

Eléments de théorie des groupes  
Résolutions des exercices

Enoncés de Josette Calais.  
Résolutions de Oestromemes abonnez vous

---

# Table des matières

---

1	Structure de groupe	2
2	Classes modulo un sous-groupe	21

# STRUCTURE DE GROUPE

1) Soit  $\mathbb{Z}$  l'ensemble des entiers rationnels, muni de la loi de composition interne notée  $*$ , définie par :

$$\begin{aligned} * : \mathbb{Z} \times \mathbb{Z} &\rightarrow \mathbb{Z}, \\ (a, b) &\mapsto a - b. \end{aligned}$$

- a) La loi  $*$  est-elle associative ? commutative ?  
 b) Vérifier qu'il existe dans  $(\mathbb{Z}, *)$  un élément neutre à droite, c'est-à-dire un élément  $e$  tel que

$$\forall a \in \mathbb{Z}, a * e = a.$$

$e$  est-il neutre dans  $(\mathbb{Z}, *)$  ?

- c) Existe-t-il, pour tout  $a \in \mathbb{Z}$ , un symétrique à droite relativement à  $e$ , c'est-à-dire un élément  $a'$  tel que  $a * a' = e$

- 
- a)  $\forall a, b, c \in \mathbb{Z}, (a * b) * c = a - b - c$ , et  $a * (b * c) = a - b + c$ , la loi n'est pas associative car par exemple on a  $(0 * 0) * 1 = -1 \neq 1 = 0 * (0 * 1)$ . Et  $2 * 1 = 1 \neq -1 = 1 * 2$  montre qu'elle n'est pas non plus commutative.  
 b) On vérifie que 0 est un neutre à droite pour  $*$  :  $\forall a \in \mathbb{Z}, a * 0 = a - 0 = a$ . Il n'est cependant pas un neutre pour  $*$ , car  $0 * a = -a \neq a$ , car on a par exemple  $0 * 1 = -1 \neq 1$ .  
 c)  $\forall a \in \mathbb{Z}, a * a' = e \Rightarrow a = a'$ . Pour tout élément  $a \in \mathbb{Z}$ ,  $a$  est son propre inverse à droite.

2) Soit  $\mathbb{Q}$  l'ensemble des nombres rationnels muni de la loi de composition interne notée  $*$  définie par :

$$\begin{aligned} * : \mathbb{Q} \times \mathbb{Q} &\rightarrow \mathbb{Q}, \\ (a, b) &\mapsto a + b + ab. \end{aligned}$$

$(\mathbb{Q}, *)$  est-il un groupe ?

---

La loi  $*$  admet 0 comme élément neutre, en effet,  $\forall a \in \mathbb{Q}, a * 0 = 0 * a = a$ . Cependant,  $-1$  n'est pas symétrisable par cette loi, car on a  $\forall a \in \mathbb{Q} a * -1 = a - 1 - a = -1 \neq 0$ , donc  $(\mathbb{Q}, *)$  n'est pas un groupe.

---

3) Soit  $G$  un ensemble non vide muni d'une loi de composition interne *associative* notée  $\cdot$  : on suppose que dans  $(G, \cdot)$  les deux conditions suivantes sont vérifiées :

- 1° il existe un élément *neutre à droite*  $e$  (voir exercice 1) ;  
 2° tout élément  $x \in G$  admet un *symétrique à droite*,  $x'$  (voir exercice 1).

Démontrer que  $(G, \cdot)$  est un groupe ; vérifier, par un contre exemple, que, sans l'associativité de la loi  $\cdot$ , ce résultat n'est plus vrai.

---

Montrons que le symétrique à droite de tout élément  $a$  de  $G$  est aussi son symétrique à gauche.

$$\begin{aligned} aa' = e &\Rightarrow a'(aa') = a', \\ &\Rightarrow (a'a)a' = a'. \end{aligned}$$

En multipliant des deux cotés par le symétrique à droite de  $a'$ , on obtient :

$$a'a = e.$$

Ainsi, le symétrique à droite de  $a$  est aussi son symétrique à gauche.

Montrons que le neutre à droite de  $G$  est aussi un neutre à gauche, et donc un neutre tout court.

$$\begin{aligned} \forall a \in G, \quad ea &= (aa')a, \\ &= a(a'a), \\ &= a. \end{aligned}$$

Ainsi, le neutre à droite de  $G$  est aussi un neutre à gauche.

$(G, \cdot)$  est donc un groupe.

On a vérifié dans l'exercice 1 que pour  $(\mathbb{Z}, -)$ , la loi n'est pas associative, mais que 0 est un neutre à droite (et non à gauche) et que tout élément est symétrisable.

4) Soit  $G$  un ensemble *fini*, non vide, muni d'une loi de composition interne notée  $\cdot$ ; on suppose que la loi  $\cdot$  est associative et que dans  $(G, \cdot)$  tout élément est simplifiable à droite et à gauche.

Démontrer que  $(G, \cdot)$  est un groupe.

Comme tout les éléments de  $G$  sont simplifiables à droite et à gauche, les applications :

$$\begin{aligned} \tau_g^y : G &\rightarrow G, & \tau_d^y : G &\rightarrow G \\ x &\mapsto yx, & x &\mapsto xy, \end{aligned}$$

Sont injectives. Le cardinal de  $G$  étant fini, ces translations sont bijectives.

Ainsi, pour  $a$  et  $b$  fixé, les équations  $a = xb$  et  $a = bx$  ont chacune une unique solution.

En particulier, pour chaque élément  $a$  de  $G$ , il existe des uniques  $e_d^a$  et  $e_g^a$  tel que  $a = e_d^a a$  et  $a = a e_g^a$ .

Vérifions qu'ils sont égaux :

$$\begin{aligned} \forall a \in G, \quad aa &= aa, \\ a(e_g^a a) &= (a e_d^a) a, \\ a e_g^a a &= a e_d^a a, \\ a e_g^a &= a e_d^a \text{ (Simplification à droite),} \\ e_g^a &= e_d^a \text{ (Simplification à gauche).} \end{aligned}$$

Vérifions maintenant que tout les éléments ont le même neutre :

$$\begin{aligned} \forall a, b \in G, \quad ab &= ab, \\ (a e^a) b &= a(e^b b), \\ a e^a b &= a e^b b, \\ a e^a &= a e^b \text{ (Simplification à droite),} \\ e^a &= e^b \text{ (Simplification à gauche).} \end{aligned}$$

Ainsi, dans  $G$ , il existe un unique élément neutre  $e$ .

Reste à montrer que chaque élément  $a$  admet un unique inverse  $a^{-1}$ .

On sait que les équations  $e = ax$  et  $e = xa$  ont une unique solution chacune, notées respectivement  $a_g^*$  et  $a_d^*$ . Vérifions qu'il est le même des deux cotés, et est donc l'inverse de  $a$ .

$$\begin{aligned} \forall a \in G, \quad a &= a, \\ a(a_g^* a) &= (a a_d^*) a, \\ a a_g^* a &= a a_d^* a, \\ a_g^* &= a_d^* \text{ en simplifiant à droite et à gauche.} \end{aligned}$$

Chaque élément possède un unique inverse, et  $G$  possède un élément neutre pour la loi associative  $\cdot$ . Ainsi,  $(G, \cdot)$  est un groupe.

5) Soit  $G$  un groupe d'élément unité  $e$  vérifiant la condition (C) :

$$\forall x \in G, x^2 = e.$$

- a) Donner au moins un exemple de groupe, non réduit à l'élément unité, vérifiant la condition (C).
- b) Démontrer que tout groupe vérifiant la condition (C) est abélien.

a) Le groupe  $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}, +\right)$  vérifie de façon évidente la condition.

b) la condition (C) implique que chaque élément est son propre inverse, ainsi :

$$\begin{aligned} \forall a, b \in G, \quad (ab)^2 &= e, \\ abab &= e, \\ bab &= a, \\ ab &= ba. \end{aligned}$$

Tout groupe vérifiant la propriété est donc abélien.

6)  $G$  étant un groupe, prouver que l'application  $f: \begin{matrix} G & \rightarrow & G, \\ x & \mapsto & x^{-1}. \end{matrix}$  est une permutation de  $G$  et que  $f$

est un automorphisme si et seulement si  $G$  est abélien.

Chaque élément d'un groupe possède un unique inverse, l'application est donc trivialement bijective.

Supposons que  $G$  soit abélien :

$$\begin{aligned} \forall a, b \in G, \quad f(ab) &= (ab)^{-1}, \\ &= b^{-1}a^{-1}, \\ &= a^{-1}b^{-1}, \\ &= f(a)f(b). \end{aligned}$$

Donc  $G$  abélien  $\Rightarrow f$  est un automorphisme.

Supposons que  $f$  soit un automorphisme :

$$\begin{aligned} \forall a, b \in G, \quad f(ab) &= f(a)f(b) \Rightarrow b^{-1}a^{-1} = a^{-1}b^{-1}, \\ &\Rightarrow ab = ba \text{ en appliquant } f \text{ des deux côtés.} \end{aligned}$$

ainsi,  $f$  est un automorphisme si et seulement si  $G$  est abélien.

7) Montrer que si  $G$  est un groupe fini d'ordre pair, il existe au moins un élément  $x \neq e$ , dans  $G$ , tel que  $x^2 = e$ .

Soit  $G$  d'ordre  $2n$ , définissons la relation d'équivalence :

$$x\mathcal{R}y \Leftrightarrow x = y \text{ ou } x = y^{-1}.$$

Soit  $\{x_i\}_{i \in I}$  une famille de représentants des classes modulo  $\mathcal{R}$ . pour tout  $\bar{x} \in G/\mathcal{R}$  a  $1 \leq |\bar{x}| \leq 2$ . le groupe se partitionne en  $k$  classes d'un élément (correspondant aux éléments qui sont leur propre inverse) et  $l$  classes de deux éléments de la forme  $\{x, x^{-1}\}$ , et on a donc :

$$2n = k + 2l$$

Pour respecter la parité, il faut donc que  $k$  soit pair, et sachant que  $k > 1$ , qu'il existe au moins un élément différent du neutre tel que  $x^2 = e$ .

8) Dans l'ensemble des entiers  $\mathbb{Z}$ , on pose  $U = \{-1, 1\}$ .

a) Vérifier que  $U$  est un groupe relativement à la multiplication des entiers, donc un sous-groupe de  $(\mathbb{Q}^*, \times)$ .

b) Montrer que le groupe  $U$  est isomorphe au groupe  $\left(\frac{\mathbb{Z}}{(2)}, +\right)$ .

a) On a  $U \subset \mathbb{Z}$ . On vérifie aussi que,  $\forall x, y \in U$ ,  $xy \in U$  et  $x^{-1} \in U$ , c'est donc un sous-groupe de  $(\mathbb{Q}^*, \times)$ .

b) On pose l'application :

$$\begin{aligned} \varphi : \frac{\mathbb{Z}}{2\mathbb{Z}} &\rightarrow U, \\ x &\mapsto \begin{cases} 1 & \text{si } x = \bar{0} \\ -1 & \text{si } x = \bar{1} \end{cases}. \end{aligned}$$

On vérifie de façon exhaustive que c'est un morphisme :

$$\begin{aligned} \varphi(\overline{0+0}) &= 1 = 1 \times 1 = \varphi(\bar{0})\varphi(\bar{0}) \\ \varphi(\overline{0+1}) &= -1 = 1 \times -1 = \varphi(\bar{0})\varphi(\bar{1}) \\ \varphi(\overline{1+0}) &= -1 = -1 \times 1 = \varphi(\bar{1})\varphi(\bar{0}) \\ \varphi(\overline{1+1}) &= 1 = -1 \times -1 = \varphi(\bar{1})\varphi(\bar{1}) \end{aligned}$$

Elle est aussi bijective par définition, ainsi,  $U$  est isomorphe à  $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}, +\right)$

9) Soit  $\mathbf{D}$  le sous ensemble de  $\mathbb{Q}$  formé par les nombres décimaux :

$$\mathbf{D} = \left\{ \frac{a}{10^n}; a \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

Prouvez que  $\mathbf{D}$  est un sous-groupe de  $(\mathbb{Q}, +)$ .

De façon évidente,  $\mathbf{D} \subset \mathbb{Q}$ . Soit  $\frac{a}{10^n}, \frac{b}{10^m} \in \mathbf{D}$ ,

$$\frac{a}{10^n} - \frac{b}{10^m} = \frac{10^m a - 10^n b}{10^{n+m}}.$$

On a  $10^m a - 10^n b \in \mathbb{Z}$  car  $a, b \in \mathbb{Z}$ , et  $n + m \in \mathbb{N}$ , donc  $\frac{a}{10^n} - \frac{b}{10^m} \in \mathbf{D}$ , ainsi  $(\mathbf{D}, +)$  est un sous groupe de  $(\mathbb{Q}, +)$

10) Soit, dans  $\mathbb{N}$ , un nombre premier  $p$ . On pose :

$$\mathbb{Q}_p = \left\{ \frac{a}{p^n}; a \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

a) Vérifier que  $\mathbb{Q}_p$  est un sous-groupe de  $(\mathbb{Q}, +)$  et que  $\mathbb{Q}_p = \bigcup_{n \in \mathbb{N}} \langle \frac{1}{p^n} \rangle$ .

b) Montrer que l'application  $\varphi : \mathbb{Q}_p \rightarrow \mathbb{Q}_p$ , est une permutation de  $\mathbb{Q}_p$ . L'application  $\varphi$  est-elle un automorphisme de  $(\mathbb{Q}_p, +)$ ?

a)  $\mathbb{Q}_p \in \mathbb{Q}$ , et soit  $\frac{a}{p^n}, \frac{b}{p^m} \in \mathbb{Q}_p$  :

$$\frac{a}{p^n} - \frac{b}{p^m} = \frac{p^m a - p^n b}{p^{n+m}}.$$

On a  $p^m a - p^n b \in \mathbb{Z}$ , et  $n + m \in \mathbb{N}$ , donc  $\frac{a}{p^n} - \frac{b}{p^m} \in \mathbb{Q}_p$ , ainsi  $(\mathbb{Q}_p, +)$  est un sous groupe de  $(\mathbb{Q}, +)$ . De plus :

$$\bigcup_{n \in \mathbb{N}} \langle \frac{1}{p^n} \rangle = \bigcup_{n \in \mathbb{N}} \left\{ \frac{a}{p^n}; a \in \mathbb{Z} \right\} = \left\{ \frac{a}{p^n}; a \in \mathbb{Z}, n \in \mathbb{N} \right\} = \mathbb{Q}_p.$$

b)  $\varphi$  est clairement injective. De plus, comme  $\frac{a}{p^n} = p \frac{a}{p^{n+1}}$ , on en déduit que  $\varphi$  est surjective, donc que c'est une permutation.

$$\begin{aligned} \forall x, y \in \mathbb{Q}_p, \quad \varphi(x + y) &= p(x + y), \\ &= px + py, \\ &= \varphi(x) + \varphi(y). \end{aligned}$$

ce qui prouve que  $\varphi$  est un morphisme, et donc un automorphisme.

**11)** Soit  $p$  un nombre premier dans  $\mathbb{N}$ . Vérifier les propriétés suivantes :

- $\{a + b\sqrt{p}; (a, b) \in \mathbb{Z} \times \mathbb{Z}\} < (\mathbb{R}, +)$
- $\{a + b\sqrt{p}; a \text{ et } b \text{ dans } \mathbb{Q} \text{ et non simultanément nuls}\} < (\mathbb{R}^*, \times)$
- $\{a + ib\sqrt{p}; (a, b) \in \mathbb{Z} \times \mathbb{Z}\} < (\mathbb{C}, +)$
- $\{a + ib\sqrt{p}; a \text{ et } b \text{ dans } \mathbb{Q} \text{ et non simultanément nuls}\} < (\mathbb{C}^*, \times)$

On note que si  $p$  n'est pas un carré parfait,  $\sqrt{p}$  est irrationnel, chaque élément du groupe s'écrit de façon unique et tout se passe nickel.

Posons  $G = \{a + b\sqrt{p}; (a, b) \in \mathbb{Z} \times \mathbb{Z}\}$

De façon évidente,  $G \subset \mathbb{R}$ . Soit  $a + b\sqrt{p}, a' + b'\sqrt{p} \in G$  :

$$a + b\sqrt{p} - (a' + b'\sqrt{p}) = (a - a') + (b - b')\sqrt{p} \in G$$

Et idem pour les 3 autres flemmes.

**12)** On pose :

$$\Gamma_\infty = \{z \in \mathbb{C}; \exists n \in \mathbb{N}, z^n = 1\}.$$

Vérifier que  $\Gamma_\infty$  est un sous-groupe de  $(\mathbb{C}^*, \times)$ .

$\Gamma_\infty \subset \mathbb{C}$ , soit  $z_1, z_2 \in \Gamma_\infty$ , il existe  $n_1, n_2 \in \mathbb{N}$  tel que  $z_1^{n_1} = z_2^{n_2} = 1$ .

On constate que  $(z_1 z_2^{-1})^{n_1 n_2} = (z_1^{n_1})^{n_2} (z_2^{n_2})^{-n_1} = 1$ , et donc  $z_1 (z_2)^{-1} \in \Gamma_\infty$ , donc  $\Gamma_\infty$  est un sous-groupe de  $(\mathbb{C}^*, \times)$ .

**13)** A tout nombre réel  $a$  on associe l'application

$$\begin{aligned} \tau_a : \mathbb{R} &\rightarrow \mathbb{R}, \\ x &\mapsto a + x. \end{aligned}$$

Justifier la propriété :

$T = \{\tau_a; a \in \mathbb{R}\}$  est un sous-groupe du groupe symétrique  $S_{\mathbb{R}}$  et le groupe  $T$  est isomorphe au groupe  $(\mathbb{R}, +)$ .

Lemme (1.77)

**14)** On considère les groupes multiplicatifs  $\mathbb{R}^*$ ,  $\mathbb{R}_+^*$  et  $\mathbb{C}^*$  (voir exemple (1.29)) et les applications :

$$f: \mathbb{R}^* \rightarrow \mathbb{R}_+^*, \quad \text{où } |x| \text{ est la valeur absolue de } x.$$

$$x \mapsto |x|.$$

et  $g: \mathbb{C}^* \rightarrow \mathbb{R}_+^*$ , où  $|z|$  est le module de  $z$ .

$$z \mapsto |z|.$$

Vérifier que  $f$  et  $g$  sont des épimorphismes de groupes.

Déterminer les noyaux de  $f$  et  $g$ .

Soit  $x$  un élément de  $\mathbb{R}_+^*$ , on a  $f(x) = x$ , donc  $f$  est surjective, vérifions que c'est un morphisme :

$$\begin{aligned} \forall x, y \in \mathbb{R}, \quad f(xy) &= |xy|, \\ &= |x||y|, \\ &= f(x)f(y). \end{aligned}$$

C'est donc un épimorphisme de groupe, déterminons son noyau :

$$\begin{aligned} \text{Ker } f &= \{x \in \mathbb{R}^*, f(x) = 1\}, \\ &= \{x \in \mathbb{R}^*, |x| = 1\}, \\ &= \{-1, 1\}. \end{aligned}$$

Soit  $x$  un élément de  $\mathbb{R}_+^*$ , on a  $g(x) = x$ , donc  $g$  est surjective, vérifions que c'est un morphisme :

$$\begin{aligned} \forall x, y \in \mathbb{R}, \quad g(xy) &= |xy|, \\ &= |x||y|, \\ &= g(x)g(y). \end{aligned}$$

C'est donc un épimorphisme de groupe, déterminons son noyau :

$$\begin{aligned} \text{Ker } g &= \{x \in \mathbb{C}^*, f(x) = 1\}, \\ &= \{x \in \mathbb{C}^*, |x| = 1\}, \\ &= \mathbb{U}. \end{aligned}$$

**15)** Démontrer que l'application  $\lambda: \mathbb{R} \rightarrow \mathbb{R}_+^*$ , est un isomorphisme du groupe  $(\mathbb{R}, +)$  sur le groupe

$$x \mapsto 10^x.$$

$(\mathbb{R}_+^*, \times)$ .

Vérifions que c'est une morphisme :

$$\begin{aligned} \forall a, b \in \mathbb{R}, \quad \lambda(a+b) &= 10^{a+b}, \\ &= 10^a 10^b, \\ &= \lambda(a)\lambda(b). \end{aligned}$$

L'injectivité :

$$x \in \text{Ker } \lambda \Rightarrow 10^x = 1 \Rightarrow x = 0.$$

La surjectivité :

$$\forall y \in \mathbb{R}_+^*, \quad \lambda(\log_{10} y) = y.$$

Donc  $\lambda$  est une isomorphisme de groupe.



**16)**

a) Le centre d'un groupe  $G$  étant désigné par  $Z(G)$ , démontrer la propriété :

$$H \leq G \Rightarrow Z(G) \cap H \leq Z(H)$$

b)  $G$  et  $G'$  étant deux groupes, si  $f$  est un épimorphisme de  $G$  sur  $G'$ , prouver que l'on a :  $f(Z(G)) \leq Z(G')$

a) Un élément de  $H$  qui commute avec tout les éléments de  $G$  commute aussi avec tout les éléments de  $H$ , d'où  $Z(G) \cap H \subset Z(H)$ . De plus, l'intersection de sous-groupes est un sous-groupe, donc  $Z(G) \cap H \leq Z(H)$ .

b) Soit  $y \in f(Z(G))$ , il existe  $x \in Z(G)$  tel que  $y = f(x)$ .  $f$  étant surjective, pour tout  $z \in G'$ , il existe  $w \in G$  tel que  $z = f(w)$ . On a donc :

$$yz = f(x)f(w) = f(xw) = f(wx) = f(w)f(x) = zy.$$

D'où  $y \in Z(G')$ , et comme  $f(Z(G))$  est un sous-groupe de  $G'$  inclus dans  $Z(G')$ , on a bien  $f(Z(G)) \leq Z(G')$ .

**17)** Soit  $S$  une partie non vide d'un groupe  $G$ ; on pose :

$$C_G(S) = \{g \in G; gx = xg, \forall x \in S\}.$$

a) Vérifier que  $C_G(S)$  est un sous-groupe de  $G$ .

$C_G(S)$  est appelé le *centralisateur* de  $S$  dans  $G$ . Si  $S = \{x\}$ , on le note  $C_G(x)$  et on l'appelle le *centralisateur* de  $x$  dans  $G$ .

b)  $Z(G)$  étant le centre de  $G$ , démontrer la relation :  $\bigcap_{x \in G} C_G(x) = Z(G)$

c) Pour  $x \in G$ , posons  $H = C_G(x)$ ; Vérifier que  $x \in Z(H)$ .

a) Soit  $h, g \in C_G(S)$ , pour tout  $x \in S$ , on a :

$$(hg^{-1})x = hxg^{-1} = xhg^{-1}.$$

Donc  $\forall h, g \in C_G(S)$ ,  $hg^{-1} \in C_G(S)$ , c'est donc bien un sous-groupe de  $G$ .

b)

$$g \in Z(G) \Leftrightarrow \forall x \in G, gx = xg \Leftrightarrow \forall x \in G, g \in C_G(x) \Leftrightarrow g \in \bigcap_{x \in G} C_G(x)$$

c)

$$H = C_G(x) \Leftrightarrow \forall h \in H, hx = xh \Leftrightarrow x \in Z(H).$$

**18)** Soit  $A, B, C$  trois parties non vides d'un groupe  $G$ .

Soit  $H = \langle A, B \rangle$  le sous-groupe de  $G$  engendré par  $A \cup B$ .

Si  $K = \langle A, B, C \rangle$  est le sous-groupe de  $G$  engendré par  $A \cup B \cup C$ , démontrer que  $K = \langle H, C \rangle$ .

(j'ai repris la demo d'un mec, qui est pas complete je crois, la mienne a environ 200 indices avec des sommes donc chiant a taper)

Soit  $\mathcal{H}_S$  l'ensemble des sous groupe de  $G$  contenant  $S$ . Par définition,

$$H = \bigcap_{L \in \mathcal{H}_{A \cup B}} L, \quad K = \bigcap_{L \in \mathcal{H}_{A \cup B \cup C}} L.$$

Montrons que  $\mathcal{H}_{A \cup B \cup C} = \mathcal{H}_{H \cup C}$

Soit  $L \in \mathcal{H}_{A \cup B \cup C}$ , comme  $A \cup B \subset L$ , on a  $L \in \mathcal{H}_{A \cup B}$ , et donc  $L \in \mathcal{H}_{H \cup C}$ .

De façon réciproque, soit  $L \in \mathcal{H}_{H \cup C}$ , on a  $A \cup B \subset H \subset L$ , donc  $L \in \mathcal{H}_{A \cup B \cup C}$ .

Ainsi, on a  $\mathcal{H}_{A \cup B \cup C} = \mathcal{H}_{H \cup C}$ , et donc que  $K = \langle H, C \rangle$ .

**19)** Démontrer que le groupe des quaternions (exemple (1.16)) est engendré par les matrices :

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Soit le groupe des quaternions :

$$\left\{ \begin{array}{l} q_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, q_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, q_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, q_4 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \\ q_5 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, q_6 = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, q_7 = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, q_8 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \end{array} \right\}$$

On peut exprimer tout les  $q_i$  en fonction de  $A, B$  :

- $q_1 = A^0$
- $q_2 = A^2 = B^2$
- $q_3 = A$
- $q_4 = q_2 A = A^3$
- $q_5 = B$
- $q_6 = q_2 B = B^3$
- $q_7 = BA$
- $q_8 = B^3 A$

**20)** Dans l'ensemble  $M_2(\mathbb{R})$  des matrices carrées d'ordre 2 sur  $\mathbb{R}$ , on considère le sous-ensemble  $\Gamma$  tel que :

$$\Gamma = \left\{ \begin{pmatrix} x & x \\ 0 & 0 \end{pmatrix} : x \in \mathbb{R}^* \right\}.$$

Démontrer que  $\Gamma$  est un groupe par rapport à la multiplication des matrices, mais que ce groupe n'est pas un sous-groupe de  $GL_2(\mathbb{R})$ .

Vérifier que le groupe  $\Gamma$  est isomorphe au groupe  $(\mathbb{R}^*, \times)$ .

Soit  $\begin{pmatrix} x & x \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} y & y \\ 0 & 0 \end{pmatrix} \in \Gamma$  :

$$\begin{pmatrix} x & x \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} y & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} xy & xy \\ 0 & 0 \end{pmatrix} \in \Gamma.$$

De plus, pour tout  $\begin{pmatrix} x & x \\ 0 & 0 \end{pmatrix} \in \Gamma$ , son inverse  $\begin{pmatrix} 1/x & 1/x \\ 0 & 0 \end{pmatrix} \in \Gamma$ , et  $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$  est le neutre pour la multiplication des matrices dans cet ensemble.

On sait la loi associative, ainsi,  $\Gamma$  est un groupe pour la multiplication des matrices.

Ce n'est cependant pas un sous-groupe de  $GL_2(\mathbb{R})$ , car elles ne sont pas inversibles, ayant toutes un déterminant nul.

On vérifie directement que  $\varphi : \mathbb{R}^* \rightarrow \Gamma$ , est un isomorphisme de groupe.

$$x \mapsto \begin{pmatrix} x & x \\ 0 & 0 \end{pmatrix}.$$

**21)** Soit  $n > 1$  dans  $\mathbb{N}$  et  $\left(\frac{\mathbb{Z}}{(n)}, +\right)$  le groupe des classes de congruence modulo  $n$ . On considère la correspondance  $\mu$  définie par :

$$\begin{aligned} \mu : \frac{\mathbb{Z}}{(n)} \times \frac{\mathbb{Z}}{(n)} &\rightarrow \frac{\mathbb{Z}}{(n)}, \\ (\bar{x}, \bar{y}) &\mapsto \overline{xy}. \end{aligned}$$

- a) Prouver que la correspondance  $\mu$  est une application [c'est-à-dire que :  $(\overline{x'} = \overline{x}$  et  $\overline{y'} = \overline{y} \Rightarrow \overline{x'y'} = \overline{xy})$ ].  
En déduire que l'on peut définir dans  $\frac{\mathbb{Z}}{(n)}$  une multiplication telle que  $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$ .  
Montrer alors que  $\frac{\mathbb{Z}}{(n)}$  est un anneau unitaire. et commutatif.
- b) Soit, dans  $\mathbb{N}$ , un nombre premier  $p$ . On désigne par  $G_p$  l'ensemble des éléments non nuls de  $\frac{\mathbb{Z}}{(p)}$ .  
Prouver, en utilisant le résultat de l'exercice 4, que  $G_p$  est un groupe par rapport à la multiplication définie dans  $\frac{\mathbb{Z}}{(p)}$ .  
En conclure que  $\frac{\mathbb{Z}}{(p)}$  est un corps.
- c) Vérifier que si  $n$  n'est pas premier  $\frac{\mathbb{Z}}{(p)}$  n'est pas un corps.

- a) Soit  $x, y, x', y' \in \mathbb{Z}$  tel que  $\overline{x} = \overline{x'}$  et  $\overline{y} = \overline{y'}$ . On rappelle que :

$$\begin{aligned}\overline{x} = \overline{x'} &\Leftrightarrow \exists k \in \mathbb{Z}, x = x' + kn, \\ \overline{y} = \overline{y'} &\Leftrightarrow \exists k' \in \mathbb{Z}, y = y' + k'n.\end{aligned}$$

Ainsi :

$$\begin{aligned}\overline{xy} &= \overline{(x' + kn)(y' + k'n)}, \\ &= \overline{x'y' + x'k'n + y'kn + kk'n^2}, \\ &= \overline{x'y' + n(x'k' + y'k + kk'n)}, \\ &= \overline{x'y'}.\end{aligned}$$

la multiplication ainsi définie est associative, commutative, de neutre  $\overline{1}$ , et est distributive par rapport à l'addition.  $\frac{\mathbb{Z}}{n\mathbb{Z}}$  est donc un anneau unitaire commutatif.

- b) L'ensemble  $G_p$  est fini, est dans le a) on a montré que la loi de multiplication associée est associative. Montrons que chaque élément est simplifiable à droite et à gauche. Soit  $\overline{a}, \overline{x}, \overline{y} \in G_p$  tel que  $\overline{ax} = \overline{ay}$ . On a  $\overline{ax} = \overline{ay}$ , autrement dit, que  $ax - ay = a(x - y)$  est un multiple de  $p$ . Comme  $p$  est un nombre premier ne divisant pas  $a$  par hypothèse,  $x - y$  est un multiple de  $p$  d'après le lemme d'Euclide, et donc  $\overline{x} = \overline{y}$ . Par commutativité, tout les éléments sont simplifiable à droite et à gauche. D'après l'exo 4,  $G_p$  est un groupe.  
De plus, tout élément non nul de  $\frac{\mathbb{Z}}{p\mathbb{Z}}$  est inversible, donc c'est un corps.

- c) Chapitre 3.

**22)** Vérifier que

$$\Gamma = \left\{ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \gamma_1 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \gamma_2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \gamma_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \gamma_4 = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, \gamma_5 = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \right\}$$

est un sous-groupe de  $GL(2, \mathbb{R})$  isomorphe au groupe  $GL\left(2, \frac{\mathbb{Z}}{(2)}\right)$ .

Ecrire la table de multiplication du groupe  $\Gamma$ ; en déduire que  $\Gamma$  est isomorphe au groupe symétrique  $S_3$ .

Toutes les matrices de cet ensemble ont pour déterminant 1, la multiplication des matrices est associative, et  $I \in \Gamma$ . Posons dès maintenant la table de multiplication de  $\Gamma$  :

$\times$	$I$	$\gamma_1$	$\gamma_2$	$\gamma_3$	$\gamma_4$	$\gamma_5$
$I$	$I$	$\gamma_1$	$\gamma_2$	$\gamma_3$	$\gamma_4$	$\gamma_5$
$\gamma_1$	$\gamma_1$	$\gamma_2$	$I$	$\gamma_5$	$\gamma_3$	$\gamma_4$
$\gamma_2$	$\gamma_2$	$I$	$\gamma_1$	$\gamma_4$	$\gamma_5$	$\gamma_3$
$\gamma_3$	$\gamma_3$	$\gamma_4$	$\gamma_5$	$I$	$\gamma_1$	$\gamma_2$
$\gamma_4$	$\gamma_4$	$\gamma_5$	$\gamma_3$	$\gamma_2$	$I$	$\gamma_1$
$\gamma_5$	$\gamma_5$	$\gamma_3$	$\gamma_4$	$\gamma_1$	$\gamma_2$	$I$

On remarque que chaque élément possède un unique inverse.  $\Gamma$  est donc bien un sous-groupe de  $GL(2, \mathbb{R})$ .

On constate que ce groupe se décompose en deux sous-groupes,  $H = \{I, \gamma_1, \gamma_2\}$  et  $K = \{I, \gamma_4\}$ , tel que  $\Gamma = HK$ . D'où l'isomorphisme évident (aka, flemme de rédiger) avec  $GL(2, \frac{\mathbb{Z}}{2\mathbb{Z}})$  et  $S_3$ .

### 23)

a) Démontrer les résultats suivants :

$$\Gamma_1 = \left\{ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \gamma_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \gamma_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \gamma_3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$$

est un sous-groupe de  $GL(2, \mathbb{R})$ .

$$\Gamma_2 = \{1, i, -1, -i\} \text{ où } i^2 = -1,$$

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

$$\Gamma_3 = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

sous-ensemble de  $\frac{\mathbb{Z}}{(5)}$  est un groupe par rapport à la multiplication définie dans  $\frac{\mathbb{Z}}{(5)}$ .

b) Prouver que  $\Gamma_1, \Gamma_2, \Gamma_3$  sont trois groupes isomorphes. Sont-ils cycliques ?

De façon immédiate, on a que  $\Gamma_1 \subset GL(2, \mathbb{R})$ ,  $\Gamma_2 \subset \mathbb{C}^*$  et  $\Gamma_3 \subset \frac{\mathbb{Z}}{5\mathbb{Z}}$ . Ecrivons leur table de Cayley pour vérifier la stabilité et l'existence d'un unique inverse.

$\times$	$I$	$\gamma_1$	$\gamma_2$	$\gamma_3$	$\times$	$1$	$i$	$-1$	$-i$	$\times$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$I$	$I$	$\gamma_1$	$\gamma_2$	$\gamma_3$	$1$	$1$	$i$	$-1$	$-i$	$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\gamma_1$	$\gamma_1$	$\gamma_2$	$\gamma_3$	$I$	$i$	$i$	$-1$	$-i$	$1$	$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\gamma_2$	$\gamma_2$	$\gamma_3$	$I$	$\gamma_1$	$-1$	$-1$	$-i$	$1$	$i$	$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\gamma_3$	$\gamma_3$	$I$	$\gamma_1$	$\gamma_2$	$-i$	$-i$	$1$	$i$	$-1$	$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

On remarque que ce sont tous des groupes cyclique d'ordre 4, avec  $\Gamma_1 = \langle \gamma_1 \rangle$ ,  $\Gamma_2 = \langle i \rangle$  et  $\Gamma_3 = \langle \bar{2} \rangle$ , ils sont donc tous isomorphes entre eux.

### 24)

a) Montrer que :

$$K_1 = \left\{ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

est un sous-groupe de  $GL(2, \mathbb{R})$  et que  $K_2 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ , sous-ensemble de  $\frac{\mathbb{Z}}{(8)}$ , est un groupe par rapport à la multiplication définie dans  $\frac{\mathbb{Z}}{(8)}$ .

b) Vérifier que ces deux groupes sont isomorphes. Ces groupes sont-ils isomorphes au groupe de Klein ?

- a) On sait la multiplication de matrice associative, et que  $I$  est le neutre pour cette opération. Vérifions la fermeture et l'inversibilité :

$\times$	$I$	$A$	$B$	$C$
$I$	$I$	$A$	$B$	$C$
$A$	$A$	$I$	$C$	$B$
$B$	$B$	$C$	$I$	$A$
$C$	$C$	$B$	$A$	$I$

On a bien  $K_1$  est un sous-groupe de  $GL(2, \mathbb{R})$ . Faisons pareil pour  $K_2$ , dont on sait la loi associative :

$\times$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

On vérifie bien que  $K_2$  est un groupe.

- b) Il n'existe à isomorphisme près que 2 groupes d'ordre 4,  $\frac{\mathbb{Z}}{4\mathbb{Z}}$  et  $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ . Comme il n'existe pas d'élément d'ordre 4 dans  $K_1$  ou  $K_2$ , on en déduit qu'ils sont isomorphes entre eux et au groupe de Klein.

## 25)

- a) Montrer que le groupe symétrique  $S_3$ , les groupes  $\Gamma_2$  et  $\Gamma_3$  de l'exercice 23 et le groupe  $K_2$  de l'exercice 24 admettent chacun une représentation matricielle fidèle de degré 2 sur  $\mathbb{R}$ .
- b) En associant à tout nombre complexe non nul  $a+ib$  la matrice  $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ , vérifier que le groupe multiplicatif  $\mathbb{C}^*$  admet aussi une représentation fidèle de degré 2 sur  $\mathbb{R}$ .

- a) On a démontré que  $\Gamma_1 \simeq \Gamma_2 \simeq \Gamma_3$ .  $\Gamma_1$  étant un sous-groupe de  $GL(2, \mathbb{R})$ ,  $\Gamma_2$  et  $\Gamma_3$  admettent un morphisme bijectif pour un sous-groupe  $GL(2, \mathbb{R})$ , qui est aussi un morphisme injectif dans  $GL(2, \mathbb{R})$ . En appliquant le même raisonnement pour  $K_2$  et  $S_3$ , on trouve que ces 4 groupes admettent une représentation matricielle de degré 2 sur  $\mathbb{R}$ .
- b) Posons l'application  $\varphi$  tel que :

$$\varphi : \mathbb{C}^* \rightarrow GL(2, \mathbb{R}),$$

$$a + ib \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Vérifions tout d'abord que toute image est bien dans  $GL(2, \mathbb{R})$  :

$$\forall a + ib \in \mathbb{C}, \det(\varphi(a + ib)) = a^2 + b^2 \neq 0.$$

Vérifions que c'est un morphisme :

$$\begin{aligned} \forall a + ib, c + id \in \mathbb{C}^*, \varphi((a + ib) + (c + id)) &= \varphi((a + c) + i(b + d)), \\ &= \begin{pmatrix} a + c & -(b + d) \\ b + d & a + c \end{pmatrix}, \\ &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix}, \\ &= \varphi(a + ib)\varphi(c + id). \end{aligned}$$

Enfin, vérifions son injectivité :

$$\begin{aligned}\text{Ker } (\varphi) &= \{a + ib \in C^*, \varphi(a + ib) = I_2\}, \\ &= \{a + ib \in C^*, a = 1 \wedge b = 0\}, \\ &= \{1\}.\end{aligned}$$

Ainsi, le groupe multiplicatif  $C^*$  admet une représentation matricielle de degré 2 sur  $\mathbb{R}$ .

**26)** Soit  $P$  le plan affine euclidien. Si  $f$  est une isométrie du plan  $P$ , on dit qu'un point  $A$  est fixe pour  $f$  si  $f(A) = A$ .

On désigne par  $\mathcal{I}(2)$  l'ensemble des isométries du plan  $P$ .

Si  $\Delta$  est une droite de  $P$ , on note  $s_\Delta$  la symétrie du plan par rapport à  $\Delta$ ;  $s_\Delta : \begin{matrix} P & \rightarrow & P, \\ A & \mapsto & A'. \end{matrix}$ ,  $A'$  est tel

que  $\Delta$  est la médiatrice de  $AA'$ .

a) Vérifier les propriétés suivantes :

- L'identité de  $P$ , notée  $id_P$ , appartient à  $\mathcal{I}(2)$ .
- quelle que soit la droite  $\Delta$ ,  $s_\Delta$  appartient à  $\mathcal{I}(2)$  et  $s_\Delta \circ s_\Delta = id_P$ .
- Si  $f_1$  et  $f_2$  sont dans  $\mathcal{I}(2)$ , alors  $f_2 \circ f_1 \in \mathcal{I}(2)$ ;  $f_2 \circ f_1$  sera appelé le produit de  $f_1$  et  $f_2$  dans  $\mathcal{I}(2)$ .

b) Soit  $f \in \mathcal{I}(2)$ ; montrer que :

- si  $f$  a deux points fixes distincts  $A$  et  $B$ , alors tout point de la droite  $AB$  est fixe pour  $f$ ;
- Si  $f$  a trois points fixes,  $A, B, C$  non alignés, alors  $f = id_P$ .

c) Démontrer que toute isométrie  $f \in \mathcal{I}(2)$  est le produit de 0, 1, 2, ou 3 symétries.

d) Prouver que  $\mathcal{I}(2)$  est un sous-groupe du groupe symétrique  $S_P$  et que  $\mathcal{I}(2)$  est non-abélien.

e) A tout vecteur  $v$  de l'espace vectoriel  $\mathbb{R}^2$  on associe la translation de vecteur  $v$  du plan affine  $P$ , notée  $t_v$ . Montrer à l'aide de (c) que  $t_v \in \mathcal{I}(2)$  et que  $\mathcal{T}(P) = \{t_v; v \in \mathbb{R}^2\}$  est un sous-groupe abélien de  $\mathcal{I}(2)$ , isomorphe à  $(\mathbb{R}^2, +)$ .

f) Soit  $O$  un point du plan  $P$ , pour  $\alpha \in \mathbb{R}$ ; on note  $r_{O,\alpha}$  la rotation du plan  $P$  de centre  $O$  et d'angle  $\alpha$ .

Montrer à l'aide de (c) que  $r_{O,\alpha} \in \mathcal{I}(2)$ .  $\mathcal{R}(P, O)$  désignant l'ensemble de toutes les rotations  $R_{O,\alpha}$  pour  $\alpha \in \mathbb{R}$ , vérifier que  $\mathcal{R}(P, O) = \{r_{O,\alpha}; 0 \leq \alpha < 2\pi\}$  et que  $\mathcal{R}(P, O)$  est un sous-groupe abélien de  $\mathcal{I}(2)$ .

a) —  $\forall A \in P, ||id_P(A)|| = ||A||$ , l'identité est donc une isométrie.

— Pour toute droite  $\Delta$  et point  $A$  avec son symétrique par rapport à  $\Delta$   $A'$ , on pose le repère de centre  $O$  l'intersection entre  $\Delta$  et  $AA'$  et d'axes  $\vec{OA'}$  et  $\Delta$ . Dans ce repère, le symétrique d'un point  $(x, y)$  est  $(-x, y)$ . Ainsi :

$$\forall (x, y) \in \mathbb{R}^2, ||s_\Delta(x, y)|| = ||(-x, y)|| = ||(x, y)||$$

et on a

$$\forall (x, y) \in \mathbb{R}^2, s_\Delta(s_\Delta((x, y))) = s_\Delta((-x, y)) = (x, y) = id_P((x, y)).$$

—

$$\begin{aligned}\forall f_1, f_2 \in \mathcal{I}(2), \forall A \in P, ||f_2 \circ f_1 \circ A|| &= ||f_1 \circ A|| \text{ car } f_2 \text{ est une isométrie,} \\ &= ||A|| \text{ car } f_1 \text{ est une isométrie.}\end{aligned}$$

Ainsi, le produit de deux isométries est une isométrie.

b) — Soit  $M$  un point de la droite  $AB$ ,  $d$  la fonction distance, comme  $f$  est une isométrie, on a

$$d(f(A), f(M)) = d(A, M), \quad d(f(B), f(M)) = d(B, M)$$

De plus, comme  $A$  et  $B$  sont des points fixes, on a

$$d(A, f(M)) = d(A, M), \quad d(B, f(M)) = d(B, M)$$

Donc le point  $f(M)$  est à la même distance de  $A$  et  $B$  que le point  $M$ . Donc, les points  $M$  et  $f(M)$  sont sur le même cercle centré en  $A$  de rayon  $AM$ , et aussi sur le même cercle centré en  $B$  de rayon  $BM$ , cercles tangents en  $M$ .

Ainsi,  $f(M) = M$ .

- c)
- d)
- e)
- f)

**27)** Notons  $\mathbb{C}$  le plan complexe, c'est-à-dire le plan affine euclidien  $R^2$  rapporté à un système d'axes ortho-normés Oxy et dont tout point  $M(x, y)$  est considéré comme l'image du nombre complexe  $z = x + iy$ .

A toute famille de 4 nombres complexes  $(a, b, c, d)$  telle que  $ad - bc \neq 0$ , on associe l'application :

$$f : \mathbb{C} \rightarrow \mathbb{C},$$

$$z \mapsto \frac{az + b}{cz + d}, \text{ où } z \in \mathbb{C}.$$

On remarque que si  $c \neq 0$ , le point  $-\frac{d}{c}$  n'a aucune image par  $f$  ; d'autre part le point  $\frac{a}{c}$  n'est l'image d'aucun point de  $\mathbb{C}$ . Pour remédier à ces difficultés, on rajoute au plan complexe un point dit à l'infini et noté  $\infty$ .

On pose  $\tilde{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ , pour  $c \neq 0$ ,  $f\left(-\frac{d}{c}\right) = \infty$  et  $f(\infty) = \frac{a}{c}$ .

Une application telle que  $f$  est appelée une homographie du plan complexe.

- a) Montrer que toute homographie  $f$  est une permutation de  $\tilde{\mathbb{C}}$ .
- b) Démontrer que l'ensemble  $\mathcal{H}$  des homographies du plan complexe est un sous-groupe du groupe symétrique  $S_{\tilde{\mathbb{C}}}$ .
- c) En considérant le cas où  $c = 0$ , prouver que  $\mathcal{H}$  contient comme sous-groupes le groupe des similitudes et translations du plan complexe.
- d) Vérifier que l'homographie  $z \mapsto \frac{1}{z}$  est le produit (commutatif) de l'inversion de centre O et de puissance 1. et de la symétrie par rapport à l'axe Ox.
- e) Démontrer que toute homographie  $f$  du plan complexe conserve les angles et leurs orientation, ce que l'on exprime en disant que  $f$  est une transformation conforme du plan.
- f) Prouver que les homographies :

$$f_1 : z \mapsto z; \quad f_2 : z \mapsto -z; \quad f_3 : z \mapsto \frac{1}{z}; \quad f_4 : z \mapsto -\frac{1}{z}$$

forment un sous-groupe de  $\mathcal{H}$  isomorphe au groupe de Klein.

- g) Prouver que les homographies :

$$g_1 : z \mapsto z; \quad g_2 : z \mapsto \frac{1}{1-z}; \quad g_3 : z \mapsto \frac{z-1}{z},$$

$$g_4 : z \mapsto \frac{1}{z}; \quad g_5 : z \mapsto 1-z; \quad g_6 : z \mapsto \frac{z}{z-1}$$

forment un sous-groupe de  $\mathcal{H}$  isomorphe au groupe symétrique  $S_3$ .

- a) Vérifions l'injectivité de  $f$  :

$$\begin{aligned} \forall x, y \in \tilde{\mathbb{C}}, \quad f(x) = f(y) &\Rightarrow \frac{ax + b}{cx + d} = \frac{ay + b}{cy + d}, \\ &\Rightarrow (ax + b)(cy + d) = (ay + b)(cx + d), \\ &\Rightarrow acxy + adx + bcy + bd = acxy + ady + bcx + bd, \\ &\Rightarrow adx + bcy = ady + bcx, \\ &\Rightarrow ad(x - y) + bc(y - x) = 0, \\ &\Rightarrow (ad - bc)(x - y) = 0, \\ &\Rightarrow x = y, \text{ car on sait que } ad - bc \neq 0. \end{aligned}$$

Vérifions la surjectivité,  $\forall w \in \mathbb{C}^*$ , on vérifie que  $f\left(\frac{wd-b}{-wc+a}\right) = w$ . avec par définition quand  $c$  est non nul  $f\left(\frac{-d}{c}\right) = \infty$  et  $f(\infty) = \frac{a}{c}$ .

- b) L'ensemble  $\mathcal{H}$  est non vide, l'application identité  $f(z) = z$  étant une homographie de paramètre  $\{1, 0, 0, 1\}$ . De plus, chaque homographie est inversible, et son inverse est aussi une homographie. Vérifions que cet ensemble est stable par composition, soit  $f$  une homographie de paramètres  $\{a, b, c, d\}$  et  $g$  une homographie de paramètres  $\{\alpha, \beta, \gamma, \delta\}$  :

$$(f \circ g)(z) = \frac{(a\alpha + b\gamma)z + (a\beta + b\delta)}{(c\alpha + d\gamma) + c\beta + d\delta}.$$

Avec  $(a\alpha + b\gamma)(c\beta + d\delta) - (a\beta + b\delta)(c\alpha + d\gamma) \neq 0$ , donc  $\mathcal{H}$  est stable par composition.

La composition de fonctions étant associative, on conclut que  $\mathcal{H}$  est un sous-groupe de  $\tilde{\mathbb{C}}$ .

- c) Le groupe des similitudes de  $\mathbb{C}$  étant les application de la forme  $az + b$  avec  $a \in \mathbb{C}^*, b \in \mathbb{C}$ , on constate que ce sont les homographie de paramètres  $\{a, b, 0, 1\}$ . Les translations étant des similitudes où  $a = 1$ , on vérifie immédiatement qu'elles sont incluses dans le groupe des homographies.

- d) L'inversion de centre O est  $z \mapsto \frac{1}{\bar{z}}$ , et la symétrie par Ox  $z \mapsto \bar{z}$ . Le produit des deux est donc l'homographie  $z \mapsto \frac{1}{z}$ .

- e) Quand  $c = 0$ , les homographies sont des similitudes, qui préservent les angles et leurs orientations. Soit  $f$  une homographie de paramètres  $\{a, b, c, d\}$ , avec  $c \neq 0$ . On peut écrire

$$a + bz = \frac{a}{c}(cz + d) - \frac{ad - bc}{c},$$

ce qui permet de réécrire  $f$  comme :

$$f = \frac{a}{c} - \frac{ad - bc}{c^2} \frac{1}{z + \frac{d}{c}}.$$

On peut décomposer  $f$  comme une composition de :

- $t : z \mapsto z + \frac{d}{c}$ , une translations,
- $i : z \mapsto \frac{1}{\bar{z}}$ , une inversion de centre O et de puissance 1,
- $c : z \mapsto \bar{z}$ , une symétrie selon l'axe Ox,
- $s : z \mapsto -\frac{ad - bc}{c^2}z + \frac{a}{c}$  une similitude,

telle que  $f = s \circ c \circ i \circ t$ .

Toutes ces applications préservent les angles, de plus  $i$  et  $c$  changent l'orientation. On en conclut que  $f$  est une transformation conforme du plan.

- f) Soit  $K = \{f_1, f_2, f_3, f_4\}$ , posons la table de Cayley de cet ensemble muni de la composition :

$\circ$	$f_1$	$f_2$	$f_3$	$f_4$
$f_1$	$f_1$	$f_2$	$f_3$	$f_4$
$f_2$	$f_2$	$f_1$	$f_4$	$f_3$
$f_3$	$f_3$	$f_4$	$f_1$	$f_2$
$f_4$	$f_4$	$f_3$	$f_2$	$f_1$

Qui permet immédiatement de conclure que K est isomorphe au groupe de Klein.

- g) Posons  $H = \{g_1, g_2, g_3, g_4, g_5, g_6\}$ , et posons sa table de Cayley encore :

$\circ$	$g_1$	$g_2$	$g_3$	$g_4$	$g_5$	$g_6$
$g_1$	$g_1$	$g_2$	$g_3$	$g_4$	$g_5$	$g_6$
$g_2$	$g_2$	$g_3$	$g_1$	$g_6$	$g_4$	$g_5$
$g_3$	$g_3$	$g_1$	$g_2$	$g_5$	$g_6$	$g_4$
$g_4$	$g_4$	$g_5$	$g_6$	$g_1$	$g_2$	$g_3$
$g_5$	$g_5$	$g_6$	$g_4$	$g_3$	$g_1$	$g_2$
$g_6$	$g_6$	$g_4$	$g_5$	$g_2$	$g_3$	$g_1$



$H$  est stable par composition et passage à l'inverse, c'est donc un sous-groupe de  $\mathcal{H}$ . En posant la bijection avec  $S_3$  :

$$e \mapsto g_1, \sigma_1 \mapsto g_2, \sigma_2 \mapsto g_3, t_1 \mapsto g_4, t_2 \mapsto g_5, t_3 \mapsto g_6$$

on constate que les tables de Cayley sont identitiques, donc que  $H$  et  $S_3$  sont isomorphes.

28)

- a) Démontrer le corollaire (1.49)
- b) Démontrer la proposition (1.53)

- a) Démontrons par récurrence sur  $n$ .

— Initialisation :

Soit  $H_1, H_2$  deux sous-groupes de  $G$  tel que  $H_1 H_2$  est un sous-groupe de  $G$ , la propriété est vérifiée.

— Hérédité :

Supposons qu'il existe  $n$  tel que la propriété est vraie, c'est à dire que pour  $\{H_i\}_{1 \leq i \leq n}$  une famille de sous-groupe de  $G$  tel que  $H_i H_j = H_j H_i$  pour tout  $(i, j)$  tel que  $1 \leq i < j \leq n$ ,  $H_1 H_2 \dots H_n$  est un sous-groupe de  $G$ . Vérifions que la propriété est vraie pour  $n + 1$ .

Soit une  $\{H_i\}_{1 \leq i \leq n+1}$  une famille de sous-groupe de  $G$  tel que  $H_i H_j = H_j H_i$  pour tout  $(i, j)$  tel que  $1 \leq i < j \leq n + 1$ , on a :

$$\begin{aligned} (H_1 H_2 \dots H_{n-1} H_n) H_{n+1} &= H_1 H_2 \dots H_{n-1} H_{n+1} H_n, \text{ par hypothèse,} \\ &= H_1 H_2 \dots H_{n+1} H_{n-1} H_n, \\ &\vdots \\ &= H_{n+1} (H_1 H_2 \dots H_{n-1} H_n). \end{aligned}$$

De plus, par hypothèse de récurrence,  $(H_1 H_2 \dots H_{n-1} H_n)$  est un sous-groupe de  $G$ .

Ainsi,  $H_1 H_2 \dots H_n H_{n+1}$  est un sous-groupe de  $G$ .

— Conclusion :

Le corollaire est démontré.

- b) Soit  $I$  un ensemble non vide et  $\{H_i\}_{i \in I}$  une famille de sous-groupes d'un groupe abélien  $G$ . Montrons que le sous-groupe  $G' \Sigma_{i \in I} H_i$  est en somme directe si et seulement si tout  $x \in G'$  s'écrit de façon unique :

$$x \in \sum_{i \in I} x_{i_k}.$$

Supposons que chaque  $z \in G'$  s'écrit de façon unique. Soit  $Z \in \bigcap_{i \in I} H_i$ , pour tout  $j \in J$ , on peut écrire :

$$z = \underbrace{z}_{\in H_j} + \underbrace{0}_{\in \sum_{i \neq j} H_i} = \underbrace{0}_{\in H_j} + \underbrace{z}_{\in \sum_{i \neq j} H_i}$$

$z$  s'écrivant de façon unique, on en conclut que  $z = 0$ , donc  $G'$  est en somme directe.

Supposons que  $G'$  soit en somme directe, c'est-à-dire que  $\bigcap_{i \in I} H_i = \{0\}$ . Soit  $z \in G'$ , supposons que  $z$  s'écrit de deux façons différentes :

$$z = \sum_{i \in I} x_i = \sum_{i \in I} x'_i, \text{ avec au moins un } i \text{ tel que } x_i \neq x'_i$$

pour tout  $j \in I$ , on peut écrire :

$$x_j - x'_j = \sum_{\substack{i \in I \\ i \neq j}} x'_i - \sum_{\substack{i \in I \\ i \neq j}} x_i = \sum_{\substack{i \in I \\ i \neq j}} x'_i - x_i.$$

On a  $x_j - x'_j \in H_j$ , et  $\sum_{\substack{i \in I \\ i \neq j}} x'_i - x_i \in \sum_{\substack{i \in I \\ i \neq j}} H_i$ , donc  $x_j - x'_j \in H_j \cap \sum_{\substack{i \in I \\ i \neq j}} x'_i - x_i = 0$ .

Donc, pour tout  $j \in I$ ,  $z$  s'écrit de façon unique.

**29)** Soit  $E$  un ensemble non vide et  $G$  un groupe d'élément unité  $e$ . On désigne par  $G^E$  l'ensemble des applications  $f$  de  $E$  dans  $G$ . On considère la loi de composition définie dans  $G^E$  par :

$$\begin{aligned} G^E \times G^E &\rightarrow G^E \\ (f, g) &\mapsto fg, \end{aligned}$$

Où  $fg$  est telle que pour tout  $x \in E$ ,  $(fg)(x) = f(x)g(x)$ .

Prouver que  $(G^E)$  est ainsi muni d'une structure de groupe.

Vérifier que  $G^E$  est un groupe abélien si et seulement si  $G$  est abélien.

La loi de composition est clairement une loi interne. Vérifions qu'elle est associative :

$$\begin{aligned} \forall f, g, h \in G^E, (f(gh))(x) &= f(x)((gh)(x)), \\ &= f(x)(g(x)h(x)), \\ &= (f(x)g(x))h(x) \text{ car } f(x), g(x), h(x) \in G, \text{ un groupe,} \\ &= ((fg)(x))(h(x)), \\ &= ((fg)h)(x). \end{aligned}$$

Vérifions l'existence d'un élément neutre. Soit  $e$  le neutre de  $G$ , et  $i(x) \in G^E$ , tel que  $\forall x \in E, i(x) = e$ , pour tout  $x$  dans  $E$  on a  $(fi)(x) = f(x)i(x) = f(x) = i(x)f(x) = (if)(x)$ ,  $i$  est donc un neutre.

Pour tout  $f \in G^E$ , on pose  $g$  tel que  $\forall x \in E, g(x) = f(x)^{-1}$ . On vérifie que  $\forall x \in E, (fg)(x) = f(x)g(x) = f(x)f(x)^{-1} = e = i(x)$ , et pareil pour  $gf$ .

On en conclut que  $G^E$  est un groupe.

Supposons que  $G$  soit abélien, soit  $f, g \in G^E$  :

$$\begin{aligned} \forall x \in E, (fg)(x) &= f(x)g(x), \\ &= g(x)f(x), \\ &= (gf)(x). \end{aligned}$$

Supposons que  $G^E$  soit abélien. Pour tout  $a, b \in G$ , on pose  $f, g \in G^E$  tel que  $\forall x \in E, f(x) = a$  et  $g(x) = b$ . Ainsi on a :

$$\begin{aligned} \forall a, b \in G, \forall x \in E, ab &= f(x)g(x), \\ &= (fg)(x), \\ &= (gf)(x), \\ &= g(x)f(x), \\ &= ba. \end{aligned}$$

On conclut que  $G^E$  est un groupe abélien si et seulement si  $G$  est abélien.

**30)**  $\mathbb{R}$  désignant le groupe additif des réels, on pose :

$$J = \{x \in \mathbb{R}; 0 \leq x \leq 1\}.$$

L'addition de  $\mathbb{R}$  induit dans l'ensemble  $\mathbb{R}^J$  une structure de groupe additif abélien.

a) Vérifier les propriétés suivantes :

- l'ensemble des fonctions  $f \in \mathbb{R}^J$ , continues sur  $J$ , est un sous-groupe de  $(\mathbb{R}^J, +)$ , que l'on notera  $\mathcal{C}(J)$ ;

— si, pour tout  $a \in \mathbb{R}$ , on note  $c_a$  la fonction constante de  $J$  dans  $\mathbb{R}$  telle que  $c_a(x) = a$  pour tout  $x \in J$ , alors  $\Gamma = \{c_a; a \in \mathbb{R}\}$  est un sous-groupe de  $(\mathcal{C}(J), +)$ .

b) On considère les applications  $F_i$  de  $\mathcal{C}(J)$  dans  $\mathbb{R}$  telles que :

$$F_1 : f \mapsto f(1), \quad F_2 : f \mapsto |f(0)|, \quad F_3 : f \mapsto \int_0^1 f(x)dx$$

$$F_4 : f \mapsto \frac{\pi}{3} \int_0^1 f(x) \cos \frac{\pi x}{6} dx, \quad F_5 : f \mapsto \int_0^1 \cos \frac{\pi f(x)}{6} dx.$$

Déterminer les  $F_i$  qui sont des homomorphismes de groupes de  $(\mathcal{C}(J), +)$  dans  $(\mathbb{R}, +)$ . Pour chacun des morphismes de groupes  $F_i$ , prouver que, quel que soit  $a \in \mathbb{R}$ ,  $F_i(c_a) = a$  et montrer qu'il existe un unique  $m_i \in \mathbb{R}$  tel que  $F_i(\text{id}_J - c_{m_i}) = 0$ . En déduire que les  $\text{Ker } F_i$  sont deux à deux distincts.

c) Démontrer que pour tout  $F \in \text{Hom}(\mathcal{C}(J), \mathbb{R})$ , tel que  $F(c_a) = a$ , quel que soit  $a \in \mathbb{R}$ , on a

$$\mathcal{C}(J) = \text{Ker } F \oplus \Gamma.$$

En conclure qu'il existe de nombreux sous-groupes de  $\mathcal{C}(J)$  tels que  $\mathcal{C}(J) = H \oplus \Gamma$ .

a) Les fonctions de  $\mathbb{R}^J$  continues sur  $J$  sont un sous-ensemble des fonctions de  $\mathbb{R}^J$ . De plus, la différence de deux fonctions continues est continue. Donc  $\mathcal{C}(J)$  est un sous-groupe de  $(\mathbb{R}^J, +)$ .

De la même façon, les fonctions constantes sont des fonctions continues, et  $c_a - c_b = c_{a-b}$ .

b)  $F_1, F_3, F_4$  sont des morphismes, en effet,  $\forall f, g \in \mathcal{C}(J)$  :

$$\begin{aligned} F_1(f+g) &= (f+g)(1) = f(1) + g(1) = F_1(f) + F_1(g), \\ F_3(f+g) &= \int_0^1 (f+g)(x)dx = \int_0^1 f(x)dx + \int_0^1 g(x)dx = F_3(f) + F_3(g), \\ F_4 &: \text{Par linéarité de l'intégrale comme } F_3. \end{aligned}$$

Cependant,  $F_2(c_{-1} + c_1) = F_2(c_0) = 0$ , mais  $F_2(c_{-1}) + F_2(c_1) = 2$ , ce n'est pas un morphisme.

Et  $F_5(c_0) = 1 \neq 0$ , donc ce n'est pas un morphisme non plus.

On vérifie trivialement (que j'ai la flemme de le taper) que pour ces morphismes,  $\forall a \in \mathbb{R}, F_i(c_a) = a$ .

Posons le calcul pour  $F_1$  :

$$\begin{aligned} F_1(\text{Id}_J - c_m) &= 0 \Rightarrow F_1(\text{Id}_J) - F_1(c_m) = 0 \\ &\Rightarrow F_1(\text{Id}_J) = F_1(c_m), \\ &\Rightarrow \text{Id}_J(1) = m, \\ &\Rightarrow m = 1. \end{aligned}$$

Et on vérifie qu'on a bien  $F_1(\text{Id}_J - c_1) = 0$  (Peut être qu'en bossant par équivalences successives on aurait pas à révéifier, mais j'suis traumatisée car j'en mettais trop), l'unique  $m_1$  est donc 1. De la même façon,

on trouve  $m_3 = 0.5$  et  $m_4 = 1 + \frac{6\sqrt{3} - 12}{\pi}$ .

Comme le  $c_m$  est unique pour chacun de ses morphismes, on en conclut que leurs noyaux sont distincts.

c) Soit  $f \in \mathcal{C}(J)$ , on peut écrire

$$f = \underbrace{f - c_{F(f)}}_{\in \text{Ker } F} + \underbrace{c_{F(f)}}_{\in \Gamma}.$$

Vérifions ensuite que l'intersection de ces deux ensembles est triviale. Soit  $c_a \in \Gamma$ ,  $F(c_a) = a$ , donc on a bien  $\text{Ker } F \cap \Gamma = \{c_0\}$ .

Soit la famille de morphismes  $\{F_\alpha\}$  avec  $\alpha \in [0; 1]$ , tel que  $F_\alpha = \frac{1}{\alpha} \int_0^\alpha f(x)dx$ .

Par linéarité de l'intégrale, ce sont bien des morphismes. De plus,  $\forall a \in \mathbb{R}, F_\alpha(c_a) = a$ . De la même façon que précédemment, on vérifie que  $F_\alpha(\text{Id}_J - c_{m_\alpha}) = 0$  admet une unique solution  $m_\alpha = \alpha$ . On a donc une famille infinie de morphismes allant des noyaux distincts, ces noyaux permettant la décomposition de  $\mathcal{C}(J)$  en somme directe de  $\text{Ker } F_\alpha$  et  $\Gamma$ .

**31)** Soit deux groupes  $G_1$  et  $G_2$ .

- a) Prouver que les groupes  $G_1 \times G_2$  et  $G_2 \times G_1$  sont isomorphes.
- b)  $\Gamma_1$  et  $\Gamma_2$  étant aussi deux groupes, démontrer la propriété :  $(\Gamma_1 \simeq G_1 \text{ et } \Gamma_2 \simeq G_2) \Rightarrow \Gamma_1 \times \Gamma_2 \simeq G_1 \times G_2$ .
- c) Si  $H_1$  et  $H_2$  sont respectivement des sous-groupes de  $G_1$  et  $G_2$ , montrer que  $H_1 \times H_2$  est un sous-groupe de  $G_1 \times G_2$ .

Déterminer tous les sous-groupes de  $\frac{\mathbb{Z}}{(2)} \times \frac{\mathbb{Z}}{(2)}$  ; en déduire compte tenu des notations précédentes, qu'un sous-groupe de  $G_1 \times G_2$  n'est pas nécessairement de la forme  $H_1 \times H_2$ .

- a) Vérifions que l'application suivante est un isomorphisme de groupe :

$$\begin{aligned} \varphi : G_1 \times G_2 &\rightarrow G_2 \times G_1, \\ (g_1, g_2) &\mapsto (g_2, g_1). \end{aligned}$$

$\varphi$  est un morphisme, en effet :

$$\begin{aligned} \forall (g_1, g_2), (h_1, h_2) \in G_1 \times G_2, \quad \varphi((g_1, g_2)(h_1, h_2)) &= \varphi((g_1 h_1, g_2 h_2)), \\ &= (g_2 h_2, g_1 h_1), \\ &= (g_2, g_1)(h_2, h_1), \\ &= \varphi(g_1, g_1)\varphi(h_1, h_2). \end{aligned}$$

Vérifions qu'elle est injective :

$$\forall (g_1, g_2) \in G_1 \times G_2, \quad \varphi(g_1, g_2) = (e_2, e_1) \Leftrightarrow (g_2, g_1) = (e_2, e_1).$$

Elle est aussi trivialement surjective, car pour tout  $(g_2, g_1) \in G_2 \times G_1$ , on a  $\varphi(g_1, g_2) = (g_2, g_1)$ .

Ainsi,  $\varphi$  est un isomorphisme, donc pour tout groupe  $G_1$  et  $G_2$ , on a  $G_1 \times G_2 \cong G_2 \times G_1$ .

- b) Soit  $\varphi_1$  un isomorphisme de  $\Gamma_1$  vers  $G_1$  et  $\varphi_2$  un isomorphisme de  $\Gamma_2$  vers  $G_2$ .

On vérifie de la même façon que a) que :

$$\begin{aligned} \varphi : \Gamma_1 \times \Gamma_2 &\rightarrow G_1 \times G_2, \\ (\gamma_1, \gamma_2) &\mapsto (\varphi_1(\gamma_1), \varphi_2(\gamma_2)). \end{aligned}$$

est un isomorphisme de groupe (flemme de taper, et franchement c'est la même chose que a)), donc on a  $\Gamma_1 \times \Gamma_2 \cong G_1 \times G_2$ .

- c) On a  $H_1 \times H_2 \subseteq G_1 \times G_2$ , et

$$\begin{aligned} \forall (h_1, h_2), (k_1, k_2) \in H_1 \times H_2, \quad (h_1, h_2)(k_1, k_2)^{-1} &= (h_1, h_2)(k_1^{-1}, k_2^{-1}), \\ &= (h_1 k_1^{-1}, h_2 k_2^{-1}) \in H_1 \times H_2. \end{aligned}$$

Donc  $H_1 \times H_2$  est un sous-groupe de  $G_1 \times G_2$ .

Les sous groupes de  $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$  sont :

$$\{(\bar{0}, \bar{0})\}, \{(\bar{0}, \bar{0}), (\bar{1}, \bar{1})\}, \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1})\}, \{(\bar{0}, \bar{0}), (\bar{1}, \bar{0})\},$$

On constate que  $\{(\bar{0}, \bar{0}), (\bar{1}, \bar{1})\}$  n'est pas produit de sous-groupes de  $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ , mais est un sous-groupe de  $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ .

**32)** Pour deux groupes  $G_1$  et  $G_2$ , démontrer les propriétés :

- a)  $G_1 \simeq G_2 \Rightarrow \text{Aut}(G_1) \simeq \text{Aut}(G_2)$
- b)  $G_1 \simeq G_2 \Rightarrow \text{Int}(G_1) \simeq \text{Int}(G_2)$ .

a) Soit  $G_1$  et  $G_2$  deux groupes isomorphes et  $\varphi$  un isomorphisme de  $G_1$  vers  $G_2$ .

$$\begin{array}{ccc} G_1 & \xrightarrow{\varphi} & G_2 \\ \downarrow \alpha & & \downarrow \\ G_1 & \xrightarrow{\varphi} & G_2 \end{array}$$

On pose l'application  $\Psi$  tel que :

$$\begin{aligned} \Psi : \text{Aut}(G_1) &\rightarrow \text{Aut}(G_2), \\ a &\mapsto \varphi \circ \alpha \circ \varphi^{-1}. \end{aligned}$$

C'est un morphisme, en effet :

$$\begin{aligned} \forall \alpha_1, \alpha_2 \in \text{Aut}(G_1), \quad \Psi(\alpha_1 \circ \alpha_2) &= \varphi \circ (\alpha_1 \circ \alpha_2) \circ \varphi^{-1}, \\ &= \varphi \circ \alpha_1 \circ \alpha_2 \circ \varphi^{-1}, \\ &= \varphi \circ \alpha_1 \circ \varphi^{-1} \circ \varphi \circ \alpha_2 \circ \varphi^{-1}, \\ &= \Psi(\alpha_1) \circ \Psi(\alpha_2). \end{aligned}$$

Vérifions l'injectivité :

$$\begin{aligned} \forall \alpha \in \text{Aut}(G_1), \quad \Psi(\alpha) = \text{Id}_{G_2} &\Leftrightarrow \varphi \circ \alpha \circ \varphi^{-1} = \text{Id}_{G_2}, \\ &\Leftrightarrow \varphi \circ \alpha = \varphi, \\ &\Leftrightarrow \alpha = \text{Id}_{G_1}. \end{aligned}$$

Et si  $\alpha \in \text{Aut}(G_2)$ , on a  $\Psi(\varphi^{-1} \circ \alpha \circ \varphi) = \alpha$ , montrant la surjectivité, et donc que  $G_1 \cong G_2 \Rightarrow \text{Aut}(G_1) \cong \text{Aut}(G_2)$ .

b) De la même façon, on pose :

$$\begin{aligned} \Psi_{\text{Int}} : \text{Int}(G_1) &\rightarrow \text{Int}(G_2), \\ \sigma_g &\mapsto \Psi(\sigma_g). \end{aligned}$$

On vérifie que  $\Psi_{\text{Int}}$  est bien définie, avec  $\Psi_{\text{Int}}(\sigma_g) = \sigma_{\varphi(g)}$ . De la même façon que a), on montre que  $\Psi_{\text{Int}}$  est un isomorphisme de groupes, et donc que  $G_1 \cong G_2 \Rightarrow \text{Int}(G_1) \cong \text{Int}(G_2)$ .

**33)** Soit  $\{G_i\}_{i \in I}$  une famille de groupes ; montrer que, pour tout groupe  $G$ , l'ensemble  $\text{Hom}\left(G, \prod_{i \in I} G_i\right)$

est équipotent à l'ensemble  $\prod_{i \in I} \text{Hom}(G, G_i)$ .

Même démo que le théorème 1.91 mais pour tout n.