THÉORIE DES GROUPES - SÉRIES 1+2

20 et 27 septembre 2019

Groupes

Exercice 1. Soit $(G, \cdot, e)$ un groupe. Montrer que:

(a) si $g \cdot a = g \cdot b$ ou $a \cdot g = b \cdot g$, alors $a = b$, pour tous $a, b, g \in G$,

(b) l'élément e est l'unique élément de G tel que $e \cdot g = g = g \cdot e$ pour tout $g \in G$,

(c) chaque élément $g \in G$ a un unique inverse $h \in G$ tel que $h \cdot g = e = g \cdot h$; on écrit $h = g^{-1}$,

(d) $(g^{-1})^{-1} = g$, pour tout $g \in G$.

(e) l'unique élément tel que $g \cdot g = g$ est l'élément e.

Solution.

(a) Soit h l'inverse de g. Alors

$$a = e \cdot a = (h \cdot g) \cdot a = h \cdot (g \cdot a) = h \cdot (g \cdot b) = (h \cdot g) \cdot b = e \cdot b = b.$$

On prouve l'autre cas similairement.

(b) Supposons qu'on ait $f \in G$ tel que $f \cdot g = g = g \cdot f$ pour tout $g \in G$. Alors

$$e = e \cdot f = f,$$

en utilisant les équations pour e et f respectivement.

(c) Soit $h' \in G$ tel que $h' \cdot g = e = g \cdot h'$. Alors

$$h' = h' \cdot e = h' \cdot (g \cdot h) = (h' \cdot g) \cdot h = e \cdot h = h.$$

(d) On a que

$$g = g \cdot e = g \cdot (g^{-1} \cdot (g^{-1})^{-1}) = (g \cdot g^{-1}) \cdot (g^{-1})^{-1} = e \cdot (g^{-1})^{-1} = (g^{-1})^{-1}.$$

(e) Supposons qu'on ait $g \in G$ tel que $g \cdot g = g$. Par (a), on obtient directement que $g = e$ puisque $g \cdot g = g = g \cdot e$.

Exercice 2. Déterminer si chacune des structures suivantes est une structure de groupe. Si oui, déterminer si la structure est abélienne.

(a) les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ munis de l'addition;

(b) les ensembles $\mathbb{N}^*$, $\mathbb{Z}^*$, $\mathbb{Q}^*$ et $\mathbb{R}^*$ munis de la multiplication;

(c) l'ensemble $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ muni de la multiplication;

(d) l'ensemble des parties $\mathcal{P}(X) = \{A \mid A \subset X\}$ d'un ensemble X muni de la différence symétrique $A + B = (A \setminus B) \cup (B \setminus A)$, pour $A, B \subseteq X$;

(e) l'ensemble $GL_n(\mathbb{R})$ des matrices inversibles de taille $n \times n$ muni de la multiplication matricielle;

(f) étant donné un groupe abélien G et un groupe non-abélien H, leur produit cartésien $G \times H$ muni de la loi $(g, h) \cdot (g', h') = (gg', hh')$;

(g) l'ensemble $\mathbb{R}$ muni de la loi $x \cdot y = xy + 1$, pour $x, y \in \mathbb{R}$;

(h) l'ensemble $\mathbb{R}^2$ muni de la loi $(a, b) \cdot (c, d) = (ac, bc + d)$, pour $(a, b), (c, d) \in \mathbb{R}^2$;

Solution.

(a) On vérifie que l'addition donne une structure de groupe à $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$. En effet, elle est associative, l'élément neutre est 0, et l'inverse d'un élément x est $-x$. Ces groupes sont clairement abélien. En revanche, $\mathbb{N}$ n'est pas un groupe muni de l'addition, car $n \in \mathbb{N} \setminus \{0\}$ n'admet pas d'inverse dans $\mathbb{N}$, vu que tous les éléments de $\mathbb{N}$ sont positifs.

(b) On vérifie que la multiplication donne une structure de groupe à $\mathbb{Q}^*$ et $\mathbb{R}^*$. En effet, elle est associative, l'élément neutre est 1, et l'inverse d'un élément x est $\frac{1}{x}$. Ces groupes sont clairement abélien. En revanche, $\mathbb{N}$ et $\mathbb{Z}$ ne sont pas des groupes munis de la multiplication. Par exemple, 2 n'admet pas d'inverse pour la multiplication dans $\mathbb{N}$ ou $\mathbb{Z}$, car $\frac{1}{2}$ n'est pas entier.

(c) On vérifie que S^1 est un groupe. En effet, si $z, w \in S^1$, alors $|zw| = |z| \cdot |w| = 1$ et donc $zw \in S^1$, ce qui montre que la multiplication est bien définie. De plus, elle est associative d'élément neutre 1. Finalement, l'inverse d'un élément $z \in S^1$ est son conjugué $\bar{z}$, qui appartient aussi à S^1 vu que $|\bar{z}| = |z| = 1$. Clairement, S^1 est abélien.

(d) On vérifie que $\mathcal{P}(X)$ forme un groupe. La différence symétrique est associative, vu que la réunion et l'intersection sont associatives, l'élément neutre est l'ensemble vide $\emptyset$ et l'inverse de $A \subset X$ est A. En effet, $A + A = A \setminus A = \emptyset$. Clairement, $\mathcal{P}(X)$ est abélien.

(e) On vérifie que $GL_n(\mathbb{R})$ forme un groupe. La multiplication matricielle est associative, l'élément neutre est donné par la matrice identité I_n, et l'inverse de $A \in GL_n(\mathbb{R})$ est A^{-1}. Par contre, $GL_n(\mathbb{R})$ n'est pas abélien, car la multiplication matricielle n'est pas commutative.

(f) Le produit cartésien $G \times H$ est un groupe. L'associativité découle de l'associativité des structures de groupe de G et H. L'élément neutre est donné par $(1_G, 1_H)$, où 1_G est l'élément neutre de G et 1_H celui de H. L'inverse d'un élément (g, h) est donné par (g^{-1}, h^{-1}). Par contre, $G \times H$ n'est pas abélien, puisque H ne l'est pas.

(g) L'ensemble $\mathbb{R}$ muni de cette loi n'est pas un groupe. En effet, il n'y a aucun élément neutre pour cette relation. Supposons par l'absurde qu'il existe $e \in \mathbb{R}$ tel que $e \times x = x$ pour tout $x \in \mathbb{R}$. Alors

$$e \cdot x = x \quad \forall x \in \mathbb{R} \iff ex + 1 = x \quad \forall x \in \mathbb{R} \iff e = \frac{x-1}{x} \quad \forall x \in \mathbb{R}$$

ce qui est absurde.

(h) L'ensemble $\mathbb{R}^2$ muni de cette loi forme un groupe. On montre l'associativité: pour tous $(a, b), (c, d), (e, f) \in \mathbb{R}^2$, on a

$$\begin{aligned}((a, b) \cdot (c, d)) \cdot (e, f) &= (ac, bc + d) \cdot (e, f) = (ace, (bc + d)e + f) = (ace, bce + de + f) \\ &= (a, b) \cdot (ce, de + f) = (a, b) \cdot ((c, d) \cdot (e, f)).\end{aligned}$$

L'élément neutre est donné par $(1,0)$: pour tout $(a,b) \in \mathbb{R}^2$, on a

$$(1,0) \cdot (a,b) = (a,b) = (a,b) \cdot (1,0).$$

L'inverse d'un élément $(a,b) \in \mathbb{R}^2$ est donné par $(\frac{1}{a}, -\frac{b}{a})$, puisque

$$(a,b) \cdot (\frac{1}{a}, -\frac{b}{a}) = (1,0) = (\frac{1}{a}, -\frac{b}{a}) \cdot (a,b).$$

Par contre, ce n'est pas un groupe abélien. Par exemple,

$$(1,1) \cdot (2,0) = (2,1) \neq (2,2) = (2,0) \cdot (1,1).$$

Exercice 3. Soit G un ensemble. On suppose que G admette deux structures de groupes $(\cdot, e)$ et $(*, f)$ telles que, pour tous $a, b, c, d \in G$,

$$(a \cdot b) * (c \cdot d) = (a * c) \cdot (b * d).$$

Montrer que:

(a) les deux structures de groupe sur G coïncident, i.e. $e = f$ et $g \cdot h = g * h$ pour tous $g, h \in G$,

(b) le groupe G muni de ces structures est abélien.

Solution. On prend $a = d = e$ et $b = c = f$, ce qui donne

$$f = f * f = (e \cdot f) * (f \cdot e) = (e * f) \cdot (f * e) = e \cdot e = e.$$

Ainsi $e = f$ et on écrit e pour l'élément neutre de $*$ également. Soit $g, h \in G$. On prend $a = g$, $d = h$ et $b = c = e$ et on obtient

$$g * h = (g \cdot e) * (e \cdot h) = (g * e) \cdot (e * h) = g \cdot h,$$

ce qui prouve que les deux structures $\cdot$ et $*$ coïncident. Il reste à montrer que $g \cdot h = h \cdot g$. On prend $a = d = e$ et $b = g$, $c = h$ et on obtient

$$g \cdot h = g * h = (e \cdot g) * (h \cdot e) = (e * h) \cdot (g * e) = h \cdot g.$$

On conclut que G est abélien.
Remarque: Ce résultat s'appelle l'argument de Eckmann-Hilton.

Exercice 4. Soit G un groupe fini d'ordre n. Montrer que:

(a) si n est pair, alors le nombre d'éléments d'ordre 2 est impair. En particulier, G contient au moins un élément d'ordre 2.

(b) si tous les éléments (sauf l'élément neutre) du groupe G sont d'ordre 2, alors G est abélien.

Solution. On écrit $\mathrm{ord}(x)$ pour l'ordre d'un élément $x \in G$.

(a) On pose $A = \{x \in G \mid \mathrm{ord}(x) = 2\}$ et $B = \{x \in G \mid \mathrm{ord}(x) > 2\}$. Alors $G \setminus A = B \cup \{e\}$. Or B est de cardinalité paire, car on peut coupler chaque élément avec son inverse. Ainsi, comme $n = \#G = (\#A) + (\#B) + 1$ et $\#G = n$ et $\#B$ sont pairs, alors $\#A$ est impair. En particulier, $\#A$ vaut au moins 1.

(b) Pour chaque $x \in G$, on a que $x^2 = e$, donc x est son propre inverse. Ainsi, pour $x, y \in G$,

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$

et G est abélien.

Sous-groupes

Exercice 5. Vérifier ou réfuter les affirmations suivantes.

(a) L'intersection de n'importe quelle famille de sous-groupes est un sous-groupe.

(b) La réunion de n'importe quelle famille de sous-groupes est un sous-groupe.

(c) L'intersection d'un nombre fini de sous-groupes est un sous-groupe.

(d) La réunion d'un nombre fini de sous-groupes est un sous-groupe.

Solution. Les affirmations (a) et (c) sont vraies et les affirmations (b) et (d) sont fausses.

On prouve (a) et (c) découle directement de (a). Soit G un groupe et $\{H_i \mid i \in I\}$ une collection de sous-groupes de G indexée par un ensemble I. On montre que $H = \bigcap_{i\in I} H_i$ est un sous-groupe de G. Soit $h, k \in H$. Alors $h, k \in H_i$ pour tout $i \in I$. Comme chaque H_i est un sous-groupe, alors $h^{-1} \in H_i$ et $hk \in H_i$ pour tout $i \in I$. Ainsi $h^{-1} \in H$ et $hk \in H$, ce qui montre que H est bien un sous-groupe.

On trouve un contre-exemple pour les affirmations (b) et (d). On considère le groupe $\mathbb{Z}$ avec l'addition. Alors $2\mathbb{Z}$ et $3\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$ (vérifiez!). Or $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous-groupe, car $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, mais $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

Exercice 6. Déterminer si chacun des sous-ensembles suivants est un sous-groupe.

(a) munis de l'addition, $\mathbb{N} \subset \mathbb{Z}$, $\mathbb{Z} \subset \mathbb{Q}$, $\mathbb{Q} \subset \mathbb{R}$ et $\mathbb{R}_+ \subset \mathbb{R}$, où $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x \geq 0\}$;

(b) munis de la multiplication, $\mathbb{Z}^* \subset \mathbb{Q}^*$, $\mathbb{Q}^* \subset \mathbb{R}^*$ et $\mathbb{R}^*_+ \subset \mathbb{R}^*$, où $\mathbb{R}^*_+ = \{x \in \mathbb{R} \mid x > 0\}$;

(c) le sous-ensemble $\mu_n = \{z \in \mathbb{C} \mid z^n = 1\} \subset S^1$ des racines $n^{\text{ème}}$ de l'unité, muni de la multiplication;

(d) le sous-ensemble $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det(A) = 1\} \subset GL_n(\mathbb{R})$ muni de la multiplication matricielle.

Solution.

(a) Munis de l'addition: $\mathbb{N}$ n'est pas un sous-groupe de $\mathbb{Z}$, car par exemple -2 est l'inverse de $2 \in \mathbb{N}$ mais n'appartient pas à $\mathbb{N}$. $\mathbb{Z}$ est bien un sous-groupe de $\mathbb{Q}$, car l'inverse d'un élément $n \in \mathbb{Z}$ est $-n \in \mathbb{Z}$ et la multiplication de deux entiers reste entière. $\mathbb{Q}$ est bien un sous-groupe de $\mathbb{R}$, car l'inverse d'un élément $q \in \mathbb{Q}$ est $-q \in \mathbb{Q}$ et $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \in \mathbb{Q}$, pour tous $a, b, c, d \in \mathbb{Z}$. $\mathbb{R}_+$ n'est pas un sous-groupe de $\mathbb{R}$, car par exemple $-\pi$ est l'inverse de $\pi \in \mathbb{R}_+$ mais n'appartient pas à $\mathbb{R}_+$.

(b) Munis de la multiplication: $\mathbb{Z}$ n'est pas un sous-groupe de $\mathbb{Q}$, car par exemple $\frac{1}{2}$ est l'inverse de $2 \in \mathbb{Z}$ mais n'appartient pas à $\mathbb{Z}$. $\mathbb{Q}^*$ est bien un sous-groupe de $\mathbb{R}^*$, car l'inverse d'un élément $\frac{a}{b} \in \mathbb{Q}$, où $a, b \in \mathbb{Z}$, est $\frac{b}{a} \in \mathbb{Q}$ et $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in \mathbb{Q}$, pour tous $a, b, c, d \in \mathbb{Z}$. $\mathbb{R}^*_+$ est bien un sous-groupe de $\mathbb{R}^*$, car l'inverse d'un élément $r \in \mathbb{R}^*_+$ est $\frac{1}{r} \in \mathbb{R}^*_+$ et la multiplication de réels strictement positifs reste strictement positive.

(c) μ_n est bien un sous-groupe de S^1. En effet, si $z \in \mu^n$, alors $\bar{z}^n = \bar{z}^n z^n = (\bar{z}z)^n = 1^n = 1$. Donc $z^{-1} = \bar{z} \in \mu_n$. De plus, si $z, w \in \mu_n$, alors $(zw)^n = z^n w^n = 1$ et $zw \in \mu_n$.

(d) $SL_n(\mathbb{R})$ est bien un sous-groupe de $GL_n(\mathbb{R})$. Si $A \in SL_n(\mathbb{R})$, $\det(A^{-1}) = (\det(A))^{-1} = 1$ et $A^{-1} \in SL_n(\mathbb{R})$. Et, si $A, B \in SL_n(\mathbb{R})$, $\det(AB) = \det(A)\det(B) = 1$ et $AB \in SL_n(\mathbb{R})$.

Homomorphismes de groupes

Exercice 7. Soit $f\colon (G,\cdot,e) \to (H,*,e')$ un homomorphisme de groupe. Montrer que:

(a) $f(e) = e'$,

(b) si $g \in G$, alors $f(g^{-1}) = f(g)^{-1}$,

(c) si f est bijectif, alors son inverse $f^{-1}\colon H \to G$ est aussi un isomorphisme de groupes.

Solution.

(a) On a que $f(e) * f(e) = f(e \cdot e) = f(e)$. Par l'Exercice 1 (e), on obtient $f(e) = e'$.

(b) Pour $g \in G$, on a que $f(g) * f(g^{-1}) = f(g \cdot g^{-1}) = f(e) = e'$. Par unicité de l'inverse (Exercice 1 (c)), on obtient $f(g^{-1}) = f(g)^{-1}$.

(c) On montre que, pour tous $h, h' \in H$, $f^{-1}(h * h') = f^{-1}(h) \cdot f^{-1}(h')$. Soit $g, g' \in G$ tels que $f(g) = h$ et $f(g') = h'$. Alors

$$f^{-1}(h * h') = f^{-1}(f(g) * f(g')) = f^{-1}(f(g \cdot g')) = g \cdot g' = f^{-1}(h) \cdot f^{-1}(h').$$

Donc f^{-1} est aussi un homomorphisme de groupes.

Exercice 8. Soit $f\colon (G,\cdot,e) \to (H,*,e')$ un homomorphisme de groupe. Vérifier ou réfuter les affirmations suivantes.

(a) Le noyau de f est un sous-groupe de G.

(b) L'image de f est un sous-groupe de H.

(c) La préimage $f^{-1}(K)$ d'un sous-groupe $K \subset H$ est un sous-groupe de G.

(d) L'image $f(L)$ d'un sous-groupe $L \subset G$ est un sous-groupe de H.

Solution.

(a) VRAI. On rappelle que $\mathrm{Ker}(f) = \{x \in G \mid f(x) = e'\}$. Soit $x, y \in \mathrm{Ker}(f)$. Alors $f(x^{-1}) = f(x)^{-1} = e'$ et $f(x \cdot y) = f(x) * f(y) = e' * e' = e'$. Donc x^{-1} et $x \cdot y$ appartiennent bien à $\mathrm{Ker}(f)$.

(b) VRAI. Soit $a, b \in \mathrm{Im}(f)$. Alors il existe $x, y \in G$ tels que $f(x) = a$ et $f(y) = b$. On a que $a^{-1} = f(x)^{-1} = f(x^{-1}) \in \mathrm{Im}(f)$ et $a * b = f(x) * f(y) = f(x \cdot y) \in \mathrm{Im}(f)$.

(c) VRAI. Soit $x, y \in f^{-1}(K)$. Alors $f(x^{-1}) = f(x)^{-1} \in K$ et $f(x \cdot y) = f(x) * f(y) \in K$ puisque K est un sous-groupe de H et $f(x), f(y) \in K$. Donc x^{-1} et $x \cdot y$ appartiennent bien à $f^{-1}(K)$.

(d) VRAI. Soit $a, b \in f(L)$. Alors il existe $x, y \in L$ tels que $f(x) = a$ et $f(y) = b$. On a que $a^{-1} = f(x)^{-1} = f(x^{-1}) \in f(L)$ et $a * b = f(x) * f(y) = f(x \cdot y) \in f(L)$ puisque L est un sous-groupe de G.

Exercice 9. Vérifier si les applications suivantes sont des homomorphismes de groupes. Si tel est le cas, calculer leur noyau et leur image.

(a) l'application $f\colon \mathbb{Z} \to \mathbb{Z},\ k \mapsto n \cdot k$, où $\mathbb{Z}$ est muni de l'addition et $n \in \mathbb{N}$ est fixé;

(b) l'inclusion $f\colon \{0,1\} \to \mathbb{Z}$, où $\mathbb{Z}$ est muni de l'addition et $\{0,1\}$ est tel que 0 est l'élément neutre et $1+1=0$;

(c) l'application $f\colon \mathbb{Z} \to \{0,1\}$ qui envoie un nombre pair sur 0 et un nombre impair sur 1, où $\mathbb{Z}$ et $\{0,1\}$ sont définis comme ci-dessus;

(d) l'application $f_r\colon \mathbb{R} \to S^1,\ x \mapsto \exp(irx)$, où $\mathbb{R}$ est muni de l'addition, S^1 est muni de la multiplication et $r \in \mathbb{R}$ est fixé;

(e) l'application $\exp\colon \mathbb{R} \to \mathbb{R}^*,\ x \mapsto \exp(x)$, où $\mathbb{R}$ est muni de l'addition et $\mathbb{R}^*$ de la multiplication;

(f) l'application $\exp\colon \mathbb{C} \to \mathbb{C}^*,\ z \mapsto \exp(z)$, où $\mathbb{C}$ est muni de l'addition et $\mathbb{C}^*$ de la multiplication;

(g) l'application $\gamma_x\colon G \to G,\ g \mapsto x \cdot g \cdot x^{-1}$, où G est un groupe et $x \in G$ est fixé.

Solution.

(a) Pour $k, l \in \mathbb{Z}$, on a $f(k+l) = n \cdot (k+l) = n \cdot k + n \cdot l = f(k) + f(l)$. Donc f est bien un homéomorphisme. Le noyau est $\{0\}$ et l'image $n\mathbb{Z} = \{n \cdot k \mid k \in \mathbb{Z}\}$. En particulier, par l'Exercice 8, on remarque que $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ pour tout $n \in \mathbb{N}$.

(b) L'application f n'est pas un homomorphisme de groupe, car $0 = f(0) = f(1+1) \neq f(1) + f(1) = 1 + 1 = 2$.

(c) Soit $n, m \in \mathbb{Z}$. On considère différents cas.

- si n et m sont pairs, alors $n+m$ est pair et $f(n+m) = 0 = 0 + 0 = f(n) + f(m)$;
- si n est pair et m est impair, alors $n+m$ est impair et $f(n+m) = 1 = 0 + 1 = f(n) + f(m)$;
- si n et m sont impairs, alors $n+m$ est pair et $f(n+m) = 0 = 1 + 1 = f(n) + f(m)$.

Donc f est bien un homéomorphisme. Son noyau se constitue de tous les entiers pairs, i.e. son noyau est $2\mathbb{Z}$. Son image est $\{0,1\}$.

(d) Pour $x, y \in \mathbb{R}$, on a $f_r(x+y) = \exp(ir(x+y)) = \exp(irx + iry) = \exp(irx)\exp(iry) = f_r(x)f_r(y)$. Donc f_r est bien un homéomorphisme. Son noyau est $\{\frac{2\pi}{r} \cdot n \mid n \in \mathbb{Z}\}$ et l'application est surjective.

(e) Pour $x, y \in \mathbb{R}$, on a $\exp(x+y) = \exp(x)\exp(y)$, donc exp est bien un homomorphisme. Son noyau est nul et l'application est surjective. En particulier, c'est un isomorphisme de groupe.

(f) Pour $x, y \in \mathbb{C}$, on a $\exp(x+y) = \exp(x)\exp(y)$, donc exp est bien un homomorphisme. Son noyau est $\{2\pi i n \mid n \in \mathbb{Z}\}$ et l'application est surjective. Remarquez que ce n'est pas un isomorphisme de groupe!

(g) Pour $g, h \in G$, on a que $\gamma_x(g \cdot h) = x \cdot g \cdot h \cdot x^{-1} = x \cdot g \cdot x^{-1} \cdot x \cdot h \cdot x^{-1} = \gamma_x(g) \cdot \gamma_x(h)$. Donc γ_x est bien un homomorphisme. C'est un isomorphisme d'inverse $\gamma_{x^{-1}}$.

Exercice 10 (A rendre). Soit G un groupe.

(a) Montrer que G est abélien si et seulement si l'application $f\colon G \to G,\ g \mapsto g^{-1}$ est un homomorphisme de groupes.

(b) Supposons que G soit fini. Soit $f\colon G \to G$ un isomorphisme tel que

(i) si $f(g) = g$, alors $g = e$, et

(ii) $f \circ f$ est l'identité sur G.

Montrer que G est abélien.

Astuce: remarquez que tous les éléments de G sont de la forme $g^{-1} \cdot f(g)$.

Solution.

(a) On observe que, pour tout groupe G et pour tous $g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$. Si G est abélien, alors pour $g, h \in G$

$$f(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1} = f(g)f(h).$$

Donc f est bien un homomorphisme. Réciproquement, si f est un homomorphisme, alors pour tous $g, h \in G$,

$$gh = f(g^{-1})f(h^{-1}) = f(g^{-1}h^{-1}) = (g^{-1}h^{-1})^{-1} = hg.$$

Donc G est abélien.

(b) On montre que l'application $G \to G, g \mapsto g^{-1} \cdot f(g)$ est bijective. Comme G est fini, il suffit de montrer l'injectivité. Soit $g, h \in G$ tels que $g^{-1} \cdot f(g) = h^{-1} \cdot f(h)$. Alors

$$f(g{\cdot}h^{-1}) = f(g){\cdot}f(h^{-1}) = f(g){\cdot}f(h)^{-1} = g{\cdot}g^{-1}f(g){\cdot}f(h)^{-1} = g{\cdot}h^{-1}{\cdot}f(h){\cdot}f(h)^{-1} = g{\cdot}h^{-1}.$$

Par (i), on a donc $g \cdot h^{-1} = e$, i.e. $g = h$, ce qui prouve l'injectivité. Ainsi tout élément de $x \in G$ est de la forme $x = g^{-1} \cdot f(g)$. On a donc

$$f(x) = f(g^{-1} \cdot f(g)) = f(g)^{-1} \cdot f(f(g)) = f(g)^{-1} \cdot g = (g^{-1} \cdot f(g))^{-1} = x^{-1}.$$

Comme f est un homomorphisme par hypothèse, on conclut par (a).

Exercice 11. On pose

$$G = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \;\middle|\; x, y \in \mathbb{R},\ x^2 + y^2 \neq 0 \right\}.$$

Montrer que G est un groupe muni de la muliplication matricielle. Construire un isomorphisme entre G et $\mathbb{C}^*$ (muni de la multiplication).

Solution. On montre que G est un sous-groupe de $GL_2(\mathbb{R})$, ce qui prouve que G est bien un groupe. Soit

$$A = \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \in G.$$

Alors $\det(A) = x^2 + y^2 \neq 0$, par hypothèse. Donc $G \subset GL_2(\mathbb{R})$. Soit $x, y, z, t \in \mathbb{R}$ tels que $x^2 + y^2 \neq 0$ et $z^2 + t^2 \neq 0$. Alors on calcule

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \begin{pmatrix} z & t \\ -t & z \end{pmatrix} = \begin{pmatrix} xz - yt & xt + yz \\ -xt - yz & xz - yt \end{pmatrix}$$

avec $(xz - yt)^2 + (xt + yz)^2 = (x^2 + y^2)(z^2 + t^2) \neq 0$. Donc la multiplication de deux éléments de G reste dans G. De plus, l'inverse d'un élément est donné par

$$A = \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \in G; \quad A^{-1} = \frac{1}{x^2 + y^2} \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$$

avec $\det(A^{-1}) = \frac{1}{x^2+y^2} \neq 0$, d'où $A^{-1} \in G$. Donc G est bien un groupe muni de la multiplication matricielle.

On construit une application

$$f \colon G \to \mathbb{C}^*, \quad \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \mapsto x + iy.$$

Clairement, f est bijective. On montre que c'est un homomorphisme de groupe. On a

$$\begin{aligned} f\left(\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \begin{pmatrix} z & t \\ -t & z \end{pmatrix}\right) &= f\left(\begin{pmatrix} xz - yt & xt + yz \\ -xt - yz & xz - yt \end{pmatrix}\right) = (xz - yt) + i(xt + yz) \\ &= (x + iy)(z + it) = f\left(\begin{pmatrix} x & y \\ -y & x \end{pmatrix}\right) f\left(\begin{pmatrix} z & t \\ -t & z \end{pmatrix}\right). \end{aligned}$$

On a donc un isomorphisme de groupes entre G et $\mathbb{C}^*$.