

# TD 15 : STRUCTURES ALGÈBRIQUES

## ► Lois de composition interne

**EXERCICE 15.1** Soit  $(E, \leq)$  un ensemble totalement ordonné. Alors pour tout  $(x, y) \in E^2$ ,  $\max(x, y)$  est bien défini. On définit ainsi une loi de composition interne, notée  $\max$  sur  $E$ .

PD

1. Montrer que la loi  $\max$  est associative et commutative.
2. Donner une condition nécessaire et suffisante pour que  $(E, \max)$  possède un élément neutre.
3. Lorsque cette condition est vérifiée, quels sont les éléments inversibles de  $E$  ?

## EXERCICE 15.2 Éléments réguliers

Soit  $E$  un ensemble muni d'une loi de composition interne  $\star$ , associative, et possédant un élément neutre  $e$ . Un élément  $x \in E$  est dit régulier à gauche si  $\forall (y, z) \in E^2, x \star y = x \star z \Rightarrow y = z$  et régulier à droite si  $\forall (y, z) \in E^2, y \star x = z \star x \Rightarrow y = z$ .

AD

1. Quels sont les éléments réguliers (à droite ou à gauche) de  $(\mathbf{Z}, \times)$  ?
2. Soit  $A$  un ensemble. Montrer que dans  $(\mathcal{F}(A, A), \circ)$ , un élément  $f$  est régulier à droite si et seulement si  $f$  est surjective. Donner une condition nécessaire et suffisante pour que  $f$  soit régulier à gauche.

## ► Groupes

**EXERCICE 15.3** On définit une loi de composition interne  $\star$  sur  $\mathbf{R}$  par :  $\forall (x, y) \in \mathbf{R}^2, x \star y = \sqrt[3]{x^3 + y^3}$ . Montrer que  $(\mathbf{R}, \star)$  est un groupe abélien.

PD

**EXERCICE 15.4** Soit  $E$  un ensemble muni d'une loi de composition interne associative  $\star$ , possédant un élément neutre  $e$ , et telle que  $\forall x \in E, x \star x = e$ . Prouver que  $(E, \star)$  est un groupe commutatif.

F

## EXERCICE 15.5 Centre d'un groupe

Soit  $G$  un groupe. On appelle centre de  $G$  l'ensemble  $\mathcal{Z}(G) = \{x \in G, \forall y \in G, xy = yx\}$  des éléments commutant avec tous les éléments de  $G$ . Montrer que  $\mathcal{Z}(G)$  est un sous-groupe de  $G$ . À quelle condition a-t-on  $\mathcal{Z}(G) = G$  ?

PD

## EXERCICE 15.6 Divers sous-groupes

Dans chacun des cas suivants, déterminer si  $H$  est ou non un sous-groupe de  $G$ .

PD

1.  $G = (\mathbf{C}^*, \times)$ ,  $H = \bigcup_{n \in \mathbf{N}^*} \mathbf{U}_n$  tous les coefficients sont dans  $\mathbf{Z}$ .
2.  $G = \mathcal{M}_n(\mathbf{C})$ ,  $H$  l'ensemble des matrices triangulaires supérieures de  $G$ .
3.  $G = GL_2(\mathbf{R})$ ,  $H$  l'ensemble des éléments de  $G$  dont
4.  $G = GL_n(\mathbf{R})$ ,  $H$  l'ensemble des matrices triangulaires supérieures dont les coefficients diagonaux valent 1.
5.  $G = \mathfrak{S}_n$ ,  $H = \{\sigma \in \mathfrak{S}_n \mid \sigma(1) = 2\}$

**EXERCICE 15.7** Donner les tables de multiplication de  $\mathbf{U}_4$  et  $\mathbf{U}_2 \times \mathbf{U}_2$ . Prouver alors que ces deux groupes ne sont pas isomorphes (c'est-à-dire qu'il n'existe pas d'isomorphisme entre ces groupes), bien que de même cardinal.

AD

**EXERCICE 15.8** Soit  $G$  un groupe non réduit à un élément tel que pour tout  $g \in G, g^2 = e$ .

D

1. Montrer que tout élément est égal à son propre inverse. En déduire que  $G$  est abélien.
2. Montrer que  $G$  possède au moins un sous-groupe de cardinal 2.
3. On suppose que  $G$  contient au moins trois éléments. Soit  $H$  un sous-groupe fini de  $G$ , différent de  $\{e\}$  ou de  $G$ , et soit  $g \in G \setminus H$ . On pose alors  $gH = \{gh, h \in H\}$ .
  - (a) Montrer que  $H \cup gH$  est un sous-groupe de cardinal  $2|H|$ .
  - (b) Montrer que si  $G$  est fini, alors son cardinal est une puissance de 2.

## EXERCICE 15.9 Un cas particulier du théorème de Lagrange

Soit  $G$  un groupe commutatif fini, de cardinal  $n$ .

AD

1. Soit  $g \in G$ . Montrer que  $x \mapsto gx$  est une bijection de  $G$  sur lui-même.
2. Soit  $g \in G$ . En calculant de deux manières le produit  $\prod_{x \in G} (gx)$ , montrer que  $g^n = 1_G$ .
3. Déterminer tous les sous-groupes finis de  $(\mathbf{C}^*, \times)$ .

## EXERCICE 15.10 Union de sous-groupes

AD

1. Donner un exemple de deux sous-groupes de  $(\mathbf{R}^*, \times)$  dont l'union n'est pas un sous-groupe.
2. Soit  $G$  un groupe,  $H$  et  $K$  deux sous-groupes de  $G$ . Montrer que  $H \cup K$  est un sous-groupe si et seulement si  $H \subset K$  ou  $K \subset H$ .
3. Soit  $(H_n)_{n \in \mathbf{N}}$  une union croissante de sous-groupes de  $G$ . Montrer que  $\bigcup_{n \in \mathbf{N}} H_n$  est un sous-groupe de  $G$ .

### EXERCICE 15.11 Opérations sur les sous-groupes

Soit  $G$  un groupe,  $H$  et  $K$  deux sous-groupes de  $G$ . On note  $HK = \{h \cdot k, (h, k) \in H \times K\}$

1. Montrer que  $H \cap K$  est un sous-groupe de  $G$ .
2. Si  $G$  est abélien, montrer que  $HK$  est un sous-groupe de  $G$ .
3. (★) Prouver que  $HK$  est un sous-groupe de  $G$  si et seulement si  $HK = KH$ .

**EXERCICE 15.12** Dans cet exercice, on note  $G$  l'ensemble des similitudes directes du plan, qu'on assimile à l'ensemble des fonctions  $f : \mathbf{C} \rightarrow \mathbf{C}$  telles qu'il existe  $(a, b) \in \mathbf{C}^* \times \mathbf{C}$  tels que  $\forall z \in \mathbf{C}, f(z) = az + b$ .

1. Montrer que  $(G, \circ)$  est un groupe, et qu'il n'est pas abélien.
2. Soit  $z_0 \in \mathbf{C}$ . On pose  $G_{z_0} = \{g \in G \mid g(z_0) = z_0\}$ .  
Montrer que  $G_{z_0}$  est un sous-groupe de  $G$ , isomorphe à  $\mathbf{C}^*$ . Est-il abélien ?

**EXERCICE 15.13** Soit  $G$  un groupe abélien fini avec un seul élément  $f$  d'ordre 2 (c'est-à-dire tel que  $f^2 = e$  et  $f \neq e$ ).  
Montrer que  $\prod_{g \in G} g = f$ .

**EXERCICE 15.14** Soit  $G$  un groupe, et soit  $x \in G$ . On dit que  $x$  est d'ordre fini s'il existe  $n \in \mathbf{N}^*$  tel que  $x^n = e_G$ .

1. Montrer que si  $G$  est abélien, et que  $x$  et  $y$  sont d'ordre fini, alors  $xy$  est encore d'ordre fini.
2. Le résultat de la question précédente reste-t-il vrai si  $G$  n'est plus abélien ?

### EXERCICE 15.15 Conjugaison dans un groupe

Soit  $G$  un groupe. Pour  $a \in G$ , on pose  $\tau_a : \begin{cases} G & \longrightarrow & G \\ g & \longmapsto & aga^{-1} \end{cases}$ .

1. Montrer que  $\tau_a$  est un morphisme bijectif de  $G$  dans lui-même (on parle alors d'automorphisme).
2. On pose  $\mathcal{C}(G) = \{\tau_a, a \in G\}$ . Montrer qu'il s'agit d'un sous-groupe de  $(\mathfrak{S}(G), \circ)$ .
3. Montrer que l'application  $\varphi : G \rightarrow \mathfrak{S}(G)$  qui à  $a \in G$  associe  $\tau_a$  est un morphisme de groupes. Quel est son noyau ?

**EXERCICE 15.16** Soit  $f : G_1 \rightarrow G_2$  un morphisme de groupes.

1. Prouver que pour tout sous-groupe  $H_1$  de  $G_1$ ,  $f(H_1)$  est un sous-groupe de  $G_2$ .
2. Prouver que pour tout sous-groupe  $H_2$  de  $G_2$ ,  $f^{-1}(H_2)$  est un sous-groupe de  $G_1$ . En déduire que  $\text{Ker } f$  est un sous-groupe de  $G_1$ .

**EXERCICE 15.17** Déterminer tous les morphismes de groupe de  $(\mathbf{Z}, +)$  dans  $(\mathbf{Z}, +)$ . De  $(\mathbf{Q}, +)$  dans  $(\mathbf{Z}, +)$ .

**EXERCICE 15.18** Soit  $(G, *)$  un groupe, et soit  $A$  une partie non vide finie de  $G$ , stable par  $*$ . Prouver que  $A$  est un sous-groupe de  $G$ .

**EXERCICE 15.19** Soit  $G$  un groupe possédant exactement deux sous-groupes.  
Montrer qu'il existe  $x \in G$  tel que  $G = \langle x \rangle$ , que  $G$  est fini, et que son cardinal est premier.

## ► Anneaux, corps

**EXERCICE 15.20** Montrer que  $\mathbf{Z}[\sqrt{2}] = \{x + y\sqrt{2}, (x, y) \in \mathbf{Z}^2\}$  est un anneau.

Prouver que  $\mathbf{Q}(\sqrt{2}) = \{x + y\sqrt{2}, (x, y) \in \mathbf{Q}^2\}$  est un corps.

**EXERCICE 15.21** Soit  $\mathbb{D}$  l'ensemble des nombres décimaux. Montrer que  $(\mathbb{D}, +, \times)$  est un anneau. Est-ce un corps ?

### EXERCICE 15.22 Produit direct d'anneaux

Soient  $(A, +_A, \times_A)$  et  $(B, +_B, \times_B)$  deux anneaux. On munit  $A \times B$  de deux lois de composition  $\oplus$  et  $\otimes$  définies par :

$$(a, b) \oplus (a', b') = (a +_A a', b +_B b') \text{ et } (a, b) \otimes (a', b') = (a \times_A a', b \times_B b').$$

Montrer que  $(A \times B, \oplus, \otimes)$  est un anneau, commutatif si  $A$  et  $B$  le sont. Cet anneau est-il intègre ?

**EXERCICE 15.23** Parmi les ensembles suivants, lesquels sont des sous-anneaux de  $\mathbf{R}^{\mathbf{N}}$ , l'anneau des suites réelles ?

1. l'ensemble des suites de limite nulle
2. l'ensemble des suites croissantes
3. l'ensemble des suites convergentes
4. l'ensemble des suites divergentes
5. l'ensemble des suites bornées
6. l'ensemble des suites  $(u_n)$  telles que  $\lim_{n \rightarrow +\infty} u_n = +\infty$
7. l'ensemble des suites stationnaires
8. l'ensemble des suites nulles à partir d'un certain rang

**EXERCICE 15.24** Soit  $(A, +, \times)$  un anneau commutatif. Pour  $a \in A$ , on appelle racine carrée de  $a$  tout élément dont le carré vaut  $a$ .

1. Prouver que si  $A$  est intègre, alors tout élément de  $A$  admet au plus deux racines carrées.
2. En revanche, prouver que dans  $(\mathcal{F}(\mathbf{R}, \mathbf{R}), +, \times)$ , la fonction constante  $x \mapsto 1$  possède une infinité de racines carrées.

**EXERCICE 15.25** Soit  $A$  un anneau commutatif et  $E$  un ensemble non vide. À quelle condition  $\mathcal{F}(E, A)$  est-il intègre ?

**EXERCICE 15.26** Soit  $(A, +, \times)$  un anneau. Un élément  $a \in A$  est dit nilpotent s'il existe  $n \in \mathbf{N}$  tel que  $a^n = 0_A$ .

1. Soient  $x, y$  deux éléments nilpotents de  $A$ , qui commutent. Montrer que  $xy$  et  $x + y$  sont nilpotents.
2. Montrer que si  $x \in A$  est nilpotent, alors  $1_A - x \in A^\times$ .

**EXERCICE 15.27** Montrer qu'un anneau commutatif intègre fini est un corps.

**EXERCICE 15.28 Idéaux premiers (D'après oral ENS)**

Soit  $A$  un anneau commutatif non nul. On appelle idéal de  $A$  tout sous-groupe  $I$  de  $(A, +)$  tel que  $\forall (a, x) \in A \times I, ax \in I$ .

1. Montrer que pour tout  $x \in A, xA = \{ax, a \in A\}$  est un idéal de  $A$ .
2. Un idéal  $I$  est dit maximal si tout idéal de  $A$ , différent de  $A$ , et qui contient  $I$  est égal à  $I$  lui-même.  
Et un idéal  $I$  différent de  $A$  est dit premier si  $\forall (a, b) \in A^2, ab \in I \Rightarrow a \in I$  ou  $b \in I$ .
  - (a) Montrer qu'un idéal  $I$  est maximal si et seulement si pour tout  $x \in A \setminus I, I + xA = A$  (où  $I + xA$  est l'ensemble des éléments qui s'écrivent comme somme d'un élément de  $I$  et d'un élément de  $xA$ ).
  - (b) Prouver qu'un idéal maximal est premier.
3. Montrer que  $A$  est un corps si et seulement si tout idéal de  $A$  autre que  $A$  est premier.

AD

PD

D

TD

## CORRECTION DES EXERCICES DU TD 15

## SOLUTION DE L'EXERCICE 15.1

- C'est trivial.
- Supposons que  $E$  contienne un élément neutre  $e$  pour  $\max$ . Alors, pour tout  $x \in E$ ,  $\max(x, e) = x$ , et donc  $e \leq x$ .  
Donc un élément neutre est forcément un minorant de  $E$ , et étant dans  $E$ , c'est le plus petit élément de  $E$ .  
Inversement, si  $E$  possède un plus petit élément  $e$ , alors pour tout  $x \in E$ ,  $\max(x, e) = x$ , et donc  $e$  est élément neutre.  
Ainsi,  $(E, \max)$  possède un élément neutre si et seulement si il possède un plus petit élément.
- L'élément neutre est bien entendu inversible, égal à son propre inverse.  
Soit  $x \in E$  un élément inversible. Alors il existe  $y \in E$  tel que  $\max(x, y) = e$ .  
Donc soit  $x = e$ , soit  $y = e$ .  
Mais si  $y = e$ , alors  $y$  est l'inverse de  $x$ , et donc  $x = y^{-1} = e^{-1} = e$ .  
Donc  $e$  est l'unique élément inversible de  $E$ .

## SOLUTION DE L'EXERCICE 15.2

- Notons que  $\mathbf{Z}$  étant commutatif, les éléments réguliers à droite et réguliers à gauche sont les mêmes.  
Supposons donc que  $x$  soit régulier, et soient  $y, z \in \mathbf{Z}$  tels que  $xy = xz$ .  
Alors  $x(y - z) = 0$ . Et donc soit  $x = 0$ , soit  $y - z = 0 \Leftrightarrow y = z$ .  
Il est clair que  $0$  n'est pas régulier car  $0 \cdot 1 = 0 \cdot 2$ . Donc tout élément non nul de  $\mathbf{Z}$  est régulier.
- Supposons que  $f$  soit surjective, et soient  $g, h \in \mathcal{F}(A, A)$  telles que  $g \circ f = h \circ f$ .  
Soit alors  $y \in A$ . Par surjectivité de  $f$ , il existe  $x \in A$  tel que  $y = f(x)$ .  
Et alors  $g(y) = g(f(x)) = h(f(x)) = h(y)$ . Ceci étant vrai quel que soit  $y \in A$ , on en déduit que  $g = h$ , donc que  $f$  est régulier à droite.

En revanche, si  $f$  n'est pas surjective, alors il existe  $y \in A$  qui ne possède pas d'antécédent par  $f$ . Et alors deux fonctions  $g$  et  $h$  qui diffèrent uniquement en  $y$  vérifient  $\forall x \in A, g(f(x)) = h(f(x))$  car  $f(x) \neq y$ .  
Pourtant  $h \neq g$  par hypothèse, donc  $f$  n'est pas régulier à droite.

## Autrement dit

On suppose que  $g(x) = h(x)$  pour tout  $x \neq y$  et que  $g(y) \neq h(y)$ .

Si  $f$  est injective, soient alors  $g$  et  $h$  deux fonctions telles que  $f \circ g = f \circ h$ .  
Alors pour tout  $x \in A$ ,  $f(g(x)) = f(h(x))$ , et donc  $g(x) = h(x)$ . Donc  $g = h$  :  $f$  est régulier à gauche.  
Inversement, soit  $f$  une fonction régulière à gauche pour la composition, et soient  $x_1, x_2 \in A$  tels que  $f(x_1) = f(x_2)$ .  
Soient alors  $g$  et  $h$  les fonctions constantes égales respectivement à  $x_1$  et  $x_2$ .  
On a donc  $f \circ g = f \circ h$ . Et donc  $g = h$ , de sorte que  $x_1 = x_2$ .

## SOLUTION DE L'EXERCICE 15.3

Commençons par prouver l'associativité de la loi  $\star$  : soient  $x, y, z$  trois réels. Alors

$$x \star (y \star z) = \sqrt[3]{x^3 + \left(\sqrt[3]{y^3 + z^3}\right)^3} = \sqrt[3]{x^3 + y^3 + z^3}.$$

Et d'autre part,

$$(x \star y) \star z = \sqrt[3]{\left(\sqrt[3]{x^3 + y^3}\right)^3 + z^3} = \sqrt[3]{x^3 + y^3 + z^3} = x \star (y \star z).$$

Donc  $\star$  est une loi de composition associative.

Notons qu'elle est clairement commutative, puisque la somme dans  $\mathbf{R}$  est commutative, et donc  $x^3 + y^3 = y^3 + x^3$ .

0 est l'élément neutre pour  $\star$ , puisque pour tout  $x \in \mathbf{R}$ ,  $x \star 0 = \sqrt[3]{x^3} = x$ . Et par commutativité,  $0 \star x = x \star 0 = x$ .

Enfin, tout élément admet bien un inverse, qui est  $-x$ , puisque

$$x \star (-x) = \sqrt[3]{x^3 + (-x)^3} = \sqrt[3]{x^3 - x^3} = \sqrt[3]{0} = 0.$$

Et par commutativité,  $(-x) \star x = 0$ .

Ainsi,  $(\mathbf{R}, \star)$  est bien un groupe.

### SOLUTION DE L'EXERCICE 15.4

Il s'agit donc de prouver que tout élément est inversible, ainsi que la commutativité de  $\star$ . Mais puisque pour tout  $x \in E$ ,  $x \star x = e$ ,  $x$  est inversible, égal à son propre inverse.

Et pour  $(x, y) \in E^2$ , on a  $x \star y = (x \star y)^{-1} = y^{-1} \star x^{-1} = y \star x$ .

Donc  $\star$  est commutative.

### SOLUTION DE L'EXERCICE 15.5

Pour tout  $x \in G$ ,  $ex = xe = x$ , donc  $e \in \mathcal{Z}(G)$ .

Soit  $g \in \mathcal{Z}(G)$ , et soit  $x \in G$ . Alors  $gx^{-1} = x^{-1}g$ , et donc en passant à l'inverse,  $xg^{-1} = g^{-1}x$ , de sorte que  $x$  et  $g^{-1}$  commutent. Ceci étant vrai pour tout  $x \in G$ ,  $g^{-1} \in \mathcal{Z}(G)$ .

Enfin, si  $g, h \in \mathcal{Z}(G)$ , alors pour tout  $x \in G$ ,

$$ghx = g(hx) = g(xh) = (gx)h = xgh.$$

Donc  $gh$  et  $x$  commutent, de sorte que  $gh \in \mathcal{Z}(G)$ .

Et donc nous avons bien vérifié les quatre points caractérisant un sous-groupe,  $\mathcal{Z}(G)$  est un sous-groupe de  $G$ .

On a alors  $\mathcal{Z}(G) = G$  si et seulement si

$$\forall g \in G, g \in \mathcal{Z}(G) \Leftrightarrow \forall (g, h) \in G^2, hg = gh.$$

Soit encore si et seulement si  $G$  est abélien.

### SOLUTION DE L'EXERCICE 15.6

1. 1 (qui est l'élément neutre de  $\mathbf{C}^*$ ) est dans tous les  $\mathbf{U}_n$ , donc dans leur union.

Soient  $x, y \in \bigcup_{n \in \mathbf{N}^*} \mathbf{U}_n$ .

Alors il existe  $n \in \mathbf{N}^*$  tel que  $x^n = 1$  et il existe  $p \in \mathbf{N}^*$  tel que  $y^p = 1$ .

Mais alors  $(xy)^{np} = x^{np}y^{np} = (x^n)^p (y^p)^n = 1^p 1^n = 1$ .

Donc  $xy \in H$ .

De plus, si  $x \in H$ , alors il existe  $n \in \mathbf{N}^*$  tel que  $x^n = 1$ , et donc  $\left(\frac{1}{x}\right)^n = 1$ , donc  $\frac{1}{x} \in \mathbf{U}_n \subset H$ .

Ainsi,  $H$  est un sous-groupe de  $G$ .

2. La matrice nulle est dans  $H$ .

La somme<sup>1</sup> de deux matrices triangulaires supérieures est encore triangulaire supérieure.

Et si  $M \in H$ , alors  $-M$  (qui est l'inverse de  $M$  pour l'addition) est encore dans  $H$ .

Donc  $H$  est un sous-groupe de  $\mathcal{M}_n(\mathbf{C})$ .

3.  $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$  est dans  $H$ , mais son inverse,  $\begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix}$  n'est pas dans  $H$ , donc  $H$  n'est pas un sous-groupe de  $G$ .

4. La matrice  $I_n$  est dans  $H$ .

Le produit de deux matrices de  $H$  est dans  $H$ .

Et si  $M \in H$ , alors son inverse est triangulaire supérieure, et ses coefficients diagonaux sont les inverses de ceux de  $M$ , donc valent tous 1.

Donc  $M^{-1} \in H$  :  $H$  est un sous-groupe de  $G$ .

5.  $\text{id}(1) = 1 \neq 2$ , donc  $\text{id}$ , qui est l'élément neutre de  $\mathfrak{S}_n$  n'est pas dans  $H$  :  $H$  n'est pas un sous-groupe de  $G$ .

### SOLUTION DE L'EXERCICE 15.7

Pour  $\mathbf{U}_4 = \{1, -1, i, -i\}$ , il n'y a pas de difficulté :

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

#### Remarque

Bien que l'élément neutre soit le même que celui du groupe  $(\mathbf{R}, +)$ , et que l'inverse d'un élément  $x$  soit également le même que dans  $(\mathbf{R}, +)$ , il ne s'agit pas du même groupe, car en général,

$$x \star y \neq x + y.$$

Par exemple

$$1 \star 1 = \sqrt[3]{2} \neq 2 = 1 + 1.$$

#### Danger !

$n$  et  $p$  n'ont aucune raison d'être égaux.

<sup>1</sup> Ici,  $\mathcal{M}_n(\mathbf{C})$  est bien muni de la somme.

#### Remarque

Si on ajoute la condition que  $\det A = \pm 1$ , alors  $H$  devient un sous-groupe de  $G$ .

Puisque  $U_2 = \{-1, 1\}$ , le groupe  $U_2 \times U_2$  contient 4 éléments :  $(1, 1)$ ,  $(-1, -1)$ ,  $(1, -1)$ ,  $(-1, 1)$ , et on a alors

$\times$	$(1, 1)$	$(-1, -1)$	$(-1, 1)$	$(1, -1)$
$(1, 1)$	$(1, 1)$	$(-1, -1)$	$(-1, 1)$	$(1, -1)$
$(-1, -1)$	$(-1, -1)$	$(1, 1)$	$(1, -1)$	$(-1, 1)$
$(-1, 1)$	$(-1, 1)$	$(1, -1)$	$(1, 1)$	$(-1, -1)$
$(1, -1)$	$(1, -1)$	$(-1, 1)$	$(-1, -1)$	$(1, 1)$

En particulier, pour tout  $x$  dans  $U_2 \times U_2$ , on a  $x^2 = (1, 1)$  l'élément neutre.

Supposons par l'absurde qu'il existe un isomorphisme  $\varphi : U_2 \times U_2 \rightarrow U_4$ .

Alors pour tout  $y \in U_4$ , il existe un unique  $x \in U_2 \times U_2$  tel que  $y = \varphi(x)$ . Et alors  $y^2 = \varphi(x)^2 = \varphi(x^2) = \varphi((1, 1)) = 1$ .

Autrement dit, le carré de tout élément de  $U_4$  est égal à 1. Ceci est manifestement faux, puisque  $i^2 = -1 \neq 1$ .

Par conséquent, il n'existe pas d'isomorphisme de  $U_2 \times U_2 \rightarrow U_4$ .

### SOLUTION DE L'EXERCICE 15.8

1. Pour tout  $x \in G$ ,  $xx = x^2 = e$ , et donc  $x^{-1} = x$ .
2. Soient  $x, y \in G$ . Alors  $xy = (xy)^{-1}$ . Mais  $(xy)^{-1} = y^{-1}x^{-1}$ , qui par la question précédente vaut  $yx$ . Et donc  $xy = yx$ , si bien que  $G$  est abélien.
3. Il existe  $x \in G$  tel que  $x \neq e$ . Et alors  $\{e, x\}$  est un sous-groupe de  $G$ , de cardinal 2.
- 4.a. Notons qu'un tel sous-groupe  $H$  existe par la question précédente.  
Puisque  $e \in H$ ,  $e \in H \cup gH$ .  
Soient  $g_1, g_2 \in H \cup gH$ . Soit  $g_1 \in H$ , soit il existe  $h_1 \in H$  tel que  $g_1 = gh_1$ .  
De même, soit  $g_2 \in H$ , soit il existe  $h_2 \in H$  tel que  $g_2 = gh_2$ .

Montrons que  $g_1g_2 \in H \cup gH$  est stable par produit, puisque tout élément étant égal à son propre inverse, on aura donc,  $g_1g_2^{-1} = g_1g_2 \in H \cup gH$ .

► Si  $g_1, g_2 \in H$ . Alors  $g_1g_2 \in H$  par définition d'un sous-groupe.

► Si  $g_1 \in H$  et  $g_2 \notin H$ . Alors  $g_1g_2 = g_1gh_2 = g \underbrace{(g_1h_2)}_{\in H} \in gH \subset H \cup gH$ .

► Si  $g_1 \notin H$  et  $g_2 \in H$ . Alors  $g_1g_2 = g \underbrace{(h_1g_2)}_{\in H}$ .

► Si  $g_1 \notin H$  et  $g_2 \notin H$ . Alors  $g_1g_2 = gh_1gh_2 = g^2h_1h_2 = h_1h_2 \in H \subset H \cup gH$ .

Donc nous avons bien prouvé que pour tout  $g_1, g_2 \in H \cup gH$ ,  $g_1g_2 \in H \cup gH$ , qui est donc un sous-groupe de  $G$ .

Puisque la translation à gauche par  $g$  est bijective,  $h \mapsto gh$  est une bijection de  $H$  sur  $gH$ , qui a donc même cardinal que  $H$ .

Par ailleurs,  $H$  et  $gH$  sont disjoints. En effet, supposons par l'absurde qu'il existe  $x \in H \cap gH$ . Alors  $x \in H$  et il existe  $h \in H$  tel que  $x = gh$ . Et alors  $g = xh^{-1} \in H$ , ce qui est absurde puisque l'on a supposé  $g \notin H$ .

Donc  $H \cup gH$  est de cardinal  $\text{Card}(H) + \text{Card}(gH) = 2\text{Card}(H)$ .

- 4.b. Supposons par l'absurde que  $\text{Card}(G)$  ne soit pas une puissance de 2.  
Soit alors  $H_1$  un sous-groupe de  $G$  de cardinal 2. Alors  $H_1 \neq G$ , et donc il existe  $g_1 \in G \setminus H_1$ .  
Donc  $H_2 = H_1 \cup g_1H_1$  est un sous-groupe de  $G$  de cardinal 4.  
Mais alors  $H_2 \neq G$  puisque  $G$  n'est pas de cardinal 4. Donc il existe  $g_2 \in G \setminus H_2$ . Et alors  $H_3 = H_2 \cup g_2H_2$  est un sous-groupe de  $G$  de cardinal 8.  
Mais  $H_3$  n'est pas égal à  $G$ , etc.  
On construit donc par récurrence une suite de sous-groupes  $(H_k)_{k \geq 1}$  tels que  $H_k$  soit de cardinal  $2^k$ .  
Mais si  $k$  est suffisamment grand,  $2^k > \text{Card}(G)$ , ce qui est absurde.  
Donc  $\text{Card}(G)$  est nécessairement une puissance de 2.

### SOLUTION DE L'EXERCICE 15.9

1. Notons  $f_g : x \mapsto gx$ , et  $f_{g^{-1}} : x \mapsto g^{-1}x$ . Alors, pour tout  $x \in G$ ,

$$(f_g \circ f_{g^{-1}})(x) = g(g^{-1}x) = x \text{ et de même } (f_{g^{-1}} \circ f_g)(x) = g^{-1}(gx) = x.$$

Donc non seulement  $f_g$  est bijective, mais en plus, nous savons que son inverse est  $f_{g^{-1}}$ .

#### Rappel

Un morphisme envoie toujours l'élément neutre sur l'élément neutre.

2. D'une part,  $f_g$  étant bijective, on a, avec le changement de variable  $y = gx$ ,

$$\prod_{x \in G} (gx) = \prod_{y \in G} y.$$

D'autre part,  $G$  étant commutatif, on a

$$\prod_{g \in G} (gx) = g^n \prod_{x \in G} x.$$

Détaillons un poil ce calcul pour bien voir où l'hypothèse de commutativité est indispensable : notons  $G = \{g_1, g_2, \dots, g_n\}$ . Alors

$$\begin{aligned} \prod_{x \in G} (gx) &= \prod_{i=1}^n (gx_i) \\ &= (gx_1)(gx_2) \cdots (gx_n) = gx_1gx_2 \cdots gx_n \\ &= ggx_1x_2gx_3 \cdots gx_n \\ &= \cdots = \underbrace{g \cdots g}_{n \text{ fois}} (x_1x_2 \cdots x_n) \\ &= g^n \prod_{x \in G} x. \end{aligned}$$

En notant  $A = \prod_{x \in G} x$ , on a donc  $g^n A = A$ , et donc en multipliant à droite par  $A^{-1}$ ,  $g^n = 1_G$ .

3. D'après la question précédente, un sous-groupe de cardinal  $n$  de  $(\mathbb{C}^*, \times)$ , qui sera forcément commutatif car  $(\mathbb{C}^*, \times)$  l'est, est formé d'éléments  $z$  tels que  $z^n = 1$ . Par conséquent, il est formé de racines  $n^{\text{èmes}}$  de l'unité. Autrement dit, si  $G$  est un sous-groupe de  $(\mathbb{C}^*, \times)$  de cardinal  $n$ , alors  $G \subset \mathbf{U}_n$ . Mais  $\mathbf{U}_n$  est lui-même de cardinal  $n$ , et donc  $G = \mathbf{U}_n$ . Donc pour tout  $n \in \mathbb{N}^*$ ,  $(\mathbb{C}^*, \times)$  possède un unique sous-groupe de cardinal  $n$ , qui est  $\mathbf{U}_n$ .

### SOLUTION DE L'EXERCICE 15.11

1. C'est du cours, mais reprouvons-le tout de même :
- ▶  $e_G \in H$  car  $H$  est un sous-groupe, et de même,  $e_G \in K$ . Donc  $e_G \in H \cap K$ .
  - ▶ soient  $g_1, g_2 \in H \cap K$ . Alors  $g_1g_2 \in H$  car  $H$  est un sous-groupe, et de même,  $g_1g_2 \in K$ , donc  $g_1g_2 \in H \cap K$  :  $H \cap K$  est stable par produit.
  - ▶ enfin, si  $g \in H \cap K$ , alors  $g^{-1} \in H$ , puisque  $H$  est un sous-groupe, et de même  $g^{-1} \in K$ , donc  $g^{-1} \in H \cap K$ .

Et donc  $H \cap K$  est un sous-groupe de  $G$ .

2. Si l'un des deux sous-groupes est inclus dans l'autre, alors il est évident que  $H \cup K$  est un sous-groupe<sup>2</sup>. Inversement supposons que  $H \cup K$  soit un sous-groupe de  $G$ , et supposons que  $H \not\subset K$  et  $K \not\subset H$ . Alors il existe  $h \in H \setminus K$  et il existe  $k \in K \setminus H$ . Alors  $hk \in H \cup K$ .  
 ▶ Si  $hk \in H$  : alors  $h^{-1} \in H$  et donc  $k = h^{-1}(hk) \in H$ , ce qui est absurde.  
 ▶ Si  $hk \in K$  : alors  $k^{-1} \in K$  et donc  $h = (hk)k^{-1} \in K$ , ce qui est absurde.  
 Dans tous les cas, on aboutit à une contradiction, et donc  $H \cup K$  sous-groupe de  $G$  implique  $H \subset K$  ou  $K \subset H$ .

3. Déjà,  $e_G = \underbrace{e_G}_{\in H} \underbrace{e_G}_{\in K} \in HK$ .

Soient  $x, y \in HK$ . Alors il existe  $(h, h') \in H^2$  et  $(k, k') \in K^2$  tels que  $x = hk$  et  $y = h'k'$ .

Et alors  $xy = (hk)(h'k') = kh'h'k' = hh'kk' = \underbrace{hh'}_{\in H} \underbrace{kk'}_{\in K} \in HK$ .

Et avec les mêmes notations,  $x^{-1} = (hk)^{-1} = k^{-1}h^{-1} = \underbrace{h^{-1}}_{\in H} \underbrace{k^{-1}}_{\in K} \in HK$ .

Donc  $HK$  est un sous-groupe de  $G$ .

### Explication

La bijectivité nous dit que les  $gx$ , quant  $x$  parcourt  $G$ , prennent une et une seule fois chaque valeur dans  $G$ . Et donc le produit des  $gx$  est le même que le produit des  $x, x \in G$ .

Remarquons au passage que cette notation produit n'a de sens que parce que le groupe est commutatif, sans cela, on ne saurait pas dans quel ordre a lieu le produit.

L'associativité nous permet de nous passer des parenthèses.

La commutativité sert ici : on peut permuter l'ordre de deux facteurs.

<sup>2</sup> Puisqu'il est égal soit à  $H$  soit à  $K$ .

### Rédaction

Attention aux quantificateurs : il existe un élément dans  $H$  pas dans  $K$ , mais ce n'est pas le cas de tous les éléments de  $H$  (ne serait-ce que parce que  $e_G$  est dans  $H$  et dans  $K$ ).



4. Supposons que  $KH = HK$ . Prouvons qu'alors  $HK$  est un sous-groupe de  $G$ .

Il contient évidemment  $e_G = e_G \cdot e_G$ .

Soient  $x, y \in HK$ . Alors il existe  $h_1, h_2 \in H$  et  $k_1, k_2 \in K$  tels que  $x = h_1k_1$  et  $y = h_2k_2$ .

Et alors  $xy^{-1} = (h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1}$ .

Mais  $(k_1k_2^{-1})h_2^{-1} \in KH = HK$ . Donc il existe  $h \in H$  et  $k \in K$  tels que  $(k_1k_2^{-1})h_2^{-1} = hk$ .

Et alors  $xy^{-1} = h_1hk = (h_1h)k \in HK$ . Donc  $HK$  est un sous-groupe de  $G$ .

Inversement, supposons que  $HK$  soit un sous-groupe de  $G$ .

Alors  $K \subset HK$  (puisque  $h \in H$  s'écrit  $h \cdot e_G$ ) et  $H \subset HK$ , par stabilité de  $HK$  par produit,

$KH \subset HK$ . Inversement, soit  $x \in HK$ . Alors  $x^{-1} \in HK$ . Et donc il existe  $h \in H$  et  $k \in K$  tels

que  $x^{-1} = hk$ , de sorte que  $x = k^{-1}h^{-1} \in KH$ . Donc  $KH = HK$ .

### SOLUTION DE L'EXERCICE 15.12

1. Puisque les similitudes directes sont des bijections de  $\mathbb{C}$  dans  $\mathbb{C}$ , nous allons prouver que  $G$  est un sous-groupe du groupe  $\mathfrak{S}(\mathbb{C})$  des bijections de  $\mathbb{C}$  dans  $\mathbb{C}$ .

$G$  contient évidemment  $\text{id}_{\mathbb{C}} : z \mapsto z$ .

Il est évident que la composée de deux similitudes directes est encore une similitude directe, donc  $G$  est stable par produit. Et si  $f : z \mapsto az + b$  est une similitude directe, alors

$f^{-1} : z \mapsto \frac{z-b}{a}$  est également une similitude directe.

Donc  $G$  est stable par passage à l'inverse, et donc est un sous-groupe de  $(\mathfrak{S}(\mathbb{C}), \circ)$ .

Il ne s'agit pas d'un groupe abélien, par exemple car  $f : z \mapsto -z$  et  $g : z \mapsto z + 1$  ne commutent pas :

$$f \circ g : z \mapsto -z - 1 \text{ et } g \circ f : z \mapsto -z - 1.$$

2. Donc  $G_{z_0}$  est l'ensemble des similitudes qui ont  $z_0$  pour point fixe.

C'est bien le cas de l'identité, si  $f$  et  $g$  ont  $z_0$  pour point fixe, alors  $g(z_0) = z_0 \Leftrightarrow g^{-1}(z_0) = z_0$ , si bien que  $(f \circ g^{-1})(z_0) = f(z_0) = z_0$  et donc  $f \circ g^{-1} \in G_{z_0}$ .

Ainsi,  $G_{z_0}$  est un sous-groupe de  $G$ .

Soit alors  $\varphi : \begin{cases} \mathbb{C}^* & \longrightarrow G_{z_0} \\ \alpha & \longmapsto z \mapsto \alpha(z - z_0) + z_0 \end{cases}$ .

Nous savons que toute similitude directe qui possède  $z_0$  comme point fixe est de la forme  $z \mapsto re^{i\theta}(z - z_0) + z_0$  où  $r$  est le rapport et  $\theta$  l'angle de la similitude.

Donc  $\varphi$  est surjective, et même bijective puisque l'écriture d'une similitude sous la forme  $z \mapsto az + b$  est unique.

Reste donc à voir qu'ils s'agit d'un morphisme de groupes.

Soient  $\alpha_1, \alpha_2 \in \mathbb{C}^*$ . Notons  $f_1 = \varphi(\alpha_1) : z \mapsto \alpha_1(z - z_0) + z_0$  et  $f_2 = \varphi(\alpha_2) : z \mapsto \alpha_2(z - z_0) + z_0$ .

Alors  $f_1 \circ f_2$  est une fonction affine, qui possède  $z_0$  comme point fixe (car il est point fixe de  $f_1$  et de  $f_2$ ), et qui possède  $\alpha_1\alpha_2$  comme coefficient dominant.

Donc pour tout  $z \in \mathbb{C}$ ,  $(f_1 \circ f_2)(z) = \alpha_1\alpha_2(z - z_0) + z_0$ , c'est donc  $\varphi(\alpha_1\alpha_2)$ .

Et donc  $f$  est un morphisme de groupes, c'est donc un isomorphisme de groupes.

### SOLUTION DE L'EXERCICE 15.14

1. Si  $G$  est abélien, alors les puissances de  $x$  et de  $y$  commutent.

Donc en particulier, si  $n, p$  sont deux entiers strictement positifs tels que  $x^n = y^p = e_G$ , alors  $(xy)^{np} = x^{np}y^{np} = (x^n)^p (y^p)^n = e_G$ .

Et donc  $xy$  est d'ordre fini.

2. Le résultat n'est plus vrai si  $G$  n'est pas abélien. Par exemple, dans le groupe des similitudes directes du plan<sup>3</sup>, une rotation d'angle  $\pi$  est d'ordre fini, puisqu'élevée au carré, elle est égale à l'identité.

En revanche, la composée de deux rotations d'angle  $\pi$ , de centre distincts est une translation de vecteur non nul.

En effet, si  $\alpha \neq \beta$  sont deux complexes, si  $f : z \mapsto -z + \alpha$  et  $g : z \mapsto -z + \beta$  sont deux rotations d'angle  $\pi$ , alors  $g \circ f : z \mapsto z + (\beta - \alpha)$ .

Or, une translation  $\tau$  de vecteur non nul  $\vec{u}$  n'est jamais d'ordre fini puisque pour tout  $n \in \mathbb{N}^*$ ,  $\tau^n$  est<sup>4</sup> la translation de vecteur  $n\vec{u} \neq \vec{0}$ .

### SOLUTION DE L'EXERCICE 15.15

1. Soient  $(g, h) \in G^2$ . Alors

$$\tau_a(g)\tau_a(h) = aga^{-1}aha^{-1} = agha^{-1} = \tau_a(h).$$

#### Rappel

Il a été prouvé en cours que l'ensemble des permutations d'un ensemble est un groupe pour la composition.

#### Alternative

Si vous n'êtes pas convaincu, faire le calcul !

<sup>3</sup> Voir l'exercice précédent.

<sup>4</sup> Passer par les complexes si vous avez besoin de vous en convaincre.



Donc  $\tau_a$  est un morphisme de  $G$  dans lui-même.

Pour montrer la bijectivité, il y a deux options :

- ▶ soit prouver injectivité et surjectivité
- ▶ soit exhiber la bijection réciproque si on la voit.

Ici, la seconde option est de loin la plus facile, puisque pour tout  $g \in G$ ,

$$(\tau_{a^{-1}} \circ \tau_a)(g) = a^{-1}\tau_a(g)a = a^{-1}aga^{-1}a = g = \text{id}_G(g).$$

Et de même,  $\tau_a \circ \tau_{a^{-1}} = \text{id}$ , donc  $\tau_{a^{-1}}$  est la bijection réciproque de  $\tau_a$ .

Prouvons tout de même injectivité et surjectivité.

Pour l'injectivité, soit  $g \in \text{Ker } \tau_a$ .

Alors  $aga^{-1} = e \Leftrightarrow ag = ea \Leftrightarrow g = e$ .

Donc  $\tau_a$  est injectif.

Soit à présent  $y \in G$ . Alors  $y = a(a^{-1}ya)a^{-1} = \tau_a(a^{-1}ya)$ , et donc  $\tau_a$  est surjectif.

On en déduit donc que  $\tau_a$  est bijectif.

2. Nous venons de prouver que les  $\tau_a$  sont des éléments de  $\mathfrak{S}(G)$ , car bijectifs.

On a  $\tau_e = \text{id}_G \in \mathcal{C}(G)$ .

Et pour  $(a, b) \in G^2$  et  $g \in G$ , on a

$$(\tau_a \circ \tau_b^{-1})(g) = (\tau_a \circ \tau_{b^{-1}})(g) = \tau_a(b^{-1}gb) = ab^{-1}g(ab^{-1})^{-1}(g).$$

Et donc  $\tau_a \circ \tau_b^{-1} = \tau_{ab^{-1}} \in \mathcal{C}(G)$ .

Ainsi,  $\mathcal{C}(G)$  est bien un sous-groupe de  $(\mathfrak{S}(G), \circ)$ .

3. Le calcul réalisé à l'instant prouve que pour  $(a, b) \in G^2$ ,  $\tau_a \circ \tau_b = \tau_{ab}$ , soit encore que  $\varphi(ab) = \varphi(a) \circ \varphi(b)$ , et donc  $\varphi$  est un morphisme de groupes.

### SOLUTION DE L'EXERCICE 15.16

1. Soit  $H_1$  un sous-groupe de  $G_1$ , et soient  $y_1, y_2 \in f(H_1)$ . Alors il existe deux éléments  $x_1, x_2 \in H_1$  tels que  $y_1 = f(x_1)$  et  $y_2 = f(x_2)$ .  
Et alors  $y_1 y_2^{-1} = f(x_1) f(x_2)^{-1} = f(x_1 x_2^{-1})$ . Puisque  $H_1$  est un sous-groupe de  $G_1$ ,  $x_1 x_2^{-1} \in H_1$  et donc  $y_1 y_2^{-1} \in f(H_1)$ , de sorte que  $f(H_1)$  est un sous-groupe de  $G_2$ .
2. Soit  $H_2$  un sous-groupe de  $G_2$ , et soient  $x_1, x_2 \in f^{-1}(H_2)$ .  
Alors  $f(x_1) \in H_2$  et  $f(x_2) \in H_2$ .  
Donc  $f(x_1 x_2^{-1}) = f(x_1) f(x_2)^{-1} \in H_2$ , de sorte que  $x_1 x_2^{-1} \in f^{-1}(H_2)$ .  
Donc  $f^{-1}(H_2)$  est un sous-groupe de  $G_2$ .

En particulier,  $\text{Ker } f = f^{-1}(\{e_{G_2}\})$ , et  $\{e_{G_2}\}$  est un sous-groupe de  $G_2$ , donc  $\text{Ker } f$  est un sous-groupe de  $G_1$ .

### SOLUTION DE L'EXERCICE 15.17

Soit  $\varphi : \mathbf{Z} \rightarrow \mathbf{Z}$  un morphisme de groupes. Alors  $\varphi(0) = 0$ .

Notons  $k = \varphi(1)$ . Alors  $\varphi(2) = \varphi(1+1) = \varphi(1) + \varphi(1) = k + k = 2k$ .

Puis  $\varphi(3) = \varphi(2+1) = \varphi(2) + \varphi(1) = 2k + k = 3k$ .

Une récurrence facile prouve alors que pour tout  $n \in \mathbf{N}$ ,  $\varphi(n) = nk$ .

Et pour  $n \in \mathbf{Z}$  négatif,  $\varphi(n) = -\varphi(-n)$ , où  $-n \in \mathbf{N}$  et donc  $\varphi(n) = -(-nk) = nk$ .

Inversement, il est facile de constater que pour  $k \in \mathbf{Z}$  fixé,  $\varphi : n \mapsto nk$  est bien un morphisme de  $(\mathbf{Z}, +)$  dans lui-même car

$$\forall (p, q) \in \mathbf{Z}^2, \varphi(p+q) = (p+q)k = pk + qk = \varphi(p) + \varphi(q).$$

Donc les morphismes de  $(\mathbf{Z}, +)$  dans lui-même sont les  $n \mapsto kn$ ,  $k \in \mathbf{Z}$ .

Soit à présent  $\varphi : \mathbf{Q} \rightarrow \mathbf{Z}$  un morphisme. Soit alors  $r \in \mathbf{Q}$  non nul, et soit  $n \in \mathbf{N}$ .

$$\text{Alors } \varphi(r) = \varphi\left(\frac{r}{n} + \frac{r}{n} + \dots + \frac{r}{n}\right) = \varphi\left(\frac{r}{n}\right) + \dots + \varphi\left(\frac{r}{n}\right) = n\varphi\left(\frac{r}{n}\right).$$

Or,  $\varphi(r)$ ,  $\varphi\left(\frac{r}{n}\right)$  et  $n$  sont tous des entiers, donc  $n$  divise  $\varphi(r)$ , et ce quel que soit  $n \in \mathbf{N}$ .

Le seul entier étant divisible par tous les autres est 0, et donc  $\varphi(r) = 0$  pour tout  $r \in \mathbf{Q}$  :  $\varphi$  est le morphisme nul.

#### Méthode

Pour prouver l'injectivité d'un morphisme, il suffit de prouver que son noyau est réduit à l'élément neutre. Et puisqu'on a toujours  $\{e_G\} \subset \text{Ker } \varphi$ , il suffit de prouver l'inclusion réciproque, c'est à dire

$$x \in \text{Ker } \varphi \Rightarrow x = e_G.$$

#### Remarque

Notons que nous venons de trouver l'unique antécédent de  $y$ , et donc la bijection réciproque de  $\tau_a$ .

**SOLUTION DE L'EXERCICE 15.18**

Soit  $a \in A$ . Puisque  $A$  est stable par  $*$ , pour tout  $n \in \mathbf{N}^*$ ,  $a^n \in A$ .

Mais  $A$  étant fini, ces puissances ne sauraient être toutes distinctes : il existe deux entiers distincts  $n$  et  $p$  tels que  $a^n = a^p$ .

Quitte à échanger  $n$  et  $p$ , supposons que  $p > n$ . Alors  $a^n = a^p \Leftrightarrow a^{p-n} = e_G$ .

Donc déjà,  $e_G \in A$  car  $p - n \in \mathbf{N}^*$ .

De plus,  $a * a^{p-n-1} = e_G$ , de sorte que  $a^{p-n-1} = a^{-1}$ .

Or,  $p - n - 1 \geq 0$ , donc  $a^{-1} \in A$ .

Ainsi, nous avons prouvé que  $A$  contient l'élément neutre, et est stable par passage à l'inverse : si  $a \in A$ , alors  $a^{-1} \in A$ .

Puisque  $A$  est de plus stable par  $*$ , il s'agit d'un sous-groupe de  $G$ .

⚠ Attention !

On ne sait pas encore si  $a^0 = e_G$  est dans  $A$ .