Exercice 3
Soit G un groupe d'ordre 4, d'élément neutre e.

(1) On suppose dans cette question qu'il existe un élément x de G tel que $x^2 \neq e$; x^2 est noté y, et on note z le quatrième élément de G Déterminer la table de Cayley de G.

(2) On suppose à l'inverse que le carré de tout élément de G est e, et on note x, y, z les éléments de G distincts de e. Déterminer la table de Cayley de G.

(3) En déduire que tout groupe d'ordre 4 est commutatif.

Solution de (1) : Dans ce cas, $G = \{e, x, y, z\}$ et x n'est pas son propre inverse. On calcule xz. On ne peut pas avoir $xz = x$ car $z \neq e$. L'égalité $xz = z$ n'est pas possible non plus car $x \neq e$. L'égalité $xz = y$ est également impossible car sinon $xz = y = x^2 \Longrightarrow xz = xx \Longrightarrow z = x$, ce qui est faux. Donc la seule possibilité est $xz = e$. De manière analogue on trouve $zx = e$ et donc, jusqu'ici, on sait que

$$xz = zx = e. \tag{1}$$

En utilisant (1) on trouve aussi

$$yz = x^2 z = x(xz) = xe = x \Longrightarrow yz = x. \tag{2}$$

Avec les informations (1) et (2) on obtient la table de Cayley partiellement remplie

$\cdot$	e	x	y	z
e	e	x	y	z
x	x	y		e
y	y			x
z	z	e		

Puisque la table d'un groupe est un carré latin, on peut compléter la table ci-dessus et trouver

$\cdot$	e	x	y	z
e	e	x	y	z
x	x	y	z	e
y	y	z	e	x
z	z	e	x	y

(3)

On note que dans ce cas, G est abélien et $G \cong \mathbb{Z}/4\mathbb{Z}$.

Solution de (2) : Dans ce cas $G = \{e, x, y, z\}$ avec $x^2 = y^2 = z^2 = e$. Alors la table de Cayley partiellement remplie est

$\cdot$	e	x	y	z
e	e	x	y	z
x	x	e		
y	y		e	
z	z			e

Encore une fois, puisque ta table d'un groupe est un carré latin, on peut utiliser les "techniques de Sudoku" pour compléter la table de Cayley de G et obtenir

$\cdot$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

(4)

On note qu'encore une fois, G est abélien et que $G \cong K$, où K est le groupe de Klein

$$K = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

Solution de (3) : On note que les points (1) et (2) couvrent tous les cas possibles. En effet, soit tout carré est l'élément neutre, soit il existe un carré qui n'est pas l'élément neutre. Par conséquent, pour tout groupe G d'ordre 4, soit (3) est la table de Cayley de G, soit (4) l'est. Autrement dit, il n'existe que deux groupes d'ordre 4 (à un isomorphisme près) et dans les deux cas les groupes sont abéliens.

Exercice 7
Soit G un sous-groupe de $(\mathbb{R}, +)$ tel que $G \neq \{0\}$.

(1) Montrer que $G \cap \mathbb{R}_+^*$ admet une borne inférieure, que l'on notera a.

(2) Supposons que $a > 0$. Montrer que $a \in G$ (on pourra raisonner par l'absurde). En déduire que $G = a\mathbb{Z}$.

(3) Supposons que $a = 0$. Montrer que G est dense dans $\mathbb{R}$, c'est-à-dire que pour tous réels $x < y$, il existe $g \in G$ tel que $x < g < y$.

Solution de (1) : Puisque $G \neq \{0\}$, il existe $x \in G \subset \mathbb{R}$ tel que $x \neq 0$. L'inverse $-x$ de x est aussi un élément de G et l'un des deux, x ou $-x$, est positif. Donc, $G \cap \mathbb{R}_+^* \neq \varnothing$. Alors, $G \cap \mathbb{R}_+^*$ est une partie non-vide et minorée de $\mathbb{R}$. Par conséquent, $G \cap \mathbb{R}_+^*$ admet une borne inférieure. On note

$$a = \inf G \cap \mathbb{R}_+^*.$$

Solution de (2) : On suppose par l'absurde que $0 < a \notin G$. Comme $a > 0$, on trouve que

$$2a > a = \inf G \cap \mathbb{R}_+^*$$

et donc $2a$ n'est pas un minorant de $G \cap \mathbb{R}_+^*$, càd qu'il existe $b \in G \cap \mathbb{R}_+^*$ tel que $b < 2a$. Comme $a = \inf G \cap \mathbb{R}_+^*$ n'appartient pas à G, on conclut que

$$a < b < 2a. \tag{5}$$

On répète l'argument avec $b > a = \inf G \cap \mathbb{R}_+^*$ afin de trouver $c \in G$ tel que

$$a < c < b. \tag{6}$$

Puisque G est groupe et $b > c$, on trouve que $0 < b - c \in G \cap \mathbb{R}_+^*$. De (5) et (6) on trouve

$$0 < b - c < 2a - a = a = \inf G \cap \mathbb{R}_+^*,$$

ce qui est une contradiction avec la définition de borne inférieure.

Il reste à montrer que $G = a\mathbb{Z}$. Comme G est un sous-groupe de $(\mathbb{R}, +)$ contenant a, on a $a\mathbb{Z} \subset G$. Réciproquement, soit $x \in G$. Comme $a > 0$, il existe un (unique) entier n tel que

$$na \leq x < (n+1)a\,; \tag{7}$$

x et na sont deux éléments de G donc $x - na$ appartient aussi à G. Or d'après (7),

$$0 \leq x - na < a\,.$$

D'après la définition de a, $x - na$ n'est pas dans $\mathbb{R}_+^*$ donc $x - na = 0$, d'où $x \in a\mathbb{Z}$. On a ainsi montré que $a\mathbb{Z} = G$.

Solution de (3) : On suppose que $a = 0$ et on montre que G est dense dans $\mathbb{R}$. Soit $x < y$ des réels quelconques. Alors

$$y - x > 0 = a = \inf G \cap \mathbb{R}_+^*$$

et donc $y - x$ n'est pas minorant de $G \cap \mathbb{R}_+^*$. Càd qu'il existe $g_0 \in G \cap \mathbb{R}_+^*$ tel que

$$0 < g_0 < y - x. \tag{8}$$

Soit $n \in \mathbb{Z}$ l'unique entier relatif tel que

$$(n-1)g_0 \leq x < ng_0.$$

On pose $g = ng_0 \in G$ et on montre que g est l'élément de G qu'on cherchait. En effet, en utilisant (8) on trouve

$$x < g = ng_0 = (n-1)g_0 + g_0 \leq x + g_0 < x + (y - x) = y$$

et donc

$$x < g < y.$$

Exercice 9
Soit $H = \langle a \rangle$ un groupe cyclique d'ordre n.

(1) Montrer que a^m est un générateur de H si et seulement si m est premier avec n.

(2) Quel est le nombre générateurs de H pour $n = 36$? Donner la liste de tous les générateurs de H.

Solution de (1) : On se rappelle d'abord du fameux Théorème de Bézout :

Deux nombres $m, n \in \mathbb{N}$ sont premiers entre eux si, et seulement si, il existe $x, y \in \mathbb{Z}$ tels que $mx + ny = 1$.

Il nous sera également utile le résultat suivant :

Si G est un groupe et $a \in G$ est un élément d'ordre n, alors $a^m = e$ si, et seulement si, $n \mid m$.

En utilisant ces résultats, on obtient:

$$\begin{aligned} a^m \text{ est un générateur de } H &\Leftrightarrow \langle a \rangle = \langle a^m \rangle \\ &\Leftrightarrow a \in \langle a^m \rangle \\ &\Leftrightarrow \text{il existe } x \in \mathbb{Z} \text{ tel que } a = a^{mx} \\ &\Leftrightarrow \text{il existe } x \in \mathbb{Z} \text{ tel que } a^{mx-1} = e \\ &\Leftrightarrow \text{il existe } x \in \mathbb{Z} \text{ tel que } n \mid (mx - 1) \\ &\Leftrightarrow \text{il existe } x, y \in \mathbb{Z} \text{ tel que } mx + ny = 1 \\ &\Leftrightarrow m \text{ et } n \text{ sont premiers entre eux.} \end{aligned}$$

Solution de (2) : Les nombres premiers avec $n = 36$ sont

$$1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35,$$

d'où le nombre de générateurs de H est 12, ce sont

$$a^1, a^5, a^7, a^{11}, a^{13}, a^{17}, a^{19}, a^{23}, a^{25}, a^{29}, a^{31}, a^{35}.$$

Exercice 10
Soir G le groupe $\mathbb{Z}/36\mathbb{Z}$ et $\sigma : \mathbb{Z} \to \mathbb{Z}/36\mathbb{Z}$ la surjection canonique.

(1) Montrer que si H est un sous-groupe de $(\mathbb{Z}/36\mathbb{Z}, +)$, alors $\sigma^{-1}(H)$ est un sous-groupe de $(\mathbb{Z}, +)$ contenant $36\mathbb{Z}$.

(2) Déterminer tous les sous-groupes du groupe $\mathbb{Z}/36\mathbb{Z}$.

(3) Donner la liste de tous les générateurs de $\mathbb{Z}/36\mathbb{Z}$.

(4) Quel est l'ordre du sous-groupe engendré par $\overline{9}$?

Solution de (1) : Soit H sous-groupe de $\mathbb{Z}/36\mathbb{Z}$. On montre que $\sigma^{-1}(H)$ est sous-groupe de $(\mathbb{Z},+)$.

- Puisque H est sous-groupe de $\mathbb{Z}/36\mathbb{Z}$, on a $\overline{0} \in H$. Comme tout élément $x \in 36\mathbb{Z}$ satisfait $\sigma(x) = \overline{0}$, on trouve que $\sigma(36\mathbb{Z}) \subset \overline{0}$ et donc $36\mathbb{Z} \subset \sigma^{-1}(H)$. En particulier, $\sigma^{-1}(H) \neq \varnothing$.
- Soit $x, y \in \sigma^{-1}(H)$. Alors $\sigma(x), \sigma(y) \in H$ et, comme H est groupe,

$$\sigma(x+y) = \overline{x+y} = \overline{x} + \overline{y} = \sigma(x) + \sigma(y) \in H,$$

  càd, $x + y \in \sigma^{-1}(H)$. Donc $\sigma^{-1}(H)$ est stable par l'opération $+$.
- Soit $x \in \sigma^{-1}(H)$. Alors $\overline{x} = \sigma(x) \in H$ et, donc, $\overline{x}^{-1} = \overline{-x} \in H$, càd, $-x \in \sigma^{-1}(H)$. Autrement dit, $\sigma^{-1}(H)$ est stable par passage à l'inverse.

Par conséquent, $\sigma^{-1}(H)$ est sous-groupe de $(\mathbb{Z},+)$ contenant $36\mathbb{Z}$.

Solution de (2) : Soit H un sous-groupe de $\mathbb{Z}/36\mathbb{Z}$. Alors $\sigma^{-1}(H)$ est un sous-groupe de $(\mathbb{Z},+)$, autrement dit, il existe $p \in \mathbb{N}$ tel que $\sigma^{-1}(H) = p\mathbb{Z}$. Par conséquent,

$$36 \in 36\mathbb{Z} \subset \sigma^{-1}(H) = p\mathbb{Z} \Longrightarrow 36 \in p\mathbb{Z} \Longrightarrow p|36 \Longrightarrow p \in \{1,2,3,4,6,9,12,18,36\}.$$

Par conséquent,

$$H = \sigma(p\mathbb{Z}) = \{\overline{pk} : k \in \mathbb{Z}\} = \{\overline{p}^k : k \in \mathbb{Z}\} = \langle \overline{p} \rangle,$$

où $p \in \{1,2,3,4,6,9,12,18,36\}$, càd, les sous-groupes de $\mathbb{Z}/36\mathbb{Z}$ sont

- $\langle \overline{1} \rangle = \mathbb{Z}/36\mathbb{Z}$ (ordre 36) ;
- $\langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, ..., \overline{34}\}$ (ordre 18) ;
- $\langle \overline{3} \rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}, ..., \overline{33}\}$ (ordre 12) ;
- $\langle \overline{4} \rangle = \{\overline{0}, \overline{4}, \overline{8}, \overline{12}, \overline{16}, \overline{20}, ..., \overline{32}\}$ (ordre 9) ;
- $\langle \overline{6} \rangle = \{\overline{0}, \overline{6}, \overline{12}, \overline{18}, \overline{24}, \overline{30}\}$ (ordre 6) ;
- $\langle \overline{9} \rangle = \{\overline{0}, \overline{9}, \overline{18}, \overline{27}\}$ (ordre 4) ;
- $\langle \overline{12} \rangle = \{\overline{0}, \overline{12}, \overline{24}\}$ (ordre 3) ;
- $\langle \overline{18} \rangle = \{\overline{0}, \overline{18}\}$ (ordre 2) ;
- $\langle \overline{36} \rangle = \langle \overline{0} \rangle = \{\overline{0}\}$ (ordre 1).

Solution de (3) : On sait que $\mathbb{Z}/36\mathbb{Z}$ est cyclique d'ordre 36. En effet, $\mathbb{Z}/36\mathbb{Z} = \langle \overline{1} \rangle$. D'après le théorème de Bézout (voir Exercice 9), $\overline{p} = \overline{1}^p$ est générateur de $\mathbb{Z}/36\mathbb{Z}$ si et seulement si $\text{pgcd}(p;36) = 1$, donc les générateurs de $\mathbb{Z}/36\mathbb{Z}$ sont $\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{25}, \overline{29}, \overline{31}, \overline{35}$.

Solution de (4) : On a $\langle \overline{9} \rangle = \{\overline{0}, \overline{9}, \overline{18}, \overline{27}\}$, donc $\text{Ord}(\langle \overline{9} \rangle) = 4$.

Exercice 12
Soit G un groupe. Pour tout $a \in G$, on définit l'application $\varphi_a : G \to G$ par

$$\varphi_a(x) = axa^{-1}.$$

(1) Vérifier que φ_a est un automorphisme de G.

(2) On pose $H = \{\varphi_a : a \in G\}$. Montrer que H est un sous-groupe du groupe des permutations $\mathcal{S}(G)$.

(3) Soit $\Psi : G \to \mathcal{S}(G)$ l'application définie par $\Psi : a \mapsto \varphi_a$. Vérifier que Ψ est un morphisme de groupes.

(4) Notons $Z(G)$ le centre de G :

$$Z(G) = \{y \in G : \forall x \in G, xy = yx\}.$$

Montrer que $Z(G)$ est un sous-groupe de G et que $G/Z(G)$ est un groupe isomorphe à H.

Solution de (1) : L'application φ_a est clairement bien définie sur G. Pour tous $x, y \in G$, on a

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

Donc φ_a est un endomorphisme. On vérifie que φ_a bijective.

$$\varphi_a(x) = \varphi_a(y) \Longrightarrow axa^{-1} = aya^{-1} \Longrightarrow x = a^{-1}(axa^{-1})a = a^{-1}(aya^{-1})a = y \Longrightarrow x = y,$$

d'où φ_a est injective. En plus, pour tous $y \in G$, on pose $x = a^{-1}ya$ et on voit que

$$\varphi_a(x) = axa^{-1} = aa^{-1}xa^{-1}a = y,$$

d'où la bijectivité de φ_a. Par conséquent, φ_a est bijective et, donc, φ_a est un automorphisme de G.

Solution de (2) : On vient de montrer que $H \subset \mathcal{S}(G)$. En plus, H est non-vide car $id_G = \varphi_e \in H$. Soit $\varphi_a, \varphi_b \in H$. Alors pour tous $x \in G$ on a

$$(\varphi_a \circ \varphi_b)(x) = \varphi_a(bxb^{-1}) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} == \varphi_{ab}(x),$$

donc $\varphi_a \circ \varphi_b = \varphi_{ab} \in H$, càd, H est stable par loi de composition. En plus, pour tout $\varphi_a \in H$, il n'est pas difficile de vérifier que $(\varphi_a)^{-1} = \varphi_{a^{-1}} \in H$ et donc H est stable par passage à l'inverse. Par conséquent, H est sous-groupe de $\mathcal{S}(G)$.

Solution de (3) : L'application $\Psi = G \to \mathcal{S}(G)$ est clairement bien définie. En plus, pour tous $a, b \in G$,

$$\Psi(ab) = \varphi_{ab} = \varphi_a \circ \varphi_b = \Psi(a) \circ \Psi(b),$$

donc Ψ est un morphisme du groupe G vers le groupe $\mathcal{S}(G)$.

Solution de (4) : On commence par montrer que $Z(G) \subset G$ est sous-groupe. Déjà, $Z(G)$ est non-vide car il contient au moins l'élément neutre e de G. Soit $x, y \in Z(G)$. Alors, pour tout $z \in G$,

$$z(xy) = (zx)y = (xz)y = x(zy) = x(yz) = (xy)z,$$

d'où $xy \in Z(G)$. Donc $Z(G)$ est stable par loi de composition. En plus, si $x \in Z(G)$, alors, pour tout $y \in G$,

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

d'où $x^{-1} \in Z(G)$. Donc $Z(G)$ est stable par passage à l'inverse et, par conséquent, $Z(G)$ est sous-groupe de G.

Maintenant, on montre que $G/Z(G)$ est un groupe isomorphe à H. Il n'est pas difficile de montrer que $G/Z(G)$ muni de $\bar{a}\bar{b} = \overline{ab}, a, b \in G$, est effectivement un groupe d'élément neutre $\bar{e}$. On définit

$$\begin{aligned} \Phi : G/Z(G) &\to H \\ \bar{a} &\mapsto \phi_a. \end{aligned}$$

Le premier pas c'est de montrer que Φ est une application bien définie, càd, que l'image ϕ_a de $\bar{a}$ par Φ ne dépend pas du choix du représentant de la classe d'équivalence $\bar{a}$. En effet, soit $b \in \bar{a}$ quelconque. On veut montrer que $\varphi_b = \varphi_a$. D'abord on note que, comme $b \in \bar{a}$, par définition on a $a^{-1}b \in Z(G)$ et donc $a^{-1}b$ commute avec tous les éléments de G. Soit $x \in G$ arbitraire, on obtient

$$\varphi_b(x) = bxb^{-1} = (aa^{-1})bxb^{-1} = a(a^{-1}b)xb^{-1} = ax(a^{-1}b)b^{-1} = axa^{-1} = \varphi_a(x),$$

donc $\varphi_b = \varphi_a$, ce qui monte que Φ est une application bien définie.

Ensuite, on voit que, pour tous $\bar{a}, \bar{b} \in G/Z(G)$,

$$\Phi(\bar{a}\bar{b}) = \Phi(\overline{ab}) = \varphi_{ab} = \varphi_a \circ \varphi_b = \Phi(\bar{a}) \circ \Phi(\bar{b}),$$

et donc Φ est un morphisme de groupes. On montre que Φ est injectif.

$$\begin{aligned} \bar{a} \in \ker \Phi &\Rightarrow \Phi(\bar{a}) = id_G \\ &\Rightarrow \varphi_a = id_G \\ &\Rightarrow \varphi_a(x) = x, \forall x \in G \\ &\Rightarrow axa^{-1} = x, \forall x \in G \\ &\Rightarrow ax = xa, \forall x \in G \\ &\Rightarrow a \in Z(G) \\ &\Rightarrow \bar{a} = \bar{e}, \end{aligned}$$

d'où $\ker \Phi = \{\bar{e}\}$ et donc Φ est injectif. En plus, Φ est clairement surjectif car pour tout $\varphi_a \in H$ on a $\Phi(\bar{a}) = \varphi_a$. Par conséquent, Φ est un isomorphisme de groupes.