

6

STRUCTURES

I. APPLICATIONS

INJECTIVITÉ, SURJECTIVITÉ, BIJECTIVITÉ

Soit E et F deux ensembles et f une application de E dans F .

Définition 1

- f est une *surjection* si tout élément de F admet au moins un antécédent.
- f est une *injection* si tout élément de F admet au plus un antécédent
- f est une *bijection* si tout élément de F admet un et un seul un antécédent

Méthode

Soit $f : E \rightarrow F$

- Surjective : soit $y \in F$, on explicite les conditions qui traduisent que $y \in F \dots$ on a trouvé/construit $x \in E$ tel que $y = f(x)$.
- Injectivité : on prouve que si deux éléments x et x' ont la même image alors ce sont les mêmes : soit $x, x' \in E$ tels que $f(x) = f(x') \dots$ on a $x = x'$.
- f est bijective : la plupart du temps, on montre séparément l'injectivité et la surjectivité.

Définition 2 (Application réciproque)

Soit f est une application bijective de E dans F . Il existe une unique application g de F dans E telle que $y = f(x)$ équivaut à $x = g(y)$ (pour $x \in E$ et $y \in F$). Cette application est appelée *application réciproque* de f (ou simplement *réciproque* ou *inverse*), elle est notée f^{-1} .

Proposition 1 (Composition)

Soient $f : E \rightarrow F$ et $g : F \rightarrow G$ deux applications.

- Si f et g sont surjectives alors $g \circ f$ est surjective.
- Si f et g sont injectives alors $g \circ f$ est injective.
- Si f et g sont bijectives alors $g \circ f$ est bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Exercice 1

Montrer ces propriétés.



Inverses à droite ou à gauche

$f : E \rightarrow F$ est inversible lorsqu'il existe une fonction $g : F \rightarrow E$ telle que $g \circ f = id_E$ (inverse à gauche) et $f \circ g = id_F$ (inverse à droite). L'existence d'une seule de ces conditions ne permet pas d'affirmer que f est bijective. En revanche, si on sait par ailleurs que f est bijective, il suffit de trouver g telle que $f \circ g = id$ ou $g \circ f = id$.

IMAGES DIRECTES ET RÉCIPROQUES

Méthode (Rappels sur les ensembles)

- Pour montrer qu'un ensemble A est inclus dans un ensemble B , la démonstration se fait toujours de la même façon :

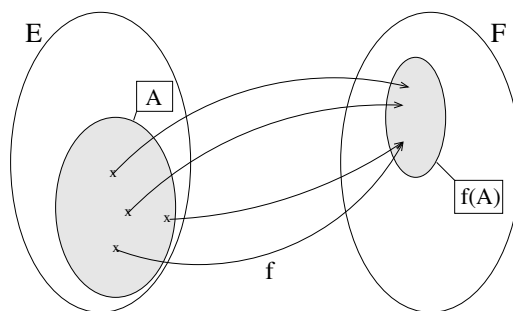
Soit $x \in A$, on traduit les conditions sur $x \dots$ alors $x \in B$.

- Pour montrer que deux ensembles A et B sont égaux, on montre les deux inclusions $A \subset B$ et $B \subset A$.
- Pour prouver qu'un élément est dans l'intersection $A \cap B$, on montre qu'il est à la fois dans A et dans B .

Définition 3 (Image directe)

Soit $f : E \rightarrow F$ une application et $A \subset E$. On note $f(A)$ le sous-ensemble de F appelé *image directe* de A par f , défini par

$$f(A) = \{y \in F \mid \exists x \in A, y = f(x)\} = \{f(x) \mid x \in A\}.$$

**Méthode (Image directe)**

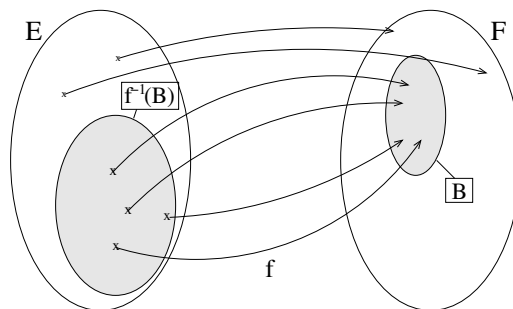
- Lorsqu'on doit montrer qu'un élément y est dans $f(A)$, on construit $x \in A$ tel que $y = f(x)$.
- Lorsqu'on a besoin de $y \in f(A)$, on écrit : soit $y \in f(A)$, il existe $x \in A$ tel que $y = f(x)$.

Définition 4 (Image réciproque)

Soit $f : E \rightarrow F$ une application et $B \subset F$. On note $f^{-1}(B)$ le sous-ensemble de E appelé image réciproque de B par f , défini par

$$f^{-1}(B) = \{x \in E \mid f(x) \in B\}.$$

Il faut comprendre ce que désigne cet ensemble en « lisant à l'envers l'application » : $f^{-1}(B)$ désigne l'ensemble des éléments de l'ensemble de départ dont l'image tombe dans B .

**Méthode (Image réciproque)**

- Pour prouver qu'un élément x est dans $f^{-1}(B)$: il suffit de montrer que $f(x) \in B$.
- Lorsqu'on utilise un élément x de $f^{-1}(B)$, on écrit $f(x) \in B$ pour poursuivre la démonstration.

**Deux notations**

Il ne faut pas confondre

- l'application réciproque f^{-1} qui n'existe que lorsque f est bijective et elle agit sur les éléments de l'ensemble d'arrivée,
- l'application « image réciproque » qui agit sur les sous-ensembles de l'ensemble d'arrivée et qui existe toujours.

Lorsque f est bijective, ces deux notations sont liées car on a $f^{-1}(\{y\}) = \{f^{-1}(y)\}$.

Propriété 2 (Images directes et réciproques)

Soit $f : E \rightarrow F$, A et B des sous-ensembles de E ou F :

- $A \subset B$ implique $f(A) \subset f(B)$.
- $f(A \cap B) \subset f(A) \cap f(B)$ avec égalité lorsque f est injective.
- $f(A \cup B) = f(A) \cup f(B)$
- $A \subset B$ implique $f^{-1}(A) \subset f^{-1}(B)$.
- $f(f^{-1}(B)) \subset B$ avec égalité si f est surjective.
- $B \subset f^{-1}(f(B))$ avec égalité si f est injective.
- $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.
- $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.
- si $f : E \rightarrow F$ et $g : F \rightarrow G$:
 - si $A \subset E$ alors $g(f(A)) = (g \circ f)(A)$
 - si $B \subset G$ alors $f^{-1}(g^{-1}(B)) = (g \circ f)^{-1}(B)$

Exercice 2

Montrer ces propriétés



RELATION D'ÉQUIVALENCE ET ENSEMBLE QUOTIENT

Définition 5 (Relation d'équivalence, ensemble quotient)

Soit E un ensemble. On dit qu'une relation entre deux éléments $x \mathcal{R} y$ est une relation d'équivalence lorsqu'elle est

- *réflexive* : pour tout $x \in E$, $x \mathcal{R} x$,
- *symétrique* : pour tout $x, y \in E$, si $x \mathcal{R} y$ alors $y \mathcal{R} x$,
- *transitive* : si $x \mathcal{R} y$ et $y \mathcal{R} z$ alors $x \mathcal{R} z$.

On peut alors créer une partie de l'ensemble en considérant les sous-ensembles suivants, appelés classes d'équivalence

$$\text{si } x \in E, \bar{x} = \{y \in E, x \mathcal{R} y\}.$$

Si $x, y \in E$, on a soit $\bar{x} = \bar{y}$, soit $\bar{x} \cap \bar{y} = \emptyset$. On note alors E/\mathcal{R} l'ensemble constitué par les classes d'équivalences créées par cette relation. Si $z \in E/\mathcal{R}$ est une classe d'équivalence, on appelle représentant de cette classe tout élément $x \in E$ tel que $\bar{x} = z$. On définit alors une surjection (appelée surjection canonique) :

$$p: \begin{cases} E & \rightarrow & E/\mathcal{R} \\ x & \mapsto & \bar{x} \end{cases}$$

II. GROUPES

GROUPES ET SOUS-GROUPES

Définition 6 (Groupe)

Ensemble G muni d'une loi de composition interne $*$:

- (associative) $a * (b * c) = (a * b) * c$,
- (élément neutre) $\exists e \in G, \forall g \in G, g * e = e * g = g$,
- (symétrique) $\forall g \in G, \exists g' \in G$ tel que $g * g' = g' * g = e$ (g' noté g^{-1})

On a

- G est commutatif (ou abélien) lorsque $g * g' = g' * g$ pour tout $g, g' \in G$.
- G est fini lorsqu'il a un nombre fini d'éléments. On appelle alors *ordre* de G son nombre d'éléments.

Définition 7 (Sous-groupes)

$H \subset G$ est un sous-groupe de G lorsque H est non vide, que la loi est stable dans H et que $(H, *)$ a une structure de groupe. En pratique :

- H est non vide
- pour tout $g, h \in H$, $g * h \in H$ et $g^{-1} \in H$ (ou simplement $g * h^{-1} \in H$).

L'essentiel (groupes et sous-groupes)

- calculs : unicité de l'élément neutre, de l'inverse
- si $a \in G$, l'application « de translation à gauche » $g \mapsto a * g$ (ou « à droite » $g \mapsto g * a$) est une bijection de G sur G (lorsque g décrit G entièrement, les éléments $a * g$ redécrivent - d'une autre manière - tous les éléments de G (une et une seule fois).
- Opérations sur les groupes/sous-groupes (et construction) : structure de groupe sur un produit fini de groupes, intersection de sous-groupes de G , sous-groupe engendré par une partie de G .
- G est un sous-groupe de $(\mathbb{Z}, +)$ si et seulement si il existe $n \in \mathbb{Z}$ tel que $G = n\mathbb{Z}$.

MORPHISMES DE GROUPES

L'essentiel (Morphismes)

- définition d'un morphisme entre les groupes $(G, *)$ et $(G', *)$, isomorphismes, automorphismes.
- propriétés : $f(e_G) = e_{G'}$ et $f(g^{-1}) = (f(g))^{-1}$.
- image et noyau de $f: G \rightarrow G'$ un morphisme de groupes. $\text{Im } f$ et $\ker f$ sont des sous-groupes respectivement de G' et G .

Exercice 3

Pour $\theta \in \mathbb{R}$, on note $A(\theta) = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$ et $B(\theta) = \begin{pmatrix} \text{ch } \theta & \text{sh } \theta \\ \text{sh } \theta & \text{ch } \theta \end{pmatrix}$. On définit $G = \{A(\theta), \theta \in \mathbb{R}\}$ et $H = \{B(\theta), \theta \in \mathbb{R}\}$.

1. Vérifier que G et H sont deux sous-groupes de $GL_2(\mathbb{R})$.
2. Résoudre l'équation $X^2 = I_2$ dans G et H . Les deux sous-groupes sont-ils isomorphes?

Exercice 4

Soient G et H des groupes finis.



1. Soit f un morphisme de G dans H . Montrer que la relation $x\mathcal{R}y$ lorsque $f(x) = f(y)$ définit une relation d'équivalence sur G . Combien y-a-t-il de classes d'équivalences? On pourra utiliser l'application suivante, après avoir justifié qu'elle existe :

$$\tilde{f} : \bar{x} \in G/\mathcal{R} \mapsto f(x) \in \text{Im } f.$$

2. En déduire $|G| = |\text{Im } f| \cdot |\ker f|$.
3. Soit f un morphisme de groupes de G dans lui-même. Montrer que $\ker f = \ker f^2 \Leftrightarrow \text{Im } f = \text{Im } f^2$.

III. AUTRES STRUCTURES

ANNEAUX (2 LOIS)

Définition 8 (Anneau)

ensemble A muni de deux lois $+$ et \times tel que

1. $(A, +)$ groupe commutatif (élément neutre noté 0).
2. la loi (produit) \times est interne et associative.
3. le produit est distributif à droite et à gauche par rapport à l'addition.
4. il existe un élément neutre, noté 1, pour la multiplication.

Définition 9 (Vocabulaire)

soit $(A, +, \times)$ un anneau

- A est *commutatif* si la loi \times est commutative.
- $a \in A$ est un *diviseur de 0* s'il est non nul et s'il existe $b \neq 0$ tel que $a \times b = 0$.
- A est *intègre* s'il n'a aucun diviseur de 0. Cela revient à dire que : pour tout $a, b \in A$, $a \times b = 0$ si et seulement si $a = 0$ ou $b = 0$.

Définition 10 (Sous-anneau)

$B \subset A$ est un sous-anneau de A s'il contient 1, est stable pour les deux lois et B muni des lois induites $(+, \times)$ possède une structure d'anneau. On montre que B est un sous-anneau de A en montrant :

- $B \subset A$ et $1_A \in B$,
- pour tout $a, b \in B$, $a - b$ et $a \times b \in B$.

Exemple

- $(\mathbb{Z}, +, \times)$ et $(\mathbb{R}[X], +, \times)$ sont des anneaux commutatifs et intègres.
- $(\mathcal{C}^0(I, \mathbb{R}), +, \times)$ est un anneau commutatif mais il n'est pas intègre.
- Si E est un espace vectoriel, $(\mathcal{L}(E), +, \circ)$ est un anneau non commutatif, non intègre.

Définition 11 (Morphisme d'anneaux)

Soit A et A' deux anneaux, $f : A \rightarrow A'$ est un morphisme d'anneaux si

- $f(1_A) = 1_{A'}$
- $\forall (a_1, a_2) \in A \times A$, $f(a_1 + a_2) = f(a_1) + f(a_2)$ et $f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2)$

Propriété 3 (Règles de calcul)

si $a, b \in A$ commutent alors

- $(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k},$
- $a^n - b^n = (a - b) \left(\sum_{k=0}^{n-1} a^k b^{n-1-k} \right).$

CORPS (2 LOIS)

Définition 12 (Corps)

On dit que $(K, +, \times)$ est un corps si

1. $(K, +, \cdot)$ est un anneau commutatif. On note 0 l'élément neutre pour $+$ (appelé élément nul) et 1 l'élément neutre pour \times
2. tout $x \in K$ non nul est inversible : il existe $y \in K$ tel que $x \times y = y \times x = 1$ (on note alors $y = x^{-1}$).

on définit comme précédemment les notions de sous-corps et de morphismes de corps.

**Exemple**

- \mathbb{Q}, \mathbb{R} et \mathbb{C} sont des corps. Dans cet ordre, ils sont des sous-corps du corps suivant.
- Dans un corps, tous les éléments non nuls sont simplifiables, il n'y a donc pas de diviseur de zéro. Pour qu'un anneau ait une chance d'être un corps, il faut donc qu'il soit intègre (mais ce n'est pas suffisant).

ESPACES VECTORIELS (2 LOIS)**Définition 13** (*Espace vectoriel*)

Soit $(\mathbb{K}, +, \cdot)$ un corps commutatif. On dit que $(E, +, \cdot)$ est un espace vectoriel sur \mathbb{K} si

1. la loi $+$ est une loi interne et $(E, +)$ est un groupe commutatif.

2. la loi \cdot est une loi externe : $\begin{cases} \mathbb{K} \times E & \rightarrow E \\ (\lambda, x) & \mapsto \lambda \cdot x \end{cases}$ qui vérifie

$$\rightarrow (\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$$

$$\rightarrow \lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$$

$$\rightarrow \lambda \cdot (\mu \cdot x) = (\lambda \cdot \mu) \cdot x$$

$$\rightarrow 1 \cdot x = x$$

Les éléments d'un espace vectoriel sont appelés les *vecteurs*, les éléments du corps de base \mathbb{K} sont appelés *scalaires*. Le vecteur $\lambda \cdot x$ est noté simplement λx .

Proposition 4 (*Règles de calcul*)

Soit E un \mathbb{K} -espace vectoriel, on a $(x, y \in E \text{ et } \lambda \in \mathbb{K})$

1. $0_{\mathbb{K}} \cdot x = 0_E$.
2. $\lambda \cdot 0_E = 0_E$.
3. $-(\lambda x) = (-\lambda)x = \lambda(-x)$
4. $\lambda(x - y) = \lambda x - \lambda y$

ALGÈBRE (3 LOIS)**Définition 14** (*Algèbre*)

Soit \mathbb{K} un corps. On dit que $(A, +, \star, \cdot)$ est une \mathbb{K} -algèbre si

1. $(A, +, \cdot)$ est un \mathbb{K} -espace vectoriel.
2. $(A, +, \star)$ est un anneau.
3. $(\lambda \cdot x) \star y = x \star (\lambda \cdot y) = \lambda \cdot (x \star y)$ pour $\lambda \in \mathbb{K}$ et $x, y \in A$.

En pratique, il y a une loi interne « additive » et deux lois « multiplicatives », l'une correspond à la multiplication par les constantes, l'autre à une multiplication interne. On peut également voir une algèbre comme un espace vectoriel muni d'une multiplication interne (avec des propriétés entre les deux multiplications).

Exemple

- $\mathcal{F}(A, \mathbb{K})$ (ensemble des applications d'un ensemble A dans $\mathbb{K} = \mathbb{R}$ ou \mathbb{C}) est une algèbre.
- $\mathcal{C}^0(I, \mathbb{K}), \mathcal{C}^k(I, \mathbb{K})$ ou $\mathcal{C}^\infty(I, \mathbb{K})$ sont des algèbres.
- $\mathbb{R}[X]$ et $\mathbb{C}[X]$ sont des algèbres.
- $\mathbb{R}^{\mathbb{N}}$ ou $\mathbb{C}^{\mathbb{N}}$ les ensembles des suites à valeurs dans \mathbb{R} ou \mathbb{C} sont des algèbres.
- $(\mathcal{L}(E), +, \circ, \cdot)$ l'ensemble des endomorphismes d'un espace vectoriel E est une algèbre.
- $M_n(\mathbb{K})$ l'ensemble des matrices carrées de taille n est une algèbre.

IV. EXERCICES**Exercice 5**

Soit $G = \{x + \sqrt{2}y, x \in \mathbb{N}^*, y \in \mathbb{Z} \text{ et } x^2 - 2y^2 = 1\}$.

1. Vérifier que $G \subset \mathbb{R}_+^*$.
2. Montrer que G est un sous-groupe de (\mathbb{R}_+^*, \times) . Quel est le symétrique de $x + y\sqrt{2}$?
3. Soit $x + y\sqrt{2} \in G$ avec $y \in \mathbb{N}^*$. Vérifier que $x - y\sqrt{2} \in]0, 1[$.
4. Montrer qu'il existe un plus petit élément g_0 dans $G \cap]1, +\infty[$ et le déterminer.
5. Montrer que $G = \{g_0^n, n \in \mathbb{Z}\}$. Qu'a-t-on prouvé?