Feuille 1 : Notions sur les groupes

Groupes - Sous-groupes

► **Exercice 1 (Un exemple simple)** On considère les quatre fonctions de $\mathbb{R}^*$ dans $\mathbb{R}^*$ définies par

$$f_1(x) = x, \qquad f_2(x) = \frac{1}{x}, \qquad f_3(x) = -x \quad \text{et} \quad f_4(x) = -\frac{1}{x}.$$

Montrer que $G = \{f_1, f_2, f_3, f_4\}$ est un groupe pour la loi de composition des applications.

► **Exercice 2 (D'autres lois sur $\mathbb{Z}$)**
1) Montrer que $\mathbb{Z}$ muni de la loi de composition interne $*$ définie par

$$a * b = a + b + 1$$

est un groupe. Quel en est l'élément neutre ? Déterminer le symétrique de 79.

2) Même question avec la loi $\bullet$ définie par $a \bullet b = a + (-1)^a b$.

► **Exercice 3 (Une autre loi sur $\mathbb{R}$)** Montrer que $\mathbb{R}$ muni de la loi de composition interne $*$ définie par $x * y = x + y - 1$ est un groupe. Quel en est l'élément neutre ? Quel est le symétrique de 2 ? de π ? de 1 ?

► **Exercice 4 (Tables de multiplication)** Étant donné un groupe G ayant n éléments $x_1, \ldots, x_n$, la *table de multiplication* de G est donnée par le tableau suivant :

	x_1	$\ldots$	x_j	$\ldots$	x_n
x_1	x_1x_1	$\ldots$	x_1x_j	$\ldots$	x_1x_n
$\vdots$	$\vdots$		$\vdots$		$\vdots$
x_i	x_ix_1	$\ldots$	x_ix_j	$\ldots$	x_ix_n
$\vdots$	$\vdots$		$\vdots$		$\vdots$
x_n	x_nx_1	$\ldots$	x_nx_j	$\ldots$	x_nx_n

En général, on suppose que $x_1 = e$, l'élément neutre de G.

1) Soit $\mathbb{U}_n$ le groupe des racines n-ièmes de l'unité :

$$\mathbb{U}_n = \left\{ x_k = e^{\frac{2\pi i(k-1)}{n}} \,/\, k = 1, \ldots, n \right\}.$$

Écrire les tables de $\mathbb{U}_2$, $\mathbb{U}_3$ et $\mathbb{U}_4$.

2) Écrire les tables d'addition et de multiplication des ensembles $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$ et $\mathbb{Z}_6$ (rappelons que si $n \in \mathbb{N}$, $\mathbb{Z}_n = \{0, 1, ..., n-1\}$). Déduire de ces tables une liste exhaustive de tous les groupes apparaissant parmi et dans ces cinq ensembles.

3) On pose $x_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $x_2 = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $x_3 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ et $x_4 = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Écrire la table de multiplication pour le produit matriciel. L'ensemble $\{x_1, \ldots, x_4\}$ muni de ce produit est-il un groupe ? Interpréter géométriquement les matrices x_i, $i = 1, \ldots, 4$.

4) On pose $x_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $x_2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $x_3 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ et $x_4 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Écrire la table de multiplication pour le produit matriciel. L'ensemble $\{x_1, \ldots, x_4\}$ muni de ce produit est-il un groupe ? Interpréter géométriquement les matrices x_i, $i = 1, \ldots, 4$.

5) Soit S_3 le groupe des permutations de l'ensemble $\{1, 2, 3\}$. Déterminer la table de multiplication de S_3.

► **Exercice 5 (Un groupe donné par sa table)** On considère un ensemble E de quatre éléments e, i, j, k et une loi de composition $*$ interne ayant pour table

$*\nearrow$	e	i	j	k
e	e	i	j	k
i	i	j	k	e
j	j	k	e	i
k	k	e	i	j

Montrer que l'on a défini sur E une structure de groupe abélien.

► **Exercice 6 (Encore des tables)** Déterminer les tables possibles définissant un groupe ayant 1, 2, 3 ou 4 éléments.

► **Exercice 7 (Un nouvel exemple : $\mathbb{Z}_{23} \setminus \{0\}$)** Pourquoi $\mathbb{Z}_{23} \setminus \{0\}$ est-il un groupe pour la multiplication ? Déterminer l'inverse de 7.

► **Exercice 8 ($x^2 = e$ pour tout x)** Soit G un groupe vérifiant $x^2 = e$ pour tout $x \in G$. Montrer que G est commutatif.

► **Exercice 9 (Exemple de sous-groupes)** Parmi les sous-ensembles suivants, lesquels sont des sous-groupes ?

1) $\mathrm{GL}_n(\mathbb{R}) \subset \mathrm{GL}_n(\mathbb{C})$ (pour $n \geqslant 1$) ;

2) $\{-1, 1\} \subset (\mathbb{R}^*, \times)$;

3) $\mathbb{N} \subset (\mathbb{Z}, +)$;

4) $\mathbb{Q}^* \subset (\mathbb{R}^*, \times)$;

5) $\{-1, 0, 1\} \subset (\mathbb{Z}, +)$;

6) pour $n \geqslant 2$, $\{A \in \mathrm{GL}_n(\mathbb{R}) \,/\, {}^tA = A\} \subset \mathrm{GL}_n(\mathbb{R})$;

7) pour G un groupe d'élément neutre e, $\{x \in G \,/\, x^2 = e\} \subset G$.

► **Exercice 10 (Le cercle unité)** Montrer que S^1, l'ensemble des nombres complexes de module 1, est un sous-groupe de $(\mathbb{C}^*, \times)$.

► **Exercice 11 (Les sous-groupes classiques de matrices)**

1) Montrer que $\mathrm{O}(n)$, l'ensemble des matrices orthogonales de taille n, est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.

2) Montrer que l'ensemble des matrices réelles de taille n dont le déterminant vaut 1 est un sous-groupe distingué de $\mathrm{GL}_n(\mathbb{R})$.

3) Montrer que $\mathrm{SO}(n)$, l'ensemble des matrices orthogonales de taille n dont le déterminant vaut 1, est un sous-groupe distingué de $\mathrm{O}(n)$. Que peut-on dire de $\mathrm{SO}(n)$ dans $\mathrm{GL}_n(\mathbb{R})$?

► **Exercice 12 (Un exemple de sous-groupe engendré par un élément)** Quels sont les éléments du sous-groupe engendré par $\left(\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ dans $\mathrm{GL}_2(\mathbb{R})$?

► **Exercice 13 (PGCD et PPCM)** Soient a et b deux entiers relatifs.

1) Montrer que $a\mathbb{Z} \cap b\mathbb{Z}$ est un groupe. Qu'en déduisez-vous ?

2) Décrire le sous-groupe de $\mathbb{Z}$ engendré par $\{a, b\}$.

► **Exercice 14 (Sous-groupes de $\mathbb{Z}_{12}$)**

1) Montrer que dans $\mathbb{Z}_{12}$, les sous-groupes engendrés par 10 et 2 coïncident.

2) Déterminer tous les sous-groupes cycliques de $\mathbb{Z}_{12}$.

3) Plus généralement, si $a \in \mathbb{Z}_n$ et $d = a \wedge n$, montrer que les sous-groupes engendrés par a et d coïncident.

► **Exercice 15 (Sous-groupes finis de $\mathbb{C}^*$)** Déterminer les sous-groupes finis de $(\mathbb{C}^*, \times)$.

► **Exercice 16 (Groupe produit)** Soient G et H deux groupes. On munit le produit $G \times H$ de la loi de composition interne définie par

$$\Big((g,h),(g',h')\Big) \mapsto \big(gg', hh'\big).$$

Montrer que cette loi fait de $G \times H$ un groupe. En donner l'élément neutre et déterminer le symétrique de $(g,h) \in G \times H$.

► **Exercice 17 (Commutateurs $[H,K]$)** Soient H et K deux sous-groupes distingués d'un groupe G. Pour tout $(h,k) \in H \times K$, montrer que le commutateur $[h,k]$ appartient à $H \cap K$.

► **Exercice 18 (Groupe diédral)** On note G le groupe des bijections de $\mathbb{C}$ dans $\mathbb{C}$ muni de la loi de composition des applications. Pour $a \in \mathbb{C}$, on définit

$$r_a : \begin{pmatrix} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & az \end{pmatrix} \quad \text{et} \quad s_a : \begin{pmatrix} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & a\overline{z} \end{pmatrix}.$$

1) Montrer que, pour tout $a \neq 0$, r_a et s_a sont des éléments de G.

Pour $n \in \mathbb{N}$, on définit $D_n \subset G$ de la façon suivante :

$$D_n = \{r_a, s_a \,/\, a \in \mathbb{U}_n\}$$

où $\mathbb{U}_n$ est le groupe des racines $n^{\text{ièmes}}$ de l'unité.

2) Montrer que D_n est un groupe pour la composition des applications. Est-il commutatif ?

3) Écrire la table des groupes D_3 et D_4.

4) Donner un système de générateurs à deux éléments de D_n.

► **Exercice 19 (Si deux générateurs commutent ...)** Dans un groupe G, on considère un sous-groupe H engendré par deux éléments a et b. Montrer que si $ab = ba$, alors H est abélien.

► **Exercice 20 (Centre d'un groupe)** Soit G un groupe. On définit le centre de G, noté $Z(G)$, par :

$$Z(G) = \{g \in G \,/\, gx = xg \text{ pour tout } x \text{ dans } G\}.$$

1) Calculer $Z(G)$ lorsque G est abélien. Énoncer/étudier une éventuelle réciproque à ce résultat.

2) Montrer que $Z(G)$ est un sous-groupe distingué de G.

3) Déterminer le centre de $\mathbb{Z}$ et du groupe symétrique S_3.

Ordre d'un élément

► **Exercice 21 (Exemples de calculs d'ordres dans $\mathbb{Z}_n$)** Déterminer les ordres de chacun des éléments de $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_6$ et $\mathbb{Z}_{149}$.

► **Exercice 22 (Exemple dans $\mathbb{C}^*$)** Dans $\mathbb{C}^*$, déterminer l'ordre de $\left(-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)$ et de $\left(-\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right)$.

► **Exercice 23 (Groupes d'ordre pair)** Soit G un groupe fini d'ordre pair. Montrer qu'il existe un élément $x \in G$, $x \neq e$ tel que $x^2 = e$.

► **Exercice 24 (Exemples de calculs d'ordres dans S_n)** Soit S_n l'ensemble des bijections de $\{1, 2, \ldots, n\}$.

1) Combien S_n a-t-il d'éléments ?

2) Soit c la permutation circulaire $k \mapsto k+1$ si $k < n$ et $n \mapsto 1$, et t la transposition qui échange 1 et n. Déterminer l'ordre de c, t, ct et tc.

► **Exercice 25 (Éléments ayant même ordre)**

1) Dans un groupe G, montrer que pour tous éléments a et b :

a) a et a^{-1} ont le même ordre ;

b) a et bab^{-1} ont le même ordre ;

c) ab et ba ont le même ordre.

2) Dans $\mathrm{GL}_2(\mathbb{R})$, déterminer l'ordre des éléments suivants :

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \quad \text{et} \quad AB.$$

► **Exercice 26 (Ordre d'un produit)** Soit G un groupe et a, b deux éléments d'ordres finis dans G tels que $ab = ba$.

1) Montrer que ab est d'ordre fini et que l'ordre de ab divise le ppcm des ordres de a et b.

2) Montrer que si G est abélien, l'ensemble des éléments d'ordre fini de G forme un sous-groupe.

3) Montrer que si les ordres de a et b sont premiers entre eux, l'ordre de ab est égal au ppcm des ordres de a et de b.

► **Exercice 27 (Ordre de x^2)** Soit G un groupe et x un élément d'ordre n dans G. Quel est l'ordre de x^2 ?

► **Exercice 28 (Générateurs d'un groupe cyclique)**

1) Dans un groupe G engendré par un élément a, montrer que tout sous-groupe est engendré par un élément a^m où m est un entier positif.

2) Soit G un groupe cyclique d'ordre n : $G = \{e, a, a^2 \dots a^{n-1}\}$. Montrer que a^k engendre G si, et seulement si, k est premier avec n.

► **Exercice 29 (Ordre de (x, y))** Soient G et H deux groupes et x, y deux éléments d'ordre finis respectivement dans G et H. Quel est l'ordre de (x, y) dans le groupe produit $G \times H$?

Morphismes de groupes

► **Exercice 30 (Homomorphismes classiques de groupes)**

1) Les applications suivantes sont-elles des morphismes de groupes ?

a) $\exp : (\mathbb{R}, +) \to (\mathbb{R}^*, \times)$;

b) $\ln : (\mathbb{R}_+^*, \times) \to (\mathbb{R}, +)$;

c) $\det : (\mathrm{Gl}_n(\mathbb{C}), \circ) \to (\mathbb{C}^*, \times)$.

d) $f : (\mathbb{R}, +) \to (\mathbb{R}, +)$, $f(x) = x^2$.

e) $g : (\mathbb{R}^*, \times) \to (\mathbb{R}^*, \times)$, $g(x) = x^2$.

f) $h : (\mathbb{R}^*, \times) \to (\mathbb{R}^*, \times)$, $h(x) = x^3$.

2) Peut-on parler d'injectivité, de surjectivité, d'image, de noyau en ce qui concerne ces applications ? Si oui, les décrire. Donner les inverses de celles qui sont bijectives.

► **Exercice 31 (Rotations vectorielles planes)** Soit P un plan vectoriel euclidien et $\mathrm{SO}(P)$ l'ensemble des isométries directes de P. Montrer que les trois groupes $(S^1, \times)$, $(\mathrm{SO}(2), \cdot)$ et $(\mathrm{SO}(P), \circ)$ sont isomorphes.

► **Exercice 32 (Morphismes et ordres)**

1) Soit $\varphi : G \to G'$ un morphisme de groupes et x un élément d'ordre n dans G.

a) Montrer que $\varphi(x)$ est d'ordre fini, et que son ordre divise n.

b) Montrer que si φ est injectif, l'ordre de $\varphi(x)$ est égal à n.

2) Combien existe-t-il de morphismes de $\mathbb{Z}/5\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$? De $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$?

3) Les groupes $\mathbb{Z}/8\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ et $(\mathbb{Z}/2\mathbb{Z})^3$ sont-ils deux à deux isomorphes ?

4) Combien y a-t-il de morphismes de groupes de S_3 dans $\mathbb{Z}_{45}$? Et de $\mathbb{Z}_{45}$ dans S_3 ?

► **Exercice 33 (Restriction d'un morphisme)** Soient G et K deux groupes, H un sous-groupe de G et $f : G \to K$ un morphisme de groupes.

1) Déterminer le noyau de la restriction de f à H.

2) On suppose que f est surjectif. Donner une condition nécessaire et suffisante pour que la restriction de f à H soit injective (resp. surjective, bijective).

► **Exercice 34 (Groupe des automorphismes)** Soit G un groupe. On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G, c'est-à-dire l'ensemble des morphismes bijectifs de G dans lui-même. Montrer que $\mathrm{Aut}(G)$ est un groupe pour la composition des applications.

► **Exercice 35 (Un exemple d'isomorphisme)** Soit G le produit direct de $(\mathbb{R}_+^*, \times)$ avec $(\{-1, 1\}, \times)$. Montrer que G est isomorphe à $(\mathbb{R}^*, \times)$.

► **Exercice 36 (Endomorphismes d'un groupe cyclique)** Soit G un groupe cyclique engendré par un élément g. On note $\mathrm{End}(G)$ l'ensemble des endomorphismes de G (*i.e.* l'ensemble des morphismes de groupes de G dans lui-même).

1) Montrer que l'application $\Psi : \mathrm{End}(G) \to G$ définie par $\Psi(\varphi) = \varphi(g)$ est une bijection.

2) On rappelle que $\mathrm{Aut}(G)$, l'ensemble des automorphismes de G, est un groupe pour la composition des applications.

a) Soit $\varphi \in \mathrm{End}(G)$. Montrer que $\varphi \in \mathrm{Aut}(G)$ si, et seulement si, $\varphi(g)$ est un générateur de G.

b) Déterminer le groupe $\mathrm{Aut}(\mathbb{Z})$.

► **Exercice 37 (Morphismes et éléments d'ordre 2)** Soit $\varphi : G \to H$ un morphisme de groupes. On suppose que G est engendré par des éléments d'ordre 2 et que H est fini, d'ordre impair. Montrer que φ est trivial. Donner un exemple de tels groupes G et H.

► **Exercice 38 (Un isomorphisme inattendu)** On note G l'ensemble $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ et on définit sur G la loi de composition suivante :

$$(a, x) * (b, y) = \begin{cases} (\bar{0}, x + y - 1) & \text{si } a = b = \bar{1}, \\ (a + b, x + y) & \text{sinon.} \end{cases}$$

1) Montrer que cette loi fait de G un groupe abélien.

2) Montrer que $(G, *)$ est isomorphe à $(\mathbb{Z}, +)$.

Théorème de Lagrange

► **Exercice 39 (Groupes d'ordre premier)**

1) Soit G un groupe fini d'ordre p premier. Combien G a-t-il de sous-groupes ? Que peut-on en déduire ?

2) Soit G un groupe n'admettant aucun sous-groupe non trivial ; montrer que G est fini et que son ordre est premier.

3) En déduire que si G est un groupe d'ordre p^n alors G contient un sous-groupe d'ordre p.

► **Exercice 40 (Petit théorème de Fermat)** Soit p un nombre premier.

1) Montrer que pour tout nombre entier a premier avec p, l'entier $a^{p-1} - 1$ est divisible par p.

2) Montrer que pour tout entier relatif a, $a^p \equiv a \mod p$.

► **Exercice 41 (Intersection de sous-groupes)**

1) Soient S_1 et S_2 deux sous-groupes finis d'un groupe G d'ordres respectifs n_1 et n_2. Montrer que si n_1 est premier avec n_2 alors $S_1 \cap S_2 = \{e\}$.

2) Montrer que si deux éléments d'un groupe ont des ordres finis premiers entre eux, l'intersection des sous-groupes qu'ils engendrent est réduite au singleton $\{1\}$.

3) Soient H_1 et H_2 deux sous-groupes d'un groupe G. On suppose que H_1 et H_2 sont de même ordre p premier. Montrer que $H_1 = H_2$ ou $H_1 \cap H_2 = \{1\}$.

4) Montrer que tout groupe abélien d'ordre 77 est cyclique.

► **Exercice 42 (Groupes d'ordre 6)** Soit G un groupe d'ordre 6.

1) Quels sont les ordres possibles des éléments de G ? À quelle condition G est-il cyclique ?

2) Montrer qu'il existe un élément d'ordre 3 dans G.

3) On suppose que G n'est pas cyclique. On considère un élément a d'ordre 3 et un élément b qui n'appartient pas au sous-groupe engendré a. Montrer que l'on a $G = \{e, a, a^2, b, ab, a^2b\}$. En déduire $b^2 = e$ puis la table de G. Montrer que G est isomorphe à S_3.

EXERCICES D'ENTRAÎNEMENT

► **Exercice 43 (Groupe ou pas groupe ?)** Pour chaque loi de composition interne définie ci-dessous, déterminer si elle munit l'ensemble considéré d'une structure de groupe. Dans l'affirmative, donner l'élément neutre et le symétrique d'un élément x ; dans le cas contraire, préciser quel axiome est en défaut.

1) $x * y = \min\{x, y\}$ sur $\mathbb{Z}$;

2) $x * y = \max\{x, y\}$ sur $\mathbb{Z}$;

3) $x * y = \frac{1}{x} + \frac{1}{y}$ sur $\mathbb{Q}_+^*$;

4) $x * y = xy + 1$ sur $\mathbb{R}^*$;

5) multiplication matricielle sur $\left\{ \left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right) / x, y \in \mathbb{R} \right\}$;

6) $x * y = 2^{xy}$ sur $\mathbb{N}^*$;

7) $x * y = x^y$ sur $\mathbb{N}^*$;

8) $A * B = A \cap B$ sur $\mathcal{P}(E)$, l'ensemble des parties d'un ensemble E ;

9) $A * B = A \cup B$ sur $\mathcal{P}(E)$, l'ensemble des parties d'un ensemble E.

► **Exercice 44 (Exemples de calculs dans un groupe)**

1) Soient a et b deux éléments d'un groupe G et $n \in \mathbb{Z}$. Montrer que $(aba^{-1})^n = ab^na^{-1}$.

2) Soit trois éléments x, y et z d'un groupe vérifiant $xyz = e$. Que peut-on dire de yzx ? Et de yxz ?

3) Soit G un groupe tel que, pour tous g et h dans G, on ait $(gh)^{-1} = g^{-1}h^{-1}$. Montrer que G est commutatif.

4) Soient a et b deux éléments d'un groupe G. Montrer que si $(ab)^2 = a^2b^2$, alors a et b commutent.

5) (Difficile) A-t-on le même résultat si l'on suppose que a et b vérifient $(ab)^3 = a^3b^3$?

► **Exercice 45 (Une l.c.i. sur $\mathbb{Q}^*$)** On définit sur $\mathbb{Q}^*$ une loi de composition interne par $a \bullet b = \frac{ab}{2}$. Montrer $(\mathbb{Q}^*, \bullet)$ est un groupe abélien.

► **Exercice 46 (Similitudes directes du plan)** Pour $(\alpha, \beta) \in \mathbb{C}^* \times \mathbb{C}$, on définit l'application $\tau_{\alpha,\beta} : \mathbb{C} \to \mathbb{C}$ par $\tau_{\alpha,\beta}(z) = \alpha z + \beta$. On considère l'ensemble G de ces applications :

$$G = \{\tau_{\alpha,\beta} \,/\, (\alpha, \beta) \in \mathbb{C}^* \times \mathbb{C}\}.$$

1) Montrer que G est un groupe pour la composition des applications.

2) Pour chacun des sous-ensembles H de G suivants, établir si H est un sous-groupe de G et, dans l'affirmative, s'il est distingué. Dans chaque cas, donner une interprétation géométrique.

a) $H = \{\tau_{\alpha,\beta} \,/\, (\alpha, \beta) \in \mathbb{R}^* \times \mathbb{C}\}$.

b) $H = \{\tau_{1,\beta} \,/\, \beta \in \mathbb{C}\}$.

c) $H = \{\tau_{\alpha,\beta} \,/\, (\alpha, \beta) \in S^1 \times \mathbb{C}\}$.

d) $H = \{\tau_{\alpha,0} \,/\, \alpha \in \mathbb{C}^*\}$.

e) $H = \{\tau_{\alpha,\alpha} \,/\, \alpha \in \mathbb{C}^*\}$.

► **Exercice 47 (Groupe engendré par deux éléments)** Soit G un groupe tel qu'il existe deux éléments a et b dans G vérifiant $G = \langle a, b\rangle$. Montrer que $\langle a\rangle \cap \langle b\rangle$ est un sous-groupe de $Z(G)$, le centre de G.

► **Exercice 48 (Un sous-groupe distingué de cardinal 2 est central)** Soit G un groupe. Soit H un sous-groupe distingué de G tel que $\mathrm{Card}(H) = 2$. Montrer que H est contenu dans le centre de G.

► **Exercice 49 (Exemples de sous-groupes de matrices)** On rappelle que l'ensemble $\mathrm{GL}_n(\mathbb{R})$ des matrices inversibles de taille n à coefficients réels, muni du produit des matrices, est un groupe.

1) Notons $\mathcal{M}_n(\mathbb{Z})$ l'ensemble des matrices carrées de taille n à coefficients dans $\mathbb{Z}$, et $\mathrm{GL}_n(\mathbb{Z}) \subset \mathcal{M}_n(\mathbb{Z})$ le sous-ensemble des matrices dont le déterminant vaut ± 1. Montrer que $\mathrm{GL}_n(\mathbb{Z})$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.

2) Supposons $n \geqslant 2$. On considère le sous-ensemble de $\mathrm{GL}_n(\mathbb{R})$ formé par les matrices inversibles de trace nulle. Est-ce un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$?

3) Supposons $n = 2$. Montrer que la partie $\mathbf{U}$ suivante est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$:

$$\mathbf{U} = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \,/\, x \in \mathbb{R} \right\}.$$

► **Exercice 50 (Groupe cyclique et ordre)** Montrer qu'un groupe fini G d'ordre n est cyclique si, et seulement si, il contient un élément d'ordre n.

► **Exercice 51 (Encore des sous-groupes de matrices)** Soit G, H_1 et H_2 les parties de $\mathcal{M}_2(\mathbb{R})$ définies par

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \,/\, (a, b) \in \mathbb{R} \times \mathbb{R}^* \right\}, \quad H_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \,/\, b \in \mathbb{R}^* \right\} \quad \text{et} \quad H_2 = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \,/\, a \in \mathbb{R} \right\}.$$

1) Montrer que G est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$.

2) Montrer que H_1 est un sous-groupe de G. Y est-il distingué ?

3) Montrer que H_2 est un sous-groupe de G. Y est-il distingué ?

4) On considère les quatre applications f, g, h_1 et h_2 suivantes :

$$f : \left(\begin{array}{ccc} G & \to & \mathbb{R}^* \\ \left(\begin{smallmatrix} 1 & a \\ 0 & b \end{smallmatrix}\right) & \mapsto & b \end{array} \right), \ g : \left(\begin{array}{ccc} G & \to & \mathbb{R} \\ \left(\begin{smallmatrix} 1 & a \\ 0 & b \end{smallmatrix}\right) & \mapsto & a \end{array} \right), \ h_1 : \left(\begin{array}{ccc} \mathbb{R}^* & \to & H_1 \\ b & \mapsto & \left(\begin{smallmatrix} 1 & 0 \\ 0 & b \end{smallmatrix}\right) \end{array} \right), \ \text{et} \ h_2 : \left(\begin{array}{ccc} \mathbb{R} & \to & H_2 \\ a & \mapsto & \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \end{array} \right).$$

Pour chacune de ces applications, dire si c'est un morphisme de groupes ; si tel est le cas, préciser le noyau, l'image et en déduire si c'est un isomorphisme ou non.

► **Exercice 52 (Un exemple d'automorphisme de $\mathbf{GL}_n(\mathbb{R})$)** Montrer que l'application f de $\mathrm{GL}_n(\mathbb{R})$ dans lui-même définie par $f(A) = \left({}^t A\right)^{-1}$ est un automorphisme.

► **Exercice 53 (Le groupe $(\mathbb{Z}/31\mathbb{Z})^*$)**

1) On note comme d'habitude $(\mathbb{Z}/31\mathbb{Z})^*$ la partie de $\mathbb{Z}/31\mathbb{Z}$ constituée des classes d'entiers $\bar{n}$ telles que n ne soit pas un multiple de 31. Pourquoi est-ce un groupe ?

2) Quel peut être l'ordre d'un élément de $(\mathbb{Z}/31\mathbb{Z})^*$? Montrer que ce groupe est cyclique.

► **Exercice 54 (Morphisme et groupe monogène)** Soient G_1 un groupe monogène et $f : G_1 \to G_2$ un morphisme surjectif de groupes. Montrer que G_2 est monogène.

Exercices complémentaires

► **Exercice 55 (Le groupe des parties d'un ensemble)** Soit X un ensemble et $P(X)$ l'ensemble de toutes les parties de X. Pour $A, B \subset X$, on pose $A * B := (A \cup B) \setminus (A \cap B)$.

1) Montrer que $P(X)$ muni de l'opération $*$ est un groupe. Donner l'élément neutre et le symétrique d'un élément A de $P(X)$.

2) Écrire la table de ce groupe lorsque $X = \{1, 2\}$ puis lorsque $X = \{1, 2, 3\}$.

3) Déterminer l'ordre d'un élément A de $P(X)$.

► **Exercice 56 (Le groupe G^X)** Soient X un ensemble non vide et G un groupe. On note G^X l'ensemble des applications de X dans G. Munir G^X d'une structure de groupe.

► **Exercice 57 (Neutre et inverse à gauche)** Soit G un ensemble muni d'une loi $\cdot$ associative telle que

- $*$ il existe un élément neutre à gauche e (*i.e.* $\forall x \in G,\ e \cdot x = x$) ;
- $*$ tout élément possède un inverse à gauche (*i.e.* $\forall x \in G,\ \exists y \in G$ tel que $y \cdot x = e$).

On veut montrer que G est un groupe pour cette loi.

1) Soit $x \in G$ et x^{-1} un inverse à gauche, *i.e.* $x^{-1} \cdot x = e$. Soit $y := x \cdot x^{-1}$. Montrer que $yy = y$. En déduire que x^{-1} est aussi un inverse à droite.

2) Montrer qu'un élément neutre à gauche est aussi un élément neutre à droite.

3) Conclure.

► **Exercice 58 (Solutions d'équations dans un groupe)**

1) Soit G un groupe, $a, b \in G$. Montrer qu'il existe un seul élément x et un seul élément y dans G tels que

$$xa = b \quad \text{et} \quad ay = b.$$

2) Réciproquement, montrer que si $\cdot$ est une loi associative sur un ensemble G telle que pour tous $a, b \in G$, il existe un unique couple $(x, y) \in G^2$ avec

$$x \cdot a = b \quad \text{et} \quad a \cdot y = b,$$

alors G est un groupe.

► **Exercice 59 (Élément dans la table)**

1) Soit G un groupe fini. On considère sa table de multiplication. Montrer que chaque élément x de G figure exactement une fois dans chaque ligne et chaque colonne.

2) Montrer réciproquement que si G est un ensemble tel que la loi définie par une telle table soit associative, alors si tout élément x de G figure exactement une fois dans chaque ligne et chaque colonne, G est un groupe.

► **Exercice 60 (Partie stable par la l.c.i.)** Soit H un sous-ensemble non vide d'un groupe G. Peut-on dire que H est un sous-groupe de G si l'on suppose qu'il est stable par la loi de groupe ? Qu'en est-il si l'on suppose de plus que H est fini ?

► **Exercice 61 (Critère de décomposition en produit direct)**

1) On suppose que H et K sont des sous-groupes d'un groupe G vérifiant les trois propositions suivantes :

(i) Pour tout $x \in H$ et $y \in K$, $xy = yx$;

(ii) $H \cup K$ engendre G ;

(iii) $H \cap K = \{e\}$, où e est l'élément neutre de G.

Soit $f\colon H \times K \to G$ l'application définie par $f\big((x,y)\big) = xy$. Montrer que f est un isomorphisme de groupes.

2) Déduire du 1) que si H et K sont des sous-groupes distingués d'un groupe G vérifiant :

(i) $H \cap K = \{e\}$;

(ii) $H.K = G$ (où $H.K = \{hk \,/\, h \in H$ et $k \in K\}$),

alors le groupe produit $H \times K$ est isomorphe à G.

► **Exercice 62 (Exposant d'un groupe abélien)** Soit G un groupe abélien fini. Si g est un élément de G, on note $\omega(g)$ son ordre. Comme d'habitude, si p et q sont deux nombres entiers, $p \wedge q$ désignera leur PGCD et $p \vee q$ leur PPCM.

1) Jusitifier l'existence d'un plus petit entier naturel n tel que $g^n = 1$ pour tout $g \in G$.

Cet entier est appelé *exposant* de G, et noté $\mathrm{Exp}(G)$.

2) Soient a un élément de G et r un entier naturel. Quel est l'ordre de a^r ?

3) Soient a et b deux éléments de G. Montrer que si $\omega(a) \wedge \omega(b) = 1$, alors $\omega(ab) = \omega(a)\omega(b)$.

4) Pour a et b éléments de G, montrer qu'il existe $g \in G$ tel que $\omega(g) = \omega(a) \vee \omega(b)$.

5) Montrer que $\mathrm{Exp}(G)$ divise $\mathrm{Card}(G)$.

6) Montrer qu'il existe $g \in G$ tel que $\omega(g) = \mathrm{Exp}(G)$. En déduire que si $\mathrm{Exp}(G) = \mathrm{Card}(G)$, alors G est cyclique.

► **Exercice 63 (Sous-groupe de $\mathbb{R}$ engendré par les nombres premiers)** Déterminer le sous-groupe de $(\mathbb{R}^*, \times)$ engendré par les nombres premiers.

► **Exercice 64 (Un sous-groupe de S^1)** Soit l'ensemble $G = \left\{e^{2i\pi x} \,/\, x \in \mathbb{Q}\right\}$.

1) Montrer que G est un sous-groupe de S^1.

2) Montrer que tout élément de G est d'ordre fini.

3) Montrer que pour tout élément g de G et tout entier naturel non nul n, il existe h dans G tel que $g = h^n$ (on dit que G est *divisible*).

► **Exercice 65 (Nombres de Mersenne)** Soit n un entier supérieur à 3.

1) Montrer que si $2^n - 1$ est premier, alors n l'est également.

2) On suppose que n est un nombre premier impair. Soit p un diviseur premier de $2^n - 1$. Montrer que $2n$ divise $p - 1$.
Indication : on pourra considérer l'ordre de 2 dans le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$.

3) L'entier n peut-il être premier sans que $2^n - 1$ le soit ?

► **Exercice 66 (Un exemple de calcul de groupe dérivé)** Soit $G = \left\{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \,/\, (a,b,c) \in \mathbb{R}^3,\ ac \neq 0\right\}$.

1) Montrer que G est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$.

2) Montrer que le groupe dérivé $D(G)$ est égal à $\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \,/\, b \in \mathbb{R}\}$.

► **Exercice 67 (Caractère sur un groupe abélien)**

Si G est un groupe, on appelle *caractère* sur G un morphisme de G dans le groupe multiplicatif $\mathbb{C}^*$. On note $\widehat{G}$ l'ensemble des caractères sur G. On suppose dans cet exercice que G est un groupe abélien.

1) Montrer que $\widehat{G}$ est un groupe abélien.

2) Montrer que si G est fini et φ est un caractère sur G, alors $\varphi(g)$ est une racine de l'unité pour tout $g \in G$.

3) Montrer que si G est fini et g et g' sont deux éléments distincts de G, alors il existe $\varphi \in \widehat{G}$ tel que $\varphi(g) \neq \varphi(g')$.

4) Montrer que si G est fini, alors G et $\widehat{G}$ sont isomorphes.

5) Montrer que si G est fini et $\varphi \in \widehat{G}$, $\varphi \neq 1$, alors $\displaystyle\sum_{g \in G} \varphi(g) = 0$.

► **Exercice 68 (Sous-groupes de $\mathbb{R}$)**

1) Soit G un sous-groupe du groupe additif $(\mathbb{R}, +)$ non réduit à $\{0\}$. On note α la borne inférieure de $G \cap]0; +\infty[$.

a) Montrer que si $\alpha > 0$, alors $G = \alpha\mathbb{Z}$.

b) Montrer que si $\alpha = 0$, alors G est dense dans $\mathbb{R}$.

2) Soit δ un nombre réel strictement positif. Montrer que $G = \{a + b\delta \,/\, (a, b) \in \mathbb{Z}^2\}$ est un sous-groupe additif de $\mathbb{R}$. Montrer que G est dense dans $\mathbb{R}$ si, et seulement si, $\delta \notin \mathbb{Q}$.

3) Montrer que la partie $A = \left\{a + b\sqrt{2} \,/\, (a, b) \in \mathbb{Z}^2\right\}$ est dense dans $\mathbb{R}$.

Feuille 2 : Relations d'équivalence

Relations d'équivalence, ensembles quotient

► **Exercice 1** Dire si les relations suivantes sont réflexives, symétriques, antisymétriques, transitives :

1) $E = \mathbb{N}$ et $x\mathcal{R}y \iff x = -y$;

2) $E = \mathbb{R}$ et $x\mathcal{R}y \iff \cos^2 x + \sin^2 y = 1$;

3) $E = \mathbb{N}$ et $x\mathcal{R}y \iff \exists\, p, q \in \mathbb{N}^*,\ y = px^q$.

Quelles sont, parmi les exemples précédents, les relations d'ordre et les relations d'équivalence ?

► **Exercice 2** On note E l'ensemble des habitants de Loire-Atlantique et on définit deux relations sur E :

- $X\,\mathcal{R}_1\,Y$ si $X = Y$ ou X et Y ont leur résidence principale dans la même commune ;
- $X\,\mathcal{R}_2\,Y$ si $X = Y$ ou X et Y ont la même nationalité.

1) Ces relations sont-elles des relations d'équivalence sur E ? Si oui, décrire les classes d'équivalence et l'ensemble quotient (on notera $\overline{X}$ la classe de l'élément X de E).

2) L'application $f : E/\mathcal{R}_1 \to \mathbb{N}$ qui, à $\overline{X}$, associe l'âge de X, est-elle bien définie ?

3) Même question pour l'application g qui, à $\overline{X}$, associe le nom du maire de la commune de résidence principale de X.

4) Même question pour l'application h qui, à $\overline{X}$, associe le nom du conseiller général du canton où habite X.

► **Exercice 3** Soit E l'ensemble des droites du plan affine euclidien $\mathbb{R}^2$ muni d'un repère orthonormé. On définit sur E la relation $\mathcal{R}$ par

$$D\,\mathcal{R}\,\Delta \quad \text{si} \quad D \text{ et } \Delta \text{ sont parallèles.}$$

1) Montrer que $\mathcal{R}$ est une relation d'équivalence sur E. On notera $\overline{\Delta}$ la classe de la droite Δ.

2) Décrire les différentes classes d'équivalence.

3) On aimerait définir une application $f : E/\mathcal{R} \to \mathbb{R}$ qui, à la classe $\overline{\Delta}$ d'une droite Δ, associerait le coefficient directeur de Δ. Est-ce possible ?

4) Même question avec $g : E/\mathcal{R} \to \mathbb{R}$ qui, à $\overline{\Delta}$, associerait l'abscisse du point d'intersection de Δ avec l'axe des abscisses.

► **Exercice 4** Soit A un point du plan affine euclidien $\mathscr{P}$. On définit sur $\mathscr{P}$ la relation suivante :

$$M \sim N \quad \text{s'il existe une rotation } R \text{ de centre } A \text{ telle que } N = R(M).$$

Montrer que c'est une relation d'équivalence et en décrire les classes.

► **Exercice 5** On définit sur $\mathbb{R}$ la relation $x \sim y$ si $x - y \in \mathbb{Z}$. Montrer que $\sim$ est une relation d'équivalence et que l'ensemble des classes d'équivalence est en bijection avec le cercle unité de $\mathbb{R}^2$.

► **Exercice 6** On définit sur $\mathbb{Z}$ la relation

$$x \sim y \quad \text{si } x \text{ et } y \text{ ont même signe (on considère que le signe de 0 est nul).}$$

1) Montrer que c'est une relation d'équivalence sur $\mathbb{Z}$ et décrire les classes d'équivalence.

2) Montrer que l'on définit une loi de composition interne sur le quotient $\mathbb{Z}/\!\sim$ en posant $\overline{x} \bullet \overline{y} = \overline{xy}$ pour $x, y \in \mathbb{Z}$.

3) Que ce passe-t-il si l'on considère que 0 est positif ? négatif ? à la fois positif et négatif ?

4) Qu'en est-il de la «définition» suivante : $\overline{x} \boxplus \overline{y} = \overline{x + y}$?

► **Exercice 7** On définit sur $\mathbb{R}$ la relation $x\mathcal{R}y$ si $x^2 = y^2$.

1) Montrer que c'est une relation d'équivalence et décrire les classes d'équivalence.

2) Les applications f et g, de $\mathbb{R}/\!\sim$ dans $\mathbb{R}$, données par $f(\overline{x}) = x^6$ et $g(\overline{x}) = x^3$ sont-elles bien définies ?

► **Exercice 8** On note $\mathcal{T}$ l'ensemble de tous les triangles (non plats) du plan affine euclidien. On définit trois relations sur cet ensemble :

- $T\,\mathcal{R}_1\,T'$ s'il existe une bijection affine f telle que $f(T) = T'$;
- $T\,\mathcal{R}_2\,T'$ si T et T' sont semblables, c'est-à-dire qu'il existe une similitude s telle que $s(T) = T'$;
- $T\,\mathcal{R}_3\,T'$ si T et T' sont isométriques, c'est-à-dire qu'il existe une isométrie φ telle que $\varphi(T) = T'$.

Montrer que ce sont trois relations d'équivalence sur $\mathcal{T}$ et en décrire les classes.

► **Exercice 9** Pour $x \in \mathbb{Z}$ et $n \in \mathbb{N}^*$, on note $[x]_n$ la classe de x dans $\mathbb{Z}/n\mathbb{Z}$.
À quelle condition sur n et m dans $\mathbb{N}^*$ l'application $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $[x]_n \mapsto [x]_m$ est-elle bien définie ?

► **Exercice 10** Soit E un ensemble muni d'une loi de composition interne notée $\cdot$ et d'une relation d'équivalence $\mathcal{R}$. On note $[x]$ la classe d'un élément x de E. À quelle condition l'égalité

$$[x] * [y] = [x \cdot y]$$

définit-elle une loi de composition interne $*$ sur $E/\mathcal{R}$?

► **Exercice 11** Soit F un sous-espace vectoriel d'un espace vectoriel E. On définit la relation $x \sim y$ si $x-y \in F$.

1) Montrer que $\sim$ définit une relation d'équivalence sur E dont on note E/F l'ensemble des classes d'équivalence.

2) Montrer que E/F peut être muni d'une structure d'espace vectoriel, déduite de celle de E, telle que la projection canonique $\pi : E \to E/F,\ x \mapsto [x]$ soit une application linéaire.

3) Soit G un espace vectoriel de dimension finie et soit $f : E \to G$ une application linéaire. Soit $F = \ker f$ le noyau de f. Montrer qu'il existe une application linéaire $f' : E/F \to G$ telle que $f = f' \circ \pi$.

Classes à gauche, classes à droite, d'un groupe modulo un sous-groupe

► **Exercice 12** Dans le groupe symétrique S_3, décrire l'ensemble des classes à gauche et l'ensemble des classes à droite modulo le sous-groupe H lorsque :

1) H est le sous-groupe engendré par la transposition $\tau_3 = (1\,2)$;

2) H est le sous-groupe engendré par le 3-cycle $c = (1\,2\,3)$.

► **Exercice 13** Soit G un groupe cyclique d'ordre 12. Montrer qu'il existe un sous-groupe H d'ordre 4 et un seul. Déterminer l'ensemble des classes à gauche G/H.

► **Exercice 14** Soit G le groupe des transformations affines inversibles de $\mathbb{R}$.

1) Montrer qu'un élément de G s'écrit $x \mapsto ax + b,\ (a, b) \in \mathbb{R}^* \times \mathbb{R}$. En déduire une loi de groupe sur $\mathbb{R}^* \times \mathbb{R}$.

2) Montrer que l'ensemble des translations définit un sous-groupe H de G. Décrire les classes à gauche et à droite. H est-il distingué ? Décrire G/H.

3) Mêmes questions pour l'ensemble des homothéties (on rappelle que l'identité est également considérée comme une homothétie).

► **Exercice 15** Soit H un sous-groupe d'un groupe G.

1) Montrer que si l'ensemble des classes à gauche G/H a deux éléments, alors H est distingué dans G.

2) En déduire que si G est d'ordre $2n$, tout sous-groupe d'ordre n est distingué. Donner des exemples .

Exercices d'entraînement

► **Exercice 16** On note X l'ensemble des élèves d'un même collège. On définit sur X la relation

$$A \sim B \quad \text{si } A \text{ et } B \text{ sont dans la même classe.}$$

1) Montrer que l'on définit ainsi une relation d'équivalence sur X. Décrire les différentes classes d'équivalence ainsi que l'ensemble quotient $X/\!\sim$.

2) L'application $f : X/\!\sim \to \mathbb{R}$ qui, à $\overline{A}$, associe la note de A au dernier devoir de français, est-elle bien définie ?

3) Même question pour l'application g qui, à $\overline{A}$, associe le nom du professeur de mathématiques de A.

► **Exercice 17** Sur l'ensemble E des droites du plan affine euclidien, on définit la relation

$$D \,\mathcal{R}\, \Delta \quad \text{si} \quad D \text{ et } \Delta \text{ sont perpendiculaires.}$$

Est-ce une relation d'équivalence ?

► **Exercice 18 (Relation d'équivalence et fonction)** On définit sur $\mathbb{R}$ la relation $\mathcal{R}$ par

$$x\mathcal{R}y \ \text{ si } \ x^2 - y^2 = x - y.$$

1) Montrer que $\mathcal{R}$ est une relation d'équivalence.

2) Calculer la classe d'équivalence d'un élément x de $\mathbb{R}$. Combien y a-t-il d'éléments dans cette classe ?

► **Exercice 19** Soit $\mathcal{R}$ la relation sur $\mathbb{N}^2$ définie par : $(a,b)\mathcal{R}(c,d)$ si $a^2 + b^2 = c^2 + d^2$.
1) Montrer que $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{N}^2$.

2) Déterminer les classes d'équivalence de $(0,0)$, $(1,0)$, $(0,1)$ et $(3,4)$.

Exercices complémentaires

► **Exercice 20** On note E l'ensemble des applications continues de $\mathbb{R}$ dans $\mathbb{R}$ admettant une limite finie en $+\infty$. On définit sur E la relation

$$f \sim g \quad \text{si} \quad \frac{f(x)}{g(x)} \xrightarrow[x\to+\infty]{} 1.$$

1) Montrer que c'est une relation d'équivalence.

2) On note $E/\!\sim$ l'ensemble quotient et $\overline{f}$ la classe d'équivalence de f. Les trois applications suivantes sont-elles bien définies ?

$$\Phi : E/\!\sim \to \mathbb{R},\ \Phi(\overline{f}) = \lim_{x\to+\infty} f(x)\,; \qquad \Psi : E/\!\sim \to \mathbb{R},\ \Psi(\overline{f}) = \int_0^1 f(t)\mathrm{d}t\,;$$

$$\xi : E/\!\sim \to \mathbb{R},\ \xi(\overline{f}) = \begin{cases} 1 \text{ si } \int_0^{+\infty} |f(t)|\mathrm{d}t \text{ converge} \\ 0 \text{ sinon.} \end{cases}$$

► **Exercice 21** On définit une relation $\sim$ sur $\mathbb{Z} \times \mathbb{Z}^*$ par $(a,b) \sim (c,d)$ si $ad = bc$.
1) Montrer que $\sim$ est une relation d'équivalence.

2) Déterminer les classes de $(2,5)$, de $(3,1)$ et $(-6,-2)$.

3) On note $[a,b]$ la classe du couple (a,b). Montrer que les deux lois de composition

$$[a,b] \boxplus [c,d] := [ad+bc, bd] \quad \text{ et } \quad [a,b] \bullet [c,d] := [ac, bd]$$

sont bien définies sur l'ensemble quotient $(\mathbb{Z} \times \mathbb{Z}^*)/\!\sim$.

4) Mais que venons-nous de construire ?

► **Exercice 22** Soient E et F deux ensembles non vides munis des relations d'équivalence R et S respectivement.
1) Soit T la relation sur $E \times F$ définie par $(x,y)T(x',y')$ si xRx' et ySy'. Vérifier que T est une relation d'équivalence.

2) Montrer qu'il existe une bijection entre $(E \times F)/T$ et $(E/R) \times (E/S)$.

► **Exercice 23** Soient E et F deux ensembles, $f : E \to F$ une application et S une relation d'équivalence sur F.
1) Soit R la relation sur E définie par xRx' si $f(x)Sf(x')$. Vérifier que R est une relation d'équivalence.

2) Montrer que si S est l'égalité alors E/R est en bijection avec $f(E)$.

Feuille 3 : Groupes quotients - $\mathbb{Z}/n\mathbb{Z}$

Groupes quotients

► **Exercice 1 (Quotient de $\mathbb{Z}/10\mathbb{Z}$)**

1) Montrer que $H = \{\overline{0}, \overline{5}\}$ est un sous-groupe distingué de $\mathbb{Z}/10\mathbb{Z}$.

2) Décrire les classes à gauche et à droite de $\mathbb{Z}/10\mathbb{Z}$ modulo H.

3) Laquelle de ces classes est-elle le neutre du groupe quotient $(\mathbb{Z}/10\mathbb{Z})/H$?

4) Écrire la table de ce groupe quotient. Montrer qu'il est cyclique et en donner tous les générateurs.

► **Exercice 2 (Un quotient de $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$)** Soient G le groupe produit $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ et H le sous-groupe de G engendré par $\{(\overline{3}, \overline{2})\}$. Écrire la décomposition de G suivant les classes à gauche modulo H. Décrire le groupe quotient G/H.

► **Exercice 3 (Quotient de $\mathbb{C}$ par $\mathbb{R}$)** Montrer que le groupe quotient $\mathbb{C}/\mathbb{R}$ est isomorphe à $\mathbb{R}$.

► **Exercice 4 (Quotient de $\mathbb{Q}$ par $\mathbb{Z}$)** Soit G le groupe $\mathbb{Q}/\mathbb{Z}$. Si $q \in \mathbb{Q}$, on note $\mathrm{cl}(q)$ la classe de q modulo $\mathbb{Z}$.

1) Montrer que $\mathrm{cl}(\frac{35}{6}) = \mathrm{cl}(\frac{5}{6})$ et déterminer l'ordre de $\mathrm{cl}(\frac{35}{6})$.

2) Montrer que si $x \in G$, il existe un unique $\alpha \in \mathbb{Q} \cap [0, 1[$ tel que $x = \mathrm{cl}(\alpha)$.

3) Montrer que tout élément de G est d'ordre fini et qu'il existe des éléments d'ordre arbitraire.

4) Quel est le cardinal de $\mathbb{Q}/\mathbb{Z}$?

5) Soit $n \in \mathbb{N}^*$. Montrer qu'il existe dans $\mathbb{Q}/\mathbb{Z}$ un et un seul sous-groupe de cardinal n et décrire ce sous-groupe.

6) Déterminer tous les morphismes de $\mathbb{Q}/\mathbb{Z}$ dans $\mathbb{Z}$.

► **Exercice 5 (Quotient de $\mathbb{R}^*$ par $\mathbb{R}_+^*$)** Décrire le groupe quotient $\mathbb{R}^*/\mathbb{R}_+^*$.

► **Exercice 6 (Un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$)** Soit G le sous-groupe de $\mathrm{GL}_2(\mathbb{R})$ engendré par les matrices $A = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

1) Soit H le sous-groupe de G engendré par AB. Calculer $\mathrm{Card}(H)$.

2) Montrer que H est distingué dans G. Calculer le quotient G/H ; en déduire $\mathrm{Card}(G)$.

► **Exercice 7 (Quotients de $\mathbb{Z} \times \mathbb{Z}$)**

1) a) Montrer que l'application $f : \mathbb{Z}^2 \to \mathbb{Z}$, $(x, y) \mapsto 3x + 6y$ est un morphisme de groupes.

b) Déterminer le noyau $\ker f$ de f et montrer qu'il n'existe pas de couple $(p, q) \in \mathbb{Z}^2$ tel que $\ker f = p\mathbb{Z} \times q\mathbb{Z}$.

c) Montrer que le groupe quotient $\mathbb{Z}^2/\mathbb{Z}(-2, 1)$ est isomorphe à $\mathbb{Z}$.

2) Soit G le sous-groupe de $\mathbb{Z}^2$ engendré par $(2, 0)$ et $(0, 2)$. Montrer que le groupe quotient $\mathbb{Z}^2/G$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

► **Exercice 8 (Quotient du groupe affine par les translations)** On note $\mathcal{T}$ le sous-groupe des translations du groupe affine $\mathrm{GA}(\mathscr{E})$ d'un espace affine $\mathscr{E}$. Montrer que $\mathcal{T}$ est un sous-groupe distingué de $\mathrm{GA}(\mathscr{E})$ et identifier le groupe quotient $\mathrm{GA}(\mathscr{E})/\mathcal{T}$.

► **Exercice 9 (Un sous-groupe de $\mathbf{GL_2(\mathbb{C})}$)** On considère les deux parties G et H suivantes de $\mathcal{M}_2(\mathbb{C})$:

$$G = \left\{ \begin{pmatrix} x & 0 \\ y & x^{-1} \end{pmatrix} / \, x \in \mathbb{C}^*, \ y \in \mathbb{C} \right\} \quad \text{et} \quad H = \left\{ \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} / \, y \in \mathbb{C} \right\}.$$

1) Montrer que G est un sous-groupe de $\mathrm{GL}_2(\mathbb{C})$.

2) Montrer que H est un sous-groupe distingué de G.

3) Déterminer le groupe quotient G/H.

► **Exercice 10 (Deux quotients de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$)** On note G le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Si x est un entier relatif, $\bar{x}^n$ désignera la classe de x dans $\mathbb{Z}/n\mathbb{Z}$.

1) Pourquoi G n'est-il pas cyclique ?

2) Soit α et β les deux éléments de G donnés par

$$\alpha = \left(\bar{1}^2, \bar{0}^4\right) \quad \text{et} \quad \beta = \left(\bar{0}^2, \bar{2}^4\right),$$

et H (resp. K) le sous-groupe de G engendré par α (resp. β).

a) Quel est l'ordre de H ? de K ? En déduire que H et K sont isomorphes.

b) Pourquoi H et K sont-ils distingués dans G ? Déterminer le cardinal des deux groupes quotients G/H et G/K.

c) Donner la liste des éléments de G/H et G/K ainsi que leurs ordres.

d) Ces deux groupes quotients sont-ils isomorphes ?

► **Exercice 11 (Sous-groupe de A_4)** On considère la partie H de A_4 donnée par

$$H = \left\{ \mathrm{Id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3) \right\}.$$

1) Montrer que H est un sous-groupe distingué de A_4.

2) Écrire la table du groupe quotient A_4/H et identifier ce groupe quotient.

3) Mêmes questions avec S_4 : montrer que H est distingué dans S_4 et identifier le quotient.
(On pourra faire agir S_4 sur l'ensemble des doubles transpositions pour construire un morphisme de S_4 vers S_3.)

► **Exercice 12 (Où l'on quotiente pour arriver au point de départ)**
On note G l'ensemble des racines de l'unité de $\mathbb{C}$:

$$G = \left\{ z \in \mathbb{C} \, / \, \exists n \in \mathbb{N}^*, \ z^n = 1 \right\},$$

et on considère un entier naturel non nul p.

1) Montrer que G est un sous-groupe de S^1.

2) Montrer que l'application $\varphi : G \to G$, $z \mapsto z^p$, est un morphisme de groupes. Déterminer son noyau et son image.

3) Montrer qu'il existe un sous-groupe distingué non trivial H dans G tel que le groupe quotient G/H soit isomorphe à G.

► **Exercice 13 (Automorphismes intérieurs)** Soit G un groupe.

1) Soit $\mathrm{Aut}(G)$ l'ensemble des morphismes bijectifs de G sur lui-même (automorphismes). Montrer que $\mathrm{Aut}(G)$ est un sous-groupe du groupe des bijections de G.

2) Soit $g \in G$. Montrer que l'application $ad_g : G \to G$ qui, à x, associe gxg^{-1}, appartient à $\mathrm{Aut}(G)$. Ces automorphismes sont dits intérieurs et on note $\mathrm{Int}(G)$ l'ensemble des automorphismes intérieurs.

3) Montrer que l'application $g \mapsto ad_g$ est un morphisme de G dans $\mathrm{Aut}(G)$. Quels sont son image et son noyau ?

4) Montrer que $\mathrm{Int}(G)$ est un sous-groupe distingué de $\mathrm{Aut}(G)$ isomorphe à $G/Z(G)$ (où $Z(G)$ désigne le centre de G).

► **Exercice 14 (Commutateurs)** Dans un groupe G, on appelle commutateur un élément qui s'écrit $xyx^{-1}y^{-1}$ avec $(x, y) \in G^2$, et on note C l'ensemble des commutateurs.

1) Comment appelle-t-on un groupe tel que $C = \{e\}$?

2) On note $D(G)$ (ou parfois $[G, G]$) le sous-groupe de G engendré par C. Montrer qu'un élément z de $D(G)$ s'écrit comme un produit fini de commutateurs.

3) Montrer que $D(G)$ est un sous-groupe distingué de G et que le groupe quotient $G/D(G)$ est abélien.

4) Soit H un sous-groupe de G tel que $D(G) \subset H$. Montrer que H est distingué dans G.

5) Soit H un sous-groupe distingué de G. Montrer que G/H est abélien si, et seulement si, $D(G) \subset H$. Montrer que, en particulier, $D(G)$ est le plus petit sous-groupe distingué H de G tel que G/H soit commutatif.

6) On rappelle que $\mathcal{S}_3$ est le groupe des permutations de 3 éléments.

a) Montrer que $D(\mathcal{S}_3)$ est inclus dans le groupe alterné $\mathcal{A}_3$.

b) Quel est le cardinal de $\mathcal{A}_3$? Décrire les éléments de $\mathcal{A}_3$.

c) Écrire le 3-cycle $(1\,2\,3)$ comme produit de deux transpositions. En déduire qu'il existe une transposition τ et un élément σ de $\mathcal{S}_3$ tels que $(1\,2\,3) = \tau\sigma\tau^{-1}\sigma^{-1}$.

d) Déterminer le groupe des commutateurs de $\mathcal{S}_3$.

e) Plus généralement, déterminer le groupe des commutateurs de $\mathcal{S}_n$, le groupe des permutations de n éléments.

► **Exercice 15 (Quotient par le centre)**

1) Montrer que le centre $Z(G)$ d'un groupe G est un sous-groupe distingué de G.

2) Montrer que le groupe quotient $G/Z(G)$ ne peut pas être cyclique.

3) En déduire que tout groupe d'ordre p^2, avec p premier, est commutatif.

4) Montrer que tout groupe d'ordre p^α, avec p premier et $\alpha > 1$, admet au moins un sous-groupe distingué d'ordre p et un sous-groupe distingué d'indice p.

► **Exercice 16 (Tout élément est d'exposant 2)** Soit G un groupe tel que $g^2 = 1$ pour tout $g \in G$. Montrer que G est abélien. Montrer que si G est fini, l'ordre de G est une puissance de 2.

► **Exercice 17 (Sous-groupe distingué d'indice 2)**

1) Soient G un groupe fini et H un sous-groupe distingué d'indice 2 dans G. Montrer que pour tout élément g de G, g^2 appartient à H.

2) a) Montrer que pour tout 3-cycle c de S_n, il existe $\sigma \in A_n$ tel que $c = \sigma^2$.

b) En déduire qu'il n'existe pas de sous-groupe d'ordre 6 dans A_4.

► **Exercice 18 (Quotient d'un produit)** Soient G_1 et G_2 deux groupes, H_1 (resp. H_2) un sous-groupe distingué de G_1 (resp. G_2).

1) Montrer que $H_1 \times H_2$ est un sous-groupe distingué dans $G_1 \times G_2$.

2) Montrer que $(G_1 \times G_2)/(H_1 \times H_2)$ est isomorphe à $(G_1/H_1) \times (G_2/H_2)$.

Autour des groupes $\mathbb{Z}/n\mathbb{Z}$

► **Exercice 19 (Sous-groupes de $\mathbb{Z}/8\mathbb{Z}$)** Déterminer tous les sous-groupes de $\mathbb{Z}/8\mathbb{Z}$.

► **Exercice 20 (Sous-groupes de $\mathbb{Z}/54\mathbb{Z}$)** Déterminer tous les sous-groupes de $\mathbb{Z}/54\mathbb{Z}$.

► **Exercice 21 (Sous-groupe d'ordre 4 de $\mathbb{Z}/12\mathbb{Z}$; quotient)** Soit G un groupe cyclique d'ordre 12. Montrer qu'il existe un sous-groupe H d'ordre 4 et un seul. Étudier G/H.

► **Exercice 22 (Le groupe $(\mathbb{Z}/8\mathbb{Z})^\times$)** Déterminez l'ensemble $(\mathbb{Z}/8\mathbb{Z})^\times$ des entiers inversibles modulo 8. Rappelez pourquoi c'est un groupe et écrire sa table. Reconnaissez-vous ce groupe ?

► **Exercice 23 (Le groupe $(\mathbb{Z}/13\mathbb{Z})^\times$)** Déterminer l'ensemble $(\mathbb{Z}/13\mathbb{Z})^\times$ des entiers inversibles modulo 13. Rappeler pourquoi c'est un groupe. Déterminer l'ordre de $\overline{2}$ dans ce groupe. Qu'en déduisez-vous ?

► **Exercice 24 (Cyclique ou pas cyclique ?)** Les groupes suivants sont-ils cycliques :

$$\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \text{ ?} \qquad \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/31\mathbb{Z} \text{ ?}$$

► **Exercice 25** Résoudre dans $\mathbb{Z}/37\mathbb{Z}$:

1) $\begin{cases} \bar{3}\,x + \bar{7}\,y = \bar{3} \\ \bar{6}\,x - \bar{7}\,y = \bar{0}. \end{cases}$

2) $x^2 - \overline{31}\,x + \overline{18} = \bar{0}$.

3) $x^2 + x + \overline{5} = \bar{0}$.

► **Exercice 26** Des astronomes observent, depuis un lieu A, les mouvements de deux planètes. Ils ont constaté que la première planète passe à la verticale de A tous les 567 jours, la seconde tous les 125 jours. Sachant que la première planète est passée à la verticale de A le 2 janvier 460 et la seconde le 5 janvier 460, calculer combien de jours se sont écoulés entre le premier janvier 460 et le jour où les deux planètes sont passées ensemble à la verticale de A.

Premiers exercices de synthèse

► **Exercice 27 (Groupe cyclique d'ordre 315)**

1) Dans un groupe G, dont la loi est notée multiplicativement, on suppose qu'il existe un élément g d'ordre $315 = 5 \times 7 \times 9$. Quel est l'ordre de g^5 ?

Dans la suite, G est un groupe cyclique d'ordre 315 et a un générateur de G.

2) Donner trois exemples de tels groupes G.

3) Quel est l'ordre de a^2 dans le groupe G ? l'ordre de a^{10} ?

4) On note H le sous-groupe de G engendré par a^{10}.

a) Rappeler pourquoi H est distingué dans G. Le groupe quotient G/H est-il cyclique ?

b) Donner l'ordre des classes de a^2 et a^{49} dans le groupe quotient G/H.

5) On note K le sous-groupe de G engendré par a^{90}.

a) Parmi les deux groupes

$$\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/45\mathbb{Z},$$

lequel est isomorphe au groupe quotient G/K ?

b) Donner l'ordre des classes de a^2 et a^{49} dans le groupe quotient G/K.

c) Combien le groupe G/K a-t-il de sous-groupes ?

▶ **Exercice 28 (Groupes d'ordre 8)**

1) On note $\mathbb{Q}_8$ le sous-groupe de $\mathrm{GL}_2(\mathbb{C})$ engendré par les trois matrices U, V et W suivantes :

$$U = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \quad V = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad W = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

On pourra, sans les démontrer, utiliser les égalités suivantes :

$$UV = -VU = W, \; VW = -WV = U, \; WU = -UW = V, \; U^2 = V^2 = W^2 = -I,$$

où I désigne la matrice $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

a) Montrer que $\mathbb{Q}_8 = \{I, -I, U, -U, V, -V, W, -W\}$.

b) Écrire la table de ce groupe.

c) Donner un système de générateurs à deux éléments de $\mathbb{Q}_8$.

d) Le groupe $\mathbb{Q}_8$ est-il commutatif ? cyclique ?

e) Donner les ordres de tous les éléments de $\mathbb{Q}_8$.

f) Déterminer le centre $Z(\mathbb{Q}_8)$ de $\mathbb{Q}_8$ ainsi que le groupe quotient $\mathbb{Q}_8/Z(\mathbb{Q}_8)$.

g) Calculer les commutateurs $[U, V]$, $[V, W]$ et $[W, U]$. En déduire le groupe des commutateurs $D(\mathbb{Q}_8)$ et le quotient $\mathbb{Q}_8/D(Q_8)$.

h) Décrire tous les sous-groupes de $\mathbb{Q}_8$ et montrer qu'ils sont tous distingués dans $\mathbb{Q}_8$.

2) Dans le plan affine euclidien $\mathscr{P}$, on considère un carré $\mathscr{C}$ de sommets A_1, A_2, A_3, A_4 et de centre Ω. On note D_4 l'ensemble des isométries du plan laissant globalement invariant $\mathscr{C}$ et $D_4^+ = D_4 \cap Is^+(\mathscr{P})$ l'ensemble des déplacements de G.

a) Montrer que D_4 est un sous-groupe de $\mathrm{Is}(\mathscr{P})$.

b) Montrer que tout élément de D_4 admet Ω comme point fixe.

c) Quel est l'indice de D_4^+ dans D_4 ?

d) *i)* Montrer que D_4 a au plus huit éléments.

ii) En donnant une liste exhaustive des éléments de D_4, montrer que G est de cardinal huit.

iii) Écrire la table de D_4.

iv) Montrer que D_4^+ est cyclique.

e) Déterminer le centre de D_4 et le quotient $D_4/Z(D_4)$.

f) Déterminer le groupe des commutateurs $D(D_4)$ et le quotient $D_4/D(D_4)$.

g) Le groupe $\mathbb{Q}_8$ du **1**) est-il isomorphe à D_4 ?

h) Construire un morphisme injectif de D_4 dans le groupe symétrique S_4 et donner l'image de ce morphisme.

3) Soit G un groupe **non abélien** d'ordre 8 et d'élément neutre e.

a) Montrer que G contient au moins un élément d'ordre 4.

b) Si a est un tel élément et N le sous-groupe de G engendré par a, montrer que N est distingué dans G.

c) Soit b un élément de $G \setminus N$.

i) Montrer que G est engendré par $\{a, b\}$.

ii) Montrer que $b^2 \in \{e, a^2\}$.

iii) Quels sont les éléments d'ordre 4 de N ? Montrer que $bab^{-1} = a^{-1}$.

d) On suppose qu'il existe $b \in G \setminus N$ tel que $b^2 = e$.

i) Montrer que $G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$.

ii) Écrire la table de G et montrer que G est isomorphe à D_4.

e) On suppose à présent que tout élément b de $G \setminus N$ vérifie $b^2 = a^2$. Montrer que G est alors isomorphe à $\mathbb{Q}_8$.

4) Soit G un groupe **abélien** d'ordre 8.

a) Que peut-on dire s'il existe dans G un élément d'ordre 8 ?

b) On suppose qu'il n'existe pas d'élément d'ordre 8 dans G, mais qu'il existe un élément a d'ordre 4. On note H le sous-groupe de G engendré par a.

i) Montrer qu'il existe $b \in G \setminus H$ d'ordre 2 (raisonner par l'absurde et considérer a^2b^2).

ii) Montrer que G est isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

c) On suppose qu'il n'existe pas d'élément d'ordre 4 ou 8 dans G. Montrer que G est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$.

5) Montrer que si G est un groupe d'ordre 8, alors il est isomorphe à l'un des cinq groupes suivants :

$$\mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad (\mathbb{Z}/2\mathbb{Z})^3, \quad \mathbb{Q}_8, \quad D_4.$$

Montrer que ces cinq groupes sont deux à deux non isomorphes.

Exercices d'entraînement

► **Exercice 29 (Quotient d'un groupe monogène)** Montrer que tout quotient d'un groupe monogène est monogène.

► **Exercice 30 (Quotient $\mathbb{R}/\mathbb{Z}$)** Identifier le groupe quotient $\mathbb{R}/\mathbb{Z}$.

► **Exercice 31 (Quotient $\mathrm{GL}_n/\mathrm{SL}_n$)** Montrer que le groupe spécial linéaire $\mathrm{SL}_n(\mathbb{R})$ est distingué dans $\mathrm{GL}_n(\mathbb{R})$ et identifier le groupe quotient $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R})$.

► **Exercice 32 (Quotient $\mathbb{C}^*/S^1$)** Identifier le groupe quotient $\mathbb{C}^*/S^1$ où S^1 est le sous-groupe des nombres complexes de module 1.

► **Exercice 33 (Indice du centre)** Montrer que l'indice du centre d'un groupe n'est jamais un nombre premier.

► **Exercice 34 (Sous-groupe distingué d'indice n)** Soient G un groupe et H un sous-groupe distingué d'indice n dans G. Montrer que pour tout élément g de G, g^n est dans H.

► **Exercice 35 (Automorphisme et quotient)** Soient G un groupe, H un sous-groupe normal de G et f un automorphisme de G.

1) Montrer que $f(H)$ est un sous-groupe normal de G.

2) Montrer que les groupes G/H et $G/f(H)$ sont isomorphes.

► **Exercice 36 (Un quotient de $(\mathbb{Z}/21\mathbb{Z})^\times$)** On note G le groupe multiplicatif $(\mathbb{Z}/21\mathbb{Z})^\times$.

1) Décrire G et en donner le cardinal.

2) Montrer que $H = \{1, 4, 16\}$ est un sous-groupe distingué de G.

3) Décrire et identifier le groupe quotient G/H.

► **Exercice 37 (Inversibles de $\mathbb{Z}/20\mathbb{Z}$)** Déterminer l'ensemble G des inversibles de $\mathbb{Z}/20\mathbb{Z}$. Montrer que $(G, \times)$ est un groupe isomorphe à $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$.

► **Exercice 38 (Sur le groupe $\mathbb{Z}/2004\mathbb{Z}$)** On considère le groupe additif des entiers modulo $2004 = 4 \times 3 \times 167$.

1) Quel est l'ordre de 25 dans le groupe $\mathbb{Z}/2004\mathbb{Z}$?

2) Quel est l'ordre de 100 dans le groupe $\mathbb{Z}/2004\mathbb{Z}$?

Pour un entier positif n, on note $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe multiplicatif formé des classes modulo n, $k+n\mathbb{Z}$, des entiers k premiers avec n. On ne demande pas de démontrer qu'il s'agit d'un groupe.

3) Montrer que l'application diagonale :

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \\ k & \longmapsto & (k+4\mathbb{Z}, k+3\mathbb{Z}) \end{array}$$

induit un isomorphisme de groupes multiplicatifs :

$$(\mathbb{Z}/12\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times \ .$$

4) Déterminer les groupes $(\mathbb{Z}/4\mathbb{Z})^\times$ et $(\mathbb{Z}/3\mathbb{Z})^\times$. Le groupe $(\mathbb{Z}/12\mathbb{Z})^\times$ est-il cyclique ?

5) Quel est l'ordre du groupe $(\mathbb{Z}/167\mathbb{Z})^\times$?

6) En s'inspirant de la question 3, en déduire l'ordre du groupe $(\mathbb{Z}/2004\mathbb{Z})^\times$.

► **Exercice 39 (Réciproque (partielle) au théorème de Lagrange)** Soient G un groupe abélien fini d'ordre n et d un diviseur de n. Le but de cet exercice est de démontrer que G possède au moins un sous-groupe d'ordre d.

1) Soit p un facteur premier de d. Utiliser l'exercice 14 de la feuille 3 pour démontrer qu'il existe dans G un sous-groupe N de cardinal p.

2) Pourquoi N est-il distingué dans G ? Quel est le cardinal du groupe quotient G/N ?

3) Montrer par récurrence que G possède un sous-groupe de cardinal d.

4) Ce résultat subsiste–t-il si on ne suppose pas que G est abélien ?

► **Exercice 40 (Carrés modulo p)** Soit p un nombre premier impair. Comme d'habitude, $\big(\mathbb{Z}/p\mathbb{Z}\big)^\times$ désigne le groupe multiplicatif des éléments inversibles de $\mathbb{Z}/p\mathbb{Z}$. On dira qu'un entier $a \in \mathbb{Z}$ est un carré modulo p s'il existe $b \in \mathbb{Z}$ tel que $a \equiv b^2 \mod p$.

1) Montrer que l'application $\varphi : \big(\mathbb{Z}/p\mathbb{Z}\big)^\times \to \big(\mathbb{Z}/p\mathbb{Z}\big)^\times$ qui, à x, associe x^2, est un morphisme de groupes. Déterminer son noyau et son image et en déduire le nombre de carrés dans $\mathbb{Z}/p\mathbb{Z}$.

2) a) Montrer que $(p-1)! \equiv -1 \mod p$ (théorème de Wilson).

b) Soit $n = \frac{p-1}{2}$ ($n \in \mathbb{N}^*$ puisque p est impair). Montrer que $(p-1)! \equiv (-1)^n (n!)^2 \mod p$.

c) En déduire que si $p \equiv 1 \mod 4$, alors -1 est un carré modulo p.

3) On suppose dans cette question que -1 est un carré modulo p.

a) Montrer que si a est un carré modulo p, il en est de même pour $-a$.

b) En déduire que le nombre de carrés dans $\mathbb{Z}/p\mathbb{Z}$ est impair puis que $p \equiv 1 \mod 4$.

4) Déduire de ce qui précède qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.

► **Exercice 41 (Automorphismes de $\mathbb{Q}_8$)** Le but de cet exercice est de déterminer le groupe des automorphismes du groupe $\mathbb{Q}_8$ étudié à l'exercice 26. Les notations sont donc celles de cet exercice.

1) Montrer que pour tout élément φ de $\mathrm{Aut}(\mathbb{Q}_8)$, on a $\varphi(I) = I$ et $\varphi(-I) = -I$.

2) Montrer qu'un élément φ de $\mathrm{Aut}(\mathbb{Q}_8)$ est déterminé par les images de U et de V. En déduire que $\mathrm{Aut}(\mathbb{Q}_8)$ contient au plus 24 éléments.

3) On considère les sous-ensembles de $\mathcal{P}(\mathbb{Q}_8)$ (l'ensemble des parties de $\mathbb{Q}_8$) suivants :

$$X_1 = \Big\{\{U,V,W\},\{-U,-V,-W\}\Big\}, \quad X_2 = \Big\{\{-U,V,W\},\{U,-V,-W\}\Big\}$$

$$X_3 = \Big\{\{U,-V,W\},\{-U,V,-W\}\Big\} \ \text{ et } \ X_4 = \Big\{\{U,V,-W\},\{-U,-V,W\}\Big\}.$$

a) Montrer qu'un élément φ de $\mathrm{Aut}(\mathbb{Q}_8)$ permute ces quatre parties. En déduire une action de $\mathrm{Aut}(\mathbb{Q}_8)$ sur $X = \{X_1, X_2, X_3, X_4\}$ puis un morphisme f de $\mathrm{Aut}(\mathbb{Q}_8)$ vers le groupe symétrique S_4.

b) Montrer que $\varphi_1 : \mathbb{Q}_8 \to \mathbb{Q}_8$, $\varphi_1(U) = -U$ et $\varphi_1(V) = W$ définit un automorphisme de $\mathbb{Q}_8$.

c) Même question avec $\varphi_2 : \mathbb{Q}_8 \to \mathbb{Q}_8$ donné par $\varphi_2(U) = W$ et $\varphi_2(V) = V$.

d) Déterminer $f(\varphi_1)$ et $f(\varphi_2)$. En déduire que $f : \mathrm{Aut}(\mathbb{Q}_8) \to S_4$ est surjectif.

e) Conclure de ce qui précède que $\mathrm{Aut}(\mathbb{Q}_8)$ est isomorphe au groupe symétrique S_4.

► **Exercice 42 (Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est-il cyclique ?)**
On rappelle que si n est un entier strictement positif, l'ensemble des générateurs du groupe additif $\mathbb{Z}/n\mathbb{Z}$ forme un groupe pour la multiplication, qui est noté $(\mathbb{Z}/n\mathbb{Z})^\times$.

1) Soit d un diviseur d'un entier positif n. Montrer que la surjection canonique $\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ induit un morphisme de groupes $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/d\mathbb{Z})^\times$.

2) Démontrer que cet homomorphisme est surjectif (commencer par le cas où n est une puissance d'un nombre premier).

3) Vérifier que $(\mathbb{Z}/8\mathbb{Z})^\times$ n'est pas cyclique. En déduire que si k est un entier supérieur à 3 alors $(\mathbb{Z}/2^k\mathbb{Z})^\times$ n'est pas cyclique.

4) Soit $G = G_1 \times G_2$ le groupe produit de deux groupes G_1 et G_2 d'ordres respectifs n_1 et n_2. Montrer que l'ordre de tout élément du groupe G divise le *ppcm* de n_1 et n_2. En déduire que si G est cyclique alors n_1 et n_2 sont premiers entre eux.

5) Montrer que si le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique, alors n est égal à l'un des entiers suivants : 1, 2, 4, p^k ou $2p^k$, p étant un nombre premier et k un entier positif non nul. La réciproque est vraie mais on ne demande pas de l'établir.

► **Exercice 43 (Centre du groupe diédral)** Déterminer le centre $Z(D_n)$ du groupe diédral D_n ainsi que le quotient $D_n/Z(D_n)$.

Feuille 4 : Opération d'un groupe sur un ensemble
Groupes symétrique et alterné

Premiers exemples d'actions de groupes

► **Exercice 1 (Quelques exemples)** Pour chacune des actions suivantes, décrire les orbites et les stabilisateurs (et justifier que l'on est bien en présence d'une action).

1) Si E est un espace vectoriel, action du groupe linéaire $\mathrm{GL}(E)$ sur E.

2) Si E est un espace vectoriel euclidien, action du groupe orthogonal $\mathrm{O}(E)$ sur E.

3) Si E est un espace vectoriel et $\mathcal{S}(E)$ l'ensemble des sous-espaces vectoriels de E, action de $\mathrm{GL}(E)$ sur $\mathcal{S}(E)$.

4) Si $\mathscr{E}$ est un espace affine, action du groupe affine $\mathrm{Aff}(\mathscr{E})$ sur $\mathscr{E}$.

5) Si $\mathscr{E}$ est un espace affine euclidien, action du groupe des isométries $\mathrm{Is}(\mathscr{E})$ sur $\mathscr{E}$.

6) L'action de $\mathrm{GL}_n(\mathbb{R}) \times \mathrm{GL}_m(\mathbb{R})$ sur $\mathcal{M}_{n,m}(\mathbb{R})$ donnée par $(P,Q) \cdot M = PMQ^{-1}$.

7) L'action de $\mathrm{GL}_n(\mathbb{C})$ sur $\mathcal{M}_n(\mathbb{C})$ par $P \cdot A = PAP^{-1}$.

► **Exercice 2 (Action de (ℤ/22ℤ)* sur ℤ/22ℤ)** On fait agir le groupe $(\mathbb{Z}/22\mathbb{Z})^*$ par multiplication sur $\mathbb{Z}/22\mathbb{Z}$, c'est-à-dire par l'application

$$\begin{pmatrix} (\mathbb{Z}/22\mathbb{Z})^* \times \mathbb{Z}/22\mathbb{Z} & \to & \mathbb{Z}/22\mathbb{Z} \\ (a,x) & \mapsto & a \cdot x \end{pmatrix}.$$

Décrire les orbites de cette action.

► **Exercice 3 (Une homographie)** Soit $X = \mathbb{C} \setminus \{-1, 0, 1\}$ et $f : X \to X$ définie par $f(z) = \frac{z-1}{z+1}$.

1) Montrer que $f \in S(X)$.

2) Déterminer le cardinal de G, le sous-groupe de $S(X)$ engendré par f.

3) Comment peut-on faire agir naturellement G sur X ? Déterminer l'orbite et le stabilisateur de chacun des éléments de X pour cette action.

► **Exercice 4 (Formes bilinéaires symétriques)** Soit E un espace vectoriel réel. On note $\mathcal{L}_2^s(E)$ l'ensemble des formes bilinéaires symétriques sur E. Pour $u \in \mathrm{GL}(E)$ et $\Phi \in \mathcal{L}_2^s(E)$, on note $u \cdot \Phi$ l'application définie sur $E \times E$ par $(u \cdot \Phi)(x,y) = \Phi\big(u^{-1}(x), u^{-1}(y)\big)$.

1) Montrer que l'on définit ainsi une action du groupe $\mathrm{GL}(E)$ sur $\mathcal{L}_2^s(E)$.

2) Déterminer l'ensemble des orbites pour cette action.

3) Que représente le stabilisateur d'un élément Φ de $\mathcal{L}_2^s(E)$?

► **Exercice 5 (Coniques)** On note $\mathcal{E}$ l'ensemble des coniques non dégénérées du plan affine euclidien $\mathscr{P}$.

1) Montrer que le groupe affine $\mathrm{GA}(\mathscr{P})$ agit sur $\mathcal{E}$.

2) Combien y a-t-il d'orbites pour cette action ? Quelles sont-elles ?

3) Pourquoi le groupe $\mathrm{Is}(\mathscr{P})$ des isométries du plan agit-il sur $\mathcal{E}$? Décrire les orbites pour cette action.

► **Exercice 6 (Caractéristiques des actions de groupes)** On considère une action d'un groupe G sur un ensemble E que l'on notera $(g,x) \mapsto g \cdot x$. On rappelle qu'une telle action est dite :

(i) *transitive* si, pour tout $(x,y) \in E^2$, il existe un élément g de G tel que $y = g \cdot x$;

(ii) *n fois transitive* si, pour tout $(x_1, \dots, x_n)$, $(y_1, \dots, y_n)$ dans E^n tels que $x_i \neq x_j$ et $y_i \neq y_j$ si $i \neq j$, il existe un élément g de G tel que $y_k = g \cdot x_k$ pour tout $k \in [\![1, n]\!]$;

(iii) *libre* si, pour tout x dans E, on a, pour $g \in G$, $(g \cdot x = x) \Longrightarrow g = e_G$;

(iv) *fidèle* si, pour $g \in G$, on a $(g \cdot x = x$ pour tout $x \in E) \Longrightarrow g = e_G$;

(v) *simplement transitive* si, pour tout $(x,y) \in E^2$, il existe un unique élément g de G tel que $y = g \cdot x$.

1) Exprimer ces définitions en termes d'orbites et de stabilisateurs.

2) Illustrer chacune de ces définitions par un exemple.

3) Certaines de ces propriétés en impliquent-elles d'autres ? Si non, donner un contre-exemple (par exemple, une action libre est-elle fidèle ? Si non, donner un exemple d'action libre non fidèle).

► **Exercice 7 (Demi-plan de Poincaré et homographie)**

Soit $\mathcal{P}$ le demi-plan supérieur de $\mathbb{C}$, c'est-à-dire l'ensemble des nombres complexes $z = x + iy$ tels que $y > 0$. Pour tout $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$ et pour tout $z \in \mathcal{P}$, on définit $A \cdot z = \dfrac{az+b}{cz+d}$.

1) Montrer que l'on définit ainsi une action du groupe $\mathrm{SL}_2(\mathbb{R})$ sur $\mathcal{P}$.

2) Montrer que le stabilisateur de i est égal à $\mathrm{SO}(2)$.

3) Interpréter géométriquement l'action d'une matrice de la forme $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. Même question avec une matrice de la forme $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$.

4) Déterminer l'orbite de i sous l'action de $\mathrm{SL}_2(\mathbb{R})$.

5) L'action de $\mathrm{SL}_2(\mathbb{R})$ sur $\mathcal{P}$ est-elle transitive ?

► **Exercice 8 (Normalisateur)** Etant donné un sous-groupe H d'un groupe G, on définit le normalisateur $\mathrm{Nor}_G(H)$ de H dans G comme l'ensemble des éléments $g \in G$ tels que $gHg^{-1} = H$.

1) Montrer que $\mathrm{Nor}_G(H)$ est le plus grand sous-groupe de G contenant H comme sous-groupe distingué.

2) Déterminer $\mathrm{Nor}_G(H)$ dans les cas suivants :

a) G est abélien et H un sous-groupe de G ;

b) $G = S_3$ et $H = \{Id, (1\,2\,3), (1\,3\,2)\}$;

c) $G = S_3$ et $H = \{Id, (1\,2)\}$.

3) Montrer que le nombre de sous-groupes conjugués de H dans G (deux à deux distincts) est égal à l'indice $[G : \mathrm{Nor}_G(H)]$ et qu'en particulier c'est un diviseur de l'ordre de G.

► **Exercice 9 (Intersection des conjugués d'un sous-groupe)** Soit G un groupe et H un sous-groupe d'indice fini n dans G. Montrer que l'intersection H' des conjugués de H par les éléments de G est un sous-groupe distingué de G et d'indice fini dans G. Montrer que c'est le plus grand sous-groupe distingué de G contenu dans H.

Équation aux classes

► **Exercice 10 (Un groupe d'ordre 32 agit sur un ensemble de cardinal 55)** Un groupe G d'ordre 32 agit sur un ensemble X à 55 éléments. Cette action possède 5 orbites. Donner la liste des cardinaux des orbites possibles.

► **Exercice 11 (Un groupe d'ordre 15 agit sur un ensemble de cardinal 17)** Soit G un groupe de cardinal 15 agissant sur un ensemble fini X de cardinal 17. On suppose que toute orbite contient au moins deux éléments. Déterminer le nombre d'orbites et le cardinal de chacune.

► Exercice 12 (Classes de conjugaison - Groupes d'ordre p^α)
Soit G un groupe fini ; on dit que deux éléments x et y de G sont conjugués lorsqu'il existe un élément g de G pour lequel $y = gxg^{-1}$.

1) Vérifier que la relation «x est conjugué à y» est une relation d'équivalence sur G.

2) Montrer que pour $x \in G$, $N(x) = \{g \in G \mid gxg^{-1} = x\}$ est un sous-groupe de G, et que la classe de conjugaison de x est de cardinal $[G : N(x)]$.

3) On suppose que G est d'ordre p^α, avec p premier.

a) Montrer que toutes les classes de conjugaison ont pour cardinal une puissance de p.

b) Montrer que le centre $Z(G)$ est formé des éléments dont la classe de conjugaison est de cardinal 1.

c) Montrer que p divise l'ordre de $Z(G)$ puis que le centre de G n'est pas trivial.

4) Montrer que tout groupe d'ordre p^2, avec p premier, est commutatif.

► Exercice 13 (Angle de deux vecteurs) Soit E un espace vectoriel euclidien orienté de dimension n et S sa sphère unité : $S = \{u \in E \,/\, ||u|| = 1\}$.

1) On suppose dans cette question que $n = 2$.

a) Montrer que le groupe spécial orthogonal $\mathrm{SO}(E)$ agit simplement transitivement sur S, c'est-à-dire que pour tout $(u, v) \in S \times S$, il existe un unique élément f dans $\mathrm{SO}(E)$ tel que $f(u) = v$; on notera $R_{u,v}$ cet élément f dans la suite.

b) Montrer que $\mathrm{SO}(E)$ n'agit pas 2 fois transitivement sur S ; montrer que l'orbite d'un couple (u, v) d'éléments de S sous l'action de $\mathrm{SO}(E)$ est constituée des couples (x, y) vérifiant $R_{x,y} = R_{u,v}$.

c) Donner une définition de la notion d'angle orienté de deux vecteurs unitaires de E ; étendre cette défnition aux couples de vecteurs non nuls de E.

d) Montrer que l'orbite d'un couple (u, v) de $S \times S$ sous l'action du groupe orthogonal $\mathrm{O}(E)$ est l'ensemble des couples (x, y) vérifiant $R_{x,y} \in \{R_{u,v}, R_{u,v}^{-1}\}$. En déduire une définition de la notion d'angle (non orienté) de deux vecteurs non nuls de E.

2) On suppose à présent que $n \geqslant 3$.

a) Montrer que $\mathrm{SO}(E)$ agit transitivement sur S, mais pas simplement transitivement.

b) Montrer que les orbites sous l'action de $\mathrm{SO}(E)$ et $\mathrm{O}(E)$ sur $S \times S$ coïncident. En déduire qu'il n'existe pas de «bonne» notion d'angle orienté de deux vecteurs en dimension au moins 3.

► Exercice 14 (Existence d'un élément d'ordre un facteur premier de l'ordre du groupe)

Soit G un groupe de cardinal fini N $(N > 1)$ de neutre e et soit p un nombre premier. On définit $F = \{(x_1, x_2, \ldots, x_p) \in G^p \,/\, x_1 x_2 \cdots x_p = e\}$. (On pourra traiter le cas $p = 2$ à part.)

1) Calculer le cardinal de F.

2) Montrer que $g(x_1, x_2, \ldots, x_p) = (x_p, x_1, \ldots, x_{p-1})$ définit une bijection g de F sur F. Quel est l'ordre du sous-groupe H (du groupe des bijections de F) engendré par g ?

3) Expliquer rapidement pourquoi le groupe H agit sur F. Que peut-on dire du cardinal d'une orbite ? Quelles sont les orbites à un élément ?

4) Utiliser ce qui précède pour montrer que si p divise N, alors G contient au moins un élément d'ordre p.

► **Exercice 15 (Sous-groupe d'indice le plus petit facteur premier de l'ordre du groupe)**
Soit G un groupe et H un sous-groupe de G. On note G/H l'ensemble des classes à gauche de G modulo H.

1) a) Rappeler ce qu'est l'action de G par translation à gauche sur G/H. Quelles en sont les orbites ?

b) Montrer que le stabilisateur d'un élément gH de G/H est gHg^{-1}.

c) Montrer que le noyau du morphisme $\varphi : G \to S(G/H)$ associé à cette action est égal à $\bigcap\limits_{g\in G} gHg^{-1}$.

d) On restreint cette action de G à H. Après avoir expliqué ce que cela veut dire, déterminer l'orbite de l'élément H de G/H (la classe du neutre) pour cette nouvelle action.

On suppose à présent que G est un groupe fini de cardinal n et que H est d'indice p dans G, où p est le plus petit facteur premier de n.
On se propose de démontrer que H est alors distingué dans G en utilisant l'action de H décrite ci-dessus.

2) a) Si ω est une orbite pour cette action, expliquer pourquoi son cardinal vaut 1 ou est supérieur à p.

b) Écrire l'équation aux classes pour cette action.

c) En déduire que toute les orbites sont réduites à un élément.

d) Conclure.

Groupes symétriques

► **Exercice 16 (Étude d'une permutation)**

1) Décomposer en produit de cycles disjoints la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 5 & 6 & 3 & 10 & 11 & 8 & 7 & 2 & 9 & 4 & 12 & 13 & 1 \end{pmatrix}.$$

2) Déterminer l'ordre et la signature de σ. Calculer σ^{2013}.

3) Calculer σ^{-1} ainsi que son ordre et sa signature.

4) Décomposer σ en produit de transpositions. Peut-on la décomposer en un produit de 3-cycles ?

► **Exercice 17 (Un calcul d'ordre et de signature dans S_n)** Déterminer la signature et l'ordre de la permutation σ donnée par

$$\sigma = (1\,5)(1\,3\,9\,4\,8\,7\,5)(8\,2\,9\,3)(4\,8\,2\,5)(1\,6\,9\,5\,3\,2)(8\,3\,2)(1\,3\,5).$$

Décomposer σ en produit de transpositions et de 3-cycles si cela est possible.

► **Exercice 18 (Une conjugaison dans S_9)** On note σ et τ les permutations données par

$$\sigma = (1\,8\,5\,4)(2\,9)(6\,3\,7) \quad \text{et} \quad \tau = (8\,5\,1\,9\,3)(4\,7).$$

Calculer $\tau\sigma\tau^{-1}$.

► **Exercice 19 (Conjuguées ou pas conjuguées ?)** Dans le groupe symétrique S_9, on considère les permutations σ_1 et σ_2 données par :

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 6 & 7 & 2 & 1 & 4 & 5 & 3 \end{pmatrix} \quad \text{et} \quad \sigma_2 = (1\,9\,6\,4)(2\,8)(3\,7\,5).$$

1) Déterminer l'ordre et la signature de σ_1 et σ_2.

2) Calculer σ_1^{2012}.

3) Les permutations σ_1 et σ_2 sont-elles conjuguées dans S_9 ? Si oui, exhiber un élément f de S_9 tel que $\sigma_2 = f\sigma_1 f^{-1}$. Un tel élément f est-il unique ?

4) Soit σ_3 la permutation définie par $\sigma_3 = (1\,9\,3\,5)(8\,3)(5\,6\,9)$. Les permutations σ_1 et σ_3 sont-elles conjuguées dans S_9 ? Si oui, exhiber un élément g de S_9 tel que $\sigma_3 = g\sigma_1 g^{-1}$. Un tel élément g est-il unique ?

► **Exercice 20 (Générateurs de S_n)** Soit $n \in \mathbb{N}$, $n \geqslant 3$.

1) Montrer que S_n est engendré par $\{(1\,2), (1\,2\,\ldots\,n)\}$.

2) Montrer que S_n est engendré par $\{(1\,2), (2\,3), \ldots, (n-1\,n)\}$.

3) Montrer que S_n est engendré par $\{(1\,2), (2\,\ldots\,n)\}$.

4) Existe-t-il une partie génératrice de S_n formée d'un seul élément ?

► **Exercice 21 (Générateurs de A_n)**

1) Montrer que A_n est engendré par $\{(1\,2\,3), (1\,2\,4), \ldots, (1\,2\,n)\}$.

2) Montrer que le produit de deux transpositions distinctes est un 3-cycle ou un produit de deux 3-cycles. En déduire que A_n est engendré par les 3-cycles.

3) Montrer que tout 3-cycle est un carré. En déduire que le groupe alterné A_n est engendré par les carrés de permutations.

► **Exercice 22 (Nombre de k-cycles)** Compter les cycles d'ordre k dans S_n.

► **Exercice 23 (Un sous-groupe de S_n)** Montrer que l'ensemble $\{\mathrm{Id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ est un groupe pour la composition.

► **Exercice 24 (Botanique de S_3)** Décrire le groupe symétrique S_3 : ordre et signature des éléments, sous-groupes, classes de conjugaison, sous-groupes distingués.

► **Exercice 25 (Botanique de S_4)** Décrire le groupe symétrique S_4 : ordre et signature des éléments, sous-groupes, classes de conjugaison, sous-groupes distingués.

► **Exercice 26 (Une classe de conjugaison dans S_5)**

Déterminer la classe de conjugaison de $(1\,2)(3\,4\,5)$ dans S_5.

► **Exercice 27 (Classe de conjugaison dans S_5 et A_5)**

1) Décrire les classes de conjugaison de S_5.

2) Décrire les classes de conjugaison de A_5.

3) Montrer que A_5 est simple, c'est-à-dire qu'il n'admet pas d'autre sous-groupe distingué que lui-même et $\{\mathrm{Id}\}$.

► **Exercice 28 (Carré ou pas carré ?)**

1) Déterminer toutes les permutations σ de S_4 telles que $\sigma^2 = (1\,2)(3\,4)$.

2) Pour $n \geqslant 2$, existe-t-il une permutation σ dans S_n telle que $\sigma^2 = (1\,2)$?

3) Pour $n \geqslant 6$, existe-t-il une permutation σ dans S_n telle que $\sigma^2 = (1\,2)(3\,4\,5\,6)$?

► **Exercice 29 (Existence d'éléments d'ordre donné dans S_8)** Existe-t-il un élément d'ordre 21 dans S_8 ? d'ordre 9 ? d'ordre 10 ? Si oui, en donner un.

► **Exercice 30 (Élement d'ordre maximal dans S_9)** Déterminer un élément d'ordre maximal dans S_9.

► **Exercice 31 (Permutation d'ordre 14 dans S_{10})** Montrer qu'une permutation de S_{10} d'ordre 14 est impaire. Combien existe-t-il de telles permutations ?

► **Exercice 32 (Sous-groupe distingué contenant une transposition)** Soit H un sous-groupe distingué du groupe symétrique S_n contenant une transposition. Montrer que $H = S_n$.

► **Exercice 33 (Groupe des isométries d'un tétraèdre régulier)**

Montrer que le groupe des isométries de l'espace affine euclidien de dimension 3 qui laissent invariant un tétraèdre régulier de sommets M_1, M_2, M_3, M_4 est isomorphe à S_4 et que le sous-groupe des isométries directes qui laissent invariant le tétraèdre est isomorphe à A_4.

► **Exercice 34 (Plan de table)** On considère n personnes assises autour d'une table ronde.

1) Montrer que l'on peut obtenir n'importe quelle nouvelle disposition autour de la table par échanges successifs de (deux) places.

2) Montrer qu'au bout d'un nombre impair d'échanges successifs de (deux) places, on ne peut pas se retrouver avec la disposition initiale.

► **Exercice 35 (Jeu de cartes)** On bat un paquet de 32 cartes en échangeant les trois cartes du dessus avec les deux cartes du dessous. Au bout de combien d'opérations retrouve-t-on le paquet initial ?

EXERCICES D'ENTRAÎNEMENT

► **Exercice 36 (Exemple d'orbites en géométrie plane)** Soit G un sous-groupe du groupe affine de $\mathbb{R}^2$ et A un point de $\mathbb{R}^2$. Déterminer l'orbite de A sous l'action de G quand G est le sous-groupe engendré par :

1) une symétrie par rapport à une droite ;

2) une rotation d'angle $\frac{\pi}{2}$;

3) une rotation d'angle $\frac{2\pi}{5}$ et une réflexion.

(*Il y a parfois différents cas à considérer.*)

► **Exercice 37 (Un calcul d'ordre et de signature dans S_8)** Décomposer en produit de cycles disjoints la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 4 & 1 & 3 & 8 & 7 & 2 \end{pmatrix}.$$

Déterminer l'ordre et la signature de σ. Calculer σ^{2013}.

► **Exercice 38 (Signature impaire, ordre pair)** Montrer que l'ordre d'une permutation impaire est un nombre pair.

► **Exercice 39 (Permutation d'ordre 10 dans S_8)** Montrer que toute permutation d'ordre 10 dans S_8 est impaire.

► **Exercice 40 (Sous-groupe d'indice 2 dans S_n)** Montrer que A_n est le seul sous-groupe de S_n d'indice 2.

► **Exercice 41 (Un groupe d'ordre 33 agit sur un ensemble de cardinal 19)** Soit G un groupe d'ordre 33 agissant sur un ensemble E de cardinal 19. Montrer qu'il existe au moins une orbite réduite à un élément.

► **Exercice 42 (Deux éléments de même ordre sont conjugués dans un certain groupe)** Soient G un groupe fini et x, y, deux éléments de G de même ordre. Montrer qu'il existe un groupe Γ contenant un sous-groupe isomorphe à G et dans lequel les images de x et y sont conjuguées.

► **Exercice 43 (Conjugaison dans S_5)** Dans S_5, on note c le cycle $(1\,2\,3\,4\,5)$ et σ la permutation définie par

$$\sigma(1) = 4,\ \sigma(2) = 5,\ \sigma(3) = 2,\ \sigma(4) = 3,\ \sigma(5) = 1.$$

1) Montrer que c et σ sont conjugués dans S_5 et expliciter une permutation τ telle que $\sigma = \tau c \tau^{-1}$. Quelle est la signature de τ ?

2) a) Combien existe-t-il de permutations f telles que $c = fcf^{-1}$?

b) Montrer que toutes ces permutations sont paires.

3) Est-ce que c et σ sont conjugués dans le groupe alterné A_5 ?

► **Exercice 44 (Indice dans un groupe d'ordre plus grand que $m!$)** Montrer que pour $m \geqslant 3$, un groupe simple d'ordre $\geqslant m!$ ne peut avoir de sous-groupe d'indice m.
(Indication : étudier l'action du groupe par translation sur l'ensemble quotient des classes modulo le sous-groupe.)

► **Exercice 45 (Un sous-groupe de S_7)** Dans S_7, on considère les deux permutations $\sigma_1 = (2\ 4\ 6)(5\ 7\ 1)$ et $\sigma_2 = (3\ 4)(5\ 6)$ et G le sous-groupe de S_7 engendré par $\{\sigma_1, \sigma_2\}$. Le but de l'exercice est de déterminer le cardinal de G. On considère les ensembles suivants :

$$G_1 = \{\varphi \in G \,/\, \varphi(1) = 1\} \qquad G_2 = \{\varphi \in G_1 \,/\, \varphi(2) = 2\} \qquad G_3 = \{\varphi \in G_2 \,/\, \varphi(3) = 3\}$$

$$X_1 = \{\varphi(1) \,/\, \varphi \in G\} \qquad X_2 = \{\varphi(2) \,/\, \varphi \in G_1\} \qquad X_3 = \{\varphi(3) \,/\, \varphi \in G_2\}$$

1) Montrer que $\mathrm{Card}(G)$ est un multiple de 6.

2) Déterminer $\sigma_1\sigma_2$. En déduire que 42 divise $\mathrm{Card}(G)$.

3) Montrer que $\mathrm{Card}(G) = \mathrm{Card}(X_1) \cdot \mathrm{Card}(X_2) \cdot \mathrm{Card}(X_3) \cdot \mathrm{Card}(G_3)$.

4) Décrire l'ensemble X_1.

5) Montrer que X_3 est l'une des deux parties $\{3, 4, 5, 6\}$ ou $\{3, 4, 5, 6, 7\}$.

6) Montrer que X_2 est l'une des deux parties $\{2, 7\}$ ou $\{2, 3, 4, 5, 6, 7\}$.

7) Pourquoi G agit-il sur l'ensemble des parties de $[\![1, 7]\!]$? Déterminer l'orbite de la partie $\{1, 2, 7\}$ sous cette action.

8) En déduire que 7 est fixé par les éléments de G_2 et que G_3 est réduit à l'identité.

9) Déterminer $\mathrm{Card}(G)$.

► **Exercice 46 (Matrice de permutation)** On considère l'application $S_n \times \mathbb{R}^n \to \mathbb{R}^n$ qui, à $\big(\sigma, (x_1, \dots, x_n)\big)$, associe $(x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)})$.

1) Vérifier que l'on définit ainsi une action de S_n sur $\mathbb{R}^n$.

2) Montrer que le morphisme $\varphi : S_n \to S(\mathbb{R}^n)$ est à valeurs dans $\mathrm{GL}(\mathbb{R}^n)$.

3) On note $P(\sigma)$ la matrice de $\varphi(\sigma)$ dans la base canonique. Montrer que $\det P(\sigma) = \varepsilon(\sigma)$.

Feuille 5 : Géométrie - Problèmes de synthèse

Espaces affines - Barycentre

► **Exercice 1 (Sous-espace affine de $\mathbb{R}^3$)**

Soit $\mathscr{E} = \{(x,y,z) \in \mathbb{R}^3 \,/\, z = 1\}$. Démontrer que $\mathcal{E}$ est un espace affine ; calculer sa dimension.

► **Exercice 2 (Espaces affines de matrices)**

1) Démontrer que $\mathscr{E} = \left\{ \begin{pmatrix} 1+2a-b & 0 \\ 2-a-b & a-b \end{pmatrix} ;\ (a,b) \in \mathbb{R}^2 \right\}$ est un sous-espace affine de $\mathcal{M}_2(\mathbb{R})$; en déterminer un point et la direction.

2) Montrer que $\mathscr{F} = \left\{ \begin{pmatrix} 19+3a & 5 \\ 4 & 13+2a \end{pmatrix} ;\ a \in \mathbb{R} \right\}$ est un sous-espace affine de $\mathcal{M}_2(\mathbb{R})$. Que peut-on dire de $\mathscr{E}$ et $\mathscr{F}$?

► **Exercice 3 (Espace affine d'applications)** Montrer que $\mathscr{F} = \{ f \in \mathbb{R}^{\mathbb{R}} \,/\, \forall x \in \mathbb{R} ,\ f(x+1) = f(x) + 1 \}$ est un sous-espace affine de $\mathbb{R}^{\mathbb{R}}$; en déterminer un point et la direction.

► **Exercice 4 (Espace affine des solutions d'une équation différentielle)** Soit $\mathscr{E}$ l'ensemble des applications y de classe C^∞ de $\mathbb{R}$ dans $\mathbb{R}$, solutions de l'équation différentielle $y'(x) - 2y(x) = e^{3x}$. Démontrer que $\mathscr{E}$ est un espace affine dont on déterminera la direction et la dimension.

► **Exercice 5 (Droites concourantes dans un tétraèdre)**

Soit (A,B,C,D) un tétraèdre d'un espace affine réel $\mathscr{E}$ de dimension 3.

1) Démontrer que la droite joignant le milieu I du segment $[A,B]$ au milieu J du segment $[C,D]$, et la droite joignant le milieu K du segment $[A,D]$ au milieu L du segment $[B,C]$ ont un point commun.
Quelle est la nature de la figure (I,L,J,K) ?

2) Donner cinq autres droites attachées au tétraèdre passant par ce point.

► **Exercice 6 (Coordonnées barycentriques en dimension 3)**

Soit (A,B,C,D) un repère de l'espace affine $\mathscr{E}$ de dimension 3 et $(\alpha,\beta,\gamma,\delta)$ les coordonnées barycentriques d'un point M de $\mathscr{E}$.

1) À quelles conditions sur $(\alpha,\beta,\gamma,\delta)$ le point M est-il distinct de A ?

2) À quelles conditions sur $(\alpha,\beta,\gamma,\delta)$ le point M est-il sur la droite (BC) ?

3) À quelles conditions sur $(\alpha,\beta,\gamma,\delta)$ le point M est-il dans le plan passant par B, parallèle au plan (ADC) ?

4) Déterminer les coordonnées barycentriques du point M, translaté du point D par le vecteur $\overrightarrow{AB}$.

► **Exercice 7 (Convexité)**

Soient X et Y deux ensembles convexes d'un espace affine $\mathscr{E}$. Démontrer que l'ensemble Z des milieux des segments qui joignent un point de X à un point de Y est convexe.

► **Exercice 8 (Théorème de LUCAS)**

Soit $P \in \mathbb{C}[X]$. Montrer que les racines de P' sont dans l'enveloppe convexe des racines de P.
Indication : décomposer $\dfrac{P'}{P}$ en éléments simples.

► **Exercice 9 (Centre du groupe affine)** $\mathscr{E}$ désigne un espace affine de dimension finie.

1) Déterminer toutes les applications affines $f : \mathscr{E} \to \mathscr{E}$ telles que, pour tout $\vec{u} \in \vec{\mathscr{E}}$, $t_{\vec{u}} \circ f = f \circ t_{\vec{u}}$.

2) En déduire le centre du groupe affine $\mathrm{GA}(\mathscr{E})$.

► **Exercice 10 (Homothéties-translations)**

1) Montrer que le groupe des homothéties-translations est un sous-groupe distingué du groupe affine.

2) Montrer que deux homothéties de même rapport sont conjuguées dans le groupe affine. En particulier, toutes les symétries centrales (homothéties de rapport -1) sont conjuguées dans le groupe affine.

► **Exercice 11 (Possible ou impossible ?)** Étant donnés n points $A_1, \ldots, A_n$ d'un plan affine $\mathscr{P}$, peut-on trouver n points $B_1, \ldots, B_n$ tels que $A_1, \ldots, A_n$ soient les milieux, respectivement, de $[B_1, B_2], \ldots, [B_n B_1]$? On étudiera en particulier les cas $n = 3$ et $n = 4$.

► **Exercice 12 (Mais le point n'est pas là !)** On a dessiné, sur une feuille de papier, deux droites $\mathscr{D}$ et $\mathscr{D}'$ qui ne sont pas parallèles, mais dont le point d'intersection ne se trouve pas sur la feuille. On place sur la même feuille un point M en dehors de $\mathscr{D}$ et $\mathscr{D}'$. Construire la droite joignant M au point d'intersection de $\mathscr{D}$ et $\mathscr{D}'$.

► **Exercice 13 (Projections - Affinités)**

Soient $\mathscr{E}$ un espace affine réel, E sa direction et F_1, F_2, deux sous-espaces vectoriels supplémentaires de E : $E = F_1 \oplus F_2$.

1) Soit $\mathscr{F}_k$ $(k=1,2)$ un sous-espace affine de $\mathscr{E}$ de direction F_k. Montrer que l'intersection $\mathscr{F}_1 \cap \mathscr{F}_2$ est réduite à un point.

2) Soit M un point de $\mathscr{E}$; on définit le point $p(M)$ comme étant le point d'intersection de $M + F_1$ avec $\mathscr{F}_2$. On définit ainsi une application $p : \mathscr{E} \to \mathscr{E}$. Montrer que p est affine. Comparer $p \circ p$ et p. Trouver l'ensemble des points fixes de p.
p est appelée *la projection de direction F_1 sur $\mathscr{F}_2$*.

3) Montrer que si $f : \mathscr{E} \to \mathscr{E}$ est une application affine vérifiant $f \circ f = f$, alors f est une projection.

4) Pour $\lambda \in \mathbb{R}$, on définit $a_\lambda : \mathscr{E} \to \mathscr{E}$ par $a_\lambda(M) = p(M) + \lambda\overrightarrow{p(M)M}$.
Montrer que a_λ est une transformation affine de $\mathscr{E}$. Déterminer l'ensemble de ses points fixes. Écrire la matrice de $\overrightarrow{a_\lambda}$ dans une base «bien choisie».
a_λ est appelée *l'affinité de direction F_1, de base $\mathscr{F}_2$ et de rapport λ*.
Etudier le cas où $\lambda = -1$.

► **Exercice 14 (Involutions)**

Trouver toutes les involutions d'un espace affine de dimension finie.

► **Exercice 15 (Conjugué d'une projection et d'une symétrie)** Soient p une projection et s une symétrie d'un espace affine $\mathscr{E}$. Pour $f \in \mathrm{GA}(\mathscr{E})$, déterminer $f \circ p \circ f^{-1}$ et $f \circ s \circ f^{-1}$.

► **Exercice 16 (Transvections)**

Si E est un espace vectoriel de dimension 2, un endomorphisme de E est appelé transvection vectorielle s'il existe une base où sa matrice est $\left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right)$, $(\alpha \neq 0)$.

1) Soit $\mathscr{E}$ un espace affine de direction E. Si O est un point de $\mathscr{E}$, on définit $f : \mathscr{E} \to \mathscr{E}$ par $f(M) = O + \varphi\left(\overrightarrow{OM}\right)$ où φ est une transvection vectorielle.

a) Montrer que f est une bijection affine.

b) Trouver tous les points fixes de f.

c) Soit $\mathscr{D}$ une droite parallèle à $\mathrm{Fix}(f)$. Montrer que $\mathscr{D}$ est stable par f et décrire la restriction de f à $\mathscr{D}$.

2) Montrer que le produit de deux symétries obliques de même axe est, en général, une transvection.

► **Exercice 17 (Sous-groupe des translations - symétries centrales)** Montrer que l'ensemble composé des translations et des symétries centrales est un groupe pour la composition.

► **Exercice 18 (Au moins deux centres de symétries)** Montrer qu'une configuration qui possède deux centres de symétrie distincts en possède une infinité.

► **Exercice 19 (Exemples d'applications affines)** Dans l'espace affine $\mathscr{E}$ de dimension 3, rapporté à un repère $(O,\vec{\imath},\vec{\jmath},\vec{k})$, décrire géométriquement les applications définies analytiquement par :

$$f_1 : \begin{cases} x' = 3x + 2y - 2z - 2 \\ y' = -2x - y + 2z + 2 \\ z' = 2x + 2y - z - 2 \end{cases}, \quad f_2 : \begin{cases} x' = 1 - y - z \\ y' = 2 - 2x - y - 2z \\ z' = -2 + 2x + 2y + 3z \end{cases}, \quad f_3 : \begin{cases} x' = \frac{1}{2}(3x + 2y + z - 1) \\ y' = \frac{1}{2}(x + 4y + z - 1) \\ z' = \frac{1}{2}(-x - 2y + z + 1) \end{cases}.$$

► **Exercice 20 (Sous-groupe engendré par deux symétries centrales planes)**

Soient $\mathscr{P}$ un plan affine et P, Q deux points de $\mathscr{P}$. On note S_P et S_Q les symétries de centres respectifs P et Q et t la composée $t = S_P \circ S_Q$.

1) Décrire géométriquement les applications suivantes :

a) t et $t \circ S_P \circ t$;

b) $t^n \circ S_P$ et $S_P \circ t^n$ pour tout entier relatif n ;

c) $g \circ S_P \circ g^{-1}$ pour toute transformation affine g de $\mathscr{P}$.

2) Soient H le sous-groupe de $\mathrm{GA}(\mathscr{P})$ engendré par $\{S_P, S_Q\}$ et K l'ensemble des translations de H. Est-ce que K est un sous-groupe distingué de H ? Quel est l'indice de K dans H ?

3) Est-ce que H contient d'autres éléments que les applications $t^n \circ S_P^{\varepsilon}$, $n \in \mathbb{Z}$ et $\varepsilon \in \{0,1\}$?

4) Dans le groupe affine $\mathrm{GA}(\mathscr{P})$, quel est le plus petit sous-groupe distingué contenant S_P ?

► **Exercice 21 (Sous-groupe engendré par une réflexion et une translation dans le plan)**

Rappel : Étant données deux droites non parallèles $\mathscr{D}$ et Δ du plan affine $\mathscr{P}$, on définit la symétrie $S_{\mathscr{D}}$ par rapport à la droite $\mathscr{D}$ parallèlement à Δ comme suit :

(i) On fixe un point $M_0 \in \mathscr{D}$;

(ii) tout point M de $\mathscr{P}$ s'exprime de manière unique sous la forme

$$M = M_0 + \vec{u} + \vec{v} \quad \text{avec} \quad \vec{u} \in \vec{\mathscr{D}} \text{ et } \vec{v} \in \vec{\Delta} \ ;$$

(iii) on pose alors $S_{\mathscr{D}}(M) = M_0 + \vec{u} - \vec{v}$.

Notations : L'image d'une droite $\mathscr{D}$ par la translation $t_{\vec{w}}$ de vecteur $\vec{w}$ sera notée $\mathscr{D} + \vec{w}$. D'autre part, $\mathrm{GA}(\mathscr{P})$ désignera le groupe affine de $\mathscr{P}$.

1) Soient $\mathscr{D}$ et Δ deux droites non parallèles du plan affine $\mathscr{P}$.

a) Pour $\vec{u} \in \vec{\mathscr{D}}$, montrer que $t_{\vec{u}} \circ S_{\mathscr{D}} = S_{\mathscr{D}} \circ t_{\vec{u}}$.

b) Pour $\vec{v} \in \vec{\Delta}$, montrer que $t_{\vec{v}} \circ S_{\mathscr{D}} = S_{\mathscr{D}+\frac{\vec{v}}{2}}$ et $S_{\mathscr{D}} \circ t_{\vec{v}} = S_{\mathscr{D}-\frac{\vec{v}}{2}}$.

On fixe dorénavant deux droites Δ_0 et $\mathscr{D}_0$ non parallèles du plan affine $\mathscr{P}$.

2) Pour $\vec{v}_0 \in \overrightarrow{\Delta_0}$, $\vec{v}_0 \neq \vec{0}$, on considère l'ensemble

$$G = \{S_{\mathscr{D}_0 + k\frac{\vec{v}_0}{2}} \,/\, k \in \mathbb{Z}\} \cup \{t_{k\vec{v}_0} \,/\, k \in \mathbb{Z}\}.$$

a) Démontrer que G est un sous-groupe de $\mathrm{GA}(\mathscr{P})$.

b) Démontrer que le groupe G est engendré par $t_{\vec{v}_0}$ et $S_{\mathscr{D}_0}$.

c) Le groupe G est-il abélien ?

3) Pour $\vec{u}_0 \in \overrightarrow{\mathscr{D}_0}$ on considère l'ensemble

$$H = \{t_{k\vec{u}_0} \circ S_{\mathscr{D}_0} \,/\, k \in \mathbb{Z}\} \cup \{t_{k\vec{u}_0} \,/\, k \in \mathbb{Z}\} \ .$$

a) Démontrer que H est un sous-groupe de $\mathrm{GA}(\mathscr{P})$.

b) Démontrer que le groupe H est engendré par $t_{\vec{u}_0}$ et $S_{\mathscr{D}_0}$.

c) Le groupe H est-il commutatif ?

Isométries

► Exercice 22 (Rotation et réflexion en dimension 3)

Soit E un espace vectoriel euclidien orienté de dimension 3.

1) Soit R une rotation vectorielle de E, d'axe orienté par un vecteur unitaire $\vec{u}$ et d'angle θ. Montrer que pour tout $\vec{x} \in E$, on a

$$R(\vec{x}) = (1 - \cos\theta)\,\langle \vec{x} \,|\, \vec{u} \rangle\, \vec{u} + (\sin\theta)\, \vec{u} \wedge \vec{x} + (\cos\theta)\vec{x}.$$

En déduire que si $\mathbf{b}$ est une base orthonormée directe de E, alors $\sin\theta$ et $\det_{\mathbf{b}}\big(\vec{u}, \vec{x}, R(\vec{x})\big)$ sont de même signe.

2) Soit s une réflexion de plan Π dans E. On considère un élément unitaire $\vec{u}$ de $\Pi^{\perp}$. Montrer que pour tout $\vec{x} \in E$, on a

$$s(\vec{x}) = \vec{x} - 2\,\langle \vec{x} \,|\, \vec{u} \rangle\, \vec{u}.$$

► Exercice 23 (Exemples d'isométries en dimension 3)

Dans l'espace affine euclidien $\mathscr{E}$ de dimension 3, rapporté à un repère orthonormé direct $(O, \vec{\imath}, \vec{\jmath}, \vec{k})$, décrire géométriquement les applications définies analytiquement par :

$$f_1 : \left\{ \begin{array}{lcl} x' & = & \frac{1}{3}(-x + 2y + 2z - 4) \\ y' & = & \frac{1}{3}(2x - y + 2z + 2) \\ z' & = & \frac{1}{3}(2x + 2y - z + 2) \end{array} \right. , \qquad f_2 : \left\{ \begin{array}{lcl} x' & = & -z + 1 \\ y' & = & x \\ z' & = & y - 2 \end{array} \right. ,$$

$$f_3 : \left\{ \begin{array}{lcl} x' & = & -z + 1 \\ y' & = & -x \\ z' & = & y - 2 \end{array} \right. , \qquad f_4 : \left\{ \begin{array}{lcl} x' & = & \frac{1}{3}(x - 2y + 2z + 6) \\ y' & = & \frac{1}{3}(-2x + y + 2z) \\ z' & = & \frac{1}{3}(2x + 2y + z) \end{array} \right. .$$

► Exercice 24 (Décomposition en produit de réflexions)

Dans l'espace affine euclidien de dimension 3, décomposer :

1) une translation, une rotation, un vissage, une symétrie glissée et une antirotation en produit de réflexions ;

2) une translation, une rotation et un vissage en produit de retournements.

► Exercice 25 (Groupe des isométries d'une partie)

Soit $\mathscr{E}$ un espace affine euclidien et X une partie de $\mathscr{E}$. On note G_X (resp. I_X) l'ensemble des transformations affines (resp. isométries) de $\mathscr{E}$ qui laissent stable X.

1) Montrer que G_X est un sous-groupe de $\mathrm{GA}(\mathscr{E})$ et que I_X est un sous-groupe de G_X.

2) On suppose que X est une partie **finie** de $\mathscr{E}$. Montrer qu'il existe un point Ω de $\mathscr{E}$ tel que $f(\Omega) = \Omega$ pour tout élément f de G_X.

► Exercice 26 (Groupe des isométries du triangle équilatéral)

Soit $A_1A_2A_3$ un triangle équilatéral d'un plan affine euclidien.

1) Montrer qu'une application affine est déterminée par ses valeurs sur l'ensemble $\{A_1, A_2, A_3\}$.

Soit G l'ensemble des isométries conservant $\{A_1, A_2, A_3\}$.

2) Montrer que G n'a pas plus de six éléments.

3) Montrer que G est un groupe.

4) Décrire ses éléments et écrire sa table de multiplication. Reconnaissez-vous G ?

5) Quel est l'ordre du sous-groupe H_1 engendré par la réflexion fixant A_1 ?

6) L'ensemble des rotations H_2 contenues dans G est-il un sous-groupe ?

7) Décrire les classes à gauche et à droite de H_1 et H_2. L'un de ces sous-groupes est-il distingué dans G ? Si oui, expliciter le groupe quotient.

► Exercice 27 (Groupe des isométries du carré)

Notations. - On note (e_1, e_2) la base canonique de $\mathbb{R}^2$, s_1 (respectivement s_2) la réflexion par rapport à $\mathbb{R}e_1$ (respectivement $\mathbb{R}e_2$), s_3 (respectivement s_4) la réflexion par rapport à $\mathbb{R}(e_1 + e_2)$ (respectivement $\mathbb{R}(e_1 - e_2)$), et r_1 (respectivement r_2) la rotation d'angle $\pi/2$ (respectivement $-\pi/2$).
Soient : $G = \{\mathrm{Id}_{\mathbb{R}^2}, s_1, s_2, s_3, s_4, r_1, r_2, -\mathrm{Id}_{\mathbb{R}^2}\}$ et $X = \{e_1 + e_2, e_1 - e_2, e_2 - e_1, -e_1 - e_2\}$.

1) Montrer que G est un sous-groupe du groupe $\mathrm{O}(\mathbb{R}^2)$. Décrire le centre $Z(G)$ de G.

2) Montrer que X est stable par chaque élément de G. En déduire un morphisme de groupes $\varphi : G \to S(X)$. Montrer que ce morphisme est injectif.

3) Montrer que G coïncide avec le groupe des isométries de $\mathbb{R}^2$ laissant stable X.

4) Le groupe G est-il isomorphe à $\mathbb{Z}/8\mathbb{Z}$? Justifier. Donner l'ordre de chaque élément de G.

5) Soit $H = \{\mathrm{Id}_{\mathbb{R}^2}, r_1, r_2, -\mathrm{Id}_{\mathbb{R}^2}\}$. Montrer que H est un sous-groupe cyclique de G. Est-il distingué dans G ?

6) Soit $K = \{\mathrm{Id}_{\mathbb{R}^2}, s_1, s_2, -\mathrm{Id}_{\mathbb{R}^2}\}$. Montrer que K est un sous-groupe de G isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$. Est-il distingué dans G ?

► Exercice 28 (Groupe des isométries de deux droites parallèles du plan)

Soient $\mathscr{D}_1$ et $\mathscr{D}_2$ deux droites de même direction $\mathbb{R}\vec{u}$ dans un plan affine euclidien $\mathscr{P}$. On se propose d'étudier l'ensemble G des isométries de $\mathscr{P}$ laissant globalement invariante l'union de ces deux droites :

$$G := \{f \in \mathrm{Is}(\mathscr{P}) \,/\, f(\mathscr{D}_1 \cup \mathscr{D}_2) = \mathscr{D}_1 \cup \mathscr{D}_2\}.$$

1) Montrer que G est un sous-groupe de $\mathrm{Is}(\mathscr{P})$.

2) Montrer que les translations appartenant à G sont celles dont le vecteur est colinéaire à $\vec{u}$.

3) Montrer que l'ensemble des points équidistants de $\mathscr{D}_1$ et $\mathscr{D}_2$ est une droite dirigée par $\mathbb{R}\vec{u}$. On notera Δ cette droite.

4) Montrer que les seules rotations appartenant à G sont les symétries centrales dont le centre est sur Δ.

5) Soit f un élément de G dont l'application linéaire $\vec{f}$ est une réflexion. Montrer que f est soit une réflexion d'axe Δ, soit une symétrie glissée d'axe Δ, soit une réflexion d'axe perpendiculaire à Δ.

6) Montrer que $G^+ := \{f \in G \,/\, \det f = 1\}$ est un sous-groupe distingué de G. Quel est son indice ?

7) Décrire tous les éléments de G^+ et tous les éléments de G.

8) On note T l'ensemble des translations de G. Montrer que T est un sous-groupe distingué de G^+ et déterminer le groupe quotient G^+/T.

► Exercice 29 (Groupe des isométries d'un polygone régulier)

Étudier le groupe des isométries d'un pentagone régulier et plus généralement, le groupe des isométries d'un polygone régulier à n sommets dans le plan affine euclidien.

► Exercice 30 (Groupe des isométries du cube)

Soit $\mathscr{E}$ l'espace affine euclidien de dimension 3. Soit $\mathcal{C}$ le groupe des isométries de $\mathscr{E}$ qui conservent un cube.

1) Montrer que $\mathcal{C}$ agit sur les paires de sommets opposés. En déduire un morphisme Φ de $\mathcal{C}$ dans S_4.

2) Déterminer le noyau de Φ.

3) Soit $\mathcal{C}^+$ le sous-groupe des déplacements de $\mathcal{C}$. Montrer que $\mathcal{C}^+$ est isomorphe à S_4.

4) Soit l'application $\lambda : \mathcal{C}^+ \times \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathcal{C}$ définie par $\begin{cases} \lambda(f,0) = f \\ \lambda(f,1) = f \circ s_O \end{cases}$ où s_O est la symétrie centrale de centre O (centre du cube). Montrer que λ est un isomorphisme de groupes. En déduire que $\mathcal{C}$ est isomorphe à $S_4 \times \mathbb{Z}/2\mathbb{Z}$.

Similitudes

► **Exercice 31 (Étude de deux similitudes planes)** Étudier (rapport, points fixes ...) les similitudes planes dont les formes complexes sont (j est le nombre complexe $e^{\frac{2i\pi}{3}}$) :

$$f_1(z) = (1+i)\bar{z} - 1 \quad ; \quad f_2(z) = j\bar{z} + 1.$$

► **Exercice 32 (Action du groupe des similitudes sur les couples de points)** Soient A, B, A' et B' quatre points du plan affine euclidien $\mathcal{P}$ tels que A (resp. A') soit distinct de B (resp. B'). Montrer qu'il existe une unique similitude directe qui envoie A sur A' et B sur B'.
Interpréter ce résultat en termes d'action de groupes.

► **Exercice 33 (Groupe des similitudes)** Montrer que l'ensemble des similitudes d'un espace affine euclidien est un groupe pour la composition des applications et que l'ensemble des similitudes directes en est un sous-groupe distingué.

► **Exercice 34 (Similitudes et angles)** Soient E un espace vectoriel euclidien et $\varphi \in \mathscr{L}(E)$.

1) Montrer que φ est une similitude si, et seulement si, φ préserve l'orthogonalité.

2) On suppose que E est de dimension 2. Montrer que φ est une similitude directe (resp. indirecte) si, et seulement si, φ préserve (resp. renverse) les angles orientés de vecteurs.

► **Exercice 35 (Actions sur l'ensemble des triangles du plan)** Dans le plan affine euclidien $\mathscr{P}$, on note $\mathscr{T}$ l'ensemble des triangles non plats (*ie* l'ensemble des triplets de points non alignés). Décrire les orbites pour l'action sur $\mathscr{T}$ respectivement du groupe affine $\mathrm{GA}(\mathscr{P})$, du groupe $\mathrm{Is}(\mathscr{P})$ des isométries de $\mathscr{P}$, du groupe des homothéties-translations et du groupe des similitudes. Quels sont les stabilisateurs ?

Problème 1 - Sous-groupe fini de rotations affines planes (examen juin 2012)

On note $\mathscr{P}$ le plan affine euclidien et $\mathrm{Is}^+(\mathscr{P})$ le groupe des déplacements de $\mathscr{P}$.

0) Soit H un sous-groupe **fini** de cardinal n de $\mathbf{S^1}$. Montrer que H coïncide avec $\mathbb{U}_n$, le groupe des racines $n^{\text{ièmes}}$ de l'unité.

1) Rappeler la nature géométrique des éléments de $\mathrm{Is}^+(\mathscr{P})$.

2) Soient R_1 et R_2 deux rotations de $\mathscr{P}$, de centres respectifs A_1, A_2 (avec $A_1 \neq A_2$) et d'angles respectifs θ_1 et θ_2.

a) Déterminer $R_1 \circ R_2 \circ R_1^{-1}$.

b) Soit R une rotation de centre A et d'angle θ_2. Montrer que $R \circ R_2^{-1}$ est une translation. Faire une figure et construire le vecteur de la translation.

c) Déterminer $R_1 \circ R_2 \circ R_1^{-1} \circ R_2^{-1}$.

3) Soit G un sous-groupe **fini** de $\mathrm{Is}^+(\mathscr{P})$.

a) Montrer que G est constitué uniquement de rotations.

b) Montrer que tous les éléments de G ont même centre (on pourra utiliser la question **2)**).

c) En déduire que G est isomorphe à un sous-groupe de $\mathbf{S^1}$ puis que G est cyclique.

Problème 2 - Un groupe d'isométries en dimension 3 (examen juin 2011)

Dans l'espace affine euclidien $\mathcal{E}$ de dimension 3, on considère :

- un plan $\mathscr{P}$;
- une droite $\mathscr{D}$ perpendiculaire à $\mathscr{P}$;
- A le point d'intersection de $\mathscr{P}$ et $\mathscr{D}$.

On note G l'ensemble des isométries f de $\mathcal{E}$ vérifiant $f(\mathscr{P}\cup\mathscr{D}) = \mathscr{P}\cup\mathscr{D}$ et G^+ le sous-ensemble des déplacements de G.

Si Π et Δ sont respectivement un plan et une droite de $\mathcal{E}$, on notera respectivement S_Π et d_Δ la réflexion de plan Π et le demi-tour de droite Δ.

1) Montrer que G est un sous-groupe de $\mathrm{Is}(\mathcal{E})$.

2) a) Montrer que G^+ est un sous-groupe distingué de G.

b) Quel est l'indice de G^+ dans G ?

3) Le groupe G^+ est-il distingué dans $\mathrm{Is}(\mathcal{E})$?

4) Montrer que G est constitué des éléments suivants :

∗ $\mathrm{Id}_{\mathcal{E}}$;
∗ les rotations d'axe $\mathscr{D}$;
∗ $S_{\mathscr{P}}$;
∗ $\{S_\Pi \,/\, \Pi$ plan contenant $\mathscr{D}\}$;
∗ $\{d_\Delta \,/\, \Delta$ droite contenant A incluse dans $\mathscr{P}\}$;
∗ les anti-rotations d'axe $\mathscr{D}$ et de plan $\mathscr{P}$.

5) On note H l'ensemble des rotations d'axe $\mathscr{D}$.

a) Montrer que H est un sous-groupe de G.

b) Montrer que H est distingué dans G.

c) Soient Π et Π' deux plans contenant $\mathscr{D}$. Montrer que les classes de S_Π et $S_{\Pi'}$ coïncident dans le groupe quotient G/H.

d) Même question avec d_Δ et $d_{\Delta'}$ où Δ et Δ' sont deux droites passant par A incluses dans $\mathscr{P}$.

e) Déduire des questions précédentes que H est d'indice 4 dans G.

f) En déduire la structure du groupe quotient G/H.

g) Montrer que H est un sous-groupe distingué de G^+ et déterminer la structure du groupe quotient G^+/H.

Problème 3 - Formule de Burnside et applications

Soit G un groupe fini agissant sur un ensemble fini E. On note :

* $\omega(x)$ l'orbite d'un élément x de E : $\omega(x) = \{g \cdot x \,/\, g \in G\}$;
* Ω l'ensemble des orbites : $\Omega = \{\omega(x) \,/\, x \in E\}$;
* $\mathrm{Stab}(x)$ le stabilisateur d'un élément x de E : $\mathrm{Stab}(x) = \{g \in G \,/\, g \cdot x = x\}$;
* $\mathrm{Fix}(g)$ l'ensemble des points fixes d'un élément g de G : $\mathrm{Fix}(g) = \{y \in E \,/\, g \cdot y = y\}$.

On rappelle que :

→ les orbites forment une partition de E : $E = \bigcup\limits_{\omega \in \Omega} \omega$ et si ω, ω' sont distinctes, alors $\omega \cap w' = \emptyset$;

→ si x est un élément de G, alors $\sharp\, \omega(x) = [G : \mathrm{Stab}(x)]$.

1) On note Γ la partie de $G \times E$ définie par $\Gamma = \big\{(g, x) \in G \times E \,/\, g \cdot x = x\big\}$.

a) Montrer que $\sharp\, \Gamma = \sum\limits_{x \in E} \sharp\, \mathrm{Stab}(x) = (\sharp\, \Omega) \times (\sharp\, G)$.

b) Montrer que $\sharp\, \Gamma = \sum\limits_{g \in G} \sharp\, \mathrm{Fix}(g)$.

c) En déduire la formule de Burnside : $\sharp\, \Omega = \dfrac{1}{\sharp\, G} \sum\limits_{g \in G} \sharp\, \mathrm{Fix}(g)$.

2) Une première application : calcul du nombre de bracelets à cinq perles et trois couleurs.

On considère un pentagone régulier de sommets $A_1, ..., A_5$ dans $\mathbb{R}^3$, les cinq sommets étant situés dans le plan $\mathbb{R}^2 \times \{0\}$. Un bracelet à cinq perles et trois couleurs est un coloriage des sommets de ce pentagone avec trois couleurs, c'est-à-dire une application de $\{A_1, ..., A_5\}$ vers l'ensemble des couleurs $\{\mathrm{Noir}, \mathrm{Bleu}, \mathrm{Rouge}\}$.
On notera E l'ensemble de ces coloriages et G l'ensemble des isométries de l'espace qui préservent le pentagone.

a) Déterminer le cardinal de E.

b) Montrer que G est un sous-groupe de $\mathrm{Is}(\mathbb{R}^3)$. Montrer que G est de cardinal 20 et décrire la liste de ces éléments.

c) Montrer que l'on définit une action de G sur E en posant, pour $g \in G$ et $c \in E$, $g \cdot c = c \circ g^{-1}$.

d) Observer que le nombre de colliers possibles n'est autre que le nombre d'orbites pour cette action.

e) Appliquer la formule de Burnside pour déterminer ce nombre.

3) Une deuxième application : nombre de façons de décomposer 1000 en produit de trois entiers naturels à l'ordre des facteurs près.

a) Le faire à la main, *ie* écrire explicitement toutes les décompositions possibles.

b) Remarquer que se donner une factorisation de 1000 en produit ordonné de trois entiers naturels revient exactement à se donner une décomposition de la forme

$1000 = (2^{\alpha_1} 5^{\beta_1})(2^{\alpha_2} 5^{\beta_2})(2^{\alpha_3} 5^{\beta_3})$ avec $(\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3) \in \mathbb{N}^6$ vérifiant $\alpha_1 + \alpha_2 + \alpha_3 = \beta_1 + \beta_2 + \beta_3 = 3$.

On note E l'ensemble de ces sextuplets :

$$E = \Big\{(\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3) \in \mathbb{N}^6 \,/\, \alpha_1 + \alpha_2 + \alpha_3 = \beta_1 + \beta_2 + \beta_3 = 3\Big\}.$$

c) Déterminer le cardinal de E.

d) Montrer que l'on définit une action du groupe symétrique S_3 sur E en posant, pour $\sigma \in S_3$ et $x = (\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3) \in E$:

$$\sigma \bullet x = \Big(\alpha_{\sigma^{-1}(1)}, \alpha_{\sigma^{-1}(2)}, \alpha_{\sigma^{-1}(3)}, \beta_{\sigma^{-1}(1)}, \beta_{\sigma^{-1}(2)}, \beta_{\sigma^{-1}(3)}\Big).$$

e) Observer que le nombre de façons dont on peut écrire 1000 comme produit de trois entiers naturels à l'ordre des facteurs près n'est autre que le nombre d'orbites pour cette action.

f) Calculer ce nombre à l'aide de la formule de Burnside.

Problème 4 - Centralisateur

Première partie.

Soient G un groupe noté multiplicativement d'élément neutre e et x un élément de G. On note $C_G(x)$ l'ensemble des éléments de G qui commutent avec x :

$$C_G(x) = \{g \in G \,/\, gx = xg\} = \{g \in G \,/\, gxg^{-1} = x\}.$$

1) Montrer que $C_G(x)$ est un sous-groupe de G contenant $\langle x \rangle$, le sous-groupe de G engendré par x.

2) Déterminer $C_G(e)$.

3) Que représente $C_G(x)$ pour l'action du groupe G sur lui-même par conjugaison ?

Le groupe $C_G(x)$ est appelé *centralisateur* de x dans G.

4) Soit H un sous-groupe de G contenant x. Déterminer $C_H(x)$.

5) Déterminer $C_G(x)$ lorsque G est abélien.

Deuxième partie : calcul d'un centralisateur dans le groupe symétrique S_n.

Soit n un entier, $n \geqslant 2$. On rappelle que si $a_1, \ldots, a_k$ sont k éléments de $\{1, 2, \ldots, n\}$, $(a_1\, a_2\, \cdots\, a_k)$ désigne le cycle de longueur k qui envoie a_1 sur a_2, a_2 sur a_3, …, a_k sur a_1. On note τ la transposition $(1\,2)$.

6) Pour f élément de S_n, déterminer $f\tau f^{-1}$.

7) Décrire les éléments de $C_{S_n}(\tau)$.

8) Montrer que $C_{S_n}(\tau)$ est engendré par $\{\tau, (3\,4), (4\,5), \ldots, (n{-}1\ n)\}$.

9) Montrer que $C_{S_n}(\tau)$ est isomorphe au groupe produit $\mathbb{Z}/2\mathbb{Z} \times S_{n-2}$.

Troisième partie : centralisateur en géométrie vectorielle euclidienne de dimension 2.

Soit E un espace vectoriel euclidien de dimension 2.

10) Soient R une rotation d'angle θ de E, S une réflexion de droite D de E et f une isométrie de E. Déterminer $f \circ R \circ f^{-1}$ et $f \circ S \circ f^{-1}$.

11) Soit R une rotation de E.

a) Déterminer le centralisateur de R dans $SO(E)$.

b) Déterminer le centralisateur de R dans $O(E)$.

12) Soit S une réflexion d'axe D de E.

a) Décrire les éléments du centralisateur de S dans $O(E)$.

b) Montrer que $C_{O(E)}(S)$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Quatrième partie : centralisateur en géométrie vectorielle euclidienne de dimension 3.

Soit E un espace vectoriel euclidien de dimension 3. On note :

- $R_{u,\theta}$ la rotation d'axe orienté par le vecteur u et d'angle θ ;
- d_D le demi-tour de droite $D = \text{vect}(u)$: $d_D = R_{u,\pi}$;
- S_P la réflexion de plan P ;
- $A_{u,\theta}$ l'antirotation de vecteur u et d'angle θ : $A_{u,\theta} = S_P \circ R_{u,\theta} = R_{u,\theta} \circ S_P$ où P est le plan orthogonal à u.

On rappelle que si $u,\ v,\ w$ sont trois vecteurs de E, g une application linéaire de E et $\mathcal{B}$ une base de E, alors :

$$\det_{\mathcal{B}}\big(g(u), g(v), g(w)\big) = \det(g)\det_{\mathcal{B}}(u, v, w).$$

13) a) Rappeler les formules démontrées dans le cours permettant de déterminer le cosinus et le sinus de l'angle de $R_{u,\theta}$.

b) À quelles conditions a-t-on $R_{u,\theta} = R_{v,\alpha}$?

14) Montrer que si ρ est une rotation, $\rho \circ R_{u,\theta} \circ \rho^{-1} = R_{\rho(u),\theta}$.

15) Montrer que $S_P \circ R_{u,\theta} \circ S_P^{-1} = R_{S_P(u),-\theta}$ et $R_{u,\theta} \circ S_P \circ R_{u,\theta}^{-1} = S_{R_{u,\theta}(P)}$.

16) Soit d_D un demi-tour d'axe D.

a) Montrer qu'un demi-tour d_Δ commute avec d_D si, et seulement si, $D = \Delta$ ou D est orthogonale à Δ.

b) Montrer qu'une rotation d'angle différent de π commute avec d_D si, et seulement si, son axe est D.

c) Décrire tous les éléments du centralisateur de d_D dans $SO(E)$.

17) Soit $R = R_{u,\theta}$ une rotation d'axe D dirigé par u et d'angle θ différent de π (R n'est pas un demi-tour).

a) Montrer qu'une rotation ρ d'axe Δ commute avec R si, et seulement si, $\Delta = D$.

b) En déduire le centralisateur de R dans $SO(E)$ et montrer qu'il est isomorphe à $SO(2)$.

c) Montrer qu'une réflexion S_P de plan P commute avec R si, et seulement si, D et P sont orthogonaux.

d) Montrer qu'une antirotation $A_{v,\alpha}$ d'angle $\alpha \neq \pi$ commute avec R si, et seulement si, v dirige D.

e) Décrire les éléments de $C_{O(E)}(R)$. Montrer que ce groupe est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times SO(2)$.

Problème 5 - Simplicité de SO(3)

Soit E un espace vectoriel euclidien orienté de dimension 3. On note $SO(E)$ le groupe des endomorphismes orthogonaux positifs (isométries vectorielles directes) de E. Le but de l'exercice est de montrer que $SO(E)$ est un groupe simple, c'est-à-dire qu'il n'admet pas de sous-groupe distingué autre que lui-même et $\{\text{Id}_E\}$. On appelle demi-tour toute rotation vectorielle d'angle π.

1) Soient $\overrightarrow{e_1}$ un vecteur unitaire de E, et f une rotation vectorielle d'axe orienté par $\overrightarrow{e_1}$ et d'angle θ.

a) Écrire la matrice de f dans une base orthonormée directe $(\overrightarrow{e_1}, \overrightarrow{e_2}, \overrightarrow{e_3})$.

b) Montrer que f peut s'écrire comme composée de deux demi-tours.

c) En déduire que les demi-tours engendrent $SO(E)$.

2) On considère de nouveau la rotation vectorielle f d'axe orienté par $\overrightarrow{e_1}$ et d'angle θ.

a) Soit $\vec{u}$ un vecteur de coordonnées (x, y, z) dans une base orthonormée directe $(\overrightarrow{e_1}, \overrightarrow{e_2}, \overrightarrow{e_3})$. Calculer le produit scalaire $\langle \vec{u}\,|f(\vec{u})\rangle$.

b) En déduire que si $\theta \in [\pi/2, \pi]$, il existe une droite vectorielle D telle que D et $f(D)$ soient orthogonales.

On note σ le demi-tour d'axe D.

c) Pour $\vec{v} \in f(D)$, calculer l'image de $\vec{v}$ par σ, puis par $\sigma \circ f \circ \sigma^{-1} \circ f^{-1}$.

d) Quelle est la nature de $\sigma \circ f \circ \sigma^{-1} \circ f^{-1}$?

3) Soit r un demi-tour d'axe la droite vectorielle de base $\overrightarrow{e_1}$.

a) Pour $g \in SO(E)$, décrire $g \circ r \circ g^{-1}$.

b) Expliquer brièvement pourquoi $SO(E)$ agit sur l'ensemble des vecteurs unitaires de E. Montrer que cette action est transitive.

c) En déduire que tout demi-tour est conjugué avec r.

4) Soient H un sous-groupe distingué de $SO(E)$ distinct de $\{Id_E\}$ et $f \in H \backslash \{Id_E\}$.

a) Expliquer pourquoi H contient une rotation dont l'angle appartient à $]0, \pi]$.

b) En considérant les itérées successives de f, montrer que H contient au moins une rotation vectorielle dont l'angle appartient à $[\pi/2, \pi]$.

c) Montrer que H contient au moins un demi-tour.

d) Montrer que H contient tous les demi-tours.

e) Conclure.

Problème 6 - Exposant d'un groupe

Soit G un groupe d'élément neutre e. Si g est un élément de G, on note $\omega(g)$ son ordre. Comme d'habitude, si p et q sont deux nombres entiers, $p \wedge q$ désignera leur PGCD et $p \vee q$ leur PPCM.

On dira que G est d'*exposant fini* s'il existe un entier $k \geqslant 1$ tel que $g^k = e$ pour tout $g \in G$. Dans ce cas, on appelle *exposant* de G le plus petit de ces entiers et on le notera $E(G)$. Si un tel entier n'existe pas, on dit que G est d'exposant infini.

1) Montrer que si G est fini, alors G est d'exposant fini. Calculer son exposant et montrer que c'est un diviseur du cardinal de G.

2) Donner un exemple de groupe infini d'exposant fini.

3) On suppose ici que G est un groupe abélien fini.

a) Soient x un élément de G et r un entier naturel. Quel est l'ordre de x^r ?

b) Soient x et y deux éléments de G. Montrer que si $\omega(x) \wedge \omega(y) = 1$, alors $\omega(xy) = \omega(x)\omega(y)$.

c) Pour x et y éléments de G, montrer qu'il existe $g \in G$ tel que $\omega(g) = \omega(x) \vee \omega(y)$.
(On pourra montrer qu'il existe deux entiers α et β premiers entre eux tels que $\omega(x) \vee \omega(y) = \alpha\beta$ et appliquer les questions a et b.)

d) Montrer qu'il existe $g \in G$ tel que $\omega(g) = E(G)$. En déduire que si $E(G) = \mathrm{Card}(G)$, alors G est cyclique.

e) Donner un exemple de groupe non cyclique, d'exposant fini égal à son cardinal.

4) On se propose ici de démontrer que si G est un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$ d'exposant fini, alors G est fini.

a) On rappelle que $A \in \mathscr{M}_n(\mathbb{C})$ est nilpotente s'il existe un entier k non nul tel que $A^k = 0$

i) Montrer qu'une matrice $A \in \mathscr{M}_n(\mathbb{C})$ est nilpotente si, et seulement si, son spectre est réduit à $\{0\}$.

ii) Montrer que la trace d'une matrice nilpotente est nulle.

iii) Soit $A \in \mathscr{M}_n(\mathbb{C})$ telle que $\mathrm{Trace}(A^k) = 0$ pour tout $k \geqslant 1$. Montrer que A est nilpotente.

b) Soit G un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$ et F le sous-espace vectoriel de $\mathscr{M}_n(\mathbb{C})$ engendré par G.

i) Pourquoi existe-t-il k éléments $A_1, \ldots, A_k$ de G tels que $(A_1, \ldots, A_k)$ soit une base de F ?

On note $\tau : G \to \mathbb{C}^k$ l'application définie par $\tau(M) = \Big(\mathrm{Trace}(MA_1), \ldots, \mathrm{Trace}(MA_k)\Big)$ et on considère deux éléments M et N de G tels que $\tau(M) = \tau(N)$. On note D la matrice MN^{-1}.

ii) Pourquoi D est-elle dans G ?

iii) Montrer que $\mathrm{Trace}(MA) = \mathrm{Trace}(NA)$ pour toute matrice $A \in G$.

iv) En déduire que $\mathrm{Trace}(D^k) = \mathrm{Trace}(D^{k-1})$ pour tout $k \geqslant 1$ puis que $\mathrm{Trace}(D^k) = n$.

v) Montrer que $\mathrm{Trace}(D - \mathrm{I}_n)^k = 0$ pour tout $k \geqslant 1$ puis que $D - \mathrm{I}_n$ est nilpotente.

vi) Montrer que si G est d'exposant fini, alors D est diagonalisable et donc $D - \mathrm{I}_n$ également. En déduire que, dans ce cas, $D = I_n$ puis que $M = N$.

On suppose toujours que G est d'exposant fini $E(G)$ et on considère la partie Λ de $\mathbb{C}$ définie par

$$\Lambda = \left\{ \sum_{i=1}^{n} \lambda_i \Big/ (\lambda_1, \ldots, \lambda_n) \in \mathbb{U}_{E(G)}^n \right\}$$

où, comme d'habitude, $\mathbb{U}_\alpha$ désigne l'ensemble des racines $\alpha^{\text{ème}}$ de l'unité.

vii) Montrer que toute matrice A appartenant à G est diagonalisable et que ses valeurs propres sont dans $\mathbb{U}_{E(G)}$. En déduire que $\tau(G)$ est une partie de Λ^k.

viii) Montrer que Λ est finie.

c) Montrer que si G est un sous-groupe d'exposant fini de $\mathrm{GL}_n(\mathbb{C})$, alors G est fini.

Problème 7 - Matrices de permutation et théorème de Brauer

On considère l'application $S_n \times \mathbb{R}^n \to \mathbb{R}^n$ qui, à $\big(\sigma, (x_1, \ldots, x_n)\big)$, associe $\sigma \cdot (x_1, \ldots, x_n) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$. On notera, pour $\sigma \in S_n$, $P_\sigma : \mathbb{R}^n \to \mathbb{R}^n$ l'application définie par $P_\sigma(x) = \sigma \cdot x$.

1) Vérifier que l'on définit ainsi une action de S_n sur $\mathbb{R}^n$.

2) Montrer que l'application $\varphi : S_n \to S(\mathbb{R}^n)$, qui à σ associe P_σ, est un morphisme de groupes à valeurs dans $\mathrm{GL}(\mathbb{R}^n)$, le groupe linéaire de $\mathbb{R}^n$.

3) Pour $\sigma \in S_n$, décrire la matrice de P_σ dans la base canonique de $\mathbb{R}^n$.

4) Montrer que $\det P_\sigma = \varepsilon(\sigma)$. Calculer la trace de P_σ.

5) Montrer que si σ et σ' sont conjuguées dans S_n, alors P_σ et $P_{\sigma'}$ sont semblables.

On se propose de démontrer la réciproque de ce résultat.

6) Pour $\sigma \in S_n$ et $k \in [\![1, n]\!]$, on note $N_k(\sigma)$ le nombre de k-cycles dans la décomposition de σ en cycles à supports disjoints ($N_1(\sigma)$ est le nombre de points fixes de σ).

a) Pour σ et σ' dans S_n, donner une condition nécessaire et suffisante sur les $N_k(\sigma)$ et $N_k(\sigma')$ pour que σ et σ' soient conjuguées.

b) Soient $\sigma \in S_n$ et $k_1, \ldots, k_s$ les cardinaux des orbites de σ (y compris celles réduites à un élément).

i) Montrer que le polynôme caractéristique de P_σ est égal à $(-1)^n \prod_{i=1}^{s} (X^{k_i} - 1)$.

ii) En déduire que $\ker(P_\sigma - \mathrm{Id}_{\mathbb{R}^n})$ est de dimension $\sum_{k=1}^{n} N_k(\sigma)$.

c) Soient $\sigma \in S_n$ et $m \in \mathbb{N}^*$.

i) On suppose que σ est un cycle de longueur k et que m divise k. Montrer que la décomposition de σ^m en cycles à supports disjoints est constituée de m cycles de longueur $\frac{k}{m}$.

ii) On suppose encore que σ est un cycle de longueur k et on note d le pgcd de k et m. Montrer que la décomposition de σ^m en cycles à supports disjoints est constituée de d cycles de longueur $\frac{k}{d}$.

iii) Montrer que le nombre de cycles dans la décomposition de σ^m en cycles à supports disjoints est égal à $\sum_{k=1}^{n} (k \wedge m) N_k(\sigma)$ (comme d'habitude, $a \wedge b$ désigne le pgcd des entiers a et b).

d) Soient σ et σ' deux permutations de S_n telles que P_σ et $P_{\sigma'}$ soient semblables.

i) Montrer que pour tout $m \in \mathbb{N}^*$, P_{σ^m} et $P_{\sigma'^m}$ sont semblables.

ii) En déduire que pour tout $m \in \mathbb{N}^*$, on a $\sum\limits_{k=1}^{n} (k \wedge m) N_k(\sigma) = \sum\limits_{k=1}^{n} (k \wedge m) N_k(\sigma')$.

iii) En considérant la matrice A de $\mathscr{M}_n(\mathbb{Z})$ dont le coefficient (i,j) vaut $i \wedge j$, montrer que $N_k(\sigma) = N_k(\sigma')$ pour tout $k \in [\![1,n]\!]$.

iv) Conclure.
