UNIVERSITÉ DE MONCTON
EDMUNDSTON MONCTON SHIPPAGAN

# MATH 2413 - Chapitre 5: Introduction aux Structures Algébriques

Ibrahima Dione

Département de Mathématiques et de Statistique

# Sommaire

- **A** Dans ce chapitre nous nous intéressons aux structures algébriques.
- **B** La structure algébrique la plus importante est sans-doute celle de groupe.
- **C** Lorsque deux opérations sont considérées, la notion d'anneau est importante, tout comme celle de corps.

# Introduction

- Avant d'introduire, nous débutons avec deux exemples simples:
  - $(\mathbb{Z}, +)$ l'ensemble des entiers avec une opération (addition).
  - $(\mathbb{Z}, +, \times)$ l'ensemble des entiers avec deux opérations (addition et multiplication).

**Exemple 1.1:**

- Que peut-on dire de $(\mathbb{Z}, +)$?
  - C'est l'ensemble des entiers, avec une **loi de composition** binaire interne (une opération: $+$) qui associe à la paire d'éléments $a, b$ leur somme $a + b$ (l'addition).
  - De plus on peut vérifier que l'addition est associative, c'est à dire pour tous éléments $a, b$ et $c$ dans $(\mathbb{Z}, +)$ alors $(a + b) + c = a + (b + c)$.

- Qu'il y a un élément neutre 0 (c'est à dire $0 + a = a + 0$ pour chaque $a$ appartenant à $(\mathbb{Z}, +)$).

- Et pour chaque entier $a$ il y a un inverse additif $(-a)$ tel que $a + (-a) = (-a) + a = 0$.

- Et finallement l'addition est commutative, c'est à dire pour tous éléments $a$ et $b$ dans $(\mathbb{Z}, +)$ alors $a + b = b + a$.

**Note:** On dira que $(\mathbb{Z}, +)$ est un groupe commutatif (ou abélien).

**Exemple 1.2:**

- Que peut-on dire de $(\mathbb{Z}, +, \times)$?
  - C'est l'ensemble des entiers, avec deux **lois de composition** binaires internes (deux opérations : $+$ et $\times$) qui associent respectivement à la paire d'éléments $a, b$ leur somme $a + b$ (l'addition) et leur produit $a \times b$ (la multiplication).
  - Comme on a déjà observé, l'addition est associative, commutative, possède un élément neutre et chaque élément possède un inverse additif.
  - Quant à la multiplication, elle est associative, commutative, elle possède un élément neutre 1; c'est à dire $1 \times a = a \times 1 = a$ pour chaque $a$ et la multiplication est distributive par rapport à l'addition.

**Note:** On dira que $(\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire.

## Définition

Soient $(*, \wedge)$ deux lois binaires internes sur les paires d'éléments de $A$.

- On dit que les éléments de $A$ sont **commutatives** par rapport aux lois $*$ et $\wedge$, si on a respectivement:

$$a * b = b * a, \text{ pour tous } a, b \text{ dans } A,$$

$$a \wedge b = b \wedge a \text{ pour tous } a, b \text{ dans } A.$$

### Exemple 1.3:

- Considérons l'ensemble $\mathbb{Z}$, muni les lois binaires $(+, \times)$. En prenant $a = 2$ et $b = 5$, on peut constater que

$$a + b = 2 + 5 = 7 \text{ et } b + a = 5 + 2 = 7. \text{ Ainsi, } a + b = b + a.$$

$$a * b = 2 * 5 = 10 \text{ et } b * a = 5 * 2 = 10. \text{ Ainsi, } a * b = b * a$$

- On dit que les éléments de $A$ sont **associatives** par rapport aux lois $*$ et $\wedge$, si on a respectivement:

$$(a * b) * c = a * (b * c) \text{ pour tous } a, b, c \text{ dans } A,$$

$$(a \wedge b) \wedge c = a \wedge (b \wedge c) \text{ pour tous } a, b, c \text{ dans } A.$$

### Exemple 1.4:

- Dans l'ensemble $\mathbb{Z}$ muni les lois binaires $(+, \times)$, prennons encore $a = 2$, $b = 5$ et $c = 6$. On peut constater que

$$\begin{cases} (a + b) + c = (2 + 5) + 6 = 7 + 6 = 13 \\ a + (b + c) = 2 + (5 + 6) = 2 + 11 = 13 \end{cases}$$

$$\begin{cases} (a * b) * c = (2 * 5) * 6 = 10 * 6 = 60 \\ a * (b * c) = 2 * (5 * 6) = 2 * 30 = 60 \end{cases}$$

On parle de la **distributivité** de $\wedge$ sur $*$, si pour $a, b, c$ dans $A$ on a:

$$a \wedge (b * c) = (a \wedge b) * (a \wedge c),$$

$$(b * c) \wedge a = (b \wedge a) * (c \wedge a).$$

### Exemple 1.5:

- Dans l'ensemble $\mathbb{Z}$ muni les lois binaires $(+, \times)$, prennons encore $a = 2$, $b = 5$ et $c = 6$. On peut constater que

$$\begin{cases} a \times (b + c) = 2 \times (5 + 6) = 2 \times 11 = 22 \\ (a \times b) + (a \times c) = (2 \times 5) + (2 \times 6) = 10 + 12 = 22 \end{cases}$$

- La loi $*$ admet un **élément neutre**, s'il existe un élément $e$ dans $A$ tel que pour chaque $a$ dans $A$ on ait

$$a * e = e * a = a$$

- La loi $\wedge$ admet un **élément neutre**, s'il existe un élément $n$ dans $A$ tel que pour chaque $a$ dans $A$ on ait

$$a \wedge n = n \wedge a = a$$

**Exemple 1.6:**

- Dans l'ensemble $\mathbb{Z}$ muni les lois binaires $(+, \times)$, zéro est l'élément neutre de la loi additive $+$.
- Alors que un est l'élément neutre de la loi multiplicative $\times$.

- L'**inverse** d'un élément $a$ dans $A$ par rapport à la loi $*$, est l'élément $\hat{a}$ qui vérifie

$$a * \hat{a} = \hat{a} * a = e \text{ (où } e \text{ est l'élément neutre de la loi } *)$$

- L'**inverse** d'un élément $a$ dans $A$ par rapport à la loi $\wedge$, est l'élément $a^{-1}$ qui vérifie

$$a \wedge a^{-1} = a^{-1} \wedge a = n \quad (n \text{ est l'élément neutre de la loi } \wedge).$$

**Exemple 1.7:**

- ▷ Dans l'ensemble $\mathbb{Z}$ muni les lois binaires $(+, \times)$, $\hat{a} = -2$ est l'inverse de $a = 2$ par rapport à la loi additive $+$.
- ▷ Alors que $2^{-1}$ est l'élément inverse de 2 par rapport à la loi multiplicative $\times$.

## Définition

Une structure algébrique dans ce cours sera la donnée de:

- Un ensemble $A$ (par exemple $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \cdots$).
- Une loi interne binaire sur les éléments de $A$, ou deux lois internes binaires sur les éléments de $A$ (par exemple addition, multiplication, composition, $\cdots$).
- Une liste des propriétés de la loi binaire sur $A$, ou des deux lois binaires sur $A$ (commutativité, associativité, élément neutre, inverse, distributivité, $\cdots$).

# Groupes, sous-groupes

**Définition**

Un groupe $(G, *)$ est un ensemble $G$ muni d'une loi interne binaire $*$ dont:

- la loi $*$ est associative,
- il existe un élément neutre $e$ dans $G$,
- chaque élément $a$ dans $G$ a un élément inverse $\hat{a}$ dans $G$.

**Définition**

Soit $(G, *)$ un groupe. Si la loi $*$ est commutative, on dira que le groupe est abélien (abélien est synonyme de commutatif).

**Exemple 2.1:**

- $(\mathbb{Z},+), (\mathbb{Q},+)$ et $(\mathbb{R},+)$ sont des groupes abéliens (additifs).
- (les rationnels positifs, $\times$) est un groupe abélien (multiplicatif).
- (les réels positifs, $\times$) est un groupe abélien (multiplicatif).
- Appelons $\mathbb{R}[x]$ l'ensemble des polynômes à une variable réelle. $(\mathbb{R}[x],+)$ est un groupe abélien ($+$ représente l'addition des polynômes).

- La notion de sous-groupe est une notion importante très simple.
- Il s'agit simplement d'un groupe qui est inclus dans un autre groupe.

**Définition**

Soit $(A, *)$ un groupe. Si $B$ est un sous-ensemble de $A$, on dira que $(B, *)$ est un sous-groupe si les conditions suivantes sont satisfaites:

1. L'opération $*$ est fermée dans $B$, c'est à dire:

$$\text{si } x, y \in B, \text{ alors } x * y \in B.$$

2. Si $a \in B$, alors son inverse $\hat{a}$ (pour la loi $*$) est aussi dans $B$.

**Note:**

- Notez que les points $\boxed{1}$ et $\boxed{2}$ entraînent que l'élément neutre pour la loi $*$ est aussi dans $B$ car si a est dans $B$, son inverse $\hat{a}$ est dans $B$ et $a * \hat{a} = e$ est dans $B$.

- Si $(A, *)$ est un groupe, dire que $B$ est un sous-groupe de $A$ revient simplement à dire que $B \subset A$ et $(B, *)$ est un groupe.

**Exemple 2.2:**

▷ Considérons le groupe $(\mathbb{Z}, +)$. Si on considère $2\mathbb{Z}$ l'ensemble de tous les entiers pairs, alors $(2\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$.

  ⋆ En effet, $2\mathbb{Z} \subset \mathbb{Z}$, la somme des deux nombres pairs est un nombre pair ($\boxed{1}$ est vérifié),

  ⋆ et l'inverse additif d'un nombre pair est un nombre pair ($\boxed{2}$ est vérifié).

- Vous pouvez vérifier facilement que le sous ensemble des entiers impairs de $\mathbb{Z}$ n'est pas un sous-groupe de $\mathbb{Z}$ (ni 1 ni 2 ne sont satisfaits).

- On observe facilement que si $(A, *)$ est un groupe et que $e$ est son élément neutre pour la loi $*$, alors $(A, *)$ et $(\{e\}, *)$ sont des sous-groupes de $(A, *)$.

> **Note:** Ce sont les **sous-groupes triviaux** de $A$, et ils existent toujours.

# Groupes cycliques, isomorphismes

# Notation additive

- Soit $(A, +)$ un groupe avec élément neutre $0$ et élément $(-a)$ inverse de $a \in A$.
- Pour $a \in A$ et $m \in \mathbb{Z}$, l'élément $ma$ est égal à
  - $a + a + \cdots + a$ ($m$ fois) si $m$ est positif,
  - $0$ si $m$ est nul,
  - $(-a) + (-a) + \cdots + (-a)$ ($-m$ fois) si $m$ est négatif.

**Définition**

- On dira que le groupe $(A, +)$ est un **groupe cyclique** s'il existe $g \in A$ tel que pour chaque $a \in A$, il existe $m \in \mathbb{Z}$ tel que $a = mg$.
- $g$ est appelé un **générateur** du groupe $A$ et on dit que chaque élément du groupe est engendré par $g$.

# Notation multiplicative

- Soit $(A, \times)$ un groupe avec élément neutre 1 et élément $a^{-1}$ inverse de $a \in A$.

- Pour $a \in A$ et $m \in \mathbb{Z}$, l'élément $a^m$ est égal à
  - $a \times a \times \cdots \times a$ ($m$ fois) si $m$ est positif,
  - 1 si $m$ est nul,
  - $a^{-1} \times a^{-1} \times \cdots \times a^{-1}$ ($-m$ fois) si $m$ est négatif.

**Définition**

- On dira que le groupe $(A, \times)$ est un **groupe cyclique** s'il existe $g \in A$ tel que pour chaque $a \in A$, il existe $m \in \mathbb{Z}$ tel que $a = g^m$.

- $g$ est appelé un **générateur** du groupe $A$ et on dit que chaque élément du groupe est engendré par $g$.

**Exemple 3.1:**

- ▷ $(\mathbb{Z}, +)$ est un groupe cyclique (infini). 1 et $-1$ sont des générateurs. Il n'y en a pas d'autres.

- ▷ Nous introduisons maintenant la notion d'isomorphisme.

- ▷ Nous utiliserons les opérations $+$ et $\times$ pour simplifier davantage.

**Définition**

Deux groupes, $(A, +)$ et $(B, \times)$ sont **isomorphes** s'il existe une fonction $f : A \to B$ qui satisfait aux deux conditions suivantes:

- $f$ est une bijection,
- pour chaque $x, y \in A, f(x+y) = f(x) \times f(y)$.

La fonction $f$ est un isomorphisme, on dit qu'il y a un isomorphisme entre les groupes $A$ et $B$.

# Anneaux, sous-anneaux

- Les anneaux et les corps sont des ensembles dans lesquels il y a deux lois binaires internes (deux opérations).

- Pour se simplifier la vie, nous utiliserons les opérations $+$ et $\times$.

- Ce qui est conforme aux exemples avec lesquels on va travailler.

**Définition**

Soit $(A, +, \times)$ un ensemble muni de deux lois binaires internes $+$ et $\times$. On dit que $(A, +, \times)$ est un **anneau** si $(A, +)$ et un groupe commutatif et si la loi $\times$ satisfait aux conditions suivantes:

- $\times$ est associative.
- $\times$ est distributive par rapport à $+$.

**Note:**

- Si la loi $\times$ est commutative, on dit que l'anneau est **commutatif**.
- Si la loi $\times$ a un élément neutre (noté habituellement 1), on dit que l'anneau est **unitaire**.
- Si la loi $\times$ a un élément neutre et si chaque élément non nul a un inverse multiplicatif, l'anneau est appelé un **corps**.

**Exemple 4.1:**

- $(\mathbb{Z}, +, \times)$ l'ensemble des entiers, avec l'addition et la multiplication usuelles, est un anneau commutatif unitaire.
- $(\mathbb{Q}, +, \times)$ l'ensemble des nombres rationnels, avec l'addition et la multiplication usuelles, est un corps commutatif.
- $(\mathbb{R}, +, \times)$ l'ensemble des nombres réels, avec l'addition et la multiplication usuelles, est un corps commutatif.

## Définition

Si $(A, +, \times)$ est un anneau et $B \subset A$ est un sous-ensemble de $A$, on dira que $(B, +, \times)$ est un sous-anneau de $(A, +, \times)$ si $(B, +, \times)$ est un anneau.

### Exemple 4.2:

- Il est évident par exemple que $(\mathbb{Z}, +, \times)$ est un sous-anneau de $(\mathbb{Q}, +, \times)$.
- Pour $m$ entier, le sous-ensemble de $\mathbb{Z}$ formé de tous les multiples de $m$ (on notera cet ensemble $m\mathbb{Z}$) est un sous-anneau (non unitaire) de $\mathbb{Z}$.

## Questions ou commentaires? Envoyez-les à:

- Ibrahima Dione (ibrahima.dione@umoncton.ca)

- Disponibilité:
  - ⋆ Lundi 13:00 - 15:00, MRR B-214
  - ⋆ Mercredi 13H00 - 15H00, MRR B-214
  - ⋆ Jeudi 12:00 - 13:15, MRR B-214