Quatrième composition de mathématiques [corrigé]

Exercice. Gudermannien.

1. **Fonction argument sinus hyperbolique.**
   (a) **Question de cours.** Rappeler la définition de la fonction sh, sa dérivée, et son graphe.

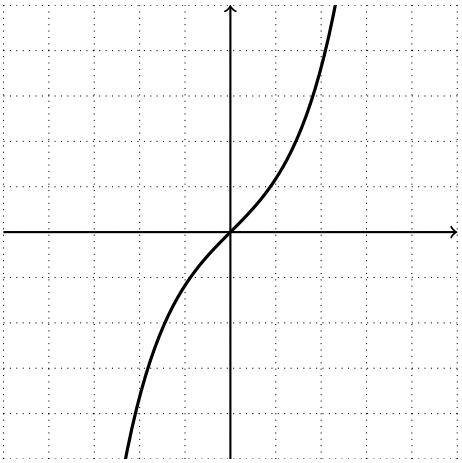
   On a

   $$\mathrm{sh} : \begin{cases} \mathbb{R} \to & \mathbb{R} \\ x \mapsto & \dfrac{e^x - e^{-x}}{2}. \end{cases}$$

   Cette fonction est dérivable par opérations. Pour tout $x \in \mathbb{R}$*, on a*

   $$\mathrm{sh}'(x) = \frac{e^x + e^{-x}}{2} = \mathrm{ch}(x).$$

   Le graphe de sh *est le suivant.*

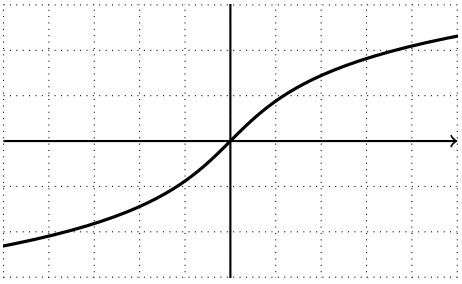


   (b) Montrer que la fonction sh est bijective et dessiner le graphe de sa réciproque.

   - *La fonction* sh *est dérivable donc continue.*
   - *Comme sa dérivée* $\mathrm{sh}' = \mathrm{ch}$ *est strictement positive, la fonction* sh *est strictement croissante.*
   - *Les limites de l'exponentielle donnent directement* $\mathrm{sh}(x) \xrightarrow[x \to \pm\infty]{} \pm\infty$.

   D'après le théorème de la bijection monotone, la fonction $\mathrm{sh} : \mathbb{R} \to \mathbb{R}$ *est donc une bijection.*

   Le graphe de sh^{-1} *est le suivant.*



Dans la suite du problème, on note argsh : $\mathbb{R} \to \mathbb{R}$ la réciproque de sh.

(c) Montrer que argsh est dérivable et que $\forall y \in \mathbb{R}, \text{argsh}'(y) = \dfrac{1}{\sqrt{y^2+1}}$.

Soit $y \in \mathbb{R}$. *On définit* $x = \text{argsh}(y)$.
On a $\text{sh}'(x) = \text{ch}(x) > 0$. *En particulier, cette dérivée ne s'annule pas.*
D'après le critère de dérivabilité des fonctions réciproques (applicable car sh *est bijective et dérivable), on en déduit que* argsh *est dérivable en* y, *de dérivée*

$$y \mapsto \frac{1}{\text{ch}(\text{argsh}\, y)} = \frac{1}{\sqrt{\text{sh}^2(\text{argsh}\, y)+1}} = \frac{1}{\sqrt{y^2+1}},$$

en utilisant notamment que $\text{ch} > 0$.

2. **Gudermannien et pendule simple**

(a) Par des études de fonctions, montrer que $\forall x \in \mathbb{R}, \arctan(\text{sh}\, x) = \arcsin(\text{th}\, x)$ et que la fonction $x \mapsto \arctan(\text{sh}\, x)$ induit une bijection gd : $\mathbb{R} \to I$, où I est un intervalle que l'on précisera.

- *La fonction* $f : x \mapsto \arctan(\text{sh}\, x)$ *est dérivable par composition. Soit* $x \in \mathbb{R}$. *On a*

$$f'(x) = \frac{\text{ch}\, x}{1+\text{sh}^2 x} = \frac{\text{ch}\, x}{\text{ch}^2 x} = \frac{1}{\text{ch}\, x}.$$

- *La fonction* th *prend ses valeurs dans* $]-1,1[$, *intervalle sur lequel la fonction* arcsin *est dérivable, donc* $g : x \mapsto \arcsin(\text{th}\, x)$ *est dérivable par composition. Soit* $x \in \mathbb{R}$. *On a*

$$g'(x) = \frac{1-\text{th}^2(x)}{\sqrt{1-\text{th}^2(x)}} = \sqrt{1-\text{th}^2(x)} = \sqrt{\frac{1}{\text{ch}^2(x)}} = \frac{1}{\text{ch}(x)},$$

car $\text{ch} > 0$.

- *Par différence, la fonction* $f - g : \mathbb{R} \to \mathbb{R}$ *est dérivable, de dérivée nulle. Comme* $\mathbb{R}$ *est un intervalle, on en déduit que* $f - g$ *est constante. Comme* $f(0) = 0 = g(0)$, *on en déduit même* $f = g$, *ce qui conclut.*
- *Par composition, comme* $\text{sh} : \mathbb{R} \to \mathbb{R}$ *et* $\arctan : \mathbb{R} \to \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$ *sont des bijections, le gudermannien est une bijection* $\text{gd} : \mathbb{R} \to \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$.

La bijection gd : $\mathbb{R} \to I$ est le *gudermannien*.

(b) Donner une expression de la réciproque $\text{gd}^{-1} : I \to \mathbb{R}$, et en déduire qu'elle est dérivable, de dérivée $y \mapsto \dfrac{1}{\cos y}$.

- *Puisque* $\text{gd} = \arctan \circ \text{sh}$, $\text{gd}^{-1} = \text{sh}^{-1} \circ \arctan^{-1}$, *ce qui montre* $\text{gd}^{-1} : y \mapsto \text{argsh}(\tan y)$.
- *La fonction* $\text{gd}^{-1} : \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[\to \mathbb{R}$ *est alors dérivable, de dérivée :*

$$(\text{gd}^{-1})' : y \mapsto \frac{1+\tan^2 y}{\sqrt{1+\tan^2 y}} = \sqrt{1+\tan^2 y} = \sqrt{\frac{1}{\cos^2 y}} = \frac{1}{\cos y},$$

car $\cos > 0$ *sur* $\left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$.

(c) Déduire de ce qui précède que $\forall x \in \mathbb{R}, \mathrm{gd}'(x) = \cos(\mathrm{gd}(x))$.

Puisque gd^{-1} *est la réciproque de* gd, *on a* $\mathrm{gd}^{-1} \circ \mathrm{gd} = \mathrm{id}_{\mathbb{R}}$.
Toutes les fonctions en présence sont dérivables. La formule de dérivation des fonctions composées donne alors $\left((\mathrm{gd}^{-1})' \circ \mathrm{gd}\right) \times \mathrm{gd}' = 1$.

Soit $x \in \mathbb{R}$. *En remplaçant* $\left(\mathrm{gd}^{-1}\right)'$ *par son expression trouvée à la question précédente et en évaluant en* x *l'égalité entre fonctions ci-dessus, on obtient*

$$\frac{1}{\cos(\mathrm{gd}(x))} \times \mathrm{gd}'(x) = 1 \qquad \textit{donc} \qquad \mathrm{gd}'(x) = \cos(\mathrm{gd}(x)).$$

(d) Montrer que la fonction $\varphi = 2\,\mathrm{gd}$ est deux fois dérivable et $\forall x \in \mathbb{R}, \varphi''(x) + \sin(\varphi(x)) = 0$.

La fonction $\mathrm{gd}' = \cos \circ \mathrm{gd}$ *est dérivable par composition, donc* gd *est deux fois dérivable, et il en va alors de même de* φ.
Soit $x \in \mathbb{R}$. *On a*

$$\begin{aligned}
\varphi''(x) &= 2\,\mathrm{gd}''(x) \\
&= -2\,\mathrm{gd}'(x)\,\sin(\mathrm{gd}(x)) \qquad \textit{(car } \mathrm{gd}' = \cos \circ \mathrm{gd}\textit{, et par dérivation des composées)} \\
&= -2\,\cos(\mathrm{gd}(x))\,\sin(\mathrm{gd}(x)) \\
&= -\sin(2\,\mathrm{gd}(x)) \\
&= -\sin(\varphi(x)),
\end{aligned}$$

ce qui conclut.

Problème. Groupes engendrés par deux involutions.

- Un élément g d'un groupe $(G, \cdot)$ est une *involution* si $g^2 = 1_G$.
- On rappelle que deux éléments g_1, g_2 d'un groupe $(G, \cdot)$ sont *conjugués* si $\exists h \in G : g_2 = h\,g_1\,h^{-1}$. On notera $\sim$ la relation de conjugaison.

Partie I. Généralités.

Soit $(G, \cdot)$ un groupe.

1. **Conjugaison.**
   (a) Montrer que la relation de conjugaison $\sim$ est une relation d'équivalence sur G.
   On notera simplement $[g]$ la classe d'un élément $g \in G$ pour cette relation d'équivalence.

   On vérifie les trois axiomes.

   Réflexivité. *Soit* $g \in G$. *On a* $g = 1_G\,g\,1_G^{-1}$, *donc* $g \sim g$.

   Symétrie. *Soit* $g_1, g_2 \in G$ *tels que* $g_1 \sim g_2$.
   On peut donc trouver $h \in G$ *tel que* $g_2 = h\,g_1\,h^{-1}$.
   On a alors $g_1 = h^{-1}\,g_2\,h$, *ce qui montre* $g_2 \sim g_1$.

   Transitivité. *Soit* $g_1, g_2, g_3 \in G$ *tels que* $g_1 \sim g_2$ *et* $g_2 \sim g_3$.
   On peut donc trouver $h, k \in G$ *tels que* $g_2 = h\,g_1\,h^{-1}$ *et* $g_3 = k\,g_2\,k^{-1}$.
   On a alors $g_3 = k\,h\,g_1\,h^{-1}\,k^{-1} = (k\,h)\,g_1\,(k\,h)^{-1}$, *donc* $g_1 \sim g_3$.

(b) On note $Z(G) = \{g \in G \mid \forall h \in G, gh = hg\}$ le *centre* de G. Soit $g \in G$.
Montrer que $g \in Z(G)$ si et seulement si sa classe de conjugaison $[g]$ est un singleton.

On a la chaîne d'équivalences

$$\begin{aligned}[g] \textit{ singleton} &\Leftrightarrow \forall h \in G, h\,g\,h^{-1} = g \\ &\Leftrightarrow \forall h \in G, h\,g = g\,h \\ &\Leftrightarrow g \in Z(G).\end{aligned}$$

(c) Montrer que deux éléments conjugués de G ont toujours le même ordre.

Soit $g_1, g_2 \in G$ *tels que* $g_1 \sim g_2$. *On peut donc trouver* $h \in G$ *tel que* $g_2 = h\,g_1\,h^{-1}$.
Une récurrence immédiate montre que $\forall n \in \mathbb{N}, g_2^n = h\,g_1^n\,h^{-1}$.
Ainsi, pour tout $n \in \mathbb{N}^*$,

- *si* $g_1^n = 1_G$, *on a* $g_2^n = h\,1_G\,h^{-1} = 1_G$;
- *on a* $g_1^n = h^{-1}\,g_2^n\,h$; *ainsi, dès que* $g_2^n = 1_G$, *on a* $g_1^n = 1_G$.

Cela montre que les entiers $n \in \mathbb{N}^*$ *tels que* $g_1^n = 1_G$ *sont les mêmes que ceux tels que* $g_2^n = 1_G$.
Cela montre notamment que g_1 *et* g_2 *ont le même ordre (fini ou infini).*

(d) Soit Q un groupe et $f : G \to Q$ un morphisme de groupes. Montrer que le noyau $\ker(f)$ est *stable par conjugaison*, c'est-à-dire que $\forall g \in \ker(f), [g] \subseteq \ker(f)$.

Soit $g \in \ker(f)$. *Soit* $g' \in [g]$. *On a donc* $g' \sim g$: *on peut trouver* $h \in G$ *tel que* $g' = h\,g\,h^{-1}$. *En particulier,*

$$f(g') = f(h\,g\,h^{-1}) = f(h)\,f(g)\,f(h)^{-1} = f(h)\,1_Q\,f(h)^{-1} = 1_Q,$$

ce qui montre $g' \in \ker(f)$, *et conclut.*

2. **Involutions.**

(a) On suppose que G est un groupe fini d'ordre 2021. Combien G a-t-il d'involutions ?

Soit $g \in G$ *une involution.*
D'après le théorème de Lagrange, l'ordre de g *divise* 2021, *c'est-à-dire que* $g^{2021} = 1_G$.
On a donc

$$1_G = g^{2021} = g^{2020}g = 1_G^{1010}g = g.$$

Autrement dit, la seule involution de G *est* 1_G, *ce qui montre que* G *a une seule involution.*

(b) Soit $a, b \in G$ deux involutions. Montrer que ab est conjugué à son propre inverse.

Comme a *et* b *sont des involutions, on a* $a = a^{-1}$ *et* $b = b^{-1}$.
On en déduit que l'inverse de ab *est* $(ab)^{-1} = b^{-1}\,a^{-1} = ba$.
Cela conclut, car $ba = a^{-1}(ab)a$ *est conjugué à* ab.

3. On suppose que G est un groupe abélien engendré par deux involutions.
Montrer que G est fini, de cardinal 1, 2 ou 4.

Soit G *un groupe abélien et* $a, b \in G$ *deux involutions.*
On va montrer que $V = \{1_G, a, b, ab\}$ *est un sous-groupe de* G.

- *Il contient clairement* 1_G.
- *Comme* $a = a^{-1}$ *et* $b = b^{-1}$, *il en va de même de* ab : $(ab)^{-1} = b^{-1}a^{-1} = ba = ab$.
  Tous les éléments de V *sont donc leurs propres inverses, ce qui montre que* V *est (trivialement) stable par inverse.*

- *Enfin, on obtient rapidement la table de multiplication suivante, qui montre que* V *est stable par produit (notons que cette table peut être redondante, au sens où rien ne garantit que* 1_G, a, b *et* ab *soient distincts) :*

$\cdot$	1_G	a	b	ab
1_G	1_G	a	b	ab
a	a	1_G	ab	b
b	b	ab	1_G	a
ab	ab	b	a	1_G

Par exemple, en effet, $(ab)a = a^2b = b$.
Puisque V *est un sous-groupe contenant* a *et* b, *on a* $G = \langle a, b\rangle \subseteq V$, *ce qui montre déjà que* G *est fini, de cardinal* $\leqslant 4$.
Enfin, G *ne peut pas être de cardinal* 3 *:*
  - *si* $a = b = 1_G$, *il est clair que* G *est le groupe trivial ;*
  - *si* $a \neq 1_G$ *ou* $b \neq 1_G$, *le groupe* G *contient un élément d'ordre exactement* 2, *donc son cardinal doit être pair, en vertu du théorème de Lagrange.*

4. **Un théorème d'isomorphisme.** Soit Q_1 et Q_2 deux groupes et $\pi_1 : G \to Q_1$ et $\pi_2 : G \to Q_2$ deux morphismes de groupes surjectifs tels que $\ker(\pi_1) = \ker(\pi_2)$.
On va montrer que cela entraîne que Q_1 et Q_2 sont isomorphes.
   (a) Montrer qu'il existe une unique application $f : Q_1 \to Q_2$ telle que $\forall \xi \in G, f\big(\pi_1(\xi)\big) = \pi_2(\xi)$.

   Existence. *Pour tout* $x \in Q_1$, *on peut trouver* $\xi \in G$ *tel que* $x = \pi_1(\xi)$, *car* π_1 *est surjectif.*
   On peut alors définir $f(x) = \pi_2(\xi)$. *Le seul problème est de vérifier que cette application est bien définie, c'est-à-dire que* $f(x)$ *ne dépend pas du choix du* π_1*-antécédent* ξ *de* x.
   Pour cela, soit $\xi, \zeta \in G$ *tels que* $\pi_1(\xi) = \pi_1(\zeta)$.
   On a donc $\pi_1(\xi\,\zeta^{-1}) = \pi_1(\xi)\,\pi_1(\zeta)^{-1} = x\,x^{-1} = 1_G$, *ce qui montre que* $\xi\,\zeta^{-1} \in \ker(\pi_1)$.
   Par hypothèse, on a donc $\xi\,\zeta^{-1} \in \ker(\pi_2)$, *ce qui montre de même que* $\pi_2(\xi) = \pi_2(\zeta)$.

   Unicité. *Soit* $f, g : Q_1 \to Q_2$ *deux telles fonctions.*
   Pour tout $x \in Q_1$, *on peut trouver* $\xi \in G$ *tel que* $x = \pi_1(\xi)$.
   On a alors $f(x) = f\big(\pi_1(\xi)\big) = \pi_2(\xi) = g\big(\pi_1(\xi)\big) = g(x)$.
   Cela montre $f = g$.

   (b) Montrer que f est un isomorphisme.

   - *Montrons que* f *est un morphisme.*
     Soit $x, y \in Q_1$. *On peut donc trouver* $\xi, \eta \in G$ *tels que* $x = \pi_1(\xi)$ *et* $y = \pi_1(\eta)$ *(et on a justifié que le choix de l'antécédent n'importait pas). On sait qu'alors* $f(x) = \pi_2(\xi)$ *et* $f(y) = \pi_2(\eta)$.
     Comme π_1 *est un morphisme, on a alors* $xy = \pi_1(\xi\eta)$, *donc*
     $$f(xy) = \pi_2(\xi\eta) = \pi_2(\xi)\pi_2(\eta) = f(x)f(y).$$
   - *Montrons que* f *est injectif.*
     Soit $x \in \ker(f)$. *On peut trouver* $\xi \in G$ *tel que* $x = \pi_1(\xi)$.
     On a alors $1_{Q_2} = f(x) = \pi_2(\xi)$, *ce qui montre que* $\xi \in \ker(\pi_2)$.
     Par hypothèse, on en déduit $\xi \in \ker(\pi_1)$, *puis* $x = \pi_1(\xi) = 1_{Q_1}$.
     Cela montre $\ker(f) = \{1_{Q_1}\}$, *et l'injectivité de* f.
   - *Montrons que* f *est surjectif.*
     Soit $y \in Q_2$. *On peut trouver* $\eta \in G$ *tel que* $\pi_2(\eta) = y$. *On a alors*
     $$f(\pi_1(\eta)) = \pi_2(\eta) = y,$$
     ce qui montre la surjectivité de f.

   Ainsi, f *est bien un isomorphisme.*

Partie II. G_0 et les groupes diédraux finis.

Groupe G_0. Pour tout $\theta \in \mathbb{R}$, on considère les matrices

$$M_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \qquad \text{et} \qquad N_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

On note $G_0 = \left\{ M_\theta \,\middle|\, \theta \in \mathbb{R} \right\} \cup \left\{ N_\theta \,\middle|\, \theta \in \mathbb{R} \right\}$ l'ensemble de ces matrices.

5. (a) Soit $\alpha, \beta, \theta \in \mathbb{R}$. Calculer les produits $M_\alpha M_\beta$, $M_\theta N_0$, $N_0 M_\theta$ et $N_0 M_\theta N_0$.
On exprimera les réponses comme des matrices M_γ ou N_γ, pour un certain $\gamma \in \mathbb{R}$.

   - *Un calcul direct (une multiplication dans $\mathbb{C}$!) montre que* $M_\alpha M_\beta = M_{\alpha+\beta}$.
   - *On voit directement que* $N_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, *ce qui donne* $M_\theta N_0 = N_\theta$, $N_0 M_\theta = N_{-\theta}$ *et enfin* $N_0 M_\theta N_0 = M_{-\theta}$.

   (b) Soit $\alpha, \beta \in \mathbb{R}$. En utilisant la question précédente, et sans revenir à des calculs de matrices, calculer $M_\alpha N_\beta$, $N_\alpha M_\beta$ et $N_\alpha N_\beta$.

   On obtient :
   - $M_\alpha N_\beta = M_\alpha M_\beta N_0 = M_{\alpha+\beta} N_0 = N_{\alpha+\beta}$;
   - $N_\alpha M_\beta = N_0 M_{-\alpha} M_\beta = N_0 M_{\beta-\alpha} = N_{\alpha-\beta}$;
   - $N_\alpha N_\beta = N_0 M_{-\alpha} M_\beta N_0 = N_0 M_{\beta-\alpha} N_0 = M_{\alpha-\beta}$.

   (c) En déduire que G_0 est un sous-groupe de $GL_2(\mathbb{R})$.

   On observe déjà que toutes les matrices de G_0 *sont de déterminant* 1 *ou* -1, *donc* $G_0 \subseteq GL_2(\mathbb{R})$.

   - *On a* $I_2 = M_0 \in G_0$.
   - *Soit* $A \in G_0$. *On peut donc trouver* $\alpha \in \mathbb{R}$ *tel que* $A = M_\alpha$ *ou* $A = N_\alpha$.
     - *Si* $A = M_\alpha$, *on voit que* A *est inversible, d'inverse* $M_{-\alpha} \in G_0$.
     - *Si* $A = N_\alpha$, *on voit que* A *est inversible, d'inverse* $N_\alpha \in G_0$.

     Ainsi, G_0 *est stable par inverse.*
   - *Soit* $A, B \in G_0$. *On peut donc trouver* $\alpha, \beta \in \mathbb{R}$ *tel que* $A \in \{M_\alpha, N_\alpha\}$ *et* $B \in \{M_\beta, N_\beta\}$.
     Les calculs précédents montrent que $AB \in \{M_{\alpha\pm\beta}, N_{\alpha\pm\beta}\}$, *donc* $AB \in G_0$.

   Ainsi, G_0 *est un sous-groupe de* $GL_2(\mathbb{R})$.

Groupes diédraux D_{2n}. Dans toute la fin de cette partie, on fixe un entier $n \in \mathbb{N}^*$. On note alors

$$D_{2n} = \left\{ M_{\frac{2\pi k}{n}} \,\middle|\, k \in \mathbb{Z} \right\} \cup \left\{ N_{\frac{2\pi k}{n}} \,\middle|\, k \in \mathbb{Z} \right\}.$$

6. (a) Montrer que D_{2n} est un sous-groupe de G_0, dont on déterminera le cardinal.

   - *Comme l'ensemble* $\left\{ \dfrac{2\pi k}{n} \,\middle|\, k \in \mathbb{Z} \right\}$ *contient* 0, *et est stable par somme et différence, les calculs de la question précédente montrent de la même façon que* D_{2n} *contient* I_2, *est stable par inverse et par produit.*
     Cela montre que D_{2n} *est un sous-groupe de* G_0.

- *On voit directement que, pour tous* $\alpha, \beta \in \mathbb{R}$, $M_\alpha = M_\beta \Leftrightarrow \alpha \equiv \beta \pmod{2\pi}$, *et* idem *pour les matrices* N_α *et* N_β.
  Par ailleurs, comme les matrices M_α *sont de déterminant* 1 *alors que les* N_β *sont de déterminant* -1, *il est clair que deux matrices de ces deux types ne peuvent pas être égales.*
  On en déduit que

$$D_{2n} = \left\{ M_{\frac{2\pi k}{n}} \;\middle|\; k \in [\![0, n-1]\!] \right\} \sqcup \left\{ N_{\frac{2\pi k}{n}} \;\middle|\; k \in [\![0, n-1]\!] \right\},$$

  et que les n *éléments écrits dans chacun des ensembles sont deux à deux distincts.*
  Ainsi, $|D_{2n}| = 2n$.

(b) Déterminer l'ordre de $M_{\frac{2\pi}{n}}$ et celui de N_0.

- *Pour tout* $k \in \mathbb{N}$, *on a* $M_{\frac{2\pi}{n}}^k = M_{\frac{2\pi k}{n}}$, *dont on a vu qu'il valait* $I_2 = M_0$ *si et seulement si on avait la congruence* $\dfrac{2\pi k}{n} \equiv 0 \pmod{2\pi}$, *c'est-à-dire si et seulement si* $n \mid k$.
  On en déduit que l'ordre de $M_{\frac{2\pi}{n}}$ *est* n.
- *La matrice* N_0 *vérifie* $N_0 \neq I_2$ *et* $N_0^2 = I_2$, *donc elle est d'ordre* 2.

(c) En déduire que D_{2n} est le sous-groupe engendré $\left\langle M_{\frac{2\pi}{n}}, N_0 \right\rangle$.

Comme $M_{\frac{2\pi}{n}}$ *est d'ordre* n, *le sous-groupe cyclique* $\left\langle M_{\frac{2\pi}{n}} \right\rangle = \left\{ M_{\frac{2\pi k}{n}} \;\middle|\; k \in \mathbb{Z} \right\}$ *est d'ordre* n.
On a alors une double inclusion

$$\left\langle M_{\frac{2\pi}{n}} \right\rangle \subseteq \left\langle M_{\frac{2\pi}{n}}, N_0 \right\rangle \subseteq D_{2n},$$

où chaque groupe est un sous-groupe du suivant.
D'après le théorème de Lagrange, on en déduit que l'ordre de $\left\langle M_{\frac{2\pi}{n}}, N_0 \right\rangle$ *est un multiple de* n *et un diviseur de* $2n$, *ce qui ne laisse que deux choix.*

Cas 1. $\left| \left\langle M_{\frac{2\pi}{n}}, N_0 \right\rangle \right| = n$.
Dans ce cas, on a $\left\langle M_{\frac{2\pi}{n}} \right\rangle = \left\langle M_{\frac{2\pi}{n}}, N_0 \right\rangle$ *par inclusion et égalité des cardinaux.*
Mais cela est en fait impossible car N_0 *n'est pas une puissance de* $M_{\frac{2\pi}{n}}$ *(par exemple, elle n'est pas de déterminant* 1*), donc elle n'appartient pas au sous-groupe engendré par cette matrice.*
Ce cas ne se produit donc pas.

Cas 2. $\left| \left\langle M_{\frac{2\pi}{n}}, N_0 \right\rangle \right| = 2n$.
Dans ce cas (qui est donc le seul !), on a $D_{2n} = \left| \left\langle M_{\frac{2\pi}{n}}, N_0 \right\rangle \right|$ *par inclusion et égalité des cardinaux, ce qui conclut.*

(d) Montrer que N_0 et $N_{\frac{2\pi}{n}}$ sont des involutions et que $D_{2n} = \left\langle N_0, N_{\frac{2\pi}{n}} \right\rangle$.

Les calculs de la question 5b montrent directement que N_0 *et* $N_{\frac{2\pi}{n}}$ *sont des involutions.*

- *L'inclusion* $\left\langle N_0, N_{\frac{2\pi}{n}} \right\rangle \subseteq D_{2n}$ *est claire.*
- *On a* $M_{\frac{2\pi}{n}} = N_{\frac{2\pi}{n}} N_0$.
  Cela montre que le sous-groupe engendré $\left\langle N_0, N_{\frac{2\pi}{n}} \right\rangle$ *doit contenir* N_0 *et* $M_{\frac{2\pi}{n}}$.
  Il doit alors contenir $\left\langle N_0, M_{\frac{2\pi}{n}} \right\rangle$ *(car ce dernier est le* ***plus petit*** *sous-groupe contenant ces deux matrices), qui vaut* D_{2n} *d'après la question précédente.*

Ainsi, $D_{2n} = \left\langle N_0, N_{\frac{2\pi}{n}} \right\rangle$.

7. On suppose n impair. Montrer qu'il existe exactement deux morphismes de groupes $D_{2n} \to \mathbb{U}_2$.

   On a déjà dit que le déterminant d'une matrice de G_0 valait 1 ou -1. On a alors déjà (trivialement ou par restriction du morphisme $\det : GL_2(\mathbb{R}) \to \mathbb{R}^*$*) deux morphismes*

$$e : \begin{cases} D_{2n} \to \mathbb{U}_2 \\ g \mapsto 1 \end{cases} \qquad \text{et} \qquad d : \begin{cases} D_{2n} \to \mathbb{U}_2 \\ g \mapsto \det(g), \end{cases}$$

   qui sont bien différents (par exemple parce que $e(N_0) = 1 \neq -1 = d(N_0)$).
   Il reste à montrer que ces deux morphismes sont les seuls.
   Soit $f : D_{2n} \to \mathbb{U}_2$ un morphisme de groupes.

   - *Comme $M_{\frac{2\pi}{n}}^n = I_2$, on doit avoir $1 = f(I_2) = f(M_{\frac{2\pi}{n}})^n$.*
     Par imparité de n, cela montre $f(M_{\frac{2\pi}{n}}) \neq -1$, et donc $f(M_{\frac{2\pi}{n}}) = 1$.
   - *Comme le codomaine de f est $\mathbb{U}_2$, on a nécessairement $f(N_0) = 1$ ou $f(N_0) = -1$.*

   Il y a ainsi deux cas.

   Cas 1. *On a $f(M_{\frac{2\pi}{n}}) = f(N_0) = 1$.*
   Dans ce cas, f et e coïncident sur ces deux matrices, qui engendrent D_{2n}.
   Par prolongement des identités, on en déduit $f = e$.

   Cas 2. *On a $f(M_{\frac{2\pi}{n}}) = 1$ et $f(N_0) = -1$.*
   Dans ce cas, f et d coïncident sur ces deux matrices, qui engendrent D_{2n}.
   Par prolongement des identités, on en déduit $f = d$.

   On a donc montré $\mathrm{Hom}(D_{2n}, \mathbb{U}_2) = \{e, d\}$, ce qui conclut.

Partie III. D_∞ et les groupes engendrés par deux involutions.

Dans toute la fin du problème, on note D_∞ l'ensemble des applications $\mathbb{Z} \to \mathbb{Z}$ qui sont :

- soit de la forme $x \mapsto x + n$, pour un certain entier $n \in \mathbb{Z}$;
- soit de la forme $x \mapsto n - x$, pour un certain entier $n \in \mathbb{Z}$.

Ces applications sont toutes bijectives (on ne demande pas de le montrer), si bien que D_∞ est une partie du groupe $(\mathfrak{S}(\mathbb{Z}), \circ)$ des bijections $\mathbb{Z} \to \mathbb{Z}$.
On note simplement id l'élément neutre $\mathrm{id}_\mathbb{Z}$ de $\mathfrak{S}(\mathbb{Z})$.
Enfin, on nomme trois éléments de D_∞ :

$$r : \begin{cases} \mathbb{Z} \to \mathbb{Z} \\ x \mapsto 1 - x \end{cases} \qquad s : \begin{cases} \mathbb{Z} \to \mathbb{Z} \\ x \mapsto -x \end{cases} \qquad \text{et} \qquad t = r \circ s : \begin{cases} \mathbb{Z} \to \mathbb{Z} \\ x \mapsto x + 1. \end{cases}$$

On utilise la notation puissance dans le groupe $(\mathfrak{S}(\mathbb{Z}), \circ)$.
Par exemple, étant donné $f \in \mathfrak{S}(\mathbb{Z})$, et $n \in \mathbb{N}^*$, la notation f^n désigne la composée $\underbrace{f \circ \cdots \circ f}_{n \text{ fois}}$.

8. Montrer que tout élément de D_∞ s'écrit de manière unique, soit sous la forme t^n, soit sous la forme $t^n \circ s$, pour un certain entier $n \in \mathbb{Z}$.

   Un calcul immédiat montre que $t^n : x \mapsto x + n$ et $t^n \circ s : x \mapsto n - x$, ce qui conclut.

9. Montrer que D_∞ est un sous-groupe infini de $\mathfrak{S}(\mathbb{Z})$ et déterminer l'ordre de chacun de ses éléments.

   On vérifie directement les trois axiomes, en vérifiant que :

   - $\mathrm{id} = t^0$;

- *pour tout $n \in \mathbb{Z}$, l'inverse (pour la composition, c'est-à-dire la réciproque) de t^n est t^{-n} et que celui de $t^n \circ s$ est $t^n \circ s$ lui-même ;*
- *que D_∞ est stable par composition, à cause de la « table de composition »*

$\circ$	t^m	$t^m \circ s$
t^n	t^{n+m}	$t^{n+m} \circ s$
$t^n \circ s$	$t^{n-m} \circ s$	t^{n-m}

Enfin,

- $t^0 = \mathrm{id}$ *est naturellement d'ordre* 1 ;
- *aucune puissance (à part t^0) de t n'est l'identité (par exemple parce que $\forall n \in \mathbb{Z}, t^n(0) = n$), donc, pour tout $k \in \mathbb{Z}$ non nul, t^k est d'ordre infini ;*
- *on vérifie directement que $(t^n \circ s) \circ (t^n \circ s) = \mathrm{id}$, ce qui montre que tous ces éléments sont d'ordre 2.*

10. Montrer que $D_\infty = \langle s, t\rangle = \langle r, s\rangle$.

- *Le fait que $D_\infty = \{t^n \mid n \in \mathbb{Z}\} \cup \{t^n \circ s \mid n \in \mathbb{Z}\}$ montre que tout élément de D_∞ est un mot en t et s, et donc l'égalité $D_\infty = \langle s, t\rangle$.*
- *Une fois que l'on constate que l'égalité $t = r \circ s$ montre que $t \in \langle r, s\rangle$, on a l'inclusion $\langle s, t\rangle \subseteq \langle r, s\rangle$, et donc l'égalité $D_\infty = \langle r, s\rangle$.*

11. **Propriété universelle.** Soit G un groupe (noté multiplicativement) et $\theta, \sigma \in G$ tels que $\sigma^2 = 1_G$ et $\sigma\theta\sigma^{-1} = \theta^{-1}$. Montrer qu'il existe un unique morphisme de groupes $f : D_\infty \to G$ tel que $f(s) = \sigma$ et $f(t) = \theta$.

- *Puisque s et t engendrent D_∞, l'unicité est une conséquence directe du théorème de prolongement des identités.*
- *On vérifie (notamment grâce à la table de composition vue plus haut) que l'application $f : D_\infty \to G$ envoyant, pour tout $n \in \mathbb{Z}$, t^n sur θ^n et $t^n \circ s$ sur $\theta^n \sigma$ est un morphisme de groupes. En effet, pour tous $n, m \in \mathbb{Z}$, on a bien*
  - $f(t^n)f(t^m) = \theta^n\theta^m = \theta^{n+m} = f(t^{n+m}) = f(t^n \circ t^m)$;
  - $f(t^n)f(t^m \circ s) = \theta^n\theta^m\sigma = \theta^{n+m}\sigma = f(t^{n+m} \circ s) = f(t^n \circ t^m \circ s)$;
  - $f(t^n \circ s)f(t^m) = \theta^n\sigma\theta^m = \theta^n(\sigma\theta^m\sigma^{-1})\sigma = \theta^n\theta^{-m}\sigma = \theta^{n-m}\sigma = f(t^{n-m} \circ s) = f(t^n \circ s \circ t^m)$;
  - $f(t^n \circ s)f(t^m \circ s) = \theta^n\sigma\theta^m\sigma = \theta^{n-m} = f(t^{n-m}) = f(t^n \circ s \circ t^m \circ s)$,

  ce qui montre $\forall g, h \in D_\infty, f(g \circ h) = f(g)f(h)$.

12. En utilisant la question précédente, construire un morphisme de groupes $f : D_\infty \to D_4$ tel que $f(r) \neq f(s)$. En déduire que r et s ne sont pas conjugués.

- *On a $D_4 = \{M_0, M_\pi, N_0, N_\pi\}$.*
  On vérifie que les éléments M_π et N_0 vérifient $N_0^2 = I_2$ et $N_0 M_\pi N_0^{-1} = M_{-\pi} = M_\pi^{-1}$ (qui vaut également M_π, mais on s'en moque pour le moment).
  D'après la question précédente, on peut donc trouver un morphisme $f : D_\infty \to D_4$ tel que $f(t) = M_\pi$ et $f(s) = N_0$.
  On a alors

$$f(r) = f(t \circ s) = f(t)f(s) = M_\pi N_0 = N_\pi \neq N_0 = f(s).$$

- *Cela montre que* r *et* s *ne sont pas conjugués, car*

$$D_4 = \{M_0, M_\pi, N_0, N_\pi\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

  est un groupe abélien.
  En effet, si l'on pouvait trouver $h \in D_\infty$ *tel que* $r = h \circ s \circ h^{-1}$*, on aurait*

$$f(r) = f(h)f(s)f(h)^{-1} = f(h)f(h)^{-1}f(s) = f(s),$$

  ce qui est exclu.

13. Montrer que les classes de conjugaison de D_∞ sont $R = \left\{ t^{2k+1} \circ s \;\middle|\; k \in \mathbb{Z} \right\}$, $S = \left\{ t^{2k} \circ s \;\middle|\; k \in \mathbb{Z} \right\}$, et un nombre infini de classes finies que l'on précisera.

- *On vérifie directement que, pour tout* $k \in \mathbb{Z}$, $t^k \circ r \circ (t^k)^{-1} = t^{2k+1} \circ s$ *et* $t^k \circ s \circ (t^k)^{-1} = t^{2k} \circ s$.
  Comme r *et* s *ne sont pas conjugués d'une part, et que* r *et* s *ne peuvent être conjugués qu'à des éléments d'ordre* 2 *d'autre part, cela montre* $R = [r]$ *et* $S = [s]$.
- *Il reste à déterminer les classes de conjugaison des éléments de* $\langle t \rangle$.
  Pour tous $k, n \in \mathbb{N}$*, on vérifie directement que*

$$(t^n) \circ (t^k) \circ (t^n)^{-1} = t^k \qquad \text{et} \qquad (t^n \circ s) \circ (t^k) \circ (t^n \circ s)^{-1} = t^{-k},$$

  ce qui montre que la classe de conjugaison de t^k *est l'ensemble fini* $\{t^k, t^{-k}\}$ *(qui est un singleton si* $k = 0$*, et une paire sinon).*

In fine, *les classes de conjugaison sont :*

$$\{\mathrm{id}\}, \quad \{t^{-k}, t^k\} \text{ (pour tout } k \in \mathbb{N}^*), \quad R \quad \text{et} \quad S.$$

14. Soit Q un groupe et $f : D_\infty \to Q$ un morphisme de groupes. Montrer que le noyau $\ker(f)$ est l'un des sous-groupes suivants :
- $\langle t^n \rangle$, pour un certain entier $n \in \mathbb{N}$;
- $R \cup \langle t^2 \rangle$ ou $S \cup \langle t^2 \rangle$;
- D_∞.

  Soit $K = \ker(f)$*. D'après la question 1d,* K *est stable par conjugaison, c'est-à-dire qu'il est une union de classes de conjugaison en plus d'être un sous-groupe de* D_∞*. On distingue alors plusieurs cas.*

- *Si* $t \in K$*, il n'y a que deux cas.*
  - *Soit* $K = \langle t \rangle$.
  - *Soit* K *contient un élément de* R *ou de* S.
    Dans ce cas, comme K *est stable par conjugaison, il doit contenir* r *ou* s.
    Comme $s = r \circ t$*, il contient en fait* s *dans les deux cas.*
    On a alors $D_\infty = \langle s, t \rangle \subseteq K$*, ce qui montre* $K = D_\infty$.
- *Si* $K \cap R \neq \varnothing$*, on doit avoir* $R \subseteq K$*. Comme par ailleurs*

$$r \circ \underbrace{(t^{-1} \circ r \circ t)}_{\in R} = t^2,$$

  on en déduit $t^2 \in K$.

- *Si* K *contient une puissance impaire de* t*, disons* t^{2k+1}*, on a alors* $t = t^{2k+1}(t^2)^{-k} \in K$*, et on est ramené au cas précédent :* $K = D_\infty$*.*
- *Dans le cas contraire,* K *ne peut contenir ni puissance impaire de* t*, ni élément de* S *(car, dans ce cas, il contiendrait* s *et donc* $t = r \circ s$*, ce qui est exclu), donc on a* $K = R \cup \langle t^2 \rangle$ *(dont on pourrait vérifier qu'il s'agit effectivement d'un sous-groupe, mais on n'en a pas besoin dans cette question).*

► *Exactement de la même façon, si* $K \cap S \neq \varnothing$*, on a* $K = S \cup \langle t^2 \rangle$ *ou* $K = D_\infty$*.*

► *Enfin, si* $K \cap (R \cup S) = \varnothing$*,* K *est un sous-groupe de* $\langle t \rangle$*.*

Comme t *est d'ordre infini, on a un isomorphisme* $\psi : \begin{cases} \mathbb{Z} \to \langle t \rangle \\ n \mapsto t^n \end{cases}$*.*

Comme $K \subseteq \langle t \rangle = \operatorname{im} \psi$*, on vérifie facilement que* $K = \psi[\psi^{-1}[K]]$*.*
L'image réciproque $\psi^{-1}[K]$ *est alors un sous-groupe de* $\mathbb{Z}$*, donc on peut trouver* $n \in \mathbb{N}$ *tel que l'on ait* $\psi^{-1}[K] = n\mathbb{Z}$*.*
On en déduit $K = \psi[n\mathbb{Z}] = \left\{ t^{nk} \,\middle|\, k \in \mathbb{Z} \right\} = \langle t^n \rangle$*.*

15. Soit G un groupe engendré par deux involutions, a et b.

(a) Montrer qu'il existe un morphisme surjectif $f : D_\infty \to G$.

On a $b^2 = 1_G$ *et* $b(ab)b^{-1} = ba = (ab)^{-1}$*. D'après la question 11, on peut donc trouver un morphisme* $f : D_\infty \to G$ *tel que* $f(s) = b$ *et* $f(t) = ab$*.*
L'image de ce morphisme contient b *et* ab*, donc elle contient leur produit* $(ab)b = a$*.*
L'image $\operatorname{im} f$ *de ce morphisme est alors un sous-groupe de* G *contenant* a *et* b*, donc on doit avoir* $\langle a, b \rangle \subseteq \operatorname{im} f$*, c'est-à-dire* $G = \operatorname{im} f$ *et* f *est bien surjectif.*

(b) Déduire de tout ce qui précède que G est soit trivial, soit isomorphe à D_{2n} pour un certain entier $n \in \mathbb{N}^*$, soit isomorphe à D_∞.

► *Soit* $n \in \mathbb{N}^*$*.*
D'après la question 11 et le fait que $N_0 M_{\frac{2\pi}{n}} N_0^{-1} = M_{-\frac{2\pi}{n}} = M_{\frac{2\pi}{n}}^{-1}$*, on peut trouver un morphisme de groupes* $f_n : D_\infty \to D_{2n}$ *tel que* $f_n(t) = M_{\frac{2\pi}{n}}$ *et* $f_n(s) = N_0$*. Comme* $M_{\frac{2\pi}{n}}$ *et* N_0 *engendrent* D_{2n}*, on a* $\operatorname{im} f_n = D_{2n}$*.*
On a alors $f_n(r) = f_n(t \circ s) = f_n(t) f_n(s) = M_{\frac{2\pi}{n}} N_0 = N_{\frac{2\pi}{n}}$*.*
Déterminons $\ker(f_n)$*.*

- *Pour* $k \in \mathbb{Z}$*, on a* $f_n(t^k) = M_{\frac{2\pi}{n}}^k = M_{\frac{2\pi k}{n}}$*, donc* $t^k \in \ker(f_n)$ *si et seulement si* n *divise* k*.*
- *Comme* $f_n(s) = N_0 \neq I_n$ *et* $f_n(r) = N_{\frac{2\pi}{n}} \neq I_n$*, le noyau* $\ker(f_n)$ *ne contient ni* r*, ni* s*.*

D'après la classification de la question précédente, on a $\ker(f_n) = \langle t^n \rangle$*.*

► *Soit maintenant* G *engendré par deux involutions. On peut donc trouver un morphisme de groupes surjectif* $f : D_\infty \to G$*.*

- *Si* $\ker(f) = \ker(f_n)$*, la question 4b montre que* G *est isomorphe à* D_{2n}*.*
- *Si* $\ker(f) = \{\mathrm{id}\}$*,* f *est injectif en plus d'être surjectif, donc il s'agit d'un isomorphisme et* G *est isomorphe à* D_∞*.*
- *Si* $\ker(f) = D_\infty$*, on a* $\operatorname{im} f = \{1_G\}$*, donc la surjectivité de* f *montre que* G *est un groupe trivial.*
- *Si* $\ker(f) = S \cup \langle t^2 \rangle$*, on montre que* $\operatorname{im}(f) = \{1_G, f(t)\}$*. En effet, pour tout* $n \in \mathbb{Z}$*, on peut écrire* $n = 2m + b$*, où* $m \in \mathbb{Z}$ *et* $b \in \{0, 1\}$*, donc*

$$f(t^n) = f(t^2)^m f(t^b) = f(t^b) \qquad \text{et} \qquad f(t^n \circ s) = f(t^2)^m f(t^b) f(s) = f(t^b).$$

Comme $t \notin \ker(f)$*, on a* $f(t) \neq 1_G$*, et le groupe* G *a deux éléments. Il est alors nécessairement cyclique (engendré par son unique élément non trivial), et donc isomorphe à* $\mathbb{Z}/2\mathbb{Z}$*, ou encore à* $D_2 = \{M_0, N_0\}$*.*

- *Si* $\ker(f) = R \cup \langle t^2 \rangle$*, on procède de même (en montrant par exemple que tout élément du groupe* D_∞ *s'écrit de manière unique sous la forme* t^n *ou* $t^n \circ r$*), et on a encore* G *isomorphe à* D_2*.*

Partie IV. Automorphismes de D_∞.

On note $\mathrm{Aut}(D_\infty)$ l'ensemble des automorphismes de D_∞, qui est un sous-groupe de $\big(\mathfrak{S}(D_\infty), \circ\big)$ (on ne demande pas de le montrer).
Pour tout $h \in D_\infty$, on note $\varphi_h : \begin{cases} D_\infty \to D_\infty \\ g \mapsto h \circ g \circ h^{-1}. \end{cases}$

16. Montrer que $\Phi : \begin{cases} D_\infty \to \mathrm{Aut}(D_\infty) \\ h \mapsto \varphi_h \end{cases}$ est un morphisme de groupes bien défini et injectif.

- *Montrons que* Φ *est bien défini, c'est-à-dire que, pour tout* $h \in D_\infty$, $\varphi_h \in \mathrm{Aut}(D_\infty)$.
  Soit $h \in D_\infty$.
  - *Soit* $g_1, g_2 \in D_\infty$*. On a*
  $$\begin{aligned} \varphi_h(g_1 \circ g_2) &= h \circ (g_1 \circ g_2) \circ h^{-1} \\ &= (h \circ g_1 \circ h^{-1}) \circ (h \circ g_2 \circ h^{-1}) \\ &= \varphi_h(g_1) \circ \varphi_h(g_2). \end{aligned}$$
  Cela montre que φ_h *est un endomorphisme de* D_∞*.*
  - *Montrons que* φ_h *est bijectif. Soit* $g_2 \in D_\infty$.
  Pour tout $g_1 \in G$*, on a la chaîne d'équivalences*
  $$\begin{aligned} \varphi_h(g_1) = g_2 &\Leftrightarrow h \circ g_1 \circ h^{-1} = g_2 \\ &\Leftrightarrow g_1 = h^{-1} \circ g_2 \circ h, \end{aligned}$$
  ce qui montre que g_2 *a un unique* φ_h*-antécédent et donc que* φ_h *est bijectif.*

  Cela conclut la démonstration de $\varphi_h \in \mathrm{Aut}(D_\infty)$*.*
- *Montrons que* Φ *est un morphisme.*
  Soit $h_1, h_2 \in D_\infty$*. Pour tout* $g \in G$*, on a*
  $$\begin{aligned} \big(\Phi(h_1) \circ \Phi(h_2)\big)(g) &= \varphi_{h_1}\left(\varphi_{h_2}(g)\right) \\ &= h_1 \circ \left(h_2 \circ g \circ h_2^{-1}\right) \circ h_1^{-1} \\ &= (h_1 \circ h_2) \circ g \circ (h_1 \circ h_2)^{-1} \\ &= \Phi(h_1 \circ h_2)(g), \end{aligned}$$
  ce qui montre que $\Phi(h_1 \circ h_2) = \Phi(h_1) \circ \Phi(h_2)$*, et donc que* Φ *est un morphisme.*
- *Montrons que* Φ *est injectif. Soit* $h \in \ker \Phi$.
  On a donc $\varphi_h = \mathrm{id}_{D_\infty}$*, c'est-à-dire* $\forall g \in D_\infty, h \circ g \circ h^{-1} = g$*, ce que l'on peut réécrire sous la forme*
  $$\forall g \in D_\infty, h \circ g = g \circ h.$$
  Autrement dit, on obtient que h *est un élément central :* $h \in Z(D_\infty)$.
  D'après la question 1b, le centre de D_∞ *est constitué des éléments* $h \in D_\infty$ *dont la classe de conjugaison est un singleton.*
  D'après la description des classes de conjugaison obtenue à la question 13, on a donc $Z(D_\infty) = \{\mathrm{id}\}$*.*
  Ainsi, on obtient $h = \mathrm{id}$*, c'est-à-dire* $\ker(\Phi) = \{\mathrm{id}\}$ *: le morphisme* Φ *est bien injectif.*

17. Montrer que Φ n'est pas un isomorphisme.

On va montrer qu'il existe $\chi \in \mathrm{Aut}(D_\infty)$ échangeant r et s.

- *Remarquons déjà que $r^2 = \mathrm{id}$ et $r \circ t^{-1} \circ r^{-1} = t$.*
  D'après la question 11, on a donc un unique morphisme $\chi : D_\infty \to D_\infty$ tel que $\chi(s) = r$ et $\chi(t) = t^{-1}$.
  Cela entraîne $\chi(r) = \chi(t \circ s) = \chi(t) \circ \chi(s) = t^{-1} \circ r = s$.
  On a donc déjà construit un endomorphisme χ de D_∞ échangeant r et s.
- *L'endomorphisme $\chi \circ \chi$ de D_∞ vérifie donc $(\chi \circ \chi)(r) = r$ et $(\chi \circ \chi)(s) = s$. Autrement dit, il coïncide avec id_{D_∞} sur $\{r, s\}$, qui est une partie génératrice de D_∞.*
  Par principe de prolongement des identités, on en déduit que $\chi \circ \chi = \mathrm{id}_{D_\infty}$, ce qui montre que χ est un automorphisme de D_∞, égal à son propre inverse.
- *Enfin, comme $\chi(r) = s$ et que r et s ne sont pas conjugués, on voit que χ ne peut pas être égal à un automorphisme φ_h, quel que soit $h \in D_\infty$, c'est-à-dire que $\chi \notin \mathrm{im}\,\Phi$.*
  (On dit que l'automorphisme χ n'est pas intérieur).

18. Malgré la question précédente, montrer que D_∞ et $\mathrm{Aut}(D_\infty)$ sont isomorphes.

Pour simplifier les calculs, remarquons

$$\varphi_s : \begin{cases} s \mapsto s \\ t \mapsto t^{-1} \end{cases} \qquad \varphi_t : \begin{cases} s \mapsto t^2 \circ s \\ t \mapsto t \end{cases} \qquad \chi : \begin{cases} s \mapsto r = t \circ s \\ t \mapsto t^{-1}. \end{cases}$$

- *Montrons d'abord que $\mathrm{Aut}(D_\infty) = \langle \varphi_s, \chi \rangle$.*
  - *On voit que la composée $\chi \circ \varphi_s$ envoie s sur $t \circ s$ et t sur t.*
    En la composant avec elle-même, on en déduit que $(\chi \circ \varphi_s)^2$ envoie s sur $t^2 \circ s$ et t sur t.
    Autrement dit, $(\chi \circ \varphi_s)^2$ et φ_t coïncident sur $\{s, t\}$.
    Par prolongement des identités, on en déduit $\varphi_t = (\chi \circ \varphi_s)^2 \in \langle \varphi_s, \chi \rangle$.
  - *Soit $\psi \in \mathrm{im}\,\Phi$. On peut donc trouver $h \in D_\infty$ tel que $\psi = \Phi(h)$.*
    - *Si l'on peut trouver $n \in \mathbb{N}$ tel que $h = t^n$, on a $\psi = \Phi(t^n) = \varphi_t^n$.*
      Comme $\varphi_t \in \langle \varphi_s, \chi \rangle$, on en déduit $\psi \in \langle \varphi_s, \chi \rangle$.
    - *Si l'on peut trouver $n \in \mathbb{N}$ tel que $h = t^n \circ s$, on a $\psi = \Phi(t^n \circ s) = \varphi_t^n \circ \varphi_s$.*
      Comme $\varphi_t, \varphi_s \in \langle \varphi_s, \chi \rangle$, on en déduit $\psi \in \langle \varphi_s, \chi \rangle$.
      Cela montre $\mathrm{im}\,\Phi \subseteq \langle \varphi_s, \chi \rangle$.
  - *Le sous-groupe $\langle \varphi_s, \chi \rangle$ de $\mathrm{Aut}(D_\infty)$ vérifie donc à la fois $\chi \in \langle \varphi_s, \chi \rangle$ et $\mathrm{im}\,\Phi \subseteq \langle \varphi_s, \chi \rangle$.*
    On va montrer que cela entraîne $\langle \varphi_s, \chi \rangle = \mathrm{Aut}(D_\infty)$, comme promis.
    Pour cela, soit $\psi \in \mathrm{Aut}(D_\infty)$. L'objectif est de montrer $\psi \in \langle \varphi_s, \chi \rangle$.

    Étape 1. *Comme R et S sont les seules classes de conjugaison d'éléments d'ordre 2 dans D_∞, on a nécessairement $\psi(s) \in R \cup S$.*

    - *Si $\psi(s) \in S$, on pose $\psi_1 = \psi$.*
    - *Si $\psi(s) \in R$, on peut trouver $h \in D_\infty$ tel que $\psi(s) = h \circ r \circ h^{-1}$, et on a alors l'égalité $(\chi \circ \psi)(s) = \chi(h) \circ s \circ \chi(h)^{-1} \in S$. On pose alors $\psi_1 = \chi \circ \psi$.*

    Dans tous les cas, on a construit $\psi_1 \in \mathrm{Aut}(D_\infty)$ vérifiant $\psi_1(s) \in S$ et tel que $\psi = \psi_1$ ou $\psi = \chi \circ \psi_1$.
    Comme $\chi^{-1} = \chi \in \langle \varphi_s, \chi \rangle$, il suffit maintenant de montrer que $\psi_1 \in \langle \varphi_s, \chi \rangle$ pour conclure.

Étape 2. *Montrons que* $\psi_1(t) \in \{t, t^{-1}\}$.

Comme t *est d'ordre infini et que* ψ_1 *est un automorphisme, on voit facilement que* $\psi_1^{-1}(t)$ *est d'ordre infini. On peut donc trouver* $k \in \mathbb{Z}$ *non nul tel que* $\psi_1^{-1}(t) = t^k$.

On a donc $\psi_1(t)^k = \psi_1(t^k) = t$.

Toute puissance d'un élément d'ordre fini étant d'ordre fini, on voit que $\psi_1(t)$ *est nécessairement d'ordre infini. On peut donc trouver* $\ell \in \mathbb{Z}$ *non nul tel que* $\psi_1(t) = t^\ell$.

On a ainsi $t = (t^\ell)^k = t^{k\ell}$.

On en déduit $k\ell = 1$, *et donc* $k \in \{\pm 1\}$ *puisque* k *et* ℓ *sont entiers.*

- ▷ *Si* $k = 1$, *on a* $\psi(t) = t$.
- ▷ *Si* $k = -1$, *on a* $\psi(t) = t^{-1}$.

Nous pouvons maintenant définir un automorphisme ψ_2.

- ▷ *Si* $\psi_1(t) = t$, *on pose* $\psi_2 = \psi_1$.
- ▷ *Si* $\psi_1(t) = t^{-1}$, *on pose* $\psi_2 = \varphi_s \circ \psi_1$, *qui vérifie d'une part* $\psi_2(t) = t$ *et d'autre part* $\psi_2(s) = \psi_1(s) \in S$.

Comme $\varphi_s^{-1} = \varphi_s \in \langle \varphi_s, \chi \rangle$, *il suffit maintenant de montrer que* $\psi_2 \in \langle \varphi_s, \chi \rangle$ *pour conclure.*

Étape 3. *À ce stade, on dispose de* $\psi_2 \in \mathrm{Aut}(D_\infty)$ *vérifiant* $\psi_2(t) = t$ *et* $\psi_2(s) \in S$.

On peut donc trouver $k \in \mathbb{Z}$ *tel que* $\psi_2(t) = t$ *et* $\psi_2(s) = t^{2k} \circ s$.

Or, on a également $\varphi_t^k(t) = t$ *et* $\varphi_t^k(s) = t^{2k} \circ s$. *Autrement dit, les automorphismes* ψ_2 *et* φ_t^k *coïncident sur* $\{s, t\}$. *Comme cette paire engendre* D_∞, *le prolongement des identités entraîne que* $\psi_2 = \varphi_t^k \in \langle \varphi_s, \chi \rangle$, *ce qui conclut, enfin !*

► *D'après le point précédent, le groupe* $\mathrm{Aut}(D_\infty)$ *est engendré par* χ *et* φ_s, *qui sont deux involutions.*

Par ailleurs, puisque $\Phi : D_\infty \to \mathrm{Aut}(D_\infty)$ *est injectif et que* D_∞ *est un groupe infini, on en déduit que* $\mathrm{Aut}(D_\infty)$ *est lui-même infini.*

D'après la question 15b, on en déduit que $\mathrm{Aut}(D_\infty)$ *est isomorphe à* D_∞, *car les autres exemples (le groupe trivial et les groupes diédraux* D_{2n}*) sont finis.*