Université Internationale d'Excellence
Tuniso-Malienne

Badalabougou en Commune 5
du District de BAMAKO
/UIE Mali
dg@uie-mali.com
+223 74 19 60 79

Université Internationale Privée d 'Excellence

Unité d'Enseignement : Algèbre

2_Business Intelligence

Charge de Cours : Dr Diawara Daouda

Maitre de Conférences

Université Internationale d'Excellence
Tuniso-Malienne

Badalabougou en Commune 5
du District de BAMAKO
/UIE Mali
dg@uie-mali.com
+223 74 19 60 79

Contenus du Cours

Chapitre 1 : Théorie Naïve d'Ensemble

Chapitre 2 : Groupes/Sous-Groupes

Chapitre 2 : Anneaux/Sous anneaux

Chapitre 2 : Corps

Chapitre 1_Theorie Naïve des ensembles

Introduction

Les notions de la théorie des ensembles et des fonctions sont à la base d'une présentation moderne des mathématiques. Immanquablement, on y fait appel pour la construction d'objets plus complexes, ou pour donner une base solide aux arguments logiques. En plus d'être des notions fondamentales pour les mathématiques, elles sont aussi cruciales en informatique, par exemple pour introduire la notion de structures de données.

I. Notion de base

Définition

Un ensemble est une collection d'objets possédant une ou plusieurs propriétés communes. Ces objets sont les éléments ou points de l'ensemble.

Notation

Généralement une lettre majuscule, mais pas obligatoirement. Un ensemble peut être donné :

- De manière explicite (définition en extension) comme par exemple :
  - $A=\{0,1\}$ *ou* $B=\{a,b,\cdots,z\}$
  - L'ensemble des entiers naturels : $\mathbb{N}:=\{0,1,2,3,\cdots\}$
  - L'ensemble des entiers relatifs : $\mathbb{Z}:=\{\cdots,-3,-2,-1,0,1,2,3,\cdots\}$
  - L'ensemble des nombres rationnels : $\mathbb{Q}:=\left\{\frac{a}{b}\,|\,a\in\mathbb{Z},b\in\mathbb{N}\ et\ b\neq 0\right\}$
  - L'ensemble $\mathbb{R}$ des nombres réels, qui inclue les nombres rationnels et tous les nombres qu'on peut construire à partir de ceux-ci par passage à la limite ; l'ensemble des entiers naturels entre 1et n
- Par une propriété caractérisant ses éléments, (définition en compréhension) comme par exemple :

$$C=\{x:x\ est\ entier\ pair\ compris\ entre\ 5\ et\ 233\}$$
$$=\{x\,|\,x\ est\ entier\ pair\ compris\ entre\ 5\ et\ 233\}$$

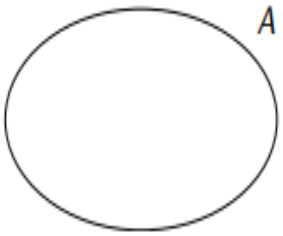
Diagrammes de Venn

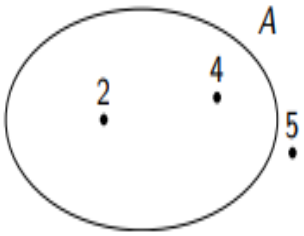
- On représente l'ensemble par un cercle ou une ellipse (appelées parfois patates).
- Si on veut marquer qu'un objet est un élément de l'ensemble, on le place dans la région correspondante.
- On représente plusieurs ensembles (généralement 2, 3 ou 4) par plusieurs patates.

Un diagramme de Venn, est une figure qui utilise des cercles ou d'autres formes (courbes fermés) entrecroisées pour mettre en évidence un ensemble et certaines de ses parties. Il est utilisé aussi pour schématiser des situations de dénombrement.

Exemple 1

Soit A l'ensemble des nombres entiers pairs.





Exemple 2

Parmi une promotion de 100 diplômés qui étaient à l'université il y a dix ans : 77 sont aujourd'hui salariés ; 35 sont pères de famille ; 27 sont salariés et pères de famille.

Quel est le nombre de diplômés qui ne sont ni salariés ni pères de famille ?

Indication de solution

Utilisons un diagramme de Venn pour dénombrer :

Soit E l'ensemble des diplômés. On désigne par A l'ensemble des diplômés qui sont salariés et par B l'ensemble des diplômés qui sont pères de famille.

Le premier nombre placé est 27 qui constitue le nombre d'éléments de $A \cap B$

On en déduit ensuite 50 = 77 – 27 et 8 = 35 –27

La somme de ces trois nombres (27 + 50 + 8 = 85) constitue le nombre d'éléments de $A \cup B$.

On en déduit enfin que le nombre de diplômés qui ne sont ni salariés ni pères de familles est 100-85 =15.

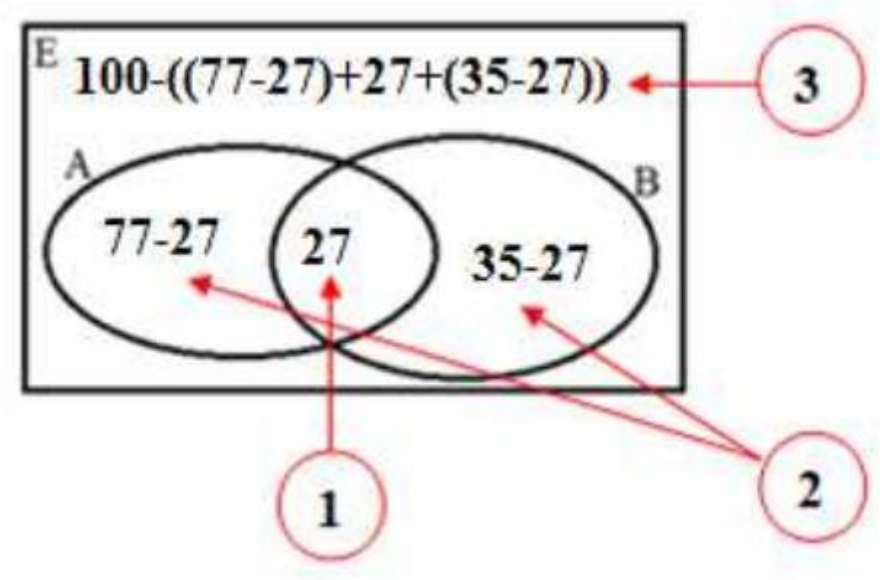


Diagramme de Carroll

Un diagramme de Carroll est un tableau à double entrée dans lequel les éléments (ou effectifs, ou fréquences) d'un ensemble sont classés selon deux critères (l'un en ligne, l'autre en colonne) de façon à mettre en évidence les sous-ensembles qui constituent ces critères

	A	$\overline{A}$	Total
B			
$\overline{B}$			
Total			

Exemple

On considère les données de l'exemple précédent : Parmi une promotion de 100 diplômés qui étaient à l'université il y a dix ans : 77 sont aujourd'hui

salariés ; 35 sont pères de famille ; 27 sont salariés et pères de famille.

En utilisant un tableau représentant ces données, répondre aux questions suivantes :

1. Quel est le nombre de diplômés qui sont aujourd'hui des pères de famille et non-salariés ?
2. Quel est le nombre de diplômés qui sont salariés et non pères de famille ?
3. Quel est le nombre de diplômés qui ne sont ni salariés ni pères de famille ?

Indication de solution

Utilisons un diagramme de Carroll pour dénombrer :

1ère étape :

Commençons par le tableau suivant dans lequel on place les données de l'exercice en utilisant la notation : A pour salarié et B pour père de famille.

	A (Salarié)	$\overline{A}$ (non salarié)	Total
B (Père de famille)	27		35
$\overline{B}$ (Non père de famille)			
Total	77		100

2ème étape :

Complétons le tableau précédent en effectuant les opérations suivantes :

	A (Salariée)	$\overline{A}$ (non salariée)	Total
B (Père de famille)	27	35-27=8	35
$\overline{B}$ (Non père de famille)	77-27=50	15	100-35=65
Total	77	100-77=23	100

On peut alors, par lecture directe du tableau, dire que :

1. Le nombre de diplômés qui sont des pères de famille et non-salariés est 8. (L'intersection de B et A).
2. Le nombre de diplômés qui sont salariés et non pères de famille est 50 (l'intersection de A et B)

Badalabougou en Commune 5
du District de BAMAKO
/UIE Mali
dg@uie-mali.com
+223 74 19 60 79

3. Le nombre de diplômés qui ne sont ni salariés ni pères de famille est 15 (l'intersection de A *et* B).

Tableau à double entrée

Un tableau à double entrée permet de traiter deux grandeurs de manière simultanée : une indiquée en ligne et l'autre en colonne.

Ce tableau permet de compter les cases vérifiant une certaine propriété.

Exemple

On lance successivement deux dés à 6 faces numérotés de 1 à 6.

1. Combien y a-t-il d'issues (résultats possibles) ?
2. Combien y a-t-il de cas où la somme des nombres inscrits sur les faces Supérieures est supérieure ou égale à 10 ?

Indication de Solution

Pour dénombrer, représentons la situation par un tableau à double entrée :

	1	2	3	4	5	6
1	$(1,1)$	$(1,2)$	$(1,3)$	$(1,4)$	$(1,5)$	$(1,6)$
2	$(2,1)$	$(2,2)$	$(2,3)$	$(2,4)$	$(2,5)$	$(2,6)$
3	$(3,1)$	$(3,2)$	$(3,3)$	$(3,4)$	$(3,5)$	$(3,6)$
4	$(4,1)$	$(4,2)$	$(4,3)$	$(4,4)$	$(4,5)$	$(4,6)$
5	$(5,1)$	$(5,2)$	$(5,3)$	$(5,4)$	$(5,5)$	$(5,6)$
6	$(6,1)$	$(6,2)$	$(6,3)$	$(6,4)$	$(6,5)$	$(6,6)$

1. On constate alors qu'il y a 6x6 = 36 résultats possibles.
2. Il y a 6 cas où la somme des nombres inscrits sur les faces supérieures est supérieure ou égale à 10 : $(4,6),(5,5),(5,6),(6,4),(6,5),(6,6)$

Premières relations

Appartenance

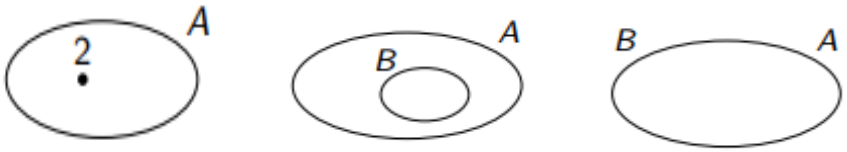
On écrit $x \in A$ (x appartient à A) pour signifier que x est un élément de l'ensemble A.

Inclusion

On écrit $B \subset A$ (B est inclus dans A, ou B est un sous-ensemble de A) quand tout élément de B est aussi un élément de A.

Egalité

On écrit $A = B$ (A *et* B sont égaux) quand les ensembles A *et* B ont les mêmes éléments. Cela se traduit aussi par le fait que $A \subset B$ et $B \subset A$.

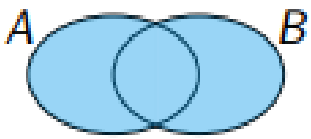


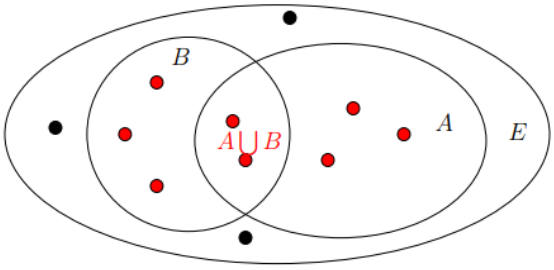
Operations sur les ensembles

Soit E un ensemble fini et A et B deux parties de E.

a. Union

On définit l'union de A et B comme : $A \cup B = \{x \in E \mid x \in A \text{ ou } x \in B\}$





L'Union des deux ensembles A et B notée $A \cup B$.Elle est définie par :

$x \in A \cup B \Leftrightarrow (x \in A \text{ ou } x \in B)$

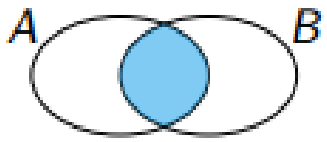
b. Intersection

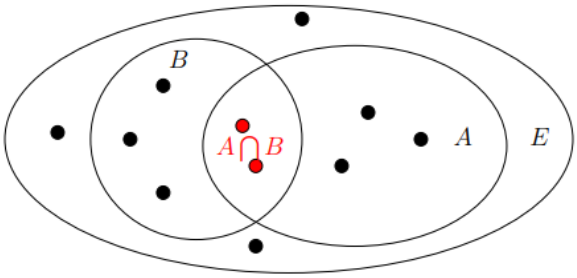
On définit l'intersection de A et B comme : $A \cap B = \{x \in E \mid x \in A \text{ et } x \in B\}$

L'intersection des deux ensembles A et B est notée $A \cap B$. Elle est définie par :

$x \in A \cap B \Leftrightarrow (x \in A \text{ et } x \in B)$

Deux ensembles A et B sont dits disjoints si $A \cap B = \varnothing$.





On a alors les relations suivantes :

Proposition

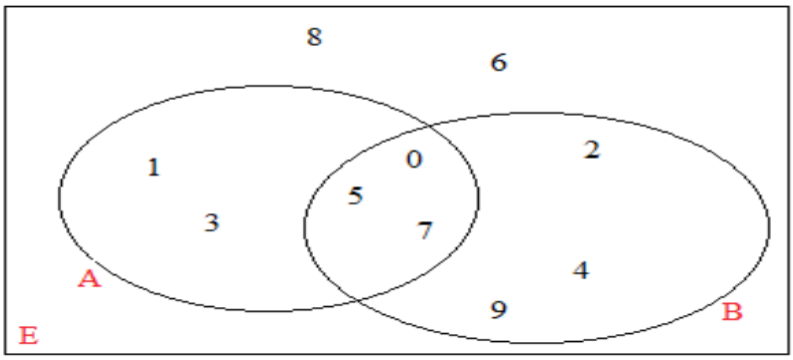
Soient E un ensemble et A, B et C des parties de E.

- $A \cap B \subset A$
- $A \subset A \cup B$
- $A \cup B = B \cup A (Commutavite)$
- $A \cap B = B \cap A (Commutavite)$
- $(A \cup B) \cup C = A \cup (B \cup C) (Associativite)$
- $(A \cap B) \cap C = A \cap (B \cap C)$
- $A \cup \varnothing = A$
- $A \cap E = A$
- $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$
- $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$

Exercice

On donne le diagramme ci-contre qui représente un ensemble E et deux

parties A *et* B de E . Ce diagramme est appelé diagramme de Venn (diagrammes d'ensembles).



1) Compléter par le symbole: $\in$ (appartient à) ou $\notin$ (n'appartient pas à) :

$0\cdots A; 8\cdots B; 3\cdots A, 5\cdots B; 4\cdots A\cap B, 5\cdots A\cup B; 6\cdots A\cup B; 6\cdots A; 3\cdots A\cap B$

2) Exprimer en extension (par liste d'éléments) chacun des ensembles suivants : $A, B, A\cap B, A\cup B, \bar{A}, \bar{B}$

3) Compléter par le symbole : $\subset$ (est inclus dans) ou $\not\subset$ (n'est pas inclus dans) :

$A\cdots E; B\cdots E; A\cdots A\cap B; B\cdots A\cup B; E\cdots A\cup B; A\cap B\cdots B; A\cup B\cdots E$

4) On exprime en extension l'ensemble E par la donnée de la liste explicite de ses éléments : $E=\{0,1,2,3,4,5,6,7,8,9\}$

Quelques ensembles particuliers

Voici quelques ensembles que nous manipulerons souvent :

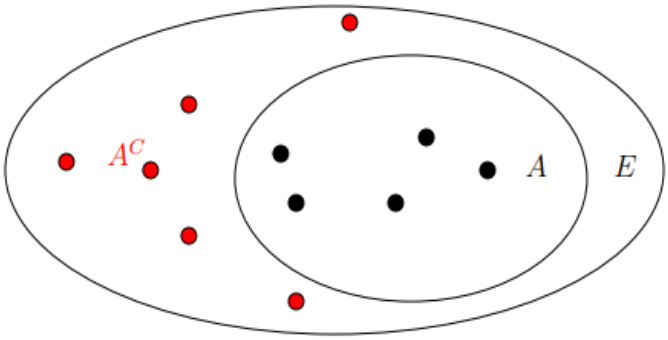
- L'ensemble ne contenant aucun élément est appelé ensemble vide, et est noté $\varnothing$ ou simplement $\{\ \}$.
- Un ensemble contenant un seul élément est appelé singleton. Si l'élément est a, on notera l'ensemble correspondant $\{a\}$

L'associativité permet de se dispenser d'écrire des parenthèses inutiles. On écrira par exemple $A\cup B\cup C$ au lieu de $(A\cup B)\cup C$

c. Complémentaire

On définit l'intersection de A dans E comme :

$$A^c = C_E^A = \{x \in E \mid x \notin A\}$$



Exemples

Notons $2\mathbb{N}$ l'ensemble des entiers pairs et $2\mathbb{N}+1$ l'ensemble des entiers impairs.

- $2\mathbb{N} \cup (2\mathbb{N}+1) = \mathbb{N}$
- $2\mathbb{N} \cap (2\mathbb{N}+1) = \varnothing$
- $(2\mathbb{N})^c = 2\mathbb{N}+1$

Proposition

Soit E un ensemble et A *et* B deux sous-ensembles de E . On a :

$(A^c)^c = A$

$A \cup A^c = E$

$A \cap A^c = \varnothing$

$A^c \cup B^c = (A \cap B)^c$ $(Loi\ de\ Morgan)$

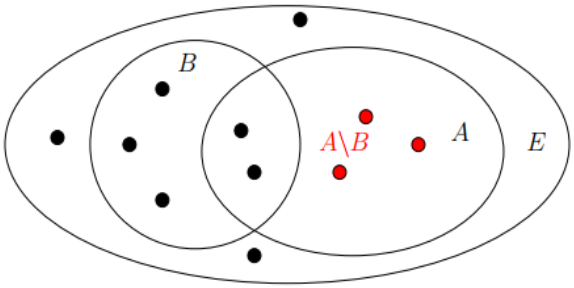
$A^c \cap B^c = (A \cup B)^c$ $(Loi\ de\ Morgan)$

On utilisera parfois également la différence et la différence symétrique de deux ensembles, définies de la façon suivante :

d. Différence

Soit E un ensemble et A *et* B deux sous-ensembles de E .

On définit la différence de A *et* B comme $A \setminus B = \{x \in E \mid x \in A \text{ et } x \notin B\}$



Exemple

Par exemple sur $\mathbb{N}$ on pose :

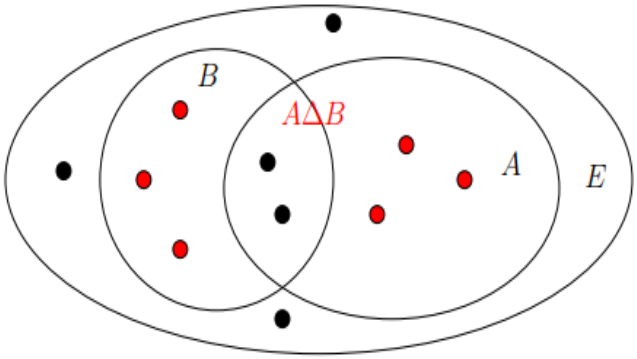
$A=\{1,2,3\}$ *et* $B=\{2,3,4\}$

$A \setminus B=\{1\}$

e. Différence symétrique

On définit la différence symétrique de A *et* B comme

$$A\Delta B=\{x\in E \mid (x\in A \text{ et } x\notin B) \text{ ou } (x\notin A \text{ et } x\in B)\}$$



Exemple

Par exemple sur $\mathbb{N}$ $\{1,2,3\}\Delta\{3,4,2\}=\{1,4\}$

f. Partition

Une famille $(A_i)_{i\in I}$ de parties d'un ensemble Ω est une partition de si

$$\begin{cases} \bigcup_{i\in I} A_i=\Omega \\ \forall (i,j)\in I^2, (i\neq j \Rightarrow A_i\cap A_j=\varnothing) \end{cases}$$

$$\begin{cases} A \subset B \Leftrightarrow \forall x \in E, x \in A \Rightarrow x \in B \\ A \subset B \Leftrightarrow A \cap B = A \\ A \text{ et } B \text{ sont disjoints si } A \cap B = \varnothing \end{cases}$$

g. Produit cartésien

Avant d'introduire la prochaine construction, rappelons que deux couples (a,b) et (c,d) sont égaux si et seulement si on a les deux égalités $a = c$ et $b = d$.

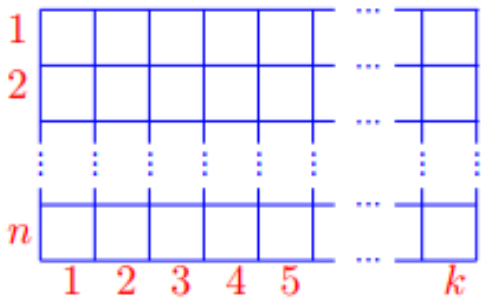
Le produit cartésien de A et B est l'ensemble de tous les couples (x,y), avec x élément de A et y élément de B. Autrement formule, on a :

$$A \times B = \{(x,y) \mid x \in A \text{ et } y \in B\}$$

Une illustration du produit cartésien est donnée par :

$$\begin{aligned} \{a,b,c,d\} \times \{1,2,3,4,5\} = \{&(a,1),(a,2),(a,3),(a,4),(a,5), \\ &(b,1),(b,2),(b,3),(b,4),(b,5), \\ &(c,1),(c,2),(c,3),(c,4),(c,5), \\ &(d,1),(d,2),(d,3),(d,4),(d,5)\} \end{aligned}$$

Dans le cas des ensembles finis $[n] = \{1,2,3,\cdots,n\}$ et $[k] = \{1,2,3,\cdots,k\}$, on constate que les éléments du produit cartésien $[n] \times [k]$ s'identifient aux *cases* d'un *tableau* (ou d'une matrice) ayant n lignes et k colonnes :



Remarquons qu'on utilise ici des coordonnées matricielles, indexant les lignes du haut vers le bas, plutôt que des coordonnées cartésiennes pour lesquelles on indexerait les lignes du bas vers le haut. A strictement parler, le produit cartésien n'est pas associatif. Ainsi, les éléments de $(A \times B) \times C$ sont de la

forme $((x,y),z)$ avec $x \in A, y \in B$ et $z \in C$; tandis que ceux de $A \times (B \times C)$ sont de la forme $(x,(y,z))$. On considère cependant souvent une construction intermédiaire, dénotée $A \times B \times C$ dont les éléments sont des triplets (x,y,z). Lorsque $A, B \text{ et } C$ sont des ensembles finis, les éléments de $A \times B \times C$ peuvent se représenter sous forme de tableau tridimensionnel (un peu comme dans la Figure ci-contre). Plus généralement, on a le produit cartésien multiple :

$$A_1 \times A_2 \times \cdots A_n = \{(x_1, x_2, \cdots x_n) \mid x_i \in A_i, 1 \le i \le n\}.$$

Cardinal d'un ensemble

Le cardial d'un ensemble E est le nombre d'éléments de cet ensemble, le cardinal de E est noter $cardE$.

Compter les éléments d'un ensemble

Lorsqu'on cherche à compter les éléments d'un ensemble A, le problème se décompose souvent en un (ou des) problèmes plus simples, selon que l'ensemble à énumérer peut se décrire en termes des constructions de base sur les ensembles.

Théorème

Si $A \text{ et } B$ sont des ensembles finis, respectivement de cardinal $n \text{ et } k$ et on note $card(A) = n \text{ ou } |A| = n \text{ et } card(B) = k \text{ ou } |B| = k$.

Alors on a les égalités suivantes :

1. $|A + B| = n + k$
2. $|A \times B| = n \times k$
3. $|\Im(A)| = 2^n$
4. $|\Im_k(A)| = \binom{n}{k}$
5. $|B^n| = k^n$

Badalabougou en Commune 5
du District de BAMAKO
/UIE Mali
dg@uie-mali.com
+223 74 19 60 79

Nous avons : $\begin{cases} card\left(A\cup B\right)=cardA+cardB-card\left(A\cap B\right) \\ card\left(A\cup \bar{A}\right)=cardA+card\bar{A} \\ A\cap B=\varnothing \Leftrightarrow card\left(A\cup B\right)=cardA+cardB \\ card\left(A\times B\right)=cardA\times cardB \\ A\subseteq B\Leftrightarrow card\left(A\cap B\right)=cardA\ et\ card\left(A\cup B\right)=cardB \end{cases}$

Si $cardA=n$ alors $card\wp\left(A\right)=2^n$, $\wp\left(A\right)$ désigne l'ensemble des parties de A

Relation d'équivalence

Définition 1

Une relation sur un ensemble E, c'est la donnée pour tout couple $\left(x,y\right)\in E\times E$ de « Vrai » (s'ils sont en relation), ou de « Faux » sinon.

Notation

On note : $x\Re y$ si $x\ et\ y$ sont en relation

Définition 2

Soit E un ensemble et $\Re$ une relation, c'est une relation d'équivalence si :

— $\forall x\in E, x\Re x$ (Réflexivité)

— $\forall x,y\in E, x\Re y\ et\ y\Re x$ (Symétrie)

— $\forall x,y,z\in E, x\Re y\ et\ y\Re z\Rightarrow x\Re z$ (Transitivité)

Exemples

1. La relation $\Re$ être parallèle est une relation d'équivalence pour l'ensemble E des droites affines du plan.
2. La relation être du même âge est une relation d'équivalence.
3. La relation être perpendiculaire n'est pas une relation d'équivalence (ni la réflexivité, ni la transitivité ne sont vérifiées).
4. La relation $\leq$ (sur $E=\mathbb{R}$ par exemple) n'est pas une relation d'équivalence (La symétrie n'est pas vérifiée).

Classes d'équivalence

Soit $\Re$ une relation d'équivalence sur un ensemble E. Soit $x\in E$, la classe d'équivalence de x est :

$\mathrm{cl}(x) = \{y \in E \mid y \Re x\}$

$\mathrm{cl}(x)$ est donc un sous-ensemble de E, on le note aussi $\overline{x}$. Si $y \in \mathrm{cl}(x)$, on dit que y un représentant de $\mathrm{cl}(x)$.

Soit E un ensemble et $\Re$ une relation d'équivalence.

Proposition

On a les propriétés suivantes :

1) $\mathrm{cl}(x) = \mathrm{cl}(y) \Leftrightarrow x \Re y$

2) Pour tout $x, y \in E, \mathrm{cl}(x) = \mathrm{cl}(y)$ *ou* $\mathrm{cl}(x) \cap \mathrm{cl}(y) = \varnothing$.

3) Soit C un ensemble de représentants de toutes les classes alors $\{\mathrm{cl}(x) \mid x \in C\}$ Constitue une partition de E.

Une partition de E est un ensemble $\{E_i\}$ de parties de E tel que :

$E = \bigcup_i E_i$ *et* $E_i \cap E_j = \varnothing (si\ i \neq j)$

Exercice 1

Définissez les ensembles suivants par compréhension :

1. L'ensemble des entiers non négatifs plus petits que 4 ;
2. L'ensemble des entiers strictement positifs divisibles par 3 et plus petits que 4 ;
3. L'ensemble des nombres impairs ;
4. L'ensemble des carrés dont la racine est située entre 10 et 22
5. L'ensemble des puissances de 2.

Exercice 2

Soit A *et* B tels que : $\begin{cases} Card(A \cap B) = 20 \\ Card(A \cup B) = 90 \end{cases}$

La proposition suivante est-elle V ou F ?

$CarA = 20$ *et* $CarB = 70$

Coefficients du binôme de Newton

Le nombre de parties à k éléments d'un ensemble à n éléments est noté $\binom{n}{k}$ *ou* C_n^k.

Exemple

Les parties à deux éléments de $\{1,2,3\}$ sont $\{1,2\},\{1,3\}$ *et* $\{2,3\}$ donc $\binom{3}{2}=3$

Le nombre de parties de $\{1,2,3,4,5\}$ $2^5=32$ dont :

- $\binom{5}{0}=1$ (La seule partie n'ayant aucun élément est l'ensemble vide),
- $\binom{5}{1}=5$ (Les parties à un seul élément : 5 singletons),
- $\binom{5}{2}=10$ (Il y a 10 paires),
- $\binom{5}{3}=10$
- $\binom{5}{4}=5$
- $\binom{5}{5}=1$ (La seule partie ayant 5 éléments est l'ensemble tout entier).

Sans calculs on peut déjà remarquer les faits suivants :

Proposition

- $\binom{n}{0}=1,\binom{n}{1}=n,\binom{n}{n}=1$
- $\binom{n}{k}=\binom{n}{n-k}$
- $\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{k}+\cdots+\binom{n}{n}=2^n$

Par exemple pour l'exemple précèdent on a :

$$\binom{5}{0}+\binom{5}{1}+\binom{5}{2}+\binom{5}{3}+\binom{5}{4}+\binom{5}{5}=32=2^5$$

Proposition

$$\binom{n}{k}=\binom{n-1}{k}+\binom{n-1}{k-1} \qquad (0<k<n)$$

Proposition Une autre façon de calculer le coefficient du binôme de Newton repose sur la formule suivante :

$$\binom{n}{k}=\frac{n!}{k!(n-k)!}$$

Formule du binôme de Newton

Théorème

Soient $a,b\in\mathbb{R}$ et n un entier positif alors : $(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k=\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}$

Autre formule

Pour tout couple (a,b) de nombres réels on a :

$$a^n-b^n=(a-b)\sum_{k=0}^{n-1}a^k b^{n-1-k}$$

Exercice

On définit sur la relation $\Re$ par : $(x,y)\Re(x',y')\Leftrightarrow x+y=x'+y'$

1. Montrer que $\Re$ une relation d'équivalence.
2. Trouver la classe d'équivalence du couple $(0,0)$

Solution

1. $\Re$ est une classe d'équivalence si et seulement si elle est réflexive et symétrique et transitive.
   a. $\Re$ est réflexive $\Leftrightarrow$ $\forall(x,y)\in\mathbb{R}^2,(x,y)\Re(x,y)$

   $(x,y)\Re(x,y)\Leftrightarrow x+y=x+y$

   D'où $\Re$ est réflexive

b. $\Re$ est symétrique si et seulement si :

$$\forall (x,y),(x',y') \in \mathbb{R}^2, (x,y)\Re(x',y') \Rightarrow (x',y')\Re(x,y)$$

$$\begin{aligned}(x,y)\Re(x',y') &\Rightarrow x+y = x'+y' \\ &\Rightarrow x'+y' = x+y \\ &\Rightarrow (x',y')\Re(x,y)\end{aligned}$$

D'où $\Re$ est symétrique

c. $\Re$ est transitive si et seulement si :

$$\forall (x,y),(x',y'),(x",y") \in \mathbb{R}^2,$$
$$(x,y)\Re(x',y') \wedge (x',y')\Re(x",y") \Rightarrow (x,y)\Re(x",y")$$

$$(x,y)\Re(x',y') \wedge (x',y')\Re(x",y")$$
$$\Rightarrow \begin{cases} x+y = x'+y' \\ \wedge \\ x'+y' = x"+y" \end{cases} \Rightarrow x+y = x"+y" \Rightarrow (x,y)\Re(x",y")$$

D'où $\Re$ est transitive

Ains $\Re$ est une relation d'équivalence.

2. Trouvons la classe d'équivalence du couple $(0,0)$

$$\begin{aligned}C((0,0)) &= \{(x,y) \in \mathbb{R}^2 / (x,y)\Re(0,0)\} \\ &= \{(x,y) \in \mathbb{R}^2 / x+y = 0\} \\ &= \{(x,y) \in \mathbb{R}^2 / y = -x\} \\ &= \{(x,-x) / x \in \mathbb{R}\}\end{aligned}$$

Exercice

Parmi les 164 étudiants de John Venn de John Venn, on a fait une enquête pour savoir quels condiments (ketchup, relish ou moutarde) ils mettent dans leurs hotdogs.

Voici les résultats.

- 10 étudiants n'ajoutent aucun condiment.
- 25 étudiants ne mettent que du ketchup.
- 27 étudiants mettent de la relish et de la moutarde.

- 15 étudiants mettent les 3 condiments.
- 70 étudiants mettent 2 condiments.
- 80 étudiants mettent de la relish.
- 19 étudiants ne mettent que du ketchup et de la moutarde.

À l'aide d'un diagramme de Venn, détermine combien d'étudiants mettent de la moutarde dans leurs hotdogs.

Indication de solution

Commencer par définir nos ensembles.

Ω : tous les étudiants de l'université de John Venn.

K : les étudiants qui mettent du ketchup dans leurs hotdogs

R : les étudiants qui mettent de la relish

M : les étudiants qui mettent de la moutarde

On analyse les indices un à la fois.

- 10 étudiants n'ajoutent **aucun condiment**.

Cela signifie que ces 10 étudiants ne se retrouvent ni dans l'ensemble K, ni dans l'ensemble R, ni dans l'ensemble M. Il faut donc inscrire 10 dans l'univers des possibles, mais à l'extérieur des cercles.

- 25 étudiants ne mettent **que du ketchup**.

On inscrit donc 25 dans la partie de l'ensemble K qui est à l'extérieur des ensembles R et M.

- 27 étudiants mettent de la relish **et** de la moutarde

Il y a donc un total de 27 étudiants dans la partie commune aux ensembles R et M. Toutefois, cette partie du diagramme se divise elle-même en 2. Il faut donc analyser d'autres indices avant de répartir ces 27 étudiants.

- 15 étudiants mettent **les 3 condiments**.

On inscrit donc 15 dans la partie commune aux 3 cercles.

On revient à l'indice laissé de côté : 27 étudiants mettent de la relish **et** de la moutarde.

On doit avoir un total de 27 dans la partie commune aux ensembles R et M.

On en a déjà placé 15. Il en reste donc 12 à placer, car 27-15=12.

- 70 étudiants mettent 2 condiments.

Autrement dit, la somme des 3 sections qui sont communes à 2 ensembles doit être de 70. On laisse cet indice de côté pour le moment.

- 80 étudiants mettent de la relish.

On doit aussi laisser cet indice de côté pour le moment, car il y a encore 2 parties de l'ensemble R à remplir.

- 19 étudiants ne mettent **que** du ketchup **et** de la moutarde.

Il faut donc placer 19 dans la partie commune aux ensembles K et M, mais à l'extérieur de R.

On revient au 1er indice laissé de côté : 70 étudiants mettent 2 condiments.

On trouve le nombre à placer dans la partie commune aux ensembles K et R, mais à l'extérieure de M en faisant 70-19-12=39.

On revient au dernier indice laissé de côté : 80 étudiants mettent de la relish.

On trouve maintenant le nombre d'étudiants qui ne mettent que de la relish en faisant 80-39-15-12=14.

Toutes les parties du diagramme de Venn ont été remplies sauf une. Pour compléter le diagramme, il faut considérer le nombre total d'élèves interrogés : 164. Ainsi, pour trouver la valeur à inscrire dans la section manquante, on fait une soustraction.

164-25-39-14-10-19-15-12=30

On peut maintenant répondre à la question.

On sait que 30 étudiants ne mettent **que de la moutarde** dans leurs hotdogs, mais si on veut connaitre le nombre total d'étudiants qui mettent de la moutarde, il faut additionner les valeurs de toutes les parties de l'ensemble M.

19+15+12+30=76

Réponse

Il y a 76 étudiants de l'université de John Venn qui mettent de la moutarde dans leurs hotdogs.

Chapitre 2_Notions fondamentales sur les groupes

I. Définitions et Exemples

On appelle groupe tout ensemble non vide G muni d'une loi de composition interne $*$ telle que :

- $\forall x, y \in G, x * y \in G$ (On dit que $*$ est une loi de composition interne)
- $\forall x, y, z \in G, (x * y) * z = x * (y * z)$ (On dit que $*$ est une loi de composition interne associative)
- Pour tout $x \in G$, il existe $e \in G$ tel que $x * e = e * x = x$ (e est l'élément neutre pour la loi $*$)
- Pour tout $x \in G$, il existe $x' \in G$ tel que $x * x' = x' * x = e$ (x' est l'inverse de x et noter x^{-1})

De plus si l'opération vérifie : $\forall x, y \in G, x * y = y * x$ (Commutativité) alors on dit que G est un groupe commutatif ou abélien

Remarque

Si e et x' existent alors ils sont uniques

Exemple 1

$(\mathbb{R}^*, \times)$ est un groupe abélien.

En effet :

— Si $x, y \in \mathbb{R}^*, x \times y \in \mathbb{R}^*$ alors ($\times$ est une loi de composition interne : LCI)

— Soient $x, y, z \in \mathbb{R}^*, x \times (y \times z) = (x \times y) \times z$ ($\times$ est une loi associative)

— Pour tout $x \in \mathbb{R}^*, 1 \times x = x \times 1 = x$ (1 est l'élément neutre pour $\times$)

— Pour tout $x \in \mathbb{R}^*$, $\frac{1}{x} \times x = x \times \frac{1}{x} = 1$ ($x' = \frac{1}{x}$ est l'inverse de x et notée x^{-1})

Ces propriétés font de $(\mathbb{R}^*, \times)$ un groupe

- E plus pour $x, y \in \mathbb{R}^*, x \times y = y \times x$ ($\times$ est une loi commutative)

Donc $(\mathbb{R}^*, \times)$ est un groupe abélien

Badalabougou en Commune 5
du District de BAMAKO
/UIE Mali
dg@uie-mali.com
+223 74 19 60 79

Exemple 2

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

Théorème

Dans un groupe $(E,*)$ l'élément neutre e est unique, de plus tout élément $x \in E$ admet un unique élément symétrique de E

Exercice 1

On munit $A=\mathbb{R}\times\mathbb{R}$ de deux lois définies par :

$(x,y)+(x',y')=(x+x',y+y')$ et $(x,y)*(x',y')=(xx',xy'+x'y)$

1. Montrer que $(A,+)$ est un groupe commutatif.
2. Montrer que :
   a. Montrer que la loi $*$ est commutative.
   b. Montrer que $*$ est associative
   c. Déterminer l'élément neutre de A pour la loi $*$.

Exercice 2

Soit $G=\mathbb{R}^*\times\mathbb{R}$ et $*$ la loi dans G définie par: $(x,y)*(x',y')=(xx',xy'+y)$

1. Montrer que $(G,*)$ est un groupe non commutatif
2. Montrer que $(]0,+\infty[\times\mathbb{R},*)$ est un sous-groupe de $(G,*)$

Exercice 3

On définit sur $G=\mathbb{R}^*\times\mathbb{R}$ loi interne $*$ comme suit :

$\forall(x,y),(x',y')\in G,(x,y)*(x',y')=(xx',xy'+y)$

1. Montrons que $(G,*)$ est un groupe non commutatif.
2. Ce groupe est-il abélien ?

Exercice 4

Soit $*$ une loi définie sur IR par : $\forall x,y\in\mathbb{R}, x*y=xy+(x^2-1)(y^2-1)$

1. Vérifier que $*$ est commutative, non associative et admet un élément neutre.

Résoudre les équations suivantes : $2*y=5,\ x*x=1$

Exercice 5

Soit $E=\{1,2,3,4\}$ et $\Re$ la relation binaire sur dont le graphe est

$\Gamma=\{(1,1),(1,2),(2,1),(2,2),(3,3),(3,4)(4,3),(4,4)\}$

1. Vérifier que la relation $\Re$ est une relation d'équivalence.
2. Faire la liste des classes d'équivalences distinctes et donner l'ensemble quotient.

II. Sous-groupes

Soit $(E,*)$ un groupe, une partie $H \subset E$ est un sous-groupe de E si :

- $H \neq \varnothing (e \in H)$
- Pour tout $x, y \in H$ on a : $x * y \in H$
- Pour tout $x \in H$,on a : $x^{-1} \in H$

Notez qu'un sous-groupe H est aussi un groupe $(H,*)$ avec la loi introduite par celle de E .

Exemple

$(\mathbb{R}_+^*,\times)$ est un sous-groupe de $(\mathbb{R}^*,\times)$

En effet

— $1 \in \mathbb{R}_+^*$

— Si $x, y \in \mathbb{R}_+^*$ alors $x \times y \in \mathbb{R}_+^*$

— Si $x \in \mathbb{R}_+^*$ alors $x^{-1} = \frac{1}{x} \in \mathbb{R}_+^*$

Remarque

Un critère pratique et plus rapide pour prouver que H est un sous-groupe de E est : $\begin{cases} H \neq \varnothing \\ \forall x, y \in H, x * y^{-1} \in H \end{cases}$

Sous-groupe de $\mathbb{Z}$

Les sous-groupes de $(\mathbb{Z},+)$ sont les $n\mathbb{Z}$, pour, $n \in \mathbb{Z}$ désigne l'ensemble des multiples de n et $n\mathbb{Z}=\{kn / k \in \mathbb{Z}\}$. Par exemple

$2\mathbb{Z}=\{\cdots,-4,-2,0,2,4,\cdots\}$ Est l'ensemble des multiples paires

Badalabougou en Commune 5
du District de BAMAKO
/UIE Mali
dg@uie-mali.com
+223 74 19 60 79

$7\mathbb{Z} = \{\cdots, -14, -7, 0, 7, 14, \cdots\}$ L'ensemble des multiples de 7

$(2\mathbb{Z}, +)$ et $(7\mathbb{Z}, +)$ sont des sous-groupes de $(\mathbb{Z}, +)$

Exercice

Montrer que les ensembles $b\mathbb{Z}$ muni de l'addition sont des sous-groupes de $(\mathbb{Z}, +)$

Remarque

Il est facile de montrer que $(n\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$

- $n\mathbb{Z} \subset \mathbb{Z}$
- $0 \in n\mathbb{Z} \Rightarrow n\mathbb{Z} \neq \varnothing$
- Soit $x, y \in n\mathbb{Z}, x = kn$ et $y = k'n$, $(k, k') \in \mathbb{Z}^2$, $x + y = kn + k'n = (k + k')n \in n\mathbb{Z}$
- Soit $x \in n\mathbb{Z}, -x = -kn = (-k)n = k'n \in n\mathbb{Z}$

Sous-groupes distingués

- Soit $(G, *)$ un groupe et H un sous-groupe de G. Nous disons que H est distingué dans G (ou normal dans G, ou encore invariant) s'il vérifie la propriété suivante : $\forall x \in G, x^{-1} * H * x \subset H \quad (1)$

En d'autres termes $\forall x \in G,\ \forall h \in H,\ x^{-1} * h * x \in H$.

L'élément $x^{-1} * h * x$ s'appelle le conjugué de h par x.

- Un sous-groupe H de G est distingué si les conjugués de ses éléments appartiennent encore à H. Certains disent que H est fermé pour la conjugaison.
- En réalité la condition (1) est équivalente à $\forall x \in G \quad x^{-1} * H * x = H$

III. Groupes quotients

Soit $(E, *)$ un groupe et H un sous-groupe de E. On définit une relation binaire $\Re$ sur E par : $\forall a, b \in E, a \Re b \Leftrightarrow ab^{-1} \in H$

Propriété

$\Re$ est une relation d'équivalence sur E.

Badalabougou en Commune 5
du District de BAMAKO
/UIE Mali
dg@uie-mali.com
+223 74 19 60 79

En effet

- R est réflexive car $\forall x \in E,$ comme H est un sous-groupe de E

alors $x * x^{-1} = e \in H$,donc $\forall x \in E, x\Re x$

- $\Re$ est symétrique

$$\begin{cases} \forall x, y \in E, x\Re y \Leftrightarrow x * y^{-1} \in H \Leftrightarrow \left(x * y^{-1}\right)^{-1} \in H \\ \Leftrightarrow y * x^{-1} \in H \Rightarrow y\Re x \end{cases}$$

- $\Re$ est transitive car $\forall x, y, z \in E$

$(x\Re y) \wedge (y\Re z) \Leftrightarrow \left[\left(xy^{-1}\right) \in H\right] \wedge \left[\left(yz^{-1}\right) \in H\right]$

$\Leftrightarrow \left(xy^{-1}\right) * \left(yz^{-1}\right) \in H$ (H est un sous-groupe)

$\Leftrightarrow \left[x * \left(y^{-1} * y\right) * z^{-1}\right] \in H$ (* est associative)

$\Leftrightarrow \left(xz^{-1}\right) \in H \Rightarrow x\Re z$

Conclusion

Des trois propriétés on déduit que $\Re$ est une relation d'équivalence. On note $E_{/H}$ l'ensemble quotient $E_{/R}$ .On définit sur $E_{/H} \times E_{/H}$ l'opération $\oplus$ par :

$$\forall \left(\dot{a}, \dot{b}\right) \in E_{/H} \times E_{/H}, \dot{a} \oplus \dot{b} = \overline{\dot{a} * \dot{b}}$$

Propriété 1

Si * est une loi commutative alors $\oplus$ est une loi de composition interne dans $E_{/H}$

Propriété 2

Si $(E,*)$ est un groupe abélien alors $(E_{/H}, \oplus)$ est aussi un groupe abélien appeler groupe quotient de E par H

Preuve

a. Dans un premier temps montrons que la loi $\oplus$ est associative :

$$\forall \dot{x}, \dot{y}, \dot{z} \in E_{/H}, \dot{x} \oplus \left(\dot{y} \oplus \dot{z}\right) = \dot{x} \oplus \overline{(y * z)} = \overline{x * (y * z)} = \overline{(x * y) * z} \Leftrightarrow \overline{(x * y)} \oplus \dot{z} = \left(\dot{x} \oplus \dot{y}\right) \oplus \dot{z}$$

car la loi * est associative

b. Elément neutre de la loi $\oplus$

Badalabougou en Commune 5
du District de BAMAKO
/UIE Mali
dg@uie-mali.com
+223 74 19 60 79

Si e est l'élément neutre pour $*$, $\dot{e}$ est l'élément neutre pour $\oplus$ car

$$\forall \dot{x} \in E_{/H}, \begin{cases} \dot{x} \oplus \dot{e} = \overline{x * e} = \dot{x} \\ \dot{e} \oplus \dot{x} = \overline{e * x} = \dot{x} \end{cases}$$

c. Elément symétrique

Soit $\dot{x} \in E_{/H}$ alors $\left(\dot{x}\right)^{-1} = \overline{x^{-1}}$

$$\dot{x} \oplus \overline{x^{-1}} = \overline{x * x^{-1}} = \dot{e}$$

d. Commutativité

$\oplus$ est commutative car la loi $*$ est commutative

De i),ii),iii) et iv) on déduit que $\left(E_{/H}, \oplus\right)$ est aussi un groupe abélien.

IV. Homomorphisme de groupes

Dans ce paragraphe on considère $(E,\circ)$ et $(F,*)$ deux groupes avec e_1 et e_2 leurs éléments neutres respectifs

Définition

Une application $f : E \to F$ est appelée homomorphisme de groupes de E dans F si : $\forall a,b \in E, f(a \circ b) = f(a) * f(b)$

- Si de plus l'application f est bijective alors on dit que f est un isomorphisme de groupes de E dans F
- Si f est un isomorphisme de groupes de E dans F alors on dit que E est isomorphe a F ou que E et F sont isomorphes
- Si $E = F$ alors on dit que f est un endomorphisme de E et si f est bijective alors on dit que f est un automorphisme de groupes de E

Exemple 1

Soit $(\mathbb{R},+)$ et $(\mathbb{R}_+^*,\times)$ deux groupes et $f : \mathbb{R} \to \mathbb{R}_+^*, x \mapsto \exp(x)$ une application

Montrer que f est un morphisme de groupes

Indication de solution

Soit $a,b \in \mathbb{R}$:

$$f(a+b)=\exp(a+b)=e^{a+b}=e^{a}\times e^{b}=\exp(a)\times\exp(b)=f(a)\times f(b)$$

$\Rightarrow$ est un morphisme de groupes

Exemple 2

Soient $(G,*)$ un groupe, et $a \in G$: On note f l'application de $(\mathbb{Z},+)\to(G,*)$ définie par $f(n)=a^{n}$ (l'image de f s'appelle le sous-groupe engendré par a)

f est un morphismes de groupe

Propriété

Soit $f : E \to F$ un morphisme de groupe. On a :

1. $f(e_E)=e_F$
2. Pour tout $x \in E$, $f(x^{-1})=[f(x)]^{-1}$
3. $\forall (x,y) \in E^2$, $f(x\circ y^{-1})=f(x)*[f(y)]^{-1}$
4. $\forall n \in \mathbb{Z}, \forall x \in E$, $f(x^{n})=[f(x)]^{n}$

Proposition

L'intersection de deux sous-groupes ou plus généralement d'une famille de sous-groupes, d'un groupe G est un sous-groupe de G .

Attention

La réunion de deux sous-groupes n'est en revanche pas un sous-groupe en général. Ce n'est même essentiellement "jamais" le cas, comme le montre l'énoncé suivant (exercice)

Si H *et* K deux sous-groupes d'un groupe G . Alors $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$

Exercice

Montrer que l'intersection de deux sous-groupes H *et* K d'un groupe G est un sous-groupe de G .

Définition

Soit S une partie d'un groupe G .

On appelle sous-groupe engendré par S , et on note $\langle S \rangle$,le plus petit sous-groupe contenant S .

C'est l'intersection de tous les sous-groupes de G qui contiennent S .

Exercice d'application 1

1. Resoudre dans $\mathbb{C}$ l'équation $z^6 = 1$

   Donner les solutions sous formes algébriques et trigonométriques

2. Montrer que $U_6 = \{z \in \mathbb{C}, z^6 = 1\}$ muni de la multiplication est un sous-groupe de $(\mathbb{C}^*, \times)$

Exercice d'application 2

1. On munit $\mathbb{R}$ de la loi de composition interne $*$ définie par :

$\forall x, y \in \mathbb{R}, x * y = xy + (x^2 - 1)(y^2 - 1)$

Montrer que $*$ est commutative, non associative, et que 1 est élément neutre.

2. On munit $\mathbb{R}_+^*$ de la loi de composition interne $*$ définie par :

$\forall x, y \in \mathbb{R}_+^*, x * y = \sqrt{x^2 + y^2}$

Montrer que $*$ est commutative, associative, et que 0 est l'élément neutre.

Montrer que aucun élément de $\mathbb{R}_+^*$ n'a de symétrique pour $*$.

3. On munit $\mathbb{R}$ de la loi de composition interne $*$ définie par :

$\forall x, y \in \mathbb{R}, x * y = \sqrt[3]{x^3 + y^3}$

Montrer que l'application $x \mapsto x^3$ est un isomorphisme de $(\mathbb{R}, *)$ vers $(\mathbb{R}, +)$. En déduire que $(\mathbb{R}, *)$ est un groupe commutatif

Indication de Solution

1. Montrer que $*$ est commutative : Sur $(\mathbb{R}, *), x * y = xy + (x^2 - 1)(y^2 - 1)$

On a : $x * y = xy + (x^2 - 1)(y^2 - 1) = yx + (y^2 - 1)(x^2 - 1) = y * x \Rightarrow$ la loi $*$ est commutative

Badalabougou en Commune 5
du District de BAMAKO
/UIE Mali
dg@uie-mali.com
+223 74 19 60 79

- Montrons ensuite que * non associative : pour cela il suffit de trouver x, y et $_z$ tels que : $(x*y)*z \neq x*(y*z)$

Prenons par exemple : $x=0, y=2$ et $z=3$

$$(x*y)*z=(0*2)*3=\left[0\times 2+\left(0^2-1\right)\left(2^2-1\right)\right]*3=[0-3]*3$$
$$=(-3)*3=\left[(-3)\times 3+(9-1)(9-1)\right]=-9+8^2=-9+64=55$$

Et $\begin{cases} x*(y*z)=0*(2*3)=0*\left[2\times 3+\left(2^2-1\right)\left(3^2-1\right)\right]=0*[6+3\times 8] \\ =0*30=0\times 30+\left(0^2-1\right)\left(30^2-1\right)=0-899=-899 \end{cases}$

On voit clairement que $(x*y)*z \neq (x*y)*z \Rightarrow *$ est non associative

- Montrer que* admet 1comme élément neutre

$$\forall x\in\mathbb{R}, 1*x=1\times x+\left(1^2-1\right)\left(x^2-1\right)=x$$

De plus, comme la loi est commutative la loi* étant commutative on a :

$$\forall x\in\mathbb{R}, x*1=1*x=x\times 1+\left(x^2-1\right)\left(1^2-1\right)=x$$

On a : $\forall x\in\mathbb{R}, \begin{cases} 1*x=1\times x+\left(1^2-1\right)\left(x^2-1\right)=x \\ x*1=x\times 1+\left(x^2-1\right)\left(1^2-1\right)=x \end{cases} \Rightarrow 1$ est l'élément neutre pour*

2. Montrer que* est commutative, associative, et que 0 est l'élément neutre

Pour $x, y\in\mathbb{R}_+^*, x*y=\sqrt{x^2+y^2}$

- On a : $x*y=\sqrt{x^2+y^2}=\sqrt{y^2+x^2}=y*x \Rightarrow *$ est commutative
- Soit $x, y, z\in\mathbb{R}_+^*$

$$(x*y)*z=\sqrt{x^2+y^2}*z=\sqrt{\left(\sqrt{x^2+y^2}\right)^2+z^2}=\sqrt{x^2+y^2+z^2}$$

Et $x*(y*z)=x*\sqrt{y^2+z^2}=\sqrt{x^2+\left(\sqrt{y^2+z^2}\right)^2}=\sqrt{x^2+y^2+z^2}$

Donc $(x*y)*z=x*(y*z)=\sqrt{x^2+y^2+z^2} \Rightarrow *$ est associative

Remarque

On aurait pu calculer aussi $(y*z)*x$

- Montrons maintenant que 0 est l'élément neutre pour cette loi*

Soit $x \in \mathbb{R}_+^*, 0 * x = x * 0$ car la loi* est commutative et

$0 * x = x * 0 = \sqrt{0^2 + x^2} = \sqrt{x^2} = |x| = x$ car $x \in \mathbb{R}_+^*$ d'où 0 est l'élément neutre pour*

- Pour le 1) montrons enfin que aucun élément de $\mathbb{R}_+^*$ n'a de symétrique pour*.

Pour cela raisonnons par absurde : Supposons que x admette un symétrique y ($x, y \in \mathbb{R}_+^*$), donc on a : $x * y = y * x \Leftrightarrow \sqrt{x^2 + y^2} = 0 \Leftrightarrow x^2 + y^2 = 0 \Leftrightarrow x = y = 0$ en contradiction avec le fait que $x, y \in \mathbb{R}_+^*$, donc $x * y = 0$ est impossible pour tout $x > 0$ et par conséquent x n'a pas de symétrique.

3. Montrons que l'application $x \mapsto x^3$ est un isomorphisme de $(\mathbb{R}, *)$ vers $(\mathbb{R}, +)$

Posons $g(x) = x^3, x \in \mathbb{R}$

On a : $\forall x \in \mathbb{R}, g'(x) = 3x^2 \geq 0 \Rightarrow g$ est une fonction croissante de $\mathbb{R}$ sur $\mathbb{R}$ donc g est une bijection de $\mathbb{R}$ sur $\mathbb{R}$. Il reste à montrer qu'il s'agit d'un morphisme.

$g(x * y) = (x * y)^3 = \left(\sqrt[3]{x^3 + y^3}\right)^3 = \left[\left(x^3 + y^3\right)^{\frac{1}{3}}\right]^3 = x^3 + y^3 = g(x) + g(y) \Rightarrow g$ est un isomorphisme de $(\mathbb{R}, *)$ vers $(\mathbb{R}, +)$

g^{-1} est un isomorphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}, *)$, donc un morphisme, $(\mathbb{R}, +)$ est un groupe commutatif et l'image d'un groupe commutatif par un morphisme de groupe est un groupe. $(\mathbb{R}, *)$ est un groupe.

Table de Cayley et isomorphisme de groupes

1. Définitions

Soit un ensemble $E = \{x_1, x_2, \cdots, x_n\}$ muni d'une opération*. On appelle table de Cayley, le tableau carré de n lignes et n colonnes obtenues en inscrivant à la i^{ieme} ligne et à la j^{ieme} colonne l'élément $x_i * x_j$.

$*$	x_1	x_2	$\cdots$	x_j	$\cdots$	x_n
x_1						
x_2						
$\cdots$						
x_i				$x_i * x_j$		
$\cdots$						
x_n						

Exemple 1

Ecrire la table de Cayley du groupe additif $\mathbb{Z}/4\mathbb{Z}$

Elément de réponse

Les éléments de cet ensemble $\mathbb{Z}/4\mathbb{Z}$ sont des classes $\mathbb{Z}/4\mathbb{Z} = \{\dot{0},\dot{1},\dot{2},\dot{3}\}$

$*$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Exemple 2

Soit $E = \{1,2,3,4\}$ mini de l'opération $*$ définie ci-dessous. Compléter les tables de Cayley. Que constatez-vous ?

$a * b = ppcm(a,b)$

*	1	2	3	4
1				
2				
3				
4				

Exemple 3

Soit $E=\{1,2,3,4\}$ mini de l'opération $*$ définie ci-dessous. Compléter les tables de Cayley. Que constatez-vous ?

$a*b=p\gcd(a,b)$

*	1	2	3	4
1				
2				
3				
4				

Exercice 1

Ecrire la table de Cayley du groupe additif $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ (donc constitué de l'ensemble des couples (a,b) avec a et b dans $\mathbb{Z}/2\mathbb{Z}$, muni de la loi de groupe $(a,b)+(c,d)=(a+b,c+d)$ On listera les éléments dans l'ordre lexicographique.

Elément de réponse

*	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$				
$(0,1)$				
$(1,0)$				
$(1,1)$				

Exercice 2

On munit l'ensemble $E=\{a,b,c.d\}$ d'une loi de composition interne, dont la table de Cayley est :

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

1. Cette loi possède-t-elle un élément neutre ? Lequel ? Chaque élément, admet-il un symétrique ? Préciser le symétrique de c.
2. Cette loi est-elle commutative ?
3. Prouver que $*$ est associative.
4. $(E,*)$ est-il un groupe ?

Exercice

Soit $*$ une loi définie sur IR par : $\forall x,y\in\mathbb{R}, x*y=xy+\left(x^2-1\right)\left(y^2-1\right)$

2. Vérifier que $*$ est commutative, non associative et admet un élément neutre.
3. Résoudre les équations suivantes : $2*y=5,\ x*x=1$

Noyau et image d'un morphisme

Soit $f:G\to G'$ un morphisme de groupes. Nous définissons deux sous-ensembles importants qui vont être des sous-groupes.

1. Noyau

On note e' l'élément neutre de G'. Le noyau de f l'ensemble

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

C'est donc un sous-ensemble de G. En termes d'image réciproque nous avons par définition $Kerf=f^{-1}(\{e'\})$.

Badalabougou en Commune 5
du District de BAMAKO
/UIE Mali
dg@uie-mali.com
+223 74 19 60 79

Attention, la notation f^{-1} ici désigne l'image réciproque, et ne signifie pas que f est bijective)

Le noyau est donc l'ensemble des éléments de G qui s'envoient par f sur l'élément neutre de G'.

Remarque

Le mot noyau se traduit par kernel en anglais et par kern en allemand.

2. Image

L'image de f l'ensemble $\text{Im } f = f(G) = \{f(x), x \in G\}$,C'est donc un sous-ensemble de G' et en termes d'image directe nous avons $\text{Im } f = f(G)$. Ce sont les éléments de G' qui ont (au moins) un antécédent par f .

Proposition

Soit $f : G \to G'$ un morphisme de groupes.

1. $Kerf$ est un sous-groupe de G .
2. $\text{Im } f$ est un sous-groupe de G'.
3. f est injective si et seulement si $Kerf = \{e\}$.
4. f est surjective si et seulement si $\text{Im } f = G'$.

Exemple

Soit un entier $k \geq 2$. Soit

$$f : \begin{cases} (\mathbb{Z}, +) \to (\mathbb{Z}, +) \\ n \mapsto f(n) = kn \end{cases}$$

1. Montrer f est un morphisme de groupes
2. Déterminer le noyau de f , f est-elle injective ?
3. *Déterminer l'image de f , f est-elle surjective ?*

Théorème

Soit f une application linéaire de E dans F avec dimension de E est finie, on a : $\dim E = \dim(\ker f) + \dim(f)$

Premier exemple de groupe

Groupes monogènes

Définition

Un groupe G est dit monogène s'il existe x tel que $G = \langle x \rangle$

Un groupe G est dit cyclique s'il est monogène et fini. Selon les notations :

$\langle x \rangle = \{x^k, k \in \mathbb{Z}\}$

Remarque

L'image du morphisme f n'est autre que l'image de l'application f .

Lemme

Soient G, G' deux groupes et soit $f : G \to G'$ un morphisme de groupes.

Si G est monogène, alors $\mathrm{Im}\, f$ est monogène.

En effet :

G Monogène $\Leftrightarrow \exists x \in G, G = \{x^k, k \in \mathbb{Z}\}$. Donc $f(G) = \{f(x)^k, k \in \mathbb{Z}\} = \langle f(x) \rangle$

Anneaux

On appelle anneau tout ensemble A muni de deux lois $+ et \times$ internes telles que :

i. $(A,+)$ est un groupe abélien.

ii. La multiplication est :

— Associative, i.e. : $\forall x, y, z \in A, (xy)z = x(yz)$

— Distributive par rapport à l'addition i.e : $\begin{cases} \forall x, y, z \in A, \text{on a:} \\ x(y+z) = xy + xz \\ (x+y)z = xz + yz \end{cases}$

- L'anneau A est dit unitaire si la multiplication admet un élément neutre généralement noter 1

- L'anneau A est dit commutatif si la multiplication est commutative i.e si :

  $\forall x, y \in A, on\ a: xy = yx$

Exemples

1) $\mathbb{Z}$ est un anneau commutatif et unitaire.
2) Soit $n \geq 1$un entier ; l'anneau $\mathbb{Z}/n\mathbb{Z}$ des entiers modulo $_n$ est un anneau commutatif et unitaire
3) L'anneau A est dit trivial si $1 = 0$i.e l'anneau contient un seul élément 0 : $A = \{0\}$

Il est non trivial si $1 \neq 0$

Corps

On corps K un anneau non trivial dont tout élément non nul est inversible i.e :

$\forall a \in \mathrm{K}$ avec $a \neq 0, \exists b \in \mathrm{K}$ vérifiant $ab = 1$

Exemple

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps

Autres exemples d'anneaux

- Soit A un anneau commutatif unitaire.

$A[X]$=ensemble des polynômes à une interminée X a coefficients dans l'anneau A est un anneau commutatif unitaire

- $A[[X]]$=ensemble des séries formelles à une interminée X a coefficients dans l'anneau A est un anneau commutatif unitaire

Exercice 1

On définit sur $\mathbb{Z}^2$ les deux lois $\oplus, \odot$ comme suit :

$\forall (x,y),(a,b) \in \mathbb{Z}^2, (x,y) \oplus (a,b) = (x+a, xb+ya)$

$\forall (x,y),(a,b) \in \mathbb{Z}^2, (x,y) \odot (a,b) = (xa, y+b)$

Montrer que $(\mathbb{Z}^2, \oplus, \odot)$ est anneau commutatif

Exercice 2

Soit $f : \mathbb{R}^3 \to \mathbb{R}^2$ définie par $f(x,y,z) = (x+y+z, -x+2y+2z)$

Badalabougou en Commune 5
du District de BAMAKO
/UIE Mali
dg@uie-mali.com
+223 74 19 60 79

On appelle $\beta=(e_1,e_2,e_3)$ la base canonique de $\mathbb{R}^3$ et $\beta_1=(f_1,f_2)$ la base canonique de $\mathbb{R}^2$.

1. Montrer que f est une application linéaire
2. Donner une base et la dimension de ker(f) et une base et la dimension de $Im(f)$.

Sous anneau

Soit A un anneau commutatif unitaire

Une partie B de A est un sous anneau de A si $(B,+)$ est un sous-groupe de A tel que : $\forall a,b\in B, ab\in B$ et si en outre $1_A\in B$

Morphisme d'anneau

Définition

Soient $A et B$ deux anneaux

On appelle morphisme de A dans B toute application $\varphi: A\to B$ vérifiant :

i. $\varphi(1_A)=1_B$

ii. $\forall a,b\in A, \varphi(a+b)=\varphi(a)+\varphi(b)$

iii. $\forall a,b\in A, \varphi(ab)=\varphi(a)\varphi(b)$

Un morphisme d'anneau bijectif s'appelle **un isomorphisme**

Si $\varphi: A\to B$ est un morphisme d'anneaux, on pose :

$\ker\varphi=\{a\in A/\varphi(a)=0\}=\varphi^{-1}(0)$ Noyau de φ

$\mathrm{Im}\,\varphi=\{\varphi(a);a\in A\}=\varphi(A)$ Image de φ

Ideal d'un anneau

Soit A un anneau commutatif unitaire

On appelle idéal de A tout sous-groupe additif I de A tel que :

$\forall a\in I, \forall x\in A, ax\in I$.

En d'autres termes $I.A\subset I$

C.N.S : pour que $I\subset A$ non vide soit un idéal de A :

i. $\forall a,b\in I, a+b\in I$

ii. $\forall a \in I, \forall x \in A, ax \in I$

Si $\varphi : A \to B$ est un morphisme d'anneaux alors :

— $\ker \varphi$ est un idéal de A

— $\mathrm{Im}\,\varphi$ n'est pas nécessairement un idéal de B sauf si φ est surjective

Ideal de type fini

Soit A un anneau commutatif unitaire. Soit F une partie non vide de A

On note : $\langle F \rangle = \bigcap_{\substack{I \text{ ideal de } A \\ \text{avec } I \supseteq F}} I$ =le plus petit idéal de A contenant F

$\langle F \rangle$ est l'idéal de A engendrer par F

Supposons que F soit finie : $F = \{x_1, \ldots, x_r\}, x_i \in A \ \ \forall i$

$\langle F \rangle = \langle x_1, \ldots, x_r \rangle = (x_1, \ldots, x_r)$ Qui est l'ensemble des combinaisons linéaires des éléments $x_1, \ldots, x_r$.

Un élément général $\langle x_1, \ldots, x_r \rangle$ s'écrit : $x = \sum_{i=1}^{r} a_i x_i, a_i \in A$

Définition

Un idéal I *de* A est dit de type fini s'il existe $x_1, \ldots, x_r \in A$ tels que :

$I = \langle x_1, \ldots, x_r \rangle$

L'Ideal est dit principal s'il existe $x \in I, I = \langle x \rangle = \{ax, a \in A\} = Ax$

Congruence modulo un idéal

Anneau quotient

Soit A un anneau commutatif unitaire et I un idéal I *de* A

On définit la congruence modulo I entre les éléments de A comme suit :

$\forall a, b \in A, a \equiv b \pmod{I} \Leftrightarrow b - a \in I$

Ceci est une relation d'équivalence

Badalabougou en Commune 5
du District de BAMAKO
/UIE Mali
dg@uie-mali.com
+223 74 19 60 79

La classe d'un élément a par cette relation d'équivalence est :

$$\begin{aligned} cl(a) &= \{b \in A; b \equiv a \pmod{I}\} \\ &= \{b \in A; \exists c \in I, b = a + c\} \\ &= \{b \in A; b \in a + I\} = a + I \end{aligned}$$

Notation

$$cl(a) = \bar{a} = a + I, \forall a \in A$$

L'ensemble quotient de A par $\equiv$ est l'ensemble des classes d'équivalence et on note A/I

Lois de A/I