Algèbre abstraite

Véronique TISSOT
Monique VOUTAZ

Table des matières

Chapitre 1

La relation d'équivalence

1.1 Introduction

Des objets mathématiques aussi divers que variés, tels que nombres entiers, réels, complexes, polynômes, fonctions, droites, applications linéaires, peuvent révéler des similitudes entre objets de même nature ou de nature différente.

L'idée est alors de définir des concepts plus abstraits, plus généraux, permettant d'unifier, d'assimiler ces similitudes et ceci suivant deux directions différentes :

- généralisation de l'*égalité* : notion de relation d'équivalence sur un ensemble, illustrée par l'étude des entiers modulo n ;
- généralisation des *opérations d'addition et multiplication*, définies sur des ensembles abstraits, mettant en évidence la structure algébrique (de calcul) commune à différents ensembles d'objets mathématiques.

1.2 Définitions et propriétés

Deux triangles, deux sous-ensembles peuvent être considérés comme égaux, eu égard respectivement à leur similitude et à leurs nombres d'éléments ; la notion de relation d'équivalence donne un point de vue unificateur de ces deux exemples.

Définition 1
Soit A un ensemble.
- Toute *relation* $\mathcal{R}$ sur A est la donnée d'un sous-ensemble $\mathcal{E}$ de $A \times A$.
- Pour a et b appartenant à A :
  on dit que a est en *relation* avec b si et seulement si $(a; b) \in \mathcal{E}$.
- On note : $a \mathcal{R} b \iff (a; b) \in \mathcal{E}$.

Exemple 1
$A = \{x;\, y;\, z\}$
$\mathcal{E} = \{(x\,;x),\, (y\,;z),\, (x\,;z)\} \subset A \times A$
Alors par définition :
$x\,\mathcal{R}\,x,\ y\,\mathcal{R}\,z$ et $x\,\mathcal{R}\,z\,.$

Exemple 2
$A = \mathbb{R}$

$\mathcal{E} = \{(x;\, y) \in \mathbb{R}^2 \,|\, x < y\} \subset \mathbb{R}^2$

On a : $x\,\mathcal{R}\,y \iff x < y$

Définition 2
Une relation $\mathcal{R}$ sur un ensemble A est dite d'*équivalence* si et seulement si elle satisfait les propriétés suivantes :

a) $\mathcal{R}$ est *réflexive* : $\forall\, a \in A : a\,\mathcal{R}\,a$,
b) $\mathcal{R}$ est *symétrique* : $\forall\, a,\, b \in A : a\,\mathcal{R}\,b \implies b\,\mathcal{R}\,a$,
c) $\mathcal{R}$ est *transitive* : $\forall\, a,\, b,\, c \in A : a\,\mathcal{R}\,b$ et $b\,\mathcal{R}\,c \implies a\,\mathcal{R}\,c$.

La relation d'équivalence $\mathcal{R}$ est alors notée : $\sim$

Intuitivement : $a \sim b$ signifie que relativement à cette relation, a et b sont *égaux*.

Définition 3
Soit $\sim$ une relation d'équivalence (ou équivalence) sur un ensemble A et $a \in A$ fixé.

On appelle *classe d'équivalence de a*, notée $\bar{a}$, l'ensemble des éléments de A équivalents à a :

$$\bar{a} = \{x \in A \,|\, x \sim a\}$$

L'élément a est un *représentant* de la classe $\bar{a}$.

Exemple 3
Le parallélisme est une relation d'équivalence sur les droites du plan ; la classe d'équivalence d'une droite donnée contient toutes les droites parallèles à celle-ci.

Exemple 4
$A = \mathbb{Z} : x \sim y \iff \exists\, l \in \mathbb{Z},\quad x - y = 2l$

Alors $\sim$ est une relation d'équivalence sur $\mathbb{Z}$.

Détermination des classes d'équivalence définies par cette relation :

- Soit $a \in \mathbb{Z}$ fixé et $a = 2k, \quad k \in \mathbb{Z}$:

  $x \sim a \iff x - a = 2l, \quad l \in \mathbb{Z}$

  $\iff \quad x = a + 2l = 2(k + l) = 2k', \quad k' \in \mathbb{Z}$

  Ainsi :
  $\bar{a} = \{x \in \mathbb{Z} | \, x \sim a\} = \{x \in \mathbb{Z} | \, x \text{ est pair}\} = \{... - 6, -4, -2, 0, 2, ...\}$
- Soit $b \in \mathbb{Z}$ fixé et $b = 2k + 1, \; k \in \mathbb{Z}$:

  $x \sim b \iff x - b = 2l, \quad l \in \mathbb{Z}$

  $\iff \quad x = b + 2l = 2k + 1 + 2l = 2k' + 1, \quad k' \in \mathbb{Z}$

  Ainsi :
  $\bar{b} = \{x \in \mathbb{Z} | \, x \sim b\} = \{x \in \mathbb{Z} | \, x \text{ est impair}\} = \{... - 5, -3, -1, 1, 3, ...\}$

Or n'importe quel élément a pair et b impair peuvent être choisis comme représentant de sa classe d'équivalence. On choisit généralement le représentant le plus simple ; dans ce cas : $a = 0$ et $b = 1$. Il y a donc deux classes d'équivalence :

$$\overline{0} = \{... - 6, -4, -2, 0, 2, ...\} = \overline{2} = \overline{-4} = ...$$

$$\overline{1} = \{... - 5, -3, -1, 1, 3, ...\} = \overline{7} = \overline{-5} = ...$$

Les propriétés des classes d'équivalence sont énoncées par le théorème suivant.

Théorème 1
Soient $\sim$ une relation d'équivalence sur un ensemble A et $a, b \in A$.

Alors :
a) $a \in \bar{a}, \quad \forall \, a \in A$
b) $\bar{a} = \bar{b} \iff a \sim b$
c) $\bar{a} \neq \bar{b} \iff \bar{a} \cap \bar{b} = \varnothing$
d) $\bigcup \bar{a} = A$

Preuve

a) Evident car $\sim$ est réflexive : $a \sim a$.
b) • Si $\bar{a} = \bar{b}$ alors par (a), $a \in \bar{b}$ et donc $a \sim b$.
  • Si $a \sim b$ alors :
  $\forall \, x \in \bar{a} : \; x \sim a$
  On a alors : $x \sim a$ et $a \sim b$
  d'où, par transitivité : $x \sim b$ et donc $x \in \bar{b}$.
  Ainsi : $\bar{a} \subset \bar{b}$
  La relation étant symétrique, on a immédiatement que $\bar{b} \subset \bar{a}$.

c) • Par l'absurde, on suppose $\bar{a} \neq \bar{b}$ et $\bar{a} \cap \bar{b} \neq \varnothing$:
$\exists x \in A$ tel que $x \in \bar{a}$ et $x \in \bar{b} \iff x \sim a$ et $x \sim b$.
Alors par symétrie et transitivité : $a \sim b$ et, par (b), $\bar{a} = \bar{b}$.
• Si $\bar{a} \cap \bar{b} = \varnothing$ alors $\bar{a} \neq \bar{b}$: évident.
d) • $\bigcup \bar{a} \subset A$: évident.
• $A \subset \bigcup \bar{a}$ car si $a \in A$ alors $a \in \bar{a}$ et donc $a \in \bigcup \bar{a}$.

Définition 4
Soit $\sim$ une équivalence sur un ensemble A. L'ensemble de toutes les classes d'équivalence est appelé *ensemble quotient*. Il est noté : $A/_\sim$.

Ainsi : $A/_\sim = \{\bar{a} \,|\, a \in A\}$

L'ensemble quotient réalise, après classification, l'égalité au niveau des classes.

Remarques

- Si $\sim$ est une relation d'équivalence sur A, alors la famille des classes d'équivalence est une *partition* de A.
- Inversément, la donnée d'une partition d'un ensemble A permet de définir une équivalence $\sim$ sur A d'une façon naturelle :
$a \sim b \iff a$ et b appartiennent à la même classe de la partition
Il est alors évident que la famille des classes d'équivalence coïncident avec les classes de la partition.

Exemple 5
$A = \mathbb{Z}$: $x \sim y \iff \exists l \in \mathbb{Z}, \quad x - y = 2l$

On a vu que :

$\overline{0} = \{... - 6, -4, -2, 0, 2, ...\}$

$\overline{1} = \{... - 5, -3, -1, 1, 3, ...\}$

Alors : $\overline{0} \cap \overline{1} = \emptyset$
$\overline{0} \cup \overline{1} = \mathbb{Z}$

$\mathbb{Z}/_\sim = \{\overline{0}, \overline{1}\}$

$\mathbb{Z}/_\sim$ est un ensemble à deux éléments.

Chapitre 2

Entiers modulo n

2.1 Généralités

La *congruence modulo* n est une généralisation du dernier exemple.

Définition 5
Soient : $n \in \mathbb{N}, n \geq 2$ et $a, b \in \mathbb{Z}$.

On dit que a est *congru à* b *modulo* n si et seulement si n est un diviseur de $a - b$.

On note : $a \equiv b \pmod{n} \iff \exists\, k \in \mathbb{Z},\ a - b = kn$

Il est évident que cette relation est une équivalence sur $\mathbb{Z}$.

Exemple 6
- $2 \equiv 5 \pmod{3}$ car $5 - 2 = 1 \cdot 3$
- $-4 \equiv 20 \pmod{6}$ car $-4 - 20 = -4 \cdot 6 = -24$
- $21832 \equiv 32 \pmod{100}$ car $21832 - 32 = 218 \cdot 100$

Le théorème suivant montre comment décrire l'ensemble quotient noté $\mathbb{Z}_n$.

Théorème 2
Soient : $a, b \in \mathbb{Z}, n \in \mathbb{N}$ et $n \geq 2$.

$a \equiv b \pmod{n}$ si et seulement si a et b admettent le même reste lors de la division par n.

Preuve

- Par hypothèse : $a \equiv b \pmod{n} \iff b - a = kn, k \in \mathbb{Z}$
  Soit $r > 0$ le reste de la division de a par n :
  $$b - a = kn \qquad k \in \mathbb{Z}$$
  $$a = nq_1 + r \qquad 0 \leq r \leq n-1$$
  D'où :
  $$b = a + kn = nq_1 + r + kn =$$
  $$= n(q_1 + k) + r = nl + r, \quad l \in \mathbb{Z} \text{ et } 0 \leq r \leq n-1$$
  Ainsi b a le même reste que a lors de la division par n.
- Par hypothèse, a et b ont même reste lors de la division par n c'est-à-dire :
  $$a = nq_1 + r \quad \text{et} \quad 0 \leq r \leq n-1$$
  $$b = nq_2 + r \quad \text{et} \quad 0 \leq r \leq n-1$$
  D'où par soustraction :
  $a - b = n(q_1 - q_2), \quad q_1 - q_2 \in \mathbb{Z}$
  $a - b = nl, \quad l \in \mathbb{Z}$
  $\iff$
  $a \equiv b \pmod{n}$

Il en résulte que toute classe d'équivalence, pour cette relation, est caractérisée par la valeur du reste lors de la division par n d'un élément a de $\mathbb{Z}$.

Ce reste peut prendre n valeurs distinctes positives : 0, 1, 2, ..., $n-1$.

L'ensemble $\mathbb{Z}_n$ comporte donc n éléments :

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$$

Définition 6
L'ensemble quotient $\mathbb{Z}_n$ est appelé *l'ensemble des entiers modulo n*, et toute classe de $\mathbb{Z}_n$ est appelée *classe résiduelle (ou reste) modulo n.*

Exemple 7
Soit $n = 4 : a \equiv b \pmod 4 \iff a - b = 4k,\ k \in \mathbb{Z}$

Les restes possibles lors de la division par 4 sont : 0, 1, 2 ou 3. On a donc :

$$\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$$

Détermination des éléments des classes d'équivalence de cette relation : $a, b \in \mathbb{Z}$ sont dans la même classe si et seulement si leur reste lors de la division par 4 est le même.

D'où :

- le reste est 0 : $\overline{0} = \{a \in \mathbb{Z} \,|\, a - 0 = 4k\}$
  $= \{a \in \mathbb{Z} \,|\, a = 4k\}$
  $= \{\ldots, -8, -4, 0, 4, 8, 12, \ldots\}$
- le reste est 1 : $\overline{1} = \{a \in \mathbb{Z} \,|\, a - 1 = 4k\}$
  $= \{a \in \mathbb{Z} \,|\, a = 4k + 1\}$
  $= \{\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots\}$

  On choisit toujours comme représentant d'une classe le reste positif : $\overline{1} = \overline{-11} = \overline{13} =$ etc.
- le reste est 2 : $\overline{2} = \{a \in \mathbb{Z} \,|\, a - 2 = 4k\}$
  $= \{a \in \mathbb{Z} \,|\, a = 4k + 2\}$
  $= \{\ldots, -6, -2, 2, 6, 10, 14, 16, \ldots\}$
- le reste est 3 : $\overline{1} = \{a \in \mathbb{Z} \,|\, a - 3 = 4k\}$
  $= \{a \in \mathbb{Z} \,|\, a = 4k + 3\}$
  $= \{\ldots, -9, -5, -1, 3, 7, 11, 15, \ldots\}$

Ainsi, dans $\mathbb{Z}_4$:

$\overline{41} = \overline{1}$ car $41 = 10 \cdot 4 + 1$

$\overline{-9} = \overline{3}$ car $-9 = (-3) \cdot 4 + 3$

Remarque

$\overline{0} \cap \overline{1} = \emptyset$

$\overline{2} \cap \overline{3} = \emptyset$, etc

$\overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} = \mathbb{Z}$

2.2 Opérations sur $\mathbb{Z}_n$

On peut étendre naturellement à $\mathbb{Z}_n$ les opérations d'addition et de multiplication connues sur $\mathbb{Z}$.

Définition 7
Soient $\bar{a}, \bar{b} \in \mathbb{Z}_n$; on définit sur $\mathbb{Z}_n$:
a) l'addition des classes : $\bar{a} + \bar{b} = \overline{a+b}$
b) la multiplication des classes : $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$

Lemme 1
Ces deux opérations ne dépendent pas des représentants choisis dans $\bar{a}$ et $\bar{b}$.

Preuve

Soient :
a, a_1 deux représentants de la classe $\bar{a}$, c'est-à-dire : $a, a_1 \in \bar{a}$,
b, b_1 deux représentants de la classe $\bar{b}$, c'est-à-dire : $b, b_1 \in \bar{b}$.

Par hypothèse, on a donc :

$$a \equiv a_1 \pmod{n} \iff \exists k \in \mathbb{Z},\ a - a_1 = kn$$

$$b \equiv b_1 \pmod{n} \iff \exists l \in \mathbb{Z},\ b - b_1 = ln$$

a) Montrons que $\overline{a+b} = \overline{a_1+b_1}$:

$$\begin{aligned} a+b &= a_1 + kn + b_1 + ln = \\ &= a_1 + b_1 + (k+l)n = \\ &= a_1 + b_1 + tn, \quad t \in \mathbb{Z} \end{aligned}$$

$\iff$

$(a+b) - (a_1+b_1) = tn$

$\iff$

$a + b \equiv a_1 + b_1 \pmod{n}$

$\iff$

$\overline{a+b} = \overline{a_1+b_1}$

b) Montrons que $\overline{a \cdot b} = \overline{a_1 \cdot b_1}$:

$$\begin{aligned} a \cdot b &= (a_1 + kn) \cdot (b_1 + ln) = \\ &= a_1 \cdot b_1 + a_1 ln + b_1 kn + kln^2 = \\ &= a_1 \cdot b_1 + n(a_1 l + b_1 k + kln) \\ &= a_1 \cdot b_1 + tn, \quad t \in \mathbb{Z} \end{aligned}$$

$\iff$

$a \cdot b - a_1 \cdot b_1 = tn$

$\iff$
$a \cdot b \equiv a_1 \cdot b_1 \pmod{n}$
$\iff$
$\overline{a \cdot b} = \overline{a_1 \cdot b_1}$

Exemple 8

- Dans $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$: $\overline{3}+\overline{5} = \overline{8} = \overline{2}$ car $8 = 1 \cdot 6 + 2$
  $\overline{3} \cdot \overline{4} = \overline{12} = \overline{0}$ bien que $\overline{3} \neq \overline{0}$ et $\overline{4} \neq \overline{0}$
- Dans $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$: $5 \cdot \overline{6} = \overline{6}+\overline{6}+\overline{6}+\overline{6}+\overline{6} = \overline{30} = \overline{2}$
  $\overline{2}^3 = \overline{2} \cdot \overline{2} \cdot \overline{2} = \overline{8} = \overline{1}$

Les propriétés de l'addition et de la multiplication dans $\mathbb{Z}$, telles que *commutativité*, *associativité*, *distributivité*, etc restent valables dans $\mathbb{Z}_n$.

En particulier :

$\overline{1}$ est l'*élément neutre* de la multiplication,
$\overline{0}$ est l'*élément neutre* de l'addition.

L'opposé de $\bar{a}$, noté $-\bar{a}$, est $\overline{(-a)}$ car :
$\bar{a} + \overline{(-a)} = \overline{a + (-a)} = \overline{a - a} = \overline{0}$

On peut donc définir une soustraction :
$\bar{a} - \bar{b} = \bar{a} + \overline{(-b)} = \overline{a - b}$.

Exemple 9
Dans $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$:

l'opposé de $\overline{2}$ est $\overline{(-2)}$ $\iff$ $-\overline{2} = \overline{(-2)}$

Or :
$-2 = -1 \cdot 5 + 3$ donc $\overline{(-2)} = \overline{3}$: l'opposé de $\overline{2}$ est $\overline{3}$ $\iff$ $\overline{2}+\overline{3} = \overline{5} = \overline{0}$

Cependant l'arithmétique de $\mathbb{Z}_n$ révèle une différence importante avec celle de $\mathbb{Z}$: c'est l'existence de *diviseurs de* $\overline{0}$.

Ainsi dans $\mathbb{Z}_6$: $\overline{2} \cdot \overline{3} = \overline{6}$ bien que $\overline{2} \neq \overline{0}$ et $\overline{3} \neq \overline{0}$

D'autre part, dans $\mathbb{Z}$, seuls 0 et 1 sont tels que $0^2 = 0$ et $1^2 = 1$, c'est-à-dire sont tels que : $k^2 = k$. Ce qui n'est pas le cas dans $\mathbb{Z}_n$.

Par exemple dans $\mathbb{Z}_6$:
on a bien que : $\overline{0}^2 = \overline{0}$ et $\overline{1}^2 = \overline{1}$
mais on a aussi : $\overline{3}^2 = \overline{9} = \overline{3}$ et $\overline{4}^2 = \overline{16} = \overline{4}$.

Exemples de table d'addition et de multiplication

a) de $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

b) de $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

2.3 Utilisation de $\mathbb{Z}_n$ pour des problèmes arithmétiques

Les deux exemples qui suivent vont montrer une utilisation de $\mathbb{Z}_n$ pour donner une solution à des problèmes dans $\mathbb{Z}$.

Exemple 10
Déterminer le reste de la division de 4^{119} par 9.

Il faut donc trouver $0 \leq r \leq 8$, tel que : $4^{119} \equiv r \pmod 9$

On observe que : $\overline{4}^3 = \overline{64} = \overline{1}$ et de plus : $119 = 3 \cdot 39 + 2$.

D'où : $\overline{4}^{119} = (\overline{4}^3)^{39} \cdot \overline{4}^2 = \overline{1}^{39} \cdot \overline{4}^2 = \overline{4}^2 = \overline{16} = \overline{7}$.

Ainsi : $4^{119} \equiv 7 \pmod 9$ et le reste est donc 7.

Exemple 11
Montrer le critère de divisibilité par 9 : un entier positif est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.

Soit $a \in \mathbb{N}$: $a = d_0 + d_1 \cdot 10 + d_2 \cdot 10^2 + \ldots + d_r \cdot 10^r$

$$\begin{aligned}
\text{Dans } \mathbb{Z}_9 : \quad \overline{a} &= \overline{d_0 + d_1 \cdot 10 + \ldots + d_r \cdot 10^r} = \\
&= \overline{d_0} + \overline{d_1 \cdot 10} + \ldots + \overline{d_r \cdot 10^r} = \\
&= \overline{d_0} + \overline{d_1} \cdot \overline{10} + \ldots + \overline{d_r} \cdot \overline{10}^r = \\
&= \overline{d_0} + \overline{d_1} \cdot \overline{1} + \ldots + \overline{d_r} \cdot \overline{1} = \\
&= \overline{d_0} + \overline{d_1} + \ldots + \overline{d_r} \\
&= \overline{d_0 + d_1 + \ldots + d_r}
\end{aligned}$$

Donc a et $d_0 + d_1 + \ldots + d_r$ ont même reste après division par 9. En particulier, si a est divisible par 9, $d_0 + d_1 + \ldots + d_r$ l'est aussi et inversément.

2.4 Résolution de l'équation $\overline{a} \cdot \overline{x} = \overline{b}$ dans $\mathbb{Z}_n$

On a vu que l'opposé additif de $\overline{b}$ est $\overline{-b}$ de telle manière que $\overline{a} - \overline{b} = \overline{a} + \overline{-b} = \overline{a + (-b)} = \overline{a - b}$.

Mais on ne sait rien jusqu'ici sur l'existence éventuelle d'un inverse multiplicatif dans $\mathbb{Z}_n$ pour un élément donné $\overline{a}$.

C'est-à-dire l'équation $\overline{a} \cdot \overline{x} = \overline{1}$ a-t-elle *toujours* une solution ?

Le théorème ci-après répond à la question ; la preuve donne une méthode pour trouver l'inverse de $\overline{a}$ et par suite donne la résolution de l'équation $\overline{a} \cdot \overline{x} = \overline{1}$.

Pour démontrer ce résultat, on a besoin du lemme suivant déduit de l'algorihtme d'Euclide.

Lemme 2
Soient m et n deux entiers non nuls.
On note $d = (m, n)$ leur plus grand commun diviseur.

Alors :
a) $\exists\, x, y \in \mathbb{Z}$ tels que $d = xm + yn$.
b) *Egalité de Bezout* : $d = 1 \iff \exists\, x, y \in \mathbb{Z}$ tels que $1 = xm + yn$

Preuve partielle

- On admet a).
  On remarque que les coefficients d, x et y sont déterminés grâce à l'algorithme d'Euclide.
- on montre b).
  i) si pgcd (m, n) = 1 alors $\exists x,\, y \in \mathbb{Z}$ tels que $1 = mx+ny$ par l'algorithme d'Euclide.
  ii) si $1 = mx + ny$ alors tout diviseur commun de m et n doit diviser 1, donc $d = 1$.

Théorème 3
Soient $a \in \mathbb{Z}$, $n \in \mathbb{N}$ et $n \geq 2$.

$\overline{a}$ est inversible dans $\mathbb{Z}_n \iff (a,\, n) = 1$

Preuve

- si $\overline{a}$ est inversible alors $\exists\, \overline{b} \in \mathbb{Z}_n$ tel que $\overline{a} \cdot \overline{b} = \overline{1}$ donc $ab \equiv 1 \pmod{n}$, c'est-à-dire $n \mid (1 - ab)$.
  Ainsi : $\exists\, k \in \mathbb{Z}$ tel que $1 - ab = kn$ et donc $1 = ab + kn$.
  Par le lemme 2, on en conclut que $(a, n) = 1$.
- si $(a, n) = 1$ alors par le lemme 2 : $\exists\, x,\, y \in \mathbb{Z}$ tels que $1 = xa + yn$.
  C'est-à-dire : $1 \equiv xa \pmod{n}$ et donc $\overline{1} = \overline{x} \cdot \overline{a}$.
  Ainsi $\overline{a}$ est inversible.

Exemple 12
Dans $\mathbb{Z}_{35}$, déterminer l'inverse de $\overline{a} = \overline{16}$, puis résoudre l'équation $\overline{16} \cdot \overline{x} = \overline{9}$.

- On détermine l'inverse de $\overline{16}$ dans $\mathbb{Z}_{35}$. On constate que $(16, 35) = 1$, donc l'inverse de $\overline{16}$ existe dans $\mathbb{Z}_{35}$.

  On applique l'algorithme d'Euclide : $35 = 2 \cdot 16 + 3$

  $16 = 5 \cdot 3 + 1$

  Ainsi : $1 = 16 - 5 \cdot 3$

  $= 16 - 5(35 - 2 \cdot 16)$

  $= 11 \cdot 16 - 5 \cdot 35$

  Donc : $1 - 11 \cdot 16 = -5 \cdot 35 \Leftrightarrow 11 \cdot 16 \equiv 1 \pmod{35}$

  $\Leftrightarrow \overline{11} \cdot \overline{16} = \overline{1}$

  $\Leftrightarrow \overline{11}$ est l'inverse de $\overline{16}$
- Résolution de l'équation $\overline{16} \cdot \overline{x} = \overline{9}$.
  On multiplie les deux membres de cette équation par l'inverse de $\overline{16}$ c'est-à-dire par $\overline{11}$:

$$\begin{aligned} \overline{16}\cdot\overline{11}\cdot\overline{x} &= \overline{9}\cdot\overline{11} \\ \overline{1}\cdot\overline{x} &= \overline{99} = \overline{29} \\ \overline{x} &= \overline{29} \end{aligned}$$

Exemple 13
Dans $\mathbb{Z}_{11} \times \mathbb{Z}_{11}$, résoudre le système suivant :

$$\left\{ \begin{array}{rcrcll} \overline{5}\cdot\overline{x} & + & \overline{8}\cdot\overline{y} & = & \overline{2} & (1) \\ \overline{3}\cdot\overline{x} & + & \overline{2}\cdot\overline{y} & = & \overline{1} & (2) \end{array} \right.$$

- On multiplie l'équation (2) par $\overline{4}$:

$$\left\{ \begin{array}{rcrcll} \overline{5}\cdot\overline{x} & + & \overline{8}\cdot\overline{y} & = & \overline{2} & (1) \\ \overline{x} & + & \overline{8}\cdot\overline{y} & = & \overline{4} & (2)' \end{array} \right.$$

- On soustrait les équations (1) et (2)′ en observant que, dans $\mathbb{Z}_{11}$, on a : $-\overline{2} = \overline{9}$:

$$\left\{ \begin{array}{rcrcll} & & \overline{4}\cdot\overline{x} & = & \overline{9} & (1) \\ \overline{x} & + & \overline{8}\cdot\overline{y} & = & \overline{4} & (2)' \end{array} \right.$$

- Or $(4, 11) = 1$ donc $\overline{4}$ possède un inverse dans $\mathbb{Z}_{11}$. On détermine que cet inverse est $\overline{3}$, d'où :

$$\begin{aligned} \overline{3}\cdot\overline{4}\cdot\overline{x} &= \overline{3}\cdot\overline{9} \\ \overline{12}\cdot\overline{x} &= \overline{27} \\ \overline{x} &= \overline{5} \end{aligned}$$

- On remplace dans (2) :

$$\begin{aligned} \overline{4} + \overline{2}\cdot\overline{y} &= \overline{1} \\ \overline{2}\cdot\overline{y} &= \overline{1} - \overline{4} \\ \overline{2}\cdot\overline{y} &= \overline{8} \end{aligned}$$

- Or $(2, 11) = 1$ donc $\overline{2}$ possède un inverse dans $\mathbb{Z}_{11}$. On détermine que cet inverse est $\overline{6}$, d'où :

$$\begin{aligned} \overline{6}\cdot\overline{2}\cdot\overline{y} &= \overline{6}\cdot\overline{8} \\ \overline{12}\cdot\overline{y} &= \overline{48} \\ \overline{y} &= \overline{4} \end{aligned}$$

D'où la solution du système : $(\overline{x}, \overline{y}) = (\overline{5}, \overline{4})$.

Exemple 14
Dans $\mathbb{Z} \times \mathbb{Z}$, résoudre l'équation suivante : $8x + 3y = 5$.

Ce type de problème est connu sous le nom d'équation de Diophante (entre 150 et 350 après J.-C.) : il s'agit de déterminer uniquement les solutions en nombres entiers d'une équation à deux ou plusieurs inconnues.

Géométriquement, déterminer les solutions de l'équation ci-dessus revient à chercher les couples de points à coordonnées entières se trouvant sur la droite $8x + 3y = 5$.

- On présente l'équation par exemple sous la forme : $8x = 5 - 3y$.
  Ce qui s'interprète ainsi : pour tout $y \in \mathbb{Z}$, $5 - 3y$ est un multiple de 8.
  C'est-à-dire :
$$5 - 3y \equiv 0 \pmod 8 \iff \overline{3} \cdot \overline{y} = \overline{5}$$
- Or $(3, 8) = 1$ donc $\overline{3}$ possède un inverse dans $\mathbb{Z}_8$. On détermine que cet inverse est $\overline{3}$, d'où :
$$\overline{y} = \overline{15} = \overline{7} \iff y = 7 + 8k, \ \forall k \in \mathbb{Z}$$
  et on remplace dans l'équation de départ :
$$8x = 5 - 3(7 + 8k) = -16 - 24k$$
$$x = -2 - 3k, \ \forall k \in \mathbb{Z}$$
- Les solutions sont donc les couples d'entiers suivants :
$$(x, y) = (-2 - 3k; 7 + 8k) \quad \forall k \in \mathbb{Z}$$

Remarque

Si a est un nombre réel, alors l'expression $x^2 + ax$ peut être complétée par le terme $(\frac{1}{2}a)^2$ afin d'obtenir un carré :
$$x^2 + ax + (\frac{1}{2}a)^2 = (x + \frac{1}{2}a)^2$$
On peut utiliser le même procédé dans $\mathbb{Z}_n$ pour autant que $\overline{2}$ soit inversible, c'est-à-dire il faut que n soit impair.

Exemple 15
Résoudre l'équation quadratique $x^2 + \overline{3}x + \overline{9} = \overline{0}$ dans $\mathbb{Z}_{13}$.

$$x^2 + \overline{3}x + \overline{9} = \overline{0}$$
$$x^2 + \overline{3}x = -\overline{9} = \overline{4}$$

Suivant la remarque ci-dessus, on additionne $((\overline{2})^{-1} \cdot \overline{3})^2$ des deux côtés pour obtenir à gauche de l'égalité un carré :

$$x^2 + \overline{3}x + ((\overline{2})^{-1} \cdot \overline{3})^2 = \overline{4} + ((\overline{2})^{-1} \cdot \overline{3}^2)$$
$$(x + ((\overline{2})^{-1} \cdot \overline{3})^2 = \overline{4} + \overline{12}$$
$$(x + \overline{21})^2 = \overline{16}$$
$$(x + \overline{8})^2 = \overline{3}$$

En utilisant la table de multiplication de $\mathbb{Z}_{13}$, on constate que deux éléments sont tels que leur carré est $\overline{3}$, c'est-à-dire : $\overline{4}^2 = \overline{16} = \overline{3}$ et $\overline{9}^2 = \overline{81} = \overline{3}$.

Donc : $x + \overline{8} = \overline{4}$ ou $x + \overline{8} = \overline{9}$.

Ainsi les solutions sont : $x = \overline{9}$ ou $x = \overline{1}$.

Remarque

Dans cet exemple, il y a exactement deux solutions car $\overline{3}$ a deux "racines carrées" dans $\mathbb{Z}_{13}$.

Mais d'autres situations sont possibles : $\overline{3}$ n'a aucune racine carrée dans $\mathbb{Z}_7$, alors que $\overline{9}$ a six racines carrées dans $\mathbb{Z}_{27}$.

2.5 Deux théorèmes importants

L'un caractérise l'existence d'un inverse dans $\mathbb{Z}_n$ à l'aide du modulo n ou de l'existence de diviseurs de $\overline{0}$, l'autre théorème permet de prouver qu'un nombre n'est pas premier.

Théorème 4
Soit $n \geq 2$.

Les trois propriétés suivantes sont équivalentes :

(1) $\forall\, \overline{a} \in \mathbb{Z}_n$, et $\overline{a} \neq \overline{0}$: $\overline{a}$ est inversible ;
(2) dans $\mathbb{Z}_n$: si $\overline{a} \cdot \overline{b} = \overline{0}$ alors $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$;
(3) n est premier.

Preuve

Il suffit de montrer : (1) $\Longrightarrow$ (2)
(2) $\Longrightarrow$ (3)
(3) $\Longrightarrow$ (1)

Les équivalences sont alors déduites par transitivité de l'implication.

- on montre (1) $\Longrightarrow$ (2)
  par hypothèse :
  $\overline{a} \neq \overline{0}$ et $\overline{a}$ est inversible c'est-à-dire : $\exists\, \overline{c} \in \mathbb{Z}_n$, $\overline{c} \neq \overline{0}$ tel que $\overline{a} \cdot \overline{c} = \overline{1}$
  et
  $\overline{a} \cdot \overline{b} = \overline{0}$.

On multiplie des deux côtés par $\overline{c}$: $\overline{c}\cdot\overline{a}\cdot\overline{b} = \overline{c}\cdot\overline{0} = \overline{0}$

$$\overline{1}\cdot\overline{b} = \overline{0}$$

$$\overline{b} = \overline{0}$$

- on montre (2) $\Longrightarrow$ (3)
  par l'absurde on suppose :
  dans $\mathbb{Z}_n$: si $\overline{a}\cdot\overline{b} = \overline{0}$ alors $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$
  et
  n n'est pas premier.
  Ainsi par hypothèse : $n = a\cdot b$ avec $2 \leq a < n$ et $2 \leq b < n$.
  Donc, dans $\mathbb{Z}_n$: $\overline{n} = \overline{a}\cdot\overline{b}$ avec $\overline{a} \neq \overline{0}$ et $\overline{b} \neq \overline{0}$.
  On a donc simultanément :
  $(\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0})$ et $\overline{a} \neq \overline{0}$ et $\overline{b} \neq \overline{0}$: ce qui est impossible.
  Ainsi n est premier.
- on montre (3) $\Longrightarrow$ (1)
  par hypothèse : n est premier.
  $\forall\, \overline{a} \in \mathbb{Z}_n$, $\overline{a} \neq \overline{0}$ donc n ne divise pas a.
  Or n étant premier, on a : pgcd $(n, a) = 1$. Ainsi par le lemme 2 :
  $\exists\, b, c \in \mathbb{Z}$ tel que $1 = a\cdot b + c\cdot n$, c'est-à-dire : $a\cdot b \equiv 1 \pmod{n}$.
  Donc dans $\mathbb{Z}_n$: $\overline{a}\cdot\overline{b} = \overline{1}$ et ainsi $\overline{a}$ est inversible.

Exemple 16
Table de multiplication de $\mathbb{Z}_5$:

$n = 5$ est premier
$\Longleftrightarrow$
quel que soit $\overline{a}, \overline{b} \in \mathbb{Z}_5$:
si $\overline{a}\cdot\overline{b} = \overline{0}$ alors $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$
$\Longleftrightarrow$
quel que soit $\overline{a} \neq \overline{0}$, $\overline{a}$ a un inverse

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Exemple 17
Table de multiplication de $\mathbb{Z}_4$:

$n = 4$ n'est pas premier
$\Longleftrightarrow$
il existe $\overline{a}, \overline{b} \in \mathbb{Z}_4$ tels que :
$\overline{a} \cdot \overline{b} = \overline{0}$ et $\overline{a} \neq \overline{0}$ et $\overline{b} \neq \overline{0}$
$\Longleftrightarrow$
il existe $\overline{a} \neq \overline{0}, \overline{a}$ n'a pas d'inverse

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

On remarque que $\overline{2}$ n'est pas inversible ; par contre $\overline{1}$ et $\overline{3}$ le sont car $\text{pgcd}(1; 4) = 1$ et $\text{pgcd}(3; 4) = 1$.

Théorème 5
Théorème de Fermat (1601-1665)

Quel que soit $p \in \mathbb{N}$: p premier $\implies \forall\, a \in \mathbb{Z},\ a^p \equiv a \pmod{p}$

Preuve

Il s'agit de montrer que $\overline{a}^p = \overline{a}$ dans $\mathbb{Z}_p$ lorsque p est premier.

- si $\overline{a} = \overline{0}$ (c'est-à-dire a est un multiple de p) alors $\overline{0}^p = \overline{0}$: le théorème est donc vrai dans ce cas.
- si $\overline{a} \neq \overline{0}$: p étant premier, par le théorème précédent, $\overline{a}$ possède un inverse $\overline{b}$ tel que $\overline{a} \cdot \overline{b} = \overline{1}$.
  Donc :

$$\begin{aligned}
\overline{a}^p &= \overline{a} \\
\overline{a}^p \cdot \overline{b} &= \overline{a} \cdot \overline{b} \\
\overline{a}^p \cdot \overline{b} &= \overline{1} \\
\overline{a}^{p-1} \cdot \overline{a} \cdot \overline{b} &= \overline{1} \\
\overline{a}^{p-1} \cdot \overline{1} &= \overline{1} \\
\overline{a}^{p-1} &= \overline{1}
\end{aligned}$$

Ainsi lorsque $\overline{a} \neq \overline{0}$, montrer que $\overline{a}^p = \overline{a}$ est équivalent à montrer que $\overline{a}^{p-1} = \overline{1}$.
On va donc montrer cette dernière égalité.
On considère alors les éléments de $\mathbb{Z}_p$ suivants :

$$\overline{a} \cdot \overline{1},\ \overline{a} \cdot \overline{2},\ \overline{a} \cdot \overline{3},\ ...,\ \overline{a} \cdot \overline{p-1}.$$

Ils sont tous non-nuls (théorème précédent), tous distincts et tous dans $\mathbb{Z}_p$: ces éléments sont donc nécessairement $\overline{1}$, $\overline{2}$, $\overline{3}$, ..., $\overline{p-1}$ dans un certain ordre. Leurs produits sont donc les mêmes, c'est-à-dire :

$$\begin{aligned} \overline{a} \cdot \overline{1} \cdot \overline{a} \cdot \overline{2} \cdot \overline{a} \cdot \overline{3} \cdot ... \overline{a} \cdot \overline{p-1} &= \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot ... \overline{p-1} \\ \overline{a}^{p-1} \cdot \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot ... \cdot \overline{p-1} &= \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot ... \overline{p-1} \end{aligned}$$

Or $\overline{2}$, $\overline{3}$, $...\overline{p-1}$ sont inversibles donc leur produit $\overline{2} \cdot \overline{3} \cdot ... \overline{p-1}$ est inversible. En multipliant par l'inverse de ce produit, on obtient : $\overline{a}^{p-1} = \overline{1}$.

Si on se préoccupe du caractère "être premier" d'un nombre, le théorème de Fermat est inutilisable dans son énoncé direct.

On considère alors l'énoncé contraposé de ce théorème :

quel que soit $p \in \mathbb{N}$: $\quad \exists\, a \in \mathbb{Z},\ a^p \not\equiv a \pmod{p} \implies$ p n'est pas premier

Donc pour montrer que $p \in \mathbb{N}$ n'est pas premier, il suffit de montrer l'existence d'un entier a qui vérifie l'hypothèse de l'énoncé contraposé.

Exemple 18
Montrer que $p = 12$ n'est pas premier.

Il s'agit de trouver $a \in \mathbb{Z}$ tel que, modulo 12, $\overline{a}^p \neq \overline{a}$.

Pour des raisons évidentes de calcul on essaie avec $a = 10$:

$$\begin{aligned} 10^{12} - 10 &= 10(10^{11} - 1) = \\ &= 10 \cdot 99'999'999'999 = \\ &= 999'999'999'990 \end{aligned}$$

Ce nombre n'est pas divisible par 4 (car les deux derniers chiffres, ici 90, ne forme pas un nombre divisible par 4) donc il n'est pas divisible par 12.

Ainsi 12 n'est pas premier.

Chapitre 3

Notion de groupes et sous-groupes

3.1 Introduction

L'addition dans $\mathbb{Z}$, dans $\mathbb{Z}_n$, la multiplication dans $\mathbb{R}^*$, $\mathbb{Q}^*$, ou encore la multiplication des matrices carrées d'ordre n inversibles, la composition d'applications bijectives, sont des opérations ayant une structure commune justifiant l'étude d'ensembles abstraits munis d'une opération abstraite, appelés groupes. La théorie des groupes est riche en résultats applicables dans des disciplines variées telles que géométrie, analyse, physique, chimie.

3.2 Définitions et propriétés

La structure commune mentionnée dans l'introduction peut se formaliser comme suit.

Définition 8
Un *groupe* est la donnée d'un ensemble G et d'une loi de composition interne dans G, qui à tout élément $(a;b)$ de $G \times G$ associe un élément de G, noté ab, de telle sorte que les axiomes suivants soient vérifiés :

a) $(ab)c = a(bc) \qquad \forall\, a, b, c \in G$
la loi de composition est dite *associative*.
b) il existe un élément e de G tel que $\quad ea = ae \quad \forall\, a \in G$
on dit que e est élément *neutre*.
c) $\forall\, a \in G$, il existe un inverse, noté a^{-1}, tel que $\quad aa^{-1} = a^{-1}a = e$
on dit que l'élément a est *inversible*.
si de plus on a :
d) $ab = ba \quad \forall\, a, b \in G$
on dit alors que G est un groupe *commutatif* ou *abélien*.

Remarques
– l'élément ab est appelé composé de a et b ;
– on note parfois $(G; e)$ un goupe d'élément neutre e ;
– si le groupe G a un nombre fini d'éléments on dit que G est d'ordre fini.

Exemple 19
$\mathbb{Z}$ muni de l'addition et admettant 0 comme élément neutre est un groupe ; on le note : $(\mathbb{Z}; +; 0)$.

D'autres groupes additifs : $(\mathbb{Q}; +; 0)$, $(\mathbb{R}; +; 0)$, $(\mathbb{Z}_n; +; \overline{0})$, $(\mathbb{C}; +; 0)$, $(\mathbb{M}_{n\times p}; +; 0)$,

$(\mathbb{R}[x]; +; 0)$, $(\mathbb{R}^n; +; (0, \dots, 0))$, $(V; +; \vec{0})$.

Exemple 20
$\mathbb{R}^*$ muni de la multiplication et admettant 1 comme élément neutre est un groupe ; on le note : $(\mathbb{R}^*; \cdot; 1)$.

D'autres groupes multiplicatifs : $(\mathbb{C}^*; \cdot; 1)$, $(\mathbb{Q}^*; \cdot; 1)$, $(\{-1; 1\}; \cdot; 1)$, $(\{-1; 1; i; -i\}; \cdot; 1)$,
$(\mathbb{Z}_n^* = \{\bar{a} \in \mathbb{Z}_n^* \mid (a, n) = 1\}; \cdot; \overline{1})$.

Exemple 21
Soit G l'ensemble des applications bijectives d'un ensemble X dans lui-même ; G muni de la composition des applications et admettant l'identité sur X comme élément neutre est un groupe. Si $X = \{1, 2, \dots, n\}$, alors G est noté S_n et est appelé groupe symétrique de degré n ; S_n est d'ordre $n!$ et est non-commutatif.

En particulier pour $n = 3$ on peut expliciter les éléments de S_3.

Par exemple, on note par $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ la permutation qui envoie 1 sur 2, 2 sur 1 et 3 sur lui-même. Ainsi,

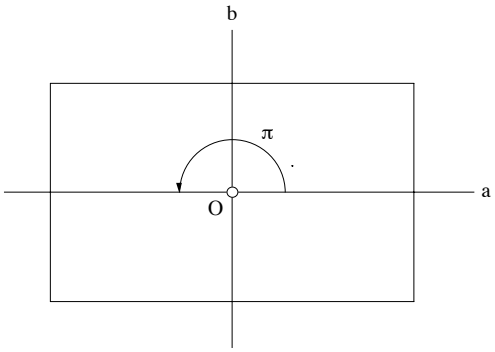
$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$ est d'ordre 6.

Exemple 22
Soit $U = \{z \in \mathbb{C} \mid |z| = 1\}$; $(\mathbb{U}; \cdot; 1)$ est le groupe commutatif du cercle.

Exemple 23
Soit $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$; $(U_n; \cdot; 1)$ est le groupe commutatif des racines n-ième de l'unité ; U_n est d'ordre n, en effet $U_n = \{\cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \mid k = 0, 1, \dots, n-1\}$.

Exemple 24
Soit N l'ensemble des matrices carrées d'ordre n, à coefficients réels et dont le déterminant est non-nul ; $(N\,;\ \cdot\ ;I_n)$ est le goupe linéaire général ; on le note $GL(n;\mathbb{R})$, il est non-commutatif.

Exemple 25
L'ensemble $\mathcal{E}$ des symétries et rotations laissant globalement invariant un rectangle est un groupe pour la composition des applications.



Les quatre éléments de $\mathcal{E}$ sont :
s_a, la symétrie d'axe a ;
s_b, la symétrie d'axe b ;
$r_{O,\pi}$ la rotation de centre O et d'amplitude π ;
$r_{O,2\pi}$ la rotation de centre O et d'amplitude 2π, cette dernière étant l'identité sur $\mathbb{R}^2$.

Par exemple :
$s_a \circ s_b = s_b \circ s_a = r_{O,\pi}$;
$r_{O,\pi}^2 = id_{\mathbb{R}^2}$;
$s_a \circ r_{O,\pi} = r_{O,\pi} \circ s_a = s_b$ etc.
$\mathcal{E}$ est un groupe commutatif d'ordre 4.

Exemple 26
On peut définir un groupe d'ordre fini par sa table de Pythagore, par exemple :

$\nearrow_{\cdot}$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$a \cdot a = b$, $a \cdot b = e$ etc.
il est facile de vérifier que $(\{e\,,a\,,b\}\,;\ \cdot\ ;e)$ est un groupe abélien.

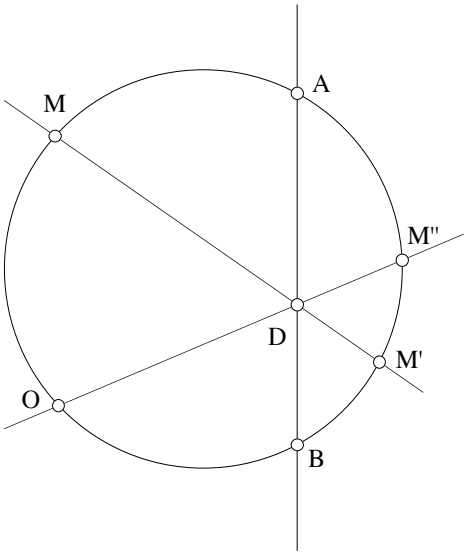
Exemple 27
On considère $\mathcal{P}(E)$ l'ensemble des parties d'un ensemble E et la différence symétrique de deux parties A et B de $\mathcal{P}(E)$ définie par : $A \triangle B = (\mathrm{C}_E A \cap B) \cup (\mathrm{C}_E B \cap A)$.
$(\mathcal{P}(E)\ ;\ \triangle\ ;\ \emptyset)$ est un groupe commutatif.

Exemple 28
Soit $\mathcal{F}$ l'ensemble des fonctions réelles à valeurs réelles qui envoient x sur x, x sur $\frac{1}{x}$, x sur $-x$ et x sur $-\frac{1}{x}$.

$(\mathcal{F}\,;\ \circ\ ;\ i_{\mathbb{R}^*})$ est un groupe abélien d'ordre 4.

Exemple 29
On considère un point O fixé sur un cercle et une droite fixée coupant le cercle en A et B. On définit une loi de composition interne sur l'ensemble $\mathcal{M}$ des points du cercle, notée $*$, qui à tout couple de points $(M; M')$ associe le point M'', unique, construit de la manière suivante :

i) la droite (MM') coupe la droite (AB) en un point D ;
ii) la droite (OD) coupe le cercle en M'', point différent de O (si (OD) est tangente au cercle $M'' \equiv O$).



On observe que la loi est associative ; de plus O est élément neutre et tout point M est inversible ; son inverse, soit M^{-1}, s'obtient par la construction suivante :

i) on considère la tangente au cercle en O ;
ii) cette tangente coupe (AB) en D ;
iii) la droite (DM) coupe le cercle en M^{-1}.

Ainsi ($\mathcal{M}$; $_*$; O) est un groupe abélien.

Il n'est pas inutile de citer quelques ensembles qui ne sont pas des groupes ; par exemple :

– Sur l'ensemble de vecteurs de $\mathbb{R}^3$ le produit vectoriel est bien une loi interne, mais celle-ci n' est pas associative et elle n'admet pas d'élément neutre.
– Sur $2\mathbb{Z}$, l'ensemble des entiers rationnels pairs, la multiplication est une loi interne associative qui n'admet pas d'élément neutre.
– Sur $\mathcal{P}(E)$, l'ensemble des parties d'un ensemble E, l'intersection est une loi interne associative qui admet E comme élément neutre, mais tout élément n'est pas inversible.

Dans un groupe , la loi de composition étant interne (stabilité), on est conduit à définir la puissance n-ième d'un élément et ceci par récurrence.

Définition 9
Soient $(G;e)$ un goupe et $n \in \mathbb{N}$; la *puissance n-ième* d'un élément a de G est définie par :

$a^0 = e \quad , \quad a^n = aa^{n-1} \quad \forall\, n \in \mathbb{N}^*$.

Les théorèmes suivants précisent les *règles de calcul*.

Théorème 6
Soient a , a_1 , a_2 ,... , a_n des éléments d'un groupe $(G;e)$.

a) e est unique.
b) a^{-1} est unique.
c) $e^{-1} = e$.
d) $(a^{-1})^{-1} = a$.
e) $(a_1\, a_2 \cdots a_n)^{-1} = {a_n}^{-1} \cdots {a_2}^{-1}\, {a_1}^{-1} \quad \forall\, n \in \mathbb{N}^*$.
f) $(a^n)^{-1} = (a^{-1})^n \quad \forall\, n \in \mathbb{N}$.

Preuves partielles

– on montre b) ;
on suppose, par l'absurde, que a admette deux inverses, soient b et b' , donc tels que $ab = ba = e$ et $ab' = b'a = e$; partons de la vérité de l'égalité $b = be$ alors $b = be \;\Leftrightarrow\; b = b(ab') \;\Leftrightarrow\; b = ba(b') \;\Leftrightarrow\; b = eb' \;\Leftrightarrow\; b = b'$;
on a à la fois $b \neq b'$ et $b = b'$, ce qui est impossible ; l'hyphothèse $b \neq b'$ est fausse, donc $b = b'$.
– on montre e) par induction sur n ;

i) l'égalité est vraie pour $n = 1$, en effet $(a_1)^{-1} = {a_1}^{-1}$;
ii) hypothèse d'induction : pour un certain n , $(a_1\, a_2 \cdots a_n)^{-1} = {a_n}^{-1} \cdots {a_2}^{-1}\, {a_1}^{-1}$;
iii) $\forall n \geq 1$; on montre que si l'égalité est vraie pour n alors elle est vraie pour $n+1$:
$({a_{n+1}}^{-1}{a_n}^{-1} \cdots {a_1}^{-1})(a_1 \cdots a_n\, a_{n+1}) = {a_{n+1}}^{-1}\,({a_n}^{-1} \cdots {a_1}^{-1})(a_1 \cdots a_n)(a_{n+1}) =$
$= {a_{n+1}}^{-1}(a_1 \cdots a_n)^{-1})(a_1 \cdots a_n)(a_{n+1}) =$
$= {a_{n+1}}^{-1} e a_{n+1} = {a_{n+1}}^{-1} a_{n+1} = e$
D'où ${a_{n+1}}^{-1}{a_n}^{-1} \cdots {a_1}^{-1} = (a_1 \cdots a_n\, a_{n+1})^{-1}$

– on montre f) comme cas particulier de e) en posant $a_1 = a_2 = \ldots = a_n = a$

Remarque

f) permet de définir a^n pour $n \in \mathbb{Z}^*_-$. On pose $n = -k \quad , \quad k \geq 1 \quad ,$ alors par définition $a^{-k} = (a^{-1})^k$.

Théorème 7
Ce théorème définit les lois *d'exponentiation* dans un groupe $(G;e)$.
a) $a^n a^m = a^{n+m} \quad \forall a \in G \quad \forall n, m \in \mathbb{Z}$
b) $(a^n)^m = a^{nm} \quad \forall a \in G \quad \forall n, m \in \mathbb{Z}$
c) soient $a, b \in G$ et $n \in \mathbb{Z}$;
si $ab = ba$ alors $(ab)^n = a^n b^n$

Preuves partielles

– On montre a) par induction sur n et pour un certain $m \in \mathbb{N}$;

i) l'égalité est vraie pour $n = 0$, en effet $a^0 a^m = ea^m = a^m = a^{0+m}$
ii) hypothèse d'induction : pour un certain n , $a^n a^m = a^{n+m}$
iii) $\forall n \geq 0$; on montre que si l'égalité est vraie pour n alors elle est vraie pour $n+1$:
$a^{n+1}a^m = (aa^n)a^m = a(a^n a^m) = a(a^{n+m}) = a^{1+(n+m)} = a^{(n+1)+m}$.

Pour $n, m \leq -1$ on utilise la définition donnée dans la remarque du théorème 6.

– On montre c) par induction sur n ;

i) l'égalité est vraie pour $n = 0$, en effet $(ab)^0 = e = ee = a^0 b^0$
ii) hypothèse d'induction : pour un certain n , $(ab)^n = a^n b^n$
iii) $\forall n \geq 0$; on montre que si l'égalité est vraie pour n alors elle est vraie pour $n+1$:
$(ab)^{n+1} = a(ba)^n b = a(ab)^n b = a(a^n b^n)b = (aa^n)(b^n b) = a^{n+1}(bb^n) = a^{n+1}b^{n+1}$.

Pour $n \leq -1$ on utilise la définition donnée dans la remarque du théorème 6.

Théorème 8
Ce théorème définit les lois de *simplification* dans un groupe $(G;e)$.

a) $ab = ac \quad \Leftrightarrow \quad b = c \quad \forall a, b, c \in G$
b) $ba = ca \quad \Leftrightarrow \quad b = c \quad \forall a, b, c \in G$

Preuve partielle

On montre a) en prouvant la proposition directe puis réciproque :
– $ab = ac \quad \Rightarrow \quad a^{-1}(ab) = a^{-1}(ac)$ car a^{-1} existe et est unique et $(x;y) \mapsto xy$ est une application.
– $b = c \quad \Rightarrow \quad ab = ac$ car $(x;y) \mapsto xy$ est une application.

Théorème 9
Soit $(G;e)$ un groupe ; l'équation $ax = b$ a une *solution unique* pour tout $a, b \in G$.

Preuve

$ax = b \quad \Leftrightarrow \quad a^{-1}ax = a^{-1}b \quad \Leftrightarrow \quad ex = a^{-1}b \quad \Leftrightarrow \quad x = a^{-1}b$; x est unique car a^{-1} est unique.

Théorème 10
Soit $(G;e)$ un groupe *d'ordre fini* ; pour tout $g \in G$ il existe $n \geq 1$ tel que $g^n = e$.

Preuve

les éléments $g^0, g^1, \ldots, g^k, \ldots$ ne peuvent pas être tous distincts, donc il existe $m \geq 0$ et $n \geq 1$ tels que $g^m = g^{m+n}$;

et on a $g^m e = g^m g^n \Leftrightarrow g^n = e$, en utilisant la loi de simplification.

Exemple 30
Dans un groupe $(G;e)$, on se propose de résoudre l'équation en x suivante :

$$ab^{-1}xb^2 = ab^n \quad , n \in \mathbb{Z}$$

$$(ab^{-1})xb^2 = ab^n \quad \Leftrightarrow \quad (ab^{-1})^{-1}(ab^{-1})xb^2 = (ab^{-1})^{-1}ab^n$$

en composant à gauche les deux membres de l'équation par l'inverse de (ab^{-1})

$$(ab^{-1})^{-1}(ab^{-1})xb^2 = (ab^{-1})^{-1}ab^n \quad \Leftrightarrow \quad xb^2 = (ba^{-1})ab^n$$

car $(ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1}$

$$xb^2 = (ba^{-1})ab^n \quad \Leftrightarrow \quad xb^2 = bb^n$$

car $a^{-1}a = e$

$$xb^2 = bb^n \quad \Leftrightarrow \quad x = b^{n+1}(b^2)^{-1}$$

en composant à droite les deux membres de l'équation par l'inverse de b^2

$$x = b^{n+1}(b^2)^{-1} \quad \Leftrightarrow \quad x = b^{n+1}b^{-2} = b^{n-1}$$

car $(b^2)^{-1} = (b^{-1})^2 = b^{-2}$

Exemple 31
Dans $(S_3\,;\circ)$ le groupe symétrique de degré 3, on se propose de résoudre l'équation en x suivante :

$$g \circ f^{126} = g \circ x \circ f^{16} \quad \text{où} \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$g \circ f^{126} = g \circ x \circ f^{16} \quad \Leftrightarrow \quad f^{126} = x \circ f^{16}$$

en composant à gauche les deux membres de l'équation par l'inverse de g

$$f^{126} = x \circ f^{16} \quad \Leftrightarrow \quad x = f^{126} \circ (f^{16})^{-1}$$

en composant à droite les deux membres de l'équation par l'inverse de f^{16}

$$x = f^{126} \circ (f^{16})^{-1} \quad \Leftrightarrow \quad x = f^{126} \circ f^{-16} = f^{110}$$

$(S_3\,;\circ)$ étant d'ordre fini, on calcule le plus petit entier positif m tel que $f^m = id_{\{1,2,3\}}$:

$f^2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \circ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$

$f^3 = f^2 \circ f = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \circ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$

Donc $f^3 = id_{\{1,2,3\}}$

D'autre part, par division euclidienne, on obtient $110 = 3 \times 36 + 2$ ce qui permet de réduire la puissance de f ainsi :

$f^{110} = (f^3)^{36} \circ f^2 = (id)^{36} \circ f^2 = f^2$

Finalement $x = f^2 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$.

Exemple 32
Soit $(U_4\,;\ \cdot\ )$; un élément de U_4 peut s'écrire $[1;\frac{n\pi}{2}]$ pour un certain $n \in \mathbb{N}$; 1 est le module du nombre complexe et $\frac{n\pi}{2}$ est son argument, celui-ci étant défini à 2π près. La table de Pythagore de ce goupe se présente ainsi :

$U_4 = \{\, [1;\frac{n\pi}{2}] \mid n = 0\,,1\,,2\,,3\,\}$

$\nearrow\cdot$	$[1;0]$	$[1;\frac{\pi}{2}]$	$[1;\pi]$	$[1;\frac{3\pi}{2}]$
$[1;0]$	$[1;0]$	$[1;\frac{\pi}{2}]$	$[1;\pi]$	$[1;\frac{3\pi}{2}]$
$[1;\frac{\pi}{2}]$	$[1;\frac{\pi}{2}]$	$[1;\pi]$	$[1;\frac{3\pi}{2}]$	$[1;0]$
$[1;\pi]$	$[1;\pi]$	$[1;\frac{3\pi}{2}]$	$[1;0]$	$[1;\frac{\pi}{2}]$
$[1;\frac{3\pi}{2}]$	$[1;\frac{3\pi}{2}]$	$[1;0]$	$[1;\frac{\pi}{2}]$	$[1;\pi]$

3.3 Sous-groupes

Certains groupes apparaissent naturellement comme sous-ensembles de groupes munis de la loi induite par ceux-ci.

Définition 10
Soit $(G : e)$ un groupe et H une partie non-vide de G ; H est un *sous-groupe* de G si et seulement si :

a) $e \in H$ — l'élément neutre de G est dans H
b) $\forall\, a, b \in H \quad , \quad ab \in H$ — stabilité de la loi dans H
c) $\forall\, a \in H \quad , \quad a^{-1} \in H$ — existence de l'inverse dans H

Remarques

– la notation $H < G$ signifie que H est un sous-groupe de G ;
– $\{e\}$ et $\{G\}$ sont appelés sous-groupes impropres de G.

Exemple 33
Trois sous-groupes additifs de $(\mathbb{C}\,;\,0)$ sont en relation de la manière suivante :

$(\mathbb{Z}\,;\,0) < (\mathbb{Q}\,;\,0) < (\mathbb{R}\,;\,0) < (\mathbb{C}\,;\,0)$.

Exemple 34
Deux sous-groupes multiplicatifs de $(\mathbb{C}^*\,;\,1)$ sont en relation de la manière suivante :

$(\mathbb{Q}^*\,;\,1) < (\mathbb{R}^*\,;\,1) < (\mathbb{C}^*\,;\,1)$.

Exemple 35
Deux autres sous-groupes multiplicatifs de $(\mathbb{C}^*\,;\,1)$ se présentent ainsi :

$(U_n\,;\,1) < (U\,;\,1) < (\mathbb{C}^*\,;\,1)$

Exemple 36
Soit $n\mathbb{Z} = \{m \in \mathbb{Z} \,|\, \exists a \in \mathbb{Z} \text{ tel que } m = na\}$ n étant un entier naturel quelconque ; $(n\mathbb{Z}\,;\,0)$ est un sous-groupe de $(\mathbb{Z}\,;\,0)$ pour l'addition.

Exemple 37
L'ensemble des homothéties du plan de centre O et rapport $k \neq 0$ est un sous-groupe du groupe des bijections du plan pour la composition des applications.

Exemple 38
L'ensemble $H = \{ A \in \mathbb{M}_n(\mathbb{R}) \,|\, \det A = 1 \}$ est un sous-groupe de $GL(n;\mathbb{R})$ pour la multiplication des matrices ; H est appelé le groupe linéaire spécial et noté $SL(n;\mathbb{R})$.

Pour caractériser un sous-groupe le théorème suivant est utile.

Théorème 11
Soit $(G;e)$ un groupe et H une partie non-vide de G ;

$$H < G \Leftrightarrow \forall a, b \in H \ , \ ab^{-1} \in H \, .$$

Preuve

On montre le théorème en prouvant la proposition directe puis réciproque :

- H étant un sous-groupe, $\forall b \in H \ , \ b^{-1} \in H$ et par la stabilité de la loi $\forall a, b \in H \ , \ ab^{-1} \in H$;
- il s'agit de prouver que H vérifie les propriétés a) à c) de la définition 10 ;
  H contient au moins un élément a et donc par hypothèse $aa^{-1} \in H$; mais $aa^{-1} = e$ ce qui prouve a) de la définition.
  $\forall a \in H$ et pour $e \in H$ on a par hypothèse $ea^{-1} = a^{-1} \in H$, ce qui prouve c) de la définition.
  $\forall a, b \in H \ , \ b^{-1} \in H$ et donc par hypothèse $a(b^{-1})^{-1} \in H$; mais $a(b^{-1})^{-1} = ab$ ce qui prouve b) de la définition.

Exemple 39
Soit $(G;e)$ un groupe abélien ;
on va montrer par le théorème 11 que $H = \{ g \in G \mid g = g^{-1} \}$ est un sous-groupe de G.

- On remarque d'abord que la condition $g = g^{-1}$ est équivalente à la condition $g^2 = e$.
- Il s'agit de montrer que $\forall g, h \in H \ , \ gh^{-1} \in H$ ou encore d'une manière équivalente que $(gh^{-1})^2 = e$.
- Soient g et h des éléments de H ;
  $(gh^{-1})^2 = g^2(h^{-1})^2 = g^2(h^2)^{-1}$ car G est abélien et $(h^{-1})^2 = (h^2)^{-1}$;
  or $g^2 = h^2 = e$, donc $(gh^{-1})^2 = ee^{-1} = ee = e$.

3.4 Groupes cycliques

Les éléments du groupe cité à l'exemple 26 ont la particularité de pouvoir s'exprimer comme puissances d'un élément fixé, en l'occurance il s'agit de a ; cette catégorie de groupes est riche en résultats intéressants et peut être définie par le théorème qui suit.

Théorème 12
Soit g un élément d'un groupe $(G; e)$; alors $H = \{ g^n \mid n \in \mathbb{Z}\}$ est un sous-groupe de G ; g est appelé un *générateur* et on dit que H est un sous-groupe *cyclique* de G *engendré* par g.

On note $H = \langle g \rangle$.

Preuve

Soient x, y des éléments de H ; il s'agit de montrer, en utilisant le critère du théorème 11, que $xy^{-1} \in H$;

$x \in H$, donc $x = g^k$; $y \in H$, donc $y = g^m$ et $y^{-1} = (g^m)^{-1} = g^{-m}$;
alors $xy^{-1} = g^k g^{-m} = g^{k-m} \in H \quad$ car $\quad (k-m) \in \mathbb{Z}$.

Exemple 40
$(\mathbb{Z}; +; 0)$ est cyclique ; 1 est générateur, -1 est également un générateur et il n'y en a pas d'autres !

$\mathbb{Z} = \{ n \cdot 1 \mid n \in \mathbb{Z} \} = \{ n(-1) \mid n \in \mathbb{Z} \}$.

Exemple 41
Soit $G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} , \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$; $(G; \cdot; I_2)$ est cyclique d'ordre 2
et $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ est le générateur unique.

$G = \left\{ \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^n \mid n \in \mathbb{Z} \right\}$.

Exemple 42
$(\mathbb{Z}_6 ; +; \overline{0})$ est cyclique d'ordre 6 ; $\overline{1}$ est un générateur, $\overline{5}$ également et ce sont les seuls !

$\mathbb{Z}_6 = \{ n\overline{1} \mid n \in \mathbb{Z} \} = \{ n\overline{5} \mid n \in \mathbb{Z} \}$.

Si $\langle g \rangle$ est fini on sait déjà qu'il existe $n \in \mathbb{Z}$ tel que $g^n = e$ on peut envisager alors le plus petit entier positif m tel que $g^m = e$.

Définition 11
Soit g un élément d'un groupe $(G;e)$; *l'ordre* de g est le plus petit entier positif m tel que $g^m = e$; on note cet ordre $|g|$.

On peut mettre en relation l'ordre d'un élément d'un groupe avec l'ordre du sous-groupe cyclique engendré par cet élément ; c'est l'objet du théorème suivant.

Théorème 13
Soit g un élément d'un groupe $(G;e)$ tel que $|g| = n$; alors $\langle g \rangle = \{e, g, \ldots, g^{n-1}\}$ est d'ordre n.

Preuve

On montre l'égalité de deux ensembles par double inclusion.
- $\{e, g, \ldots, g^{n-1}\} \subset \langle g \rangle$ par définition de $\langle g \rangle$;
- soit x un élément de $\langle g \rangle$, il existe donc $k \in \mathbb{Z}$ tel que $g^k = e$;
  alors par division euclidienne par n (avec quotient et reste), on obtient $k = nq + r$ avec $0 \leq r < n$ et on peut écrire :
  $x = g^k = (g^n)^q g^r = e^q g^r = g^r \in \{e, g, \ldots, g^{n-1}\}$
  Encore faut-il montrer que $\langle g \rangle$ est d'ordre n, donc que $e, g, \ldots, g^{n-1}$ sont tous distincts ; supposons le contraire, il existe donc k, m, tels que $0 \leq k \leq m < n$ et $g^m = g^k$, ou encore que $g^{m-k} = e$ et $0 \leq m - k < n$, ce qui contredit la minimalité de n.

Exemple 43
Soient U_5 le groupe des racines 5ème de l'unité et $g = [1 ; \frac{4\pi}{5}]$ un élément de U_5 ; l'ordre de g est 5 et $\langle g \rangle = \{g, g^2, g^3, g^4, 1\}$ est d'ordre 5 et coïncide alors avec U_5 ; on remarque que tout élément de U_5 sauf 1 peut être pris comme générateur.

Exemple 44
Soient S_3 le groupe symétrique de degré 3 et $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ un élément de S_3 ; l'ordre de g est 3 et $\langle g \rangle = \{g, g^2, 1\}$ est d'ordre 3 ; on remarque que g^2 peut être pris comme générateur.

Un groupe cyclique peut-il admettre des sous-groupes qui ne le sont pas ? La réponse est négative et le théorème suivant répond à la question.

Théorème 14
Si $(G;e)$ est cyclique, alors tout sous-groupe H de G est cyclique.

Preuve

- par hypothèse $G = \{ g^k \mid k \in \mathbb{Z} \}$ et $H < G$;
- si $H = \{e\}$, alors H est cyclique ; sinon il existe $k \in \mathbb{Z}$ et $k \neq 0$ tel que $g^k \in H$; mais puisque H est un sous-groupe, alors $(g^k)^{-1} = g^{-k}$ est aussi un élément de H ; on peut donc supposer $k > 0$.
- il est alors légitime de considérer m le plus petit entier positif tel que $g^m \in H$; il s'agit de montrer que $H = \langle g^m \rangle$, par double inclusion.
- on montre d'abord que $\langle g^m \rangle \subset H$;
  soit x un élément de $\langle g^m \rangle$, donc il existe $n \in \mathbb{Z}$ tel que $x = (g^m)^n$; or $g^m \in H$, donc $x = (g^m)^n \in H$ car la loi est stable dans H qui est un groupe.
- on montre que $H \subset \langle g^m \rangle$;
  soit x un élément de H, donc il existe $k \in \mathbb{Z}$ tel que $x = g^k$ car H est une partie de G ; on divise k par m euclidiennement et on obtient : $k = qm + r$ et $0 \leq r < m$.
  Montrons ab absurdo que r est nul ; si r est non-nul alors $r = k - qm$ avec $0 < r < m$ et on peut écrire :
  $$g^r = (g^m)^{-q} g^k$$
  Or $g^k \in H$, $g^m \in H$, $(g^m)^{-q} \in H$ et $(g^m)^{-q} g^k \in H$ car H est un groupe, ce qui contredit la minimalité de m.
  En conclusion $x = g^k = g^{qm} = (g^m)^q \in \langle g^m \rangle$.

3.5 Isomorphismes de groupes

En observant les deux groupes d'ordre 4 cités dans les exemples 25 et 28, on constate qu'on peut les assimiler, c'est-à-dire qu'il existe une bijection de l'un vers l'autre qui respecte les règles de calcul. La définition qui suit précise cette situation.

Définition 12
Soient $(G;e)$ et $(G';e')$ deux groupes munis respectivement d'une loi $*$ et d'une loi $\diamond$; G et G' sont *isomorphes* si et seulement s'il existe une bijection f de G dans G' telle que :

$$\forall\, x, y \in G, \quad f(x * y) = f(x) \diamond f(y)$$

On note $G \sim G'$.

Exemple 45
Les deux groupes multiplicatifs $(\{-1\,;\,1\}\,;\,1)$ et $(\mathbb{Z}_4^*\,;\,\overline{1})$ sont isomorphes ;
la bijection qui à 1 associe $\overline{1}$ et à -1 associe $\overline{3}$ vérifie trivialement la définition.

Exemple 46
$(\mathbb{R}_+^*\,;\,\cdot\,;1)\sim(\mathbb{R}\,;+\,;0)$ en considérant l'application log qui réalise une bijection de $\mathbb{R}_+^*$ dans $\mathbb{R}$ vérifiant :

$$\forall\, x\,, y\in\mathbb{R}_+^*\,,\quad \log(\,xy\,)=\log(\,x\,)+\log(\,y\,)$$

Exemple 47
$(\mathbb{Z}\,;+\,;0\,)\sim\left(\left\{\begin{pmatrix}1&n\\0&1\end{pmatrix}\mid n\in\mathbb{Z}\right\}\,;\,\cdot\,;I_2\right)$ en considérant l'application f définie par $f(\,n\,)=\begin{pmatrix}1&n\\0&1\end{pmatrix}$ qui réalise une bijection de $\mathbb{Z}$ dans $\left\{\begin{pmatrix}1&n\\0&1\end{pmatrix}\mid n\in\mathbb{Z}\right\}$ vérifiant :

$$\forall\, n\,, m\in\mathbb{Z}\,,\quad f(\,n+m\,)=f(\,n\,)f(\,m\,)$$

.

Exemple 48
$(\,U_n\,;\,\cdot\,;\,1\,)\sim(\,\mathbb{Z}_n\,;+\,;\,\overline{0}\,)$ en considérant l'application f définie par $f(\,\overline{k}\,)=[\,1\,;\,\frac{2k\pi}{n}\,]$ pour $k=0\,,1\,,\ldots\,,n-1\,$, qui réalise une bijection de $\mathbb{Z}_n$ dans U_n vérifiant :

$$\forall\,\overline{k}\,,\overline{i}\in\mathbb{Z}_n\,,\quad f(\,\overline{k}+\overline{i}\,)=f(\,\overline{k}\,)f(\,\overline{i}\,)\,.$$

L'isomorphisme exprime que multiplier des racines n-ièmes de l'unité revient à additionner des classes résiduelles modulo $n\,$.

Remarque

Il est intéressant de noter que tout groupe d'ordre fini est isomorphe à
un sous-groupe de $S_n\,$.

Bibliographie :

Introduction to Abstract Algebra
W. Keith Nicholson
PWS-Kent

The Fascination of Groups
F. J. Budden
Cambridge

Chapitre 4

Exercices

1. Dans chaque cas, déterminer si la relation $\mathcal{R}$ est d'équivalence sur l'ensemble A ; si oui, expliciter l'ensemble quotient $A/\sim$.
   a. $A = \{-2;\, -1;\, 0;\, 1;\, 2\}$: $\quad a \mathcal{R} b \iff a^3 - a = b^3 - b$
   b. $A = \mathbb{N}$: $\quad a \mathcal{R} b \iff a \leq b$
   c. $A = \mathbb{N}$: $\quad a \mathcal{R} b \iff \exists k \in \mathbb{N},\, b = ka$
   d. $A = \{2;\, 3;\, 4;\, 5;\, 6\}$: $\quad \mathcal{R}$ est définie par :
   $\{(2,\, 2);\, (2,\, 5);\, (3,\, 3);\, (3,\, 6);\, (4,\, 4);\, (5,\, 5);\, (5,\, 2);\, (6,\, 6);\, (6,\, 3)\}$.

2. Dans les deux cas, expliciter et représenter graphiquement la classe d'équivalence de $(3,\, -5)$ relativement aux équivalences suivantes :
   a. $A = \mathbb{R}^2$: $\quad (x,\, y) \mathcal{R} (a,\, b) \iff y - 3x = b - 3a$
   b. $A = \mathbb{R}^2$: $\quad (x,\, y) \mathcal{R} (a,\, b) \iff x^2 + y = a^2 + b$

3. Soit $U = \{1;\, 2\,; 3\}$ et $U^2 = A$.
   Sur A, on considère la relation définie ainsi :

$$(x,\, y) \mathcal{R} (a,\, b) \iff x + y = a + b.$$

   Montrer que $\mathcal{R}$ est une relation d'équivalence, expliciter les classes d'équivalence et les représenter graphiquement.

4. Les congruences suivantes sont-elles vraies ?
   a. $40 \equiv 13 \,(\mathrm{mod}\, 9)$
   b. $-29 \equiv 6 \,(\mathrm{mod}\, 7)$
   c. $8^4 \equiv 2 \,(\mathrm{mod}\, 13)$
   d. $8 \equiv 8 \,(\mathrm{mod}\, n)\,, \forall n \in \mathbb{N}^*$

5. a. Etablir les tables d'addition et de multiplication de $\mathbb{Z}_5$ et de $\mathbb{Z}_6$.

b. Quels sont les éléments de $\mathbb{Z}_8$ qui n'ont pas d'inverse multiplicatif ?

c. On note $\mathbb{Z}_n^*$ l'ensemble des éléments $\overline{p} \in \mathbb{Z}_n$ tels que p et n sont premiers entre eux : $\mathbb{Z}_n^* = \{\overline{p} \in \mathbb{Z}_n | \, (p;\, n) = 1\}$.
Déterminer les ensembles $\mathbb{Z}_5^*$, $\mathbb{Z}_8^*$ et $\mathbb{Z}_6^*$; puis etablir leurs tables de multiplication.

6. Montrer que $\overline{a}^3 = \overline{a}$ dans $\mathbb{Z}_6$, $\forall a \in \mathbb{Z}$.

7. Trouver le reste de la division de :
   a. 10^{515} par 7
   b. 8^{391} par 5

8. Montrer que :
   a. $5^{6614} - 12^{857} \equiv 1 \,(\mathrm{mod}\, 7)$
   b. $2222^{5555} + 5555^{2222} = 7k$

9. Déterminer le chiffre de l'unité décimale de :
   a. 3^{400}
   b. 3^{1027}
   c. 22^{631}

10. Montrer que, $\forall k \in \mathbb{Z}$, le chiffre de l'unité décimale de k^4 est 0, 1, 5 ou 6.

11. a. Montrer le critère de divisibilité par 6 :
    un entier n est divisible par 6 si et seulement si, en numération décimale, son chiffre des unités augmenté du quadruple de la somme de ses autres chiffres est divisible par 6.
    b. Montrer le critère de divisibilité par 4 :
    un entier n est divisible par 4 si et seulement si, en numération décimale, son chiffre des unités augmenté de 10 fois le chiffre des dizaines est divisible par 4.

12. Résoudre :
   a. $9\,x \equiv 12 \,(\mathrm{mod}\, 6)$
   b. $12 \equiv 3\,x \,(\mathrm{mod}\, 10)$
   c. $5\,x \equiv x \,(\mathrm{mod}\, 15)$
   d. $k^2 \equiv k \,(\mathrm{mod}\, 6)$

13. Dans $\mathbb{Z}_{20}$, trouver l'inverse de $\overline{11}$ et résoudre $\overline{11}\,\overline{x} = \overline{16}$.

14. Résoudre :

    a. dans $\mathbb{Z}_{11}$: $\begin{cases} \overline{3}\,\overline{x} + \overline{2}\,\overline{y} = \overline{1} \\ \overline{5}\,\overline{x} + \overline{y} = \overline{1} \end{cases}$

    b. dans $\mathbb{Z}_7$: $\begin{cases} \overline{3}\,\overline{x} + \overline{2}\,\overline{y} = \overline{1} \\ \overline{5}\,\overline{x} + \overline{y} = \overline{1} \end{cases}$

    c. dans $\mathbb{Z} \times \mathbb{Z}$: $12x + 11y - 4 = 0$

15. Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation : $5y^2 = 6x + 3$.

16. Montrer, en utilisant le théorème de Fermat, que 8 n'est pas premier.

17. a. Lesquels des ensembles suivants sont des groupes ?

    $(\mathbb{N}, +, 0)$ $(\mathbb{Q}, \cdot, 1)$
    $(\mathbb{Z}, +, 0)$ $(\mathbb{Q}^*, \cdot, 1)$
    $(\mathbb{Z}, \cdot, 1)$ $(\mathbb{R}, \cdot, 1)$
    $(\mathbb{Q}, +, 0)$

    b. Même question pour les ensembles suivants de transformations planes, munis de la composition des applications : les rotations de centre O, les translations, les homothéties de centre O et les symétries axiales.

    Pour chaque cas, précisez : le composé de deux applications, l'élément neutre éventuel et le symétrique.

    Lesquels de ces groupes sont abéliens ?

18. Soient les matrices : $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$.
    Déterminer deux matrices C et D de telle manière que $E = \{A, B, C, D\}$ soit un groupe pour la multiplication et en établir la table.

19. Dans $\mathbb{Q}$ on considère la relation d'équivalence suivante :

$$a \sim b \iff a - b \in \mathbb{Z}$$

    a. Montrer que l'on peut définer une addition dans $\mathbb{Q}/_\sim$.
    Peut-on définer une multiplication ?

    b. Montrer que $(\mathbb{Q}/_\sim; +)$ est un groupe.

20. Soit $GL(2, \mathbb{R})$ le groupe des matrices d'ordre 2 à coefficients réels de déterminant différent de zéro, muni de la multiplication.
    a. Montrer que $H = \{N \in GL(2, \mathbb{R}) \,|\, \det N = 1\}$ est un sous-groupe de $GL(2, \mathbb{R})$.
    b. Montrer que les matrices d'ordre deux qui vérifient l'équation $AA^t = I_2$ est un sous-groupe de $GL(2, \mathbb{R})$.

21. Déterminer si H est un sous-groupe de $(S_4; \circ; Id)$:
$H = \{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}; \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}; \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}\}$

Réponses

1. a. oui ; $A/\sim = \{\{-2\}; \{-1; 0; 1\}; \{-2\}\}$
   b. non
   c. non
   d. oui ; $A/\sim = \{\{4\}; \{2; 5\}; \{3; 6\}\}$

2. a. $\overline{(3; -5)} = \{(x; y) \in \mathbb{R}^2 \,|\, 3x - y - 14 = 0\}$
   b. $\overline{(3; -5)} = \{(x; y) \in \mathbb{R}^2 \,|\, y = -x^2 + 4\}$

3. $\overline{(1; 1)} = \{(1; 1)\}$
$\overline{(1; 2)} = \{(1; 2); (2; 1)\}$
$\overline{(1; 3)} = \{(1; 3); (3; 1); (2; 2)\}$
$\overline{(2; 3)} = \{(2; 3); (3; 2)\}$
$\overline{(3; 3)} = \{(3; 3)\}$

4. a. oui
   b. oui
   c. non
   d. oui

5. a. Les éléments non inversibles de $\mathbb{Z}_8$ sont $\overline{0}$, $\overline{2}$, $\overline{4}$, $\overline{6}$.
   b. $\mathbb{Z}_5^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$
   $\mathbb{Z}_6^* = \{\overline{1}, \overline{5}\}$
   $\mathbb{Z}_8^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$

7. a. $r = 5$
   b. $r = 2$

9. a. $d_0 = 1$

b. $d_0 = 7$

c. $d_0 = 8$

12. a. $x = 6k$ ou $x = 2 + 6k$ ou $x = 4 + 6k,\ k \in \mathbb{Z}$

b. $x = 4 + 10k,\ k \in \mathbb{Z}$

c. $x = 15k,\ k \in \mathbb{Z}$

d. $k = 6n$ ou $k = 1 + 6n$ ou $k = 3 + 6n$ ou $k = 4 + 6n,\ k \in \mathbb{Z}$

13. Dans $\mathbb{Z}_{20}$, l'inverse de $\overline{11}$ est $\overline{11}$.
On obtient $\overline{x} = \overline{16}$.

14. a. $(\overline{x}; \overline{y}) = (\overline{8}; \overline{5})$

b. Pas de solution

c. $(x; y) = (-7 - 11k; 8 + 12k),\ k \in \mathbb{Z}$

15. $(x; y) = (30k^2 + 30k + 7; 3 + 6k),\ k \in \mathbb{Z}$