

MPSI– Chapitre n°1

Raisonnement et vocabulaire ensembliste

Ce chapitre rassemble le vocabulaire, les notations et les modes de raisonnement indispensables à la rédaction d'une démonstration en MPSI. Le programme insiste sur la maîtrise progressive de ces notions : l'objectif n'est pas de faire une théorie formelle de la logique ou des ensembles, mais de savoir les utiliser avec précision dans tous les autres chapitres.

Compétences visées. À l'issue de ce chapitre, on doit savoir formuler et nier un énoncé quantifié, distinguer implication, réciproque et contraposée, choisir une méthode de démonstration, conduire une récurrence, manipuler les opérations ensemblistes, reconnaître une relation d'équivalence ou d'ordre, et étudier une application (image directe ou réciproque, injectivité, surjectivité, bijectivité, composition et réciproque).

1 - Rudiments de logique

Définition : Proposition et prédicat

Une **proposition mathématique** est un énoncé auquel on peut attribuer une valeur de vérité : *vrai* ou *faux*.

Un **prédicat** est un énoncé dépendant d'une ou plusieurs variables. Il ne devient une proposition qu'après avoir fixé les variables ou les avoir quantifiées.

Exemple : « 2 est pair » est une proposition vraie. « n est pair » est un prédicat portant sur l'entier n .

Définition : Connecteurs logiques

Soient P et Q deux propositions.

$P \wedge Q$ signifie « P et Q » ; cette proposition est vraie lorsque P et Q sont toutes deux vraies.

$P \vee Q$ signifie « P ou Q » au sens inclusif ; elle est vraie lorsqu'au moins l'une des deux propositions est vraie.

$\neg P$ est la négation de P .

$P \Rightarrow Q$ signifie « si P , alors Q ». Elle est fausse uniquement lorsque P est vraie et Q est fausse.

$P \Leftrightarrow Q$ signifie que P et Q ont la même valeur de vérité.

P	Q	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$	$P \Leftrightarrow Q$
V	V	V	V	V	V
V	F	F	V	F	F
F	V	F	V	V	F
F	F	F	F	V	V

Définition : Réciproque et contraposée

La **réciproque** de $P \Rightarrow Q$ est $Q \Rightarrow P$.

La **contraposée** de $P \Rightarrow Q$ est $\neg Q \Rightarrow \neg P$.

Une implication est toujours équivalente à sa contraposée, mais pas en général à sa réciproque.

Définition : Condition nécessaire et condition suffisante

Lorsque $P \Rightarrow Q$, la proposition P est une **condition suffisante** pour Q , tandis que Q est une **condition nécessaire** pour P .

Lorsque $P \Leftrightarrow Q$, chacune des deux propositions est une condition nécessaire et suffisante pour l'autre.

Propriété : Règles fondamentales de logique

Pour toutes propositions P, Q, R , on a :

$$\begin{aligned}\neg(\neg P) &\Leftrightarrow P, \\ \neg(P \vee Q) &\Leftrightarrow (\neg P) \wedge (\neg Q), \quad \neg(P \wedge Q) \Leftrightarrow (\neg P) \vee (\neg Q), \\ P \Rightarrow Q &\Leftrightarrow (\neg P) \vee Q, \quad \neg(P \Rightarrow Q) \Leftrightarrow P \wedge (\neg Q), \\ P \Rightarrow Q &\Leftrightarrow (\neg Q) \Rightarrow (\neg P), \\ [(P \Rightarrow Q) \wedge (Q \Rightarrow R)] &\Rightarrow (P \Rightarrow R).\end{aligned}$$

Démonstration : Démonstration exigible – règles de logique

Les lois de De Morgan, la formule de l'implication et la négation d'une implication se vérifient par table de vérité. Par exemple :

P	Q	$P \Rightarrow Q$	$\neg(P \Rightarrow Q)$	$P \wedge \neg Q$
V	V	V	F	F
V	F	F	V	V
F	V	V	F	F
F	F	V	F	F

Les deux dernières colonnes sont identiques, donc $\neg(P \Rightarrow Q) \Leftrightarrow P \wedge \neg Q$.

Pour la contraposition :

$$P \Rightarrow Q \Leftrightarrow \neg P \vee Q \Leftrightarrow \neg(\neg Q) \vee \neg P \Leftrightarrow (\neg Q) \Rightarrow (\neg P).$$

Enfin, si $P \Rightarrow Q$ et $Q \Rightarrow R$ sont vraies, alors lorsque P est vraie, Q l'est, puis R l'est ; ainsi $P \Rightarrow R$.

Méthode : Bien lire une implication

Pour réfuter $P \Rightarrow Q$, il faut exhiber un cas où P est vraie et Q fausse. Montrer que P est fausse ne prouve rien sur la vérité de Q .

2 - Quantificateurs

Définition : Quantificateur universel

Pour un prédicat $P(x)$ défini sur un ensemble E ,

$\forall x \in E, P(x)$ signifie que tous les éléments de E vérifient P .

Définition : Quantificateur existentiel et unicité

$\exists x \in E, P(x)$ signifie qu'il existe au moins un élément de E vérifiant P .

$\exists! x \in E, P(x)$ signifie qu'il existe un unique élément de E vérifiant P .

Propriété : Négation d'une proposition quantifiée

$$\neg(\forall x \in E, P(x)) \Leftrightarrow \exists x \in E, \neg P(x),$$

$$\neg(\exists x \in E, P(x)) \Leftrightarrow \forall x \in E, \neg P(x).$$

Exemple : La négation de « tout réel est positif » est « il existe un réel qui n'est pas positif ».

Propriété : Cas de l'ensemble vide

Pour tout prédicat P , la proposition $\forall x \in \emptyset, P(x)$ est vraie, tandis que $\exists x \in \emptyset, P(x)$ est fausse.

Méthode : Ordre des quantificateurs

Deux quantificateurs de même nature peuvent être permutés. En revanche, l'ordre de $\forall$ et $\exists$ est essentiel. Par exemple,

$$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y > x$$

est vraie, tandis que

$$\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, y > x$$

est fausse.

Méthode :

Méthode – nier une proposition à plusieurs quantificateurs On part du symbole $\neg$, puis on traverse les quantificateurs de gauche à droite en les échangeant : $\forall \leftrightarrow \exists$. On termine en niant le prédicat.

Ainsi,

$$\neg(\forall x \in E, \exists y \in F, P(x, y)) \Leftrightarrow \exists x \in E, \forall y \in F, \neg P(x, y).$$

3 - Méthodes de démonstration

Démontrer une implication directement

Pour démontrer $P \Rightarrow Q$, on suppose P vraie et l'on déduit Q par une chaîne d'implications justifiées.

Raisonner par contraposition

Pour démontrer $P \Rightarrow Q$, on peut démontrer l'énoncé équivalent $\neg Q \Rightarrow \neg P$.

Cette méthode est particulièrement efficace lorsque la négation de Q fournit une information exploitable.

Raisonner par l'absurde

Pour démontrer une proposition P , on suppose $\neg P$ et l'on en déduit une contradiction : une proposition connue fausse, ou simultanément Q et $\neg Q$. On conclut que $\neg P$ est impossible, donc P est vraie.

Raisonner par disjonction des cas

On partage les possibilités en cas couvrant toutes les situations. Si chacun des cas conduit à la même conclusion Q , alors Q est établie.

Pour deux cas P et $\neg P$, il suffit de montrer $P \Rightarrow Q$ puis $\neg P \Rightarrow Q$.

Réfuter un énoncé universel

Pour montrer que $\forall x \in E, P(x)$ est faux, un seul **contre-exemple** suffit : il faut trouver $x_0 \in E$ tel que $P(x_0)$ soit faux.

Existence et unicité

Pour démontrer l'existence d'un objet, on peut l'exhiber et vérifier qu'il possède la propriété demandée.

Pour démontrer l'unicité, on suppose que deux objets x et y conviennent, puis on montre que $x = y$.

Analyse-synthèse

Lorsqu'on cherche tous les objets satisfaisant une propriété :

Analyse : on suppose qu'un objet est solution et on déduit des conditions nécessaires qui permettent de l'identifier.

Synthèse : on reprend les candidats obtenus et on vérifie lesquels satisfont effectivement le problème.

L'analyse seule ne suffit pas : elle produit des conditions nécessaires, pas automatiquement suffisantes.

Exemple : Pour écrire une fonction $f : [0, 1] \rightarrow \mathbb{R}$ comme somme d'une fonction affine et d'une fonction s'annulant en 0 et 1, l'analyse impose les coefficients de la partie affine ; la synthèse vérifie que la construction obtenue convient.

4 - Raisonnement par récurrence

Propriété : Propriété fondamentale de $\mathbb{N}$

Toute partie non vide de $\mathbb{N}$ possède un plus petit élément. Toute partie non vide et majorée de $\mathbb{N}$ possède un plus grand élément.

Propriété : Principe de récurrence simple

Soit $P(n)$ une propriété dépendant d'un entier n . Soit $n_0 \in \mathbb{N}$. Si :

Initialisation : $P(n_0)$ est vraie ;

Hérédité : pour tout $n \geq n_0$, $P(n) \Rightarrow P(n+1)$;

alors $P(n)$ est vraie pour tout entier $n \geq n_0$.

Propriété : Récurrence double

Soit $P(n)$ une propriété. Si $P(n_0)$ et $P(n_0+1)$ sont vraies et si, pour tout $n \geq n_0$,

$$P(n) \wedge P(n+1) \Rightarrow P(n+2),$$

alors $P(n)$ est vraie pour tout $n \geq n_0$.

Propriété : Récurrence forte

Soit $P(n)$ une propriété. Si $P(n_0)$ est vraie et si, pour tout $n \geq n_0$,

$$P(n_0) \wedge P(n_0+1) \wedge \cdots \wedge P(n) \Rightarrow P(n+1),$$

alors $P(n)$ est vraie pour tout $n \geq n_0$.

Démonstration : Récurrence forte à partir de la récurrence simple

Posons $Q(n) : P(n_0) \wedge P(n_0+1) \wedge \cdots \wedge P(n)$.

L'initialisation de Q est exactement $P(n_0)$. Supposons $Q(n)$ vraie. L'hypothèse de récurrence forte donne alors $P(n+1)$, donc $Q(n+1)$ est vraie. Par récurrence simple, $Q(n)$ est vraie pour tout $n \geq n_0$, donc en particulier $P(n)$ est vraie pour tout $n \geq n_0$.

Méthode : Rédaction d'une récurrence

Toujours annoncer clairement la propriété $P(n)$, le premier rang, l'initialisation, l'hypothèse de récurrence, l'hérédité et la conclusion. Une hérédité correcte sans initialisation ne prouve rien.

5 - Ensembles et opérations ensemblistes

Définition : Appartenance, inclusion, égalité

Si x est un élément de E , on écrit $x \in E$. Sinon, $x \notin E$.

On dit que A est **inclus** dans E , et on écrit $A \subset E$, lorsque tout élément de A appartient à E .

Deux ensembles sont égaux s'ils ont exactement les mêmes éléments.

Propriété : Double inclusion

$$A = B \iff A \subset B \text{ et } B \subset A.$$

Ainsi, une méthode fondamentale pour démontrer une égalité d'ensembles consiste à établir les deux inclusions.

Définition : Ensemble vide, singleton, ensemble des parties

L'ensemble sans élément est l'**ensemble vide**, noté $\emptyset$.

Un ensemble constitué d'un seul élément est un **singleton**, par exemple $\{x\}$. Attention : x et $\{x\}$ sont de natures différentes.

L'**ensemble des parties** de E est

$$\mathcal{P}(E) = \{A ; A \subset E\}.$$

Ainsi, $A \subset E$ équivaut à $A \in \mathcal{P}(E)$.

Définition : Produit cartésien

Pour des ensembles $E_1, \dots, E_p$,

$$E_1 \times \dots \times E_p = \{(x_1, \dots, x_p) ; x_i \in E_i \text{ pour tout } i\}.$$

Lorsque tous les ensembles sont égaux à E , on note E^p . Un élément de E^p est un p -uplet d'éléments de E .

Définition : Réunion, intersection, différence, complémentaire

Pour $A, B \subset E$,

$$A \cup B = \{x \in E ; x \in A \text{ ou } x \in B\},$$

$$A \cap B = \{x \in E ; x \in A \text{ et } x \in B\},$$

$$A \setminus B = \{x \in E ; x \in A \text{ et } x \notin B\}.$$

Le complémentaire de A dans E est $E \setminus A$, également noté A^c lorsque l'ensemble ambiant est clair.

Définition : Différence symétrique

La différence symétrique de A et B est

$$A \Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

Cette notation est utile mais n'est pas centrale dans le programme officiel.

Propriété : Règles de calcul sur les ensembles

Pour $A, B, C \subset E$:

$$A \cap B = B \cap A, \quad A \cup B = B \cup A,$$

$$(A \cap B) \cap C = A \cap (B \cap C), \quad (A \cup B) \cup C = A \cup (B \cup C),$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C),$$

$$(A \cup B)^c = A^c \cap B^c, \quad (A \cap B)^c = A^c \cup B^c.$$

De plus,

$$A \subset B \Rightarrow B^c \subset A^c.$$

Démonstration : Démonstration exigible – associativité de l'intersection

On procède par double inclusion.

Soit $x \in (A \cap B) \cap C$. Alors $x \in A \cap B$ et $x \in C$, donc $x \in A$, $x \in B$ et $x \in C$. Ainsi $x \in A \cap (B \cap C)$. Donc

$$(A \cap B) \cap C \subset A \cap (B \cap C).$$

Réciproquement, si $x \in A \cap (B \cap C)$, alors $x \in A$, $x \in B$ et $x \in C$, donc $x \in (A \cap B) \cap C$. Les deux ensembles sont égaux.

Démonstration : Lois de De Morgan pour les ensembles

Soit $x \in E$. Alors

$$\begin{aligned}x \in (A \cup B)^c &\Leftrightarrow x \notin A \cup B \\&\Leftrightarrow \neg(x \in A \vee x \in B) \\&\Leftrightarrow (x \notin A) \wedge (x \notin B) \\&\Leftrightarrow x \in A^c \cap B^c.\end{aligned}$$

Donc $(A \cup B)^c = A^c \cap B^c$. La seconde loi se démontre de même.

Définition : Famille, recouvrement disjoint et partition

Une famille d'éléments de E indexée par I est notée $(x_i)_{i \in I}$. Une famille de parties de E est notée $(A_i)_{i \in I}$.

La famille $(A_i)_{i \in I}$ est un **recouvrement** de E lorsque $\bigcup_{i \in I} A_i = E$. Elle est **disjointe** lorsque les ensembles sont deux à deux disjoints.

Une **partition** de E est une famille de parties non vides, deux à deux disjointes, dont la réunion est E .

Méthode :

Pour montrer $A \subset B$, prendre un élément arbitraire $x \in A$ et démontrer $x \in B$.

Pour montrer $A = B$, faire une double inclusion ou, de manière équivalente, démontrer pour tout x :

$$x \in A \Leftrightarrow x \in B.$$

6 - Relations binaires

Définition : Relation binaire

Une relation binaire $\mathcal{R}$ sur un ensemble E est une propriété portant sur les couples $(x, y) \in E^2$. On écrit $x\mathcal{R}y$ lorsque x est en relation avec y .

Définition : Propriétés usuelles d'une relation

Une relation $\mathcal{R}$ sur E est :

réflexive si $\forall x \in E, x\mathcal{R}x$;

symétrique si $x\mathcal{R}y \Rightarrow y\mathcal{R}x$;

antisymétrique si $(x\mathcal{R}y \text{ et } y\mathcal{R}x) \Rightarrow x = y$;

transitive si $(x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z$.

Définition : Relation d'équivalence et classe d'équivalence

Une relation d'équivalence est une relation réflexive, symétrique et transitive.

Si $\mathcal{R}$ est une relation d'équivalence sur E , la classe de $x \in E$ est

$$[x] = \{y \in E ; x\mathcal{R}y\}.$$

Propriété : Les classes d'équivalence forment une partition

Pour une relation d'équivalence sur E , les classes d'équivalence sont non vides. Deux classes sont soit égales soit disjointes, et leur réunion est E .

Démonstration : Démonstration – partition en classes d'équivalence

Pour tout $x \in E$, la réflexivité donne $x\mathcal{R}x$, donc $x \in [x]$: chaque classe est non vide et chaque élément de E appartient à une classe.

Supposons $[x] \cap [y] \neq \emptyset$. Il existe z appartenant aux deux classes. Alors $x\mathcal{R}z$ et $y\mathcal{R}z$. Par symétrie, $z\mathcal{R}y$, puis par transitivité $x\mathcal{R}y$. Si $t \in [x]$, alors $x\mathcal{R}t$. De $y\mathcal{R}x$ et $x\mathcal{R}t$, on déduit $y\mathcal{R}t$, donc $t \in [y]$. Ainsi $[x] \subset [y]$, et réciproquement

$[y] \subset [x]$. Donc $[x] = [y]$.

Ainsi deux classes distinctes sont disjointes et l'ensemble des classes est une partition de E .

Définition : Relation d'ordre

Une relation d'ordre est une relation réflexive, antisymétrique et transitive.

Elle est **totale** si deux éléments quelconques sont toujours comparables : pour tous $x, y \in E$, $x \mathcal{R} y$ ou $y \mathcal{R} x$. Sinon l'ordre est **partiel**.

Exemple : La relation $\leq$ est un ordre total sur $\mathbb{R}$. La divisibilité est un ordre partiel sur $\mathbb{N}^*$: par exemple 2 et 3 ne sont pas comparables pour la divisibilité.

Définition : Ordre strict

Une relation d'ordre strict est une relation transitive et irréflexive, c'est-à-dire telle que

$$\forall x \in E, \quad \neg(x \mathcal{R} x).$$

De manière équivalente, dans les situations usuelles, on peut la voir comme la relation stricte associée à un ordre : par exemple $<$ est associée à $\leq$. Elle est alors également antisymétrique au sens strict : $x \mathcal{R} y$ interdit $y \mathcal{R} x$.

Définition : Congruence

Soit $c \neq 0$. Pour des nombres réels a, b , on écrit

$$a \equiv b [c]$$

lorsque $a - b \in c\mathbb{Z}$, c'est-à-dire lorsqu'il existe $k \in \mathbb{Z}$ tel que $a - b = kc$. Pour $a, b \in \mathbb{Z}$ et $c = n \in \mathbb{N}^*$, on retrouve la congruence modulo n .

Démonstration : Démonstration exigible – la congruence modulo n est une relation d'équivalence

Fixons $n \in \mathbb{N}^*$ et définissons sur $\mathbb{Z}$:

$$a \mathcal{R} b \iff a \equiv b [n].$$

Réflexivité : $a - a = 0 \times n$, donc $a \equiv a [n]$.

Symétrie : si $a - b = kn$, alors $b - a = (-k)n$, donc $b \equiv a [n]$.

Transitivité : si $a - b = kn$ et $b - c = k'n$, alors

$$a - c = (a - b) + (b - c) = (k + k')n,$$

donc $a \equiv c [n]$.

La relation est donc réflexive, symétrique et transitive : c'est une relation d'équivalence.

Méthode :

Pour une relation d'équivalence, vérifier dans l'ordre : réflexivité, symétrie, transitivité.

Pour une relation d'ordre, vérifier : réflexivité, antisymétrie, transitivité ; puis déterminer si l'ordre est total ou seulement partiel.

7 - Applications

Définition : Application, image et antécédent

Une application $f : E \rightarrow F$ associe à tout élément $x \in E$ un unique élément $f(x) \in F$.

E est l'ensemble de départ, F l'ensemble d'arrivée. L'élément $f(x)$ est l'image de x . Si $f(x) = y$, alors x est un antécédent de y .

Le graphe de f est

$$\Gamma_f = \{(x, f(x)) ; x \in E\} \subset E \times F.$$

On note $\mathcal{F}(E, F)$, ou encore F^E , l'ensemble des applications de E dans F .

Définition : Égalité, restriction et prolongement

Deux applications sont égales lorsqu'elles ont le même ensemble de départ, le même ensemble d'arrivée et les mêmes valeurs en tout point.

Si $A \subset E$, la restriction de $f : E \rightarrow F$ à A est l'application

$$f|_A : A \rightarrow F, \quad x \mapsto f(x).$$

Réciproquement, une application définie sur un ensemble plus grand et coïncidant avec une application donnée sur A est un **prolongement**.

Définition : Fonction indicatrice

Pour $A \subset E$, la fonction indicatrice de A est

$$\mathbf{1}_A : E \rightarrow \{0, 1\}, \quad \mathbf{1}_A(x) = \begin{cases} 1 & \text{si } x \in A, \\ 0 & \text{si } x \notin A. \end{cases}$$

Définition : Composition

Soient $f : E \rightarrow F$ et $g : F \rightarrow G$. La composée de f puis g est

$$g \circ f : E \rightarrow G, \quad x \mapsto g(f(x)).$$

La composition est associative : $h \circ (g \circ f) = (h \circ g) \circ f$.

L'identité de E est $\text{id}_E : x \mapsto x$, et

$$f \circ \text{id}_E = f, \quad \text{id}_F \circ f = f.$$

Si $f : E \rightarrow E$, on définit ses itérées par

$$f^0 = \text{id}_E, \quad f^{n+1} = f \circ f^n \quad (n \in \mathbb{N}).$$

Ainsi f^n désigne la composée de f avec elle-même n fois.

Définition : Image directe et image réciproque

Pour $A \subset E$, l'image directe est

$$f(A) = \{f(x) ; x \in A\} \subset F.$$

Pour $B \subset F$, l'image réciproque est

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

Cette notation ne suppose pas que f soit bijective : ici $f^{-1}(B)$ désigne un ensemble d'antécédents.

Propriété : Calculs d'images directes et réciproques

Pour $A, A' \subset E$ et $B, B' \subset F$:

$$\begin{aligned}A \subset A' &\Rightarrow f(A) \subset f(A'), \\f(A \cup A') &= f(A) \cup f(A'), \quad f(A \cap A') \subset f(A) \cap f(A'), \\f^{-1}(B \cup B') &= f^{-1}(B) \cup f^{-1}(B'), \\f^{-1}(B \cap B') &= f^{-1}(B) \cap f^{-1}(B'), \\f^{-1}(F \setminus B) &= E \setminus f^{-1}(B).\end{aligned}$$

L'inclusion pour l'image directe d'une intersection peut être stricte.

Définition : Injection, surjection, bijection

Une application $f : E \rightarrow F$ est **injective** si

$$\forall x, x' \in E, \quad f(x) = f(x') \Rightarrow x = x'.$$

Chaque élément de F a alors au plus un antécédent.

Elle est **surjective** si

$$\forall y \in F, \quad \exists x \in E, \quad f(x) = y.$$

Chaque élément de F a alors au moins un antécédent.

Elle est **bijective** si elle est injective et surjective; tout élément de F a alors exactement un antécédent.

Méthodes pratiques

Pour démontrer l'injectivité, partir de $f(x) = f(x')$ et montrer $x = x'$.

Pour démontrer la surjectivité, prendre un $y \in F$ arbitraire et résoudre $f(x) = y$ avec $x \in E$.

Pour démontrer la bijectivité, on peut prouver séparément injectivité et surjectivité, ou montrer directement que $f(x) = y$ possède pour tout $y \in F$ une unique solution $x \in E$.

Définition : Application réciproque

Si $f : E \rightarrow F$ est bijective, sa bijection réciproque est l'unique application $f^{-1} : F \rightarrow E$ telle que

$$f^{-1} \circ f = \text{id}_E, \quad f \circ f^{-1} = \text{id}_F.$$

Propriété : Caractérisation de la bijectivité par une réciproque

Une application $f : E \rightarrow F$ est bijective si et seulement s'il existe $g : F \rightarrow E$ telle que

$$g \circ f = \text{id}_E \quad \text{et} \quad f \circ g = \text{id}_F.$$

Dans ce cas $g = f^{-1}$.

Démonstration : Démonstration exigible – ce que l'on déduit d'une composée

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

1. Si $g \circ f$ est injective, alors f est injective.

Supposons $f(x) = f(y)$. Alors

$$g(f(x)) = g(f(y)),$$

donc $(g \circ f)(x) = (g \circ f)(y)$. L'injectivité de $g \circ f$ donne $x = y$.

2. Si $g \circ f$ est surjective, alors g est surjective.

Soit $z \in G$. Comme $g \circ f$ est surjective, il existe $x \in E$ tel que $g(f(x)) = z$. En posant $y = f(x) \in F$, on obtient $g(y) = z$. Ainsi tout $z \in G$ possède un antécédent par g .

Propriété : Conservation par composition

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

Si f et g sont injectives, alors $g \circ f$ est injective.

Si f et g sont surjectives, alors $g \circ f$ est surjective.

Si f et g sont bijectives, alors $g \circ f$ est bijective et

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Démonstration : Démonstration exigible – conservation par composition

Injectivité. Si $(g \circ f)(x) = (g \circ f)(x')$, l'injectivité de g donne $f(x) = f(x')$, puis celle de f donne $x = x'$.

Surjectivité. Soit $z \in G$. Comme g est surjective, il existe $y \in F$ tel que $g(y) = z$. Comme f est surjective, il existe $x \in E$ tel que $f(x) = y$. Alors $(g \circ f)(x) = z$.

Bijektivité et réciproque. Si f et g sont bijectives, la composée est injective et surjective. De plus,

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ \text{id}_F \circ g^{-1} = \text{id}_G,$$

et de même

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = \text{id}_E.$$

Donc $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Définition : Involution

Une application $f : E \rightarrow E$ est une **involution** lorsque

$$f \circ f = \text{id}_E.$$

Toute involution est bijective et vérifie $f^{-1} = f$.

Démonstration : Une involution est bijective

L'égalité $f \circ f = \text{id}_E$ montre que f possède à la fois un inverse à gauche et un inverse à droite, égal à elle-même. Par la caractérisation précédente, f est bijective et $f^{-1} = f$.

Le programme de colle pour ce chapitre insiste notamment sur les cinq démonstrations suivantes :

1. règles de logique (tables de vérité, contraposition, négation d'une implication) ;
2. associativité de l'intersection ou de la réunion par double inclusion ;
3. si $g \circ f$ est injective alors f est injective ; si $g \circ f$ est surjective alors g est surjective ;
4. conservation de l'injectivité, de la surjectivité et de la bijectivité par composition, avec la formule $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$;
5. la congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.