Chapitre 1 : Groupes

I Généralités

A) Définition

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

- $*$ est associative,
- il y a dans G un élément neutre pour $*$,
- tout élément de G admet un symétrique pour la loi $*$.

C'est-à-dire :

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

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 $G = \{a, b, c\}$, de loi $\heartsuit$ définie par la table de Pythagore donnant $x \heartsuit y$:

x \ y	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

(1.1)

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. Alors :

- 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. Alors $x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x''$. On note dans la suite de cette section $\bar{x}$ 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 $x, y \in G$, $\overline{x * y} = \bar{y} * \bar{x}$:
  $(x * y) * (\bar{y} * \bar{x}) = x * [y * (\bar{y} * \bar{x})] = x * [(y * \bar{y}) * \bar{x}] = x * [e * \bar{x}] = x * \bar{x} = e$, 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 $x, y, z \in G$, on a :
  1. $x * y = z \iff x = z * \bar{y}$,
  2. $y * x = z \iff x = \bar{y} * z$.

  Démonstration :
  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 $x * y = (z * \bar{y}) * y = z * (\bar{y} * \bar{y}) = z * e = z$. La démonstration est la même pour le deuxième point.
- Régularité : pour tous $x, y, z \in G$, on a :
  1. $x * z = y * z \implies x = y$,
  2. $z * x = z * y \implies x = y$,
  3. et les implications réciproques sont vraies aussi mais évidentes.

  Démonstration :
  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 le deuxième point.

  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 $x_1 * y_1 = x_1 * y_2$ / $x_1 * y_1 = x_2 * y_1$, donc $y_1 = y_2$ / $x_1 = x_2$.
- Itéré d'un élément : soit $x \in G$. On note (ici 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 » : pour $x \in G$, $n \in \mathbb{N}$, on pose $x\$(-n) = \bar{x}\$n$. Alors $x\$(-n) = \overline{x\$n}$, et 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, avec ces notations :

- $(x^{-1})^{-1} = x$,
- $(xy)^{-1} = y^{-1}x^{-1}$,
- $xy = z \iff x = zy^{-1}$,
  $yx = z \iff x = y^{-1}z$,
- $xz = yz \implies x = y$,
  $zx = zy \implies x = y$,
- $x^0 = 1_G, \quad x^1 = x$,
  $\forall n \in \mathbb{N}, x^{(n+1)} = x^n x, \quad \forall n \in \mathbb{N}, x^{-1} = (x^{-1})^n = (x^n)^{-1}$,
  $\forall n, p \in \mathbb{Z}, x^n x^p = x^{(n+p)}, \quad \forall n, p \in \mathbb{Z}, (x^n)^p = x^{n \times p}$.

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

Les règles donnent alors :

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

D) Autres exemples de groupe

1) Groupes de nombres

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

2) 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 : $\forall f,g,h\in\mathfrak{S}(E), f\circ(g\circ h)=(f\circ g)\circ h$ (c'est vrai dans un cas plus général et pas seulement pour les bijections).
- Neutre : $\mathrm{Id}_E\in\mathfrak{S}(E)$.
- 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, et soient $f,g\colon E\to E$ définies ainsi :

$$\begin{cases} f(a)=b \\ f(b)=a \\ \forall x\in E\backslash\{a,b\}, f(x)=x \end{cases}, \quad \begin{cases} g(b)=c \\ g(c)=b \\ \forall x\in E\backslash\{b,c\}, g(x)=x \end{cases}. \tag{1.2}$$

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 $f\circ g\neq g\circ f$:

$$(f\circ g)(a)=f(g(a))=f(a)=b, \tag{1.3}$$
$$(g\circ f)(a)=g(f(a))=g(b)=c. \tag{1.4}$$

Exemple :

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

Table de Pythagore de $\mathfrak{S}_2$: $\mathfrak{S}_2=\{\mathrm{Id},\tau\}$, où $\begin{array}{rcl}\mathrm{Id}\colon\{1,2\} & \longrightarrow & \{1,2\} \\ x & \longmapsto & x\end{array}$, et $\tau\colon\{1,2\}\to\{1,2\}$ est définie par $\tau(1)=2$, $\tau(2)=1$.

Tableau donnant $x\circ y$:

$x^{\,y}$	Id	τ
Id	Id	τ
τ	τ	Id

(1.5)

Table de Pythagore de $\mathfrak{S}_3$: $\mathfrak{S}_3=\{\mathrm{Id}_E,\tau_{1,2},\tau_{2,3},\tau_{3,1},s,s'\}$, où :

$\begin{array}{rcl}\mathrm{Id}\colon\{1,2,3\} & \longrightarrow & \{1,2,3\} \\ x & \longmapsto & x\end{array}$,

$\tau_{a,b}\colon\{1,2,3\}\to\{1,2,3\}$ défini par $\tau_{a,b}(a)=b$, $\tau_{a,b}(b)=a$, $\tau_{a,b}(x)=x$ sinon,

$s\colon\{1,2,3\}\to\{1,2,3\}$ définie par $s(1)=2$, $s(2)=3$, $s(3)=1$,

$s'\colon \{1,2,3\} \to \{1,2,3\}$ définie par $s'(1)=3$, $s'(2)=1$, $s'(3)=2$.

Tableau donnant $x \circ y$:

x \ 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

(1.6)

3) Groupes de fonctions

Exemple :

$(\mathscr{F}(A,G),\otimes)$, où A est un ensemble quelconque, et $(G,\times)$ est un groupe, avec $\otimes$ défini par :

$$\forall f,g \in \mathscr{F}(A,G),\quad f\otimes g\colon \begin{array}{ccc} A & \longrightarrow & G \\ x & \longmapsto & f(x)\times g(x) \end{array} \tag{1.7}$$

E) Classes d'équivalence modulo n

Soit $n \in \mathbb{N}, n \geqslant 2$. On définit sur $\mathbb{Z}$ la relation $\equiv_n$ par :

$$\forall x,y \in \mathbb{Z}, x \equiv_n y \implies y-x \in n\mathbb{Z} \tag{1.8}$$

Cette relation s'appelle la relation de congruence modulo n. On note plutôt $x \equiv y \mod n$ ou encore $x \equiv y\ [n]$. Cette relation est une relation d'équivalence.

Démonstration :

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

Cette relation est compatible avec $+$.

Démonstration :

Pour tous $x,x',y,y' \in \mathbb{Z}$, 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 n'indique pas qu'on travaille modulo n). On a alors l'équivalence :

$$\forall x,y \in \mathbb{Z}, (\dot{x}=\dot{y} \iff x \equiv y\ [n]) \tag{1.9}$$

Démonstration :

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

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

Réciproquement, si $x \equiv y\ [n]$, soit $z \in \dot{x}$. Alors $z \equiv x\ [n]$. Donc $z \equiv y\ [n]$ (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 :
$\mathbb{Z}/n\mathbb{Z}$ est fini, et de cardinal n. Pour tous $x, y \in \mathbb{Z}$, on pose $\dot{x} \oplus \dot{y} = \dot{\overline{x+y}}$.
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 $a \in [\![0, n-1]\!]$ tel que $\dot{x} = \dot{a}$, c'est-à-dire tel que $x \equiv a\ [n]$.
En effet, en prenant $a = x - nk$, où $k = \left[\frac{x}{n}\right]$, on a alors $k \leqslant \frac{x}{n} < k+1$, donc $nk \leqslant x < nk + n$, soit $0 \leqslant x - nk < n$, c'est-à-dire $0 \leqslant a \leqslant n-1$, d'où l'existence. Donc $\forall x \in \mathbb{Z}, \exists a \in [\![0, n-1]\!], \dot{x} = \dot{a}$.
Donc $\mathbb{Z}/n\mathbb{Z}$ contient au plus n éléments, à savoir les $\dot{a}, a \in [\![0, n-1]\!]$. On doit donc maintenant montrer que tous ces éléments sont distincts.
Soient $x, y \in [\![0, n-1]\!]$, 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 $0 \leqslant x \leqslant n-1$, donc $nk \leqslant y \leqslant nk + n - 1 < n(k+1)$, donc $k \leqslant \frac{y}{n} < k+1$. Donc $k = \left[\frac{y}{n}\right]$. Or, $0 \leqslant y \leqslant n-1$. Donc $0 \leqslant \frac{y}{n} \leqslant 1 - \frac{1}{n} < 1$. Donc $k = \left[\frac{y}{n}\right] = 0$. Donc $y = x + nk = x$.
Donc $\forall x, y \in [\![0, n-1]\!], \dot{x} = \dot{y} \implies x = y$, soit, par contraposée : $\forall x, y \in [\![0, n-1]\!], x \neq y \implies \dot{x} \neq \dot{y}$.
Donc $\mathbb{Z}/n\mathbb{Z}$ contient au moins n éléments, à savoir les $\dot{a}, a \in [\![0, n-1]\!]$. Donc $\mathbb{Z}/n\mathbb{Z}$ est fini, de cardinal n.

Montrons que $\oplus$ est bien définie, c'est-à-dire que pour tous $x, y \in \mathbb{Z}$, $\dot{\overline{x+y}}$ 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 $\dot{\overline{x+y}} = \dot{\overline{x'+y'}}$.

Montrons maintenant que $\oplus$ est une loi de groupe :

- $\oplus$ 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 :

$$(\dot{x} \oplus \dot{y}) \oplus \dot{z} = \dot{\overline{x+y}} \oplus \dot{z} = \dot{\overline{(x+y)+z}} = x + \dot{\overline{(y+z)}} = \dot{x} \oplus \dot{\overline{y+z}} = \dot{x} \oplus (\dot{y} \oplus \dot{z}) \tag{1.10}$$

- $\mathbb{Z}/n\mathbb{Z}$ a un élement neutre pour $\oplus$, à savoir $\dot{0}$: pour tout $x \in \mathbb{Z}$, on a :

$$\dot{x} \oplus \dot{0} = \dot{\overline{x+0}} = \dot{x} = \dot{\overline{0+x}} = \dot{0} \oplus \dot{x} \tag{1.11}$$

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

$$\dot{x} \oplus \dot{y} = \dot{\overline{x+y}} = x + \dot{\overline{(-x)}} = \dot{0} = \dot{\overline{(-x)+x}} = \dot{\overline{y+x}} = \dot{y} \oplus \dot{x} \tag{1.12}$$

  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 :

$$\dot{x} \oplus \dot{y} = \dot{\overline{x+y}} = \dot{\overline{y+x}} = \dot{y} \oplus \dot{x} \tag{1.13}$$

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

II Sous-groupes (notation multiplicative)

A) Définition

Soit $(G, \times)$ un groupe, et 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.

Démonstration :

- $\times$ 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 : $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\{0\} \cup \{z \in \mathbb{C}^*, \arg(z) = \alpha\ [\pi]\}$. (Le dernier est une droite du plan complexe passant par 0).
- 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).
- $\{\mathrm{Id}, s, s'\}$ est un sous-groupe (commutatif) de $\mathfrak{S}_3$ qui n'est pas commutatif.
- Soit $n \in \mathbb{N}^*$, A une partie de $\{1, 2, \ldots, n\}$ 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 $\sigma(A) \subset A \implies \sigma(A) = A$). Alors H est un sous-groupe de $(S_n, \circ)$:
  Démonstration :
  - ◇ $\mathrm{Id} \in H$.
  - ◇ 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 $x \in A$. Alors $x \in \sigma(A)$. Il existe donc

y dans A tel que $x = \sigma(y)$. 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 $(\mathscr{F}(\mathbb{R},\mathbb{R}),+)$:
  - ◇ L'ensemble des fonctions polynomiales.
  - ◇ $\{\lambda f, \lambda \in \mathbb{R}\}$ où f est un élément fixé de $\mathscr{F}(\mathbb{R},\mathbb{R})$.
  - ◇ $\{f \in \mathscr{F}(\mathbb{R},\mathbb{R}), f(0) = 0\}$.
  - ◇ $\mathcal{C}^n(\mathbb{R},\mathbb{R})$ où $n \in \mathbb{N}$, $\mathcal{D}^n(\mathbb{R},\mathbb{R})$ où $n \in \mathbb{N}$.
  - ◇ Ensemble des fonctions T-périodiques (à T fixé).
  - ◇ Ensemble des fonctions k-lipschitziennes (à k fixé).
  - ◇ Ensemble des fonctions uniformément continues.
  - ◇ Ensemble des fonctions paires, impaires…
- Sous-groupes de $\mathbb{Z}/6\mathbb{Z}$:

$$\{\dot{0}\}, \quad \{\dot{0},\dot{1},\dot{2},\dot{3},\dot{4},\dot{5}\}, \quad \underbrace{\{\dot{0},\dot{2},\dot{4}\}, \quad \{\dot{0},\dot{3}\}}_{\text{sous-groupes propres}} \tag{1.14}$$

$\dot{1}$ engendre $\mathbb{Z}/6\mathbb{Z}$, $\dot{5}$ aussi.
$\dot{2}$ et $\dot{4}$ engendrent $\{\dot{0},\dot{2},\dot{4}\}$.
$\dot{3}$ engendre $\{\dot{0},\dot{3}\}$.
On dit que $\dot{1}$ est un élément d'ordre 6, $\dot{2}$ et $\dot{4}$ d'ordre 3, $\dot{3}$ d'ordre 2.

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

Les $n\mathbb{Z}$, où $n \in \mathbb{N}$, sont des sous-groupes de mbZ. 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 $n \geqslant 1$. Alors $G = n\mathbb{Z}$.

Démonstration :

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 $x = nq + r$, où $q \in \mathbb{Z}$ et $r \in [\![0, n-1]\!]$. 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. Alors H est un sous-groupe de $(G,\times)$, si et seulement si

$$\begin{cases} 1_G \in H \\ \forall x, y \in H, xy^{-1} \in H \end{cases} \tag{1.15}$$

Démonstration :
La première implication est évidente. Pour l'autre : supposons que $\begin{cases} 1_G \in H \\ \forall x, y \in H, xy^{-1} \in H \end{cases}$.
Alors déjà $1_G \in H$…
En prenant $x = 1_G$, on a, 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 $H = \bigcap_{i\in I} H_i$.
Alors $1_G \in H$, 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, 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.

Exemple :

- Dans $\mathbb{Z}/6\mathbb{Z}$: $\langle \dot{2}\rangle = \{\dot{0}, \dot{2}, \dot{4}\}$, $\langle \dot{3}\rangle = \{\dot{0}, \dot{3}\}$, $\langle \dot{5}\rangle = \mathbb{Z}/6\mathbb{Z}$ (on dit que $\dot{5}$ est un générateur de $\mathbb{Z}/6\mathbb{Z}$), $\langle \{\dot{2}, \dot{3}\}\rangle = \mathbb{Z}/6\mathbb{Z}$ ($\{\dot{2}, \dot{3}\}$ est une partie génératrice de $\mathbb{Z}/6\mathbb{Z}$).
- Dans $(\mathbb{R}, +)$: $\langle 2\pi\rangle = 2\pi\mathbb{Z}$.
- Dans $\mathfrak{S}_3$: $\langle s\rangle = \{\mathrm{Id}, s, s'\}$, $\langle s'\rangle = \{\mathrm{Id}, s, s'\}$, $\langle \tau_{1,2}\rangle = \{\mathrm{Id}, \tau_{1,2}\}$, $\langle s, \tau_{a,b}\rangle = \mathfrak{S}_3$

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 :

$$\langle a\rangle = \{a^k, k \in \mathbb{Z}\} \tag{1.16}$$

Démonstration :

- 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.
- 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.

Exemple :

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

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

$(\mathbb{Z}/n\mathbb{Z}, +)$ 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 $\omega = e^{\frac{2i\pi}{n}}$.

III Morphismes de groupes

(Morphisme est une apocope de homomorphisme)

A) Définition (en notation « bizarre »)

Définition :
Soient $(G, \#)$ et $(H, \heartsuit)$ deux groupes. Un morphisme de $(G, \#)$ vers $(H, \heartsuit)$ est une application $\varphi : G \to H$ telle que $\forall x, y \in G, \varphi(x \# y) = \varphi(x) \heartsuit \varphi(y)$.

Exemple :

- 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 $\mathcal{S}_c(\mathbb{N}, \mathbb{R})$ des suites réelles convergentes est un sous-groupe de $(\mathbb{R}^{\mathbb{N}}, +)$, et l'application $u \mapsto \lim(u)$ est un morphisme de $\mathcal{S}_c(\mathbb{N}, \mathbb{R})$ vers $(\mathbb{R}, +)$.

B) Propriétés (notation multiplicative)

Proposition :

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

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

Démonstration :

Le point 1 vient de la définition.

Pour 2 : $\varphi(1_G) = \varphi(1_G \times 1_G) = \varphi(1_G) \times \varphi(1_G)$. L'élément $a = \varphi(1_G)$ de H vérifie donc $a \times a = a$. Donc $a = a \times a^{-1} = 1_H$.

Pour 3 : 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 $\varphi(x^{-1}) = (\varphi(x))^{-1}$.

Pour 4 : 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 $\operatorname{Im}\varphi$, c'est $\varphi(G)$, c'est-à-dire $\{\varphi(x), x \in G\}$. Alors $\operatorname{Im}\varphi$ est un sous-groupe de H.

Démonstration :

- $\operatorname{Im}\varphi$ contient 1_H car $1_H = \varphi(1_G)$.
- $\operatorname{Im}\varphi$ est stable par $\times$:
  Soient $u, v \in \operatorname{Im}\varphi$. Alors u s'écrit $\varphi(x)$ où $x \in G$, v s'écrit $\varphi(y)$ où $y \in G$. Donc $u \times v = \varphi(x) \times \varphi(y) = \varphi(xy) \in \operatorname{Im}\varphi$.
- $\operatorname{Im}\varphi$ est stable par passage à l'inverse :
  Soit $u \in \operatorname{Im}\varphi$. Alors u s'écrit $\varphi(x)$ où $x \in G$, et $u^{-1} = (\varphi(x))^{-1} = \varphi(x^{-1}) \in \operatorname{Im}\varphi$

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 :

$$\ker\varphi = \{x \in G, \varphi(x) = 1_H\} \tag{1.17}$$

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 $x, y \in G$, $\varphi(x) = \varphi(y) \iff xy^{-1} \in \ker\varphi$
2. φ est injective si et seulement si $\ker\varphi = \{1_G\}$.

Démonstration :
On a les équivalences :

$$\begin{aligned}\varphi(x) = \varphi(y) &\iff \varphi(x)(\varphi(y))^{-1} = 1_H \iff \varphi(x)\varphi(y^{-1}) = 1_H \\ &\iff \varphi(xy^{-1}) = 1_H \iff xy^{-1} \in \ker\varphi\end{aligned} \tag{1.18}$$

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

$$\begin{array}{rccc}\varphi\colon & \mathbb{R} & \longrightarrow & \mathbb{C}^* \\ & \theta & \longmapsto & e^{i\theta}\end{array} \tag{1.19}$$

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 $\varphi_{GH}\colon G \to H$ et $\varphi_{HI}\colon H \to I$ 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 :

$$\begin{aligned}\varphi_{HI} \circ \varphi_{GH}(x * y) &= \varphi_{HI}(\varphi_{GH}(x * y)) \\ &= \varphi_{HI}(\varphi_{GH}(x) \# \varphi_{GH}(y)) \\ &= \varphi_{HI}(\varphi_{GH}(x)) \heartsuit \varphi_{HI}(\varphi_{GH}(y)) \\ &= (\varphi_{HI} \circ \varphi_{GH}(x)) \heartsuit (\varphi_{HI} \circ \varphi_{GH}(y))\end{aligned} \tag{1.20}$$

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 $\varphi^{-1}(x\times y)=\varphi^{-1}(\varphi(u)\times\varphi(v))=\varphi^{-1}(\varphi(uv))=u\times v=\varphi^{-1}(x)\times\varphi^{-1}(y)$. Donc φ^{-1} est un morphisme de $(H,\times)$ vers $(G,\times)$.

Exemple :

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

$$\forall x,y\in\left]-\frac{\pi}{2},\frac{\pi}{2}\right[,\tan(x*y)=\tan x+\tan y, \tag{1.21}$$

  c'est-à-dire

$$\forall x,y\in\left]-\frac{\pi}{2},\frac{\pi}{2}\right[,x*y=\arctan(\tan x+\tan y) \tag{1.22}$$

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

- $\begin{array}{rccc} f\colon & \mathbb{Z} & \longrightarrow & \mathbb{U} \\ & k & \longmapsto & e^{\frac{2ik\pi}{n}} \end{array}$ est un morphisme surjectif de $(\mathbb{Z},+)$ vers $(\mathbb{U}_n,\times)$ mais non injectif. Son noyau est $n\mathbb{Z}$:

  Démonstration :

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

$$f(x+y)=e^{\frac{2i(x+y)\pi}{n}}=e^{\frac{2ix\pi}{n}}e^{\frac{2iy\pi}{n}}=f(x)f(y) \tag{1.23}$$

  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 :

$$x\in\ker f\iff f(x)=1\iff\frac{2x\pi}{n}\in 2\pi\mathbb{Z}\iff\frac{x}{n}\in\mathbb{Z}\iff x\in n\mathbb{Z} \tag{1.24}$$

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

- Par contre, $\begin{array}{rccc} \varphi\colon & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{U}_n \\ & u & \longmapsto & e^{\frac{2ik\pi}{n}} \end{array}$, où k est tel que $\dot{k}=u$, est bijectif.

  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 $k,k'\in\mathbb{Z}$, on a :

$$\varphi(u+u')=e^{\frac{2i(k+k')\pi}{n}}=e^{\frac{2ik\pi}{n}}e^{\frac{2ik'\pi}{n}}=\varphi(u)\varphi(u'). \tag{1.25}$$

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

1. $\langle a \rangle$ est fini et de cardinal n.
2. Il existe $k \in N^*$ 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

$$\begin{array}{rccc} \varphi\colon & \mathbb{Z} & \longrightarrow & G \\ & k & \longmapsto & a^k \end{array} . \tag{1.26}$$

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 : $\operatorname{Im}\varphi = \{a^k, k \in \mathbb{Z}\} = \langle a \rangle$. $\ker\varphi$ 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 $\operatorname{Im}\varphi = \langle a \rangle$. Donc $\langle a \rangle$ est infini.
- Si $m \geqslant 1$, $\langle a \rangle = \{a^0, a^1, \dots a^{m-1}\}$. En effet :
  Une première inclusion, $\{a^0, a^1, \dots a^{m-1}\} \subset \langle a \rangle$ est 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 $k = mq + r$ avec $r \in [\![0, m-1]\!]$. 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, $\operatorname{card}(\langle a \rangle) = m$: il n'existe pas i, j distincts dans $[\![0, m-1]\!]$ tels que $a^i = a^j$ car si par

exemple $0 \leqslant i < j \leqslant m-1$, et si on avait $a^i = a^j$, on aurait $a^{i-j} = 1_G$ ce qui ne se peut pas car $0 < i - j \leqslant m-1$ donc $j - i \notin m\mathbb{Z}$.

Avec cela, il est maintenant facile de montrer que $1 \implies 2 \implies 1$ et $1 \implies 3 \implies 1$:
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 $\forall k \in [\![1, m-1]\!], a^k \neq 1_G$ (puisque $a^0 = 1_G$ et on a montré que les $a^k, k \in [\![0, m-1]\!]$ sont distincts). 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 $1 \implies 2$ et $1 \implies 3$.
Supposons maintenant 3. On est alors dans la situation $m = n \geqslant 1$ (car $\ker \varphi \neq \{0\}$). Donc le sous-groupe engendré par a est de cardinal n.
De même, $2 \implies 1$.

Exemple :

- 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 : $3.\dot{2} = \dot{2}+\dot{2}+\dot{2} = \dot{0}$ et $1.\dot{2} = \dot{2} \neq \dot{0}$, $2.\dot{2} = \dot{4} \neq \dot{0}$.
- $\dot{3}$ 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 $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}$.

  Prenons par exemple

  $$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 7 & 2 & 4 & 8 & 6 & 1 \end{pmatrix}. \tag{1.27}$$

  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).