il commutatif ?

Exo 26. Montrer qu'un groupe fini G d'ordre premier est cyclique, engendré par n'importe quel élément distinct du neutre.

Exo 27. Soit G un groupe, et soient H et K deux sous-groupes de G.

1) On suppose que $|H|$ et $|K|$ sont premiers entre eux. Déterminer $H \cap K$.

2) On suppose que H et K sont d'ordre p premier. Montrer que, soit $H = K$, soit $H \cap K = \{e\}$.

Exo 28. Déterminer les sous-groupes finis de $\mathbb{C}^{\times}$.

Exo 29. Soient $m, n \geq 1$ deux entiers, et soit $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Montrer que G est cyclique si et seulement si m et n sont premiers entre eux.

Exo 30. 1) Soient $m, n \geq 1$ des entiers. On se place dans le groupe $\mathbb{Z}/n\mathbb{Z}$.

1.a) Déterminer l'unique diviseur $d \geq 1$ de n tel que $\langle \overline{m} \rangle = \langle \overline{d} \rangle$.

1.b) Quel est l'ordre de $\overline{m}$?

2) Soit G un groupe (noté multiplicativement), et soit $x \in G$ d'ordre fini $n \geq 1$. Soit $m \geq 1$ un entier. Déterminer l'ordre de x^m.

Exo 31. Soit $n \geq 3$. Soit G un groupe. On suppose que G est engendré par deux éléments σ et τ vérifiant

$$o(\sigma) = n, \quad o(\tau) = 2 \text{ et } \tau\sigma\tau^{-1} = \sigma^{-1}.$$

1) Montrer que tout élément de G s'écrit de manière unique sous la forme $\sigma^i \tau^j$ avec $i \in \{0, \ldots, n-1\}$ et $j \in \{0, 1\}$. Quel est l'ordre de G ?

2) Montrer que G est isomorphe à D_n.

Exo 32. On considère le groupe $G = \mathrm{GL}_2(\mathbb{C})$. On suppose que l'on a trois matrices $A, B, C \in G$ vérifiant

$$A^2 = B^2 = C^2 = -I_2, AB = C, BC = A, CA = B.$$

1) Montrer que $\{\pm I_2, \pm A, \pm B, \pm C\}$ est un sous-groupe de G d'ordre 8. Écrire sa table de multiplication.

Ce groupe s'appelle le groupe quaternionique, et se note H_8 ou Q_8.

2) Déterminer les sous-groupes de Q_8.

3) On cherche trois matrices vérifiant les hypothèses de l'exercice.

3.a) Montrer qu'il suffit de trouver $A, B \in G$ telles que $A^2 = B^2 = -I_2$ et $AB = -BA$.

3.b) Vérifier que $A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ et $B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ conviennent.

Exo 33. Soit G un groupe fini (noté multiplicativement), et soit p un nombre premier. On suppose que, pour tout $g \in G$, on a $g^p = e$.

1) On suppose que G est commutatif. Montrer que G est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^n$.

2) On suppose G non commutatif. Montrer que $|G| \geq p^2$.

Exo 34. Soit G un groupe d'ordre 6.

1) Montrer que G contient au moins un élément σ d'ordre 3 et un élément τ d'ordre 2. On pourra utiliser l'exercice 33.

2) Montrer que $G = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$.

3) On suppose que G est commutatif. Montrer que G est isomorphe à $\mathbb{Z}/6\mathbb{Z}$.

4) On suppose que G n'est pas commutatif. Montrer que $\tau\sigma\tau^{-1} = \sigma^{-1}$. En déduire que G est isomorphe à D_3.

5) Résumer le résultat obtenu.