

Chapitre 1 : Groupes

I Généralités

A) Définition

Un groupe est un couple $(G, *)$ constitué d'un ensemble G et d'une loi de composition interne $*$ sur G de sorte que :

- (1) $*$ est associative
- (2) Il y a dans G un élément neutre pour $*$.
- (3) Tout élément de G admet un symétrique pour la loi $*$.

C'est-à-dire :

- (1) $\forall x, y, z \in G, (x * y) * z = x * (y * z)$
- (2) $\forall x \in G, x * e = e * x = x$
- (3) $\forall x \in G, \exists y \in G, x * y = y * x = e$

Remarque :

Si $(G, *)$ est un groupe, il y a unicité du neutre (déjà vu en cas plus général).

Si de plus $*$ est commutative, on dit que $(G, *)$ est un groupe commutatif.

B) Exemples

- $(\mathbb{N}, +)$ n'est pas un groupe.
- $(\mathbb{Z}, +)$ est un groupe.
- (\mathbb{Z}, \times) n'est pas un groupe.
- (\mathbb{Q}, \times) n'est pas un groupe, mais (\mathbb{Q}^*, \times) en est un.
- Créons un groupe à trois éléments $G = \{a, b, c\}$

Loi \heartsuit définie par la table de Pythagore donnant $x \heartsuit y$:

$x \backslash y$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

On pose a comme élément neutre, et on choisit $b \heartsuit c = c \heartsuit b = a$

C) Règles de calcul

1) En notation « bizarre »

Soit G un ensemble muni d'une loi $*$ formant un groupe.

- Il y a dans G un et un seul élément neutre :
L'existence est déjà donnée par la définition d'un groupe.
Supposons que e, e' sont deux neutres.

Alors $e = e * e' = e'$ (première égalité : e' est neutre ; deuxième : e est neutre)

On peut donc parler *du* neutre du groupe $(G, *)$.

- Tout élément x de G admet un et un seul symétrique par $*$:
L'existence est toujours donnée par la définition d'un groupe.
Supposons que x', x'' sont deux symétriques de x .

$$\text{Alors } x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x''$$

On note dans ce sous paragraphe \bar{x} le symétrique de x .

- Pour tout $x \in G, \bar{\bar{x}} = x$:

$$\bar{x} * x = x * \bar{x} = e$$

Donc x est symétrique de \bar{x} .

- Pour tous $x, y \in G, \overline{x * y} = \bar{y} * \bar{x}$:

$$(x * y) * (\bar{y} * \bar{x}) = x * [y * (\bar{y} * \bar{x})] = x * [(y * \bar{y}) * \bar{x}] = x * [e * \bar{x}] = x * \bar{x} = e$$

$$\text{Et } (\bar{y} * \bar{x}) * (x * y) = [(\bar{y} * \bar{x}) * x] * y = [\bar{y} * (\bar{x} * x)] * y = [\bar{y} * e] * y = \bar{y} * y = e$$

Donc $\overline{x * y} = \bar{y} * \bar{x}$

- Remarque :

On a, pour tout $x, y, z \in G, (x * y) * z = x * (y * z)$.

On peut donc le noter sans ambiguïté $x * y * z$

- « Résolution d'équations » :

Pour tous $x, y, z \in G$:

$$(1) \quad x * y = z \Leftrightarrow x = z * \bar{y}$$

$$(2) \quad y * x = z \Leftrightarrow x = \bar{y} * z$$

Démonstration du (1) :

Si $x * y = z$, alors $(x * y) * \bar{y} = z * \bar{y}$.

Or, $(x * y) * \bar{y} = x * (y * \bar{y}) = x * e = x$. Donc $x = z * \bar{y}$

Si $x = z * \bar{y}$, alors $x * y = (z * \bar{y}) * y = z * (\bar{y} * y) = z * e = z$

La démonstration est la même pour (2)...

- Régularité

Pour tous $x, y, z \in G$, on a :

$$(1) \quad x * z = y * z \Rightarrow x = y$$

$$(2) \quad z * x = z * y \Rightarrow x = y$$

(Les autres implications sont vraies aussi mais évidentes)

Démonstration de (1) :

Si $x * z = y * z$, alors $(x * z) * \bar{z} = (y * z) * \bar{z}$

Soit $x * (z * \bar{z}) = y * (z * \bar{z})$, donc $x * e = y * e$ c'est-à-dire $x = y$

La démonstration est encore la même pour (2).

Conséquence : dans une table de Pythagore d'un groupe fini $(G, *)$, on ne voit jamais deux fois le même élément dans une même rangée (ligne ou colonne) :

Si $x_1 * y_1 = z$ et $x_1 * y_2 = z / x_2 * y_1 = z$, alors $x_1 * y_1 = x_1 * y_2 / x_1 * y_1 = x_2 * y_1$, soit $y_1 = y_2 / x_1 = x_2$.

- Itéré d'un élément :

Soit $x \in G$. On note (dans ce sous paragraphe seulement) :

$$x * x = x^2, (x * x) * x = x * x * x = x^3$$

Plus rigoureusement :

On définit, pour tout $n \in \mathbb{N}$, x^n par récurrence en posant :

$$- x^0 = e$$

$$- \forall n \in \mathbb{N}, x^{n+1} = (x^n) * x$$

Alors il est facile (mais pénible à écrire) d'établir que, pour tout $n, p \in \mathbb{N}$,
 $x(n+p) = (x(n)) * (x(p))$ et $(x(n))p = x(n \times p)$

- Itéré « un nombre négatif de fois » :

Soit $x \in G$, $n \in \mathbb{N}$.

On pose $x(-n) = \overline{x(n)}$

Alors $x(-n) = \overline{x(n)}$

Les règles précédentes se généralisent à \mathbb{Z} .

2) En notation « multiplicative » (réécriture)

Dans le groupe (G, \times) avec les notations suivantes :

- Le neutre 1_G appelé aussi élément unité
- Le symétrique de $x \in G$ est noté x^{-1} , appelé aussi inverse de x .
- L'itéré n fois est noté x^n .
- Le symbole \times est souvent omis : $x \times y$ est noté aussi xy .

Les règles précédentes donnent :

- $(x^{-1})^{-1} = x$
- $(xy)^{-1} = y^{-1}x^{-1}$
- $xy = z \Leftrightarrow x = zy^{-1}$
 $yx = z \Leftrightarrow x = y^{-1}z$
- $xz = yz \Rightarrow x = y$
 $zx = zy \Rightarrow x = y$
- $x^0 = 1_G$
 $x^1 = x$

$$\forall n \in \mathbb{N}, x^{(n+1)} = x^n x$$

$$\forall n \in \mathbb{N}, x^{-n} = (x^{-1})^n = (x^n)^{-1}$$

$$\forall n, p \in \mathbb{Z}, x^n x^p = x^{(n+p)}$$

$$(x^n)^p = x^{n \times p}$$

3) En notation « additive » (réservée aux groupes commutatifs)

Dans le groupe $(G, +)$, avec les notations suivantes :

- Le neutre 0_G est appelé l'élément nul de G
- Le symétrique de $x \in G$ est noté $-x$, appelé aussi opposé de x .
- L'itéré n fois est noté $n.x$ ou nx .
- On suppose de plus que le groupe $(G, +)$ est commutatif, c'est-à-dire :

$$\forall x, y \in G, x + y = y + x$$

Les règles donnent alors :

- $-(-x) = x$

- $-(x+y) = (-y) + (-x) = (-x) + (-y)$
- $(y+x) \Rightarrow x+y = z \Leftrightarrow x = z + (-y)$; $z + (-y)$ est noté aussi $z - y$
- $x+z = y+z \Rightarrow x = y$
- $0.x = 0_G$
- $1.x = x$
- $\forall n \in \mathbb{N}, (n+1).x = n.x + x$
- $\forall n \in \mathbb{N}, (-n).x = n.(-x) = -(n.x)$, noté aussi $-n.x$
- $\forall n, p \in \mathbb{Z}, n.x + p.x = (n+p).x$
- $p.(n.x) = (p \times n)x$

D) Autres exemples de groupe

- Rappels :

Groupes de nombres :

$(\mathbb{C}, +), (\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{Z}, +), (\mathbb{C}^*, \times), (\mathbb{R}^*, \times), (\mathbb{Q}^*, \times)$

- Groupes de permutation :

Soit E un ensemble non vide quelconque. On note $\mathfrak{S}(E)$ l'ensemble des permutations sur E (ensemble des bijections de E dans E). Alors \circ constitue une loi de composition interne sur $\mathfrak{S}(E)$, et $(\mathfrak{S}(E), \circ)$ est un groupe, appelé groupe des permutations de E . Ce groupe est non commutatif dès que E a au moins trois éléments.

Démonstration :

- On peut composer deux bijections de E dans E , et on obtient une bijection de E dans E .

- La loi \circ est associative :

$$\forall f, g, h \in \mathfrak{S}(E), f \circ (g \circ h) = (f \circ g) \circ h$$

(Démontré dans un cas plus général et pas seulement pour les bijections)

- Neutre : $\text{Id}_E \in \mathfrak{S}(E)$

- Tout $f \in \mathfrak{S}(E)$ a un symétrique pour \circ , à savoir f^{-1} .

Donc $(\mathfrak{S}(E), \circ)$ est un groupe.

Montrons que, pour un ensemble E de plus de trois éléments, $(\mathfrak{S}(E), \circ)$ n'est pas commutatif :

Soient a, b, c trois éléments de E distincts.

Soient $f, g : E \rightarrow E$ définies ainsi :

$$\left\{ \begin{array}{l} f(a) = b \\ f(b) = a \\ \forall x \in E \setminus \{a, b\}, f(x) = x \end{array} \right. \quad \left\{ \begin{array}{l} g(b) = c \\ g(c) = b \\ \forall x \in E \setminus \{b, c\}, g(x) = x \end{array} \right.$$

Alors f et g sont dans $\mathfrak{S}(E)$, puisque ce sont des applications de E dans E et inversibles d'inverse elles-mêmes (elles sont involutives).

Et on a alors $f \circ g \neq g \circ f$:

$$(f \circ g)(a) = f(g(a)) = f(a) = b$$

$$(g \circ f)(a) = g(f(a)) = g(b) = c$$

Exemples :

- On note \mathfrak{S}_n le groupe $(\mathfrak{S}(E), \circ)$ lorsque $E = \{1, 2, 3, \dots, n\}$. Ainsi, \mathfrak{S}_n est un groupe fini de cardinal $n!$.

• Table de Pythagore de \mathfrak{S}_2 :

$\mathfrak{S}_2 = \{\text{Id}, \tau\}$, où :

$\text{Id} : \{1, 2\} \rightarrow \{1, 2\}$
 $x \mapsto x$

$\tau : \{1, 2\} \rightarrow \{1, 2\}$ définie par $\tau(1) = 2$; $\tau(2) = 1$

Tableau donnant $x \circ y$:

$x \backslash y$	Id	τ
Id	Id	τ
τ	τ	Id

• Table de Pythagore de \mathfrak{S}_3 :

$\mathfrak{S}_3 = \{\text{Id}_E, \tau_{1,2}, \tau_{2,3}, \tau_{3,1}, s, s'\}$, où :

$\text{Id} : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$
 $x \mapsto x$

$\tau_{a,b} : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ défini par $\tau_{a,b}(a) = b$; $\tau_{a,b}(b) = a$; $\tau_{a,b}(x) = x$ sinon.

$s : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ définie par $s(1) = 2$; $s(2) = 3$; $s(3) = 1$

$s' : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ définie par $s'(1) = 3$; $s'(2) = 1$; $s'(3) = 2$.

Tableau donnant $x \circ y$:

$x \backslash y$	Id	$\tau_{1,2}$	$\tau_{1,3}$	$\tau_{2,3}$	s	s'
Id	Id	$\tau_{1,2}$	$\tau_{1,3}$	$\tau_{2,3}$	s	s'
$\tau_{1,2}$	$\tau_{1,2}$	Id	s'	s	$\tau_{2,3}$	$\tau_{1,3}$
$\tau_{1,3}$	$\tau_{1,3}$	s	Id	s'	$\tau_{1,2}$	$\tau_{2,3}$
$\tau_{2,3}$	$\tau_{2,3}$	s'	s	Id	$\tau_{1,3}$	$\tau_{1,2}$
s	s	$\tau_{1,3}$	$\tau_{2,3}$	$\tau_{1,2}$	s'	Id
s'	s'	$\tau_{2,3}$	$\tau_{1,2}$	$\tau_{1,3}$	Id	s

- $(\mathfrak{F}(A, G), \otimes)$, où :

A est quelconque, et (G, \times) est un groupe, avec :

\otimes défini par :

$\forall f, g \in \mathfrak{F}(A, G), f \otimes g : A \rightarrow G$
 $x \mapsto f(x) * g(x)$

E) Classes d'équivalence modulo n .

Soit $n \in \mathbb{N}, n \geq 2$.

On définit sur \mathbb{Z} la relation \equiv_n par :

Pour tous $x, y \in \mathbb{Z}, x \equiv_n y \Leftrightarrow y - x \in n\mathbb{Z}$

Cette relation s'appelle la relation de congruence modulo n .

On note plutôt $x \equiv y \pmod{n}$ ou encore $x \equiv y [n]$

Cette relation est une relation d'équivalence :

(1) $\forall x \in \mathbb{Z}, x \equiv_n x$ puisque $x - x = 0 \in n\mathbb{Z}$,

(2) Pour tous $x, y \in \mathbb{Z}$, si $x \equiv_n y$ alors $y - x \in n\mathbb{Z}$, donc $x - y \in n\mathbb{Z}$, soit $y \equiv_n x$

(3) Soient $x, y, z \in \mathbb{Z}$. Si $x \equiv_n y$ et $y \equiv_n z$, alors $y - x$ s'écrit $y - x = nk$ où $k \in \mathbb{Z}$, et $z - y$ s'écrit $z - y = nk'$ où $k' \in \mathbb{Z}$. Donc $z - x = (z - y) + (y - x) = n(k' + k) \in n\mathbb{Z}$.
Donc $x \equiv_n z$.

Donc \equiv_n est réflexive (1), symétrique (2) et transitive (3), c'est donc une relation d'équivalence.

Cette relation est compatible avec + :

Pour tout $x, x', y, y' \in \mathbb{Z}$:

Si $x \equiv_n x', y \equiv_n y'$, alors :

$x - x' \in n\mathbb{Z}$, $y - y' \in n\mathbb{Z}$, donc $x - x' + y - y' \in n\mathbb{Z}$, soit $(x' + y') - (x + y) \in n\mathbb{Z}$, c'est-à-dire $x + y \equiv_n x' + y'$.

Pour tout $x \in \mathbb{Z}$, on appelle classe d'équivalence modulo n , et on note \dot{x} , l'ensemble des éléments de \mathbb{Z} congrus à x modulo n . (Attention, la notation \dot{x} indique pas qu'on travaille modulo n). On a alors l'équivalence :

$\forall x, y \in \mathbb{Z}, (\dot{x} = \dot{y} \Leftrightarrow x \equiv_n y [n])$.

En effet :

Soient $x, y \in \mathbb{Z}$

Si $\dot{x} = \dot{y}$. Déjà, $x \in \dot{x}$ (car \equiv_n est réflexive), c'est à dire $x \equiv_n y$, donc $x \equiv_n y [n]$.

Si $x \equiv_n y [n]$. Soit $z \in \dot{x}$. Alors $z \equiv_n x [n]$. Donc $z \equiv_n y [n]$ (car \equiv_n est transitive).

Donc $z \in \dot{y}$. Donc $\dot{x} \subset \dot{y}$. De même, $\dot{y} \subset \dot{x}$. Donc $\dot{x} = \dot{y}$.

D'où l'équivalence, pour tous $x, y \in \mathbb{Z}$.

On note $\mathbb{Z}/n\mathbb{Z}$, l'ensemble des classes d'équivalences modulo n .

Ainsi, $\mathbb{Z}/n\mathbb{Z} = \{\dot{a}, a \in \mathbb{Z}\}$.

Proposition, définition :

$\mathbb{Z}/n\mathbb{Z}$ est fini, et de cardinal n .

Pour tous $x, y \in \mathbb{Z}$, on pose $\dot{x} \oplus \dot{y} = \overline{x + y}$.

Alors \oplus définit une loi de composition interne sur $\mathbb{Z}/n\mathbb{Z}$, et $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ est un groupe commutatif.

Démonstration :

• Soit $x \in \mathbb{Z}$.

Alors il existe $a \in \llbracket 0, n-1 \rrbracket$ tel que $\dot{x} = \dot{a}$, c'est-à-dire tel que $x \equiv_n a [n]$.

En effet :

En prenant $a = x - nk$, où $k = \lfloor \frac{x}{n} \rfloor$, on a alors :

$k \leq \frac{x}{n} < k + 1$, donc $nk \leq x < nk + n$, soit $0 \leq x - nk < n$, c'est-à-dire $0 \leq a \leq n - 1$,

d'où l'existence.

Donc $\forall x \in \mathbb{Z}, \exists a \in \llbracket 0, n-1 \rrbracket, \dot{x} = \dot{a}$

Donc $\mathbb{Z}/n\mathbb{Z}$ contient au plus n éléments, à savoir les $\dot{a}, a \in \llbracket 0, n-1 \rrbracket$. On doit donc maintenant montrer que tous ces éléments sont distincts.

Soient $x, y \in \llbracket 0, n-1 \rrbracket$, supposons que $\dot{x} = \dot{y}$, c'est-à-dire que $x \equiv y [n]$.

Il existe donc $k \in \mathbb{Z}$, tel que $y - x = nk$.

Alors $y = x + nk$. On a :

$$0 \leq x \leq n-1. \text{ Donc } nk \leq y \leq nk + n - 1 < n(k+1)$$

$$\text{Donc } k \leq \frac{y}{n} < k+1$$

$$\text{Donc } k = \left\lfloor \frac{y}{n} \right\rfloor. \text{ Or, } 0 \leq y \leq n-1. \text{ Donc } 0 \leq \frac{y}{n} \leq 1 - \frac{1}{n} < 1$$

$$\text{Donc } k = \left\lfloor \frac{y}{n} \right\rfloor = 0. \text{ Donc } y = x + nk = x.$$

$$\text{Donc } \forall x, y \in \llbracket 0, n-1 \rrbracket, \dot{x} = \dot{y} \Rightarrow x = y$$

Soit, par contraposée : $\forall x, y \in \llbracket 0, n-1 \rrbracket, x \neq y \Rightarrow \dot{x} \neq \dot{y}$.

Donc $\mathbb{Z}/n\mathbb{Z}$ contient au moins n éléments, à savoir les $\dot{a}, a \in \llbracket 0, n-1 \rrbracket$

Donc $\mathbb{Z}/n\mathbb{Z}$ est fini, de cardinal n .

• Montrons déjà que la loi \oplus est bien définie, c'est-à-dire que pour tous

$x, y \in \mathbb{Z}$, $\overline{x+y}$ ne dépend que de $x+y$, et non pas de x et de y :

Si x' est tel que $\dot{x}' = \dot{x}$, et y' tel que $\dot{y}' = \dot{y}$, alors $x' \equiv_n x$ et $y' \equiv_n y$, soit $x'+y' \equiv_n x+y$

donc $\overline{x+y} = \overline{x'+y'}$.

Déjà, \oplus est évidemment une loi de composition interne sur $\mathbb{Z}/n\mathbb{Z}$

\oplus est associative : en effet, pour tous $x, y, z \in \mathbb{Z}$, on a :

$$(\dot{x} \oplus \dot{y}) \oplus \dot{z} = \overline{x+y} \oplus \dot{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \dot{x} \oplus \overline{y+z} = \dot{x} \oplus (\dot{y} \oplus \dot{z})$$

Pour tout $x \in \mathbb{Z}$, on a :

$$\dot{x} \oplus \dot{0} = \overline{x+0} = \dot{x} = \overline{0+x} = \dot{0} \oplus \dot{x}$$

Donc $\mathbb{Z}/n\mathbb{Z}$ admet un élément neutre pour \oplus , à savoir $\dot{0}$.

Soit $x \in \mathbb{Z}$, posons $y = -x$ (ainsi, $y \in \mathbb{Z}$). On a alors :

$$\dot{x} \oplus \dot{y} = \overline{x+y} = \overline{x+(-x)} = \dot{0} = \overline{(-x)+x} = \overline{y+x} = \dot{y} \oplus \dot{x}$$

Donc tout élément de $\mathbb{Z}/n\mathbb{Z}$ admet un symétrique pour \oplus .

Enfin, \oplus est commutative : pour tous $x, y \in \mathbb{Z}$, on a :

$$\dot{x} \oplus \dot{y} = \overline{x+y} = \overline{y+x} = \dot{y} \oplus \dot{x}$$

Donc $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ est bien un groupe commutatif. (on notera plutôt $+$ pour \oplus)

II Sous-groupes (notation multiplicative)

A) Définition

Soit (G, \times) un groupe.

Soit H une partie de G .

On dit que H constitue un sous-groupe de (G, \times) lorsque :

(1) $1_G \in H$

(2) H est stable par \times : $\forall x, y \in H, x \times y \in H$

(3) H est stable par passage à l'inverse : $\forall x \in H, x^{-1} \in H$

Proposition :

Si H est un sous-groupe de (G, \times) , alors \times constitue une loi de composition interne sur H , et (H, \times) est un groupe.

- Déjà, \times est bien une loi de composition interne sur H d'après (2)
- L'associativité n'est pas perdue par restriction.
- Neutre : c'est 1_G qui est dans H d'après (1)
- Existence d'un inverse pour tout x de H d'après (3).

B) Exemples

- \mathbb{R}^* est un sous-groupe de (\mathbb{C}^*, \times) , \mathbb{Q}^* de (\mathbb{R}^*, \times) (et aussi de (\mathbb{C}^*, \times)), $\{2^n, n \in \mathbb{Z}\}$, $\{-1, 1\}$, \mathbb{Q}_+^* sont des sous-groupes de (\mathbb{Q}^*, \times)
- \mathbb{U} est un sous-groupe de (\mathbb{C}^*, \times) ($\mathbb{U} = \{z \in \mathbb{C}, |z| = 1\}$)
- \mathbb{U}_n est un sous-groupe de (\mathbb{U}, \times) ($\mathbb{U}_n = \{z \in \mathbb{C}, z^n = 1\}$)
- Des sous-groupes de $(\mathbb{C}, +)$ sont : $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \{0\} \cup \{z \in \mathbb{C}^*, \text{Arg}(z) = \alpha\} [\pi]$
(Le dernier est une droite du plan complexe passant par O)
- Pour $n \in \mathbb{N}$, $n\mathbb{Z}$ est un sous-groupe de \mathbb{Z} .
- Si (G, \times) est un groupe, alors $\{1_G\}$ et G sont des sous-groupes de G (les autres sous-groupes sont appelés les sous-groupes propres de G)
- $\{\text{Id}, s, s'\}$ est un sous-groupe (commutatif) de $\mathfrak{S}_3 = \{\text{Id}_E, \tau_{1,2}, \tau_{2,3}, \tau_{3,1}, s, s'\}$ qui n'est pas commutatif.

Soit $n \in \mathbb{N}^*$, A une partie de $\{1, 2, \dots, n\}$ non vide.

Soit $H = \{\sigma \in \mathfrak{S}_n, \sigma(A) \subset A\}$, c'est-à-dire que H est l'ensemble des permutations qui laissent stable A (remarque : si $\sigma \in \mathfrak{S}_n$, comme σ est bijective, $\sigma(A)$ a le même cardinal que A , donc $\sigma(A) \subset A \Leftrightarrow \sigma(A) = A$)

Alors H est un sous-groupe de (\mathfrak{S}_n, \circ) :

- $\text{Id} \in H$
- H est stable par \circ : si $\sigma(A) \subset A$, $\sigma'(A) \subset A$, alors $\sigma \circ \sigma'(A) \subset A$
- H est stable par passage au symétrique : si $\sigma(A) \subset A$, alors $\sigma^{-1}(A) \subset A$

En effet :

Supposons que $\sigma(A) \subset A$. Alors $\sigma(A) = A$

Soit $x \in A$. Donc $x \in \sigma(A)$.

Il existe donc y dans A tel que $x = \sigma(y)$, avec $y \in A$

Donc $\sigma^{-1}(x) = y$, donc $\sigma^{-1}(x) \in A$

D'où l'inclusion $\sigma^{-1}(A) \subset A$ (et même l'égalité puisque σ^{-1} est bijective)

- Des sous-groupes de $(\mathfrak{F}(\mathbb{R}, \mathbb{R}), +)$:
 - L'ensemble des fonctions polynomiales
 - $\{\lambda f, \lambda \in \mathbb{R}\}$ où f est un élément fixé de $\mathfrak{F}(\mathbb{R}, \mathbb{R})$.
 - $\{f \in \mathfrak{F}(\mathbb{R}, \mathbb{R}), f(0) = 0\}$
 - $C^n(\mathbb{R}, \mathbb{R})$ où $n \in \mathbb{N}$, $D^n(\mathbb{R}, \mathbb{R})$ où $n \in \mathbb{N}$
 - Ensemble des fonctions T -périodiques (à T fixé)
 - Ensemble des fonctions k -lipschitzienne (à k fixé)

- Ensemble des fonctions uniformément continues
- Ensemble des fonctions paires, impaires...

- Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$:

Pour $n = 6$:

$$\{0\}, \{0,1,2,3,4,5\}, \underbrace{\{0,2,4\}}_{\text{sous-groupes propres}}, \{0,3\}$$

1 engendre $\mathbb{Z}/6\mathbb{Z}$, 5 aussi.

2 et 4 engendrent $\{0,2,4\}$.

3 engendre $\{0,3\}$.

On dit que 1 est un élément d'ordre 6, 2 et 4 d'ordre 3, 3 d'ordre 2.

C) Les sous-groupes de $(\mathbb{Z}, +)$.

Déjà, les $n\mathbb{Z}$, où $n \in \mathbb{N}$, sont des sous-groupes de \mathbb{Z} .

Y en a-t-il d'autres ?

Soit G un sous-groupe de \mathbb{Z} , autre que $\{0\}$.

Il contient donc un élément non nul de \mathbb{Z} , et son opposé (l'un d'eux étant alors dans \mathbb{N}^*). Donc l'ensemble $G \cap \mathbb{N}^*$ est non vide et est une partie de \mathbb{N} . Il admet donc un plus petit élément, disons $n \geq 1$. Alors $G = n\mathbb{Z}$.

En effet :

Déjà, une récurrence rapide montre que $\forall k \in \mathbb{N}, kn \in G$, puis comme G est stable par passage à l'inverse, $\forall k \in \mathbb{Z}, kn \in G$, donc $n\mathbb{Z} \subset G$.

L'autre inclusion maintenant :

Soit $x \in G$. La division euclidienne de x par n donne :

$$x = nq + r, \text{ où } q \in \mathbb{Z} \text{ et } r \in \llbracket 0, n-1 \rrbracket.$$

$$\text{Donc } r = x - nq = \underbrace{x}_{\in G} + \underbrace{(-nq)}_{\in G}.$$

Donc $r \in G$. Comme n est le plus petit élément de $G \cap \mathbb{N}^*$, on a nécessairement $r = 0$ (car $r < n$)

Donc $x \in n\mathbb{Z}$.

Ainsi, les sous-groupes de \mathbb{Z} sont exactement les $n\mathbb{Z}$, où $n \in \mathbb{N}$.

D) Une caractérisation condensée des sous-groupes

Proposition :

Soit (G, \times) un groupe, H une partie de G .

$$\text{Alors } H \text{ est un sous-groupe de } (G, \times) \Leftrightarrow \begin{cases} 1_G \in H \\ \forall x, y \in H, xy^{-1} \in H \end{cases}$$

Démonstration :

La première implication est évidente. Pour l'autre :

$$\text{Supposons que } \begin{cases} 1_G \in H \\ \forall x, y \in H, xy^{-1} \in H \end{cases}$$

Alors déjà $1_G \in H \dots$

En prenant $x = 1_G$, Alors, pour tout $y \in H$, $y^{-1} \in H$.

Pour tout $x, y \in H$, $y^{-1} \in H$, donc $x(y^{-1})^{-1} \in H$ c'est-à-dire $xy \in H$

E) Intersections de sous-groupes

Théorème :

Soit (G, \times) un groupe.

Alors toute intersection de sous-groupes de G est un sous-groupe de G .

Démonstration :

Soit $(H_i)_{i \in I}$ une famille de sous-groupes de G indexée par I . Notons $H = \bigcap_{i \in I} H_i$

Déjà, $1_G \in H$, puisque $\forall i \in I, 1_G \in H_i$.

Soient $x, y \in H$. Alors, pour tout $i \in I$, $x \in H_i$, $y \in H_i$ donc $xy^{-1} \in H_i$.

Donc $xy^{-1} \in H$.

Donc H est un sous-groupe de (G, \times) .

F) Sous-groupe engendré par une partie

Soit (G, \times) un groupe.

Soit A une partie de G .

On appelle sous-groupe engendré par A le plus petit sous-groupe de G contenant A .

Il y en a bien un, puisque déjà G contient A . Donc l'ensemble \mathcal{E} des sous-groupes de G contenant A n'est pas vide.

Considérons alors $\bigcap_{H \in \mathcal{E}} H$. C'est un sous-groupe de G , il contient A et est contenu dans tout sous-groupe de G contenant A .

On note alors $\langle A \rangle = \bigcap_{H \in \mathcal{E}} H$

Cas particulier :

Un sous-groupe engendré par un singleton $\{a\}$ est noté $\langle a \rangle$, et on parle du sous-groupe engendré par l'élément a .

Exemples :

- Dans $\mathbb{Z}/6\mathbb{Z}$:

$$\langle \dot{2} \rangle = \{\dot{0}, \dot{2}, \dot{4}\}$$

$$\langle \dot{3} \rangle = \{\dot{0}, \dot{3}\}$$

$$\langle \dot{5} \rangle = \mathbb{Z}/6\mathbb{Z}, \text{ (on dit que } \dot{5} \text{ est un générateur de } \mathbb{Z}/6\mathbb{Z}\text{)}$$

$$\langle \{\dot{2}, \dot{3}\} \rangle = \mathbb{Z}/6\mathbb{Z}, \text{ (}\{\dot{2}, \dot{3}\}\text{ est une partie génératrice de } \mathbb{Z}/6\mathbb{Z}\text{)}$$

- Dans $(\mathbb{R}, +)$: $\langle 2\pi \rangle = 2\pi\mathbb{Z}$

- Dans $\mathfrak{S}_3 = \{\text{Id}_E, \tau_{1,2}, \tau_{2,3}, \tau_{3,1}, s, s'\}$:

$$\langle s \rangle = \{\text{Id}, s, s'\} ; \langle s' \rangle = \{\text{Id}, s, s'\} ; \langle \tau_{1,2} \rangle = \{\text{Id}, \tau_{1,2}\} ; \langle s, \tau_{a,b} \rangle = \mathfrak{S}_3$$

G) Groupe monogène

Définition :

Soit (G, \times) un groupe.

On dit que G est monogène lorsqu'il admet un générateur, c'est-à-dire lorsqu'il existe $a \in G$ tel que $\langle a \rangle = G$, c'est-à-dire : $\exists a \in G, \langle a \rangle = G$

Remarque :

$$\langle a \rangle = \{a^k, k \in \mathbb{Z}\}$$

En effet :

- Soit H un sous-groupe de G contenant a . Alors, comme H est stable par \times et passage à l'inverse, une récurrence évidente montre qu'alors H contient $\{a^k, k \in \mathbb{Z}\}$.

- L'ensemble $\{a^k, k \in \mathbb{Z}\}$ est effectivement un sous-groupe de G contenant a :

Il contient $1_G = a^0$.

Il est stable par \times , puisque pour tous $x, y \in \{a^k, k \in \mathbb{Z}\}$, x s'écrit $x = a^k$, y s'écrit $y = a^{k'}$ (où $k, k' \in \mathbb{Z}$) et $xy = a^k a^{k'} = a^{k+k'} \in \{a^k, k \in \mathbb{Z}\}$

Il est stable par passage à l'inverse puisque pour tout $x \in \{a^k, k \in \mathbb{Z}\}$, x s'écrit $x = a^k$ où $k \in \mathbb{Z}$, et $x^{-1} = (a^k)^{-1} = a^{-k} \in \{a^k, k \in \mathbb{Z}\}$.

C'est donc un sous-groupe de G , et enfin il contient a puisque $a = a^1$.

Donc $\{a^k, k \in \mathbb{Z}\}$ est un sous-groupe de G qui contient a , et c'est le plus petit.

Remarque :

Plus généralement, $\langle A \rangle$ est l'ensemble des produits de puissances d'éléments de A .

Définition :

Un groupe G est dit cyclique lorsqu'il est monogène et fini.

Exemples :

- $(\mathbb{Z}, +)$ est monogène infini : $\mathbb{Z} = \{k \cdot 1, k \in \mathbb{Z}\} = \langle 1 \rangle$ (Attention, notation additive)

Tous les sous-groupes de \mathbb{Z} sont monogènes (infinis) : $n\mathbb{Z} = \{k \cdot n, k \in \mathbb{Z}\} = \langle n \rangle$

- $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique, engendré par $\dot{1}$ (qui n'est généralement pas le seul)

- (\mathbb{U}_n, \times) est aussi cyclique : $\mathbb{U}_n = \{\omega^k, k \in \mathbb{Z}\} = \langle \omega \rangle$ où $e^{\frac{2i\pi}{n}}$.

III Morphismes de groupes

(Morphisme est une apocope de homomorphisme)

A) Définition (en notation « bizarre »)

Soient $(G, \#)$ et (H, \heartsuit) deux groupes.

Un morphisme de $(G, \#)$ vers (H, \heartsuit) est une application $\varphi: G \rightarrow H$ telle que :

$$\forall x, y \in G, \varphi(x \# y) = \varphi(x) \heartsuit \varphi(y)$$

Exemples :

- \exp est un morphisme de $(\mathbb{R}, +)$ vers (\mathbb{R}^*, \times)

- $x \mapsto \sqrt{x}$ de (\mathbb{R}_+, \times) vers (\mathbb{R}^*, \times) (ou vers (\mathbb{R}_+^*, \times) aussi)
- $x \mapsto ax$ de $(\mathbb{R}, +)$ vers $(\mathbb{R}, +)$
- $\theta \mapsto e^{i\theta}$ de $(\mathbb{R}^*, +)$ vers (\mathbb{C}^*, \times)
- L'ensemble $S_C(\mathbb{N}, \mathbb{R})$ des suites réelles convergentes est un sous-groupe de $(\mathbb{R}^{\mathbb{N}}, +)$ et l'application $u \mapsto \lim(u)$ est un morphisme de $(S_C(\mathbb{N}, \mathbb{R}), +)$ vers $(\mathbb{R}, +)$.

B) Propriétés (notation multiplicative)

Proposition :

Soit φ un morphisme d'un groupe (G, \times) vers un groupe (H, \times) .

Alors :

- $\forall x, y \in G, \varphi(xy) = \varphi(x)\varphi(y)$
- $\varphi(1_G) = 1_H$
- $\forall x \in G, \varphi(x^{-1}) = (\varphi(x))^{-1}$
- $\forall x \in G, \forall n \in \mathbb{Z}, \varphi(x^n) = (\varphi(x))^n$

Démonstration :

- C'est la définition.
- $\varphi(1_G) = \varphi(1_G \times 1_G) = \varphi(1_G) \times \varphi(1_G)$.

L'élément $a = \varphi(1_G)$ de H vérifie donc $a \times a = a$. Donc $a = a \times a^{-1} = 1_H$

- Soit $x \in G$. Alors $\varphi(x^{-1})\varphi(x) = \varphi(x^{-1}x) = \varphi(1_G) = 1_H$

De même, $\varphi(x)\varphi(x^{-1}) = 1_H$

Donc $\varphi(x^{-1}) = (\varphi(x))^{-1}$

- Soit $x \in G$. Montrons par récurrence que $\forall n \in \mathbb{N}, \varphi(x^n) = (\varphi(x))^n$:

Pour $n = 0$, $\varphi(x^0) = \varphi(1_G) = 1_H = (\varphi(x))^0$

Soit $n \in \mathbb{N}$, supposons que $\varphi(x^n) = (\varphi(x))^n$.

Alors $\varphi(x^{n+1}) = \varphi(x^n x) = \varphi(x^n)\varphi(x) = (\varphi(x))^n \varphi(x) = (\varphi(x))^{n+1}$

On passe aux n négatifs avec le point précédent.

C) Noyau et image d'un morphisme

Définition, proposition :

Soit φ un morphisme d'un groupe (G, \times) vers un groupe (H, \times) .

L'image de φ , notée $\text{Im } \varphi$, c'est $\varphi(G)$, c'est-à-dire $\{\varphi(x), x \in G\}$

Alors $\text{Im } \varphi$ est un sous-groupe de H .

Démonstration :

- $\text{Im } \varphi$ contient 1_H car $1_H = \varphi(1_G)$

- $\text{Im } \varphi$ est stable par \times :

Soient $u, v \in \text{Im } \varphi$. Alors u s'écrit $\varphi(x)$ où $x \in G$, v s'écrit $\varphi(y)$ où $y \in G$.

Donc $u \times v = \varphi(x) \times \varphi(y) = \varphi(xy) \in \text{Im } \varphi$

- $\text{Im } \varphi$ est stable par passage à l'inverse :
Soit $u \in \text{Im } \varphi$. Alors u s'écrit $\varphi(x)$ où $x \in G$.
Et : $u^{-1} = (\varphi(x))^{-1} = \varphi(x^{-1}) \in \text{Im } \varphi$

Définition :

Soit φ un morphisme d'un groupe (G, \times) vers un groupe (H, \times) .

Le noyau de φ , noté $\ker \varphi$ est par définition :

$$\ker \varphi = \{x \in G, \varphi(x) = 1_H\}$$

Proposition :

$\ker \varphi$ est un sous-groupe de G .

Démonstration :

- $1_G \in \ker \varphi$ car $\varphi(1_G) = 1_H$.
- Pour tous $x, y \in \ker \varphi$, on a $\varphi(xy) = \varphi(x) \times \varphi(y) = 1_H \times 1_H = 1_H$ donc $xy \in \ker \varphi$.
- Pour tout $x \in \ker \varphi$, $\varphi(x^{-1}) = (\varphi(x))^{-1} = (1_H)^{-1} = 1_H$ donc $x^{-1} \in \ker \varphi$.

Théorème :

Soit φ un morphisme d'un groupe (G, \times) vers un groupe (H, \times) . Alors :

(1) Pour tous $x, y \in G$, $\varphi(x) = \varphi(y) \Leftrightarrow xy^{-1} \in \ker \varphi$

(2) φ est injective $\Leftrightarrow \ker \varphi = \{1_G\}$

Démonstration :

(1) On a les équivalences :

$$\begin{aligned} \varphi(x) = \varphi(y) &\Leftrightarrow \varphi(x)(\varphi(y))^{-1} = 1_H \Leftrightarrow \varphi(x)\varphi(y^{-1}) = 1_H \Leftrightarrow \varphi(xy^{-1}) = 1_H \\ &\Leftrightarrow xy^{-1} \in \ker \varphi \end{aligned}$$

(2) Supposons φ injective :

Soit $x \in \ker \varphi$. Alors $\varphi(x) = 1_H = \varphi(1_G)$.

Donc, comme φ est injective, $x = 1_G$. Donc $\ker \varphi \subset \{1_G\}$

De plus, $\ker \varphi$ est un sous-groupe de G , donc $1_G \in \ker \varphi$, donc $\{1_G\} \subset \ker \varphi$.

D'où l'égalité.

Réciproquement, supposons que $\ker \varphi = \{1_G\}$:

Soient alors $x, y \in G$. Supposons que $\varphi(x) = \varphi(y)$.

Alors $xy^{-1} \in \ker \varphi$. Donc $xy^{-1} = 1_G$. Donc $x = y$.

Donc φ est injective.

Exemple :

L'application $\varphi: \mathbb{R} \rightarrow \mathbb{C}^*$ est un morphisme de $(\mathbb{R}, +)$ vers (\mathbb{C}^*, \times) de noyau

$2\pi\mathbb{Z}$, et d'image \mathbb{U}

D) Composition

Proposition :

La composée, quand elle est définie, de deux morphismes de groupes est un morphisme de groupes.

Démonstration :

Soient $(G,*)$, $(H,\#)$, (I,\heartsuit) trois groupes.

Soient $\varphi_{GH} : G \rightarrow H$ et $\varphi_{HI} : H \rightarrow I$ deux morphismes.

Alors $\varphi_{HI} \circ \varphi_{GH}$ est bien définie, et va de $(G,*)$ dans (I,\heartsuit) .

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

$$\begin{aligned} \varphi_{HI} \circ \varphi_{GH}(x * y) &= \varphi_{HI}(\varphi_{GH}(x * y)) \\ &= \varphi_{HI}(\varphi_{GH}(x) \# \varphi_{GH}(y)) \\ &= \varphi_{HI}(\varphi_{GH}(x)) \heartsuit \varphi_{HI}(\varphi_{GH}(y)) \\ &= (\varphi_{HI} \circ \varphi_{GH}(x)) \heartsuit (\varphi_{HI} \circ \varphi_{GH}(y)) \end{aligned}$$

E) Isomorphisme

Proposition, définition :

Soit φ un morphisme bijectif de (G,\times) vers (H,\times) . Alors φ^{-1} est un morphisme (bijectif) de (H,\times) vers (G,\times) . On dit que φ est un isomorphisme.

Lorsqu'il existe un isomorphisme entre deux groupes, on dit que ces deux groupes sont isomorphes.

Démonstration :

Soit φ un morphisme bijectif de (G,\times) vers (H,\times) .

Soient $x, y \in H$.

Soient $u, v \in G$ tels que $\varphi(u) = x$, $\varphi(v) = y$. (C'est-à-dire $u = \varphi^{-1}(x)$, $v = \varphi^{-1}(y)$).

Alors $\varphi^{-1}(x \times y) = \varphi^{-1}(\varphi(u) \times \varphi(v)) = \varphi^{-1}(\varphi(uv)) = uv = \varphi^{-1}(x) \times \varphi^{-1}(y)$

Donc φ^{-1} est un morphisme de (H,\times) vers (G,\times) .

Exemples :

- $(]-\frac{\pi}{2}, \frac{\pi}{2}[, *)$ et $(\mathbb{R}, +)$ sont isomorphes, où $*$ est la loi définie par :

$$\forall x, y \in]-\frac{\pi}{2}, \frac{\pi}{2}[, \tan(x * y) = \tan x + \tan y$$

C'est-à-dire $\forall x, y \in]-\frac{\pi}{2}, \frac{\pi}{2}[, x * y = \text{Arctan}(\tan x + \tan y)$

(Ainsi, $\forall x, y \in]-\frac{\pi}{2}, \frac{\pi}{2}[, \varphi(x * y) = \varphi(x) + \varphi(y)$, où $\varphi = \tan$, qui réalise bien une bijection de $]-\frac{\pi}{2}, \frac{\pi}{2}[$ dans \mathbb{R})

- $f : \mathbb{Z} \rightarrow \mathbb{U}_n$ est un morphisme surjectif de $(\mathbb{Z}, +)$ vers (\mathbb{U}_n, \times) mais non injectif. Son noyau est $n\mathbb{Z}$:

Déjà, c'est un morphisme, puisque pour tous $x, y \in \mathbb{Z}$, on a :

$$f(x + y) = e^{\frac{2i(x+y)\pi}{n}} = e^{\frac{2ix\pi}{n}} e^{\frac{2iy\pi}{n}} = f(x)f(y).$$

f est surjective puisque tout élément $z \in \mathbb{U}_n$ s'écrit $e^{\frac{2ik\pi}{n}}$ où $k \in \mathbb{Z}$.

Mais f n'est pas injective : pour tout $x \in \mathbb{Z}$, on a les équivalences :

$$x \in \ker f \Leftrightarrow f(x) = 1 \Leftrightarrow \frac{2x\pi}{n} \in 2\pi\mathbb{Z} \Leftrightarrow \frac{x}{n} \in \mathbb{Z} \Leftrightarrow x \in n\mathbb{Z}$$

Donc le noyau de f est $n\mathbb{Z}$, donc f n'est pas injective.

$\varphi : \mathbb{Z} / n\mathbb{Z} \rightarrow \mathbb{U}_n$ où k est tel que $k \equiv u \pmod{n}$ par contre est bijectif.

$$u \mapsto e^{\frac{2ik\pi}{n}}$$

Démonstration :

Déjà, il faut montrer que la définition de φ est cohérente, c'est-à-dire que $e^{\frac{2ik\pi}{n}}$ ne dépend que de \dot{k} et non pas de k .

Si deux éléments $k, k' \in \mathbb{Z}$ sont tels que $\dot{k} = \dot{k}'$, on a alors :

$k - k' \in n\mathbb{Z}$. Donc $k - k' \in \ker f$. Donc $f(k) = f(k')$ (on est en notation additive)

Donc $e^{\frac{2ik\pi}{n}} = e^{\frac{2ik'\pi}{n}}$.

C'est un morphisme :

Pour tous $u, u' \in \mathbb{Z}/n\mathbb{Z}$, s'écrivant $u = \dot{k}$ et $u' = \dot{k}'$ où $k, k' \in \mathbb{Z}$:

$\varphi(u + u') = e^{\frac{2i(k+k')\pi}{n}} = e^{\frac{2ik\pi}{n}} e^{\frac{2ik'\pi}{n}} = \varphi(u)\varphi(u')$.

φ est surjective, puisque tout élément $z \in \mathbb{U}_n$ s'écrit $e^{\frac{2ik\pi}{n}}$ où $k \in \mathbb{Z}$.

φ est aussi injective :

Soit $u \in \ker \varphi$. Alors u s'écrit \dot{k} où $k \in \mathbb{Z}$.

Alors $\varphi(u) = e^{\frac{2ik\pi}{n}} = 1$. Donc $k \in n\mathbb{Z}$. Donc $u = \dot{k} = \dot{0}$. Donc $\ker \varphi \subset \{\dot{0}\}$.

Comme $\ker \varphi$ est un sous-groupe de $n\mathbb{Z}$, on a aussi l'autre inclusion et donc l'égalité. Donc φ est injective.

Donc φ est bijective. Donc (\mathbb{U}_n, \times) et $(\mathbb{Z}/n\mathbb{Z}, +)$ sont isomorphes.

Remarque :

La relation « être isomorphe à » est une relation d'équivalence sur l'ensemble des groupes :

- Elle est réflexive (l'identité est un isomorphisme d'un groupe G vers G)
- Elle est symétrique (si G est isomorphe à H , alors H est isomorphe à G)
- Elle est transitive (la composée de deux isomorphismes est un isomorphisme)

F) Vocabulaire (rappels)

- Un morphisme de G vers H est aussi appelé homomorphisme de G vers H .
- Un isomorphisme de G vers H est un morphisme bijectif de G vers H .
- Un endomorphisme de G est un morphisme de G vers G .
- Un automorphisme de G est un morphisme bijectif de G vers lui-même.
isomorphisme de G vers lui-même.
endomorphisme bijectif de G .

IV Ordre d'un élément d'un groupe

Soit (G, \times) un groupe.

Théorème, définition :

Soient $a \in G, n \in \mathbb{N}^*$. Alors les trois affirmations suivantes sont équivalentes :

- (1) $\langle a \rangle$ est fini et de cardinal n .
- (2) Il existe $k \in \mathbb{N}^*$ tel que $a^k = 1_G$, et n est le plus petit des ces entiers.
- (3) L'ensemble $\{k \in \mathbb{Z}, a^k = 1_G\}$ n'est pas réduit à $\{0\}$, c'est même $n\mathbb{Z}$.

Lorsque l'une des ces affirmations (et donc les trois) est vraie, on dit que a est un élément d'ordre fini de G , égal à n .

Démonstration :

Considérons $\varphi: \mathbb{Z} \rightarrow G$. Alors φ est un morphisme de $(\mathbb{Z}, +)$ vers (G, \times) .

En effet, $\forall k, k' \in \mathbb{Z}, a^{k+k'} = a^k a^{k'}$.

On a :

$$\text{Im } \varphi = \{a^k, k \in \mathbb{Z}\} = \langle a \rangle$$

$\ker \varphi$ est un sous groupe de $(\mathbb{Z}, +)$ donc du type $m\mathbb{Z}$ où $m \in \mathbb{N}$.

- Si $m = 0$, $\ker \varphi = \{0\}$ donc φ est injective. Donc φ réalise une bijection de \mathbb{Z} sur $\text{Im } \varphi = \langle a \rangle$. Donc $\langle a \rangle$ est infini.

- Si $m \geq 1$, $\langle a \rangle = \{a^0, a^1, \dots, a^{m-1}\}$. En effet :

Une première inclusion, $\{a^0, a^1, \dots, a^{m-1}\} \subset \langle a \rangle$ est déjà évidente.

Soit maintenant $b \in \langle a \rangle$.

Alors b s'écrit a^k où $k \in \mathbb{Z}$. La division euclidienne de k par m ($m \neq 0$) donne :

$$k = mq + r \text{ avec } r \in \llbracket 0, m-1 \rrbracket.$$

Donc $b = a^{mq+r} = \underbrace{(a^m)^q}_{=1_G \text{ car } m \in m\mathbb{Z} = \ker \varphi} a^r = a^r \in \{a^0, a^1, \dots, a^{m-1}\}$, d'où l'autre inclusion, et l'égalité.

De plus, $\text{card}(\langle a \rangle) = m$: il n'existe pas i, j distincts dans $\llbracket 0, m-1 \rrbracket$ tels que $a^i = a^j$ car si par exemple $0 \leq i < j \leq m-1$, et si on avait $a^i = a^j$, on aurait $a^{i-j} = 1_G$ ce qui ne se peut pas car $0 < i-j \leq m-1$ donc $j-i \notin m\mathbb{Z}$.

Avec cela, il est maintenant facile de montrer que (1) \Rightarrow (2) \Rightarrow (1) et (1) \Rightarrow (3) \Rightarrow (1) :

Supposons (1).

Alors, en gardant les notations précédentes, $m = n$.

Donc n est bien le plus petit des $k \in \mathbb{N}^*$ tels que $a^k = 1_G$, car $a^m = 1_G$ et $\forall k \in \llbracket 1, m-1 \rrbracket, a^k \neq 1_G$ (puisque $a^0 = 1_G$ et on a montré que les $a^k, k \in \llbracket 0, m-1 \rrbracket$ sont distincts)

Et d'autre part l'ensemble des $k \in \mathbb{Z}$ tels que $a^k = 1_G$ est bien $n\mathbb{Z}$ (c'est $\ker \varphi$)

Donc (1) \Rightarrow (2) et (1) \Rightarrow (3).

Supposons maintenant (3) : On est alors dans la situation $m = n \geq 1$ (car $\ker \varphi \neq \{0\}$)

Donc le sous-groupe engendré par a est de cardinal n .

De même, (2) \Rightarrow (1).

Exemples :

Dans $(\mathbb{Z}/6\mathbb{Z}, +)$:

$\dot{2}$ est d'ordre 3 : $\langle \dot{2} \rangle = \{\dot{0}, \dot{2}, \dot{4}\}$ de cardinal 3

Autre justification : $3 \cdot \dot{2} = \dot{2} + \dot{2} + \dot{2} = \dot{0}$ et $1 \cdot \dot{2} = \dot{2} \neq \dot{0}$, $2 \cdot \dot{2} = \dot{4} \neq \dot{0}$

$\dot{3}$ est d'ordre 2, $\dot{1}$ et $\dot{5}$ sont d'ordre 6, $\dot{0}$ est d'ordre 1.

Dans $(\mathbb{Z}, +)$, 0 est d'ordre 1, tout les autres sont d'ordre infini.

Dans (\mathfrak{S}_8, \circ) :

Notation (dans \mathfrak{S}_n) : la permutation $1 \mapsto a_1 \dots$ est notée généralement $\begin{pmatrix} 1 & 2 & 3 & \dots & 8 \\ a_1 & a_2 & a_3 & \dots & a_8 \end{pmatrix}$.

Prenons par exemple $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 7 & 2 & 4 & 8 & 6 & 1 \end{pmatrix}$. Alors σ est d'ordre fini, car $\sigma \in \mathfrak{S}_8$ et \mathfrak{S}_8 est de cardinal fini (Donc au pire σ est d'ordre ce cardinal, à savoir 15)