Devoir libre $n°02$
Correction

N'hésitez pas de me signaler les erreurs rencontrées.

•••••••••

Exercice 1

1. (a) Le tableau suivant donne les valeurs de $\overline{3}^k$ pour $k \in \{0,1,2,3,4,5\}$.

k	0	1	2	3	4	5
$\overline{3}^k$	1	3	2	6	4	5

(b) Si $k \notin \{0,1,2,3,4,5\}$, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $k = 6q + r$ avec $r \in \{0,1,2,3,4,5\}$. Donc

$$3^k = 3^{6q+r} = \left(3^6\right)^q \times 3^r = 3^r.$$

2. 7 est premier donc $\left(\left(\mathbb{Z}/_{7\mathbb{Z}}\right)^*, \times\right)$ est un groupe.

3. D'après la première question le groupe engendré par 3 est $\{1,2,3,4,5,6\}$. C'est bien le même ensemble que $\left(\mathbb{Z}/_{7\mathbb{Z}}\right)^*$.

4. (a) Il faut vérifier que si $3^k = 3^l$ alors on a bien $\varphi\left(3^k\right) = \varphi\left(3^l\right)$. On a :

$$3^k = 3^l \longmapsto 3^{l-k} = 1 \Leftrightarrow \exists q \in \mathbb{Z} : l - k = 6q$$

La seconde égalité vient du fait que l'ordre de 3 est 6, d'après la première question, on obtient :

$$\varphi\left(3^l\right) = e^{\frac{il\pi}{3}}\varphi = e^{\frac{i(k+6q)\pi}{3}} = e^{2ik\pi}e^{\frac{ik\pi}{3}} = \varphi\left(3^k\right).$$

Il faut aussi vérifier que $\varphi\left(3^k\right)$, ce qui est exact car $\left(e^{\frac{ik\pi}{3}}\right)^6 = 1$.

φ est donc bien définie.

(b) Pour toutes classes a et b de $\left(\mathbb{Z}/_{7\mathbb{Z}}\right)^*$, il existe un unique $k \in \{0,1,2,3,4,5\}$ et un unique $l \in \{0,1,2,3,4,5\}$ tel que $a = 3^k$ et $b = 3^l$.

$$\varphi(a.b) = \varphi\left(3^k.3^l\right) = \varphi\left(3^{k+l}\right) = e^{\frac{i(k+l)\pi}{3}} = e^{\frac{ik\pi}{3}}e^{\frac{il\pi}{3}} = \varphi(a).\varphi(b).$$

φ est un morphisme de groupes.

(c) Soit $a \in \ker\varphi$, alors

$$\varphi(a) = 1 \Leftrightarrow \varphi\left(3^l\right) = 1 \Leftrightarrow e^{\frac{ik\pi}{3}} = 1 \Leftrightarrow \exists l \in \mathbb{Z} : \frac{k\pi}{3} = 2l\pi \Leftrightarrow \exists l \in \mathbb{Z},\ k = 6l.$$

Donc

$$a = 3^k = 3^{lk} = 1$$

le noyau de φ est réduit à l'élément neutre de $\left(\mathbb{Z}/_{p\mathbb{Z}}\right)^*$, ce qui montre que φ est injective, comme $\left(\mathbb{Z}/_{p\mathbb{Z}}\right)^*$ et $\mathbb{U}_6$ ont tous les deux 6 éléments est bijective.

Exercice 2

1. Soit O l'origine du plan complexe.
- ◇ r est la rotation de centre O et d'angle $\frac{\pi}{2}$.
- ◇ r^2 est la rotation de centre O et d'angle π.
- ◇ r^3 est la rotation de centre O et d'angle $\frac{3\pi}{2}$.
- ◇ s est la symétrie par rapport à l'axe horizontal.
- ◇ $s \circ r$ est la symétrie par rapport à la droite d'équation $y = -x$ (seconde bissectrice).
- ◇ $s \circ r^2$ est la symétrie par rapport à l'axe vertical.
- ◇ $s \circ r^3$ est la symétrie par rapport à la droite d'équation $y = x$ (première bissectrice).

2. Pour montrer que est un groupe, il suffit de vérifier que c'est un sous-groupe de l'ensemble $\mathscr{S}(\mathbb{C})$ des bijections du plan complexe dans lui-même. L'ensemble proposé est non vide. Observons ensuite que r et r^3 sont inverses l'un de l'autre, et que chacun des autres éléments de G est son propre inverse. La table de composition ci-dessous montre que le produit de deux éléments quelconques de G est encore dans G. Donc est un sous-groupe de $\mathscr{S}(\mathbb{C})$.

$\circ$	e	r	r^2	r^3	s	sr	sr^2	sr^3
e	e	r	r^2	r^3	s	sr	sr^2	sr^3
r	r	r^2	r^3	e	s^3	s	sr	sr^2
r^2	r^2	r^3	e	r	sr^2	sr^3	s	sr
r^3	r^3	e	r	r^2	sr	sr^2	sr^3	s
s	s	sr	sr^2	sr^3	e	r	r^2	r^3
sr	sr	sr^2	sr^3	s	r^3	e	r	r^2
sr^2	sr^2	r	sr^3	s	sr	r^3	e	r
sr^3	sr^3	s	sr	sr^2	r	r^2	r^3	e

3. Nous le montrons pour $\{e, r^2\}$, le raisonnement est identique pour les 4 autres. Dans la mesure où r^2 est son propre inverse, $\{e, r^2\}$ est bien un sous-groupe de G. L'application φ qui à e associe 0 et à r^2 associe 1 est une bijection, et c'est un morphisme pour la loi $\circ$ au départ, et pour l'addition modulo 2 à l'arrivée. Il suffit pour cela de s'assurer que les tables de composition correspondent.

$\circ$	e	r^2
e	e	r^2
r^2	r^2	e

$+$	0	1
0	0	1
1	1	0

Détaillons un peu, on a :

$$\varphi(e) = 0, \quad \varphi(r^2) = 1.$$
$$\varphi(r^2 \circ e) = \varphi(e \circ r^2) = \varphi(r^2) = 1.$$

Par conséquent

$$\varphi(r^2 \circ e) = 1 + 0 = \varphi(r^2) + \varphi(e).$$

Et

$$\varphi(e \circ r^2) = 0 + 1 = \varphi(e) + \varphi(r^2).$$

D'autre part,

$$\varphi(e \circ e) = \varphi(e) = 0 = 0 + 0 = \varphi(e) + \varphi(e).$$

Et

$$\varphi(r^2 \circ r^2) = \varphi(r^4) = \varphi(e) = 0 = 1 + 1 = \varphi(r^2) + \varphi(r^2).$$

Cela montre que pour tout $f, g \in \{e, r^2\}$, $\varphi(f \circ g) = \varphi(f) + \varphi(g)$, c'est bien la définition d'un morphisme de groupe.

4. Ici encore, le plus simple est de définir la bijection, puis de vérifier que c'est un morphisme pour les deux lois en comparant les tables de composition. Remarquons que l'existence d'un isomorphisme entre un sous-ensemble de G et un groupe connu, nous dispense de montrer que ce sous-ensemble est effectivement un sous-groupe. Comme bijection nous choisissons l'application , définie de $\{e, s, r^2, s \circ r^2\}$ dans $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$ par :

$$\varphi(e) = (0,0),\ \varphi(s) = (0,1),\ \varphi(r^2) = (1,0),\ \varphi(s \circ r^2) = (1,1).$$

$\circ$	e	s	r^2	sr^2
e	e	s	r^2	sr^2
s	s	e	sr^2	r^2
r^2	r^2	sr^2	e	s
sr^2	sr^2	r^2	s	e

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

5. Même technique, la bijection est définie par :

$$\varphi(e) = 0,\ \varphi(r) = 1,\ \varphi(r^2) = 2,\ \varphi(r^3) = 3.$$

$\circ$	e	r	r^2	r^3
e	e	r	r^2	r^3
r	r	r^2	r^3	e
r^2	r^2	r^3	e	r
r^3	r^3	e	r	r^2

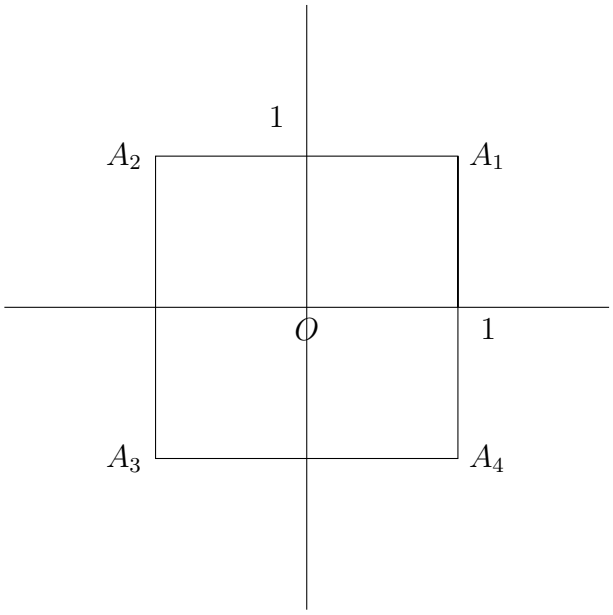
$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

6. Vérifions-le pour r et pour s.

$$r(A_1) = A_2,\ r(A_2) = A_3,\ r(A_3) = A_4,\ r(A_4) = A_1$$

$$s(A_1) = A_4,\ s(A_2) = A_3,\ r(A_3) = A_2,\ s(A_4) = A_1$$

C'est évident, il suffit de faire un dessin dans $\mathbb{R}^2$ et de placer les points A_i.
Puisque r et s laissent invariant l'ensemble $\{A_1, A_2, A_3, A_4\}$, c'est aussi le cas pour toute transformation du plan composée de r et s, donc pour tous les éléments du groupe G.



7. Soient f et g deux éléments du groupe G. Soient σ et τ les deux permutations de $\mathscr{S}_4$ telles que pour tout $i = 1, 2, 3, 4$:

$$f(A_i) = A_{\sigma(i)} \text{ et } g(A_i) = A_{\tau(i)}.$$

Alors, pour tout $i = 1, 2, 3, 4$.

$$f \circ g(A_i) = f(g(A_i)) = f(A_{\tau(i)}) = A_{\sigma(\tau(i))} = A_{\sigma\circ\tau(i)}.$$

Donc $\varphi(f\circ g) = \sigma\circ\tau = \varphi(f)\circ\varphi(g)$. Donc φ est un morphisme pour la composition des applications dans G au départ, et pour la composition des permutations à l'arrivée.

8. Voici le tableau donnant l'image par φ des éléments de G.

f	e	r	r^2	r^3	s	sr	sr^2	sr^3
$\varphi(f)$	$(1,2,3,4)$	$(2,3,4,1)$	$(3,4,1,2)$	$(4,1,2,3)$	$(4,3,2,1)$	$(3,2,1,4)$	$(2,1,4,3)$	$(1,4,3,2)$

C'est évident pour $\varphi(e)$, $\varphi(r)$ et $\varphi(s)$. On va plutôt utiliser les notations

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \text{ et } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Cherchons par exemple $\varphi(s \circ r)$, de même pour les autres. On a :

$$\varphi(s \circ r) = \varphi(s) \circ \varphi(r) = \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

9. Puisque φ est un morphisme, $H = \varphi(G)$ est un sous-groupe de $\mathscr{S}_4$. Le tableau de la question précédente liste tous les éléments de H, qui sont tous distincts. Donc $\varphi : G \to H = \varphi(G)$ est un isomorphisme.

●●●●●●●●●