# Chapitre 2

# Groupe. Morphisme. Ordre

**Sommaire**



## 2.1 La notion de groupe. Exemples

Dans les entiers on rencontre d'abord la notion de groupe additif. On peut ajouter deux nombres entiers et on a les propriétés évidentes

| | | |
|---|---|---|
| $(i)$ | associativité | $a+(b+c)=(a+b)+c$ pour tous $a$, $b$, $c$ |
| $(ii)$ | élément neutre | $a+0=0+a=a$ pour tout $a$ |
| $(iii)$ | opposé | $a+(-a)=(-a)+a=0$ pour tout $a$. |

Et on a la propriété supplémentaire de *commutativité* $a+b=b+a$ pour tous $a$ et $b$. Pour la multiplication $\times$, elle est bien définie, associative et il y a un élément neutre, 1. Par contre dans $\mathbb{Z}$, personne ou presque n'a d'inverse. On dit qu'on a un monoïde. Si on prend les rationnels sauf 0, ensemble noté $\mathbb{Q}^*$, tout le monde, sauf 0, a un inverse :

$$a \times \frac{1}{a} = 1.$$

Il faut trouver une notation générale qui regroupe $+$, $\times$, $\circ$, etc..On notera $\top$ à l'inverse de ce qui est fait dans le livre de R. Godement qui utilise $\perp$.

**Definition 2.1.** Un *groupe* $G$ est un ensemble avec un élément particulier $e$, appelé son *unité*, où une loi de composition interne $\top$ est définie, c'est-à-dire

que pour chaque paire d'éléments $a, b$ dans $G$ un élément $a \top b$ de $G$ est donné, de sorte que les axiomes suivants soient vérifiés :

| | | | |
|---|---|---|---|
| $(i)$ | associativité | $\forall a, b, c \in G,$ | $(a \top b) \top c = a \top (b \top c),$ |
| $(ii)$ | élément neutre | $\forall a \in G$ | $a \top e = e \top a = a,$ |
| $(iii)$ | inverse | $\forall a \in G,\ \exists a' \in G,$ | $a \top a' = a' \top a = e.$ |

Pour tout $a$, l'élément $a'$ est unique, car si $a$" vérifie $a \top a'' = a'' \top a = e$, en faisant appel à $(ii)$ et $(i)$ on a

$$a' = a' \top e = a' \top (a \top a") = (a' \top a) \top a" = e \top a" = a". \tag{2.1}$$

D'où $a' = a''$. On dit que $a'$ est l'*inverse* de $a$, on pourrait le noter $a'_{\top}$.
Remarque : dans un groupe $G$, un inverse à droite est toujours égal à l'unique inverse. En effet, si $a'$ est inverse à droite, c'est-à-dire si $a \top a' = e$, et si $x$ est inverse à gauche $x \top a = e$ entraîne $(x \top a) \top a' = a'$ donc $a' = x \top (a \top a') = x \top e = x$.

L'unité $e$ est le seul élément à satisfaire à $(ii)$ ; en effet soit $e'$ satisfaisant la même propriété pour tout $a$, on a

$$e' = e' \top e = e. \tag{2.2}$$

Le groupe $G$ est dit *abélien*, ou encore *commutatif*, si

$$\forall a, b \in G, \quad a \top b = b \top a. \tag{2.3}$$

**Théorème 2.1.** *Dans un groupe, quelque soit $a, b$ l'équation $x \top a = b$ possède une solution $x$ et une seule. De même l'équation $a \top y = b$ possède une solution $y$ et une seule, et si le groupe n'est pas abélien il arrive que $y$ soit différent de $x$.*

*Démonstration.* Pour la première équation on multiplie à droite par $a'$, l'inverse de $a$ :

$$(x \top a) \top a' = b \top a' \implies x \top (a \top a') = b \top a' \implies x = b \top a'.$$

Ce qui donne l'existence et l'unicité. De même pour la seconde $y = a' \top b$.

C.Q.F.D.

**Corollaire 2.2.** *Dans un groupe, quelque soit $a, b, c$, l'équation $a \top c = b \top c$ entraîne $a = b$. De même $c \top a = c \top b$ entraîne $a = b$.*

*Démonstration.* En effet il suffit de composer à droite avec l'inverse de $c$.

C.Q.F.D.

**Notation** : de façon générale, pour un groupe abélien, on préferera la notation $+$. On définit alors $nx = x + x + \cdots + x$ ($n$ termes). En théorie des groupes (où on ne suppose pas que les groupes sont abéliens), la notation multiplicative est préférée à l'usage un peu lourd de symboles comme $\top$, c'est-à-dire que l'on pose très souvent, sans plus préciser,

$$a \top b = ab. \tag{2.4}$$

Cela donne l'écriture habituelle des équations : $ax = b$ ou $ya = b$. On a bien $(ab)c = a(bc)$ donc on peut enlever les parenthèses dans les produits. Mais, en général (sauf dans le cas abélien), on doit tenir compte de l'ordre, car $ab$ peut ne pas être égal à $ba$.
On note alors $a^{-1}$ l'inverse de $a$, pour tout $a \in G$. On note aussi $a^n = a.a. \ldots a$ ($n$ facteurs). Évidemment, il peut arriver que sur un même ensemble on considère plusieurs lois de groupe, alors il faut bien revenir à l'utilisation de lettres comme $\top$, $\perp$, etc.

**Exemples** :

1. $G = \mathbb{Z}$ avec l'élément neutre 0, et la loi $+$, i.e. $a \top b = a + b$. La vérification est immédiate, l'inverse dans ce cas est l'opposé : $a' = -a$. C'est un groupe abélien. Attention : $\mathbb{N}$ avec l'unité 0 et la loi $+$ n'est pas un groupe car aucun élément sauf 0 n'a d'inverse. C'est même la raison d'être de $\mathbb{Z}$.
2. $G = \mathbb{Q}^*$, ensemble des fractions rationnelles non-nulles, avec l'unité 1 et la loi de multiplication $\times$, i.e. $a \top b = ab$. C'est aussi un groupe abélien. De même $\mathbb{R}^*$, nombres réels sauf 0 et $\mathbb{C}^*$, nombres complexes sauf 0. Attention : $\mathbb{Q}$ (ou $\mathbb{R}$ ou $\mathbb{C}$) avec l'unité 1 et la loi $\times$ n'est pas un groupe car 0 n'a pas d'inverse.

3. $G = \{+1, -1\}$ avec $e = +1$ et la loi $\times$ (ou $\cdot$), i.e. $a \top b = ab$. Là chaque élément est son inverse. La *table de la loi* est $+1. + 1 = +1, +1. - 1 = -1. + 1 = -1, -1. - 1 = +1$. Encore abélien.

4. Un qui ressemble beaucoup : $G = \mathbb{Z}/2\mathbb{Z}$, avec $e = 0$ et la loi $+$. La *table de la loi* est $0 + 0 = 0, 0 + 1 = 1 + 0 = 1, 1 + 1 = 0$. Encore abélien.

5. Plus généralement $G = \mathbb{Z}/n\mathbb{Z}$, avec $e = 0$ et la loi $+$ est un groupe abélien.

6. $\mathbb{Z}/n\mathbb{Z}$ n'est pas un groupe multiplicatif. En effet il faut de toute façon lui enlever $\dot{0}$ qui n'est pas inversible.

7. Le groupe multiplicatif $G = (\mathbb{Z}/n\mathbb{Z})^\times$ avec l'unité 1, qui possède $\varphi(n)$ éléments, où $\varphi$ est la fonction arithmétique d'Euler du chapitre précédent. Rappelons que lorsque $n$ est premier, c'est $(\mathbb{Z}/n\mathbb{Z})^\star$.

8. Enfin un exemple non-abélien, le plus petit possible, il a 6 éléments, c'est $G = \mathfrak{S}_3$, l'ensemble des *permutations* de 3 lettres, i.e. l'ensemble des bijections de $\{1, 2, 3\}$ sur lui-même. Ici $e = Id$, la bijection qui envoie 1 sur 1, 2 sur 2 et 3 sur 3. La loi interne $\top$ est la composition des applications :

$$a \top b := a \circ b \quad i.e. \quad a \top b(k) = a(b(k)).$$

Les six éléments de $\mathfrak{S}_3$ sont l'identité, les deux *cycles* d'ordre 3 ($1 \mapsto 2 \mapsto 3 \mapsto 1$, $1 \mapsto 3 \mapsto 2 \mapsto 1$) et les trois *transpositions* (cycles d'ordre 2). Notations $(123)$, $(132)$, $(12), (23), (13)$, soit

$$(123)(1,2,3) = (2,3,1), \quad (132)(1,2,3) = (3,1,2), \quad (12)(1,2,3) = (2,1,3).$$

Exercice : vérifier que ce groupe n'est pas abélien en calculant $(123) \circ (12)$ et $(12) \circ (123)$. faire la table de la loi.

$$(12)(1,2,3) = (2,1,3),$$

d'où

$$(123) \circ (12)(1,2,3) = (123)(2,1,3) = (3,2,1) = (13)(1,2,3).$$

$$(123)(1,2,3) = (2,3,1),$$

d'où

$$(12) \circ (123)(1,2,3) = (12)(2,3,1) = (1,3,2) = (321)(1,2,3).$$

On a donc

$$(123) \circ (12) = (13), \quad (12) \circ (123) = (321).$$

Ces deux permutations sont différentes.

| | Id | (123) | (132) | (12) | (23) | (13) |
|---|---|---|---|---|---|---|
| Id | Id | (123) | (132) | (12) | (23) | (13) |
| (123) | (123) | (132) | Id | (132) | (12) | (23) |
| (132) | (132) | Id | (123) | (23) | (13) | (12) |
| (12) | (12) | (23) | (13) | Id | (123) | (132) |
| (23) | (23) | (13) | (12) | (132) | Id | (123) |
| (13) | (13) | (12) | (23) | (123) | (132) | Id |

TABLE 2.1 – Table de la loi $\circ$ dans $\mathfrak{S}_3$

*Remarque.* On remarque que $(132) = (12) \circ (13) = (23) \circ (12)$ et $(123) = (12) \circ (23) = (23) \circ (13)$. Toute permutation de 3 éléments est engendrée par les transpositions, et de non de manière unique.

9. Une autre classe très importante de groupes est fournie par l'algèbre linéaire. Pour deux entiers $(m, n)$ donnés, l'ensemble des matrices à $m$ lignes et $n$ colonnes constitue un groupe additif.

10. Le groupe $GL_n(\mathbb{R})$ est l'ensemble des matrices inversibles de taille $n \times n$ à coefficients réels, la loi est le produit des matrices et l'élément neutre est la matrice $1_n$. Ce groupe se nomme *groupe linéaire*. Avec des coefficients rationnels, on a $GL_n(\mathbb{Q})$, et avec des coefficients complexes on a $GL_n(\mathbb{C})$. Mais on peut aussi prendre des coefficients entiers, en exigeant que l'inverse soit également à coefficients entiers, alors on obtient $GL_n(\mathbb{Z})$.
D'ailleurs rien n'interdit de considérer des matrices carrées à coefficients dans $\mathbb{Z}/n\mathbb{Z}$ avec la multiplication des matrices ; l'ensemble des matrices à coefficients dans $\mathbb{Z}/n\mathbb{Z}$ dont le déterminant est un élément inversible de $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire un élément de $\mathbb{Z}/n\mathbb{Z}^\times$, forme un groupe.

11. Les matrices carrés $n \times n$ de déterminant 1 forment aussi un groupe, noté $SL_n(\mathbb{R})$ ; on peut là aussi considérer des matrices à coefficients dans $\mathbb{Q}, \mathbb{C}$

ou $\mathbb{Z}$. Ce groupe se nomme *groupe spécial linéaire*.

Dès que $n \geq 2$, ces groupes sont non-abéliens. Par exemple, si $n = 2$, la loi de groupe est définie par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix} \tag{2.5}$$

En particulier

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

mais

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

*Remarque.* D'après les formules de Cramer, toute matrice $n \times n$ à coefficients dans $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$ dont le déterminant vaut 1 est inversible à coefficients dans $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$.

Inversement on peut prouver (exercice) que si une matrice à coefficients entiers relatifs a un inverse à coefficients entiers son déterminant vaut 1 ou $-1$.

**Rappel** : une application $f : X \to X'$ d'un ensemble $X$ sur un ensemble $X'$ est dite *injective* si $f(x) = f(y)$ implique $x = y$, et elle est dite *surjective* si les $f(x)$ remplissent $X'$, i.e. quelque soit $x' \in X'$ il existe au moins un $x \in X$ tel que $f(x) = x'$. On dit que $f$ est *bijective* si elle est injective et surjective. Dire que $f$ est bijective revient à dire qu'il existe $f' : X \to X$ telle que $f' \circ f = f \circ f' = Id_X$. Cette $f'$ est appelée *inverse* de $f$ et notée $f^{-1}$.

**Définition** : si $X$ est un ensemble quelconque, l'ensemble des bijections de cet ensemble sur lui-même, avec $e = Id$ et la loi de composition $f \circ g$, forme un groupe, appelé groupe des permutations de $X$ et noté $\mathfrak{S}(X)$.

Les cas les plus importants pour nous sont les groupes de permutations des ensembles finis, par exemple le groupe $G = \mathfrak{S}_n$ des permutations de $n$ lettres $\{1, 2, , ..., n\}$. Ce groupe se nomme *groupe symétrique*. Sauf pour $n = 2$ le groupe $\mathfrak{S}_n$ est non-abélien.

Pour $n = 2$, on a un cas qui ressemble comme deux gouttes d'eau à celui des exemples 2 et 3 : l'unité est $e = Id$ et l'autre élément est la transposition $\tau = (12)$, i.e. $1 \mapsto 2 \mapsto 1$ ; la table de multiplication de ce groupe est : $e \circ e = e, e \circ \tau = \tau \circ e = \tau, \tau \circ \tau = e$.

| | Id | $\tau$ |
|---|---|---|
| Id | Id | $\tau$ |
| $\tau$ | $\tau$ | Id |

TABLE 2.2 – Table de la loi $\circ$ dans $\mathfrak{S}_2$

## 2.2 Sous-groupes. Morphismes. Images, noyaux.

**Definition 2.2.** Un sous-ensemble $H$ de $G$ est un *sous-groupe* de $G$ si

1. $e \in H$,
2. $a, b \in H \implies a \top b \in H$,
3. $a \in H \implies a^{-1} \in H$.

**Proposition 2.1.** *Pour qu'un sous-ensemble $H$ d'un groupe $G$ soit un sous-groupe il faut et il suffit qu'il soit non-vide et que pour chaque paire d'éléments $(a, b)$ de $H$ l'élément $a \top b^{-1}$ appartienne à $H$.*

*Remarque.* En notation additive on trouve $a - b \in H$, en notation multiplicative $ab^{-1} \in H$,

**Exemples** :

1) $\{e\}$ tout seul, $G$ tout entier sont des sous-groupes de $G$.

2) $\{Id, (12)\}$ Ou encore $\{Id, (123), (321)\}$, dans $\mathfrak{S}_3$. Mais pas $\{Id, (12), (23)\}$, ni $\{(123), (12)\}$ .

3) Dans $(\mathbb{Z}/6\mathbb{Z}, +)$, le sous-ensemble $\{0, 3\}$ ou le sous-ensemble $\{0, 2, 4\}$.

Exercice : démontrer que avec $\{0\}$ et $\mathbb{Z}/6\mathbb{Z}$ lui-même, ce sont les seuls sous-groupes additifs.

4) Dans $(\mathbb{Z}, +)$, le "lemme clé moderne" 1.9 établissait que les sous-groupes sont les ensembles de la forme $d\mathbb{Z}$ .

5) $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$, qui est un sous-groupe de $(\mathbb{R}, +)$.

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

**Definition 2.3.** Soient $(G, \top), (G', \bot)$ deux groupes (d'unités $e, e'$ respectivement), une application $f : G \to G'$ s'appelle un *morphisme* de groupes (ou homomorphisme de groupes), si $f(e) = e'$ et si quels que soient $a, b$ dans $G$ on a $f(a \top b) = f(a) \bot f(b)$.

**Lemme 2.3.** *Si $f$ est un morphisme, pour tout $a$ dans $G$ on a $f(a^{-1}) = (f(a))^{-1}$.*

En effet, $f(a)\perp f(a^{-1}) = f(a\top a^{-1}) = f(e) = e'$.

Soit $f : E \to E'$ une application entre ensembles ; rappelons que l'image, notée $f(A)$, d'une partie $A$ de $E$ est l'ensemble des $x' \in E'$ tels que $x' = f(x)$ pour au moins un $x \in A$, et que l'image inverse, notée $f^{-1}(A')$, d'une partie $A'$ de $E'$ est l'ensemble des $x$ dans $E$ tels que $f(x) \in A'$.

$$f(A) = \{f(x),\ x \in A\}, \quad f^{-1}(A') = \{x \in A, \exists y \in A', f(x) = y\}.$$

**Théorème 2.4.** *Soit $f : G \to G'$ un morphisme, l'image $f(H)$ d'un sous-groupe $H$ de $G$ est un sous-groupe de $G'$, et l'image inverse $f^{-1}(H')$ d'un sous-groupe $H'$ de $G'$ est un sous-groupe de $G$.*

*Démonstration.* (i) D'abord l'image de $H$ contient l'unité $e'$ de $G'$ car $e \in H$ et $f(e) = e'$. Ensuite si $a', b'$ sont des éléments de $f(H)$, il existe $a, b$ dans $H$ tels que $f(a) = a'$ et $f(b) = b'$. Donc

$$f(a\top b^{-1}) = f(a)\perp f(b^{-1}) = f(a)\perp f(b)^{-1} = a'\perp b'^{-1}. \tag{2.6}$$

Donc $a'\perp b'^{-1}$ est l'image de $a\top b^{-1} \in H$. Les deux propriétés qui caractérisent un sous-groupe sont vérifiées.
(ii) l'image réciproque $f^{-1}(H')$ de $H'$ contient l'unité $e$ de $G$ car $f(e) = e'$ appartient à $H'$, et si $a, b$ sont des éléments de $f^{-1}(H')$, soit $a' = f(a)$ et $b' = f(b)$. Alors

$$a\top b^{-1} \in f^{-1}(H') \iff f(a\top b^{-1}) \in H'$$

mais

$$f(a\top b^{-1}) = f(a)\perp (f(b))^{-1} = a'\perp (b')^{-1} \in H'$$

puisque $H'$ est un sous-groupe. Donc $f^{-1}(H')$ est un sous-groupe de $G$. C.Q.F.D.

**Definition 2.4.** Le noyau d'un morphisme $f : G \to G'$ est l'image réciproque de $e'$, soit $f^{-1}(e')$. Il se note $Ker(f)$ ou $Ker\, f$ et se lit ker, abréviation de

kernel.

$$Kerf = \{x \in G,\ f(x) = e'\}.$$

**Théorème 2.5.** *Le morphisme $f$ est injectif si et seulement si son noyau est réduit à l'élément neutre.*

*Démonstration.* Par définition $f$ est injectif si

$$f(x) = f(y) \implies x = y,$$

ce qui se réécrit

$$f(x) \perp (f(y))^{-1} = e' \implies x \top y^{-1} = e,$$

ou encore puisque $f$ est un morphisme

$$f(x \top y^{-1}) = e' \implies x \top y^{-1} = e.$$

Supposons que $Kerf = \{e\}$, alors l'implication précédente est vraie. Réciproquement si l'implication précédente est vraie, et si $f(x) = e'$, alors choisissant $y = e$, on déduit que $x = e$, donc que le noyau est réduit à $e$. C.Q.F.D.

Exemples :

1. Homomorphisme *canonique* $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$, $\chi :\ x \mapsto \dot{x}$. C'est un morphisme car $\widehat{x+y} = \dot{x} + \dot{y}$. Il est surjectif par définition, et son noyau est $n\mathbb{Z}$.

2. Soient deux entiers $n$ et $a$, où $a$ divise $n$. Notons $n = ab$. L'application

$$f :\ \mathbb{Z}/n\mathbb{Z} \ \to\ \mathbb{Z}/a\mathbb{Z}, \qquad \dot{x}_n = x + n\mathbb{Z} \ \mapsto \dot{x}_a = x + a\mathbb{Z}, \tag{2.7}$$

est un morphisme de groupes additifs. En effet $f(\dot{0}_n) = \dot{0}_a$, et

$$f(\dot{x}_n + \dot{y}_n) = f((\widehat{x+y})_n) = (\widehat{x+y})_a = \dot{x}_a + \dot{y}_a.$$

Ce morphisme est surjectif par construction. Pour construire son noyau,

on regarde les images des éléments

$$\begin{array}{l}
\dot{0}_n, \dot{1}_n, \cdots, \widehat{(a-1)}_n, \\
\dot{a}_n, \widehat{(a+1)}_n, \cdots, \widehat{(2a-1)}_n, \\
\vdots \\
\widehat{((b-1)a)}_n, \widehat{((b-1)a+1)}_n, \cdots, \widehat{(ba-1)}_n, \\
\qquad\qquad \downarrow \\
\quad \dot{0}_a, \dot{1}_a, \cdots, \widehat{(a-1)}_a, \\
\quad \dot{\hat{a}}_a, \widehat{a+1}_a, \cdots, \widehat{2a-1}_a, \\
\quad \vdots \\
\quad \widehat{(b-1)a}_a, \widehat{(b-1)a+1}_a, \cdots, \widehat{ba-1}_a. \\
\qquad\qquad \downarrow \\
\qquad \dot{0}_a, \dot{1}_a, \cdots, \widehat{(a-1)}_a, \\
\qquad \dot{0}_a, \dot{1}_a, \cdots, \widehat{(a-1)}_a, \\
\qquad \vdots \\
\qquad \dot{0}_a, \dot{1}_a, \cdots, \widehat{(a-1)}_a,
\end{array}$$

$$\text{D'où} \quad Ker f = \{\dot{0}_n, \dot{a}_n, \widehat{(b-1)a)}_n\}$$

Le noyau de $f$ a $b$ éléments.

3. Rappelons qu'une transposition dans l'ensemble $\{1, \ldots, n\}$ est une permutation réduite à l'identité sauf sur deux éléments $a$ et $b$ qu'elle transpose : $\varphi(a) = b$ et $\varphi(b) = a$. Toute permutation se décompose en produit de transpositions, et la parité du nombre de transpositions est unique pour une permutation donnée. Le groupe alterné $\mathfrak{A}_n$ est le sous ensemble de $\mathcal{S}_n$ constitué des permutations paires, *i.e.* produits d'un nombre pair de transpositions. Exemples

$$\begin{aligned}
\mathfrak{A}_3 &= \{I, (123), (132)\} \\
\mathfrak{A}_4 &= \{I, (234), (243), (134), (143), (124), (142), (123), (132), \\
&\qquad\qquad (12)(34), (13)(42), (14)(23)\} .
\end{aligned}$$

**Definition 2.5.** Soient $G, G'$ deux groupes, d'identités respectives $e, e'$ et de lois respectives $\top, \top'$ on dit que ces groupes sont *isomorphes* s'il existe un morphisme $\chi : G \to G'$ qui est une bijection.

Alors l'application inverse $\chi^{-1}$ de $\varphi$ satisfait la même propriété en inversant

les rôles de $G$ et de $G'$.

**Exemples** :

1) les groupes $(\{\pm 1\}, \times)$, $(\mathbb{Z}/2\mathbb{Z}, +)$ et $(\mathfrak{S}_2, \circ)$ sont isomorphes.
Les morphismes sont définis par

$$\begin{array}{ccccc} (\{\pm 1\}, \times) & \stackrel{\varphi_1}{\longrightarrow} & (\mathbb{Z}/2\mathbb{Z}, +) & \stackrel{\varphi_2}{\longrightarrow} & (\mathfrak{S}_2, \circ), \\ \varphi_1(1) = \dot{0},\ \varphi_1(-1) = \dot{1}, & & & & \varphi_2(\dot{0}) = Id,\ \varphi_2(\dot{1}) = \tau = (12). \end{array}$$

Etudions d'abord $\varphi_1$. pour montrer que c'est un morphisme, il suffit de vérifier que $\varphi_1(xy) = \varphi_1(x) + \varphi_1(y)$ pour tous éléments $x$ et $y$ de $\{\pm 1\}$. Ceci se réduit à

$$\varphi_1(-1) = \varphi_1(1) + \varphi_1(-1),\ \text{soit } \varphi_1(1) = \dot{0} \text{ ce qui est vrai ,}$$

et

$$\varphi_1(1) = \varphi_1(-1) + \varphi_1(-1),\ \text{soit } \dot{0} = \dot{1} + \dot{1} \text{ ce qui est vrai aussi.}$$

Pour montrer que $\varphi_2$ est un morphisme, il suffit de vérifier que $\varphi_2(x + y) = \varphi_2(x) \circ \varphi_2(y)$ pour tous éléments $x$ et $y$ de $\mathbb{Z}/2\mathbb{Z}$. La seule identité non triviale est

$$\varphi_2(\dot{1} + \dot{1}) = \varphi_2(\dot{1}) \circ \varphi_2(\dot{1}),\ \text{soit } \varphi_2(\dot{0}) = \tau \circ \tau = Id \text{ ce qui est vrai .}$$

D'autre part $\varphi_1$ et $\varphi_2$ sont bien des bijections par construction.

2) Le groupe $\mathfrak{S}_3$ est isomorphe au groupe des isométries du plan euclidien qui respectent un triangle équilatéral, appelées symétries du triangle équilatéral.

3) Dans l'exemple défini par l'équation (2.7), le noyau de $f$ s'identifie à $\mathbb{Z}/b\mathbb{Z}$ par

$$\Phi\ : \dot{\widehat{(ka)}}_n\ \mapsto \dot{k}_b, \quad k = 0, \ldots b-1.$$

**Définition des groupes cycliques** : soit $x$ un symbole, $C_n(x)$ est l'ensemble à $n$ éléments suivant :

$$C_n = \{e, x = x^1, x^2, ..., x^{n-1}\}, \tag{2.8}$$

avec la loi $x^i x^j = x^k$ où $k \equiv i + j[n]$. On l'appelle groupe cyclique d'ordre $n$ car $x^n = e$.

Il est utile de pouvoir préciser le *générateur* $x$, c'est pourquoi nous notons $C_n(x)$. Si $y$ est un autre symbole, l'application qui à $y^k$ associe $x^k$ est un isomorphisme du groupe $C_n(y)$ sur le groupe $C_n(x)$. Si bien qu'il arrive que l'on note $C_n$ et qu'on parle du groupe cyclique à $n$ éléments.

Ce groupe est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$. Un isomorphisme explicite particulier est donné par

$$f(e) = 0, \quad f(x^k) = \dot{k}, \text{ pour } k < n.$$

Montrons que $f(yz) = f(y) + f(z)$ pour tout $y, z$ dans $C_n$. En effet $y$ s'écrit comme $x^i$ et $z$ comme $x^j$, donc

$$f(yz) = f(x^i x^j) = f(x^k) = \dot{k} \text{ où } k \equiv i + j\,[n]$$

Donc $\dot{k} = \dot{i} + \dot{j} = f(y) + f(z)$.

Cette formule permet de voir $f$ comme une sorte de logarithme (de base $x$). On définit de même $C_\infty(x)$ comme étant l'ensemble $e = x^0, x = x^1, x^2, ..., x^m, ...$, avec la loi $x^i x^j = x^{i+j}$, et on l'appelle groupe *cyclique infini* (ou infini cyclique). Il est isomorphe à $(\mathbb{Z}, +)$. L'isomorphisme est encore donné par $f(x^k) = \dot{k}$.

**Définition du produit de groupes** : Si $G_1$ et $G_2$ sont des groupes (notés multiplicativement), d'éléments neutres respectifs $e_1, e_2$ on définit le *groupe produit* $G_1 \times G_2$, comme l'ensemble des paires $(g_1, g_2)$ avec l'unité $(e_1, e_2)$ et la loi $(g_1, g_2)(h_1, h_2) = (g_1 h_1, g_2 h_2)$.
Vérifions que c'est un groupe.

– Associativité :

$$\begin{aligned}
(g_1, g_2)\,((h_1, h_2)(k_1, k_2)) &= (g_1, g_2)(h_1 k_1, h_2 k_2) && \text{par définition du produit dans } G_1 \times G_2 \\
&= (g_1(h_1 k_1), g_2(h_2 k_2)) && \text{par définition du produit dans } G_1 \times G_2 \\
&= ((g_1 h_1)k_1, (g_2 h_2)k_2) && \text{par associativité dans } G_1 \text{ et dans } G_2 \\
&= (g_1 h_1, g_2 h_2)(k_1, k_2) && \text{par définition du produit dans } G_1 \times G_2 \\
&= ((g_1, g_2)(h_1, h_2))\,(k_1, k_2) && \text{par définition du produit dans } G_1 \times G_2.
\end{aligned}$$

– L'élément neutre est $(e_1, e_2)$ car

$$(g_1, g_2)(e_1, e_2) = (g_1 e_1, g_2 e_2) = (g_1, g_2) = (e_1 g_1, e_2 g_2) = (e_1, e_2)(g_1, g_2).$$

– L'inverse de $(g_1, g_2)$ est $((g_1)^{-1}, (g_2))^{-1})$

On peut bien entendu itérer la définition et définir $G_1 \times G_2 \times G_3$ etcetera, avec les triplets $(g_1, g_2, g_3)$, puis les $n$-uplets $(g_1, g_2, ..., g_n)$.

Exemples

1) $\mathbb{Z} \times \mathbb{Z}$ avec 0 et la loi $+$. C'est un réseau du plan cartésien $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ (qui lui aussi est un groupe produit).

2) Le groupe de Klein $(Z/2Z, +) \times (Z/2Z, +)$. Voir Table 2.3.

3) Le produit de deux groupes cycliques

$$C_n(x) \times C_m(y) = \{(x^i, y^j), 0 \leq i \leq n-1, 0 \leq j \leq m-1\}.$$

Notons que le groupe de Klein $(Z/2Z, +) \times (Z/2Z, +)$ est isomorphe à $C_2 \times C_2$.

**Théorème 2.6.** *Si $n$ et $m$ sont premiers entre eux, le produit $C_n(x) \times C_m(y)$ est isomorphe au groupe cyclique $C_{nm}(z)$.*

*Remarque.* Ce n'est pas vrai si $n$ et $m$ ne sont pas premiers entre eux. Pourquoi ?

*Démonstration.* Définissons une application $\varphi$ du produit $C_n \times C_m$ dans $C_{nm}$, en posant

$$\varphi(x^i, y^j) = z^k \tag{2.9}$$

où $k$ est, d'après le théorème 1.36 issu du lemme chinois, le nombre, unique modulo $nm$, tel que

$$k \equiv j\,[n], \quad k \equiv i\,[m],$$

Il est calculé ainsi : par le théorème de Bézout, il existe deux nombres entiers $u, v$ tels que $un + vm = 1$. Alors $k$ est donné par $k = iun + jvm$ compté modulo $nm$.

$\varphi$ est évidemment bijective. Or $\varphi(x^0, y^0) = z^0$ et $\varphi$ respecte la multiplication, qui correspond à l'addition des exposants. Donc $\varphi$ est un isomorphisme de groupes. C.Q.F.D.

## 2.3 Ordre des éléments d'un groupe.

**Definition 2.6.** *L'ordre d'un groupe fini* est le nombre de ses éléments. *L'ordre d'un élément* $a$ dans un groupe $G$ est le plus petit $n > 0$ tel que l'on ait $a^n = e$. Lorsque $n$ n'existe pas on dit que l'ordre de $a$ est infini et on écrit $n = \infty$.

**Exemple.** Dans $\mathfrak{S}_3$, les transpositions sont d'ordre 2, les deux cycles sont d'ordre 3 (voir Table 2.1).

Dans $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$, dont la table est

| | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | e | a |
| c | c | b | a | e |

e=(0,0)
a =(0,1)
b =(1,0)
c =(1,1)

TABLE 2.3 – Table de la loi de $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$

tous les éléments sont d'ordre 2.

Dans $(\mathbb{Z}/6\mathbb{Z}, +)$, le sous-groupe $\{0, 3\}$ est d'ordre 2, tandis que le sous-groupe $\{0, 2, 4\}$ est d'ordre 3.

**Théorème 2.7.** *Soit $a \in G$, s'il existe $m \in \mathbb{Z}, m \neq 0$ tel que $a^m = e$, alors l'ordre $n$ de $a$ est fini et il divise $m$.*

*Démonstration.* Définissons

$$M = \{k \in \mathbb{Z}, \quad a^k = e\}$$

M est un sous-groupe de $\mathbb{Z}$. Par hypothèse, $m \in M$ puisque $a^m = e$. Donc $M$ n'est pas réduit à 0. On peut donc faire appel au lemme clé moderne interprété en termes de groupes, qui dit qu'il existe un entier $n > 0$ tel que $M = n\mathbb{Z}$. Donc $m$ est un multiple de $n$ et tout autre entier $m'$ tel que $a^{m'} = e$ est dans $M$, donc multiple de $n$. Donc $n$ est le plus petit, et c'est l'ordre de $a$. C.Q.F.D.

**Théorème 2.8.** *Soit $G$ un groupe, et $a$ un élément de ce groupe ; il existe un sous-groupe $H$ de $G$ qui est contenu dans tous les sous-groupes de $G$ contenant $a$, c'est l'ensemble des puissances de $a$ : $H = \{e, a, a^2, ...a^{n-1}\}$ où $n$ est l'ordre de $a$. L'ordre de $H$ est égal à l'ordre de $a$.*

*Démonstration.* La démonstration commence par la fin. Soit $H$ l'ensemble des puissances de $H$. C'est bien un sous-groupe de $G$. Par la propriété de composi-

tion interne des sous-groupes, tout sous-groupe $H'$ de $G$ qui contient $a$ contient toutes les puissances de $a$ donc $H$. $H$ est donc le plus petit. C.Q.F.D.

**Théorème 2.9.** *Si $G$ est un groupe fini, l'ordre de tout sous-groupe $H$ divise l'ordre de $G$.*

*Démonstration.* Pour tout élément $a$ de $G$ on peut définir sa *classe à gauche modulo $H$* comme l'ensemble $aH$. Si $a$ divise $n$, alors $nH \subset aH$.
L'ensemble de ces classes forme donc une partition de $G$. donc le cardinal de $G$ est la somme des ordres de ces classes. Mais d'autre part, elles ont évidemment toutes le même ordre égal à l'ordre de $H$. Donc

$$\text{card}(G) = m\text{card}(H).$$

C.Q.F.D.

*Remarque.* L'ensemble de ces classes forme le groupe quotient de $G$ par $H$ et se note $G/H$. Si $G = \mathbb{Z}$ et $H = n\mathbb{Z}$, on trouve enfin définie la notation $\mathbb{Z}/n\mathbb{Z}$.

**Corollaire 2.10** ( Lagrange)**.** *Si $G$ est fini, l'ordre de tout élément $a$ de $G$ est fini, et divise l'ordre de $G$.*

Comme corollaire, on retrouve le théorème d'Euler et le petit théorème de Fermat.

**Théorème 2.11.** *Soit $a$ un nombre entier entre $1$ et $n-1$ ; dans le groupe additif $\mathbb{Z}/n\mathbb{Z}$, l'ordre de $a$ est $n/d$ où $d = pgcd(a, n)$.*

*Démonstration.* L'ensemble $M$ des entiers $m$ tels que $ma \equiv 0\,[n]$ forme un sous-groupe additif de $\mathbb{Z}$, il est donc de la forme $m\mathbb{Z}$ pour un nombre entier positif $m$. Par définition, l'ordre de $a$ est égal à $m$. On a $m \neq 0$ car $a \neq 0$. Puisque $d$ est le pgcd de $a$ et $n$, on a

$$a = da', \quad n = dn'.$$

Donc

$$\frac{n}{d} \times a = n \times \frac{a}{d} = n \times a' \equiv 0\,[n].$$

Par suite le nombre entier $n/d$ est dans $M$, il est donc multiple de $m$ :

$$\exists k \in \mathbb{N}^*,\ n/d = km \text{ c'est-à-dire } n = kmd.$$

D'autre part puisque $ma \equiv 0\,[n]$,

$$\exists l \in \mathbb{N}^*,\ ma = ln,$$

donc $ma = lkmd$, d'où en divisant des deux côtés par $m$, $a/d = lk$. On voit que $k$ divise $a/d$ et $n/d$ qui sont premiers entre eux, donc $k = 1$ et $m = n/d$. C.Q.F.D.

**Corollaire 2.12.** *Un élément de $(\mathbb{Z}/n\mathbb{Z}, +)$ est d'ordre $n$ si et seulement si il est premier avec $n$.*
*Un tel élément $a$ est donc un* générateur *de $(\mathbb{Z}/n\mathbb{Z}, +)$ : l'application $\varphi$ de $(C_n, \times)$ dans $(\mathbb{Z}/n\mathbb{Z}, +)$ qui envoie 1 sur 0, $x$ sur $a$ et plus généralement $x^k$ sur $ka$ est un isomorphisme de groupe. C'est encore une sorte de logarithme puisque $\varphi(xy) = \varphi(x) + \varphi(y)$ pour tous les éléments $x, y$ de $C_n$. Son inverse est une sorte d'exponentielle : $\psi(ka) = x^k$.*

**Exemples** :

1) Dans $\mathbb{Z}/6\mathbb{Z}$, seules la classe de 1 et celle de $5 \equiv -1$ sont génératrices. La classe de 2, comme celle de $4 \equiv -2$, est d'ordre 3 et celle de 3 est d'ordre 2, c'est la seule.

2) Dans $\mathbb{Z}/12\mathbb{Z}$, les générateurs sont $1, 5, 7, 11$, les éléments d'ordre 6 sont 2 et 10, ceux d'ordre 4 sont 3 et 9, ceux d'ordre 3 sont 4 et 8, et un seul est d'ordre 2, c'est 6.

3) Dans $\mathfrak{S}_3$, les transpositions sont d'ordre 2, les cycles (123) et (132) sont d'ordre 3.

4) Dans $\mathfrak{S}_4$, l'ordre de (12)(34) est 2, bien que (12)(34) ne soit pas un cycle.

5) Plus généralement, dans $\mathfrak{S}_n$, pour $n \in \mathbb{N}$, $n \geq 1$, l'ordre d'un cycle $(i_1 i_2 ... i_k)$ est égal à $k$, et l'ordre d'un produit de cycles disjoints est le ppcm des ordres de ces cycles.

6)

| $a$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ | $\dot{5}$ | $\dot{6}$ | $\dot{7}$ | $\dot{8}$ | $\dot{9}$ | $\dot{10}$ |
|---|---|---|---|---|---|---|---|---|---|---|
| $ordre(a)$ | 1 | 10 | 5 | 5 | 5 | 10 | 10 | 10 | 5 | 2 |

**Proposition 2.2.** *Soit $G, G'$ deux groupes et $a$ et $a'$ des éléments de $G$ et $G'$ respectivement, l'ordre de $(a, a')$ dans le groupe produit $G \times G'$ est le ppcm de ceux de $a$ et $a'$ lorsque ces ordres sont des nombres finis et il est infini si l'ordre de $a$ ou celui de $a'$ est infini.*

*Démonstration.* Commençons par le cas où l'ordre de $a$ est un nombre fini $n$ et celui de $a'$ un nombre fini $n'$ ; soit $m$ le plus petit nombre entier strictement positif tel que $(a, a')^m = (e, e')$, on a $a^m = e$ et $a'^m = e'$ donc $m$ est un multiple commun de $n$ et $n'$, mais le ppcm $N$ de $n, n'$ satisfait aussi à $(a, a')^N = (e, e')$ donc $m = N$. Enfin, si $a$ ou $a'$ est d'ordre infini il ne peut exister de nombre entier $m > 0$ tel que $(a, a')^m = (e, e')$, donc $(a, a')$ est d'ordre infini. C.Q.F.D.

**Proposition 2.3.** *Soit $G, G'$ deux groupes et $f$ un homomorphisme de $G$ dans $G'$. Si $a$ est un élément d'ordre fini de $G$, alors l'ordre de $f(a)$ divise l'ordre de $a$. Si $f$ est injective, alors ces ordres sont égaux.*