Exercices 12 – Groupes, anneaux, corps

Groupes

Exercice 1. — Montrer que $\left(\mathbb{R}_+^*, \times\right)$ est un groupe. Peut-on remplacer $\mathbb{R}_+^*$ par $\mathbb{R}_-^*$?

- ➢ La multiplication est une **LCI sur** $\mathbb{R}_+^*$ (le produit de deux réels strictement positifs est un réel strictement positif).
- ➢ La multiplication est **associative**.
- ➢ Il existe un **élément neutre** pour la multiplication : $1 \in \mathbb{R}_+^*$.
- ➢ Tout réel strictement positif x admet **un inverse dans** $\mathbb{R}_+^*$ pour la multiplication : $\frac{1}{x} \in \mathbb{R}_+^*$ et $x \times \frac{1}{x} = 1 = \frac{1}{x} \times x$.

Conclusion. $\left(\mathbb{R}_+^*, \times\right)$ est un groupe.

En revanche, la multiplication n'est pas une LCI dans $\left(\mathbb{R}_-^*, \times\right)$, puisque par exemple : $(-2) \times (-3) = 6 \notin \mathbb{R}_-^*$. On ne peut donc pas remplacer $\mathbb{R}_+^*$ par $\mathbb{R}_-^*$ dans ce qui précède.

Exercice 2. — Montrer que $\left(\mathbb{R}^{\mathbb{R}}, +\right)$ est un groupe. A-t-on toujours un groupe si on remplace la loi "$+$" par la loi "$\circ$" (composition) ?

- ➢ L'addition est une **LCI sur** $\mathbb{R}^{\mathbb{R}}$ (la somme de deux fonctions à valeurs réelles est encore une fonction à valeurs réelles).
- ➢ L'addition dans $\mathbb{R}^{\mathbb{R}}$ est **associative**.
- ➢ Il existe un **élément neutre** pour l'addition dans $\mathbb{R}^{\mathbb{R}}$: la fonction constante égale à 0, notée $0_{\mathbb{R}^{\mathbb{R}}}$.
- ➢ Toute fonction $f \in \mathbb{R}^{\mathbb{R}}$ admet **un inverse dans** $\mathbb{R}^{\mathbb{R}}$ pour l'addition, qui est son opposée, la fonction $(-f) : (-f) \in \mathbb{R}^{\mathbb{R}}$ et $f + (-f) = 0_{\mathbb{R}^{\mathbb{R}}} = (-f) + f$.

Conclusion. $\left(\mathbb{R}^{\mathbb{R}}, +\right)$ est un groupe.

Considérons à présent le même ensemble $(\mathbb{R}^{\mathbb{R}})$, en le munissant cette fois la loi "o" au lieu de la loi "$+$". On peut alors affimer que :

- ➢ La composition est une **LCI sur** $\mathbb{R}^{\mathbb{R}}$ (si f et g sont dans $\mathbb{R}^{\mathbb{R}}$, alors $f \circ g \in \mathbb{R}^{\mathbb{R}}$).
- ➢ La composition dans $\mathbb{R}^{\mathbb{R}}$ est **associative** (car plus généralement la composition des applications est associative).
- ➢ Il existe un **élément neutre** pour la composition dans $\mathbb{R}^{\mathbb{R}}$: la fonction $\mathrm{id}_{\mathbb{R}}$ (définie par : $\forall x \in \mathbb{R},\ \mathrm{id}_{\mathbb{R}}(x) = x$).

MAIS toute fonction $f \in \mathbb{R}^{\mathbb{R}}$ n'admet pas nécessairement un inverse dans $\mathbb{R}^{\mathbb{R}}$; en effet, f est inversible dans $\mathbb{R}^{\mathbb{R}}$ SSI f est bijective.

Conclusion. $\left(\mathbb{R}^{\mathbb{R}}, \circ\right)$ n'est pas un groupe.

Remarque. Notons $\mathrm{Bij}(\mathbb{R})$ l'ensemble des fonctions bijectives de $\mathbb{R}$ dans $\mathbb{R}$.[1] Il résulte de ce qui précède que $\left(\mathrm{Bij}\left(\mathbb{R}\right), \circ\right)$ est un groupe, plus tard appelée **groupe des permutations de** $\mathbb{R}$.

1. Une fonction bijective de $\mathbb{R}$ dans $\mathbb{R}$ est appelée une **permutation** de $\mathbb{R}$.

Exercice 3. — On note $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, et $\mathbb{K}_n[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$ de degré inférieur ou égal à n (n entier naturel). Vérifier que $(\mathbb{K}_n[X], +)$ est un groupe abélien. L'ensemble des polynômes à coefficients dans $\mathbb{K}$ de degré exactement n est-il un groupe ?

- ➢ L'addition est une **LCI sur** $\mathbb{K}_n[X]$ (la somme de deux polynômes de degré $\leqslant n$ est un polynôme de degré $\leqslant n$.
- ➢ L'addition dans $\mathbb{K}_n[X]$ est **associative**.
- ➢ Il existe un **élément neutre** pour l'addition dans $\mathbb{K}_n[X]$: le polynôme nul, notée $0_{\mathbb{K}_n[X]}$.
- ➢ Tout polynôme $P \in \mathbb{K}_n[X]$ admet **un inverse dans** $\mathbb{K}_n[X]$ pour l'addition, qui est son opposé, le polynôme $(-P) : (-P) \in \mathbb{K}_n[X]$ et $P + (-P) = 0_{\mathbb{K}_n[X]} = (-P) + P$.

Conclusion. $(\mathbb{K}_n[X], +)$ est un groupe. De plus, ce groupe est abélien car l'addition dans $\mathbb{K}_n[X]$ est commutative : $\forall\ (P, Q) \in (\mathbb{K}_n[X])^2, \quad P + Q = Q + P$.

En revanche, la somme de deux polynômes de degré exactement n n'est pas nécessairement de degré n. Par exemple, les polynômes $P = X^2 + 1$ et $Q = X - X^2$ sont de degré 2, mais $P + Q = X + 1$ n'est pas de degré 2. En d'autres termes, l'addition n'est pas une LCI dans l'ensemble des polynômes à coefficients dans $\mathbb{K}$ de degré exactement n.

Conclusion. L'ensemble des polynômes à coefficients dans $\mathbb{K}$ de degré exactement n n'est pas un groupe.

Exercice 4. — On note $\mathbb{D}$ l'ensemble des nombres décimaux : $\mathbb{D} = \left\{ \dfrac{n}{10^k},\ n \in \mathbb{Z},\ k \in \mathbb{N} \right\}$. Montrer que $(\mathbb{D}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.

On vérifie les 4 axiomes permettant d'affirmer que $(\mathbb{D}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.

- ➢ **(SG1)**. $\mathbb{D} \subset \mathbb{R}$ (trivial).
- ➢ **(SG2)**. $0 \in \mathbb{D}$ (l'élément neutre pour l'addition appartient à $\mathbb{D}$).
- ➢ **(SG3)**. La somme de deux décimaux est encore un décimal (vérification aisée). L'addition est donc une LCI sur $\mathbb{D}$.
- ➢ **(SG4)**. Tout décimal x admet un inverse pour l'addition, qui est son opposé $(-x)$, et $(-x)$ est encore un décimal.

Conclusion. $(\mathbb{D}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.

Exercice 5. — Montrer que $(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

On vérifie les 4 axiomes permettant d'affirmer que $(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

- ➢ **(SG1)**. $\mathbb{U} \subset \mathbb{C}^*$ car tout nombre complexe de module 1 est en particulier non nul.
- ➢ **(SG2)**. $1 \in \mathbb{U}$ (l'élément neutre pour la multiplication appartient à $\mathbb{U}$).
- ➢ **(SG3)**. Le produit de deux éléments de $\mathbb{U}$ (deux complexes de module 1) est encore un élément de $\mathbb{U}$ (propriété immédiate, déjà vue dans le chapitre sur les complexes). La multiplication est donc une LCI sur $\mathbb{U}$.
- ➢ **(SG4)**. Tout élément de $\mathbb{U}$ (tout complexe de module 1) z admet un inverse pour la multiplication, qui est $1/z$; et $1/z$ est encore un élément de $\mathbb{U}$ (déjà vu dans le chapitre sur les complexes).

Conclusion. $(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

Exercice 6. — Soit n un entier naturel $\geqslant 2$. Montrer que $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$.

On vérifie les 4 axiomes permettant d'affirmer que $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$.

➢ **(SG1)**. $\mathbb{U}_n \subset \mathbb{U}$ car toute racine n-ème de l'unité est de module 1 (propriété vus dans le chapitre sur les complexes).

➢ **(SG2)**. $1 \in \mathbb{U}_n$ car $1^n = 1 \ldots$ (l'élément neutre pour la multiplication appartient à $\mathbb{U}_n$).

➢ **(SG3)**. Le produit de deux éléments de $\mathbb{U}_n$ (deux racines n-èmes de l'unité) est encore un élément de $\mathbb{U}_n$ (propriété vue dans le chapitre sur les complexes). La multiplication est donc une LCI sur $\mathbb{U}_n$.

➢ **(SG4)**. Tout élément de $\mathbb{U}_n$ (toute racine n-ème de l'unité) z admet un inverse pour la multiplication, qui est $1/z$; et $1/z$ est encore un élément de $\mathbb{U}_n$ (déjà vu dans le chapitre sur les complexes).

Conclusion. $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$.

Exercice 7. — Soit E un ensemble non-vide. L'ensemble $\mathscr{P}(E)$ est-il un groupe muni de la lci $\cup$? De la lci $\cap$?

Dans $\mathscr{P}(E)$, la loi $\cup$ est une LCI associative (et commutative), admettant un élément neutre (l'ensemble vide $\emptyset$).

On distingue alors deux cas, suivant que E est l'ensemble vide ou non.

➢ **Premier cas -** $E \neq \emptyset$. Alors E contient au moins un élément, que nous noterons x. Cette observation faite, le singleton $\{x\}$ est un élément de $\mathscr{P}(E)$, qui n'admet pas d'inverse pour la loi $\cup$. En effet, pour toute partie A de E, on a : $\{x\} \cup A \neq \emptyset$.

Puisqu'il existe dans $\mathscr{P}(E)$ un élément non inversible pour la loi $\cup$, on peut conclure : l'ensemble $\mathscr{P}(E)$ n'est pas un groupe muni de la lci $\cup$.

➢ **Second cas -** $E = \emptyset$. Dans ce cas, $\mathscr{P}(E)$ ne contient qu'un élément : $\mathscr{P}(E) = \{\emptyset\}$. Cet élément étant inversible pour l'union (puisque $\emptyset \cup \emptyset = \emptyset \ldots$), on peut conclure : l'ensemble $\mathscr{P}(\emptyset)$ est un groupe muni de la lci $\cup$.

➢ Des raisonnements analogues permettent d'affirmer que $(\mathscr{P}(E), \cap)$ n'est pas un groupe si $E \neq \emptyset$, et est un groupe lorsque $E = \emptyset$.

Exercice 8. — Décrire tous les groupes possédant 1, 2, 3 ou 4 éléments. Déduire de ces descriptions que tout groupe fini de cardinal inférieur ou égal à 4 est abélien.

Cet exo est l'objet de la propriété 12.4 du pdf, dont la démonstration est située entre les pages 271 et 274. Elle repose essentiellement sur l'écriture des "tables de multiplication" des groupes de cardinal $\leqslant 4$, ce qui est un petit jeu de "sudoku"...

Exercice 9. — (Groupe des permutations de $\mathbb{C}$). On appelle **permutation de** $\mathbb{C}$ une bijection de $\mathbb{C}$ dans $\mathbb{C}$. On note $\text{Bij}(\mathbb{C})$ l'ensemble des permutations de $\mathbb{C}$.

Montrer que $(\text{Bij}(\mathbb{C}), \circ)$ est un groupe, et qu'il n'est pas abélien.

➢ La composition est une **LCI sur Bij**$(\mathbb{C})$, car la composée de deux bijections de $\mathbb{C}$ dans $\mathbb{C}$ est encore une bijection de $\mathbb{C}$ dans $\mathbb{C}$.

➢ La composition dans $\text{Bij}(\mathbb{C})$ est **associative**, car la composition des applications en général est associative.

➢ Il existe un **élément neutre** pour la composition dans $\text{Bij}(\mathbb{C})$, qui est $\text{id}_{\mathbb{C}}$.

➢ Si $f \in \text{Bij}(\mathbb{C})$, alors f^{-1} existe, et est encore une bijection de $\mathbb{C}$ dans $\mathbb{C}$. Tout élément de $\text{Bij}(\mathbb{C})$ admet donc un inverse pour la composition dans $\text{Bij}(\mathbb{C})$.

Conclusion. $(\text{Bij}(\mathbb{C}), \circ)$ est un groupe.

Considérons les applications $f : z \in \mathbb{C} \longmapsto z + \text{i}$ et $g : z \in \mathbb{C} \longmapsto \overline{z}$. Il est immédiat que f et g sont des bijections de $\mathbb{C}$ dans $\mathbb{C}$, et en outre :

$$(f \circ g)(\text{i}) = 0 \text{ tandis que } (g \circ f)(\text{i}) = -2\text{i}$$

Il s'ensuit que $f \circ g \neq g \circ f$. Le groupe $(\text{Bij}(\mathbb{C}), \circ)$ est donc non-abélien.

Exercice 10. — (Groupe des translations dans le plan complexe). On appelle **translation dans le plan complexe** une application T_b définie sur $\mathbb{C}$ et à valeurs dans $\mathbb{C}$, telle que :

$$\forall z \in \mathbb{C},\ T_b(z) = z + b \qquad (\text{avec } b \in \mathbb{C})$$

On note $\text{Tr}(\mathbb{C})$ l'ensemble des translations dans le plan complexe.

Montrer que $(\text{Tr}(\mathbb{C}), \circ)$ est un groupe, en prouvant que c'est un sous-groupe de $(\text{Bij}(\mathbb{C}), \circ)$. Est-il abélien ?

On vérifie les 4 axiomes permettant d'affirmer que $(\text{Tr}(\mathbb{C}), \circ)$ est un sous-groupe de $(\text{Bij}(\mathbb{C}), \circ)$.

➢ **(SG1)**. $\text{Tr}(\mathbb{C}) \subset \text{Bij}(\mathbb{C})$ car toute translation de vecteur b est une bijection (de réciproque la translation de vecteur $-b$).

➢ **(SG2)**. $\text{id}_{\mathbb{C}} \in \text{Tr}(\mathbb{C})$ car $\text{id}_{\mathbb{C}} = T_0$ (l'identité est la translation de vecteur nul).

➢ **(SG3)**. La composée de deux translations T_b et $T_{b'}$ est une translation ($T_b \circ T_{b'} = T_{b+b'} = T_{b'} \circ T_b$). La composition est donc une LCI sur $\text{Tr}(\mathbb{C})$.

➢ **(SG4)**. Tout élément de $\text{Tr}(C)$ admet un inverse pour la composition, qui est encore une translation ($T_b \circ T_{-b} = \text{id}_{\mathbb{C}} = T_{-b} \circ T_b$).

Conclusion. $(\text{Tr}(\mathbb{C}), \circ)$ est un sous-groupe de $(\text{Bij}(\mathbb{C}), \circ)$. En outre, le groupe $(\text{Tr}(\mathbb{C}), \circ)$ est abélien, puisque $T_b \circ T_{b'} = T_{b+b'} = T_{b'} \circ T_b$ (pour tous b et b' dans $\mathbb{C}$).

Exercice 11. — (Groupe des rotations dans le plan complexe). On appelle **rotation dans le plan complexe** de centre $\Omega(\omega)$ et d'angle θ une application $R_{\omega,\theta}$ définie sur $\mathbb{C}$ et à valeurs dans $\mathbb{C}$, telle que :

$$\forall\, z \in \mathbb{C},\ R_{\omega,\theta}(z) = \mathrm{e}^{\mathrm{i}\,\theta}\,(z-\omega)+\omega \qquad (\text{avec } \Omega \in \mathbb{R} \text{ et } \omega \in \mathbb{C})$$

On note $\mathrm{Rot}\,(\mathbb{C})$ l'ensemble des rotations dans le plan complexe.

1/ Montrer que $(\mathrm{Rot}\,(\mathbb{C}),\circ)$ est un groupe, en prouvant que c'est un sous-groupe de $(\mathrm{Bij}(\mathbb{C}),\circ)$. Est-il abélien ?

WARNING !!! $(\mathrm{Rot}\,(\mathbb{C}),\circ)$ n'est pas un sous-groupe de $(\mathrm{Bij}(\mathbb{C}),\circ)$, car la composée de deux rotations n'est pas nécessairement une rotation.

Considérons en effet les rotations $R_1 = R_{0,\pi}$ et $R_2 = R_{1,\pi}$. L'image de z par R_1 est $-z$, et l'image de z par R_2 est $-z+1$.

L'image d'un complexe z par la composée $R_1 \circ R_2$ est le complexe $z-1$. En d'autres termes, la composée $R_1 \circ R_2$ est la translation de vecteur -1 ; en particulier elle n'admet aucun point fixe, ce qui ferait un peu désordre pour une rotation.

Conclusion. $(\mathrm{Rot}\,(\mathbb{C}),\circ)$ n'est pas un sous-groupe de $(\mathrm{Bij}(\mathbb{C}),\circ)$, car la composée de deux rotations n'est pas nécessairement une rotation.

Il est en revanche vrai que la composée de deux rotations d'angles θ_1 et θ_2 tels que $\theta_1+\theta_2 \neq 0\ [2\pi]$ est une rotation ; et il est également vrai que la composée de deux rotations de même centre est encore une rotation (la question 2 en est une illustration).

2/ On note $\mathrm{Rot}_0\,(\mathbb{C})$ l'ensemble des rotations de centre O. Montrer que $(\mathrm{Rot}_0\,(\mathbb{C}),\circ)$ est un sous-groupe de ~~$(\mathrm{Rot}\,(\mathbb{C}),\circ)$~~ $(\mathrm{Bij}\,(\mathbb{C}),\circ)$ et qu'il est abélien.

On vérifie les 4 axiomes permettant d'affirmer que $(\mathrm{Rot}_0\,(\mathbb{C}),\circ)$ est un sous-groupe de $(\mathrm{Bij}(\mathbb{C}),\circ)$.

- **(SG1)**. $\mathrm{Rot}_0\,(\mathbb{C}) \subset \mathrm{Bij}\,(\mathbb{C})$ car toute rotation de centre 0 s'écrit $z \longmapsto \mathrm{e}^{\mathrm{i}\theta}z$, et est bijective de réciproque $z \longmapsto \mathrm{e}^{-\mathrm{i}\theta}z$.
- **(SG2)**. $\mathrm{id}_{\mathbb{C}} \in \mathrm{Rot}_0\,(\mathbb{C})$ car $\mathrm{id}_{\mathbb{C}} = R_{0,0}$ (l'identité est la rotation de centre 0 et d'angle nul).
- **(SG3)**. La composée de deux rotations de centre 0 est encore une rotation de centre 0 ($R_{0,\theta_1} \circ R_{0,\theta_2} = R_{0,\theta_1+\theta_2} = R_{0,\theta_2} \circ R_{0,\theta_1}$). La composition est donc une LCI sur $\mathrm{Rot}_0\,(\mathbb{C})$.
- **(SG4)**. Tout élément de $\mathrm{Rot}_0\,(C)$ admet un inverse pour la composition, qui est encore une rotation ($R_{0,\theta_1} \circ R_{0,-\theta_1} = \mathrm{id}_{\mathbb{C}} = R_{0,-\theta_1} \circ R_{0,\theta_1}$).

Conclusion. $(\mathrm{Rot}_0\,(\mathbb{C}),\circ)$ est un sous-groupe de $(\mathrm{Bij}(\mathbb{C}),\circ)$. En outre, le groupe $(\mathrm{Rot}_0\,(\mathbb{C}),\circ)$ est abélien, puisque $R_{0,\theta_1} \circ R_{0,\theta_2} = R_{0,\theta_1+\theta_2} = R_{0,\theta_2} \circ R_{0,\theta_1}$ (pour tous θ_1 et θ_2 dans $\mathbb{R}$).

Exercice 12. — (Groupe des homothéties dans le plan complexe). On appelle **homothétie dans le plan complexe** de centre $\Omega(\omega)$ et de rapport k une application $H_{\omega,k}$ définie sur $\mathbb{C}$ et à valeurs dans $\mathbb{C}$, telle que :

$$\forall\, z \in \mathbb{C},\ H_{\omega,k}(z) = k\,(z-\omega)+\omega \qquad (\text{avec } k \in \mathbb{R}^* \text{ et } \omega \in \mathbb{C})$$

On note $\mathrm{Hom}\,(\mathbb{C})$ l'ensemble des homothéties dans le plan complexe.

1/ Montrer que $(\mathrm{Hom}\,(\mathbb{C}),\circ)$ est un groupe, en prouvant que c'est un sous-groupe de $(\mathrm{Bij}(\mathbb{C}),\circ)$. Est-il abélien ?

WARNING !!! $(\mathrm{Hom}\,(\mathbb{C}),\circ)$ n'est pas un sous-groupe de $(\mathrm{Bij}(\mathbb{C}),\circ)$, car la composée de deux homothéties n'est pas nécessairement une homothétie.

Considérons en effet les homothéties $H_1 = H_{0,-1}$ et $H_2 = H_{1,-1}$. L'image de z par H_1 est $-z$, et l'image de z par H_2 est $-z+1$.

L'image d'un complexe z par la composée $H_1 \circ H_2$ est le complexe $z-1$. En d'autres termes, la composée $H_1 \circ H_2$ est la translation de vecteur -1 ; en particulier elle n'admet aucun point fixe, ce qui ferait un peu désordre pour une homothétie.

Conclusion. $(\mathrm{Hom}(\mathbb{C}), \circ)$ n'est pas un sous-groupe de $(\mathrm{Bij}(\mathbb{C}), \circ)$, car la composée de deux homothéties n'est pas nécessairement une homothétie.

Il est en revanche vrai que la composée de deux homothéties de rapports k_1 et k_2 tels que $k_1 \times k_2 \neq 1$ est une homothétie ; et il est également vrai que la composée de deux homothéties de même centre est encore une homothétie (la question 2 en est une illustration).

2/ On note $\mathrm{Hom}_0(\mathbb{C})$ l'ensemble des homothéties de centre O. Montrer que $(\mathrm{Hom}_0(\mathbb{C}), \circ)$ est un sous-groupe de $(\mathrm{Bij}(\mathbb{C}), \circ)$, et qu'il est abélien.

On vérifie les 4 axiomes permettant d'affirmer que $(\mathrm{Hom}_0(\mathbb{C}), \circ)$ est un sous-groupe de $(\mathrm{Bij}(\mathbb{C}), \circ)$.

- **(SG1)**. $\mathrm{Hom}_0(\mathbb{C}) \subset \mathrm{Bij}(\mathbb{C})$ car toute homothétie de centre 0 s'écrit $z \longmapsto kz$ (avec $k \in \mathbb{R}^*$), et est bijective de réciproque $z \longmapsto \dfrac{1}{k} z$.
- **(SG2)**. $\mathrm{id}_{\mathbb{C}} \in \mathrm{Hom}_0(\mathbb{C})$ car $\mathrm{id}_{\mathbb{C}} = H_{0,1}$ (l'identité est l'homothétie de centre 0 et de rapport 1).
- **(SG3)**. La composée de deux homothéties de centre 0 est encore une homothétie de centre 0 ($H_{0,k_1} \circ H_{0,k_2} = H_{0,k_1k_2} = H_{0,k_2} \circ H_{0,k_1}$). La composition est donc une LCI sur $\mathrm{Hom}_0(\mathbb{C})$.
- **(SG4)**. Tout élément de $\mathrm{Hom}_0(C)$ admet un inverse pour la composition, qui est encore une homothétie ($H_{0,k_1} \circ H_{0,k_1^{-1}} = \mathrm{id}_{\mathbb{C}} = H_{0,k_1^{-1}} \circ H_{0,k_1}$).

Conclusion. $(\mathrm{Hom}_0(\mathbb{C}), \circ)$ est un sous-groupe de $(\mathrm{Bij}(\mathbb{C}), \circ)$. En outre, le groupe $(\mathrm{Hom}_0(\mathbb{C}), \circ)$ est abélien, puisque $H_{0,k_1} \circ H_{0,k_2} = H_{0,k_1k_2} = H_{0,k_2} \circ H_{0,k_1}$ (pour tous k_1 et k_2 dans $\mathbb{R}^*$).

Exercice 13. — (Groupe des similitudes directes). On rappelle que $\mathbb{C}^{\mathbb{C}}$ désigne l'ensemble des applications de $\mathbb{C}$ dans $\mathbb{C}$.

1/ Justifier brièvement que la composition usuelle (notée "$\circ$") est une loi de composition interne sur $\mathbb{C}^{\mathbb{C}}$, associative, et possédant un élément neutre.

La composition de deux applications de $\mathbb{C}$ dans $\mathbb{C}$ est encore une application de $\mathbb{C}$ dans $\mathbb{C}$, d'où la conclusion.

2/ $\left(\mathbb{C}^{\mathbb{C}}, \circ\right)$ est-il un groupe ?

La composition dans $\mathbb{C}^{\mathbb{C}}$ est une LCI (observation faite question précédente), associative (car la composition des applications en général l'est), qui possède un élément neutre ($\mathrm{id}_{\mathbb{C}}$).

Mais toute application de $\mathbb{C}$ dans $\mathbb{C}$ ne possède pas d'inverse pour la composition ; les seuls éléments de $\mathbb{C}^{\mathbb{C}}$ qui sont inversibles pour la loi "$\circ$" étant les bijections de $\mathbb{C}$ dans $\mathbb{C}$.

Conclusion. $\left(\mathbb{C}^{\mathbb{C}}, \circ\right)$ n'est pas un groupe.

3/ Pour tout $a \in \mathbb{C}^*$, et pour tout $b \in \mathbb{C}$ on définit l'application $f_{a,b} : \mathbb{C} \longrightarrow \mathbb{C}$ par : $f_{a,b}(z) = az + b$.

a/ Calculer : $f_{a',b'} \circ f_{a,b}$.

Soit $z \in \mathbb{C}$. On a :

$$\left(f_{a',b'} \circ f_{a,b}\right)(z) = f_{a',b'}\left(f_{a,b}(z)\right) = f_{a',b'}(az+b) = a'(az+b) + b' = a'az + a'b + b' = f_{a'a,a'b+b'}(z)$$

Conclusion. $\left(f_{a',b'} \circ f_{a,b}\right) = f_{a'a,a'b+b'}$

b/ Montrer que $(\{f_{a,b};\ a \in \mathbb{C}^*,\ b \in \mathbb{C}\}, \circ)$ est un groupe. Ce groupe est-il abélien ?

Notons : $E = \{f_{a,b};\ a \in \mathbb{C}^*,\ b \in \mathbb{C}\}$.

- ➤ D'après ce qui précède, la composition ("$\circ$") est une LCI sur E.
- ➤ Cette LCI est associative (puisque la composition des applications en général est associative).
- ➤ L'identité de $\mathbb{C}$, qui est l'élément neutre pour la composition, est un élément de E puisque : $\mathrm{id}_{\mathbb{C}} = f_{1,0}$.
- ➤ Reste à vérifier que tout élément de E est inversible dans E. A cette fin, considérons un élément quelconque $f_{a,b}$ de E, avec $a \in \mathbb{C}^*$ et $b \in \mathbb{C}$.

  Par définition, l'application $f_{a,b}$ est inversible si et seulement si :

$$\exists\, f_{a',b'} \in E, \quad f_{a,b} \circ f_{a',b'} = \mathrm{id}_{\mathbb{C}} = f_{a',b'} \circ f_{a,b}$$

  Or :

$$\left[f_{a',b'} \circ f_{a,b} = \mathrm{id}_{\mathbb{C}}\right] \iff \left[f_{a'a,a'b+b'} = \mathrm{id}_{\mathbb{C}}\right] \iff \left[f_{a'a,a'b+b'} = f_{1,0}\right] \iff [a'a = 1 \text{ et } a'b + b' = 0]$$

  Or :

$$\begin{cases} a'a = 1 \\ a'b + b' = 0 \end{cases} \iff \begin{cases} a' = \dfrac{1}{a} \\ b' = -\dfrac{b}{a} \end{cases}$$

  On en déduit que : $f_{1/a,-b/a} \circ f_{a,b} = \mathrm{id}_{\mathbb{C}}$.

  On vérifie alors aisément que : $f_{a,b} \circ f_{1/a,-b/a} = \mathrm{id}_{\mathbb{C}}$.

  En résumé, tout élément $f_{a,b}$ de E admet un inverse pour la composition, qui est encore un élément de E (puisque c'est : $f_{1/a,-b/a}$).

Conclusion. E est un ensemble muni d'une LCI ("$\circ$") associative, possédant un élément neutre, et dans lequel tout élément admet un inverse pour la composition. A ce titre, $(E, \circ)$ est un groupe.

En outre on a :

$$f_{2,1} \circ f_{1,1} = f_{2,3} \quad \text{et} \quad f_{1,1} \circ f_{2,1} = f_{2,2}$$

Donc : $f_{2,1} \circ f_{1,1} \neq f_{1,1} \circ f_{2,1}$.

On en déduit que E est un groupe non abélien.

Exercice 14. — Soient f_1, f_2, f_3 et f_4 les fonctions de $\mathbb{R}^*$ dans $\mathbb{R}^*$ définies par :

$$f_1(x) = x \qquad f_2(x) = \frac{1}{x} \qquad f_3(x) = -x \qquad f_4(x) = -\frac{1}{x}$$

1/ Montrer que $G = \{f_1, f_2, f_3, f_4\}$ muni de la composition $\circ$ est un groupe abélien.

Pour commencer, on prouve que la loi "o" est une LCI sur G en calculant toutes les composées de 2 éléments quelconques de G, càd en dressant la "table de multiplication" du groupe G, que voici :

$*$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

On déduit de cette table que la loi "o" est une LCI sur G (la composée de deux éléments quelconques de G étant encore un élément de G).

En outre, la loi "o" est associative (car la composition des applications est associative en général).

De plus, cette LCI possède un élément neutre : $f_1 = \mathrm{id}_{\mathbb{R}^*}$.

Enfin, tout élément de G possède un inverse dans G pour la loi $\circ$, puisque chacun des éléments de G est son propre inverse.

Il s'ensuit que $(G, \circ)$ est un groupe. Il résulte du cours [2] ou de la symétrie de la table ci-dessus par rapport à la diagonale que G est abélien.

Conclusion. $(G, \circ)$ est un groupe abélien.

2/ Déterminer l'ensemble de ses sous-groupes.

Observons qu'un sous-groupe H de G possède au plus 4 éléments, et au moins un élément (l'élément neutre). On distingue donc plusieurs cas suivant le cardinal (càd le nombre d'éléments) de H.

- Cas 1 — $\mathrm{Card}(H) = 1$ [3] : il existe un seul sous-groupe de G ayant pour cardinal 1, le **sous-groupe trivial** $(\{f_1\}, \circ)$.
- Cas 2 — $\mathrm{Card}(H) = 4$: il existe un seul sous-groupe de G ayant pour cardinal 4, le groupe G lui-même.
- Cas 3 — $\mathrm{Card}(H) = 2$: notons $H_1 = \{f_1, f_2\}$. $(H_1, \circ)$ est un sous-groupe de $(G, \circ)$ (essentiellement car f_1 est son propre inverse). De même, $H_2 = \{f_1, f_3\}$ et $H_3 = \{f_1, f_4\}$ sont deux autres sous-groupes de cardinal 2.

  Il n'existe pas d'autre sous-groupe de cardinal 2.

2. Tout groupe fini de cardinal 4 est abélien.
3. On note $\mathrm{Card}(H)$ le cardinal de H, càd le nombre d'éléments de H.

➤ Cas 4 — $\mathrm{Card}(H) = 3$: il n'existe aucun sous-groupe de cardinal 3 de G. En effet, s'il existait, un tel sous-groupe H devrait contenir l'élément neutre (f_1) et deux autres éléments de G ; or la composée de ces deux éléments sera égal au dernier élément de G, et n'appartiendra donc pas à H.

Pour illustrer ce propos par un exemple, considérons $H = \{f_1, f_2, f_3\}$. On a : $f_2 \circ f_3 = f_4$. Donc $f_2 \circ f_3 \notin H$. Donc la loi "$\circ$" n'est pas une LCI sur H. La conclusion est la même quels que soient les deux éléments que l'on choisit en plus de f_1.

Conclusion. G possède un sous-groupe de cardinal 4 (G lui-même), trois sous-groupes de cardinal 2 (H_1, H_2 et H_3), et un sous-groupe de cardinal 1 (le sous-groupe trivial).

Exercice 15. — (Centre d'un groupe). Soit G un groupe. On appelle **centre de G** et on note $Z(G)$ l'ensemble des éléments de G qui commutent avec tous les éléments de G, soit : $Z(G) = \{a \in G\ ,\ \forall\, g \in G,\ ag = ga\}$. Montrer que $Z(G)$ est un sous-groupe de G. Que devient $Z(G)$ lorsque G est abélien ?

On montre que $Z(G)$ est un sous-groupe de G en vérifiant les 4 axiomes du cours :

➤ (SG1) $Z(G) \subset G$ par définition même de $Z(G)$;

➤ (SG2) Pour tout $g \in G$, on a : $\mathrm{e} * g = g * \mathrm{e}$. Donc : $\mathrm{e} \in Z(G)$.

➤ (SG3) Soient a et b dans $Z(G)$. Pour tout élément g de G on a :

$$(a * b) * g = a * (b * g) = a\,(g * b) = (a * g) * b = (g * a) * b = g * (a * b)$$

On en déduit que $(a * b)$ appartient à $Z(G)$. En résumé : $[a \text{ et } b \in Z(G)] \Longrightarrow [a * b \in Z(G)]$.

➤ (SG4) Soit a dans $Z(G)$. Pour tout élément g de G on a :

$$a^{-1} * g = \left(g^{-1} * a\right)^{-1} = \left(a * g^{-1}\right)^{-1} = g * a^{-1}$$

On en déduit que a^{-1} appartient à $Z(G)$. En résumé : $[a \in Z(G)] \Longrightarrow \left[a^{-1} \in Z(G)\right]$.

Conclusion. D'après ce qui précède, $Z(G)$ est un sous-groupe de G.

Lorsque G est abélien, on a : $Z(G) = G$.

Exercice 16. — (Groupe diédral D_3). Décrire le groupe diédral $(D_3, \circ)$, c'est à dire le groupe des isométries du plan laissant invariant un triangle équilatéral de centre O.

Les isométries du plan laissant invariant un triangle équilatéral de centre O sont :

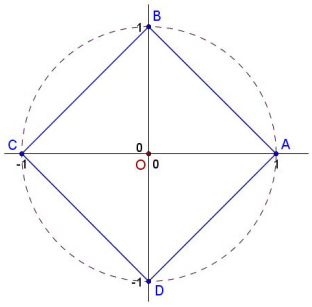
➤ l'identité ;

➤ les rotations de centre O et d'angles $2\pi/3$ et $4\pi/3$;

➤ les 3 symétries axiales ayant pour axes les 3 médiatrices de ce triangle.

Exercice 17. — (Groupe diédral D_4). La figure ci-dessous représente le carré $ABCD$, inscrit dans le cercle unité, les points A, B, C et D étant les images des racines quatrièmes de l'unité.

On dit qu'une transformation du plan **laisse le carré $ABCD$ invariant** si l'image du carré $ABCD$ par cette transformation est le carré $ABCD$ lui-même.



1/ Enumérez les huit isométries laissant le carré $ABCD$ invariant. On note D_4 l'ensemble de ces isométries.

Les isométries du plan laissant invariant le carré $ABCD$ sont :

- l'identité ;
- les rotations de centre O et d'angles $\pi/4$, $\pi/2$ et $3\pi/4$;
- les 4 symétries axiales ayant pour axes les 2 diagonales de ce carré, et les deux droites joignant les milieux des côtés opposés.

2/ Montrez que $(D_4, \circ)$ est un groupe, non-abélien (*le groupe D_4 est un exemple de ce que l'on appelle groupe* ***diédral***).

On peut montrer que $(D_4, \circ)$ est un groupe par exemple en prouvant que c'est un sous-groupe de $\big(\mathrm{Bij}(\mathbb{R}^2), \circ\big)$.

- **(SG1)**. $D_4 \subset \mathrm{Bij}\left(\mathbb{R}^2\right)$ car toute isométrie du plan est en particulier une bijection du plan dans lui-même.
- **(SG2)**. $\mathrm{id}_{\mathbb{R}^2} \in D_4$ car l'identité laisse tout le plan invariant, donc le carré $ABCD$ en particulier.
- **(SG3)**. La composée de deux éléments de D_4 est la composée de deux isométries laissant $ABCD$ invariant ; c'est donc une isométrie laissant $ABCD$ invariant !... La composition est donc une LCI sur D_4.
- **(SG4)**. Tout élément de D_4 admet un inverse pour la composition, qui est encore dans D_4 (on peut s'en convaincre rapidement en passant en revue les éléments de D_4 listés dans la question précédente).

Conclusion. $(D_4, \circ)$ est un sous-groupe de $\big(\mathrm{Bij}(\mathbb{R}^2), \circ\big)$. En outre, le groupe $(D_4, \circ)$ est non-abélien, puisque si l'on note σ la symétrie axiale d'axe (AC), on a : $\sigma \circ R(0, \pi/4) \neq R(0, \pi/4) \circ \sigma$.

Exercice 18. — (Groupe symétrique S_3). On appelle **groupe symétrique** S_3 le groupe des permutations de $[\![\, 1, 3 \,]\!]$, càd le groupe des bijections de $[\![\, 1, 3 \,]\!]$ dans lui-même.

1/ Justifier que $(S_3, \circ)$ est effectivement un groupe.

C'est un argument général, déjà évoqué en cours, et dans cette feuille d'exercices : pour tout ensemble E, l'ensemble $\mathrm{Bij}(E)$ des bijections de E dans lui-même est un groupe pour la composition des applications.

2/ Décrire en extension S_3.

$S_3 = \big\{\mathrm{id}_{[\![1,3]\!]}, (12), (13), (23), (123), (132)\big\}$

3/ Décrire tous les sous-groupes de S_3.

Observons qu'un sous-groupe H de S_3 possède au plus 6 éléments, et au moins un élément (l'élément neutre). On distingue donc plusieurs cas suivant le cardinal (càd le nombre d'éléments) de H.

- Cas 1 — $\text{Card}(H) = 1$ [4] : il existe un seul sous-groupe de S_3 ayant pour cardinal 1, le **sous-groupe trivial** $\left(\left\{\text{id}_{[\![1,3]\!]}\right\}, \circ\right)$.
- Cas 2 — $\text{Card}(H) = 6$: il existe un seul sous-groupe de S_3 ayant pour cardinal 6, le groupe H lui-même.
- Cas 3 — $\text{Card}(H) = 2$: il existe exactement trois sous-groupes de S_3 de cardinal 2, qui sont :

$$\left\{\text{id}_{[\![1,3]\!]}, (12)\right\} ; \quad \left\{\text{id}_{[\![1,3]\!]}, (13)\right\} ; \quad \left\{\text{id}_{[\![1,3]\!]}, (23)\right\}$$

- Cas 4 — $\text{Card}(H) = 3$: il existe exactement un sous-groupe de cardinal 3 de S_3, qui est :

$$\left\{\text{id}_{[\![1,3]\!]}, (123), (132)\right\}$$

- En vertu d'un théorème de Lagrange, il n'existe pas de sous-groupe de S_3 de cardinal 4 ou 5, car si G est un groupe fini de cardinal N, le cardinal d'un sous-groupe de G doit être un diviseur de N.

Conclusion. S_3 possède un sous-groupe de cardinal 6 (S_3 lui-même), trois sous-groupes de cardinal 2, un sous-groupe de cardinal 3, et un sous-groupe de cardinal 1 (le sous-groupe trivial).

Exercice 19. — (Intersection et union de sous-groupes). Soit $(G, \star)$ un groupe, H_1 et H_2 deux sous-groupes de G.

1/ Montrer que $H_1 \cap H_2$ est un sous-groupe de G.

Fait en classe.

2/ Montrer que : $[H_1 \cup H_2 \text{ est un sous-groupe de } G] \iff [H_1 \subset H_2 \text{ ou } H_2 \subset H_1]$

Fait en classe.

Exercice 20. — (Groupe additif des polynômes). Il est connu que $(\mathbb{K}[X], +)$ est un groupe. Parmi les H_i proposés ci-dessous, lesquels sont des sous-groupes additifs de $\mathbb{K}[X]$?

Dans chaque cas, il suffit de vérifier que les axiomes $(SG1)$ à $(SG4)$ lorsque la réponse est positive, ou justifier qu'un des 4 axiomes n'est pas vérifié lorsque la réponse est négative.

1/ H_1 l'ensemble des polynômes qui s'annulent en 1

H_1 est un sous-groupe additif de $\mathbb{K}[X]$.

2/ H_2 l'ensemble des pôlynômes de degré exactement 3

H_2 n'est un sous-groupe additif de $\mathbb{K}[X]$ ((SG2) n'est pas vérifié, le polynôme nul n'est pas de degré 3)

3/ H_3 l'ensemble des pôlynômes à coefficients entiers

H_3 est un sous-groupe additif de $\mathbb{K}[X]$.

4/ H_4 l'ensemble des pôlynômes représentant une fonction croissante sur $\mathbb{R}$

H_4 n'est pas un sous-groupe additif de $\mathbb{K}[X]$ ((SG4) n'est pas vérifié : X est dans H_4, mais pas $-X$).

4. On note $\text{Card}(H)$ le cardinal de H, càd le nombre d'éléments de H.

Exercice 21. — (Groupe additif des fonctions continues sur $\mathbb{R}$). Il est connu que $\left(\mathscr{C}^0(\mathbb{R},\mathbb{R}),+\right)$ est un groupe. Parmi les H_i proposés ci-dessous, lesquels sont des sous-groupes additifs de $\mathscr{C}^0(\mathbb{R},\mathbb{R})$?

Dans chaque cas, il suffit de vérifier que les axiomes $(SG1)$ à $(SG4)$ lorsque la réponse est positive, ou justifier qu'un des 4 axiomes n'est pas vérifié lorsque la réponse est négative.

1/ H_1 l'ensemble des fonctions continues sur $\mathbb{R}$ qui s'annulent en 1

H_1 est un sous-groupe additif de $\mathscr{C}^0(\mathbb{R},\mathbb{R})$.

2/ H_2 l'ensemble des fonctions constantes sur $\mathbb{R}$

H_2 est un sous-groupe additif de $\mathscr{C}^0(\mathbb{R},\mathbb{R})$.

3/ H_3 l'ensemble des fonctions continues sur $\mathbb{R}$ qui sont bornées

H_3 est un sous-groupe additif de $\mathscr{C}^0(\mathbb{R},\mathbb{R})$, et c'est un exo un peu plus amusant que les autres de le démontrer.

4/ H_4 l'ensemble des fonctions continues sur $\mathbb{R}$ qui réalisent une bijection de $\mathbb{R}$ dans $\mathbb{R}$

H_4 n'est un sous-groupe additif de $\mathscr{C}^0(\mathbb{R},\mathbb{R})$: la fonction nulle n'est pas une bijection de $\mathbb{R}$ dans $\mathbb{R}$ (l'axiome (SG2) n'est pas vérifié).

Exercice 22. — (Groupe additif des suites réelles). Il est connu que $\left(\mathbb{R}^{\mathbb{N}},+\right)$ est un groupe. Parmi les H_i proposés ci-dessous, lesquels sont des sous-groupes additifs de $\mathbb{R}^{\mathbb{N}}$?

Dans chaque cas, il suffit de vérifier que les axiomes $(SG1)$ à $(SG4)$ lorsque la réponse est positive, ou justifier qu'un des 4 axiomes n'est pas vérifié lorsque la réponse est négative.

1/ H_1 l'ensemble des suites de limite 1

H_1 n'est pas un sous-groupe additif de $\mathbb{R}^{\mathbb{N}}$ (la suite nulle n'appartient pas à H_1)

2/ H_2 l'ensemble des suites arithmétiques

H_2 est un sous-groupe additif de $\mathbb{R}^{\mathbb{N}}$

3/ H_3 l'ensemble des suites géométriques

H_3 n'est pas un sous-groupe additif de $\mathbb{R}^{\mathbb{N}}$, car la somme des suites géométriques de premier terme 1 et de raisons 2 et 3 (dont les premiers termes respectifs sont $1,2,4$ et $1,3,9$) n'est pas géométrique $(2,5,13\ldots)$

4/ H_4 l'ensemble des suites croissantes

H_4 n'est pas un sous-groupe additif de $\mathbb{R}^{\mathbb{N}}$, car la suite de terme général n est croissante, mais pas celle de terme général $-n$ (H_4 n'est pas stable par passage à l'inverse pour la loi $+$).

5/ H_5 l'ensemble des suites stationnaires

H_5 est un sous-groupe additif de $\mathbb{R}^{\mathbb{N}}$.

6/ H_6 l'ensemble des suites périodiques

H_6 est un sous-groupe additif de $\mathbb{R}^{\mathbb{N}}$.

Morphismes de groupes

Exercice 23. — (Généralités sur les morphismes de groupes).

Cet exercice est une compilation de propriétés des morphismes de groupes, démontrées en classe.

Soient $(G,*)$ et $(H,\sharp)$ deux groupes. On appelle **morphisme de groupes** une application $f : G \longrightarrow H$ telle que

$$\forall\ (g,g') \in\ G^2, \quad f\left(g *\ g'\right) = f\left(g\right) \sharp f\left(g'\right)$$

Soit f un morphisme de groupes.

1/ Montrer que $f\left(\mathrm{e}_G\right) = \mathrm{e}_H$

2/ Montrer que $f\left(g^{-1}\right) = \left[f(g)\right]^{-1}$

3/ On définit le **noyau de** f, et on note $\ker\ f$ la partie de G constituée des antécédents de e_H par f.[5] Explicitement :

$$\ker\ f = \{g \in\ G\ /\ f\left(g\right) = \mathrm{e}_H\}$$

a/ Montrer que $\ker\ f$ est un sous-groupe de G.

b/ Montrer que le morphisme f est injectif SSI $\ker\ f = \{\mathrm{e}_G\}$

4/ On définit l'**image de** f, et on note $\mathrm{im}\ f$ l'image directe de G par f. En d'autres termes :

$$\mathrm{im}\ f = f\left(G\right) = \{h \in\ H\,,\ \exists\, g \in\ G,\ f\left(g\right) = h\}$$

a/ Montrer que $\mathrm{im}\ f$ est un sous-groupe de H.

b/ Justifier que f est surjective SSI $\mathrm{im}\ f = H$.

Exercice 24. — (Groupe des automorphismes). Soit $(G,*)$ un groupe. On appelle **automorphisme** du groupe G un isomorphisme de groupes de G dans G. On note $\mathbf{Aut}\left(G\right)$ l'ensemble des automorphismes de G.

Montrer que $\left(\mathbf{Aut}\left(G\right), \circ\right)$ est un groupe.

Fait en classe.

Exercice 25. — Montrer que l'application $\begin{array}{ccc} f : (\mathbb{R},+) & \longrightarrow & \left(\mathbb{R}_+^*, \times\right) \\ x & \longmapsto & \mathrm{e}^{2x} \end{array}$ est un isomorphisme de groupes.

Il est usuel que :

$$\forall\,(x,y) \in\ \mathbb{R}^2,\ f(x+y) = \mathrm{e}^{2x+2y} = \mathrm{e}^{2x} \times \mathrm{e}^{2y} = f(x) \times f(y)$$

Il s'ensuit que f est un morphisme de groupes. Sa bijectivité est une application immédiate du théorème de la bijection (f est continue, strictement croissante, et ses limites en $-\infty$ et $+\infty$ sont respectivement 0 et $+\infty$).

Conclusion. f est un isomorphisme de groupes.

5. La notation *ker* vient de *kernel* (noyau en anglais) et/ou de *kern* (noyau en allemand).

Exercice 26. — Soit n un entier naturel $\geqslant 2$. On considère l'application : $f : (\mathbb{C}^*, \times) \longrightarrow (\mathbb{C}^*, \times)$, $z \longmapsto z^n$

1/ Montrer que f est un morphisme de groupes.

Soient z_1 et z_2 deux complexes. On a :

$$f(z_1 \times z_2) = (z_1 \times z_2)^n = z_1^n \times z_2^n = f(z_1) \times f(z_2)$$

Conclusion. f est un morphisme de groupes, car :

$$\forall\, (z_1, z_2) \in \mathbb{C}^2, \quad f(z_1 \times z_2) = (z_1 \times z_2)^n = z_1^n \times z_2^n = f(z_1) \times f(z_2)$$

2/ Déterminer le noyau de f. Le morphisme f est-il injectif ?

Par définition de noyau :

$$\ker f = \{z \in \mathbb{C}^*,\ z^n = 1\} \text{ donc } \ker f = \mathbb{U}_n$$

Puisque $\ker f \neq \{1\}$, le morphisme f n'est pas injectif.

3/ Justifier que le morphisme f est surjectif.

Selon le cours, tout complexe non-nul Z admet exactement n racines n-èmes, càd n antécédents par l'application f. On en déduit que f est surjective.

Exercice 27. — On considère l'application : $f : (\mathbb{U}_8, \times) \longrightarrow (\mathbb{U}_4, \times)$, $z \longmapsto z^2$

1/ Montrer que l'application f est bien définie, càd justifier que : $f(\mathbb{U}_8) \subset \mathbb{U}_4$.

Soit $z \in \mathbb{U}_8$. On a : $f(z)^4 = \left(z^2\right)^4 = z^8 = 1$. D'où : $f(z) \in \mathbb{U}_4$.

Conclusion. $f(\mathbb{U}_8) \subset \mathbb{U}_4$

2/ Montrer que f est un morphisme de groupes, et qu'il est surjectif.

Soient z_1 et z_2 deux éléments de $\mathbb{U}_8$. On a :

$$f(z_1 \times z_2) = (z_1 \times z_2)^2 = z_1^2 \times z_2^2 = f(z_1) \times f(z_2)$$

Ainsi f est un morphisme de groupes.

En outre, f est surjectif car : $1 = f(1)$; $\mathrm{i} = f(\mathrm{e}^{\mathrm{i}\pi/4})$; $-1 = f(\mathrm{i})$; et $-\mathrm{i} = f(\mathrm{e}^{3\mathrm{i}\pi/4})$.

Conclusion. f est un morphisme de groupes surjectif.

$$\forall\, (z_1, z_2) \in \mathbb{C}^2, \quad f(z_1 \times z_2) = (z_1 \times z_2)^n = z_1^n \times z_2^n = f(z_1) \times f(z_2)$$

3/ Déterminer le noyau de f. Est-il injectif ?

Par définition de noyau :

$$\ker f = \left\{z \in \mathbb{U}_8,\ z^2 = 1\right\} \text{ donc } \ker f = \mathbb{U}_2$$

Puisque $\ker f \neq \{1\}$, le morphisme f n'est pas injectif.

Exercice 28. — On considère l'application [6] : $f : (\mathbb{R}_2[X], +) \longrightarrow (\mathbb{R}, +)$

$$P \longmapsto \int_0^1 P(t)\,\mathrm{d}t$$

1/ Montrer que f est un morphisme de groupes.

Pour tout couple de polynômes (P, Q) de $\mathbb{R}_2[X]$, on a :

$$f(P+Q) = \int_0^1 (P+Q)(t)\,\mathrm{d}t = \int_0^1 P(t)+Q(t)\,\mathrm{d}t = \int_0^1 P(t)\,\mathrm{d}t + \int_0^1 Q(t)\,\mathrm{d}t = f(P)+f(Q)$$

la première égalité provenant de la définition de f, la deuxième de celle de la fonction $(P+Q)$, et la troisième de la linéarité de l'intégrale.

Conclusion. f est un morphisme de groupes.

2/ Déterminer le noyau de f. Le morphisme f est-il injectif ?

Soit $P = aX^2 + bX + c$ dans $\mathbb{R}_2[X]$. On a :

$$\begin{aligned}
&P \in \ker f \\
&\iff f(P) = 0 \\
&\iff \int_0^1 at^2 + bt + c\,\mathrm{d}t = 0 \\
&\iff \frac{a}{3} + \frac{b}{2} + c = 0 \\
&\iff c = -\frac{a}{3} - \frac{b}{2}
\end{aligned}$$

En résumé :

$$[P \in \ker f] \iff \left[\exists\,(a,b) \in \mathbb{R}^2,\ P = aX^2 + bX - \frac{a}{3} - \frac{b}{2}\right]$$

Soit encore :

$$[P \in \ker f] \iff \left[\exists\,(a,b) \in \mathbb{R}^2,\ P = a\left(X^2 - \frac{1}{3}\right) + b\left(X - \frac{1}{2}\right)\right]$$

Conclusion. $\ker f = \left\{a\left(X^2 - \frac{1}{3}\right) + b\left(X - \frac{1}{2}\right),\ (a,b) \in \mathbb{R}^2\right\}$

En d'autres termes, $\ker f$ est l'ensemble des combinaisons linéaires des polynômes $X^2 - \frac{1}{3}$ et $X - \frac{1}{2}$; dans un sens qui sera rendu plus précis au second semestre, c'est le plan engendré par les polynômes $X^2 - \frac{1}{3}$ et $X - \frac{1}{2}$.

En particulier, puisque $\ker f \neq \{\tilde{0}\}$, le morphisme f n'est pas injectif.

3/ Justifier que le morphisme f est surjectif.

Pour tout $c \in \mathbb{R}$, on a : $c = \int_0^1 c\,\mathrm{d}t = f(c)$. Donc : $\mathrm{im}\ f = \mathbb{R}$.

Conclusion. Le morphisme f est surjectif.

---

6. On rappelle que $\mathbb{R}_2[X]$ désigne l'ensemble des polynômes à coefficients réels, de degré inférieur ou égal à 2. Explicitement, tout élément de $\mathbb{R}_2[X]$ peut s'écrire $aX^2 + bX + c$, avec $(a,b,c) \in \mathbb{R}^3$.

Exercice 29. — On considère l'application : $f : \left(\mathbb{R}^{\mathbb{N}}, +\right) \longrightarrow \left(\mathbb{R}^2, +\right)$
$$(u_n)_n \longmapsto (u_0, u_1)$$

1/ Montrer que f est un morphisme de groupes.

Il est immédiat que :

$$\forall\, ((u_n)_n, (v_n)_n) \in \mathbb{R}^{\mathbb{N}} \times \mathbb{R}^{\mathbb{N}}, \quad f\left((u_n)_n + (v_n)_n\right) = (u_0 + v_0, u_1 + v_1) = f\left((u_n)_n\right) + f\left((v_n)_n\right)$$

Conclusion. f est un morphisme de groupes.

2/ Justifier que le morphisme f est surjectif, et non-injectif.

Le morphisme f est surjectif car on peut trouver une suite réelle dont les 2 premiers termes sont deux réels quelconques (et même une infinité !).

Le morphisme f n'est pas injectif car une suite réelle n'est pas définie de manière unique par ses deux premiers termes...

Exercice 30. — Lorsque $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est une matrice de $\mathrm{M}_2(\mathbb{R})$, on appelle **déterminant** de A et on note $\det(A)$ (ou $|A|$) le réel :
$$\det(A) = ad - bc$$
Par ailleurs, on note $\mathrm{GL}_2(\mathbb{R})$ le groupe multiplicatif des matrices inversibles de $\mathrm{M}_2(\mathbb{R})$.

1/ Etablir que l'application $\det : \left(\mathrm{GL}_2(\mathbb{R}), \times\right) \longrightarrow (\mathbb{R}\times)$ est un morphisme de groupes.
$$A \longmapsto \det(A)$$

A l'aide d'une vérification laborieuse mais sans aucune difficulté, on peut établir que :

$$\det(A \times B) = \det(A) \times \det(B)$$

Cette propriété sera démontrée dans le cadre plus général des matrices carrées de taille quelconque au second semestre.

2/ Quel est le noyau du morphisme det ?

Le noyau du morphisme det est :

$$\ker \det = \{A \in \mathrm{GL}_2(\mathbb{R}),\ \det(A) = 1\}$$

Selon le cours, c'est une sous-groupe de $\mathrm{GL}_2(\mathbb{R})$, que l'on appellera groupe **spécial linéaire** au second semestre.

3/ Justifier que le morphisme det est surjectif.

Tout réel x non nul admet au moins un antécédent par le morphisme det, par exemple :

$$\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$$

Ce qui prouve la surjectivité de det.

Exercice 31. — On considère l'application : $\Delta : \left(\mathscr{C}^1(\mathbb{R},\mathbb{R}),+\right) \longrightarrow \left(\mathscr{C}^0(\mathbb{R},\mathbb{R}),+\right)$, $f \longmapsto f'$

1/ Justifier que Δ est un morphisme de groupes, et qu'il est surjectif.

Δ est un morphisme de groupes par linéarité de la dérivation ; il est surjectif d'après le théorème fondamental de l'Analyse.

2/ Déterminer le noyau de Δ. Est-il injectif ?

$\ker\Delta$ est l'ensemble des fonctions constantes sur $\mathbb{R}$; puisque c'est un sous-groupe non trivial de $\left(\mathscr{C}^1(\mathbb{R},\mathbb{R}),+\right)$, le morphisme Δ n'est pas injectif.

Exercice 32. — Montrer que $(\mathrm{Tr}(\mathbb{C}),\circ)$ et $(\mathbb{C},+)$ sont isomorphes.

Il suffit par exemple de vérifier que l'application

$$f : (\mathrm{Tr}(\mathbb{C}),\circ) \longrightarrow (\mathbb{C},+), \quad T_b \longmapsto b$$

est un isomorphisme de groupes.

Exercice 33. — Montrer que $(D_3,\circ)$ et $(S_3,\circ)$ sont isomorphes.

En numérotant 1, 2 et 3 les sommets d'un triangle équilatéral de côté O, on peut associer naturellement à tout élément de D_3 un élément de S_3 ; ce procédé induit un isomorphisme de groupes entre $(D_3,\circ)$ et $(S_3,\circ)$.

Exercice 34. — Montrer que $(D_4,\circ)$ et $(S_4,\circ)$ ne sont pas isomorphes.

$(D_4,\circ)$ et $(S_4,\circ)$ ne sont pas isomorphes car les ensembles D_4 et S_4 ne sont pas de même cardinal (8 pour D_4, et 24 pour S_4).

Anneaux, corps

Exercice 35. — On note $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, et $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$. Montrer que $(\mathbb{K}[X],+,\times)$ est un anneau commutatif. Est-ce encore vrai si l'on remplace $\mathbb{K}[X]$ par $\mathbb{K}_n[X]$?

On montre que $(\mathbb{K}[X],+,\times)$ est un anneau commutatif en passant en revue le catalogue d'axiomes du cours qui permettent de l'affirmer. Ceci fait, on pourra à l'avenir utiliser la conscience tranquille ce résultat comme un "théorème général" !

En revanche, $\mathbb{K}_n[X]$ n'est pas un anneau car il n'est pas stable pour la multiplication (sauf si $n = 0\ldots$).

Exercice 36. — On note $\mathbb{D}$ l'ensemble des nombres décimaux : $\mathbb{D} = \left\{ \frac{n}{10^k} \;|n \in \mathbb{Z},\ k \in \mathbb{N} \right\}$. Montrer que $\mathbb{D}$ est un sous-anneau de $(\mathbb{R},+,\times)$.

$(\mathbb{D},+,\times)$ est un sous-anneau de $(\mathbb{R},+,\times)$ car :

- $(\mathbb{D},+)$ est un sous-groupe de $(\mathbb{R},+)$ selon un exercice précédent de cette feuille.
- La multiplication est une LCI associative sur $\mathbb{D}$ (il suffit de vérifier que le produit de deux décimaux est encore décimal), et possède un élément neutre (1 est un décimal, puisque $1 = 1/10^0\ldots$).

On peut observer que l'anneau $\mathbb{D}$ n'est pas un corps, puisque 3 est décimal mais que son inverse pour la multiplication ne l'est pas.

Exercice 37. — Montrer que $(\mathscr{F}(\mathbb{R},\mathbb{R}),+,\times)$ est un anneau commutatif. Est-il intègre ?

$(\mathscr{F}(\mathbb{R},\mathbb{R}),+,\times)$ est un anneau commutatif car :

- $(\mathscr{F}(\mathbb{R},\mathbb{R}),+)$ est un groupe abélien : l'addition est une LCI associative et commutative, possédant un élément neutre (la fonction identiquement nulle sur $\mathbb{R}$), et toute fonction f définie sur $\mathbb{R}$ admet un inverse pour la l'addition (son opposée $-f$).
- La multiplication est une LCI associative sur $\mathscr{F}(\mathbb{R},\mathbb{R})$, et possède un élément neutre (la fonction constante égale à 1 sur $\mathbb{R}$), et la multiplication est distributive par rapport à l'addition dans $\mathscr{F}(\mathbb{R},\mathbb{R})$.

On peut observer que l'anneau $\mathscr{F}(\mathbb{R},\mathbb{R})$ n'est pas un corps, puisque la fonction sin (qui est non nulle) n'est pas inversible pour la multiplication dans $\mathscr{F}(\mathbb{R},\mathbb{R})$ (la fonction $1/\sin$ n'est pas définie sur $\mathbb{R}$ tout entier).

Exercice 38. — **(Anneau des entiers de Gauss).** On pose $\mathbb{Z}[i]=\{a+ib,\,(a,b)\in\mathbb{Z}^2\}$. Montrer que $(\mathbb{Z}[i],+,\times)$ est un anneau commutatif. Est-ce un corps ?

On peut montrer que $(\mathbb{Z}[\mathrm{i}],+,\times)$ est un anneau commutatif directement, ou en prouvant que c'est un sous-anneau de $(\mathbb{C},+,\times)$. On utilise ici cette seconde méthode, pour changer :

- $(\mathbb{Z}[\mathrm{i}],+)$ est un sous-groupe de $(\mathbb{C},+)$ car $\mathbb{Z}[\mathrm{i}]\subset\mathbb{C}$, $0\in\mathbb{Z}[\mathrm{i}]$ (car $0=0+\mathrm{i}0$, pas d'applaudissements...), la somme de deux éléments de $\mathbb{Z}[\mathrm{i}]$ est encore dans $\mathbb{Z}[\mathrm{i}]$, et si tout élément $a+\mathrm{i}b$ de $\mathbb{Z}[\mathrm{i}]$ admet un inverse pour la loi $+$ dans $\mathbb{Z}[\mathrm{i}]$ (son opposé $-a-\mathrm{i}b$).
- La multiplication est une LCI associative sur $\mathbb{Z}[\mathrm{i}]$ (il suffit de vérifier que le produit de deux entiers de Gauss en est encore un), et possède un élément neutre (1 est un décimal, puisque $1=1+\mathrm{i}0\ldots$).

On en déduit que $\mathbb{Z}[\mathrm{i}]$ est un sous-anneau de l'anneau des nombres complexes. A ce titre, $\mathbb{Z}[\mathrm{i}]$ est un anneau.

En revanche, l'anneau $\mathbb{Z}[\mathrm{i}]$ des entiers de Gauss n'est pas un corps : 2 est un entier de Gauss, mais son inverse $1/2$ n'est pas dans $\mathbb{Z}[\mathrm{i}]$.

Exercice 39. — On pose $\mathbb{Q}[i]=\{a+ib,\,(a,b)\in\mathbb{Q}^2\}$. Montrer que $(\mathbb{Q}[i],+,\times)$ est un corps.

On peut montrer comme dans l'exercice précédent que $(\mathbb{Q}[\mathrm{i}],+,\times)$ est un anneau commutatif en prouvant que c'est un sous-anneau de $(\mathbb{C},+,\times)$.

Pour prouver que c'est un corps, il suffit de prouver que tout élément non nul de $\mathbb{Q}[\mathrm{i}]$ est inversible pour la multiplication dans $\mathbb{Q}[\mathrm{i}]$.

Soit $a+\mathrm{i}b\neq 0$ dans $\mathbb{Q}[\mathrm{i}]$ (a et b sont donc rationnels). Alors :

$$\frac{1}{a+\mathrm{i}b}=\frac{a-\mathrm{i}b}{a^2+b^2}=\frac{a}{a^2+b^2}+\frac{-b}{a^2+b^2}\,\mathrm{i}$$

Puisque $\dfrac{a}{a^2+b^2}$ et $\dfrac{-b}{a^2+b^2}$ sont rationnels (a et b le sont, $a^2+b^2\neq 0$, et $\mathbb{Q}$ est un corps), on en déduit que $\dfrac{1}{a+\mathrm{i}b}\in\mathbb{Q}[\mathrm{i}]$. Donc tout élément non nul de $\mathbb{Q}[\mathrm{i}]$ est inversible pour la multiplication dans $\mathbb{Q}[\mathrm{i}]$.

On en déduit que $(\mathbb{Q}[\mathrm{i}],+,\times)$ est un corps (c'est d'ailleurs un sous-corps de $\mathbb{C}$).

Exercice 40. — On note $\mathbb{Q}(\sqrt{2})$ l'ensemble des nombres réels pouvant s'écrire $a+b\sqrt{2}$ (avec $a\in\mathbb{Q}$ et $b\in\mathbb{Q}$). Montrer que $\mathbb{Q}(\sqrt{2})$ est un sous-corps de $(\mathbb{R},+,\times)$.

Copier-coller-adapter de l'exo précédent.

Exercice 41. — **(Eléments nilpotents dans un anneau).** Soit $(A, +, \times)$ un anneau.

Un élément a de A est dit **nilpotent** s'il existe un entier naturel n non nul tel que $a^n = 0_A$.

1/ Soit $a \in A$. On suppose que a est nilpotent. Montrer que a n'est pas inversible.

On peut raisonner par l'absurde : si a est inversible, alors a^n est inversible pour tout $n \in \mathbb{N}$, donc ne peut être nul.

2/ Soient a et b deux éléments nilpotents de A. **On suppose que** $ab = ba$.

a/ Montrer que ab est nilpotent.

Utiliser la définition de nilpotent, et le fait que si $ab = ba$, alors : $(ab)^n = a^n b^n$ pour tout entier naturel n.

b/ Montrer que $a + b$ est nilpotent.

Utiliser la définition de nilpotent, et le fait que si $ab = ba$, alors on peut utiliser le binôme de Newton pour calculer $(a + b)^n$ pour tout entier naturel n.

3/ Soit $a \in A$. On suppose que a est nilpotent. Montrer que $1_A - a$ est inversible, et déterminer son inverse.

Supposons que a est nilpotent, et notons n un entier naturel non nul tel que $a^n = 0_A$.

Selon le cours :

$$1_A - a^n = (1_A - a) \times \sum_{k=0}^{n-1} a^k \iff (1_A - a) \times \sum_{k=0}^{n-1} a^k = 1$$

Il s'ensuit que $1_A - a$ est inversible, et : $(1_A - a)^{-1} = \sum_{k=0}^{n-1} a^k$.

Exercice 42. — Soit n un entier naturel supérieur ou égal à 2. On considère les applications :

$$\Delta : (\mathbb{R}_n[X], +) \longrightarrow (\mathbb{R}_n[X], +) \qquad P \longmapsto P'$$

et

$$\varphi : (\mathbb{R}_n[X], +) \longrightarrow (\mathbb{R}_n[X], +) \qquad P \longmapsto P - P'$$

1/ Justifier brièvement que Δ et φ sont des morphismes de groupes.

Pour tout couple de polynômes (P, Q) on vérifie sans peine que

$$\Delta(P + Q) = \Delta(P) + \Delta(Q) \quad \text{et} \quad \varphi(P + Q) = \varphi(P) + \varphi(Q)$$

2/ Etablir que $\Delta^{n+1} = 0$.

La dérivée $(n + 1)$-ème d'un polynôme de degré au plus n est clairement nulle.

3/ Montrer que φ est un isomorphisme de groupes, et déterminer explicitement φ^{-1}.

D'après l'exercice précédent, φ est inversible pour la loi $\circ$ et :

$$\varphi^{-1} = \sum_{k=0}^{n} \varphi^k$$

Exercice 43. — **(Anneau des entiers de Gauss)**. On pose $\mathbb{Z}[i] = \{a + ib \,|\, (a,b) \in \mathbb{Z}^2\}$ et $\mathbb{Q}[i] = \{a + ib \,|\, (a,b) \in \mathbb{Q}^2\}$. Il a déjà été établi au cours des exercices précédents que le premier est un anneau commutatif, et le second un corps.

On définit l'application $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$ par : $\forall z \in \mathbb{Z}[i]$, $N(z) = z\bar{z}$.

1/ Montrer que pour tout $(z, z') \in \mathbb{Z}[i]^2$, $N(zz') = N(z)N(z')$.

Soient z et z' dans $\mathbb{Z}[i]$. On a : $N(zz') = zz'\overline{zz'} = z\bar{z}z'\overline{z'} = N(z)N(z')$.

2/ En déduire que : z est inversible dans $\mathbb{Z}[i] \iff N(z) = 1$

Soit $z \in \mathbb{Z}[i]$. Si z est inversible dans $\mathbb{Z}[i]$, alors il existe $z' \in \mathbb{Z}[i]$ tel que : $zz' = 1$.

On en déduit que : $N(zz') = N(1)$. D'après la question précédente, on a donc : $N(z)N(z') = 1$. Or $N(z)$ $N(z')$ sont des entiers naturels ; il s'ensuit que $N(z) = N(z') = 1$.

Ce qui prouve l'implication : z est inversible dans $\mathbb{Z}[i] \Longrightarrow N(z) = 1$.

Réciproquement, supposons que $N(z) = 1$. Alors $z = a + ib$ avec a et b entiers naturels tels que : $a^2 + b^2 = 1$. Ceci implique que ($a = \pm 1$ et $b = 0$) ou ($a = 0$ et $b = \pm 1$). D'où $z = \pm 1$ ou $z = \pm \mathrm{i}$. Chacun de ces 4 entiers de Gauss étant inversible pour la multiplication dans $\mathbb{Z}[i]$ (1 et -1 sont leurs propres inverses, i et $-\mathrm{i}$ sont inverses l'un de l'autre), on a prouvé l'implication réciproque.

Conclusion. z est inversible dans $\mathbb{Z}[i] \iff N(z) = 1$

3/ Déterminer l'ensemble des éléments inversibles de $\mathbb{Z}[i]$. Vérifier qu'il s'agit d'un groupe bien connu.

D'après les calculs de la question précédente, l'ensemble des éléments inversibles (pour la multiplication) de $\mathbb{Z}[i]$ est :

$$(\mathbb{Z}\,[\mathrm{i}])^* = \{1, -1, \mathrm{i}, -\mathrm{i}\}$$

En d'autres termes : $(\mathbb{Z}\,[\mathrm{i}])^* = \mathbb{U}_4$. D'après le cours [7], $(\mathbb{Z}\,[\mathrm{i}])^*$ est un groupe (abélien).

Exercice 44. — Soit F un sous-corps de $(\mathbb{Q}, +, \times)$. Montrer que $F = \mathbb{Q}$.

Plan de la preuve :

- $1 \in F$ par définition de sous-corps.
- Donc $\mathbb{N} \subset F$ par récurrence, et en utilisant le fait que l'addition est une LCI sur F.
- Donc $\mathbb{Z} \subset F$ en utilisant le fait précédent, et le fait que l'opposé de tout élément de F est encore dans F, puisque $(F, +)$ est un sous-groupe de $(\mathbb{Q}, +)$.
- Soit $\dfrac{a}{b}$ un rationnel, avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Alors $a \in F$ (cf second point) ; et $1/b \in F$, puisque b est un élément non nul de $\mathbb{N}$ donc de F, et que tout élément non nul de F est inversible dans F (puisque F est un sous-corps de $\mathbb{Q}$ par hypothèse). On en déduit que $a \times (1/b)$ est un élément de F (la multiplication étant une LCI sur F, toujours par hypothèse). Donc : $\dfrac{a}{b} \in F$.
- Ce qui précède prouve que : $\mathbb{Q} \subset F$. Or $F \subset \mathbb{Q}$ par hypothèse. D'après la règle de double inclusion, on en déduit que $F = \mathbb{Q}$.

Conclusion. $\mathbb{Q}$ n'admet pas d'autre sous-corps que $\mathbb{Q}$ lui-même.

7. Vous pouvez utiliser sans justification le résultat du cours affirmant que $(\mathbb{U}_n, \times)$ est un groupe (abélien), car c'est un sous-groupe de $(\mathbb{U}, \times)$, qui est lui-même un sous-groupe de $(\mathbb{C}^*, \times)$.

Exercice 45. — (Un théorème de Lagrange sur les groupes finis). *Ce problème a pour objectif la preuve d'un théorème dû à Lagrange (1736-1813) concernant les groupes finis, qui permet de démontrer en particulier que tout groupe de cardinal 5 est abélien.*

Notations et rappels. Soit $(G,*)$ un groupe. Pour tout élément g de G, on note $g^2 = g*g$; $g^3 = g*g*g$ et plus généralement pour tout entier $n \in \mathbb{N}$: $g^n = \underbrace{g*g*\cdots*g}_{n \text{ termes}}$.

Cette définition est étendue à un exposant dans $\mathbb{Z}$, en posant pour tout $n \in \mathbb{Z}_-$: $g^n = \left(g^{-1}\right)^{-n}$.

On note par ailleurs : $\langle g \rangle = \left\{g^k \ / \ k \in \mathbb{Z}\right\}$.

➤ **Partie A - Ordre d'un élément dans un groupe**.

Soient $(G,*)$ un groupe, d'élément neutre e, et g un élément de G.

1/ Montrer que $\langle g \rangle$ est un sous-groupe de G *(qui sera appelé le* ***sous-groupe engendré par*** *g).*

2/ **Deux exemples**.

a/ Dans $(S_3, \circ)$, quel est le sous groupe engendré par le 3-cycle (132) ?

b/ Dans $(\mathbb{Z}, +)$, quel est le sous-groupe engendré par 2 ?

3/ On revient au cas général. On dit qu'un élément g de G est **d'ordre fini** s'il existe un entier naturel N non nul tel que $g^N = \text{e}$. Dans ce cas, on appelle **ordre de** g le plus petit N non nul tel que $g^N = \text{e}$.

a/ Exemple 1 : dans $(S_3, \circ)$, quel est l'ordre du 3-cycle $\sigma = (123)$?

b/ Exemple 2 : dans $(\mathrm{GL}_2(\mathbb{R}), \times)$, donner un exemple d'élément qui n'est pas d'ordre fini.

c/ Montrer que si G est fini, tout élément g de G est d'ordre fini.

d/ Soit g un élément de G d'ordre N, et soit m un entier. Etablir que $g^m = \text{e}$ si et seulement si N divise m.

➤ **Partie B - Un théorème de Lagrange**. Le but de cette partie est d'établir que le cardinal de tout sous-groupe d'un groupe fini divise le cardinal de G. Soient donc G un groupe fini, et H un sous-groupe de G. Pour tout élément g de G, on note : $gH = \{g*h\,,\ h \in H\}$.

4/ Etablir que pour tout élément g de G, on a : $\mathrm{Card}\,(gH) = \mathrm{Card}\,(H)$.

5/ Soient g et g' deux éléments de G. Montrer que les ensembles gH et $g'H$ sont soit égaux, soit disjoints.

6/ En déduire que le cardinal de H divise celui de G.

7/ Application : établir que l'ordre d'un élément g de G divise le cardinal de G.

➤ **Partie C - Abélianité des groupes de cardinal 5**.

Un groupe G fini est appelé **cyclique** s'il existe un élément g de G tel que $G = \langle g \rangle$.

8/ Etablir que si G est un groupe cyclique, alors G est abélien.

9/ Montrer que si G est de cardinal 5, alors G est cyclique (donc abélien). [8]

8. Ce qui évite la très rébarbative rédaction de toutes les tables de multiplication possibles pour un groupe de cardinal 5. Plus généralement, la méthode utilisée dans ce problème permet d'affirmer que tout groupe dont le cardinal est un nombre premier est abélien.

➤ Partie A - Générateurs du groupe alterné.

1) $S_3 = \{\mathrm{id}, (12), (13), (23), (123), (132)\}$ et $A_3 = \{\mathrm{id}, (123), (132)\}$.

Le groupe A_3 a exactement deux sous-groupes : $\{\mathrm{id}\}$ et A_3.

2) a) Soient τ_1 et τ_2 deux transpositions de S_n. Leurs supports (de cardinal 2) peuvent avoir une intersection constituée de 0, 1 ou 2 éléments.

1er cas — Si $\mathrm{Card}\,(\mathrm{supp}\,(\tau_1) \cap \mathrm{supp}\,(\tau_2)) = 0$: alors il existe quatre entiers distincts i, j, k et l tels que $\tau_1 = (ij)$ et $\tau_2 = (kl)$.

Dans ce cas on a : $\tau_1\tau_2 = (ij)(kl) = (kjl)(ikj)$.

2ème cas — Si $\mathrm{Card}\,(\mathrm{supp}\,(\tau_1) \cap \mathrm{supp}\,(\tau_2)) = 1$: alors il existe trois entiers distincts i, j et k tels que $\tau_1 = (ij)$ et $\tau_2 = (ik)$.
Dans ce cas on a : $\tau_1\tau_2 = (ij)(ik) = (ikj)$.

3ème cas — Si $\mathrm{Card}\,(\mathrm{supp}\,(\tau_1) \cap \mathrm{supp}\,(\tau_2)) = 2$: alors il existe deux entiers distincts i et j tels que $\tau_1 = (ij)$ et $\tau_2 = (ij)$.
Dans ce cas on a : $\tau_1\tau_2 = (ij)(ij) = \mathrm{id} = (123)\,(132)$ (par exemple).

Bilan : dans tous les cas, on a pu écrire $\tau_1\tau_2$ soit comme un 3-cycle, soit comme un produit de deux 3-cycles.

Conclusion. Le produit de deux transpositions de S_n est soit un 3-cycle, soit le produit de deux 3-cycles.

b) Soit σ un élément de A_n. Puisque S_n est engendré par les transpositions, il existe m transpositions $\tau_1, \ldots, \tau_m$ telles que : $\sigma = \prod_{k=1}^{m} \tau_k$. Or, σ étant un élément de A_n, l'entier m est nécessairement pair ; ainsi il existe un entier m' tel que $m = 2m'$. On a donc :

$$\sigma = \prod_{k=1}^{2m'} \tau_k \qquad \text{soit}\ ^{9} : \qquad \sigma = \prod_{k=1}^{m'} (\tau_{2k-1}\tau_{2k})$$

Or d'après la question précédente, chacun des termes $\tau_{2k-1}\tau_{2k}$ est un 3-cycle, ou un produit de 3-cycles. Il s'ensuit que σ est un produit de 3-cycles.

Conclusion. Tout élément de A_n peut s'écrire comme un produit de 3-cycles. En d'autres termes, le groupe alterné A_n est engendré par les 3-cycles.

➤ Partie B - Ordre d'un élément dans un groupe.

3) Soit g un élément de G. Montrons que $\langle g\rangle$ est un sous-groupe de G.

SG1 : $\langle g\rangle \subset G$ par définition.

SG2 : $\mathrm{id} = g^0 \in \langle g\rangle$.

SG3 : soient γ et γ' deux éléments de $\langle g\rangle$. Par définition de $\langle g\rangle$, il existe deux entiers k et k' tels que : $\gamma = g^k$ et $\gamma' = g^{k'}$. Il s'ensuit que : $\gamma * \gamma' = g^{k+k'}$, d'où en particulier $\gamma * \gamma' \in \langle g\rangle$.
En résumé : $\left[(\gamma, \gamma') \in \langle g\rangle^2\right] \Longrightarrow [(\gamma * \gamma') \in \langle g\rangle]$

SG4 : soit γ un élément de $\langle g\rangle$. Par définition de $\langle g\rangle$, il existe un entier k tel que : $\gamma = g^k$. Il s'ensuit que : $\gamma^{-1} = g^{-k}$, d'où en particulier $\gamma^{-1} \in \langle g\rangle$. En résumé : $[\gamma \in \langle g\rangle] \Longrightarrow \left[\gamma^{-1} \in \langle g\rangle\right]$

Conclusion. Pour tout élément g de G, $\langle g\rangle$ est un sous-groupe de G.

4) a) On a : $(123)^0 = \mathrm{id}$; $(123)^1 = (123)$; $(123)^2 = (132)$ et $(123)^3 = \mathrm{id}$. Il s'ensuit que $\langle(123)\rangle = A_3$.

b) Dans $(\mathbb{Z}, +)$, le sous-groupe engendré par 2 est $2\mathbb{Z}$, le sous-groupe des entiers pairs.

9. En "faisant des paquets de deux".

5) a) On a : $(1234)^1 = (1234)$; $(1234)^2 = (13)(24)$; $(1234)^3 = (1432)$ et $(1234)^4 = \mathrm{id}$.

Il s'ensuit que le 4-cycle (1234) est d'ordre 4.

b) Dans $(\mathrm{GL}_2(\mathbb{R}), \times)$, on considère $g = 2\mathrm{I}_2$. La matrice g est telle que : $\forall\, n \in \mathbb{N},\ g^n = 2^n \mathrm{I}_2$. Par conséquent : $\forall\, n \in \mathbb{N}^*,\ g^n \neq \mathrm{I}_2$. Il s'ensuit que la matrice g n'est pas d'ordre fini dans $\mathrm{GL}_2(\mathbb{R})$.

c) Soient G un groupe fini, et g un élément de G. Notons $n = \mathrm{Card}(G)$. On considère l'ensemble : $\{g^k \,/\, k \in [\![\, 0, n \,]\!]\}$. Si tous les éléments de cet ensemble étaient distincts, alors son cardinal serait $(n+1)$; ceci est absurde, puisqu'il s'agit d'une partie de G, qui est de cardinal n par hypothèse.

Il existe donc deux entiers k et k' distincts dans $[\![\, 0, n \,]\!]$ tels que : $g^k = g^{k'}$. Sans nuire à la généralité on peut supposer que $k < k'$ (si ce n'est pas le cas, on permute les rôles de k et k'). On a alors : $g^0 = g^{k'-k}$, c'est à dire : $g^{k'-k} = \mathrm{e}$.
En observant que $k' - k$ est un entier naturel non nul (puisque $k < k'$), on a établi l'existence d'un élément N de $\mathbb{N}^*$ tel que $g^N = \mathrm{e}$. Ce qui signifie que g est d'ordre fini.

Conclusion. Tout élément d'un groupe fini est d'ordre fini.

d) Soit g un élément de G d'ordre N, et soit m un entier.

Supposons que N divise m : alors il existe un entier k tel que $m = kN$. Il s'ensuit que : $g^m = g^{kN} = \left(g^N\right)^k = \mathrm{e}^k = \mathrm{e}$. D'où : $[N \text{ divise } m] \Longrightarrow [g^m = \mathrm{e}]$.

Réciproquement, supposons que $g^m = \mathrm{e}$. D'après le théorème de la division euclidienne, il existe un (unique) couple (q, r) tel que $m = Nq + r$ avec $q \in \mathbb{Z}$ et $r \in [\![\, 0, N-1 \,]\!]$. On a alors : $g^{Nq+r} = g^{Nq} * g^r = \mathrm{e} * g^r = g^r$; et donc $g^r = \mathrm{e}$.

Si r était non nul, on aurait alors prouvé l'existence d'un élément r de $\mathbb{N}^*$ tel que $g^r = \mathrm{e}$, avec r strictement inférieur à l'ordre de g : contradiction.

On en déduit que $r = 0$, ce qui implique que $m = Nq$, et donc que N divise m. D'où : $[g^m = \mathrm{e}] \Longrightarrow [N \text{ divise } m]$.

Conclusion. Pour g un élément d'ordre N on a : $[g^m = \mathrm{e}] \Longleftrightarrow [N \text{ divise } m]$.

➤ **Partie C - Un théorème de Lagrange**. Le but de cette partie est d'établir que le cardinal de tout sous-groupe d'un groupe fini divise le cardinal de G.

6) Soit H un sous-groupe d'un groupe fini G. Observons que H est de cardinal fini, en tant que partie d'un ensemble fini.

Soit g un élément arbitraire de G.

Les applications $\varphi : H \longrightarrow gH$ et $\psi : gH \longrightarrow H$ sont clairement réciproques l'une de l'autre.

$$h \longmapsto g * h \qquad x \longmapsto g^{-1} * x$$

En particulier φ et ψ sont bijectives ; les ensembles H et gH sont donc équipotents. D'où : $\mathrm{Card}(H) = \mathrm{Card}(gH)$.

Conclusion. Pour tout élément g de G on a : $\mathrm{Card}(H) = \mathrm{Card}(gH)$.

7) Soient g et g' deux éléments de G. Supposons que gH et $g'H$ ne sont pas disjoints. Alors il existe deux éléments h et k dans H tels que : $g * h = g' * k$. En particulier : $g^{-1} * g' = h * k^{-1} \in H$. [10]

Soit alors γ un élément quelconque de $g'H$. Il existe un élément h_0 de H tel que : $\gamma = g' * h_0$. On écrit alors judicieusement : $\gamma = g * g^{-1} * g' * h_0$. On en déduit que : $\gamma = g * \underbrace{h * k^{-1} * h_0}_{\in H}$. Par suite : $\gamma \in gH$.

On a ainsi établi que : $g'H \subset gH$.

En réécrivant le même raisonnement en permutant g et g', ou en observant que g et g' jouent des rôles symétriques dans le raisonnement précédent, on obtient l'autre inclusion : $gH \subset g'H$. Finalement, lorsque gH et $g'H$ ne sont pas disjoints, ils sont égaux.

Conclusion. Pour tout couple (g, g') d'éléments de G, on a $[gH = g'H]$ ou $[gh \cap g'H = \emptyset]$.

8) Le groupe G est fini par hypothèse. On peut donc noter : $G = \{g_1, \ldots, g_n\}$ (avec $n = \mathrm{Card}(G)$). On a alors :

10. En effet, k est un élément de H. Puisque H est un sous-groupe, k^{-1} est un élément de H. Par ailleurs, h est un autre élément de H. En utilisant une nouvelle fois le fait que H est un sous-groupe, on en déduit que : $h * k^{-1} \in H$.

$G = \bigcup_{i=1}^{n} \{g_i\}$ et donc $G = \bigcup_{i=1}^{n} g_i H$. La première égalité provient de l'observation puissante selon laquelle un ensemble fini est la réunion des singletons qui le composent ; la seconde découle de la première et du fait que pour tout entier i on a : $\{g_i\} \subset g_i H \subset G$.

D'après la question précédente, il peut exister parmi les $g_i H$ des ensembles égaux. Notons alors k le nombre de parties disjointes parmi ces $g_i H$. Quitte à renuméroter les g_i, on peut supposer qu'il s'agit des k premières parties, et on alors : $G = \bigcup_{i=1}^{k} g_i H$. Cette union étant disjointe, on a donc : $\text{Card}(G) = \sum_{i=1}^{k} \text{Card}\,(g_i H)$. Or d'après la question 6, on a : $\text{Card}(g_i H) = \text{Card}(H)$ (pour tout g_i).

On en déduit que : $\text{Card}(G) = \sum_{i=1}^{k} \text{Card}\,(H)$ d'où : $\text{Card}(G) = k\text{Card}\,(H)$. Finalement, le cardinal de G est multiple de celui de H.

Conclusion. Si G est un groupe fini, le cardinal de tout sous-groupe de G divise le cardinal de G.

9) Soit g un élément d'un groupe fini G. Alors g est d'ordre fini (d'après la question 5-c), et son ordre est le cardinal de $\langle g \rangle$. Or $\langle g \rangle$ est un sous-groupe de G (d'après la question 3), donc son ordre divise celui de G (d'après la question précédente).

Conclusion. Dans un groupe fini G, tout élément g est d'ordre fini, et l'ordre de g divise le cardinal de G.

➤ **Partie D - Abélianité des groupes de cardinal 5**.

10) D'après la définition, il est équivalent de dire que G est cyclique ou qu'il existe un élément g de G dont l'ordre est égal au cardinal de G.

Or dans le groupe S_3, les éléments peuvent être d'ordre 1 (l'identité), d'ordre 2 (les trois transpositions) ou d'ordre 3 (les deux 3-cycles). Aucun élément n'a donc un ordre égal au cardinal de S_3, qui vaut 6. Donc S_3 n'est pas cyclique.

En revanche le groupe A_3 est cyclique, puisque $A_3 = \langle (123) \rangle$ (ou $A_3 = \langle (132) \rangle$).

11) Si G est un groupe cyclique, alors il existe un élément g de G tel que $G = \left\{ g^k \,/ k \in \mathbb{Z} \right\}$. Il est alors clair que G est abélien (essentiellement car $g^k * g^{k'} = g^{k+k'} = g^{k'} * g^k$). **Conclusion**. [$G$ cyclique] $\Longrightarrow$ [G abélien].

12) Soit G un groupe de cardinal 5. Soit g un élément de G, distinct de l'élément neutre. On sait que g est d'ordre fini, et que cet ordre divise 5 (d'après la question 9). Ainsi l'ordre de g pourrait valoir 1 ou 5 ; mais $g \neq \text{e}$, donc g n'est pas d'ordre 1. Il s'ensuit que g est d'ordre 5, ce qui signifie que : $G = \langle g \rangle$. D'où le groupe G est cyclique, donc abélien d'après la question précédente.

Conclusion. Tout groupe fini de cardinal 5 est abélien.

Complément. Tout groupe fini de cardinal p premier est abélien.

QCM DE SYNTHESE

GROUPES, ANNEAUX, CORPS : MAINTENANT, TESTEZ-VOUS !

En prévision des futures évaluations, vous devez pouvoir répondre sans coup férir aux rapides questions suivantes, qui vous permettront de savoir si vous avez retenu les principaux mécanismes relatifs aux groupes, anneaux et corps.

NB : une ou plusieurs questions pourront vous être posées rapidement en début de colle 12.

A propos des groupes

1/ **Citer de mémoire 4 exemples de groupes : deux abéliens et deux non abéliens.**

2 groupes abéliens : $(\mathbb{U}_4, \times)$ et $(\mathbb{K}[X], +)$. 2 groupes non abéliens : $(\mathrm{Bij}(\mathbb{C}), \circ)$ et $(\mathrm{GL}_2(\mathbb{R}), \times)$.

2/ **Le produit scalaire est une ℓci sur $\mathbb{R}^2$.** ☐ Oui ☐ Non

Non

3/ $(\mathbb{R}, -)$ **est un groupe.** ☐ Oui ☐ Non

Non

4/ **Si E est un ensemble non vide, $(E^E, \circ)$ est un groupe.** ☐ Oui ☐ Non

Non

5/ **Si E et F sont deux ensembles non vides, l'ensemble des bijections de E dans F est un groupe pour la composition.** ☐ Oui ☐ Non

Non

6/ **L'ensemble des similitudes directes, muni de la composition, est un groupe abélien.** ☐ Oui ☐ Non

Non

7/ **L'ensemble des rotations de centre O, muni de la composition, est un groupe abélien.** ☐ Oui ☐ Non

Oui

8/ **L'ensemble des homothéties, muni de la composition, est un groupe.** ☐ Oui ☐ Non

Non

9/ $(\mathbb{K}_n[X], +)$ **est un groupe.** ☐ Oui ☐ Non

Oui

10/ **Tout sous-groupe de $\mathrm{GL}_2(\mathbb{R})$ est non abélien.** ☐ Oui ☐ Non

Non

A propos des anneaux

11/ **Citer de mémoire 4 exemples d'anneaux, dont au moins deux non intègres.**

Exemples d'anneaux : $\mathbb{Z}$, $\mathbb{K}[X]$, $\mathrm{M}_2(\mathbb{R})$ et $\mathscr{C}^0(\mathbb{R}, \mathbb{C})$. Seuls les deux premiers sont intègres.

12/ $(\mathbb{N}, +, \times)$ **est un anneau.** ☐ Oui ☐ Non

Non

13/ $(\mathbb{R}_+^*, +, \times)$ **est un anneau.** ☐ Oui ☐ Non

Non

14/ **Les sous-ensembles de $\mathbb{R}^{\mathbb{N}}$ suivants constituent-ils des sous-anneaux de $\left(\mathbb{R}^{\mathbb{N}}, +, \times\right)$?**

a/ L'ensemble des suites de limite 0. ☐ Oui ☐ Non

Oui

b/ L'ensemble des suites de limite 1. ☐ Oui ☐ Non

Non

c/ L'ensemble des suites convergentes. ☐ Oui ☐ Non

Oui

d/ L'ensemble des suites divergentes. ☐ Oui ☐ Non

Non

e/ L'ensemble des suites positives. ☐ Oui ☐ Non

Non

f/ L'ensemble des suites majorées. ☐ Oui ☐ Non

Oui

g/ L'ensemble des suites bornées. ☐ Oui ☐ Non

Oui

h/ L'ensemble des suites périodiques. ☐ Oui ☐ Non

Oui

15/ **Les sous-ensembles de $\mathbb{R}^{\mathbb{R}}$ suivants constituent-ils des sous-anneaux de $\left(\mathbb{R}^{\mathbb{R}}, +, \times\right)$? L'ensemble...**

a/ ... des fonctions continues et tendant vers 0 en $+\infty$. ☐ Oui ☐ Non

Oui

b/ ... des fonctions continues et tendant vers $+\infty$ en $+\infty$. ☐ Oui ☐ Non

Non

c/ ... des fonctions de classe $\mathscr{C}^1$ sur $\mathbb{R}$. ☐ Oui ☐ Non

Oui

d/ ... des combinaisons linéaires de cos et de de sin ("$f = \lambda\cos + \mu\sin$"). ☐ Oui ☐ Non

Non

e/ ... des fonctions continues et 2π-périodiques. ☐ Oui ☐ Non

Oui

16/ [11] **Les sous-ensembles de $\mathbf{M}_2(\mathbb{R})$ suivants constituent-ils des sous-anneaux de $\left(\mathbf{M}_2(\mathbb{R}), +, \times\right)$? L'ensemble...**

a/ ... des matrices inversibles. ☐ Oui ☐ Non

Non

b/ ... des matrices diagonales, càd de la forme $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. ☐ Oui ☐ Non

Oui

11. Attendre le prochain chapitre pour répondre à cette question.

c/ ... des matrices triangulaires supérieures, càd de la forme $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$. ☐ Oui ☐ Non

Oui

d/ ... des matrices scalaires, càd de la forme $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. ☐ Oui ☐ Non

Oui

e/ ... des matrices symétriques, càd de la forme $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$. ☐ Oui ☐ Non

Non

f/ ... des matrices antisymétriques, càd de la forme $\begin{pmatrix} 0 & -b \\ b & 0 \end{pmatrix}$. ☐ Oui ☐ Non

Non

A propos des corps

17/ **Citer de mémoire 3 exemples de corps, et 3 exemples d'anneaux commutatifs qui ne sont pas des corps.**

Exemples de corps : $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{K}(X)$.

Exemples d'anneaux commutatifs qui ne sont pas des corps : $\mathbb{Z}$, $\mathbb{C}[X]$ et $\mathbb{R}^{\mathbb{N}}$

18/ $\mathbb{Z}$ **est un corps.** ☐ Oui ☐ Non

Non

19/ $\mathbb{R}_+^*$ **est un corps.** ☐ Oui ☐ Non

Non

20/ $\mathbb{R}$ **est un corps.** ☐ Oui ☐ Non

Oui

21/ $\mathbb{K}[X]$ **est un corps.** ☐ Oui ☐ Non

Non

22/ $\mathbb{C}$ **n'a d'autre sous-corps que** $\mathbb{C}$ **lui-même.** ☐ Oui ☐ Non

Non

23/ $\mathbb{Q}$ **n'a d'autre sous-corps que** $\mathbb{Q}$ **lui-même.** ☐ Oui ☐ Non

Oui