C.T. MOLEKA BATUMBI Octave

ALGÈBRE 1

Centre de Recherche pour l'Enseignement de Mathématique
IREM
Université Pédagogique Nationale
Kinshasa-RDC

Table des matières

Bibliographie

1. Roger Godement, Cours d'Algèbre,
   Hermann, Paris, 1966.
2. Mavinga Panzu, Cours d'Algèbre
   P.U.Z-Rectorat. Kinshasa, 1978
3. A. Danedou, Structures fondamentales
   Librairie Vuibert, 1984
4. Michel Queysanne, Algèbre
   A. Colin, Paris 1971

ALGEBRE

Présentation

L'algèbre est une branche des mathématiques qui étudie la résolution d'équations à l'aide de symboles (Algèbre classique) et les structures mathématiques telles que les groupes, les anneaux et les corps, … (Algèbre moderne). L'algèbre linéaire s'intéresse à la structure d'espace vectoriel et aux notions associées.

Première partie :

- **Ensembles**
- **Relations**
- **Fonctions**
- **Familles d'ensembles**
- **Combinatoire**
- **Lois algébriques**

Chap. 1. Ensembles. Relations. Fonctions. Familles d'ensembles. Combinatoire

§1. Ensembles, Eléments

1.1. *La notion d'ensemble* est, en mathématique, une notion première (ou primitive) c'est-à-dire qu'elle n'est pas susceptible d'une définition. Intuitivement, le mot " ensemble " évoque une idée de collection, de groupement, de classe … d'objets de nature quelconque : une escadrille d'avions, une famille des pygmées, un troupeau de moutons, un banc de poissons … une école est un ensemble de classes, chaque classe étant un ensemble d'élèves.
Nous appellerons ensemble toute collection ou famille d'objets bien définies, et sera noté à l'aide de lettres majuscules A, B, C, E, X, Y, Z … Les objets constituant un ensemble sont appelés ***éléments*** de l'ensemble et seront notés à l'aide de lettres minuscules a, b, c, e, x, y, z …

L'assertion « a est un élément de E » équivalent à
« a appartient à E »
S'écrit $a \in E$
Sa négation s'écrit $a \notin E$ et se lit
« a n'appartient pas à E » ou
« a n'est pas élément de E ».

On utilise aussi les notations $E \ni a$ et $E \not\ni a$ qui se lisent respectivement : E contient a et E ne contient pas a.

1.2. **Comment définir un ensemble ?**

Deux manières sont généralement utilisées pour définir un ensemble :

a. Définition en extension de l'ensemble E

Elle s'obtient en énumérant si possible tous les éléments appartenant à E

Exemple : On écrit :
$C.E.P.G.L. = \{\text{R. D. C, Rwanda, Burundi}\}$
$A = \{0, 10, 20, 30, 40, \ldots\}$ à condition que les points de suspension … voulant dire « ainsi de suite » ne prêtent à aucune confusion quant à la détermination de l'ensemble A des entiers positifs et multiples de 10.

b. Définition en compréhension de l'ensemble E

Elle consiste à indiquer une propriété (ou des propriétés) caractéristique(s) des éléments de E.

Exemple : • L'ensemble E des étudiants de 1er gr/Math A à l'U.P.N qui ont un âge supérieur à 19 ans.
• $E = \{x/x \in \mathbb{Q} \text{ et } 0 < x < 1\}$

En général, si $\mathcal{p}$ est la propriété, on écrira
$\{x/\mathcal{p}(x)\}$

1.3. Comparaison des ensembles

a. Egalité des ensembles

Un ensemble A n'est égal à un ensemble B, ce qu'on écrit
$A = B$ et qui se lit
A et B possèdent exactement les mêmes éléments
$A = B$ si et seulement si
$\forall x, x \in A \iff x \in B$
Sinon $A \neq B$

b. Sous-ensemble. Inclusion

On dit que l'ensemble A est un sous-ensemble (une partie de l'ensemble B ou encore que :
A est inclus dans B
ce qu'on écrit : $A \subseteq B$ si et seulement si
tout élément de A est également un élément de B
$A \subseteq B$ si et seulement si
$\forall x, x \in A \implies x \in B$ (inclusion au sens large)
Sinon $A \nsubseteq B$
La notation
$B \supseteq A$ qu'on lit
B inclut A ou B admet A pour partie ou encore B est un sur-ensemble de A est aussi utilisé.
Si $A \subseteq B$ et $A \neq B$, on dit que l'inclusion est stricte et A est une partie propre de B ou A est inclus proprement dans B.
Nous écrirons quelque fois l'inclusion stricte par
$A \subset B$
Par exemple :
$\mathbb{N} = \mathbb{Z}^*$
$\mathbb{N} \subseteq \mathbb{Z}^*, \mathbb{N} \subset \mathbb{Z}, \mathbb{N} \not\subset \mathbb{N}, \mathbb{Z} \not\subset \mathbb{Z}, \mathbb{Z} \nsubseteq \mathbb{N}$
Si $A \subset B$, il est impossible d'avoir
$B \subset A$

1.4. Ensemble vide. Ensemble universel. Ensembles numériques

a. Ensemble vide

Cet ensemble, noté $\emptyset$, ne possède aucun élément.

Il se définit par l'écriture :

$\forall x, x \notin \emptyset$ Ce qui signifie : quel que soit l'objet x, x n'est pas élément de $\emptyset$.

L'ensemble vide est une partie de tout autre ensemble.

b. Ensemble universel

Dans toute application de la théorie des ensembles, les ensembles considérés sont tous des sous-ensembles d'un certain ensemble bien fixé. On dit alors de cet ensemble bien spécial qu'il est l'ensemble ***référentiel*** ou l'ensemble universel.
Nous le désignerons dans notre cours par U
Pour tout ensemble A,

$\emptyset \subseteq A \subseteq U$

Par exemple en géométrie plane, U est constitué par l'ensemble des points du plan.

c. Ensembles numériques

Ce sont les ensembles de nombres

c.1. L'ensemble $\mathbb{N}$ des nombres naturels

$\mathbb{N} = \{0,1,2, \dots, n, \dots\}$

Les éléments de $\mathbb{N}$ sont les nombres naturels ou simplement les naturels.

c.2. L'ensemble $\mathbb{Z}$ des entiers rationnels

$\mathbb{Z} = \{0,1,-1,2,-2,3,-3, \dots, n, -n, \dots\}$

Les éléments de $\mathbb{Z}$ sont des entiers rationnels

c.3. L'ensemble $\mathbb{Q}$ des nombres rationnels

$\mathbb{Q} = \left\{\frac{x}{y} \ / \ x, y \ \in \mathbb{Z} \text{ et } y \neq 0\right\}$

Ses éléments sont des nombres rationnels ou simplement des rationnels
On a :

$\forall x, x \in \mathbb{Z} \Longrightarrow x = \frac{x}{1} \in \mathbb{Q}$

D'où

$\mathbb{Z} \subseteq \mathbb{Q}$

Un nombre qui ne peut se mettre sous la forme $\frac{x}{y}$, avec $x, y \in \mathbb{Z}$ et $y \neq 0$, est un nombre irrationnel ou simplement un irrationnel

c.4. L'ensemble $\mathbb{R}$ des réels

L'ensemble $\mathbb{R}$ des réels est la réunion de l'ensemble $\mathbb{Q}$ des rationnels et de l'ensemble $\mathbb{R} \setminus \mathbb{Q}$ des irrationnels. Donc, l'ensemble $\mathbb{R} \setminus \mathbb{Q}$ des irrationnels est défini par :

$\mathbb{R} \setminus \mathbb{Q} = \{x \in \mathbb{R} / x \notin \mathbb{Q}\}$

c.5. L'ensemble $\mathbb{C}$ des nombres complexes

$\mathbb{C} = \{x + iy / x, y \in \mathbb{R}\}$

On a :

$$\forall x, x \in \mathbb{R} \Longrightarrow x = x + 0i \in \mathbb{C}$$

D'où

$$\mathbb{R} \subseteq \mathbb{C}$$

Remarque

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$
$$\mathbb{N} \neq \mathbb{Z} \neq \mathbb{Q} \neq \mathbb{R} \neq \mathbb{C}$$

1.5. Parties d'un ensemble donné. Ensemble des parties

Soit E un ensemble. L'ensemble des parties de E constituent un ensemble noté $\mathcal{P}(E)$

Par définition,

$$\mathcal{P}(E) = \{A / A \subseteq E\}$$

Autrement dit

$$A \in \mathcal{P}(E) \Leftrightarrow A \subseteq E$$

De cette façon

$\mathbb{N} \in \mathcal{P}(\mathbb{Z})$ car $\mathbb{N} \subseteq \mathbb{Z}$

$\mathbb{Z} \in \mathcal{P}(\mathbb{Z})$ car $\mathbb{Z} \subseteq \mathbb{Z}$

Si $E = \{a, \{a\}\}$, alors

$$\mathcal{P}(E) = \{\emptyset, \{a\}, \{\{a\}\}, E\}$$

Retenez en passant que lorsque le nombre d'éléments appartenant à E est n, le nombre de parties de E est 2^n

1.6. Opérations sur les ensembles

a. Réunion

La réunion de deux ensembles A et B, notée $A \cup B$, est définie par

$$A \cup B = \{x / x \in A \text{ ou } x \in B\}$$

L'ensemble $A \cup B$ se lit

« A union B »

$x \in A \cup B \Leftrightarrow x$ appartient à *au moins* un des ensembles A et B

De ce fait on a toujours

$$A \subseteq A \cup B \; ; \; B \subseteq A \cup B$$

b. Intersection

L'intersection de deux ensembles A et B, notée $A \cap B$, est définie par

$$A \cap B = \{x / x \in A \text{ et } x \in B\}$$

L'ensemble $A \cap B$ se lit

« A inter B »

Lorsque $A \cap B = \emptyset$, on dit que A et B sont disjoints

c. Différence

c.1. On définit la différence de deux ensembles A et B, notée $A \setminus B$, par

$$A \setminus B = \{x / x \in A \text{ et } x \notin B\}$$

L'ensemble $A \setminus B$, que l'on lit « A moins B », est aussi appelé ***complémentaire*** de B relativement à A.

Observez que $A \setminus B$ est toujours une partie de A, et que

$$A \setminus B = \emptyset \Leftrightarrow A \subset B$$

En outre $(A \setminus B) \cap B = \emptyset$ c'est-à-dire $A \setminus B$ et B sont disjoints

c.2. Etant donnée une partie A de l'ensemble universel U, on appelle complémentaire de A par rapport à U, l'ensemble noté $\complement_U^A$ et défini par

$$\complement_U^A = \{x / x \in U \text{ et } x \notin A\}$$

On appelle simplement complémentaire de A et on le note simplement $\complement A$ si aucune confusion n'est à craindre sur l'ensemble référentiel U

c.3. On appelle différence symétrique des ensembles A et B, l'ensemble défini par

$$A \triangle B = (A \cup B) \setminus (A \cap B)$$

On démontre que

$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$

d. Propriétés

Quels que soient les ensembles A, B et C, on a :

d.1. $A \cup B = B \cup A$ (commutativité)
$A \cap B = B \cap A$

d.2. $(A \cup B) \cup C = A \cup (B \cup C)$ (associativité)
$(A \cap B) \cap C = A \cap (B \cap C)$

d.3. $A \cup A = A$ (idempotence)
$A \cap A = A$

d.4. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (distributivité)
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

d.5. $A \cup \emptyset = A$; $A \cup U = U$
$A \cap \emptyset = \emptyset$; $A \cap U = A$
(les opérations de réunion et d'intersection ont chacune un ensemble neutre et un annulateur)

d.6. $A \cup \complement A = U$; $\complement\complement A = A$; $\complement\emptyset = U$; $A \cap \complement A = \emptyset$; $\complement U = \emptyset$

d.7. $\complement(A \cup B) = \complement A \cap \complement B$ (Lois de Morgan)
$\complement(A \cap B) = \complement A \cup \complement B$

e. Propositions

Chacune des conditions suivantes sont équivalentes

i) $A \subseteq B$

ii) $A \cap B = A$

iii) $A \cup B = B$

iv) $\complement B \subseteq \complement A$

v) $A \cap \complement B = \emptyset$

vi) $\complement A \cup B = U$

§2. Relations binaires

2.1. Couple

a. Etant donné deux objets mathématiques a et b pris dans cet ordre, on peut former un troisième objet (a, b), appelé couple a, b ou doublet a, b Soit (a', b') un autre couple, alors

$$(a, b) = (a', b') \Leftrightarrow a = a' \text{ et } b = b'$$

$$(a, b) \neq (a', b') \Leftrightarrow a \neq a' \text{ ou } b \neq b'$$

Pour un couple (a, b), a est appelé première coordonnée ou première projection du couple et b est appelé seconde coordonnée ou seconde projection du couple

b. La notion de couple s'étend de la manière suivante :
Etant donné trois objets a, b et c ;
On pose : $(a, b, c) = \big((a, b), c\big)$
et on dit que (a, b, c) est un triplet. On a :

$$(a, b, c) = (a', b', c') \Leftrightarrow a = a', b = b', c = c'$$

De même, étant donné quatre objets a, b, c et d. On pose :

$$(a, b, c, d) = \big((a, b, c), d\big)$$

et on dit que (a, b, c, d) est un quadruplet, ainsi de suite…

2.2. Produit cartésien. Ensemble produit

a. *Soient A et B deux ensembles*. Le produit cartésien (ou simplement produit) de A et B est l'ensemble noté $A \times B$ et défini par :

$$A \times B = \{(a, b)/a \in A \text{ et } b \in B\}.$$ On lit
A croix B

b. Soient A, B et C trois ensembles

$$A \times B \times C = \{(a, b, c)/a \in A, b \in B \text{ et } c \in C\}$$

c. La notion d'ensemble produit se généralise à un nombre fini n d'ensembles

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n)/a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n\}$$

C'est l'ensemble de tous les $n - uplets$ $(a_1, a_2, \dots, a_n)$ où $a_i \in A_i$; $i = 1,2, \dots, n$

En particulier

$$A \times A \times \dots \times A = \{(a_1, a_2, \dots, a_n)/a_i \in A\}$$

Généralement noté A^n. Dès lors

$\mathbb{N}^n =$ ..... $\mathbb{Q}^n =$.....

$\mathbb{R}^n =$ ..... $\mathbb{C}^n =$.....

d. Propriétés (à démontrer aux T.P)

$$(A' \subset A \; et \; B' \subset B) \Longrightarrow A' \times B' \subseteq A \times B$$

$$A \times B = \emptyset \Leftrightarrow A = \emptyset \text{ ou } B = \emptyset$$

$$A \times (B \cap C) = (A \times B) \cap (A \times C)$$

$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$

$$(C \neq \emptyset \text{ et } A \times C = B \times C) \Longrightarrow A = B$$

2.3. **Relation binaire définie sur** A × B

a. Définition

Une relation binaire (ou relation) $\mathcal{R}$ d'un ensemble A dans un ensemble B est une correspondance qui associe à chaque couple (a, b) de $A \times B$ une et une seule des assertions suivantes :

i) « a est lié à b », on écrit
$a \; \mathcal{R} \; b$ ou $\mathcal{R}(a, b)$ et on dit que
a est en relation $\mathcal{R}$ avec b

ii) « a n'est pas lié à b », on écrit
$a \; \not\mathcal{R} \; b$ et on dit que
a n'est pas en relation $\mathcal{R}$ avec b

Une relation d'un ensemble A dans lui-même s'appelle une relation dans A (ou une relation définie dans A)

b. Graphe d'une relation

Etant donné une relation $\mathcal{R}$ de A dans B, le graphe de $\mathcal{R}$ noté $G_{\mathcal{R}}$ est l'ensemble définie par :

$$G_{\mathcal{R}} = \{(a, b)/a \; \mathcal{R} \; b\}$$

Réciproquement, tout sous-ensemble $G_{\mathcal{R}}$ de $A \times B$ permet de définir une relation $\mathcal{R}_G$ de A dans B de la façon suivante :

$$a \; \mathcal{R}_G b \Leftrightarrow (a, b) \in G_{\mathcal{R}}$$

D'où une relation de A dans B est un sous-ensemble de $A \times B$. Le domaine et l'image d'une relation $\mathcal{R}$ de A dans B notés respectivement $Dom_{\mathcal{R}}$ et $Im_{\mathcal{R}}$ sont les ensembles

$$Dom_{\mathcal{R}} = \{a/(a, b) \in G_{\mathcal{R}}\}$$

$$Im_{\mathcal{R}} = \{b/(a, b) \in G_{\mathcal{R}}\}$$

Exemple

Considérons la relation $\mathcal{R}$ définie sur $A = \{13,8,0,1,-2,10,5,4\}$ comme suit

$a\ \mathcal{R}\ b \Leftrightarrow a - b = 5$

On a :

$9\ \mathcal{R}\ 4, 8\ \mathcal{R}\ 3, \ldots$ car $9 - 4 = 5, 8 - 3 = 5, \ldots$

$G_{\mathcal{R}} = \{(9,4), (8,3), (5,0), (10,5), (13,8), (3,-2)\}$

$Dom_{\mathcal{R}} = \{9,8,5,10,13,3\}$

$Im_{\mathcal{R}} = \{4,3,0,5,8,-2\}$

c. Relations particulières

Une relation $\mathcal{R}$ dans un ensemble E est dite

c.1. **Réflexive** si et seulement si : $\forall a \in E, a\ \mathcal{R}\ a$

c.2. **Symétrique** si et seulement si : $\forall a, b \in E, a\ \mathcal{R}\ b \Longrightarrow b\ \mathcal{R}\ a$

c.3. **Antisymétrique** si et seulement si : $\forall a, b \in E, a\ \mathcal{R}\ b$ et $b\ \mathcal{R}\ a \Longrightarrow a = b$

c.4. **Transitive** si et seulement si : $\forall a, b, c \in E, a\ \mathcal{R}\ b$ et $b\ \mathcal{R}\ c \Longrightarrow a\ \mathcal{R}\ c$

Exemples

- Dans l'ensemble $\mathcal{P}(E)$ des parties de E, la relation $\mathcal{R}$ définie par :

  $\forall A, B \in \mathcal{P}(E), A\ \mathcal{R}\ B \Leftrightarrow A \subseteq B\ \ est$

  - ❖ Réflexive. En effet, $\forall A \in \mathcal{P}(E), A \subseteq A$
  - ❖ Non symétrique car, $\forall A, B \in \mathcal{P}(E), A \subseteq B \nRightarrow B \subseteq A$
  - ❖ Antisymétrique. En effet, $\forall A, B \in \mathcal{P}(E), A \subseteq B$ et $B \subseteq A \Longrightarrow A = B$
  - ❖ Transitive. En effet, $\forall A, B, C \in \mathcal{P}(E), A \subseteq B$ et $B \subseteq C \Longrightarrow A \subseteq C$

- Dans l'ensemble T des habitants de la Terre, montrer que la relation « a est né la même année que b » est à la fois réflexive, symétrique et transitive.

d. Composition de relations

Etant donné une relation $\mathcal{R}$ de A vers B et une relation $\mathcal{S}$ de B vers C, on définit une relation $\mathcal{S} \circ \mathcal{R}$ de A vers C appelée la ***composée*** de $\mathcal{R}$ suivie de $\mathcal{S}$ par :

$a(\mathcal{S} \circ \mathcal{R}\ )c \Leftrightarrow \exists b \in B / a\ \mathcal{R}\ b$ et $b\ \mathcal{R}\ c$

L'écriture $\mathcal{S} \circ \mathcal{R}$ se lit

« $\mathcal{S}$ rond $\mathcal{R}$ » ou « $\mathcal{R}$ suivi de $\mathcal{S}$ »

e. Relation réciproque ou relation duale

Soit une relation $\mathcal{R}$ de A vers B, alors on peut définir une relation, notée $\mathcal{R}^{-1}$ ou $\mathcal{R}^*$ de B vers A de la manière suivante :

$b\ \mathcal{R}^{-1} a \Leftrightarrow a\mathcal{R}b$

Cette relation $\mathcal{R}^{-1}$ s'appelle relation réciproque (ou relation duale) de $\mathcal{R}$.

Par exemple : si $\mathcal{R}$ est la relation définie de $A = \{0,2,3,8,6,18\}$ vers $B = \{0,1,2,4,9,100\}$ par $a\,\mathcal{R}\,b \iff a$ est le double de b. Alors $\mathcal{R}^{-1}$ de B vers A sera définie par :

$b\,\mathcal{R}^{-1}a \iff b$ est la moitié de a et

$G_{\mathcal{R}^{-1}} = \{(0,0), (1,2), (4,8), (9,18)\}$

2.4. Relation d'ordre

a. Définitions

i. On appelle **relation d'ordre** dans un ensemble E toute relation dans E à la fois réflexive, antisymétrique et transitive

Exemple

La relation $\subseteq$ dans $\mathcal{P}(E)$ est une relation d'ordre.

Notation

Une relation d'ordre est souvent noté $\leq$ et sa réciproque $\geq$

ii. Un **ensemble ordonné** est un couple $(E, \leq)$ composé d'un ensemble E et d'une relation d'ordre sur cet ensemble.

iii. Soient $(E, \leq)$ un ensemble ordonné et a, b deux éléments de E. On dit que a et b sont **comparables** si l'on a :

$$a \leq b \text{ ou } b \leq a$$

iv. Un ensemble ordonné $(E, \leq)$ est dit **totalement ordonné** si

$$\forall a, b \in E, a \leq b \text{ ou } b \leq a$$

Exemple : $(\mathbb{R}, \leq)$ est un ensemble totalement ordonné.

b. Eléments remarquables dans un ensemble ordonné E

i. Soit $(E, \leq)$ un ensemble ordonné. On dit qu'un élément $a_0 \in E$ est un **plus petit élément** (ou élément minimum) de E si et seulement si

$$\forall x \in E, a_0 \leq x$$

ii. De même un élément $b_0 \in E$ est un **plus grand élément** (ou élément maximum) de E si et seulement si

$$\forall x \in E, x \leq b_0$$

Exemples

$(\mathbb{N}, \leq)$, 0 est le plus petit élément.

$(\mathcal{P}(E), \subseteq)$ admet $\emptyset$ comme plus petit élément et E comme plus grand élément.

L'ensemble $(\mathbb{Z}, \leq)$ n'a ni plus petit élément ni plus grand élément

iii. Un élément m est appelé **élément maximal** dans un ensemble ordonné $(E, \leq)$ s'il n'existe pas d'élément

$x \in E / x \neq m$ et $m \leq x$. Autrement dit

$m \leq x \Longrightarrow m = x$

iv. Un élément n est dit **minimal** dans un ensemble ordonné $(E, \leq)$ lorsque
$$x \leq n \Longrightarrow n = x$$

v. Soient $(E, \leq)$ un ensemble ordonné et $A \subseteq E$. On dit que $t \in E$ est un **minorant** de A si et seulement si
$$\forall x \in A, t \leq x$$
On pose
$$\text{Min } A = \{t \in E / t \text{ minorant de } A\}$$
Si l'ensemble Min A possède un plus grand élément, on dit que cet élément est la **borne inférieure** de A et on le note inf A.

vi. Soient $(E, \leq)$ un ensemble ordonné et $A \subseteq E$. On dit que $s \in E$ est un **majorant** de A si et seulement si
$$\forall x \in A, x \leq s$$
On pose
$$\text{Maj } A = \{s \in E / s \text{ majorant de } A\}$$
Si l'ensemble Maj A possède un plus petit élément, on dit que cet élément est la **borne supérieure** de A et on le note sup A.

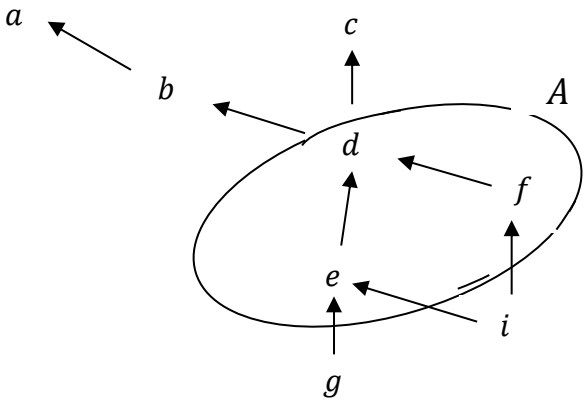
vii. On dit que A est **borné supérieurement** si A admet un majorant et **borné inférieurement** s'il admet un minorant. Si A admet à la fois un majorant et un minorant, on dit que A est **borné**.

c. Bon ordre

On dit qu'une relation d'ordre $\leq$ sur E est un **bon ordre**, ou qu'un ensemble $(E, \leq)$ est bien ordonné si toute partie non vide de E admet un plus grand élément. *Par exemple*, $(\mathbb{N}, \leq)$ est bien ordonné.

Exemple

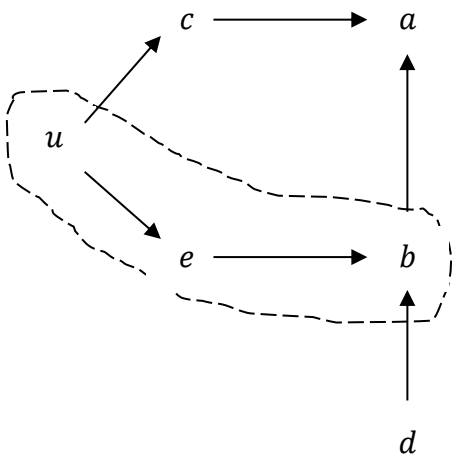
Soit $E = \{a, b, c, d, e, f, g, i\}$ un ensemble ordonné à l'aide du diagramme suivant



Soit $A = \{d, e, f\}$. Alors
Maj $A = \{a, b, c, d\}, d = \sup A \in A$
$d = \sup A \in A$: c'est le plus grand élément de A

Min $A = \{i\}$
$i = \inf A \notin A$: ce n'est pas le plus petit élément de A.
A n'a pas de plus petit élément
g et i sont les deux éléments minimaux de E
a et c sont les deux éléments maximaux de E
E n'a ni plus petit élément ni plus grand élément

Exercice
Soit $E = \{a, b, c, d, e, u\}$ muni de l'ordre $\longrightarrow$ comme indique le schéma



Trouver les éléments minimaux, maximaux
Existe-t-il un plus grand élément, un plus petit élément ?
Quels sont les majorants, les minorants de $A = \{b, e, u\}$

2.5. Relation d'équivalence

a. Définition
Une relation $\mathcal{R}$ dans un ensemble E est une relation d'équivalence si et seulement si elle est à la fois réflexive, symétrique et transitive.

b. Classes d'équivalence. Ensemble quotient

Soit $\mathcal{R}$ une relation d'équivalence dans un ensemble E.

i. On appelle **classe d'équivalence** d'un élément $a \in E$ pour la relation $\mathcal{R}$ (ou modulo $\mathcal{R}$), notée $cl(a)$ ou $[a]$ ou encore $\dot{a}$, l'ensemble
$$cl(a) = \{x / x \in E \text{ et } x \mathcal{R} a\}$$
On dira que a est le représentant de sa classe. L'écriture $cl_{\mathcal{R}}(a)$ ou $[a]_{\mathcal{R}}$ est souhaitée s'il y a crainte de confusion sur la relation de référence $\mathcal{R}$.

ii. L'ensemble des classes d'équivalence d'éléments de E, modulo $\mathcal{R}$, est appelé **ensemble quotient** de E par $\mathcal{R}$ et est noté $E/\mathcal{R}$
$$E/\mathcal{R} = \{cl(a) / a \in E\}$$

Exemple
Considérons la relation $\equiv$ suivante dans $\mathbb{Z}$

$x \equiv y \Leftrightarrow x - y$ est multiple de 5 (ou $x - y$ est divisible par 5) qui s'énonce « x est congru à y modulo 5 »

- La relation $\equiv$ est une relation d'équivalence sur $\mathbb{Z}$. Car elle est :
  Réflexive : $\forall x \in \mathbb{Z}, x \equiv x$. En effet, $x - x = 0$ multiple de 5
  Symétrique : $\forall x, y \in \mathbb{Z}, x \equiv y \Leftrightarrow y \equiv x$
  En effet, $x \equiv y \Leftrightarrow x - y = 5k, k \in \mathbb{Z}$
  $\Longrightarrow y - x = 5(-k)$ multiple de 5
  D'où $y \equiv x$
  Transitive : $\forall x, y, z \in \mathbb{Z}, x \equiv y$ et $y \equiv z \implies x \equiv z$
  En effet, $x \equiv y \Leftrightarrow x - y = 5k, k \in \mathbb{Z}$
  $y \equiv z \Leftrightarrow y - z = 5k', k' \in \mathbb{Z}$
  Alors $(x - y) + (y - z) = x - z = 5(k + k')$ multiple de 5
  D'où $x \equiv z$
- Il existe exactement 5 classes d'équivalence distinctes dans $\mathbb{Z}/\mathcal{R}$:

$A_0 = cl(0) = \{\dots, -10, -5, 0, 5, 10, \dots\} = \cdots = cl(-10) = cl(-5) = cl(0) = cl(5) = \cdots$
$A_1 = cl(1) = \{\dots, -9, -4, 1, 6, 11, \dots\} = \cdots = cl(-9) = cl(-4) = cl(1) = cl(6) = \cdots$
$A_2 = cl(2) = \{\dots, -8, -3, 2, 7, 12, \dots\} = \cdots = cl(-8) = cl(-3) = cl(2) = cl(7) = \cdots$
$A_3 = cl(3) = \{\dots, -7, -2, 3, 8, 13, \dots\} = \cdots = cl(-7) = cl(-2) = cl(3) = cl(8) = \cdots$
$A_4 = cl(4) = \{\dots, -6, -1, 4, 9, 14, \dots\} = \cdots = cl(-6) = cl(-1) = cl(4) = cl(9) = \cdots$

- Notons que
  $\forall x \in \mathbb{Z}, x = 5q + r \Longrightarrow x \in A_r$ où r est le reste de la division de x par 5
  $\forall A_r \in \mathbb{Z}/\mathcal{R}, A_r \neq \emptyset$
  $\forall A_r, A_{r'} \in \mathbb{Z}/\mathcal{R}, r \neq r' \Longrightarrow A_r \cap A_{r'} = \emptyset$

$$\mathbb{Z} = A_0 \cup A_1 \cup A_2 \cup A_3 \cup A_4 = \bigcup_{i=0}^{4} A_i$$

c. <u>Théorème</u>
Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. Alors l'ensemble quotient $E/\mathcal{R}$ est une partition de E.

d. <u>Théorème</u>
Si $\mathcal{R}$ est une relation d'équivalence dans E, alors
d.1. $\forall a \in A, a \in cl(a)$
d.2. $cl(a) = cl(b) \Leftrightarrow a \mathcal{R} b$
d.3. $cl(a) \neq cl(b) \Longrightarrow cl(a) \cap cl(b) = \emptyset$
<u>Démonstration</u>
<u>d.1.</u> Puisque $\mathcal{R}$ est réflexive, $\forall a \in E, a \mathcal{R} a$ et donc $a \in cl(a)$
<u>d.2.</u> $\Longrightarrow$: Supposons $cl(a) = cl(b)$
Alors $a \in cl(b)$ d'après *i)* et donc $a \mathcal{R} b$
$\Longleftarrow$: Supposons $a \mathcal{R} b$
Si $x \in cl(b)$, c'est-à-dire $x \mathcal{R} a$, alors $x \mathcal{R} b$ (car $a \mathcal{R} b$ et $x \mathcal{R} a$)
Ceci montre que $cl(a) \subseteq cl(b)$. Un raisonnement analogue montre que … $cl(b) \subseteq cl(a)$
<u>d.3.</u> Démontrons la contraposée c'est-à-dire :
$cl(a) \cap cl(b) \neq \emptyset \Longrightarrow cl(a) = cl(b)$

En effet, $cl(a) \cap cl(b) \neq \emptyset \Longrightarrow \exists x \in E / x \in cl(a) \cap cl(b)$
Par suite $a \mathcal{R} x$ et $x \mathcal{R} b$, donc $a \mathcal{R} b$
D'où $cl(a) = cl(b)$ d'après *ii)*

§3. Fonctions

3.1. Définition

On appelle ***fonction*** ou ***application*** de l'ensemble A dans un autre ensemble B, toute relation f de A vers B qui, à tout élément $x \in A$ associe un et un seul élément $y \in B$
L'unique élément $y \in B$ associé à $x \in A$ par la fonction f se note $f(x)$
x s'appelle variable ou argument
$f(x)$ l'image de x ou encore la valeur de f en x
A ensemble de départ ou source ou encore ensemble de définition de f
B ensemble d'arrivé ou but de f
Le ***graphe*** de la fonction f est la partie de $A \times B$ définie par

$$G_f = \{(x, f(x)) \in A \times B / x \in A\}$$

3.2. Notations

Une application f de A dans B est notée

$$f : A \longrightarrow B \text{ ou } A \xrightarrow{f} B$$

L'ensemble de toutes les applications de A dans B est noté $\mathfrak{F}(A, B)$ ou B^A

Exemple
Voici $\mathbb{N}$ ensemble des naturels
$\mathbb{P}$ ensemble des nombres pairs et la relation « a pour moitié »
C'est une simple relation lorsqu'elle est définie de $\mathbb{N}$ vers $\mathbb{P}$. Tandis qu'elle devient une fonction lorsqu'elle est définie de $\mathbb{P}$ dans $\mathbb{N}$.
On écrit :

$$f : \mathbb{P} \longrightarrow \mathbb{N} : x \longmapsto f(x) = \frac{x}{2}$$
$$G_f = \left\{\left(x, \frac{x}{2}\right) / x \in \mathbb{P}\right\}$$

3.3. Remarques importantes

a. Il faut soigneusement distinguer les symboles x, $f(x)$ et f car $x \in A$, $f(x) \in B$ et $f \in B^A$

b. Une application $f : A \longrightarrow B$ est définie par A, B et $G_f \subseteq A \times B$

3.4. Egalité

Soient deux applications $f: A \longrightarrow B$ et $g: A' \longrightarrow B'$
Alors

$$f = g \Leftrightarrow i) A = A' \text{et } B = B'$$
$$ii) \forall x \in A, f(x) = g(x) \text{ c.à.d. } G_f = G_g$$
$$f \neq g \Leftrightarrow \text{ au moins une des conditions } i) \text{ et } ii) \text{ n'est pas remplie}$$

En particulier, si f et $g \in B^A$, alors

$$f = g \Leftrightarrow \forall x \in A, f(x) = g(x)$$
$$f \neq g \Leftrightarrow \exists x \in A / f(x) \neq g(x)$$

Exemple
Soient $f : \{-2,-1,0,1,2\} \longrightarrow \mathbb{Z} : x \longmapsto f(x) = x^5 + 4x$
et $g : \{-2,-1,0,1,2\} \longrightarrow \mathbb{Z} : x \longmapsto g(x) = 5x^3$
Alors $f = g$ (pourquoi ?)

3.5. Images directes et Images réciproques

Considérons une application $f : A \longrightarrow B$
Si $S \subseteq A$, l'ensemble $f(S) = \{f(x)/x \in S\}$ est appelé image de S par f. $f(S) \subseteq B$
Si $S = A$, $f(A)$ est appelé ***image*** de f. On note : $Im\ f$
Si $T \subseteq B$, l'ensemble $f^{-1}(T) = \{x/x \in A \text{ et } f(x) \in T\}$ est appelé ***image réciproque*** de T par f. $f^{-1}(T) \subseteq A$

Exemple
Soit $f : \mathbb{Z} \longrightarrow \mathbb{N} : x \longmapsto f(x) = x^2$
Si $S = \{-4,6,-1,3,1\}$, alors $f(S) = \{16,36,1,9\}$

3.6. Restrictions et prolongements de fonctions

a. Soit $f : A \longrightarrow B, S \subseteq A$
La ***restriction*** de f au sous – ensemble S de A est la fonction notée f/S ou f_s et définie par

$$f/S : S \longrightarrow B : x \longmapsto f/S\,(x) = f(x)$$

b. Etant donné deux fonctions

$$f : A \longrightarrow B \text{ et } g : A' \longrightarrow B' \text{ avec } S \subseteq A \text{ et } S \subseteq A', \text{ on dit que } f \text{ et } g$$

coïncident sur S si

$$\forall x \in S, f(x) = g(x)$$

c. Soit $f : A \longrightarrow B, A \subseteq C$
Un ***prolongement*** (ou extension) de f à l'ensemble C est une fonction

$$g : C \longrightarrow B \text{ telle que } g/A = f$$

Exemples

1. Soient $f : \mathbb{Z} \longrightarrow \mathbb{Z} : x \longmapsto f(x) = x^3 + 2x$
et $h : S = \{0,1,2\} \longrightarrow \mathbb{Z} : x \longmapsto f(x) = 3x^2$

Alors
La fonction $f/\mathbb{N} : \mathbb{N} \longrightarrow \mathbb{Z} : x \longmapsto f_{\mathbb{N}}(x) = x^3 + 2x$ est la restriction de f au sous – ensemble $\mathbb{N}$ de $\mathbb{Z}$

2. La fonction $f : \mathbb{Z} \longrightarrow \mathbb{Z} : x \longmapsto f(x) = x^3 + 2x$ est le prolongement de la fonction h à l'ensemble $\mathbb{Z}$ car f est telle que $f/S = h$

3. La fonction $f : \mathbb{Z} \longrightarrow \mathbb{Z} : x \longmapsto f(x) = x^3 + 2x$ est aussi le prolongement de la fonction $f/\mathbb{N}$ à l'ensemble $\mathbb{Z}$
Les fonctions f et h coïncident sur S (Pourquoi ?)

3.7. Composition de fonctions

a. Définition

Soient $f : A \longrightarrow B$ et $g : B \longrightarrow C$. La composé de f et g est l'application notée $g \circ f$

$$g \circ f : A \longrightarrow C : x \longmapsto (g \circ f)(x) = g[f(x)]$$

Illustration

$$A \xrightarrow{f} B \xrightarrow{g} C \qquad A \xrightarrow{g \circ f} C$$

Exemple
Si $f : \mathbb{N} \longrightarrow \mathbb{Z} : x \longmapsto f(x) = x^3 + 2x$
Et $g : \mathbb{Z} \longrightarrow \mathbb{R} : x \longmapsto g(x) = e^x$, alors

$$\begin{aligned} g \circ f : \mathbb{N} \longrightarrow \mathbb{R} : x \longmapsto (g \circ f)(x) &= g[f(x)] \\ &= g(x^3 + 2x) \\ &= e^{x^3+2x} \end{aligned}$$

b. Théorème

Si $f : A \longrightarrow B$, alors $h \circ (g \circ f) = (h \circ g) \circ f$
$g : B \longrightarrow C$ (Vérifier aux T.P)
$h : C \longrightarrow D$

3.8. Applications injectives et surjectives

Une application
$f : A \longrightarrow B$ est dite

a. Injective (ou une injection) si et seulement si
$\forall x, y \in A, x \neq y \Longrightarrow f(x) \neq f(y)$
ou $\forall x, y \in A, f(x) = f(y) \Longrightarrow x = y$

b. Surjective (ou une surjection) si et seulement si
$\forall y \in B,\ \exists x \in A / y = f(x)$

Exemples
(1) La fonction $f : \mathbb{N} \longrightarrow \mathbb{Z} : x \longmapsto f(x) = -x$ est injective et non surjective

(2) La fonction $g : \mathbb{Z} \longrightarrow \mathbb{N} : x \longmapsto f(x) = |x|$ est surjective et non injective
(3) La fonction $h : \mathbb{Z} \longrightarrow \mathbb{Z} : x \longmapsto f(x) = |x|$ n'est ni injective ni surjective
(4) La fonction de Dirichlet $d : \mathbb{R} \longrightarrow \mathbb{R}$, définie par

$d(x) = \begin{cases} 0 \text{ si } x \in \mathbb{Q} \\ 1 \text{ si } x \in \mathbb{R} \setminus \mathbb{Q} \end{cases}$ est – elle injective ? surjective ?

(5) La fonction $\ell : \mathbb{N} \longrightarrow \mathbb{N}$ définie par

$\ell(x) = \begin{cases} \frac{x}{2} \text{ si } x \text{ est pair} \\ \frac{x-1}{2} \text{ si } x \text{ est impair est surjective et non injective} \end{cases}$

(Justifier ces exemples)

3.9. Applications bijectives

Une application
$f : A \longrightarrow B$ est dite bijective (ou une bijection) si et seulement si elle est à la fois injective et surjective.
Autrement dit
f est bijective $\Leftrightarrow \forall y \in B, \exists! x \in A / y = f(x)$

Exemple
La fonction
$f : \mathbb{Z} \longrightarrow \mathbb{Z} : x \longmapsto f(x) = -x$ est une bijection

a. Proposition
Si $f : A \longrightarrow B$ est une bijection, la relation réciproque
$f^{-1} : B \longrightarrow A$, appelée aussi ***inverse*** de f, est une application

Démonstration
D'après la définition de la bijection
$\forall y \in B, \exists! x \in A / y = f(x)$ Cette propriété définit la relation f^{-1} de B sur A, qui à tout $y \in B$ fait correspondre l'élément $x \in A$, dont y est l'image par f.
On écrit alors $x = f^{-1}(y)$.
Réciproquement, si la relation inverse f^{-1} d'une application est une application, alors f est bijective.

b. Proposition
Si $f : A \longrightarrow B$ est une bijection, alors la fonction inverse
$f^{-1} : B \longrightarrow A$ est une bijection
Démonstration
f étant une application, on a :
$\forall x \in A, \exists! y \in B / y = f(x)$. Donc $x = f^{-1}(y)$ ce qui montre que f^{-1} est surjective
En outre, deux éléments distincts y et y' correspondent aux éléments x et x' distincts de A. Ce qui montre que f^{-1} est injective.

3.10. Applications particulières

a. Pour tout ensemble A, il existe une application notée Id_A ou 1_A
$id_A : A \longrightarrow A : x \longmapsto id_A(x) = x$ et appelée ***identité*** sur A

b. Si $A \subseteq B$, l'application
$i : A \longrightarrow B : x \longmapsto i(x) = x$ s'appelle ***injection canonique*** ou inclusion d'une partie A de B dans B

c. Soient deux ensembles A et B, $B \neq \emptyset$. $\forall b \in B$, il existe une fonction notée C_b
$C_b : A \longrightarrow B : x \longmapsto C_b(x) = b, \quad \forall x \in A$. On l'appelle ***application constante***.

d. Si $\mathcal{R}$ est une relation d'équivalente sur un ensemble E, on définit une application
$\mathcal{s} : E \longrightarrow E/\mathcal{R} : x \longmapsto \mathcal{s}(x) = \dot{x}$
$\mathcal{s}$ est une surjection et est appelée ***surjection canonique***.

e. Soient A et B deux ensembles. L'application notée
$Pr_1 : A \times B \longrightarrow B : (x, y) \longmapsto Pr_1(x, y) = x$ est la fonction appelée ***1ère projection canonique***. De même on définit
$Pr_2 : A \times B \longrightarrow B : (x, y) \longmapsto Pr_2(x, y) = y$. C'est la fonction ***2ème projection canonique***.

f. Soit E un ensemble et A une de ses parties. L'application
$\varphi_A : E \longrightarrow \{0,1\}$ définie par
$\varphi_A(x) = \begin{cases} 1 \text{ si } x \in A \\ 0 \text{ si } x \in E - A \end{cases}$ est appelée ***fonction caractéristique*** de la partie A de E.

g. Proposition
Soient $f : A \longrightarrow B$ une fonction et $S \subseteq A$
$i : S \longrightarrow A$ injection canonique
Alors $f_S : i \circ f$
En effet :
$f_S(x) = (i \circ f)(x) = i[f(x)] = f(x)$
Décomposition canonique d'une application.

3.11. Fonctions de plusieurs variables

On parle de fonctions de plusieurs variables quand l'ensemble de départ est un produit cartésien ou contenu dans un tel produit.

a. Si l'ensemble de départ est le produit cartésien $A_1 \times A_2$ et l'ensemble d'arrivée est B, l'application
$f : A_1 \times A_2 \longrightarrow B : (x, y) \longmapsto f(x, y)$ est appelée ***fonction de deux variables*** ou à deux arguments x, y.

b. De même l'application
$f : A_1 \times A_2 \times A_3 \longrightarrow B : (x_1, x_2, x_3) \longmapsto f(x_1, x_2, x_3)$

c. Généralisons : étant donné n ensembles $A_1, A_2, \dots, A_n$, l'application

$f : A_1 \times A_2 \times \ldots \times A_n \longrightarrow B : (x_1, x_2, \ldots, x_n) \longmapsto f(x_1, x_2, \ldots, x_n)$ est une application de n variables $x_1, x_2, \ldots, x_n$.

Exemple

L'application $i - ième$ fonction coordonnée pr_i

$$pr_i : A_1, A_2, \ldots, A_n \longrightarrow A_i$$
$$(x_1, x_2, \ldots, x_n) \longmapsto pr_i(x_1, x_2, \ldots, x_n) = x_i$$

d. En pratique, on considère aussi des fonctions dont les ensembles de départ et d'arrivée sont des produits cartésiens.

Par exemple

$$f : A_1 \times A_2 \longrightarrow B_1 \times B_2 \times B_3$$
$$(x, y) \longmapsto f(x, y) = \big(f_1(x, y), f_2(x, y), f_3(x, y)\big)$$

Dans la pratique on écrit

$$f = (f_1, f_2, f_3)$$

Un autre exemple

Soit l'application

$$f : U \subseteq \mathbb{R}^3 \longrightarrow \mathbb{R}^3$$
$$(x, y, z) \longmapsto f(x, y, z) = (\cos(x + y), \cos(y + z), e^{xyz})$$

On note $f = (f_1, f_2, f_3)$ avec $f_1(x, y, z) = \cos(x + y)$
$f_2(x, y, z) = \cos(y + z)$
$f_3(x, y, z) = e^{xyz}$

§4. Familles d'ensembles

Soit I un ensemble

4.1. Définitions

a. Une famille d'ensembles indexés par I est une correspondance qui associe un ensemble A_i à chaque élément $i \in I$. On la note alors
$\{A_i : i \in I\}$ ou $(A_i)_{i \in I}$ ou même A_i si l'ensemble I est évident par le contexte.
I est appelé l'ensemble d'indices de la famille. Les éléments de I sont appelés ***indices***.

b. Si $J \subseteq I$, l'ensemble $(A_i)_{i \in J}$ est une sous–famille de (ou ***famille extraite*** de la famille) $(A_i)_{i \in I}$

c. Si l'ensemble des indices est un produit cartésien $I \times J$, on définit une famille double
$\big(A_{ij}\big)_{(i,j) \in I \times J}$

4.2. Opérations

Soit $(A_i)_{i \in I}$ une famille d'ensembles indexés par I

a. Réunion

$$\bigcup_{i\in I} A_i = \{x/(\exists i)(i \in I \text{ et } x \in A_1)\}$$

La famille $(A_i)_{i\in I}$ est un recouvrement d'un ensemble S si et seulement si $S \subset \bigcup_{i\in I} A_i$

b. Intersection

$$\bigcap_{i\in I} A_i = \{x/\forall i \in I, x \in A_i\}$$

Exemple

Soient $I = \mathbb{N}^*$ et $A_i = \{x \in \mathbb{N}^* \text{ et } x \text{ divisible par } i\}$

Alors :

$$\bigcup_{i\in\mathbb{N}^*} A_i = \bigcup_{i=1}^{\infty} A_i = \mathbb{N}^*$$

et

$$\bigcap_{i\in I} A_i = \bigcap_{i=1}^{\infty} A_i = \emptyset$$

4.3. Propriétés

a. Si $(A_i)_{i\in I}$ est une famille d'ensembles et B ensemble
Alors
a.1. $B \cap (\bigcup A_i) = \bigcup(B \cap A_i)$
a.2. $B \cup (\bigcap A_i) = \bigcap(B \cup A_i)$

b. Si $(A_i)_{i\in I}$ est une famille de sous – ensembles de l'ensemble référentiel U.
b.1. $\complement(\bigcup_{i\in I} A_i) = \bigcap_{i\in I} \complement A_i$

b.2. $\complement(\bigcap_{i\in I} A_i) = \bigcup_{i\in I} \complement A_i$ (à démontrer aux T.P)

§5. Combinatoire

5.1. Qu'est – ce que la combinatoire ?

La combinatoire (ou les mathématiques combinatoires ou encore l'analyse combinatoire) est une discipline mathématique qui a trait à l'étude de la disposition d'éléments dans des ensembles généralement finis. La manière de disposer ces éléments est régie par des conditions de limitation imposées par l'objet d'étude. Dénombrer ces éléments est un des problèmes de la combinatoire.

5.2. Le raisonnement par récurrence

a. Récurrence dans $\mathbb{N}$

Soit $p(n)$ une proposition définie pour $n \in \mathbb{N}$
Si $p(0)$ est vraie, et s'il est vrai que $\forall n \in \mathbb{N}, p(n) \Longrightarrow p(n+1)$
Alors $\forall n \in \mathbb{N}, p(n)$ est vraie.

b. Récurrence limitée

Soient $p(n)$ une proposition définie pour $n \in \mathbb{N}$ et $a, b \in \mathbb{N} \,/\, a < b$
Si $p(a)$ est vraie pour $a \geq 0$
Et s'il est vrai que $\forall n \in \mathbb{N} \,/\, a \leq n < b, p(n) \Longrightarrow p(n+1)$
Alors $\forall n \in \mathbb{N} \,/\, a \leq n \leq b, p(n)$ est vraie.

Exemple
Montrons par récurrence l'égalité

$$1^3+2^3+3^3+\cdots+n^3 = \frac{n^2(n+1)^2}{4}$$

En effet,

$p(1)$ est vraie car $1^3 = \frac{1^2(1+1)^2}{4}$

Supposons $p(n)$ vraie c'est – à – dire

$1^3+2^3+3^3+\cdots+n^3 = \frac{n^2(n+1)^2}{4}$ (Hypothèse de récurrence) et montrons qu'elle entraine $p(n+1)$ vraie
On a :

$$p(n+1): 1^3+2^3+3^3+\cdots+n^3+(n+1)^3 = \frac{n^2(n+1)^2}{4}+(n+1)^3$$
$$= \frac{(n+1)^2\left(n^2+4n+4\right)}{4}$$
$$= \frac{(n+1)^2[(n+1)+1]^2}{4}$$

Vrai donc.

5.3. Nombre d'applications d'un ensemble fini dans un ensemble fini

Théorème
A et B étant finis non vides de cardinaux respectifs m et n, l'ensemble des applications B^A est fini et a pour cardinal n^m

Démonstration
Posons B^A l'ensemble des applications de A vers B
Si $m = 1, A = \{a\}\ et\ B = \{b_1, b_2, \ldots, b_n\}$
Les applications de A dans B sont définis par

$$a \longmapsto f_i(a) = b_i$$

D'où $\sharp\ B^A = n$ fini

Supposons que pour $m = p - 1, B^A$ soit fini (Hypothèse de récurrence)
Soit $m = p$ et $a \in A$
Posons $A' = A \setminus \{a\}, A'' = \{a\}$ et définissons l'application

$$F : B^A \longrightarrow B^{A'}$$
$$f \longmapsto F(f) = f_{A'}$$

F est surjective.

$F^{-1}(f_{A'})$ est l'ensemble des prolongements de $f_{A'}$ deux à deux disjoints. $f(a) \in B$ détermine chacun d'eux.
Donc $\sharp\, F^{-1}(f_{A'}) = \sharp\, B = n$ et B^A est donc fini
Posons $\varphi(p, n) = \sharp\, B^A$; lorsque $\sharp\, A = p$, nous avons

$$\varphi(1, n) = n$$
$$\varphi(2, n) = n\,\varphi(1, n)$$
$$\dots$$
$$\varphi(p, n) = n\,\varphi(p-1, n)$$
$$\dots$$
$$\varphi(m, n) = n\,\varphi(m-1, n)$$

Multiplions ces égalités membre à membre, nous avons

$$\varphi(m, n) = n^m$$

5.4. Arrangements

a. <u>Définition</u>

Le nombre d'arrangements de n éléments pris m à m, noté A_n^m, est le nombre de sous – ensembles de m éléments que l'on peut former avec les n éléments.
Ces sous – ensembles étant distincts soit par la **nature**, soit par l'**ordre** des éléments qui entrent dans la composition du sous – ensemble.

b. <u>Calcul de</u> A_n^m

On montre que le nombre des arrangements de n éléments pris m à m est obtenu de la façon ci – après

$$\underset{1}{n} \times \underset{2}{(n-1)} \times \underset{3}{(n-2)} \times \dots \times \underset{m}{(n-m+1)}$$

C'est – à – dire par la multiplication de m nombres entiers consécutifs décroissants, le premier de ces nombres étant égal à n, nombre d'éléments.

$$\mathrm{A}_n^m = n(n-1)(n-2)\dots(n-m+1) \qquad (1^{\text{ère}} \text{ forme})$$

Si nous multiplions et divisons l'expression de A_n^m par $(n-m)(n-m-1)\dots 3 \times 2 \times 1$, nous obtenons

$$\mathrm{A}_n^m = \frac{n(n-1)(n-2)\dots(n-m+1)(n-m)(n-m-1)\times\dots\times 2\times 1}{(n-m)(n-m-1)\times\dots\times 2\times 1}$$

Soit

$$\mathrm{A}_n^m = \frac{n!}{(n-m)!} \qquad (2^{\text{ème}} \text{ forme})$$

c. Remarques

$n!$ se lit **factorielle** n
$n! = n(n-1)(n-2) \ldots 3.2.1$
Par exemple : $6! = 6 \times 5 \times 4 \times 3 \times 2 \times 1$

Exemple
Avec les lettres du mot « Cargo », combien de mots différents de 3 lettres peut – on former ?
Il s'agit de l'arrangement de 5 lettres pris 3 à 3
On a : $\mathrm{A}_5^3 = 60$ mots

d. Application : recherche du nombre des injections d'un ensemble fini dans un ensemble fini

e. Théorème
A et B étant deux ensembles finis non vides de cardinaux respectifs m et n $(m \leq n)$, l'ensemble des injections de A dans B est fini et a pour cardinal

$$n(n-1)(n-2) \ldots (n-m+1) = \frac{n!}{(n-m)!}$$

Démonstration
Posons $A_m = [1, m]$
$I(A, B)$ l'ensemble des injections de A dans B et raisonnons par récurrence sur m, limitée à $[1, n]$
Si $m = 1, A_1 = \{1\}$, alors $\sharp\, I(A_1, B) = n$
Soit $1 \leq m < n$. Supposons que $\sharp\, I(A_m, B) = n(n-1)(n-2) \ldots (n-m+1)$
Démontrons que

$$\sharp\, I(A_{m+1}, B) = n(n-1)(n-2) \ldots (n-m)$$

Déduit du précédent par multiplication par $n - m$
Soit f une injection de A_m dans B
Comme f est une injection, $\sharp\, f(A_m) = m$ éléments
On peut alors prolonger f en une injection de A_{m+1} dans B en définissant $f(m+1)$. Toute injection de A_m dans B se prolonge par conséquent en $n - m$ injections de A_m dans B.
Comme toute injection de A_{m+1} dans B est le prolongement d'une injection de A_m dans B, le théorème est démontré.
A et B étant deux ensembles finis non vides de cardinaux respectifs m et n $(m \leq n)$, le nombre des injections de A dans B est le nombre des arrangements de n éléments pris m à m.

f. Définition

On appelle arrangement des n objets de B, m à m, l'image d'une injection quelconque de $A_m = [1, m]$ dans B.

5.5. Permutations

a. Définition

Le nombre de permutations de n éléments distincts, noté P_n, est le nombre d'ensembles que l'on peut former avec les n éléments. Ces ensembles étant distincts par l'**ordre** des éléments qui entrent dans la composition des éléments de l'ensemble.

b. Calcul de P_n

D'une façon générale, n éléments distincts donnent lieu à :

$$\mathrm{P}_n = n(n-1)(n-2) \times \ldots \times 3 \times 2 \times 1$$ permutations, soit à un nombre de permutations égal au produit des n premiers nombres entiers, résultat qui se note $n!$ D'où

$$\mathrm{P}_n = n!$$

Ce nombre se déduit de la formule précédente (5.4.b) ; c'est en effet le nombre d'arrangements de ces n objets pris n à n. Donc

$$\mathrm{P}_n = \mathrm{A}_n^n = n(n-1)(n-2) \times \ldots \times 3 \times 2 \times 1$$

Exemple

De combien de façons différentes peut – on placer 4 personnes sur un banc ? En effet, deux groupes distincts diffèrent seulement par l'ordre.

D'où il y aura $\mathrm{P}_4 = 4! = 24$ façons différentes (permutations)

c. Application : recherche du nombre des bijections d'un ensemble E à n éléments sur lui – même

d. Théorème

Il y a $n!$ bijections d'un ensemble E à n éléments sur lui – même.

Démonstration

C'est le corollaire du théorème précédent du §5-5.4.e

En effet, si $\sharp\, A = \sharp\, B = \sharp\, E = n$, sachant qu'une injection de E sur lui – même est une bijection, alors

$$\mathrm{A}_n^m = \mathrm{A}_n^n = n! = \mathrm{P}_n$$ bijections d'un ensemble E à n éléments sur lui–même.

e. Définition

Ces bijections d'un ensemble E à n éléments sur lui – même sont aussi appelés **permutations**.

5.6. Combinaisons

a. Définition

Le nombre des combinaisons de n éléments distincts pris m à m, noté C_n^m ou $\binom{n}{m}$, est défini exactement de la même façon que le nombre des arrangements A_n^m, sauf en ce qui concerne la distinction des sous – ensembles : dans les arrangements, les sous – ensembles diffèrent par la nature ou par l'ordre des éléments qui les constituent, tandis que dans les combinaisons, les sous – ensembles diffèrent seulement par la **nature** des éléments qui les constituent.

b. Calcul de C_n^m

Par définition,

$$A_n^m = P_n . C_n^m \Rightarrow C_n^m = \frac{A_n^m}{P_n}$$

D'où

$$C_n^m = \frac{n(n-1)(n-2)\dots(n-m+1)}{m(m-1)(m-2)\dots 3.2.1}$$

ou

$$C_n^m = \frac{n!}{m!\,(n-m)!}$$

Exemple

De combien de manières un comité de 4 personnes peut – il être choisi d'un groupe de 10 personnes. En effet, deux comités seront différents seulement par la nature des personnes qui les composent. Dès lors il y aura

$C_{10}^4 = 1260$ manières à le choisir

c. Propriétés

c.1. $C_n^m = C_n^{n-m}$

c.2. $n > m \geq 1 \Rightarrow C_n^m = C_{n-1}^m + C_{n-1}^{m-1}$

Démonstration

c.1. $C_n^m = \frac{n!}{m!(n-m)!}$ ne change pas si on remplace n par $n-m$

c.2. En effet :

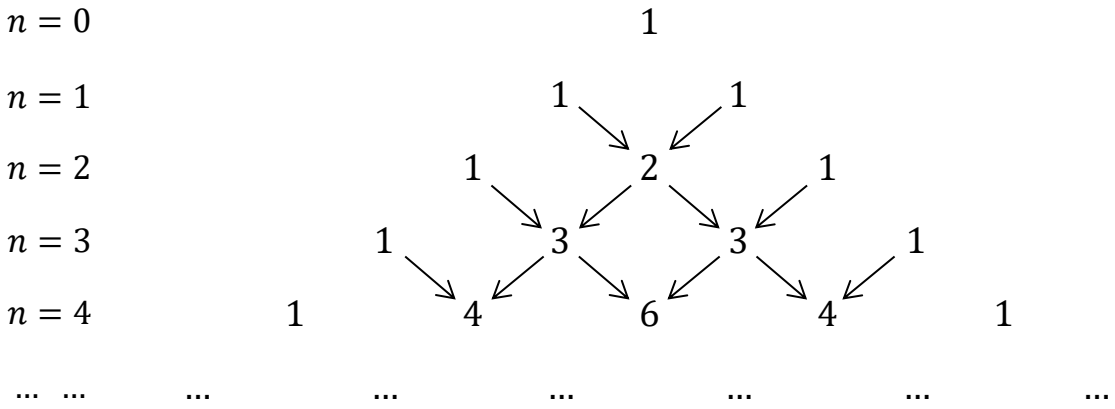
$$C_{n-1}^m + C_{n-1}^{m-1} = \frac{(n-1)!}{m![(n-1)-m]!} + \frac{(n-1)!}{(m-1)![(n-1)-(m-1)]!}$$

$$= \frac{(n-1)!}{m(m-1)!(n-m-1)!} + \frac{(n-1)!}{(m-1)!(n-m)(n-m-1)!}$$

$$= \frac{(n-1)!}{(m-1)!(n-m-1)!} \times \frac{n}{m(n-m)} = \frac{n!}{m!(n-m)!} = C_n^m$$

d. Triangle de Pascal

Notez que la formule c.2 précédente indique une procédure pour le calcul effectif des coefficients du développement du binôme de Newton $(x+y)^n$, procédure connue sous le nom du **Triangle de Pascal**. On l'illustre schématiquement par le diagramme ci – après :



Démontrer que $(x+y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k}$

e. Application : recherche du nombre de parties à m éléments d'un ensemble E à n éléments

f. Théorème

Le nombre de parties à m éléments d'un ensemble E à n éléments est égal à

$$\mathrm{C}_n^m = \frac{n!}{m!\,(n-m)!}$$

Démonstration

Soit I ensemble de toutes les injections de $A_m = [1, m]$ dans E

On sait que $\sharp\, I = n(n-1)(n-2)\ldots(n-m+1)$ injections

Si $f \in I$, alors

$f(A_m)$ est une partie de E ayant m éléments.

Dénombrons, dans I, les injections qui donnent de A_m la même image $B \subseteq E$. A cet effet, étudions la relation binaire suivante

$$f \equiv g \Leftrightarrow f(A_m) = g(A_m)$$

C'est une relation d'équivalence (à vérifier)

D'où I est partagé en classes d'équivalence

Toutes les injections d'une classe donnent la même image B dans E et toute partie B de E telle que

$\sharp\, B = n$ définit une classe et une seule.

Le nombre des classes est par conséquent égal au nombre cherché des parties de E ayant m éléments.

Cherchons maintenant le nombre des injections dans chaque classe.

A tout couple f, g tel que $f \equiv g$, associons une application

$$h : A_m \longrightarrow A_m : x \longmapsto h(x) = y \text{ et } f(x) = g(y)$$

h est bien définie et, en plus, est bijective

D'où h est une permutation de A_m et

$$\forall x \in A_m,\ f(x) = g[h(x)]$$

Donc $f = g \circ h$

Enfin, pour tout f, g appartenant à une même classe, la permutation h est unique.

Désignons par $\mathcal{P}$ l'ensemble des permutations de A_m. On a montré que

$f \equiv g \Longrightarrow \exists! h \mathcal{P} / f = g \circ h$ et réciproquement s'il existe une permutation h de

$A_m / f = g \circ h$, on a

$f(A_m) = g(A_m)$

Donc $f = g$

Par conséquent, le nombre des éléments f d'une classe d'équivalence représentée par g est égal au nombre des permutations de A_m.

Or $\sharp\, \mathcal{P} = n!$ (Théorème du §5-5.5.d)

D'où le nombre total des classes est

$$\frac{A_n^m}{m!} = \frac{n!}{m!\,(n-m)!} \left(\text{Etant donné que } \sharp\, I = A_n^m\right)$$

§6. Exercices

6.1. Exercices corrigés

6.1.1. $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ étant les ensembles numériques, complétez par $\in$ ou $\notin$

a. 7 … … $\mathbb{C}$ c. $-\frac{4}{2}$ … … $\mathbb{Z}$ e. π … … $\mathbb{R} \setminus \mathbb{Q}$

b. $0{,}2$ … … $\mathbb{Q}$ d. $\frac{3}{2}$ … … $\mathbb{R} \setminus \mathbb{Q}$ f. $\frac{-6}{-2}$ … … $\mathbb{N}$

6.1.2. Décrire les ensembles suivants par énumération des éléments, si possible
$A = \{x/x$ est un entier naturel diviseur de $24\}$
$B = \{x/x$ est un entier naturel pair inférieur ou égal à $10\}$
$C = \{x/x$ est un entier naturel pair diviseur de 18 et $30\}$

6.1.3. Décrire $\mathcal{P}(E)$, dans les cas suivants :
a. $E = \{1,2,3,4\}$
b. $E = \{2, \{a, b\}\}$

6.1.4. Si $A = \{1,2\}$, $B = \{\{1\}, \{2\}\}$, $C = \{\{1\}, \{1,2\}\}$, $D = \{\{1\}, \{2\}, \{1,2\}\}$
Lesquelles des affirmations suivantes sont vraies et pourquoi ?

$A = B$	$A \in C$	$B \subset D$
$A \subseteq B$	$A \subset D$	$B \in D$
$A \subset C$	$B \subset C$	$A \in D$

6.1.5. Soient $A = \{1,2,3, \{1,2,3\}\}$ et $B = \{\{1,2\}, 1,2\}$, décrire $A \cup B$; $A \setminus B$; $B \setminus A$

6.1.6. Montrer que $(A \setminus B) \cap B = \emptyset$

6.1.7. Montrer que $B \setminus A = B \cap \complement A$

6.1.8. Démontrer la loi de De Morgan $\complement(A \cup B) = \complement A \cap \complement B$

6.1.9. Effectuer les opérations indiquées, à la fois analytiquement et graphiquement
a. $(3 + 4i) + (5 + 2i)$ b. $(6 - 2i) - (2 - 5i)$

6.1.10. Montrer que
$|z_1 + z_2| \leq |z_1| + |z_2|$

6.1.11. Mettre chacun des nombres complexes suivants sous forme polaire
a. $2 + 2\sqrt{3}i$ b. $-5 + 5i$ c. $-\sqrt{6} - \sqrt{2}i$

6.1.12. Si $z_1 = r_1(\cos\theta_1 + i\sin\theta_1)$ et $z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$, démontrer que
a. $z_1 z_2 = r_1 r_2[\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2)]$

b. $\frac{z_1}{z_2} = \frac{r_1}{r_2}[\cos(\theta_1 - \theta_2) + i\sin(\theta_1 - \theta_2)]$

6.1.13. Résoudre dans $\mathbb{C}$ l'équation $z^5 + 32 = 0$

6.1.14. Soit $w = \sqrt[3]{-1+i}$
Déterminer et représenter dans le plan complexe ses racines

6.1.15. Résoudre l'équation $z^2 + 2iz + 5 - i - 3z = 0$

6.1.16. Trouver toutes les racines cinquièmes de l'unité

6.1.17. Enoncer en langage courant une proposition qui ait le même sens que :
« pour tout x, si x est un chien, alors x a un bon odorat » et qui ne contienne ni quantificateurs ni variables.

6.1.18. En posant des quantificateurs contenant les variables « x » et « y » devant la fonction propositionnelle[1]:
« x est le père de y »
On peut obtenir diverses propositions. Formulez toutes ces propositions et déterminez lesquelles sont vraies.

6.1.19. Répondre par vrai ou faux
a. $(x < 7) \Longrightarrow (x < 10)$
b. $(x > 2) \Longrightarrow (x < 6)$
c. $(x = 4) \Longrightarrow (x < 3)$
d. $(x = 4) \Longrightarrow (x > 2)$

6.1.20. Exprimer la contraposée de $p \Longrightarrow q$ dans chacun des cas suivants
a. $p : A \cap B = \emptyset$; $q = A \neq B$
b. $p : f$ est une bijection ; $q : f$ est une injection

6.1.21. Dans les énoncés suivants, remplacer les … par l'un des symboles « $\Longrightarrow$ » ou « $\Leftrightarrow$ »
a. $x < y$ et $y = z$ … $x < z$
b. $x \in A$ et $A \subset B$ … $x \in B$
c. $A \subset B$ et $B \subset A$ … $A = B$

6.1.22. Soit $\mathcal{R}$ la relation $<$ de l'ensemble $A = \{1,2,3,4\}$ dans l'ensemble $B = \{1,3,5\}$ c'est – à – dire $(a,b) \in G_{\mathcal{R}}$ si et seulement si $a < b$
a. Ecrire $\mathcal{R}$ sous la forme d'un ensemble de couples
b. Représenter $\mathcal{R}$ sur un diagramme cartésien de $A \times B$
c. Déterminer le domaine de $\mathcal{R}$, l'image de $\mathcal{R}$ et la relation $\mathcal{R}^{-1}$

[1] Une fonction propositionnelle ou une forme propositionnelle est l'expression qui renferme une ou plusieurs variables et qui devient une proposition quand on remplace ces variables par des constantes

d. Déterminer $\mathcal{R} \circ \mathcal{R}^{-1}$

6.1.23. Soit $G_{\mathcal{R}} = \{(1,1), (2,3), (3,2)\}$ le graphe de la relation $\mathcal{R}$ définie dans $E = \{1,2,3\}$. Déterminer si $\mathcal{R}$ est
a. Réflexive
b. Symétrique
c. Transitive

6.1.24. Considérons l'ensemble $\mathbb{N} \times \mathbb{N}$ des couples de nombres entiers positifs. Soit $\mathcal{R}$ la relation, notée $\simeq$ et définie dans $\mathbb{N} \times \mathbb{N}$ par

$$(a, b) \simeq (c, d) \text{ si et seulement si } ad = bc$$

Démontrer que $\mathcal{R}$ est une relation d'équivalence

6.1.25. Soit $E = \{1,2,3,4\}$. Dire si chacune des relations suivantes est une application de E dans E
a. $G_{\mathcal{R}} = \{(2,3), (1,4), (2,1), (3,2), (4,4)\}$
b. $G_{\mathcal{S}} = \{(3,1), (4,2), (1,1)\}$
c. $G_{\mathcal{T}} = \{(2,1), (3,4), (1,4), (2,1), (4,4)\}$

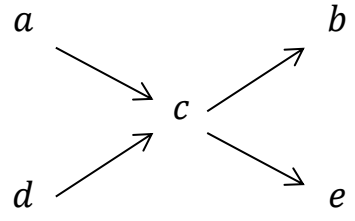
6.1.26. Considérons les applications $f : \mathbb{R} \longrightarrow \mathbb{R}$ et $g : \mathbb{R} \longrightarrow \mathbb{R}$ définies par les formules

$$f(x) = 2\sqrt{x} + 1, \qquad g(x) = e^{\sqrt{x}+5}$$

Trouver les formules permettant de définir les applications composées $g \circ f$ et $f \circ g$

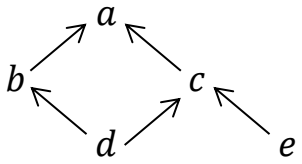
6.1.27. Soient $A_n = \{x : x \text{ est un multiple de } n\}$, où $n \in \mathbb{N}$ et $B_i = [i, i+1]$, où $i \in \mathbb{Z}$. Déterminer
a. $A_3 \cap A_5$
b. $\cup \{A_i : i \in P\}$ où P désigne l'ensemble des nombres premiers
c. $B_3 \cap B_4$
d. $\cup \{B_i : i \in \mathbb{Z}\}$

6.1.28. Soit l'ensemble $E = \{a, b, c, d, e\}$
L'ordre est défini par le diagramme
C'est – à – dire
$x, y \in E, x \leq y \Leftrightarrow x = y$ ou si l'on peut aller de x à y sur le diagramme dans le sens des flèches.



Montrer que
a. Les ensembles $\{a, c, d\}$ et $\{b, e\}$ sont des sous – ensembles totalement ordonnés.
b. Les ensembles $\{a, b, c\}$ et $\{d, e\}$ ne sont pas des sous – ensembles totalement ordonnés.

6.1.29. Soit $E = \{a, b, c, d, e\}$ un ensemble ordonné à l'aide du diagramme

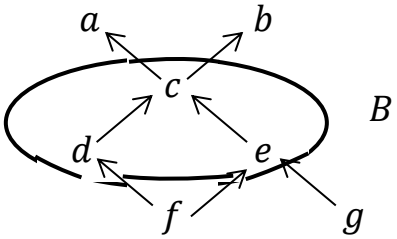


Quel est
a. Le plus grand élément de E
b. Le plus petit élément de E

6.1.30. Quel est
a. Le plus petit élément de $\mathbb{N}^*$
b. Le plus grand élément de $\mathbb{N}^*$
c. Le plus petit élément de $\mathbb{Z}$
d. Le plus grand élément de $\mathbb{Z}$

6.1.31. Soit $E = \{a, b, c, d, e\}$ l'ensemble ordonné, à l'aide du diagramme de l'exercice 6.1.30.
Quels sont
a. Les éléments minimaux
b. Les éléments maximaux

6.1.32. Soit $E = \{a, b, c, d, e, f\}$ un ensemble ordonné à l'aide du diagramme suivant
Soit $B = \{c, d, e\}$
Quels sont
a. Les majorants de B
b. Les minorants de B
Quel est
a. $\sup(B)$
b. $\inf(B)$



6.1.33. Soit $\mathbb{Q}$ l'ensemble des rationnels
Posons $B = \{x : x \in \mathbb{Q}, x > 0,\ 2 < x^2 < 3\}$
Déterminer
a. Les minorants de B
b. Les majorants de B
c. $\inf(B)$
d. $\sup(B)$
Utilisez le principe de récurrence pour résoudre les exercices 6.1.35 et 6.1.36

6.1.34. $p(n) : 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{6}[n(n+1)(2n+1)]$

6.1.35. $p(m)$: Si $a > b$, alors $a^m > b^m$ dans N
6.1.36. Soient $A = \{1,2\}$ et $B = \{5,6,7\}$
Trouver toutes les applications possibles de A dans B

6.1.37. 15 chevaux prennent le départ d'une course.
Calculer le nombre d'ordres d'arrivées possibles de 3 premiers ? (sans exæquo).

6.1.38. Une assemblée de 20 personnes doit élire un comité composé de 4 membres : un président, un vice – président, un trésorier et un secrétaire.

a. Quel est le nombre de comités possibles peut – on élire ? ou former ?
b. Calculer ce nombre si, parmi ces 20 personnes, figurent 15 hommes et 5 femmes, et si les postes de président et de vice – président doivent être occupés par des hommes et les deux autres occupés par des femmes ?

6.1.39. Le nombre des arrangements de n objets 4 à 4, est 12 fois celui des arrangements de n objets 2 à 2.
Combien y a – t – il d'objets ?

6.1.40. Soient $E = \{a, b, c, d\}$ et $A \subset E$ avec $A = \{a, b\}$
Trouver toutes les injections possibles de $\{a, b\}$ dans E.

6.1.41. On considère l'ensemble $A = \{c, l, a, r, t, e\}$ des 6 lettres du mot clarté. Déterminer le nombre de mots ou anagrammes distincts (ayant un sens ou non) qu'il est possible de former avec ces 6 lettres.

6.1.42. Un championnat de football groupe 16 équipes. Chacune de ces 16 équipes doit rencontrer chacune de 15 autres. A combien de rencontres donnera lieu la compétition si l'on admet :
a. Que deux équipes ne se rencontrent qu'une fois
b. Que le championnat a lieu par matches aller – retour

6.1.43. De combien de manières peut – on choisir un groupe de 4 hommes et de 3 femmes lorsqu'il y a 10 hommes et 8 femmes ?

Solution ou indications de solution

6.1.1. a. $7 \in \mathbb{C}$ c. $-\frac{4}{2} \in \mathbb{Z}$ e. $\pi \in \mathbb{R} \setminus \mathbb{Q}$

b. $0{,}2 \in \mathbb{Q}$ d. $\frac{3}{2} \notin \mathbb{R} \setminus \mathbb{Q}$ f. $\frac{-6}{-2} \in \mathbb{N}$

6.1.2. $A = \{1,2,3,4,6,8,12,24\}$
$B = \{0,2,4,6,8,10\}$
$C = \{2,6\}$

6.1.3.
a. $\mathcal{P}(E) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}, \{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}, E\}$
b. $\mathcal{P}(E) = \{\emptyset, \{2\}, \{\{a,b\}\}, E\}$

6.1.4. $A \in C$ car A est un élément de C
$B \subset D$ car tout élément de B est élément de D

6.1.5. $A \cup B = \{1,2,3, \{1,2\}, \{1,2,3\}\}$
$A \setminus B = \{3, \{1,2,3\}\}$
$B \setminus A = \{\{1,2\}\}$

6.1.6. $(A \setminus B) \cap B = \{x / x \in B \text{ et } x \in A \setminus B\}$
$= \{x / x \in B \text{ et } x \in A \text{ et } x \notin B\}$
$= \emptyset$
Car il n'existe pas d'élément x vérifiant à la fois $x \in B$ et $x \notin B$

6.1.7. $B \setminus A = B \cap \complement A$
En effet $B \setminus A = \{x / x \in B \text{ et } x \notin A\}$
$= \{x / x \in B \text{ et } x \in \complement A\}$
$= B \cap \complement A$

6.1.8. $\complement A \cup B = \complement A \cap \complement B$
En effet,
$\complement A \cup B = \{x / x \notin A \cup B\}$
$= \{x / x \notin A \text{ et } x \notin B\}$
$= \{x / x \in \complement A \text{ et } x \in \complement B\}$
$= \complement A \cap \complement B$

De même démontrer que $\complement A \cap B = \complement A \cup \complement B$

6.1.9.

a. Analytiquement $(3+4i)+(5+2i)=3+5+4i+2i=8+6i$

Graphiquement voir *fig.1*

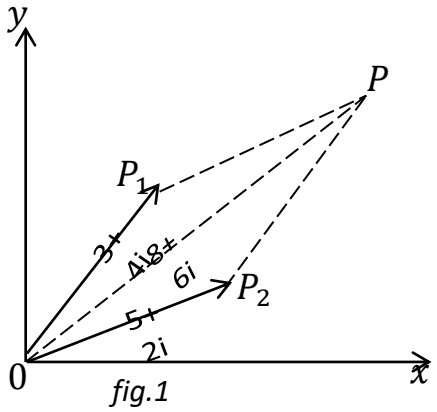


fig.1

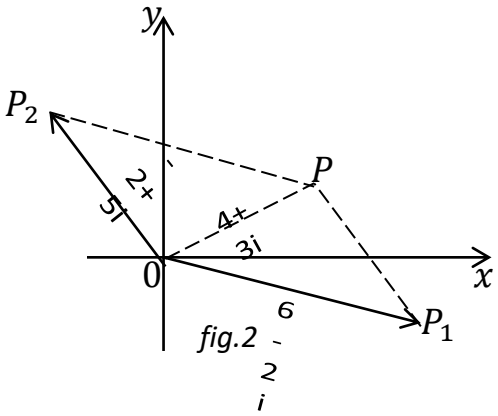


fig.2

b. Analytiquement $(6-2i)-(2-5i)=6-2-2i+5i=4+3i$

Graphiquement voir *fig.2*

Il est souvent commode de considérer un nombre complexe $x+yi$ comme un vecteur de composantes x, y sur les axes des x et des y et d'appliquer la loi d'addition des vecteurs.

6.1.10. En vertu des propriétés

$\overline{z_1 \pm z_2} = \bar{z}_1 \pm \bar{z}_2$ et $|z|^2 = z\bar{z}$, on a :

$$\begin{aligned}|z_1+z_2|^2 &= (z_1+z_2)(\overline{z_1+z_2}) = (z_1+z_2)(\bar{z}_1+\bar{z}_2)\\ &= z_1\bar{z}_1 + z_1\bar{z}_2 + \bar{z}_1 z_2 + z_2\bar{z}_2\\ &= |z_1|^2 + 2\text{Re}\, z_1\bar{z}_2 + |z_2|^2\end{aligned}$$

Puisque $2\text{Re}\, z_1\bar{z}_2 = z_1\bar{z}_2 + \bar{z}_1 z_2$. Donc

$$|z_1+z_2|^2 = |z_1|^2 + |z_2|^2 + 2\text{Re}\, z_1\bar{z}_2 \quad (1)$$

D'après les propriétés $|z_1 z_2| = |z_1||z_2|$, $|\bar{z}| = |z|$ et $-|z| \le \text{Re}\, z \le |z|$, on a :

$$2\text{Re}\, z_1\bar{z}_2 \le 2|z_1\bar{z}_2| = 2|z_1||\bar{z}_2| - 2|z_1||z_2|$$

Donc (1) devient

$$\begin{aligned}|z_1+z_2|^2 &= |z_1|^2 + |z_2|^2 + 2\text{Re}\, z_1\bar{z}_2 \le |z_1|^2 + |z_2|^2 + 2|z_1||z_2|\\ &\le |z_1|^2 + |z_2|^2 + 2|z_1||z_2| = (|z_1|+|z_2|)^2\\ &\le (|z_1|+|z_2|)^2\end{aligned}$$

$$\Longrightarrow |z_1+z_2| \le |z_1| + |z_2|$$

6.1.11. Soient $\begin{cases} z_1 = 2+2\sqrt{3}i \\ \theta_1 : \text{ son argument} \end{cases}$, $\begin{cases} z_2 = -5+5i \\ \theta_2 : \text{ son argument} \end{cases}$,

$\begin{cases} z_3 = -\sqrt{6}-\sqrt{2}\,i \\ \theta_3 : \text{ son argument} \end{cases}$

a. $|z_1| = \left|2+2\sqrt{3}i\right| = \sqrt{4+12} = 4$

$$\cos\theta_1 = \frac{2}{4} = \frac{1}{2} \Longrightarrow \theta_1 = 60° = \frac{\pi}{3}$$

$\sin\theta_1 = \frac{2\sqrt{3}}{4} = \frac{\sqrt{3}}{2} \Longrightarrow \theta_1 = 60° = \frac{\pi}{3}$

Donc $2 + 2\sqrt{3}i = 4(\cos 60° + i \sin 60°) = 4\left(\cos\frac{\pi}{3} + i \sin\frac{\pi}{3}\right)$

b. $|z_2| = |-5 + 5i| = \sqrt{25 + 25} = 5\sqrt{2}$

$\cos\theta_2 = -\frac{5}{5\sqrt{2}} = -\frac{1}{\sqrt{2}} = -\frac{\sqrt{2}}{2}$ On sait que $\cos(180° - \alpha) = -\cos\alpha$

D'où $\cos(180° - 45°) = -\cos 45° = -\frac{\sqrt{2}}{2}$

D'où $\theta_2 = 180° - 45° = 135° = \frac{3\pi}{4}$

et $-5 + 5i = 5\sqrt{2}(\cos 135° + i \sin 135°) = 5\sqrt{2}\left(\cos\frac{3\pi}{4} + i \sin\frac{3\pi}{4}\right)$

c. $|z_3| = \left|-\sqrt{6} - \sqrt{2}\,i\right| = \sqrt{6 + 2} = 2\sqrt{2}$

$\cos\theta_3 = \frac{-\sqrt{6}}{2\sqrt{2}} = -\frac{\sqrt{3}}{2}$ On sait que $\cos(180° + \alpha) = -\cos(-\alpha)$

$= -\cos\alpha$

D'où $\cos(180° + 30°) = -\cos(-30°) = -\cos 30° = -\frac{\sqrt{3}}{2}$

Donc $\theta_3 = 180° + 30° = 210° = \frac{7\pi}{4}$

et $-\sqrt{6} - \sqrt{2}\,i = 2\sqrt{2}(\cos 210° + i \sin 210°) = 2\sqrt{2}\left(\cos\frac{7\pi}{4} + i \sin\frac{7\pi}{4}\right)$

6.1.12.

a. $z_1 z_2 = r_1 r_2[\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2)]$

En effet,

$$\begin{aligned} z_1 z_2 &= r_1 r_2[(\cos\theta_1 + i \sin\theta_1)(\cos\theta_2 + i \sin\theta_2)] \\ &= r_1 r_2[(\cos\theta_1 \cos\theta_2 + i \cos\theta_1 \sin\theta_2 + i \sin\theta_1 \cos\theta_2 - \sin\theta_1 \sin\theta_2)] \\ &= r_1 r_2[(\cos\theta_1 \cos\theta_2 - \sin\theta_1 \sin\theta_2) + i(\cos\theta_1 \sin\theta_2 + \sin\theta_1 \cos\theta_2)] \\ &= r_1 r_2[\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2)] \end{aligned}$$

b. $\frac{z_1}{z_2} = \frac{r_1}{r_2}[\cos(\theta_1 - \theta_2) + i \sin(\theta_1 - \theta_2)]$

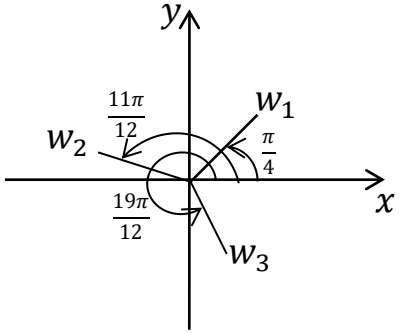
En effet,

$$\begin{aligned} \frac{z_1}{z_2} &= \frac{r_1(\cos\theta_1 + i \sin\theta_1)}{r_2(\cos\theta_2 + i \sin\theta_2)} \\ &= \frac{r_1[(\cos\theta_1 + i \sin\theta_1)(\cos\theta_2 - i \sin\theta_2)]}{r_2[(\cos\theta_2 + i \sin\theta_2)(\cos\theta_2 - i \sin\theta_2)]} \\ &= \frac{r_1[(\cos\theta_1 \cos\theta_2 - i \cos\theta_1 \sin\theta_2 + i \sin\theta_1 \cos\theta_2 + \sin\theta_1 \sin\theta_2)]}{r_2(\cos^2\theta_2 + \sin^2\theta_2)} \\ &= \frac{r_1}{r_2}[(\cos\theta_1 \cos\theta_2 + \sin\theta_1 \sin\theta_2) + i(\sin\theta_1 \cos\theta_2 - \cos\theta_1 \sin\theta_2)] \\ &= \frac{r_1}{r_2}[\cos(\theta_1 - \theta_2) + i \sin(\theta_1 - \theta_2)] \end{aligned}$$

6.1.13.
Sous la forme polaire
$$-32 = 32[\cos(\pi + 2k\pi) + i\sin(\pi + 2k\pi)], k = 0, \pm1, \pm2, \dots$$
D'après la formule de De Moivre
Si $z = r(\cos\theta + i\sin\theta)$, alors $z^5 = r^5(\cos 5\theta + i\sin 5\theta)$
Alors
$$z^5 + 32 = 0 \Longrightarrow z^5 = -32$$
$$z^5 = 32[\cos(\pi + 2k\pi) + i\sin(\pi + 2k\pi)]$$
Ou encore
$$r^5(\cos 5\theta + i\sin 5\theta) = 32[\cos(\pi + 2k\pi) + i\sin(\pi + 2k\pi)]$$
$$\Longrightarrow \begin{cases} r^5 = 32 \\ 5\theta = \pi + 2k\pi \end{cases} \quad \text{soit} \quad \begin{cases} r = 2 \\ \theta = \frac{\pi+2k\pi}{5} \end{cases}$$
D'où $z_k = 2\left[\cos\left(\frac{\pi+2k\pi}{5}\right) + i\sin\left(\frac{\pi+2k\pi}{5}\right)\right], k = 0,1,2, \dots$
Si $k = 0, z_1 = 2\left(\cos\frac{\pi}{5} + i\sin\frac{\pi}{5}\right)$
Si $k = 1, z_2 = 2\left(\cos\frac{3\pi}{5} + i\sin\frac{3\pi}{5}\right)$
Si $k = 2, z_3 = 2(\cos\pi + i\sin\pi) \dots$

6.1.14. $w = \sqrt[3]{-1+i}$
On a :
$$-1 + i = \sqrt{2}\left[\cos\left(\frac{3\pi}{4} + 2k\pi\right) + i\sin\left(\frac{3\pi}{4} + 2k\pi\right)\right]$$
$$\sqrt[3]{-1+i} = (-1+i)^{\frac{1}{3}}$$
$$= 2^{1/6}\left[\cos\left(\frac{\frac{3\pi}{4}+2k\pi}{3}\right) + i\sin\left(\frac{\frac{3\pi}{4}+2k\pi}{3}\right)\right]$$
Si $k = 0, w_1 = 2^{1/6}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)$
Si $k = 1, w_2 = 2^{1/6}\left(\cos\frac{11\pi}{12} + i\sin\frac{11\pi}{12}\right)$
Si $k = 2, w_3 = 2^{1/6}\left(\cos\frac{19\pi}{12} + i\sin\frac{19\pi}{12}\right)$

Ces racines sont représentées dans la figure ci – contre



6.1.15. Soit l'équation $z^2 + (2i-3)z + 5 - i = 0$
D'après la forme générale des équations du second degré, $a = 1,\ b = 2i-3,$
$c = 5 - i$ et les solutions sont donc
$$z_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a} = \frac{-(2i-3) \pm \sqrt{(2i-3)^2-4(1)(5-i)}}{2(1)} = \frac{3-2i \pm \sqrt{-15-8i}}{2}$$
$$= \frac{3-2i \pm (1-4i)}{2} \quad \text{D'où} \quad \begin{cases} z_1 = 2-3i \\ z_2 = 1+i \end{cases}$$

Sachant $\sqrt{\Delta}= \sqrt{-15-8i} = \pm(1-4i)$
Vérifier que les valeurs trouvées satisfont l'équation proposée.

6.1.16.
$z^5 = 1 = \cos 2k\pi + i \sin 2k\pi = e^{2k\pi i}$ où $k = 0, \pm1, \pm2, \ldots$
Donc $z_k = \cos\frac{2k\pi}{5} + i \sin\frac{2k\pi}{5} = e^{\frac{2k\pi i}{5}}$
Où il suffit de prendre $k = 0, 1, 2, 3, 4$
Les racines sont donc

$z_1 = 1$ $\quad z_3 = e^{\frac{4\pi i}{5}}$ $\quad z_5 = e^{\frac{8\pi i}{5}}$
$z_2 = e^{\frac{2\pi i}{5}}$ $\quad z_4 = e^{\frac{6\pi i}{5}}$

6.1.17. Tous les chiens ont un bon odorat

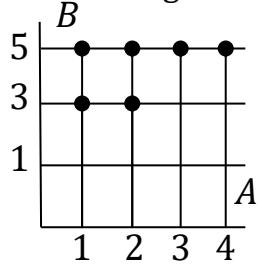
6.1.18.
1. Pour tous les hommes x et y, x est le père de y _____ F
2. Pour tout homme x, Il existe un homme y tel que x est le père de y _____ F
3. Il existe des hommes x et y tels que x est le père y _____ V
4. Il y a un homme x tel que, pour tout homme y, x est le père de y _____ F
5. Pour tout homme y, il existe un homme x tel que x est le père de y _____ F
6. Il y a un homme y tel que, pour tout homme x, x est le père de y _____ F

6.1.19.
a. V
b. F
c. V
d. V

6.1.20.
a. $A = B \Longrightarrow A \cap B \neq \emptyset$
b. f n'est pas une injection $\Longrightarrow f$ n'est pas une bijection

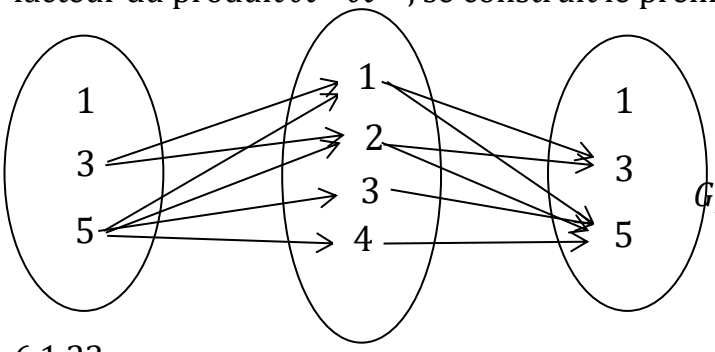
6.1.21.
a. $\Longrightarrow$
b. $\Longrightarrow$
c. $\Leftrightarrow$

6.1.22.
a. $G_{\mathcal{R}} = \{(1,3), (1,5), (2,3), (2,5), (3,5), (4,5)\}$
b. $\mathcal{R}$ est représenté sur le diagramme cartésien $A \times B$ tracé ci – dessous



c. $Dom\,\mathcal{R} = \{1,2,3,4\}$
$Im\,\mathcal{R} = \{3,5\}$
$G_{\mathcal{R}^{-1}} = \{(3,1),(5,1),(3,2),(5,2),(5,3),(5,4)\}$

d. Pour obtenir $\mathcal{R} \circ \mathcal{R}^{-1}$, on construit les diagrammes de $\mathcal{R}^{-1}$ et de $\mathcal{R}$. $\mathcal{R}^{-1}$, le second facteur du produit $\mathcal{R} \circ \mathcal{R}^{-1}$, se construit le premier.



$G_{\mathcal{R}\circ\mathcal{R}^{-1}} = \{(3,3),(3,5),(5,3),(5,5)\}$

6.1.23.
a. $\mathcal{R}$ n'est pas réflexive puisque $2 \in E$, $2 \not\mathcal{R}\ 2$
b. $\mathcal{R}$ est symétrique puisque $\forall x, y \in E, x\ \mathcal{R}\ y \Longrightarrow y\ \mathcal{R}\ x$ on a bien $G_{\mathcal{R}} = G_{\mathcal{R}^{-1}}$
c. $\mathcal{R}$ n'est pas transitive. En effet $3\ \mathcal{R}\ 2, 2\ \mathcal{R}\ 3$ mais $3 \not\mathcal{R}\ 3$

6.1.24.
- Réflexivité
$\forall (a,b) \in \mathbb{N} \times \mathbb{N}, (a,b) \simeq (a,b)$ car $ab = ba$
- Symétrie
$\forall (a,b),(c,d) \in \mathbb{N} \times \mathbb{N}, (a,b) \simeq (c,d) \Leftrightarrow ad = bc$
$\Longrightarrow bc = ad$
$cb = da$
Donc $(c,d) \simeq (a,b)$
- Transitivité
$\forall (a,b),(c,d),(e,f) \in \mathbb{N} \times \mathbb{N}$
Supposons que $(a,b) \simeq (c,d)$ et $(c,d) \simeq (e,f)$, alors
$ad = bc$
$cf = de$
$\Longrightarrow (ad)(cf) = (bc)(de)$
$adcf = bcde$
D'où $af = be$, Donc $(a,b) \simeq (e,f)$

6.1.25. a. Non. Pourquoi ?
b. Non. Pourquoi ?
c. Oui. Pourquoi ?

6.1.26. Calculons $g \circ f : \mathbb{R} \longrightarrow \mathbb{R}$ de la façon suivante

$$(g \circ f)(x) = g[f(x)] = g\left(2\sqrt{x} + 1\right) = e^{\sqrt{2\sqrt{x}+1}+5}$$

On calculera de manière analogue

$f \circ g : \mathbb{R} \longrightarrow \mathbb{R}$

$$(f \circ g)(x) = f[g(x)] = f\left(e^{\sqrt{x}+5}\right)$$
$$= 2\sqrt{e^{\sqrt{x}+5}} + 1$$

6.1.27.
a. $A_3 \cap A_5 = A_{15}$
Les nombres qui sont simultanément multiples de 3 et de 5 sont des multiples de 15
b. $\cup \{A_i : i \in P\}$ où P désigne l'ensemble des nombres premiers
$= \{2,3,4, \dots\} = \mathbb{N} \setminus \{1\}$
Tout entier positif distinct de 1 est un multiple d'au moins un nombre premier
c. $B_3 \cap B_4 = \{4\}$
d. $\cup \{B_i : i \in \mathbb{Z}\} = \mathbb{R}$

6.1.28. Vérifier
a. Que deux éléments quelconques de ces sous – ensembles sont comparables
b. Qu'il existe, dans ces sous – ensembles, des éléments non comparables
Par exemple, les éléments d et e du sous – ensemble $\{d, e\}$ ne sont pas comparables.

6.1.29. a. Le plus grand élément de E est a
b. E n'a pas de plus petit élément. Pourquoi ?

6.1.30. a. 1 b. n'a pas de plus grand élément
c. n'a pas de plus petit élément d. ni de plus grand élément

6.1.31. a. Les éléments d et e sont tous les deux minimaux
b. L'élément a est maximal

6.1.32. a. Les majorants de B sont : a, b et c
b. f est l'unique minorant de B
a. $\sup(B) = c$
b. $\inf(B) = f$
Pourquoi est – ce que g n'est pas minorant de B ?

6.1.33. Autrement dit
$B = \{x \in \mathbb{Q} / \sqrt{2} < x < \sqrt{3}\}$
a. B admet une infinité de minorants. Donner quelques exemples
b. B admet une infinité de majorants. Exemples ?
c. $\inf(B)$ n'existe pas. Pourquoi ?
d. $\sup(B)$ n'existe pas.

6.1.34.
$p(n) : 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$
Si $n = 1, 1^2 = \frac{1(1+1)(2.1+1)}{6} = 1$

Si $n = 2, 1^2 + 2^2 = \frac{2(2+1)(2.2+1)}{6} = 5$
Hypothèse de récurrence : supposons que $p(k)$ est vrai et montrons que $p(k+1)$ est vrai

En effet :

$$p(k+1) = 1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2$$
$$= \frac{k(k+1)(2k+1)}{6} + (k+1)^2$$
$$= \frac{(k+1)\left(2k^2+7k+6\right)}{6} = \frac{(k+1)(k+2)(2k+3)}{6}$$
$$= \frac{(k+1)[(k+1)+1][2(k+1)+1]}{6} = p(k+1)$$

$p(k) \Longrightarrow p(k+1)$ vrai

Donc, $\forall n \in \mathbb{N}^*, p(n)$ vrai

6.1.35. Dans $\mathbb{N}$,

$p(n)$: Si $a > b$, alors $a^m > b^m$

- Vérifions cette proposition pour $m = 2$ et $m = 3$

  Si $m = 2$, posons $a = b + k$

  $$\Longrightarrow a^2 = (b+k)a = (b+k)(b+k) = (b+k)^2$$
  $$= b^2 + 2bk + k^2$$

  D'où $a^2 > b^2$

  Si $m = 3$, multiplions les deux membres de la dernière égalité par a

  On a : $a^2.a > b^2.a$

  Ce qui donne

  $$a^2.a = a^3$$
  $$b^2.a = b^2(b+k) = b^3 + b^2k$$

  Donc $a^3 > b^3$

- Hypothèse de récurrence : $p(k) : a^k > b^k$ est vrai et montrons que $p(k) \Longrightarrow p(k+x)$

  En effet : $a^k > b^k \quad (+)$

  Multiplions les deux membres de $(+)$ par a ou $(b+k)$

  On a :

  $$a^{k+1} > b^k(b+k) = b^{k+1} + kb^k$$

  Donc $a^{k+1} > b^{k+1}$

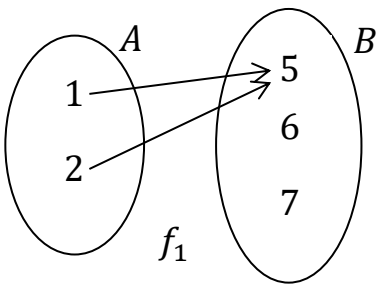
- Or la loi est vraie jusqu'à 3, donc elle est vraie pour $m = 4,5,6,\ldots$ c'est – à – dire la loi est vraie pour tout m

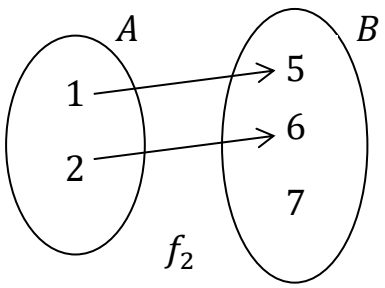
6.1.36.

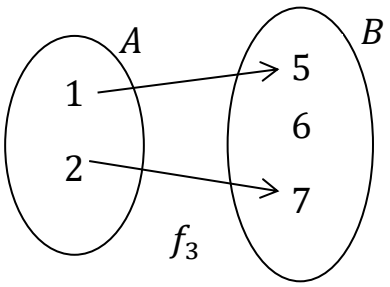
$A = \{1,2\}$ et $B = \{5,6,7\}$

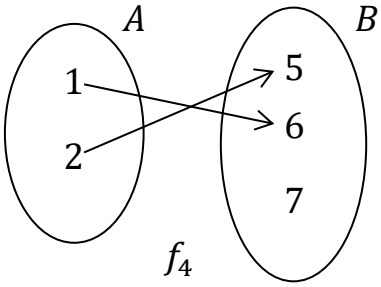
Il y a 3^2 applications distinctes possibles de A dans B : $f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9$

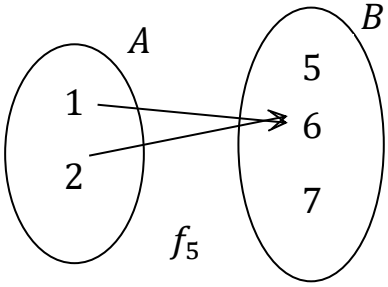
Représentation graphique

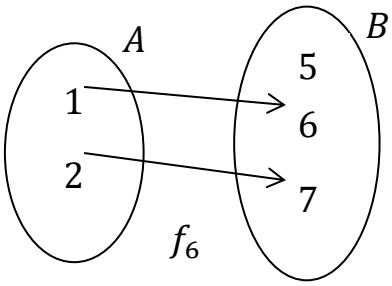


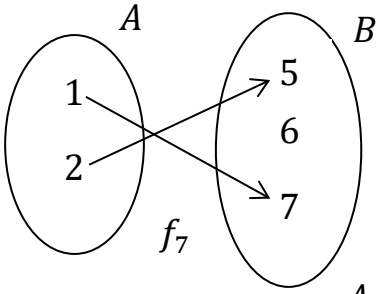


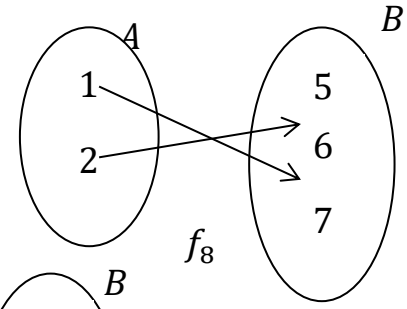


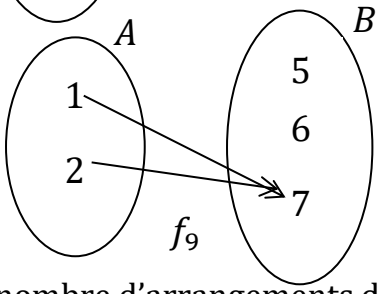












6.1.37.

Ce nombre est égal au nombre d'arrangements de 15 chevaux pris 3 à 3 c'est – à – dire

$$A_{15}^{3} = 15(15-1)(15-2) = 15.14.13 = 2730$$

6.1.38.

a. $A_{20}^{4} = 20 \times 19 \times 18 \times 17 = 116280$

b. $A_{15}^{2} \times A_{5}^{2} = 15 \times 14 \times 5 \times 4 = 4200$

6.1.39.

On a $A_n^4 = 12\,A_n^2 \Leftrightarrow \frac{n!}{(n-4)!} = 12\frac{n!}{(n-2)!}$

$\Rightarrow n!\,(n-2)! = 12n!\,(n-4)!$

$(n-2)! = 12(n-4)!$

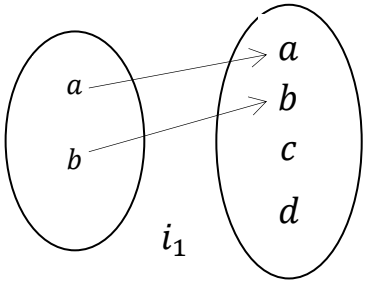
$(n-2)(n-3)(n-4)! = 12(n-4)!$

$(n-2)(n-3) = 12$ ou $n^2 - 5n - 6 = 0$

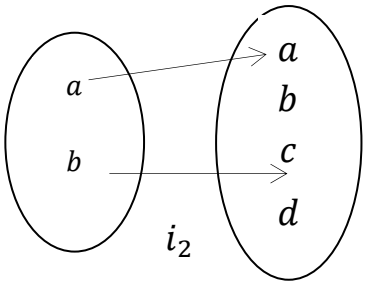
D'où $n = 6$ ou $n = -1$ (à rejeter)

6.1.40.

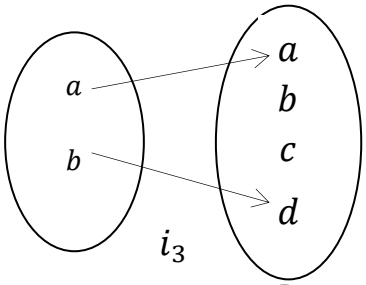
Il y en a $A_4^2 = 4.3 = 12$



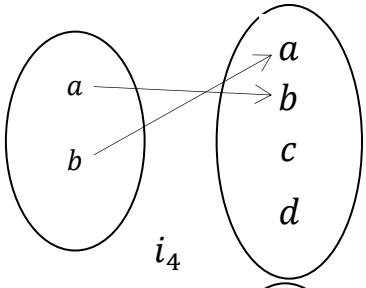
i_1



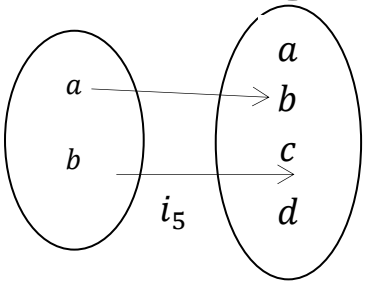
i_2



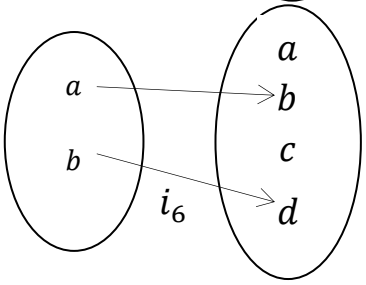
i_3



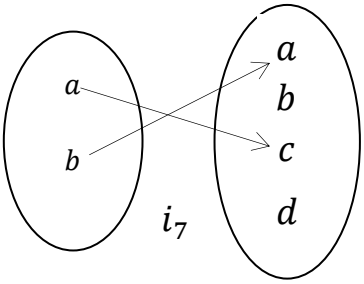
i_4



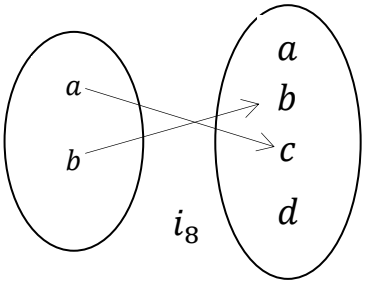
i_5



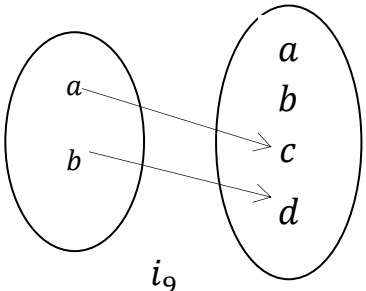
i_6



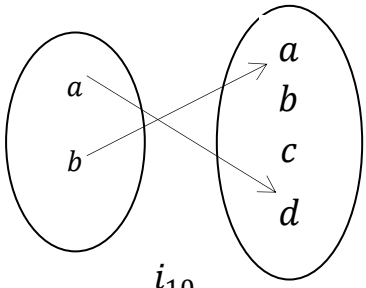
i_7



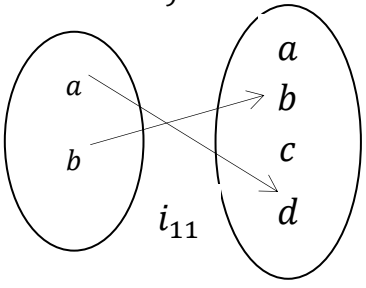
i_8



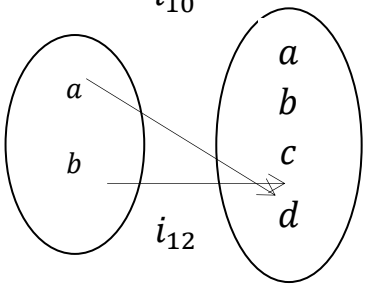
i_9



i_{10}



i_{11}



i_{12}

6.1.41.

Ce nombre de mots correspond à $A_6^3 = 6.5.4 = 120$ mots

6.1.42.

a. Toute rencontre constitue un choix de 2 équipes parmi 16 ; deux choix différents uniquement par leur composition

D'où le nombre de rencontres est $C_{16}^2 = 120$

b. Quand la compétition a lieu par matches aller – retour, deux choix différents également par l'ordre dans lequel les 2 équipes sont disposées. Il y a d'ailleurs dans ce cas 2 fois plus de rencontres que dans le cas précédent, soit $A_{16}^2 = 240$

6.1.43. $C_{10}^4 . C_8^3$ manières.

6.2. Exercices proposés

6.2.1. Déterminer parmi les ensembles suivants ceux qui sont égaux à l'ensemble vide

a. $\{x \in \mathbb{R}/1 < x < 2\}$ c. $\{x/x \in \emptyset\}$

b. $\{x \in \mathbb{N}/1 < x < 2\}$ d. $\{x \in \mathbb{R}/x^2 < x\}$

6.2.2. Déterminer toutes les relations d'inclusion et d'appartenance possibles entre les trois ensembles suivants

$$\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}$$

6.2.3. Trouver l'ensemble des parties $\mathcal{P}(E)$ de E

$$E = \{0, \emptyset, \{0, \emptyset\}, \{0, \emptyset, \{\emptyset\}\}\}$$

6.2.4. Soit $\mathcal{R}$ la relation dans l'ensemble $\mathbb{N}$ des entiers positifs définies par

$$x \mathcal{R} y \iff x + 2y = 12$$

a. Ecrire $\mathcal{R}$ sous forme d'un ensemble des couples
b. Trouver le domaine de $\mathcal{R}$
c. L'image de $\mathcal{R}$ et $\mathcal{R}^{-1}$?
d. Déterminer $\mathcal{R}^{-1} \circ \mathcal{R}$

6.2.5. On considère l'ensemble $\mathbb{N} \times \mathbb{N}$ des couples d'entiers positifs.

Soit $\simeq$ la relation dans $\mathbb{N} \times \mathbb{N}$ définie par

$$(a, b) \simeq (c, d) \text{ ssi } a + d = b + c$$

a. Démontrer que $\simeq$ est une relation d'équivalence
b. Trouver la classe d'équivalence de $(2,5)$

6.2.6. Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ et $g : \mathbb{R} \longrightarrow \mathbb{R}$ définies par

$$f(x) = x^2 + 3x + 1$$
$$g(x) = e^{2x+3}$$

Trouver les formules permettant de définir les applications composées suivantes

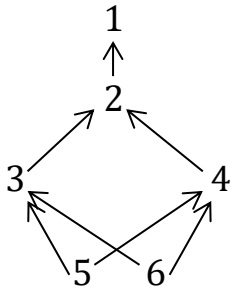
a. $f \circ g$ b. $g \circ f$ c. $f \circ f$

6.2.7. Soit $A = [-1, +1]$. Considérons les trois applications

$f : A \longrightarrow A, g : A \longrightarrow A$ et $h : A \longrightarrow A$ définies par
$f(x) = \sin x\,, g(x) = \sin \pi x,\ \ h(x) = \sin \frac{\pi}{2} x$
Indiquer si chacune de ces applications est
a. Injective b. Surjective c. Bijective

6.2.8. Soit $D_n = \left[0, \frac{1}{n}\right], n \in \mathbb{N}$
Calculer $\cap \{D_n : n \in \mathbb{N}\}$

6.2.9. Soit $E = \{1,2,3?\,4,5,6\}$, ordonnons E à l'aide de diagramme ci – contre
Considérons le sous – ensemble $A = \{2,3,4\}$ de E



- Trouver les éléments maximaux de E
- Trouver les éléments minimaux de E
- Déterminer si E possède un plus petit élément
- Déterminer si E possède un plus grand élément
- Trouver l'ensemble des majorants de A
- Trouver l'ensemble des minorants de A
- $\sup(A)$ existe – t – il ?
- $\inf(A)$ existe – t – il ?

6.2.10. Montrer par récurrence les égalités suivantes
a. $1 + 3 + 5 + \cdots + (2n - 1) = n^2$
b. $1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$

6.2.11. Démontrer les propriétés
d.1 à d.2 des pages 6 et 7
De même a et b de la page 24

6.2.12. Démontrer les propositions ci – après :
Si $f : A \longrightarrow B$, alors on a :

a. $Y_1 \subset Y_2 \Longrightarrow f^{-1}(y_1) \subset f^{-1}(y_2)$
b. $f^{-1}(\emptyset) = \emptyset$ mais $f^{-1}(y) = \emptyset$ n'implique pas nécessairement que $Y = \emptyset$
c. $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$
d. $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$
e. $f^{-1}(\complement\, Y) = \complement\big(f^{-1}(Y)\big)$
f. $f^{-1}\big(f(X)\big) \supset X, X$ sous – ensemble de A
g. $f\big(f^{-1}(Y)\big) \subset Y$ où $Y \subseteq B$
h. $X_1 \subset X_2 \Longrightarrow f(X_1) \subset f(X_2)$
i. $f(X) = \emptyset \Leftrightarrow X = \emptyset$
j. $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$
k. $f(X_1 \cap X_2) \subset f(X_1) \cap f(X_2)$
l. f injective $\Leftrightarrow \forall X_1, X_2 \subset A, f(X_1 \cap X_2) = f(X_1) \cap f(X_2)$

6.2.13. Soit $f_1 : X_1 \longrightarrow Y_1$ et $f_2 : X_2 \longrightarrow Y_2$
Montrer qu'il existe une et une seule application
$$f_1 \times f_2 : X_1 \times X_2 \longrightarrow Y_1 \times Y_2$$

$$Proj_{1,Y_1\times Y_2} \circ (f_1 \times f_2) = f_1 \circ proj_{1,X_1\times X_2}$$

et $$Proj_{2,Y_1\times Y_2} \circ (f_1 \times f_2) = f_2 \circ proj_{2,X_1\times X_2}$$

C'est – à – dire $f_1 \times f_2$ est l'unique application de $X_1 \times X_2$ dans $Y_1 \times Y_2$ rendant le diagramme commutatif.

6.2.14. Démontrer que

$\forall x, y \in \mathbb{R}$ et $n \in \mathbb{N}^*$, $(x+y)^n = \sum_{k=0}^{n} C_n^k \, x^{n-k} y^k$

6.2.15. Pour tout ensemble fini E, si E a n éléments, alors $\mathcal{P}(E)$ a 2^n éléments.

Chap. 2. Lois algébriques

§1. Lois de composition internes

1.1. Définitions

Soit E un ensemble

a. On appelle loi de composition interne (L.C.I.) – on dit aussi loi interne ou opération interne – sur un ensemble E, toute application du produit cartésien $E \times E$ dans E

Notations

Outre les notations habituelles : " $+$ " , " $-$ ", " $\times$ ", " $\div$ ", " $\circ$ ", " $\cap$ ", " $\cup$ ", " $\triangle$ " on se sert aussi de symboles tels que " $*$ " (étoile), " $\intercal$ " (truc), " $\perp$ " (anti – truc) pour désigner une L.C.I.

On peut donc écrire

Une L.C.I. est une application

$$E \times E \longrightarrow E : (x, y) \longmapsto x * y = z$$

x et y s'appellent les termes de l'opération

z est le résultat ou, mieux le composé de x et y par l'opération $*$

Un ensemble E muni d'une L.C.I. $*$ est un couple $(E,*)$ que l'on appelle **magma**.

On écrit $(E,*,\intercal)$ un ensemble E muni de deux L.C.I., " $*$ " et " $\intercal$ "

b. Une partie A de $(E,*)$ est dite **stable** par " $*$ " si et seulement si

$$\forall (x, y) \in A \times A, x * y \in A \text{ et}$$

L'application

$A \times A \longrightarrow A : (x, y) \longmapsto x * y$ est une opération dans A induite par " $*$ ", appelée **Loi induite** sur A

Exemples

(1) L'addition et la multiplication sont des opérations internes sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, ou $\mathbb{C}$

(2) L'addition est une L.C.I. sur $\mathbb{R}^2, \mathbb{R}^3, \dots, \mathbb{R}^3$ respectivement définie par

$$\big((x_1, y_1), (x_2, y_2)\big) \longmapsto (x_1, y_1) + (x_2, y_2) = (x_1 + y_1, x_2 + y_2)$$

$$\begin{aligned}\big((x_1, x_2, x_3), (y_1, y_2, y_3)\big) &\longmapsto (x_1, x_2, x_3) + (y_1, y_2, y_3) \\ &= (x_1 + y_1, x_2 + y_2, x_3 + y_3)\end{aligned}$$

$$\begin{aligned}\big((x_1, x_2, \dots, x_n), (y_1, y_2, \dots, y_n)\big) &\longmapsto (x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) \\ &= (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)\end{aligned}$$

(3) Soit E un ensemble et $\mathcal{P}(E)$ ensemble des parties de E. L'intersection et la réunion sont des lois internes dans $\mathcal{P}(E)$

(4) Dans $\mathbb{N}^*$, la division n'est pas une loi interne. C'est une opération seulement. $a \div b$ n'est défini dans $\mathbb{N}$ que si b est un multiple de a

(5) Si E est un ensemble fini, on peut dresser la **table de Pythagore** de la loi de composition. Par exemple,
Soit $E = \{a, b, c, d\}$ et définissons sur E la loi $*$ illustrée par la table ci – après :

2ème terme ⟶

$*$	a	b	c	d
a	c	c	a	b
b	a	b	b	a
c	d	d	d	c
d	c	a	b	d

1er terme ↑

On peut lire par exemple
$c * b = d$
$d * c = b$
…

1.2. Associativité et commutativité

Soit $(E,*)$ un magma

a. La loi $*$ est dite associative si et seulement si
$\forall x, y, z \in E, (x * y) * z = x * (y * z)$
b. La loi $*$ est dite commutative si et seulement si
$\forall x, y \in E, x * y = y * x$

Exemples

(1) Les L.C.E. $+$ et $\cdot$ dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$ sont associatives et commutatives

(2)

On a, en général, dans $\mathbb{R}^n$

$\forall x = (x_1, x_2, \dots, x_n), y = (y_1, y_2, \dots y_n), z = (z_1, z_2, \dots, z_n) \in \mathbb{R}^n$

$$\begin{aligned}(x + y) + z &= [(x_1, x_2, \dots, x_n) + (y_1, y_2, \dots y_n)] + (z_1, z_2, \dots, z_n)\\ &= [(x_1 + y_1, x_2 + y_2, \dots, x_n + y_n) + (z_1, z_2, \dots, z_n)]\\ &= [(x_1 + y_1) + z_1, (x_2 + y_2) + z_2, \dots, (x_n + y_n) + z_n]\\ &= [x_1 + (y_1 + z_1), x_2 + (y_2 + z_2), \dots, x_n + (y_n + z_n)]\\ &= [(x_1, x_2, \dots, x_n) + (y_1 + z_1, y_2 + z_2, \dots, y_n + z_n)]\\ &= (x_1, x_2, \dots, x_n) + [(y_1, y_2, \dots y_n) + (z_1, z_2, \dots, z_n)]\\ &= x + (y + z)\end{aligned}$$

(justifiez ces égalités)

$\forall x = (x_1, x_2, \dots, x_n), y = (y_1, y_2, \dots y_n) \in \mathbb{R}^n$

$$\begin{aligned}x + y &= (x_1, x_2, \dots, x_n) + (y_1, y_2, \dots y_n)\\ &= (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)\\ &= (y_1 + x_1, y_2 + x_2, \dots, y_n + x_n)\\ &= (y_1, y_2, \dots y_n) + (x_1, x_2, \dots, x_n)\\ &= y + x\end{aligned}$$

(3) L'intersection et la réunion dans $\mathcal{P}(E)$ sont aussi associatives et commutatives

(4) Cependant la soustraction $\mathbb{Z}$ ou $\mathbb{Q}$ n'est ni associative ni commutative

1.3. Elément neutre

Soit $(E,*)$ un magma

Un élément e de $(E,*)$ est dit :

a. Neutre à droite si $\forall x \in E, x * e = x$
b. Neutre à gauche si $\forall x \in E, e * x = x$
c. Neutre s'il est neutre à droite et à gauche c'est – à – dire

$$\forall x \in E, x * e = e * x = x$$

Exemples

(1) Dans $\mathbb{N}$ ou ($\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, $\mathbb{C}$), 0 est un élément neutre pour l'addition et 1 est un élément neutre pour la multiplication

(2) $(\mathcal{P}(E),\cup)$ et $(\mathcal{P}(E),\cap)$ admettent – ils un élément neutre ?

(3) Quel est l'élément neutre de $(\mathfrak{I}(E,E),\circ)$; $(\mathfrak{I}(E,E),\cdot)$; $(\mathbb{R}^n, \cdot)$

(4) ……. La division n'admet pas d'élément neutre.

d. Proposition

Si l'élément neutre existe, il est unique

Démonstration

Supposons que le magma $(E,*)$ ait deux éléments neutres e et e'

Alors $e * e' = e'$ (car e élément neutre et $e \in E$) et, aussi

$e * e' = e$ (car e' élément neutre et $e' \in E$)

Donc $e = e'$

1.4. Eléments réguliers, Eléments symétrisables

Soit $(E,*)$ un magma. On dit qu'un élément $a \in E$ est

a. Régulier à droite si : $\forall x, y \in E, x * a = y * a \Longrightarrow x = y$

b. Régulier à gauche si : $\forall x, y \in E, a * x = a * y \Longrightarrow x = y$

c. Régulier s'il est régulier à droite et à gauche c'est – à – dire

$$\forall x, y \in E, \begin{matrix} x*a=y*a \Longrightarrow x=y \\ a*x=a*y \Longrightarrow x=y \end{matrix} \text{ et}$$

Remarque : on utilise aussi l'expression : "élément simplifiable" au lieu de "élément régulier"

On suppose que le magma $(E,*)$ a un élément neutre e, (magma unifère)

Un élément $x \in E$ admet

d. Un symétrique à droite s'il existe $y \in E$, $x * y = e$

e. Un symétrique à gauche s'il existe $z \in E$, $z * x = e$

f. Un symétrique s'il existe un élément $x' \in E$ qui soit à la fois symétrique à droite et à gauche de x

Autrement dit, x' est symétrique de x si et seulement si

$$x * x' = x' * x = e$$

Remarques

Un élément x est dit symétrisable s'il admet un symétrique. Ce symétrique sera noté $\bar{x}$. On note

a^{-1} le symétrique de a dans $(E, \cdot)$ et on l'appelle inverse de a

$-a$ le symétrique de a dans $(E, +)$ et on l'appelle opposé de a

Exemples

(1) $\forall a \in \mathbb{N}$ (ou $\mathbb{Z}$) a est régulier pour l'addition

En effet : $\forall x, y \in \mathbb{N}, \begin{matrix} x+a=y+a \Longrightarrow x=y \\ a+x=a+y \Longrightarrow x=y \end{matrix}$

(2) $\forall a \in \mathbb{N}^*$ (ou $\mathbb{Z}^*$), a est simplifiable pour la multiplication

(3) Dans $\mathcal{P}(E)$, aucun élément, sauf E, n'est simplifiable pour $\cap$

(4) Dans $(\mathcal{P}(E),\cup)$, y a – t – il d'éléments simplifiables ?

(5) Dans $\mathbb{N}$, aucun élément, sauf 0, n'est symétrisable pour $+$

(6) Dans $(\mathbb{Z}, +)$ tout élément admet un opposé
Car $\forall x \in \mathbb{Z}, \exists -x \in \mathbb{Z} / x + (-x) = 0$

(7) Dans $(\mathbb{R}^*, \cdot)$ tout élément admet un inverse
Car $\forall x \in \mathbb{R}^*, \exists x^{-1} = \frac{1}{x} \in \mathbb{R}^* / x \cdot x^{-1} = 1$

(8) Pour la multiplication dans $\mathbb{N}$, aucun élément, sauf 1, n'est symétrisable

(9) Pour la réunion ou l'intersection dans $\mathcal{P}(E)$, aucun élément, sauf l'élément neutre, n'est symétrisable

1.5. Distributivité

Soit $(E, *, \intercal)$ un ensemble E muni de deux L.C.I. " $*$ " et " $\intercal$ " on dit que la loi $*$ est

a. Distributive à droite par rapport à $\intercal$ si :
$\forall x, y, z \in E, (x \intercal y) * z = (x * z) \intercal (y * z)$

b. Distributive à gauche par rapport à $\intercal$ si :
$\forall x, y, z \in E, x * (y \intercal z) *= (x * y) \intercal (x * z)$

c. Distributive par rapport à " $\intercal$ " lorsqu'elle est distributive à droite et distributive à gauche

Exemples

(1) Dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, ou $\mathbb{C}$ la multiplication est distributive par rapport à l'addition

(2) Dans $\mathcal{P}(E)$ chacune des lois $\cup$ et $\cap$ est distributive par rapport à l'autre.
En effet :
$$\forall A, B, C \in \mathcal{P}(E), \begin{matrix} A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \\ A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \end{matrix}$$

(3) Soit $(\mathbb{Z}, +)$ le groupe additif des entiers rationnels et considérons une autre loi interne " $\intercal$ " définie sur $\mathbb{Z}$ par
$(a, b) \longmapsto a \intercal b = a$
La loi " $\intercal$ " est – elle distributive par rapport à la loi " $+$ "

1.6. Compatibilité

a. Définition
Soit $(E, *)$ un magma et considérons une relation binaire $\mathcal{R}$ sur E. On dit que la relation binaire

a.1. est compatible à droite avec la loi $*$ si
$\forall x, y \in E, x \mathcal{R} y \Longrightarrow \forall z \in E, (x * z) \mathcal{R} (y * z)$

a.2. est compatible à gauche avec la loi $*$ si
$\forall x, y \in E, x \mathcal{R} y \Longrightarrow \forall z \in E, (z * x) \mathcal{R} (z * y)$

a.3. est compatible avec la loi $*$
$\forall x, y, x', y' \in E, x \mathcal{R} y$ et $x' \mathcal{R} y' \Longrightarrow (x * x') \mathcal{R} (y * y')$

Exemples

- Soit le magma $(\mathbb{N}, +)$

(1) La relation $\leq$ est compatible avec la loi $+$
En effet,
$\forall x, y, x', y' \in \mathbb{N}, x \leq y$ et $x' \leq y' \Longrightarrow (x + x') \leq (y + y')$

(2) La relation de divisibilité / n'est pas compatible avec la loi $+$. Car

$$\exists x, y, x', y' \in \mathbb{N},\ x/y \text{ et } x'/y' \text{ et } x + x'/y + y' \text{ (ne divise pas)}$$

b. Compatibilité d'une relation d'équivalence avec une L.C.I.

b.1. Considérons un ensemble E sur lequel sont définies une relation d'équivalence $\mathcal{R} : x \equiv y (\mathrm{mod}\ \mathcal{R})$ et une L.C.I. $*$

On dit que la relation d'équivalence est

- Compatible à droite avec la loi $*$ si

$$\forall x, y \in E, x \equiv y (\mathrm{mod}\ \mathcal{R}) \Longrightarrow \forall z \in E, x * z \equiv y * z (\mathrm{mod}\ \mathcal{R})$$

- Compatible à gauche avec la loi $*$ si

$$\forall x, y \in E, x \equiv y (\mathrm{mod}\ \mathcal{R}) \Longrightarrow \forall z \in E, z * x \equiv z * y (\mathrm{mod}\ \mathcal{R})$$

- Compatible avec la loi $*$

$$\forall x, y, x', y' \in E, [x \equiv y (\mathrm{mod}\ \mathcal{R}) \text{ et } x' \equiv y' (\mathrm{mod}\ \mathcal{R})] \Longrightarrow x * x' \equiv y * y' (\mathrm{mod}\ \mathcal{R})$$

b.2. La relation d'équivalence $\mathcal{R}$ est compatible avec la loi $*$, alors la correspondance

$E/_{\mathcal{R}} \times E/_{\mathcal{R}} \longrightarrow E/_{\mathcal{R}} : (\dot{x}, \dot{y}) \longmapsto \widehat{x * y}$ est une application. Montrez – le

b.3. Cette application définit une L.C.I. sur $E/_{\mathcal{R}}$ que l'on notera $\dot{*}$. On a :

$$\forall \dot{x}, \dot{y} \in E/_{\mathcal{R}}, \dot{x} \dot{*} \dot{y} = \widehat{x * y}$$

$\dot{*}$ s'appelle la loi – quotient de $*$ par la relation d'équivalence $\mathcal{R}$

Exemple

Dans $\mathbb{Z}$, la relation $\equiv$ suivante

$x \equiv y \Leftrightarrow x - y$ est divisible par p $(p > 0)$ est compatible avec l'addition et la multiplication dans $\mathbb{Z}$

Montrer, à l'aide de la table de multiplication pour $p = 6$, que x peut être régulier pour la loi définie sur E et $\dot{x}$ ne pas l'être pour la loi quotient

§2. Lois de composition externes

2.1. Définitions

On appelle loi de composition externe (L.C.E.) ou simplement loi externe. On dit aussi opération externe ou action d'un ensemble K sur un autre ensemble E, toute application

$$\mu : K \times E \longrightarrow E : (\alpha, x) \longmapsto \mu(\alpha, x)$$

$\mu(\alpha, x)$ s'écrit généralement $\alpha.x$ ou αx et s'appelle la composée de α et de x pour la L.C.E. considérée

2.2. Relations entre L.C.I. et L.C.E.

Le cas le plus intéressant est celui où K et E sont eux – mêmes munis d'un ou plusieurs L.C.I. et qu'il en résulte des relations entre la loi externe et ces lois internes. Notons celles que nous aurons à utiliser au chap.2 de la 2ème partie : soient $(K,\top)$ et $(E,*)$ des magmas,

Si $\forall \alpha, \beta \in K; \forall x, y \in E$:

a. $\alpha(x * y) = \alpha x * \alpha y$, on dit que la L.C.E. est distributive par rapport à la L.C.I. de E
b. $(\alpha \top \beta)x = \alpha x * \beta y$, on dit que la L.C.E. est distributive par rapport aux L.C.I. $\top$,$*$
c. $(\alpha \top \beta)x = \alpha(\beta x)$, on dit que la L.C.E. est associative par rapport à la loi $\top$ de K
d. Il existe un élément neutre $e \in K$ pour la loi $\top$ telle que $e \top x = x$

Exemples

(1) Soit $K = \mathbb{R}$ et $E = \mathcal{V}$ ensemble des vecteurs libres de la géométrie élémentaire. Ainsi la multiplication d'un vecteur $\vec{v}$ par un réel α c'est – à – dire l'application

$$\mathbb{R} \times \mathcal{V} \longrightarrow \mathcal{V}$$
$$(\alpha, \vec{v}) \longmapsto \alpha.\vec{v} \text{ est une L.C.E. de } \mathbb{R} \text{ sur } \mathcal{V}$$

(2) Quels que soient les ensembles K et E,

$$pr_2 : K \times E \longrightarrow E \text{ est une action}$$

(3) Une loi externe de $\mathbb{R}$ sur $\mathbb{R}, \mathbb{R}^2, \dots, \mathbb{R}^n$ est définie respectivement par les applications ci – après :

$$\mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R} : (\alpha, x) \longmapsto \alpha x$$
$$\mathbb{R} \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2 : \big(\alpha, (x, y)\big) \longmapsto \alpha(x, y) = (\alpha x, \alpha y)$$
$$\mathbb{R} \times \mathbb{R}^3 \longrightarrow \mathbb{R}^3 : \big(\alpha, (x, y, z)\big) \longmapsto \alpha(x, y, z) = (\alpha x, \alpha y, \alpha z)$$
$$\dots \quad \dots \quad \dots$$
$$\mathbb{R} \times \mathbb{R}^n \longrightarrow \mathbb{R}^n : \big(\alpha, (x_1, x_2, \dots, x_n)\big) \longmapsto \alpha(x_1, x_2, \dots, x_n) = (\alpha x_1, \alpha x_2, \dots, \alpha x_n)$$

- Montrer que dans chaque cas les relations $i), ii), iii)$ et $iv)$ ci – dessus sont vérifiées. Par exemple,

$\forall \alpha, \beta \in \mathbb{R}; \forall (x, y), (x', y') \in \mathbb{R}^2$,

i) $\alpha[(x, y) + (x', y')] = \alpha(x, y) + \alpha(x', y')$
ii) $(\alpha + \beta)(x, y) = \alpha(x, y) + \beta(x, y)$
iii) $\alpha[\beta(x, y)] = (\alpha\beta)(x, y)$
iv) $1(x, y) = (x, y)$

(4) L'application

$$\mathbb{R} \times \mathbb{R}^{\mathbb{R}} \longrightarrow \mathbb{R}^{\mathbb{R}} : (\alpha, f) \longmapsto \alpha f$$

Définit une action de $\mathbb{R}$ sur $\mathbb{R}^{\mathbb{R}}$

Noter que

$$\alpha f : \mathbb{R} \longrightarrow \mathbb{R} : x \longmapsto (\alpha f)(x) = \alpha f(x)$$

- Vérifier les propriétés $i), ii), iii)$ et $iv)$

(5) On a une loi externe de $\mathbb{R}$ sur $\mathbb{R}[x]$ telle que si $\alpha \in \mathbb{R}$ et

$$p(x) = \sum a_i x^i \in \mathbb{R}[x], \alpha p(x) = \sum (\alpha a_i) x^i$$

- Etablir les relations $i), ii), iii)$ et $iv)$ entre la L.C.I. $+$ dans $\mathbb{R}$ et la L.C.E.

Chap. 3. Structure de demi – groupes et monoïdes, groupes, anneaux et corps

§1. Structures de demi – groupes et monoïdes

1.1. Définitions

Soit $(E,*)$ un magma

a. On appelle demi – groupe, un magma $(E,*)$ tel que la loi $*$ est associative sur E
b. On appelle monoïde, un demi – groupe $(E,*)$ tel que la loi $*$ admet un élément neutre

Exemples

(1) $(\mathbb{N},+)$ est un demi – groupe. Il est en plus un monoïde
(2) Si E est un ensemble quelconque, alors $(\mathcal{P}(E),\cup)$ et $(\mathcal{P}(E),\cap)$ sont des monoïdes

1.2. Propositions

a. Proposition

Tout élément symétrisable d'un monoïde est régulier

Démonstration

Soient a élément symétrisable d'un monoïde $(E,*)$ et $\bar{a}$ le symétrique de a, on a :

$$a * x = a * y \Longrightarrow \bar{a} * (a * x) = \bar{a} * (a * y)$$
$$(\bar{a} * a) * x = (\bar{a} * a) * y \quad (* \text{ est associative})$$
$$e * x = e * y \qquad (\bar{a} * a = e)$$

D'où $x = y$

b. Proposition

Soit $(E,*)$ un monoïde

Si un élément x de E admet un symétrique à gauche et un symétrique à droite, les deux symétriques coïncident et x est alors symétrisable.

Démonstration

Soient z un symétrique à gauche et z' un symétrique à droite de x et e élément neutre dans E

On a : $z = z * e = z * (x * z') = (z * x) * z' = e * z' = z'$

D'où $z = z'$

c. Proposition

Soit $(E,*)$ un monoïde

Si un élément x de E est symétrisable, son symétrique $\bar{x}$ est également symétrisable et $x$est le symétrique de $\bar{x}$.

Si des éléments x et y de E sont symétrisables, $x * y$ est également symétrisable et

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

Démonstration

- La relation $x * \bar{x} = e = \bar{x} * x$ exprime aussi bien « $\bar{x}$ est le symétrique de x » que « x est le symétrique de $\bar{x}$ »
- Soient $\bar{x}$ le symétrique de x
  $\bar{y}$ le symétrique de y
  Alors $\bar{y} * \bar{x}$ est le symétrique de $x * y$
  En effet $(x * y) * (\bar{y} * \bar{x}) = x * (y * \bar{y}) * \bar{x} = x * e * \bar{x} = x * \bar{x} = e$
  et $(\bar{y} * \bar{x}) * (x * y) = \bar{y} * (\bar{x} * x) * y = \bar{y} * e * y = \bar{y} * y = e$

§2. Structures de groupes

2.1. Définition

Un groupe est un monoïde $(G,*)$ où tout élément de G est symétrisable.
En d'autres termes
Un groupe est un couple $(G,*)$, formé d'un ensemble G et d'une loi de composition interne $*$ sur G telle que

a. La loi $*$ est associative
b. La loi $*$ admet un élément neutre, et
c. Tout élément de G admet un symétrique.

Exemples

(1) $(\mathbb{Z},+)$; $(\mathbb{Q},+)$; $(\mathbb{R},+)$; … ; $(\mathbb{R}^n,+)$; $(\mathbb{C},+)$ sont des groupes
(2) $(\mathbb{Q}^*,\cdot)$; $(\mathbb{Q}^+,\cdot)$; $(\mathbb{R}^*,\cdot)$; $(\mathbb{C}^*,\cdot)$ sont des groupes
(3) Soit A un ensemble quelconque. Désignons par $\sum A$ l'ensemble des bijections de A vers A le couple $(\sum A,\circ)$ est un groupe, appelé groupe des permutations de l'ensemble A
(4) $(\mathbb{R}^{\mathbb{R}},+)$; $(\mathbb{R}^{\mathbb{R}},\cdot)$ et $(\mathbb{R}^{\mathbb{R}},\circ)$ sont des groupes

2.2. Théorème

Pour un demi – groupe $(G,*)$, les affirmations suivantes sont équivalentes

i. $(G,*)$ est un groupe
ii. $G \neq \emptyset$ et $\forall a,b \in G$, les équations $a * x = b$ et $y * a = b$ admettent une et une seule solution dans G

Démonstration

$i \Longrightarrow ii$

Soit $(G,*)$ un groupe. Considérons l'équation $a * x = b$

On a : $\bar{a} * (a * x) = \bar{a} * b$ ($\bar{a}$ symétrique de a)
$(\bar{a} * a) * x = \bar{a} * b$ (associativité de $*$)
$e * x = \bar{a} * b$ (e élément neutre de G)
$x = \bar{a} * b$ Solution de l'équation $a * x = b$

Cette solution est unique

Car si x et x' sont des solutions
On a : $a * x = b = a * x'$ et donc $x = x'$ (car tout élément de G est régulier)
$ii \Longrightarrow i$ C'est – à – dire
Si $E \neq \emptyset$ et que les équations $a * x = b$ et $y * a = b$ admettent chacune une solution
$\forall a, b \in G$, montrons que $(G,*)$ est un groupe

- La loi $*$ a été supposée associative
- Comme $G \neq \emptyset$, soit $a \in G$

L'équation $a * x = a$ admet e comme une solution
L'équation $y * a = a$ admet e' comme une solution
$\forall z \in G$, soient $y, y' \in G / \ z = y * a$ et $z = a * y'$

On a : $z * e = (y * a) * e = y * (a * e)$ (associativité de $*$)
$= y * a$ (e solution de $a * x = a$)
$= z$

$e' * z = e' * (a * y') = (e' * a) * y'$
$= a * y'$ (e' solution de $y * a = a$)
$= z$

D'où $\forall z \in G, \ z * e = z$, en particulier $e' * e = e'$
$e' * z = z$, en particulier $e' * e = e$
Donc $e = e'$ et e élément neutre

- $\forall z \in G$, soient $\bar{z}$ et z' solution des équations $z * \bar{z} = e$
  $z' * z = e$
  Alors d'après la proposition 2-1.3, $\bar{z}$ et z' sont le symétrique de z.
  Donc $(G,*)$ est un groupe.

2.3. Groupe abélien

a. <u>Définition</u>

Un couple $(G,*)$ est dit abélien ou commutatif si la loi interne $*$ est commutative
<u>Exemple</u>
$(\mathbb{Z}, +)$; $(\mathbb{Q}, +)$; $(\mathbb{R}, +)$; … ; $(\mathbb{R}^n, +)$; $(\mathbb{C}, +)$ sont des groupes abélien
Par contre $(\sum A, \circ)$ est en général non abélien

b. <u>Remarque</u>

Dans un groupe abélien, la loi de composition est habituellement notée $+$, comme addition. On dit alors que la loi est notée additivement. Dans ce cas la définition de groupe abélien se traduit par

i) $\forall x, y, z \in G, (x + y) + z = x + (y + z)$
ii) $\exists 0 \in G / \forall x \in G, x + 0 = x$
iii) $\forall x \in G, \exists \bar{x} \in G$ noté $-x / x + (-x) = 0$ ($\bar{x} = -x$: opposé de x)
iv) $\forall x, y \in G, x + y = y + x$

2.4. Groupes finis

a) Définitions

Un groupe $(G,*)$ est dit fini si l'ensemble G a un nombre fini d'éléments. On appelle **ordre** de G, le nombre d'éléments de G

Notation

L'ordre de G se note $|G|$ ou $\#\ G$

Exemple

Soit $G = \{1,2,3\}$, alors $(\sum G,\circ)$ est un groupe fini

On a : $\mathscr{p}_1 : (1,2,3) \longmapsto (1,2,3)$ $\quad$ $\mathscr{p}_4 : (1,2,3) \longmapsto (2,3,1)$

$\mathscr{p}_2 : (1,2,3) \longmapsto (1,3,2)$ $\quad$ $\mathscr{p}_5 : (1,2,3) \longmapsto (3,1,2)$

$\mathscr{p}_3 : (1,2,3) \longmapsto (2,1,3)$ $\quad$ $\mathscr{p}_6 : (1,2,3) \longmapsto (3,2,1)$

D'où $\sum G = \{\mathscr{p}_1, \mathscr{p}_2, \mathscr{p}_3, \mathscr{p}_4, \mathscr{p}_5, \mathscr{p}_6\}$

Donc $|\sum G| = 6$ et $(\sum G\ ,\ \circ)$ est un groupe

Si $|G| = n$, alors $|\sum G| = n!$

b) Remarque

L'ensemble sous – jacent à un groupe doit contenir au moins un élément, à savoir l'élément neutre

2.5. Sous – groupes d'un groupe

a. Définition

Soit $(G,*)$ un groupe

Un sous – ensemble $P \subseteq G$ est appelé sous – groupe (s.g.) du groupe $(G,*)$ lorsque la loi interne $*$ restreinte aux éléments de P est interne et définit une structure de groupe sur P

Exemples

1) $\mathbb{Z}$ est un sous – groupe de $(\mathbb{Q},+)$ car $\mathbb{Z} \subset \mathbb{Q}$ et $(\mathbb{Z},+)$ est un groupe
   De même
2) $\mathbb{Q}$ est un sous – groupe de $(\mathbb{R},+)$
3) $\mathbb{R}$ est un sous – groupe de $(\mathbb{C},+)$
4) $\mathbb{Z},\mathbb{Q},\mathbb{R}$ sont des sous – groupes de $(\mathbb{C},+)$, etc.

b. Proposition

Soient $(G,*)$ un groupe et $P \subseteq G$

P sous – groupe de $(G,*) \Leftrightarrow i) P \neq \emptyset$

$ii) \forall x,y \in P, x * \bar{y} \in P$

Démonstration

$\Longrightarrow$

P s.g. est, par définition, un groupe. Donc $P \neq \emptyset$

En outre, $\forall x,y \in P$, le symétrique de y, soit $\bar{y} \in P$

D'où $x * \bar{y} \in P$ (car $*$ est une loi de composition interne)

$\Leftarrow$

Soit $a \in P$, on a : $a * \bar{a} = e \in P$. D'où P contient un élément neutre.

$\forall z \in P, \bar{z} = e * \bar{z} \in P$ d'où P contient les symétriques de ses éléments

$\forall x, y \in P, y$ est le symétrique de $\bar{y} \Longrightarrow x * y \in P$ ($*$ une loi de composition interne)

En plus $*$ est associative (par hypothèse)

Donc $(P,*)$ est un groupe.

c. <u>Relation d'équivalence modulo un sous – groupe</u>

Soient $(G,*)$ un groupe et P s.g. de $(G,*)$ considérons la relation $\equiv$ définie sur G par

$$x \equiv y \Leftrightarrow \bar{x} * y \in P$$

La relation ainsi définie est une relation d'équivalence

En effet,

i) Réflexivité : $\forall x \in G, x \equiv x$ car $\bar{x} * x = e \in P$

ii) Symétrie : $\forall x, y \in G, x \equiv y \Longrightarrow y \equiv x$

Car $x \equiv y \Longrightarrow \bar{x} * y \in P$

$\Longrightarrow \overline{\bar{x} * y} = \bar{y} * \bar{\bar{x}} = \bar{y} * x \in P$

D'où $y \equiv x$

iii) Transitivité : $\forall x, y, z \in G, x \equiv y$ et $y \equiv z \Longrightarrow x \equiv z$

Car $\left.\begin{matrix} x \equiv y \Leftrightarrow \bar{x} * y \in P \\ y \equiv z \Leftrightarrow \bar{y} * z \in P \end{matrix}\right\} \Longrightarrow (\bar{x} * y) * (\bar{y} * z) \in P$

Mais $(\bar{x} * y) * (\bar{y} * z)$

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

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

$= \bar{x} * z \in P$

D'où $x \equiv z$

Cette relation d'équivalence établie sur E s'appelle **équivalence à droite** modulo P

La classe d'équivalence d'un élément $a \in G$ s'appelle **classe à droite** de a modulo P

On a :

$$cl(a) = \{x \in G / a \equiv x\}$$
$$= \{x \in G / \bar{a} * x \in P\}$$
$$\bar{a} * x \in P \Leftrightarrow x \in a * P$$
$$\text{où } a * P = \{a * u / u \in P\}$$

Donc, la classe à droite de a modulo P est le sous – ensemble $a * P$

De même on définit sur G la relation d'équivalence à gauche modulo P

$$x \equiv y \Leftrightarrow x * \bar{y} \in P$$

La classe à gauche modulo P d'un élément $a \in G$ est le sous – ensemble

$$P * a = \{u * a / u \in P\}$$

d. <u>Application</u>

Soit le sous – groupe $4\mathbb{Z}$ de $(\mathbb{Z}, +)$

$4\mathbb{Z} = \{4u / u \in \mathbb{Z}\}$

$= \{\dots, -16, -12, -8, -4, 0, 4, 8, 12, 16, 20, \dots\}$

La relation d'équivalence modulo $4\mathbb{Z}$ est définie par

$$x \equiv y \Leftrightarrow y - x \in 4\mathbb{Z}$$

Ou encore

$$x \equiv y \Leftrightarrow \exists k \in \mathbb{Z} / y - x = 4k$$

Par exemple, la classe modulo $4\mathbb{Z}$ de l'entier 2 est le sous – ensemble

$$2 + 4\mathbb{Z} = \{2 + 4u / u \in \mathbb{Z}\}$$
$$= \{\dots, -10, -6, -2, 2, 6, 10, 14, 18, \dots\}$$

On a, par exemple, $2 \equiv -10$ car $-10 - 2 = -12 \in 4\mathbb{Z}$

$2 \equiv -2$ car $-2 - 2 = -4 \in 4\mathbb{Z}$

En général, on peut considérer le s.g. $n\mathbb{Z}$, pour n entier quelconque. Comme $(\mathbb{Z}, +)$ est abélien, l'équivalence à droite et l'équivalence à gauche coïncident.

Au lieu de :

- Equivalence modulo $n\mathbb{Z}$, on dit congruence modulo n
- Classe modulo $n\mathbb{Z}$, on dit classe modulo n

e. <u>Théorème</u>

Soient $(G, *)$ un groupe et P un s.g. de $(G, *)$

Toutes les classes d'équivalence à droite (à gauche) modulo P ont même cardinal

<u>Démonstration</u>

$\forall a \in G$, considérons l'application

$$f : a * P \longrightarrow P$$
$$x \longmapsto f(x) = \bar{a} * x$$

i) f est injectif

En effet, $f(x_1) = f(x_2) \Longrightarrow x_1 = x_2$

$$\Updownarrow$$

$$\bar{a} * x_1 = \bar{a} * x_2 \Longrightarrow x_1 = x_2$$

ii) f est surjectif

En effet, $\forall u \in P, \exists x \in a * P / f(x) = u$

$$\Updownarrow$$

$$\bar{a} * x = u$$

On a : $a * (\bar{a} * x) = a * u$

$$(a * \bar{a}) * x = a * u$$
$$e * x = a * u$$
$$\Longrightarrow x = a * u$$

D'où $|a * P| = |P|$

f. <u>Corollaire</u> : théorème de Lagrange

Soient G un groupe fini d'ordre n

P un s.g. de G

Alors l'ordre de P divise n

<u>Démonstration</u>

Les classes modulo P ont chacune le même nombre d'éléments, soit p l'ordre de P.

Puisque les classes d'équivalences distinctes sont disjointes et que G est la réunion de toutes les classes, si k est le nombre de toutes les classes, on a :

$$n = |E| = k|P| = kp \Longrightarrow p \text{ divise } n$$

g. Soient $(G,*)$ un groupe et P un sous – groupe

- Alors le quotient de l'ensemble G par la relation d'équivalence à droite modulo P est noté G/P.
  $G/P = \{cl(a)/a \in G\}$

2.6. Sous – groupe normal – Groupe quotient

a. Définition

Un sous–groupe P d'un groupe $(G,*)$ est dit **normal** lorsque $\forall a \in G, a * P = P * a$
Cette relation s'exprime encore par

$$\forall a \in G, \forall h \in P, a * h * \bar{a} \in P$$

Au lieu de normal, on dit aussi **distingué** ou **invariant**

Exemple

$4\mathbb{Z}$ est un sous – groupe normal de $(\mathbb{Z}, +)$ car $\forall a \in \mathbb{Z}, a + 4\mathbb{Z} = 4\mathbb{Z} + a$

b. Théorème

Soient $(G,*)$ un groupe et P un sous–groupe. Les affirmations suivantes sont équivalentes

i) P est un sous – groupe distingué
ii) La relation d'équivalence à droite et la relation d'équivalence à gauche modulo P coïncident
iii) La relation d'équivalence modulo P est compatible avec l'opération interne sur G
iv) Il existe une loi de composition interne $\perp$ sur l'ensemble quotient G/P telle que

$$cl(x) \perp cl(y) = cl(x * y) \quad \forall x, y \in G$$

Démonstration

$$\begin{array}{ccc} i & \Longrightarrow & ii \\ \Uparrow & & \Downarrow \\ iv & \Longleftarrow & iii \end{array}$$

- Montrons que $i \Longrightarrow ii$

En effet, $\forall x \in G$, la classe à droite mod P de x est $x * P$
la classe à gauche mod P de x est $P * x$
Alors si P est un sous – groupe distingué, $x * P = P * x$ et par conséquent les deux relations d'équivalence (à droite et à gauche mod P) sont identiques

- Montrons que $ii \Longrightarrow iii$

En effet, $\forall x, y \in G$, si x et y sont équivalents mod P
On a : $\bar{x} * y \in P$

$x * \bar{y} \in P$ (cas les deux relations sont identiques)

De $\bar{x} * y \in P$, on a : $(\bar{x} * y * z) * \bar{z} \in P$, $\forall z \in P$

ou $\bar{z} * (\bar{x} * y * z) \in P$

$\Longrightarrow (\bar{z} * \bar{x}) * (y * z) \in P$

ou $(\overline{x * z}) * (y * z) \in P$

Ceci montre que si

x est équivalent mod P y, alors

$x * z$ est équivalent mod P $y * z$

De $x * \bar{y} \in P$, on a : $(x * \bar{y} * \bar{z}) * z \in P$

$\Longrightarrow (z * x) * (\bar{y} * \bar{z}) \in P$

ou $(z * x) * (\overline{z * y}) \in P$

D'où si « x est équivalent mod P y »

Alors « $z * x$ est équivalent mod P $z * y$ »

- Montrons que $iii \Longrightarrow iv$
  Supposons que la relation d'équivalence mod P est compatible avec la loi interne $*$ et $x \equiv x'$
  $y \equiv y'$
  On a : $x * y \equiv x' * y$ et $x' * y \equiv x' * y'$ donc $x * y \equiv x' * y'$
  $\Longrightarrow cl(x * y) = cl(x' * y')$ $\forall x' \in cl(x)$ et $\forall y' \in cl(y)$ et la formule $cl(x) \perp cl(y) = cl(x * y)$ définit une loi de composition interne sur G
- Montrons enfin que $iv \Longrightarrow i$
  $\forall a \in G$ et $\forall h \in P$,
  $cl(a) = cl(e * a) = cl(e) \perp cl(a) = cl(h) \perp cl(a) = cl(h * a)$
  D'où $\bar{a} * h * a \in P$ ou $P * a = a * P$
  Donc P est distingué.

c. <u>Groupe quotient</u>

Lorsque l'une des conditions $i) \dots iv)$ du théorème précédent est réalisée, le couple $(G/P, \perp)$ est un groupe appelé **groupe quotient** de G par P

<u>Exemple d'application</u>

Soit n un entier quelconque, le sous – groupe $n\mathbb{Z}$ de $(\mathbb{Z}, +)$ est distingué (car $(\mathbb{Z}, +)$ est abélien)

Alors $\left(\mathbb{Z}/_{n\mathbb{Z}}, \perp\right)$ est un groupe quotient de $\mathbb{Z}$ par $n\mathbb{Z}$

La formule $cl(x) \perp cl(y) = cl(x + y)$ définit la loi de composition interne sur $\mathbb{Z}/_{n\mathbb{Z}}$

La relation $\equiv$ d'équivalence mod $n\mathbb{Z}$ se traduit par

$x \equiv y \Leftrightarrow y - x$ est un multiple de n

Au lieu de « Equivalence modulo $n\mathbb{Z}$ », on dit

« **Congruence modulo** n »

A cet effet, si x et y sont équivalents modulo $n\mathbb{Z}$, on dit x et y sont congrus modulo n et on écrit $x \equiv y \bmod n$

On note aussi $\mathbb{Z}/_{n\mathbb{Z}}$ par $\mathbb{Z}_n$

$\mathbb{Z}_n = \{\hat{0}, \hat{1}, \hat{2}, \dots, \widehat{n-1}\}$

Si $n = 5, \mathbb{Z}_5 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}\}$

Construire la table de Pythagore de l'addition dans $\mathbb{Z}_5$

2.7. Homomorphisme de groupes

a. Définition

Soient $(G,*)$ et $(G',\perp)$ des groupes

On appelle homomorphisme de $(G,*)$ dans $(G',\perp)$, toute application

$$f : G \longrightarrow G' / f(x * y) = f(x) \perp f(y)\ ;\ \ \forall x, y \in G$$

Exemples

(1) Soit $\mathbb{Z}$ un groupe additif, alors

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}$$

$$x \longmapsto f(x) = tx\ ;\ t \text{ un entier quelconque, est un homomorphisme de groupe car}$$

$$\forall x, y \in \mathbb{Z}, f(x+y) = t(x+y) = tx + ty = f(x) + f(y)$$

(2) Soient $\mathbb{Z}$ un groupe additif

F un groupe multiplicatif arbitraire

Alors $\forall a \in F, f : \mathbb{Z} \longrightarrow F / f(n) = a^n \quad \forall n \in \mathbb{Z}$ est un homomorphisme de groupes

En effet, $\forall m, n \in \mathbb{Z}, f(m+n) = a^{m+n} = a^m . a^n = f(m).f(n)$

(3) Soit n entier quelconque, l'application canonique

$cl : \mathbb{Z} \longrightarrow {}^{\mathbb{Z}}/_{n\mathbb{Z}}$ est un homomorphisme de groupe additif $\mathbb{Z}$ sur le groupe additif ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$

Car $\forall x, y \in \mathbb{Z}, cl(x+y) = cl(x) + cl(y)$

b. Définitions

b.1. Un endomorphisme de G est un homomorphisme de G sur G. Dans ce cas,

$$f : G \longrightarrow G / \forall x, y \in G, f(x * y) = f(x) * f(y)$$

b.2. On dit que f est un isomorphisme de groupes si f est un homomorphisme bijectif de groupes.

b.3. Un automorphisme de G est un isomorphisme de G sur G

b.4. Deux groupes sont dits isomorphes s'il existe un isomorphisme de l'un sur l'autre

b.5. Le noyau d'un homomorphisme $f : (G,*) \longrightarrow (G',\perp)$ est le sous – ensemble de G noté ker f et défini par

$$\ker f = \{x / x \in G \text{ et } f(x) = e'\}$$

b.6. L'image d'un homomorphisme $f : (G,*) \longrightarrow (G',\perp)$ est le sous – ensemble de G' noté $Im\ f$ ou $f(G)$ et définie par

$$Im\ f \text{ ou } f(G) = \{f(x) / x \in G\}$$

b.7. L'image indirecte d'un homomorphisme $f : (G,*) \longrightarrow (G',\perp)$ est le sous – ensemble de G noté $f^{-1}(G')$ et définie par

$$f^{-1}(G') = \{x / x \in G \text{ et } f(x) \in G\}$$

c. Propositions et théorèmes

c.1. Proposition

Soit $f : (G,*) \longrightarrow (G', \perp)$ un homomorphisme de groupes

Si e est l'élément neutre de $(G,*)$

e' est l'élément neutre de $(G', \perp)$

Alors

i. $f(e) = e'$

ii. $\forall a \in G, f(\bar{a}) = \overline{f(a)}$

Démonstration

$i)\ f(e) = f(e * e) = f(e) \perp f(e) \Longrightarrow f(e) = e' \in G'$

$ii)\ e' = f(e) = f(a * \bar{a}) = f(a) \perp f(\bar{a})$

$e' = f(a) \perp f(\bar{a}) \Longrightarrow f(\bar{a})$ est le symétrique de $f(a)$

Donc $f(\bar{a}) = \overline{f(a)}$

c.2. Proposition

Le noyau d'un homomorphisme $f : (G,*) \longrightarrow (G', \perp)$ est un sous – groupe distingué de $(G,*)$

Démonstration

Il faut montrer que $i)$ $\ker f \neq \emptyset$

$ii) \forall x, y \in \ker f, x * \bar{y} \in \ker f$

$iii) \forall a \in G$ et $\forall h \in \ker f, a * h * \bar{a} \in \ker f$

En effet,

$i)$ Comme $f(e) = e' \Longrightarrow \ker f \neq \emptyset$ (car il contient au moins l'élément neutre e)

$ii)\ \forall x, y \in \ker f,\ f(x * \bar{y}) = f(x) \perp f(\bar{y}) = f(x) \perp \overline{f(y)} = e' \perp \overline{e'} = e' \perp e' = e'$

D'où $x * \bar{y} \in \ker f$

$iii) \forall a \in G, \forall h \in \ker f$, on a :

$$\begin{aligned} f(a * h * \bar{a}) &= f(a) \perp f(h) \perp f(\bar{a}) && (f \text{ homomorphisme}) \\ &= f(a) \perp e' \perp f(\bar{a}) && (h \in \ker f) \\ &= f(a) \perp f(\bar{a}) && (e' : \text{élément neutre}) \\ &= f(a) \perp \overline{f(a)} && (f(\bar{a}) = \overline{f(a)}) \\ &= e' && (f(\bar{a}) \text{ symétrique de } f(a)) \end{aligned}$$

D'où $a * h * \bar{a} \in \ker f$

c.3. Proposition

$Im\ f$ est un sous – groupe de G'

Démonstration

Comme $f(e) = e' \Longrightarrow Im\ f \neq \emptyset$

Soient x' et $y' \in Im\ f$, on a : $x' \in Im\ f \Longrightarrow \exists x \in G / x' = f(x)$

$y' \in Im\ f \Longrightarrow \exists y \in G / y' = f(y)$

Finalement, $x' \perp y' = f(x) \perp \overline{f(y)} = f(x) \perp f(\bar{y}) = f(x * \bar{y}) \in Im\ f$

c.4. Théorème

Soient G et G' deux groupes et un homomorphisme $f : (G,*) \longrightarrow (G', \perp)$. Pour que f soit injectif, il faut et il suffit que son noyau soit réduit à l'élément neutre. En d'autres mots :

f injectif $\Leftrightarrow \ker f = \{e\}$

Démonstration

$\Longrightarrow$

Comme $f(e) = e'$ (f homomorphisme)

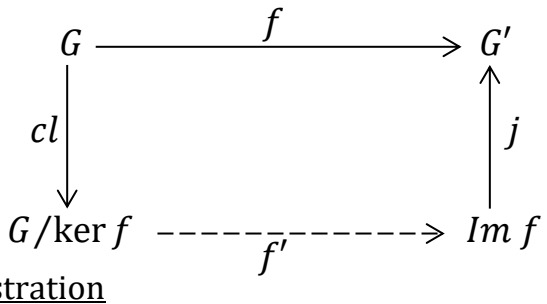
La relation $f(x) = e' \Longrightarrow f(x) = f(e)$
Si f est injectif, $f(x) = f(e) \Longrightarrow x = e$
D'où $\ker f = \{e\}$
$\Leftarrow$ $f(x) = f(y) \Longrightarrow x * \bar{y} \in \ker f$ car
$f(x) = f(y) \Longrightarrow f(x) \perp f(\bar{y}) = f(x * \bar{y}) = e'$
Comme $\ker f = \{e\}$, $x * \bar{y} \in \ker f \Longrightarrow x * \bar{y} = e$
D'où $x = y$ et f injectif

c.5. Théorème

Soit $f : (G,*) \longrightarrow (G', \perp)$ un homomorphisme
Il existe un isomorphisme canonique

$$f' : G/\ker f \longrightarrow Im\, f$$

tel que le diagramme suivant commute



C'est – à – dire $f = j \circ f' \circ cl$
j : injection canonique

Démonstration

Il faut montrer que
$i)$ $f' : G/\ker f \longrightarrow Im\, f$ définit une fonction
$cl(x) \longmapsto f'\big(cl(x)\big) = f(x)$
$ii)$ f' est un isomorphisme
$iii)$ $\forall x \in G, (j \circ f' \circ cl)(x) = f(x)$

d. Applications aux groupes cycliques

d.1. Définitions

On appelle **groupe cyclique**, tout groupe G pour lequel il existe un $x \in G$ tel que tout élément de G soit une puissance de x.
On dit que x est un **générateur** de G c'est – à – dire
$\exists x \in G / \forall a \in G, \exists p \in \mathbb{Z}$ avec $a = x^p$

Exemples

Le groupe additif $\mathbb{Z}$ est cyclique : 1 (ou -1) est générateur
Le groupe multiplicatif $P = \{\varepsilon_0, \varepsilon_1, \varepsilon_2\}$ où ε_0, ε_1 et ε_2 sont les racines de l'équation $z^3 - 1 = 0$ est cyclique : ε_1 est générateur. En effet,

$$\varepsilon_0 = \varepsilon_1^0 = \left(e^{i\frac{2\pi}{3}}\right)^0 = 1$$
$$\varepsilon_1 = \varepsilon_1^1 = \left(e^{i\frac{2\pi}{3}}\right)^1 = e^{i\frac{2\pi}{3}}$$
$$\varepsilon_2 = \varepsilon_1^2 = \left(e^{i\frac{2\pi}{3}}\right)^2 = e^{i\frac{4\pi}{3}}$$

D'où P est un groupe cyclique car
$(P,\circ) = (\{\varepsilon_0, \varepsilon_1, \varepsilon_2\},\circ)$ est un groupe et, en plus,
$P = \{\varepsilon_1^0, \varepsilon_1^1, \varepsilon_1^2\}$

d.2. Théorème

Tout groupe cyclique est isomorphe au groupe additif $(\mathbb{Z}, +)$

Tout groupe cyclique fini à p éléments (on dit aussi d'ordre p) est isomorphe au groupe additif $\mathbb{Z}/_{p\mathbb{Z}}$

Démonstration

Soit $G = \{x^n / n \in \mathbb{Z}\} = \{\dots, x^{-2}, x^{-3}, e, x, x^2, \dots\}$

Alors i) G est un groupe cyclique ou monogène (vérifier)

ii) Ce groupe est commutatif

Car $\forall x^m, x^n \in G, x^m.x^n = x^{m+n} = x^{n+m} = x^n.x^m$

iii) De plus l'application

$$f : \mathbb{Z} \longrightarrow G \quad \text{est un homomorphisme}$$
$$n \longmapsto x^n \quad \text{il est surjectif par définition}$$

On a, $\forall m, n \in \mathbb{Z}, f(m+n) = x^{m+n} = x^m.x^n = f(m).f(n)$

iv) $\ker f = \{n \in \mathbb{Z} / x^n = e\}$ est un sous – groupe distingué de $(\mathbb{Z}, +)$ car $(\mathbb{Z}, +)$ est abélien.

Alors $\exists! p \in \mathbb{N}$ tel que $p\mathbb{Z} = \ker f$

1er cas : si $p = 0 \Longrightarrow f$ injectif d'où $p = 0 \Longrightarrow f$ bijectif

Donc $(\mathbb{Z}, +)$ est isomorphe à G auquel cas G est infini.

2ème cas : Si $p \neq 0$, d'après le théorème 2-3.4.

Le groupe additif $\mathbb{Z}/_{p\mathbb{Z}}$ est isomorphe à G. Auquel cas G est fini et est d'ordre p.

2.8. Groupe produit

a. Soient $(G_1, \top_1), (G_2, \top_2)$ deux groupes. Nous pouvons définir une loi de composition interne $*$ sur l'ensemble produit

$G = G_1 \times G_2$

par la formule suivante

$(x_1, x_2) * (y_1, y_2) = (x_1 \top_1 y_1, x_2 \top_2 y_2)$ Les trois lois $\top_1$, $\top_2$, $*$ peuvent être notées de la même manière si aucune confusion n'est à craindre. Par exemple en notation additive, ou multiplicative

$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$

$(x_1, x_2)(y_1, y_2) = (x_1 y_1, x_2 y_2)$

Vérifier que

Le magma $(G, *)$ a une structure de groupe

On l'appelle **groupe produit** (cartésien) des groupes G_1 et G_2 et la loi $*$ s'appelle loi produit

Ce groupe $(G, *)$ est commutatif ssi G_1 et G_2 le sont.

b. De la même façon, nous pouvons définir une loi de composition interne sur le produit cartésien

$G = G_1 \times G_2 \times \dots \times G_n$ de n groupes

Enfin, si $G_1 = G_2 = \dots = G_n$, on a le groupe produit $(G^n, *)$

Si la loi de composition interne de G et $*$ sont notées additivement, on a, dans G^n

$(x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$

$e = (0,0,\dots,0)$ élément neutre

$-(x_1, x_2, \dots, x_n) = (-x_1, -x_2, \dots, -x_n)$ est le symétrique de $(x_1, x_2, \dots, x_n)$

Exemples

Les groupes additifs $\mathbb{Z}^n$, $\mathbb{Q}^n$, $\mathbb{R}^n$. La loi interne $+$ étant donnée par la formule

$$(x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$$

c. Proposition

Si P_1 est un sous – groupe de $(G_1, \top_1)$ et P_2 de $(G_2, \top_2)$, alors $P_1 \times P_2$ est un sous – groupe de $(G_1 \times G_2, *)$. Montrez – le.

Exemple et Exercice

(1) $\mathbb{Z}^n$ est un sous – groupe de $\mathbb{R}^n$

(2) P_1 et P_2 étant des sous – groupes distingués respectifs de G_1 et G_2, démontrer que $P_1 \times P_2$ est un sous – groupe distingué de $G_1 \times G_2$

Considérer l'application

$f_1 : G_1 \longrightarrow G_1 \times \{e_2\} : x_1 \longmapsto f(x_1) = (x_1, e_2)$ et f_2 (à définir) et démontrer le théorème ci – après :

d. Théorème

d.1. Le groupe G_1 est isomorphe au sous – groupe $G'_1 = G_1 \times \{e_2\}$ de $G_1 \times G_2$

d.2. Le groupe G_2 est isomorphe au sous – groupe $G'_2 = \{e_1\} \times G_2$ de $G_1 \times G_2$

2.9. Somme directe

a. Considérons G_1 et G_2 groupes commutatifs.

La loi étant notée additivement, on a :

$x = (x_1, x_2) = (x_1, e_2) + (e_1, x_2) \in G_1 \times G_2$

C'est – à – dire

$$G_1 \times G_2 = G'_1 + G'_2$$

Et cette décomposition de l'élément $x \in G_1 \times G_2$ est unique

En outre si $(x_1, x_2) \in G'_1$ et à G'_2, alors $x_1 = e_1$ et $x_2 = e_2$

Donc, en posant $e = (e_1, e_2)$ élément neutre de $G_1 \times G_2$:

$$G'_1 \cap G'_2 = \{e\}$$

b. Théorème

Un groupe abélien G étant la somme de deux de ses sous – groupes P_1, P_2 , les deux propriétés suivantes sont équivalentes :

$i)$ Tout x de G s'écrit d'une manière unique

$x = x_1 + x_2$; $x_1 \in P_1, x_2 \in P_2$

$ii)$ $P_1 \cap P_2 = \{e\}$

Démonstration

$i) \Longrightarrow ii)$

Soit $x = x_1 + x_2$ est une écriture unique, $x \in G = P_1 + P_2$

On a : $x \in P_1 \cap P_2 \Longrightarrow x = x + e$ avec $x \in P_1$ et $e \in P_2$

$x = e + x$ avec $e \in P_1$ et $x \in P_2$

D'où $x = e$ d'après $i)$

$ii) \Longrightarrow i)$

Supposons $G = P_1 + P_2$ et $P_1 \cap P_2 = \{e\}$
Si $x = x_1 + x_2 = y_1 + y_2$ avec $x_1, y_1 \in P_1$; $x_2, y_2 \in P_2$
Alors $x_1 - y_1 = x_2 - y_2$ avec $x_1 - y_1 \in P_1$; $x_2 - y_2 \in P_2$
D'où $x_1 - y_1 = x_2 - y_2 \in P_1 \cap P_2 = \{e\}$
Donc …

c. Définition
Si deux sous – groupes P_1 et P_2 de G n'ont en commun que l'élément neutre e, leur somme est dite **somme directe**.
On la note alors : $P_1 \oplus P_2$
Ainsi $G = P_1 \oplus P_2 \Leftrightarrow P_1 \cap P_2 = \{e\}$
$G = P_1 + P_2$
Considérer l'application
$f : P_1 \times P_2 \longrightarrow G : (x_1, x_2) \longmapsto f(x_1, x_2) = x_1 + x_2$
et démontrer le théorème suivant :

d. Théorème
d.1. $G = P_1 \oplus P_2$ est isomorphe au groupe produit $P_1 \times P_2$
d.2. G/P_1 est isomorphe à P_2
d.3. G/P_2 est isomorphe à P_1

2.10. Groupe de permutations d'un ensemble E

a. Définition
Soit E un ensemble fini de cardinal $n, n \in \mathbb{N}^*$
On appelle permutation de E, toute bijection de E sur lui – même (voir 1ère partie §5-5.5.d)

b. Notations
Une permutation p de $[1, n]$ sera notée $i \longmapsto p(i) = p_i$ ou encore

$$\begin{pmatrix} 1 & 2 & \dots & i & \dots & n \\ p_1 & p_2 & \dots & p_i & \dots & p_n \end{pmatrix}$$

ou encore si $i \longmapsto a_i$ est une bijection de $[1, n]$

$$\begin{pmatrix} a_1 & a_2 & \dots & a_i & \dots & a_n \\ p_{a_1} & p_{a_2} & \dots & p_{a_i} & \dots & p_{a_n} \end{pmatrix}$$

L'ensemble des permutations d'un ensemble E sera noté $\mathcal{S}(E)$
$p \circ q$ ou pq est la composée de deux permutations p et q qu'on appelle par abus de langage **produit** des deux permutations p et q
$p^2 = p \circ p$ $\quad p^3 = p \circ p \circ p$ $\quad p^k = p^{k-1} \circ p$

Exemple
Soit $E = \{a, b, c, d\}$. L'ensemble $\mathcal{S}(E)$ des permutations de E contient $4! = 24$ éléments. Lesquels ? Montrer que $(\mathcal{S}(E), \circ)$ est un groupe.

c. Propositions et définitions

c.1. $(\mathcal{s}(E),\circ)$ est un groupe d'ordre $n!$. Démontrer. Ce groupe est appelé le groupe des permutations, ou **groupe symétrique** de E.

c.2. Le groupe des permutations de $\{1,2,3,\dots,n\}$ s'appelle le groupe symétrique d'ordre n et se note $\mathcal{s}_n$. $\text{Card}(\mathcal{s}_n) = n!$

c.3. Le groupe $\mathcal{s}(E)$ n'est pas commutatif si $n \geq 3$

En effet,

Soit $p, q \in \mathcal{s}(E)$ et tels qu'ils laissent invariants tous les éléments de $[1,n] - \{a_1, a_2, a_3\}$:

$$p = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \dots & a_n \\ a_2 & a_3 & a_1 & a_4 & \dots & a_n \end{pmatrix} \qquad q = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \dots & a_n \\ a_2 & a_1 & a_3 & a_4 & \dots & a_n \end{pmatrix}$$

On a :

$$p \circ q = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \dots & a_n \\ a_3 & a_2 & a_1 & a_4 & \dots & a_n \end{pmatrix} \neq q \circ p = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \dots & a_n \\ a_1 & a_3 & a_2 & a_4 & \dots & a_n \end{pmatrix}$$

d. Définition

On dit qu'une permutation p opère sur une partie P de E si p laisse invariant chaque élément de $E - P$.

e. Transpositions et Cycles

e.1. On appelle **transposition** de E, une permutation de E qui laisse invariants tous les éléments de E sauf deux. Autrement dit :

$t \in \mathcal{s}(E)$ est une transposition de E ssi

$\exists a, b \in E \qquad t(a) = b$ et $t(b) = a$

$\forall x \in E - \{a, b\} \quad t(x) = x$

Donc t opère sur $\{a, b\}$ et est distinct de l'identité.

e.2. On appelle cycle de E, une permutation c de E telle que

$1 \leq p \leq n$, on ait : $(i = 1,2,\dots,p-1) \qquad c(a_i) = a_{i+1}$

$c(a_p) = a_1$ et

$(j = p+1,\dots,n) \qquad c(a_j) = a_j$

e.3. Notation

$$c = \begin{pmatrix} a_1 & a_2 & \dots & a_{p-1} & a_p & a_{p+1} & \dots & a_n \\ a_2 & a_3 & \dots & a_p & a_1 & a_{p+1} & \dots & a_n \end{pmatrix}$$

ou simplement

$$c = (a_1 \ a_2 \ \dots \ a_p)$$

Vérifier que pour $1 < k < p$,

$$c^k = \begin{pmatrix} a_1 & \dots & a_p & a_{p+1} & \dots & a_n \\ a_{k+1} & \dots & a_k & a_{p+1} & \dots & a_n \end{pmatrix} \neq e$$: permutation identique

p est le plus petit entier $h > 0$ tel que $c^h = e$

Donc le cycle $c = (a_1, a_2, \dots, a_p)$ opérant sur p éléments d'un ensemble à n éléments est un élément d'ordre p du groupe $\mathcal{s}(E)$ appelé aussi **permutation circulaire** d'ordre p.

Exemples

(1) $t = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 4 & 5 & 6 \end{pmatrix} \in \mathcal{s}_6$ est une transposition

(2) Toute transposition est un cycle d'ordre 2

(3) $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 5 & 6 \end{pmatrix} \in \mathcal{s}_6$ est un cycle d'ordre 4

f. Inversion d'une permutation

Un couple (a, b) d'éléments de E présente une inversion pour une permutation $p \in \mathcal{s}(E)$ si

$$a < b \Longrightarrow p(a) > p(b)$$

Exemple

Soit $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 6 & 5 & 1 \end{pmatrix} \in \mathcal{s}_6$

Alors le couple $(2,3)$ présente une inversion car $2 < 3$ et $p(2) > p(3)$

De même avec les couples $(1,6)$; $(4,5)$; $(5,6)$; $(2,6)$; $(4,6)$ et $(3,6)$. Pourquoi ?

g. Signature d'une permutation

Soit $p \in \mathcal{s}(E)$. Posons

$I(p)$: le nombre total d'inversions de p

$\mathcal{E}(p)$: la signature ou parité de p

Alors

$$\mathcal{E}(p) = (-1)^{I(p)} = \begin{cases} 1 \text{ si } I(p)=2n, \text{ on dit que } p \text{ est une permutation paire} \\ -1 \text{ si } I(p)=2n+1, \text{ on dit que } p \text{ est une permutation impaire} \end{cases}$$

Exemple

La signature $\mathcal{E}(p)$ de la permutation p ci – dessus est

$\mathcal{E}(p) = (-1)^7 = -1$. C'est donc une permutation impaire.

h. Théorèmes et définition

h.1. L'application

$$\mathcal{E} : \mathcal{s}(E) \longrightarrow \{-1, +1\} : p \longmapsto \mathcal{E}(p)$$

est un homomorphisme du groupe symétrique $\mathcal{s}(E)$ sur le groupe multiplicatif $\{-1, +1\}$ des éléments inversibles de $\mathbb{Z}$

h.2. L'ensemble $\mathcal{A}(E) = \{p \in \mathcal{s}(E) / \mathcal{E}(p) = 1\}$ des permutations paires, noyau de l'homomorphisme $\mathcal{E}$, est un sous – groupe de $\mathcal{s}(E)$ appelé **groupe alterné** d'ordre n.

C'est un sous – groupe invariant du groupe symétrique $\mathcal{s}(E)$

En effet :

$$\forall p, q \in \mathcal{A}(E), p \circ q \in \mathcal{A}(E) \text{ car } p, q \in \mathcal{A}(E), \mathcal{E}(p \circ q) = \mathcal{E}(p)\mathcal{E}(q) = 1$$

$$p^{-1} \in \mathcal{A}(E) \text{ car } p, e \in \mathcal{A}(E)$$

$$p \circ p^{-1} = e \Longrightarrow \mathcal{E}(p \circ p^{-1}) = \mathcal{E}(p)\mathcal{E}(p^{-1}) = 1$$

D'où $\mathcal{E}(p^{-1}) = 1$

§3. Structures d'anneaux et de corps

3.1. Définitions

a. On appelle Anneau, un triplet $(A, +, \cdot)$ formé d'un ensemble A et de deux lois internes sur A notées $+$ et $\cdot$ telles que les conditions suivantes soient vérifiées
   i) Le couple $(A, +)$ est un groupe abélien (« + » : addition)
   ii) La loi interne $\cdot$ est associative
   C'est – à – dire $(A, \cdot)$ est un demi – groupe (" $\cdot$ " : multiplication)
   iii) La multiplication est distributive par rapport à l'addition
   C'est – à – dire $\forall x, y, z \in A, (x + y) \cdot z = xz + yz$
   $z \cdot (x + y) = zx + zy$

b. On dit qu'un anneau $(A, +, \cdot)$ a un élément unité ou qu'il est unitaire, lorsque la multiplication admet un élément neutre, noté 1, et appelé unité
   On a : $\forall x \in A, 1 \cdot x = x \cdot 1 = x$
c. Un anneau A est commutatif lorsque la multiplication est commutative
d. Dans un anneau A non forcément commutatif, deux éléments x et y sont dits commutables (ou permutables) si $xy = yx$
e. Lorsqu'il existe dans un anneau A des éléments x,y tels que $x \neq 0$ et $y \neq 0 \Longrightarrow x \cdot y = 0$, on dit que x et y sont des diviseurs de zéro
f. L'anneau A est appelé anneau d'intégrité ou anneau intègre s'il est commutatif, non réduit à $\{0\}$ et dépourvu de diviseurs de zéro c'est – à – dire
   $\forall x, y \in A, x \cdot y = 0 \Longrightarrow x = 0$ ou $y = 0$
g. Dans un anneau A, un élément x est dit inversible s'il admet un inverse pour la loi multiplication c'est – à – dire
   $\forall x \in A, \exists x^{-1} \in A / x \cdot x^{-1} = x^{-1} \cdot x = 1$
h. Si l'anneau A est un anneau unitaire tel que tout élément non nul est inversible, alors A est un corps. En d'autres termes $(K, +, \cdot)$ est un corps si et seulement si
   i) $(K, +)$ est un groupe abélien (0 : élément neutre)
   ii) $(K \setminus \{0\}, \cdot)$ est un groupe (1 : élément neutre)
   iii) La multiplication est distributive par rapport à l'addition
i. Ce corps est commutatif dès que la loi multiplication est commutative dans A. Un corps commutatif est aussi appelé **champ**.
   Exemples
   (1) $(\mathbb{Z}, +, \cdot)$ est anneau commutatif appelé **anneau des entiers rationnels**
   (2) $(\mathbb{Q}, +, \cdot)$; $(\mathbb{R}, +, \cdot)$; $(\mathbb{C}, +, \cdot)$ sont des anneaux commutatifs. Ils sont en plus des champs

3.2. Règles de signe – Notation

a. Proposition

Soit $(A, +, \cdot)$ un anneau dont l'élément neutre pour $+$ est noté 0

Alors $\forall a, b \in A$, on a : $i) 0a = a0 = 0$

$ii) a(-b) = (-a)b$

$iii) (-a)(-b) = ab$

Démonstration

i) $0a = (0+0)a = 0a + 0a \Longrightarrow \begin{cases} 0a = 0 \\ a0 = 0 \end{cases}$ car $(A, +)$ est un groupe

$a0 = a(0+0) = a0 + a0$

ii) $a(-b) + ab = a(-b+b) = a0 = 0$

et $(-a)b + ab = (-a+a)b = 0b = 0$

Etant donné que chaque élément de A dont ab ne peut avoir qu'un seul opposé, on a :

$a(-b) = -(ab) = (-a)b$

iii) D'après ii) $(-a)(-b) = [-(a)(-b)] = -(-a)b = ab$

b. Notation

Soit $(A, +, \cdot)$ un anneau. Dans le groupe abélien $(A, +)$, nous noterons, si $n \in \mathbb{Z}$ et $x \in A$:

$$nx = \begin{cases} x + x + \cdots + x & (n \text{ fois}) \text{ si } n \geq 1 \\ 0 & \text{si } n = 0 \\ (-x) + (-x) + \cdots + (-x) & (-n \text{ fois}) \text{ si } n \leq -1 \end{cases}$$

3.3. Homomorphisme d'anneaux

a. Un homomorphisme d'anneau $(A, +, \cdot)$ dans un anneau $(A', +, \cdot)$ est une application

$$f : A \longrightarrow A' / \forall x, y \in A, \quad \begin{matrix} f(x+y) = f(x) + f(y) \\ f(x \cdot y) = f(x) \cdot f(y) \end{matrix}$$

Lorsqu'il s'agit des corps, ces mêmes conditions définissent un homomorphisme de corps $(A, +, \cdot)$

b. Un isomorphe d'anneaux (respectivement de corps) est un homomorphisme d'anneaux (respectivement de corps) qui est bijectif

Deux anneaux (respectivement corps) sont dits isomorphes lorsqu'il existe un isomorphisme entre les deux.

Exemples

(1) L'application canonique $cl : \mathbb{Z} \longrightarrow \mathbb{Z}_p$ est un homomorphisme d'anneaux. Car

$\forall x, y \in \mathbb{Z}, cl(x+y) = cl(x) + cl(y)$

$cl(x \cdot y) = cl(x) \cdot cl(y)$

(2) Soit l'anneau $\mathcal{C}([0,1], \mathbb{R})$

Vérifier que l'application $\varphi_0 : \mathcal{C}([0,1], \mathbb{R}) \longrightarrow \mathbb{R}$

$f \longmapsto \varphi_0(f) = f(0)$

est un homomorphisme d'anneaux.

3.4. Sous – anneaux – Extension de corps

a. Un sous – anneau d'un anneau $(A, +, \cdot)$ est un sous – ensemble $S \subseteq A$ qui est lui – même un anneau avec les lois internes $+$ et $\cdot$ restreintes aux éléments de S

b. Théorème
Soit $(A, +, \cdot)$ un anneau
Une partie $S \subseteq A$ est un sous – anneau de $(A, +, \cdot)$ si et seulement si elle vérifie les conditions suivantes
i) S est un sous – groupe de $(A, +)$
ii) $\forall x, y \in S, x \cdot y \in S$

c. Soient $(K, +, \cdot)$ un corps et $L \subseteq K$
On dit que L est un sous – corps de $(K, +, \cdot)$ lorsque L est lui – même un corps pour les lois internes $+$ et $\cdot$ restreintes sur L. On a aussi le théorème suivant :

d. Théorème
Un sous – ensemble L d'un corps $(K, +, \cdot)$ est un sous – corps ssi
$\forall x, y \in L, y \neq 0$, on a : $i)\ x - y \in L$
$ii)\ xy^{-1} \in L$

e. Si L est un sous – corps de $(K, +, \cdot)$, alors on dit que K est une extension du corps $(L, +, \cdot)$
Exemples
$\mathbb{Q}$ est un sous – corps de $\mathbb{R}$; $\mathbb{R}$ est un sous – corps de $\mathbb{C}$. On dit que $\mathbb{R}$ est une extension de $\mathbb{Q}$ …

3.5. Idéaux d'un anneau

a. Définitions
a.1. On appelle idéal à droite (respectivement à gauche) d'un anneau $(A, +, \cdot)$, toute partie $I \subseteq A$ telle que
i) I est sous – groupe de $(A, +)$
ii) $\forall a \in A, \forall x \in I, xa \in I$ (respectivement $ax \in I$)
a.2. Un idéal à la fois à droite et à gauche est dit bilatère
Exemples
Soit a élément fixé de l'anneau A. Alors
(1) $aA = \{ax / x \in A\}$ est un idéal à droite de A engendré par a
(2) $Aa = \{xa / x \in A\}$ est un idéal à gauche de A engendré par a
(3) $2\mathbb{Z} = \{2x / x \in \mathbb{Z}\}$ est un idéal bilatère de l'anneau $\mathbb{Z}$

b. Proposition
Soient $(A, +, \cdot)$ et $(A', +, \cdot)$ des anneaux et
$f : A \longrightarrow A'$ un homomorphisme d'anneaux
Alors $\ker f$ est un idéal bilatère de A

Démonstration

i) $\ker f$ est un sous – groupe de $(A,+)$ (déjà démontré 1ère partie 2.7 Prop.c.2)

ii) Montrons que $\forall a \in A$ et $\forall x \in \ker f$ et $ax \in \ker f$

En effet : $f(xa) = f(x) \cdot f(a) = 0 \cdot f(a) = 0 \Longrightarrow xa \in \ker f$

De même : $f(ax) = f(a) \cdot f(x) = f(a) \cdot 0 = 0 \Longrightarrow ax \in \ker f$

c. Proposition

c.1. Tout idéal de A est un sous – anneau de A

D'après les conditions $i)$ et $ii)$ de la définition d'un idéal

c.2. L'intersection d'une famille d'idéaux à droite (respectivement à gauche) d'un anneau A est un idéal à droite (respectivement à gauche) de A

Démonstration

$$x, y \in I + J \Longrightarrow \exists x_1, y_1 \in I \text{ et } x_2, y_2 \in J / \begin{matrix} x = x_1 + x_2 \\ \text{et } y = y_1 + y_2 \end{matrix}$$

On a :

$x - y = (x_1 - y_1) + (x_2 - y_2) \in I + J$. En outre, $\forall a \in A$,

$xa = (x_1 + x_2)a = x_1 a + x_2 a \in I + J$

En conséquence, si $(I_m)_{m \in M}$ est une famille finie d'idéaux à droite (respectivement à gauche) de A, alors

$I_1 + I_2 + \cdots + I_n = \{x = x_1 + x_2 + \cdots + x_n / x_1 \in I_1, x_2 \in I_2, \ldots, x_n \in I_n\}$ est un idéal à droite (respectivement à gauche) de A

Exemple

Soit $2\mathbb{Z}$ et $3\mathbb{Z}$ deux idéaux de $\mathbb{Z}$. Alors

$2\mathbb{Z} + 3\mathbb{Z} =$... est un idéal de $\mathbb{Z}$

d. Radical d'un idéal

Soient A anneau et $I \subseteq A$ idéal

d.1. Définition

On appelle **radical** de I l'ensemble $\vartheta(I)$ avec

$\vartheta(I) = \{x \in A / \exists n \in \mathbb{N}^* \text{ t.q. } x^n \in I\}$

d.2. Propositions

Démontrez que $i)$ $\vartheta(I)$ est un idéal de A

$ii) I \subseteq \vartheta(I)$

$iii) \vartheta(I \cap J) = \vartheta(I) \cap \vartheta(J)$

$iv) I \subseteq J \Longrightarrow \vartheta(I) \subseteq \vartheta(J)$

$v) \vartheta(I.J) \subseteq \vartheta(I) \cap \vartheta(J)$

$vi) \vartheta(I + J) \supseteq \vartheta(I) + \vartheta(J)$

$vii) \vartheta\big(\vartheta(I)\big) = I$

e. Idéal principal. Anneau principal

Soit a élément fixé de l'anneau A. On sait que aA est un idéal à droite de A et Aa est un idéal à gauche de A engendrés par a

e.1. Définition

Un idéal I de A est dit **principal** s'il existe $a \in A$ tel que

$I = aA = Aa$

Notation

$I = (a)$ Un idéal principal est donc bilatère.

e.2. Définition

Un anneau A est dit principal si tout idéal de A est principal

Exemples

(1) L'ensemble $\{0\}$ est un idéal principal de tout anneau

(2) L'ensemble $2\mathbb{Z}$ est un idéal principal de l'anneau $\mathbb{Z}$

(3) Plus généralement, si A est un anneau commutatif unitaire

Alors $I = \{\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n / \alpha_1, \alpha_2, \dots, \alpha_n \in A\}$ est un idéal principal engendré par $a_1, a_2, \dots, a_n$

Notations

$$I = (a_1, a_2, \dots, a_n)$$

(4) $\mathbb{Z}$ est un anneau principal

e.3. Proposition

Tout anneau principal est unitaire

Démonstration

A est un idéal bilatère de A

or A est principal

D'où $\exists a \in A / aA = Aa = A$

Donc les applications $\begin{matrix} f:A \longrightarrow aA : x \longmapsto f(x)=ax \\ g:A \longrightarrow Aa : x \longmapsto g(x)=xa \end{matrix}$ sont surjectives.

Par conséquent,

$\exists e \in A$ et $u \in A / ae = a$ et $ua = a$

Alors $\forall y \in A, \exists x \in A / y = ax \Longrightarrow uy = u(ax) = (ua)x = ax = y$

et $\exists x' \in A / y = x'a \Longrightarrow ye = (x'a)e = x'(ae) = x'a = y$

Donc, $\forall y \in A, uy = y$ (1) et $ye = y$ (2)

En particulier, si $y = e$ dans (1) et $y = u$ dans (2)

On a : $ue = e$ et $ue = u$ D'où $u = e$ est un élément neutre de la multiplication

3.6. Idéaux de $\mathbb{Z}$

a. Théorème

Soit $I \subseteq \mathbb{Z}$, les affirmations suivantes sont équivalentes

i) I est un idéal de $(\mathbb{Z}, +)$

ii) I est un sous – groupe de $(\mathbb{Z}, +)$

iii) I est de la forme de $n\mathbb{Z}$ pour un entier n

Autrement dit $I = n\mathbb{Z}$

Démonstration

$i) \Longrightarrow ii)$ par définition de I

$ii) \Longrightarrow iii)$

Soit n le plus petit entier strictement positif $\in I$

Si $k \in \mathbb{Z}, nk \in n\mathbb{Z}$ et on a : $nk = n + n + \cdots + n$ (k fois)

D'où $nk \in I$ (I sous – groupe de $\mathbb{Z}$)

Donc $n\mathbb{Z} \subseteq I$

Si $x \in I, x = nq + r$ avec $0 \leq r < n$ (Division euclidienne)

D'où $r = x - nq$

Or $x, nq \in I$
Donc $r = x - nq \in I$
Mais n est le plus petit entier strictement positif $\in I$
D'où $r = 0$ et $x = nq \in n\mathbb{Z}$
Donc $I \subseteq n\mathbb{Z}$

$iii) \Longrightarrow i)$
Pour ce faire, on vérifie simplement la définition de l'idéal
En effet :

- $I = n\mathbb{Z}$ est un sous – groupe de $(\mathbb{Z}, +)$
- $\forall a \in \mathbb{Z}$ et $\forall x \in I, ax \in I$
  On a : $x \in I \Longrightarrow x = nk$ avec $k \in \mathbb{Z}$
  D'où $ax = a(nk) = ank = n(ak) = nk' \in I, k' \in \mathbb{Z}$

b. <u>Somme de deux idéaux de $\mathbb{Z}$</u>
Soient $I_1 = a\mathbb{Z}$ et $I_2 = b\mathbb{Z}$ deux idéaux de $\mathbb{Z}$ respectivement engendrés par a et b
Alors $I_1 + I_2 = a\mathbb{Z} + b\mathbb{Z}$ est un idéal de $\mathbb{Z}$
$= \{u_1 + u_2 / u_1 \in a\mathbb{Z} \text{ et } u_2 \in b\mathbb{Z}\}$
$= \{ax + by / x \in \mathbb{Z} \text{ et } y \in \mathbb{Z}\}$

c. <u>Somme d'une famille d'idéaux de $\mathbb{Z}$</u>
…….. (à définir)

d. <u>Division euclidienne dans $\mathbb{Z}$</u>

1. <u>Théorème et définitions</u>
Etant donné un couple $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$, il existe un couple unique $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que
$a = bq + r$ et $0 \leq r < b$
Calculer ce couple (q, r) c'est effectuer la division euclidienne de a par b. On appelle a le dividende, b le diviseur, q le quotient euclidien et r le reste.
<u>Démonstration</u>
On sait que, dans $\mathbb{N}$, étant donné un couple $(a, b) \in \mathbb{N} \times \mathbb{N}^*$, il existe un entier q et un seul tel que
$bq \leq a < b(q + 1)$
Etablissons un résultat analogue dans le cas où a est négatif et b positif. En effet,
$bq \leq a < b(q + 1)$ entraine, en changeant les signes,
$b(-q - 1) < -a \leq b(-q)$
<u>1er cas</u> : $(-a) = b(-q)$, on dit que b divise – a
$-q$ est le quotient exacte de $(-a)$ par b
$\Longrightarrow r = 0$
<u>2ème cas</u> : $b(-q - 1) < -a < b(-q)$
$-q - 1$ est le quotient euclidien de $(-a)$ par b. Il est unique
Par définition, le reste est
$r = (-a) - b(-q - 1) = -a + b(q + 1)$

2. Divisibilité – Multiples – ppcm

d.1. Définitions

Soit $a, b \in \mathbb{Z}$. Rappelons que

$b/a \Leftrightarrow \exists q \in \mathbb{Z}/a = bq$

$\mathcal{M}(b) = b\mathbb{Z}$ est l'ensemble des multiples de b

$b/a \Leftrightarrow a \in b\mathbb{Z}$

d.2. Propriétés

i) $b/a \Leftrightarrow a\mathbb{Z} \subseteq b\mathbb{Z}$

ii) a/b et $b/a \Longrightarrow a = \pm b$

iii) a/b et $b/c \Longrightarrow a/c$

Démonstration

$b/a \Longrightarrow$ tout multiple de a est un multiple de b

D'où $a\mathbb{Z} \subseteq b\mathbb{Z}$

Soit $a\mathbb{Z} \subseteq b\mathbb{Z}$, on a : $a \in a\mathbb{Z} \Longrightarrow a \in b\mathbb{Z}$ et b/a

d.3. Définition (multiple commun et $p.p.c.m.$)

Soit $a, b \in \mathbb{Z}$

i) On appelle multiple commun de a et b tout élément de l'intersection $a\mathbb{Z} \cap b\mathbb{Z}$

ii) On appelle plus petit commun multiple de a et b, un entier naturel m unique tel que

$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$

Notation : $m = p.p.c.m.(a, b)$ ou $m = a \vee b$

Exemples

(1) $0, \pm 12, \pm 24$ sont des multiples communs de 4 et 6

(2) $12 = 4 \vee 6$ car $4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$

d.4. Définitions (multiple commun d'une famille finie et, plus généralement, soit une famille finie d'entiers

$a_1, a_2, \dots, a_n \in \mathbb{Z}$

i) On appelle multiple commun de ces n entiers, tout élément de l'intersection

$a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \dots \cap a_n\mathbb{Z}$

ii) On appelle plus petit commun multiple de ces n entiers $a_1, a_2, \dots, a_n$, un entier naturel m unique tel que

$a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \dots \cap a_n\mathbb{Z} = m\mathbb{Z}$

Notation : $m = p.p.c.m.(a_1, a_2, \dots, a_n)$ ou $m = a_1 \vee a_2 \vee \dots \vee a_n$

e. Diviseurs communs et pgcd

Soit $a, b \in \mathbb{Z}$

Posons $\mathfrak{D}(a) = \{x \in \mathbb{Z}/\ x/a\}$: ensemble des diviseurs de a

Par exemple $\mathfrak{D}(0) = \mathbb{Z}$, $\mathfrak{D}(8) = \{\pm 1, \pm 2, \pm 4, \pm 8\}$

e.1. Définitions (Diviseur commun)

i) On appelle diviseur commun de a et b, tout élément de l'intersection

$\mathfrak{D}(a) \cap \mathfrak{D}(b)$

ii) On appelle diviseur commun de n entiers $a_1, a_2, \dots, a_n \in \mathbb{Z}$, tout élément de l'intersection

$\mathfrak{D} = \mathfrak{D}(a_1) \cap \mathfrak{D}(a_2) \cap \dots \cap \mathfrak{D}(a_n)$

e.2. Propriétés

i) $\mathcal{S} \in \mathfrak{D}(a) \cap \mathfrak{D}(b) \Leftrightarrow a\mathbb{Z} + b\mathbb{Z} \subseteq \mathcal{S}\mathbb{Z}$

Démonstration $i)$

Si $\mathcal{S} \in \mathfrak{D}(a) \cap \mathfrak{D}(b)$, alors $a\mathbb{Z} \subseteq \mathcal{S}\mathbb{Z}$ et $b\mathbb{Z} \subseteq \mathcal{S}\mathbb{Z}$ (voir propr.d.2 ci – dessus)

D'où $a\mathbb{Z} + b\mathbb{Z} \subseteq \mathcal{S}\mathbb{Z}$

Si $a\mathbb{Z} + b\mathbb{Z} \subseteq \mathcal{S}\mathbb{Z}$, alors $a\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z} \subseteq \mathcal{S}\mathbb{Z}$ et $\mathcal{S}/a$ de même $\mathcal{S}/b$

Comme tout idéal de $\mathbb{Z}$ est principal, il existe un entier naturel d unique tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$

Par la propriété e.2, d est un diviseur commun de a et b

De plus, $\mathcal{S}$ est un diviseur commun de a et b si et seulement si $d\mathbb{Z} \subseteq \mathcal{S}\mathbb{Z}$ d'où par la propriété d.2.i) ci – dessus $\mathcal{S}$ divise d

e.3. Définitions $(p.g.c.d.)$

i) On appelle plus grand commun diviseur de a et b, un entier naturel d unique tel que

$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$

Notation : $d = p.g.c.d.(a, b)$ ou $d = a \wedge b$

ii) En général, on appelle plus grand commun diviseur de n entiers $a_1, a_2, \dots, a_n \in \mathbb{Z}$, un entier naturel d unique tel que

$a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z} = d\mathbb{Z}$

Notation : $d = p.g.c.d.(a_1, a_2, \dots, a_n)$ ou $d = a_1 \wedge a_2 \wedge \dots \wedge a_n$

e.4. Théorème

i) $\mathfrak{D}(a) \cap \mathfrak{D}(b) = \mathfrak{D}(a \wedge b)$

ii) En général, $\mathfrak{D}(a_1) \cap \mathfrak{D}(a_2) \cap \dots \cap \mathfrak{D}(a_n) = \mathfrak{D}(a_1 \wedge a_2 \wedge \dots \wedge a_n)$

f. Entiers premiers entre eux

f.1. Définitions

i) Deux entiers a et $b \in \mathbb{Z}$ sont dits premiers entre eux ou étrangers entre eux si et seulement si

$a \wedge b = 1$. Ce qui est équivalent à $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$

ii) On dit que les entiers $a_1, a_2, \dots, a_n \in \mathbb{Z}$ sont premiers entre eux dans leur ensemble si et seulement si

$a_1 \wedge a_2 \wedge \dots \wedge a_n = 1$. Ce qui est équivalent à $a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z} = \mathbb{Z}$

Exemples

(1) 14 et 15 sont étrangers entre eux

(2) 5,10 et 12 sont premiers entre eux dans leur ensemble

f.2. Théorème de Bézout

i) Deux entiers $a, b \in \mathbb{Z}$ sont premiers entre eux si et seulement si il existe des entiers $u, v \in \mathbb{Z}$ tels que $au + bv = 1$

ii) En général, les n entiers $a_1, a_2, \dots, a_n \in \mathbb{Z}$ sont premiers entre eux dans leur ensemble si et seulement si il existe n entiers $u_1, u_2, \dots, u_n \in \mathbb{Z}$ tels que

$a_1u_1 + a_2u_2 + \cdots + a_nu_n = 1$

f.3. Proposition

$\forall a, b, c \in \mathbb{Z}, ca \wedge cb = |c|(a \wedge b)$

Démonstration
Si $I = a\mathbb{Z} + b\mathbb{Z}$ est l'idéal engendré par a et b alors pour tout $c \in \mathbb{Z}$, l'idéal engendré par ca et cb est
$\{cax + cby = c(ax + by)/x, y \in \mathbb{Z}\} = cI$. On a :
$ca\mathbb{Z} + cb\mathbb{Z} = c(a\mathbb{Z} + b\mathbb{Z}) = c(a \wedge b)\mathbb{Z}$

f.4. Théorème de la divisibilité
Si a divise bc et si a est premier avec b, alors a divise c
Démonstration
D'après la prop.f.3 ci – dessus,
$a \wedge b = 1 \Longrightarrow ca \wedge cb = |c|$
Puisque a/bc et a/ac
Alors $a/ca \wedge cb = |c|$

3.7. Idéaux d'un corps

a. Théorème
Les seuls idéaux d'un corps $(K, +, \cdot)$ sont $\{0\}$ et K lui – même
Démonstration
Supposons $I \neq \{0\} \Longrightarrow \exists a \in I$ et $a \neq 0$
Comme K est un corps tout élément non nul est inversible
Comme I est un idéal, on a :
$a^{-1} \cdot a = 1 \in I$ (De même $a \cdot a^{-1} = 1 \in I$)
D'où $\forall x \in K,\ x = x \cdot 1 = 1 \cdot x \in I$ Donc $I = K$

3.8. Anneaux produits

a. Soit A_1 et A_2 deux anneaux
On munit
$A = A_1 \times A_2$ de deux opérations internes
$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2);\ (x_1, x_2) \cdot (y_1, y_2) = (x_1 \cdot y_1, x_2 \cdot y_2)$
$(A, +, \cdot)$ est un anneau appelé **anneau produit cartésien** de A_1 et A_2 (vérifiez – le)

b. Caractériser A_1 et A_2 pour que $A_1 \times A_2$ soit
- Unitaire
- Commutatif
- Intègre

3.9. Anneau quotient

a. Proposition
Si I est un idéal bilatère d'un anneau $(A, +, \cdot)$, il existe une et une seule structure d'anneau sur le quotient A/I telle que la surjection canonique

$cl : A \longrightarrow A/I$

Soit un homomorphisme d'anneaux

Démonstration

Comme $(A, +)$ est un groupe commutatif, le sous – groupe I est normal (on applique le théorème 2.6.b : A/I désigne le quotient du groupe additif mod I considéré comme sous – groupe

- L'addition sur A/I est définie par $cl(x) + cl(y) = cl(x + y)$
- De même, la multiplication sur A/I est définie par $cl(x) \cdot cl(y) = cl(x \cdot y)$ vérifier que $(A/I, +, \cdot)$ est un anneau

b. Anneau des entiers modulo n

Soit n, un entier. L'ensemble $n\mathbb{Z}$ des multiples de n est un idéal bilatère de $\mathbb{Z}$

Soit $\mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}_n$ ensemble des entiers modulo n

Alors $(\mathbb{Z}_n, +, \cdot)$ est un anneau appelé l'anneau des entiers modulo n

Les deux lois $+$ et $\cdot$ sont respectivement définies par

$cl(x) + cl(y) = cl(x + y)$; $cl(x) \cdot cl(y) = cl(x \cdot y)$

- Dresser la table de Pythagore de $+$ et $\cdot$ dans $\mathbb{Z}_7$

c. Théorème

Pour tout entier $p \geq 2, \mathbb{Z}_p$ est un corps si et seulement si p est premier

Démonstration

$\Longrightarrow$

$\mathbb{Z}_p$ est un corps $\Longrightarrow \forall \alpha, \beta \in \mathbb{Z}_p, \alpha\beta = 0$ alors $\alpha = 0$ ou $\beta = 0$

Soit $p = xy$ avec $x \geq 1,\ p \geq y$

Posons $\alpha = cl(x) \bmod p,\ \beta = cl(y) \bmod p$

Alors $\alpha, \beta \in \mathbb{Z}_p, \alpha\beta = 0 \Longrightarrow \alpha = 0$ ou $\beta = 0$

Mais $\alpha = 0 \Longrightarrow p/x$ alors $x = 1$ ou $x = p$

$\beta = 0 \Longrightarrow p/y$ alors $y = 1$ ou $y = p$

D'où p est un nombre premier.

$\Longleftarrow$

$\forall p \geq 2, p$ est premier, alors $\mathbb{Z}_p$ est un corps

En effet, si p est premier, alors

$\forall x, y$, produit d'entiers, $p/x.y \Leftrightarrow p/x$ ou p/y

Si $\alpha, \beta \in \mathbb{Z}_p, \alpha\beta = 0 \Longrightarrow \alpha = 0$ ou $\beta = 0$

Montrons que tout élément $\alpha \neq 0$ de $\mathbb{Z}_p$ est inversible

Pour cela considérons les éléments $1\alpha, 2\alpha, \dots, (p-1)\alpha$ (tous distincts et différents de 0)

Comme ces éléments sont au nombre de $p - 1$, ces éléments sont

$1, 2, \dots, p - 1$

Il existe $k \in \mathbb{N}, 1 \leq k \leq p - 1/k\alpha = 1 \Longrightarrow k = \frac{1}{\alpha}$

Donc $\alpha' = cl(k) \bmod p$ est l'inverse de l'élément cherché.

3.10. Anneau de polynôme

Soit $(A, +, \cdot)$ un anneau avec élément unité

a. Définition
Un polynôme à une indéterminée x et à coefficient dans A est une somme formelle

$$p(x) = a_0 + a_1x + a_2x^2 + \cdots = \sum a_k x^k$$

où les $a_k \in A$ sont presque tous nuls
a_k : $k-$ème coefficient de $p(x)$

b. Notation
$p(x) = (a_0, a_1, a_2, \dots)$ avec $a_0, a_1, a_2, \dots \in A$
Exemple
$p(x) = (10,1,0,0-1, \dots)$
$= 10 + x + 0x^2 + 0x^3 - x^4 = 10 + x + x^4$ (pour alléger l'écriture)

c. Soit $A[x]$ l'ensemble des polynômes à une indéterminée x à coefficients dans A.
On a :

- $A \subset A[x]$ car $a \in A, a = (a, 0,0, \dots)$ est un polynôme particulier appelé polynôme constant ou mieux **scalaire**
- L'indéterminée $x = (0,1,0, \dots)$

d. Egalité
Soient $p(x) = \sum a_k x^k$ et $q(x) = \sum b_k x^k \in A[x]$
Alors $p(x) = q(x) \Leftrightarrow a_k = b_k, \forall k = 0,1,2, \dots$

e. Somme et produit de polynômes
Soient $p(x) = \sum a_k x^k$ et $q(x) = \sum b_k x^k \in A[x]$
Alors $p(x) + q(x) = c_0 + c_1x + c_2x^2 + \cdots$
$p(x) \cdot q(x) = d_0 + d_1x + d_2x^2 + \cdots$
où $c_r = a_r + b_r$
$d_r = a_0b_r + a_1b_{r-1} + \cdots + a_{r-1}b_1 + a_rb_0$
$= \sum_{i=0}^{r} a_i b_{r-i}$, $r = 0,1,2, \dots$
ou $= \sum_{p+q=r} a_p b_q$

f. $(A[x], +, \cdot)$ est un anneau avec élément unité
(Vérifier) T.P.

g. L'injection canonique $A \longrightarrow A[x]$
$a \longmapsto (a, 0,0, \dots)$ est un homomorphisme d'anneaux
(Vérifier)

h. Le degré d'un polynôme $p(x) = a_0 + a_1x + a_2x^2 + \cdots$ est le plus grand entier r tel que $a_r \neq 0$
Notation : $\deg p(x)$
Exemple : soit $p(x) = \left(-3,0,4, {}^{-4}/_{5}, 0, \dots\right)$
Alors $\deg p(x) = 3$
Convention : le polynôme nul $(0,0,0, \dots)$ est de degré 0
Soient $p(x), q(x) \in A[x]$, alors
$\deg\big(p(x) + q(x)\big) \leq \max\big(\deg p(x), \deg q(x)\big)$

$$\deg\big(p(x)\cdot q(x)\big) \leq \deg p(x) + \deg q(x)$$

i. Division euclidienne de polynôme

Considérons les coefficients dans un champ

i.1. Théorème

Soit $(A,+,\cdot)$ un champ

Soient $a(x)$ et $b(x) \in A[x]$ avec $b(x) \neq 0$

Alors il existe deux polynômes uniques $q(x)$, le quotient et $r(x)$, le reste tels que

$$a(x) = b(x)q(x) + r(x) \text{ et } 0 \leq \deg r(x) < \deg b(x)$$

Démonstration

Remarquons d'abord que si $b(x)$ est un scalaire c'est – à – dire

si $b(x) = \beta \in K$ et $\beta \neq 0$ alors $q(x) = \frac{1}{\beta}a(x)$ et $r(x) = 0$

On a bien $a(x) = \beta\frac{1}{\beta}a(x), 0 \leq \deg r(x) < \deg b(x)$

Nous allons raisonner par récurrence sur le degré de n

- Si $\deg a(x) = 0$ ou $\deg a(x) < \deg b(x)$

  Alors $q(x) = 0$ et $r(x) = a(x)$

  On a bien $a(x) = b(x)\cdot 0 + a(x)$
- Si $\deg a(x) \geq \deg b(x)$

  Alors supposons que le théorème est démontré pour les degrés de $a(x)$ inférieurs à n (Hypothèse de récurrence)

  Soient $a(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$ et

  $b(x) = \beta_0 + \beta_1 x + \cdots + \beta_m x^m$

  où $\alpha_n \neq 0, \beta_m \neq 0$ et $n \geq m$

  Considérons le polynôme

  $$a_1(x) = a(x) - \frac{\alpha_n}{\beta_m}x^{n-m}\cdot b(x)$$

  En effectuant

  $$a_1(x) = (\alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n) - \left(\frac{\alpha_n}{\beta_m}\beta_0 x^{n-m} + \cdots + \frac{\alpha_n}{\beta_m}\beta_{n-1}x^{n-1} + \alpha_n x^n\right)$$

  On voit que le terme de degré s'annule et donc

  $$\deg a_1(x) \leq n-1 < \deg a(x)$$

  Par hypothèse de récurrence, il existe alors $q_1(x)$ et $r(x)$ tels que

  $$\deg r(x) < \deg b(x) \text{ et } a_1(x) = b(x)\cdot q_1(x) + r(x)$$

  Finalement

  $$a(x) = a_1(x) + \frac{\alpha_n}{\beta_m}x^{n-m}\cdot b(x) = b(x)\left(q_1(x) + \frac{\alpha_n}{\beta_m}x^{n-m}\right) + r(x)$$

  Donc $q(x) = q_1(x) + \frac{\alpha_n}{\beta_m}x^{n-m}$ et $r(x)$ répondent au théorème

  Unicité de $q(x)$ et $r(x)$

  Supposons qu'il existe $q'(x)$ et $r'(x)$ qui répondent à la question

On a :

$$a(x) = b(x)q(x) + r(x) \text{ avec } 0 \leq \deg r(x) < \deg b(x)$$
$$-a(x) = b(x)q'(x) + r'(x) \text{ avec } 0 \leq \deg r'(x) < \deg b(x)$$
$$0 = b(x)q(x) - b(x)q'(x) + r(x) - r'(x)$$

Ce qui donne

$$b(x)q(x) - b(x)q'(x) = r'(x) - r(x)$$
$$\Longrightarrow \deg\Big(b(x)\big(q(x) - q'(x)\big)\Big) = \deg\big(r'(x) - r(x)\big) < \deg b(x)$$

Ceci n'est pas possible que si $q(x) - q'(x) = 0 \Longrightarrow q(x) = q'(x)$
et $r'(x) - r(x) = 0 \Longrightarrow r'(x) = r(x)$

i.2. Définition

Lorsque $r(x) = 0$ dans le théorème, on dit que $b(x)$ est un diviseur de $a(x)$ ou $b(x)$ divise $a(x)$

Exemple : Chercher, dans $\mathbb{R}[x]$, $q(x)$ et $r(x)$ pour

$a(x) = x^4 + 2x^3 - 4x^2 + 3x - 1$
$b(x) = 2x^2 - 3x + 2$

$$\begin{array}{l|l}
x^4 + 2x^3 - 4x^2 + 3x - 1 & 2x^2 - 3x + 2 \\
\hline
-x^4 + \frac{3x^3}{2} - x^2 & \frac{x^2}{2} + \frac{7x}{4} + \frac{1}{8} \\
\hline
\frac{7x^3}{2} - 5x^2 + 3x - 1 & \\
-\frac{7x^3}{2} + \frac{21x^2}{4} - \frac{7x}{2} & \\
\hline
\frac{x^2}{4} - \frac{x}{2} - 1 & \\
-\frac{x^2}{4} + \frac{3x}{8} - \frac{1}{4} & \\
\hline
-\frac{x}{8} - \frac{5}{4} &
\end{array}$$

On a bien

$$x^4 + 2x^3 - 4x^2 + 3x - 1 = \left[(2x^2 - 3x + 2)\left(\frac{x^2}{2} + \frac{7x}{4} + \frac{1}{8}\right)\right] - \frac{x}{8} - \frac{5}{4}$$

et $\deg\left(-\frac{x}{8} - \frac{5}{4}\right) < \deg(2x^2 - 3x + 2)$

3.11. Anneau de matrices

Soit $(K, +, \cdot)$ anneau avec élément unité 1

a. Définition de matrice

Considérons deux entiers naturels m et n

Posons $I(m,n) = \{1,2,\dots,m\} \times \{1,2,\dots,n\}$

Toute application $a : I(m,n) \longrightarrow K$ est appelé **matrice du type** (m,n) ou matrice à m lignes et n colonnes à coefficients dans K

L'image d'un couple $(i,j) \in I(m,n)$ est notée a_{ij} et appelée coefficient d'ordre (i,j) de la matrice

Une matrice est habituellement notée par un tableau

$$a = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

Dans ce tableau, le coefficient d'ordre (i,j) figure à l'intersection de la $i^{\text{ème}}$ ligne et de la $j^{\text{ème}}$ colonne

Notations

$a = (a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ ou simplement a_{ij}

Ou encore par une simple lettre majuscule A

L'ensemble des matrices du type (m,n) à coefficients dans K sera désigné par

$\mathfrak{M}_{m,n}(K)$

b. Opérations sur les matrices

b.1. Matrices égales

Deux matrices $a = (a_{ij})$ et $b = (b_{ij})$, $1 \le i,j \le n$ sont dites égales si elles sont de même ordre et si chaque élément de l'une est égal à l'élément correspondant de l'autre.

b.2. Somme de deux matrices de même type

Soient $a = (a_{ij}), b = (b_{ij}) \in \mathfrak{M}_{n,n}(K)$

Alors $a + b = (a_{ij} + b_{ij}) \in \mathfrak{M}_{n,n}(K)$

Exemple

Si $a = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}$ et $b = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{pmatrix}$

Alors $a + b = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & a_{13}+b_{13} \\ a_{21}+b_{21} & a_{22}+b_{22} & a_{23}+b_{23} \end{pmatrix}$

$$a - b = \begin{pmatrix} a_{11}-b_{11} & a_{12}-b_{12} & a_{13}-b_{13} \\ a_{21}-b_{21} & a_{22}-b_{22} & a_{23}-b_{23} \end{pmatrix}$$

b.3. Proposition

$(\mathfrak{M}_{m,n}(K), +)$ est un groupe abélien

L'élément neutre de la matrice nulle $0 = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$

L'opposé d'une manière $a = (a_{ij})$
est égale à $-a = (-a_{ij})$

b.4. Multiplication par un scalaire

Soient $\alpha \in K$ et $a = (a_{ij})$

Alors $\alpha a = \alpha(a_{ij}) = (\alpha a_{ij})$

Exemple : si $a = \begin{pmatrix} \frac{1}{2} & 3 \\ 2 & -1 \end{pmatrix}$ alors $\alpha a = \begin{pmatrix} \frac{\alpha}{2} & \alpha 3 \\ \alpha 2 & \alpha(-1) \end{pmatrix}$

b.5. Multiplication matricielle

Soient $a = (a_{ij})$ une matrice du type (m, n)

$b = (b_{ij})$ une matrice du type (n, q)

Alors le produit $a \cdot b$ est la matrice $c = (c_{ij})$ du type (m, q)

telle que

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj} = \sum_{k=1}^{n} a_{ik}b_{kj}\,, \forall (i,j) \in I(m,n)$$

Schéma

Ligne i $\begin{pmatrix} \cdots & \cdots & \cdots & \cdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \cdots & \cdots & \cdots & \cdots \end{pmatrix} \begin{pmatrix} \cdots & b_{1j} & \cdots \\ \cdots & b_{2j} & \cdots \\ \cdots & \cdots & \cdots \\ \cdots & b_{nj} & \cdots \end{pmatrix} = \begin{pmatrix} \cdots & \cdots & \cdots \\ \cdots & c_{ij} & \cdots \\ \cdots & \cdots & \cdots \end{pmatrix}$

Colonne j

Exemple

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \\ b_{31} & b_{32} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} + a_{13}b_{31} & a_{11}b_{12} + a_{12}b_{22} + a_{13}b_{32} \\ a_{21}b_{11} + a_{22}b_{21} + a_{23}b_{31} & a_{21}b_{12} + a_{22}b_{22} + a_{23}b_{32} \end{pmatrix}$$

$\in \mathfrak{M}_{2,3}(K)$ $\quad \in \mathfrak{M}_{3,2}(K)$ $\qquad\qquad \in \mathfrak{M}_{2,2}(K)$

Remarque

Le produit $a \cdot b$ n'est défini que lorsque le nombre de colonnes de la matrice a égale le nombre de lignes de la matrice b

b.6. Proposition

La multiplication matricielle est associative et distributive par rapport à l'addition des matrices

- Distributivité

  Soient a une matrice du type (m, n)

  b et c des matrices du type (n, q)

  Alors $a(b + c) = ab + ac$ et $(b + c)a = ba + ca$

  Car $\forall (i, j) \in I(m, q)$, on a :

  $$\sum_{k=1}^{n} a_{ik}(b_{kj} + c_{kj}) = \sum_{k=1}^{n} (a_{ik}b_{kj} + a_{ik}c_{kj}) = \sum_{k=1}^{n} a_{ik}b_{kj} + \sum_{k=1}^{n} a_{ik}c_{kj}$$

  (1) (2)

  (1) : le coefficient de $a(b + c)$ d'ordre (i, j)

  (2) : le coefficient de $ab + ac$ d'ordre (i, j)

  D'où $a(b + c) = ab + ac$. De même on vérifie $(b + c)a = ba + ca$

- Associativité

Supposons a, b et c des matrices telles que les produits $a(bc) = (ab)c$ sont définies, alors

$a(bc) = (ab)c$

En effet,

Si d_{ij} désigne le coefficient d'ordre (i,j) de $(ab)c$

et e_{ij} désigne le coefficient d'ordre (i,j) de $a(bc)$

$$d_{ij} = \sum_k \left(\sum_r a_{ir} b_{rk} \right) c_{kj} = \sum_r a_{ir} \left(\sum_k b_{rk} c_{kj} \right) = e_{ij}$$

b.7. Définition

$\forall n \in \mathbb{N}$, une matrice du type (n,n) est appelée **matrice carrée** d'ordre n

Notation

$\mathfrak{M}_n(K)$: désigne l'ensemble des matrices carrées d'ordre n

b.8. Proposition

$(\mathfrak{M}_n(K), +, \cdot)$ est un anneau unitaire (non commutatif en général) T.P.

- Lorsque K est commutatif, l'anneau $\mathfrak{M}_n(K)$ n'est jamais commutatif si $n \geq 2$

En effet, pour $n = 2$, il suffit, pour le voir, d'observer que

$$\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x & xy \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}$$

Pour que $ab = ba$, il faut que $xy = y$

3.12. Le corps $\mathbb{R}$ des nombres réels

a. $(\mathbb{R}, +, \cdot)$ est un champ (T.P.)

b. $(\mathbb{R}, \leq)$ est un ensemble totalement ordonné (T.P.)

c. $(\mathbb{R}, \leq)$ est compatible avec la structure de corps au sens suivant

$\forall x, y, z \in \mathbb{R}, x \leq y \Longrightarrow x + z \leq y + z$

$\forall x, y \in \mathbb{R}, x > 0$ et $y > 0 \Longrightarrow xy > 0$

3.13. Le corps des nombres complexes

a. Définitions

Un nombre complexe est un couple de nombres réels

Notation

L'ensemble des nombres complexes est noté $\mathbb{C}$

$\mathbb{C} = \{(x,y)/x, y \in \mathbb{R}\} = \mathbb{R} \times \mathbb{R}$

b. $\mathbb{C}$ est muni de deux opérations

- L'addition

$+ : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}$

$\big((x,y),(x',y')\big) \longmapsto (x,y) + (x',y') = (x + x', y + y')$

- La multiplication

$\cdot : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}$

$\big((x,y),(x',y')\big) \longmapsto (x,y) \cdot (x',y') = (xx' - yy', xy' + yx')$

§4. Exercices

4.1. Exercices résolus

4.1.1. Lesquelles des correspondances suivantes définissent une loi de composition interne sur l'ensemble cité

a. Sur $\mathbb{Z}$, à (x, y) on associe $\frac{2x}{y}$
b. Sur $\mathbb{Z}^*$, à (x, y) on associe $\frac{3x}{y}$
c. Sur $\mathbb{Q}$, à (x, y) on associe $\frac{x}{y}$
d. Sur $\mathbb{Q}^*$, à (x, y) on associe $\frac{x}{y}$

4.1.2. Lesquelles des opérations internes suivantes sont commutatives, associatives ?

a. Sur $\mathbb{N}$, à (x, y) on associe y^x
b. Sur $\mathbb{Q}$, à (x, y) on associe $\frac{xy}{4}$
c. Sur $\mathbb{R}$, à (x, y) on associe $x^2 + y$

4.1.3. Soient

P : L'ensemble des nombres pairs

et I : L'ensemble des nombres impairs

$(P, +)$ et $(I, +)$ sont – ils

a. Des demis – groupes ?
b. Des monoïdes ?

4.1.4. Pour chacune des lois de composition suivantes, dire si on a un groupe ou non. Justifier la réponse

a. Sur $\mathbb{Q}$, $x * y = xy$
b. Sur $\mathbb{Q}^*$, $x * y = x + y$
c. Sur $\mathbb{Z}$, $x * y = x - y$
d. Sur $\mathbb{Q}$, $x * y = x + y - 5$

4.1.5. Oui ou Non (justifiez la réponse)

a. L'ensemble $\mathbb{N}$ est – il un sous – groupe de $(\mathbb{Z}, +)$?
b. L'ensemble $\mathbb{Z}''$ des entiers relatifs impairs est – il un sous – groupe de $(\mathbb{Z}, +)$?
c. L'ensemble $\mathbb{R}^{*+}$ est – il un sous – groupe de $(\mathbb{R}^*, +)$?

4.1.6. Montrer que

a) $(\mathbb{Z}, +, \cdot)$ est un anneau
b) $(\mathbb{Q}, +, \cdot)$; $(\mathbb{R}, +, \cdot)$ et $(\mathbb{C}, +, \cdot)$ sont des corps

4.1.7. a. $\mathbb{Z}$ est – il un sous – corps de $\mathbb{Q}$?
b. $\mathbb{Q}$ est – il un sous – corps de $\mathbb{R}$?
c. $\mathbb{Q}^{*+}$ est – il un sous – corps de $\mathbb{R}$?

4.1.8. a. L'ensemble $\mathbb{R}$ est – il un espace vectoriel sur le corps $\mathbb{Q}$?
b. L'ensemble $\mathbb{Q}$ est – il un espace vectoriel sur le corps $\mathbb{R}$?

4.1.9. Calculer le $20^{\text{ème}}$ terme des P.A suivantes, puis la somme des 20 premiers termes
a. 2 ; 6 ; 10 ; 14 ; …
b. -5 ; $-3{,}5$; -2 ; $-0{,}5$; …

4.1.10. Dans une P.A., on donne :
a. $t_1 = 4$; $r = 2$, trouver t_8 et S_8
b. $r = 4$; $t_{10} = 39$, trouver t_1 et S_{10}
c. $t_1 = 3$; $t_n = 21, S_n = 120$, trouver r et n
d. $t_{100} = 199$; $S_{100} = 10000$, trouver t_1 et r

4.1.11. a. Former une P.A. dont le $4^{\text{ème}}$ terme soit 40 et le $12^{\text{ème}}$ terme 52
b. Dans une P.A., la somme du $8^{\text{ème}}$ et du $14^{\text{ème}}$ terme égale à 50 et le $5^{\text{ème}}$ terme est 13. Déterminer cette progression

4.1.12. Dans une P.G., on demande de calculer
a. t_5 et S_5, connaissant $t_1 = 3$ et $q = 4$
b. t_1 et S_7, connaissant $t_5 = 32$ et $q = -2$

4.1.13. a. Soit 2 le premier terme d'une P.G. de raison 4 calculer P_6 et S_5
b. Dans une P.G., le premier et le troisième termes sont 8 et 18. Trouver le cinquième terme

4.1.14. Trouver 3 nombres dont la somme est 49, le produit 2744 et qui sont en P.G.

4.1.15. Déterminer 4 nombres en P.G., sachant que la somme des deux premiers est 14 et la somme des deux derniers est 126

4.2. Exercices proposés

4.2.1. Lesquelles des correspondances suivantes définissent une loi de composition interne sur l'ensemble cité

a. Sur $\mathbb{R}$, à (x, y) on associe $\sqrt{xy}$

b. Sur $\mathbb{R}$, à (x, y) on associe $\sqrt[3]{xy}$

4.2.2. Lesquelles des opérations internes suivantes sont commutatives, associatives ?

a. Sur $\mathbb{Q}$, à (x, y) on associe $xy + 1$

b. Sur $\mathbb{N}$, à (x, y) on associe 2^{xy}

4.2.3. Pour chacune des lois de composition suivantes dire si on a un groupe ou non Justifier la réponse

a. Sur $\mathbb{R}$, $x * y = \sqrt[3]{x^3 + y^3}$
b. Sur $\mathbb{R}^-$, $x * y = x.y$

4.2.4. Soit $E = \mathbb{R}\backslash\{-1\}$. Pour tout couple (x, y) d'éléments de E, posons :

$$x \perp y = x + y + xy$$

a. Montrer que $\perp$ est une opération interne sur E ;
b. Montrer que $(E, \perp)$ est un groupe commutatif
c. Trouver la solution générale de l'équation $a \perp x = b$
d. Trouver la solution de l'équation

$5 \perp x = 8$; $\frac{1}{2} \perp x = -5$; $3 \perp x \perp (-1) = 4$

4.2.5. Dans une P.A., on donne

a. $t_1 = 23$; $r = -2$; $S_n = 140$, trouver t_n et n

b. $t_n = 20$; $r = 5$; $S_n = 20$, trouver t_1 et n

4.2.6. Dans une P.A. de 10 termes, la somme des termes est 245 et la différence des extrêmes est 45. Quelle est cette progression ?

4.2.7. Déterminer 4 nombres en P.G., sachant que la somme des deux premiers est 14 et la somme des deux derniers est 126

4.2.8. Etablir ces implications vraies

a. $\left(\vec{u} \neq \vec{0} \text{ et } \lambda\vec{u} = \mu\vec{u}\right) \Longrightarrow (\lambda = \mu)$

b. $(\lambda \neq 0 \text{ et } \lambda\vec{u} = \mu\vec{v}) \Longrightarrow (\vec{u} = \vec{v})$

4.2.9. Pour un demi – groupe $(E,*)$, les affirmations suivantes sont équivalentes

1. $(E,*)$ est un groupe
2. $E \neq \emptyset$ et $\forall a, b \in E$ chacune des équations
   $a * x = b$ et $y * a = b$ admet une et une seule solution dans E

4.2.10. Etudier les propriétés de la loi $*$ définie sur $\mathbb{R}$ par :

$$x * y = x + y - xy$$

4.2.11. On appelle centre d'un groupe $(G,*)$ l'ensemble C des éléments de G qui commutent avec tout élément de G

Montrer que C est un sous – groupe distingué de G

4.2.12. Parmi les ensembles suivants, lesquels sont sous – groupes de $(\mathbb{R}, +)$? de $(\mathbb{Q}^+,\cdot)$?

a. $\mathbb{Q}^+$ b. $6\mathbb{Z}$ c. $\{10^n/n \in \mathbb{Z}\}$ d. $\{a + b\sqrt{3}/a, b \in \mathbb{Z}\}$

4.2.13. Lesquelles des applications suivantes sont des homomorphismes de groupes
a. $f : \mathbb{Z} \longrightarrow \mathbb{R} \quad f(x) = x$
b. $f : \mathbb{R}^* \longrightarrow \mathbb{R}^* \quad f(x) = |x|$
c. $f : \mathbb{Z}_5 \longrightarrow \mathbb{Z}_2 \quad f(x) = cl(x) \bmod 2$

4.2.14. Soient $(G,*)$ un groupe et $a \in G$, montrer que la fonction
$f : \mathbb{Z} \longrightarrow G : x \longmapsto f(x) = a^x$ est un homomorphisme de $(\mathbb{Z}, +)$ vers $(G,*)$
Décrire le noyau et l'image de f

4.2.15. Vérifier que l'ensemble $\{a + b\sqrt{2}/a, b \in \mathbb{Z}\}$ est un sous – anneau de $(\mathbb{R}, +, \cdot)$
De même $\{a + b\sqrt{2}/a, b \in \mathbb{Q}\}$ est un sous – corps de $(\mathbb{R}, +, \cdot)$

4.2.16. Si $(A, +, \cdot)$ est un anneau tel que $a^2 = 0, \forall a \in A$
Montrer que $2a = 0,\ ab = -ba \quad \forall a, b \in A$

4.2.17. Soit $(A, +, \cdot)$ un anneau
Montrer que pour tout élément $a \in A$, l'ensemble $I_a = \{x/x \in A \text{ et } ax = 0\}$ est un idéal à droite de A

4.2.18. Dans $(\mathbb{Z}_7, +, \cdot)$ résoudre les équations
a. $5x + 1 = 3$ b. $2x - 3 =$ c. $3x + 2 = 4$

4.2.19. Résoudre le système d'équations ci – après dans $(\mathbb{Z}_{11}, +, \cdot)$

$$\begin{cases} 2x - 8y = 3 \\ 7x + y = 10 \end{cases}$$

4.2.20. Effectuer $A.B$, $A + B$ dans $\mathfrak{M}_3(\mathbb{C})$

$$A = \begin{pmatrix} -3 & \frac{1}{2} & 1 \\ 2 & 7 & \frac{2}{5} \\ 2 & 0 & -2 \end{pmatrix} \qquad B = \begin{pmatrix} 4 & -1 & 1 \\ 0 & 2 & \frac{1}{3} \\ \frac{-5}{6} & 1 & 5 \end{pmatrix}$$

4.2.21. Montrer que la fonction

$\varphi : \mathbb{C} \longrightarrow \mathfrak{M}_2(\mathbb{R}) \quad \varphi\big((x,y)\big) = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ est un homomorphisme d'anneaux et qu'elle est injective

4.2.22. Trouver le quotient $q(x)$ et le reste $r(x)$ pour les polynômes $a(x)$ et $b(x)$ suivants dans $K[x]$, K spécifié :
a. $a(x) = -2 + x^2 + 4x^3$ dans $\mathbb{Q}[x]$
$b(x) = 1 - 3x$
b. $a(x) = 24 - 9x + 6x^2 + 8x^3 - 2x^5$ dans $\mathbb{Q}[x]$
$b(x) = 2 + 2x + x^2$
c. $a(x) = 2 - 3x + 4x^2 + 3x^5 + x^6$ dans $\mathbb{Z}_7[x]$
$b(x) = -3 + 2x + x^2$

Solution ou indications de solution

4.1.1. d. Sur $\mathbb{Q}^*$, à (x, y) on associe $\frac{x}{y}$

4.1.2. – Opération interne, commutative
b. Sur $\mathbb{Q}$, à (x, y) on associe $\frac{xy}{3}$
– Opération interne, associative
b. Sur $\mathbb{Q}$, à (x, y) on associe xy

4.1.3. a.1. $(P, +)$ est un demi – groupe
Car (1) la loi + est interne c'est – à – dire $\forall x, y \in P, x + y \in P$
On a : $x \in P \Leftrightarrow x = 2x', x' \in \mathbb{N}$
$y \in P \Leftrightarrow y = 2y', y' \in \mathbb{N}$
D'où $x + y = 2x' + 2y' = 2(x' + y') = 2z' \in P$, avec $z' \in \mathbb{N}$
(2) La loi + est associative
C'est – à – dire $\forall x, y, z \in P, (x + y) + z = x + (y + z)$ cette associativité découle de celle de la loi + dans $\mathbb{N}$
a.2. $(P, +)$ est un monoïde
Car $(P, +)$ est un demi – groupe dont la loi + admet l'élément neutre $0 \in P$
On a : $\forall x \in P, 0 + x = x + 0 = x$
b.1. $(I, +)$ n'est pas un demi – groupe
Car la loi + n'est pas interne
En effet : $\forall x, y \in I, x + y \in I$ n'est pas interne
Contre – exemple : $3{,}5 \in I, 3 + 5 = 8 \notin I$
b.2. $(I, +)$ n'est pas un monoïde
Car $(I, +)$ n'est pas un demi – groupe et en plus la loi + dans I n'admet pas d'élément neutre

4.1.4. a. Non
Car tout élément appartenant à $\mathbb{Q}$ n'est pas inversible (plus exactement, $0 \in \mathbb{Q}$ n'est pas inversible)
b. Non
Car la loi $*$ n'est pas associative. En plus elle n'admet pas d'élément neutre.
c. Oui car la loi + est interne et associative
La loi + admet 5 comme élément neutre et enfin tout élément $x \in \mathbb{Q}$ a un symétrique $-x \in \mathbb{Q}$

4.1.5. a. Non car $(\mathbb{N}, +)$ n'est pas un groupe
b. Non car $0 \notin \mathbb{Z}''$
En plus $\mathbb{Z}''$ n'est pas stable pour la loi +
c. Oui

4.1.6. a. $(\mathbb{Z}, +, \cdot)$ est un anneau parce que

(1) $(\mathbb{Z}, +)$ est un groupe commutatif
(2) $(\mathbb{Z}, \cdot)$ est un demi – groupe
(3) $\forall x, y, z \in \mathbb{Z}, x(y+z) = xy + xz$
b. $(\mathbb{Q}, +, \cdot)$ est un corps. Il est en plus un corps commutatif
En effet (1) $(\mathbb{Q}, +)$ est un groupe commutatif
(2) $(\mathbb{Q}^*, \cdot)$ est un groupe
(3) $\forall a, b, c \in \mathbb{Q}, a(b+c) = ab + ac$
Même procédure avec $(\mathbb{R}, +, \cdot)$ et $(\mathbb{C}, +, \cdot)$ ce sont en plus des corps commutatifs

4.1.7. a. Non : il manque à $\mathbb{Z}$ la propriété selon laquelle
$\forall x \neq 0, \exists x^{-1} / x.x^{-1} = 1, \quad x, x^{-1} \in \mathbb{Z}$
b. Oui
c. Non

4.1.8. a. Oui
b. Non
} Pourquoi ?

4.1.9. On applique la formule
a. $t_n = t_1 + (n-1)r \qquad n = 20$ et $r = 4$
b. $S_n = \frac{t_1 + t_n}{2} n$

4.1.10. a. $t_8 = 4 + 7 \times 2 = 18$
D'où $S_8 = \frac{4+18}{2} \times 8 = 88$
c. $n = \frac{2S_n}{t_1 + t_n} = \frac{2 \times 120}{3+21} = 10$
$r = \frac{t_n - t_1}{n-1} = \frac{18}{9} = 2$

4.1.11. a. $t_4 = 40 = t_1 + 3r$
$t_{12} = 52 = t_1 + 11r$
D'où ce système de deux équations du premier degré à deux inconnues t_1 et r

$$\begin{cases} t_1 + 3r = 40 \\ t_1 + 11r = 52 \end{cases}$$

Sa solution soit par la méthode de substitution, soit par la méthode de comparaison, soit encore par la méthode de réduction au même coefficient donne $t_1 = 35{,}5$ et $r = 1{,}5$
Cette P.A. est donc
35,5 ; 37; 38,5 ; 40 ; 41,5 ; 43 ; 44,5 ; 46 ; 47,5 ; 49 ; 50,5 ; 52

4.1.12. a. Par définition, on a : $t_5 = 3.4^4 = 768$
En vertu de la formule de la somme $S_5 = 3\frac{4^5 - 1}{4-1} = 1023$

4.1.13. b. D'après 2.2.d et 2.2.a du §2. Chap.4

On a : $t_2 = \sqrt{8.18} = \sqrt{144} = 12 \Longrightarrow q = \frac{t_3}{t_2} = \frac{18}{12} = \frac{3}{2}$

4.1.14. Soit x, y, z ces nombres, on a :

$\begin{cases} x+y+z = 49 \\ xyz = 2744 \end{cases} \Leftrightarrow \begin{cases} x(1+q+q^2) = 49 & (1) \\ x^3q^3 = 2744 & (2) \end{cases}$ (voir 2.2.6.)

De (2) $q = \sqrt[3]{\frac{2744}{x^3}} = \frac{14}{x}$ (3)

(3) dans (1) $\Longrightarrow x^2 - 35x + 196 = 0$. D'où $\begin{cases} x = 28 \\ x = 7 \end{cases}$ ou

Donc si $x = 28$, alors $q = \frac{1}{2}$ d'où la P.G. $x = 28, y = 14$ et $z = 7$

Si $x = 7$, alors $q = 2$ d'où la P.G. $x = 7, y = 14$ et $z = 28$

Vérification

On a bien $\begin{cases} 28+14+7 = 49 \\ 28.14.7 = 2744 \end{cases}$

4.1.15. Soit y le premier terme et q la raison

On a $y + yq = 14 \Longrightarrow y(1+q) = 14$ (1)

$yq^2 + yq^3 = 126 \Longrightarrow yq^2(1+q) = 126$ (2)

De (1), on tire $1 + q = \frac{14}{y}$ (1')

De (2), on tire $1 + q = \frac{126}{yq^2}$ (2')

(1') et (2') $\Longrightarrow \frac{14}{y} = \frac{126}{yq^2}$ et $q^2 = \frac{126}{14} = 9 \Longrightarrow q = \pm 3$

Si $q = 3$, alors $y(1+q) = 14 \Longrightarrow y = \frac{14}{4} = 3{,}5$ et les 4 nombres sont :

3,5 ; 10,5 ; 31,5 ; et 94,5

Si $q = -3$, alors $y(1+q) = 14 \Longrightarrow y = -\frac{14}{2} = -7$ et les 4 nombres sont :

-7 ; 21 ; -63 et 189