Groupes, anneaux, corps

Exercice 1.

1. On munit $\mathbb{R}$ de la loi de composition interne $*$ définie par :
$$\forall x, y \in \mathbb{R}, \qquad x * y = xy + (x^2 - 1)(y^2 - 1)$$
Montrer que $*$ est commutative, non associative, et que 1 est élément neutre.
2. On munit $\mathbb{R}^{+*}$ de la loi de composition interne $*$ définie par :
$$\forall x, y \in \mathbb{R}^{+*}, \qquad x * y = \sqrt{x^2 + y^2}$$
Montrer que $*$ est commutative, associative, et que 0 est élément neutre. Montrer que aucun élément de $\mathbb{R}^{+*}$ n'a de symétrique pour $*$.
3. On munit $\mathbb{R}$ de la loi de composition interne $*$ définie par :
$$\forall x, y \in \mathbb{R}, \qquad x * y = \sqrt[3]{x^3 + y^3}$$
Montrer que l'application $x \mapsto x^3$ est un isomorphisme de $(\mathbb{R},*)$ vers $(\mathbb{R},+)$. En déduire que $(\mathbb{R},*)$ est un groupe commutatif.

Allez à : Correction exercice 1

Exercice 2.

Soit $G = \mathbb{R}^* \times \mathbb{R}$ et $*$ la loi dans G définie par $(x, y) * (x', y') = (xx', xy' + y)$

1. Montrer que $(G,*)$ est un groupe non commutatif
2. Montrer que $]0, +\infty[\times \mathbb{R},*)$ est un sous-groupe de $(G,*)$.

Allez à : Correction exercice 2

Exercice 3.

On munit $A = \mathbb{R} \times \mathbb{R}$ de deux lois définies par :
$$(x, y) + (x', y') = (x + x', y + y') \quad \text{et} \quad (x, y) * (x', y') = (xx', xy' + x'y)$$

1. Montrer que $(A, +)$ est un groupe commutatif.
2.
   a) Montrer que la loi $*$ est commutative.
   b) Montrer que $*$ est associative
   c) Déterminer l'élément neutre de A pour la loi $*$.
   d) Montrer que $(A, +,*)$ est un anneau commutatif.

Allez à : Correction exercice 3

Exercice 4.

On pose
$$id = (1,2,3,4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$
$$c_1 = (2,3,4,1) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$
$$\alpha = (3,4,1,2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$
$$c_2 = (4,1,2,3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$
Calculer, $c_1 \circ c_2$, $c_1 \circ c_1$, $c_1 \circ \alpha$, $c_2 \circ \alpha$.

Allez à : Correction exercice 4

Exercice 5.

Montrer que l'intersection de deux sous-groupes H et K de G est un sous-groupe de G.

Allez à : Correction exercice 5

Exercice 6.

Montrer que les ensembles $b\mathbb{Z}$ muni de l'addition sous des sous-groupes de $(\mathbb{Z},+)$

Allez à : Correction exercice 6

Exercice 7.

Soit $(G,*)$ un groupe, et soit e son élément neutre.

1. Soient $x,y \in G$, déterminer $(x*y)^{-1}$.
   On suppose que pour tout $g \in G$, $g^2 = g*g = e$
2. Soient $x,y \in G$, déterminer x^{-1} et y^{-1}.
3. En déduire que $(G,*)$ est commutatif.

Allez à : Correction exercice 7

Exercice 8.

Soit $G = \{e,\alpha,\beta,\gamma,\delta,\epsilon\}$ muni de la loi $*$ un groupe. Compléter sa table. On ne demande pas de justification.

e est l'élément neutre de G

$*$	e	α	β	γ	δ	ϵ
e						
α			δ			γ
β		ϵ		δ	γ	
γ		δ				
δ			α		ϵ	e
ϵ		β		α		

Allez à : Correction exercice 8

Exercice 9.

Montrer que $\mathcal{U} = \{z \in \mathbb{C}, |z| = 1\}$ muni de la multiplication est un sous-groupe de $(\mathbb{C}^*,\times)$.

Allez à : Correction exercice 9

Exercice 10.

Dresser les tables des groupes $(\mathbb{Z}/5\mathbb{Z},+)$ et $(\mathcal{U}_5,\times)$ où $\mathcal{U}_5 = \{z \in \mathbb{C}, z^5 = 1\}$ et montrer qu'il existe un isomorphisme entre ces deux groupes.

Pour simplifier les notations on pourra poser $\omega = e^{\frac{2i\pi}{5}}$ et exprimer les éléments de $\mathcal{U}_5$ en fonction des puissances de ω.

Allez à : Correction exercice 10

Exercice 11.

Soit $j = e^{\frac{2i\pi}{3}}$

Soit $\mathcal{U} = \{z \in \mathbb{C},\ z^6 = 1\}$

1. Montrer que U muni de la multiplication est un groupe.
2. Déterminer tous les éléments de $\mathcal{U}$, on les exprimera en fonction de j, puis déterminer les ordres possibles des éléments de $\mathcal{U}$, puis enfin déterminer l'ordre de chacun de ces éléments.
3. A l'aide de la question précédente, déterminer deux sous-groupes de $(\mathcal{U},\times)$, écrire leur table de multiplication.

Allez à : Correction exercice 11

Exercice 12.

1. Résoudre dans $\mathbb{C}$, l'équation $X^6 = 1$ (donner les solutions sous forme algébrique et trigonométrique), et exprimer ces solution en fonction de j.
2. Montrer que $\mathcal{U}_6 = \{z \in \mathbb{C}, z^6 = 1\}$ muni de la multiplication est un sous-groupe de $(\mathbb{C}^*,\times)$.
3. Déterminer les ordres possible des sous-groupes de $(\mathcal{U}_6,\times)$, en déduire tous les sous-groupes de $(\mathcal{U}_6,\times)$.

Allez à : Correction exercice 12

Exercice 13.

Soit $n \geq 3$.

On pose $\mathcal{U}_n = \left\{e^{\frac{2ik\pi}{n}}, k \in \{0,1,2,\dots,n-1\}\right\}$. Soit $\omega_{k_0} = e^{\frac{2ik_0\pi}{n}}$, avec $k_0 \geq 1$, et d_0 l'ordre de ω_{k_0}, on rappelle que d_0 est le plus petit entier non nul tel que $\omega_{k_0}^{d_0} = 1$.

1. Montrer que $(\mathcal{U}_n,\times)$ est un sous-groupe de $(\mathbb{C}^*,\times)$.
2.

a) En faisant la division euclidienne de $k_0 d_0$ par n montrer que $k_0 d_0$ est un multiple de n.

b) Montrer que si k_0 et n sont premiers entre eux alors l'ordre de ω_{k_0} est n.

3. Montrer que si $D = PGCD(n, k_0) > 1$ alors l'ordre de ω_{k_0} est strictement inférieur à n.
4. Que peut-on conclure à l'aide des questions 2°) et 3°).
   Montrer que si l'ordre de ω_{k_0} est n alors k_0 et n sont premiers entre eux. (On pourra montrer la contraposée)

Allez à : Correction exercice 13

Exercice 14.

Soit E l'ensemble des fonctions $f:]0,+\infty[\to]0,+\infty[$ telles qu'il existe $\alpha \in \mathbb{R}^*$ vérifiant :

$$\forall x \in]0,+\infty[, \quad f(x) = x^\alpha$$

1. Montrer que pour tout $\alpha \in \mathbb{R}^*$, f est une bijection de $]0,+\infty[$ sur $]0,+\infty[$.
2. Montrer que E muni de la loi de composition $\circ$ des fonctions est un groupe.

Allez à : Correction exercice 14

Exercice 15.

On sait que si n est un entier premier, $H_n = \{\overline{1}, \overline{2}, \dots, \overline{n-1}\}$ est un groupe pour la multiplication des classes.

1. Trouver deux entiers relatifs u et v tels que $8u + 29v = 1$.
2. En déduire le symétrique de $\overline{8}$ dans le groupe H_{29}.
3. Déterminer les $x \in \mathbb{Z}$ solutions de $8x \equiv 9 \mod 29$.

Allez à : Correction exercice 15

Exercice 16.

1. Existe-t-il un inverse pour la multiplication de $\overline{8}$ dans $(\mathbb{Z}/24\mathbb{Z})^*$.
2. Trouver tous les éléments de $(\mathbb{Z}/24\mathbb{Z})^*$ qui admettent un inverse dans $(\mathbb{Z}/24\mathbb{Z})^*$.
3. Trouver l'inverse pour la multiplication de la classe de 5 dans $(\mathbb{Z}/11\mathbb{Z})^*$.
4. Montrer que pour tous éléments de $(\mathbb{Z}/11\mathbb{Z})^*$, $x^9 = x^{-1}$, où x^{-1} désigne l'inverse de x pour la multiplication dans $(\mathbb{Z}/11\mathbb{Z})^*$.
5. En déduire les solutions de $x^9 + 5 = 0$.

Allez à : Correction exercice 16

Exercice 17.

On considère les groupes $\mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$ (pour l'addition). On notera $\bar{l}$ la classe de l'entier l dans $\mathbb{Z}/6\mathbb{Z}$ et $\hat{l}$ la classe de l'entier l dans $\mathbb{Z}/2\mathbb{Z}$.

1. Montrer que l'application $f: \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ définie par $f(\bar{l}) = \hat{l}$ est bien définie et que c'est un morphisme surjectif de groupes.
2. Déterminer le noyau $\ker(f)$ et dresser sa table de composition.
3. Construire un isomorphisme entre $\ker(f)$ et $\mathbb{Z}/3\mathbb{Z}$.

Allez à : Correction exercice 17

Exercice 18.

1. Montrer que l'application
$$f: \mathcal{U}_8 \to \mathcal{U}_2 : z \mapsto z^4$$
Est bien définie et que c'est un morphisme surjectif de groupes.
2. Déterminer le noyau $\ker(f)$ du morphisme f et dresser sa table de multiplication.
3. Expliciter un isomorphisme du groupe $\mathbb{Z}/4\mathbb{Z}$ pour l'addition sur le groupe $\ker(f)$.

Allez à : Correction exercice 18

Exercice 19.

On note $H = \{z \in \mathbb{C},\ z^8 = 1\}$, où $\mathbb{C}$ est l'ensemble des nombres complexes.

1. Montrer que $(H, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.
2. Pour $z_1 \in H$ et $z_2 \in H$ on pose $z_1 \sim z_2 \Leftrightarrow z_1^4 = z_2^4$.
Montrer que $\sim$ est une relation d'équivalence sur H.
3. Montrer que H admet deux classes d'équivalence.
Déterminer les éléments de ces deux classes d'équivalence.

Allez à : Correction exercice 19

Exercice 20.

Soit $n \in \mathbb{N}^*$; on note $U_n = \{z \in \mathbb{C},\ z^n = 1\}$.

1. Démontrer que c'est un sous-groupe de $\mathbb{C}^*$ pour la multiplication.
2. Montrer que si $n \in \mathbb{N}^*$, $m \in \mathbb{N}^*$ et n divise m alors $U_n \subseteq U_m$.
3. Montrer que si $d = PGCD(n, m)$ alors $U_d = U_n \cap U_m$.
4. Pour $n = 5$: on pose $f: \mathbb{Z} \to \mathbb{C}$ telle que $f(k) = e^{i\frac{2k\pi}{5}}$. Montrer que f est un morphisme du groupe additif $\mathbb{Z}$ dans le groupe multiplicatif U_5. Déterminer $\ker(f)$.

Allez à : Correction exercice 20

Exercice 21.

Pour tout $x \in \mathbb{Z}$, on appelle classe de x, notée $\overline{x}$, l'ensemble des entiers congrus à x modulo 7.

On appelle $\mathbb{Z}/7\mathbb{Z}$ l'ensemble des classe d'équivalence modulo 7 et $(\mathbb{Z}/7\mathbb{Z})^*$ l'ensemble des classes d'équivalence modulo 7 différentes de $\overline{0}$.

On appelle groupe engendré par $\overline{x}$ l'ensemble des puissances de $\overline{x}$, c'est-à-dire $\left\{\overline{x}^k, k \in \mathbb{Z}\right\}$

On appelle $\mathcal{U}_6 = \{z \in \mathbb{C}, z^6 = 1\}$ l'ensemble des racines sixième de l'unité.

1.
   a) Calculer $\overline{3}^k$ pour $k \in \{0,1,2,3,4,5\}$
   b) Déterminer $\overline{3}^k$ pour tout $k \in \mathbb{Z}$.
   On pourra utiliser la division euclidienne de k par 6.
2. Pour quelle raison $((\mathbb{Z}/7\mathbb{Z})^*, \times)$ est-il un groupe ?
3. Montrer que le groupe engendré par $\overline{3}$ est égal à $(\mathbb{Z}/7\mathbb{Z})^*$.

4. Soit φ définie pour tout $k \in \mathbb{Z}$ par
$$\varphi\left(\overline{3}^k\right) = e^{\frac{ik\pi}{3}}$$
   a) Montrer que φ est bien définie.
   b) Montrer que φ est un morphisme de $((\mathbb{Z}/7\mathbb{Z})^*, \times)$ sur $(\mathcal{U}_6, \times)$.
   c) Déterminer le noyau de φ et en déduire que φ est un isomorphisme (morphisme bijectif) de $((\mathbb{Z}/7\mathbb{Z})^*, \times)$ sur $(\mathcal{U}_6, \times)$.

Allez à : Correction exercice 21

Exercice 22.

Soit $(G, *)$ un groupe. Pour tout $g \in G$, on note γ_g l'application de multiplication à gauche par g, qui va de G dans G et associe $g * h$ à tout $h \in G$; autrement dit on a $\gamma_g(h) = g * h$ pour tous g et h dans G.

1. Prouver que pour $g \in G$, l'application γ_g est dans le groupe symétrique $\mathcal{S}_G$, autrement dit que γ_g est une bijection de G sur G.
2. Démontrer que l'application $\varphi: g \mapsto \gamma_g$ est un homomorphisme de groupe de $(G, *)$ dans $(\mathcal{S}_G, \circ)$.
3. Démontrer que l'application φ est injective.

   Pour tout $g \in G$, on note δ_g l'application de multiplication à droite par g, qui va de G dans G et associe $h * g$ à tout $h \in G$; autrement dit on a $\delta_g(h) = h * g$ pour tous g et h dans G.
4. Prouver que pour tout $g \in G$, l'application δ_g est dans le groupe symétrique $\mathcal{S}_G$, puis que l'application $\psi: g \mapsto \delta_g$ est une injection de G dans $\mathcal{S}_G$.
5. Démontrer que ψ est un homomorphisme de groupe si et seulement si le groupe G est abélien.

Allez à : Correction exercice 22

Exercice 23.

Soit $(G, *)$ un groupe d'élément neutre e.

1. Soit φ l'application de G dans G qui à tout élément $g \in G$ son inverse g^{-1}.
   Prouver que φ est un (homo)morphisme de groupe si et seulement si G est abélien.
2. Soit x un élément d'ordre fini m de G. Justifier que la partie $\{e, x, x^2, \dots, x^{m-1}\}$ est un sous-groupe de G.
3. On suppose maintenant que G est fini, de cardinal impair n. En utilisant le théorème de Lagrange, prouver que l'application ψ qui à g associe g^2 est surjective.
4. Donner une condition simple assurant que ψ est un (homo)morphisme de G vers G.

Allez à : Correction exercice 23

Exercice 24.

Soit $(G, *)$ un groupe. On considère le centre Z de G défini par :
$$Z = \{z \in G, \forall g \in G \quad z * g = g * z\}$$

1. Montrer que $(Z, *)$ est un sous-groupe de G.
2. Si G est un groupe commutatif, que vaut Z ?

Allez à : Correction exercice 24

Exercice 25.

Soit E l'ensemble des parties d'un ensemble à deux éléments, par exemple $E = \mathcal{P}(\{0,1\})$ donc
$$E = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$$
On considère les lois de composition $*$ suivantes sur l'ensemble E.

1. Réunion : $A * B = A \cup B$.
2. Intersection : $A * B = A \cap B$

3. Différence symétrique : $A * B = (A \setminus B) \cup (B \setminus A)$
4. Réunion des complémentaires : $A * B = \overline{A} \cup \overline{B}$
5. Intersection des complémentaires : $A * B = \overline{A} \cap \overline{B}$

Pour chacune d'entre elles :

a) Écrire la table de composition de la loi $*$.
b) L'ensemble E possède-t-il un élément neutre pour la loi $*$?
c) La loi $*$ est-elle associative ?
d) La loi $*$est-elle commutative ?
e) L'ensemble E muni de la loi $*$ est-il un groupe ?
f) Répondre aux questions 2 à 5 en remplaçant E par l'ensemble des parties d'un ensemble quelconque.

Allez à : Correction exercice 25

Exercice 26.

Le but de l'exercice est d'étudier les groupes à 1, 2, 3 ou 4 éléments.

1. Ecrire la table de composition d'un groupe à 1 élément.
2. Ecrire la table de composition d'un groupe à 2 éléments. Vérifier qu'il est isomorphe aux groupes suivants.
$$(\mathbb{Z}/2\mathbb{Z}, +)\ ;\ (\{-1,1\}, \times)\ ; \left(\left\{x \mapsto x, x \mapsto \frac{1}{x}\right\}, \circ\right)$$
3. Ecrire la table de composition d'un groupe à 3 éléments. Vérifier qu'il est isomorphe aux groupes suivants.
$$(\mathbb{Z}/3\mathbb{Z}, +)\ ;\ \left(\left\{1, e^{\frac{2i\pi}{3}}, e^{\frac{4i\pi}{3}}\right\}, \times\right);\ \ (\{(1,2,3),(2,3,1),(3,1,2)\}, \circ)$$
4. Soit $(\{e,a,b,c\}, *)$ un groupe à 4 éléments, d'élément neutre e.
   a) Montrer qu'il existe au moins un élément, autre que l'élément neutre, qui est son propre symétrique. On suppose désormais que b est son propre symétrique.
   b) On suppose $a * c = c * a = e$. Remplir la table de composition du groupe. Montrer qu'il est isomorphe aux groupes suivants.
   $$(\mathbb{Z}/4\mathbb{Z}, +)\ ; (\{1, i, -1, -i\}, \times); (\{(1,2,3,4),(2,3,4,1),(3,4,1,2),(4,1,2,3)\}, \circ)$$
   c) On suppose $a * a = c * c = e$. Remplir la table de composition du groupe. Montrer qu'il est isomorphe aux groupes suivants.
   $$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)\ ; (\{(1,2,3,4),(1,2,4,3),(2,1,3,4),(2,1,4,3)\}, \circ)$$
   d) Vérifier que l'on est toujours dans le cas de la question (4b) ou dans le cas de la question (4c).
5. Vérifier que tous les groupes de cet exercice sont abéliens.

Allez à : Correction exercice 26

Exercice 27.

On considère les éléments suivants de $\mathcal{S}_5$.
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix} \text{ et } \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$$
Calculer les puissances successives et déterminer l'ordre de σ et ρ, ainsi que de $\sigma\rho$, $\rho\sigma$, $\sigma\rho^{-1}$ et $\rho\sigma^{-1}$.

Allez à : Correction exercice 27

Exercice 28.

On considère un pentagone régulier : pour fixer les idées, l'ensemble des points du plan complexe dont des sommets ont pour affixes les racines cinquièmes de l'unité, soit
$$P = \left\{e^{\frac{2ik\pi}{5}}, k = 0,1,2,3,4\right\}$$
Le but de l'exercice est d'étudier le groupe (pour la composition des applications) des isométries du plan complexe qui laissent invariant ce pentagone. On notera ρ la rotation de centre l'origine et d'angle $\frac{2\pi}{5}$, et σ la symétrie qui à un nombre complexe associe son conjugué.
$$\rho : z \mapsto ze^{\frac{2i\pi}{5}};\quad \sigma : z \mapsto \overline{z}$$

1. Vérifier que σ et ρ laissent invariant l'ensemble P.

2. Vérifier que les puissances successives de ρ sont des rotations dont on donnera l'angle, et déterminer l'ordre de ρ.
3. Pour $n = 0,1,2,3,4$, montrer que $\sigma\rho^n$ et $\rho^n\sigma$ sont des symétries par rapport à un axe passant par l'origine, dont on donnera l'angle par rapport à l'axe réel.
4. Quel est l'ordre d'une symétrie ?
5. Montrer que le produit de deux des symétries de la question 3°) est une puissance de ρ.
6. Montrer que le plus petit groupe contenant ρ et σ possède 10 éléments.

Allez à : Correction exercice 28

Exercice 29.

1. Montrer que l'ordre de $\overline{1}$ dans $\mathbb{Z}/n\mathbb{Z}$ vaut n.
2. Montrer que l'ordre de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$ vaut n si et seulement si k est premier avec n.
3. Si k est un diviseur de n, montrer que l'ordre de $\overline{k}$ est le quotient de n par k.
4. Soit $(G,*)$ un groupe de cardinal n. On suppose que G contient un élément a d'ordre n. On note f l'application de $\mathbb{Z}/n\mathbb{Z}$ dans G qui à $\overline{0}$ associe l'élément neutre de G et à $\overline{k}$ associe la puissance k-ième de a dans G. Montrer que f est un isomorphisme de groupes.

Allez à : Correction exercice 29

Exercice 30.

$+$ est l'addition entre deux classes d'équivalence de $\mathbb{Z}/2\mathbb{Z}$

$\times$ est la multiplication entre deux classes d'équivalence de $\mathbb{Z}/2\mathbb{Z}$

1.
   a) Pourquoi $(\mathbb{Z}/2\mathbb{Z},+,\times)$ est-il un corps ?
   b) Donner la table d'addition de $\mathbb{Z}/2\mathbb{Z}$.
2. Soit $A = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

   On munit A d'une addition que l'on notera $\oplus$ définie par :

$$(\bar{a},\bar{b}) \oplus (\bar{c},\bar{d}) = (\bar{a}+\bar{c},\bar{b}+\bar{d})$$

   On munit A d'une multiplication que l'on notera $\otimes$ définie par :

$$(\bar{a},\bar{b}) \otimes (\bar{c},\bar{d}) = (\bar{a}\times\bar{c},\bar{b}\times\bar{d})$$

   a) Montrer que $(A,\oplus)$ est un groupe commutatif.
   b) Montrer que la multiplication est commutative.
   c) Montrer que la multiplication est une loi interne.
   d) Montrer que la multiplication est distributive sur l'addition
   e) Montrer que A possède un élément neutre pour la multiplication.
   f) $(A,\oplus,\otimes)$ est-il un anneau commutatif unitaire, un corps ?

Allez à : Correction exercice 30

Exercice 31.

1. Soit S un ensemble quelconque et $E = \{0,1\}^S$ l'ensemble des applications de S dans $\{0,1\}$. On munit E de l'addition modulo 2 des images : pour tout $f, g \in E$, $f \oplus g$ est l'application de S dans $\{0,1\}$ définie par :

$$(f \oplus g)(x) = \begin{cases} 1 & \text{si } f(x) \neq g(x) \\ 0 & \text{si } f(x) = g(x) \end{cases}$$

   Montrer que $(E,\oplus)$ est un groupe abélien, dans lequel chaque élément est son propre symétrique.
2. Soit $F = \mathcal{P}(S)$ l'ensemble des parties de S. On munit F de la différence symétrique ensembliste. On considère l'application ϕ, de F dans E qui, à une partie de S, associe sa fonction indicatrice :

$$\phi : A \in \mathcal{P}(S) \mapsto \mathbb{I}_A$$

   où pour tout $x \in S, \mathbb{I}_A(x) = 1$ si $x \in A$ et $\mathbb{I}_A(x) = 0$ sinon.
   Montrer que ϕ est un isomorphisme de F vers E, pour les lois Δ et $\oplus$. En déduire que (F,Δ) est un groupe

abélien, dans lequel chaque élément est son propre symétrique.
Dans toute la suite, G désigne un groupe dans lequel chaque élément est son propre symétrique.

3. Montrer que G est abélien.
4. Soit a un élément quelconque de G, différent de l'élément neutre. On définit la relation $\sim$ sur G par :
$$\forall x, y \in G, \qquad x \sim y \Leftrightarrow (x = y \text{ ou } x = ay)$$
Montrer que $\sim$ est une relation d'équivalence sur G. Montrer que chaque classe d'équivalence a deux éléments.
5. On définit la loi $*$ sur l'ensemble-quotient $G/\sim$ par :
$$\forall x, y \in G, \quad \text{cl}(x) * \text{cl}(y) = \text{cl}(xy)$$
Montrer que $*$ est une loi de composition interne sur $G/\sim$, et que $G/\sim$ muni de $*$ est un groupe abélien, dans lequel chaque élément est son propre symétrique.
6. On suppose que G est fini. Déduire des questions précédentes que le cardinal de G est une puissance de 2.

Allez à : Correction exercice 31

Exercice 32.

On considère les applications suivantes, de $\mathbb{R} \setminus \{0, 1\}$ dans lui-même.
$$f_1 : x \mapsto x; \quad f_2 : x \mapsto 1 - x; \quad f_3 : x \mapsto \frac{1}{1-x}; \quad f_4 : x \mapsto \frac{1}{x}; \quad f_5 : x \mapsto \frac{x}{x-1}; \quad f_6 : x \mapsto \frac{x-1}{x}$$
On munit l'ensemble $E = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ de la composition des applications.

1. Écrire la table de composition de $(E, \circ)$
2. Montrer que $G = (E, \circ)$ est un groupe.
3. Est-ce un groupe abélien ?
4. Déterminer tous les sous-groupes de G.
5. Déterminer l'ordre de chacun des éléments de G.
6. Quels sont les éléments de $< f_2 >$?
7. Quels sont les éléments de $< f_3 >$?

Allez à : Correction exercice 32

Exercice 33.

Soient $(E, *)$ et $(F, .)$ deux groupes. On munit l'ensemble produit $E \times F$ de la loi de composition $\odot$ définie par :
$$\forall (x, y), (x', y') \in E \times F, \qquad (x, y) \odot (x', y') = (x * x', y . y')$$

1. Montrer que $(E \times F, \odot)$ est un groupe.
2. Soit E' un sous-groupe de E, F' un sous-groupe de F. Montrer que $E' \times F'$ est un sous-groupe de $E \times F$, muni de la loi $\odot$.

Allez à : Correction exercice 33

Exercice 34.

Montrer que les ensembles suivants d'applications de $\mathbb{C}$ dans $\mathbb{C}$, munis de la loi de composition des applications, sont des groupes.

1. $E_1 = \{z \mapsto z + t, t \in \mathbb{Z}\}$
2. $E_2 = \{z \mapsto z + t, t \in \mathbb{C}\}$
3. $E_3 = \{z \mapsto e^{i\theta} z, \theta \in \mathbb{R}\}$
4. $E_4 = \{z \mapsto sz + t, (s, t) \in \mathbb{C}^* \times \mathbb{C}\}$

Allez à : Correction exercice 34

Exercice 35.

Soit G un sous-groupe additif de $\mathbb{R}^*$. On supppose que $G \neq \{0\}$.

1. Montrer que $G \cap \mathbb{R}^{+*}$ possède une borne inférieure, que l'on notera b.
2. Montrer que $b \in G$.
3. On suppose $b > 0$. Montrer que $G = b\mathbb{Z}$.

4. On suppose $b = 0$. Montrer que si x et y sont deux réels tels que $x < y$, l'intervalle $]x, y[$ contient au moins un élément de G (on dit que G est dense dans $\mathbb{R}$).
5. Montrer que l'ensemble $\{m + n\sqrt{2}\,, (n, m) \in \mathbb{Z}^2\}$ muni de l'addition est un sous-groupe de $(\mathbb{R}, +)$, et qu'il est dense dans $\mathbb{R}$ (on rappelle que $\sqrt{2}$ est irrationnel).

Allez à : Correction exercice 35

Exercice 36.

Soit $\mathbb{K}$ l'ensemble des complexes de la forme $z = r + is$ où $r \in \mathbb{Q}$ et $s \in \mathbb{Q}$.

1. Montrer que $(\mathbb{K}, +)$ est un groupe commutatif.
2. Montrer que $(\mathbb{K}^*, .)$ est un groupe commutatif.
3. En déduire que $(\mathbb{K}, +, .)$ est un corps commutatif.

Allez à : Correction exercice 36

Exercice 37.

On note $\mathbb{Z}[\sqrt{2}\,]$ l'ensemble de réels suivant :

$$\mathbb{Z}[\sqrt{2}\,] = \{m + n\sqrt{2}, m, n \in \mathbb{Z}\}$$

1. Montrer que $\mathbb{Z}[\sqrt{2}\,]$, muni de l'addition et de la multiplication des réels, est un sous-anneau de $\mathbb{R}$.
2. On considère l'application ϕ, de $\mathbb{Z}[\sqrt{2}\,]$ dans lui-même, qui à $m + n\sqrt{2}$ associe
$$\phi(m + n\sqrt{2}) = m - n\sqrt{2}$$
Montrer que ϕ est un automorphisme de l'anneau $(\mathbb{Z}[\sqrt{2}\,], +, \times)$ (c'est une bijection, et un morphisme pour chacune des deux lois).
3. Pour tout $x \in \mathbb{Z}[\sqrt{2}\,]$, on pose $N(x) = x\phi(x)$. Montrer que N est une application de $\mathbb{Z}[\sqrt{2}\,]$ dans $\mathbb{Z}$, qui est un morphisme pour la multiplication.
4. Démontrer que x est un élément inversible de $\mathbb{Z}[\sqrt{2}\,]$ si et seulement si $N(x) = \pm 1$.
5. Vérifier que $3 + 2\sqrt{2}$ et $-3 + 2\sqrt{2}$ sont inversibles dans $\mathbb{Z}[\sqrt{2}\,]$.

Allez à : Correction exercice 37

Exercice 38.

Soient r et s les applications de $\mathbb{C}$ dans lui-même définies comme suit.

$$r: \begin{matrix}\mathbb{C} \to \mathbb{C} \\ z \mapsto iz\end{matrix} \quad ; \quad s: \begin{matrix}\mathbb{C} \to \mathbb{C} \\ z \mapsto \overline{z}\end{matrix}$$

Dans tout l'exercice, on identifiera l'application f de $\mathbb{C}$ dans $\mathbb{C}$, avec l'application du plan complexe dans lui-même, qui à un point M d'affixe z associe le point M' d'affixe $f(z)$.

1. On note r_2 et r_3 les composées $r^2 = r \circ r$ et $r^3 = r \circ r \circ r$. Interpréter comme transformations géométriques du plan complexe les applications r, r^2, r^3, s, $s \circ r$, $s \circ r^2$ et $s \circ r^3$.
2. On note e l'application identité du plan complexe. Montrer que l'ensemble,
$$\{e, r, r^2, r^3, s, s \circ r, s \circ r^2, s \circ r^3\}$$
muni de la composition des applications est un groupe, dont on donnera la table de composition. Il sera noté G.
3. Montrer que $\{e, r^2\}$, $\{e, s\}$, $\{e, s \circ r\}$, $\{e, s \circ r^2\}$, $\{e, s \circ r^3\}$, sont des sous-groupes de G, tous isomorphes à $\mathbb{Z}/2\mathbb{Z}$.
4. Montrer que $\{e, s, r^2, s \circ r^2\}$ est un sous-groupe de G, isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
5. Montrer que $\{e, r, r^2, r^3\}$ est un sous-groupe de G, isomorphe à $\mathbb{Z}/4\mathbb{Z}$.
6. On note :
A_1 le point du plan complexe d'affixe $1 + i$,
A_2 le point du plan complexe d'affixe $-1 + i$,
A_3 le point du plan complexe d'affixe $-1 - i$,
A_4 le point du plan complexe d'affixe $1 - i$,
Vérifier que chaque élément du groupe G laisse invariant l'ensemble $\{A_1, A_2, A_3, A_4\}$
7. Étant donné un élément f du groupe G, on lui associe la permutation $\varphi(f)$ de $\{1, 2, 3, 4\}$ définie par :

$$\forall i,j \in \{1,2,3,4\}, \varphi(f)(i) = j \Leftrightarrow f(A_i) = A_j$$

On définit ainsi une application φ de G dans $\mathcal{S}_4$. Montrer que φ est un morphisme de groupes.

8. Écrire in extenso l'image par φ de chacun des éléments de G.
9. Soit H l'image de G par φ. Montrer que H est un sous-groupe de$\mathcal{S}_4$, isomorphe à G.

Allez à : Correction exercice 38

Exercice 39.

On note A l'ensemble de réels suivant :

$$A = \{m + n\sqrt{6}, m, n \in \mathbb{Z}\}$$

1. Montrer que $(A, +, \times)$ (ensemble A muni de l'addition et de la multiplication des réels), est un sous-anneau de $(R, +, \times)$.
2. On considère l'application φ, de A dans lui-même, qui à $m + n\sqrt{6}$ associe :
$$\varphi(m + n\sqrt{6}) = m - n\sqrt{6}$$
Montrer que φ est un automorphisme de l'anneau $(A, +, \times)$ (c'est-à-dire une bijection, et un morphisme pour chacune des deux lois).
3. Pour tout $x \in A$, on pose $N(x) = x\varphi(x)$. Montrer que N est une application de A dans $\mathbb{Z}$, qui est un morphisme pour la multiplication.
4. Démontrer que x est un élément inversible de A si et seulement si $N(x) = \pm 1$.
5. Vérifier que $5 + 2\sqrt{6}$ est inversible dans A et calculer son inverse.

Allez à : Correction exercice 39

CORRECTION

Correction exercice 1.

1.
$$x * y = xy + (x^2 - 1)(y^2 - 1) = yx + (y^2 - 1)(x^2 - 1) = y * x$$
La loi $*$ est commutative
Pour montrer que la loi n'est pas associative, il suffit de trouver x, y et z tels que :
$$x * (y * z) \neq (x * y) * z$$
Comme on le verra ci-dessous, 1 sera l'élément neutre il ne faut pas prendre 1 dans x, y et z.
Prenons, par exemple : $x = 0$, $y = 2$ et $z = 3$
$$x * (y * z) = 0 * (2 * 3) = 0 * \left(2 \times 3 + (2^2 - 1)(3^2 - 1)\right) = 0 * (6 + 3 \times 8) = 0 * 30$$
$$= 0 \times 30 + (0^2 - 1)(30^2 - 1) = -899$$
$$(x * y) * z = (0 * 2) * 3 = \left(0 \times 2 + (0^2 - 1)(2^2 - 1)\right) * 3 = (-3) * 3$$
$$= -3 \times 3 + ((-3)^2 - 1)(3^2 - 1) = -9 + 8^2 = 55$$
La loi $*$ n'est pas associative
$$1 * x = 1 \times x + (1^2 - 1)(x^2 - 1) = x$$
De plus, comme la loi est commutative $x * 1 = 1 * x$
On a bien $x * 1 = 1 * x = x$, 1 est l'élément neutre.

2.
$$x * y = \sqrt{x^2 + y^2} = \sqrt{y^2 + x^2} = y * x$$
La loi $*$ est commutative.
$$(x * y) * z = \sqrt{x^2 + y^2} * z = \sqrt{\left(\sqrt{x^2 + y^2}\right)^2 + z^2} = \sqrt{x^2 + y^2 + z^2}$$
En reprenant le calcul ci-dessus en changeant (x, y, z) en (y, z, x) :
$$(y * z) * x = \sqrt{y^2 + z^2 + x^2}$$
Comme $*$ est commutative :
$$(y * z) * x = x * (y * z)$$
Et finalement :
$$(x * y) * z = x * (y * z)$$
La loi $*$ est associative.
Remarque : On aurait pu calculer directement $x * (y * z)$

$$0 * x = \sqrt{0^2 + x^2} = |x| = x, \quad \text{car } x \geq 0$$

Comme $*$ est commutative

$$0 * x = x * 0$$

Et finalement

$$0 * x = x * 0 = x$$

0 est l'élément neutre.

Supposons que x admette un symétrique y

$$x * y = 0 \Leftrightarrow \sqrt{x^2 + y^2} = 0 \Leftrightarrow x^2 + y^2 = 0 \Leftrightarrow x = y = 0$$

Or $x > 0$ et $y > 0$ donc $x * y = 0$ est impossible, pour tout $x > 0$, x n'a pas de symétrique.

3. On pose $\varphi(x) = x^3$, $\varphi'(x) > 0$ pour tout $x \neq 0$ et est nul en 0, φ est une fonction strictement croissante de $\mathbb{R}$ sur $\mathbb{R}$, φ est une bijection de $\mathbb{R}$ sur $\mathbb{R}$. Il reste à montrer qu'il s'agit d'un morphisme.

$$\varphi(x * y) = (x * y)^3 = \left(\sqrt[3]{x^3 + y^3}\right)^3 = x^3 + y^3 = \varphi(x) + \varphi(y)$$

φ est un morphisme de $(\mathbb{R},*)$ dans $(\mathbb{R},+)$ et donc un isomorphisme de $(\mathbb{R},*)$ dans $(\mathbb{R},+)$ (puisque φ est bijective).

φ^{-1} est un isomorphisme de $(\mathbb{R},+)$ dans $(\mathbb{R},*)$, donc un morphisme, $(\mathbb{R},+)$ est un groupe commutatif et l'image d'un groupe commutatif par un morphisme de groupe est un groupe. $(\mathbb{R},*)$ est un groupe.

Allez à : Exercice 1

Correction exercice 2.

1. Si $x \neq 0$ et $x' \neq 0$ alors $xx' \neq 0$ donc $(x,y) * (x',y') = (xx', xy' + y) \in \mathbb{R}^* \times \mathbb{R}$.

   La loi $*$ est une loi interne.

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

   Et

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

   Donc la loi $*$ est associative.

   Soit (a,b) tel que pour tout $(x,y) \in G$:

$$(a,b) * (x,y) = (x,y) = (x,y) * (a,b)$$

   Ces égalités équivalent à :

$$(ax, ay + b) = (x,y) = (xa, xb + y) \Leftrightarrow \begin{cases} ax = x = xa \\ ay + b = y = xb + y \end{cases} \Leftrightarrow \begin{cases} a = 1 \\ b = 0 \end{cases}$$

   Donc $(1,0)$ est l'élément neutre.

   Soit $(x,y) \in G$, on cherche (x',y') tel que $(x,y) * (x',y') = (1,0) = (x',y') * (x,y)$

   Ces égalités équivalent à :

$$(xx', xy' + y) = (1,0) = (x'x, x'y + y') \Leftrightarrow \begin{cases} xx' = 1 = x'x \\ xy' + y = 0 = x'y + y' \end{cases} \Leftrightarrow \begin{cases} x' = \dfrac{1}{x} \\ xy' + y = 0 = \dfrac{1}{x}y + y' \end{cases}$$

$$\Leftrightarrow \begin{cases} x' = \dfrac{1}{x} \neq 0 \\ y' = -\dfrac{y}{x} \end{cases}$$

   Le symétrique de (x,y) est $\left(\frac{1}{x}, -\frac{y}{x}\right)$.

   Donc $(G,*)$ est un groupe.

   Comme $(1,2) * (2,0) = (2,2)$ et que $(2,0) * (1,2) = (2,4)$ il est clair que ce groupe n'est pas commutatif.

2. L'élément neutre de $(G,*)$, $(1,0) \in]0,+\infty[\times \mathbb{R}$.

   Soit $(x,y) \in]0,+\infty[\times \mathbb{R}$ et $(x',y') \in]0,+\infty[\times \mathbb{R}$. Alors

$$(x,y)*\left(\frac{1}{x'},-\frac{y'}{x'}\right)=\left(\frac{x}{x'},x\left(-\frac{y'}{x'}\right)+y\right)=\left(\frac{x}{x'},\frac{-xy'+x'y}{x'}\right)$$

Comme $\frac{x}{x'}>0$ alors $\left(\frac{x}{x'},\frac{-xy'+x'y}{x'}\right)\in]0,+\infty[\times\mathbb{R}$.

Donc $(]0,+\infty[\times\mathbb{R},*)$ est un sous-groupe de $(G,*)$.

Allez à : Exercice 2

Correction exercice 3.

1. $(x,y)+(x',y')=(x+x',y+y')\in A$ donc la loi est interne.

$$(x,y)+[(x',y')+(x'',y'')]=(x,y)+(x'+x'',y'+y'')=\big(x+(x'+x''),y+(y'+y'')\big)$$
$$=\big((x+x')+x'',(y+y')+y''\big)=[(x,y)+(x',y')]+(x'',y'')$$

Donc la loi $+$ est associative.

$$(x,y)+(x',y')=(x+x',y+y')=(x'+x,y'+y)=(x',y')+(x,y)$$

Donc la loi $+$ est commutative

Soit (a,b) tel que $(x,y)+(a,b)=(x,y)$, il est clair que $(a,b)=(0,0)$ est l'unique élément neutre.

Soit (x',y') tel que $(x,y)+(x',y')=(0,0)$ cela équivaut à

$$(x+x',y+y')=(0,0)\Leftrightarrow\begin{cases}x+x'=0\\y+y'=0\end{cases}\Leftrightarrow\begin{cases}x'=-x\\y'=-y\end{cases}$$

Donc le symétrique de (x,y) est $(-x,-y)$.

Donc $(A,+)$ est un groupe commutatif.

2.

a) $(x,y)*(x',y')=(xx',xy'+x'y)=(x'x,x'y+xy')=(x',y')*(x,y)$ donc $*$ est commutative.

b)

$$[(x,y)*(x',y')]*(x'',y'')=(xx',xy'+x'y)*(x'',y'')=\big(xx'x'',xx'y''+x''(xy'+x'y)\big)$$
$$=(xx'x'',xx'y''+x''xy'+x''x'y)$$
$$(x,y)*[(x',y')*(x'',y'')]=(x,y)*(x'x'',x'y''+x''y')=(xx'x'',x(x'y''+x''y')+x'x''y)$$
$$=(xx'x'',xx'y''+xx''y'+x'x''y)$$

Donc $[(x,y)*(x',y')]*(x'',y'')=(x,y)*[(x',y')*(x'',y'')]$

La loi $*$ est associative.

c) Soit (e,f) tel que pour tout $(x,y)\in A$, $(x,y)*(e,f)=(x,y)$, e et f vérifient :

$$\begin{cases}xe=x\\xf+ye=y\end{cases}\Leftrightarrow\begin{cases}e=1\\xf+y=y\end{cases}\Leftrightarrow\begin{cases}e=1\\f=0\end{cases}$$

$(1,0)\in A$ est l'élément neutre de A pour la loi $*$.

d) Toutes les propriétés pour qu'un ensemble muni de deux lois soit un anneau sont dans les questions précédentes sauf la distributivité de $*$ par rapport à l'addition (à gauche ou à droite puisque la loi $*$ est commutative, c'est d'ailleurs cette commutativité qui rend l'anneau commutatif).

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

Et voilà, $(A,+,*)$ est un anneau commutatif.

Allez à : Exercice 3

Correction exercice 4.

$$c_1\circ c_2=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\circ\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&1&2&3\\1&2&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=id$$

$$c_1 \circ c_1 = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} \circ \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} = \begin{pmatrix}1&2&3&4\\2&3&4&1\\3&4&1&2\end{pmatrix} = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} = \alpha$$

$$c_1 \circ \alpha = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} \circ \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} = \begin{pmatrix}1&2&3&4\\3&4&1&2\\4&1&2&3\end{pmatrix} = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix} = c_2$$

$$c_2 \circ \alpha = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix} \circ \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} = \begin{pmatrix}1&2&3&4\\3&4&1&2\\2&3&4&1\end{pmatrix} = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} = c_1$$

Allez à : Exercice 4

Correction exercice 5.

$e \in H$ et $e \in K$ donc $e \in H \cap K$.

Soient $a \in H \cap K$ et $b \in H \cap K$.

$a * b^{-1} \in H$, car H est un sous-groupe de G et $a * b^{-1} \in K$, car K est un sous-groupe de G donc

$$a * b^{-1} \in H \cap K$$

Cela montre que $H \cap K$ est un sous-groupe de G.

Allez à : Exercice 5

Correction exercice 6.

Vérifions que les $b\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$.

$0 = b \times 0 \in b\mathbb{Z}$.

Si $x \in b\mathbb{Z}$ et $y \in b$, il existe $k \in \mathbb{Z}$ tel que $x = kb$ et $l \in \mathbb{Z}$ tel que $y = lb$, on en déduit que

$$x - y = (k - l)b \in \mathbb{Z}$$

donc $b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Allez à : Exercice 6

Correction exercice 7.

1. $(x * y)^{-1} = y^{-1} * x^{-1}$
2. $x * x = e \Rightarrow x^{-1} = x$ de même $y^{-1} = y$.
3. $x * y = (x * y)^{-1} = y^{-1} * x^{-1}$ d'après 1°), puis $x * y = y * x$ d'après 2.

Allez à : Exercice 7

Correction exercice 8.

$\circ$	e	α	β	γ	δ	ϵ
e	e	α	β	γ	δ	ϵ
α	α	e	δ	ϵ	β	γ
β	β	ϵ	e	δ	γ	α
γ	γ	δ	ϵ	e	α	β
δ	δ	γ	α	β	ϵ	e
ϵ	ϵ	β	γ	α	e	δ

Allez à : Exercice 8

Correction exercice 9.

$|1| = 1$ donc $1 \in \mathcal{U}$, soient $z_1 \in \mathcal{U}$ et $z_2 \in \mathcal{U}$ donc $|z_1| = 1$ et $|z_2| = 1$

$$|z_1 z_2^{-1}| = \left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|} = \frac{1}{1} = 1$$

donc $z_1 z_2^{-1} \in \mathcal{U}$, $(\mathcal{U},\times)$ est un sous-groupe de $(\mathbb{C}^*,\times)$.

Allez à : Exercice 9

Correction exercice 10.

$$z \in \mathcal{U}_5 \Leftrightarrow \exists k \in \{0,1,2,3,4\}, z = e^{\frac{2ik\pi}{5}} = \omega^k$$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\times$	1	ω	ω^2	ω^3	ω^4
1	1	ω	ω^2	ω^3	ω^4
ω	ω	ω^2	ω^3	ω^4	1
ω^2	ω^2	ω^3	ω^4	1	ω
ω^3	ω^3	ω^4	1	ω	ω^2
ω^4	ω^4	1	ω	ω^2	ω^3

Pour tout $k \in \{0,1,2,3,4\}$ on pose $\varphi(\overline{k}) = \omega^k$, il s'agit évidemment d'une bijection, de plus la place de $\overline{k}$ dans la table de $(\mathbb{Z}/5\mathbb{Z},+)$ est la même que celle de $\omega^k = \varphi(\overline{k})$ dans la table de $(\mathcal{U}_5,\times)$ donc il s'agit d'un morphisme, finalement φ est un isomorphisme de $(\mathbb{Z}/5\mathbb{Z},+)$ sur $(\mathcal{U}_5,\times)$.

Allez à : Exercice 10

Correction exercice 11.

1. Montrons que $\mathcal{U}$ est un sous-groupe de $\mathbb{C}^*$.
   $1^6 = 1$ donc l'élément neutre de $\mathbb{C}^*$ appartient à $\mathcal{U}$.
   Soient z_1 et z_2 deux éléments de $\mathcal{U}$, $(z_1 z_2^{-1})^6 = \left(\frac{z_1}{z_2}\right)^6 = \frac{z_1^6}{z_2^6} = \frac{1}{1} = 1$ donc $z_1 z_2^{-1} \in \mathcal{U}$.
   $\mathcal{U}$ est un sous-groupe de $\mathbb{C}$.
2. $z \in \mathcal{U} \Leftrightarrow \exists k \in \{0,1,2,3,4,5\}, z = e^{\frac{2ik\pi}{6}} = e^{\frac{ik\pi}{3}}$, $\mathcal{U} = \{1, -j^2, j, -1, j^2, -j\}$
   L'ordre d'un élément de $\mathcal{U}$ divise $Card(\mathcal{U}) = 6$, il vaut 1,2,3 ou 6.
   L'ordre de 1 est 1.
   L'ordre de $-j^2$ est 6, car $(-j^2)^2 = j \neq 1$, $(-j^2)^3 = -j^6 = -1 \neq 1$, son ordre est donc 6.
   L'ordre de j est 3.
   L'ordre de -1 est 2.
   L'ordre de j^2 est 3, car $(j^2)^2 = j^4 = j \neq 1$ et $(j^2)^3 = j^6 = 1$.
   L'ordre de $-j$ est 6, car $(-j)^2 = j^2 \neq 1$, $(-j)^3 = -j^3 = -1 \neq 1$, son ordre est donc 6.
3. $\mathcal{H}_1 = \{-1,1\}$ est un sous-groupe de $\mathcal{U}$ d'ordre 2.
   $\mathcal{H}_2 = \{1, j, j^2\}$ est un sous-groupe d'ordre 3.

$\times$	1	-1
1	1	-1
-1	-1	1

$\times$	1	j	j^2
1	1	j	j^2
j	j	j^2	1
j^2	j^2	1	j

Allez à : Exercice 11

Correction exercice 12.

1. $X_k = e^{\frac{2ik\pi}{6}} = e^{\frac{ik\pi}{3}}$ avec $k \in \{0,1,2,3,4,5\}$
   $X_0 = 1, X_1 = e^{\frac{i\pi}{3}} = \frac{1}{2} + i\frac{\sqrt{3}}{2} = -j^2, X_2 = e^{\frac{2i\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = j, X_3 = e^{\frac{3i\pi}{3}} = e^{i\pi} = -1,$
   $X_4 = e^{\frac{4i\pi}{3}} = -\frac{1}{2} - i\frac{\sqrt{3}}{2} = j^2, X_5 = e^{\frac{5i\pi}{3}} = \frac{1}{2} - i\frac{\sqrt{3}}{2} = -j.$
2. $1^6 = 1$ donc $1 \in \mathcal{U}_6$
   Soient $z_1 \in \mathcal{U}_6$ et $z_2 \in \mathcal{U}_6$, $z_1^6 = 1$ et $z_2^6 = 1$
   $(z_1 z_2^{-1})^6 = \left(\frac{z_1}{z_2}\right)^6 = \frac{z_1^6}{z_2^6} = \frac{1}{1} = 1$ donc $z_1 z_2^{-1} \in \mathcal{U}_6$.
   $(\mathcal{U}_6, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.
3. L'ordre des sous-groupes de $(\mathcal{U}_6, \times)$ divise l'ordre de $(\mathcal{U}_6, \times)$, c'est-à-dire le nombre d'éléments de $\mathcal{U}_6$, soit 6. L'ordre des sous-groupes des $(\mathcal{U}_6, \times)$ sont d'ordre 1,2,3 ou 6.
   Il y a un sous-groupe d'ordre 1 : $\{1\}$.
   Il y a un sous-groupe d'ordre 6 : $\{1, -j^2, j, -1, j^2, -j\} = \mathcal{U}_6$.
   Dans les sous-groupes d'ordre 2, il y a forcément 1 et un élément d'ordre 2, parmi $\{-j^2, j, -1, j^2, -j\}$ il n'y a que -1 qui soit d'ordre 2, il n'y a qu'un sous-groupe d'ordre 2 : $\{1, -1\}$.
   Dans les sous-groupes d'ordre 3, il y a forcément 1 et deux éléments dont l'ordre divise 3, ce sont donc des éléments d'ordre 3.
   j est d'ordre 3 (car $j^3 = 1$), le troisième éléments du sous-groupe est $j^{-1} = j^2$, $\{1, j, j^2\}$ est un sous-groupe d'ordre 3 de $(\mathcal{U}_6, \times)$.
   j^2 est aussi un élément d'ordre 3 (car $(j^2)^3 = j^6 = (j^3)^2 = 1^2 = 1$), le troisième élément est j, on retombe sur le cas précédent.
   $-j^2$ n'est pas d'ordre 3 car $(-j^2)^3 = -j^6 = -1 \neq 1$. $-j$ n'est pas d'ordre 3 car $(-j)^3 = -j^3 = -1 \neq 1$, -1 est d'ordre 2, donc n'est pas d'ordre 3. Il n'y a pas d'autre sous-groupe d'ordre 3.

Allez à : Exercice 12

Correction exercice 13.

1. $\mathcal{U}_n = \{z \in \mathbb{C}, z^n = 1\}$, $1^n = 1$ donc $1 \in \mathcal{U}_n$, si $z_1 \in \mathcal{U}_n$ et $z_2 \in \mathcal{U}_n$ alors $(z_1 z_2^{-1})^n = \left(\frac{z_1}{z_2}\right)^n = \frac{z_1^n}{z_2^n} = \frac{1}{1} = 1$ donc $z_1 z_2^{-1} \in \mathcal{U}_n$, par conséquent $(\mathcal{U}_n, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.
2. a) Par définition de l'ordre d_0 est le plus petit entier supérieur ou égal à 1 tel que $\left(\omega_{k_0}\right)^{d_0} = 1$, ce qui équivaut à $e^{\frac{2ik_0d_0\pi}{n}} = 1$. La division euclidienne de k_0d_0 par n donne qu'il existe un unique couple d'entiers (q, r) avec $0 \leq r < n$ tel que $k_0d_0 = qn + r$. $e^{\frac{2ik_0d_0\pi}{n}} = 1 \Leftrightarrow e^{\frac{2i(qn+r)\pi}{n}} = 1 \Leftrightarrow e^{2iq\pi}e^{\frac{2ir\pi}{n}} = 1 \Leftrightarrow e^{\frac{2ir\pi}{n}} = 1$, or $0 \leq r < n \Leftrightarrow 0 \leq \frac{2r\pi}{n} < 2\pi$ donc $r = 0$. On en déduit que $k_0d_0 = qn$.
   b) D'après le théorème de Gauss k_0 divise qn et k_0 est premier avec n entraine que k_0 divise q, il exite donc $a \in \mathbb{N}$ tel que $q = ak_0$. D'autre part l'ordre de ω_{k_0} divise n d'après le théorème de Lagrange donc il existe $b \in \mathbb{N}$ tel que $n = bd_0$ on a donc
   $$k_0d_0 = qn \Leftrightarrow k_0d_0 = abk_0d_0 \Leftrightarrow 1 = ab$$
   Par conséquent $a = b = 1$ et alors $n = d_0$.

3. Si k_0 et n ne sont pas premiers entre eux alors l'ordre de ω_{k_0} n'est pas n. Soit $D = PGCD(n, k_0) > 1$, il existe alors $a \in \mathbb{N}$ et $b \in \mathbb{N}$ tels que $n = aD$ et $k_0 = bD$, donc $\omega_{k_0} = e^{\frac{2ik_0\pi}{n}} = e^{\frac{2ib\pi}{a}}$, on en déduit alors que $\left(\omega_{k_0}\right)^a = e^{2ib\pi} = 1$. Et évidemment $a < n$ car sinon $D = 1$.
   Ce qui montre que l'ordre de ω_{k_0} n'est pas n.
4. 3. est la contraposée de « si l'ordre de ω_{k_0}est n alors k_0 et n sont premiers entre eux », on en déduit que « l'ordre de ω_{k_0} est n si et seulement si k_0 et n sont premier entre eux ».

Allez à : Exercice 13

Correction exercice 14.

1. Si $\alpha > 0$ alors $f'(x) = \alpha x^{\alpha-1} > 0$ donc f est croissante, de plus $\lim_{x\to 0^*} x^\alpha = 0$ et $\lim_{x\to+\infty} x^\alpha = +\infty$
   f est une bijection de $]0, +\infty[$ sur $]0, +\infty[$.
   Si $\alpha < 0$ alors $f'(x) = \alpha x^{\alpha-1} < 0$ donc f est décroissante, de plus $\lim_{x\to 0^*} x^\alpha = +\infty$ et $\lim_{x\to+\infty} x^\alpha = 0$
   f est une bijection de $]0, +\infty[$ sur $]0, +\infty[$.
2. Rappelons que la composition est une loi associative.
   Soit $Id_{]0,+\infty[}$ définie pour tout $x \in]0, +\infty[$, $Id_{]0,+\infty[}(x) = x = x^1$, $Id_{]0,+\infty[} \in E$ car $1 \in \mathbb{R}^*$.
   Soient $f \in E$ et $g \in E$, ils existent $\alpha \in \mathbb{R}^*$ et $\beta \in \mathbb{R}^*$ tels que pour tout $x \in]0, +\infty[$:
   $f(x) = x^\alpha$ et $g(x) = x^\beta$
   $f \circ g$ est une fonction de $]0, +\infty[$ dans $]0, +\infty[$ et $f \circ g(x) = f\big(g(x)\big) = f\left(x^\beta\right) = \left(x^\beta\right)^\alpha = x^{\alpha\beta}$
   $\alpha\beta \in \mathbb{R}^*$ donc $f \circ g \in E$
   Le symétrique de f pour la composition est sa bijection réciproque, de plus $f^{-1}(x) = x^{\frac{1}{\alpha}}$, comme $\frac{1}{\alpha} \in \mathbb{R}^*$, $f^{-1} \in E$.
   Conclusion, $\circ$ est une loi interne, associative, qui admet $Id_{]0,+\infty[} \in E$ comme élément neutre et la bijection réciproque de f comme symétrique dans E. $(E, \circ)$ est un groupe.

Allez à : Exercice 14

Correction exercice 15.

1. Utilisons l'algorithme d'Euclide
$$29 = 3 \times 8 + 5$$
$$8 = 1 \times 5 + 3$$
$$5 = 1 \times 3 + 2$$
$$3 = 1 \times 2 + 1$$
$$2 = 2 \times 1 + 0$$
$$1 = 3 - 1 \times 2 = 3 - 1 \times (5 - 1 \times 3) = -1 \times 5 + 2 \times 3 = -1 \times 5 + 2 \times (8 - 1 \times 5) = 2 \times 8 - 3 \times 5$$
$$= 2 \times 8 - 3 \times (29 - 3 \times 8) = -3 \times 29 + 11 \times 8$$
   $u = 11$ et $v = -3$ est un couple de solution.
2. D'après la question précédente, $-3 \times 29 + 11 \times 8 = 1$, donc la classe de $-3 \times 29 + 11 \times 8$ dans H_{29} est égal à la classe de 1 dans H_{29}.
$$\overline{-3 \times 29 + 11 \times 8} = \overline{1} \Leftrightarrow \overline{-3} \times \overline{29} + \overline{11} \times \overline{8} = \overline{1} \Leftrightarrow \overline{11} \times \overline{8} = \overline{1}$$
   Car $\overline{29} = \overline{0}$, le symétrique de $\overline{8}$ est $\overline{11}$.
3. Les classes sont celles de H_{29}.
   $8x \equiv 9 \mod 29$ équivaut à $\overline{8x} = \overline{9}$, en multipliant par $\overline{11}$ à gauche et à droite :
$$\overline{11} \times \overline{8} \times \overline{x} = \overline{11} \times \overline{9} \Leftrightarrow \overline{1} \times \overline{x} = \overline{99} \Leftrightarrow \overline{x} = \overline{3 \times 29 + 12} \Leftrightarrow \overline{x} = \overline{3 \times 29} + \overline{12} = \overline{12}$$

Les solutions sont donc les entiers x congrus à 12 modulo 29.

Allez à : Exercice 15

Correction exercice 16.

1. On cherche $\overline{u} \in (\mathbb{Z}/24\mathbb{Z})^*$ tel que :
$$\overline{8}\overline{u} = \overline{1} \Leftrightarrow \exists k \in \mathbb{Z}, 8u = 1 + 24k \Leftrightarrow \exists k \in \mathbb{Z}, 8u - 24k = 1$$
$PGCD(8,24) = 8$ qui ne divise pas 1 donc $\overline{8}$ n'admet pas d'inverse.
2. Soit $\overline{a} \in (\mathbb{Z}/24\mathbb{Z})^*$, $\overline{a}$ admet un inverse si et seulement s'il existe $\overline{u} \in (\mathbb{Z}/24\mathbb{Z})^*$ tel que
$$\overline{a} \times \overline{u} = \overline{1}$$
Ce qui équivaut à, il existe $k \in \mathbb{Z}$ tel que $au = 1 + 24k$, autrement dit $au - 24k = 1$
Finalement à ce que a et 24 sont premiers entre eux, l'ensemble recherché est
$$\{1,5,7,11,13,17,19,23\}$$
3. On cherche $\overline{u} \in (\mathbb{Z}/11\mathbb{Z})^*$ tel que :
$$\overline{5}\overline{u} = \overline{1} \Leftrightarrow \exists k \in \mathbb{Z}, 5u = 1 + 11k \Leftrightarrow \exists k \in \mathbb{Z}, 5u - 11k = 1$$
Soit on voit une solution évidente $(u,k) = (-2,-1)$ soit on utilise l'algorithme d'Euclide
$$5 \times (-2) - 11 \times (-1) = 1 \Leftrightarrow 5 \times (-2) = 1 + 11 \times (-1) \Rightarrow \overline{5} \times \overline{-2} = \overline{1}$$
L'inverse de $\overline{5}$ est $\overline{-2} = \overline{9}$.
4. $(\mathbb{Z}/11\mathbb{Z})^*$ est un groupe multiplicatif à 10 éléments donc, pour tout $x \in (\mathbb{Z}/11\mathbb{Z})^*$, $x^{10} = \overline{1}$
Par conséquent $x^9 = x^{-1}$
5.
$$x^9 + \overline{5} = \overline{0} \Leftrightarrow x^{-1} + \overline{5} = \overline{0} \Leftrightarrow \overline{1} + \overline{5}x = \overline{0} \Leftrightarrow -x \times \overline{5} = \overline{1}$$
On a vu à la question 3. que l'opposé de la classe de 5 est $\overline{-2}$ donc $x = \overline{2}$.

Allez à : Exercice 16

Correction exercice 17.

1. Soit $l' \in \overline{l}$, il existe $k \in \mathbb{Z}$ tel que $l' = l + 6k$, donc $l' = l + 2 \times (3k) \equiv l$ [2] par conséquent
$$f(\overline{l'}) = \hat{l}$$
Si on change de représentant dans la classe de l dans $\mathbb{Z}/6\mathbb{Z}$, on ne change pas la valeur de $f(\overline{l})$ donc f est bien définie.
On notera $+$ l'addition dans $\mathbb{Z}/6\mathbb{Z}$ et dans $\mathbb{Z}/2\mathbb{Z}$, c'est un peu abusif mais pas trop.
$$f(\overline{l_1} + \overline{l_2}) = f(\overline{l_1 + l_2}) = \widehat{l_1 + l_2} = \hat{l_1} + \hat{l_2} = f(\overline{l_1}) + f(\overline{l_2})$$
f est bien un morphisme de groupe.
Il reste à montrer que f est surjectif. Dans $\mathbb{Z}/2\mathbb{Z}$ il n' y a que deux classes $\hat{0}$ et $\hat{1}$, comme
$$f(\overline{0}) = \hat{0} \quad \text{et} \quad f(\overline{1}) = \hat{1}$$
Ces deux classes ont au moins un antécédent.

Remarque :

Celui-ci n'a aucun chance d'être unique pour plein de raison, la première est que sinon f serait une bijection d'un ensemble à 6 éléments sur un ensemble à 2 éléments, ce qui est bien sur complétement impossible, la seconde est que
$f(\overline{2}) = \hat{2} = \hat{0}$; $f(\overline{3}) = \hat{3} = \hat{1}$; $f(\overline{4}) = \hat{4} = \hat{0}$ et $f(\overline{5}) = \hat{5} = \hat{1}$.

2. Si on reprend la remarque on a
$$\ker(f) = \{\overline{0}, \overline{2}, \overline{4}\}$$
Sinon (pour faire plus général), on cherche $\overline{l} \in \mathbb{Z}/6\mathbb{Z}$ tel que

$$f(\bar{l}) = \hat{0} \Leftrightarrow \hat{l} = \hat{0} \Leftrightarrow \exists k \in \mathbb{Z}, l = 0 + 2k = 2k \Leftrightarrow \exists k \in \mathbb{Z}, \bar{l} = \overline{2k}$$

Dans $\mathbb{Z}/6\mathbb{Z}$ il y a trois classes « paires », $\bar{0}$, $\bar{2}$ et $\bar{4}$.

On rappelle que le noyau d'un morphisme est un sous-groupe de l'ensemble de départ.

$+$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{0}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{2}$

3. On notera $\dot{l}$ les classes de $\mathbb{Z}/3\mathbb{Z}$. On définit φ de $\ker(f)$ dans $\mathbb{Z}/3\mathbb{Z}$ par :

$$\varphi(\bar{0}) = \dot{0};\ \varphi(\bar{2}) = \dot{1} \text{ et } \varphi(\bar{4}) = \dot{2}$$

Soit d'une manière plus générale $\varphi(\overline{2k}) = \dot{k}$.

Comme pour f on doit se demander ce qu'il se passe si on change de représentant dans $\overline{2k}$, est-ce que l'on retombe bien sur la même classe modulo 3 ?

Soit $2k' \in \overline{2k}$, il existe $n \in \mathbb{Z}$ tel que $2k' = 2k + 6n$, ce qui entraine que $k' = k + 3n$ et que par conséquent $\dot{k'} = \dot{k}$, tout va bien.

Manifestement φ est une bijection, est-ce un morphisme ?

$$\varphi(\overline{2k_1} + \overline{2k_2}) = \varphi(\overline{2k_1 + 2k_2}) = \widehat{2k_1 + 2k_2} = \widehat{2k_1} + \widehat{2k_2} = \varphi(\overline{2k_1}) + \varphi(\overline{2k_2})$$

φ est bien un morphisme.

Autre méthode :

On pouvait dresser la table de $\mathbb{Z}/3\mathbb{Z}$ et constater qu'elle est identique à celle de $\ker(f)$.

Allez à : Exercice 17

Correction exercice 18.

1. Il faut vérifier que l'image de $\mathcal{U}_8$ par f est bien incluse dans $\mathcal{U}_2$, or pour tout $z \in \mathcal{U}_8$, $z^8 = 1$ par conséquent $\big(f(z)\big)^2 = (z^4)^2 = z^8 = 1$ ce qui montre que $f(z) \in \mathcal{U}_2$.
2. Soit $z \in \mathcal{U}_8$, $z \in Ker(f) \Leftrightarrow f(z) = 1 \Leftrightarrow z^4 = 1 \Leftrightarrow z \in \{1, i, -1, -i\}$
   Donc $\ker(f) = \{1, i, -1, -i\} = \mathcal{U}_4$

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

3.

Première méthode compliquée mais qui se généralise aux isomorphismes de $\mathbb{Z}/n\mathbb{Z}$ sur $\mathcal{U}_n$.

On pose $\varphi(\bar{a}) = e^{\frac{2ia\pi}{4}} = e^{\frac{ia\pi}{2}}$, où $\bar{k} \in \mathbb{Z}/4\mathbb{Z}$.

Il faut d'abord vérifier que φ est bien définie, c'est-à-dire que si on change de représentant dans $\bar{a}$ alors l'image est bien la même. Soit $b \in \bar{a}$, $b = a + 4k$, $k \in \mathbb{Z}$.

$$e^{\frac{2ib\pi}{4}} = e^{\frac{2i(a+4k)\pi}{4}} = e^{\frac{2ia\pi + 2i\times 4k\pi}{4}} = e^{\frac{2ia\pi}{4}} e^{\frac{2ik\times 4\pi}{4}} = e^{\frac{2ia\pi}{4}} \times e^{2ik\pi} = e^{\frac{2ia\pi}{4}} \times 1 = e^{\frac{2ia\pi}{4}}$$

Donc tout va bien.

$$\varphi(\bar{a} + \bar{b}) = \varphi(\overline{a+b}) = e^{\frac{i(a+b)\pi}{2}} = e^{\frac{ia\pi}{2}} e^{\frac{ib\pi}{2}} = \varphi(\bar{a})\varphi(\bar{b})$$

φ est bien un morphisme de $\mathbb{Z}/4\mathbb{Z}$ sur $\mathcal{U}_4$.

Montrons que le noyau de φ est bien réduit à $\overline{0}$ (l'élément neutre de $\mathbb{Z}/4\mathbb{Z}$), ce qui montrera que φ est injective.

$$\overline{a} \in Ker(\varphi) \Leftrightarrow \varphi(\overline{a}) = 1 \Leftrightarrow e^{\frac{ia\pi}{2}} = 1 \Leftrightarrow \text{il existe } k \in \mathbb{Z}, \frac{a\pi}{2} = 2k\pi \Leftrightarrow \text{il existe } k \in \mathbb{Z}, a = 4k \Leftrightarrow \overline{a} = \overline{0}$$

Donc φ est injective.

Comme le cardinal de $\mathbb{Z}/4\mathbb{Z}$ est le même que le cardinal de $\mathcal{U}_4$, on en déduit que φ est bijective, finalement φ est un isomorphisme de groupe.

Deuxième méthode.

On pose $\varphi(\overline{0}) = 1$, $\varphi(\overline{1}) = i$, $\varphi(\overline{2}) = -1$ et $\varphi(\overline{3}) = -i$

Chaque élément de $\mathcal{U}_4$ admet un unique antécédent donc φ est une bijection.

Il reste à montrer que c'est un morphisme.

Le plus simple est de comparer la table de $(\mathbb{Z}/4\mathbb{Z}, +)$ avec celle de $(\mathcal{U}_4, \times)$

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

Les éléments de chaque groupe étant situé au même endroit, φ est un morphisme entre ces deux groupes

Sinon on peut faire l'effort de vérifier « à la main » que tout marche bien.

$$\varphi(\overline{0}+\overline{0}) = \varphi(\overline{0}) = 1 = 1 \times 1 = \varphi(\overline{0})\varphi(\overline{0})$$
$$\varphi(\overline{0}+\overline{1}) = \varphi(\overline{1}) = i = 1 \times i = \varphi(\overline{0})\varphi(\overline{1})$$
$$\varphi(\overline{0}+\overline{2}) = \varphi(\overline{2}) = -1 = 1 \times (-1) = \varphi(\overline{0})\varphi(\overline{2})$$
$$\varphi(\overline{0}+\overline{3}) = \varphi(\overline{3}) = -i = 1 \times (-i) = \varphi(\overline{0})\varphi(\overline{3})$$

$$\varphi(\overline{1}+\overline{1}) = \varphi(\overline{2}) = -1 = i \times i = \varphi(\overline{1})\varphi(\overline{1})$$
$$\varphi(\overline{1}+\overline{2}) = \varphi(\overline{3}) = -i = i \times (-1) = \varphi(\overline{1})\varphi(\overline{2})$$
$$\varphi(\overline{1}+\overline{3}) = \varphi(\overline{0}) = 1 = i \times (-i) = \varphi(\overline{1})\varphi(\overline{3})$$

$$\varphi(\overline{2}+\overline{2}) = \varphi(\overline{0}) = 1 = (-1) \times (-1) = \varphi(\overline{2})\varphi(\overline{2})$$
$$\varphi(\overline{2}+\overline{3}) = \varphi(\overline{1}) = i = (-1) \times (-i) = \varphi(\overline{2})\varphi(\overline{3})$$

$$\varphi(\overline{3}+\overline{3}) = \varphi(\overline{2}) = -1 = (-i) \times (-i) = \varphi(\overline{3})\varphi(\overline{3})$$

Par commutativité on obtient ceux qui manquent.

φ est bien un morphisme de groupe. Comme il est bijectif, c'est un isomorphisme.

Allez à : Exercice 18

Correction exercice 19.

1. $1^8 = 1$ donc $1 \in H$. Soient $z_1 \in H$ et $z_2 \in H$ alors $(z_1 z_2^{-1})^8 = \left(\frac{z_1}{z_2}\right)^8 = \frac{z_1^8}{z_2^8} = \frac{1}{1} = 1$ donc $z_1 z_2^{-1} \in H$, $(H, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.
2. $z^4 = z^4$ donc $z \sim z$, autrement dit $\sim$ est réflexive.

$z_1 \sim z_2 \Rightarrow z_1^4 = z_2^4 \Rightarrow z_2^4 = z_1^4 \Rightarrow z_2 \sim z_1$ donc $\sim$ est symétrique.

$\begin{cases} z_1 \sim z_2 \\ z_2 \sim z_3 \end{cases} \Rightarrow \begin{cases} z_1^4 = z_2^4 \\ z_2^4 = z_3^4 \end{cases} \Rightarrow z_1^4 = z_3^4 \Rightarrow z_1 \sim z_3$ donc $\sim$ est transitive, $\sim$ est une relation d'équivalence.

3. Soit $a \in H$, $z \in \dot{a} \Leftrightarrow z^4 = a^4 \Leftrightarrow \left(\frac{z}{a}\right)^4 = 1$ or les racines quatrième de 1 sont $\{1, i, -1, -i\}$ donc $\frac{z}{a} \in \{1, i, -1, -i\}$ ou encore $z \in \{a, ai, -a, -ia\}$, et donc $\dot{a} = \{a, ai, -a, -ia\}$.
   Ces éléments sont évidemment tous distincts (sauf pour $a = 0$, mais $0 \notin H$) donc une classe pour cette relation d'équivalence a 4 éléments, or le cardinal de H est 8, il y a donc deux classes d'équivalence.
   $\dot{1} = \{1, i, -1, -i\}$ il reste à trouver une racine huitième de 1 qui ne soit pas dans $\dot{1}$. Par exemple $\omega = e^{\frac{2i\pi}{8}} = e^{\frac{i\pi}{4}}$, La seconde classe d'équivalence est alors $\dot{\omega} = \{\omega, \omega i, -\omega, -i\omega\}$. On peut un peu améliorer la « clarté » de ces complexes, en effet $\omega i = e^{\frac{i\pi}{4}} e^{\frac{i\pi}{2}} = e^{\frac{3i\pi}{4}}$, $-\omega = -e^{\frac{i\pi}{4}} = e^{i\pi} e^{\frac{i\pi}{4}} = e^{\frac{5i\pi}{4}}$, $-i\omega = e^{\frac{3i\pi}{2}} e^{\frac{i\pi}{4}} = e^{\frac{7i\pi}{4}}$.

Allez à : Exercice 19

Correction exercice 20.

1. $1^n = 1$ donc $1 \in U_n$
   Soient $z \in U_n$ et $z' \in U_n$ donc $z^n = 1$ et $z'^n = 1$
   $$(zz'^{-1})^n = \left(\frac{z}{z'}\right)^n = \frac{z^n}{z'^n} = \frac{1}{1} = 1$$
   Cela montre que $zz'^{-1} \in U_n$, U_n muni de la multiplication est un sous-groupe de $\mathbb{C}^*$.
2. Comme n divise m, il existe $k \in \mathbb{N}$ tel que $m = kn$.
   Soit $z \in U_n$, alors $z^n = 1$.
   $$z^m = z^{kn} = (z^n)^k = 1^k = 1$$
   Ce qui montre que $z \in U_m$ et que $U_n \subset U_m$.
3. d divise n, d'après b) $U_d \subset U_n$, de même d divise m, d'après b) $U_d \subset U_m$, cela montre que $U_d \subset U_n \cap U_m$
   Soit $z \in U_n \cap U_m$, $z \in U_n$ et $z \in U_m$ donc $z^n = 1$ et $z^m = 1$. D'après l'identité de Bézout il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que $nu + mv = d$, on en déduit que $z^d = z^{nu+mv} = (z^n)^u (z^m)^v = 1^u \times 1^v = 1$, ce qui montre que $z \in U_d$, par conséquent $U_n \cap U_m \subset U_d$.
   D'après cette double inclusion : $U_d = U_n \cap U_m$.
4. Soient $k \in \mathbb{Z}$ et $k' \in \mathbb{Z}$
   $$f(k + k') = e^{i\frac{2(k+k')\pi}{5}} = e^{i\left(\frac{2k\pi}{5} + \frac{2k'\pi}{5}\right)} = e^{i\frac{2k\pi}{5}} e^{i\frac{2k'\pi}{5}} = f(k) f(k')$$

   Cela montre que f est un morphisme du groupe additif $\mathbb{Z}$ dans le groupe multiplicatif $\mathbb{C}^*$. Il reste à montrer que l'image de $\mathbb{Z}$ par f est incluse dans U_5.

   Pour tout $k \in \mathbb{Z}$, $\big(f(k)\big)^5 = \left(e^{i\frac{2k\pi}{5}}\right)^5 = e^{2i\pi} = 1$, ce qui montre que $f(k) \in U_5$.

   f est un morphisme du groupe additif $\mathbb{Z}$ dans le groupe multiplicatif U_5.
   $$k \in \ker(f) \Leftrightarrow f(k) = 1$$
   Le « 1 » est l'élément neutre du groupe U_5 muni de la multiplication.

   $k \in \ker(f) \Leftrightarrow f(k) = 1 \Leftrightarrow e^{i\frac{2k\pi}{5}} = 1 \Leftrightarrow$il existe $k' \in \mathbb{Z}$ tel que $\frac{2k\pi}{5} = 2k'\pi$, autrement dit $k = 5k'$
   $\ker(f)$ est l'ensemble des multiples de 5, ce qui s'écrit aussi $5\mathbb{Z}$.

Allez à : Exercice 20

Correction exercice 21.

1.

a)

$$\overline{3}^0 = \overline{1}$$
$$\overline{3}^1 = \overline{3}$$
$$\overline{3}^2 = \overline{9} = \overline{2}$$
$$\overline{3}^3 = \overline{3}^2 \times \overline{3} = \overline{2} \times \overline{3} = \overline{6}$$
$$\overline{3}^4 = \overline{3}^3 \times \overline{3} = \overline{6} \times \overline{3} = \overline{18} = \overline{4}$$
$$\overline{3}^5 = \overline{3}^4 \times \overline{3} = \overline{4} \times \overline{3} = \overline{12} = \overline{5}$$
$$\overline{3}^6 = \overline{1}$$

La dernière égalité n'étant que le petit théorème de Fermat.

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

$$\overline{3}^k = \overline{3}^{6q+r} = \left(\overline{3}^6\right)^q \times \overline{3}^r = \left(\overline{1}\right)^q \times \overline{3}^r = \overline{3}^r \in \left\{\overline{3}^k, k \in \{0,1,2,3,4,5\}\right\}$$

2. 7 est premier donc $((\mathbb{Z}/7\mathbb{Z})^*, \times)$ est un groupe.
3. D'après la première question le groupe engendré par $\overline{3}$ est

$$\{\overline{1}, \overline{3}, \overline{2}, \overline{6}, \overline{4}, \overline{5}\}$$

C'est bien le même ensemble que $(\mathbb{Z}/7\mathbb{Z})^*$.

4.

a) Il faut vérifier que si $\overline{3}^{k'} = \overline{3}^k$ alors on a bien $\varphi\left(\overline{3}^{k'}\right) = \varphi\left(\overline{3}^k\right)$

$$\overline{3}^{k'} = \overline{3}^k \Leftrightarrow \overline{3}^{k'-k} = \overline{1} \Leftrightarrow \exists l \in \mathbb{Z}, k' - k = 6l \Leftrightarrow \exists l \in \mathbb{Z}, k' = k + 6l$$

La seconde égalité vient du fait que l'ordre de $\overline{3}$ est 6, d'après la première question.

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

Il faut aussi vérifier que $\varphi\left(\overline{3}^k\right) \in \mathcal{U}_6$, ce qui est exact car $\left(e^{\frac{ik\pi}{3}}\right)^6 = e^{2ik\pi} = 1$

φ est bien définie.

b) Pour toutes classes a et b de $(\mathbb{Z}/7\mathbb{Z})^*$, 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 $a = \overline{3}^k$ et $b = \overline{3}^l$

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

φ est un morphisme de groupe.

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

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

Donc

$$a = \overline{3}^k = \overline{3}^{6k'} = \left(\overline{3}^6\right)^{k'} = \overline{1}^{k'} = \overline{1}$$

le noyau de φ est réduit à l'élément neutre de $(\mathbb{Z}/7\mathbb{Z})^*$, ce qui montre que φ est injective, comme $(\mathbb{Z}/7\mathbb{Z})^*$
et $\mathcal{U}_6$ ont tous les deux 6 éléments φ est bijective.

Allez à : Exercice 21

Correction exercice 22.

1. Pour tout $k \in G$, il existe un unique $h = g^{-1} * k \in G$ tel que $\gamma_g(h) = \gamma_g(g^{-1} * k) = g * g^{-1} * k = k$
   Donc γ_g est une bijection de G sur G.
2. Pour tout $g, g' \in G$ et pour tout $h \in G$
   $$\varphi(g * g')(h) = \gamma_{g*g'}(h) = (g * g') * h = g * (g' * h) = g * \gamma_{g'}(h) = \gamma_g\left(\gamma_{g'}(h)\right) = \gamma_g \circ \gamma_{g'}(h)$$
   Par conséquent
   $$\varphi(g * g') = \gamma_g \circ \gamma_{g'} = \varphi(g) \circ \varphi(g')$$
   Ce qui montre que φ est un morphisme de $(G,*)$ dans $(\mathcal{S}_G,\circ)$.
3. Pour montrer que φ est injective il faut et il suffit de montrer que le noyau de φ est réduit à l'élément neutre de G car φ est un morphisme.
   $$g \in \ker(\varphi) \Leftrightarrow \varphi(g) = Id_G \Leftrightarrow \forall h \in G, \varphi(g)(h) = h \Leftrightarrow \forall h \in G, \gamma_g(h) = h \Leftrightarrow \forall h \in G, g * h = h \Leftrightarrow g = e$$
   Ce qui montre que $\ker(\varphi) = \{e\}$, et que donc φ est injective.
4. Pour tout $k \in G$, il existe un unique $h = k * g^{-1} \in G$ tel que $\delta_g(h) = \delta_g(k * g^{-1}) = k * g^{-1} * g = k$
   Donc δ_g est une bijection de G sur G.
   Pour montrer l'injectivité de ψ on ne peut pas utiliser le « noyau » puisque pour l'instant ψ n'est pas un morphisme.
   $$\psi(g) = \psi(g') \Leftrightarrow \forall h \in G, \psi(g)(h) = \psi(g')(h) \Leftrightarrow \forall h \in G, \delta_g(h) = \delta_{g'}(h)$$
   $$\Leftrightarrow \forall h \in G, h * g = h * g' \Leftrightarrow g = g'$$
   ψ est injective.
5.

Si ψ est un (homo)morphisme de groupe

Pour tous $g, g' \in G$, $\psi(g * g') = \psi(g) \circ \psi(g')$, donc pour tout $h \in G$

$$\psi(g * g')(h) = \psi(g) \circ \psi(g')(h) \Leftrightarrow \delta_{g*g'}(h) = \delta_g \circ \delta_{g'}(h) \Leftrightarrow h * (g * g') = \delta_g\left(\delta_{g'}(h)\right)$$
$$\Leftrightarrow h * (g * g') = \delta_g(h * g') \Leftrightarrow h * g * g' = h * g' * g$$

Il reste à composer par h^{-1} à gauche pour en déduire que pour tous $g, g' \in G$, $g * g' = g' * g$, autrement dit G est abélien.

Réciproque, supposons que G soit abélien.

C'est pareil dans l'autre sens, faisons le tout de même.

Pour tout $g, g', h \in G$

$$h * g * g' = h * g' * g \Leftrightarrow h * (g * g') = \delta_g(h * g') \Leftrightarrow h * (g * g') = \delta_g\left(\delta_{g'}(h)\right) \Leftrightarrow h * (g * g')$$
$$= \delta_g\left(\delta_{g'}(h)\right) \Leftrightarrow \delta_{g*g'}(h) = \delta_g \circ \delta_{g'}(h) \psi(g * g')(h) = \psi(g) \circ \psi(g')(h)$$
$$\Leftrightarrow \psi(g * g') = \psi(g) \circ \psi(g')$$

Ce qui montre que ψ est un morphisme de groupe.

Allez à : Exercice 22

Correction exercice 23.

1. Si φ est un morphisme de G
   Pour tout $g, g' \in G$
   $$\varphi\left(g^{-1} * g'^{-1}\right) = \varphi(g^{-1}) * \varphi\left(g'^{-1}\right) \Rightarrow \left(g^{-1} * g'^{-1}\right)^{-1} = (g^{-1})^{-1} * (g'^{-1})^{-1}$$
   $$\Rightarrow (g'^{-1})^{-1} * (g^{-1})^{-1} = g * g' \Rightarrow g' * g = g * g'$$
   Ce qui montre que le groupe est abélien.
   Si le groupe est abélien alors pour tous $g, g' \in G$, $g^{-1} * g'^{-1} = g'^{-1} * g^{-1}$
   $$g^{-1} * g'^{-1} = g'^{-1} * g^{-1} \Rightarrow \varphi(g) * \varphi(g') = (g * g')^{-1} = \varphi(g * g')$$
   Ce qui montre que φ est un morphisme de G.

Ces deux implications montre que φ est un morphisme si et seulement si G est abélien.

2. $e \in \{e, x, x^2, \dots, x^{m-1}\}$

Soit $g, h \in \{e, x, x^2, \dots, x^{m-1}\}$, il existe $a, b \in \{0,1,2, \dots, m-1\}$ tels que $g = x^p$ et $h = x^q$

Donc $g * h^{-1} = x^a * x^{-b} = x^{a-b}$

On effectue la division euclidienne de $a - b$ par m, il existe un unique couple $(q, r) \in \mathbb{Z} \times \{0,1,2, \dots, m-1\}$ tel que $a - b = mq + r$, par conséquent

$$g * h^{-1} = x^{mq+r} = (x^m)^q * x^r = e^q * x^r = x^r \in \{e, x, x^2, \dots, x^{m-1}\}$$

Ces deux propriétés montrent que $\{e, x, x^2, \dots, x^{m-1}\}$ muni de $*$ est un sous-groupe de $(G,*)$.

3. n est pair donc il existe $n' \in \mathbb{N}$ tel que $n = 2n' - 1$, une des conséquences du théorème de Lagrange veut que pour tout $g \in G$, $g^n = e$, par conséquent

$$g^{2n'-1} = e \Leftrightarrow g^{2n'} = g \Leftrightarrow \left(g^{n'}\right)^2 = g \Leftrightarrow \psi\left(g^{n'}\right) = g$$

Donc pour tout $g \in G$ il existe $h = g^{n'}$ tel que $g = \psi(h)$, ce qui montre que ψ est surjective.

4. Supposons que ψ soit un morphisme, pour tous $g, g' \in G$

$$\psi(g * g') = \psi(g) * \psi(g') \Leftrightarrow (g * g')^2 = g^2 * g'^2 \Leftrightarrow g * g' * g * g' = g * g * g' * g' \Leftrightarrow g' * g = g * g'$$

En simplifiant à gauche par g et à droite par g'

Bref ψ est un morphisme si et seulement si G est abélien.

Allez à : Exercice 23

Correction exercice 24.

1. $\forall g \in G \quad e * g = g * e$ donc $e \in Z$.

Pour tout $z_1 \in Z$ et pour tout $z_2 \in Z$,

$$(z_1 * z_2^{-1}) * g = z_1 * (z_2^{-1} * g) = z_1 * (g^{-1} * z_2)^{-1}$$

Or $g^{-1} \in G$ donc $g^{-1} * z_2 = z_2 * g^{-1}$

$$(z_1 * z_2^{-1}) * g = z_1 * (g^{-1} * z_2)^{-1} = z_1 * (z_2 * g^{-1})^{-1} = z_1 * (g * z_2^{-1}) = (z_1 * g) * z_2^{-1} = (g * z_1) * z_2^{-1} = g * (z_1 * z_2^{-1})$$

Ce qui montre que $z_1 * z_2^{-1} \in Z$.

Donc $(Z,*)$ est un sous-groupe de $(G,*)$

2. Si G est commutatif alors pour tout $z \in G$ et pour $g \in G$, $z * g = g * z$ donc $Z = G$.

Allez à : Exercice 24

Correction exercice 25.

1.

a)

$A \cup B$	$\emptyset$	$\{0\}$	$\{1\}$	$\{0,1\}$
$\emptyset$	$\emptyset$	$\{0\}$	$\{1\}$	$\{0,1\}$
$\{0\}$	$\{0\}$	$\{0\}$	$\{0,1\}$	$\{0,1\}$
$\{1\}$	$\{1\}$	$\{0,1\}$	$\{1\}$	$\{0,1\}$
$\{0,1\}$	$\{0,1\}$	$\{0,1\}$	$\{0,1\}$	$\{0,1\}$

b) $\emptyset$ est l'élément neutre pour la réunion.

c) Oui, la réunion est toujours associative.

d) Oui, la réunion est toujours commutative.

e) Non, par exemple $\{1\} \cup B$ n'est jamais égal à $\{0\}$, ce qui signifie que $\{1\}$ n'a pas de symétrique.

f) Même réponse pour les questions de b à e.

Allez à : Exercice 25

2.

$A \cap B$	$\emptyset$	$\{0\}$	$\{1\}$	$\{0,1\}$

a)

$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{0\}$	$\emptyset$	$\{0\}$	$\{0\}$	$\{0\}$
$\{1\}$	$\emptyset$	$\emptyset$	$\{1\}$	$\{1\}$
$\{0,1\}$	$\emptyset$	$\{0\}$	$\{1\}$	$\{0,1\}$

b) $\{0,1\}$ est l'élément neutre pour l'intersection.
c) Oui, l'intersection est toujours associative.
d) Oui, l'intersection est toujours commutative.
e) Non, par exemple $\{0\} \cap B$ n'est jamais égal à $\{0,1\}$, donc $\{0\}$ n'a pas de symétrique.
f) Même réponse pour les questions de b à e.

Allez à : Exercice 25

3.

a)

$(A \setminus B) \cup (B \setminus A)$	$\emptyset$	$\{0\}$	$\{1\}$	$\{0,1\}$
$\emptyset$	$\emptyset$	$\{0\}$	$\{1\}$	$\{0,1\}$
$\{0\}$	$\{0\}$	$\emptyset$	$\{0,1\}$	$\{1\}$
$\{1\}$	$\{1\}$	$\{0,1\}$	$\emptyset$	$\{0\}$
$\{0,1\}$	$\{0,1\}$	$\{1\}$	$\{0\}$	$\emptyset$

b) $\emptyset$ est l'élément neutre pour la différence symétrique.
c) d) e) Sur chaque ligne de la table il y a, une et une seule fois, chacun des 4 éléments de E ce qui entraine que E muni de la différence symétrique est un groupe, cette loi est associative et commutative, le symétrique de $\emptyset$ est $\emptyset$, celui de $\{0\}$ est $\{0\}$, celui de $\{1\}$ est $\{1\}$ et celui de $\{0,1\}$ est $\{0,1\}$.
f)

$$(\emptyset \setminus B) \cup (B \setminus \emptyset) = \emptyset \cup B = B$$

Donc $\emptyset$ est l'élément neutre.
On a besoin de rappeler un résultat avant de montrer l'associativité basé sur le fait que $A \setminus B = A \cap \overline{B}$

$$A * B = (A \setminus B) \cup (B \setminus A) = \left(A \cap \overline{B}\right) \cup \left(B \cap \overline{A}\right) = (A \cup B) \cap \left(A \cup \overline{A}\right) \cap \left(\overline{B} \cup B\right) \cap \left(\overline{B} \cup \overline{A}\right)$$
$$= (A \cup B) \cap E \cap E \cap \left(\overline{B} \cup \overline{A}\right) = (A \cup B) \cap \left(\overline{B} \cup \overline{A}\right) = (A \cup B) \cap \left(\overline{B \cap A}\right)$$

$$(A * B) * C = \left((A \cup B) \cap \left(\overline{A \cap B}\right)\right) * C = \left(\left((A \cup B) \cap \left(\overline{A \cap B}\right)\right) \cup C\right) \cap \overline{\left(\left((A \cup B) \cap \left(\overline{A \cap B}\right)\right) \cap C\right)}$$
$$= \left(\left((A \cup B) \cup C\right) \cap \left(\left(\overline{A \cap B}\right) \cup C\right)\right) \cap \overline{\left((A \cup B) \cap \left(\overline{A \cap B}\right) \cup \overline{C}\right)}$$
$$= (A \cup B \cup C) \cap \left(\overline{A} \cup \overline{B} \cup C\right) \cap \left(\left(\overline{A \cup B}\right) \cup \left(\overline{\overline{A \cap B}}\right) \cup \overline{C}\right)$$
$$= (A \cup B \cup C) \cap \left(\overline{A} \cup \overline{B} \cup C\right) \cap \left(\left(\overline{A} \cap \overline{B}\right) \cup (A \cap B) \cup \overline{C}\right)$$

Faisons un petit calcul intermédiaire

$$\left(\overline{A} \cap \overline{B}\right) \cup (A \cap B) = \left(\overline{A} \cup A\right) \cap \left(\overline{A} \cup B\right) \cap \left(\overline{B} \cup A\right) \cap \left(\overline{B} \cup B\right) = E \cap \left(\overline{A} \cup B\right) \cap \left(\overline{B} \cup A\right) \cap E$$
$$= \left(\overline{A} \cup B\right) \cap \left(\overline{B} \cup A\right)$$

Reprenons le calcul de $(A * B) * C$.

$$(A * B) * C = (A \cup B \cup C) \cap \left(\overline{A} \cup \overline{B} \cup C\right) \cap \left(\left(\left(\overline{A} \cup B\right) \cap \left(\overline{B} \cup A\right)\right) \cup \overline{C}\right)$$
$$= (A \cup B \cup C) \cap \left(\overline{A} \cup \overline{B} \cup C\right) \cap \left(\left(\overline{A} \cup B\right) \cup \overline{C}\right) \cap \left(\left(\overline{B} \cup A\right) \cup \overline{C}\right)$$
$$= (A \cup B \cup C) \cap \left(\overline{A} \cup \overline{B} \cup C\right) \cap \left(\overline{A} \cup B \cup \overline{C}\right) \cap \left(A \cup \overline{B} \cup \overline{C}\right)$$

Ce calcul est assez compliqué c'est pourquoi on va éviter d'en refaire un aussi compliqué pour calculer $A * (B * C)$, la loi est clairement commutative, on va utiliser ce résultat dans la suite. Avec un peu

d'expérience, dès que dans $(A * B) * C$, on peut intervertir A, B et C on est sûr de l'associativité de la loi.
Calcul de $C * (B * A)$, on reprend le calcul de $A * (B * C)$ en changeant A et C, on constate que cela ne change rien donc $C * (B * A) = A * (B * C)$, d'autre part $B * A = A * B$ donc $C * (B * A) = C * (A * B)$, la loi étant commutative $C * (A * B) = (A * B) * C$, on a bien

$$A * (B * C) = (A * B) * C$$

La différence symétrique est associative.
On n'en a pas parlé mais la loi est évidemment une loi interne.
Il reste à montrer que tous les ensembles admettent un symétrique.
Soit A un ensemble, on cherche B tel que :

$$(A \setminus B) \cup (B \setminus A) = (A \cup B) \cap \left(\overline{B \cap A}\right) = \emptyset$$

Comme $U \setminus V = U \cap \overline{V}$, $(A \cup B) \cap \left(\overline{B \cap A}\right) = (A \cup B) \setminus (A \cap B)$
Donc B vérifie $(A \cup B) \setminus (A \cap B) = \emptyset$, autrement dit $A \cup B \subset A \cap B$, or $A \cap B \subset A \cup B$, d'où l'on déduit que : $A \cap B = A \cup B$, je crois que là c'est clair, $B = A$.
Remarque : si on s'aperçoit que $B = A$ est solution, par unicité du symétrique c'est la seule solution possible.
Finalement E muni de la différence symétrique est un groupe commutatif.

Allez à : Exercice 25

4.

a)

$\overline{A} \cup \overline{B}$	$\emptyset$	{0}	{1}	{0,1}
$\emptyset$	{0,1}	{0,1}	{0,1}	{0,1}
{0}	{0,1}	{1}	{0,1}	{1}
{1}	{0,1}	{0,1}	{0}	{0}
{0,1}	{0,1}	{1}	{0}	$\emptyset$

b) Il est clair (enfin j'espère) qu'il n'y a pas d'élément neutre.
c) La réunion est toujours associative.
d) La réunion est toujours commutative.
e) Comme il n'y a pas d'élément neutre, il ne peut pas y avoir de symétrique.
f) Il n'y a pas d'élément neutre, la loi est associative et commutative et bien sur il n'y a pas de symétrique.

Allez à : Exercice 25

5.

a)

$\overline{A} \cap \overline{B}$	$\emptyset$	{0}	{1}	{0,1}
$\emptyset$	{0,1}	{1}	{0}	$\emptyset$
{0}	{1}	{1}	$\emptyset$	$\emptyset$
{1}	{0}	$\emptyset$	{0}	$\emptyset$
{0,1}	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$

b) Il est clair (enfin j'espère) qu'il n'y a pas d'élément neutre.
c) L'intersection est toujours associative.
d) L'intersection est toujours commutative.
e) Comme il n'y a pas d'élément neutre, il ne peut pas y avoir de symétrique.
f) Il n'y a pas d'élément neutre, la loi est associative et commutative et bien sur il n'y a pas de symétrique.

Allez à : Exercice 25

Correction exercice 26.
Tous les groupes possèdent un élément neutre, notons le e. Et notons $*$ la loi.

1.

$*$	e

e	e

Car $e * e = e$

Allez à : Exercice 26

2. Dans un groupe à deux éléments, il y a e l'élément neutre, notons a l'autre élément, donc $G = \{e, a\}$.
On a $a * e = e * a = a$.
Que vaut $a * a = a^2$? a^2 vaut soit e soit a car la loi est interne. Considérons a^{-1} le symétrique de a, celui-ci appartient à $G = \{e, a\}$, il n'est pas possible que $a^{-1} = e$ sinon $a = e$, par conséquent $a^{-1} = a$, en multipliant à gauche (ou à droite) par a : $a * a^{-1} = a * a \Leftrightarrow e = a * a$. On en déduit que :

$*$	e	a
e	e	a
a	a	e

Montrons que $(G,*)$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z}, +)$.
Soit $\varphi : (G,*) \to (\mathbb{Z}/2\mathbb{Z}, +)$ définit par $\varphi(e) = \overline{0}$ et $\varphi(a) = \overline{1}$, φ est une bijection (c'est évident).

$$\varphi(e * a) = \varphi(a) = \overline{1} = \overline{0} + \overline{1} = \varphi(e) + \varphi(a)$$

De même

$$\varphi(a * e) = \varphi(a) = \overline{1} = \overline{1} + \overline{0} = \varphi(a) + \varphi(e)$$

Et enfin

$$\varphi(a * a) = \varphi(e) = \overline{0} = \overline{1} + \overline{1} = \varphi(a) + \varphi(a)$$

Cela montre que φ est un morphisme. Finalement φ est un isomorphisme et $(G,*)$ et $(\mathbb{Z}/2\mathbb{Z}, +)$ sont isomorphes. Une autre façon de faire est d'écrire la table du groupe $(\mathbb{Z}/2\mathbb{Z}, +)$.

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

Et de constater que le e et le a sont aux mêmes endroits que le $\overline{0}$ et le $\overline{1}$.
Montrons que $(G;*)$ et $(\{-1,1\},\times)$ sont isomorphes.
Soit $\varphi: (G,*) \to (\{-1,1\},\times)$ définit par $\varphi(e) = 1$ et $\varphi(a) = -1$

$$\varphi(e * a) = \varphi(a) = -1 = 1 \times 1 = \varphi(e) \times \varphi(a)$$

De même

$$\varphi(a * e) = \varphi(a) = -1 = -1 \times 1 = \varphi(a) \times \varphi(e)$$

Et enfin

$$\varphi(a * a) = \varphi(e) = 1 = 1 \times 1 = \varphi(a) \times \varphi(a)$$

Cela montre que φ est un morphisme. Finalement φ est un isomorphisme et $(G,*)$ et $(\{-1,1\},\times)$ sont isomorphes. Une autre façon de faire est d'écrire la table du groupe $(\{-1,1\},\times)$

$\times$	1	-1
1	1	-1
-1	-1	1

Et de constater que le e et le a sont aux mêmes endroits que le 1 et le -1.
Montrons que $(G,*)$ et $\left(\left\{x \mapsto x, x \mapsto \frac{1}{x}\right\},\circ\right)$ sont isomorphes. C'est formellement un peu plus compliqué, notons $id(x) = x$ et $f(x) = \frac{1}{x}$, pour tout $x \neq 0$

$$f \circ f(x) = f\big(f(x)\big) = f\left(\frac{1}{x}\right) = \frac{1}{\frac{1}{x}} = x = id(x)$$

Posons $\varphi: (G,*) \to \left(\left\{x \mapsto x, x \mapsto \frac{1}{x}\right\},\circ\right)$ définit par $\varphi(e) = id$ et $\varphi(a) = f$

$$\varphi(e * a) = \varphi(a) = f = Id \circ f = \varphi(e) \circ \varphi(a)$$

De même

$$\varphi(a * e) = \varphi(a) = f = f \circ id = \varphi(a) \circ \varphi(e)$$

Et enfin

$$\varphi(a * a) = \varphi(e) = id = f \circ f = \varphi(a) \circ \varphi(a)$$

Cela montre que φ est un morphisme. Finalement φ est un isomorphisme et $(G,*)$ et $\left(\left\{x \mapsto x, x \mapsto \frac{1}{x}\right\},\circ\right)$ sont isomorphes. Une autre façon de faire est d'écrire la table du groupe $\left(\left\{x \mapsto x, x \mapsto \frac{1}{x}\right\},\circ\right)$

$+$	id	f
id	id	f
f	f	id

Et de constater que le e et le a sont aux mêmes endroits que le id et le f.

Allez à : Exercice 26

3. On note $*$ la loi du groupe, e l'élément neutre, a et b les autres éléments du groupe donc $G = \{e, a, b\}$
Il faut calculer $a * b$, $b * a$, $a * a = a^2$ et $b * b = b^2$. Pour les autres produits c'est évident
$$e * e = e, \quad a * e = e * a = a \quad \text{et} \quad b * e = e * b = b$$
On va chercher ce que vaut le produit $a * b$, celui appartient à G par conséquent
$$a * b = e \quad \text{ou} \quad a * b = a \quad \text{ou} \quad a * b = b$$
Si $a * b = a$, en multipliant à gauche par a^{-1}, on a
$$a^{-1} * (a * b) = a^{-1} * a \Leftrightarrow (a^{-1} * a) * b = e \Leftrightarrow e * b = e \Leftrightarrow b = e$$
En utilisant d'abord l'associativité de la multiplication, puis que $a^{-1} * a = e$.
Ce n'est pas possible puisque $b \neq e$.
De même $a * b \neq b$ car en multipliant à droite par b^{-1} on trouve que $a = e$ ce qui n'est pas possible.
Par conséquent $a * b = e$.
On ne peut pas en déduire immédiatement que $b * a = e$, mais avec un raisonnement analogue, c'est-à-dire que l'on suppose que $b * a$ égal à a, puis à b, on en déduit que $b * a = e$.
Table intermédiaire

$*$	e	a	b
e	e	a	b
a	a		e
b	b	e	

Première méthode :
Sur chaque ligne et sur chaque colonne il y a une et une seule fois chaque élément du groupe donc $a * a = a^2 = b$ et $b * b = b^2 = a$.

Deuxième méthode :
$a^2 \in \{e, a, b\}$,
Si $a^2 = e$ alors $a^{-1} = a$ (en multipliant à gauche ou à droite par a^{-1}) mais $a * b = e$ entraine que $a^{-1} = b$ et par conséquent $a = b$ ce qui est impossible d'après ce que l'on a vu ci-dessus.
Si $a^2 = a$ alors $a^{-1} * a^2 = a^{-1} * a$ et donc $a = e$ ce qui est faux puisque $a \neq e$.
La seule solution est $a^2 = b$.
Le même raisonnement entraine que $b^2 = a$.
On peut compléter la table :

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Montrons que $(G,*)$ est isomorphe à $(\mathbb{Z}/3\mathbb{Z},+)$.
Soit $\varphi : (G,*) \to (\mathbb{Z}/3\mathbb{Z},+)$ définit par $\varphi(e) = \overline{0}$, $\varphi(a) = \overline{1}$ et $\varphi(b) = \overline{2}$ (on aurait pu prendre $\varphi(a) = \overline{2}$ et $\varphi(b) = \overline{1}$, cela ne change rien, sauf que dans ce cas il est préférable d'écrire la table de $(G,*)$ en intervertissant a et b). φ est une bijection.

Première méthode :
Il faut montrer que :
$$\varphi(e * a) = \varphi(e) + \varphi(a);\ \varphi(a * e) = \varphi(a) + \varphi(e);\ \varphi(e * b) = \varphi(e) + \varphi(b);$$
$$\varphi(b * e) = \varphi(b) + \varphi(e);\ \varphi(a * b) = \varphi(a) + \varphi(b);\ \varphi(b * a) = \varphi(b) + \varphi(a);$$
$$\varphi(a * a) = \varphi(a) + \varphi(a);\ \varphi(b * b) = \varphi(b) + \varphi(b)$$
Cela va être long, on passe à la deuxième méthode.

Deuxième méthode :

On va comparer les tables des deux groupes $(G,*)$ et $(\mathbb{Z}/3\mathbb{Z},+)$.

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

On constate que le e, le a et le b sont aux mêmes endroits que le $\overline{0}$, le $\overline{1}$ et le $\overline{2}$. Ces deux groupes sont isomorphes.

Montrons que $(G,*)$ est isomorphe à $\left(\left\{1, e^{\frac{2i\pi}{3}}, e^{\frac{4i\pi}{3}}\right\},\times\right)$, on va écrire la table de ce groupe.

On remarque que :

$$e^{\frac{2i\pi}{3}} \times e^{\frac{2i\pi}{3}} = e^{\frac{4i\pi}{3}};\ e^{\frac{2i\pi}{3}} \times e^{\frac{4i\pi}{3}} = 1 \ \ et \ \ e^{\frac{4i\pi}{3}} \times e^{\frac{4i\pi}{3}} = e^{\frac{8i\pi}{3}} = e^{\frac{2i\pi}{3}}$$

La commutativité de la multiplication fait le reste.

$\times$	1	$e^{\frac{2i\pi}{3}}$	$e^{\frac{4i\pi}{3}}$
1	1	$e^{\frac{2i\pi}{3}}$	$e^{\frac{4i\pi}{3}}$
$e^{\frac{2i\pi}{3}}$	$e^{\frac{2i\pi}{3}}$	$e^{\frac{4i\pi}{3}}$	1
$e^{\frac{4i\pi}{3}}$	$e^{\frac{4i\pi}{3}}$	1	$e^{\frac{2i\pi}{3}}$

On constate que le e, le a et le b sont aux mêmes endroits que le 1, le $e^{\frac{2i\pi}{3}}$ et le $e^{\frac{4i\pi}{3}}$. Ces deux groupes sont isomorphes.

Remarque : $e^{\frac{2i\pi}{3}} = j$ et $e^{\frac{4i\pi}{3}} = j^2$.

Montrons que $(G,*)$ est isomorphe à $(\{(1,2,3),(2,3,1),(3,1,2)\},\circ)$, on va écrire la table de ce groupe.

On pose

$$id = (1,2,3) = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}; c_1 = (2,3,1) = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}; c_2 = (3,1,2) = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

On remarque :

$$c_1 \circ c_2 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \circ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\\1&2&3\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = id$$

$$c_2 \circ c_1 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \circ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\\1&2&3\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = id$$

$$c_2 \circ c_2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \circ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = c_1$$

$$c_1 \circ c_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \circ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = c_2$$

$\circ$	id	c_1	c_2
id	id	c_1	c_2
c_1	c_1	c_2	id
c_2	c_2	id	c_1

On constate que le e, le a et le b sont aux mêmes endroits que le id, le c_1 et le c_2. Ces deux groupes sont isomorphes.

Allez à : Exercice 26

4.

a) Si $a^2 = a$ alors $a = e$ (on a déjà vu cela dans les exercices précédents), ce qui est impossible car $a \neq e$, donc $a^2 \neq a$ de même $b^2 \neq b$ et $c^2 \neq c$.
Supposons que $a^2 \neq e$, $b^2 \neq e$ et $c^2 \neq e$.
Que vaut a^2 ? $a^2 \in \{e,a,b,c\}$ par conséquent , soit $a^2 = b$ soit $a^2 = c$.

Si $a^2 = b$

L'ordre d'un élément divise l'ordre du groupe, si on appelle k l'ordre de a^2, comme l'ordre (=le cardinal) de G est 4, il existe $l \in \mathbb{N}$ tel que $4 = lk$ donc

$$b^2 = (a^2)^2 = a^4 = a^{kl} = (a^k)^l = e^l = e$$

Ce qui entraine que $b^2 = e$ ce qui est impossible.

Si $a^2 = c$

On montre de même que $c^2 = e$ ce qui est impossible aussi.

Par conséquent $a^2 \neq e$, $b^2 \neq e$ et $c^2 \neq e$ est faux, il y en a un des trois qui vaut e, l'énoncé impose que $b^2 = e$.

b) On suppose que $a * c = c * a = e$, on écrit la table intermédiaire.

$*$	e	a	b	c
e	e	a	b	c
a	a			e
b	b		e	
c	c	e		

En regardant la

a	a			e

ligne

$a^2 = b$ ou $a^2 = c$

Si $a^2 = c$ alors $a^3 = a * c = e$ (en multipliant à gauche par a), ce qui n'est pas possible d'après théorème de Lagrange car 3 ne divise pas 4.

On en déduit que $a^2 = b$.

En regardant la

c	a	e		

ligne

$c^2 = a$ ou $c^2 = b$

Si $c^2 = a$ alors $c^3 = c * a = e$ (en multipliant à droite par a), ce qui n'est pas possible car l'ordre de c : 3 ne divise pas 4.

On en déduit que $c^2 = a$.

Table intermédiaire

$*$	e	a	b	c
e	e	a	b	c
a	a	b		e
b	b		e	
c	c	e		a

En regardant la

a	a	b		e

ligne

On en déduit que $a * b = c$. Les valeurs e, a et b sont déjà prises.

En regardant la

c	c	e		a

ligne

On en déduit que $c * b = b$. Les valeurs e, a et c sont déjà prises.

En regardant la deuxième colonne (celle de a), $b * a = c$. Les valeurs e, a et b sont déjà prises.

En regardant la quatrième colonne (celle de c), $b * c = b$. Les valeurs e, a et c sont déjà prises.

Table complète

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	b
c	c	e	b	a

Remarque :

Ce n'est pas la seule méthode possible, on aurait pu raisonner sur les colonnes ou simultanément sur les lignes et les colonnes …

Montrons que $(G,*)$ est isomorphe à $(\mathbb{Z}/4\mathbb{Z},+)$, pour cela on va écrire la table de $(\mathbb{Z}/4\mathbb{Z},+)$.

On pose $\varphi: G \to \mathbb{Z}/4\mathbb{Z}$ définit par $\varphi(e) = \overline{0}$, $\varphi(a) = \overline{1}$, $\varphi(b) = \overline{2}$ et $\varphi(c) = \overline{3}$, il s'agit d'une bijection.

Pour que cela soit un morphisme il faut vérifier que pour tout x et y dans G, $\varphi(x * y) = \varphi(x) + \varphi(y)$,

en particulier $\varphi(b*b)=\varphi(b)+\varphi(b) \Leftrightarrow \varphi(e)=\varphi(b)+\varphi(b) \Leftrightarrow \overline{0}=\varphi(b)+\varphi(b)$, il faut donc faire attention à l'ordre dans lequel on place les quatre éléments de $\mathbb{Z}/4\mathbb{Z}$ car le seul élément qui vérifie $\overline{0}=\overline{\alpha}+\overline{\alpha}$ est $\overline{\alpha}=\overline{2}$ (ceci dit si on ne fait pas attention le $\overline{2}$ tombe naturellement à la bonne place).

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

On constate que le e, le a, le b et le c sont aux mêmes endroits que le $\overline{0}$, le $\overline{1}$, le $\overline{2}$ et le $\overline{3}$. Ces deux groupes sont isomorphes.

Montrons que $(G,*)$ est isomorphe à $(\mathbb{Z}/4\mathbb{Z},+)$, pour cela on va écrire la table de $(\mathbb{Z}/4\mathbb{Z},+)$.

On pose $\varphi: G \to (\{1,i,-1,-i\},\times)$ définit par $\varphi(e)=1$, $\varphi(a)=i$, $\varphi(b)=-1$ et $\varphi(c)=-i$, il s'agit d'une bijection. Pour que cela soit un morphisme il faut vérifier que pour tout x et y dans G, $\varphi(x*y)=\varphi(x)\times\varphi(y)$, en particulier

$\varphi(b*b)=\varphi(b)\times\varphi(b) \Leftrightarrow \varphi(e)=\varphi(b)\times\varphi(b) \Leftrightarrow 1=\varphi(b)\times\varphi(b)$, il faut donc faire attention à l'ordre dans lequel on place les quatre éléments de $\{1,i,-1,-i\}$ car le seul élément qui vérifie $1=\alpha\times\alpha$ est $\alpha=-1$. Ici c'est moins évident parce que si on écrit $\{1,-1,i,-i\}$ on se complique sérieusement la vie car les deux tables ne vont pas se ressembler au premier coup d'œil.

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	-1
$-i$	$-i$	1	-1	i

On constate que le e, le a, le b et le c sont aux mêmes endroits que le 1 le i, le -1 et le $-i$. Ces deux groupes sont isomorphes.

Montrons que $(G,*)$ est isomorphe à $(\{(1,2,3,4),(2,3,4,1),(3,4,1,2),(4,1,2,3)\},\circ)$, pour cela on va écrire la table de $(\{(1,2,3,4),(2,3,4,1),(3,4,1,2),(4,1,2,3)\},\circ)$.

On pose

$$id=(1,2,3,4)=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$$
$$c_1=(2,3,4,1)=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$$
$$\alpha=(3,4,1,2)=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$$
$$c_2=(4,1,2,3)=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$$

Pour définir l'isomorphisme φ il faut « repérer » lequel de ces éléments, différent de l'identité, vérifie $\beta\circ\beta=id$ avec $\beta\in\{c_1,\alpha,c_2\}$

Pour remplir la table il faut calculer, $c_1\circ c_2$, $c_2\circ c_1$, $c_1\circ c_1$, $c_2\circ c_2$, $c_1\circ\alpha$, $\alpha\circ c_1$, $c_2\circ\alpha$, $\alpha\circ c_2$ et $\alpha\circ\alpha$.

$$c_1\circ c_2=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\circ\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&1&2&3\\1&2&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=id$$
$$c_2\circ c_1=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}\circ\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&3&4&1\\1&2&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=id$$
$$c_1\circ c_1=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\circ\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&3&4&1\\3&4&1&2\end{pmatrix}=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=\alpha$$
$$c_2\circ c_2=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}\circ\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&1&2&3\\3&4&1&2\end{pmatrix}=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=\alpha$$

$$c_1 \circ \alpha = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} \circ \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} = \begin{pmatrix}1&2&3&4\\3&4&1&2\\4&1&2&3\end{pmatrix} = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix} = c_2$$

$$\alpha \circ c_1 = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} \circ \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} = \begin{pmatrix}1&2&3&4\\2&3&4&1\\4&1&2&3\end{pmatrix} = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix} = c_2$$

$$c_2 \circ \alpha = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix} \circ \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} = \begin{pmatrix}1&2&3&4\\3&4&1&2\\2&3&4&1\end{pmatrix} = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} = c_1$$

$$\alpha \circ c_2 = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} \circ \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix} = \begin{pmatrix}1&2&3&4\\4&1&2&3\\2&3&4&1\end{pmatrix} = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} = c_1$$

$$\alpha \circ \alpha = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} \circ \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} = \begin{pmatrix}1&2&3&4\\3&4&1&2\\1&2&3&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} = id$$

Maintenant on va écrire la table de $\{id, c_1, \alpha, c_2\}$ dans cet ordre là, en tout les cas il faut mettre α à cette place parce que c'est le seul qui vérifie $\alpha^2 = id$, par contre rien n'empêche d'intervertir c_1 et c_2.

$\circ$	id	c_1	α	c_2
id	id	c_1	α	c_2
c_1	c_1	α	c_2	id
α	α	c_2	id	c_1
c_2	c_2	id	c_1	α

$\varphi: G \to \{(1,2,3,4), (2,3,4,1), (3,4,1,2), (4,1,2,3)\}$ définit par :
$\varphi(e) = id$, $\varphi(a) = c_1$, $\varphi(b) = \alpha$ et $\varphi(c) = c_2$, c'est une bijection et la table montre que c'est un morphisme de groupe parce que e, a, b et c sont aux mêmes places que id, c_1, α et c_2.

c) Si $a * a = c * c = e$, on rappelle que $b * b = e$.

Table intermédiaire

$*$	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			

Si on regarde la ligne

a	a	e		

$a * b = b$ ou $a *$ $b = c$

Si $a * b = b$ alors $a = e$ (en multipliant par b^{-1} à gauche ou à droite) ce qui est impossible car $a \neq e$.
Par conséquent $a * b = c$, puis en complétant cette ligne $a * c = b$.

On regarde la ligne

b	b		e	

$b * a = a$ ou $b *$ $a = c$

Si $b * a = a$ alors $b = e$ (en multipliant par a^{-1} à gauche ou à droite) ce qui est impossible car $b \neq e$.
Par conséquent $b * a = c$, puis en complétant cette ligne $b * c = a$.

Table intermédiaire

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c			

On regarde les trois dernières colonnes et on complète par l'élément qui manque.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Remarque :

Ce n'est pas la seule méthode.

Montrons que $(G,*)$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},+)$, pour cela on va écrire la table de $(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},+)$.

$+$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{1})$
$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{1})$
$(\overline{1},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{1})$
$(\overline{1},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$
$(\overline{0},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{0})$

On pose $\varphi: G\to\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, définit par :
$\varphi(e)=(\overline{0},\overline{0})$, $\varphi(a)=(\overline{1},\overline{0})$, $\varphi(b)=(\overline{1},\overline{1})$ et $\varphi(c)=(\overline{0},\overline{1})$, c'est une bijection et la table montre que c'est un morphisme de groupe parce que e, a, b et c sont aux mêmes places que $(\overline{0},\overline{0})$, $(\overline{1},\overline{0})$, $(\overline{1},\overline{1})$ et $(\overline{0},\overline{1})$.
Cela montre que pour tout $x,y\in\{e,a,b,c\}$, $\varphi(x*y)=\varphi(x)+\varphi(y)$.

Remarque :

Ce n'est pas le seul isomorphisme possible, si par exemple, on prend
$\varphi(e)=(\overline{0},\overline{0})$, $\varphi(a)=(\overline{1},\overline{1})$, $\varphi(b)=(\overline{1},\overline{0})$ et $\varphi(c)=(\overline{0},\overline{1})$, pour « visualiser » le morphisme sur la table, il faut écrire la table de $\left((\overline{0},\overline{0}),(\overline{1},\overline{1}),(\overline{1},\overline{0}),(\overline{0},\overline{1})\right)$ de façon à respecter les places.

Montrons que $(G,*)$ est isomorphe à $(\{(1,2,3,4),(1,2,4,3),(2,1,3,4),(2,1,4,3)\},\circ)$, pour cela on va écrire la table de $(\{(1,2,3,4),(1,2,4,3),(2,1,3,4),(2,1,4,3)\},\circ)$.
On pose

$$id=(1,2,3,4)=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$$
$$\tau_1=(1,2,4,3)=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}$$
$$\tau_2=(2,1,3,4)=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}$$
$$\beta=(2,1,4,3)=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$$

Il faut calculer $\tau_1\circ\tau_2$, $\tau_2\circ\tau_1$, $\tau_1\circ\beta$, $\beta\circ\tau_1$, $\tau_2\circ\beta$, $\beta\circ\tau_2$, $\tau_1\circ\tau_1$, $\tau_2\circ\tau_2$ et $\beta\circ\beta$.

$$\tau_1\circ\tau_2=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}\circ\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&1&3&4\\2&1&4&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=\beta$$
$$\tau_2\circ\tau_1=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}\circ\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&2&4&3\\2&1&4&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=\beta$$
$$\tau_1\circ\beta=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}\circ\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&1&4&3\\2&1&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}=\tau_2$$
$$\beta\circ\tau_1=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\circ\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&2&4&3\\2&1&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}=\tau_2$$
$$\tau_2\circ\beta=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}\circ\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&1&4&3\\1&2&4&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}=\tau_1$$
$$\beta\circ\tau_2=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\circ\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&1&3&4\\1&2&4&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}=\tau_1$$
$$\tau_1\circ\tau_1=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}\circ\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&2&4&3\\1&2&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=id$$

$$\tau_2 \circ \tau_2 = \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix} \circ \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\2&1&3&4\\1&2&3&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} = id$$

$$\beta \circ \beta = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix} \circ \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix} = \begin{pmatrix}1&2&3&4\\2&1&4&3\\1&2&3&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} = id$$

Maintenant on va écrire la table de $\{id, \tau_1, \tau_2, \beta\}$, dans cet exercice l'ordre de τ_1, τ_2 et β n'a pas d'importance.

$*$	id	τ_1	τ_2	β
id	id	τ_1	τ_2	β
τ_1	τ_1	id	β	τ_2
τ_2	τ_2	β	id	τ_1
β	β	τ_2	τ_1	id

On pose $\varphi: G \to \{(1,2,3,4), (1,2,4,3), (2,1,3,4), (2,1,4,3)\}$ définit par :
$\varphi(e) = id$, $\varphi(a) = \tau_1$, $\varphi(b) = \tau_2$ et $\varphi(c) = \beta$, c'est une bijection et la table montre que c'est un morphisme de groupe parce que e, a, b et c sont aux mêmes places que id, τ_1, τ_2 et β.

d) Le symétrique de $a \in \{e, a, b, c\}$, ce ne peut pas être e sinon $a = e$, ce ne peut pas être b car b est son propre symétrique (car $b^2 = b * b = e$) donc soit $a^{-1} = a$ soit $a^{-1} = c$.
Si $a^{-1} = a$ alors $a * a = e$, d'autre part le symétrique de $c \in \{e, a, b, c\}$, ce ne peut-être e, ni b et ni a car dans ce cas le symétrique de a est a, par conséquent le symétrique de c est c et donc $c * c = e$.
Si $a^{-1} = c$ alors $a * c = c * a = e$ par définition d'un symétrique.
On a deux solution soit $a * c = c * a = e$ soit $a * a = c * c = e$.

Allez à : Exercice 26

5. Il suffit de regarder la table de chacun de ces groupes, elles sont toutes symétriques suivant la diagonale (en haut à gauche, en bas à droite).

Allez à : Exercice 26

Correction exercice 27.

$$\sigma^2 = \sigma \circ \sigma = \begin{pmatrix}1&2&3&4&5\\3&4&2&5&1\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\3&4&2&5&1\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\3&4&2&5&1\\2&5&4&1&3\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\2&5&4&1&3\end{pmatrix}$$

$$\sigma^3 = \sigma^2 \circ \sigma = \begin{pmatrix}1&2&3&4&5\\2&5&4&1&3\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\3&4&2&5&1\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\3&4&2&5&1\\4&1&5&3&2\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\4&1&5&3&2\end{pmatrix}$$

$$\sigma^4 = \sigma^3 \circ \sigma = \begin{pmatrix}1&2&3&4&5\\4&1&5&3&2\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\3&4&2&5&1\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\3&4&2&5&1\\5&3&1&2&4\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\5&3&1&2&4\end{pmatrix}$$

$$\sigma^5 = \sigma^4 \circ \sigma = \begin{pmatrix}1&2&3&4&5\\5&3&1&2&4\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\3&4&2&5&1\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\3&4&2&5&1\\1&2&3&4&5\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}$$

$$= id$$

L'ordre de σ est 5.

$$\rho^2 = \rho \circ \rho = \begin{pmatrix}1&2&3&4&5\\5&4&1&2&3\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\5&4&1&2&3\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\5&4&1&2&3\\3&2&5&4&1\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\3&2&5&4&1\end{pmatrix}$$

$$\rho^3 = \rho^2 \circ \rho = \begin{pmatrix}1&2&3&4&5\\3&2&5&4&1\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\5&4&1&2&3\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\5&4&1&2&3\\1&4&3&2&5\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\1&4&3&2&5\end{pmatrix}$$

$$\rho^4 = \rho^3 \circ \rho = \begin{pmatrix}1&2&3&4&5\\1&4&3&2&5\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\5&4&1&2&3\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\5&4&1&2&3\\5&2&1&4&3\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\5&2&1&4&3\end{pmatrix}$$

$$\rho^5 = \rho^4 \circ \rho = \begin{pmatrix}1&2&3&4&5\\5&2&1&4&3\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\5&4&1&2&3\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\5&4&1&2&3\\3&4&5&2&1\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\3&4&5&2&1\end{pmatrix}$$

$$\rho^6 = \rho^5 \circ \rho = \begin{pmatrix}1&2&3&4&5\\3&4&5&2&1\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\5&4&1&2&3\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\5&4&1&2&3\\1&2&3&4&5\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}$$
$$= id$$

L'ordre de ρ est 6.

Remarque :

Le cardinal de $\mathcal{S}_5$ est $5! = 120$ et l'ordre de σ divise bien 120 et l'ordre de ρ divise bien 120.

$$\sigma\rho = \sigma \circ \rho = \begin{pmatrix}1&2&3&4&5\\3&4&2&5&1\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\5&4&1&2&3\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\5&4&1&2&3\\1&5&3&4&2\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\1&5&3&4&2\end{pmatrix}$$
$$(\sigma\rho)^2 = \begin{pmatrix}1&2&3&4&5\\1&5&3&4&2\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\1&5&3&4&2\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\1&5&3&4&2\\1&2&3&4&5\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}$$

L'ordre de $\sigma\rho$ est 2.

$$\rho\sigma = \rho \circ \sigma = \begin{pmatrix}1&2&3&4&5\\5&4&1&2&3\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\3&4&2&5&1\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\3&4&2&5&1\\1&2&4&3&5\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\1&2&4&3&5\end{pmatrix}$$
$$(\rho\sigma)^2 = \begin{pmatrix}1&2&3&4&5\\1&2&4&3&5\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\1&2&4&3&5\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\1&2&4&3&5\\1&2&3&4&5\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}$$

L'ordre de $\rho\sigma$ est 2.

Autre méthode :

$$(\sigma\rho)^2 = id \Leftrightarrow \sigma\rho\sigma\rho = id \Leftrightarrow \sigma\rho\sigma = \rho^{-1}$$

En multipliant à droite par ρ^{-1}.

$$(\sigma\rho)^2 = id \Leftrightarrow \rho\sigma\rho\sigma = id$$

En multipliant à gauche par ρ.

$$(\sigma\rho)^2 = id \Leftrightarrow (\rho\sigma)^2 = id$$

Remarque :

$\sigma\rho$ intervertit 2 et 5, c'est une transposition, donc son carré rechange 2 et 5, il était donc clair que le carré de $\sigma\rho$ était égal à l'identité. Même remarque pour $\rho\sigma$, c'est la transposition qui intervertit 3 et 4.

$$\rho^6 = id \Leftrightarrow \rho \circ \rho^5 = \rho^5 \circ \rho = id$$

Cela montre que $\rho^{-1} = \rho^5$, l'égalité $\rho^5 \circ \rho = id$ est une évidence parce qu'il est clair que ρ^5 et ρ commutent, en fait, dans ce cas on peut se contenter d'écrire que $\rho \circ \rho^5 = id$ pour en déduire que $\rho^{-1} = \rho^5$.

$$\sigma\rho^{-1} = \sigma \circ \rho^{-1} = \sigma \circ \rho^5 = \begin{pmatrix}1&2&3&4&5\\3&4&2&5&1\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\3&4&5&2&1\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\3&4&5&2&1\\2&5&1&4&3\end{pmatrix}$$
$$= \begin{pmatrix}1&2&3&4&5\\2&5&1&4&3\end{pmatrix}$$
$$(\sigma\rho^{-1})^2 = \begin{pmatrix}1&2&3&4&5\\2&5&1&4&3\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\2&5&1&4&3\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\2&5&1&4&3\\5&3&2&4&1\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\5&3&2&4&1\end{pmatrix}$$

Ici, si on est malin, on peut s'apercevoir que le carré de cette permutation est l'identité car cela revient à intervertir, à la fois 2 et 3 et puis 1 et 5.

$$(\sigma\rho^{-1})^3 = (\sigma\rho^{-1})^2 \circ \sigma\rho^{-1} = \begin{pmatrix}1&2&3&4&5\\5&3&2&4&1\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\2&5&1&4&3\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\2&5&1&4&3\\3&1&5&4&2\end{pmatrix}$$
$$= \begin{pmatrix}1&2&3&4&5\\3&1&5&4&2\end{pmatrix}$$
$$(\sigma\rho^{-1})^4 = (\sigma\rho^{-1})^3 \circ \sigma\rho^{-1} = \begin{pmatrix}1&2&3&4&5\\3&1&5&4&2\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\2&5&1&4&3\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\2&5&1&4&3\\1&2&3&4&5\end{pmatrix}$$
$$= \begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix} = id$$

L'ordre de $\sigma\rho^{-1}$ est 4.

Comme

$$\sigma^5 = \sigma^4 \circ \sigma = id \Leftrightarrow \sigma^{-1} = \sigma^4$$

$$\rho\sigma^{-1} = \rho \circ \sigma^{-1} = \rho \circ \sigma^4 = \begin{pmatrix}1&2&3&4&5\\5&4&1&2&3\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\5&3&1&2&4\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\5&3&1&2&4\\3&1&5&4&2\end{pmatrix}$$

$$= \begin{pmatrix}1&2&3&4&5\\3&1&5&4&2\end{pmatrix}$$

$$(\rho\sigma^{-1})^2 = \begin{pmatrix}1&2&3&4&5\\3&1&5&4&2\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\3&1&5&4&2\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\3&1&5&4&2\\5&3&2&4&1\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\5&3&2&4&1\end{pmatrix}$$

$$(\rho\sigma^{-1})^3 = (\rho\sigma^{-1})^2 \circ \rho\sigma^{-1} = \begin{pmatrix}1&2&3&4&5\\5&3&2&4&1\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\3&1&5&4&2\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\3&1&5&4&2\\2&5&1&4&3\end{pmatrix}$$

$$= \begin{pmatrix}1&2&3&4&5\\2&5&1&4&3\end{pmatrix}$$

$$(\rho\sigma^{-1})^4 = (\rho\sigma^{-1})^3 \circ \rho\sigma^{-1} = \begin{pmatrix}1&2&3&4&5\\2&5&1&4&3\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\3&1&5&4&2\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\3&1&5&4&2\\1&2&3&4&5\end{pmatrix}$$

$$= \begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix} = id$$

L'ordre de $\rho\sigma^{-1}$ est 4.

Autre méthode :

$$(\rho\sigma^{-1})^{-1} = (\sigma^{-1})^{-1}\rho^{-1} = \sigma\rho^{-1}$$

L'ordre de $\sigma\rho^{-1}$ est 4 donc l'ordre de $(\rho\sigma^{-1})^{-1}$ est 4, par conséquent l'ordre de $\rho\sigma^{-1}$ est 4.

Allez à : Exercice 27

Correction exercice 28.

Remarque :

Dans cet exercice on confondra le complexe z et le point d'affixe z. En particulier lorsque l'on parlera d'une rotation ou d'une symétrie, en général ce genre d'application transforme un point en un autre point, ici ces applications transforment un complexe en un autre complexe.

1. $\forall k \in \{0,1,2,3,4\}$

$$\sigma\left(e^{\frac{2ik\pi}{5}}\right) = \overline{e^{\frac{2ik\pi}{5}}} = e^{-\frac{2ik\pi}{5}} = e^{\frac{2i(-k)\pi}{5}}$$

On fait la division euclidienne de $-k$ par 5, il existe un unique couple $(q,r) \in \mathbb{Z} \times \{0,1,2,3,4\}$ tel que :

$$-k = 5q + r$$

Donc

$$\sigma\left(e^{\frac{2ik\pi}{5}}\right) = e^{\frac{2i(5q+r)\pi}{5}} = e^{\frac{2i\times 5q\pi}{5}} e^{\frac{2ir\pi}{5}} = e^{2iq\pi} e^{\frac{2ir\pi}{5}} = e^{\frac{2ir\pi}{5}} \in P$$

On vient de montrer que pour tout $z \in P$, $\sigma(z) \in P$, autrement dit P est invariant par σ.

$$\rho\left(e^{\frac{2ik\pi}{5}}\right) = e^{\frac{2ik\pi}{5}} e^{\frac{2i\pi}{5}} = e^{\frac{2i(k+1)\pi}{5}}$$

On fait la division euclidienne de $k+1$ par 5, il existe un unique couple $(q,r) \in \mathbb{Z} \times \{0,1,2,3,4\}$ tel que :

$$k + 1 = 5q + r$$

Donc

$$\rho\left(e^{\frac{2ik\pi}{5}}\right) = e^{\frac{2i(5q+r)\pi}{5}} = e^{\frac{2i\times 5q\pi}{5}} e^{\frac{2ir\pi}{5}} = e^{2iq\pi} e^{\frac{2ir\pi}{5}} = e^{\frac{2ir\pi}{5}} \in P$$

On vient de montrer que pour tout $z \in P$, $\rho(z) \in P$, autrement dit P est invariant par ρ.

Allez à : Exercice 28

2. Pour tout $z = Re^{i\theta} \in \mathbb{C}$

$$\rho(z) = Re^{i\theta} e^{\frac{2i\pi}{5}} = Re^{i\theta + \frac{2i\pi}{5}} = Re^{i\left(\theta + \frac{2\pi}{5}\right)}$$

$\rho(z)$ est le nombre complexe de module $R = |z|$ et d'argument $\theta + \frac{2\pi}{5}$, le point d'affixe $\rho(z)$ est l'image de z par la rotation d'angle $\theta + \frac{2\pi}{5} - \theta = \frac{2\pi}{5}$.

$$\rho^2(z) = \rho\big(\rho(z)\big) = \rho\left(Re^{i\left(\theta+\frac{2\pi}{5}\right)}\right) = Re^{i\left(\theta+\frac{2\pi}{5}\right)}e^{\frac{2i\pi}{5}} = Re^{i\left(\theta+\frac{4\pi}{5}\right)}$$

$\rho^2(z)$ est le nombre complexe de module $R = |z|$ et d'argument $\theta + \frac{4\pi}{5}$, le point d'affixe $\rho^2(z)$ est l'image de z par la rotation d'angle $\theta + \frac{4\pi}{5} - \theta = \frac{4\pi}{5}$.

$$\rho^3(z) = \rho^2\big(\rho(z)\big) = \rho^2\left(Re^{i\left(\theta+\frac{2\pi}{5}\right)}\right) = Re^{i\left(\theta+\frac{4\pi}{5}\right)}e^{\frac{2i\pi}{5}} = Re^{i\left(\theta+\frac{6\pi}{5}\right)}$$

$\rho^3(z)$ est le nombre complexe de module $R = |z|$ et d'argument $\theta + \frac{6\pi}{5}$, le point d'affixe $\rho^3(z)$ est l'image de z par la rotation d'angle $\theta + \frac{6\pi}{5} - \theta = \frac{6\pi}{5}$.

$$\rho^4(z) = \rho^3\big(\rho(z)\big) = \rho^3\left(Re^{i\left(\theta+\frac{2\pi}{5}\right)}\right) = Re^{i\left(\theta+\frac{6\pi}{5}\right)}e^{\frac{2i\pi}{5}} = Re^{i\left(\theta+\frac{8\pi}{5}\right)}$$

$\rho^4(z)$ est le nombre complexe de module $R = |z|$ et d'argument $\theta + \frac{8\pi}{5}$, le point d'affixe $\rho^4(z)$ est l'image de z par la rotation d'angle $\theta + \frac{8\pi}{5} - \theta = \frac{8\pi}{5}$.

$$\rho^5(z) = \rho^4\big(\rho(z)\big) = \rho^4\left(Re^{i\left(\theta+\frac{2\pi}{5}\right)}\right) = Re^{i\left(\theta+\frac{8\pi}{5}\right)}e^{\frac{2i\pi}{5}} = Re^{i\left(\theta+\frac{10\pi}{5}\right)} = Re^{i(\theta+2\pi)}$$

$\rho^4(z)$ est le nombre complexe de module $R = |z|$ et d'argument $\theta + 2\pi$, le point d'affixe $\rho^4(z)$ est l'image de z par la rotation d'angle $\theta + 2\pi - \theta = 2\pi$, autrement dit $\rho^5 = id$.
Par une récurrence assez immédiate, on en déduit que pour tout $q \in \mathbb{Z}$, $\rho^{5q} = id$.
Remarque : les puissances négatives sont les bijections réciproques des puissances positives, par exemple ρ^{-5} est la bijection réciproque de $\rho^5 = id$, par conséquent $\rho^{-5} = id$.
Pour tout $k \in \mathbb{Z}$, effectuons la division euclidienne de k par 5 :
Il existe un unique couple $(q, r) \in \mathbb{Z} \times \{0,1,2,3,4\}$ tel que : $k = 5q + r$

$$\rho^k(z) = \rho^{5q+r}(z) = \rho^r\big(\rho^{5q}(z)\big) = \rho^r(z)$$

Or pour tout $r \in \{0,1,2,3,4\}$, ρ^r est une rotation d'angle $\frac{2r\pi}{5}$ comme on l'a vu plus haut, donc pour tout $k \in \mathbb{Z}$ ρ^k est une rotation d'angle $\frac{2r\pi}{5}$ où r est le reste de la division euclidienne de k par 5.
Au passage on a montré que $\rho^5 = id$ et que pour tout $\in \{0,1,2,3,4\}$ $\rho^k \neq id$, l'ordre de ρ est 5.

Allez à : Exercice 28

3. Rappel : $s: \mathbb{C} \to \mathbb{C}$ est une symétrie si et seulement si la somme des arguments de z et $s(z)$ est constant modulo 2π et si les modules de z et $s(z)$ sont égaux, s est alors la symétrie par rapport à la droite passant par l'origine et d'angle $\frac{\arg(\sigma\rho(z))+\arg(z)}{2}$.
Pour tout $z = Re^{i\theta} \in \mathbb{C}$,

$$\sigma\rho(z) = \sigma\big(\rho(z)\big) = \sigma\left(Re^{i\left(\theta+\frac{2\pi}{5}\right)}\right) = \overline{Re^{i\left(\theta+\frac{2\pi}{5}\right)}} = Re^{-i\left(\theta+\frac{2\pi}{5}\right)}$$

On a $|\sigma\rho(z)| = R = |z|$ et $\arg\big(\sigma\rho(z)\big) + \arg(z) = -\left(\theta + \frac{2\pi}{5}\right) + \theta + 2k\pi = -\frac{2\pi}{5} + 2k\pi$
$\sigma\rho$ est la symétrie par rapport à la droite passant par l'origine et d'angle $\frac{-\frac{2\pi}{5}}{2} = -\frac{\pi}{5}$.

$$\sigma\rho^2(z) = \sigma\big(\rho^2(z)\big) = \sigma\left(Re^{i\left(\theta+\frac{4\pi}{5}\right)}\right) = \overline{Re^{i\left(\theta+\frac{4\pi}{5}\right)}} = Re^{-i\left(\theta+\frac{4\pi}{5}\right)}$$

On a $|\sigma\rho^2(z)| = R = |z|$ et $\arg\big(\sigma\rho^2(z)\big) + \arg(z) = -\left(\theta + \frac{4\pi}{5}\right) + \theta + 2k\pi = -\frac{4\pi}{5} + 2k\pi$
$\sigma\rho^2$ est la symétrie par rapport à la droite passant par l'origine et d'angle $\frac{-\frac{4\pi}{5}}{2} = -\frac{2\pi}{5}$.

$$\sigma\rho^3(z) = \sigma\big(\rho^3(z)\big) = \sigma\left(Re^{i\left(\theta+\frac{6\pi}{5}\right)}\right) = \overline{Re^{i\left(\theta+\frac{6\pi}{5}\right)}} = Re^{-i\left(\theta+\frac{6\pi}{5}\right)}$$

On a $|\sigma\rho^3(z)| = R = |z|$ et $\arg\big(\sigma\rho^3(z)\big) + \arg(z) = -\left(\theta + \frac{6\pi}{5}\right) + \theta + 2k\pi = -\frac{6\pi}{5} + 2k\pi$

$\sigma\rho^3$ est la symétrie par rapport à la droite passant par l'origine et d'angle $\frac{-\frac{6\pi}{5}}{2} = -\frac{3\pi}{5}$.

$$\sigma\rho^4(z) = \sigma\left(\rho^4(z)\right) = \sigma\left(Re^{i\left(\theta+\frac{8\pi}{5}\right)}\right) = \overline{Re^{i\left(\theta+\frac{8\pi}{5}\right)}} = Re^{-i\left(\theta+\frac{8\pi}{5}\right)}$$

On a $|\sigma\rho^4(z)| = R = |z|$ et $\arg\left(\sigma\rho^4(z)\right) + \arg(z) = -\left(\theta + \frac{8\pi}{5}\right) + \theta + 2k\pi = -\frac{8\pi}{5} + 2k\pi$

$\sigma\rho^4$ est la symétrie par rapport à la droite passant par l'origine et d'angle $\frac{-\frac{8\pi}{5}}{2} = -\frac{4\pi}{5}$.

Remarque :

On aurait pu traiter tous ces cas en une seule fois de la façon suivante :
Pour tout $n \in \{0,1,2,3,4\}$

$$\sigma\rho^n(z) = \sigma\left(\rho^n(z)\right) = \sigma\left(Re^{i\left(\theta+\frac{2n\pi}{5}\right)}\right) = \overline{Re^{i\left(\theta+\frac{2n\pi}{5}\right)}} = Re^{-i\left(\theta+\frac{2n\pi}{5}\right)}$$

On a $|\sigma\rho^n(z)| = R = |z|$ et $\arg\left(\sigma\rho^n(z)\right) + \arg(z) = -\left(\theta + \frac{2n\pi}{5}\right) + \theta + 2k\pi = -\frac{2n\pi}{5} + 2k\pi$

$\sigma\rho^n$ est la symétrie par rapport à la droite passant par l'origine et d'angle $\frac{-\frac{2n\pi}{5}}{2} = -\frac{n\pi}{5}$.

Pour les transformations $\rho^n\sigma$, on va tout traiter en une seule fois.
Pour tout $z = Re^{i\theta} \in \mathbb{C}$

$$\rho^n\sigma(z) = \rho^n\left(\sigma(z)\right) = \rho^n(\overline{z}) = \rho^n\left(Re^{-i\theta}\right) = Re^{i\left(-\theta+\frac{2n\pi}{5}\right)}$$

On a $|\rho^n\sigma(z)| = R = |z|$ et $\arg\left(\rho^n\sigma(z)\right) + \arg(z) = -\theta + \frac{2n\pi}{5} + \theta + 2k\pi = \frac{2n\pi}{5} + 2k\pi$

$\rho^n\sigma$ est la symétrie par rapport à la droite passant par l'origine et d'angle $\frac{\frac{2n\pi}{5}}{2} = \frac{n\pi}{5}$.

Allez à : Exercice 28

4. Si s est une symétrique différente de l'identité (l'identité est une symétrie par rapport à n'importe qu'elle droite et d'angle 0) alors $s^2 = id$, l'ordre d'une symétrie est 2.

Remarque :

Si $s = id$ son ordre est 1.

Allez à : Exercice 28

5. Pour tout $z = Re^{i\theta} \in \mathbb{C}$, on pose r le reste de la division euclidienne de $n + m$ par 5.

$$(\sigma\rho^n)(\rho^m\sigma)(z) = \sigma\rho^{n+m}\sigma(z) = \sigma\rho^r\sigma(z) = \sigma\rho^r\left(\sigma(z)\right) = \sigma\rho^r\left(Re^{-i\theta}\right) = \sigma\left(\rho^r\left(Re^{-i\theta}\right)\right)$$
$$= \sigma\left(Re^{i\left(-\theta+\frac{r\pi}{5}\right)}\right) = Re^{-i\left(-\theta+\frac{r\pi}{5}\right)} = Re^{i\left(\theta-\frac{r\pi}{5}\right)} = \rho^{-r}(z)$$

Donc $(\sigma\rho^n)(\rho^n\sigma) = \rho^{-r}$

$$(\rho^n\sigma)(\sigma\rho^n)(z) = \rho^n\sigma\sigma\rho^n = \rho^n\sigma^2\rho^n = \rho^n\rho^n = \rho^{2n} = \rho^r$$

Donc $(\rho^n\sigma)(\sigma\rho^n) = \rho^r$

Remarque :

On est obligé de faire deux cas car la composée des fonctions n'est pas commutative.

Allez à : Exercice 28

6. Si un groupe contient σ et ρ alors il contient toutes les transformations de la forme $\sigma^n\rho^m$ avec $n \in \{0,1\}$ et $m \in \{0,1,2,3,4\}$ ce qui en fait $2 \times 5 = 10$ mais pour l'instant rien ne dit qu'il n'y en a pas plus en particulier $\rho\sigma$ doit être dans le groupe mais à première vue il n'est pas de la forme $\sigma^n\rho^m$ alors il va falloir réfléchir.
On pose $G = \left\{\sigma^n\rho^m, n \in \{0,1\}, m \in \{0,1,2,3,4\}\right\}$. On va montrer que G muni de la composée des applications est un sous-groupe du groupe des bijections de $\mathbb{C}$ sur $\mathbb{C}$.
$id = \sigma^0\rho^0 \in G$
Soit $\alpha_1 = \sigma^{n_1}\rho^{m_1}$ et $\alpha_2 = \sigma^{n_2}\rho^{m_2}$ deux éléments de G.

$$\alpha_1\alpha_2^{-1} = \sigma^{n_1}\rho^{m_1}(\sigma^{n_2}\rho^{m_2})^{-1} = \sigma^{n_1}\rho^{m_1}\rho^{-m_2}\sigma^{-n_2}$$

Le but est de montrer que $\alpha_1\alpha_2^{-1} \in G$, c'est-à-dire qu'il existe $n \in \{0,1\}$ et $m \in \{0,1,2,3,4\}$ $\alpha_1\alpha_2^{-1} = \sigma^n\rho^m$.

Premier cas : $n_2 = 0$

$$\alpha_1\alpha_2^{-1} = \sigma^{n_1}\rho^{m_1}\rho^{-m_2}\sigma^0 = \sigma^{n_1}\rho^{m_1-m_2} \in G$$

Deuxième cas : $n_2 = 1$ et $n_1 = 1$

$\sigma^{-1} = \sigma$ car $\sigma^2 = id$ donc

$$\alpha_1\alpha_2^{-1} = \sigma^{n_1}\rho^{m_1}\rho^{-m_2}\sigma^{-n_2} = \sigma\rho^{m_1-m_2}\sigma = \rho^r = \sigma^0\rho^r \in G$$

où r est le reste de la division euclidienne de $m_1 - m_2$ par 5 d'après la question 5°).

Troisième cas : $n_2 = 1$ et $n_1 = 0$,

$$\alpha_1\alpha_2^{-1} = \sigma^{n_1}\rho^{m_1}\rho^{-m_2}\sigma^{-n_2} = \rho^{m_1-m_2}\sigma = \rho^r\sigma$$

On a vu à la question 3°) que

$\sigma\rho^n$ est la symétrie par rapport à la droite passant par l'origine et d'angle $-\frac{n\pi}{5}$ et que $\rho^r\sigma$ est la symétrie par rapport à la droite passant par l'origine et d'angle $\frac{r\pi}{5}$.

$\sigma\rho$ est la symétrie par rapport à la droite passant par l'origine et d'angle $-\frac{\pi}{5}$ et que $\rho^4\sigma$ est la symétrie par rapport à la droite passant par l'origine et d'angle $\frac{4\pi}{5}$. Or l'angle définissant une droite passant par l'origine est définie à π près (quand on fait faire un demi-tour à une droite on retombe sur la même droite) on en déduit que : $\rho^4\sigma$ est la symétrie par rapport à la droite passant par l'origine et d'angle $\frac{4\pi}{5} - \pi = -\frac{\pi}{5}$. Par conséquent

$$\sigma\rho = \rho^4\sigma$$

De même $\sigma\rho^2 = \rho^3\sigma$, $\sigma\rho^3 = \rho^2\sigma$ et $\sigma\rho^4 = \rho\sigma$, bref pour tout $r \in \{1,2,3,4\}$ $\rho^r\sigma = \sigma\rho^{5-r}$ d'où

$$\alpha_1\alpha_2^{-1} = \rho^r\sigma = \sigma\rho^{5-r}$$

Comme $r \in \{1,2,3,4\}$ entraine que $5 - r \in \{1,2,3,4\}$ on a bien montré que $\alpha_1\alpha_2^{-1} \in G$

Le cas $r = 0$ est trivial car $\alpha_1\alpha_2^{-1} = \rho^r\sigma = \sigma = \sigma\rho^0 \in G$.

Dans tous les cas $\alpha_1\alpha_2^{-1} \in G$, cela montre bien que G est un sous-groupe du groupe des bijections de $\mathbb{C}$ sur $\mathbb{C}$.

Remarque :

(a) Si dans le 3. l'énoncé avait demandé de montrer que « pour tout $n \in \mathbb{Z}$, $\sigma\rho^n$ et $\rho^n\sigma$ sont des symétries par rapport à un axe passant par l'origine, dont on donnera l'angle par rapport à l'axe réel » la rédaction de ce troisième cas aurait été plus simple (mais il aurait fallu travailler davantage au 3.).

(b) σ est d'ordre 2, 2 divise le cardinal de G et ρ est d'ordre 5 donc 5 divise le cardinal de G, on en déduit que $2 \times 5 = 10$ divise l'ordre de G (car 2 et 5 sont premiers entre eux), mais rien ne dit qu'il n'y a pas de groupe contenant σ et ρ d'ordre $10k$, d'ailleurs c'est le cas.

Allez à : Exercice 28

Correction exercice 29.

1. Rappel : l'ordre d'un élément g d'un groupe $(G,*)$ est le plus petit entier strictement positif p tel que

$$\underbrace{g * g * \ldots * g}_{p\times} = e$$

e étant l'élément neutre.

Souvent on note multiplicativement les lois abstraites et la condition ci-dessus s'écrit : $g^n = e$

$\mathbb{Z}/n\mathbb{Z}$ est un groupe pour l'addition (et certainement pas pour la multiplication) donc l'ordre d'un élément $a \in \mathbb{Z}/n\mathbb{Z}$ est le plus petit entier strictement positif p tel que :

$$\underbrace{a + a + \cdots + a}_{p\times} = \overline{0}$$

Car $\overline{0}$ est l'élément neutre de $(\mathbb{Z}/n\mathbb{Z}, +)$.

Cette condition s'écrit $pa = \overline{0}$.

Il faut montrer que le plus petit entier p tel que $p\overline{1} = \overline{0}$ est n.

Il existe $l \in \mathbb{Z}$ tel que $p \times 1 = ln$, manifestement $l < 0$ et $l = 0$ sont impossible donc $l \geq 1$ alors $ln \geq n$ donc $p \geq n$, comme $n \times 1 = 1 \times n$ on a $p = n$ (avec $l = 1$).

Allez à : Exercice 29

2. Par contraposition pour montrer que :

« Si l'ordre de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$ vaut n alors k est premier avec n »

On va montrer que :

« Si k n'est pas premier avec n alors l'ordre de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$ ne vaut pas n »

$n = ud \quad et \quad k = vd$ avec $u > 0$ et $v > 0$ premiers entre eux, on en déduit que : $nv = ku$

$d > 1$ car n et k ne sont pas premiers entre eux, comme $ud = n$ on a $u < n$.

$nv = ku \Rightarrow \overline{u}\overline{k} = \overline{0} \Rightarrow u\overline{k} = \overline{0}$, l'ordre de $\overline{k}$ est inférieur ou égal à u avec $0 < u < n$ ce qui montre bien que l'ordre de $\overline{k}$ n'est pas n.

Réciproque :

On appelle p l'ordre de $\overline{k}$. Comme $n\overline{k} = \overline{0}$ l'ordre de $\overline{k}$ est inférieur à n. On a $p\overline{k} = \overline{0}$. Ce qui implique qu'il existe $l \in \mathbb{N}$ tel que $pk = ln$. Comme k divise n et que k est premier avec n, d'après le théorème de Gauss k divise l, il existe donc $a \in \mathbb{N}^*$ tel que $l = ka$, ce que l'on remplace dans $pk = ln$, $pk = kan \Leftrightarrow p = an$ ce qui entraine que $p \geq n$, on rappelle que $0 < p \leq n$ pour en déduire que $p = n$.

Allez à : Exercice 29

3. Il existe $p \in \mathbb{N}$ tel que $n = pk$, il faut montrer que p est l'ordre de $\overline{k}$. On appelle q l'ordre de $\overline{k}$.

$p\overline{k} = \overline{n} = \overline{0}$ donc $q \leq p$. Comme q est l'ordre de $\overline{k}$, $q\overline{k} = \overline{0}$ donc il existe $l \in \mathbb{N}$ tel que $qk = ln$, or $n = pk$ ce que l'on remplace dans $qk = ln$, cela donne $qk = lpk \Leftrightarrow q = lp$ ce qui entraine que $q \geq p$ (l ne peut être nul car un ordre n'est pas nul), on en déduit que $q = p$.

L'ordre de $\overline{k}$ est p où $n = pk$.

Allez à : Exercice 29

4. Par définition de f, pour tout $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$

$$f(\overline{k}) = a^k$$

Est-ce que f est bien définie ? on peut avoir $\overline{k} = \overline{k'}$ sans que $k = k'$ mais a-t-on $f(\overline{k}) = f(\overline{k'})$?

Si $\overline{k'} = \overline{k}$, il existe $l \in \mathbb{Z}$ tel que $k' = k + ln$ donc

$$f(\overline{k'}) = a^{k+ln} = a^k a^{ln} = a^k (a^n)^l = a^k e^l = a^k e = a^k = f(\overline{k})$$

Car pour tout élément g dans G de cardinal n, $g^n = e$.

L'application f est bien définie.

Montrons que $e, a, a^2, \dots, a^{n-1}$ sont tous distincts.

S'il existe $k, l \in \{0,1, \dots, n-1\}$, $k \neq l$ tels que $a^k = a^l$ alors $a^k a^{-l} = e$ ce qui implique que $a^{k-l} = e$,

On fait la division euclidienne de $k - l$ par n, il existe un unique $(q, r) \in \mathbb{Z} \times \{0,1, \dots, n-1\}$ tel que :

$$k - l = qn + r$$

$$a^{k-l} = e \Leftrightarrow a^{qn+r} = e \Leftrightarrow (a^n)^q a^r = e \Leftrightarrow a^r = e$$

r est strictement inférieur à l'ordre de a, c'est-à-dire n donc $r = 0$. On en déduit que $k - l$ est un multiple de l'ordre de a c'est-à-dire de n, $k - l = qn$.

$$\begin{cases} 0 \leq k \leq n-1 \\ 0 \leq l \leq n-1 \end{cases} \Rightarrow \begin{cases} 0 \leq k \leq n-1 \\ -(n-1) \leq -l \leq 0 \end{cases} \Rightarrow -(n-1) \leq k - l \leq n-1$$

Le seul multiple de n dans $\{-(n-1), \dots, -1, 0, 1, \dots, n-1\}$ est 0, ce qui entraine que $k = l$, effectivement les $e, a, a^2, \dots, a^{n-1}$ sont tous distincts. Cette démonstration fait partie du cours mais c'est ce que demande cet exercice.

Les n éléments de $\{0,1, \dots, n-1\}$ ont tous une image distincte dans l'ensemble à n éléments de $\{e, a, \dots, a^{n-1}\}$, f est une bijection. Il reste à montrer qu'il s'agit d'un morphisme de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans $(G, *)$

$$f(\overline{k+l}) = a^{k+l} = a^k a^l = f(\overline{k}) f(\overline{l})$$

f est un isomorphisme de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans $(G, *)$.

Allez à : Exercice 29

Correction exercice 30.

1.

a) 2 est un nombre premier donc $(\mathbb{Z}/2\mathbb{Z}, +, \times)$ est un corps.

b)

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

2.

a)

$$(\bar{a},\bar{b})\oplus(\bar{c},\bar{d})=(\bar{a}+\bar{c},\bar{b}+\bar{d})=(\overline{a+c},\overline{b+d})=(\overline{c+a},\overline{d+c})=(\bar{c}+\bar{a},\bar{d}+\bar{b})$$
$$=(\bar{c},\bar{d})\oplus(\bar{a},\bar{b})$$

La loi $\oplus$ est commutative.

$$(\bar{a},\bar{b})\oplus(\bar{c},\bar{d})=(\overline{a+c},\overline{b+d})\in\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$$

b) La loi $\oplus$ est interne.

$$(\bar{a},\bar{b})\oplus\big((\bar{c},\bar{d})\oplus(\bar{e},\bar{f})\big)=(\bar{a},\bar{b})\oplus(\bar{c}+\bar{e},\bar{d}+\bar{f})=(\bar{a},\bar{b})\oplus(\overline{c+e},\overline{d+f})$$
$$=(\bar{a}+\overline{c+e},\bar{b}+\overline{d+f})=(\overline{a+c+e},\overline{b+d+f})=(\overline{a+c}+\bar{e},\overline{b+d}+\bar{f})$$
$$=(\overline{a+c},\overline{b+d})\oplus(\bar{e},\bar{f})=(\bar{a}+\bar{c},\bar{b}+\bar{d})\oplus(\bar{e},\bar{f})=\big((\bar{a},\bar{b})\oplus(\bar{c},\bar{d})\big)\oplus(\bar{e},\bar{f})$$

Donc la loi $\oplus$ est associative.

$$(\bar{a},\bar{b})\oplus(\bar{0},\bar{0})=(\bar{a}+\bar{0},\bar{b}+\bar{0})=(\overline{a+0},\overline{b+0})=(\bar{a},\bar{b})$$

Donc $(\bar{0},\bar{0})$ est l'élément neutre pour la loi $\oplus$.

Et enfin $(\overline{-a},\overline{-b})\in A$ est le symétrique de $(\bar{a},\bar{b})$, car

$$(\bar{a},\bar{b})\oplus(\overline{-a},\overline{-b})=(\bar{a}+\overline{-a},\bar{b}+\overline{-b})=(\overline{a-a},\overline{b-b})=(\bar{0},\bar{0})$$

c)

$$(\bar{a},\bar{b})\otimes(\bar{c},\bar{d})=(\bar{a}\times\bar{c},\bar{b}\times\bar{d})=(\overline{ac},\overline{bd})=(\overline{ca},\overline{da})=(\bar{c}\times\bar{a},\bar{d}\times\bar{b})=(\bar{c},\bar{d})\otimes(\bar{a},\bar{b})$$

donc la loi $\otimes$ est commutative.

c) $(\bar{a},\bar{b})\otimes(\bar{c},\bar{d})=(\bar{a}\times\bar{c},\bar{b}\times\bar{d})=(\overline{ac},\overline{bd})\in A$

Donc la loi $\otimes$ est une loi interne.

d)

$$(\bar{a},\bar{b})\otimes\big((\bar{c},\bar{d})\oplus(\bar{e},\bar{f})\big)=(\bar{a},\bar{b})\otimes(\bar{c}+\bar{e},\bar{d}+\bar{f})=(\bar{a},\bar{b})\otimes(\overline{c+e},\overline{d+f})$$
$$=(\bar{a}\times\overline{c+e},\bar{b}\times\overline{d+f})=(\overline{a(c+e)},\overline{b(d+f)})=(\overline{ac+ae},\overline{bd+bf})$$
$$=(\overline{ac}+\overline{ae},\overline{bd}+\overline{bf})=(\overline{ac},\overline{bd})\oplus(\overline{ae},\overline{bf})=(\bar{a}\times\bar{c},\bar{b}\times\bar{d})\oplus(\bar{a}\times\bar{e},\bar{b}\times\bar{f})$$
$$=(\bar{a},\bar{b})\otimes(\bar{c},\bar{d})\oplus(\bar{a},\bar{b})\otimes(\bar{e},\bar{f})$$

Donc la multiplication est distributive sur l'addition.

e)

$$(\bar{a},\bar{b})\otimes(\bar{1},\bar{1})=(\bar{a}\times\bar{1},\bar{b}\times\bar{1})=(\bar{a},\bar{b})$$

Donc $(\bar{1},\bar{1})$ est l'élément neutre pour la multiplication.

f) Toutes les propriétés ci-dessus montre que $(A,\oplus,\otimes)$ est un anneau commutatif unitaire.

Pour montrer que c'est un corps il reste à montrer que chaque $(\bar{a},\bar{b})$ différent de $(\bar{0},\bar{0})$ admet un symétrique $(\overline{a'},\overline{b'})\in A$ pour la multiplication.

Allez à : Exercice 30

Correction exercice 31.

1.

Remarque préliminaire :

Pour tout $f\in E$:

$$f(x)=\begin{cases}1 & \text{si } f(x)\neq 0\\ 0 & \text{si } f(x)=0\end{cases}=\begin{cases}1 & \text{si } f(x)=1\\ 0 & \text{si } f(x)=0\end{cases}$$

En effet $f(x) = 1 \Leftrightarrow f(x) \neq 0$ et évidemment $f(x) = 0 \Leftrightarrow f(x) = 0$.

Montrons que $(E,\oplus)$ est un groupe abélien (commutatif).

$(f \oplus g)(x) = \begin{cases} 1 & \text{si } f(x) \neq g(x) \\ 0 & \text{si } f(x) = g(x) \end{cases}$ donc $f \oplus g \in E$, $\oplus$ est une loi interne.

Soit $\theta_S : S \to \{0,1\}$ définie par pour $x \in S$, $\theta_S(x) = 0$, $\theta_S \in E$ donc E est non vide.

Pour tout $f \in E$ et pour tout $x \in S$:

$$(f \oplus \theta_S)(x) = \begin{cases} 1 & \text{si } f(x) \neq \theta_S(x) = 0 \\ 0 & \text{si } f(x) = \theta_S(x) = 0 \end{cases} = f(x)$$

$$(\theta_S \oplus f)(x) = \begin{cases} 1 & \text{si } \theta_S(x) \neq f(x) = 0 \\ 0 & \text{si } \theta_S(x) = f(x) = 0 \end{cases} = f(x)$$

$$f \oplus \theta_S = \theta_S \oplus f = f$$

θ_S est l'élément neutre.

Pour tout $f \in E$ et pour tout $x \in S$:

$$(f \oplus f)(x) = \begin{cases} 1 & \text{si } f(x) \neq f(x) \\ 0 & \text{si } f(x) = g(x) \end{cases} = 0 = \theta_S$$

Donc le symétrique de f est f. (Et donc tous les éléments de E admettent un symétrique).

Commutativité :

Pour tout $f, g \in E$ et pour tout $x \in S$:

$$(f \oplus g)(x) = \begin{cases} 1 & \text{si } f(x) \neq g(x) \\ 0 & \text{si } f(x) = g(x) \end{cases} = \begin{cases} 1 & \text{si } g(x) \neq f(x) \\ 0 & \text{si } g(x) = f(x) \end{cases} = (g \oplus f)(x)$$

Donc

$$f \oplus g = g \oplus f$$

$\oplus$ est commutative.

Associativité :

Pour tout $f, g, h \in E$ et pour tout $x \in S$:

$$\big((f \oplus g) \oplus h\big)(x) = \begin{cases} 1 & \text{si } (f \oplus g)(x) \neq h(x) \\ 0 & \text{si } (f \oplus g)(x) = h(x) \end{cases}$$

$$\big(f \oplus (g \oplus h)\big)(x) = \begin{cases} 1 & \text{si } f(x) \neq (g \oplus h)(x) \\ 0 & \text{si } f(x) = (g \oplus h)(x) \end{cases}$$

$$(f \oplus g)(x) = \begin{cases} 1 & \text{si } f(x) \neq g(x) \\ 0 & \text{si } f(x) = g(x) \end{cases}$$

$$(g \oplus h)(x) = \begin{cases} 1 & \text{si } g(x) \neq h(x) \\ 0 & \text{si } g(x) = h(x) \end{cases}$$

Si $f(x) = 0, g(x) = 0$ et $h(x) = 0$

$\forall x \in S, (f \oplus g)(x) = 0$ et $h(x) = 0$ donc $\big((f \oplus g) \oplus h\big)(x) = 0$

$\forall x \in S, (g \oplus h)(x) = 0$ et $f(x) = 0$ donc $\big(f \oplus (g \oplus h)\big)(x) = 0$

$$\big((f \oplus g) \oplus h\big)(x) = \big(f \oplus (g \oplus h)\big)(x)$$

Si $f(x) = 0, g(x) = 0$ et $h(x) = 1$

$\forall x \in S, (f \oplus g)(x) = 0$ et $h(x) = 1$ donc $\big((f \oplus g) \oplus h\big)(x) = 1$

$\forall x \in S, (g \oplus h)(x) = 1$ et $f(x) = 0$ donc $\big(f \oplus (g \oplus h)\big)(x) = 1$

$$\big((f \oplus g) \oplus h\big)(x) = \big(f \oplus (g \oplus h)\big)(x)$$

Si $f(x) = 0, g(x) = 1$ et $h(x) = 0$

$\forall x \in S, (f \oplus g)(x) = 1$ et $h(x) = 0$ donc $\big((f \oplus g) \oplus h\big)(x) = 1$

$\forall x \in S, (g \oplus h)(x) = 1$ et $f(x) = 0$ donc $\big(f \oplus (g \oplus h)\big)(x) = 1$

$$\big((f \oplus g) \oplus h\big)(x) = \big(f \oplus (g \oplus h)\big)(x)$$

Si $f(x) = 0, g(x) = 1$ et $h(x) = 1$

$\forall x \in S, (f \oplus g)(x) = 1$ et $h(x) = 1$ donc $\big((f \oplus g) \oplus h\big)(x) = 0$

$\forall x \in S, (g \oplus h)(x) = 0$ et $f(x) = 0$ donc $\big(f \oplus (g \oplus h)\big)(x) = 0$

$$\big((f \oplus g) \oplus h\big)(x) = \big(f \oplus (g \oplus h)\big)(x)$$

Si $f(x) = 1, g(x) = 0$ et $h(x) = 0$

$\forall x \in S, (f \oplus g)(x) = 1$ et $h(x) = 0$ donc $\big((f \oplus g) \oplus h\big)(x) = 1$
$\forall x \in S, (g \oplus h)(x) = 0$ et $f(x) = 1$ donc $\big(f \oplus (g \oplus h)\big)(x) = 1$
$$\big((f \oplus g) \oplus h\big)(x) = \big(f \oplus (g \oplus h)\big)(x)$$
Si $f(x) = 1, g(x) = 0$ et $h(x) = 1$
$\forall x \in S, (f \oplus g)(x) = 1$ et $h(x) = 1$ donc $\big((f \oplus g) \oplus h\big)(x) = 0$
$\forall x \in S, (g \oplus h)(x) = 1$ et $f(x) = 1$ donc $\big(f \oplus (g \oplus h)\big)(x) = 0$
$$\big((f \oplus g) \oplus h\big)(x) = \big(f \oplus (g \oplus h)\big)(x)$$
Si $f(x) = 1, g(x) = 1$ *et* $h(x) = 0$
$\forall x \in S, (f \oplus g)(x) = 0$ et $h(x) = 0$ donc $\big((f \oplus g) \oplus h\big)(x) = 0$
$\forall x \in S, (g \oplus h)(x) = 1$ et $f(x) = 1$ donc $\big(f \oplus (g \oplus h)\big)(x) = 0$
$$\big((f \oplus g) \oplus h\big)(x) = \big(f \oplus (g \oplus h)\big)(x)$$
Si $f(x) = 1, g(x) = 1$ *et* $h(x) = 1$
$\forall x \in S, (f \oplus g)(x) = 0$ et $h(x) = 1$ donc $\big((f \oplus g) \oplus h\big)(x) = 1$
$\forall x \in S, (g \oplus h)(x) = 0$ et $f(x) = 1$ donc $\big(f \oplus (g \oplus h)\big)(x) = 1$
$$\big((f \oplus g) \oplus h\big)(x) = \big(f \oplus (g \oplus h)\big)(x)$$
Dans tous les cas, c'est-à-dire pour tout $x \in S$, pour tout $f, g, h \in E$
$$\big((f \oplus g) \oplus h\big)(x) = \big(f \oplus (g \oplus h)\big)(x)$$
Donc
$$(f \oplus g) \oplus h = f \oplus (g \oplus h)$$
La loi $\oplus$ est associative.
Autre méthode pour montrer l'associativité
On pose $F_0 = \{x \in S, f(x) = 0\}$, $F_1 = \{x \in S, f(x) = 1\}$, $G_0 = \{x \in S, g(x) = 0\}$, $G_1 = \{x \in S, f(x) = 1\}$,
$H_0 = \{x \in S, h(x) = 0\}$ et $H_1 = \{x \in S, h(x) = 1\}$.
On remarque que l'ensemble des $x \in S$ tels que $f(x) \neq g(x)$ est $(F_0 \cap G_1) \cup (F_1 \cap G_0)$ et que l'ensemble des $x \in S$ tels que $f(x) = g(x)$ est $(F_0 \cap G_0) \cup (F_1 \cap G_1)$.
De même l'ensemble des $x \in S$ tels que $g(x) \neq h(x)$ est $(G_0 \cup H_0) \cap (H_1 \cup G_1)$.
$$\big((f \oplus g) \oplus h\big)(x) = \begin{cases} 1 \text{ si } \begin{cases} 1 \text{ si } f(x) \neq g(x) \\ 0 \text{ si } f(x) = g(x) \end{cases} \neq \begin{cases} 1 \text{ si } h(x) = 1 \\ 0 \text{ si } h(x) = 0 \end{cases} \\ 0 \text{ si } \begin{cases} 1 \text{ si } f(x) \neq g(x) \\ 0 \text{ si } f(x) = g(x) \end{cases} = \begin{cases} 1 \text{ si } h(x) = 1 \\ 0 \text{ si } h(x) = 0 \end{cases} \end{cases}$$
L'ensemble des $x \in S$ tels que $\big((f \oplus g) \oplus h\big)(x) = 0$ est l'ensemble des $x \in S$ tels que :
$(f(x) \neq g(x)$ et $h(x) = 1)$ ou $(f(x) = g(x)$ et $h(x) = 0)$.
Le première ensemble est :
$$\big((F_0 \cap G_1) \cup (F_1 \cap G_0)\big) \cap H_1 = \big((F_0 \cap G_1) \cap H_1\big) \cup \big((F_1 \cap G_0) \cap H_1\big)$$
$$= (F_0 \cap G_1 \cap H_1) \cup (F_1 \cap G_0 \cap H_1)$$
Le deuxième ensemble est :
$$\big((F_0 \cap G_0) \cup (F_1 \cap G_1)\big) \cap H_0 = \big((F_0 \cap G_0) \cap H_0\big) \cup \big((F_1 \cap G_1) \cap H_0\big)$$
$$= (F_0 \cap G_0 \cap H_0) \cup (F_1 \cap G_1 \cap H_0)$$
Autrement dit si $\big(f(x), g(x), h(x)\big) \in \{(0,1,1), (1,0,1), (0,0,0), (1,1,0)\}$ alors
$$\big((f \oplus g) \oplus h\big)(x) = 0$$
Dans tous les autres cas, c'est-à-dire si $\big(f(x), g(x), h(x)\big) \in \{(1,0,0), (0,1,0), (0,0,1), (1,1,1)\}$ alors
$$\big((f \oplus g) \oplus h\big)(x) = 1$$
$$\big(f \oplus (g \oplus h)\big)(x) = \begin{cases} 1 \text{ si } \begin{cases} 1 \text{ si } f(x) = 1 \\ 0 \text{ si } f(x) = 0 \end{cases} \neq \begin{cases} 1 \text{ si } g(x) \neq h(x) \\ 0 \text{ si } g(x) = h(x) \end{cases} \\ 0 \text{ si } \begin{cases} 1 \text{ si } f(x) = 1 \\ 0 \text{ si } f(x) = 0 \end{cases} = \begin{cases} 1 \text{ si } g(x) \neq h(x) \\ 0 \text{ si } g(x) = h(x) \end{cases} \end{cases}$$
L'ensemble des $x \in S$ tels que $\big(f \oplus (g \oplus h)\big)(x) = 0$ est l'ensemble des $x \in S$ tels que :
$(f(x) = 1$ et $g(x) \neq h(x))$ ou $(f(x) = 0$ et $g(x) = h(x))$.
Le premier ensemble est :

$$F_1 \cap \big((G_0 \cap H_1) \cup (G_1 \cap H_0)\big) = \big(F_1 \cap (G_0 \cap H_1)\big) \cup \big(F_1 \cap (G_1 \cap H_0)\big)$$
$$= (F_1 \cap G_0 \cap H_1) \cup (F_1 \cap G_1 \cap H_0)$$

Le deuxième ensemble :

$$F_0 \cap \big((G_0 \cap H_0) \cup (G_1 \cap H_1)\big) = \big(F_0 \cap (G_0 \cap H_0)\big) \cup \big(F_0 \cap (G_1 \cap H_1)\big)$$
$$= (F_0 \cap G_0 \cap H_0) \cup (F_0 \cap G_1 \cap H_1)$$

Autrement dit si $\big(f(x), g(x), h(x)\big) \in \{(1,0,1), (1,1,0), (0,0,0), (0,1,1)\}$ alors

$$\big(f \oplus (g \oplus h)\big)(x) = 0$$

Dans tous les autres cas, c'est-à-dire si $\big(f(x), g(x), h(x)\big) \in \{(1,0,0), (0,1,0), (0,0,1), (1,1,1)\}$ alors

$$\big(f \oplus (g \oplus h)\big)(x) = 1$$

Finalement pour tout $x \in S$, $\big((f \oplus g) \oplus h\big)(x) = \big(f \oplus (g \oplus h)\big)(x)$ et donc

$$(f \oplus g) \oplus h = \big(f \oplus (g \oplus h)\big)$$

La loi $\oplus$ est associative.

$(E, \oplus)$ est un groupe abélien.

Allez à : Exercice 31

2. Montrons que ϕ est une bijection de F sur E.
Pour toute partie $f \in E$, on pose $A = f^{-1}(1) = \{x \in S, f(x) = 1\}$
$\phi(A) = \mathbb{I}_A$ définie par :
Si $x \in A$, $\phi(A)(x) = \mathbb{I}_A(x) = 1$ et si $x \notin A$, $\phi(A)(x) = \mathbb{I}_A(x) = 0$. Or si $x \in A$, $f(x) = 1$ et si $x \notin A$ $f(x) = 0$, on a $\mathbb{I}_A = f$, autrement dit pour tout $f \in E$, il existe $A \in F$ ($A = f^{-1}(1) = \{x \in S, f(x) = 1\}$) tel que :

$$f = \phi(A)$$

Cela montre que ϕ est surjective et même bijective parce qu'il est assez peu vraisemblable qu'il puisse exister un autre ensemble A' qui vérifie $f = \phi(A')$ mais on va quand même faire l'effort de montrer l'injectivité.
Pour montrer que $\phi(A) = \phi(A') \Rightarrow A = A'$ on va montrer que $A \neq A' \Rightarrow \phi(A) \neq \phi(A')$
Il existe, soit $x \in A$ et $x \notin A'$ soit $x \notin A$ et $x \in A'$. Prenons le premier cas (le second se traite exactement de la même façon).

$$\phi(A)(x) = \mathbb{I}_A(x) = 1 \quad \text{et} \quad \phi(A')(x) = \mathbb{I}_{A'}(x) = 0$$

Donc $\phi(A) \neq \phi(A')$, ϕ est injective et donc bijective.
Il reste à montrer que ϕ est un morphisme de (F, Δ) vers $(E, \oplus)$.
Pour tout $A, B \in F$. Pour tout $x \in S$

$$\phi(A \Delta B)(x) = \mathbb{I}_{A \Delta B}(x)$$

On rappelle que $A \Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$ et que donc $\{A \setminus B, B \setminus A, A \cap B, A \cup B\}$ forme une partition de S.
Si $x \in A \setminus B$ alors $\mathbb{I}_{A \Delta B}(x) = 1$
Si $x \in B \setminus A$ alors $\mathbb{I}_{A \Delta B}(x) = 1$
Si $x \in A \cap B$ alors $\mathbb{I}_{A \Delta B}(x) = 0$
Si $x \in \overline{A \cup B}$ alors $\mathbb{I}_{A \Delta B}(x) = 0$

$$\big(\phi(A) \oplus \phi(A')\big)(x) = (\mathbb{I}_A \oplus \mathbb{I}_B)(x) = \begin{cases} 1 & \text{si } \mathbb{I}_A(x) \neq \mathbb{I}_B(x) \\ 0 & \text{si } \mathbb{I}_A(x) = \mathbb{I}_B(x) \end{cases}$$

Si $x \in A \setminus B$ alors $\mathbb{I}_A(x) = 1$ et $\mathbb{I}_B(x) = 0$ donc $(\mathbb{I}_A \oplus \mathbb{I}_B)(x) = 1$
Si $x \in B \setminus A$ alors $\mathbb{I}_A(x) = 0$ et $\mathbb{I}_B(x) = 1$ donc $(\mathbb{I}_A \oplus \mathbb{I}_B)(x) = 1$
Si $x \in A \cap B$ alors $\mathbb{I}_A(x) = 1$ et $\mathbb{I}_B(x) = 1$ donc $(\mathbb{I}_A \oplus \mathbb{I}_B)(x) = 0$
Si $x \in \overline{A \cup B}$ alors $\mathbb{I}_A(x) = 0$ et $\mathbb{I}_B(x) = 0$ donc $(\mathbb{I}_A \oplus \mathbb{I}_B)(x) = 0$
Par conséquent pour tout $x \in S$:

$$\phi(A \Delta B)(x) = \big(\phi(A) \oplus \phi(A')\big)(x)$$

Et que donc

$$\phi(A \Delta B) = \phi(A) \oplus \phi(A')$$

ϕ est un morphisme, comme ϕ est bijective c'est un isomorphisme, donc ϕ^{-1} est un isomorphisme de $(E, \oplus)$ sur (F, Δ) or $(E, \oplus)$ est un groupe abélien, on en déduit que (F, Δ) est un groupe. Que tout élément soit son propre symétrique provient du fait que dans $(E, \oplus)$ tout élément est son propre

symétrique, redémontrons le. Il est à peu près clair que $\phi(\emptyset) = \theta_S$ ce qui montre que l'élément neutre de (F, Δ) est $\emptyset$.
Pour tout $A \in F$, il existe (un unique) $f \in E$ tel que $A = \phi^{-1}(f)$ or pour tout $f \in E$, $f \oplus f = \theta_S$ d'où

$$A\Delta A = \phi^{-1}(f)\Delta\phi^{-1}(f) = \phi^{-1}(f \oplus f) = \phi^{-1}(\theta_S) = \emptyset$$
$$A\Delta A = \emptyset$$

Chaque élément de F est son propre symétrique.
Allez à : Exercice 31

3. Pour tous $x, y \in G$,

$$x^2 = e \Leftrightarrow x * x = e \Leftrightarrow x^{-1} = x$$
$$y^2 = e \Leftrightarrow y * y = e \Leftrightarrow y^{-1} = y$$
$$(x * y)^2 = e \Leftrightarrow x * y = (x * y)^{-1} = y^{-1} * x^{-1} = y * x$$

Cela montre bien que $x * y = y * x$, G est abélien.
Allez à : Exercice 31

4. $\forall x \in G,\ (x = x \text{ ou } x = ax) \Leftrightarrow x \sim x$ donc $\sim$ est réflexive.

$$\forall x, y \in G, \quad x \sim y \Leftrightarrow (x = y \text{ ou } x = ay) \Leftrightarrow (y = x \text{ ou } y = a^{-1}x)$$

Dans G tous les éléments sont leur propre symétrique donc $a^2 = e \Leftrightarrow a * a = e$, ce qui signifie que $a^{-1} = a$.
Par conséquent

$$\forall x, y \in G, \quad x \sim y \Leftrightarrow (y = x \text{ ou } y = ax) \Leftrightarrow y \sim x$$

La relation est symétrique.
$\forall x, y, z \in G$,

$$\begin{cases} x \sim y \\ y \sim z \end{cases} \Rightarrow \begin{cases} x = y \text{ ou } x = ay \\ y = z \text{ ou } y = az \end{cases} \Rightarrow \begin{cases} x = y \\ y = z \end{cases} \text{ ou } \begin{cases} x = y \\ y = az \end{cases} \text{ ou } \begin{cases} x = ay \\ y = z \end{cases} \text{ ou } \begin{cases} x = ay \\ y = az \end{cases}$$
$$\Rightarrow x = z \text{ ou } x = az \text{ ou } x = az \text{ ou } x = a^2 z = z$$
$$\Rightarrow \begin{cases} x = z \\ x = az \end{cases} \Rightarrow x \sim z$$

La relation est transitive.
Finalement la relation est une relation d'équivalence.
Soit $b \in G$ et $x \in \text{cl}(b)$, $x = b$ ou $x = ab$, la classe de b à au plus deux éléments b et ab, ces deux éléments peuvent-ils être égaux, $b = ab \Leftrightarrow e = a$ ce qui est impossible puisque $a \neq e$.

$$\text{cl}(b) = \{b, ab\}$$

Allez à : Exercice 31

5. Prenons deux éléments de $G/\sim$, $\text{cl}(x)$ et $\text{cl}(y)$. Or

$$\forall x, y \in G, \quad \text{cl}(x) * \text{cl}(y) = \text{cl}(xy) \in G/\sim$$

Car $xy \in G$. $*$ est une loi interne.
$\text{cl}(e) = \{e, a\} \in G/\sim$ donc $G/\sim$ n'est pas vide.
Il reste à chercher le symétrique d'un élément de $G/\sim$.
Pour cela il faut chercher l'élément neutre :

$$\forall x \in G, \text{cl}(x) * \text{cl}(e) = \text{cl}(xe) = \text{cl}(x) = \text{cl}(ex) = \text{cl}(e) * \text{cl}(x)$$

$\text{cl}(e) = \{e, a\}$ est l'élément neutre.

$$\forall x \in G, \text{cl}(x) * \text{cl}(x^{-1}) = \text{cl}(xx^{-1}) = \text{cl}(e) = \text{cl}(x^{-1}x) = \text{cl}(x^{-1}) * \text{cl}(x)$$

Donc $\text{cl}(x^{-1}) \in G/\sim$ (car $x^{-1} \in G$) est le symétrique de $\text{cl}(x)$.

$$\forall x, y, z \in G, \text{cl}(x) * \big(\text{cl}(y) * \text{cl}(z)\big) = \big(\text{cl}(x) * \text{cl}(y)\big) * \text{cl}(z)$$

La loi est associative.
$(G/\sim, *)$ est un groupe.

$$\forall x \in G, \text{cl}(x) * \text{cl}(x) = \text{cl}(x^2) = \text{cl}(e) \Leftrightarrow \text{cl}(x)^{-1} = \text{cl}(x)$$

Chaque élément est son propre symétrique.
Allez à : Exercice 31

6. On pose $n = card(G)$.

$G_1 = G/\sim$ est un groupe de cardinal $\frac{n}{2}$, puisqu'il y a deux éléments dans chaque classe et que l'ensemble des classes forment une partition de G.
G_1 est un groupe dont chaque élément est son propre symétrique donc on peut définir une relation d'équivalence $\sim_1$ (comme sur G) telle que $G_1/\sim_1$ soit un groupe dont tous les éléments sont leur propre symétrique. Comme précédemment le cardinal de $G_1/\sim_1$ est la moitié du cardinal de G_1, soit $\frac{n}{4}$.
On définit ainsi une suite de groupes quotients jusqu'à ce qu'il ne reste plus qu'un élément dans le dernier groupe quotient, on en déduit qu'il existe $p \in \mathbb{N}$ tel que $\frac{n}{2^p} = 1$, autrement dit $n = 2^p$.
Cette démonstration est un peu « vaseuse » mais j'espère que cela donne une idée de ce qu'il se passe. La mise en forme d'une démonstration « parfaite » avec une démonstration par récurrence rigoureuse ne me paraît pas utile.

Allez à : Exercice 31

Correction exercice 32.

1. Pour tout $i \in \{2,3,4,5,6\}$, $f_1 \circ f_i = f_i \circ f_1$ car $f_1 = id$.
   Pour tout $x \in \mathbb{R} \setminus \{0,1\}$

$$f_2 \circ f_2(x) = f_2(f_2(x)) = f_2(1-x) = 1-(1-x) = x = f_1(x) \Rightarrow f_2 \circ f_2 = f_1$$

$$f_2 \circ f_3(x) = f_2(f_3(x)) = f_2\left(\frac{1}{1-x}\right) = 1 - \frac{1}{1-x} = \frac{1-x-1}{1-x} = -\frac{x}{1-x} = \frac{x}{x-1} = f_5(x) \Rightarrow f_2 \circ f_3 = f_5$$

$$f_2 \circ f_4(x) = f_2(f_4(x)) = f_2\left(\frac{1}{x}\right) = 1 - \frac{1}{x} = \frac{x-1}{x} = f_6(x) \Rightarrow f_2 \circ f_4 = f_6$$

$$f_2 \circ f_5(x) = f_2(f_5(x)) = f_2\left(\frac{x}{x-1}\right) = 1 - \frac{x}{x-1} = \frac{x-1-x}{x-1} = \frac{-1}{x-1} = \frac{1}{1-x} = f_3(x) \Rightarrow f_2 \circ f_5 = f_3$$

On ne peut pas en déduire que $f_2 \circ f_6 = f_4$ car on ne sait pas que $(E,\circ)$ est un groupe, mais si l'énoncé est correct c'est le résultat que l'on va trouvé.

$$f_2 \circ f_6(x) = f_2(f_6(x)) = f_2\left(\frac{x-1}{x}\right) = 1 - \frac{x-1}{x} = \frac{x-(x-1)}{x} = \frac{1}{x} = f_4(x) \Rightarrow f_2 \circ f_6 = f_4$$

$$f_3 \circ f_2(x) = f_3(f_2(x)) = f_2(1-x) = \frac{1}{1-(1-x)} = \frac{1}{x} = f_4(x) \Rightarrow f_3 \circ f_2 = f_4$$

$$f_3 \circ f_3(x) = f_3(f_3(x)) = f_2\left(\frac{1}{1-x}\right) = \frac{1}{1-\frac{1}{1-x}} = \frac{1-x}{1-x-1} = \frac{1-x}{-x} = \frac{x-1}{x} = f_6(x) \Rightarrow f_3 \circ f_3 = f_6$$

$$f_3 \circ f_4(x) = f_3(f_4(x)) = f_2\left(\frac{1}{x}\right) = \frac{1}{1-\frac{1}{x}} = \frac{x}{x-1} = f_5(x) \Rightarrow f_3 \circ f_4 = f_5$$

$$f_3 \circ f_5(x) = f_3(f_5(x)) = f_2\left(\frac{x}{x-1}\right) = \frac{1}{1-\frac{x}{x-1}} = \frac{x-1}{x-1-x} = \frac{x-1}{-1} = 1-x = f_2(x) \Rightarrow f_3 \circ f_5 = f_2$$

$$f_3 \circ f_6(x) = f_3(f_6(x)) = f_2\left(\frac{x-1}{x}\right) = \frac{1}{1-\frac{x-1}{x}} = \frac{x}{x-(x-1)} = x = f_1(x) \Rightarrow f_3 \circ f_6 = f_1$$

$$f_4 \circ f_2(x) = f_4(f_2(x)) = f_4(1-x) = \frac{1}{1-x} = f_3(x) \Rightarrow f_4 \circ f_2 = f_3$$

$$f_4 \circ f_3(x) = f_4(f_3(x)) = f_4\left(\frac{1}{1-x}\right) = 1-x = f_2(x) \Rightarrow f_4 \circ f_3 = f_2$$

$$f_4 \circ f_4(x) = f_4(f_4(x)) = f_4\left(\frac{1}{x}\right) = x = f_1(x) \Rightarrow f_4 \circ f_4 = f_1$$

$$f_4 \circ f_5(x) = f_4(f_5(x)) = f_4\left(\frac{x}{x-1}\right) = \frac{x-1}{x} = f_6(x) \Rightarrow f_4 \circ f_5 = f_6$$

$$f_4 \circ f_6(x) = f_4(f_6(x)) = f_4\left(\frac{x-1}{x}\right) = \frac{x}{x-1} = f_5(x) \Rightarrow f_4 \circ f_6 = f_5$$

$$f_5 \circ f_2(x) = f_5\big(f_2(x)\big) = f_5(1-x) = \frac{1-x}{1-x-1} = \frac{1-x}{-x} = \frac{x-1}{x} = f_6(x) \Rightarrow f_5 \circ f_2 = f_6$$

$$f_5 \circ f_3(x) = f_5\big(f_3(x)\big) = f_5\left(\frac{1}{1-x}\right) = \frac{\frac{1}{1-x}}{\frac{1}{1-x}-1} = \frac{1}{1-(1-x)} = \frac{1}{x} = f_4(x) \Rightarrow f_5 \circ f_3 = f_4$$

$$f_5 \circ f_4(x) = f_5\big(f_4(x)\big) = f_5\left(\frac{1}{x}\right) = \frac{\frac{1}{x}}{\frac{1}{x}-1} = \frac{1}{1-x} = f_3(x) \Rightarrow f_5 \circ f_4 = f_3$$

$$f_5 \circ f_5(x) = f_5\big(f_5(x)\big) = f_5\left(\frac{x}{x-1}\right) = \frac{\frac{x}{x-1}}{\frac{x}{x-1}-1} = \frac{x}{x-(x-1)} = x = f_1(x) \Rightarrow f_5 \circ f_5 = f_1$$

$$f_5 \circ f_6(x) = f_5\big(f_6(x)\big) = f_5\left(\frac{x-1}{x}\right) = \frac{\frac{x-1}{x}}{\frac{x-1}{x}-1} = \frac{x-1}{x-1-x} = \frac{x-1}{-1} = 1-x = f_2(x) \Rightarrow f_5 \circ f_6 = f_2$$

$$f_6 \circ f_2(x) = f_6\big(f_2(x)\big) = f_6(1-x) = \frac{1-x-1}{1-x} = \frac{-x}{1-x} = \frac{x}{x-1} = f_5(x) \Rightarrow f_6 \circ f_2 = f_5$$

$$f_6 \circ f_3(x) = f_6\big(f_3(x)\big) = f_5\left(\frac{1}{1-x}\right) = \frac{\frac{1}{1-x}-1}{\frac{1}{1-x}} = 1-(1-x) = x = f_1(x) \Rightarrow f_6 \circ f_3 = f_1$$

$$f_6 \circ f_4(x) = f_6\big(f_4(x)\big) = f_6\left(\frac{1}{x}\right) = \frac{\frac{1}{x}-1}{\frac{1}{x}} = 1-x = f_2(x) \Rightarrow f_6 \circ f_4 = f_2$$

$$f_6 \circ f_5(x) = f_6\big(f_5(x)\big) = f_6\left(\frac{x}{x-1}\right) = \frac{\frac{x}{x-1}-1}{\frac{x}{x-1}} = \frac{x-(x-1)}{x} = \frac{1}{x} = f_4(x) \Rightarrow f_6 \circ f_5 = f_4$$

$$f_6 \circ f_6(x) = f_6\big(f_6(x)\big) = f_6\left(\frac{x-1}{x}\right) = \frac{\frac{x-1}{x}-1}{\frac{x-1}{x}} = \frac{x-1-x}{x-1} = \frac{-1}{x-1} = \frac{1}{1-x} = f_3(x) \Rightarrow f_6 \circ f_6 = f_3$$

Ouf !!!!

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_4	f_6	f_5	f_2	f_1
f_4	f_4	f_3	f_2	f_1	f_6	f_5
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_5	f_1	f_2	f_4	f_3

Allez à : Exercice 32

2. $\circ$ est une loi interne, on le voit sur la table, pour tout $i, j \in \{1,2,3,4,5,6\}$, il existe $k \in \{1,2,3,4,5,6\}$ tel que : $f_i \circ f_j = f_k$
   f_1 est l'élément neutre.
   Chaque f_i admet un unique symétrique f_j car sur chaque ligne et chaque colonne il y a une et une seule fois f_1 qui est l'élément neutre.
   G est un sous-groupe de l'ensemble des bijections de $\mathbb{R} \setminus \{0,1\}$.

Allez à : Exercice 32

3. par exemple : $f_2 \circ f_5 = f_3$ et $f_5 \circ f_2 = f_6$ donc le groupe n'est pas abélien.

Allez à : Exercice 32

4. D'après le théorème de Lagrange, l'ordre des sous-groupes H de G divise l'ordre de G donc l'ordre des sous-groupes de G divise 6, leur ordre sont 1, 2, 3 et 6.
Si l'ordre est 1, $H = \{f_1\}$
Si l'ordre est 6, $H = \{f_1, f_2, f_3, f_4, f_5, f_6\}$.
Si l'ordre est 2, il y a f_1 et l'autre élément vérifie $f_i \circ f_i = f_1$ donc
$$H = \{f_1, f_2\} \quad \text{ou} \quad H = \{f_1, f_4\} \quad \text{ou} \quad H = \{f_1, f_5\}$$
Si l'ordre est 3, il y a f_1 et l'ordre des deux autres éléments n'est pas 2 puisque leur ordre doit diviser 3 autrement dit leur ordre est 3, donc il n'y a pas f_2, ni f_4, ni f_5. Il reste éventuellement f_3 et f_6, on écrit la table de $\{f_1, f_3, f_6\}$

$\circ$	f_1	f_3	f_6
f_1	f_1	f_3	f_6
f_3	f_3	f_6	f_1
f_6	f_6	f_1	f_3

La loi est interne, chaque élément admet un symétrique, c'est un sous-groupe de G et c'est le seul d'ordre 3.

Allez à : Exercice 32

5. Il sont d'ordre 1 pour $\{f_1\}$, d'ordre 2 pour $\{f_1, f_2\}$, $\{f_1, f_4\}$ et $\{f_1, f_4\}$, d'ordre 3 pour $\{f_1, f_3, f_6\}$ et d'ordre 6 pour $\{f_1, f_2, f_3, f_4, f_5, f_6\}$.

Allez à : Exercice 32

6. $< f_2 >= \{f_1, f_2\}$.

Allez à : Exercice 32

7. $< f_3 >= \{f_1, f_3, f_6\}$.

Allez à : Exercice 32

Correction exercice 33.

1.
$$\forall (x,y),(x',y') \in E \times F \qquad (x,y) \odot (x',y') = (x * x', y.y') \in E \times F$$
Car E étant un groupe, la loi est interne donc $x * x' \in E$, de même F est un groupe donc $y.y' \in F$
On note e_E l'élément neutre de E et e_F celui de F
$$\forall (x,y) \in E \times F \quad (x,y) \odot (e_E, e_F) = (x * e_E, y.e_F) = (x,y) = (e_E * x, e_F.y) = (e_E, e_F) \odot (x,y)$$
$$(x,y) \odot (e_E, e_F) = (x,y) = (e_E, e_F) \odot (x,y)$$
Montre que (e_E, e_F) est l'élément neutre pour la loi $\odot$.
On appelle x^{-1} le symétrique de x pour la loi $*$ et y^{-1} le symétrique de y pour la loi .
$$(x,y) \odot (x^{-1}, y^{-1}) = (x * x^{-1}, y.y^{-1}) = (e_E, e_F) = (x^{-1} * x, y^{-1}.y) = (x^{-1}, y^{-1}) \odot (x,y)$$
$$(x,y) \odot (x^{-1}, y^{-1}) = (e_E, e_F) = (x^{-1}, y^{-1}) \odot (x,y)$$
Montre que le symétrique de (x,y) pour la loi $\odot$ est $(x^{-1}, y^{-1}) \in E \times F$ en effet $x^{-1} \in E$ et $y^{-1} \in F$ car E et F sont des groupes.
Il reste l'associativité
$$\forall (x,y),(x',y'),(x'',y'') \in E \times F \quad (x,y) \odot \big((x',y') \odot (x'',y'')\big) = (x,y) \odot (x' * x'', y'.y'')$$
$$= \big(x * (x' * x''), y.(y'.y'')\big) = \big((x * x') * x'', (y.y').y''\big) = (x * x', y.y') \odot (x'',y'')$$
$$= ((x,y) \odot x', y')) \odot (x'',y'')$$
$$(x,y) \odot \big((x',y') \odot (x'',y'')\big) = ((x,y) \odot x', y')) \odot (x'',y'')$$
Montre que la loi $\odot$ est associative car $*$ et . sont deux lois associatives.
Finalement $(E \times F, \odot)$ est un groupe.

2. E' est un sous-groupe de E donc $e_E \in E'$, F' est un sous-groupe de F donc $e_F \in F'$, par conséquent $(e_E, e_F) \in E' \times F'$.
$\forall (x,y),(x',y') \in E' \times F'$, $(x,y) \odot (x',y')^{-1} = (x,y) \odot \big(x'^{-1}, y'^{-1}\big) = (x * x'^{-1}, y.y'^{-1})$
Comme E' est un sous-groupe de E, pour tout $x, x' \in E'$, $x * x'^{-1} \in E'$, de même comme F' est un sous-groupe de F, pour tout $y, y' \in F'$, $y.y'^{-1} \in F'$, par conséquent
$(x,y) \odot (x',y')^{-1} = \big(x * x'^{-1}, y.y'^{-1}\big) \in E' \times F'$

Cela montre que $E' \times F'$ est un sous-groupe de $E \times F$.

Allez à : Exercice 33

Correction exercice 34.

Rappel :

L'ensemble des applications de $\mathbb{C}$ dans $\mathbb{C}$, munis de la loi de composition des applications n'est pas un groupe, pour que cela soit un groupe il faut que ces applications admettent un symétrique, c'est-à-dire une bijection réciproque. C'est pour cela que l'on va montrer que les ensembles suivants sont des sous-groupes de l'ensemble des bijections de $\mathbb{C}$ dans $\mathbb{C}$, noté $\mathcal{S}(\mathbb{C})$.

1. On appelle f_t l'application définie pour tout $z \in \mathbb{C}$ par $f_t(z) = z + t$.
   $f_0(z) = z + 0 = z \Rightarrow f_0 = id$, id est l'élément neutre de $(\mathcal{S}(\mathbb{C}),\circ)$, il appartient à E_1.
   Pour tout $t, t' \in \mathbb{Z}$, $f_t \circ f_{t'}(z) = f_t\big(f_{t'}(z)\big) = f_t(z + t') = z + t + t'$, $t + t' \in \mathbb{Z}$ donc $f_t \circ f_{t'} \in E_1$.
   Pour tout $t \in \mathbb{Z}$, $f_t \circ f_{-t}(z) = f_t\big(f_{-t}(z)\big) = f_t(z - t) = z - t + t = z$, donc f_{-t} est le symétrique de f_t et $f_{-t} \in E_1$ car $-t \in \mathbb{Z}$.
   $(E_1,\circ)$ est un sous-groupe de $(\mathcal{S}(\mathbb{C}),\circ)$.
2. Même démonstration.
3. On pose f_θ l'application définie pour tout $z \in \mathbb{C}$ par $f_\theta(z) = e^{i\theta}z$
   $f_0(z) = e^0 z = z \Rightarrow f_0 = id$, id est l'élément neutre de $(\mathcal{S}(\mathbb{C}),\circ)$, il appartient à E_3.
   Pour tout $\theta, \theta' \in \mathbb{R}$, $f_\theta \circ f_{\theta'}(z) = f_\theta\big(f_{\theta'}(z)\big) = f_\theta\big(e^{i\theta'}z\big) = e^{i\theta}e^{i\theta'}z = e^{i\theta+i\theta'}z = e^{i(\theta+\theta')}z$
   $\theta + \theta' \in \mathbb{R}$ donc $f_\theta \circ f_{\theta'} \in E_3$.
   Pour tout $\theta \in \mathbb{R}$, $f_\theta \circ f_{-\theta}(z) = f_\theta\big(f_{-\theta}(z)\big) = f_\theta\big(e^{-i\theta}z\big) = e^{i\theta}e^{-i\theta}z = e^{i\theta-i\theta}z = e^0 z = z$
   Donc $(f_\theta)^{-1} = f_{-\theta} \in E_3$ car $-\theta \in \mathbb{R}$.
   $(E_3,\circ)$ est un sous-groupe de $(\mathcal{S}(\mathbb{C}),\circ)$.
4. On pose $f_{s,t}$ l'application définie pour tout $z \in \mathbb{C}$ par $f_{s,t}(z) = sz + t$
   $f_{1,0}(z) = z \Rightarrow f_{1,0} = id$, id est l'élément neutre de $(\mathcal{S}(\mathbb{C}),\circ)$, il appartient à E_4.
   Pour tout $(s,t),(s',t') \in \mathbb{C}^* \times \mathbb{C}$,
   $$f_{s,t} \circ f_{s',t'}(z) = f_{s,t}\left(f_{s',t'}(z)\right) = f_{s,t}(s'z + t') = s(s'z + t') + t = ss'z + st' + t$$
   $(ss', st' + t) \in \mathbb{C}^* \times \mathbb{C}$ donc $f_{s,t} \circ f_{s',t'} \in E_4$.
   Pour tout $(s,t) \in \mathbb{C}^* \times \mathbb{C}$,
   $$f_{s,t} \circ f_{\frac{1}{s},-\frac{t}{s}}(z) = f_{s,t}\left(f_{\frac{1}{s},-\frac{t}{s}}(z)\right) = f_{s,t}\left(\frac{1}{s}z - \frac{t}{s}\right) = s\left(\frac{1}{s}z - \frac{t}{s}\right) + t = z$$
   $\left(\frac{1}{s}, -\frac{t}{s}\right) \in \mathbb{C}^* \times \mathbb{C}$, donc $\left(f_{s,t}\right)^{-1} = f_{\frac{1}{s},-\frac{t}{s}} \in E_4$
   $(E_4,\circ)$ est un sous-groupe de $(\mathcal{S}(\mathbb{C}),\circ)$.

Allez à : Exercice 34

Correction exercice 35.

1. $G \cap \mathbb{R}^{+*}$ est un ensemble minoré par 0 donc il admet une borne inférieure $b \geq 0$.
2. Supposons que $b \notin G$, il existe $g \in G \cap \mathbb{R}^{+*}$ tel que $b < g < 2b$ et il existe $g' \in G$ tel que $b < g' < g$.
   On pose $h = g - g'$, $h > 0$ car $g > g'$ et $h \in G$ car g et g' sont dans G qui est un groupe additif.
   De plus
   $$\begin{cases} b < g < 2b \\ b < g' < g \end{cases} \Rightarrow \begin{cases} b < g < 2b \\ -g < -g' < -b \end{cases} \Rightarrow b - g < g - g' < 2b - b = b \Rightarrow h < b$$
   On a construit un élément de $G \cap \mathbb{R}^{+*}$ qui est inférieur à b, il y a une contradiction puisque $b = \inf(G \cap \mathbb{R}^{+*})$, par conséquent $b \in G$.
3. Il est évident que $b\mathbb{Z} \subset G$. Montrons l'inclusion dans l'autre sens.
   Soit $g \in G$, on pose $m = E\left(\frac{g}{b}\right) \in \mathbb{Z}$ où $E\left(\frac{g}{b}\right)$ est la partie entière de $\frac{g}{b}$. Par définition de la partie entière, puisque $b > 0$:
   $$\frac{g}{b} \leq m < \frac{g}{b} + 1 \Leftrightarrow g \leq mb < g + b \Leftrightarrow 0 \leq mb - g < b$$

Si $0 < mb - g$, comme $b \in G$, $mh \in G$ et $g \in G$, G étant un groupe $mb - g \in G$, comme $mb - g < b$, il y a une contradiction puisque $b = \inf(G \cap \mathbb{R}^{+*})$ donc $mb - g = 0 \Leftrightarrow g = mb \in b\mathbb{Z}$.
Cela montre l'inclusion dans l'autre sens. Finalement $G = b\mathbb{Z}$.

4. Il existe un élément g de $G \cap \mathbb{R}^{+*}$ tel que $0 < g < y - x$. On pose $n = E\left(\frac{x}{g}\right) \in \mathbb{Z}$. On a alors, puisque $g > 0$,
$$n \leq \frac{x}{g} < n + 1 \Leftrightarrow ng \leq x < ng + g \Leftrightarrow x - g < ng \leq x$$
$$\begin{cases} 0 < g < y - x \\ x - g < ng \leq x \end{cases} \Rightarrow x < x - g \leq ng + g < y - x + x = y \Rightarrow x < (n+1)g < y$$
On pose $h = (n+1)g$, $n + 1 \in \mathbb{Z}$ donc $h \in G$ avec $h \in]x, y[$.
5. On pose $G = \{m + n\sqrt{2}\,, (n, m) \in \mathbb{Z}^2\}$
$0 = 0 + 0 \times \sqrt{2} \in G$,
Soient $m + n\sqrt{2} \in G$ et $m' + n'\sqrt{2} \in G$, $m + n\sqrt{2} - \left(m' + n'\sqrt{2}\right) = (m - m') + (n - n')\sqrt{2} \in G$ car $m - m' \in \mathbb{Z}$ et $n - n' \in \mathbb{Z}$.
Cela montre que $(G, +)$ est un sous-groupe de $(\mathbb{R}, +)$.
D'après 2. $\inf(G) \in G$ donc il existe $m_0, n_0 \in \mathbb{Z}$ tel que $m_0 + n_0\sqrt{2} = \inf(G)$, supposons que $m_0 + n_0\sqrt{2} \neq 0$ alors $G = \left(m_0 + n_0\sqrt{2}\right)\mathbb{Z}$, autrement dit pour tout élément $m + n\sqrt{2} \in G$ il existe $p \in \mathbb{Z}$ tel que :
$$m + n\sqrt{2} = \left(m_0 + n_0\sqrt{2}\right)p = m_0 p + n_0 p\sqrt{2}$$
Donc
$$m - m_0 p = (n_0 p - n)\sqrt{2}$$
Si $n_0 p - n \neq 0$ alors $\sqrt{2} = \frac{m - m_0 p}{n_0 p - n} \in \mathbb{Q}$ ce qui est faux, donc $n_0 p - n = 0$ et par conséquent
$$m - m_0 p = 0$$
On a montré que pour tout $m, n \in \mathbb{Z}$ il existe $p \in \mathbb{Z}$ tel que :
$$\begin{cases} n = pn_0 \\ m = pm_0 \end{cases} \Rightarrow m_0 n = m n_0$$
Si $n_0 \neq 0$, pour tout $m \in \mathbb{Z}$ et pour tout $n \in \mathbb{Z}^*$, $\frac{m}{n} = \frac{m_0}{n_0}$ ce qui veut dire que le quotient de deux entiers est constant, ce qui est faux.
Si $n_0 = 0$, pour tout $n \in \mathbb{Z}$, $n = 0$ ce qui est faux.
L'hypothèse $m_0 + n_0\sqrt{2} \neq 0$ est fausse par conséquent $m_0 + n_0\sqrt{2} = 0$ et G est dense dans $\mathbb{R}$ d'après 4.

Allez à : Exercice 35

Correction exercice 36.

1. $0 = 0 + i.0 \in \mathbb{K}$ car $0 \in \mathbb{Q}$ et $0 \in \mathbb{Q}$.
Soient $z_1 = r_1 + is_1 \in \mathbb{K}$ et $z_2 = r_2 + is_2 \in \mathbb{K}$, $z_1 = r_1 + is_1 - (r_2 + is_2) = r_1 - r_2 + i(s_1 - s_2) \in \mathbb{K}$ car $r_1 - r_2 \in \mathbb{Q}$ et $s_1 - s_2 \in \mathbb{Q}$.
L'addition étant commutative dans $\mathbb{C}$, $(\mathbb{K}, +)$ est un sous-groupe commutatif de $(\mathbb{C}, +)$.
2. $1 = 1 + i.0 \in \mathbb{K}$ car $1 \in \mathbb{Q}$ et $0 \in \mathbb{Q}$.
Soient $z_1 = r_1 + is_1 \in \mathbb{K}$ et $z_2 = r_2 + is_2 \in \mathbb{K}$,
$$z_1 z_2^{-1} = \frac{r_1 + is_1}{r_2 + is_2} = \frac{(r_1 + is_1)(r_2 - is_2)}{r_2^2 + s_2^2} = \frac{r_1 r_2 + s_1 s_2 + i(r_2 s_1 - r_1 s_2)}{r_2^2 + s_2^2} = \frac{r_1 r_2 + s_1 s_2}{r_2^2 + s_2^2} + i\frac{r_2 s_1 - r_1 s_2}{r_2^2 + s_2^2}$$
$z_1 z_2^{-1} \in \mathbb{K}$ car $\frac{r_1 r_2 + s_1 s_2}{r_2^2 + s_2^2} \in \mathbb{Q}$ et $\frac{r_2 s_1 - r_1 s_2}{r_2^2 + s_2^2} \in \mathbb{Q}$
La multiplication étant commutative dans $\mathbb{C}$, $(\mathbb{K}^*, .)$ est un sous-groupe commutatif de $(\mathbb{C}^*, .)$.
3. Il ne reste plus qu'à rappeler que la multiplication est distributive par rapport à l'addition dans $\mathbb{C}$ pour conclure que $(\mathbb{K}, +, .)$ est un corps commutatif, car la multiplication est commutative.

Allez à : Exercice 36

Correction exercice 37.

1. $0 = 0 + 0 \times \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$,
   Soient $m + n\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ et $m' + n'\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$,
   $$m + n\sqrt{2} - (m' + n'\sqrt{2}) = (m - m') + (n - n')\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$
   car $m - m' \in \mathbb{Z}$ et $n - n' \in \mathbb{Z}$.
   Cela montre que $(\mathbb{Z}[\sqrt{2}], +)$ est un sous-groupe de $(\mathbb{R}, +)$.
   Soient $m + n\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ et $m' + n'\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$,
   $$(m + n\sqrt{2})(m' + n'\sqrt{2}) = mm' + 2nn' + (mn' + m'n)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$
   La multiplication est une loi interne sur $\mathbb{Z}[\sqrt{2}]$.
   $1 = 1 + 0 \times \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$,
   $(\mathbb{Z}[\sqrt{2}], +, \times)$ est un sous-anneau de $(\mathbb{R}, +, \times)$.

Remarque :

Les propriétés de distributivité et l'associativité de la multiplication sont évidentes dans $\mathbb{R}$.

2. Pour tout $a + b\sqrt{2}$ il existe un unique $a - b\sqrt{2}$ tel que $\phi(a - b\sqrt{2}) = a + b\sqrt{2}$, ϕ est une bijection de $\mathbb{Z}[\sqrt{2}]$ sur $\mathbb{Z}[\sqrt{2}]$.
   Soient $m + n\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ et $m' + n'\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$,
   $$\phi(m + n\sqrt{2} + m' + n'\sqrt{2}) = \phi\left((m + m') + (n + n')\sqrt{2}\right) = (m + m') - (n + n')\sqrt{2}$$
   $$= m - n\sqrt{2} + m' - n'\sqrt{2} = \phi(m + n\sqrt{2}) + \phi(m' + n'\sqrt{2})$$
   ϕ est un morphisme pour la loi $+$.
   $$\phi\left((m + n\sqrt{2})(m' + n'\sqrt{2})\right) = \phi(mm' + 2nn' + (mn' + m'n)\sqrt{2})$$
   $$= mm' + 2nn' - (mn' + m'n)\sqrt{2}$$
   Et d'autre part
   $$\phi(m + n\sqrt{2})\phi(m' + n'\sqrt{2}) = (m - n\sqrt{2})(m' - n'\sqrt{2}) = mm' + 2nn' - (mn' + m'n)\sqrt{2}$$
   On a bien $\phi\left((m + n\sqrt{2})(m' + n'\sqrt{2})\right) = \phi(m + n\sqrt{2})\phi(m' + n'\sqrt{2})$
   ϕ est un morphisme pour la loi $\times$.

3. Pour tout $x \in \mathbb{Z}[\sqrt{2}]$, on pose $N(x) = x\phi(x)$. Montrer que N est une application de $\mathbb{Z}[\sqrt{2}]$ dans $\mathbb{Z}$, qui est un morphisme pour la multiplication.
   Pour tout $x = m + n\sqrt{2}$
   $$N(m + n\sqrt{2}) = (m + n\sqrt{2})(m - n\sqrt{2}) = m^2 - 2n^2 \in \mathbb{Z}$$
   Soient $m + n\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ et $m' + n'\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$,
   $$N\left((m + n\sqrt{2})(m' + n'\sqrt{2})\right) = N(mm' + 2nn' + (mn' + m'n)\sqrt{2})$$
   $$= (mm' + 2nn' + (mn' + m'n)\sqrt{2})(mm' + 2nn' - (mn' + m'n)\sqrt{2})$$
   $$= (mm' + 2nn')^2 - 2(mn' + m'n)^2$$
   $$= mm'^2 + 4mm'nn' + 4n^2n'^2 - 2(m^2n'^2 + 2mn'm'n + m'^2n^2)$$
   $$= mm'^2 + 4n^2n'^2 - 2m^2n'^2 - 2m'^2n^2$$
   $$N(m + n\sqrt{2})N(m' + n'\sqrt{2}) = (m^2 - 2n^2)(m'^2 - 2n'^2) = m^2m'^2 - 2m^2n'^2 - 2n^2m'^2 + 4n^2n'^2$$
   On a bien
   $$N\left((m + n\sqrt{2})(m' + n'\sqrt{2})\right) = N(m + n\sqrt{2})N(m' + n'\sqrt{2})$$
   N est un morphisme d'anneau pour la loi $\times$.

4. Soit $x = m + n\sqrt{2}$ un élément inversible de $\mathbb{Z}[\sqrt{2}]$, $\frac{1}{x} \in \mathbb{Z}[\sqrt{2}]$
   $$N(x)N\left(\frac{1}{x}\right) = N\left(x \times \frac{1}{x}\right) = N(1) = 1$$
   Comme pour tout $y \in \mathbb{Z}[\sqrt{2}]$, $N(y) \in \mathbb{Z}$,

$$N(x)N\left(\frac{1}{x}\right)=1 \Leftrightarrow \begin{cases} N(x)=N\left(\frac{1}{x}\right)=1 \\ N(x)=N\left(\frac{1}{x}\right)=-1 \end{cases}$$

Cela montre que si x est inversible alors $N(x)=\pm 1$.
Réciproque : si $N(x)=\pm 1$.

$$\frac{1}{x}=\frac{1}{m+n\sqrt{2}}=\frac{m-n\sqrt{2}}{(m+n\sqrt{2})(m-n\sqrt{2})}=\frac{m-n\sqrt{2}}{m^2-2n^2}=\frac{m-n\sqrt{2}}{N(x)}=\pm(m-n\sqrt{2})\in\mathbb{Z}[\sqrt{2}\,]$$

Cela montre que x est inversible dans $\mathbb{Z}[\sqrt{2}\,]$.

5. $3+2\sqrt{2}$ et $-3+2\sqrt{2}$
   $N(3+2\sqrt{2})=3^2-2\times 2^2=1$ donc $3+2\sqrt{2}$ est inversible.
   $N(-3+2\sqrt{2})=(-3)^2-2\times 2^2=1$ donc $-3+2\sqrt{2}$ est inversible.

Allez à : Exercice 37

Correction exercice 38.

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 $\frac{3\pi}{2}$ (ou $-\frac{\pi}{2}$).
   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).

Allez à : Exercice 38

2. Pour montrer que G est un groupe, il suffit de vérifier que c'est un sous-groupe de l'ensemble $S(\mathbb{C})$ 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 G est un sous-groupe de $S(\mathbb{C})$. Dans cette table, nous omettons les signes $\circ$ par souci de clarté.

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

Allez à : Exercice 38

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

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

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. Dans la suite on se contentera de constater que les tables correspondent.

Allez à : Exercice 38

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 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)

Allez à : Exercice 38

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

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Allez à : Exercice 38

6. Vérifions-le pour r et pour s.

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

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.

Allez à : Exercice 38

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

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

Autrement dit

$$\sigma = (2,3,4,1) \quad \text{et} \quad \tau = (4,3,2,1)$$

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

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

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.

Allez à : Exercice 38

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 la notation

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

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

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

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

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

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

Allez à : Exercice 38

9. Puisque φ est un morphisme, H est un sous-groupe de G. Le tableau de la question précédente liste tous les éléments de H, qui sont tous distincts. Donc la restriction de φ à H à l'arrivée est une bijection : φ est donc un isomorphisme de G sur H.

Allez à : Exercice 38

Correction exercice 39.

1. L'ensemble A est non vide. Il suffit de vérifier que A est un sous-groupe pour l'addition, et que la multiplication est stable. Soient m, n, m', n' quatre éléments de $\mathbb{Z}$.

$$\left(m + n\sqrt{6}\right) - \left(m' + n'\sqrt{6}\right) = (m - m') + (n - n')\sqrt{6}$$

Donc

$$\left(m + n\sqrt{6}\right) - \left(m' + n'\sqrt{6}\right) \in A$$

$$\left(m + n\sqrt{6}\right) \times \left(m' + n'\sqrt{6}\right) = (mm' + 6nn') + (mn' + m'n)\sqrt{6}$$

Donc

$$\left(m + n\sqrt{6}\right) \times \left(m' + n'\sqrt{6}\right) \in A$$

2. Observons d'abord que pour tout élément a de A, $\varphi\big(\varphi(a)\big) = a$. Donc φ est une bijection, puisque tout élément de A a pour antécédent $\varphi(a)$.
Montrons maintenant que φ est un morphisme pour l'addition.

$$\varphi\left(\left(m + n\sqrt{6}\right) + \left(m' + n'\sqrt{6}\right)\right) = \varphi\left((m + m') + (n + n')\sqrt{6}\right) = (m + m') - (n + n')\sqrt{6}$$
$$= \left(m - n\sqrt{6}\right) + \left(m' - n'\sqrt{6}\right) = \varphi\left(m + n\sqrt{6}\right) + \varphi\left(m' + n'\sqrt{6}\right)$$

Montrons enfin que φ est un morphisme pour la multiplication.

$$\varphi\left(\left(m+n\sqrt{6}\right)\times\left(m'+n'\sqrt{6}\right)\right)=\varphi\left((mm'+6nn')+(mn'+m'n)\sqrt{6}\right)$$
$$=(mm'+6nn')-(mn'+m'n)\sqrt{6}=\left(m-n\sqrt{6}\right)\times\left(m'-n'\sqrt{6}\right)$$
$$=\varphi\left(m+n\sqrt{6}\right)\times\varphi\left(m'+n'\sqrt{6}\right)$$

3. Soit $a=m+n\sqrt{6}$ un élément quelconque de A.
$$N(a)=a\varphi(a)=\left(m+n\sqrt{6}\right)\times\left(m-n\sqrt{6}\right)=m^2-6n^2$$
Donc N est bien une application de A dans $\mathbb{Z}$. Montrons que c'est un morphisme pour la multiplication. Soient a et a' deux éléments de A.
$$N(aa')=aa'\varphi(aa')=aa'\varphi(a)\varphi(a')=\left(a\varphi(a)\right)\left(a'\varphi(a')\right)=N(a)N(a')$$
En utilisant le fait que φ est un morphisme pour la multiplication.
4. Si $N(x)=x\varphi(x)=1$, alors $\varphi(x)$ est inverse de x, et si $N(x)=x\varphi(x)=-1$, alors $-\varphi(x)$ est inverse de x : la condition est suffisante. Montrons qu'elle est nécessaire. Soit x un élément inversible de A : il existe y tel que $xy=1$. Mais comme N est un morphisme pour la multiplication, $N(x)N(y)=1$. Or $N(x)$ et $N(y)$ sont des entiers. Les seuls éléments de $\mathbb{Z}$ inversibles pour la multiplication sont 1 et -1. D'où le résultat.
5. Il suffit de calculer l'image par N, et d'appliquer le résultat de la question précédente.
$$N\left(5+2\sqrt{6}\right)=25-24=1$$
L'inverse de $5+2\sqrt{6}$ est $5-2\sqrt{6}$.

Allez à : Exercice 39