

# Groupes

## Morphismes de groupes

### Exercice 1 [02218] [Correction]

Soient  $n \in \mathbb{N}^*$  et  $f: \mathbb{R}^* \rightarrow \mathbb{R}$  définie par  $f(x) = x^n$ .

Montrer que  $f$  est un morphisme du groupe  $(\mathbb{R}^*, \times)$  dans lui-même.

En déterminer image et noyau.

### Exercice 2 [02219] [Correction]

Justifier que  $\exp: \mathbb{C} \rightarrow \mathbb{C}^*$  est un morphisme du groupe  $(\mathbb{C}, +)$  vers  $(\mathbb{C}^*, \times)$ .

En déterminer image et noyau.

### Exercice 3 [02221] [Correction]

Soit  $(G, *)$ ,  $(G', \top)$  deux groupes et  $f: G \rightarrow G'$  un morphisme de groupes.

- Montrer que pour tout sous-groupe  $H$  de  $G$ ,  $f(H)$  est un sous-groupe de  $(G', \top)$ .
- Montrer que pour tout sous-groupe  $H'$  de  $G'$ ,  $f^{-1}(H')$  est un sous-groupe de  $(G, *)$ .

### Exercice 4 [02220] [Correction]

Soit  $G$  un groupe noté multiplicativement. Pour  $a \in G$ , on note  $\tau_a$  l'application de  $G$  vers  $G$  définie par  $\tau_a(x) = axa^{-1}$ .

- Montrer que  $\tau_a$  est un morphisme du groupe  $(G, \times)$  dans lui-même.
- Vérifier que
 
$$\forall a, b \in G, \tau_a \circ \tau_b = \tau_{ab}$$
- Montrer que  $\tau_a$  est bijective et déterminer son application réciproque.
- En déduire que  $\mathcal{T} = \{\tau_a \mid a \in G\}$  muni du produit de composition est un groupe.

### Exercice 5 [02222] [Correction]

On note  $\text{Aut}(G)$  l'ensemble des isomorphismes d'un groupe  $(G, *)$  dans lui-même.

Montrer que  $\text{Aut}(G)$  est un sous-groupe du groupe des permutations  $(\mathcal{S}_G, \circ)$ .

### Exercice 6 [02223] [Correction]

Soit  $(G, *)$  un groupe et  $a \in G$ .

On définit une loi de composition interne  $\top$  sur  $G$  par  $x \top y = x * a * y$ .

- Montrer que  $(G, \top)$  est un groupe.
- Soit  $H$  un sous groupe de  $(G, *)$  et  $K = \text{sym}(a) * H = \{\text{sym}(a) * x \mid x \in H\}$ .  
Montrer que  $K$  est un sous groupe de  $(G, \top)$ .
- Montrer que  $f: x \mapsto x * \text{sym}(a)$  est un isomorphisme de  $(G, *)$  vers  $(G, \top)$ .

### Exercice 7 [00119] [Correction]

Soit  $n \in \mathbb{N}$  tel que  $n \geq 2$ . Déterminer les morphismes du groupe  $(\mathcal{S}_n, \circ)$  vers  $(\mathbb{C}^*, \times)$ .

### Exercice 8 [03368] [Correction]

Soit  $\varphi$  un morphisme d'un groupe fini  $(G, *)$  vers  $(\mathbb{C}^*, \times)$ .

On suppose que  $\varphi$  n'est pas une application constante. Calculer

$$\sum_{x \in G} \varphi(x)$$

## Sous-groupes

### Exercice 9 [00113] [Correction]

Un sous-groupe d'un groupe produit est-il nécessairement produit de deux sous-groupes ?

### Exercice 10 [00114] [Correction]

Soient  $H$  et  $K$  deux sous-groupes d'un groupe  $(G, *)$ .

À quelle condition l'ensemble  $H \cup K$  est-il un sous-groupe de  $(G, *)$  ?

### Exercice 11 [03432] [Correction]

Un sous-groupe  $H$  de  $(G, \cdot)$  est dit distingué si

$$\forall x \in H, \forall a \in G, axa^{-1} \in H$$

- Montrer que le noyau d'un morphisme de groupes au départ de  $(G, \cdot)$  est distingué.

- b) Soient  $H, K$  deux sous-groupes de  $(G, \cdot)$ .  
On suppose le sous-groupe  $H$  distingué, montrer que l'ensemble

$$HK = \{xy \mid x \in H, y \in K\}$$

est un sous-groupe de  $(G, \cdot)$ .

**Exercice 12** [00115] [Correction]

Montrer que le sous-ensemble formé des éléments d'ordre fini d'un groupe abélien en est un sous-groupe.

**Exercice 13** [00117] [Correction]

[Théorème de Lagrange] Soit  $H$  un sous-groupe d'un groupe  $(G, \cdot)$  fini.

- Montrer que les ensembles  $aH = \{ax \mid x \in H\}$  avec  $a \in G$  ont tous le cardinal de  $H$ .
- Montrer que les ensembles  $aH$  avec  $a \in G$  sont deux à deux confondus ou disjoints.
- En déduire que le cardinal de  $H$  divise celui de  $G$ .
- Application : Montrer que tout élément de  $G$  est d'ordre fini et que cet ordre divise le cardinal de  $G$ .

**Exercice 14** [02366] [Correction]

Montrer que

$$\left\{ x + y\sqrt{3} \mid x \in \mathbb{N}, y \in \mathbb{Z}, x^2 - 3y^2 = 1 \right\}$$

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

**Exercice 15** [02648] [Correction]

Soit  $G$  un groupe,  $H$  un sous-groupe de  $G$ ,  $A$  une partie non vide de  $G$ . On pose  $AH = \{ah \mid a \in A, h \in H\}$ . Montrer que  $AH = H$  si, et seulement si,  $A \subset H$ .

**Exercice 16** [02948] [Correction]

- Montrer que tout sous-groupe additif de  $\mathbb{R}$  qui n'est pas monogène est dense dans  $\mathbb{R}$ .

- Soit  $x \in \mathbb{R} \setminus \mathbb{Q}$ . Montrer qu'il existe une infinité de  $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$  tels que

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^2}$$

- Montrer la divergence de la suite de terme général

$$u_n = \frac{1}{n \sin n}$$

## Eléments d'ordre fini

**Exercice 17** [03453] [Correction]

Soit  $(G, \cdot)$  un groupe de cardinal  $2n$ .

- Justifier que l'on définit une relation d'équivalence  $\mathcal{R}$  sur  $G$  en posant

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

- En déduire l'existence dans  $G$  d'un élément d'ordre 2.

**Exercice 18** [00116] [Correction]

Soient  $(G, *)$  un groupe fini commutatif d'ordre  $n$  et  $a \in G$ .

- Justifier que l'application  $x \mapsto a * x$  est une permutation de  $G$ .
- En considérant le produit des éléments de  $G$ , établir que  $a^n = e$ .

**Exercice 19** [02363] [Correction]

Quel est le plus petit entier  $n$  tel qu'il existe un groupe non commutatif de cardinal  $n$  ?

**Exercice 20** [03292] [Correction]

Soient  $a$  et  $b$  deux éléments d'ordre respectifs  $p$  et  $q$  d'un groupe abélien  $(G, *)$ .

- On suppose que  $p$  et  $q$  sont premiers entre eux.  
Montrer que l'élément  $ab$  est d'ordre  $pq$ .
- On ne suppose plus  $p$  et  $q$  premiers entre eux.  
L'élément  $ab$  est-il nécessairement d'ordre  $\text{ppcm}(p, q)$  ?

**Exercice 21** [ 03332 ] [Correction]

Soient  $a$  et  $b$  deux éléments d'ordre respectifs  $p$  et  $q$  d'un groupe abélien  $(G, *)$ .

- a) On suppose dans cette question seulement que  $p$  et  $q$  sont premiers entre eux. Montrer que l'élément  $ab$  est d'ordre  $pq$ .
- b) Soit  $d$  un diviseur de  $p$ . Montrer qu'il existe un élément d'ordre  $d$  dans  $(G, *)$ .
- c) Existe-t-il dans  $G$  un élément d'ordre  $m = \text{ppcm}(p, q)$  ?

**Exercice 22** [ 04053 ] [Correction]

Soit  $(G, .)$  un groupe abélien fini de neutre  $e$ .

- a) Soient  $x$  et  $y$  deux éléments de  $G$  d'ordres finis  $p$  et  $q$  premiers entre eux. Montrer que l'élément  $z = xy$  est d'ordre  $pq$ .
- b) On note  $m$  le ppcm des ordres des éléments de  $(G, .)$  et l'on introduit sa décomposition en facteurs premiers

$$m = p_1^{\alpha_1} \dots p_N^{\alpha_N}$$

Montrer que pour chaque  $i \in \llbracket 1; N \rrbracket$ , il existe un élément  $x_i$  dans  $G$  d'ordre  $p_i^{\alpha_i}$ .

- c) Établir l'existence dans  $G$  d'un élément d'ordre  $m$  exactement.

**Exercice 23** [ 04151 ] [Correction]

Dans tout ce sujet  $n$  désigne un naturel non nul.

On note  $\varphi(n)$  l'indicatrice d'Euler de  $n$ ,  $U_n$  l'ensemble des racines  $n$ -ième de l'unité et  $U_n^*$  l'ensemble des racines de l'unité d'ordre exactement  $n$ . Enin, pour  $d \in \mathbb{N}^*$ , on pose

$$\Phi_d = \prod_{z \in U_d^*} (X - z)$$

- a) Écrire en Python la fonction `liste(n)` qui renvoie

$$\{k \in \llbracket 1; n \rrbracket \mid k \wedge n = 1\}$$

Écrire la fonction `phi(n)` qui renvoie  $\varphi(n)$  puis `sumphi(n)` qui renvoie

$$\sum_{d|n} \varphi(d)$$

- b) Montrer

$$X^n - 1 = \prod_{d|n} \Phi_d$$

- c) Justifier

$$\sum_{d|n} \varphi(d) = n$$

- d) Montrer que  $\Phi_n$  est un polynôme à coefficients entiers.

On pose  $Q_n = X^n - 1$  et on choisit  $p, q, r$  des nombres premiers vérifiant

$$p < q < r < p + q$$

On pose

$$n = pqr \text{ et } R = \frac{Q_p Q_q Q_r}{X - 1}$$

- e) Montrer

$$\Phi_n = \frac{Q_n R}{Q_{pq} Q_{qr} Q_{rp}}$$

- f) Montrer qu'il existe un polynôme  $S$  tel que

$$\Phi_n - R = X^{pq} S$$

- g) En déduire que le coefficient de  $X^r$  dans  $\Phi_n$  est égal à  $-2$ .

## Parties génératrices

**Exercice 24** [ 02229 ] [Correction]

Dans  $(\mathcal{S}_n, \circ)$  on considère les permutations

$$\tau = (1 \ 2) \text{ et } \sigma = (1 \ 2 \ \dots \ n)$$

- a) Calculer  $\sigma^k \circ \tau \circ \sigma^{-k}$  pour  $0 \leq k \leq n - 2$ .
- b) En déduire que tout élément de  $\mathcal{S}_n$  peut s'écrire comme un produit de  $\sigma$  et de  $\tau$ .

**Exercice 25** [ 00120 ] [Correction]

Soit  $n \in \mathbb{N}$  tel que  $n \geq 3$ . On considère la transposition  $\tau = (1 \ 2)$  et le  $n$ -cycle  $\chi = (1 \ 2 \ \dots \ n)$ .

- a) Justifier que l'ensemble  $\{\tau, \chi\}$  forme une partie génératrice de  $(\mathcal{S}_n, \circ)$ .
- b) Existe-t-il une partie génératrice de  $(\mathcal{S}_n, \circ)$  formée d'un seul élément ?

**Exercice 26** [ 02368 ] [Correction]

Soit  $n$  un entier naturel non nul,  $(e_1, \dots, e_n)$  la base canonique de  $E = \mathbb{R}^n$ .

Soit  $\mathcal{S}_n$  l'ensemble des permutations de  $\{1, 2, \dots, n\}$ . Soit  $t_i = (1, i)$ .

Pour  $s \in \mathcal{S}_n$ , on définit  $u_s(e_i) = e_{s(i)}$ .

- Montrer que  $(t_2, t_3, \dots, t_n)$  engendre  $\mathcal{S}_n$ .
- Interpréter géométriquement  $u_s$  lorsque  $s$  est une transposition.
- Soit  $s = (1\ 2 \dots n-1\ n)$ . On suppose que  $s$  est la composée de  $p$  transpositions. Montrer que  $p \geq n-1$ .
- Quel est le cardinal minimal d'une famille de transpositions génératrice de  $\mathcal{S}_n$  ?

**Exercice 27** [ 03256 ] [Correction]

Soit  $H$  un sous-groupe strict d'un groupe  $(G, *)$ . Déterminer le groupe engendré par le complémentaire de  $H$  dans  $G$ .

## Groupes cycliques

**Exercice 28** [ 03364 ] [Correction]

Soit  $x$  est un élément d'un groupe cyclique de cardinal  $n$ . Calculer  $x^n$ .

**Exercice 29** [ 00123 ] [Correction]

On désire établir que tout sous-groupe d'un groupe cyclique est lui-même cyclique : on introduit  $(G, *)$  un groupe cyclique de générateur  $a$  et  $H$  un sous-groupe de  $(G, *)$ .

- Justifier l'existence d'un plus petit entier naturel non nul tel que  $a^n \in H$ .
- Établir qu'alors  $H$  est le groupe engendré par  $a^n$ .

**Exercice 30** [ 00124 ] [Correction]

Soit  $G$  un groupe cyclique de cardinal  $n$ .

Montrer, que pour tout diviseur  $d \in \mathbb{N}^*$  de  $n$ ,  $G$  possède un et un seul sous-groupe de cardinal  $d$ .

**Exercice 31** [ 00125 ] [Correction]

Soient  $H$  et  $K$  deux groupes notés multiplicativement.

a) Montrer que si  $h$  est un élément d'ordre  $p$  de  $H$  et  $k$  un élément d'ordre  $q$  de  $K$  alors  $(h, k)$  est un élément d'ordre  $\text{ppcm}(p, q)$  de  $H \times K$ .

b) On suppose  $H$  et  $K$  cycliques. Montrer que le groupe produit  $H \times K$  est cyclique si, et seulement si, les ordres de  $H$  et  $K$  sont premiers entre eux.

**Exercice 32** [ 02365 ] [Correction]

[Groupe quasi-cyclique de Prüfer] Soit  $p$  un nombre premier. On pose

$$G_p = \left\{ z \in \mathbb{C} \mid \exists k \in \mathbb{N}, z^{p^k} = 1 \right\}$$

- Montrer que  $G_p$  est un sous-groupe de  $(\mathbb{C}^*, \times)$ .
- Montrer que les sous-groupes propres de  $G_p$  sont cycliques et qu'aucun d'eux n'est maximal pour l'inclusion.
- Montrer que  $G_p$  n'est pas engendré par un système fini d'éléments.

**Exercice 33** [ 03444 ] [Correction]

Soit  $n$  un entier  $\geq 3$ .

- Montrer que pour tout entier impair  $a$ , on a

$$a^{2^{n-2}} \equiv 1 \pmod{2^n}$$

- Le groupe  $((\mathbb{Z}/2^n\mathbb{Z})^*, \times)$  est-il cyclique ?

**Exercice 34** [ 02505 ] [Correction]

Soit

$$M = \begin{pmatrix} 0 & 1 & & (0) \\ & \ddots & \ddots & \\ (0) & & \ddots & 1 \\ 1 & (0) & & 0 \end{pmatrix} \in \mathcal{M}_n(\mathbb{C})$$

- Calculer le polynôme caractéristique de  $M$ . La matrice  $M$  est-elle diagonalisable ? est-elle inversible ?
- Soit  $G = \{M^k \mid k \in \mathbb{Z}\}$ . Montrer que  $G$  est une groupe cyclique et préciser son cardinal.

**Exercice 35** [ 03715 ] [\[Correction\]](#)

Soit  $(G, *)$  un groupe cyclique à  $n$  élément engendré par  $a$ .

Pour  $r \in \mathbb{N}^*$ , on introduit l'application  $f: G \rightarrow G$  définie par

$$\forall x \in G, f(x) = x^r$$

- Vérifier que  $f$  est un endomorphisme de  $(G, *)$ .
- Déterminer le noyau  $f$ .
- Montrer que l'image de  $f$  est le sous-groupe engendré par  $a^d$  avec  $d = \text{pgcd}(n, r)$ .
- Pour  $y \in G$ , combien l'équation  $x^r = y$  possède-t-elle de solutions?

**Exercice 36** [ 03845 ] [\[Correction\]](#)

Montrer que les sous-groupes finis du groupe  $(\text{SO}(2), \times)$  des rotations du plan sont cycliques.

## Groupes isomorphes

**Exercice 37** [ 02650 ] [\[Correction\]](#)

On note  $V$  l'ensemble des matrices à coefficients entiers du type

$$\begin{pmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{pmatrix}$$

et  $G$  l'ensemble des  $M \in V$  inversibles dans  $\mathcal{M}_4(\mathbb{R})$  et dont l'inverse est dans  $V$ .

- Quelle est la structure de  $G$ ?
- Soit  $M \in V$ . Montrer que  $M \in G$  si, et seulement si,  $\det M = \pm 1$ .
- Donner un groupe standard isomorphe à  $G$  muni du produit.

**Exercice 38** [ 00122 ] [\[Correction\]](#)

Les groupes  $(\mathbb{Q}, +)$  et  $(\mathbb{Q}^*, \times)$  sont-ils isomorphes?

## Corrections

### Exercice 1 : [énoncé]

Pour  $x \in \mathbb{R}^*$ , on a bien  $f(x) \in \mathbb{R}^*$ . Pour  $x, y \in \mathbb{R}^*$

$$f(xy) = (xy)^n = x^n y^n = f(x)f(y)$$

donc  $f$  est un morphisme de  $(\mathbb{R}^*, \times)$  vers lui-même.

$\ker f = f^{-1}(\{1\})$  et  $\text{Im } f = \{x^n \mid x \in \mathbb{R}^*\}$ .

Si  $n$  est pair alors

$$\ker f = \{1, -1\} \text{ et } \text{Im } f = \mathbb{R}_+^*$$

Si  $n$  est impair alors

$$\ker f = \{1\} \text{ et } \text{Im } f = \mathbb{R}^*$$

### Exercice 2 : [énoncé]

On sait

$$\forall x, y \in \mathbb{C}, \exp(x + y) = \exp(x) \exp(y)$$

donc  $\exp: \mathbb{C} \rightarrow \mathbb{C}^*$  est un morphisme de groupes.

$$\exp(x) = 1 \iff \exists k \in \mathbb{Z}, x = 2ik\pi$$

donc

$$\ker \exp = \{2ik\pi \mid k \in \mathbb{Z}\}$$

La fonction exponentielle complexe prend toutes les valeurs de  $\mathbb{C}^*$  donc

$$\text{Im } \exp = \mathbb{C}^*$$

### Exercice 3 : [énoncé]

a)  $f(H) \subset G'$ ,  $e' = f(e) \in f(H)$  car  $e \in H$ .

Soit  $y, y' \in f(H)$ , on peut écrire  $y = f(x)$  et  $y' = f(x')$  avec  $x, x' \in H$ .

$$y \top y'^{-1} = f(x) \top f(x')^{-1} = f(x) \top f(x'^{-1}) = f(x * x'^{-1})$$

avec  $x * x'^{-1} \in H$  donc  $y \top y'^{-1} \in f(H)$ .

Ainsi  $f(H)$  est un sous-groupe de  $(G', \top)$ .

b)  $f^{-1}(H') \subset G$  et  $e \in f^{-1}(H')$  car  $f(e) = e' \in H'$ .

Soit  $x, x' \in f^{-1}(H')$ . On a  $f(x), f(x') \in H'$ .

$$f(x * x'^{-1}) = f(x) \top f(x'^{-1}) = f(x) \top f(x')^{-1} \in H'$$

donc  $x * x'^{-1} \in f^{-1}(H')$ .

Ainsi  $f^{-1}(H')$  est un sous-groupe de  $(G, *)$ .

### Exercice 4 : [énoncé]

a) Soient  $x, y \in G$ . On a

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

$\tau_a$  est donc un endomorphisme du groupe  $(G, \times)$ .

b) Pour tout  $x \in G$ ,

$$(\tau_a \circ \tau_b)(x) = \tau_a(bxb^{-1}) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = \tau_{ab}(x)$$

donc

$$\tau_a \circ \tau_b = \tau_{ab}$$

c)  $(\tau_a \circ \tau_{a^{-1}}) = \tau_1 = \text{Id}_G$  et  $(\tau_{a^{-1}} \circ \tau_a) = \tau_1 = \text{Id}_G$  donc  $\tau_a$  est bijective et  $(\tau_a)^{-1} = \tau_{a^{-1}}$ .

d) Montrons que  $\mathcal{T}$  est un sous-groupe du groupe des permutations  $(\mathcal{S}_G, \circ)$ .  
 $\mathcal{T} \subset \mathcal{S}_G$  et  $\text{Id}_G \in \mathcal{T}$  car  $\text{Id}_G = \tau_1$ .

Soit  $f, g \in \mathcal{T}$ , on peut écrire  $f = \tau_a$  et  $g = \tau_b$  avec  $a, b \in G$ . On a alors

$$f \circ g^{-1} = \tau_a \circ (\tau_b)^{-1} = \tau_a \circ \tau_{b^{-1}} = \tau_{ab^{-1}} \in \mathcal{T}$$

car  $ab^{-1} \in G$ .

Ainsi  $\mathcal{T}$  est un sous-groupe de  $(\mathcal{S}_G, \circ)$  et donc  $(\mathcal{T}, \circ)$  est un groupe.

### Exercice 5 : [énoncé]

$\text{Aut}(G) \subset \mathcal{S}_G$  et  $\text{Id}_G \in \text{Aut}(G)$ .

Pour tout  $f, g \in \text{Aut}(G)$ , on a  $f \circ g \in \text{Aut}(G)$  et  $f^{-1} \in \text{Aut}(G)$  par les propriétés sur les automorphismes.

Ainsi  $\text{Aut}(G)$  est un sous-groupe de  $(\mathcal{S}_G, \circ)$ .

**Exercice 6 :** [énoncé]

a) Soit  $x, y, z \in G$ ,

$$(x \top y) \top z = (x * a * y) * a * z = x * a * (y * a * z) = x \top (y \top z)$$

L'élément  $\text{sym}(a)$  est neutre pour la loi  $\top$ . En effet, pour  $x \in G$ , on a

$$x \top \text{sym}(a) = x = \text{sym}(a) \top x$$

Soit  $x \in G$ . Posons  $y = \text{sym}(a) * \text{sym}(x) * \text{sym}(a) \in G$ . On a

$$x \top y = y \top x = \text{sym}(a)$$

b)  $K \subset G$ ,  $\text{sym}(a) = \text{sym}(a) * e$  donc  $\text{sym}(a) \in K$ .

Soit  $\text{sym}(a) * x, \text{sym}(a) * y \in K$ . On a

$$(\text{sym}(a) * x) \top (\text{sym}(a) * y) \top (-1) = \text{sym}(a) * x * a * \text{sym}(a) * \text{sym}(y) * a * \text{sym}(a) = \text{sym}(a) * (x * \text{sym}(y)) \in K$$

c) Pour  $x, y \in G$ ,

$$f(x * y) = x * y * \text{sym}(a) = (x * \text{sym}(a)) \top (y * \text{sym}(a)) = f(x) \top f(y)$$

$f$  est un morphisme de groupe et il est bijectif d'application réciproque

$$g: x \mapsto x * a.$$

**Exercice 7 :** [énoncé]

Soient  $\varphi$  un tel morphisme et  $\tau$  la transposition qui échange 1 et 2. On a  $\tau^2 = \text{Id}$  donc  $\varphi(\tau)^2 = 1$  d'où  $\varphi(\tau) = 1$  ou  $-1$ . Soit  $\tau' = \begin{pmatrix} i & j \end{pmatrix}$  une transposition quelconque de  $\mathcal{S}_n$ . Il existe une permutation  $\sigma \in \mathcal{S}_n$  telle que  $\tau' = \sigma \circ \tau \circ \sigma^{-1}$  et alors  $\varphi(\tau') = \varphi(\tau)$ . Sachant enfin que tout élément de  $\mathcal{S}_n$  est produit de transpositions on peut conclure :

Si  $\varphi(\tau) = 1$  alors  $\varphi: \sigma \mapsto 1$ . Si  $\varphi(\tau) = -1$  alors  $\varphi = \varepsilon$  (morphisme signature).

**Exercice 8 :** [énoncé]

Si l'application  $\varphi$  était constante, elle serait constante égale à 1 car c'est un morphisme. Puisque  $\varphi$  n'est pas constante, il existe  $a \in G$  tel que  $\varphi(a) \neq 1$ . On vérifie que l'application  $x \mapsto a * x$  est une permutation de  $G$  car

$$\forall y \in G, \exists ! x \in G, y = a * x$$

On en déduit

$$\sum_{x \in G} \varphi(a * x) = \sum_{x \in G} \varphi(x)$$

car les deux sommes comportent les mêmes termes. Or  $\varphi(a * x) = \varphi(a)\varphi(x)$  donc

$$\sum_{x \in G} \varphi(a * x) = \varphi(a) \sum_{x \in G} \varphi(x)$$

Puisque  $\varphi(a) \neq 1$ , on conclut

$$\sum_{x \in G} \varphi(x) = 0$$

**Exercice 9 :** [énoncé]

Non,  $\{(x, x) \mid x \in \mathbb{Z}\}$  est un sous-groupe de  $(\mathbb{Z}^2, +)$  mais n'est pas produit de deux sous-groupes de  $(\mathbb{Z}, +)$  !

**Exercice 10 :** [énoncé]

Si  $H \subset K$  ou  $K \subset H$  alors  $H \cup K = K$  (resp.  $H$ ) et donc  $H \cup K$  est un sous-groupe de  $(G, *)$

Inversement, supposons que  $H \cup K$  est un sous groupe et que  $H \not\subset K$ . Il existe alors  $h \in H$  tel que  $h \notin K$ .

Pour tout  $k \in K$ , on a  $k * h \in H \cup K$  car  $H \cup K$  est stable.

Si  $k * h \in K$  alors  $h = k^{-1} * (k * h) \in K$  ce qui est exclu.

Il reste  $k * h \in H$  qui donne  $k = (k * h) * h^{-1} \in H$ . Ainsi  $K \subset H$ .

Ainsi si  $H \cup K$  est un sous-groupe alors  $H \subset K$  ou  $K \subset H$ .

**Exercice 11 :** [énoncé]

a) Soit  $\varphi: G \rightarrow G'$  un tel morphisme et  $H = \{x \in G \mid \varphi(x) = e_{G'}\}$  son noyau.

On sait déjà que  $H$  est un sous-groupe de  $(G, \cdot)$ .

Soient  $x \in H$  et  $a \in G$ . On a

$$\varphi(axa^{-1}) = \varphi(a)\varphi(x)\varphi(a)^{-1} = \varphi(a)e_{G'}\varphi(a)^{-1} = e_{G'}$$

donc  $axa^{-1} \in H$ .

b)  $HK \subset G$  et  $e = e.e \in HK$ .

Soient  $a, b \in HK$ . On peut écrire

$$a = xy \text{ et } b = x'y' \text{ avec } x, x' \in H \text{ et } y, y' \in K$$

On a alors

$$ab = xyx'y'$$

Puisque  $z = yx'y^{-1} \in H$ , on a encore

$$ab = (xz)(yy') \in HK$$

Aussi

$$a^{-1} = y^{-1}x^{-1} = zy^{-1} \in HK$$

avec  $z = y^{-1}x^{-1}y \in H$ .

Ainsi  $HK$  est bien un sous-groupe de  $(G, \cdot)$ .

**Exercice 12 :** [\[énoncé\]](#)

Notons  $T$  l'ensemble des éléments d'ordre fini d'un groupe abélien  $(G, *)$  de neutre  $e$ .

On a évidemment  $T \subset G$  et  $e \in T$ .

Si  $x, y \in T$  avec  $x^n = y^m = e$  alors

$$(x * y^{-1})^{mn} = x^{mn} * y^{-mn} = e$$

donc  $x * y^{-1} \in T$ .

**Exercice 13 :** [\[énoncé\]](#)

- a) L'application  $f: H \rightarrow aH$  définie par  $f(x) = ax$  est bijective.
- b) Si  $aH \cap bH \neq \emptyset$  alors  $b^{-1}a \in H$  et alors puisque  $ax = bb^{-1}ax$  on a  $aH \subset bH$ . Par symétrie  $aH = bH$ .
- c) Notons  $k$  le nombre d'ensembles  $aH$  deux à deux distincts. La réunion de ceux-ci est égale à  $G$  donc par cardinalité  $\text{Card } G = k \text{ Card } H$  d'où  $\text{Card } H \mid \text{Card } G$ .
- d)  $\langle x \rangle$  est un sous-groupe de  $(G, \cdot)$  de cardinal égal à l'ordre de l'élément  $x$ .

**Exercice 14 :** [\[énoncé\]](#)

Notons

$$H = \left\{ x + y\sqrt{3} \mid x \in \mathbb{N}, y \in \mathbb{Z}, x^2 - 3y^2 = 1 \right\}$$

Pour  $a \in H$ ,  $a = x + y\sqrt{3}$  avec  $x \in \mathbb{N}$ ,  $y \in \mathbb{Z}$  et  $x^2 - 3y^2 = 1$ . On a donc  $x = \sqrt{1 + 3y^2} > \sqrt{3}|y|$  puis  $a > 0$ . Ainsi  $H \subset \mathbb{R}_+^*$ .

$1 \in H$  car on peut écrire  $1 = 1 + 0\sqrt{3}$  avec  $1^2 - 3 \cdot 0^2 = 1$ .  
Pour  $a \in H$ , on a avec des notations immédiates,

$$\frac{1}{a} = x - y\sqrt{3}$$

avec  $x \in \mathbb{N}$ ,  $-y \in \mathbb{Z}$  et  $x^2 - 3(-y)^2 = 1$ . Ainsi  $1/a \in H$ .  
Pour  $a, b \in H$  et avec des notations immédiates,

$$ab = xx' + 3yy' + (xy' + x'y)\sqrt{3}$$

avec  $xx' + 3yy' \in \mathbb{Z}$ ,  $xy' + x'y \in \mathbb{Z}$  et  $(xx' + 3yy')^2 - 3(xy' + x'y)^2 = 1$ .

Enfin puisque  $x > \sqrt{3}|y|$  et  $x' > \sqrt{3}|y'|$ , on a  $xx' + 3yy' \geq 0$  et finalement  $ab \in H$ .

**Exercice 15 :** [\[énoncé\]](#)

Supposons  $AH = H$ .

$$\forall a \in A, a = ae \in AH = H$$

donc  $A \subset H$ .

Supposons  $A \subset H$ . Pour  $x \in AH$ ,  $x = ah$  avec  $a \in A$ ,  $h \in H$ . Or  $a, h \in H$  donc  $x = ah \in H$ .

Ainsi  $AH \subset H$ .

Inversement, pour  $a \in A$  (il en existe car  $A \neq \emptyset$ ) et pour tout  $h \in H$ ,  $h = a(a^{-1}h)$  avec  $a^{-1}h \in H$  donc  $h \in AH$ . Ainsi  $H \subset AH$  puis =.

**Exercice 16 :** [\[énoncé\]](#)

- a) Soit  $H$  un tel groupe. Nécessairement  $H \neq \{0\}$  ce qui permet d'introduire

$$a = \inf \{h > 0 \mid h \in H\}$$

Si  $a \neq 0$ , on montre que  $a \in H$  puis par division euclidienne que tout  $x \in H$  est multiple de  $a$ . Ainsi  $H = a\mathbb{Z}$  ce qui est exclu. Il reste  $a = 0$  et alors pour tout  $\varepsilon > 0$ , il existe  $\alpha \in H \cap ]0; \varepsilon]$ . On a alors  $\alpha\mathbb{Z} \subset H$  et donc pour tout  $x \in \mathbb{R}$ , il existe  $h \in \alpha\mathbb{Z} \subset H$  vérifiant  $|x - h| \leq \alpha \leq \varepsilon$ . Ainsi  $H$  est dense dans  $\mathbb{R}$ .

- b) Soit  $x \in \mathbb{R} \setminus \mathbb{Q}$ . Pour  $N \in \mathbb{N}^*$ , considérons l'application

$$f: \{0, \dots, N\} \rightarrow [0; 1[$$

définie par  $f(k) = kx - [kx]$ . Puisque les  $N + 1$  valeurs prises par  $f$  sont dans les  $N$  intervalles  $[i/N; (i + 1)/N[$  (avec  $i \in \{0, \dots, N - 1\}$ ), il existe au

moins deux valeurs prises dans le même intervalle. Ainsi, il existe  $k < k' \in \{0, \dots, N\}$  tel que

$$|f(k') - f(k)| < \frac{1}{N}$$

. En posant  $p = \lfloor k'x \rfloor - \lfloor kx \rfloor \in \mathbb{Z}$  et  $q = k' - k \in \{1, \dots, N\}$ , on a  $|qx - p| < 1/N$  et donc

$$\left| x - \frac{p}{q} \right| < \frac{1}{Nq} < \frac{1}{q^2}$$

En faisant varier  $N$ , on peut construire des couples  $(p, q)$  distincts et donc affirmer qu'il existe une infinité de couple  $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$  vérifiant

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^2}$$

c) Puisque  $\pi$  est irrationnel, il existe une suite de rationnels  $p_n/q_n$  vérifiant

$$\left| \pi - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}$$

avec  $q_n \rightarrow +\infty$ .

On a alors

$$|u_{p_n}| = \left| \frac{1}{p_n \sin p_n} \right| = \left| \frac{1}{p_n \sin(p_n - q_n \pi)} \right| \geq \frac{1}{|p_n|} \frac{1}{|p_n - q_n \pi|} \geq \frac{q_n}{p_n} \rightarrow \frac{1}{\pi}$$

Ainsi la suite  $(u_n)$  ne tend pas vers 0.

$$\{|\sin n| \mid n \in \mathbb{N}\} = \{|\sin(n + 2k\pi)| \mid n \in \mathbb{Z}, k \in \mathbb{Z}\} = |\sin(\mathbb{Z} + 2\pi\mathbb{Z})|$$

Puisque le sous-groupe  $H = \mathbb{Z} + 2\pi\mathbb{Z}$ , n'est pas monogène (car  $\pi$  irrationnel),  $H$  est dense dans  $\mathbb{R}$  et par l'application  $|\sin(\cdot)|$  qui est une surjection continue de  $\mathbb{R}$  sur  $[0; 1]$ , on peut affirmer que  $\{|\sin n| \mid n \in \mathbb{N}\}$  est dense dans  $[0; 1]$ .

En particulier, il existe une infinité de  $n$  tel que  $|\sin n| \geq 1/2$  et pour ceux-ci  $|u_n| \leq 2/n$ .

Ainsi, il existe une suite extraite de  $(u_n)$  convergeant vers 0.

Au final, la suite  $(u_n)$  diverge.

**Exercice 17 :** [énoncé]

a) La relation est immédiatement réflexive et symétrique.

En discutant selon les cas d'égalité, on montre aussi qu'elle est transitive.

b) S'il n'existe pas dans  $(G, \cdot)$  d'élément d'ordre 2, les classes d'équivalence de la relation  $\mathcal{R}$  comportent toutes deux éléments sauf celle de  $e$  qui ne comporte qu'un élément. Les classes d'équivalence étant disjointes de réunion  $G$ , le cardinal de  $G$  est alors impair ce qui est contraire aux hypothèses.

**Exercice 18 :** [énoncé]

a) Puisque  $a$  est inversible,  $a$  est régulier ce qui fournit l'injectivité de l'application  $x \mapsto a * x$ .

Un argument de cardinalité finie donne la bijectivité de l'application.

b) Par permutation

$$\prod_{x \in G} x = \prod_{x \in G} (a * x) = a^n * \prod_{x \in G} x$$

donc  $a^n = e$ .

**Exercice 19 :** [énoncé]

Notons, pour  $n = 6$  que  $(\mathcal{S}_3, \circ)$  est un groupe non commutatif à 6 éléments.

Un groupe à  $n = 1$  élément est évidemment commutatif.

Pour  $n = 2, 3$  ou  $5$ , les éléments d'un groupe à  $n$  éléments vérifient  $x^n = e$ .

Puisque  $n$  est premier, un élément autre que  $e$  de ce groupe est un élément d'ordre  $n$  et le groupe est donc cyclique donc commutatif.

Pour  $n = 4$ , s'il y a un élément d'ordre 4 dans le groupe, celui-ci est cyclique.

Sinon, tous les éléments du groupe vérifient  $x^2 = e$ . Il est alors classique de justifier que le groupe est commutatif.

**Exercice 20 :** [énoncé]

a) On a évidemment

$$(ab)^{pq} = (a^p)^q (b^q)^p = e$$

Inversement, supposons  $(ab)^r = e$ . On a alors

$$a^{qr} = (a^r)^q = (b^{-r})^q = (b^q)^{-r} = e$$

et donc  $p$  divise  $qr$ . Or  $p$  et  $q$  sont premiers entre eux donc  $p$  divise  $r$ .

Mutatis mutandis, on obtient que  $q$  divise  $r$  et donc  $pq$  divise  $r$  car  $p$  et  $q$  sont premiers entre eux.

Finalement  $ab$  est un élément d'ordre  $pq$  exactement.

- b) Dans  $(\mathbb{C}^*, \times)$ ,  $a = -1$  est d'ordre 2 et  $b = -j$  est d'ordre 6 tandis que  $ab = j$  est d'ordre 3.  
Plus simplement encore, si  $x$  est d'ordre  $n$  alors  $x \times x^{-1}$  est d'ordre 1.

**Exercice 21 :** [énoncé]

- a) On a évidemment

$$(ab)^{pq} = (a^p)^q (b^q)^p = e$$

Inversement, supposons  $(ab)^r = e$ . On a alors

$$a^{qr} = (a^r)^q = (b^{-r})^q = (b^q)^{-r} = e$$

et donc  $p$  divise  $qr$ . Or  $p$  et  $q$  sont premiers entre eux donc  $p$  divise  $r$ .  
Mutatis mutandis, on obtient que  $q$  divise  $r$  et donc  $pq$  divise  $r$  car  $p$  et  $q$  sont premiers entre eux.  
Finalement  $ab$  est un élément d'ordre  $pq$  exactement.

- b) On peut écrire  $p = dp'$ . Considérons alors  $x = a^{p'}$ .  
On a

$$x^k = e \iff a^{kp'} = e \iff p \mid kp' \iff d \mid k$$

et donc  $x$  est un élément d'ordre  $k$ .

- c) Écrivons les décompositions en facteurs premiers de  $p$  et  $q$  (avec des facteurs premiers communs quitte à autoriser les exposants à être nuls)

$$p = p_1^{\alpha_1} \dots p_N^{\alpha_N} \text{ et } q = p_1^{\beta_1} \dots p_N^{\beta_N}$$

On sait qu'alors

$$m = p_1^{\max(\alpha_1, \beta_1)} \dots p_N^{\max(\alpha_N, \beta_N)}$$

Par la question b), il est possible de déterminer  $a_i$  élément d'ordre  $p_i^{\max(\alpha_i, \beta_i)}$  et puisque les  $a_1, \dots, a_N$  sont deux à deux premiers entre eux,  $x = a_1 \dots a_N$  est un élément d'ordre  $m$  comme le montre un raisonnement par récurrence basé sur le résultat de la question a).

**Exercice 22 :** [énoncé]

- a) Puisque  $G$  est abélien

$$z^{pq} = x^{pq} y^{pq} = (x^p)^q (y^q)^p = e$$

De plus, pour  $k \in \mathbb{N}$ , si  $z^k = e$  alors  $z^{kp} = e$  donc  $y^{kp} = e$  ce qui entraîne que  $q$  divise  $kp$ . Or  $p$  et  $q$  sont premiers entre eux donc  $q$  divise  $k$ . De même, on obtient que  $p$  divise  $k$ . À nouveau puisque  $p$  et  $q$  sont premiers entre eux, on conclut que  $pq$  divise  $k$ . L'ordre de  $z$  est donc exactement  $pq$ .

- b) Puisque  $p_i^{\alpha_i}$  est facteur du ppcm des ordres des éléments de  $(G, \cdot)$ , il existe un élément  $x$  dans  $G$  d'ordre  $p_i^{\alpha_i} d$  pour un certain  $d \in \mathbb{N}^*$ . L'élément  $x_i = x^d$  est alors d'ordre exactement  $p_i^{\alpha_i}$ .  
c) Une petite récurrence et l'élément  $y = x_1 \dots x_m$  fait l'affaire.

**Exercice 23 :** [énoncé]

```
a) def liste(n):
    L = []
    for k in range(1,n):
        if n % k == 0: L.append(k)
    return L
def phi(n):
    return len(liste(n))
def sumphi(n):
    return sum(liste(n))
```

- b)  $U_n$  est un groupe à  $n$ . Les éléments de ce groupe ont un ordre divisant  $n$  et pour tout  $d$  divisant  $n$ , les éléments du groupe  $U_n$  d'ordre  $d$  sont exactement ceux de  $U_d^*$ . On en déduit que  $U_n$  est la réunion disjointe des  $U_d^*$  pour  $d$  parcourant les diviseurs de  $n$ . On en déduit

$$X^n - 1 = \prod_{z \in U_d} (X - z) = \prod_{d \mid n} \Phi_d$$

- c) Le polynôme  $\Phi_n$  est de degré  $\varphi(n)$  car les racines de l'unité d'ordre  $n$  sont les  $e^{2ik\pi/n}$  avec  $k \in \llbracket 1; n \rrbracket, k \wedge n = 1$

L'identité précédente donne la relation voulue en passant celle-ci au degré.

- d) Par récurrence forte sur l'entier  $n \geq 1$ .

La propriété est immédiate quand  $n = 1$ . Supposons la propriété vérifiée jusqu'au rang  $n - 1$ .

On a

$$X^n - 1 = \prod_{d \mid n, d \neq n} \Phi_d \times \Phi_n$$

Le polynôme  $X^n - 1$  est à coefficients entiers et  $\prod_{d|n, d \neq n}$  l'est aussi. De plus, le coefficient dominant de ce dernier vaut 1. On réalisant une division euclidienne, le calcul de  $\Phi_n$  détermine un polynôme à coefficients entiers.

e) Les diviseurs de  $n$  sont  $1, p, q, r, pq, qr, rp$  et  $n$  donc

$$Q_n = (X - 1)\Phi_p\Phi_q\Phi_r\Phi_{pq}\Phi_{qr}\Phi_{rp}\Phi_n$$

De même

$$Q_{pq} = (X - 1)\Phi_p\Phi_q\Phi_{pq}, \text{ etc}$$

La relation demandée s'en déduit.

f) Par ce qui précède, on peut écrire

$$(\Phi_n - R)Q_{pq}Q_{qr}Q_{rp} = R(Q_n - Q_{pq}Q_{qr}Q_{rp})$$

0 n'est pas racine de  $Q_{pq}Q_{qr}Q_{rp}$ , ni de  $R$ , mais

$$Q_n - Q_{pq}Q_{qr}Q_{rp} = X^{pq} + \dots$$

On en déduit que 0 est racine de multiplicité  $pq$  de  $\Phi_n - R$ .

g) Puisque  $r < pq$ , le coefficient de  $X^r$  dans  $\Phi_n$  est celui de  $X^r$  dans  $P$ . Or

$$\begin{aligned} P &= (X^p - 1)(X^q - 1)(1 + X + \dots + X^{r-1}) \\ &= (1 - X^p - X^q + X^{p+q})(1 + X + \dots + X^{r-1}) \end{aligned}$$

Le coefficient de  $X^r$  dans ce polynôme est  $-2$  car  $p + q > r$ .

**Exercice 24 :** [énoncé]

- a)  $\sigma \circ \tau \circ \sigma^{-1} = (2 \ 3), \sigma^2 \circ \tau \circ \sigma^{-2} = (3 \ 4), \dots, \sigma^k \circ \tau \circ \sigma^{-k} = (k+1 \ k+2)$ .
- b) Il est « connu » que toute permutation de  $\mathcal{S}_n$  peut s'écrire comme produit de transpositions de la forme  $(k \ k+1)$ . Ces dernières peuvent s'écrire comme produit de  $\sigma$ , de  $\tau$ , et de  $\sigma^{-1}$ . Or  $\sigma^n = \text{Id}$  et donc  $\sigma^{-1} = \sigma^{n-1}$  et par conséquent,  $\sigma^{-1}$  peut s'écrire comme produit de  $\sigma$ .

**Exercice 25 :** [énoncé]

- a)  $\chi \circ \tau \circ \chi^{-1} = (2 \ 3), \chi^2 \circ \tau \circ \chi^{-2} = (3 \ 4), \text{ etc.}$   
Les transpositions de la forme  $(i \ i+1)$  appartiennent au sous-groupe engendré par  $\chi$  et  $\tau$ . Or pour  $1 \leq i < j \leq n$ , on observe

$$(i \ j) = (i \ i+1) \circ \dots \circ (j-1 \ j) \circ \dots \circ (i \ i+1)$$

donc toutes les transpositions appartiennent au sous-groupe engendré par  $\chi$  et  $\tau$ . Sachant que toute permutation est produit de transposition, on peut conclure que  $\{\chi, \tau\}$  engendre le groupe  $(\mathcal{S}_n, \circ)$ .

- b) Le groupe  $(\mathcal{S}_n, \circ)$  n'étant pas commutatif ( $n \geq 3$ ), il n'est pas monogène.

**Exercice 26 :** [énoncé]

- a) Pour  $i \neq j \in \{2, \dots, n\}$ ,

$$(i, j) = (1, i) \circ (1, j) \circ (1, i)$$

Toute transposition appartient à  $\langle t_2, t_3, \dots, t_n \rangle$  et puisque celles-ci engendrent  $S_n$ ,

$$S_n = \langle t_2, t_3, \dots, t_n \rangle$$

- b) Si  $s = (i, j)$ ,  $u_s$  est la réflexion par rapport à l'hyperplan de vecteur normal  $e_i - e_j$ .
- c) Si  $s$  est le produit de  $p$  transpositions alors  $\ker(u_s - \text{Id}_E)$  contient l'intersection de  $p$  hyperplans (ceux correspondant aux transpositions comme décrit ci-dessus). Or, ici  $\ker(u_s - \text{Id}_E) = \text{Vect}(e_1 + \dots + e_n)$  et donc  $p \geq n - 1$ .
- d)  $n - 1$  en conséquence de ce qui précède.

**Exercice 27 :** [énoncé]

Notons  $K$  le complémentaire de  $H$  dans  $G$  et montrons  $\langle K \rangle = G$ .

On a évidemment  $\langle K \rangle \subset G$ .

Inversement, on a  $K \subset \langle K \rangle$  et il suffit d'établir  $H \subset \langle K \rangle$  pour conclure.

Puisque  $H$  est un sous-groupe strict de  $G$ , son complémentaire  $K$  est non vide et donc il existe  $a \in K$ .

Pour  $x \in H$ , l'élément  $a * x$  ne peut appartenir à  $H$  car sinon  $a = (a * x) * x^{-1}$  serait élément du sous-groupe  $H$ . On en déduit que  $a * x \in K$  et donc

$$x = a^{-1} * (a * x) \in \langle K \rangle$$

Ainsi

$$G = H \cup K \subset \langle K \rangle$$

et on peut conclure  $\langle K \rangle = G$ .

**Exercice 28 :** [énoncé]

Soit  $a$  un générateur du groupe cyclique  $(G, *)$  introduit dans l'énoncé.

On sait

$$G = \{e, a, a^2, \dots, a^{n-1}\} \text{ avec } a^n = e$$

Puisque  $x$  est élément de  $G$ , il existe  $k \in \llbracket 0; n-1 \rrbracket$  tel que  $x = a^k$  et alors

$$x^n = a^{kn} = e$$

**Exercice 29 :** [énoncé]

a) L'ensemble des  $n \in \mathbb{N}^*$  est une partie non vide (car  $a^{\text{Card } G} = e \in H$ ) de  $\mathbb{N}$ , elle possède donc un plus petit élément.

b) Posons  $b = a^n$ . Puisque  $b$  appartient au sous-groupe  $H$ ,  $\langle b \rangle \subset H$ .  
Considérons ensuite  $x \in H$ . Il existe  $p \in \mathbb{Z}$  tel que  $x = a^p$ . Soit  $r$  le reste de la division euclidienne de  $p$  par  $n$

$$p = nq + r \text{ avec } 0 \leq r < n$$

Comme  $a^r = a^{p-nq} = x b^{-q}$ , on a  $a^r \in H$  et par définition de  $n$ , on obtient  $r = 0$ .

Par suite  $x = a^{nq} = b^q$  et donc  $x \in \langle b \rangle$ . Ainsi  $H = \langle b \rangle$  est cyclique.

**Exercice 30 :** [énoncé]

Par isomorphisme, on peut supposer que  $G = \mathbb{Z}/n\mathbb{Z}$  ce qui rend les choses plus concrètes.

Soient  $d \in \mathbb{N}^*$  un diviseur de  $n$  et  $d'$  son complément à  $n$  :  $d' = n/d$ .

$H = \langle \bar{d}' \rangle = \{0, \bar{d}', 2\bar{d}', \dots, (d-1)\bar{d}'\}$  est un sous-groupe de  $\mathbb{Z}/n\mathbb{Z}$  à  $d$  éléments.

Inversement, considérons un sous-groupe  $H$  à  $d$  éléments.

Pour tout  $\bar{x}$  de  $H$ , on a  $d\bar{x} = \bar{0}$  car l'ordre d'un élément divise celui du groupe.

Par suite  $n \mid dx$  puis  $d' \mid x$  ce qui donne  $\bar{x} \in \{0, \bar{d}', 2\bar{d}', \dots, (d-1)\bar{d}'\}$ .

Ainsi  $H \subset \{0, \bar{d}', 2\bar{d}', \dots, (d-1)\bar{d}'\}$  puis l'égalité par cardinalité.

**Exercice 31 :** [énoncé]

a)  $(h, k)^n = 1_{H \times K} \iff p \mid n \text{ et } q \mid n$  donc  $(h, k)$  est un élément d'ordre  $\text{ppcm}(p, q)$ .

b) Posons  $p$  et  $q$  les ordres de  $H$  et  $K$ .

Supposons  $p$  et  $q$  premiers entre eux.

Si  $h$  et  $k$  sont générateurs de  $H$  et  $K$  alors  $(h, k)$  est un élément d'ordre  $\text{ppcm}(p, q) = pq$  de  $H \times K$ .

Or  $\text{Card } H \times K = pq$  donc  $H \times K$  est cyclique.

Inversement, supposons  $H \times K$  cyclique.

Si  $(h, k)$  est générateur de  $H \times K$  alors  $h$  et  $k$  sont respectivement générateurs de  $H$  et  $K$ .

On en déduit que  $h$  est un élément d'ordre  $p$ ,  $k$  d'ordre  $q$  et puisque  $(h, k)$  est d'ordre  $\text{ppcm}(p, q)$  et  $pq$ , on conclut que  $p$  et  $q$  sont premiers entre eux.

**Exercice 32 :** [énoncé]

a)  $G_p \subset \mathbb{C}^*$ ,  $1 \in G_p$ , pour  $z \in G_p$ , il existe  $k \in \mathbb{N}$  tel que  $z^{p^k} = 1$  et alors  $(1/z)^{p^k} = 1$  donc  $1/z \in G_p$ .

Si de plus  $z' \in G_p$ , il existe  $k' \in \mathbb{N}$  vérifiant  $z'^{p^{k'}} = 1$  et alors

$$(zz')^{p^{k+k'}} = (z^{p^k})^{p^{k'}} (z'^{p^{k'}})^{p^k} = 1 \text{ donc } zz' \in G_p.$$

b) Notons

$$U_{p^k} = \{z \in \mathbb{C} \mid z^{p^k} = 1\}$$

Soit  $H$  un sous-groupe de  $G_p$  différent de  $G_p$ .

S'il existe une infinité de  $k \in \mathbb{N}$  vérifiant  $U_{p^k} \subset H$  alors  $H = G_p$  car  $G_p$  est la réunion croissante de  $U_{p^k}$ .

Ceci étant exclu, on peut introduire le plus grand  $k \in \mathbb{N}$  vérifiant  $U_{p^k} \subset H$ .

Pour  $\ell > k$ , tous les éléments de  $U_{p^\ell} \setminus U_{p^k}$  engendrent au moins  $U_{p^{k+1}}$ , or  $U_{p^{k+1}} \not\subset H$  donc  $H \subset U_{p^k}$  puis  $H = U_{p^k}$ .

$H$  est donc un sous-groupe cyclique et ne peut être maximal pour l'inclusion car inclus dans le sous-groupe propre  $U_{p^{k+1}}$ .

c) Si  $G_p$  pouvait être engendré par un système fini d'éléments, il existerait  $k \in \mathbb{N}$  tel que ses éléments sont tous racines  $p^k$ -ième de l'unité et alors  $G_p \subset U_{p^k}$  ce qui est absurde.

**Exercice 33 :** [énoncé]

a) Par la factorisation  $a^2 - b^2 = (a - b)(a + b)$

$$a^{2^{n-2}} - 1 = (a^{2^{n-3}} + 1)(a^{2^{n-3}} - 1)$$

et en répétant l'opération

$$a^{2^{n-2}} - 1 = (a^{2^{n-3}} + 1)(a^{2^{n-4}} + 1) \dots (a^{2^0} + 1)(a^{2^0} - 1)$$

Il y a  $n - 1$  facteurs dans ce produit et ceux-ci sont tous pairs car  $a$  est impair. De plus, les deux derniers facteurs sont  $a + 1$  et  $a - 1$  et parmi ces deux figure un multiple de 4.

On en déduit que  $2^n$  divise  $a^{2^{n-2}} - 1$  et donc  $a^{2^{n-2}} \equiv 1 \pmod{2^n}$ .

b) Par l'absurde supposons  $(\mathbb{Z}/2^n\mathbb{Z})^*$  cyclique.

Les éléments de ce groupe sont les  $\bar{k}$  avec  $2 \nmid k = 1$ , ce sont donc les classes des entiers impairs. Il y en a exactement  $2^{n-1}$ . Si  $\bar{a}$  est un générateur de  $(\mathbb{Z}/2^n\mathbb{Z})^*$  alors  $a$  est un entier impair et  $\bar{a}$  est un élément d'ordre  $2^{n-1}$ . Or le résultat précédent donne  $\bar{a}^{2^{n-2}} = \bar{1}$  et donc l'ordre de  $a$  est inférieur à  $2^{n-2} < 2^{n-1}$ . C'est absurde.

**Exercice 34 :** [\[énoncé\]](#)

a) On obtient  $\chi_M(X) = (-1)^n(X^n - 1)$ .

Les racines de  $\chi_M$  sont les racines de l'unité, il y en a  $n$  ce qui est la taille de la matrice et donc  $M$  est diagonalisable.

Puisque 0 n'est pas racine de  $\chi_M$ , la matrice  $M$  est inversible.

b) Par Cayley-Hamilton, nous savons  $M^n = I_n$  et donc  $M$  est un élément d'ordre fini du groupe  $(GL_n(\mathbb{C}), \times)$ . Par calcul ou par considération de polynôme minimal, on peut affirmer que  $n$  est le plus petit exposant  $p > 0$  tel que  $M^p = I_n$  et donc  $M$  est un élément d'ordre exactement  $n$ . On en déduit que  $G$  est un groupe cyclique de cardinal  $n$ .

**Exercice 35 :** [\[énoncé\]](#)

a) Le groupe  $(G, *)$  est nécessairement commutatif car cyclique. Pour tout  $x, y \in G$ , on a

$$f(x * y) = (x * y)^r = x^r * y^r = f(x) * f(y)$$

b) Pour  $x \in G$ , on peut écrire  $x = a^k$  avec  $k \in \mathbb{Z}$  et alors

$$f(x) = e \iff a^{kr} = e$$

Puisque  $a$  est d'ordre  $n$

$$f(x) = e \iff n \mid kr$$

En introduisant  $d = \text{pgcd}(n, r)$ , on peut écrire  $n = dn'$  et  $r = dr'$  avec  $n' \wedge r' = 1$  et alors le théorème de Gauss donne

$$n \mid kr \iff n' \mid k$$

Par conséquent

$$\ker f = \langle a^{n'} \rangle$$

c) Par l'égalité de Bézout, on peut écrire  $nu + rv = d$  et alors

$$a^d = a^{nu} * a^{rv} = a^{rv} = f(a^v) \in \text{Im } f$$

Puisque  $\text{Im } f$  est un sous-groupe, on a déjà  $\langle a^d \rangle \subset \text{Im } f$ .

Inversement, soit  $y \in \text{Im } f$ . On peut écrire  $y = x^r$  avec  $x$  de la forme  $a^k$  où  $k \in \mathbb{Z}$ . On a donc

$$y = a^{kr}$$

Or  $d \mid r$  et donc  $y \in \langle a^d \rangle$ . Ainsi  $\text{Im } f \subset \langle a^d \rangle$  puis l'égalité.

d) Si  $y \notin \text{Im } f$ , l'équation n'a pas de solution. Sinon, il existe  $x_0 \in G$  tel que  $x_0^r = y$  et alors

$$x^r = y \iff (x * x_0^{-1})^r = e$$

Ceci permet de mettre en correspondance bijective les solutions de l'équation  $x^r = y$  avec les éléments du noyau de  $f$ . Dans ce cas, il y a exactement  $n/n' = d$  solutions à l'équation.

**Exercice 36 :** [\[énoncé\]](#)

Commençons par rappeler que les éléments de  $\text{SO}(2)$  sont les matrices

$$R(\theta) = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

Soit  $G$  un sous-groupe fini de  $(\text{SO}(2), \times)$ .

L'ensemble  $T = \{\theta > 0 \mid R(\theta) \in G\}$  est une partie non vide (car  $2\pi$  en est élément) et minorée de  $\mathbb{R}$ . On peut donc introduire

$$\theta_0 = \inf T \in \mathbb{R}_+$$

Commençons par établir que  $\theta_0$  est élément de  $T$ .

On peut construire une suite  $(\theta_n)_{n \geq 1}$  d'éléments de  $T$  convergeant vers  $\theta_0$ .

Puisque l'ensemble  $G$  est fini, l'ensemble des  $R(\theta_n)$  est lui aussi fini. Il existe donc une infinité d'indices  $n$  pour lesquels les  $\theta_n$  sont égaux modulo  $2\pi$  à une valeur  $\alpha$ .

Puisque  $\theta_n \rightarrow \theta_0$ , il y a une infinité de  $\theta_n$  égaux à  $\theta_0$  et donc  $\theta_0 \in T$ .

Puisque  $R(\theta_0) \in G$ , on a  $\langle R(\theta_0) \rangle \subset G$ .

Inversement, soit  $R$  un élément de  $G$ . Il existe  $\theta \in \mathbb{R}$  tel que  $R = R(\theta)$ . On peut écrire  $\theta = q\theta_0 + \theta'$  avec  $q \in \mathbb{Z}$  et  $\theta' \in [0; 2\pi[$ . On a alors

$$R(\theta') = R(\theta)R(\theta_0)^{-q} \in G$$

Si  $\theta' > 0$  alors  $\theta' \in T$  ce qui contredit la définition de  $\theta_0 = \inf T$  car  $\theta' < \theta_0$ .

Nécessairement  $\theta' = 0$  et donc  $\theta = q\theta_0$  ce qui donne  $R = R(\theta_0)^q \in \langle R(\theta_0) \rangle$ .

Finalement

$$G = \langle R(\theta_0) \rangle$$

### Exercice 37 : [énoncé]

a)  $G \subset \text{GL}_4(\mathbb{R})$ ,  $G$  est non vide, stable par passage à l'inverse et par produit car  $V$  l'est. Ainsi  $G$  est un sous-groupe de  $\text{GL}_4(\mathbb{R})$  donc un groupe.

b) Si  $M \in G$  alors  $\det M, \det M^{-1} \in \mathbb{Z}$  et  $\det M \times \det M^{-1} = \det I_4 = 1$  donc  $\det M = \pm 1$ .

Inversement si  $\det M = \pm 1$  alors  $M^{-1} = {}^t \text{Com } M \in V$  donc  $M \in G$ .

c)

$$\det M = ((a+c)^2 - (b+d)^2)((a-c)^2 + (b-d)^2)$$

donc

$$\det M = \pm 1 \iff \begin{cases} (a+c)^2 - (b+d)^2 = \pm 1 \\ (a-c)^2 + (b-d)^2 = \pm 1 \end{cases}$$

La résolution de ce système à coefficients entiers donne à l'ordre près :

$a, b, c, d = \pm 1, 0, 0, 0$ .

Posons  $J$  la matrice obtenue pour  $a = c = d = 0$  et  $b = 1$ . On vérifie  $J^4 = I_4$ .

L'application  $\varphi: U_2 \times \mathbb{Z}/4\mathbb{Z} \rightarrow G$  définie par  $\varphi(\varepsilon, n) = \varepsilon J^n$  est bien définie, c'est un morphisme de groupe, injectif et surjectif. Ainsi  $G$  est isomorphe à  $U_2 \times \mathbb{Z}/4\mathbb{Z}$  ou plus élégamment à  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ .

### Exercice 38 : [énoncé]

Non, l'équation  $x^2 = 1$  admet deux solutions dans  $(\mathbb{Q}^*, \times)$  alors que l'équation analogue dans  $(\mathbb{Q}, +)$ , à savoir  $2x = 0$ , n'admet qu'une solution.