# GROUPES

## Solution 1

Notons H le sous-groupe de G engendré par E. Nous allons montrer que E = H. Montrons d'abord que tout élément de H peut s'écrire comme produit d'éléments distincts de E. Remarquons que si x = ab avec  $a, b \in E$ , x = ba' avec  $a' = b^{-1}ab \in E$  car a' est un conjugué de a donc de même ordre que a. Soit  $x \in H$ , x s'écrit  $x_1x_2 \dots x_n$  (l'écriture de x ne comporte pas d'inverses car l'inverse d'un élément d'ordre fini est aussi d'ordre fini) où n est le nombre minimal d'éléments de E avec lesquels on peut écrire a. Supposons que cette écriture comporte deux éléments identiques i.e. il existe i < j tels que  $x_i = x_j = a$ . En répétant la méthode décrite précédemment,  $x = x_1 \dots x_i x_j x'_{i+1} \dots x'_{j-1} x_{j+1} \dots x_n$  où les  $x'_k$  appartiennent aussi à E. Mais  $x_i x_j = a^2$  qui est aussi d'ordre fini et x s'écrit avec n-1 éléments de E, ce qui contredit la minimalité de n. Notons r = |E|, l'écriture de longueur minimale de tout élément de H ne comporte qu'au plus r éléments tous distincts donc  $|H| \le r!$ . En particulier, H est d'ordre fini donc tous ses éléments sont d'ordre fini. Ainsi  $H \subset E$ . Comme on a évidemment  $E \subset H$ , c'est que E = H et E est un sous-groupe de E.

## Solution 2

Pour  $x \in G$ , on note  $\langle x \rangle$  le sous-groupe de G engendré par x. Remarquons que  $\langle x \rangle$  est d'ordre fini, sinon il serait isomorphe à  $(\mathbb{Z},+)$  qui possède un nombre infini de sous-groupes. Comme G possède un nombre fini de sous-groupes, les sous-groupes de la forme  $\langle x \rangle$  sont en nombre fini : on les notera  $\langle x_1 \rangle, \dots, \langle x_n \rangle$ . Soit  $y \in G : \langle y \rangle$  est un des sous-groupes  $\langle x_i \rangle$ . En particulier, y appartient à l'un des  $\langle x_i \rangle$ . Ainsi  $G = \bigcup_{i=1}^n \langle x_i \rangle$ . Comme les  $\langle x_i \rangle$  sont tous d'ordre fini, G est fini.

## **Solution 3**

Tout d'abord, S(x) est bien une partie de S(E).

Ensuite,  $Id_E \in S(x)$  puisque  $Id_E(x) = x$ .

Enfin, soient  $\sigma, \sigma' \in S(x)$ . Montrons que  $\sigma^{-1} \circ \sigma' \in S(x)$ . On a  $\sigma^{-1} \circ \sigma'(x) = \sigma^{-1}(x)$  car  $\sigma'(x) = x$ . Or  $\sigma(x) = x$  donc, en composant par  $\sigma^{-1}$ ,  $\sigma^{-1}(x) = x$ . Donc  $\sigma^{-1} \circ \sigma'(x) = \sigma^{-1}(x) = x$  et  $\sigma^{-1} \circ \sigma' \in S(x)$ .

S(x) est bien un sous-groupe de  $(S(E), \circ)$ .

**Remarque.** S(x) est appelé le stabilisateur de x.

#### **Solution 4**

**1.** Soient (x, y) et (x', y') dans G. Comme  $x, x' \in \mathbb{R}^*$ ,  $xx' \in \mathbb{R}^*$  et il est évident que  $xy' + y \in \mathbb{R}$ . Donc  $(x, y) * (x', y') \in G$ . Soient (x, y), (x', y') et (x'', y'') dans G. On voit facilement que :

$$((x,y)*(x',y'))*(x'',y'') = (x,y)*((x',y')*(x'',y''))$$
$$= (xx'x'',xx'y'' + xy' + y)$$

2. G possède un élément neutre à savoir (1,0). Soit  $(x,y) \in G$  et cherchons  $(x',y') \in G$  tel que (x,y)\*(x',y')=(1,0). Ceci équivaut à résoudre

$$\begin{cases} xx' = 1 \\ xy' + y = 0 \end{cases} \iff \begin{cases} x' = \frac{1}{x} \\ y' = -\frac{y}{x} \end{cases} \text{ car } x \neq 0$$

Donc (x, y) admet pour inverse à droite  $\left(\frac{1}{x}, -\frac{y}{x}\right)$ . On vérifie facilement que c'est aussi l'inverse à gauche, donc l'inverse. En conclusion, (G, \*) est bien un groupe. On voit qu'il n'est pas commutatif car (1, 1) \* (2, 2) = (2, 4) et (2, 2) \* (1, 1) = (2, 3).

3. A partir des premières valeurs de n, on conjecture  $(x,y)^{*n}=(x^n,y+yx+\cdots+yx^{n-1})$ . **Initialisation :** La formule est clairement vraie pour n=0.

**Hérédité**: On suppose  $(x, y)^{*n} = (x^n, y + yx + \dots + yx^{n-1})$  pour un certain n. Alors

$$(x,y)^{*(n+1)} = (x,y) * (x,y)^{*n}$$
  
=  $(x,y) * (x^n, y + yx + \dots + yx^{n-1})$   
=  $(x^{n+1}, y + yx + \dots + yx^n)$ 

On conclut par récurrence.

En outre, en utilisant la somme des termes d'une suite géométrique, on a :

$$(x,y)^{*n} = \begin{cases} \left(x^n, y \cdot \frac{1-x^n}{1-x}\right) & \text{si } x \neq 1\\ (x,ny) & \text{sinon} \end{cases}$$

#### **Solution 5**

**1.** Soient  $x, y \in G$ . Comme th induit une bijection de  $\mathbb{R}$  sur ]-1,1[, il existe  $a,b \in \mathbb{R}$  tels que x= th a et y= th b. Alors x\*y= th $(a+b) \in ]-1,1[$ .

Soient maintenant  $x, y, z \in G$ . De la même façon, il existe  $a, b, c \in \mathbb{R}$  tels que  $x = \operatorname{th} a$ ,  $y = \operatorname{th} b$  et  $z = \operatorname{th} c$ . On voit alors facilement que

$$(x * y) * z = x * (y * z) = th(a + b + c)$$

En conclusion, \* est une loi interne associative sur G.

- 2. Il est clair que 0 est l'élément neutre de (G, \*) et que tout  $x \in G$  admet -x pour inverse. G est donc un groupe. L'expression de x \* y est symétrique en x et y: le groupe est donc commutatif.
- 3. Soit  $x \in G$  et  $a \in \mathbb{R}$  tel que  $x = \operatorname{th} a$ . On a donc  $x^{*n} = \operatorname{th}(na)$ . Or  $a = \operatorname{argth} x = \frac{1}{2} \ln \left( \frac{1+x}{1-x} \right)$ . Par conséquent,

$$th(na) = \frac{\left(\frac{1+x}{1-x}\right)^{\frac{n}{2}} - \left(\frac{1+x}{1-x}\right)^{-\frac{n}{2}}}{\left(\frac{1+x}{1-x}\right)^{\frac{n}{2}} + \left(\frac{1+x}{1-x}\right)^{-\frac{n}{2}}} = \frac{(1+x)^n - (1-x)^n}{(1+x)^n + (1-x)^n}$$

**Remarque.** On a en fait montré que th était un morphisme de  $(\mathbb{R}, +)$  sur (G, \*).

# **Solution 6**

1. Notons *e* l'élément neutre de G. Comme H et K sont des sous-groupes de G, ils contiennent tous deux l'élément neutre *e*. Donc *e* ∈ H ∩ K.

Soit  $h, k \in H \cap K$ . Comme H est un sous-groupe de G,  $h^{-1}k \in H$ . De même,  $h^{-1}k \in K$ . Par conséquent,  $h^{-1}k \in H \cap K$ . En conclusion,  $H \cap K$  est un sous-groupe de G.

2. Si H ⊂ K ou K ⊂ H, on a H ∪ K = K ou H ∪ K = H. Donc H ∪ K est bien un sous-groupe de G. Réciproquement, supposons que H ∪ K est un sous-groupe de G. Supposons de plus que H ⊄ K et montrons que K ⊂ H. Comme H ⊄ K, il existe h<sub>0</sub> ∈ H \ K. Soit maintenant k ∈ K. Comme h<sub>0</sub>, k ∈ H ∪ K et que H ∪ K est un sous-groupe de G, h<sub>0</sub>k ∈ H ∪ K. On ne peut avoir h<sub>0</sub>k ∈ K car sinon h<sub>0</sub> = (h<sub>0</sub>k)k<sup>-1</sup> ∈ K, ce qui n'est pas. Donc h<sub>0</sub>k ∈ H. Or k = h<sub>0</sub><sup>-1</sup>(h<sub>0</sub>k) ∈ H. Ceci étant vrai pour tout élément k de K, on a donc K ⊂ H.

## **Solution 7**

**1.** On a pour tous  $x, y \in G$ ,

$$\varphi(x)\varphi(y) = axa^{-1}aya^{-1} = axya^{-1} = \varphi_a(xy).$$

Ainsi  $\varphi_a$  est bien un endomorphisme de G.

Pour  $x, y \in G$ ,

$$y = \varphi_a(x) \iff y = axa^{-1} \iff a^{-1}ya = x \iff x = \varphi_{a^{-1}}(y)$$

Ainsi  $va_a$  est bien bijectif : c'est un automorphisme de G. On a en fait aussi prouvé que  $\varphi_a^{-1} = \varphi_{a^{-1}}$ .

- Comme pour tout a ∈ G, φ<sub>a</sub> est bijectif, ℑ(G) ⊂ Aut(G). On a Id<sub>G</sub> = φ<sub>e</sub> ∈ ℑ(G). De plus, on vérifie que pour a, b ∈ G, φ<sub>a</sub> ∘ φ<sub>b</sub> = φ<sub>ab</sub> ∈ ℑ(G). Enfin, on a vu à la question précédente que pour a ∈ G, φ<sub>a</sub><sup>-1</sup> = φ<sub>a-1</sub> ∈ ℑ(G). Par conséquent, ℑ(G) est un sous-groupe de (Aut(G), ∘).
- 3. On a montré à la question précédente que  $\varphi_a \circ \varphi_b = \varphi_{ab}$  i.e.  $\varphi(a) \circ \varphi(b) = \varphi(ab)$ . Ainsi  $\varphi$  est un morphisme de groupes.

## **Solution 8**

Si f est un automorphisme, c'est en particulier un morphisme. Donc pour tous  $a, b \in G$ , f(ab) = f(a)f(b) i.e.

$$(ab)^{-1} = a^{-1}b^{-1} \iff (ab)^{-1} = (ba)^{-1} \iff ab = ba$$

Ainsi G est commutatif.

Réciproquement si G est commutatif, le raisonnement inverse nous montre que f est un morphisme. De plus,  $f \circ f = \mathrm{Id}_{G}$ , donc f est bijectif (d'application réciproque lui-même). f est bien un automorphisme.

# **Solution 9**

Soit  $r \in \mathbb{Q}$ . Montrons que f(r) = 0. Soit  $n \in \mathbb{N}^*$ . On a

$$f(r) = f\left(n\frac{r}{n}\right) = nf\left(\frac{r}{n}\right)$$

Or f(r), n et  $f\left(\frac{r}{n}\right)$  sont des entiers. Donc f(r) est divisible par n.

Ainsi f(r) est divisible par tout entier  $n \in \mathbb{N}^*$ . On a forcément f(r) = 0. En conclusion, le seul morphisme de  $(\mathbb{Q}, +)$  dans  $(\mathbb{Z}, +)$  est le morphisme nul.

## **Solution 10**

On remarque que pour tout  $x \in G$ ,  $x^{-1} = x$ . Soient  $x, y \in G$ . On a donc  $(xy)^{-1} = xy$ . Mais on a aussi  $(xy)^{-1} = y^{-1}x^{-1} = yx$ . Par conséquent, yx = xy. Ceci étant valable pour tous  $x, y \in G$ , G est commutatif.

# **Solution 11**

Il est clair que les homothéties sont bien des endomorphismes de  $(\mathbb{R}, +)$ .

Soit maintenant f est un endomorphisme de  $(\mathbb{R}, +)$ . On a donc pour tous  $x, y \in \mathbb{R}$ , f(x + y) = f(x) + f(y). On montre par récurrence que f(nx) = nf(x) pour tout  $x \in \mathbb{R}$  et pour tout  $n \in \mathbb{R}$  puis pour tout  $n \in \mathbb{R}$  en passant à l'opposé. Soit maintenant r un rationnel. Il existe donc deux entiers p et q avec  $q \ne 0$  tels que  $r = \frac{p}{q}$ . On a d'une part

$$f(p) = f(qr) = qf(r)$$

et d'autre part

$$f(p) = pf(1)$$

Donc f(r) = rf(1). Posons donc  $\lambda = f(1)$ . Soit maintenant  $x \in \mathbb{R}$ . On sait que x est limite d'une suite de rationnels  $(r_n)$ . Or f étant continue sur  $\mathbb{R}$  et donc en x, la suite  $(f(r_n))$  tend vers f(x). Or  $f(r_n) = \lambda r_n$  pour tout  $n \in \mathbb{N}$ . Par passage à la limite, on a donc  $f(x) = \lambda x$ .

# **Solution 12**

Notons e l'élément neutre de G.

- Tout d'abord, pour tout  $x \in G$ , ex = xe = x donc  $e \in Z(G)$ .
- Soient  $(a, b) \in Z(G)^2$  et  $x \in G$ . Alors

$$(ab)x = a(bx)$$
 par associativité  
 $= a(xb)$  car  $b \in Z(G)$   
 $= (ax)b$  par associativité  
 $= (xa)b$  car  $a \in Z(G)$   
 $= x(ab)$  par associativité

Ainsi  $ab \in Z(G)$  de sorte que Z(G) est stable par produit.

• Soient  $a \in Z(G)$  et  $x \in G$ . Alors ax = xa, puis  $a^{-1}ax = a^{-1}xa$  i.e.  $x = a^{-1}xa$ . Enfin  $xa^{-1} = a^{-1}xaa^{-1} = a^{-1}x$  de sorte que  $a^{-1} \in Z(G)$ . Z(G) est donc stable par inversion.

Ainsi Z(G) est un sous-groupe de G.

#### **Solution 13**

Pour tout  $a \in \mathbb{R}$ , a \* 0 = 0 \* a = a donc 0 est élément neutre. Mais pour tout  $a \in \mathbb{R}$ ,  $(-1) * a = -1 \neq 0$  donc -1 n'admet pas d'inverse pour la loi \*.  $(\mathbb{R}, *)$  n'est donc pas un groupe.

## **Solution 14**

- **1.** Il suffit de chosir  $n = \left| \frac{\beta}{\alpha} \right|$ .
- **2.** Comme  $G \neq \{0\}$  et  $0 \in G$ , G contient un élément non nul a. Si a > 0,  $G \cap \mathbb{R}_+^*$  est non vide. Sinon, G étant un groupe,  $-a \in G$  et à nouveau  $G \cap \mathbb{R}_+^*$  est non vide.

De plus,  $G \cap \mathbb{R}_+^*$  est minorée par 0. Ainsi  $G \cap \mathbb{R}_+^*$  admet une borne inférieure.

- **3. a.** Comme  $a = \inf G \cap \mathbb{R}_+^*$  et que a > 0, il existe  $x \in G \cap \mathbb{R}_+^*$  tel que  $a \le x < a + a = 2a$ . Comme on a supposé  $a \notin G$ , on a en fait a < x < 2a. Puisque x a > 0, il existe  $y \in G \cap \mathbb{R}_+^*$  tel que  $a \le y < a + (x a) = x$ . A nouveau  $a \notin G$  donc a < y < x < 2a. Les réels x et y sont bien deux éléments distincts de  $a \in A$ .
  - **b.** Comme a < y < x < 2a, 0 < x y < a. Comme G est un sous-groupe de  $\mathbb{R}$ ,  $y x \in G$ . On a donc  $y x \in G \cap \mathbb{R}_+^*$  et y x < a, ce qui contredit le fait que  $a = \inf G \cap \mathbb{R}_+^*$ . On a donc  $a \in G$ .
  - **c.** Comme G est un sous-groupe de  $\mathbb{R}$ ,  $na \in G$  pour tout  $n \in \mathbb{Z}$ . On a donc  $a\mathbb{Z} \subset G$ .
  - **d.** D'après la question 1, il existe  $n \in \mathbb{Z}$  tel que  $na \le z < (n+1)a$ . Comme z et a sont des éléments du sous-groupe G, z na est également un élément de G. Or  $0 \le z na < a$  et  $a = \inf G \cap \mathbb{R}_+^*$ . On a donc nécessairement z na = 0 i.e. z = na.
  - **e.** Les deux questions précédentes montrent que  $G \subset a\mathbb{Z}$ . Par double inclusion,  $G = a\mathbb{Z}$ .
- **4.** a. Comme inf  $G \cap \mathbb{R}_+^* = 0$ , il existe  $\varepsilon' \in G \cap \mathbb{R}_+^*$  tel que  $0 < \varepsilon' < \varepsilon$ . D'après la question 1, il existe  $n \in \mathbb{Z}$  tel que  $n\varepsilon' \le t < (n+1)\varepsilon'$ . Posons  $g = n\varepsilon'$ .  $g \in G$  puisque  $\varepsilon' \in G$ . De plus,  $0 \le t g < \varepsilon' < \varepsilon$  donc  $|g t| < \varepsilon$ .
  - **b.** On a prouvé que pour tout élément t de  $\mathbb{R}$  et tout  $\varepsilon > 0$ , il existe un élément de G dans  $]t \varepsilon, t + \varepsilon[$  : ceci signifie que G est dense dans  $\mathbb{R}$ .

#### **Solution 15**

- **1.** Il suffit de vérifier que pour tout  $p, q \in \mathbb{Z}$ ,  $f_n(p+q) = f_n(p)f_n(q)$ .
- **2.** On vérifie que pour tout  $p \in \mathbb{Z}$ ,  $|f_n(p)| = 1$ .
- 3.  $f_n$  est injective si et seulement si Ker  $f_n = \{0\}$ . Il est donc équivalent de montrer que Ker  $f_n \neq \{0\}$  si et seulement si  $\alpha \in \mathbb{Q}$ . Si  $\alpha \in \mathbb{Q}$ , alors il existe  $a \in \mathbb{Z}$  et  $b \in \mathbb{N}^*$  tels que  $\alpha = \frac{a}{b}$ . On vérifie alors que  $f_n(b) = 1$  i.e.  $b \in \text{Ker } f_n$  et donc Ker  $f_n \neq \{0\}$ . Si Ker  $f \neq \{0\}$ , il existe  $b \in \text{Ker } f$  tel que  $b \neq 0$ . On a alors f(b) = 1 i.e.  $2\pi nb\alpha \equiv 0[2\pi]$  ou encore  $nb\alpha \equiv 0[1]$ . Autrement dit,  $nb\alpha$  est entier, ce qui signifie que  $\alpha$  est rationnel.
- **4. a.** On vérifie que pour tout  $p \in \mathbb{Z}$ ,  $f_1(p)^s = 1$  donc Im  $f_1 \subset \mathbb{U}_s$ .
  - **b.** Comme  $r \wedge s = 1$ , il existe  $u, v \in \mathbb{Z}$  tels que ur + vs = 1. On en déduit que  $f_1(u) = e^{\frac{2i\pi}{s}} \in \operatorname{Im} f_1$ . Comme  $\operatorname{Im} f_1$  est un sous-groupe de  $(\mathbb{C}^*, \times), \left(e^{\frac{2ik\pi}{s}}\right) \in \operatorname{Im} f_1$  pour tout  $k \in \mathbb{Z}$ . Ainsi  $\mathbb{U}_s \in \operatorname{Im} f_1$ .
  - **c.** On vérifie que pour tout  $k \in \mathbb{Z}$ ,  $f_1(sk) = 1$  donc  $s\mathbb{Z} \subset \operatorname{Ker} f_1$ . Soit  $p \in \operatorname{Ker} f_1$ . On a donc  $\frac{pr}{s} \in \mathbb{Z}$ . Ainsi s divise pr et puisque  $s \wedge r = 1$ , s divise p. D'où  $\operatorname{Ker} f_1 \subset \mathbb{Z}$ .
- **5. a.**  $n \wedge s$  divise s donc m est entier.

- **b.** Tout diviseur commun de n et s est un diviseur commun de nr et s.
  - Soit d un diviseur commun de nr et s. Un diviseur commun de d et s est a fortiori un diviseur commun de r et s et ne peut donc être égal qu'à  $\pm 1$ . Ceci prouve que  $d \wedge r = 1$ . D'après le théorème de Gauss, d divise n. Ainsi d est un diviseur commun de nr et s.

Finalement,  $n \wedge s = nr \wedge s$ .

- **c.** On vérifie que pour tout  $p \in \mathbb{Z}$ ,  $f_n(p)^m = 1$  car  $n \wedge s$  divise n. On a donc Im  $f_n \subset \mathbb{U}_m$ .
- **d.** Comme  $nr \wedge s = n \wedge s$ , il existe  $u, v \in \mathbb{Z}$  tels que  $unr + vs = n \wedge s$ . On en déduit que  $f_n(u) = e^{\frac{2i\pi}{m}} \in \operatorname{Im} f_n$ . Comme  $\operatorname{Im} f_n$  est un sous-groupe de  $(\mathbb{C}^*, \times), \left(e^{\frac{2ik\pi}{m}}\right) \in \operatorname{Im} f_n$  pour tout  $k \in \mathbb{Z}$ . Ainsi  $\mathbb{U}_m \in \operatorname{Im} f_n$ .
- **e.** On vérifie que pour tout  $k \in \mathbb{Z}$ ,  $f_n(mk) = 1$  car  $n \wedge s$  divise n. Ainsi  $m\mathbb{Z} \subset \operatorname{Ker} f_n$ . Soit  $p \in \operatorname{Ker} f_n$ . Ainsi  $\frac{npr}{s} \in \mathbb{Z}$  et puisque  $s \wedge r = 1$ , s divise np. Par conséquent,  $m = \frac{s}{n \wedge s}$  divise  $\frac{n}{n \wedge s}p$ . Comme  $\frac{s}{n \wedge s} \wedge \frac{n}{n \wedge s} = 1$ , m divise p. Ainsi  $\operatorname{Ker} f_n \subset m\mathbb{Z}$ .

## **Solution 16**

#### Première méthode :

Notons p le produit recherché et e l'élément neutre de G. Dans le produit, les éléments x de G tels que  $x \neq x^{-1}$  i.e.  $x^2 \neq e$  se simplifient avec leur inverse. Notons  $A = \{x \in G \mid x^2 = e\}$ . On a donc  $p = \prod_{x \in A} x$ . Les éléments de A sont d'ordre 1 ou 2. Comme l'ordre de G est impair, les éléments de A sont tous d'ordre 1, autrement dit  $A = \{e\}$  et p = e.

# Seconde méthode:

L'application  $x \mapsto x^{-1}$  est une permutation de G. Ainsi  $p = \prod_{x \in G} x = \prod_{x \in G} x^{-1}$ . D'où  $p^2 = e$ . p est donc d'ordre 1 ou 2. Comme G est d'ordre impair, p est d'ordre 1 i.e. p = e.

#### **Solution 17**

Soit f un morphisme de  $(GL_n(\mathbb{R}), \times)$  dans  $(\mathbb{Z}/m\mathbb{Z}, +)$ . On note  $D_i(\lambda) = I_n + (\lambda - 1)E_{ii}$  pour  $1 \le i \le n$  et  $\lambda \in \mathbb{R}^*$  les matrices de dilatations. On note  $T_{ij}(\lambda) = I_n + \lambda E_{ij}$  pour  $1 \le i \ne j \le n$  et  $\lambda \in \mathbb{R}$  les matrices de transvection.

On rappelle que la multiplication d'une matrice de  $\mathcal{M}_n(\mathbb{R})$  à gauche par  $T_{ij}(\lambda)$  correspond à l'opération sur les lignes  $L_i \leftarrow L_i + \lambda L_j$  et la multiplication d'une matrice de  $\mathcal{M}_n(\mathbb{R})$  à droite par  $T_{ij}(\lambda)$  correspond à l'opération sur les lignes  $C_i \leftarrow C_i + \lambda C_i$ .

Enfin, on peut échanger les lignes  $L_i$  et  $L_j$  «au signe près» en effectuant à la suite les opérations  $L_i \leftarrow L_i + L_j$ ,  $L_j \leftarrow L_j - L_i$ ,  $L_i \leftarrow L_i + L_j$ , autrement dit en multipliant à gauche par  $T_{ij}(1)T_{ji}(-1)T_{ij}(1)$ . La ligne  $L_i$  sera transformée en la ligne  $L_j$  et la ligne  $L_j$  sera transformée en la ligne  $-L_i$ .

Montrons par récurrence sur n via l'algorithme du pivot de Gauss que pour toute matrice  $A \in GL_n(\mathbb{R})$ , il existe  $M, N \in GL_n(\mathbb{R})$  telles que  $MAN = D_n(\det A)$  avec M et N des produits de matrice de transvection.

Si n = 1, il n'y a rien à faire.

Supposons que la propriété à vérifier soit vraie à un certain rang  $n-1 \ge 1$ . Soit  $A \in GL_n(\mathbb{R})$ . La première colonne de A étant non nulle, il existe  $i \in [1, n]$  tel que  $a_{i,1} \ne 0$ .

- S'il existe  $i \in [2, n]$  tel que  $a_{i,2} \neq 0$ , l'opération  $L_1 \leftarrow L_1 + \frac{1 a_{1,1}}{a_{i,1}} L_i$  permet de placer un 1 en position (1, 1).
- Si pour tout  $i \in [2, n]$ , on a  $a_{i,2} = 0$ , l'échange des lignes  $L_1$  et  $L_2$  «au signe près» permet de se ramener au cas précédent.

Il est alors aisé d'annuler tous les coefficients de la première ligne et la première colonne (hormis le 1 en position (1,1)) à l'aide d'opérations sur les lignes et les colonnes. Autrement dit, il existe deux matrices M' et N' qui sont des produits de matrice de transvection telles que

$$M'AN' = \begin{pmatrix} 1 & 0 \\ 0 & A' \end{pmatrix}$$
. Il suffit alors d'appliquer l'hypothèse de récurrence à A'.

**Remarque.** On a en fait montré que  $SL_n(\mathbb{R})$  est engendré par les matrices de transvection et que  $GL_n(\mathbb{R})$  est engendré par les matrices de transvection et les matrices de dilatation.

Puisque  $T_{ij}(\lambda) = T_{ij}\left(\frac{\lambda}{m}\right)^m$ , on a  $f\left(T_{ij}(\lambda)\right) = 0$ . On en déduit que pour tout  $A \in GL_n(\mathbb{R})$ ,  $f(A) = f(D_n(\det A))$ .

Si m est impair, pour tout  $\lambda \in \mathbb{R}^*$ ,  $D_n(\lambda) = D_n \left( \sqrt[m]{\lambda} \right)^m$  donc  $f(A) = \bar{0}$  pour tout  $A \in GL_n(\mathbb{R})$ . f est donc le morphisme trivial.

Si m est pair, pour tout  $\lambda \in \mathbb{R}_+^*$ ,  $D_n(\lambda) = D_n \binom{n}{\sqrt{\lambda}}^{m'}$  donc  $f(A) = \bar{0}$  pour tout  $A \in GL_n^+(\mathbb{R})$ . De plus, si  $\lambda \in \mathbb{R}_-^*$ ,  $D_n(\lambda) = D_n(-1)D_n(-\lambda)$ . Ainsi, pour tout  $A \in GL_n^-(\mathbb{R})$ ,  $f(A) = f(D_n(-1))$ . Or  $D_n(-1)^2 = I_n$  donc  $f(D_n(-1)) = \bar{0}$  ou  $f(D_n(-1)) = \bar{p}$  où m = 2p. f est donc soit le morphisme trivial, soit le morphisme valant  $\bar{0}$  sur  $GL_n^+(\mathbb{R})$  et  $\bar{p}$  sur  $GL_n^-(\mathbb{R})$ .

#### **Solution 18**

## Associativité:

Soient  $x, y, z \in H$ .

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

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

$$= f((f^{-1}(x) * f^{-1}(y)) * f^{-1}(z)) \text{ par associativit\'e de } *$$

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

$$= (x.y).z$$

## Elément neutre :

Notons e l'élément neutre de (G, \*). Pour tout  $x \in H$ 

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

Donc (H, .) admet un élément neutre, à savoir f(e).

## Inversibilité:

Soit  $x \in H$ .

$$x.f\left(\left(f^{-1}(x)\right)^{-1}\right) = f\left(f^{-1}(x) * \left(f^{-1}(x)\right)^{-1}\right) = f(e)$$
$$f\left(\left(f^{-1}(x)\right)^{-1}\right).x = f\left(\left(f^{-1}(x)\right)^{-1} * f^{-1}(x)\right) = f(e)$$

Ainsi tout élément x de G est inversible (d'inverse  $(f^{-1}(x))^{-1}$ ).

**Remarque.** On a des résultats similaires pour les anneaux et les corps. La bijection f permet de «transporter» la structure de G sur H.

# **Solution 19**

## Associativité:

Soient  $x', y', z' \in H$ . Comme f est surjective, x', y', z' admmettent des antécédents x, y, z par f dans G.

$$x'.(y'.z') = f(x).(f(y).f(z))$$

$$= f(x).f(y*z)$$

$$= f(x*(y*z))$$

$$= f((x*y)*z) \text{par associativit\'e de } *$$

$$= f(x*y).f(z)$$

$$= (f(x).f(y)).f(z)$$

$$= (x'.y').z'$$

#### Elément neutre :

Notons e l'élément neutre de G. Soit  $x' \in G$ . Comme f est surjective, x' admet un antécédent x par f dans G

$$x'.f(e) = f(x).f(e) = f(x*e) = f(x) = x'$$
  
 $f(e).x' = f(e).f(x) = f(e*x) = f(x) = x'$ 

Ainsi (H, .) admet un élément neutre, à savoir f(e).

## Inversibilité:

Soit  $x' \in G$ . Comme f est surjective, x' admet un antécédent x par f dans G.

$$x'.f(x^{-1}) = f(x).f(x^{-1}) = f(x * x^{-1}) = f(e)$$
  
 $f(x^{-1}).x' = f(x^{-1}).f(x) = f(x^{-1} * x) = f(e)$ 

Ainsi tout élément de G est inversible.

Puisque G et H sont des groupes, f est un morphisme de groupes.

**Remarque.** On a des résultats pour les anneaux et les corps. La surjection f permet de «transporter» la structure de G sur H.

#### Solution 20

Notons e l'élément neutre de G.

Pour tout  $x \in G$ ,  $x = e^{-1}xe$  donc  $x \sim x$ . Ainsi  $\sim$  est réflexive.

Soit  $(x, y) \in G^2$  tel que  $x \sim y$ . Il existe donc  $g \in G$  tel que  $y = g^{-1}xg$ . Mais alors  $x = gyg^{-1} = (g^{-1})^{-1}x(g^{-1})$  donc  $y \sim y$ . Ainsi  $\sim$  est symétrique.

Soit  $(x, y, z) \in G^3$  tel que  $x \sim y$  et  $y \sim z$ . Il existe donc  $(g, h) \in G^2$  tel que  $y = g^{-1}xg$  et  $z = h^{-1}yh$ . Mais alors  $z = h^{-1}g^{-1}xgh = (gh)^{-1}x(gh)$  donc  $x \sim z$ . Ainsi  $\sim$  est transitive.

Finalement, ~ est bien une relation d'équivalence.

## **Solution 21**

Notons e l'élément neutre de G.

Pour tout  $x \in G$ , x = xe et  $e \in H$  car H est un sous-groupe de G donc  $x \sim x$ . Ainsi  $\sim$  est réflexive.

Soit  $(x, y) \in G^2$  tel que  $x \sim y$ . Il existe donc  $h \in H$  tel que y = xh. Mais alors  $x = yh^{-1}$  et  $h^{-1} \in H$  car H est un sous-groupe de G donc  $y \sim y$ . Ainsi  $\sim$  est symétrique.

Soit  $(x, y, z) \in G^3$  tel que  $x \sim y$  et  $y \sim z$ . Il existe donc  $(h, k) \in H^2$  tel que y = xh et z = yk. Mais alors z = xhk et  $hk \in H$  car H est un sous-groupe de G donc  $x \sim z$ . Ainsi  $\sim$  est transitive.

Finalement, ~ est bien une relation d'équivalence.

Remarque. On montrerait de la même manière que la relation binaire ~ définie par

$$\forall (x, y) \in G^2, x \sim y \iff \exists h \in H, y = hx$$

est également une relation d'équivalence.

#### Solution 22

On notera e l'élément neutre de G.

Relation  $\sim$ :

**Réflexivité** Pour tout  $x \in G$ ,  $x = e^{-1}xe$  et  $e \in H$  car H est un sous-groupe de G donc  $x \sim x$ .

Symétrie Soit  $(x, y) \in G^2$  tel que  $x \sim y$ . Il existe donc  $h \in H$  tel que  $y = h^{-1}xh$ . Alors  $x = hyh^{-1} = (h^{-1})^{-1}yh^{-1}$  et  $h^{-1} \in H$  car H est un sous-groupe de G donc  $y \sim x$ .

**Transitivité** Soit  $(x, y, z) \in G^3$  tel que  $x \sim y$  et  $y \sim z$ . Il existe donc  $(h, k) \in H^2$  tel que  $y = h^{-1}xh$  et  $z = k^{-1}yk$ . Donc  $z = k^{-1}h^{-1}xhk = (hk)^{-1}(hk)$  et  $hk \in H$  car H est un sous-groupe de G donc  $x \sim z$ .

Relation  $\sim_g$ :

**Réflexivité** Pour tout  $x \in G$ , x = ex et  $e \in H$  car H est un sous-groupe de G donc  $x \sim_g x$ .

**Symétrie** Soit  $(x, y) \in G^2$  tel que  $x \sim_g y$ . Il existe donc  $h \in H$  tel que y = hx. Alors  $x = h^{-1}y$  et  $h^{-1} \in H$  car H est un sous-groupe de G donc  $y \sim_g x$ .

**Transitivité** Soit  $(x, y, z) \in G^3$  tel que  $x \sim_g y$  et  $y \sim_g z$ . Il existe donc  $(h, k) \in H^2$  tel que y = hx et z = ky. Donc z = khx et  $kh \in H$  car H est un sous-groupe de G donc  $x \sim_g z$ .

**Relation**  $\sim_d$ :

**Réflexivité** Pour tout  $x \in G$ , x = xe et  $e \in H$  car H est un sous-groupe de G donc  $x \sim_d x$ .

**Symétrie** Soit  $(x, y) \in G^2$  tel que  $x \sim_d y$ . Il existe donc  $h \in H$  tel que y = xh. Alors  $x = yh^{-1}$  et  $h^{-1} \in H$  car H est un sous-groupe de G donc  $y \sim_d x$ .

**Transitivité** Soit  $(x, y, z) \in G^3$  tel que  $x \sim_d y$  et  $y \sim_d z$ . Il existe donc  $(h, k) \in H^2$  tel que y = xh et z = yk. Donc z = xhk et  $hk \in H$  car H est un sous-groupe de G donc  $x \sim_d z$ .

#### Solution 23

- 1. On rappelle que  $S(\mathbb{C})$  désigne l'ensemble des bijections de  $\mathbb{C}$  dans  $\mathbb{C}$ . On va montrer que G est un sous-groupe de  $S(\mathbb{C})$ .
  - Montrons que  $G \subset S(\mathbb{C})$ . Soit  $f \in G$ . Il existe donc  $(a, b) \in \mathbb{C}^* \times \mathbb{C}$  tel que f(z) = az + b pour tout  $z \in \mathbb{C}$ . On montre alors que f est bijective en vérifiant que  $z \mapsto \frac{1}{z}(z-b)$  est sa bijection réciproque.
  - Clairement, Id<sub>ℂ</sub> ∈ G, puisque Id<sub>ℂ</sub> est par exemple la translation de vecteur nul ou une rotation d'angle nul (et de centre quelconque).
  - Montrons que G est stable par composition. Soit  $(f,g) \in G^2$ . Il existe donc  $(a,b,c,d) \in \mathbb{C}^* \times \mathbb{C} \times \mathbb{C}^* \times \mathbb{C}$  tel que f(z) = az + b et g(z) = cz + d pour tout  $z \in \mathbb{C}$ . Alors  $g \circ f(z) = caz + cb + d$  pour tout  $z \in \mathbb{C}$ .  $g \circ f$  est bien une translation ou une similitude directe puisque  $ca \neq 0$ .
  - Montrons que G est stable par inversion. Soit  $f \in G$ . Il existe donc  $(a, b) \in \mathbb{C}^* \times \mathbb{C}$  tel que f(z) = az + b pour tout  $z \in \mathbb{C}$ . On a montré précédemment que  $f^{-1}(z) = \frac{1}{a}z \frac{b}{a}$  pour tout  $z \in \mathbb{C}$ . Ceci montre que  $f^{-1}$  est bien une translation ou une similitude directe puisque  $\frac{1}{a} \neq 0$ .

On a donc montré que G était un sous-groupe de  $S(\mathbb{C})$  et donc un groupe.

- 2. A nouveau, Id<sub>C</sub> ∈ H, puisque Id<sub>C</sub> est par exemple la translation de vecteur nul ou une rotation d'angle nul (et de centre quel-conque).
  - Montrons que H est stable par composition. Soit  $(f,g) \in H^2$ . Il existe donc  $(a,b,c,d) \in \mathbb{U} \times \mathbb{C} \times \mathbb{U} \times \mathbb{C}$  tel que f(z) = az + b et g(z) = cz + d pour tout  $z \in \mathbb{C}$ . Alors  $g \circ f(z) = caz + cb + d$  pour tout  $z \in \mathbb{C}$ .  $g \circ f$  est bien une translation ou une rotation puisque  $ca \in \mathbb{U}$ .
  - Montrons que H est stable par inversion. Soit  $f \in H$ . Il existe donc  $(a,b) \in \mathbb{U} \times \mathbb{C}$  tel que f(z) = az + b pour tout  $z \in \mathbb{C}$ . On a montré précédemment que  $f^{-1}(z) = \frac{1}{a}z \frac{b}{a}$  pour tout  $z \in \mathbb{C}$ . Ceci montre que  $f^{-1}$  est bien une translation ou une rotation puisque  $ca \in \mathbb{U}$ .

On a donc montré que H était un sous-groupe de G.

#### **Solution 24**

- 1. On sait que thest strictement croissante et continue sur  $\mathbb{R}$ . De plus,  $\lim_{-\infty} th = -1$  et  $\lim_{+\infty} th = 1$ . Donc thinduit une bijection de  $\mathbb{R}$  sur G.
- 2. Soit  $(a,b) \in \mathbb{R}^2$ .

$$\begin{split} \frac{\operatorname{th}(a) + \operatorname{th}(b)}{1 + \operatorname{th}(a) \operatorname{th}(b)} &= \frac{\frac{\operatorname{sh} a}{\operatorname{ch} a} + \frac{\operatorname{sh} b}{\operatorname{ch} b}}{1 + \frac{\operatorname{sh} a}{\operatorname{ch} a} \cdot \frac{\operatorname{sh} b}{\operatorname{ch} b}} \\ &= \frac{\operatorname{sh} a \operatorname{ch} b + \operatorname{sh} b \operatorname{ch} a}{\operatorname{ch} a \operatorname{ch} b + \operatorname{sh} a \operatorname{sh} b} \\ &= \frac{(e^a - e^{-a})(e^b + e^{-b}) + (e^b - e^{-b})(e^a + e^{-a})}{(e^a + e^{-a})(e^b + e^{-b}) + (e^b - e^{-b})(e^a - e^{-a})} \\ &= \frac{e^{a+b} - e^{-(a+b)}}{e^{a+b} + e^{-(a+b)}} = \operatorname{th}(a+b) \end{split}$$

3. Vérifions que  $\star$  est une loi interne sur G. Soit  $(x, y) \in G^2$ . Par surjectivité de th sur G, il existe  $(a, b) \in \mathbb{R}^2$  tel que x = th a et y = th b. Alors  $x \star y = \text{th}(a + b) \in G$ .

La loi ★ est clairement commutative.

Vérifions que ★ est associative. Soit  $(x, y, z) \in G^3$ . Comme précédemment, il existe  $(a, b, c) \in \mathbb{R}^3$  tel que  $(x, y, z) = (\operatorname{th} a, \operatorname{th} b, \operatorname{th} c)$ . Alors

$$(x \star y) \star z = \operatorname{th}(a+b) \star \operatorname{th} c = \operatorname{th}(a+b+c) = \operatorname{th} a \star \operatorname{th}(b+c) = x \star (y \star z)$$

Pour tout  $x \in G$ ,  $0 \star x = x \star 0 = x$  et  $0 \in G$  donc 0 est neutre pour  $\star$ .

Enfin, pour tout  $x \in G$ ,  $x \star (-x) = (-x) \star x = 0$  et  $-x \in G$  donc tout élément de G est inversible pour la loi  $\star$ .

Tout ceci prouve que  $(G, \star)$  est un groupe commutatif.

**4.** Tout d'abord  $x^{\star 0} = 0 = \frac{(1+x)^0 - (1-x)^0}{(1+x)^0 + (1-x)^0}$ . Supposons que  $x^{\star n} = \frac{(1+x)^n - (1-x)^n}{(1+x)^n + (1-x)^n}$  pour un certain  $n \in \mathbb{N}$ . Alors

$$\begin{split} x^{\star(n+1)} &= x \star x^{\star n} \\ &= \frac{x + x^{\star n}}{1 + x \cdot x^{\star n}} \\ &= \frac{x + \frac{(1+x)^n - (1-x)^n}{(1+x)^n + (1-x)^n}}{1 + x \cdot \frac{(1+x)^n - (1-x)^n}{(1+x)^n + (1-x)^n}} \\ &= \frac{x(1+x)^n + x(1-x)^n + (1+x)^n - (1-x)^n}{(1+x)^n + (1-x)^n + x(1+x)^n - x(1-x)^n} \\ &= \frac{(1+x)(1+x)^n - (1-x)(1-x)^n}{(1+x)(1+x)^n + (1-x)(1-x)^n} \\ &= \frac{(1+x)^{n+1} - (1-x)^{n+1}}{(1+x)^{n+1} + (1-x)^{n+1}} \end{split}$$

Par récurrence, l'égalité de l'énoncé est vraie pour tout  $n \in \mathbb{N}$ . Enfin, si  $n \in \mathbb{Z}_+$ , en utilisant le fait que  $-n \in \mathbb{N}$ ,

$$x^{*n} = (x^{*-1})^{*(-n)} = (-x)^{*(-n)}$$

$$= \frac{(1+(-x))^{-n} - (1-(-x))^{-n}}{(1+(-x))^{-n} + (1-(-x))^{-n}}$$

$$= \frac{\frac{1}{(1-x)^n} - \frac{1}{(1+x)^n}}{\frac{1}{(1-x)^n} + \frac{1}{(1+x)^n}}$$

$$= \frac{(1+x)^n - (1-x)^n}{(1+x)^n + (1-x)^n}$$

## **Solution 25**

Suppospons G fini. Alors l'ensemble de ses parties est également fini. A fortiori, l'ensemble de ses sous-groupes est fini. Supposons que l'ensemble des sous-groupes de G est fini. Montrons d'abord que tout élément de G est d'ordre fini. Soit  $x \in G$ . Si x n'est pas d'ordre fini, alors les sous-groupes  $\langle x^k \rangle$  pour  $k \in \mathbb{N}$  sont distincts et en nombre infini, ce qui contredit l'hypothèse de départ. De plus,  $G = \bigcup_{x \in G} \langle x \rangle$ . Mais les sous-groupes  $\langle x \rangle$  sont en nombre fini par hypothèse et sont tous finis car tout  $x \in G$  est d'ordre fini. Par conséquent, G est fini.

#### Solution 26

Soit G un groupe cyclique d'ordre n et g un de ses générateurs. Notons p le plus petit entier naturel non nul tel que  $g^p \in H$ . On va montrer que H est le sous-groupe engendré par  $g^p$ . Ce sera donc un sous-groupe cyclique. Puisque  $g^p \in H$ , le sous-groupe engendré par  $g^p$  est bien inclus dans H. Soit maintenant  $h \in H$ . Puisque g engrendre G, il existe  $q \in \mathbb{N}^*$  tel que  $h = g^q$ . Effectuons la division euclidienne de q par p: il existe  $(a,b) \in \mathbb{N}$  tel que q = ap + b et b < p. Mais alors  $g^b = h(g^p)^{-a} \in H$  de sorte que, par minimalité de p, p = 0. Ainsi p = p

## **Solution 27**

Soient g un générateur de G et d un diviseur de n. Posons  $k = \frac{n}{d}$ . On va montrer que le sous-groupe H engendré par  $g^k$  est l'unique sous-groupe de G d'ordre d.

Montrons tout d'abord que H est bien d'ordre d. L'ordre de H est l'ordre de  $g^k$ : il s'agit donc de montrer que l'ordre p de  $g^k$  vaut bien d. Puisque  $(g^k)^d = g^n = e$ , p divise d. Si on avait p < d, alors  $g^n = g^{kp} = e$  et kp < kd = n, ce qui contredit que g est un générateur de G. Ainsi p = d.

Montrons maintenant que H est bien l'unique sous-groupe de G d'ordre d. Soit K un sous-groupe de G d'ordre d. Puisque K et H sont tous deux d'ordre d, il suffit de montrer que K  $\subset$  H. Soit  $x \in$  K. Il existe alors un entier p tel que  $g^p = x$ . Puisque K est d'ordre d,  $g^{pd} = k^d = e$ . Ainsi n = kd divise pd puis k divise p. Il existe donc un entier q tel que p = kq. Mais alors  $x = g^p = g^{kq} = (g^k)^q \in$  H. Ainsi K  $\subset$  H puis K = H par égalité des ordres de K et H.

# **Solution 28**

Remarquons déjà que G est commutatif. En effet, si  $(x, y) \in G^2$ , alors  $(xy)^2 = e$  où e est le neutre. Ainsi xyxy = e puis en multipliant par yx à droite, xy = yx.

Comme G est fini, il admet une partie génératrice minimale  $\{g_1, \dots, g_r\}$ . On montre alors que l'application  $\begin{cases} (\mathbb{Z}/2\mathbb{Z})^r & \longrightarrow & G \\ (\bar{\varepsilon}_1, \dots, \bar{\varepsilon}_r) & \longmapsto & g_1^{\varepsilon_1} \dots g_r^{\varepsilon_r} \end{cases}$  est un isomorphisme de groupes. On en déduit que  $|G| = |(\mathbb{Z}/2\mathbb{Z})^r| = 2^r$ .

## Solution 29

Soit G un groupe d'ordre p premier. Soit x un élément non neutre de G. L'ordre de x divise donc p. Comme p est premier, l'ordre de x vaut 1 ou p. Mais x n'est pas neutre donc son ordre ne vaut pas 1. Ainsi l'ordre de x est p et G est cyclique.

#### Solution 30

Tout d'abord, comme x et y commutent,  $(xy)^{pq} = x^{pq}y^{pq} = (x^p)^qy^{(q)}^p = e$  où e est le neutre de G. Ainsi l'ordre d de xy divise pq. Par ailleurs,  $(xy)^d = e$  i.e.  $x^d = y^{-d}$  et  $y^d = x^{-d}$ . Ainsi  $x^{dq} = y^{dp} = e$  puis p divise dq et q divise dp. Comme p et q sont premiers entre eux, p divise d et q divise d d'après le lemme de Gauss. Mais en utilisant à nouveau le fait que p et q sont premiers entre eux, pq divise d. Finalement, d = pq.

#### Solution 31

On notera e l'élément neutre de G. Les éléments de G sont d'ordre 1, 2, 3 ou 6.

Si G possède un élément d'ordre 6, alors G est cyclique et donc isomorphe à  $\mathbb{Z}/6\mathbb{Z}$ .

Supposons que G ne possède pas d'élément d'ordre 6. Evidemment, les éléments de G ne peuvent pas tous être d'ordre 1 (seul l'élément neutre est d'ordre 1).

Supposons que G ne possède que des éléments d'ordre 2 hormis l'élément neutre.

Supposons que G ne possède que des éléments d'ordre 2 hormis l'élément neutre.

Ainsi G possède un élément  $\tau$  d'ordre 2 et un élément  $\gamma$  d'ordre 3. Par conséquent,  $\{e, \tau, \gamma, \tau\gamma, \gamma\tau, \tau\gamma\tau\} \subset G$ . On vérifie que les 6 élément sont bien deux à deux distincts.

- e,  $\tau$  et  $\gamma$  sont bien deux à deux distincts puisqu'ils sont d'ordre deux à deux distincts.
- τγ

#### **Solution 32**

- 1.  $\mathbb{U} \subset \mathbb{C}^* \operatorname{car} |0| = 0 \neq 1$ .
  - $1 \in \mathbb{U} \text{ car } |1| = 1.$
  - Soit  $(z_1, z_2) \in \mathbb{U}^2$ . Alors  $\left| \frac{z_1}{z_2} \right| = \frac{|z_1|}{|z_2|} = \frac{1}{1} = 1$  donc  $\frac{z_1}{z_2} \in \mathbb{U}$ .

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

- **2.**  $\mathbb{U}_n \subset \mathbb{C}^*$  car pour  $0^n = 0 \neq 1$ .
  - $1 \in \mathbb{U}_n \operatorname{car} 1^n = 1$ .
  - Soit  $(z_1, z_2) \in \mathbb{U}_n^2$ . Alors  $\left(\frac{z_1}{z_2}\right)^n = \frac{z_1^n}{z_2^n} = \frac{1}{1} = 1$  donc  $\frac{z_1}{z_2} \in \mathbb{U}_n$ .

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

- **3.** a. Soit  $(z_1, z_2) \in (\mathbb{C}^*)^2$ . Alors  $f(z_1 z_2) = (z_1 z_2)^n = z_1^n z_2^n = f(z_1) f(z_2)$ . f est donc un endomorphisme de  $(\mathbb{C}^*, \times)$ .
  - **b.** Ker  $f = \{z \in \mathbb{C}^*, z^n = 1\} = \mathbb{U}_n$ . Le noyau de f étant un sous-groupe du groupe de départ,  $\mathbb{U}_n$  est un sous-groupe de  $(\mathbb{C}^*, \times)$ .
  - c. Si n = 1,  $f = \text{Id}_{\mathbb{C}^*}$  donc f est injectif. Sinon, card  $\text{Ker } f = \text{card } \mathbb{U}_n = n > 1$  donc  $\text{Ker } f \neq \{1\}$ . Ainsi f n'est pas injectif.
  - **d.** Tout nombre complexe non nul admet une racine  $n^{\text{ème}}$  non nulle (il en admet même n) donc  $\text{Im } f = \mathbb{C}^*$  et f est surjectif.
- **4.** a. Soit  $(\theta_1, \theta_2) \in \mathbb{R}^2$ . Alors  $g(\theta_1 + \theta_2) = e^{i(\theta_1 + \theta_2)} = e^{i\theta_1}e^{i\theta_2} = g(\theta_1)g(\theta_2)$ . g est donc un morphisme du groupe  $(\mathbb{R}, +)$  dans le groupe  $(\mathbb{C}^*, \times)$ .
  - **b.** Ker  $g = 2\pi \mathbb{Z} \neq \{0\}$  donc g n'est pas injectif.

- **c.** Im  $g = \{e^{i\theta}, \theta \in \mathbb{R}\} = \mathbb{U}$ . L'image de g étant un sous-groupe du groupe d'arrivée,  $\mathbb{U}$  est un sous-groupe de  $(\mathbb{C}^*, \times)$ .
- **d.** Im  $g = \mathbb{U} \neq \mathbb{C}^*$  donc g n'est pas surjectif.
- **5. a.** Soit  $(z_1, z_2) \in (\mathbb{C}^*)^2$ . Alors  $h(z_1 z_2) = |z_1 z_2| = |z_1| |z_2| = h(z_1) h(z_2)$ . h est donc un morphisme de  $(\mathbb{C}^*, \times)$  dans  $(\mathbb{R}^*, \times)$ .
  - **b.** Ker  $h = \{z \in \mathbb{C}^*, |z| = 1\} = \mathbb{U}$ . Le noyau de h étant un sous-groupe du groupe de départ,  $\mathbb{U}$  est un sous-groupe de  $(\mathbb{C}^*, \times)$ .
  - **c.** Ker  $h = \mathbb{U} \neq \{1\}$  donc h n'est pas injectif.
  - **d.** Im  $h = \mathbb{R}_+^* \neq \mathbb{R}^*$  donc h n'est pas surjectif.