Les ensembles, c'est tout

(version provisoire du 22 juillet 2008)

Jean-Marie Lion
Université de Rennes 1

On débute par une introduction à la logique élémentaire en donnant les règles de déduction naturelle. Ensuite on essaie de donner un sens mathématique à la notion intuitive d'ensemble et d'élément. Pour y arriver on tente de donner une présentation succincte de la théorie Zermelo et Fraenkel avec l'axiome du choix. On finit par étudier les applications et les relations en particulier des relations d'ordre.

I. Le langage de la théorie des ensembles, les démonstrations

Dans cette partie la théorie des ensembles ne sera évoquée que par le symbole $\in$ (appartient à). On décrit seulement le langage qu'on utilisera dans la théorie des ensembles et on explique ce qu'on entend par démonstration. On utilise les symboles suivants :
- les connecteurs logiques : $\wedge$ (et), $\neg$ (non), $\vee$ (ou), $\Rightarrow$ (implique) ;
- les quantificateurs $\exists$ (il existe), $\forall$ (pour tout) ;
- les parenthèses (et) ;
- des lettres appelées variables ;
- le symbole $=$ (est égal à) ;
- le symbole $\in$ (appartient à)
- le symbole $|$ qui indique une substitution.

Ces symboles permettent d'écrire des *formules* ou *prédicats* en respectant quelques règles :
- si x et y sont deux variables alors $x = y$ et $x \in y$ sont des prédicats sans variable liée et dont les variables libres sont x et y ;
- si A est un prédicat alors $\neg A$ est un prédicat qui possède les mêmes variables liées et les mêmes variables libres que A ;
- si x est une variable libre du prédicat A alors $\exists x A$ et $\forall x A$ sont des prédicats dont les variables libres sont celles de A à l'exception de x et les variables liées sont celles de A auxquelles est ajoutée x ($\exists x$ se lit "il existe x tel que" et $\forall x$ se lit "pour tout x") ;
- si A et B sont des prédicats tels que si une variable est libre pour l'un elle n'est pas liée pour l'autre alors $A \wedge B$, $A \vee B$ et $A \Rightarrow B$ sont des prédicats dont les variables libres et les variables liées sont celles de A et B ;

- si x est une variable libre du prédicat A et y n'est pas une variable liée de A alors $A(y|x)$ est le prédicat obtenu en substituant y à x dans A.

Les prédicats $\neg(x = y)$ et $\neg(x \in y)$ s'écrivent également $x \neq y$ et $x \notin y$.

Un prédicat A qui possède comme variables libres les variables $x_1, ..., x_n$ peut être noté $A(x_1, ..., x_n)$.

Un prédicat sans variable libre s'appelle une *assertion.*

Un prédicat est souvent fomés de prédicats imbriqués. Il peut être utile d'utiliser des parenthèses pour faciliter la lecture et lever toute ambiguïté. On suivra l'ordre de priorité suivant : $\neg, \vee, \wedge, \Rightarrow$. Ainsi $\neg A \wedge B \vee C \Rightarrow D$ est le même prédicat que $((\neg A) \wedge (B \vee C)) \Rightarrow D$.

Faire une démonstration consiste à déterminer si un prédicat est *vrai* ou *faux* sous certaines hypothèses et en appliquant certaines *règles de déduction.* Avec ce point de vue les vérités sont relatives. On part d'une famille de prédicats supposés vrais (*hypothèse*) et on espère qu'en appliquant certaine règles on pourra montrer qu'un prédicat donné est vrai (*conclusion*). Au cours d'une démonstration on peut être amenés à rajouter puis à abandonner de nouvelles hypotèses dites *hypothèses auxiliaires.* Voici les treize règles.

- Le modus ponens *Si A est vrai et $A \Rightarrow B$ est vrai alors B est vrai.*
- Abandon de l'hypothèse auxiliaire *Si en supposant A vrai (c'est à dire en considérant qu'on rajoute A comme une hypothèse supplémentaire) on démontre que B est vrai alors $A \Rightarrow B$ est vrai.*
- L'analyse *Si $A \wedge B$ est vrai alors A est vrai et B est vrai.*
- La synthèse *Si A est vrai et B est vrai alors $A \wedge B$ est vrai.*
- La disjonction des hypothèses *Si $A \Rightarrow C$ est vrai et $B \Rightarrow C$ est vrai alors $(A \vee B) \Rightarrow C$ est vrai.*
- L'affaiblissement d'une thèse *Si A est vrai alors $A \vee B$ est vrai et $B \vee A$ est vrai.*
- La réduction à l'absurde ou reductio ad absurdum *Si $A \Rightarrow (B \wedge \neg B)$ alors $\neg A$ est vrai.*
- La double négation *Si $\neg\neg A$ est vrai alors A est vrai.*
- La singularisation *Si $\forall x A(x)$ est vrai et si y n'est pas une variable liée de A alors $A(y|x)$ est vrai.*
- La généralisation *Si A est vrai, si $A \Rightarrow B(x)$ et si x n'est pas une variable libre de A alors $\forall x B(x)$ est vrai.*
- Preuve directe de l'existence *Si $A(x)$ est vrai alors $\exists x A(x)$ est vrai.*
- Conséquence de l'existence *Si $\exists x A(x)$ est vrai, si $A(x) \Rightarrow B$ est vrai et*

si x n'est pas une variable libre de B alors B est vrai.

– Répétition *Si B est démontré sous l'hypothèse auxiliaire A on peut répéter B tant que A n'est pas abandonnée.*

Ces règles de déduction sont celles de la *logique classique*, en particulier la règle de la double négation que n'acceptent pas certains logiciens dits *intuitionnistes*.

Une *proposition* est l'énoncé d'un prédicat vrai. Il prend souvent l'une des formes suivantes :

proposition $A \Rightarrow B$
proposition *Si A est vrai alors B est vrai.*
proposition *Si A alors B.*

où A est l'hypohèse et B la conclusion. Suivant l'intérêt qu'on porte à une proposition on l'appellera *théorème* (d'un intérêt théorique) ou *lemme* (d'un intérêt pratique pour démontrer des théorèmes ou des propositions).

En utilisant ces règles de déduction on démontre que si A B et C sont des prédicats alors

I.1. proposition (La contraposée ou modus tollens)

$$(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$$

I.2. proposition (Le tiers exclus)

$$A \vee \neg A$$

I.3. proposition (La non contradiction)

$$\neg(A \wedge \neg A)$$

I.4. proposition (Du faux découle ce que l'on veut ou ex falso sequitur quodlibet)

$$(A \wedge \neg A) \Rightarrow B$$

I.5. proposition (La transitivité de l'implication)

$$((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$$

I.6. proposition (La loi de Pierce)

$$((A \Rightarrow B) \Rightarrow A) \Rightarrow A$$

I.7. proposition (Les lois de Morgan)

$$\begin{array}{rcl} (\neg A \wedge \neg B) & \Rightarrow & \neg(A \vee B) \\ (\neg A \vee \neg B) & \Rightarrow & \neg(A \wedge B) \\ \neg(A \vee B) & \Rightarrow & (\neg A \wedge \neg B) \\ \neg(A \wedge B) & \Rightarrow & (\neg A \vee \neg B) \end{array}$$

Ces propositions ne dépendent pas des prédicats A, B et C. C'est ce qu'on appelle des *tautologies.*

I.8. définition On note $A \Leftrightarrow B$ le prédicat $(A \Rightarrow B) \wedge (B \Rightarrow A)$ et on dit A est équivalent à B.

I.9. exemple Soient A et B deux prédicats. Supposons $A \Leftrightarrow B$ vrai. D'après le principe du tiers exclus soit A est vrai soit $\neg A$ est vrai. Si A est vrai alors B est vrai (d'après le modus ponens). Si $\neg A$ est vrai alors $\neg B$ est vrai (d'après le modus tollens). Réciproquement si A et B sont vrais ou si $\neg A$ et $\neg B$ sont vrais alors $A \Leftrightarrow B$.

On a les tautologies suivantes. Soient A, B et C des prédicats.

I.10. proposition (commutativité, associativité et distributivité de $\wedge$ et $\vee$)

$$\begin{array}{rcl} (A \wedge B) & \Leftrightarrow & (B \wedge A) \\ (A \vee B) & \Leftrightarrow & (B \vee A) \\ ((A \wedge B) \wedge C) & \Leftrightarrow & (A \wedge (B \wedge C)) \\ ((A \vee B) \vee C) & \Leftrightarrow & (A \vee (B \vee C)) \\ ((A \vee B) \wedge C) & \Leftrightarrow & ((A \wedge C) \vee (B \wedge C)) \\ ((A \wedge B) \vee C) & \Leftrightarrow & ((A \vee C) \wedge (B \vee C)) \end{array}$$

I.11. proposition

$$\begin{array}{rcl} (A \wedge B) & \Leftrightarrow & \neg(\neg B \vee \neg A) \\ (A \vee B) & \Leftrightarrow & \neg(\neg B \wedge \neg A) \end{array}$$

Ainsi $\neg$ et $\wedge$ permettent d'exprimer $\vee$ et $\neg$ et $\vee$ permettent d'exprimer $\wedge$.

I.12. proposition

$$(A \Rightarrow B) \quad \Leftrightarrow \quad (\neg A \vee B)$$

Ceci signifie que $\Rightarrow$ s'exprime à l'aide de $\neg$ et $\vee$.

À l'aide de ces tautologies, on construit des tables dites *tables de vérité* qui permettent de déterminer les valeurs logiques (vrai (V) ou faux (F)) des prédicats $\neg A$, $A \wedge B$, $A \vee B$, $A \Rightarrow B$ et $A \Leftrightarrow B$ en fonction de celles de A et B :

A	$\neg A$
V	F
F	V

et

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
V	V	V	V	V	V
V	F	F	V	F	F
F	V	F	V	V	F
F	F	F	F	V	V

Nous donnons maintenant une série de tautologies liées à $\forall$ et $\exists$. Le recours aux règles de singularisation, de généralisation, de preuve directe de l'existence et de conséquence de l'existence est nécessaire pour les établir.

I.13. proposition *Si A et B sont des prédicats alors*

$$\begin{array}{rcll}
(\exists x A) & \Leftrightarrow & \neg(\forall x \neg A) & \\
(\forall x A) & \Leftrightarrow & \neg(\exists x \neg A) & \\
(\exists x \exists y A) & \Leftrightarrow & (\exists y \exists x A) & \\
(\forall x \forall y A) & \Leftrightarrow & (\forall y \forall x A) & \\
(\forall x (A \wedge B)) & \Leftrightarrow & (A \wedge (\forall x B)) & \textit{si } x \textit{ n'est pas une variable libre de } A \\
(\forall x (A \vee B)) & \Leftrightarrow & (A \vee (\forall x B) & \textit{si } x \textit{ n'est pas une variable libre de } A \\
(\forall x \forall y (A \wedge B)) & \Leftrightarrow & ((\forall x A) \wedge (\forall y B)) & \textit{si } x \textit{ n'est pas une variable libre de } B \\
 & & & \textit{et } y \textit{ n'est pas une variable libre de } A \\
(\forall x \forall y (A \vee B)) & \Leftrightarrow & ((\forall x A) \vee (\forall y B)) & \textit{si } x \textit{ n'est pas une variable libre de } B \\
 & & & \textit{et } y \textit{ n'est pas une variable libre de } A.
\end{array}$$

I.14. remarque En général les prédicats $\exists x \forall y A$ et $\forall y \exists x A$ ne sont pas synomymes. En revanche $(\exists x \forall y A) \Rightarrow (\forall y \exists x A)$ est toujours vrai.

D'une certaine façon le travail mathématique consiste à déterminer la véracité de prédicats. Dans un texte mathématique on rencontre des assertions dont on sait qu'elles sont vraies, dans ce cas on ne l'indique généralement pas, et d'autres dont on essaie de savoir si elles le sont.

Dans la suite on aura pour règle d'éviter le plus possible de représenter les connecteurs logiques et les quantificateurs par les symboles $\wedge$, $\neg$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, $\exists$, et $\forall$. On préférera les paraphraser par des mots du langage courant.

II. Les axiomes de la théorie des ensembles La *théorie des ensembles* consiste à considérer une collection d'objets appelés *ensembles* et caractérisés par certaines propriétés qu'on va décrire : les axiomes de la théorie des ensembles. Ils fondent la théorie des ensembles. De ces axiomes on pourra déduire ensuite la véracité de prédicats : on établira des propositions qui préciseront des propriétés caractéristiques des ensembles et déduites des axiomes. La famille de ces propositions formera la connaissance que l'on a de la théorie des ensembles.

Voici maintenant les propriétés fondamentales (*axiomes*) qui décrivent les ensembles et leurs relations. Ces propriétés sont énoncées sous deux formes. D'abord à l'aide d'une phrase, ensuite à l'aide d'une assertion construite avec les règles syntaxiques exposées précédemment.

1 - Deux ensembles sont égaux si tout élément de l'un est élément de l'autre :

$$\forall x \forall y((x = y) \Leftrightarrow (\forall z((z \in x) \Leftrightarrow (z \in y))).$$

2 - Il existe un ensemble sans élément. Il est appelé *ensemble vide* et noté $\emptyset$:

$$\exists x \forall y(\neg(y \in x)).$$

3 - Étant donnés deux ensembles il existe un ensemble appelé *paire* dont les éléments sont exactement ces deux ensembles. Si les deux ensembles donnés sont égaux alors on parle de *singleton* associé à cet ensemble donné :

$$\forall x \forall y \exists z \forall t(((x \in z) \wedge (y \in z)) \wedge ((t \in z) \Rightarrow ((t = x) \vee (t = y)))).$$

4 - Étant donné un ensemble il existe un ensemble dont les éléments sont exactement les éléments des éléments de cet ensemble donné. C'est la *réunion* des ensembles qui sont éléments de l'ensemble donné :

$$\forall x \exists y \forall z((\exists t((z \in t) \wedge (t \in x))) \Leftrightarrow (z \in y)).$$

5 - Étant donné un ensemble et une prédicat $A(x)$ alors les éléments a de l'ensemble donné tels que $A(a)$ est vraie forment un ensemble. C'est le *sous-ensemble* de l'ensemble donné *défini par compréhension* à partir du prédicat $A(x)$:

$$\forall X \exists Y \forall x((x \in Y) \Leftrightarrow ((x \in X) \wedge (A(x)))).$$

Il est noté $\{x \in X : A(x)\}$.
6. Étant donné un ensemble il existe un ensemble dont les éléments sont exactement les ensembles dont les éléments sont également des éléments de l'ensemble donné. C'est ensemble est l'ensemble des *parties* ou des *sous-ensembles* de l'ensemble donné :

$$\forall x \exists y \forall z((\forall t((t \in z) \Rightarrow (t \in x))) \Leftrightarrow (z \in y)).$$

7 - Il existe un ensemble dont l'ensemble vide est un élément et tel que si un second ensemble est élément quelconque de cet ensemble alors la réunion de ce second ensemble et du singleton associé à ce second ensemble est un élément de cet ensemble. Ceci signifie qu'il existe un ensemble *infini* :

$$\exists E \forall x \exists y \forall z((\emptyset \in E) \wedge ((x \in E) \Rightarrow ((z \in y) \Leftrightarrow ((z \in x) \vee (z = x))))).$$

8 - Étant donné un ensemble et un prédicat $A(x, y)$ tel que pour tout élément a de l'ensemble donné il existe au plus un ensemble b tel que $A(a, b)$ soit vraie alors les ensembles b ainsi obtenus quand a décrit l'ensemble donné forment un ensemble appelé *image* de l'ensemble donné par A :

$$\begin{array}{c}(\forall x \forall y \forall y'((A(x, y) \wedge (A(x, y')) \Rightarrow (y = y'))) \\ \Downarrow \\ (\forall X \exists Y \forall y((\exists x((x \in X) \wedge A(x, y))) \Leftrightarrow (y \in Y))).\end{array}$$

9 - Étant donné un ensemble non vide il existe un élément qui appartient à cet ensemble et qui ne possède aucun élément en commun avec l'ensemble donné. En particulier un ensemble n'est jamais élément de lui-même :

$$\forall x \exists y \forall z((x = \emptyset) \vee ((y \in x) \wedge ((z \in y) \Rightarrow (\neg(z \in x))))).$$

Soit y un ensemble non vide et x le singleton $x = \{y\}$. D'après l'axiome 9 si z est un élément de y $(z \in y)$ alors z n'est pas y qui est l'unique un élément de x : $(\neg(z = y))$. En particulier $(\neg(y \in y))$: un ensemble n'est jamais élément de lui même.
10 - Étant donné un ensemble dont tous les éléments sont des ensembles non vides il existe un ensemble qui a en commun avec chaque élément de l'ensemble donné un et un seul élément :

$$\forall x \left((\emptyset \in x) \vee \left(\exists y \forall t \left((t \in x) \Rightarrow \left(\exists z \forall u \left(\begin{array}{c} ((z \in t) \wedge (z \in y)) \\ \wedge \\ (((u \in t) \wedge (u \in y)) \Rightarrow (u = z)) \end{array} \right) \right) \right) \right) \right).$$

On peut *choisir* simultanément un élément dans chaque ensemble d'une famille d'ensembles non vides.

Ces règles sont les 9 *axiomes* de la théorie des ensembles de Zermelo et Fraenkel auxquels on a ajouté l'axiome du choix. L'axiome 2 nous garantit l'existence d'au moins un ensemble, l'ensemble vide. Les autres axiomes nous garantissent l'existence de nombreux ensembles. Les six premiers axiomes permettent de donner un sens en termes d'ensembles aux notions de *couple,* de *produit cartésien,* d'*intersection,* de *réunion,* de *différence,* de *projection sur un des facteurs d'un sous-ensemble d'un produit cartésien.* L'axiome 7 assure l'existence d'un ensemble infini et mermet de construire les entiers naturels. Les axiomes 8, 9 et 10 sont plus difficiles à saisir. Le dernier, appelé *axiome du choix* a une importance importante dans toutes les branches des mathématiques.

Gödel montre qu'il existe des assertions dont on ne peut dire si elles sont vraies ou fausses en utilisant les 10 axiomes précédents et le langage de la théorie des ensembles. Il montre également que pour montrer qu'il n'existe pas d'assertions contradictoires dans la théorie des ensembles il faut raisonner dans une théorie plus forte que la théorie des ensembles.

III. Définition par compréhension, inclusion, intersection, réunion, différence, complémentaire, couple, produit cartésien, projection

Notation Si X est un ensemble et A un prédicat $(\forall x \in X\ A)$ est synonyme de $(\forall x((x \in X) \Rightarrow A))$ et $(\exists x \in X\ A)$ est synonyme de $(\exists x((x \in X) \wedge A))$. Le prédicat $(\forall x \in X\ A)$ se lit "pour tout x dans X on a A" ou "si x dans X alors A". Le prédicat $(\exists x \in X\ A)$ se lit "il existe x dans X tel que A".

L'ensemble des parties Si X est un ensemble, l'ensemble des parties de X donné par l'axiome 6 est noté $\mathcal{P}(X)$ ou 2^X.

Inclusion Soit X et Y deux ensembles. On dit que Y est inclus dans X et on écrit $Y \subset X$ ou $X \supset Y$ si l'assertion

$$\forall x((x \in Y) \Rightarrow (x \in X))$$

est vraie. D'après le premier axiome $X = Y$ si $Y \subset X$ et $X \subset Y$. On note $Y \not\subset X$ la négation $(\neg(Y \subset X))$.

Définition par compréhension Soit X un ensemble et $A(x)$ un prédicat

qui possède une variable libre. Alors le sous-ensemble

$$Y = \{x \in X : A(x)\}$$

de X défini par compréhension à partir du prédicat $A(x)$ (voir axiome 5) est caractérisé de la façon suivante

$$\forall x((x \in Y) \Leftrightarrow ((x \in X) \wedge A(x))).$$

Réunion Si X et Y sont deux ensembles alors la réunion $X \cup Y$ vérifie

$$\forall x(((x \in X) \vee (x \in Y)) \Leftrightarrow (x \in X \cup Y)).$$

Si I est un ensemble et $(X_i)_{i \in I}$ est une famille d'ensembles indexée par I alors la réunion $X = \bigcup_{i \in I} X_i$ donnée par le quatrième axiome vérifie

$$\forall x((\exists i((i \in I) \wedge (x \in X_i))) \Leftrightarrow (x \in X)).$$

Intersection Si X et Y sont deux ensembles alors l'intersection $X \cap Y$ vérifie

$$\forall x(((x \in X) \wedge (x \in Y)) \Leftrightarrow (x \in X \cap Y))).$$

Si I est un ensemble non vide et $(X_i)_{i \in I}$ est une famille d'ensembles indexée par I alors l'intersection $X = \bigcap_{i \in I} X_i$ est l'ensemble

$$X = \{x \in X_{i_0} : \forall i((i \in I) \Rightarrow (x \in X_i))\}$$

où i_0 est un élément quelconque de I.

Différence et complémentaire Si X et Y sont deux ensembles alors la différence $X \setminus Y$ et le sous-ensemble de X défini par

$$X \setminus Y = \{x \in X : (\neg(x \in Y))\}.$$

Si $Y \subset X$ alors $X \setminus Y$ s'appelle le complémentaire de Y dans X.

Couple Soit x et y deux ensembles alors l'ensemble $\{x, \{x, y\}\}$ s'appelle le *couple de premier terme x et de second terme y*. Il est noté (x, y). Le couple (x, y) existe par l'axiome 3 : c'est la paire obtenue à partir de x et de la paire obtenue à partir de x et de y. Il est unique par l'axiome 1 :

Produit cartésien Soit X et Y deux ensembles. Le produit cartésien $X \times Y$ est le sous-ensemble de $\mathcal{P}(X \cup Y)$ défini par

$$X \times Y = \{z \in \mathcal{P}(X \cup Y) : (\exists x \exists y(((x \in X) \wedge (y \in Y)) \wedge (z = (x, y))))\}.$$

C'est l'ensemble des couples (x, y) avec $x \in X$ et $y \in Y$.

Projection Soit X et Y deux ensembles et Z un sous-ensemble du produit cartésien $X \times Y$. Alors la *projection de Z sur X parallèlement à Y* est le sous-ensemble de $\pi_X(Z)$ défini par

$$\pi_X(Z) = \{x \in X : \exists y((x, y) \in Z\}.$$

C'est l'ensemble des éléments x de X pour les quels il existe au moins un $y \in Y$ tel que le couple (x, y) soit dans Z. On définit de façon analogue la *projection de Z sur Y parallèlement à X* en posant

$$\pi_Y(Z) = \{y \in Y : \exists x((x, y) \in Z\}.$$

Propriétés Soit X, Y, Z et T quatre ensembles et A et B des prédicats avec une variable libre . Alors
- $(X \cap Y) \subset X$, $(X \cap Y) \subset Y$,
- $X \cap X = X$, $X \cap Y = Y \cap X$, $X \cap (Y \cap Z) = (X \cap Y) \cap Z$,
- $X \subset (X \cup Y)$, $Y \subset (X \cup Y)$,
- $X \cup X = X$, $X \cup Y = Y \cup X$, $X \cup (Y \cup Z) = (X \cup Y) \cup Z$,
- $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Y)$, $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Y)$,
- si $Z \subset Y$ et $Y \subset X$ alors $Z \subset X$,
- si $Y \subset X$ alors $X = Y \cup (X \setminus Y)$, $\emptyset = Y \cap (X \setminus Y)$, $Y = X \setminus (X \setminus Y)$,
- si $Y = \{x \in X : A(x)\}$ et $Z = \{x \in X : B(x)\}$ alors

$$\begin{array}{rcl} X \setminus Y & = & \{x \in X : (\neg A(x))\}, \\ Y \cap Z & = & \{x \in X : (A(x) \wedge B(x))\}, \\ Y \cup Z & = & \{x \in X : (A(x) \vee B(x))\}, \end{array}$$

- si Z et T sont des sous-ensembles de $X \times Y$ alors

$$\pi_X(Z \cup T) = \pi_X(Z) \cup \pi_X(T), \quad \pi_X(Z \cap T) \subset \pi_X(Z) \cap \pi_X(T)$$

et si de plus $Z \subset T$ alors $\pi_X(Z) \subset \pi_X(T)$.

Propriétés Soit I un ensemble non vide, Y un ensemble et $(X_i)_{i\in I}$ une famille d'ensembles. Alors

$$\begin{aligned}\left(\bigcup_{i\in I} X_i\right)\cap Y &= \bigcup_{i\in I}(X_i\cap Y),\\ \left(\bigcap_{i\in I} X_i\right)\cup Y &= \bigcap_{i\in I}(X_i\cup Y).\end{aligned}$$

Si $\left(\bigcup_{i\in I} X_i\right)\subset Y$ alors

$$\begin{aligned}Y\setminus\left(\bigcup_{i\in I} X_i\right) &= \bigcap_{i\in I}(Y\setminus X_i),\\ Y\setminus\left(\bigcap_{i\in I} X_i\right) &= \bigcup_{i\in I}(Y\setminus X_i).\end{aligned}$$

Propriétés Soit Iet J des ensembles non vides, soit $(I_j)_{j\in J}$ une famille de sous-ensembles non vides de I dont la réunion est I et $(X_i)_{i\in I}$ une famille d'ensembles. Alors

$$\bigcup_{i\in I} X_i = \bigcup_{j\in J}\left(\bigcup_{i\in I_j} X_i\right) \text{ et } \bigcap_{i\in I} X_i = \bigcap_{j\in J}\left(\bigcap_{i\in I_j} X_i\right).$$

Propriétés Soit X et Y des ensembles, I un ensemble non vide et $(Z_i)_{i\in I}$ une famille de sous-ensembles de $X\times Y$ alors

$$\pi_X\left(\bigcup_{i\in I} Z_i\right) = \left(\bigcup_{i\in I}\pi_X(Z_i)\right), \pi_X\left(\bigcap_{i\in I} Z_i\right)\subset\left(\bigcap_{i\in I}\pi_X(Z_i)\right)$$

et

$$\pi_Y\left(\bigcup_{i\in I} Z_i\right) = \left(\bigcup_{i\in I}\pi_Y(Z_i)\right), \pi_Y\left(\bigcap_{i\in I} Z_i\right)\subset\left(\bigcap_{i\in I}\pi_Y(Z_i)\right).$$

IV. Applications

IV.1. définition Une *application* est un triplet $f=(E,F,\mathcal{G})$ où E et F sont des ensembles et $\mathcal{G}$ un sous-ensemble de $E\times F$ tel que si $x\in E$ alors il existe un et un seul $y\in F$ et noté $f(x)$ tel que $(x,y)\in\mathcal{G}$. L'application f est

souvent notée $f : E \to F$. L'ensemble E s'apelle le *domaine* ou l'*ensemble de départ de* f, l'ensemble F s'appelle l'*ensemble d'arrivée* et l'ensemble $\mathcal{G}$ s'appelle le *graphe de* f. Si $(x, y) \in \mathcal{G}$ alors y est appelée *image de* x *par* f ou *valeur de* f *en* x et x est appelé *antécédent de* y *par* f. Si $X \subset E$ Le sous-ensemble des éléments de F qui sont des images d'éléments de X par f s'appelle *l'image de* X par f et il est noté $f(X)$. L'ensemble $f(E)$ s'appelle *ensemble des valeurs de* f ou *l'image de* f. Si $Y \subset F$ Le sous-ensemble des éléments de E qui sont les antécédents des éléments de Y par f s'appelle *l'image réciproque de* Y par f et il est noté $f^{-1}(Y)$.

IV.2. exemple Si E est un ensemble alors l'ensemble $\mathcal{I}_E = \{(x, x) : x \in E\}$ est le graphe d'une application de Id_E de E dans E appelée *identité* de E : si $x \in E$ alors $Id_E(x) = x$.

IV.3. exemple Soit E et F deux ensembles. Soit $y \in F$. On appelle *application constante* y l'application f de E dans F définie par $f(x) = y$ si $x \in E$. Son graphe est l'ensemble $\{(x, y) : x \in E\}$.

IV.4. proposition *Soit $f : E \to F$ et $f' : E \to F$ deux applications. Si pour tout $x \in E$ on a $f(x) = f'(x)$ alors $f = f'$.*

IV.5. preuve Soit $\mathcal{G}$ et $\mathcal{G}'$ les graphes de f et f'. Soit $(x, y) \in \mathcal{G}$ et $(x, y') \in \mathcal{G}'$. On a $y = f(x)$ et $y' = f'(x)$. Or $f(x) = f'(x)$. Donc $y = f(x) = f'(x) = y'$ et $(x, y) = (x, y')$. Ceci montre que les éléments de $\mathcal{G}$ et $\mathcal{G}'$ coïncident. Par conséquent les deux sous-ensembles $\mathcal{G}$ et $\mathcal{G}'$ de $E \times F$ sont égaux. Ainsi $f = f'$.

IV.6. définition Soit $E \subset E'$, $f : E \to F$ et $f' : E' \to F$. On dit que f est une *restriction* de f' à E ou que f' est un *prolongement* de f à E' si pour tout $x \in E$ on a $f(x) = f'(x)$.

IV.7. proposition *Soit $E \subset E'$ et $f : E \to F$. Alors il existe un prolongement f' de f à E'.*

IV.8. preuve Soit $y \in F$. L'application f' de E' dans F définie par $f'(x) = f(x)$ si $x \in E$ et $f(x) = y$ si $x \in E' \setminus E$ est un prolongement de f à E'.

IV.9. proposition *Soit $E \subset E'$ et $f' : E' \to F$. Alors il existe une et une seule restriction de f' à f.*

IV.10. preuve Si $\mathcal{G}'$ est le graphe de f' alors $\mathcal{G} \cap (E \times F)$ est le graphe d'une restriction f à E. Si $g : E \to F$ est une restriction de f' à E alors pour tout $x \in E$ on a $g(x) = f'(x) = f(x)$. Donc $f = g$.

IV.11. définition Soit $F \subset F'$, $f : E \to F$ et $f' : E \to F'$. On dit que f

est une *corestriction* de f' à F ou que f' est un *coprolongement* de f à F' si pour tout $x \in E$ on a $f(x) = f'(x)$.

IV.12. proposition *Soit $E \subset F'$ et $f : E \to F$. Alors il existe un et un seul coprolongement f' de f à F'. Les graphes de f et f' sont égaux et $f'(E) = f(E)$.*

IV.13. preuve Soit $\mathcal{G}$ le graphe de f. Puisque $F \subset F'$ on a $\mathcal{G} \subset E \times F \subset E \times F'$. Soit $x \in E$. On a $f(x) \in F \subset F'$ et $(x, f(x)) \in \mathcal{G}$. Soit $y' \in F'$ tel que $(x, y') \in \mathcal{G}$. On a donc $(x, y') \in E \times F$ et donc $y' \in F$. Or, puisque $\mathcal{G}$ est le graphe de f, nécessairement $y' = f(x)$. Ceci prouve que si $x \in E$ il existe un et un seul $y' \in F'$ tel que $(x, y') \in \mathcal{G}$, c'est $y' = f(x)$. Ainsi $\mathcal{G}$ est bien le graphe d'une application f' de E dans F', et on a pour tout $x \in E$, $f(x) = f'(x)$. L'application f' est un coprolongement de f à F'.

Soit f'' un coprolongement de f à F'. Alors pour tout $x \in E$ on a $f''(x) = f(x) = f'(x)$. Par conséquent $f'' = f'$.

Soit $y \in f(E)$ et $y' \in f'(E)$. Il existe $x, x' \in E$ tels que $f(x) = y$ et $f'(x') = y'$. On a donc $f(x) = f'(x) = y \in f'(E)$ et $f'(x') = f(x') = y' \in f(E)$. Ainsi $f'(E) = f(E)$.

IV.14. proposition *Soit $F \subset F'$ et $f' : E \to F'$ telle que $f'(E) \subset F$. Alors il existe une unique corestriction f de f' à F. Les graphes de f et f' sont égaux et $f'(E) = f(E)$.*

IV.15. preuve Puisque $f'(E) \subset F$ son graphe $\mathcal{G}'$ est inclus dans $E \times F$. De plus si $x \in E$ il existe un et un seul $y' \in F'$ tel que $(x, y') \in \mathcal{G}'$ donc d'une part il existe au plus un $y \in F \subset F'$ tel que $(x, y) \in \mathcal{G}'$ mais d'autre part il en existe au moins un, $f'(x)$ qui est dans F par hypothèse. Ainsi $\mathcal{G}'$ est bien le graphe d'une application f de E dans F qui vérifie pour tout $x \in E$, $f(x) = f'(x)$. L'application f est une corestriction de f' à F.

Soit f'' une corestriction de f' à F. Alors pour tout $x \in E$ on a $f''(x) = f'(x) = f(x)$. Par conséquent $f'' = f$.

Soit $y \in f(E)$ et $y' \in f'(E)$. Il existe $x, x' \in E$ tels que $f(x) = y$ et $f'(x') = y'$. On a donc $f(x) = f'(x) = y \in f'(E)$ et $f'(x') = f(x') = y' \in f(E)$. Ainsi $f'(E) = f(E)$.

IV.16. proposition *Si E et F sont deux ensembles, il existe un ensemble noté E^F dont les éléments sont les applications de E dans F.*

IV.17. preuve Soit $\mathcal{G}$ l'ensemble des parties de $E \times F$. Alors l'ensemble E^F

est le sous-ensemble

$$E^F = \{f \in \mathcal{G} : \ (\forall x \in E \exists y \in F(x,y) \in f) \\ \wedge \\ (\forall (x,y,y') \in E \times F \times F(\{(x,y),(x,y')\} \subset f) \Rightarrow y = y')\}.$$

IV.18. remarque Si F est un ensemble alors $\emptyset^F = \{(\emptyset, F, \emptyset)\}$. Si E est un ensemble non vide alors $E^\emptyset = \emptyset$.

IV.19. proposition *Soit $f : E \to F$ et $g : F' \to H$ deux applications de graphes $\mathcal{F}$ et $\mathcal{G}$. Si $F \subset F'$ alors l'ensemble*

$$\mathcal{H} = \{(x,z) \in E \times H : \exists y \in F \ (x,y) \in \mathcal{F} \text{ et } (y,z) \in \mathcal{G}\}$$

est le graphe d'une application h de domaine E et d'ensemble d'arrivée H. Si $x \in E$ alors $(x, g(f(x))) \in \mathcal{H}$.

IV.20. preuve Soit $x \in E$. Alors le couple $(x, g(f(x))) \in \mathcal{H}$ car $(x, f(x)) \in \mathcal{F}$, donc $f(x) \in F \subset F'$ et par conséquent $g(f(x))$ existe et $(f(x), g(f(x))) \in \mathcal{G}$. Ainsi il existe bien un couple $(x,z) \in \mathcal{H}$. De plus si $(x,z') \in \mathcal{H}$ alors il existe $y' \in F$ tel que $(x,y') \in \mathcal{F}$ et $(y',z') \in \mathcal{G}$. Puisque (x,y') est dans le graphe de f on a nécessairement $y' = f(x) = y$. Puisque $(y,z') = (y',z')$ est dans le graphe de g on a nécessairement $z' = g(y') = g(y) = z$ et donc $z' = g(f(x)) = z$. Ainsi il existe un et un seul $z \in H$ tel que $(x,z) \in \mathcal{H}$ et $\mathcal{H}$ est bien le graphe d'une application de E dans H.

IV.21. définition Soit $f : E \to F$ et $g : F' \to H$ deux applications de graphes $\mathcal{F}$ et $\mathcal{G}$. Si $F \subset F'$ l'application dont le graphe est l'ensemble

$$\mathcal{H} = \{(x,z) \in E \times H : \exists y \in F \ (x,y) \in \mathcal{F} \text{ et } (y,z) \in \mathcal{G}\}$$

est appelée *composée f suivie de g* et est notée $g \circ f$ (lire g rond f). On a $(g \circ f)(x) = g(f(x))$ si $x \in E$.

IV.22. exemple Si $f : E \to F$ alors $f = Id_F \circ f = f \circ Id_E$.

IV.23. proposition *Soit E, F, F' et G quatre ensembles tels que $F \subset F'$. Alors l'ensemble*

$$\mathcal{H} = \{(f,g,h) \in E^F \times {F'}^G \times E^G : \forall x \in E, h(x) = g(f(x))\}$$

est le graphe d'une application de $E^F \times {F'}^G$ dans E^G appelée composée. Si $(f,g,h) \in \mathcal{H}$ alors $h = g \circ f$.

IV.24. proposition *Si $f : E \to F$, $g : F' \to H$, $h : H' \to K$ telles que $F \subset F'$ et $H \subset H'$ alors $h \circ (g \circ f) = (h \circ g) \circ f$.*

IV.25. preuve Soit $x \in E$. On a

$$\begin{aligned} h \circ (g \circ f)(x) &= h(g \circ f(x)) \\ &= h(g(f(x))) \\ &= (h \circ g)(f(x)) \\ &= (h \circ g) \circ f(x). \end{aligned}$$

IV.26. définition Soit $f : E \to F$ une application. Elle est dite *injective* si deux éléments distincts quelconques de E ont toujours des images distinctes, c'est à dire si pour tout $y \in F$ l'ensemble $f^{-1}(\{y\})$ est vide ou un singleton. Elle est dite *surjective* si tout élément de F admet au moins un antécédent c'est à dire si $f(E) = F$. Elle est dite *bijective* si elle est à la fois injective et surjective. Une *injection* est une application injective, une *surjection* est une application surjective et une *bijection* est une application bijective.

IV.27. exemple Soit F un ensemble. La seule application de $\emptyset$ dans F est $(\emptyset, F, \emptyset)$ qui est clairement injecive. Elle est surjective donc bijective si et seulement si $F = \emptyset$.

IV.28. exemple Si E est un ensemble alors Id_E est une bijection.

IV.29. proposition *La restriction, la corestriction ou le coprolongement d'une injection sont injectifs.*

IV.30. preuve Soit f une application injective et f' une application qui est soit une restriction, soit une corestriction, soit un coprolongement de f. Soit x, x' dans le domaine de f' et tels que $f'(x) = f'(x')$. Alors on a $f(x) = f'(x) = f'(x') = f(x')$. Puisque f est injective on a $x = x'$. Ceci prouve que f' est injective.

IV.31. exemple Si $E \subset F$ le coprolongement de Id_E à F est une injection appelée *injection canonique* ou *inclusion* de E dans F.

IV.32. proposition *Soit $f : E \to F$ et $g : F \to G$ deux applications. 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 $g \circ f$ est injective alors f est injective. Si $g \circ f$ est surjective alors g est surjective.*

IV.33. preuve On suppose f et g injectives. Soit $z \in G$ et x, x' tels que $g \circ f(x) = g \circ f(x') = z$. On a donc $g(f(x)) = g(f(x')) = z$. Puisque g est

injective on a donc $f(x) = f(x')$. Puisque f est injective on a donc $x = x'$. Ainsi $g \circ f$ est injective dès que f et g le sont.

On suppose f et g surjectives. Soit $z \in G$. Puisque g est surjective il existe $y \in F$ tel que $g(y) = z$. Puisque f est surjective il existe $x \in E$ tel que $f(x) = y$. On a doncc $g \circ f(x) = g(f(x)) = z$. Ainsi $g \circ f$ est surjective dès que f et g le sont.

On suppose que f n'est pas injective. Il existe donc $y \in F$ et $x, x' \in E$ tels que $x \neq x'$ et $f(x) = f(x') = y$. Soit $z = g(y)$. On a $g(f(x)) = g(f(x')) = z$ et donc $g \circ f(x) = g \circ f(x') = z$ alors que $x \neq x'$. Ainsi $g \circ f$ n'est pas injective dès que f ne l'est pas. Par contraposée, f est injective dès que $g \circ f$ l'est.

On suppose que $g \circ f$ est surjective. Soit $z \in G$. Il existe $x \in E$ tel que $g \circ f(x) = z$. On a donc $g(f(x)) = z$. On pose $y = f(x)$. On a $g(y) = z$ et donc z a un antécédent par g. Ainsi g est surjective dès que $g \circ f$ est surjective.

IV.34. définition Soit $f : E \to F$ une application. Une application $g : F \to E$ est appelée *réciproque de f* ou *inverse de f pour la composition* si pour $x \in E$ et $y \in F$ on a $g(f(x)) = x$ et $f(g(y)) = y$.

IV.35. remarque Si g est une réciproque de f alors f est une réciproque de g.

IV.36. proposition *Si $g : F \to E$ et $g' : F \to E$ sont deux réciproques d'une application $f : E \to F$ alors $g = g'$.*

IV.37. preuve Soit $y \in F$. On a $f(g(y)) = y$. Or si $x \in E$ on a $g'(f(x)) = x$. Par conséquent on a $g'(y) = g'(f(g(y))) = g(y)$. Ainsi $g = g'$.

IV.38. proposition *Une application $f : E \to F$ possède une réciproque si et seulement si f est bijective.*

IV.39. preuve Supposons que f possède une réciproque g. Soit $y \in F$ alors $g(y)$ est un antécédent de y par f car $f(g(y)) = y$. Par conséquent f est surjective. Soit $x, x' \in E$ tels que $f(x) = f(x')$. Alors $x = g(f(x)) = g(f(x')) = x'$. Par conséquent f est injective. Ceci prouve que f est bijective si elle possède une réciproque.

Supposons f bijective. On note $\mathcal{G}$ son graphe et $\mathcal{G}'$ le sous-ensemble de $F \times E$ formé des (y, x) tels que $(x, y) \in \mathcal{G}$. Soit $y \in F$. Puisque f est surjective il existe $x \in E$ tel que $f(x) = y$: on a donc $(x, y) \in \mathcal{G}$ et par conséquent $(y, x) \in \mathcal{G}'$. Soit $x', x'' \in E$ tels que $(y, x'), (y, x'') \in \mathcal{G}'$. On a donc $f(x') = f(x'') = y$. Puisque f est injective on a donc $x' = x''$. Ceci prouve

que $\mathcal{G}'$ est le graphe d'une application g de F dans E.

Soit $x \in E$. On a $(x, f(x)) \in \mathcal{G}$ donc $(f(x), x) \in \mathcal{G}'$ c'est à dire $g(f(x)) = x$. Soit $y \in F$. On a $(y, g(y)) \in \mathcal{G}'$ donc $(g(y), y) \in \mathcal{G}$ c'est à dire $f(g(y)) = y$.

On vient de prouver que si $x \in E$ et $y \in F$ alors $g(f(x)) = x$ et $f(g(y)) = y$. L'application g est une réciproque de f.

IV.40. notation Si $f : E \to F$ admet une réciproque alors cette réciproque, qui est unique est noté f^{-1}.

IV.41. corollaire *La réciproque f^{-1} d'une bijection est également une bijection.*

IV.42. preuve En effet puisque f^{-1} admet une réciproque, l'application f et qu'une condition nécessaire et suffisante pour admettre une réciproque est d'être bijective.

IV.43. définition D'après ce qui précède, s'il existe une bijection d'un premier ensemble dans un second, il existe aussi une bijection du second dans le premier. C'est pourquoi on dit que deux ensembles sont *en bijection* s'il existe une bijection de l'un dans l'autre.

IV.44. proposition *Soit $f : E \to F$ une bijection et $g : F \to E$. Si pour tout $x \in E$ on a $g(f(x)) = x$ alors g est la réciproque de f. Si pour tout $y \in F$ on a $f(g(y)) = y$ alors g est la réciproque de f.*

IV.45. preuve On suppose que pour tout $x \in E$ on a $g(f(x)) = x$. Soit $y \in F$. On a $f^{-1}(y) \in E$ donc $g(f(f^{-1}(y))) = f^{-1}(y)$. or $f(f^{-1}(y)) = y$. Donc on a $g(y) = f^{-1}(y)$. Ainsi $g = f^{-1}$.

On suppose que pour tout $y \in F$ on a $f(g(y)) = y$. Soit $y \in F$. On a $f^{-1}(f(g(y))) = f^{-1}(y)$. Or $f^{-1}(f(g(y))) = f^{-1} \circ f(g(y)) = g(y)$. Donc $f^{-1}(y) = g(y)$. Ainsi $f^{-1} = g$.

IV.46. exemple Soit $f : E \to F$ une application et $\mathcal{G}$ son graphe. Alors E et $\mathcal{G}$ sont en bijection : l'application qui à $x \in E$ associe $(x, f(x)) \in \mathcal{G}$ est une bijection.

IV.47. proposition *Soit $f : E \to F$ et $g, h : F \to E$ telles que si $x \in E$ et $y \in F$ alors $g(f(x)) = x$ et $f(h(y)) = y$. Alors f est bijective et $f^{-1} = g = h$.*

IV.48. preuve Soit $y \in F$. On a $f(h(y)) = y$. Or si $x \in E$ on a $g(f(x)) = x$. Par conséquent on a $h(y) = h(f(g(y))) = g(y)$. Ainsi $g = h$. Ceci implique que g est la réciproque de f et donc que f est bijective.

IV.49. définition Soit E un ensemble et $f \in E^E$. On dit que f est une

involution si $f \circ f = Id_E$ c'est à dire si f est son propre inverse.

IV.50. définition Soit E un ensemble et $a, b \in E$. La *transposition de a et b* est l'application σ_{ab}^E définie par $\sigma_{ab}^E(a) = b$, $\sigma_{ab}^E(b) = a$ et $\sigma_{ab}^E(x) = x$ si $x \in E \setminus \{a, b\}$.

IV.51. remarque Soit E un ensemble et $a, b \in E$. La transposition σ_{ab}^E est l'identité si et seulement si $a = b$.

IV.52. proposition *Les transpositions sont des involutions.*

IV.53. preuve Soit E un ensemble et $a, b \in E$. Alors $\sigma_{ab}^E(\sigma_{ab}^E(a)) = \sigma_{ab}^E(b) = a$, $\sigma_{ab}^E(\sigma_{ab}^E(b)) = \sigma_{ab}^E(a) = b$ et si $x \in E \setminus \{a, b\}$ alors $\sigma_{ab}^E(\sigma_{ab}^E(x)) = \sigma_{ab}^E(x) = x$. On a donc bien $\sigma_{ab} \circ \sigma_{ab} = Id_E$.

IV.54. remarque Une transposition est une bijection puisque elle possède un inverse, elle même.

IV.55. proposition *Soit $f : E \to F$. Si f est injective alors il existe une surjection $g : F \to E$ telle que si $x \in E$ alors $g(f(x)) = x$. Si f est surjective alors il existe une injection $g : F \to E$ telle que si $y \in F$ alors $f(g(y)) = y$.*

IV.56. preuve On suppose f injective. Alors la corestriction f' de f à $F' = f(E)$ est injective comme f. Elle est surjective car $f'(E) = f(E) = F'$. Soit $f'^{-1} : F' \to E$ la réciproque de f'. On a $f'^{-1}(F') = E$. On a aussi $F' \subset F$. Il existe donc un prolongement g de f'^{-1} à F. Si $x \in E$ alors $f(x) = f'(x) \in F'$ et donc $g(f(x)) = g(f'(x)) = f'^{-1}(f'(x)) = x$. En particulier $f(x)$ est un antécédent de x par g. Par conséquent g est surjective.

On suppose f surjective. On considère le sous-ensemble $\mathcal{E}$ des parties de E formé des images réciproques $f^{-1}(\{y\})$ lorsque y décrit F :

$$\mathcal{E} = \{f^{-1}(\{y\}) : y \in F\}.$$

Puisque f est surjective l'ensemble vide $\emptyset$ n'est pas un élément de $\mathcal{E}$. D'après l'axiome du choix, il existe un ensemble E' tel que pour tout $y \in F$ l'intersection $f^{-1}(\{y\}) \cap E'$ est un singleton ($f^{-1}(\{y\}) \cap E' \subset E$ car $f^{-1}(\{y\}) \subset E$). Par conséquent l'ensemble

$$\{(y, x) \in F \times E : x \in f^{-1}(\{y\}) \cap E'\}$$

est le graphe d'une application g de F dans E. De plus, si $y \in F$ alors $g(y)$ est l'unique élément de $f^{-1}(\{y\}) \cap E'$ par conséquent $f(g(y)) = y$. Enfin g est injective car si $y, y' \in F$ et $g(y) = g(y')$ alors $y = f(g(y)) = f(g(y')) = y'$.

IV.57. proposition *Soit $f : E \to F$ de graphe $\mathcal{F}$ et $g : E \to G$ de graphe $\mathcal{G}$. Alors l'ensemble*

$$\mathcal{H} = \{(x, y, z) \in E \times F \times G : (x, y) \in \mathcal{F}, (x, z) \in \mathcal{G}\}$$

est le graphe d'une application $h : E \to F \times G$ telle que si $x \in E$ alors $h(x) = (f(x), g(x))$.

IV.58. preuve Soit $x \in E$. Alors le triplet $(x, f(x), g(x)) \in \mathcal{H}$ car $(x, f(x)) \in \mathcal{F}$ et $(x, g(x)) \in \mathcal{G}$. Ainsi il existe bien un triplet $(x, y, z) \in \mathcal{H}$. De plus si $(x, y', z') \in \mathcal{H}$ alors $(x, y') \in \mathcal{F}$ donc $y' = f(x) = y$ et $(x, z') \in \mathcal{G}$ donc $z' = g(x) = z$. Ainsi il existe un et un seul $(y, z) \in F \times G$ tel que $(x, y, z) \in \mathcal{H}$, c'est $(f(x), g(x))$ et $\mathcal{H}$ est bien le graphe d'une application de E dans $F \times G$.

IV.59. définition Soit $f : E \to F$ de graphe $\mathcal{F}$ et $g : E \to G$ de graphe $\mathcal{G}$ deux applications définies sur le même ensemble de départ. Alors l'application de graphe

$$\mathcal{H} = \{(x, y, z) \in E \times F \times G : (x, y) \in \mathcal{F}, (x, z) \in \mathcal{G}\}$$

est notée (f, g). Si $x \in E$ alors $(f, g)(x) = (f(x), g(x))$.

IV.60. proposition *Soit $f : E \to F$ de graphe $\mathcal{F}$ et $f' : E' \to F'$ de graphe $\mathcal{F}'$ deux applications. Alors l'ensemble*

$$\mathcal{H} = \{(x, x'), (y, y') \in (E \times E') \times (F \times F') : (x, y) \in \mathcal{F}, (x', y') \in \mathcal{F}\}$$

est le graphe d'une application $h : E \times E' \to F \times F'$ telle que si $(x, x') \in E \times E'$ $h(x, x') = (f(x), f'(x'))$.

IV.61. preuve Soit $(x, x') \in E \times E'$. Alors $((x, x'), (f(x), f'(x'))) \in \mathcal{H}$ car $(x, f(x)) \in \mathcal{F}$ et $(x', f'(x')) \in \mathcal{F}'$. Ainsi il existe bien triplet $((x, x'), (y, y')) \in \mathcal{H}$. De plus si $((x, x'), (z, z')) \in \mathcal{H}$ alors $(x, z) \in \mathcal{F}$ donc $z = f(x) = y$ et $(x', z') \in \mathcal{F}'$ donc $z' = f'(x') = z$. Ainsi il existe un et un seul $(z, z') \in F \times F'$ tel que $((x, x'), (z, z')) \in \mathcal{H}$ et $\mathcal{H}$ est bien le graphe d'une application h de $E \times E'$ dans $F \times F'$. Si $(x, x') \in E \times E'$ on a $h(x, x') = (f(x), f'(x'))$.

IV.62. proposition *Soit $f : E \to F$ de graphe $\mathcal{F}$ et $f' : E' \to F'$ de graphe $\mathcal{F}'$ deux applications et soit $h : E \times E' \to F \times F'$ l'application de*

$$\mathcal{H} = \{(x, x'), (y, y') \in (E \times E') \times (F \times F') : (x, y) \in \mathcal{F}, (x', y') \in \mathcal{F}\}.$$

L'application h est injective si et seulement si f et et f' le sont. Elle est surjective si et seulement f et f' le sont.

IV.63. preuve On suppose h injective. Soit $(x, x') \in E \times E'$ et $(t, t') \in E \times E'$. Si $f(x) = f(t)$ alors $h(x, x') = (f(x), f'(x')) = (f(t), f'(x')) = h(t, x')$. Puisque h est injective, on a $(x, x') = (t, x')$ et donc $x = t$. Ainsi f est injective. Si $f'(x') = f'(t')$ alors $h(x, x') = (f(x), f'(x')) = (f(x), f'(t')) = h(x, t')$. Puisque h est injective, on a $(x, x') = (x, t')$ et donc $x' = t'$. Ainsi f' est injective.

On suppose que f et f' sont injectives. Soit $(x, x') \in E \times E'$ et $(t, t') \in E \times E'$ tels que $h(x, x') = h(t, t')$. Ceci signifie $(f(x), f'(x')) = (f(t), f'(t'))$ et donc $f(x) = f(t)$ et $f'(x') = f'(t')$. Puisque f et f' sont injectives ceci implique que $x = t$ et $x' = t'$ c'est à dire $(x, x') = (t, t')$. Ainsi h est injective.

Si $(x, x') \in E \times E'$ alors $h(x, x') = (f(x), f(x'))$. Par conséquent, si $(y, y') \in F \times F'$ pour qu'il existe $(x, x') \in E \times E'$ tel que $h(x, x') = (y, y')$ il faut et il suffit qu'il existe $(x, x') \in E \times E'$ tel que $f(x) = y$ et $f'(x') = y'$. Par conséquent h est surjective si et seulement si f et f' le sont.

IV.64. proposition *Soit $f : E \to F$ de graphe $\mathcal{F}$ et $f' : E' \to F'$ de graphe $\mathcal{F}'$ deux applications. On suppose que $E \cap E' = \emptyset$. Alors $\mathcal{G} = \mathcal{F} \cup \mathcal{F}'$ est le graphe d'une application $g : E \cup E' \to F \cup F'$ telle que $g(x) = f(x)$ si $x \in E$ et $g(x) = f'(x')$. On a $g(E \cup E') = f(E) \cup f'(E')$. Si f et f' sont des bijections et $F \cap F' = \emptyset$ alors g est une bijection.*

IV.65. preuve Soit $a \in E \cup E'$. Alors $a \in E$ et $f(a) \in F$, $(a, f(a)) \in \mathcal{F} \subset \mathcal{G}$, ou $a \in e'$ et $f'(a) \in F'$, $(a, f'a)) \in \mathcal{F}' \subset \mathcal{G}$. Dans tous les cas il existe $b \in F \cup F'$ tel que $(a, b) \in \mathcal{G}$.

Soit $(a, b) \in \mathcal{G}$. Alors $(a, b) \in \mathcal{F}$ ou $(a, b) \in \mathcal{F}'$. Si $(a, b) \in \mathcal{F}$ alors $a \in E$, $b = f(a) \in F$ et $(a, b) \in (E \cup E') \times (F \cup F')$. Si $(a, b) \in \mathcal{F}'$ alors $a \in E'$, $b = f'(a) \in F'$ et $(a, b) \in (E \cup E') \times (F \cup F')$. Ceci prouve que $\mathcal{G} \subset (E \cup E') \times (F \cup F')$.

Soit $(a, b), (a, b') \in \mathcal{G}$. Alors soit $a \in E$ soit $a \in E'$. Si $a \in E$ alors $a \notin E'$ donc $(a, b), (a, b') \in \mathcal{F}$ et $b = b' = f(a)$. Si $a \in E'$ alors $a \notin E$ donc $(a, b), (a, b) \in \mathcal{F}'$ et $b = b' = f('a)$.

Ceci prouve que $\mathcal{G}$ est le graphe d'une application g de $E \cup E'$ dans $F \cup F'$ telle que $g(x) = f(x)$ si $x \in E$ et $g(x) = f'(x')$.

On suppose que f et f' sont des bijections et que $F \cap F' = \emptyset$. Soit $b \in F \cup F'$. Si $b \in F$ alors pour tout $a' \in E'$ $g(a') = f'(a') \neq b$ car $F \cap F' = \emptyset$. De plus puisque f est bijective et que la restriction de g à E est égale au coprolongement de f à $F \cup F'$, il existe un unique $a \in E$ tel que $g(a) = f(a) = b$. C'est le seul antécédent de b par g : l'application g est bien bijective.

V. Relation d'ordre total et ensemble bien ordonné

V.1. définition Soit E un ensemble. Une *relation binaire* $\mathcal{R}$ définie sur E est un sous-ensemble de $E \times E$. Soit $(x, y) \in E \times E$. On écrit $x\mathcal{R}y$ ou $\mathcal{R}(x, y)$ si $(x, y) \in \mathcal{R}$.

V.2. définition Soit E un ensemble muni d'une relation binaire $\mathcal{R}$. La relation $\mathcal{R}$ est dite *réflexive* si pour tout $x \in E$ on a $x\mathcal{R}x$. Elle est dite *transitive* si pour tout $(x, y, z) \in E \times E \times E$ tel que $x\mathcal{R}y$ et $y\mathcal{R}z$ on a $x\mathcal{R}z$. Elle est dite *anti-symétrique* si pour tout $(x, y) \in E \times E$ tel que $x\mathcal{R}y$ et $y\mathcal{R}x$ on a $x = y$. La relation $\mathcal{R}$ est une *relation d'ordre* ou un *ordre* si elle est réflexive, transitive et antisymétrique. C'est une *relation d'ordre total* ou un *ordre total* si c'est une relation d'ordre et si pour tout $(x, y) \in E \times E$ on a $x\mathcal{R}y$ ou $y\mathcal{R}x$.

V.3. proposition *Soit E un ensemble muni d'une relation d'ordre $\mathcal{R}$ et soient $x, y, z \in E$ tels que $x\mathcal{R}y$ et $y\mathcal{R}z$. Si $x \neq y$ ou $y \neq z$ alors $x \neq z$.*

V.4. preuve Puisque $x\mathcal{R}y$ et $y\mathcal{R}z$ on a par transitivité $x\mathcal{R}z$. Si $x = z$ alors $z\mathcal{R}x$ et donc par transitivité on a $z\mathcal{R}y$ et $y\mathcal{R}x$. Ceci implique que $x = y = z$.

V.5. définition Soit $(E, \mathcal{R})$ un ensemble ordonné, c'est à dire un ensemble E muni d'une relation d'ordre $\mathcal{R}$. Un élément y de E est un *minorant* (respectivement *majorant*) d'un sous-ensemble X de E si pour tout $x \in X$ on a $y\mathcal{R}x$ (respectivement $x\mathcal{R}y$). Si un sous-ensemble X de E admet un minorant (respectivement majorant) on dit que X est minoré (respectivement majoré). Un élément y de E est un *plus petit élément* (respectivement *plus grand élément*) d'un sous-ensemble X de E si $y \in X$ et si c'est un minorant (respectivement majorant) de X. L'ensemble ordonné $(E, \mathcal{R})$ est dit bien ordonné et $\mathcal{R}$ est un *bon ordre* si tout sous-ensemble non vide de X possède un plus petit élément.

V.6. proposition *Soit $(E, \mathcal{R})$ un ensemble ordonné. Si x et y sont des plus petits éléments (respectivement plus grands éléments) d'un sous-ensemble non vide $X \subset E$ alors $x = y$.*

V.7. preuve Supposons par exemple que x et y soient des plus petits éléments de X. Alors x et y sont des éléments de X et $x\mathcal{R}y$ (x est un plus petit élément de X) et $y\mathcal{R}x$ (y est un plus petit élément de X). Puisque $\mathcal{R}$ est antisymétrique $x = y$. Le cas où x et y sont des plus grands éléments de X se traite de façon analogue.

V.8. proposition *Soit $(E, \mathcal{R})$ un ensemble bien ordonné. Alors $\mathcal{R}$ est un ordre total.*

V.9. preuve Puisque E est bien ordonné si x et y sont deux éléments de E le sous-ensemble $\{x, y\}$ admet un plus petit élément. Si c'est x alors $x\mathcal{R}y$ et si c'est y alors $y\mathcal{R}x$. Ainsi l'ordre $\mathcal{R}$ est bien total.

V.10. notation On note souvent une relation d'ordre avec le symbole $\leq$. Lorsqu'on écrit $x \leq y$ on lit *x est inférieur ou égal à y* ou *y est supérieur ou égal à y*. L'assertion « $x \leq y$ et $x \neq y$ » est notée $x < y$. Lorsqu'on écrit $x < y$ on lit *x est strictement inférieur à y* ou *y est strictement supérieur à y*. Les symboles $\geq$ et $>$ sont définis de la façon suivante : l'assertion $x \leq y$ est équivalente à l'assertion $y \geq x$ et l'assertion $x < y$ est équivalente à l'assertion $y > x$.

V.11. définition Une application $f : E \to E'$ entre deux ensembles ordonnés $(E, \mathcal{R})$ et $(E', \mathcal{R}')$ est dite *croissante* (respectivement *décroissante*) si pour tout $(x, y) \in E \times E$ tel que $x\mathcal{R}y$ on a $f(x)\mathcal{R}'f(y)$ (respectivement $f(y)\mathcal{R}'f(x)$). Elle est dite *strictement croissante* (respectivement *strictement décroissante*) si elle est injective et croissante (respectivement décroissante). Un *isomorphisme d'ensembles ordonnés* est une bijection $f : E \to E'$ entre deux ensembles ordonnés $(E, \mathcal{R})$ et $(E', \mathcal{R}')$ telle que f et f^{-1} soient strictement croissantes.

V.12. proposition *Soient $f : E \to E'$ une bijection entre deux ensembles totalement ordonnés $(E, \mathcal{R})$ et $(E', \mathcal{R}')$. Il suffit que l'application f soit strictement croissante pour que ce soit un isomorphisme d'ensembles ordonnés.*

V.13. preuve Il suffit de montrer que si $x', y' \in E'$ sont tels que $x'\mathcal{R}'y'$ et $x' \neq y'$ alors $f^{-1}(x')\mathcal{R}f^{-1}(y')$ et $f^{-1}(x') \neq f^{-1}(y')$. Si ce n'est pas le cas alors $f^{-1}(x') = f^{-1}(y')$ ou $f^{-1}(y')\mathcal{R}f^{-1}(x')$ et $f^{-1}(x')\mathcal{R}f^{-1}(y')$. Puisque f est bijective et que $x' \neq y'$, nécessairement $f^{-1}(x') \neq f^{-1}(y')$. Si $f^{-1}(y')\mathcal{R}f^{-1}(x')$ on aurait alors, puisque f est strictement croissante

$$y' = f(f^{-1}(y'))\mathcal{R}f(f^{-1}(x')) = x'$$

et donc $y'\mathcal{R}x'$. Puisque par hypothèse $x'\mathcal{R}y'$ on aurait donc en raison de l'antisymétrie de $\mathcal{R}'$ l'égalité $x' = y'$. C'est la contradiction recherchée qui établit que

$$f^{-1}(x')\mathcal{R}f^{-1}(y') \text{ et } f^{-1}(x') \neq f^{-1}(y').$$

VI. Loi, groupe et respect

Dans cette partie nous allons enfreindre le principe du début qui était d'éviter le recours aux quantificateurs.

VI.1. définition Soit E un ensemble. Une *loi de composition interne* sur E est une application $\top$ de $E \times E$ dans E. Si $x, y \in E$ on pose

$$\top(x, y) = x \top y.$$

La loi $\top$ est dite *associative* si

$$\forall (x, y, z) \in E^3 \; x \top (y \top z) = (x \top y) \top z.$$

Elle est dite *commutative* si

$$\forall (x, y) \in E^2 \; x \top y = y \top x.$$

Un élément $e \in E$ est appelé *neutre* pour $\top$ si

$$\forall x \in E \; x \top e = e \top x = x.$$

Un élément $a \in E$ est dit *absorbant* pour $\top$ si

$$\forall x \in E \; x \top a = a \top x = a.$$

VI.2. exemple Si E un ensemble non vide la composition des applications induit sur E^E une loi de composition interne : si $f, g \in E^E$ alors $g \circ f$ est définie et appartient à E^E. Cette loi est associative et admet comme neutre l'identité de E, Id_E.

VI.3. exemple Soit E un ensemble. Supposons qu'il existe $a, b, c \in E$ tels que $a \neq b, c$ et $b \neq c$. On note f la transposition σ_{ab}^E et g la transposition σ_{ac}. Alors $g \circ f(a) = b$ et $f \circ g(a) = c$ donc $f \neq g$ et $\circ$ n'est pas commutative.

VI.4. proposition *Si $\top$ est une loi de composition interne sur E alors elle admet au plus un neutre et au plus un élément absorbant.*

VI.5. preuve Si e et e' sont des neutres pour $\top$ alors on a

$$e = e \top e' = e'.$$

Si a et a' sont absorbants pour $\top$ alors on a

$$a = a \top a' = a'.$$

VI.6. définition Soit E un ensemble muni d'une loi de composition interne $\top$. On suppose que la loi $\top$ possède un neutre e. Alors deux éléments x et y de E sont dits *inverses* l'un de l'autre pour $\top$ si

$$x \top y = y \top x = e.$$

VI.7. exemple On a déjà vu qu'une application $f \in E^E$ admet un inverse pour la composition des applications si et seulement si elle est bijective. C'est le cas par exemple d'une involution : elle est son propre inverse.

VI.8. proposition *Soit E un ensemble muni d'une loi de composition interne $\top$. On suppose que la loi $\top$ possède un neutre e et qu'elle est associative. Si y et z sont les inverses d'un élément x de E alors $y = z$.*

VI.9. preuve En raison de l'associativité de $\top$ on a

$$y = y \top e = y \top (x \top z) = (y \top x) \top z = e \top z = z.$$

VI.10. définition Soit E un ensemble muni de deux lois de compositions internes $\top$ et $\perp$. La loi $\perp$ est dite *distributive* par rapport à la loi $\top$ si

$$\forall (x,y,z) \in E^3 \quad \begin{array}{c} x \perp (y \top z) = (x \perp y) \top (x \perp z) \\ \text{et} \\ (x \top y) \perp z = (x \perp z) \top (y \perp z). \end{array}$$

VI.11. définition Un *groupe* est un couple $(G, \top)$ où G est un ensemble non vide et $\top$ est une loi de composition interne associative qui admet un élément neutre et telle que tout élémentde G admet un inverse. Si de plus $\top$ est commutative on dit que $(G, \top)$ est un *groupe commutatif.*

VI.12. notation Si E est un ensemble on note $\mathcal{S}(E)$ le sous-ensemble de E^E formé des bijections de E dans E.

VI.13. proposition *L'ensemble $\mathcal{S}(E)$ des bijections d'un ensemble E dans lui-même est un sous-ensemble de E^E stable pour la composition des applications et $(\mathcal{S}(E), \circ)$ est un groupe.*

VI.14. preuve L'identité de E, Id_E est une bijection donc $\mathcal{S}(E)$ est non vide. Puisque la composée de deux bijections est une bijection, le sous-ensemble $\mathcal{S}(E)$ est stable par composition. La composition des applications est associative. Puisqu'une bijection admet un inverse pour la composition qui est également une bijection, tout élément de $(\mathcal{S}(E), \circ)$ possède un inverse.

VI.15. proposition *S'il existe* $a, b, c \in E$ *tels que* $a \neq b, c$ *et* $b \neq c$ *alors* $(\mathcal{S}(E), \circ)$ *n'est pas un groupe commutatif.*

VI.16. preuve Les transposition σ_{ab}^E et σ_{ac}^E sont des éléments de $\mathcal{E}$ puisque ce sont des involutions donc des bijections et elles ne commutent pas.

VI.17. définition Soit $(E, \mathcal{R}, \top)$ un ensemble muni d'une relation d'ordre et d'une loi de composition interne. La loi $\top$ *respecte* l'ordre $\mathcal{R}$ si

$$\forall (x, y, z) \in E^3 \ ((x \mathcal{R} y) \Rightarrow (((x \top z) \mathcal{R} (y \top z)) \wedge ((z \top x) \mathcal{R} (z \top y)))).$$

VI.18. remarque On dit plus souvent que la relation d'ordre est *compatible* ou *respecte* la loi. La définition précédente vaut plus généralement pour toute relation binaire.

VI.19. définition Soit $(E, \mathcal{R}, \top)$ un ensemble muni d'une relation d'ordre et d'une loi de composition interne. La loi $\top$ *respecte strictement* l'ordre $\mathcal{R}$ si elle respecte l'ordre et si

$$\forall (x, y, z) \in E^3 \ ((x \neq y) \Rightarrow (((x \top z) \neq (y \top z)) \wedge ((z \top x) \neq (z \top y)))).$$