LOGIQUE ET THÉORIE DES ENSEMBLES

Booléens et opérateurs logiques

Définitions

• Une assertion est une proposition mathématique sans variable qui est soit vraie soit fausse, sans autre possibilité.
Les propositions « 2+2=4 » et « 0=1 » sont deux assertions, l'une vraie et l'autre fausse.

• Ces deux valeurs « vraie » et « fausse » différentes l'une de l'autre sont appelées booléens et notées V et F.

• La notion d'assertion, comme plusieurs autres définitions de ce chapitre, est une notion première ; cette notion ne peut pas être définie qu'en utilisant d'autres mots qu'ils faudraient à leur tour définir.

Dans la suite A, B, C et D sont des assertions.

• Les opérateurs logiques NON, ET et OU définissent les assertions NON A, A ET B et A OU B par ces tables de vérité :

A	NON A
F	V
V	F

A	B	A ET B
F	F	F
F	V	F
V	F	F
V	V	V

A	B	A OU B
F	F	F
F	V	V
V	F	V
V	V	V

• Deux assertions $P(A, B, C, \cdots)$ et $Q(A, B, C, \cdots)$ sont équivalentes si et seulement si elles ont même table de vérité ; ceci signifie que pour toutes les valeurs possibles des paramètres A, B, C, etc. les assertions $P(A, B, C, \cdots)$ et $Q(A, B, C, \cdots)$ sont soit toutes les deux vraies soit toutes les deux fausses ; une telle équivalence est notée $P(A, B, C, \cdots) \equiv Q(A, B, C, \cdots)$.

• De façon usuelle l'opérateur NON est prioritaire sur ET qui est prioritaire sur OU, lui-même prioritaire sur $\Longleftrightarrow$ et $\Longrightarrow$ définis par la suite ; les parenthèses sont donc superflues dans l'expression suivante :

$$\text{NON } A \text{ OU NON } B \text{ ET } C \equiv (\text{NON } A) \text{ OU } [(\text{NON } B) \text{ ET } C]$$

• Les circuits électroniques sont essentiellement composés de transistors qui peuvent être utilisés comme des interrupteurs commandés électriquement. Montés en dérivation ou en série ils permettent de construire des circuits élémentaires, appelés portes logiques, se comportant comme les opérateurs OU ou ET. La tension disponible à la sortie du circuit est nulle ou non en fonction des tensions imposées aux entrées du circuit.
La construction d'une porte NON est aussi possible, elle dépend du type de transistors employés et nécessite généralement de deux transistors.
Combiner les portes logiques entre elles permet de définir des assertions de plus en plus complexes, d'effectuer des opérations binaires et de construire des mémoires informatiques. Les micro-processeurs sont constitués de millions de portes logiques.

Formulaire

• Les propriétés de base des opérateurs logiques sont celles-ci :

Commutativité	A ET $B \equiv B$ ET A	A OU $B \equiv B$ OU A
Involution	NON (NON A) $\equiv A$	A ET $A \equiv A$ OU $A \equiv A$
Élément neutre	A ET V $\equiv$ V ET $A \equiv A$	A OU F $\equiv$ F OU $A \equiv A$
Élément absorbant	A ET F $\equiv$ F ET $A \equiv$ F	A OU V $\equiv$ V OU $A \equiv$ V

• Ces propriétés découlent directement des tables de vérité précédentes.

• L'associativité des opérateurs ET et OU justifie les écritures sans parenthèse de la forme A ET B ET C :

$$(A \text{ ET } B) \text{ ET } C \equiv A \text{ ET } (B \text{ ET } C)$$
$$(A \text{ OU } B) \text{ OU } C \equiv A \text{ OU } (B \text{ OU } C)$$

• Une vérification de l'associativité de ET consite à énumérer dans une table de vérité les huit cas possibles pour A, B et C pour justifier que les deux assertions sont vraies uniquement si les trois termes A, B et C sont vrais, et fausses toutes les deux dans les sept autres cas.

• L'ordre d'énumération de tous les cas suit généralement l'ordre lexicographique qui correspond à l'ordre alphabétique :

$$(\text{F}, \text{F}, \text{F})\ (\text{F}, \text{F}, \text{V})\ (\text{F}, \text{V}, \text{F})\ (\text{F}, \text{V}, \text{V})$$
$$(\text{V}, \text{F}, \text{F})\ (\text{V}, \text{F}, \text{V})\ (\text{V}, \text{V}, \text{F})\ (\text{V}, \text{V}, \text{V})$$

Lois de Morgan

• Les lois de Morgan déterminent la négation d'une expression en fonction de la négation de chacun de ses termes, les opérateurs ET et OU sont alors échangés :

$$\mathsf{NON}\,(A\,\mathsf{ET}\,B) \equiv (\mathsf{NON}\ A)\,\mathsf{OU}\,(\mathsf{NON}\ B)$$
$$\mathsf{NON}\,(A\,\mathsf{OU}\,B) \equiv (\mathsf{NON}\ A)\,\mathsf{ET}\,(\mathsf{NON}\ B)$$

• La table suivante justifie la première de ces deux équivalences :

A	B	$\mathsf{NON}\,(A\,\mathsf{ET}\,B)$		$(\mathsf{NON}\ A)\,\mathsf{OU}\,(\mathsf{NON}\ B)$		
		$A\,\mathsf{ET}\,B$		$\mathsf{NON}\ A$	$\mathsf{NON}\ B$	
F	F	F	V	V	V	V
F	V	F	V	V	F	V
V	F	F	V	F	V	V
V	V	V	F	F	F	F

L'autre démonstration peut se faire de façon similaire.

• Il est aussi possible de justifier l'une de ces équivalences à partir de l'autre, en appliquant sa négation aux assertions $\mathsf{NON}\ A$, $\mathsf{NON}\ B$ et $\mathsf{NON}\ C$ à la place de A, B et C. Les équivalences ci-dessous prouvent la seconde loi à partir de la première :

$$\mathsf{NON}\,(\mathsf{NON}\,(\mathsf{NON}\ A\,\mathsf{ET}\,\mathsf{NON}\ B)) \equiv \underline{(\mathsf{NON}\ A)\,\mathsf{ET}\,(\mathsf{NON}\ B)}$$
$$\equiv \mathsf{NON}\,(\mathsf{NON}\,(\mathsf{NON}\ A)\,\mathsf{OU}\,\mathsf{NON}\,(\mathsf{NON}\ B)) \equiv \underline{\mathsf{NON}\,(A\,\mathsf{OU}\,B)}$$

Distributivité

• Chaque opérateur booléen ET ou OU est distributif par rapport à l'autre :

$$A\,\mathsf{ET}\,(B\,\mathsf{OU}\,C) \equiv (A\,\mathsf{ET}\,B)\,\mathsf{OU}\,(A\,\mathsf{ET}\,C)$$
$$A\,\mathsf{OU}\,(B\,\mathsf{ET}\,C) \equiv (A\,\mathsf{OU}\,B)\,\mathsf{ET}\,(A\,\mathsf{OU}\,C)$$

• Au contraire la distributivité de la multiplication par rapport à l'addition se traduit par cette égalité numérique, mais l'addition n'est pas distributive par rapport à la multiplication :

$$x(y+z) = xy + xz \qquad 1 + (2 \times 3) = 7 \neq 12 = (1+2) \times (1+3)$$

• Cette table de vérité, en énumérant toutes les possibiltés pour les variables A, B et C, justifie la première équivalence :

A	B	C	$A\,\mathsf{ET}\,(B\,\mathsf{OU}\,C)$		$(A\,\mathsf{ET}\,B)\,\mathsf{OU}\,(A\,\mathsf{ET}\,C)$		
			$B\,\mathsf{OU}\,C$		$A\,\mathsf{ET}\,B$	$A\,\mathsf{ET}\,C$	
F	F	F	F	F	F	F	F
F	F	V	V	F	F	F	F
F	V	F	V	F	F	F	F
F	V	V	V	F	F	F	F
V	F	F	F	F	F	F	F
V	F	V	V	V	F	V	V
V	V	F	V	V	V	F	V
V	V	V	V	V	V	V	V

• Une table de vérité similaire démontre la distributivité de OU par rapport à ET. Une autre démonstration consiste à appliquer les lois de Morgan à la négation de l'équivalence précédente aux assertions $\mathsf{NON}\ A$, $\mathsf{NON}\ B$ et $\mathsf{NON}\ C$:

$$\mathsf{NON}\,(\mathsf{NON}\ A\,\mathsf{ET}\,(\mathsf{NON}\ B\,\mathsf{OU}\,\mathsf{NON}\ C))$$
$$\equiv A\,\mathsf{OU}\,\mathsf{NON}\,(\mathsf{NON}\ B\,\mathsf{OU}\,\mathsf{NON}\ C) \equiv \underline{A\,\mathsf{OU}\,(B\,\mathsf{ET}\,C)}$$
$$\equiv \mathsf{NON}\,((\mathsf{NON}\ A\,\mathsf{ET}\,\mathsf{NON}\ B)\,\mathsf{OU}\,(\mathsf{NON}\ A\,\mathsf{ET}\,\mathsf{NON}\ C))$$
$$\equiv \mathsf{NON}\,(\mathsf{NON}\ A\,\mathsf{ET}\,\mathsf{NON}\ B)\,\mathsf{ET}\,\mathsf{NON}\,(\mathsf{NON}\ A\,\mathsf{ET}\,\mathsf{NON}\ C))$$
$$\equiv \underline{(A\,\mathsf{OU}\,B)\,\mathsf{ET}\,(A\,\mathsf{OU}\,C)}$$

Tautologies

• Une tautologie est une assertion de valeur vraie pour toutes les valeurs possibles de ses paramètres.

• La tautologie du tiers exclu signifie qu'une assertion est vraie ou fausse, sans autre possibilité. La tautologie de non contradiction illustre qu'une assertion ne peut pas être simultanément vraie et fausse :

Tautologie du tiers exclu $A\,\mathsf{OU}\,\mathsf{NON}\ A \equiv \mathsf{V}$

Tautologie de non contradiction $\mathsf{NON}\,(A\,\mathsf{ET}\,\mathsf{NON}\ A) \equiv \mathsf{V}$

• Les lois de Morgan justifient l'équivalence de ces deux tautologies :

$$A\,\mathsf{OU}\,(\mathsf{NON}\ A) \equiv \mathsf{NON}\,(\mathsf{NON}\,(A\,\mathsf{OU}\,(\mathsf{NON}\ A)))$$
$$\equiv \mathsf{NON}\,(\mathsf{NON}\,(A\,\mathsf{OU}\,(\mathsf{NON}\ A))) \equiv \mathsf{NON}\ A\,\mathsf{ET}\,\mathsf{NON}\,(\mathsf{NON}\ A))$$
$$\equiv \mathsf{NON}\,(\mathsf{NON}\ A\,\mathsf{ET}\,A)$$

L'implication et l'équivalence

Présentation de l'implication

• L'opérateur d'implication $A \Longrightarrow B$ est défini ainsi :

$$A \Longrightarrow B \equiv (\mathsf{NON}\ A)\ \mathsf{OU}\ B$$

A	B	NON A	$A \Longrightarrow B$
F	F	V	V
F	V	V	V
V	F	F	F
V	V	F	V

• Supposer que les assertions A et $A \Longrightarrow B$ sont vraies impose que B est vraie ; cette propriété est appelée *Modus ponens*.
L'implication $A \Longrightarrow B$ traduit donc la formule *si A [est vraie] alors B [est vraie]*.
Au contraire dans le cas où A est vraie et B est fausse, l'implication $A \Longrightarrow B$ est erronée et l'assertion B ne se déduit pas de A.
Des maximes comme « si les poules avaient des dents alors tout serait possible » et « avec des si on pourrait mettre Paris dans une bouteille » illustrent indirectement que l'implication $A \Longrightarrow B$ est vraie lorsque l'assertion A est fausse.

• Les démonstrations mathématiques sont construites à partir de déductions successives : une suite finie de « donc » ; l'opérateur d'implication $\Longrightarrow$ formalise les règles de déductions sans aucune ambiguïté.

• La rédaction d'une démonstration prouvant $A \Longrightarrow B$ commence par supposer l'assertion A pour en déduire B.

Présentation de l'équivalence

• L'opérateur $\Longleftrightarrow$ définit l'équivalence logique :

$$\begin{aligned} &A \Longleftrightarrow B \\ \equiv\ &(A \Longrightarrow B)\ \mathsf{ET}\ (B \Longrightarrow A) \end{aligned}$$

A	B	$A \Longrightarrow B$	$A \Longrightarrow B$	$A \Longleftrightarrow B$
F	F	V	V	V
F	V	V	F	F
V	F	F	V	F
V	V	V	V	V

• L'équivalence $A \Longleftrightarrow B$ est vraie si et seulement si les deux assertions A et B ont la même valeur : vraies toutes les deux ou fausses toutes les deux :

$$A \Longleftrightarrow B \equiv (A\ \mathsf{ET}\ B)\ \mathsf{OU}\ (\mathsf{NON}\ A\ \mathsf{ET}\ \mathsf{NON}\ B)$$

• La démontration repose sur la distributivité de ET par rapport à OU :

$$\begin{aligned} &(A \Longrightarrow B)\ \mathsf{ET}\ (B \Longrightarrow A) \equiv (\mathsf{NON}\ A\ \mathsf{OU}\ B)\ \mathsf{ET}\ (\mathsf{NON}\ B\ \mathsf{OU}\ A) \\ \equiv\ &((\mathsf{NON}\ A\ \mathsf{OU}\ B)\ \mathsf{ET}\ \mathsf{NON}\ B)\ \mathsf{OU}\ ((\mathsf{NON}\ A\ \mathsf{OU}\ B)\ \mathsf{ET}\ A) \\ \equiv\ &\quad ((\mathsf{NON}\ A\ \mathsf{ET}\ \mathsf{NON}\ B)\ \mathsf{OU}\ (B\ \mathsf{ET}\ \mathsf{NON}\ B)) \\ &\mathsf{OU}\ ((\mathsf{NON}\ A\ \mathsf{ET}\ A)\ \mathsf{OU}\ (B\ \mathsf{ET}\ A)) \\ \equiv\ &(\mathsf{NON}\ A\ \mathsf{ET}\ \mathsf{NON}\ B)\ \mathsf{OU}\ \mathsf{F}\ \mathsf{OU}\ \mathsf{F}\ \mathsf{OU}\ (B\ \mathsf{ET}\ A) \\ \equiv\ &(\mathsf{NON}\ A\ \mathsf{ET}\ \mathsf{NON}\ B)\ \mathsf{OU}\ (A\ \mathsf{ET}\ B) \end{aligned}$$

• Les formules mathématiques omettent généralement de rappeler qu'un argument est vrai car cela est sous-entendu.
Les trois notations $A \equiv B$, $A \Longleftrightarrow B \equiv \mathsf{V}$ et $A \Longleftrightarrow B$ signifient la même chose ; la dernière est celle qui est désormais employée.
Des assertions équivalentes ont toutes la même table de vérité ; ceci justifie les démonstrations par des suites d'équivalences et traduit la transitivité de l'équivalence.

• Plus généralemement l'équivalence est réflexive, symétrique et transitive, et ces propriétés définissent une relation d'équivalence :

Réflexive	$A \Longleftrightarrow A$
Symétrique	$(A \Longleftrightarrow B) \Longleftrightarrow (B \Longleftrightarrow A)$
Transitivité	$((A \Longleftrightarrow B)\ \mathsf{ET}\ (B \Longleftrightarrow C)) \Longrightarrow (A \Longleftrightarrow C)$

• Ces expressions sont des tautologies mettant en œuvre ces nouvelles notations même si elles ne le précisent par un $\cdots \equiv \mathsf{V}$ explicite.

• Les propriétés précédentes sont à la base des démonstrations constituées d'une suite d'équivalence.

• La réflexivité et la symétrie de l'opérateur $\Longleftrightarrow$ proviennent directement de la symétrie de sa définition et de sa table de vérité.
Une table de vérité permet de vérifier la transitivité de l'équivalence.

• Le plus souvent la démonstration d'une propriété de la forme $A \Longleftrightarrow B$ vérifie séparément $A \Longrightarrow B$ et $B \Longrightarrow A$.

Propriétés de l'implication

• L'implication vérifie ces quatre propriétés élémentaires :

$$A \Longrightarrow A \qquad A \Longrightarrow (A \text{ OU } B) \qquad (A \text{ ET } B) \Longrightarrow A$$
$$\textit{Modus ponens} \qquad (A \text{ ET } (A \Longrightarrow B)) \Longrightarrow B$$

• La preuve provient de ces équivalences logiques qui démontrent que ces expressions sont des tautologies :

$$\begin{aligned}
(A \Longrightarrow A) &\Longleftrightarrow (\text{NON } A \text{ OU } A)\\
&\Longleftrightarrow \text{V}\\
(A \Longrightarrow (A \text{ OU } B)) &\Longleftrightarrow \text{NON } A \text{ OU } (A \text{ OU } B)\\
&\Longleftrightarrow (\text{NON } A \text{ OU } A) \text{ OU } B\\
&\Longleftrightarrow \text{V OU } B\\
&\Longleftrightarrow \text{V}\\
((A \text{ ET } B) \Longrightarrow A) &\Longleftrightarrow \text{NON } (A \text{ ET } B) \text{ OU } A\\
&\Longleftrightarrow \text{NON } A \text{ OU NON } B \text{ OU } A\\
&\Longleftrightarrow \text{NON } A \text{ OU } A \text{ OU NON } B\\
&\Longleftrightarrow \text{V}\\
&\qquad ((A \text{ ET } (A \Longrightarrow B)) \Longrightarrow B)\\
&\Longleftrightarrow \text{NON } (A \text{ ET } (\text{NON } A \text{ OU } B)) \text{ OU } B\\
&\Longleftrightarrow (\text{NON } A \text{ OU } (A \text{ ET NON } B)) \text{ OU } B\\
&\Longleftrightarrow ((\text{NON } A \text{ OU } A) \text{ ET } (\text{NON } A \text{ OU NON } B)) \text{ OU } B\\
&\Longleftrightarrow (\text{V ET } (\text{NON } A \text{ OU NON } B)) \text{ OU } B\\
&\Longleftrightarrow \text{NON } A \text{ OU NON } B \text{ OU } B\\
&\Longleftrightarrow \text{NON } A \text{ OU V}\\
&\Longleftrightarrow \text{V}
\end{aligned}$$

• De nombreuses démonstrations mathématiques reposent sur les propriétés suivantes de l'implication :

Négation	$(\text{NON } (A \Longrightarrow B)) \Longleftrightarrow A \text{ ET } (\text{NON } B)$
Contraposée	$((\text{NON } B) \Longrightarrow (\text{NON } A)) \Longleftrightarrow (A \Longrightarrow B)$
Démonstration par l'absurde	$((\text{NON } A) \Longrightarrow \text{F}) \Longleftrightarrow A$
Transitivité	$((A \Longrightarrow B) \text{ ET } (B \Longrightarrow C)) \Longrightarrow (A \Longrightarrow C)$

• Démontrer que l'implication $A \Longrightarrow B$ est fausse consiste donc à justifier $A \text{ ET } (\text{NON } B)$.
Les deux propositions $A \Longrightarrow B$ et $(\text{NON } B) \Longrightarrow (\text{NON } A)$ sont équivalentes l'une de l'autre et appelées contraposées : la preuve de l'une est donc obtenue à partir de la justification de l'autre.
La preuve par l'absurde d'une assertion A consiste à montrer que la

négation de A implique une contradiction $\text{NON } A \Longrightarrow \text{F}$, la condition fausse pouvant être par exemple $0 = 1$.

• Des suites d'équivalences démontrent ces propriétés :

$$\begin{aligned}
\text{NON } (A \Longrightarrow B) &\Longleftrightarrow \text{NON } (\text{NON } A \text{ OU } B)\\
&\Longleftrightarrow \text{NON } (\text{NON } A) \text{ ET } (\text{NON } B)\\
&\Longleftrightarrow A \text{ ET } (\text{NON } B)\\
((\text{NON } B) \Longrightarrow (\text{NON } A)) &\Longleftrightarrow \text{NON } (\text{NON } B) \text{ OU } (\text{NON } A)\\
&\Longleftrightarrow B \text{ OU } (\text{NON } A)\\
&\Longleftrightarrow (A \Longrightarrow B)\\
\text{NON } (A \Longrightarrow \text{F}) &\Longleftrightarrow \text{NON } (\text{NON } A \text{ OU F})\\
&\Longleftrightarrow A \text{ ET V}\\
&\Longleftrightarrow A
\end{aligned}$$

• La méthode des tables de vérité permet de justifier la transitivité de l'implication. Une démonstration développant cette expression logique par distributivité de l'opérateur OU est aussi possible :

$$\begin{aligned}
&\Big(((A \Longrightarrow B) \text{ ET } (B \Longrightarrow C)) \Longrightarrow (A \Longrightarrow C)\Big)\\
\Longleftrightarrow &\text{NON } (A \Longrightarrow B) \text{ ET } (B \Longrightarrow C)) \text{ OU } (A \Longrightarrow C)\\
\Longleftrightarrow &(\text{NON } A \Longrightarrow B) \text{ OU NON } (B \Longrightarrow C) \text{ OU } (A \Longrightarrow C)\\
\Longleftrightarrow &(A \text{ ET NON } B) \text{ OU } (B \text{ ET NON } C) \text{ OU NON } A \text{ OU } C\\
\Longleftrightarrow &((A \text{ ET NON } B) \text{ OU NON } A) \text{ OU } ((B \text{ ET NON } C) \text{ OU } C)\\
\Longleftrightarrow &((A \text{ OU NON } A) \text{ ET } (\text{NON } B \text{ OU NON } A))\\
&\qquad \text{OU } ((B \text{ OU } C) \text{ ET } (\text{NON } C \text{ OU } C))\\
\Longleftrightarrow &(\text{V ET } (\text{NON } B \text{ OU NON } A)) \text{ OU } ((B \text{ OU } C) \text{ ET V})\\
\Longleftrightarrow &(\text{NON } B \text{ OU NON } A) \text{ OU } (B \text{ OU } C)\\
\Longleftrightarrow &\text{NON } B \text{ OU NON } A \text{ OU } B \text{ OU } C\\
\Longleftrightarrow &(\text{NON } B \text{ OU } B) \text{ OU NON } A \text{ OU } C\\
\Longleftrightarrow &\text{V OU NON } A \text{ OU } C\\
\Longleftrightarrow &\text{V}
\end{aligned}$$

Méthodes classiques de démonstration

• Les propriétés suivantes de l'équivalence interviennent régulièrement dans les démonstrations :

Négation $\quad (A \iff B) \iff (\mathsf{NON}\ A \iff \mathsf{NON}\ B)$

Équivalence démontrée par implications circulaires

$$((A \implies B)\ \mathsf{ET}\ (B \implies C)\ \mathsf{ET}\ (C \implies A)) \iff ((A \iff B)\ \mathsf{ET}\ (B \iff C))$$

Autres méthodes de démonstration

$$(A \implies (B\ \mathsf{ET}\ C)) \iff ((A \implies B)\ \mathsf{ET}\ (A \implies C))$$
$$(A \implies (B\ \mathsf{OU}\ C)) \iff ((A \implies B)\ \mathsf{OU}\ (A \implies C))$$
$$((A\ \mathsf{OU}\ B) \implies C) \iff ((A \implies C)\ \mathsf{ET}\ (B \implies C))$$
$$((A\ \mathsf{ET}\ B) \implies C) \iff (A \implies (B \implies C))$$
$$((A \implies B)\ \mathsf{ET}\ (C \implies D)) \implies ((A\ \mathsf{ET}\ C) \implies (B\ \mathsf{ET}\ D))$$

• L'équivalence $(A \implies (B\ \mathsf{ET}\ C)) \iff ((A \implies B)\ \mathsf{ET}\ (A \implies C))$ énonce que la preuve de la première implication peut se faire en justifiant les deux implications $A \implies B$ et $A \implies C$.
Montrer que l'hypothèse A ou l'hypothèse B aboutit à la propriété C se démontre généralement en montrant les deux implications $A \implies C$ et $B \implies C$.
Un énoncé comme « dans le cas où A [est vraie], montrer que $B \implies C$ » consiste à prouver C à partir des hypothèses A et B et correspond à $(A\ \mathsf{ET}\ B) \implies C$.
La réciproque de la dernière implication est fausse, par exemple si A, B et C sont de valeurs V, F et F.

• Les preuves de ces propriétés reposent sur les mêmes méthodes que les précédentes : étude des tables de vérité ou recherche d'équivalents.

Prédicats et quantificateurs

Définitions

• Un prédicat est un énoncé mathématique contenant une ou plusieurs variables tel que le remplacement de chaque variable par un objet mathématique est une assertion. Par exemple « $x + 2 = 4$ » est un prédicat qui dépend de la variable numérique x.
La définition des opérateurs logiques s'étend aux prédicats.

Dans la suite $P(x)$, $Q(x, y)$, etc. sont des prédicats.

• L'asssertion $\forall\, x\ P(x)$ — dite *pour tout x...* — signifie que pour tout objet mathématique a l'assertion $P(a)$ est vraie.

• L'asssertion $\exists\, x\ P(x)$ — dite *il existe x...* — signifie qu'il existe au moins un objet mathématique a pour lequel l'assertion $P(a)$ est vraie.

• Les symboles $\forall$ et $\exists$ sont appelés respectivement quantificateur universel et quantificateur existentiel.

• L'expression $P(x)$ est un prédicat dont la valeur dépend de la variable x ; au contraire $\forall\, x\ P(x)$ est une assertion qui est soit vraie soit fausse, sans faire intervenir de variable.
Les assertions $\forall\, x\ P(x)$ et $\forall\, y\ P(y)$ sont identiques.

• Les opérateurs mathématiques sont prioritaires sur les quantificateurs.

• L'assertion $\exists!\, x\ P(x)$ signifie qu'il existe un unique objet mathématique a vérifiant $P(a)$; pour tout autre objet mathématique $b \neq a$ l'assertion $P(b)$ est fausse :

$$\exists\, x \quad (P(x)\ \mathsf{ET}\ (\forall\, y \quad x \neq y \implies \mathsf{NON}\ P(y)))$$

• La rédaction d'une démonstration de la forme $\forall\, x\ P(x)$ commence par « Soit x, montrons $P(x)$ ».
Une démonstration de la forme $\exists\, x\ P(x)$ consiste généralement à vérifier que telle valeur de x convient.

Axiomes et règles d'emploi des quantificateurs

• Un axiome est une relation énoncée explicitement une fois pour toute à partir desquels sont construits démonstrations et théorèmes.
Comme tout axiome, les propositions suivantes ne peuvent pas se démontrer.

• Les axiomes suivants formalisent, en suivant le sens commun, les règles d'emploi des quantificateurs.

• Certains de ces axiomes sont des équivalences et autorisent la transformation d'une expression en appliquant ces équivalences de la gauche vers la droite, ou de la droite vers la gauche.
D'autres axiomes sont des implications et ne permettent de transformer les propositions qu'en suivant le sens de l'implication.

Axiomes de négation des quantificateurs

• Ces deux axiomes permettent d'exprimer de façon équivalente une proposition comportant un quantificateur et l'opérateur NON .

$$\mathsf{NON}\,(\forall\, x\ P(x)) \iff (\exists\, x\ \mathsf{NON}\ P(x))$$
$$\mathsf{NON}\,(\exists\, x\ P(x)) \iff (\forall\, x\ \mathsf{NON}\ P(x))$$

• Ces deux axiomes sont équivalents car ils se déduisent l'un de l'autre ; ainsi appliquer le premier axiome au prédicat $\mathsf{NON}\ P(x)$ à la place de $P(x)$ puis nier les deux termes de l'équivalence montre le second :

$$\mathsf{NON}\,(\forall\, x\ \mathsf{NON}\ P(x)) \iff (\exists\, x\ P(x))$$
$$\text{puis}\quad (\forall\, x\ \mathsf{NON}\ P(x)) \iff \mathsf{NON}\,(\exists\, x\ P(x))$$

La démonstration réciproque est similaire.

Axiomes de permutation des quantificateurs

• Ces deux axiomes de permutation de deux quantificateurs identiques expriment une équivalence et sont équivalents :

$$(\forall\, x\ \forall\, y\ P(x,y)) \iff (\forall\, y\ \forall\, x\ P(x,y))$$
$$(\exists\, x\ \exists\, y\ P(x,y)) \iff (\exists\, y\ \exists\, x\ P(x,y))$$

• L'axiome suivant énonce que l'existence d'un même x qui convient pour tout y entraîne que pour tout y il existe une valeur de x qui convient :

$$(\exists\, x\ \forall\, y\ P(x,y)) \implies (\forall\, y\ \exists\, x\ P(x,y))$$

• La réciproque est généralement fausse, si pour tout y il existe une valeur possible de x, il n'y a aucune raison pour que cette valeur de x soit indépendante de y.
Pour des variables numériques x et y, la première proposition est vraie en prenant $x = y - 2$ et la seconde fausse car elle aboutit à $0 = 1$ en prenant $y = 0$ et $y = 1$.

$$\forall\, y\ \exists\, x\ y = x + 2 \qquad \exists\, x\ \forall\, y\ y = x + 2$$

Axiomes relatifs aux quantificateurs et aux opérateurs logiques

• Sur le même principe, les deux premiers axiomes d'une part et les deux suivants d'autre part sont équivalents :

$$(\forall\, x\ P(x)\ \mathsf{ET}\ Q(x)) \iff (\forall\, x\ P(x))\ \mathsf{ET}\ (\forall\, x\ Q(x))$$
$$(\exists\, x\ P(x)\ \mathsf{OU}\ Q(x)) \iff (\exists\, x\ P(x))\ \mathsf{OU}\ (\exists\, x\ Q(x))$$
$$(\exists\, x\ P(x)\ \mathsf{ET}\ Q(x)) \implies (\exists\, x\ P(x))\ \mathsf{ET}\ (\exists\, x\ Q(x))$$
$$(\forall\, x\ P(x))\ \mathsf{OU}\ (\forall\, x\ Q(x)) \implies (\forall\, x\ P(x)\ \mathsf{OU}\ Q(x))$$

• La réciproque de la troisième proposition est fausse, il n'y a aucune raison pour que la même valeur de x conviennent pour $P(x)$ et $Q(x)$. La réciproque du dernier axiome est aussi fausse ; l'hypothèse du membre de droite, n'affirme pas que l'un des prédicats $P(x)$ ou $Q(x)$ soit valable pour tout x.

• Les deux assertions suivantes sont mathématiquement équivalentes, la seconde écriture entraîne cependant moins de confusions de lecture que la première et est préférable, car elle n'incite pas à identifier les valeurs indépendantes de x valable pour chaque prédicat :

$$(\exists\, x\ P(x))\ \mathsf{ET}\ (\exists\, x\ Q(x)) \qquad (\exists\, u\ P(u))\ \mathsf{ET}\ (\exists\, v\ Q(v))$$

Ensembles

Ce cours ne présente pas de théorie axiomatique des ensembles qui définit les ensembles uniquement à partir d'axiomes.
Il admet les propositions qui fondent la théorie des ensembles comme l'axiome des parties, l'égalité des ensembles, l'existence de la réunion de deux ensembles, l'axiome de séparation, etc.
Selon la famille d'axiomes retenus pour la théorie des ensembles ces propositions sont des axiomes ou des propriétés, c'est-à-dire des conséquences de axiomes retenus.

Définition des ensembles

Présentation

• La notion d'ensemble est une notion première avec son sens usuel. Plus précisément pour un ensemble E et un objet mathématique a, l'expression $a \in E$ — dite *a appartient à E* — est une assertion, qui est vraie ou fausse selon que a est un élément de E ou non. Le symbole $\notin$ représente la négation de $\in$:

$$\mathsf{NON}\,(a \in E) \iff a \notin E$$

Axiomes de l'égalité

• La notion d'égalité est une notion première qui permet de dire si deux objet mathématiques x et y sont égaux et noté $x = y$, ou non et noté $x \neq y$; ses axiomes sont les suivants :

réflexivité	$\forall\, x$	$x = x$
symétrie	$\forall\, x\ \forall\, y$	$x = y \iff y = x$
transitivité	$\forall\, x\ \forall\, y\ \forall\, z$	$x = y\ \mathsf{ET}\ y = z \implies x = z$
pour tout prédicat $P(x)$	$\forall\, x\ \forall\, y$	$x = y \implies P(x) = P(y)$

• Cette dernière proposition est l'axiome qui justifie les implications comme $x = y \implies 2x = 2y$.

Axiomes d'existence

• L'existence d'ensembles est un axiome.

• Si $a_1, a_2, \cdots, a_n$ sont un nombre fini d'objets mathématiques alors il existe un unique ensemble E contenant exactement ces éléments ; un tel ensemble qui est noté $E = \{a_1, a_2, \cdots, a_n\}$ est dit fini :

$$\forall\, x \quad (x \in E \iff x = a_1\ \mathsf{OU}\ x = a_2\ \mathsf{OU} \cdots \mathsf{OU}\ x = a_n)$$

• Avec cette présentation, la définition précédente des ensembles finis correspond en fait à une notion première ; elle fait intervenir la notion d'énumération finie qui n'a pas été précédemment définie.
Le but de la *théorie des ensembles* est d'éviter de telles ambigüités.

• L'ordre d'énumération des éléments, par commutativité du OU, n'intervient pas dans la définition d'un ensemble.
Pour la même raison un ensemble ne change pas si sa définition contient une ou plusieurs fois un certain élément, mais par convention chaque élément est généralement énuméré qu'une seule fois, comme dans cette seconde égalité :

$$\{a, b\} = \{b, a\} \qquad \{a, b, a, c, a, b\} = \{a, b, c\}$$

$$\begin{aligned} & x \in \{a, b, a, c, a, b\} \\ \iff & x = a\ \mathsf{OU}\ x = b\ \mathsf{OU}\ x = a\ \mathsf{OU}\ x = c\ \mathsf{OU}\ x = a\ \mathsf{OU}\ x = b \\ \iff & x = a\ \mathsf{OU}\ x = b\ \mathsf{OU}\ x = c \\ \iff & x \in \{a, b, c\} \end{aligned}$$

• Un ensemble $\{a\}$ à un seul élément a est appelé singleton.

• Il existe des ensembles qui ne sont pas finis, appelés ensembles infinis.
L'existence d'ensembles infinis est un axiome.
Le premier exemple d'ensemble infini est l'ensemble des entiers $\mathbb{N}$:

$$\mathbb{N} = \{0, 1, 2, 3, 4, \cdots\}$$

Opérations sur les ensembles

Dans la suite E, F, G et H sont des ensembles.

Inclusion

• L'ensemble E est un sous-ensemble de F — *noté $E \subset F$ et aussi $F \supset E$* — si et seulement si tout élément de E est élément de F :

$$\forall\, x \quad x \in E \implies x \in F \qquad \text{abrégé en } \forall\, x \in E\ x \in F$$

Axiome des parties

• Il existe un unique ensemble $\mathcal{P}(E)$ des sous-ensembles X de E, autrement dit :

$$X \in \mathcal{P}(E) \iff X \subset E \qquad \mathcal{P}(E) = \{X \ / \ X \subset E\}$$

Axiome de l'égalité de deux ensembles

• Deux ensembles sont égaux si et seulement s'ils contiennent les mêmes éléments ; ils ont en conséquence les mêmes propriétés :

$$E = F \iff E \subset F\ \mathsf{ET}\ F \subset E \iff (\forall\, x\ x \in E \iff x \in F)$$

• En pratique la démonstration de l'égalité de deux ensembles E et F repose le plus souvent sur la preuve des deux inclusions $E \subset F$ et $F \subset E$.

Axiome de séparation

• Si E est un ensemble et $P(x)$ un prédicat alors il existe un unique sous-ensemble F des éléments x de E vérifiant le prédicat $P(x)$:

$$F = \{x \in E \ / \ P(x)\} \qquad \forall\, x \quad x \in F \iff (x \in E\ \mathsf{ET}\ P(x))$$

Union et intersection d'ensembles

• La réunion et l'intersection de deux ensembles sont les ensembles définis ainsi :

$$E \cup F = \{x \ / \ x \in E\ \mathsf{OU}\ x \in F\} \qquad E \cap F = \{x \ / \ x \in E\ \mathsf{ET}\ x \in F\}$$

• L'existence de l'ensemble constitué de la réunion de deux ensembles est généralement un axiome, mais la construction de l'intersection de deux ensembles peut se faire à partir de l'axiome de séparation appliqué au prédicat $x \in F$:

$$E \cap F = \{x \in E \ / \ x \in F\}$$

Ensemble vide

• Il existe un unique ensemble noté $\emptyset$ ne contenant aucun élément :
$$\forall x \quad x \notin \emptyset$$

• Un ensemble E non vide contient au moins un élément :
$$E \neq \emptyset \iff (\exists x \quad x \in E)$$

• L'existence et l'unicité de l'ensemble vide se déduisent des axiomes précédents.

• Deux ensembles E et F sont dits disjoints si et seulement si $E \cap F = \emptyset$.

Notations avec des quantificateurs

• Les équivalences suivantes sont des abus de notations définis ainsi :
$$\begin{aligned}
(\exists\, x \in E \;\; P(x)) &\iff (\exists\, x \;\; (x \in E \;\mathsf{ET}\; P(x))) \\
(\forall\, x \in E \;\; P(x)) &\iff (\forall\, x \;\; (x \in E \Longrightarrow P(x))) \\
\text{exemple : } E \subset F &\iff (\forall\, x \in E \;\; x \in F) \iff (\forall\, x \;\; (x \in E \Longrightarrow x \in F)) \\
F \not\subset E &\iff (\exists\, x \in E \;\; x \notin F) \iff (\exists\, x \;\; (x \in E \;\mathsf{ET}\; x \notin F))
\end{aligned}$$

• La rédaction d'une preuve de $\forall\, x \in E \;\; P(x)$ commence par « Soit $x \in E$, montrons $P(x)$ ».
Une preuve de $\forall\, x \in E \;\; P(x) \Longrightarrow Q(x)$ se rédige le plus souvent sous la forme « Soit $x \in E$ vérifiant $P(x)$, montrons $Q(x)$ » .

Propriétés élémentaires

Formulaire

• Ce formulaire sur les ensembles est comparable à celui sur les booléens :

Involution	$E \cap E = E \cup E = E$	
Commutativité	$E \cap F = F \cap E$	$E \cup F = F \cup E$
Associativité	$(E \cap F) \cap G = E \cap (F \cap G)$	
	$(E \cup F) \cup G = E \cup (F \cup G)$	
Distributivité	$E \cap (F \cup G) = (E \cap F) \cup (E \cap G)$	
	$E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$	

• La preuve d'une de ces égalités provient de ces équivalences :

$$\begin{aligned}
x \in E \cup F &\iff x \in E \;\mathsf{ET}\; x \in F \\
&\iff x \in F \;\mathsf{ET}\; x \in E \\
&\iff x \in F \cup E \qquad \text{ainsi } E \cup F = F \cup E.
\end{aligned}$$

Propriétés de l'inclusion

• Les premières propriétés de l'inclusion sont celle-ci :
$E \subset E \qquad E \subset F \;\mathsf{ET}\; F \subset G \Longrightarrow E \subset G \qquad E \cap F \subset E \qquad E \subset E \cup F$

• L'inclusion possède de nombreuses autres propriétés :
$$\begin{gathered}
E \subset F \Longrightarrow E \cap G \subset F \cap G \qquad E \subset F \Longrightarrow E \cup G \subset F \cup G \\
E \subset F \iff E \cap F = E \iff E \cup F = F \\
(E \subset F) \;\mathsf{ET}\; (E \subset G) \iff E \subset F \cap G \\
(E \subset G) \;\mathsf{ET}\; (F \subset G) \iff E \cup F \subset G
\end{gathered}$$

• Un paragraphe suivant détaille quelques unes de ces démonstrations.

Propriétés de l'ensemble vide

• Les opérations de base sur l'ensemble vide sont celles-ci :
$$\emptyset \subset E \qquad E \cap \emptyset = \emptyset \qquad E \cup \emptyset = E$$

• Pour tout ensemble E, l'ensemble vide est un élément de l'ensemble des parties de E :
$$\begin{aligned}
\mathcal{P}(\{a,b\}) &= \{\emptyset, \{a\}, \{b\}, \{a,b\}\} \\
\mathcal{P}(\{a,b,c\}) &= \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}
\end{aligned}$$

• Dire que « tous les éléments x de l'ensemble vide vérifient n'importe quel prédicat $P(x)$ » est une assertion mathématiquement vraie.
$$\begin{aligned}
\forall\, x \in \emptyset \quad & P(x) \\
\iff & \forall\, x \quad x \in \emptyset \Longrightarrow P(x) \\
\iff & \forall\, x \quad \mathsf{F} \Longrightarrow P(x) \\
\iff & \forall\, x \quad \mathsf{V} \iff \mathsf{V}
\end{aligned}$$
Par exemple tous les entiers pairs et impairs sont des multiples de trois est une proposition vraie ; l'ensemble des entiers pairs et impairs est l'ensemble vide $E = \emptyset$.

• L'assertion « tout élément x de E vérifie le prédicat P(x) » entraine l'assertion « il existe un élément x de E vérifiant le prédicat P(x) » uniquement si l'ensemble E n'est pas vide.
Cette propriété est fausse pour l'ensemble vide. « Toutes les licornes

sont bleues » est une proposition mathématiquement vraie, mais « il existe une licorne bleue » est une erreur zoologique. *A priori* l'ensemble des licornes est vide...

Différence de deux ensembles

• La définition et les propriétés de la différence de deux ensembles sont celles-ci :

$$E \setminus F = \{x \ / \ x \in E \ \mathsf{ET} \ x \notin F\} \qquad E \setminus \emptyset = E \qquad E \setminus E = \emptyset$$
$$E \setminus (F \cap G) = (E \setminus F) \cup (E \setminus G) \qquad E \setminus (F \cup G) = (E \setminus F) \cap (E \setminus G)$$

Complémentaire

• Le complémentaire d'un ensemble F ou G par rapport à E suppose que $F \subset E$ et $G \subset E$:

$$\complement_E F = E \setminus F \qquad \complement_E(\complement_E F) = F \qquad F \subset G \Longleftrightarrow \complement_E G \subset \complement_E F$$

Exemples de démonstrations sur les ensembles

• Ce premier exemple prouve la transitivité de l'inclusion :

$$E \subset F \ \mathsf{ET} \ F \subset G \implies E \subset G$$

La démonstration de cette implication suppose ces deux hypothèses :

$$E \subset F \quad \text{c'est-à-dire} \quad \forall x \in E \quad x \in F$$
$$F \subset G \quad \text{c'est-à-dire} \quad \forall y \in F \quad x \in G$$

Cette preuve consiste à justifier la propriété suivante à partir des hypothèses précédentes :

$$E \subset G \quad \text{c'est-à-dire} \quad \forall u \in E \ u \in G$$

La suite de la démonstration commence donc par le quantificateur $\forall$, elle se rédige ainsi.
Soit $u \in E$; la première hypothèse est valable pour tout $u \in E$, et en particulier pour $x = u \in E$, donc $u \in F$. De même la deuxième hypothèse est valable pour tout $y \in F$, et en particulier pour $y = u \in F$, ainsi $u \in G$.
En conclusion tout élément $u \in E$ appartient à G, et $E \subset G$.

• Cet exemple illustre la démonstration de la propriété suivante :

$$E \subset F \implies E \cap G \subset F \cap G$$

La preuve d'une implication consiste à supposer la partie gauche de l'implication pour justifier la partie droite, et la preuve d'une inclusion,

à prouver que tout élément du petit ensemble est dans le grand.
Cette démonstration commence donc par supposer $E \subset F$ pour montrer l'inclusion $E \cap G \subset F \cap G$.
Soit $x \in E \cap G$, alors $x \in E$ et $x \in G$. L'hypothèse $E \subset F$ associée à $x \in E$ entraîne $x \in F$; en outre par hypothèse $x \in G$, et ainsi $x \in F \cap G$. Les arguments précédents justifient cette implication traduisant l'inclusion recherchée lorsque $E \subset F$:

$$\forall x \quad x \in E \cap G \implies x \in F \cap G \quad \text{c'est-à-dire} \quad E \cap G \subset F \cap G$$

• Les preuves de ces équivalences appliquent les mêmes méthodes :

$$E \subset F \Longleftrightarrow E \cap F = E \Longleftrightarrow E \cup F = F$$

Trois implications circulaires permettent de montrer ces équivalences.
La démonstration de $E \subset F \implies E \cap F = E$ consiste à supposer $E \subset F$ et à prouver les deux inclusions $E \cap F \subset E$ et $E \subset E \cap F$.
La première inclusion $E \cap F \subset E$ correspond à une propriété usuelle de l'inclusion.
Réciproquement si $x \in E$ alors $x \in F$ car $E \subset F$, donc $x \in E \cap F$.
En conclusion $E \subset F \implies E \cap F = E$.
La justification de $E \cap F = E \implies E \cup F = F$ est comparable, et suppose $E \cap F = E$ pour justifier $F \subset E \cup F$ et $E \cup F \subset F$.
La première inclusion $F \subset E \cup F$ correspond aussi à une propriété usuelle.
Réciproquement, soit $x \in E \cup F$, deux cas sont possibles $x \in E$ ou $x \in F$. Dans le premier cas $x \in E = E \cap F$ par hypothèse, et l'inclusion $E \cap F \subset F$ justifie $x \in F$. Dans le second $x \in F$ par construction.
Donc tout $x \in E \cup F$ vérifie, dans tous ces cas, $x \in F$; ceci termine la preuve de l'implication $E \cap F = E \implies E \cup F = F$.
La preuve de $E \cup F = F \implies E \subset F$ s'obtient directement à partir de l'inclusion élémentaire $E \subset E \cup F = F$.

Couples et produit cartésien

• Le couple (x, y) où x est appelé la première coordonnée et y la seconde est un objet mathématique soumi à la condition suivante :

$$(x, y) = (z, t) \Longleftrightarrow x = z \ \mathsf{ET} \ y = t$$

Cette définition s'étend aux triplets (x, y, z) et n-uplets $(x_1, x_2, \cdots, x_n)$.

• Le produit cartésien $E \times F$ est l'ensemble des couples (x, y) avec

$x \in E$ et $y \in F$:

$$E \times F = \{(x,y) \ / \ x \in E \ \mathsf{ET} \ y \in F\}$$
$$\{a,b,c\} \times \{1,2\} = \{(a,1),(a,2),(b,1),(b,2),(c,1),(c,2)\}$$

• Cette notion se généralise aux produits de trois, quatre, etc. ensembles.
Les produits cartésiens du même ensemble E sont notés $E^2 = E \times E$, $E^3 = E \times E \times E$, etc.

• Le produit cartésien vérifie ces égalités :

$(E \cup F) \times G = (E \times G) \cup (F \times G) \quad (E \cap F) \times G = (E \times G) \cap (F \times G)$
$E \times (F \cup G) = (E \times F) \cup (E \times G) \quad E \times (F \cap G) = (E \times F) \cap (E \times G)$

$$E \subset G \ \mathsf{ET} \ F \subset H \Longrightarrow E \times F \subset G \times H$$

• Le produit cartésien $E \times F$ n'est pas vide si et seulement s'il contient un couple (x,y) d'un élément $x \in E$ et $y \in F$:

$$E \times F = \emptyset \Longleftrightarrow E = \emptyset \ \mathsf{OU} \ F = \emptyset$$

• Cette condition relative à un produit cartésien vide entraîne que la réciproque de la dernière implication sur les inclusions est fausse :

$$\emptyset \times \{1,2,3\} = \emptyset \subset \{a,b\} \times \{1,a\} \ \mathsf{ET} \ \{1,2,3\} \not\subset \{1,a\}$$

Applications

Définition et premières propriétés

• Une application f de E dans F fait correspondre à chaque élément x de E un et un seul élément noté $f(x)$ de F. Le graphe de l'application est l'ensemble G qui vérifie ces propriétés :

$$\begin{array}{l} f : E \longrightarrow F \\ \quad x \longmapsto f(x) \end{array} \qquad G = \{(x, f(x)) \ / \ x \in E\}$$
$$\forall x \in E \ \exists ! y \in F \ (x,y) \in G$$

• E est appelé ensemble de départ, F ensemble d'arrivée, $f(x) \in F$ est l'image de $x \in E$ par f, et un antécédent de $y \in F$ est un élément $x \in E$ tel que $y = f(x)$.

• Deux applications f et g sont égales si et seulement si elles ont même ensemble de départ E, même ensemble d'arrivée, et même graphe ce qui correspond à $\forall x \in E \ f(x) = g(x)$.

• L'ensemble des applications de E dans F est notée F^E.

• Une application de E dans E est appelée application sur E.

• L'application identité sur E est définie de E dans E par $\mathrm{Id}_E : x \mapsto x$.

Restriction et prolongement

• Si l'application f est définie à partir d'un ensemble de départ E et si F est un sous-ensemble de E alors la restriction de f à F est l'application $f_{/F}$ définie sur F qui prend les mêmes valeurs que f :

$$F \subset E \qquad \begin{array}{l} f : E \longrightarrow \mathbb{R} \\ \quad x \longmapsto f(x) \end{array} \qquad \begin{array}{l} f_{/F} : F \longrightarrow \mathbb{R} \\ \quad x \longmapsto f_{/F}(x) = f(x) \end{array}$$

• Lorsque l'ensemble E est contenu dans l'ensemble G, l'application g dont l'ensemble de départ est G est un prolongement de f défini à partir de E si et seulement si f est la restriction de g à E :

$$E \subset G \qquad g_{/E} = f \qquad \forall x \in E \quad f(x) = g(x)$$

La suite de ce cours suppose que les ensembles de départ et d'arrivée ne sont pas vides.

• Plusieurs applications peuvent être un prolongement d'une même fonction, mais une restriction est nécessairement unique.

Application composée

Dans ce paragraphe les applications f, g et h sont supposées définies par $f : E \to F$, $g : F \to G$ et $h : G \to H$.

• L'application $g \circ f$ de E dans G est définie pour tout $x \in E$ par $(g \circ f)(x) = g(f(x))$. L'opérateur $\circ$ est appelé opérateur de composition des applications :

$$\begin{array}{l} g \circ f : E \longrightarrow G \\ \quad x \longmapsto (g \circ f)(x) = g(f(x)) \end{array}$$

• La composition des applications est associative, elle vérifie ces propriétés et suit ces notations :

$$(h \circ g) \circ f = h \circ (g \circ f) \qquad f \circ \mathrm{Id}_E = \mathrm{Id}_F \circ f = f$$
$$f^2 = f \circ f \qquad f^3 = f^2 \circ f = f \circ f^2 = f \circ f \circ f \qquad \text{etc., lorsque } E = F$$

• L'associativité provient de ces égalités issues de la définition même de la composition des applications pour tout $x \in E$:

$$((h\circ g)\circ f)(x) = (h\circ g)(f(x)) = (h(g(f(x))$$
$$= h((g\circ f)(x)) = (h\circ(g\circ f))(x)$$

Image directe et image réciproque

Dans ce paragraphe $f : E \to F$, A, A_1 et A_2 sont des sous-ensembles de E, et B, B_1 et B_2 des sous-ensembles de F.

Définitions et premières propriétés

• L'image directe $f(A)$ de A par f est l'ensemble des images des éléments de A par f :

$$f(A) = \{y\in F \;/\; \exists\, a\in A \;\; y = f(a)\} = \{f(a) \;/\; a\in A\} \subset F$$
$$y\in f(A) \Longleftrightarrow \exists\, a\in A \;\; f(a) = y$$

• En particulier tout élément $a\in A$ vérifie $f(a)\in f(A)$.

• Par définition l'image de f est $\operatorname{Im} f = f(E) \subset F$ est le sous-ensemble des éléments de f qui possède au moins un antécédent par f.

• L'image réciproque $f^{-1}(B)$ de B par f est l'ensemble des antécédents des éléments de B par f :

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

La dernière équivalence est la méthode usuelle de preuve de $x\in f^{-1}(B)$.

• Ces exemples illustrent les définitions précédentes :

$$f : \mathbb{Z} \longrightarrow \mathbb{Z},\; n \longmapsto |n| \qquad f^{-1}(\{1,2\}) = \{-1,1,-2,2\} \qquad f^{-1}(\{-1,-2\}) = \emptyset$$

• Les premières propriétés des images directes et des images réciproques sont les suivantes :

$$f(\emptyset) = \emptyset \qquad f^{-1}(\emptyset) = \emptyset$$
$$f(E) = \operatorname{Im} f \subset F \qquad f^{-1}(F) = E$$
$$A_1 \subset A_2 \Longrightarrow f(A_1) \subset f(A_2) \quad B_1 \subset B_2 \Longrightarrow f^{-1}(B_1) \subset f^{-1}(B_2)$$

• Les images directes et réciproques de l'ensemble vide peuvent se démontrer à partir de la définition de l'ensemble vide ou être considérées comme des conventions cohérentes.

• Les inclusions entre les images directes et les images réciproques sont les suivantes :

$$A \subset f^{-1}(f(A)) \qquad f(f^{-1}(B)) \subset B$$

• Les preuves exploitent uniquement les définitions de ces ensembles. Si $x\in A$ alors $f(x)\in f(A)$ ce qui correspond à $x\in f^{-1}(f(A))$. Ces deux arguments terminent la démonstration de $A \subset f^{-1}(f(A))$.
La propriété $y\in f(f^{-1}(B))$ équivaut à l'existence de $x\in f^{-1}(B)$ vérifiant $f(x) = y$. La définition de l'image réciproque justifie que $f(x)\in B$, en conclusion $y = f(x)\in B$ ce qui prouve $f(f^{-1}(B)) \subset B$.

• L'exemple ci-dessous vérifie que ces ensembles ne sont pas nécessairement égaux :

$$f : \mathbb{Z} \longrightarrow \mathbb{Z},\; n \longmapsto |n| \qquad f(f^{-1}(\{-2,1\})) = f(\{-1,1\}) = \{1\} \subset \{-2,1\}$$
$$f^{-1}(f(\{-2,1\})) = \{-1,1,-2,2\} \supset \{-2,1\}$$

Intersections et réunions

• Les intersections et réunions des images réciproques vérifient cette inclusion et ces égalités :

$$f(A_1\cap A_2)\subset f(A_1)\cap f(A_2) \quad f^{-1}(B_1\cap B_2)=f^{-1}(B_1)\cap f^{-1}(B_2)$$
$$f(A_1\cup A_2)=f(A_1)\cup f(A_2) \quad f^{-1}(B_1\cup B_2)=f^{-1}(B_1)\cup f^{-1}(B_2)$$

• Ces équivalences démontrent $f^{-1}(B_1\cup B_2) = f^{-1}(B_1)\cup f^{-1}(B_2)$:

$$x\in f^{-1}(B_1\cup B_2) \Longleftrightarrow f(x)\in B_1\cup B_2$$
$$\Longleftrightarrow f(x)\in B_1 \;\mathsf{OU}\; f(x)\in B_2$$
$$\Longleftrightarrow x\in f^{-1}(B_1) \;\mathsf{OU}\; x\in f^{-1}(B_2)$$
$$\Longleftrightarrow x\in f^{-1}(B_1)\cup f^{-1}(B_2)$$

Remplacer OU par ET dans cette démonstration prouve l'égalité pour l'intersection.

• Ces équivalences montrent l'égalité des images directes d'une réunion :

$$y\in f(A_1\cup A_2) \Longleftrightarrow (\exists\, x\in A_1\cup A_2 \;\; y = f(x))$$
$$\Longleftrightarrow (\exists\, x \;\; x\in A_1\cup A_2 \;\mathsf{ET}\; y = f(x))$$
$$\Longleftrightarrow (\exists\, x \;\; (x\in A_1 \;\mathsf{OU}\; x\in A_2) \;\mathsf{ET}\; y = f(x))$$
$$\Longleftrightarrow (\exists\, x \;\; (x\in A_1 \;\mathsf{ET}\; y = f(x)) \;\mathsf{OU}\; (x\in A_2 \;\mathsf{ET}\; y = f(x)))$$
$$\Longleftrightarrow (\exists\, x \;\; x\in A_1 \;\mathsf{ET}\; y = f(x)) \;\mathsf{OU}\; (\exists\, x\in A_2 \;\mathsf{ET}\; y = f(x)))$$
$$\Longleftrightarrow y\in f(A_1) \;\mathsf{OU}\; y\in f(A_2)$$
$$\Longleftrightarrow y\in f(A_1)\cup f(A_2) \qquad f(A_1\cup A_2) = f(A_1)\cup f(A_2)$$

• Au contraire, la démonstration suivante justifie, par une implication,

l'inclusion relative à l'image directe d'une intersection :

$$\begin{aligned}
& y \in f(A_1 \cap A_2) \\
\iff & (\exists\, x \in A_1 \cap A_2 \;\; y = f(x)) \\
\iff & (\exists\, x \;\; x \in A_1 \cap A_2 \;\mathsf{ET}\; y = f(x)) \\
\iff & (\exists\, x \;\; (x \in A_1 \;\mathsf{ET}\; x \in A_2) \;\mathsf{ET}\; y = f(x)) \\
\iff & (\exists\, x \;\; (x \in A_1 \;\mathsf{ET}\; y = f(x)) \;\mathsf{ET}\; (x \in A_2 \;\mathsf{ET}\; y = f(x))) \\
\underline{\Longrightarrow} & (\exists\, x \;\; x \in A_1 \;\mathsf{ET}\; y = f(x)) \;\mathsf{ET}\; (\exists\, x \in A_2 \;\mathsf{ET}\; y = f(x))) \\
\iff & y \in f(A_1) \;\mathsf{ET}\; y \in f(A_2) \\
\iff & y \in f(A_1) \cap f(A_2) \qquad f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)
\end{aligned}$$

• Ces deux démonstrations reposent essentiellement sur les axiomes relatifs au quantificateur $\exists$ et aux opérateurs OU et ET ; l'axiome du OU comporte une équivalence et justifie l'égalité des ensembles, celui du ET énonce une implication et prouve une inclusion :

$$(\exists\, x \;\; (P(x) \;\mathsf{OU}\; Q(x))) \iff (\exists\, x \;\; P(x)) \;\mathsf{OU}\; (\exists\, x \;\; Q(x))$$
$$(\exists\, x \;\; (P(x) \;\mathsf{ET}\; Q(x))) \implies (\exists\, u \;\; P(u)) \;\mathsf{ET}\; (\exists\, v \;\; Q(v))$$

Réciproquement l'existence de u et de v n'entraine pas $u = v$ et n'implique pas l'existence de x.

• L'exemple suivant illustre une inclusion stricte :

$$\begin{array}{ll}
f : \mathbb{Z} \longrightarrow \mathbb{Z} & f(\{1,2,4\} \cap \{-2,1,3\}) = f(\{1\}) = \{1\} \\
\quad n \longmapsto |n| & f(\{1,2,4\}) \cap f(\{-2,1,3\}) = \{1,2,4\} \cap \{1,2,3\} = \{1,2\}
\end{array}$$

Étude d'un exemple

• La démonstration suivante justifie l'égalité $f(A \cap f^{-1}(B)) = f(A) \cap B$ avec les notations précédentes.
Cette preuve démontre les deux inclusions $f(A \cap f^{-1}(B)) \subset f(A) \cap B$ et $f(A) \cap B f(A \cap f^{-1}(B))$.
La justification la plus directe de la première inclusion exploite les propriétés élémentaires déjà énoncées :

$$f(A \cap f^{-1}(B)) \subset f(A) \cap f(f^{-1}(B)) \subset f(A) \cap B$$

Une démonstration faisant intervenir un élément $y \in f(A \cap f^{-1}(B))$ pour justifier que $x \in f(A) \cap B$ est aussi possible.
La preuve de l'inclusion réciproque suppose $y \in f(A) \cap B$, ainsi il existe $a \in A$ tel que $f(a) = y$ et $y \in B$. Par conséquent $f(a) \in B$ et $a \in f^{-1}(B)$

par définition de l'image réciproque.
En conclusion $a \in A \cap f^{-1}(B)$ et $y = f(a) \in f(A \cap f^{-1}(B))$.

Applications injectives et surjectives

Applications injectives

• L'application $f : E \to F$ est injective si et seulement si tout élément de l'ensemble d'arrivée a au maximum un antécédent :

$$\forall\, (u,v) \in E^2 \quad f(u) = f(v) \implies u = v$$

Autrement dit si les images de deux éléments sont identiques alors ces éléments sont égaux.

• La condition suivante est équivalente à la définition précédente, par contraposée, et correspond plus directement à la définition précédente :

$$\forall\, (u,v) \in E^2 \quad u \neq v \implies f(u) \neq f(v)$$

Cette implication est cependant d'un emploi plus difficile car les propriétés de l'égalité sont plus nombreuses que celles des différences, ainsi $2 \times 2 = 4 = 3 + 1$ justifie $2 \times 2 = 3 + 1$, mais l'abus de notation $0 \neq 1 \neq 2 \neq 0$ ne permet pas de conclure $0 \neq 0$.

• Une application n'est pas injective lorsqu'un élément possède au moins deux antécédents différents :

$$\exists\, (u,v) \in E^2 \quad u \neq v \;\mathsf{ET}\; f(u) = f(v)$$

Cette propriété correspond à la négation des deux propositions contraposées précédentes.

• L'injection canonique j de $F \subset E$ dans E est définie ainsi :

$$\begin{array}{c}
j : F \longrightarrow E \\
x \longmapsto x
\end{array}$$

Applications surjectives

• L'application $f : E \to F$ est surjective si et seulement si tout élément de l'ensemble d'arrivée a au minimum un antécédent :

$$\forall\, y \in F \;\exists\, x \in E \quad y = f(x) \qquad \text{c'est-à-dire } \operatorname{Im} f = F$$

• Une application n'est pas surjective si et seulement si un élément de l'ensemble d'arrivée ne possède pas d'antécédent, ou dit autrement, l'ensemble des antécédents d'un certain élément est vide :

$$\exists\, y \in F \quad \forall\, x \in E \quad f(x) \neq y \qquad \exists\, y \in F \quad f^{-1}(y) = \emptyset$$

• Toute application $f : E \to F$ peut être considérée comme une application surjective de E dans $\operatorname{Im} f = f(E)$.
L'image $f(x)$ de tout élément $x \in E$ est dans $\operatorname{Im} f = f(E)$, et donc l'application est bien définie de E dans $\operatorname{Im} f$.
Tout élément y de $\operatorname{Im} f$ est de la forme $y = f(x)$ avec $x \in E$ et a au moins un antécédent x par f.

Propriétés

• L'application constante $f : x \mapsto 1$ définie sur $\mathbb{N}$ n'est ni surjective car 0 n'a pas d'antécédent, ni injective car $f(0) = f(1)$.

La suite de ce paragraphe suppose $f : E \to F$ et $g : F \to G$.

• La composée de deux applications injectives est injective.
La composée de deux applications surjectives est surjective.

• Si la composée $g \circ f$ est injective alors f est injective.
Si la composée $g \circ f$ est surjective alors g est surjective.

• La contraposée de la première de ces deux implications énonce que si f n'est pas injective alors $g \circ f$ n'est pas injective.
S'il existe $(u, v) \in E^2$ tel que $u \neq v$ et $f(u) = f(v)$ alors $g(f(u)) = g(f(v))$ et donc $(g \circ f)(u) = (g \circ f)(v)$.

• La contraposée de la seconde implication énonce que si g n'est pas surjective alors $g \circ f$ n'est pas surjective.
Si $z \in G$ n'a pas d'antécédent par g alors z n'est pas de la forme $z = g(y)$ et ne peut pas être de la forme $z = (g \circ f)(x)$.

• L'application f est injective si et seulement s'il existe une application $\varphi : F \to E$ vérifiant $\varphi \circ f = \mathrm{Id}_E$.
L'application f est surjective si et seulement s'il existe une application $\psi : F \to E$ vérifiant $f \circ \psi = \mathrm{Id}_F$.

Démonstrations des propriétés

• Montrer que l'application $g \circ f$ est injective dès que les applications f et g sont injectives consiste à vérifier cette proposition :

$$\forall\, (u, v) \in E^2 \quad (g \circ f)(u) = (g \circ f)(v) \Longrightarrow u = v$$

Soit $(u, v) \in E^2$ vérifiant $(g \circ f)(u) = (g \circ f)(v)$; cette hypothèse correspond à $g(f(u)) = g(f(v))$. L'hypothèse g injective entraîne $f(u) = f(v)$. Puis l'hypothèse f injective implique $u = v$, ce qui termine la preuve.

• La preuve que l'application $g \circ f$ est surjective lorsque les applications f et g sont surjectives démontre cette propriété :

$$\forall\, z \in G \quad \exists\, x \in E \quad (g \circ f)(x) = z$$

Soit $z \in G$, l'hypothèse que g est surjective énonce qu'il existe $y \in F$ vérifiant $z = g(y)$. De même l'hypothèse que g est surjective justifie l'existence de $x \in E$ tel que $y = f(x)$.
En conclusion il existe $x \in E$ vérifiant $z = g(f(x)) = (g \circ f)(x)$.

• Cette preuve démontre que f est injective dès que $g \circ f$ est injective.
Soit $(u, v) \in E^2$ vérifiant $f(u) = f(v)$, et donc $g(f(u)) = g(f(v))$ et $(g \circ f)(u) = (g \circ f)(v)$; l'hypothèse que $g \circ f$ est injective justifie $u = v$.

• Les arguments suivants justifient que l'application g est surjective lorsque l'application $g \circ f$ est surjective.
Soit $z \in G$, l'élément z possède un antécédent x par l'application surjective $g \circ f$, ainsi $z = (g \circ f)(x) = g(f(x))$ et $f(x)$ est un antécédent de z par g. En conclusion tout élément de G possède un antécédent par g et l'application g est surjective.

• L'application Id_E est injective : $\mathrm{Id}_E(x) = \mathrm{Id}_E(y) \Longrightarrow x = y$.
S'il existe une application φ vérifiant $\varphi \circ f = \mathrm{Id}_E$ alors la propriété précédente justifie que l'application f est injective.
Réciproquement si l'application f est injective, il suffit de construire une application φ vérifiant $\varphi \circ f = \mathrm{Id}_E$. L'ensemble E est supposé non vide et contient donc au moins un élément $a \in E$
Soit $y \in G$, deux cas sont possibles $y \in \operatorname{Im} f$ ou $y \notin \operatorname{Im} f$.
Dans le premier cas si $y \in \operatorname{Im} f$ alors y possède exactement un antécédent $x_y \in E$ par f, au moins un car $y \in \operatorname{Im} f$ et au plus un car f est injective. Dans ce cas l'image de y par φ est $\varphi(y) = x_y$.
Dans le second cas $\varphi(y) = a$.
L'application φ est donc bien définie par l'image de chaque élément de F et vérifie $(\varphi \circ f)(x) = \varphi(f(x)) = x$ pour tout $x \in E$ car le seul antécédent de $f(x) \in \operatorname{Im} f$ par f est $x = \varphi(f(x))$. En conclusion l'application φ vérifie $\varphi \circ f = \mathrm{Id}_E$.

• L'application Id_F est surjective : tout élément $y \in F$ a un antécédent, lui-même, car $\mathrm{Id}_F(y) = y$.
S'il existe une application ψ vérifiant $f \circ \psi = \mathrm{Id}_F$ alors la propriété précédente justifie que l'application f est surjective.

Réciproquement si l'application f est surjective, il suffit de construire une application ψ vérifiant $f \circ \psi = \mathrm{Id}_F$. Tout élément $y \in F$ possède au moins un antécédent : $\exists\, x \in E\ f(x) = y$.
L'application ψ associe à chaque $y \in F$ un de ses antécédents x, et vérifie donc $(f \circ \psi)(y) = f(\psi(y)) = f(x) = y$. Comme expliqué à la fin de ce chapitre cette propriété fait intervenir l'axiome du choix.

Applications bijectives

• Une application $f : E \to F$ est bijective si et seulement si tout élément de F possède exactement un antécédent : elle est injective et surjective.

• L'application f est bijective si et seulement si elle vérifie ces conditions :

$$\left\{ \begin{array}{ll} & \exists\, \varphi : F \to E \quad \varphi \circ f = \mathrm{Id}_E \\ \mathsf{ET} & \exists\, \psi : F \to E \quad f \circ \psi = \mathrm{Id}_F \end{array} \right.$$

Dans ce cas les applications φ et ψ sont uniques et égales.
Elles définissent l'application réciproque $f^{-1} = \varphi = \psi$.

• L'application réciproque d'une application bijective f est donc l'application qui à $y \in F$ associe l'unique antécédent $x \in E$ de y.

• L'équivalence précédente consiste à appliquer les deux propositions correspondantes relatives aux applications injectives et surjectives.
La preuve de l'unicité de φ suppose que les applications φ_1 et φ_2 conviennent et démontre $\varphi_1 = \varphi_2$:

$$\begin{aligned} \varphi_1 = \varphi_1 \circ \mathrm{Id}_F = \varphi_1 \circ (f \circ \psi) = (\varphi_1 \circ f) \circ \psi \\ = \mathrm{Id}_E \circ \psi = (\varphi_2 \circ f) \circ \psi = \varphi_2 \circ (f \circ \psi) = \varphi_2 \circ \mathrm{Id}_F = \varphi_2 \end{aligned}$$

L'application φ est donc unique, et la méthode est la même pour ψ :

$$\psi_1 = \varphi \circ f \circ \psi_1 = \varphi = \varphi \circ f \circ \psi_2 = \psi_2$$

Ainsi les applications φ et ψ sont uniques et égales.

• L'application Id_E est bijective ; si les applications f et g sont bijectives alors f^{-1} et $g \circ f$ sont bijectives et vérifient ces égalités :

$$f^{-1} \circ f = \mathrm{Id}_E \qquad f \circ f^{-1} = \mathrm{Id}_F$$

$$\mathrm{Id}_E^{-1} = \mathrm{Id}_E \qquad (f^{-1})^{-1} = f \qquad (g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

• La démonstration consiste à appliquer les équivalences précédentes.
Ainsi l'égalité $\mathrm{Id}_E \circ \mathrm{Id}_E = \mathrm{Id}_E$ est de la forme $\varphi \circ f = f \circ \psi = \mathrm{Id}_E$

avec $f = \mathrm{Id}_E = \varphi = \psi$; le théorème précédent s'applique et énonce que l'identité est bijective et d'application réciproque $\mathrm{Id}_E^{-1} = \mathrm{Id}_E$.
De même les deux égalités $f^{-1} \circ f = \mathrm{Id}_E$ et $f \circ f^{-1} = \mathrm{Id}_F$ sont valables dès que l'application f est bijective ; le fait que l'application f^{-1} vérifie ces égalités justifie alors que f^{-1} est bijective et que $(f^{-1})^{-1} = f$.
Les deux égalités suivantes prouvent bien que $g \circ f$ est bijective dès que f et g sont bijectives :

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ \mathrm{Id}_F \circ g^{-1} = g \circ g^{-1} = \mathrm{Id}_G$$
$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ \mathrm{Id}_G \circ f = f^{-1} \circ f = \mathrm{Id}_E$$

• L'ensemble des applications bijectives sur E est noté $\mathcal{S}_E$.

• Une involution est une application sur un ensemble telle que $f^2 = \mathrm{Id}$: dans ce cas $f^{-1} = f$.

• Dans le cas où l'application f est bijective, il suffit de vérifier l'une des deux égalités $g \circ f = \mathrm{Id}_E$ ou $f \circ g = \mathrm{Id}_F$ pour montrer que $f^{-1} = g$.

• Si l'application f est bijective alors l'application f^{-1} est bien définie et l'associativité de la composition aboutit à $f^{-1} = g$:

$$f^{-1} = \mathrm{Id}_E \circ f^{-1} = (g \circ f) \circ f^{-1} = g \circ (f \circ f^{-1}) = g \circ \mathrm{Id}_F = g$$

La démonstration est similaire lorsque $f \circ g = \mathrm{Id}_F$.

• La condition $f \circ g = \mathrm{Id}_F$ n'entraîne pas que f ou g est bijective.
Par exemple les applications f et g suivantes vérifient $g \circ f = \mathrm{Id}_{\mathbb{N}}$ et ni f ni g ne sont bijectives :

$$\begin{array}{ll} f : \mathbb{N} \longrightarrow \mathbb{N} & g : \mathbb{N} \longrightarrow \mathbb{N} \\ \quad n \longmapsto n+1 & \quad n \longmapsto \max(0, n-1) \end{array} \qquad (g \circ f)(n) = g(n+1) = n$$

L'application g est surjective sans être injective car 0 a deux antécédents : $g(0) = g(1) = 0$.
L'application f est injective sans être surjective car 0 n'a pas d'antécédents. L'application $f \circ g$ n'est pas l'identité car $(f \circ g)(0) = f(0) = 1 \neq 0$.

• Si l'application f est injective de E dans F, alors l'application f étudiée de E dans $\mathrm{Im}\, f$ est bijective.

Applications et ensemble vide

• Pour toute application f l'image réciproque de l'ensemble vide est l'ensemble vide ; la preuve provient de la définition $x \in \emptyset \iff \mathsf{F}$ de l'ensemble vide :

$$\begin{aligned} x \in f^{-1}(\emptyset) &\iff f(x) \in \emptyset \\ &\iff \mathsf{F} \\ &\iff x \in \emptyset \qquad f^{-1}(\emptyset) = \emptyset \end{aligned}$$

• Pour toute application f l'image directe de l'ensemble vide est l'ensemble vide. La démonstration repose sur le fait que toute implication $\mathsf{F} \Longrightarrow \cdots$ est vraie, et sur l'équivalence $x \in \emptyset \iff \mathsf{F}$:

$$\begin{aligned} y \in f(\emptyset) &\iff (\exists\, x \in \emptyset \;\; f(x) = y) \\ &\iff (\exists\, x \quad x \in \emptyset \;\mathsf{ET}\; f(x) = y) \\ &\iff (\exists\, x \quad \mathsf{F} \;\mathsf{ET}\; f(x) = y) \\ &\iff \mathsf{F} \\ &\iff y \in \emptyset \qquad\qquad f(\emptyset) = \emptyset \end{aligned}$$

• Il n'existe aucune application d'un ensemble E non vide dans l'ensemble vide $\emptyset$.

• Il existe une application $f : \emptyset \to E$ de l'ensemble vide $\emptyset$ dans un ensemble E quelconque.
Le graphe de f est l'ensemble vide et l'application f est injective.
Si en outre $E = \emptyset$, alors $f : \emptyset \to \emptyset$ est bijective.

Familles d'ensembles

Dans ce paragraphe $(E_i)_{i\in\mathcal{I}}$ est une famille d'ensembles indexée par $\mathcal{I} \neq \emptyset$, c'est-à-dire qu'à tout $i \in \mathcal{I}$ est associé un ensemble noté E_i.

Réunion et intersection

• La réunion et l'intersection de la famille d'ensembles $(E_i)_{i\in\mathcal{I}}$ sont les ensembles suivants :

$$\bigcup_{i\in\mathcal{I}} E_i = \{x \;/\; \exists\, i \in I \;\; x \in E_i\} \qquad \bigcap_{i\in\mathcal{I}} E_i = \{x \;/\; \forall\, i \in I \;\; x \in E_i\}$$

Les propriétés démontrées pour l'intersection, la réunion et l'inclusion de deux ensembles se généralisent aux familles d'ensembles.

• Ainsi les deux définitions de la réunion sont équivalentes pour les familles finis d'ensembles :

$$\begin{aligned} x \in E_1 \cup E_2 &\iff (x \in E_1)\; \mathsf{OU}\; (x \in E_2) \\ &\iff (\forall\, i \in \{1,2\} \;\; x \in E_i) \\ &\iff x \in \bigcup_{i\in\{1,2\}} E_i \end{aligned}$$

• Ces exemples illustrent les définitions précédentes :

$$\bigcup_{n\in\mathbb{N}^*} [1/n,\, n] = \bigcup_{n\in\mathbb{N}^*}]1/n,\, n[= \mathbb{R}_+^*$$

$$\bigcap_{n\in\mathbb{N}^*} [1 - 1/n,\, 2 + 1/n] = \bigcap_{n\in\mathbb{N}^*}]1 - 1/n,\, 2 + 1/n[= [1,\, 2]$$

• La démonstration de la première égalité repose sur deux inclusions dont la première se justifie ainsi :

$$\forall\, n \in \mathbb{N}^* \quad [1/n,\, n] \subset \mathbb{R}_+^* \quad \text{donc} \quad \bigcup_{n\in\mathbb{N}^*} [1/n,\, n] \subset \mathbb{R}_+^*$$

$$\text{sur le principe de} \quad E \subset G \;\mathsf{ET}\; F \subset G \Longrightarrow E \cup F \subset G$$

L'inclusion réciproque provient des encadrement suivants :
Soit $x \in \mathbb{R}_+^*$; d'une part $p = \mathrm{E}(x) + 1 \in \mathbb{N}^*$ vérifie $p \geq x$.
D'autre part $q = \mathrm{E}(1/x) + 1 \in \mathbb{N}^*$ vérifie $q \geq 1/x > 0$ donc $0 < 1/q \leq x$.
Cet encadrement termine la preuve de l'inclusion où $m = \max(p, q) \in \mathbb{N}^*$:

$$0 < 1/m \leq 1/q \leq x \leq p \leq m \qquad x \in [1/m,\, m] \subset \bigcup_{n\in\mathbb{N}^*} [1/n,\, n]$$

$$\mathbb{R}_+^* \subset \bigcup_{n\in\mathbb{N}^*} [1/n,\, n]$$

Les démonstrations des autres égalités sont similaires.

• Une partition de E est une famille $(E_i)_{i\in\mathcal{I}}$ ou un ensemble de sous-ensembles non vides et disjoints deux à deux de E dont la réunion est E :

$$\begin{aligned} &\forall\, i \in \mathcal{I} \quad E_i \neq \emptyset \\ &\bigcup_{i\in\mathcal{I}} E_i = E \\ &\forall\, (i,j) \in \mathcal{I}^2 \quad i \neq j \Longrightarrow E_i \cap E_j = \emptyset \end{aligned}$$

• L'intersection n'est pas définie si $\mathcal{I} = \emptyset$, et par convention cohérente une réunion d'indicée par l'ensemble vide est l'ensemble vide :

$$x\in\bigcup_{i\in\emptyset}E_i\iff\exists\,i\in\emptyset\quad x\in E_i$$
$$\iff\exists\,i\quad i\in\emptyset\ \mathsf{ET}\ x\in E_i$$
$$\iff\mathsf{F}$$
$$\iff x\in\emptyset\qquad\emptyset=\bigcup_{i\in\emptyset}E_i$$

Produit cartésien

• Le produit de la famille $(E_i)_{i\in\mathcal{I}}$ est l'ensemble $\prod_{i\in\mathcal{I}}E_i$ des familles $(x_i)_{i\in\mathcal{I}}$ vérifiant $\forall\,i\in\mathcal{I}\ x_i\in E_i$.

• Cette définition généralise le produit cartésien de deux ensembles, et ses propriétés sont similaires une fois admis l'axiome du choix présenté à la fin de ce chapitre.

Relations binaires

Définitions et exemples

• Une relation binaire $\mathcal{R}$ sur un ensemble E est définie par son graphe $G\subset E^2$; elle est notée $x\ \mathcal{R}\ y$ pour signifier $(x,y)\in G$.

• Les propositions ci-dessous caractérisent certaines relations binaires :

Réflexive	$\forall\,x\in E$	$x\ \mathcal{R}\ x$
Symétrique	$\forall\,(x,y)\in E^2$	$x\ \mathcal{R}\ y\Longrightarrow y\ \mathcal{R}\ x$
Anti-symétrique	$\forall\,(x,y)\in E^2$	$(x\ \mathcal{R}\ y\ \mathsf{ET}\ y\ \mathcal{R}\ x)\Longrightarrow x=y$
Transitive	$\forall\,(x,y,z)\in E^3$	$(x\ \mathcal{R}\ y\ \mathsf{ET}\ y\ \mathcal{R}\ z)\Longrightarrow x\ \mathcal{R}\ z$

• La relation $\leq$ est une relation réflexive, anti-symétrique et transitive sur $\mathbb{R}$.
Lorsque E est un ensemble quelconque, les propriétés des ensembles prouvent que la relation d'inclusion $\subset$ sur $\mathcal{P}(E)$ est une relation réflexive, anti-symétrique et transitive sur $P(E)$.

• La relation $\mathcal{R}$ définie sur $\mathbb{Z}$ par $x\mathcal{R}y$ si et seulement si $x-y$ est multiple de 3 est une relation réflexive, symétrique et transitive :

$$x\mathcal{R}y\iff y-x\in3\mathbb{Z}$$

Réflexive $\quad x-x=0\in3\mathbb{Z}\Longrightarrow x\mathcal{R}x$

Symétrique $\quad x\mathcal{R}y\Longrightarrow x-y\in3\mathbb{Z}$
$$\Longrightarrow y-x=-(x-y)\in3\mathbb{Z}$$
$$\Longrightarrow y\mathcal{R}x$$

Transitive $\quad x\mathcal{R}y\ \mathsf{ET}\ y\mathcal{R}z\Longrightarrow x-y\in3\mathbb{Z}\ \mathsf{ET}\ y-z\in3\mathbb{Z}$
$$\Longrightarrow x-z=(x-y)+(y-z)\in3\mathbb{Z}$$
$$\Longrightarrow x\mathcal{R}z$$

Relation d'équivalence

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

• La classe d'équivalence de $a\in E$ pour la relation d'équivalence $\mathcal{R}$ est l'ensemble des éléments en relation avec a :

$$\dot{a}=\{x\in E\ /\ x\ \mathcal{R}\ a\}=\{x\in E\ /\ a\ \mathcal{R}\ x\}\subset E$$

• Les écritures $x\ \mathcal{R}\ a$ et $x\ \mathcal{R}\ a$ sont équivalentes car la relation $\mathcal{R}$ est supposée symétrique.

• Les classes d'équivalences vérifient en particulier $a\in\dot{a}$ et $\dot{a}\neq\emptyset$.

• L'ensemble quotient est l'ensemble ${}^{E}/_{\mathcal{R}}=\{\dot{a}\ /\ a\in E\}\subset\mathcal{P}(E)$ des classes d'équivalences

• La relation $\mathcal{R}$ sur $\mathbb{Z}$ de l'exemple précédent est une relation d'équivalence. Les classes d'équivalences sont les suivantes :

$$\dot{0}=\{x\in\mathbb{Z}\ /\ x-0\in3\mathbb{Z}\}=\{0,\pm3,\pm6,\pm9,\pm12,\cdots\}=3\mathbb{Z}$$
$$\dot{1}=\{x\in\mathbb{Z}\ /\ x-1\in3\mathbb{Z}\}=\{1,4,7,10,13,\cdots,-2,-5,-8,-11,\cdots\}$$
$$\dot{2}=\{x\in\mathbb{Z}\ /\ x-2\in3\mathbb{Z}\}=\{2,5,8,11,14,\cdots,-1,-4,-7,-10,\cdots\}$$
$$\dot{3}=\{x\in\mathbb{Z}\ /\ x-3\in3\mathbb{Z}\}=3\mathbb{Z}+3=3\mathbb{Z}=\dot{0}=\pm\dot{6}=\pm\dot{9}=\cdots$$
$$\dot{1}=\dot{4}=\dot{7}=\dot{10}=\cdots=\dot{-2}=\dot{-5}=\dot{-8}=\cdots$$
$$\dot{2}=\dot{5}=\dot{8}=\dot{11}=\cdots=\dot{-1}=\dot{-4}=\dot{-7}=\cdots$$

$\mathbb{Z}/\mathcal{R}=\{\dot{0},\dot{1},\dot{2}\}$
Cette définition des congruences modulo 3 sur $\mathbb{Z}$ se généralise à tout entier $p\neq0$.

• Toute relation d'équivalence $\mathcal{R}$ sur E vérifie ces propriétés lorsque $(a,b)\in E^2$:

$$a\ \mathcal{R}\ b\iff a\in\dot{b}\iff\dot{a}\subset\dot{b}\iff\dot{a}=\dot{b}\iff\dot{a}\cap\dot{b}\neq\emptyset$$

• La première équivalence correspond à la définition de la classe d'équivalence $\dot{b}$. Les équivalences suivantes peuvent être démontrées par implications circulaires.
Supposons $a \in \dot{b}$ et montrons $\dot{a} \subset \dot{b}$. Soit $x \in \dot{a}$, donc $x \mathcal{R} a$ et, par hypothèse $a \mathcal{R} b$. La transitivité de $\mathcal{R}$ prouve $x \mathcal{R} b$ et $b \in \dot{b}$. En conclusion $\dot{a} \subset \dot{b}$.
Dans le cas où $\dot{a} \subset \dot{b}$, montrons $\dot{b} \subset \dot{a}$ pour montrer $\dot{a} = \dot{b}$. Soit $x \in \dot{b}$, donc $x \mathcal{R} b$; par ailleurs $a \in \dot{a} \subset \dot{b}$ et $b \mathcal{R} a$. Par transitivité, $x \mathcal{R} a$ et $\dot{b} \subset \dot{a}$.
Lorsque $\dot{a} = \dot{b}$ alors $a \in \dot{a} = \dot{b}$ et $\dot{a} \cap \dot{b} \neq \emptyset$.
Si $\dot{a} \cap \dot{b} \neq \emptyset$ alors il existe $u \in \dot{a} \cap \dot{b}$ qui vérifie $a \mathcal{R} u$ et $u \mathcal{R} b$, donc $a \mathcal{R} b$.
Cette dernière démonstration termine la preuve de ces équivalences.

• L'ensemble quotient $E/\mathcal{R}$ est une partition de E :

$$\forall\, \dot{a} \in E/\mathcal{R} \quad \dot{a} \neq \emptyset$$
$$\bigcup_{\dot{a} \in E/\mathcal{R}} \dot{a} = E$$
$$\forall\, (\dot{a}, \dot{b}) \in E/\mathcal{R} \quad \dot{a} \neq \dot{b} \Longrightarrow \dot{a} \cap \dot{b} = \emptyset$$

• La première condition est justifiée par $a \in \dot{a}$.
Une double inclusion prouve la seconde égalité :

$$\forall\, u \in E \quad u \in \dot{u} \subset \bigcup_{\dot{a} \in E/\mathcal{R}} \dot{a} \quad \text{donc } E \subset \bigcup_{\dot{a} \in E/\mathcal{R}} \dot{a}$$
$$\dot{u} \subset E \quad \text{donc} \bigcup_{\dot{a} \in E/\mathcal{R}} \dot{a} \subset E$$

La dernière implication est la contraposée de $\dot{a} \cap \dot{b} \neq \emptyset \Longrightarrow \dot{a} = \dot{b}$.

Relation d'ordre

• Une relation d'ordre sur E est une relation binaire qui est réflexive, anti-symétrique et transitive.

• La relation de comparaison $\leq$ des réels est une relation d'ordre sur $\mathbb{R}$.
La relation de comparaison stricte $<$ des nombres réels n'est pas réflexive car $1 < 1$ est faux, et n'est donc pas une relation d'ordre.
L'inclusion $\subset$ des sous-ensembles de E est une relation d'ordre sur $\mathcal{P}(E)$; l'inclusion est réflexive, symétrique et transitive.

• Une relation d'ordre est généralement notée par un symbole de la

forme $\preceq$; les expressions $x \preceq y$ et $y \succeq x$ sont équivalentes. En outre $x \preceq y \preceq z$ signifie $x \preceq y \,\mathsf{ET}\, y \preceq z$, et $x \prec y$ représente $x \preceq y \,\mathsf{ET}\, x \neq y$.

• Une relation d'ordre $\preceq$ sur E est totale si et seulement si deux éléments quelconques sont comparables :

$$\forall\, (x, y) \in E^2 \quad x \preceq y \,\mathsf{OU}\, y \preceq x$$

La comparaison $\leq$ des nombres réels est une relation d'ordre totale.

• Dès qu'un ensemble E comporte deux éléments différents x et $y \neq x$, la relation d'ordre de l'inclusion n'est pas totale car les deux ensembles $\{x\}$ et $\{y\}$ ne sont pas inclus l'un dans l'autre.
L'inclusion est une relation d'ordre total sur l'ensemble vide et les ensembles à un élément car ces inclusions énumèrent toutes les possibilités :

$$\emptyset \subset \emptyset \qquad \emptyset \subset \{a\} \qquad \{a\} \subset \{a\}$$

• Le plus petit élément m de $F \subset E$ vérifie $m \in F \,\mathsf{ET}\, (\forall\, x \in F\ m \preceq x)$; s'il existe, il est unique et noté $\min F$. L'éventuel plus grand élément de F est défini de façon similaire et noté $\max F$:

$$m = \min F \Longleftrightarrow m \in F \,\mathsf{ET}\, (\forall\, x \in F\ m \preceq x)$$
$$M = \max F \Longleftrightarrow M \in F \,\mathsf{ET}\, (\forall\, x \in F\ x \preceq M)$$

• La preuve de l'unicité suppose que m_1 et m_2 sont deux plus petits éléments de F et exploite l'anti-symétrie de $\leq$ pour montrer l'égalité $m_1 = m_2$:

$$\forall\, x \in F \quad m_1 \leq x \quad \text{et} \quad m_2 \in F \quad \text{donc} \quad m_1 \leq m_2$$
$$\forall\, x \in F \quad m_2 \leq x \quad \text{et} \quad m_1 \in F \quad \text{donc} \quad m_2 \leq m_1$$

La démonstration est similaire pour le plus grand élément.

Remarques sur la théorie des ensembles

Deux ensembles impossibles

• La théorie des ensembles a donc pour but de définir des axiomes sur lesquels se fondent toutes les mathématiques. Ceux-ci sont définis pour éviter que les mathématiques soient contradictoires : aucune démonstration ne doit aboutir à $\mathsf{V} \Longleftrightarrow \mathsf{F}$.

• Ces axiomes permettent par exemple de montrer par l'absurde qu'il n'existe pas d'ensemble $\mathcal{E}$ de tous les ensembles.

Si cet ensemble $\mathcal{E}$ existait alors l'axiome de séparation permettrait de construire le sous-ensemble $\mathcal{S}$ des ensembles de $\mathcal{E}$ vérifiant $X \notin X$:

$$\mathcal{S} = \{X \in \mathcal{E} \ / \ X \notin X\}$$

Deux cas sont possibles soit $\mathcal{S} \in \mathcal{S}$ soit $\mathcal{S} \notin \mathcal{S}$. Dans le premier cas la définition de $\mathcal{S}$ énonce $\mathcal{S} \notin \mathcal{S}$. Dans le second cas $\mathcal{S} \notin \mathcal{S}$ aboutit à $\mathcal{S} \in \mathcal{S}$. En conclusion $\mathcal{S} \in \mathcal{S} \iff \mathcal{S} \notin \mathcal{S} \iff \mathsf{NON}\,(\mathcal{S} \in \mathcal{S})$ qui est une contradiction de la forme $A \iff \mathsf{NON}\ A$.
Cette preuve démontre que l'existence de $\mathcal{E}$ implique F, et donc que l'ensemble $\mathcal{E}$ de tous les ensembles n'existe pas.

• L'axiome de séparation appliqué au prédicat « X est un ensemble » permet d'affirmer que si l'ensemble $\mathcal{U}$ de tous les objets mathématiques existait alors le sous-ensemble $\mathcal{E}$ de tous les ensembles existerait :

$$\mathcal{E} = \{X \in \mathcal{U} \ / \ X \text{ est un ensemble}\}$$

La contraposée de cette implication justifie que l'ensemble $\mathcal{U}$ n'existe pas car l'ensemble $\mathcal{E}$ n'existe pas.

L'axiome du choix

• Ce cours admet implicitemenent l'axiome du choix.
L'axiome du choix pose qu'un produit infini d'ensembles $(E_i)_{i\in\mathcal{I}}$ non vide n'est pas vide :

$$(\forall\, i \in \mathcal{I}\ E_i \neq \emptyset) \Longrightarrow \prod_{i\in\mathcal{I}} E_i \neq \emptyset$$

La construction même du produit cartésien de deux ensembles affirme que le produit de deux ensembles non vide n'est pas vide :

$$\begin{aligned} E \neq \emptyset\ \mathsf{ET}\ F \neq \emptyset &\Longrightarrow (\exists\, x \in E)\ \mathsf{ET}\ (\exists\, y \in F) \\ &\Longrightarrow (\exists\, (x,y) \in E \times F) \\ &\Longrightarrow E \times F \neq \emptyset \end{aligned}$$

Plus généralement la propriété précédente peut s'écrire explicitement pour un nombre fini d'ensembles, mais ne peut pas s'énoncer de la même manière avec un nombre fini de symboles quand la famille d'ensembles est infinie.
L'axiome du choix généralise cette proposition aux familles infinies d'ensembles.

• La construction d'une application ψ vérifiant $f \circ \psi = \mathrm{Id}_F$ à partir d'une application $f : E \to F$ surjective exploite l'axiome du choix.

L'application ψ est construite élément par élément pour tout $y \in F$ à partir du choix d'un antécédent $x_y \in E$ de y :

$$\forall\, y \in F \quad \exists\, x_y \in E \quad f(x_y) = y \qquad \text{défini } \psi(y) = x_y$$

La construction de l'application ψ fait donc intervenir l'axiome du choix en choisissant pour image de tout $y \in F$ un antécédent de y dans l'ensemble $f^{-1}(\{y\}) \neq \emptyset$.

• Au contraire la construction d'une application φ vérifiant $\varphi \circ f = \mathrm{Id}_E$ à partir d'une application $f : E \to F$ injective ne fait pas intervenir l'axiome du choix.
Tout $y \in \mathrm{Im}\, f$ possède un et un seul antécédent noté $x_y \in E$ qui définit sans ambiguïté $\varphi(y)$. Par ailleurs l'image par φ d'un élément $y \notin \mathrm{Im}\, f$ peut-être un élément quelconque de $E : \exists\, a \in E$. Une fois fixé l'élément $a \in E$, la construction de l'application φ est explicite et ne fait intervenir ni un élément dans un produit infini d'ensemble ni l'axiome du choix.