ENSEMBLES, FONCTIONS, RELATIONS

PLAN

Ce chapitre vise à regrouper le vocabulaire usuellement appliqué aux ensembles, fonctions, relations, structures algébriques. Sa lecture en une seule fois est rebutante. Il vaut mieux s'y reporter régulièrement si on veut se référer précisément à une des notions introduites.

I : Vocabulaire

1- Règles usuelles et notations

En mathématiques, la notion d'ensemble et d'appartenance sont des notions primitives. Elles ne sont pas définies. Les règles d'utilisation sont régies par des **axiomes** (propositions supposées vraies a priori) qui ne sont pas détaillés ici. On se contentera d'une notion intuitive : un ensemble A est une collection d'éléments x. On note $x \in A$ pour dire qu'un élément x appartient à A et $x \notin A$ pour dire que x n'appartient pas à A.

Si P(x) est une propriété portant sur un élément x, on note :

$\forall\, x$, P(x) pour exprimer que P est vérifiée sur tout élément x. $\forall$ se lit *quel que soit*.

$\exists\, x$, P(x) pour exprimer que P est vérifiée sur au moins un élément x. $\exists$ se lit *il existe*.

$\forall$ et $\exists$ s'appellent des **quantificateurs** (respectivement universel et existentiel).

L'ensemble des x d'un ensemble A vérifiant P(x) se note $\{x \in E \mid P(x)\}$ ou $\{x \in E, P(x)\}$.

Si A et B sont deux ensembles, on dit que A est **inclus** dans B et on note $A \subset B$ si : $\forall\, x \in A$, $x \in B$ (quel que soit x appartenant à A, x appartient à B).

DEFINITIONS

A, B *et* C *étant les parties d'un ensemble* E, *on note* :

$A \cup B = \{x \in E \mid x \in A \text{ ou } x \in B\}$ (**réunion** *de* A *et* B. *Se lit* : A union B). *Le* ou *est pris au sens large* ; *l'une des deux proprétés au moins* $x \in A$, $x \in B$ *est vérifiée* (*et peut-être les deux*)

$A \cap B = \{x \in E \mid x \in A \text{ et } x \in B\}$ (**intersection** *de* A *et* B. *Se lit* A inter B)

$A^c = \{x \in E \mid x \notin A\}$ (**complémentaire** *de* A *dans* E), *parfois noté* $\complement A$, *ou* $\complement_E A$ *si on veut préciser aussi l'ensemble* E.

$A \setminus B = \{x \in E \mid x \in A \text{ et } x \notin B\} = A \cap B^c$ (**différence** *de* A *par* B. *Se lit* A moins B)

$A \Delta B = (A \setminus B) \cup (B \setminus A)$ est la **différence symétrique** de A et B.

$\varnothing$ *désigne l'***ensemble vide**, *ensemble qui ne possède aucun élément*.

On a ainsi $A \cap A^c = \varnothing$ puisqu'un élément x ne peut pas à la fois appartenir à A et ne pas lui appartenir. Plus généralement, deux parties A et B sont **disjointes** si $A \cap B = \varnothing$, i.e. il n'y a pas d'éléments communs à A et B. $A \setminus B$ se note aussi $A - B$.

PROPOSITION

A, B, C *étant des parties d'un ensemble* E, *on a* :

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

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

(iii) $(A \cap B)^c = A^c \cup B^c$

(iv) $(A \cup B)^c = A^c \cap B^c$

(v) $A \subset B \Leftrightarrow B^c \subset A^c$

(vi) $(A^c)^c = A$

Démonstration :

Une égalité de deux ensembles se montre par double inclusion.

❑ (i) Soit x élément de $A \cup (B \cap C)$. Alors $x \in A$ ou $x \in B \cap C$.

Si $x \in A$, alors a fortiori, $x \in A \cup B$ et $x \in A \cup C$, donc $x \in (A \cup B) \cap (A \cup C)$

Si $x \in B \cap C$, alors $x \in B$ (donc $x \in A \cup B$) et $x \in C$ (donc $x \in A \cup C$), donc $x \in (A \cup B) \cap (A \cup C)$.

Dans tous les cas, on a bien $x \in (A \cup B) \cap (A \cup C)$.

On a montré que $A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$

Réciproquement, soit x élément de $(A \cup B) \cap (A \cup C)$. On a donc $x \in A \cup B$ et $x \in A \cup C$.

Si $x \in A$, a fortiori $x \in A \cup (B \cap C)$

Si ce n'est pas le cas, alors, puisque $x \in A \cup B$, nécessairement $x \in B$, et puisque $x \in A \cup C$, nécessairement, $x \in C$. Donc $x \in B \cap C$, et a fortiori, $x \in A \cup (B \cap C)$.

Dans tous les cas, on a montré que $x \in A \cup (B \cap C)$.
On a montré que $(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$

Puisque les deux ensembles sont inclus l'un dans l'autre, ils ont exactement les mêmes éléments et sont égaux.

❑ (ii) laissé au lecteur

❑ (iii) On procède par équivalence, chaque affirmation étant remplacée par une affirmation ayant le même sens :

$x \in (A \cap B)^c$
$\Leftrightarrow$ $x \notin A \cap B$
$\Leftrightarrow$ x n'appartient pas simultanément aux deux ensembles A et B
$\Leftrightarrow$ x n'appartient pas à au moins l'un des deux ensembles A et B
$\Leftrightarrow$ $x \notin A$ ou $x \notin B$
$\Leftrightarrow$ $x \in A^c$ ou $x \in B^c$
$\Leftrightarrow$ $x \in A^c \cup B^c$

Il en résulte que $(A \cap B)^c$ et $A^c \cup B^c$ possèdent les mêmes éléments, donc sont égaux.

❑ (iv) laissé au lecteur

❑ (v) Supposons que $A \subset B$ et soit $x \in B^c$. Donc $x \notin B$. Il en résulte qu'on ne peut avoir $x \in A$ car l'inclusion $A \subset B$ impliquerait que $x \in B$, ce qui n'est pas vrai. Donc $x \notin A$, ou encore $x \in A^c$. On a bien montré que $B^c \subset A^c$. Ainsi, $A \subset B \Rightarrow B^c \subset A^c$. La réciproque est laissée au lecteur.

❑ (vi) $x \in (A^c)^c \Leftrightarrow x \notin A^c \Leftrightarrow x \in A$

EXEMPLES :

❑ $A - (B \cup C) = (A - B) \cap (A - C)$
car $A - (B \cup C) = A \cap (B \cup C)^c = A \cap B^c \cap C^c$
et $(A - B) \cap (A - C) = (A \cap B^c) \cap (A \cap C^c) = A \cap B^c \cap C^c$

❑ $A - (B \cap C) = (A - B) \cup (A - C)$
car $A - (B \cap C) = A \cap (B \cap C)^c = A \cap (B^c \cup C^c)$
$= (A \cap B^c) \cup (A \cap C^c) = (A - B) \cup (A - C)$

❑ $A - (B - A) = A$
car $A - (B - A) = A \cap (B - A)^c = A \cap (B \cap A^c)^c$
$= A \cap (B^c \cup A) = (A \cap B^c) \cup (A \cap A)$
$= (A \cap B^c) \cup A = A$ car $A \cap B^c \subset A$

❑ $A \cap (B - C) = (A \cap B) - (A \cap C) = (A \cap B) - C$
car $A \cap (B - C) = A \cap B \cap C^c = (A \cap B) - C$
et $(A \cap B) - (A \cap C) = A \cap B \cap (A \cap C)^c = A \cap B \cap (A^c \cup C^c)$
$= (A \cap B \cap A^c) \cup (A \cap B \cap C^c)$
$= \varnothing \cup (A \cap B \cap C^c)$

$= A \cap B \cap C^c = (A \cap B) - C$

DEFINITIONS

On peut définir une réunion ou une intersection quelconque, finie ou non. Si I *désigne un ensemble quelconque d'indices, on pose* :

$x \in \bigcup_{i \in I} A_i \Leftrightarrow \exists\, i,\ x \in A_i$ (x est dans l'un des A_i)

$x \in \bigcap_{i \in I} A_i \Leftrightarrow \forall\, i,\ x \in A_i$ (x est dans tous les A_i)

EXEMPLES :

❑ $\bigcup_{n \in \mathbb{N}^*} [\frac{1}{n}, 1] =]0, 1]$

En effet, si $x \in \bigcup_{n \in \mathbb{N}^*} [\frac{1}{n}, 1]$, alors $\exists\, n \in \mathbb{N}^*$, $x \in [\frac{1}{n}, 1]$ donc a fortiori, $0 < x \leq 1$. Réciproquement, si x vérifie $0 < x \leq 1$, on peut choisir n assez grand de façon que $\frac{1}{n} \leq x$, et donc, $\exists\, n$, $x \in [\frac{1}{n}, 1]$

❑ $\bigcap_{n \in \mathbb{N}^*} [1 - \frac{1}{n}, 1] = \{1\}$

En effet, si $x \in \bigcap_{n \in \mathbb{N}^*} [1 - \frac{1}{n}, 1]$, alors : $\forall\, n \in \mathbb{N}^*$, $1 - \frac{1}{n} \leq x \leq 1$. Ces inégalités étant vérifiées pour tout entier n, on peut passer à la limite, et on obtient $1 \leq x \leq 1$, donc $x = 1$. Réciproquement, si $x = 1$, il est clair que : $\forall\, n \in \mathbb{N}^*$, $1 - \frac{1}{n} \leq x \leq 1$

❑ $\bigcap_{n \in \mathbb{N}^*} [1 - \frac{1}{n}, 1[= \varnothing$

En effet, si on suppose qu'il existe x tel que $x \in \bigcap_{n \in \mathbb{N}^*} [1 - \frac{1}{n}, 1[$, alors, $\forall\, n \in \mathbb{N}^*$, $1 - \frac{1}{n} \leq x < 1$. Si on passe à la limite dans l'inégalité de gauche (tout en gardant celle de droite, qui ne dépend pas de n, inchangée), on obtient $1 \leq x < 1$ et donc $1 < 1$ ce qui est absurde. Aucun élément x ne peut donc appartenir à $\bigcap_{n \in \mathbb{N}^*} [1 - \frac{1}{n}, 1[$, qui est donc vide.

❑ Soit $(A_{n,m})$ une famille de parties indexées par n et m entiers. Posons :

$X = \bigcap_{n=0}^{\infty} \bigcup_{m=0}^{\infty} A_{n,m}$ et $Y = \bigcup_{m=0}^{\infty} \bigcap_{n=0}^{\infty} A_{n,m}$

Alors :

$x \in X \Leftrightarrow \forall\, n, \exists\, m, x \in A_{n,m} \Leftrightarrow$ pour tout n, x appartient à l'un des $A_{n,m}$ mais m peut dépendre de n

$x \in Y \Leftrightarrow \exists\, m, \forall\, n, x \in A_{n,m} \Leftrightarrow$ pour tout n, x appartient à $A_{n,m}$, m étant le même pour tout n

Donc $Y \subset X$. La réciproque est fausse en général.

PROPOSITION

(i) $A \cup (\bigcap_{i\in I} B_i) = \bigcap_{i\in I} (A \cup B_i)$

(ii) $A \cap (\bigcup_{i\in I} B_i) = \bigcup_{i\in I} (A \cap B_i)$

(iii) $(\bigcap_{i\in I} A_i)^c = \bigcup_{i\in I} A_i^c$

(iv) $(\bigcup_{i\in I} A_i)^c = \bigcap_{i\in I} A_i^c$

Démonstration :

❑ (i) Soit x élément de $A \cup (\bigcap_{i\in I} B_i)$. Alors $x \in A$ ou $x \in \bigcap_{i\in I} B_i$.

Si $x \in A$, alors, pour tout i, $x \in A \cup B_i$, donc $x \in \bigcap_{i\in I} (A \cup B_i)$

Si $x \in \bigcap_{i\in I} B_i$, alors, pour tout i, $x \in B_i$, donc $x \in A \cup B_i$, donc $x \in \bigcap_{i\in I} (A \cup B_i)$

Dans les deux cas, on a montré que $x \in \bigcap_{i\in I} (A \cup B_i)$.

On a donc montré que $A \cup (\bigcap_{i\in I} B_i) \subset \bigcap_{i\in I} (A \cup B_i)$

Réciproquement, soit x élément de $\bigcap_{i\in I} (A \cup B_i)$. Alors, pour tout i, $x \in A \cup B_i$.

Si $x \in A$, alors $x \in A \cup (\bigcap_{i\in I} B_i)$

Si ce n'est pas le cas, comme pour tout i, $x \in A \cup B_i$, alors $x \in B_i$, donc $x \in \bigcap_{i\in I} B_i$, et, a fortiori, $x \in A \cup (\bigcap_{i\in I} B_i)$

Dans les deux cas, on a montré que $x \in A \cup (\bigcap_{i\in I} B_i)$.

On a donc montré que $\bigcap_{i\in I} (A \cup B_i) \subset A \cup (\bigcap_{i\in I} B_i)$

Les deux inclusions ayant été montrée, on a $A \cup (\bigcap_{i\in I} B_i) = \bigcap_{i\in I} (A \cup B_i)$

❑ (ii) laissé au lecteur

❑ (iii) Soit x élément de $(\bigcap_{i\in I} A_i)^c$. Alors $x \notin \bigcap_{i\in I} A_i$, autrement dit, x n'appartient pas à tous les A_i. Il existe donc au moins un i tel que $x \notin A_i$, donc il existe i tel que $x \in A_i^c$, donc $x \in \bigcup_{i\in I} A_i^c$.

On a donc montré que $(\bigcap_{i\in I} A_i)^c \subset \bigcup_{i\in I} A_i^c$

Réciproquement, si x est élément de $\bigcup_{i\in I} A_i^c$, on peut remonter pas à pas le raisonnement précédent, permettant de montrer que $x \in (\bigcap_{i\in I} A_i)^c$, prouvant ainsi l'inclusion inverse.

❑ (iv) laissé au lecteur.

Toutes les parties de E, depuis l'ensemble vide ∅ jusqu'à E lui-même, forment un ensemble appelé **ensemble des parties** de E et noté $\mathcal{P}(E)$. Par exemple, si E = {0, 1, 2}, les parties de E sont ∅, {0}, {1}, {2}, {0, 1}, {0, 2}, {1, 2}, {1, 2, 3}, donc :

$\mathcal{P}(\{0, 1, 2\}) = \{\varnothing, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{1, 2, 3\}\}$

Etant donné deux ensembles E et F, on appelle **produit cartésien** et on note E × F l'ensemble des couples (x, y), où x est élément de E et y élément de F. Par exemple, l'ensemble des couples de réels est noté $\mathbb{R} \times \mathbb{R}$, ou $\mathbb{R}^2$. L'ensemble des n-uplets ou n-listes $(x_1, x_2, ..., x_n)$ d'éléments de E est noté E^n. L'ensemble des suites $(x_i)_{i\in I}$ d'éléments de E, indicées par un ensemble I fini ou non, est noté E^I.

2- Logique

Une proposition mathématique P est une phrase pouvant prendre les valeurs *vrai* ou *faux*. Par exemple, dans les entiers naturels :

P : $\forall\, n, \exists\, m, m = n^2$ est vrai

Q : $\forall\, n, \exists\, m, n = m^2$ est faux

Etant donné une proposition, le travail du mathématicien consiste à déterminer si elle est vraie ou fausse. S'il arrive à démontrer qu'elle est vraie, cette proposition est un **théorème**. Certaines propositions, considérées comme vraies a priori, sont à la base des théories mathématiques. Ce sont les **axiomes**. Par exemple, le principe de récurrence dans $\mathbb{N}$ ne se prouve pas. C'est un axiome, supposé vérifié.

On peut définir les opérations logiques suivantes portant sur diverses propositions :

a) <u>la conjonction</u> : "P et Q" est une proposition qui sera vraie si et seulement si les deux propositions P et Q sont simultanément vraies.

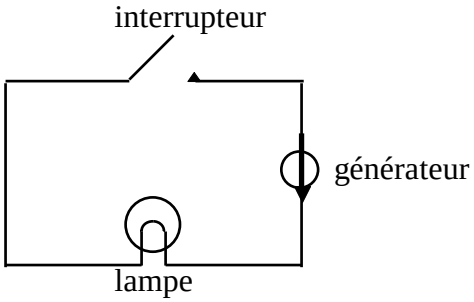
b) <u>la dijonction</u> : "P ou Q" est une proposition qui est vraie si et seulement si au moins une des deux propositions P ou Q est vraie. Les deux peuvent être vraies. le "ou" a un sens inclusif. (Il existe un "ou" exclusif, mais qui n'est pas utilisé de façon usuelle).

c) <u>l'équivalence</u> : "P ⇔ Q" est vraie si et seulement si P et Q sont simultanément vraies ou simultanément fausses, autrement dit, si P et Q ont même valeurs de vérité. Par exemple, dans $\mathbb{R}$:

$$x = e^y \Leftrightarrow x > 0 \text{ et } y = \ln(x)$$

L'équivalence peut s'appliquer à des propositions fausses. Par exemple, si on veut montrer qu'une proposition P est fausse, on peut chercher une proposition Q équivalente à P et montrer que Q est fausse.

d) <u>l'implication logique</u> : "P $\Rightarrow$ Q" est vraie si et seulement si P est fausse ou Q est vraie. Cette notion est la plus difficile à maîtriser, contrairement à ce qu'on peut penser au premier abord. Prenons un exemple pour illustrer ce fait. Considérons un circuit électrique en série constitué d'un générateur de courant, d'un interrupteur et d'une lampe.



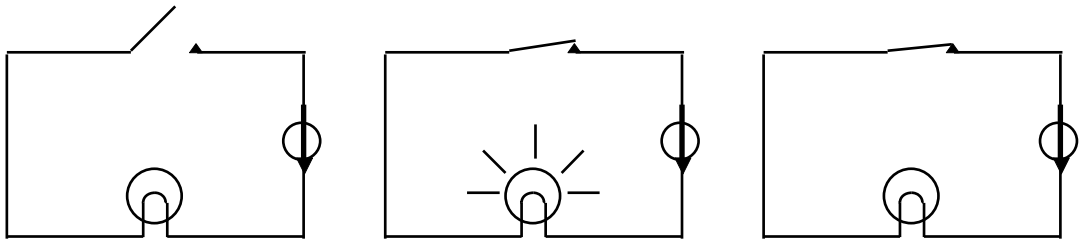
L'interrupteur peut être ouvert ou fermé ; la lampe peut être allumée ou éteinte.

Soit P la proposition : la lampe est allumée.

Soit Q la proposition : l'interrupteur est fermé.

Quelle est la relation d'implication logique entre P et Q ? A-t-on P $\Rightarrow$ Q ? Q $\Rightarrow$ P ? A-t-on l'équivalence P $\Leftrightarrow$ Q ? Précisons qu'on ne recherche pas une relation causale, telle que le conçoit le physicien. Nous cherchons une relation logique permettant de faire une déduction.

Il y a trois situations possibles :



interrupteur ouvert
lampe éteinte

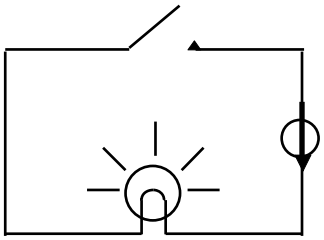
interrupteur fermé
lampe allumée

interrupteur fermé
lampe éteinte

situations les plus courantes

situation inhabituelle
mais pas impossible :
lampe grillée, voltage trop faible, ...

Une seule situation est impossible :



interrupteur ouvert
lampe allumée.

La seule implication *logique* est la suivante :

P ⇒ Q : si la lampe est allumée, alors l'interrupteur est fermé.

L'implication Q ⇒ P (si l'interrupteur est fermé, alors la lampe est allumée) correspond certes à une explication *causale* de l'allumage de la lampe, mais n'est possible que dans un monde idéal et parfait où les lampes ne tombent jamais en panne, et ne constitue en rien une conséquence logique.

On réfléchira au fait que toutes les phrases qui suivent ont la même signification :

P ⇒ Q	lampe allumée ⇒ interrupteur fermé
non Q ⇒ non P (**contraposée**)	interrupteur ouvert ⇒ lampe éteinte
si P alors Q	si la lampe est allumée, alors on en déduit que l'interrupteur est fermé.
P est **suffisant** pour Q il suffit P pour avoir Q	il suffit que la lampe soit allumée pour conclure que l'interrupteur est fermé.
P seulement si Q	la lampe est allumée seulement si l'interrupteur est fermé.
Q est **nécessaire** pour P il faut Q pour avoir P	il faut que l'interrupteur soit fermé pour que la lampe soit allumée.
non P ou Q	la lampe est éteinte, ou l'interrupteur est fermé

Il résulte de cela que l'implication est vérifiée dans les trois cas suivants (correspondant à nos trois dessins) :

P est vrai et Q est vrai
P est faux et Q est vrai
P est faux et Q est faux

Ainsi, si P est faux, Q est quelconque et il n'y a rien à montrer. La seule chose à montrer est donc bien que si P est vrai, alors Q est vrai.

L'implication est fausse dans le seul cas suivant :

P est vrai et Q est faux

Il ne peut y avoir d'implication, puisque l'hypothèse est vérifiée, mais pas la conclusion.

La **réciproque** de l'implication P ⇒ Q est Q ⇒ P. Elle peut être vraie ou fausse, indépendamment de la valeur de vérité de P ⇒ Q. Dans notre exemple, la réciproque est fausse. Toutes les phrases qui suivent sont équivalentes à Q ⇒ P. Elles sont donc fausses, le contre-exemple étant donné par le troisième dessin :

Q ⇒ P	interrupteur fermé ⇒ lampe allumée
non P ⇒ non Q (contraposée)	lampe éteinte ⇒ interrupteur ouvert
si Q alors P	si l'interrupteur est fermé, alors la lampe est allumée.
Q est suffisant pour P il suffit Q pour avoir P	il suffit que l'interrupteur soit fermé pour conclure que la lampe est allumée.
Q seulement si P	l'interrupteur est fermé seulement si la lampe est allumée.
P est nécessaire pour Q il faut P pour avoir Q	il faut que la lampe soit allumée pour conclure que l'interrupteur est fermé.
non Q ou P	l'interrupteur est ouvert, ou la lampe est allumée

Enfin, dire que P ⇒ Q et Q ⇒ P, c'est dire que P ⇔ Q.

e) la négation

La négation d'une proposition P est notée "non P". La négation d'une proposition P vraie sera fausse et la négation d'une proposition P fausse sera vraie.

La négation de "P et Q" est "non P ou non Q". En effet, dire que "P et Q" est fausse, c'est dire qu'une au moins des deux propositions est fausse.

La négation de "P ou Q" est "non P et non Q". En effet, nier le fait qu'au moins une des deux propositions est vraie, c'est dire qu'elles sont toutes deux fausses.

La négation de "P ⇒ Q" est "P et non Q". En effet, nous avons vu que "P ⇒ Q" est synonyme de "non P ou Q". La négation est donc bien "P et non Q". Dire que l'implication est fausse, c'est dire qu'on a l'hypothèse P, mais pas la conclusion Q.

La négation de "P ⇔ Q" est "(P et non Q) ou (Q et non P)".

La négation de "∀ x, P(x)" est "∃ x, non P(x)". En effet, dire qu'il est faux que P soit vraie pour tout x, c'est dire que P est faux pour au moins un x.

La négation de "$\exists\, x$, P(x)" est "$\forall\, x$, non P(x)". En effet, dire qu'il n'existe aucun x vérifiant P, c'est dire que tous les x vérifient la négation de P.

Il résulte des deux derniers cas que, pour prendre la négation d'une proposition enchaînant les quantificateurs $\forall$ et $\exists$, il suffit de lire la proposition de gauche à droite, de changer les $\forall$ en $\exists$, de changer les $\exists$ en $\forall$ puis de prendre la négation de ce qui reste.

EXEMPLE :

❑ La négation de :

$$\forall\, x, \forall\, \varepsilon > 0, \exists\, \delta > 0, \forall\, y, \left|y - x\right| < \delta \Rightarrow \left|f(x) - f(y)\right| < \varepsilon$$

est :

$$\exists\, x, \exists\, \varepsilon > 0, \forall\, \delta > 0, \exists\, y, \left|y - x\right| < \delta \text{ et } \left|f(x) - f(y)\right| \geq \varepsilon$$

(La première proposition si mystérieuse exprime la continuité d'une fonction f en tout point x. La deuxième exprime la non-continuité de f en un point x)

On notera enfin que :

$\forall\, x \in$ A, P(x) est une abréviation pour : $\forall\, x, x \in \text{A} \Rightarrow$ P(x)

et a donc pour négation :

$\exists\, x, x \in$ A et non P(x), ce qu'on abrège en : $\exists\, x \in$ A, non P(x)

De même, la négation de $\exists\, x \in$ A, P(x) est $\forall\, x \in$ A, non P(x).

On utilisera au besoin des parenthèses pour lever toute ambiguïté. Par exemple, dans les entiers, les deux propositions suivantes ont des sens différents. La première est vraie, la seconde est fausse.

$$\forall\, n, [(\forall\, m, mn \text{ pair}) \Rightarrow n \text{ pair}]$$

$$\forall\, n, [\forall\, m\, (mn \text{ pair} \Rightarrow n \text{ pair})]$$

En effet, dans la première proposition, n étant donné, on suppose que mn est pair pour tout entier m, en particulier pour $m = 1$. Donc n est pair. Dans la deuxième proposition, n étant donné, on suppose que c'est l'implication mn pair $\Rightarrow$ n pair qui est vraie pour tout m. Or cette implication est fausse pour $m = 2$ et $n = 3$ par exemple. $n = 3$ ne vérifie donc pas la condition demandée.

EXEMPLE :

❑ On considère une propriété P définie sur $\mathbb{N}$. P(n) est vraie ou fausse suivant les valeurs de n.

Considérons les propositions suivantes.

a) P(n) n'est vraie que pour un nombre fini de valeurs n.

Cela est équivalent à : $\exists$ N, $\forall\, n \geq$ N, non (P(n)).

b) P(n) est vraie pour toute valeur de n, sauf un nombre fini.

Cela est équivalent à : $\exists$ N, $\forall\, n \geq$ N, P(n).

c) P(n) est vraie pour une infinité de valeurs de n.

Cela est équivalent à : $\forall$ N, $\exists\, n \geq$ N, P(n).

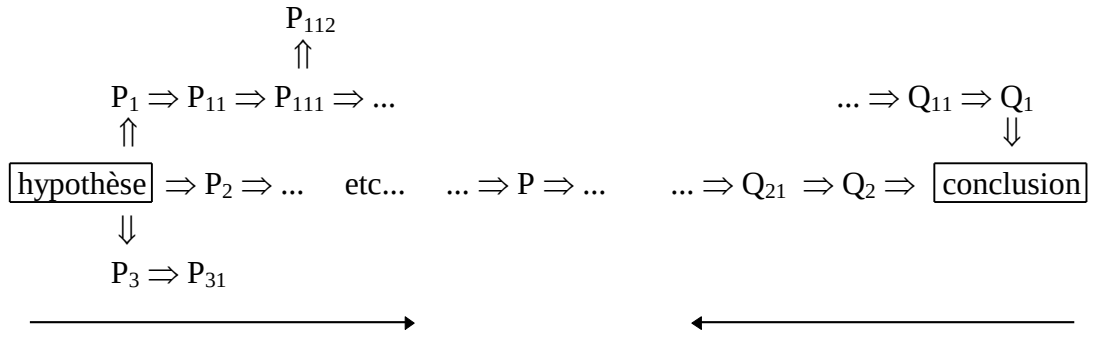
3- Introduction à la démonstration

Lorsqu'un mathématicien, après des heures, des jours, voire des années de labeur, pense qu'une propriété est vraie, il fait une **conjecture**. Pour être certain que cette propriété soit vraie et pour la faire valider par l'ensemble de la communauté mathématique ou scientifique, il faut une démonstration. La démonstration n'est donc pas la tâche essentielle du travail du mathématicien, mais son achèvement. Dans une moindre mesure, on demande la même chose à l'étudiant

scientifique. Ce dernier, apprenti mathématicien, a parfois du mal à mettre en forme une démonstration. Ce paragraphe peut lui donner quelques procédés méthodiques.

La démarche démonstrative repose sur une liste de connaissances appelée à évoluer. Cette liste comprend tous les axiomes et théorèmes connus du démonstrateur, mais peut également évoluer par ajout de propriétés au cours de la démonstration. La démonstration doit démontrer une proposition, c'est à dire une phrase mathématique que le démonstrateur pense être vraie. Nous avons vu dans le paragraphe précédent qu'une proposition peut être construite à partir de propriétés élémentaires en utilisant itérativement conjonction (et), disjonction (ou), implication ($\Rightarrow$), et négation (non). L'équivalence ($\Leftrightarrow$), quant à elle, n'est que la conjonction de deux implications ($\Rightarrow$ et $\Leftarrow$). A cela, on ajoute les quantificateurs existentiel ($\exists$) et universel ($\forall$).

Il convient d'abord de clairement séparer ce qu'on sait vrai (liste des connaissances, hypothèses diverses) de la conclusion à laquelle on veut arriver. Par ailleurs, il convient de savoir qu'une démonstration ne consiste pas forcément à partir de l'hypothèse, puis par une suite de déductions logiques, à arriver à la conclusion. On peut bien sûr partir de l'hypothèse pour en déduire diverses propriétés en espérant que l'une d'elles finira par être la conclusion cherchée, mais on peut aussi partir de la conclusion pour trouver des propriétés à partir desquelles la conclusion se déduit, en espérant ainsi remonter jusqu'aux hypothèses. On peut également opérer simultanément les deux démarches jusqu'à tomber sur une propriété faisant le lien entre les deux. Ci-dessous, P est une propriété pouvant servir de jonction entre une progression venant de l'hypothèse et une progression venant de la conclusion :



Sens dans lequel s'opère la recherche de nouvelles propriétés qui se déduisent de l'hypothèse

Sens dans lequel s'opère la recherche de nouvelles propriétés d'où découle la conclusion

Il convient également de distinguer ce qu'il faut faire pour **montrer** une conjecture, de ce qu'il faut faire pour **utiliser** une propriété déjà prouvée et faisant donc partie de la liste des connaissances. Certaines indications données ci-dessous paraîtront triviales. D'autres le sont beaucoup moins. Par ailleurs, les approches proposées ne sont pas uniques et d'autres peuvent être envisagées (par exemple pour l'implication, prendre la contraposée). Nous notons par A, B, C... des propriétés à prouver, et par P, Q, R... des propriétés déjà prouvées, et faisant donc partie de la liste des connaissances. La classification ci-dessous est utilisée dans les assistants de preuve, logiciels permettant de valider automatiquement les démonstrations.

(Règles d'introduction) POUR MONTRER...
(i) ...une conjonction A et B : montrer A et montrer B.

(ii) ...une disjonction A ou B : montrer A ou montrer B.

(iii) ...une implication A $\Rightarrow$ B : ajouter A comme hypothèse à sa liste de connaissances (autrement dit, supposer A) et montrer B.

(iv) ...une négation non(A) : ajouter A comme hypothèse à sa liste de connaissance et montrer qu'on aboutit à une contradiction. A est alors nécessairement faux. Autrement dit, non(A) est synonyme de A $\Rightarrow$ contradiction.

(v) ... $\exists x$ A(x) : exhiber un élément t bien choisi et montrer A(t).

(vi) ... $\forall x$ A(x) : montrer A(u), u étant un symbole quelconque non encore utilisé par ailleurs.

(Règles d'élimination) POUR UTILISER...
(a) ...une conjonction P et Q : ajouter P à la liste des connaissances et ajouter Q.

(b) ...une disjonction P ou Q : en déduire la validité d'une proposition R en montrant P $\Rightarrow$ R **et** Q $\Rightarrow$ R (méthode de **disjonction des cas**). Pour montrer par exemple qu'une suite monotone (i.e. croissante **ou** décroissante) bornée converge, il suffit de montrer qu'une suite croissante bornée converge **et** qu'une suite décroissante bornée converge.

(c) ...une implication P $\Rightarrow$ Q : ajouter Q à la liste des connaissances à condition que P y soit déjà.

(d) ...une négation non(P) : déduire une contradiction si P fait également partie de la liste des connaissances. Autrement dit, une contradiction est un synonyme de (P et non(P)).

(e) ... $\exists x$ P(x), ajouter P(u) à la liste des connaissances, u étant un symbole quelconque non déjà utilisé par ailleurs. u désigne ici l'élément particulier qui vérifie la propriété P. On prendra garde à ne pas choisir un u intervenant dans une autre propriété.

(f) ... $\forall x$ P(x), ajouter P(t) à la liste des connaissances, t étant un objet choisi à notre gré.

LE RAISONNEMENT PAR L'ABSURDE
En logique classique, on ajoute la règle suivante, dite de **raisonnement par l'absurde**.
Pour montrer P, ajouter non(P) à la liste des connaissances et montrer une contradiction. Autrement dit, si non(P) $\Rightarrow$ contradiction, on a prouvé P. Cette règle s'appelle également simplification de la double négation, puisque non(P) $\Rightarrow$ contradiction est synonyme de non(non(P)).

Cette règle est utilisée implicitement dans :
❑ Le **tiers exclu** : pour toute propriété P, on a (P ou non(P)). En effet, dans le cas contraire, on aurait non (P ou non(P)), c'est-à-dire non(P) et non(non P) ce qui est contradictoire. Donc on a bien P ou non(P).

❑ La **contraposition** : si (non(P) $\Rightarrow$ non(Q)) alors (Q $\Rightarrow$ P). En effet, supposons que l'on ait non(P) $\Rightarrow$ non(Q) et que Q soit vrai. Il s'agit de montrer que P est vrai. Raisonnons par l'absurde et

supposons non(P). On a alors non(Q) d'après la première implication. Ayant Q et non(Q), on aboutit à une contradiction. Donc non(P) est absurde et P est vrai.

On pourra vérifier que **toutes** les démonstrations mathématiques utilisent ces principes.

EXEMPLE 1 :

❑ Montrer que : $\forall\, n \in \mathbb{N}$, [$n^2$ impair $\Rightarrow$ n impair]

D'après (vi), nous allons montrer que n^2 impair $\Rightarrow$ n impair, n étant un nombre quelconque. D'après (iii), nous allons supposer que n^2 est impair et montrer que n est impair.

On sait ou on suppose que :	On veut montrer que :
n^2 est impair	n est impair

Raisonnons par l'absurde. Nous allons supposer n non impair (i.e. n pair) et arriver à une contradiction. Si on y parvient, on aura prouvé que n est effectivement impair.

On sait ou on suppose que :	On veut montrer :
n^2 est impair n pair	une contradiction

On utilise la définition de la parité :

n pair $\Leftrightarrow \exists\, p \in \mathbb{N}$, $n = 2p$ (définition de la propriété "être pair")

On sait ou on suppose que :	On veut montrer :
n^2 est impair $\exists\, p \in \mathbb{N}$, $n = 2p$	une contradiction

On a $n = 2p$ (utilisation implicite de (e)) donc $n^2 = 4p^2$ qui est pair et non impair. On a bien obtenu une contradiction. CQFD.

On notera que la démonstration utilise le fait que n est pair. La plupart des étudiants partent de $n^2 = 2p + 1$, démarche généralement vouée à l'échec.

EXEMPLE 2 :

❑ Toute suite réelle croissante majorée converge (il convient de lire cet exemple après avoir acquis les connaissances sur les réels et la notion de borne supérieure. Voir L1/REELS.PDF et L1/SUITES.PDF). Bien entendu, dans le chapitre SUITES.PDF, nous allons plus vite au but, mais on pourra se rendre compte que la démonstration est basée sur une application des principes (i) à (vi) et (a) à (f), ce que nous développons ci-dessous de façon outrageusement détaillée. Insistons sur le fait que le mathématicien ne développe jamais dans ses moindres détails une telle démarche. Ce

développement a seulement pour but de mettre à jour les utilisations souvent implicites des dits principes.

Il s'agit de montrer que :

$\forall\ (u_n)$, [(u_n) est croissante et (u_n) est majorée $\Rightarrow$ (u_n) converge]

D'après (vi) et (iii), on a :

On sait ou on suppose que :	On veut montrer que :
(u_n) est croissante et (u_n) est majorée	(u_n) converge

On traduit chaque propriété (croissance, majoration, convergence) :

On sait ou on suppose que :	On veut montrer que :
$\forall n\ u_n \leq u_{n+1}$ $\exists M\ \forall n\ u_n \leq M$	$\exists l\ \forall \varepsilon > 0\ \exists N\ \forall n \geq N,\ l - \varepsilon < u_n < l + \varepsilon$

Nous avons un théorème d'existence de la borne supérieure (cf le chapitre *Suites* dans le fichier SUITES.PDF) qui dit : $\exists M\ \forall n\ u_n \leq M \Rightarrow \text{Sup}\ \{u_n,\ n \in \mathbb{N}\}$ existe. L'application de la règle (c) donne donc, en abrégeant la liste des connaissances (ce que nous ferons plusieurs fois pour alléger) :

On sait ou on suppose que :	On veut montrer que :
$\forall n\ u_n \leq u_{n+1}$ $\text{Sup}(u_n)$ existe	$\exists l\ \forall \varepsilon > 0\ \exists N\ \forall n \geq N,\ l - \varepsilon < u_n < l + \varepsilon$

Nous allons prendre $l = \text{Sup}\ \{u_n,\ n \in \mathbb{N}\}$ (application de la règle (v)). C'est évidemment le travail du mathématicien de faire le bon choix de l et il n'y a hélas aucune méthode automatique pour cela ☹). On peut simplement dire qu'on cherche un réel particulier l et que le seul dont on ait connaissance, à part les termes de la suite, c'est la borne supérieure. D'où l'idée de prendre $l = \text{Sup}(u_n)$.

On sait ou on suppose que :	On veut montrer que :
$\forall n\ u_n \leq u_{n+1}$ $l = \text{Sup}(u_n)$	$\forall \varepsilon > 0\ \exists N\ \forall n \geq N,\ l - \varepsilon < u_n < l + \varepsilon$

D'après la règle (vi), nous prenons $\varepsilon > 0$ quelconque. Comme la formulation $\forall\ \varepsilon > 0$ ... est une abréviation de $\forall\ \varepsilon,\ \varepsilon > 0 \Rightarrow$ ..., la règle (iii) ajoute la condition $\varepsilon > 0$ aux hypothèses. Nous remplaçons également $l = \text{Sup}(u_n)$ par la définition de la borne supérieure :

On sait ou on suppose que :	On veut montrer que :
$\forall n\ u_n \leq u_{n+1}$ $\forall n\ u_n \leq l$ $\forall \alpha > 0\ \exists m\ l - \alpha < u_m$ $\varepsilon > 0$	$\exists N\ \forall n \geq N,\ l - \varepsilon < u_n < l + \varepsilon$

Le α pouvant être choisi à notre gré selon la règle (f), nous prendrons $\alpha = \varepsilon$. Là aussi, le choix du α relève de l'intuition du mathématicien ...☹

On sait ou on suppose que :	On veut montrer que :
$\forall n\ u_n \leq u_{n+1}$ $\forall n\ u_n \leq l$ $\exists m\ l - \varepsilon < u_m$ $\varepsilon > 0$	$\exists N\ \forall n \geq N,\ l - \varepsilon < u_n < l + \varepsilon$

Nous appliquons la règle (v) en choisissant N = m (le m de la liste des connaissances). ☹

On sait ou on suppose que :	On veut montrer que :
$\forall n\ u_n \leq u_{n+1}$ $\forall n\ u_n \leq l$ $\exists m\ l - \varepsilon < u_m$ $\varepsilon > 0$	$\forall n \geq m,\ l - \varepsilon < u_n < l + \varepsilon$

Nous prenons n quelconque supérieur ou égal à m en application de la règle (vi). Comme $\forall\ n \geq m$ ... est une abréviation de $\forall\ n,\ n \geq m \Rightarrow$ ..., d'après (iii), on ajoute $n \geq m$ à nos hypothèses, et plutôt que n dont le symbole est déjà utilisé dans la liste des connaissances, nous noterons cet entier p :

On sait ou on suppose que :	On veut montrer que :
$\forall n\ u_n \leq u_{n+1}$ $\forall n\ u_n \leq l$ $\exists m\ l - \varepsilon < u_m$ $\varepsilon > 0$ $p \geq m$	$l - \varepsilon < u_p < l + \varepsilon$

Dans la deuxième propriété de la liste des connaissances, nous choisissons (règle (f)) $n = p$.

On sait ou on suppose que :	On veut montrer que :
$\forall n\ u_n \leq u_{n+1}$ $u_p \leq l$ $\exists m\ l - \varepsilon < u_m$ $\varepsilon > 0$ $p \geq m$	$l - \varepsilon < u_p < l + \varepsilon$

Nous appliquons la règle (e) à la troisième propriété de la liste des connaissances. *m* désigne un élément sur lequel nous n'avons aucune possibilité de choix.

On sait ou on suppose que :	On veut montrer que :
$\forall n\ u_n \leq u_{n+1}$ $u_p \leq l$ $l - \varepsilon < u_m$ $\varepsilon > 0$ $p \geq m$	$l - \varepsilon < u_p < l + \varepsilon$

Enfin, dans la première propriété de la liste des connaissances, nous choisissons (règle (f) itérée plusieurs fois) $n = m$, $n = m + 1$, ... $n = p - 1$, $n = p$.

On sait ou on suppose que :	On veut montrer que :
$u_m \leq u_{m+1} \leq ... \leq u_{p-1} \leq u_p$ $u_p \leq l$ $l - \varepsilon < u_m$ $\varepsilon > 0$ $p \geq m$	$l - \varepsilon < u_p < l + \varepsilon$

Ce qu'on peut encore écrire :

On sait ou on suppose que :	On veut montrer que :
$l - \varepsilon < u_m \leq u_{m+1} \leq ... \leq u_{p-1} \leq u_p \leq l$ $\varepsilon > 0$	$l - \varepsilon < u_p < l + \varepsilon$

Ou encore plus brièvement :

On sait ou on suppose que :	On veut montrer que :
$l - \varepsilon < u_p \leq l$ $\varepsilon > 0$	$l - \varepsilon < u_p < l + \varepsilon$

La conclusion à montrer est bien vraie puisque $l \leq l + \varepsilon$.

On aura remarqué que le choix de tel ou tel élément *x* au gré du démonstrateur se manifeste :

ou bien dans la liste des connaissances sur une propriété du type $\forall x$ P(x) (règle (f))

ou bien dans la conclusion à montrer sur une propriété du type $\exists x$ A(x) (règle (v))

En effet, dans le premier cas, la propriété P(x) étant vraie pour tout x, on est libre de l'appliquer au x que l'on veut.

Dans le second cas, puisqu'on doit montrer la propriété A(x) pour un certain x, on peut choisir le x qui nous paraît répondre à la question (c'est là la partie la moins évidente), et, si notre choix a été judicieux, parvenir à prouver A(x) pour ce x bien choisi.

A l'inverse, le démonstrateur n'a aucune liberté de choix sur l'élément *x* qui intervient :

dans la liste des connaissances sous la forme $\exists x$ P(x) (règle (e))

dans la conclusion à montrer sous la forme $\forall x$ A(x) (règle (vi))

Dans le premier cas, on suppose l'existence d'un x vérifiant P(x) mais ce x nous est imposé.

Dans le second cas, on ne peut se contenter de montrer A(x) pour un x de notre choix puisqu'il s'agit de montrer A(x) pour tous les x.

La compréhension de ce mécanisme est essentielle pour mener à bien des démonstrations correctes et pour savoir sur quels éléments on peut faire un choix.

4- Fonctions, injections, surjections

a) Fonction

Une fonction f (ou application) d'un ensemble E dans un ensemble F établit une relation entre les éléments de E et ceux de F. Chaque élément x de E est associé à un unique élément de F, noté $f(x)$. $f(x)$ est l'**image** de x par f. Si y est dans F et s'il existe x dans E tel que $y = f(x)$, x est un **antécédent** de y par f. Certains éléments y de F peuvent n'être l'image d'aucun élément de E, et certains éléments y de F peuvent être l'image de plusieurs éléments de E, d'où les définitions d'injection et de surjection dans la suite du paragraphe.

La partie G de E × F égale à $\{(x, y), y = f(x)\}$ s'appelle graphe de f. On note $\mathcal{F}$(E, F) (ou parfois F^E) l'ensemble des applications de E dans F.

Si on dispose d'une application f de E dans F et d'une application g de F dans H, on peut définir la **composée** $g \circ f$ de E dans H par : $(g \circ f)(x) = g(f(x))$.

L'**application identique** (ou **identité**) Id_E est l'application de E dans E définie par $Id_E(x) = x$.

Si A est inclus dans E, la **restriction** de f à A est l'application $f|_A$ de A dans F définie par $f|_A(x) = f(x)$ pour tout x de A. La seule différence entre f et $f|_A$ est l'ensemble de définition des applications : f est définie sur E alors que $f|_A$ est définie sur A.

Inversement, si E est inclus dans H et s'il existe une application g de H dans F telle que $g|_E = f$, on dit que g est un **prolongement** de f à H.

b) Injection

Une fonction f d'un ensemble E dans un ensemble F est dite **injective** (one to one en anglais) si :

$$\forall\, x \in E,\ \forall\, x' \in E,\ x \neq x' \Rightarrow f(x) \neq f(x')$$

ou encore (ce qui est plus couramment utilisé) :

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

Si f est injective, l'équation $f(x) = y$ a au plus une solution, quel que soit y.

Si f et g sont injectives, alors $g \circ f$ l'est. En effet :

$(g \circ f)(x) = (g \circ f)(x')$
$\Rightarrow$ $(g(f(x)) = g(f(x'))$ (définition de $g \circ f$)
$\Rightarrow$ $f(x) = f(x')$ (injectivité de g)
$\Rightarrow$ $x = x'$ (injectivité de f)

Si $g \circ f$ est injective, alors f l'est. En effet :

$f(x) = f(x')$
$\Rightarrow$ $(g(f(x)) = g(f(x'))$
$\Rightarrow$ $(g \circ f)(x) = (g \circ f)(x')$
$\Rightarrow$ $x = x'$ (car $g \circ f$ est injective)

c) Surjection

Une fonction est dite **surjective** (onto en anglais) si :

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

Si f est surjective, l'équation $f(x) = y$ a au moins une solution, quel que soit y.

Si f et g sont surjectives, alors $g \circ f$ l'est. En effet :

$\forall\, z,\ \exists\, y,\ z = g(y)$ (surjectivité de g)
donc $\forall\, z,\ \exists\, y,\ \exists\, x,\ z = g(y)$ et $y = f(x)$ (surjectivité de f)
donc $\forall\, z,\ \exists\, x,\ z = g(f(x))$
donc $\forall\, z,\ \exists\, x,\ z = (g \circ f)(x)$ (définition de $g \circ f$)

Si $g \circ f$ est surjective, g l'est aussi. En effet :

$\forall\, z,\ \exists\, x,\ z = (g \circ f)(x)$
donc $\forall\, z,\ \exists\, x,\ z = g(f(x))$
donc $\forall\, z,\ \exists\, y,\ z = g(y)$ (en prenant $y = f(x)$)

d) Bijection

f est dite **bijective** si elle est à la fois surjective et injective.

Si f est bijective, l'équation $f(x) = y$ a exactement une solution x, quel que soit y. On peut alors définir la **fonction réciproque** f^{-1} de f par l'équivalence :

$$y = f(x) \Leftrightarrow x = f^{-1}(y).$$

On a alors $f(f^{-1}(y)) = f(x) = y$ ce qu'on écrit encore $f \circ f^{-1} = \mathrm{Id}_F$ et $f^{-1}(f(x)) = f^{-1}(y) = x$ ce qui s'écrit $f^{-1} \circ f = \mathrm{Id}_E$.

Si f et g sont bijectives, alors $g \circ f$ l'est et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. En effet :

$z = (g \circ f)(x)$
$\Rightarrow \quad z = g(f(x))$
$\Rightarrow \quad g^{-1}(z) = f(x)$
$\Rightarrow \quad f^{-1}(g^{-1}(z)) = x$
$\Rightarrow \quad x = (f^{-1} \circ g^{-1})(z)$

S'il existe une application g de F dans E telle que $f \circ g = \mathrm{Id}_F$ et $g \circ f = \mathrm{Id}_E$, alors f et g sont bijectives et réciproques l'une de l'autre. En effet, la seule solution x possible à l'équation $y = f(x)$ est $x = g(y)$. C'est bien une solution puisque $f(g(y)) = y$. Il n'y en a pas d'autre puisque :

$y = f(x) \Rightarrow g(y) = g(f(x)) = x$

On notera que l'on a besoin des deux relations $f \circ g = \mathrm{Id}_F$ et $g \circ f = \mathrm{Id}_E$ pour prouver l'existence et l'unicité. La première relation $f \circ g = \mathrm{Id}_F$ montre l'existence de la solution et prouve que f est surjective. La seconde relation $g \circ f = \mathrm{Id}_E$ montre l'unicité de la solution et prouve que f est injective.

EXEMPLE 1 :

❑ L'application $x \to \sin(x)$ est :

injective si l'ensemble de départ est $[-\frac{\pi}{2}, \frac{\pi}{2}]$

surjective si, de plus, l'ensemble d'arrivée est [–1, 1]

On notera que, si f est une application de E dans F avec Card(E) = Card(F) (fini), alors, il y a équivalence entre injective, surjective et bijective. En effet, sous l'hypothèse précédente, si f est injective, on a :

$$\left[\begin{array}{l}\mathrm{Card}(F) = \mathrm{Card}(E) \\ \mathrm{Card}(E) = \mathrm{Card}(f(E))\end{array}\right. \text{ donc } \mathrm{Card}(f(E)) = \mathrm{Card}(F)$$

or f(E) est inclus dans F. Ayant le même nombre d'élément que F, f(E) = F et f est surjective.

De même, si f est surjective, on a :

$$\left[\begin{array}{l}\mathrm{Card}(F) = \mathrm{Card}(E) \\ \mathrm{Card}(F) = \mathrm{Card}(f(E))\end{array}\right. \text{ donc } \mathrm{Card}(f(E)) = \mathrm{Card}(E)$$

donc deux éléments distincts de E ne peuvent avoir deux images identiques. f est donc injective.
Ces remarques sont fausses si E et F sont des ensembles infinis.

EXEMPLE 2 :

❑ Pour n entier naturel, notons $[\![1, n]\!]$ l'ensemble des entiers de 1 à n. Alors il existe une bijection entre $[\![1, n]\!]$ et $[\![1, p]\!]$ si et seulement si $n = p$.

EXEMPLE 3 :

❑ Il n'existe aucune bijection entre E et $\mathcal{P}$(E), que E soit fini ou non. C'est clair si E est fini avec n éléments, puisque E et $\mathcal{P}$(E) n'ont pas le même nombre d'éléments (n et 2^n respectivement), plus délicat à montrer si E est infini. Pour cela, nous allons montrer que, quelles que soient les fonctions f de E dans $\mathcal{P}$(E) et g de $\mathcal{P}$(E) dans E, on a $f \circ g \neq \mathrm{Id}_{\mathcal{P}(E)}$. Il est par contre tout à fait possible d'avoir $g \circ f = \mathrm{Id}_E$. Il suffit pour cela de prendre $f(x) = \{x\}$ et g(A) = un élément donné de A.

Pour montrer que :

(1) $f \circ g \neq \mathrm{Id}_{\mathcal{P}(E)}$

nous allons modifier cette proposition jusqu'à obtenir une affirmation manifestement vraie dont (1) découle. La difficulté essentielle est de bien comprendre qu'un *élément* de E a pour image par f une *partie* de E, et qu'une *partie* de E a pour image par g un *élément* de E. On peut déjà écrire que (1) équivaut à :

(2) $\exists$ A $\subset$ E, $(f \circ g)(A) \neq A$

On écrit ensuite le fait que les deux parties A et $(f \circ g)(A)$ sont différentes, à savoir l'appartenance à la première partie ne saurait être équivalente à l'appartenance à l'autre partie :

(3) $\exists$ A $\subset$ E, $\exists\, x$, non $[x \in A \Leftrightarrow x \in (f \circ g)(A)]$

(On aurait pu écrire aussi qu'il existe un x dans la première partie et pas dans la seconde, à moins que x soit dans la seconde et pas dans la première, ce qui est strictement identique à la formulation ci-dessus).

Comment trouver ce x à partir de A ? Nous ne connaissons qu'un seul élément de E en liaison avec A, c'est $x = g(A)$. Pour que (3) soit vérifié, il suffit donc d'avoir :

(4) $\exists$ A $\subset$ E, non $[g(A) \in A \Leftrightarrow g(A) \in (f \circ g)(A)]$

$g(A)$ étant un élément de E, la précédente proposition sera elle-même vérifiée si :

(5) $\exists$ A $\subset$ E, $\forall\, x$, non $[x \in A \Leftrightarrow x \in f(x)]$

Il suffit en effet d'appliquer (5) au x particulier égal à $g(A)$ pour retrouver (4).

On peut aussi écrire (5) sous la forme équivalente :

(6) $\exists$ A $\subset$ E, $\forall\, x$, $[x \in A \Leftrightarrow x \notin f(x)]$

Cette dernière proposition est vraie si l'on choisit précisément $A = \{x \mid x \notin f(x)\}$. On a alors la chaîne de déduction suivante :

(6) vrai $\Leftrightarrow$ (5) $\Rightarrow$ (4) $\Rightarrow$ (3) $\Leftrightarrow$ (2) $\Leftrightarrow$ (1).

Une variante ainsi que des conséquences de cet exemple sont présentées en annexe.

EXEMPLE 4 :

❑ Donnons un exemple d'applications f et g telles que f et g soient non bijectives, mais où $g \circ f = Id_E$:

$\mathbb{N} \to \mathbb{N}$

$f : n \to n + 1$ — f est injective mais non surjective

$g : n \to \begin{cases} 0 \text{ si } n = 0 \\ n - 1 \text{ si } n \neq 0 \end{cases}$ — g est surjective, mais non injective

Pour tout n entier naturel, on a $n + 1 \neq 0$ donc $(g \circ f)(n) = g(n + 1) = n + 1 - 1 = n$. Donc $g \circ f = Id_E$.

e) <u>Image directe d'une partie</u>

Soit A une partie de E. L'**image directe** de A par f est l'ensemble noté $f(A)$ défini par :

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

Autrement dit :

$$y \in f(A) \Leftrightarrow \exists\, x \in A,\ y = f(x)$$

$f(A)$ est l'ensemble des images des éléments de A par f.

EXEMPLE :

❑ Si f est la fonction sinus, alors $f([0, \frac{3\pi}{4}]) = [0, 1]$

f) Image réciproque

Soit B une partie de F. L'**image réciproque** de B par f est l'ensemble noté $f^{-1}(B)$ défini par :

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

Autrement dit :

$$x \in f^{-1}(B) \Leftrightarrow f(x) \in B$$

$f^{-1}(B)$ est l'ensemble des antécédents des éléments de B.

EXEMPLES :

❑ Si f est la fonction sinus, $f^{-1}([0, 1]) = \bigcup_{n\in\mathbf{Z}} [2n\pi, 2n\pi + \pi]$

On prendra garde que cette partie est définie même si f n'est pas bijective, que $f^{-1}(\{y\})$ est l'ensemble (éventuellement vide ou constitué de plus d'un élément) des antécédents de y, et que la notation $f^{-1}(y)$, elle, n'est tolérée que si f est bijective ; on désigne ainsi l'antécédent unique de y.

❑ Toujours avec $f = \sin$, $f^{-1}(\{0\}) = \{n\pi, n \in \mathbf{Z}\} = \pi\mathbf{Z}$.
$f^{-1}(0)$ n'existe pas.

L'image réciproque est compatible avec les opérations ensemblistes, mais pas l'image directe sans hypothèse supplémentaire, comme le montre la proposition suivante, où les complémentaires dans E et dans F sont ici notés respectivement $\complement_E$ et $\complement_F$:

PROPOSITION

Soit $f : E \to F$ *une application. Pour toute partie* A *et* B *de* E, *et toute partie* C *de* F, *on a* :

(i) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$

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

(iii) $f^{-1}(\complement_F C) = \complement_E f^{-1}(C)$

(iv) $f(A \cup B)$ et $f(A) \cup f(B)$

(v) $f(A \cap B) \subset f(A) \cap f(B)$. *On a l'égalité pour tout* A *et* B *si et seulement si f est injective.*

(vi) *f injective* $\Leftrightarrow \forall$ A, $f(\complement_E A) \subset \complement_F f(A)$

(vii) *f surjective* $\Leftrightarrow \forall$ A, $\complement_F f(A) \subset f(\complement_E A)$

(viii) $f(f^{-1}(C)) \subset C$. *On a l'égalité pour tout* C *si et seulement si f est surjective.*

(ix) $A \subset f^{-1}(f(A))$. *On a l'égalité pour tout* A *si et seulement si f est injective.*

Démonstration :

❑ (i) $x \in f^{-1}(A \cup B)$
$\Leftrightarrow$ $f(x) \in A \cup B$
$\Leftrightarrow$ $f(x) \in A$ ou $f(x) \in B$
$\Leftrightarrow$ $x \in f^{-1}(A)$ ou $x \in f^{-1}(B)$
$\Leftrightarrow$ $x \in f^{-1}(A) \cup f^{-1}(B)$

❑ (ii) laissé au lecteur

❑ (iii) $x \in f^{-1}(\complement_F C)$

$\Leftrightarrow \quad f(x) \in \complement_F C$

$\Leftrightarrow \quad f(x) \notin C$

$\Leftrightarrow \quad x \notin f^{-1}(C)$

$\Leftrightarrow \quad x \in \complement_E f^{-1}(C)$

❑ (iv) $y \in f(A \cup B)$

$\Leftrightarrow \quad \exists\, x \in A \cup B,\ y = f(x)$

$\Leftrightarrow \quad \exists\, x \in A,\ y = f(x)$ ou $\exists\, x' \in B,\ y = f(x')$

$\Leftrightarrow \quad y \in f(A)$ ou $y \in f(B)$

$\Leftrightarrow \quad y \in f(A) \cup f(B)$

❑ (v) $y \in f(A \cap B)$

$\Leftrightarrow \quad \exists\, x \in A \cap B,\ y = f(x)$

$\Rightarrow \quad \exists\, x \in A,\ y = f(x)$ et $\exists\, x' \in B,\ y = f(x')$

$\Leftrightarrow \quad y \in f(A)$ et $y \in f(B)$

$\Leftrightarrow \quad y \in f(A) \cap f(B)$

On a montré $f(A \cap B) \subset f(A) \cap f(B)$

Il y a une difficulté pour la réciproque à la troisième ligne, ce qui permettrait de montrer l'égalité. Si on suppose que :

$\exists\, x \in A,\ y = f(x)$ et $\exists\, x' \in B,\ y = f(x')$

on ignore si $x = x'$, permettant de remonter à la ligne précédente. Ce sera bien le cas si f est injective. On a alors :

f injective $\Rightarrow f(A \cap B) = f(A) \cap f(B)$

Réciproquement, supposons qu'on a l'égalité pour tout A et B et montrons f injective. Soient x et s' tels que $f(x) = f(x') = y$. Prenons $A = \{x\}$ et $B = \{x'\}$. Alors :

$f(\{x\} \cap \{x'\}) = f(\{x\}) \cap f(\{x'\}) = \{y\} \cap \{y\} = \{y\} \neq \varnothing$

donc $\{x\} \cap \{x'\} \neq \varnothing$ ce qui impose $x = x'$, et f est injective.

(vi) Supposons f injective et soit $y \in f(\complement_E A)$. Il existe un unique x dans $\complement_E A$ tel que $y = f(x)$. Dans ce cas, y ne peut appartenir à $f(A)$ sinon il aurait un autre antécédent dans A, contredisant l'injectivité de f. Donc $y \in \complement_F f(A)$. Ainsi : $f(\complement_E A) \subset \complement_F f(A)$.

Réciproquement, supposons que, pour tout A, $f(\complement_E A) \subset \complement_F f(A)$ et montrons que f est injective. Soit x et x' tels que $f(x) = f(x') = y$ et soit $A = \{x\}$, de sorte que $y = f(x) \in f(A)$. Supposons par l'absurde que $x' \neq x$, alors $x' \in \complement_E A$ et $y = f(x') \in f(\complement_E A)$ donc $y \in \complement_F f(A)$ puisque $f(\complement_E A) \subset \complement_F f(A)$. Mais on aurait y simultanément élément de $f(A)$ et de son complémentaire, ce qui est absurde.

(vii) Supposons f surjective et soit $y \in \complement_F f(A)$. Donc $y \notin f(A)$ et y n'a aucun antécédent dans A. Mais f étant surjective, y a au moins un antécédent x. Ne pouvant être dans A, x est dans $\complement_E A$, donc $y \in f(\complement_E A)$. Ainsi : $\complement_F f(A) \subset f(\complement_E A)$.

Réciproquement supposons que, pour tout A, $\complement_F f(A) \subset f(\complement_E A)$ et montrons que f est surjective. Soit A = E. On a $\complement_F f(E) \subset f(\complement_E E) = f(\varnothing) = \varnothing$, donc $\complement_F f(E) = \varnothing$ donc $f(E) = F$, donc f est surjective, tout élément de F ayant un antécédent dans E.

(viii) Soit $y \in f(f^{-1}(C))$. Alors $\exists\, x \in f^{-1}(C)$, $y = f(x)$, mais si $x \in f^{-1}(C)$, $f(x) \in C$. Donc $y \in C$ et on a montré que $f(f^{-1}(C)) \subset C$.
Supposons f surjective, et soit $y \in C$. f étant surjective, y possède un antécédent x. On a alors $f(x) = y \in C$, donc $x \in f^{-1}(C)$ et $y \in f(f^{-1}(C))$. Ainsi : $f(f^{-1}(C)) = C$
Réciproquement, supposons qu'on ait l'égalité pour tout C et montrons que f est surjective. Prenons C = F. On a alors $f(f^{-1}(F)) = F$ donc tout élément de F possède un antécédent par f (antécédent qui est dans $f^{-1}(F)$).

(ix) Soit $x \in A$. Alors $y = f(x) \in f(A)$ et x est l'antécédent d'un élément de $f(A)$, donc $x \in f^{-1}(f(A))$. On a ainsi montré que $A \subset f^{-1}(f(A))$.
Supposons f injective, et soit x élément de $f^{-1}(f(A))$. Donc $f(x) \in f(A)$. Donc $\exists\, x' \in A$, $f(x) = f(x')$, mais f étant injective, on a $x = x'$ et donc $x \in A$. Ainsi : $A = f^{-1}(f(A))$.
Réciproquement, supposons qu'on ait l'égalité pour tout A et montrons que f est injective. Soit x et x' tels que $f(x) = f(x')$ et prenons $A = \{x\}$. On a $f(x) \in f(A)$, donc $f(x') \in f(A)$ donc $x' \in f^{-1}(f(A)) = A$ donc $x' \in \{x\}$, donc $x' = x$.

g) Fonction indicatrice

A chaque partie A d'un ensemble E, on associe sa **fonction indicatrice** $\mathbf{1}_A$ de E dans {0, 1} définie par :

$$\mathbf{1}_A(x) = \begin{cases} 1 \text{ si } x \in A \\ 0 \text{ si } x \notin A \end{cases}$$

On a alors :

$\mathbf{1}_E = 1$
$\mathbf{1}_\varnothing = 0$
$\mathbf{1}_{A^c} = 1 - \mathbf{1}_A$
$\mathbf{1}_{A \cap B} = \mathbf{1}_A \times \mathbf{1}_B$
$\mathbf{1}_{A \cup B} = \mathbf{1}_A + \mathbf{1}_B - \mathbf{1}_A \times \mathbf{1}_B = \text{Max}(\mathbf{1}_A, \mathbf{1}_B)$
$\mathbf{1}_{A \setminus B} = \mathbf{1}_A - \mathbf{1}_A \times \mathbf{1}_B$

Deux fonctions indicatrices $\mathbf{1}_A$ et $\mathbf{1}_B$ sont égales si et seulement si A = B, puisqu'on a $A = \{x \mid \mathbf{1}_A(x) = 1\}$. Les fonctions indicatrices peuvent alors permettre de prouver des formules ensemblistes. Par exemple, montrons que $(A \cup B)^c = A^c \cap B^c$:

$$\mathbf{1}_{(A \cup B)^c} = 1 - \mathbf{1}_{A \cup B} = 1 - (\mathbf{1}_A + \mathbf{1}_B - \mathbf{1}_A \times \mathbf{1}_B) = 1 - \mathbf{1}_A - \mathbf{1}_B + \mathbf{1}_A \times \mathbf{1}_B$$
$$= (1 - \mathbf{1}_A) \times (1 - \mathbf{1}_B) = \mathbf{1}_{A^c} \times \mathbf{1}_{B^c} = \mathbf{1}_{A^c \cap B^c}$$

Les fonctions indicatrices jouent également un rôle intéressant en probabilités.

5- Ensembles finis et cardinal

Nous énonçons ci-dessous un certain nombre de propriétés sur les ensembles finis, sans chercher à les justifier outre mesure.

E est un **ensemble fini** s'il existe un entier naturel n et une bijection de $[\![1, n]\!]$ sur E, où l'on note $[\![1, n]\!]$ l'ensemble des entiers de 1 à n. n est le **cardinal** de E, noté Card(E).

Une partie de $\mathbb{N}$ est finie si et seulement si elle est majorée. Si n est le cardinal de cette partie, il existe une bijection strictement croissante et une seule entre cette partie et $[\![1, n]\!]$. 1 est l'image de l'élément le plus petit, 2 l'image du suivant, etc...

$\text{Card}(\varnothing) = 0$

Si E' est inclus dans E, alors $\text{Card}(E') \leq \text{Card}(E)$, avec égalité si et seulement si E' = E.

Si f est une application de E dans F ensembles finis, et si Card(E) = Card(F), alors, il y a équivalence entre injective, surjective et bijective. En effet, compte tenu de l'égalité entre Card(F) et Card(E), on a :

f injective $\Rightarrow \text{Card}(E) = \text{Card}(f(E)) \Rightarrow \text{Card}(F) = \text{Card}(f(E))$

or $f(E)$ est inclus dans F, donc $f(E) = F$ puisqu'ils ont même nombre d'éléments, et f est surjective.
De même :

f surjective $\Rightarrow f(E) = F \Rightarrow \text{Card}(F) = \text{Card}(f(E)) \Rightarrow \text{Card}(E) = \text{Card}(f(E))$

donc deux éléments distincts de E ne peuvent avoir deux images identiques, sinon $f(E)$ aurait strictement moins d'éléments que E. f est donc injective.
Ces remarques sont fausses si E et F sont des ensembles infinis.

La réunion de deux parties finies est finie et l'on a :

$$\text{Card}(A \cup B) = \text{Card}(A) + \text{Card}(B) - \text{Card}(A \cap B)$$

En effet, dans Card(A) + Card(B), on compte deux fois les éléments de $A \cap B$. Il faut donc retrancher $\text{Card}(A \cap B)$ pour compter une fois et une seule les éléments de $A \cup B$. Cette formule est analogue à celle vue précédemment sur les fonctions indicatrices :

$$\mathbf{1}_{A \cup B} = \mathbf{1}_A + \mathbf{1}_B - \mathbf{1}_A \times \mathbf{1}_B$$

Evidemment, si A et B sont disjoints, on a $\text{Card}(A \cup B) = \text{Card}(A) + \text{Card}(B)$.

On pourra de même réfléchir que :

$$\text{Card}(A \cup B \cup C) = \text{Card}(A) + \text{Card}(B) + \text{Card}(C) - \text{Card}(A \cap B) - \text{Card}(A \cap C) - \text{Card}(B \cap C) + \text{Card}(A \cap B \cap C)$$

On a $\text{Card}(E \times F) = \text{Card}(E) \times \text{Card}(F)$

Le cardinal de l'ensemble $\mathcal{F}(E, F)$ des applications de E dans F est égal à $\text{Card}(F)^{\text{Card}(E)}$. En effet, pour chaque élément de E, il y a Card(F) choix possibles pour son image. Ainsi, le nombre d'applications de E dans {0, 1} est égal à $2^{\text{Card}(E)}$ de même que $\text{Card}(\mathcal{P}(E))$. En effet chaque partie A de E est caractérisée par sa fonction indicatrice $\mathbf{1}_A$. Il y a donc autant de parties dans E que de fonctions de E dans {0, 1}.

Si Card(E) = n, le nombre de bijections de E est égal à $n!$. En effet, il y a n choix possibles pour l'image du premier élément de E, mais seulement $n - 1$ pour le suivant, $n - 2$ pour le suivant, etc...

jusqu'au dernier où il ne restera plus qu'un seul choix possible. Les bijections d'un ensemble fini s'appellent aussi **permutations** de cet ensemble.

On dit que deux ensembles infinis ont **même cardinal** s'il existe une bijection entre ces deux ensembles. Ici, le cardinal ne désigne pas un nombre entier. Il regroupe des ensembles infinis en bijection. Dans l'annexe I, on justifie que $\mathbb{N}$, $\mathbb{Z}$, et $\mathbb{Q}$ ont même cardinal entre eux, mais pas avec $\mathbb{R}$.

II : Relations

1- Exemples et définition

Soit E un ensemble. Une relation $\mathcal{R}$ est donné par une partie G de E × E appelé son graphe. On note $x \mathcal{R} y$ en lieu et place de $(x, y) \in G$. Voici quelques exemples, où l'on indique successivement l'ensemble considéré, la relation choisie et sa signification :

	E	$\mathcal{R}$	$x \mathcal{R} y$
a)	E	la différence	$x \neq y$
b)	{Droites}	le parallélisme	D // D'
c)	E	l'égalité	$x = y$
d)	$\mathbb{R}$	l'infériorité	$x \leq y$
e)	$\mathcal{P}$(E)	l'inclusion	A ⊂ B
f)	$\mathbb{Z}$	la congruence	$x \equiv y \bmod p$
g)	$\mathbb{N}^*$	la divisibilité	$n \mid m$
h)	$\mathbb{Z} \times \mathbb{Z}^*$		$(a, b) \mathcal{R} (a', b')$ $\Leftrightarrow ab' = ba'$

La congruence dans $\mathbb{Z}$ est définie par :

$$x \equiv y \bmod p \Leftrightarrow \exists\, k \in \mathbb{Z},\ x - y = kp$$

La divisibilité est définie par :

$$n \mid m \Leftrightarrow \exists\, k \in \mathbb{Z},\ m = kn$$

Si le graphe G de la relation vérifie la condition :

$$\forall\, x, \forall\, y, \forall\, z, (x, y) \in G \text{ et } (x, z) \in G \Rightarrow y = z$$

il s'agit d'une relation fonctionnelle. Chaque x est associé à au plus un élément. Cet élément peut alors être noté $f(x)$. Le **domaine de définition** de f est $\{x \mid \exists\, y\ (x, y) \in G\}$.

2- Relations d'ordre

a) Définition

Dans les exemples donnés plus haut, certaines relations permettent de comparer les éléments entre un plus petit et un plus grand. C'est le cas des exemples :

d) $\mathbb{R}$ l'infériorité $x \leq y$

e) $\mathcal{P}(E)$ l'inclusion $A \subset B$

g) $\mathbb{N}^*$ la divisibilité $n \mid p$

Soit E un ensemble. Une relation binaire $\mathcal{R}$ sur E est une relation d'ordre si elle est :

réflexive
antisymétrique
transitive

Une relation d'ordre sert à établir une hiérarchie parmi les éléments de E. Si $x \mathcal{R} y$, x sera le plus souvent considéré comme "inférieur ou égal" à y (la convention inverse peut également être prise). $x \mathcal{R} y$ doit être compris comme une phrase du type x est plus petit que y, ou bien x est avant y (et éventuellement, $x = y$).

i) La **réflexivité** s'applique aux relations vérifiant :

$$\forall x \in E, x \mathcal{R} x$$

(x est "inférieur ou égal" à lui-même).

iii) L'**antisymétrie** s'applique aux relations vérifiant :

$$\forall x \in E, \forall y \in E, (x \mathcal{R} y \text{ et } y \mathcal{R} x) \Rightarrow x = y$$

(si x est "inférieur ou égal" à y et y est "inférieur ou égal" à x, alors $x = y$).

iv) La **transitivité** s'applique aux relations vérifiant :

$$\forall x \in E, \forall y \in E, \forall z \in E, (x \mathcal{R} y \text{ et } y \mathcal{R} z) \Rightarrow x \mathcal{R} z$$

(si x est "inférieur ou égal" à y et y est "inférieur ou égal" à z, alors x est "inférieur ou égal" à z).

Du fait de l'antisymétrie et de la transitivité, il est impossible d'avoir un cycle d'éléments distincts vérifiant $x_1 \mathcal{R} x_2$, $x_2 \mathcal{R} x_3$, ..., $x_{n-1} \mathcal{R} x_n$, $x_n \mathcal{R} x_1$.

Voici un dernier exemple : dans l'ensemble des mots sur un alphabet (un mot est une suite finie de lettres de l'alphabet), l'ordre alphabétique ou **lexicographique** est une relation d'ordre. Cette relation existe dans de nombreux langages de programmation :

'ABBC' ≤ 'ABC' est vrai
'ABBC' ≤ 'ABB' est faux

REMARQUE : si on définit une relation ≤ dans $\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{R}$, il n'en est pas de même dans $\mathbb{C}$. Pourquoi ? Les relations définies sur les ensembles de nombres présentent une certaine compatibilité avec les lois + et × définies sur ces ensembles. En particulier, on a :

$$a \geq 0 \text{ et } b \geq 0 \Rightarrow a + b \geq 0 \text{ et } ab \geq 0.$$

Si l'on avait, sur $\mathbb{C}$, une relation du type $i \geq 0$, alors, en effectuant le produit, on obtiendrait $-1 \geq 0$. De même si $-i \geq 0$. Cela ne veut pas dire qu'il est impossible de définir une relation d'ordre sur $\mathbb{C}$, mais que cette relation ne présentera aucun caractère de compatibilité avec les lois + et ×. Son intérêt algébrique sera alors très limité.

b) Ordre total, ordre partiel

On remarquera que l'exemple d) diffère des exemples e) et g) du point de vue suivant :

Dans le cas d), pour tout élément x et y, l'une des deux propriétés $x \mathcal{R} y$ ou $y \mathcal{R} x$ est vérifiée, ce qui n'est pas vrai dans les cas e) et g). Par exemple, on n'a pas $2 \mid 3$, ni $3 \mid 2$. De même $\{1, 2\}$ n'est pas inclus dans $\{3\}$, pas plus que $\{3\}$ n'est inclus dans $\{1, 2\}$. On parle respectivement d'ordre total et partiel.

Une relation d'ordre $\mathcal{R}$ sur un ensemble E est dit d'**ordre total** si :

$$\forall x \in E, \forall y \in E, x \mathcal{R} y \text{ ou } y \mathcal{R} x$$

Dans le cas contraire, $\mathcal{R}$ est une relation d'**ordre partiel** :

$$\exists x \in E, \exists y \in E, \text{non}(x \mathcal{R} y) \text{ et non}(y \mathcal{R} x)$$

c) Majorant, minorant, maximum, minimum

a) Soit E muni d'une relation d'ordre R. Une partie A de E est **minorée** par a (a est un **minorant** de A) si :

$$\forall x \in A, a \mathcal{R} x$$

A est **majorée** par b (b est un **majorant** de A) si :

$$\forall x \in A, x \mathcal{R} b$$

EXEMPLE :

❑ [0, 1] est majoré par 2, et minoré par –1.

b) Soit E muni d'une relation d'ordre R. Une partie A de E admet un **minimum** a si :

$$a \in A \text{ et } \forall x \in A, a \mathcal{R} x$$

a est donc un minorant de A, lui–même élément de A. On note $a = \min(A)$.

A admet un **maximum** b si :

$$b \in A \text{ et } \forall x \in A, x \mathcal{R} b$$

b est donc un majorant de A, lui–même élément de A. On note $b = \max(A)$.

EXEMPLES :

❑ 0 est le minimum de [0, 1] (avec la relation usuelle) et 1 est son maximum.

❑]0, 1] n'admet pas de minimum, mais admet 1 comme maximum.

❑]0, 1[n'admet ni maximum ni minimum.

❑ $\varnothing$ est le minimum de $\mathcal{P}$(E) pour la relation d'inclusion. E est le maximum.

❑ Si $\mathcal{A}$ est l'ensemble de tous les singletons de E, $\mathcal{A}$ n'admet ni minimum, ni maximum.

❑ Pour la relation de divisibilité de $\mathbb{N}$, 1 est le minimum, il n'y a pas de maximum.

3- Relations d'équivalence

a) Exemples et définition

Une relation $\mathcal{R}$ sur un ensemble E sera une relation d'équivalence si elle vérifie les propriétés suivantes. Elle est :

réflexive
symétrique
transitive

La **symétrie** s'applique aux relations vérifiant :

$$\forall\, x \in \mathrm{E},\ \forall\, y \in \mathrm{E},\ x\ \mathcal{R}\ y \Rightarrow y\ \mathcal{R}\ x$$

$x\ \mathcal{R}\ y$ signifie que x et y partage une même propriété définie par $\mathcal{R}$.

EXEMPLES :

❑ Dans un ensemble quelconque, l'égalité est une relation d'équivalence triviale. La propriété commune est d'être identique. C'est aussi une relation d'ordre. Une relation peut donc être à la fois symétrique et antisymétrique. Plus généralement, les relations à la fois symétriques et antisymétriques d'un ensemble E sont celles qui sont définies par : $x = y$ et $x \in \mathrm{A}$, où A est une partie donnée de E.

❑ Dans l'ensemble des droites affines du plan, D // D' (D est parallèle à D') si et seulement si D et D' ont même vecteur directeur. La propriété commune à D et D' est d'avoir une même direction.

❑ Dans $\mathbb{Z}$, soit p un nombre donné. Pour tout couple (n, m) de $\mathbb{Z}^2$, on pose :

$$n \equiv m \bmod p \Leftrightarrow \exists\, k,\ n = m + kp$$

On dit que n est congru à m modulo p. La propriété commune à n et m est d'avoir même reste dans la division euclidienne par p.

❑ Dans $\mathbb{R}$, soit α un réel. On dispose d'une définition analogue :

$$x \equiv y \bmod \alpha \Leftrightarrow \exists\, k,\ n = m + k\alpha$$

Un exemple classique intervient avec $\alpha = 2\pi$ pour les mesures des angles.

❑ Dans $\mathbb{Z} \times \mathbb{Z}^*$, on considère la relation $ab' = ba'$ entre deux couples (a, b) et (a', b'). La propriété commune est de représenter le même rationnel $\frac{a}{b} = \frac{a'}{b'}$. Vérifions qu'il s'agit bien d'une relation d'équivalence.

Pour tout (a, b) de $\mathbb{Z} \times \mathbb{Z}^*$, on a $(a, b)\ \mathcal{R}\ (a, b)$ puisque $ab = ba$

Pour tout (a, b) et (a', b') de $\mathbb{Z} \times \mathbb{Z}^*$, si on a $(a, b)\ \mathcal{R}\ (a', b')$, alors $ab' = ba'$ donc $a'b = b'a$ donc $(a', b')\ \mathcal{R}\ (a, b)$

Pour tout (a, b), (a', b') et (a'', b'') de $\mathbb{Z} \times \mathbb{Z}^*$, si on a $(a, b)\ \mathcal{R}\ (a', b')$ et $(a', b')\ \mathcal{R}\ (a'', b'')$, alors $ab' = ba'$ et $a'b'' = b'a''$. Si $a' = 0$, alors $a = a'' = 0$ car $b' \neq 0$ et $b'' \neq 0$. Dans ce cas, on a

$ab'' = ba''$. Si $a' \neq 0$, en multipliant membre à membre les deux égalités, on obtient $aa'b'b'' = a'a''bb'$, mais $b' \neq 0$ et $a' \neq 0$, donc $ab'' = a''b$. Dans les deux cas, on obtient bien $(a, b)\ \mathcal{R}(a'', b'')$.

b) Partition et classes d'équivalence

Une **partition** d'un ensemble E est une famille $(A_i)_{i\in I}$ vérifiant :

$\forall\ i,\ A_i \neq \varnothing$

$\forall\ i, \forall\ j,\ i \neq j \Rightarrow A_i \cap A_j = \varnothing$

$\bigcup_{i\in I} A_i = E$

Une partition permet de définir une relation $\mathcal{R}$ de la façon suivante :

$x\ \mathcal{R} y \Leftrightarrow \exists\ i,\ x \in A_i$ et $y \in A_i$

$\mathcal{R}$ définit la relation "appartenir au même A_i". Il s'agit d'une relation d'équivalence.

Réciproquement, une relation d'équivalence permet de définir une partition de E.

DEFINITION

Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. *La* **classe d'équivalence** C_x *d'un élément x est l'ensemble* $\{y \in E \mid y\ \mathcal{R} x\}$.

La classe de x rassemble tous les éléments en relation avec x (qui ont même propriété que x pour la relation donnée).

PROPOSITION

Les classes d'équivalence d'une relation $\mathcal{R}$ forment une partition de E.

Démonstration :

❑ Pour tout x, $x\ \mathcal{R} x$, donc $x \in C_x$ donc $C_x \neq \varnothing$. Les classes d'équivalence sont non vides. De plus, la réunion de toutes les classes est égale à E puisque tout x de E appartient à sa propre classe.

Il reste à montrer que les classes sont deux à deux disjointes, ce que nous ferons en montrant deux résultats intermédiaires :

❑ Montrons que $x\ \mathcal{R} y \Leftrightarrow C_x = C_y$

($\Rightarrow$) Si $z \in C_x$, alors $z\ \mathcal{R} x$ or on suppose que $x\ \mathcal{R} y$ donc par transitivité $z\ \mathcal{R} y$, donc $z \in C_y$. On a montré que $C_x \subset C_y$. La relation $x\ \mathcal{R} y$ étant symétrique, on aura de même $C_y \subset C_x$.

($\Leftarrow$) Si $C_x = C_y$, comme $x \in C_x$, $x \in C_y$ donc $x\ \mathcal{R} y$

❑ Montrons que non$(x\ \mathcal{R} y) \Leftrightarrow C_x \cap C_y = \varnothing$

($\Rightarrow$) Par l'absurde, s'il existe $z \in C_x \cap C_y$, alors $z\ \mathcal{R} x$ et $z\ \mathcal{R} y$, donc $x\ \mathcal{R} z$ et $z\ \mathcal{R} y$ par symétrie, donc $x\ \mathcal{R} y$ par transitivité, contrairement à l'hypothèse.

($\Leftarrow$) Si $C_x \cap C_y = \varnothing$, on ne peut avoir $x\ \mathcal{R} y$ car on aurait $x \in C_y$ et on sait par ailleurs que $x \in C_x$ donc $C_x \cap C_y$ serait non vide.

En conséquence, deux classes d'équivalences C_x et C_y différentes sont telles que non($x \mathcal{R} y$), et donc telles que $C_x \cap C_y = \varnothing$. Les classes d'équivalence sont donc deux à deux disjointes.

L'**ensemble quotient** d'une relation d'équivalence est l'ensemble des classes d'équivalence. On le note $E/\mathcal{R}$.

EXEMPLES :
❑ Une classe d'équivalence pour la relation de parallélisme est définie par la direction d'une droite. L'ensemble quotient est l'ensemble des directions de droite.

❑ La classe d'équivalence d'un élément x pour la relation de congruence module p est de la forme $\{x + kp \mid k \in \mathbb{Z}\}$. L'ensemble quotient, noté $\mathbb{Z}/p\mathbb{Z}$ est l'ensemble des entiers définis modulo p. Dans l'ensemble quotient, on ne fait pas de différence entre x et $x + p$. Par exemple, pour $p = 2$, les deux classes d'équivalence sont formées de l'ensemble des nombres pairs et de l'ensemble des nombres impairs. Dans l'ensemble quotient $\mathbb{Z}/2\mathbb{Z}$, on ne s'intéresse qu'à la parité des nombres et non à leur valeur.

❑ La classe d'équivalence dans $\mathbb{Z} \times \mathbb{Z}^*$ pour la relation $(a, b)\ \mathcal{R}\ (a', b') \Leftrightarrow ab' = ba'$ permet de définir le rationnel $\frac{a}{b} = \frac{a'}{b'}$ indépendamment de la façon dont on décide de le représenter. L'ensemble quotient est $\mathbb{Q}$.

❑ Un exemple fondamental de relation d'équivalence intervient en Physique dans le domaine de la thermodynamique. Il est tellement banal qu'il faut se forcer à se poser la question de savoir pourquoi cette propriété est vérifiée. Considérons trois corps A, B et C, chacun en équilibre thermique. On dira que A et B ont même température si, lorsque A et B sont mis en contact, aucun échange thermique n'a lieu entre eux. Supposons que A et B aient même température, et que B et C aient même température. Peut-on dire que A et C ont même température ? On doit prendre conscience que la réponse oui donnée à cette question ne doit pas reposer sur une utilisation syntaxique du vocabulaire (A et B ont même température, B et C ont même température donc A et C ont même température), mais sur des expériences physiques répétées. Ces expériences, nous les effectuons plus ou moins consciemment tous les jours, et la réponse à ces expériences est positive. Le physicien pose alors comme principe que cette règle est universellement respectée. C'est le principe zéro de la thermodynamique, qui exprime donc le fait que la propriété "avoir même température" est une relation d'équivalence. Ce principe, pour être énoncé, n'a pas besoin de définir ce qu'est la température. Il énonce simplement le résultat attendu d'un protocole expérimental entre trois corps A, B et C. C'est seulement une fois ce principe posé qu'on peut définir la température comme représentant la classe d'équivalence de corps mutuellement en équilibre thermique. Pour définir précisément et mesurer cette température, on choisit un corps de référence A (en général modélisé par un gaz parfait) à partir duquel on définit la température de A, puis la température de tout corps en équilibre thermique avec A. Ainsi, la notion de température devient une notion dérivée d'un principe premier basé sur l'existence a priori d'une relation d'équivalence entre corps, postulée sur des résultats expérimentaux.

III : Structures algébriques

1- Loi de composition interne

a) Définition

Soit E un ensemble. On appelle **loi de composition interne** de E, notée par exemple $*$, une opération qui permet d'associer, à deux éléments quelconques de E a et b, un troisième élément noté $a * b$.

EXEMPLES :

❑ Les lois de compositions internes les plus courantes sont :

- $+$ dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.
- $-$ dans les mêmes ensembles.
- $\times$ dans les mêmes ensembles.
- $/$ dans $\mathbb{Q}^*$, $\mathbb{R}^*$, ou $\mathbb{C}^*$.
- div (division entière) dans $\mathbb{N}^*$ ou $\mathbb{Z}^*$.
- $\circ$ dans l'ensemble des applications de E dans E.
- $\cap$ dans l'ensemble $\mathcal{P}(\Omega)$ des parties d'un ensemble Ω.
- $\cup$ dans l'ensemble des parties d'un ensemble.
- $\wedge$ (produit vectoriel) dans l'espace euclidien orienté de dimension 3

b) Associativité

Soit E *un ensemble muni d'une loi de composition interne notée* $*$. *Cette loi est dite* ***associative*** *si :*

$$\forall\, a \in \mathrm{E},\ \forall\, b \in \mathrm{E},\ \forall\, c \in \mathrm{E},\ (a * b) * c = a * (b * c)$$

L'intérêt d'une telle notion est que les parenthèses deviennent inutiles, la notation $a * b * c$ valant indifféremment l'une ou l'autre des expressions. Les lois suivantes, dans les ensembles du paragraphe précédent, sont associatives : $+$, $\times$, $\circ$, $\cap$, $\cup$. Les lois suivantes ne le sont pas : $-$, $/$, div, $\wedge$.

On notera que l'absence de parenthèses dans l'écriture :

$$7 - 5 - 1 = 1$$

signifie implicitement qu'une convention est adoptée pour distinguer entre $(7 - 5) - 1$ et $7 - (5 - 1)$, la convention étant ici *que le calcul se fait de gauche à droite*, mais rien ne nous aurait empêché de prendre la convention inverse : faire les calculs de droite à gauche. Ce qui aurait conduit au résultat, qui nous paraît faux : $7 - 5 - 1 = 3$!!

Quant à la notation $a/b/c$, elle est à éviter, aucune convention n'ayant été définie à son sujet.

c) Commutativité

Soit E *un ensemble muni d'une loi de composition interne notée* $*$. *Cette loi est dite* ***commutative*** *si :*

$$\forall\, a \in \mathrm{E},\ \forall\, b \in \mathrm{E},\ a * b = b * a$$

L'intérêt d'une telle notion est que l'ordre dans lequel les éléments sont placés est indifférent. Les lois suivantes, dans les ensembles du paragraphe précédent, sont commutatives : $+$, $\times$, $\cap$, $\cup$. Les lois

suivantes ne le sont pas : $\circ$ (sauf si les fonctions sont définies sur un ensemble possédant un seul élément), –, /, div, $\wedge$.

Dans le cas d'une loi $*$ commutative et associative, l'expression suivante possède un sens :

$$\mathop{\Large *}_{i \in I} x_i$$

où I est un ensemble fini d'indices. Par exemple, si I = {1, ..., *n*}, l'expression précédente est égale à $x_1 * x_2 * ... * x_n$, l'ordre des termes étant indifférent.

EXEMPLES :

❑ $\sum_{i=1}^{n} x_i$ désigne la somme des éléments x_i

❑ $\prod_{i=1}^{n} x_i$ désigne le produit des éléments x_i

❑ $\bigcap_{i \in I} A_i$ désigne l'intersection des parties A_i

❑ $\bigcup_{i \in I} A_i$ désigne la réunion des parties A_i

On notera, que, si I et J sont deux ensembles disjoints d'indices, on a :

$$\mathop{\Large *}_{i \in I \cup J} x_i = \mathop{\Large *}_{i \in I} x_i * \mathop{\Large *}_{i \in J} x_i \qquad \text{(i)}$$

d) Elément neutre

Soit E *muni d'une loi interne* $*$. *On dit que e est* **élément neutre** *de la loi* $*$ *si :*

$$\forall\, a \in E,\ a * e = e * a = a$$

EXEMPLES :

❑ Le neutre de + est 0. Celui de $\times$ est 1. Celui de $\circ$ est Id. Celui de $\cap$ est Ω (l'ensemble entier). Celui de $\cup$ est $\varnothing$. – et / n'ont pas d'éléments neutres. Si $*$ est associative, commutative, et admet un élément neutre *e*, alors la formule (i) nous conduit à poser :

$$\mathop{\Large *}_{i \in \varnothing} x_i = e$$

Le neutre, s'il existe est unique. En effet, si *e* et *e*' sont deux neutres, on a :

$e * e' = e$ car *e*' est neutre

$e * e' = e'$ car *e* est neutre

donc $e = e'$.

e) Elément symétrique

Soit E *muni d'une loi* $*$, *et d'un élément neutre e. On appelle symétrique d'un élément x de* E *un élément x*' *de* E *tel que* :

$$x * x' = x' * x = e$$

EXEMPLES :

❑ Dans $\mathbb{R}$, Le symétrique de x pour + est $-x$ (appelé opposé de x).

❑ Dans $\mathbb{R}$, Le symétrique de x non nul pour $\times$ est $\frac{1}{x}$ (appelé inverse de x)

❑ Le symétrique de f bijective pour $\circ$ est f^{-1} (appelé réciproque)

Il n'y a en général pas de symétrique pour $\cap$ et $\cup$.

– et /, n'ayant aucune propriété particulière, apparaissent ici comme symétrisations des opérations + et $\times$.

Le symétrique, s'il existe, et si la loi est associative, est unique. En effet, si x' et x'' sont deux symétriques de x, alors on a :

$$x' * x * x'' = (x' * x) * x'' = e * x'' = x''$$
$$= x' * (x * x'') = x' * e = x'.$$

donc $x' = x''$. Ce symétrique est souvent noté x^{-1}.

EXERCICE : Si $*$ est associative, commutative, admet un élément neutre e, et si tout élément admet un symétrique, alors on a, avec I et J quelconques :

$$\mathop{*}_{i \in I \cup J} x_i = \mathop{*}_{i \in I} x_i * \mathop{*}_{i \in J} x_i * \left(\mathop{*}_{i \in I \cap J} x_i\right)^{-1}$$

2- Définition d'un groupe

Une étude plus complète des groupes est menée dans L2/GROUPES.PDF.

Un ensemble (G, $*$) *est un* **groupe** *si* :

i) *G est non vide*.
ii) $*$ *est une loi de composition interne.*
iii) $*$ *est associative.*
iv) $*$ *admet un élément neutre e*.
v) *tout x de* G *admet un symétrique x'*.

Si, en outre, $*$ est commutative, le groupe est dit **commutatif** ou **abélien** (Niels Abel, mathématicien norvégien, 1802-1829).

On note parfois la loi du groupe multiplicativement (ab au lieu de $a * b$) ou additivement ($a + b$ au lieu de $a * b$), mais la notation additive est réservée aux groupes commutatifs. $a * a * ... * a$ est alors noté a^n dans le cas multiplicatif ou na dans le cas additif.

Les axiomes des groupes permettent de simplifier les équations. Ainsi :

$a * x = a * y \Rightarrow x = y$ (composer à gauche par le symétrique de a)
$x * a = y * a \Rightarrow x = y$ (composer à droite par le symétrique de a)

EXEMPLE 1 :

❑ On peut citer le groupe des complexes de module 1, le groupe des racines $n^{ème}$ complexes de l'unité, le groupe des similitudes directes du plan.

Voici d'autres exemples.
EXEMPLE 2 :
❑ Voici quelques groupes à deux éléments :

{σ, Id} où σ est une symétrie, muni de la loi ○.

$U_2 = \{+1, -1\}$ muni du produit (groupe des racines carrées de l'unité, ou règle des signes).

$\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ muni de la loi +. Dans cet ensemble, on pose 1 + 1 = 0.

{Croissance, Decroissance} muni de la loi ○, et de la règle donnant le sens de variation de la composée de deux fonctions monotones.

{true, false} (en programmation), muni de la loi xor (ou exclusif).

Tous ces groupes sont en fait identiques au suivant :
Groupe à deux éléments {*a*, *e*}. La table d'opération de ce groupe est :

*	*a*	*e*
a	*e*	*a*
e	*a*	*e*

On a nécessairement $a^2 = e$ car si $a^2 = a$, en simplifiant par *a*, on obtient $a = e$.

La correspondance se fait de la façon suivante :

Groupe	*	*a*	*e*
{σ, Id}	○	σ	Id
{+1, –1}	×	–1	+1
$\mathbb{Z}/2\mathbb{Z}$	+	1	0
{Croissance, Décroissance}	○	Decroissante	Croissante
{true, false}	xor	true	false

Tous ces groupes sont dits **isomorphes**. Un théorème démontré pour l'un d'entre eux l'est pour tous.

Par exemple : la valeur d'un produit en fonction de la parité du nombre de *a* est *a* si ce nombre est impair, *e* si ce nombre est pair. Ce résultat se traduit de la façon suivante dans quelques situations courantes :

$\sigma^{2p} = Id$ et $\sigma^{2p+1} = \sigma$ pour une symétrie σ

Le produit d'un nombre pair de termes négatifs est positif, le produit d'un nombre impair de termes négatifs est négatif.

La composée d'un nombre pair de fonctions décroissantes et d'un nombre quelconque de fonctions croissantes est croissante ; La composée d'un nombre impair de fonctions décroissantes et d'un nombre quelconque de fonctions croissantes est décroissante.

EXEMPLE 3 :
❑ L'exemple suivant n'est pas un groupe :

*	*a*	*e*
a	*a*	*a*
e	*a*	*e*

On trouve cependant cette situation dans les cas suivants :

$\{a, e\}$	$*$	a	e
$\mathbf{Z}/2\mathbf{Z}$	$\times$	0	1
$\{f$ paire, f impaire$\}$	$\circ$	paire	impaire
{true, false}	or	true	false
{false, true}	and	false	true
$\{\Omega, \varnothing\}$	$\cap$	$\varnothing$	Ω
$\{\varnothing, \Omega\}$	$\cup$	Ω	$\varnothing$

Ici, a est dit **absorbant**. Il vérifie : $\forall\, x,\ x * a = a * x = a$.

EXEMPLE 4 :
❑ Quels sont les groupes à trois éléments ?
Il n'y en a qu'un :

$*$	a	b	e
a	b	e	a
b	e	a	b
e	a	b	e

Pour le remplir, on remarque que, pour chaque élément y, l'application : $x \in G \to yx \in G$ est bijective. Chaque élément du groupe apparaît donc une fois et une seule dans chaque ligne y. De même, l'application $x \to xy$ est bijective, donc chaque élément du groupe apparaît une fois et une seule dans chaque colonne y. En outre $ab = b$ est impossible car cela implique, en simplifiant par b, que $a = e$. De même $ab = a$ est impossible, donc $ab = e$, etc... Il est alors facile de compléter le tableau.

Tous les groupes à trois éléments sont donc isomorphes. En voici quelques exemples :

G	$*$	a	b	e
$\mathbf{U}_3 = \{1, j, j^2\}$	$\times$	j	j^2	1

où j est une racine cubique complexe de l'unité. $\mathbf{U}_3$ est le groupe des racines cubiques de l'unité.

$\{1, \sigma, \sigma^2\}$	$\circ$	σ	σ^2	Id

où σ est une rotation de $2\pi/3$

$\mathbf{Z}/3\mathbf{Z}$	+	1	2	0

constitué des éléments {0, 1, 2} où le calcul se fait modulo 3 (i.e. à un multiple de 3 près).

EXEMPLE 5 :
❑ Quels sont les groupes à 4 éléments ? On n'en trouve que deux :

*	*a*	*b*	*c*	*e*
a	*e*	*c*	*b*	*a*
b	*c*	*a*	*e*	*b*
c	*b*	*e*	*a*	*c*
e	*a*	*b*	*c*	*e*

*	*a*	*b*	*c*	*e*
a	*e*	*c*	*b*	*a*
b	*c*	*e*	*a*	*b*
c	*b*	*a*	*e*	*c*
e	*a*	*b*	*c*	*e*

Le premier n'est autre que $(\mathbb{Z}/4\mathbb{Z}, +)$, c'est à dire le groupe des éléments {0, 1, 2, 3} où les calculs se font modulo 4, ou encore le groupe $\mathbb{U}_4$ des racines quatrièmes complexes de l'unité :

G	*	*c*	*a*	*b*	*e*
$\mathbb{U}_4 = \{1, -1, i, -i\}$	×	*i*	–1	*–i*	1
groupe des racines quatrième de l'unité.					
$\mathbb{Z}/4\mathbb{Z}$	+	1	2	3	0

Le second est $(\mathbb{Z}/2\mathbb{Z})^2$:

G	*	*a*	*b*	*c*	*e*
$(\mathbb{Z}/2\mathbb{Z})^2$	+	(1, 0)	(0, 1)	(1, 1)	(0, 0)

Ce dernier groupe se trouve également dans la situation suivante : considérons un matelas. Il peut être laissé dans la position initiale (Id). On peut le tourner dans le sens de la longueur (σ). On peut le tourner dans le sens de la largeur (θ). On peut lui faire un demi–tour à plat (φ). {Id, σ, θ, φ} n'est autre que le second groupe.

EXEMPLE 6 :

- $\mathbb{U}_n$ groupe des racines $n^{\text{ème}}$ de l'unité dans $\mathbb{C}$, muni du produit
- $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, ..., n - 1\}$ où les calculs se font modulo n.

3- Sous-groupe

Définition : Soit (G, ∗) *un groupe et* G' *une partie de* G. *On dit que* G' *est un sous-groupe de* G *si, muni de la loi* ∗, (G', ∗) *est un groupe*. Il suffit de vérifier les propriétés suivantes :

- G' est non vide
- G' est stable pour ∗ (ce qui signifie que ∗ est une loi interne à G') :

$$\forall\, x \in G',\ \forall\, y \in G',\ x * y \in G'$$

- G' est stable par passage au symétrique : $\forall\, x \in G',\ x^{-1} \in G'$

Il est inutile de vérifier que G' dispose d'un élément neutre. En effet, si *e* est le neutre de G, on montre que *e* est également neutre de G'. En effet :

G' est non vide, donc il existe *x* élément de G'

$x \in G'$ donc $x^{-1} \in G'$

$x \in$ G' et $x^{-1} \in$ G' donc $x * x^{-1} \in$ G' donc $e \in$ G'

$\forall\, x \in$ G, $e * x = x * e = x$ donc ceci reste vrai a fortiori pour x dans G'

L'associativité étant vraie dans G est a fortiori vraie dans G'. Il en est de même de l'éventuelle commutativité.

On montre aisément que l'intersection de deux ou plusieurs sous-groupes est lui–même un sous-groupe.

EXEMPLE 1 :

❑ Dans le plan $\mathbb{R}^2$, considérons les applications qui au vecteur (x, y) associe le vecteur $(x', y') = (ax + by, cx + dy)$, avec $ad - bc \neq 0$, ce qu'on note :

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

L'ensemble de ces applications, muni de la loi de composition $\circ$, forme un groupe appelé groupe linéaire.
L'ensemble des applications pour lesquelles $ad - bc = \pm 1$ en forme un sous-groupe.
L'ensemble des applications orthogonales (rotations et symétries) forme un sous-groupe de ce sous-groupe appelé groupe orthogonal.
L'ensemble des rotations forme lui–même un sous-groupe du groupe orthogonal.

EXEMPLE 2 :

❑ L'ensemble des nombres pairs forme un sous–groupe de $(\mathbb{Z}, +)$.

4- Anneaux et corps

Un **anneau** (A, +, ×) est un ensemble non vide muni de deux lois internes + et × vérifiant les propriétés suivantes :

(A, +) est un groupe commutatif. Son neutre est noté 0.

× est une loi associative possédant un élément neutre généralement noté 1, et **distributive** par rapport à l'addition, i.e. :

$$\forall\, a, \forall\, b, \forall\, c,\ a \times (b + c) = ab + ac \text{ et } (b + c) \times a = ba + ca$$

Le produit × peut ne pas être commutatif. Un exemple non commutatif est donné par l'anneau des matrices carrées (voir L1/MATRICES.PDF).

0 est nécessairement absorbant. Soit x un élément quelconque. On a :

$x \times 0 = x \times (0 + 0) = x \times 0 + x \times 0$

$\Rightarrow$ $0 = x \times 0$ en simplifiant par $x \times 0$

De même, $0 \times x = 0$.

On suppose généralement que $0 \neq 1$, sinon, pour tout x de A, on aurait $0 = 0 \times x = 1 \times x = x$ et A serait réduit à {0}.

0 étant absorbant et différent de 1, il ne peut avoir de symétrique pour le produit. Si tout élément non nul admet un symétrique pour le produit, l'ensemble considéré est un **corps**. On réserve en général cette appellation au cas où, de plus, le produit × est commutatif.

A' est un sous-anneau de A si A' est inclus dans A, et si (A', +, ×) est un anneau ; on convient également que le neutre de A et de A' est identique.

EXEMPLES :

❑ ($\mathbb{Z}$, +, ×) est un anneau. Les matrices carrées munies de la somme et du produit des matrices forment un anneau.

❑ ($\mathbb{Q}$, +, ×) est un corps, sous-corps de $\mathbb{R}$, lui-même sous-corps de $\mathbb{C}$. Les fractions rationnelles de polynômes, de la forme $\frac{P}{Q}$ où P et Q sont des polynômes (avec $Q \neq 0$) forment un corps.

❑ Considérons les quatres opérations élémentaires +, –, × et /, ainsi que la fonction $\sqrt{}$. Partant des rationnels, construisons de proche en proche de nouveaux nombres en itérant les opérations précédentes. On obtient ainsi par exemple les nombres $\sqrt{2}$ ou $\frac{1+\sqrt{5}}{2}$ ou $\sqrt{2-\sqrt{2+\sqrt{2+\sqrt{2+\sqrt{2}}}}}$. En continuant indéfiniment, on forme un corps appelé corps des **nombres constructibles**. On peut montrer que, dans le plan, les points à coordonnées constructibles dans un repère orthonormé sont précisément les points constructibles à la règle et au compas à partir de l'origine du repère et des vecteurs de base. (Cela résulte du fait que l'intersection d'un cercle et d'une droite conduit à une équation du second degré, dont la résolution ne fait appel qu'aux opérations +, –, ×, / et $\sqrt{}$). On a montré au XIXème que les nombres π, $\sqrt[3]{2}$ ou $\cos(\frac{\pi}{9})$ ne sont pas constructibles, rendant impossible la résolution de problèmes millénaires posés pas les Grecs Anciens, celui de la quadrature du cercle, de la duplication du cube ou de la trisection de l'angle.

❑ Considérons l'ensemble $\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$ avec les lois commutatives + et × définies comme suit :

0 est le neutre de la somme
1 est le neutre du produit

$\alpha^2 = \beta$	$\alpha\beta = 1$	$\beta^2 = \alpha$
$1 + \alpha = \beta$	$1 + \beta = \alpha$	$\alpha + \beta = 1$

Ces opérations donnent à $\mathbb{F}_4$ une structure de corps. $\mathbb{F}_4$ est le seul corps à quatre éléments. En ce qui concerne la somme, sa structure de groupe est isomorphe à celle de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ avec l'isomorphisme suivant :

$\mathbb{F}_4$	$\rightarrow$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
0	$\rightarrow$	(0, 0)
1	$\rightarrow$	(1, 1)
α	$\rightarrow$	(0, 1)
β	$\rightarrow$	(1, 0)

mais il n'y a pas d'isomorphisme pour le produit. $\mathbb{F}_4$ est un corps, ce que n'est pas $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. (On a $\alpha\beta = 1$ mais $(0, 1) \times (1, 0) = (0, 0)$ et non (1, 1)). Ce type de corps est largement utilisé aujourd'hui dans le chiffrement des données.

Annexe I : ensembles dénombrables et non dénombrables

On pourrait penser qu'il n'y a que deux types d'ensembles, les ensembles finis et les ensembles infinis, ces derniers étant tous de même nature. Cette vision a été mise en défaut par Georg Cantor

(1845 - 1918). Ses travaux sont à la base de la théorie des ensembles au XX^{ème} siècle. Il définit plusieurs types d'infinis.

Un ensemble infini est en bijection avec l'une de ses parties strictes. Par exemple, $\mathbb{N}$ est en bijection avec $\mathbb{N}^*$, au moyen de la bijection suivante :

$$\mathbb{N} \to \mathbb{N}^*$$
$$n \to n + 1$$

Soit plusieurs ensembles infinis, par exemple $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$. Sont–ils en bijection les uns avec les autres ? On peut prouver que $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$ sont effectivement en bijection, mais ce n'est pas le cas de $\mathbb{R}$. Les premiers sont dits **dénombrables**.

Galilée a bien remarqué que les termes "autant d'éléments", "moins d'éléments" ou "plus d'éléments" ne peuvent s'appliquer sans paradoxe aux ensembles infinis. Le terme *bijection* n'était pas encore inventé, mais Galilée a mis en évidence une bijection entre $\mathbb{N}$ et une partie stricte de $\mathbb{N}$:

1	2	3	4	...	n	...
1	4	9	16	...	n^2	...

Deux ensembles en bijection sont dits **équipotents**. S'ils sont finis, cela signifie simplement qu'ils ont le même nombre d'éléments. Soit E un ensemble quelconque, et $\mathcal{P}$(E) l'ensemble de ses parties. Alors E et $\mathcal{P}$(E) ne sont pas équipotents. Nous avons en effet montré qu'il n'existe aucune bijection entre E et $\mathcal{P}$(E). Cette proposition assure l'existence d'ensembles non dénombrables, c'est–à–dire qui ne sont pas en bijection avec $\mathbb{N}$, par exemple $\mathcal{P}(\mathbb{N})$. On conçoit même une hiérarchie infinie d'espaces $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, ...

$\mathbb{N}$ est le plus petit ensemble infini. Si E est un ensemble quelconque, alors ou bien E est fini, ou bien il est dénombrable (en bijection avec $\mathbb{N}$), ou bien il existe une injection de $\mathbb{N}$ dans E mais pas de bijection (exemples: E = $\mathcal{P}(\mathbb{N})$ ou E = $\mathbb{R}$). Un ensemble dénombrable, étant en bijection avec $\mathbb{N}$, peut s'écrire sous la forme $\{x_n \mid n \in \mathbb{N}\}$; la bijection est l'application $f : \mathbb{N} \to E$, $n \to x_n$. Un ensemble dénombrable se reconnaît à ce qu'on peut énumérer ses éléments.

Toute partie d'un ensemble dénombrable est finie ou dénombrable, toute image d'un ensemble dénombrable est finie ou dénombrable.

La réunion de deux ensembles dénombrables est dénombrable. Ainsi $\mathbb{Z}$ est dénombrable. Voici une bijection entre $\mathbb{N}$ et $\mathbb{Z}$:

$$f : \mathbb{N} \to \mathbb{Z}$$
$$n \to \begin{cases} \frac{n}{2} \text{ si } n \text{ est pair} \\ -\frac{n+1}{2} \text{ si } n \text{ est impair} \end{cases}$$

Le produit de deux ensembles dénombrables est dénombrable. Ainsi $\mathbb{N}^2$ est dénombrable. Il suffit d'énumérer ses éléments dans l'ordre suivant :

1					
(0, 0)					
2	3				
(1, 0)	(0, 1)				
4	5	6			
(2, 0)	(1, 1)	(0, 2)			
7	8	9	10		
(3, 0)	(2, 1)	(1, 2)	(0, 3)		
11	12	13	14	15	
(4, 0)	(3, 1)	(2, 2)	(1, 3)	(0, 4)	
...					
$\frac{n(n-1)}{2}+1$	...			...	$\frac{n(n+1)}{2}$
$(n-1, 0)$	$(n-2, 1)$	$(n-3, 2)$		...	$(0, n-1)$
...					

D'une façon générale, le couple (a, b) est situé à la place de rang $\frac{(a+b)(a+b+1)}{2} + b + 1$. En effet, il y a $1 + 2 + 3 + ... + (a + b)$ couples depuis $(0, 0)$ jusqu'à $(0, a + b - 1)$, puis encore $b + 1$ couples depuis $(a + b, 0)$ jusqu'à (a, b). La bijection entre $\mathbb{N}^2$ et $\mathbb{N}^*$ est ici :

$$(a, b) \in \mathbb{N}^2 \rightarrow \frac{(a+b)(a+b+1)}{2} + b + 1 = m \in \mathbb{N}^*$$

La bijection réciproque se calcule comme suit. Soit $m \in \mathbb{N}^*$. Soit $\frac{k(k+1)}{2}$ le plus grand nombre triangulaire strictement inférieur à m. Alors $b = m - \frac{k(k+1)}{2} - 1$ et $a = m - b$.

En particulier $\mathbb{Q}$ est dénombrable. En effet $\mathbb{Q}^+$ peut s'injecter dans $\mathbb{N}^2$ au moyen d'une application du type $\frac{p}{q} \rightarrow (p, q)$.

A titre indicatif, voici une bijection curieuse entre $\mathbb{Q}^{+}*$ et $\mathbb{N}$. On définit la fonction f de $\mathbb{N}$ dans $\mathbb{N}^*$ de la façon suivante :

$$f(0) = 1 \text{ et } \forall\, n,\ f(2n + 1) = f(n),\ f(2n + 2) = f(n) + f(n + 1)$$

de sorte que les valeurs de f sont :

$$1, 1, 2, 1, 3, 2, 3, 1, 4, 3, 5, 2, 5, 3, 4, 1, 5, 4, 7, 3, 8 \ ...$$
$$\uparrow\uparrow \qquad\qquad \uparrow\uparrow$$
$$n\ n{+}1 \qquad 2n{+}1\ 2n{+}2$$

Les valeurs successives de $\frac{f(n)}{f(n+1)}$ sont :

$$1, \frac{1}{2}, 2, \frac{1}{3}, \frac{3}{2}, \frac{2}{3}, 3, \frac{1}{4}, \frac{4}{3}, \frac{3}{5}, \frac{5}{2}, \frac{2}{5}, \frac{5}{3}, \frac{3}{4}, 4, \frac{1}{5}, \frac{5}{4}, \frac{4}{7}, \frac{7}{3}, \frac{3}{8} \ ...$$

On montre que tous les rationnels positifs apparaissent une fois et une seule dans cette liste, de sorte que l'application $n \to \frac{f(n)}{f(n+1)}$ forme une bijection de $\mathbb{N}$ dans $\mathbb{Q}^{+*}$. La suite $(\frac{f(n)}{f(n+1)})$ est aussi égale à la suite (x_n) définie de l'une ou l'autre façon suivante :

$x_0 = 1$ et $x_n = \frac{1}{1 + 2p_n - x_{n-1}}$, où p_n est le plus grand entier k tel que 2^k divise $n + 1$

ou $x_0 = 1$ et $x_n = \frac{1}{1 + 2\lfloor x_{n-1} \rfloor - x_{n-1}}$, où $\lfloor\ \rfloor$ désigne la partie entière.

A un décalage près d'indice, la suite $(f(n))$ est la suite **diatomique de Stern**[1].

$\mathbb{R}$ n'est pas dénombrable. S'il l'était, il en serait de même de [0, 1[. Considérons alors une énumération $(x_n)_{n\in\mathbb{N}^*}$ de [0, 1[, obtenue au moyen d'une bijection $f : \mathbb{N}^* \to [0, 1[$, $n \to x_n$, et considérons le développement décimal des x_n.

$x_1 = 0,a_{11}a_{12}a_{13}...a_{1p}...$

$x_2 = 0,a_{21}a_{22}a_{23}...a_{2p}...$

...

$x_n = 0,a_{n1}a_{n2}a_{n3}...a_{np}...$

...

a_{np} est le $p^{\text{ème}}$ chiffre de la décomposition décimale de x_n. C'est un élément de {0, 1, ..., 9}.
Considérons maintenant l'élément y de]0, 1[défini de la façon suivante :

$y = 0,b_1b_2b_3...b_p...$

où $b_p = 0$ si $a_{pp} \neq 0$ et $b_p = 1$ si $a_{pp} = 0$.
On obtient le développement décimal d'un réel distinct de tous les x_n. En effet, le n^{eme} chiffre de x_n et y sont différents ($\forall\ n,\ b_n \neq a_{nn}$). Par ailleurs, il est évident que y appartient à [0, 1[. Cela est contradictoire avec le fait que f soit bijective, puisqu'alors, tout élément de [0, 1[serait de la forme d'un des x_n. Cette démonstration est connue sous le nom de diagonalisation de Cantor.

On peut prouver que $\mathbb{R}$ est équipotent à $\mathcal{P}(\mathbb{N})$, et que les trois ensembles suivants sont équipotents : $\mathcal{P}(\mathbb{R})$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$ et $C^0(\mathbb{R})$ l'ensemble des fonctions continues sur $\mathbb{R}$.

Signalons également une question étonnante. Peut–on trouver un ensemble E compris entre $\mathbb{N}$ et $\mathbb{R}$, mais qui ne soit équipotent ni à $\mathbb{N}$, ni à $\mathbb{R}$? On aurait seulement des injections de $\mathbb{N}$ dans E et de E dans $\mathbb{R}$. Rappelons que $\mathbb{Q}$ ne répond pas à la question puisqu'il est en bijection avec $\mathbb{N}$. On a prouvé qu'il était *impossible* de répondre à cette question. Cela ne signifie pas qu'on n'ait pas encore trouvé si cette propriété était vraie ou fausse, mais bel et bien qu'on ne peut ni prouver qu'elle est vraie, ni prouver qu'elle est fausse. Elle est dite **indécidable**. Elle ne découle pas des axiomes de la théorie des ensembles, pas plus que sa négation. Cela signifie également qu'on peut prendre comme

[1] Le lecteur intéressé pourra consulter les articles suivants :
- N. Calkin and H. S. Wilf : *Recounting the rationals*, 107:4, Amer. Math. Monthly, (avril 2000), 360-363.
- Problème n° 10906, *Recounting the Rationals, Continued*, 110:7, Amer. Math. Monthly, (août-septembre 2003), 642-643, Solution de C. P. Rupert.
- Sam Northshield, *Stern's diatomic sequence*, 0, 1, 1, 2, 1, 3, 2, 3, 1, 4, ..., 117:7, Amer. Math. Monhtly, (août-septembre 2010), 581-598.
- S. P. Glasby, *Enumerating the rationals from left to right*, 118:9, Amer. Math. Monthly, (novembre 2011), 830-835.
- Aimeric Malter, Dierk Schleicher, Don Zagler, *New looks at old number theory*, 120:3, Amer. Math. Monthly, (mars 2013), 243-264.

axiome supplémentaire l'existence d'un tel ensemble E sans apporter de contradiction à l'édifice des mathématiques, ou au contraire, de prendre comme axiome la non-existence de E. Dans ce dernier cas, on adopte ce qu'on appelle l'**hypothèse du continu**. L'un ou l'autre choix conduit donc à deux théories mathématiques différentes.

Ces considérations n'ont aucune importance en ce qui nous concerne, car nous n'utiliserons jamais cette propriété, ni sa négation !

Donnons enfin une conséquence curieuse de ce qui précède en informatique. On peut montrer que l'ensemble de tous les algorithmes possibles est dénombrable, alors que l'ensemble des fonctions de $\mathbb{N}$ dans $\mathbb{N}$ est équipotent à $\mathbb{R}$. Il y a donc des fonctions de $\mathbb{N}$ dans $\mathbb{N}$ qui ne sont calculables par aucun ordinateur. Aucun algorithme ne permet de les calculer. De telles fonctions ont été explicitement définies.

Annexe II : les axiomes

1- Qu'est-ce qu'un axiome ?

D'Alembert écrit, dans son Encyclopédie (1788) :

> ***Axiome*** *: En Mathématiques, on appelle axiomes des propositions évidentes par elles-mêmes, et qui n'ont pas besoin de démonstrations. Telles sont les propositions suivantes : le tout est plus grand que la partie ; si à deux grandeurs égales on ajoute des grandeurs égales, les sommes seront égales ; si deux figures étant appliquées l'une sur l'autre se couvrent parfaitement, ces deux figures sont égales en tout.*
>
> ***Théorème*** *: c'est une proposition qui énonce et démontre une vérité.*

Notre conception moderne des axiomes ne correspond plus à des notions déclarées évidentes par elles-mêmes. On fait actuellement reposer une théorie mathématique sur des notions primitives (non définies) et les axiomes ne servent qu'à décrire les règles d'utilisation de ces notions primitives. Voici des exemples modernes d'axiomes et de notions primitives :

i) La notion d'ensemble et d'appartenance est une notion primitive. On ne cherchera à définir ni l'une ni l'autre.

ii) Frege, en 1893, avait proposé comme axiome le suivant : Φ étant un prédicat quelconque, il existe un ensemble A tel que, pour tout x, x appartient à A si et seulement si $\Phi(x)$ est vrai. Russel, en 1902, proposa de prendre comme prédicat : $\Phi(x) \Leftrightarrow x \notin x$. D'après Frege, il existe alors un ensemble A tel que :

$$\forall\, x,\ x \in A \Leftrightarrow x \notin x$$

Cette équivalence est vraie en particulier lorsque $x = A$, ce qui donne :

$$A \in A \Leftrightarrow A \notin A$$

ce qui contradictoire. Cet exemple montre la difficulté à déterminer correctement des axiomes, en particulier en ce qui concerne la construction des ensembles.

Voici quelques axiomes actuellement en vigueur :

- ❑ La réunion d'une famille d'ensemble (indicée par un ensemble) est un ensemble.
- ❑ La famille constituée des parties d'un ensemble est un ensemble.
- ❑ Il existe un ensemble infini
- ❑ Le principe de récurrence dans $\mathbb{N}$

❑ Le 5ème postulat d'Euclide en géométrie euclidienne : par un point donné, il passe une parallèle à une droite donnée et une seule. Le rejet de cet axiome conduit à des géométries dites non-euclidiennes.
❑ L'existence de la borne supérieure dans $\mathbb{R}$

2- Un axiome curieux, l'axiome du choix

Considérons la proposition suivante :
Soit f une application injective de E *dans* F. *Alors il existe une application surjective g de* F *dans* E *telle que* $g \circ f = \mathrm{Id}_E$.

Démonstration :
❑ Soit a un élément quelconque de E. On pose :
i) si y appartient à f(E), $g(y) = x$ où x est l'unique élément tel que $y = f(x)$.
ii) si y n'appartient pas à f(E), on pose $g(y) = a$.
On a alors g surjective et $g \circ f = \mathrm{Id}_E$.

Considérons maintenant la proposition suivante :
Soit f une application surjective de E *dans* F. *Alors il existe une application injective g de* F *dans* E *telle que* $f \circ g = \mathrm{Id}_F$.

Démonstration :
❑ Pour tout y de F, $f^{-1}(\{y\})$ est non vide. Soit $g(y)$ un élément de cette partie. Alors g est injective et $f \circ g = \mathrm{Id}_F$.

Il y a une différence fondamentale entre ces deux démonstrations. La première ne fait appel qu'au choix arbitraire d'un unique élément a, alors que la seconde fait appel au choix simultané et arbitraire d'un nombre quelconque et éventuellement infini (si F est infini) d'éléments $g(y)$. La possibilité d'un tel choix a été vivement contesté au début du XXème siècle et nécessite un axiome : l'axiome du choix. Ce dernier est également lié à la question de munir un ensemble d'un "bon ordre" ; un ensemble est dit **bien ordonné** si toute partie non vide admet un minimum. Un exemple typique d'ensemble bien ordonné est $\mathbb{N}$. Par contre, $\mathbb{R}$ n'est pas bien ordonné avec l'ordre usuel. Cantor pensait que tout ensemble pouvait être muni d'un bon ordre, et la nécessité d'une démonstration s'est posé. On peut se demander en effet comment il peut être possible de munir par exemple $\mathbb{R}$ d'un bon ordre. Au début du siècle, on pensa avoir montré l'impossibilité de munir $\mathbb{R}$ d'un bon ordre. Mais Zermelo prouva le contraire en utilisant pour la première fois ce qui allait devenir l'**axiome du choix** :
Soit $(A_i)_{i \in I}$ *une famille d'ensembles non vides, indicée par un ensemble* I *quelconque et soit* A *la réunion des* A_i. *Alors il existe une application f de* I *dans* A *telle que :*

$$\forall\, i \in I,\ f(i) \in A_i.$$

La fonction f permet de choisir un élément noté $f(i)$ dans chaque A_i. D'autres formulations équivalentes sont possibles. Par exemple, le produit $\prod_{i \in I} A_i$ est non vide.

On montre que cet axiome permet de munir $\mathbb{R}$ d'un bon ordre, sans qu'on puisse cependant l'expliciter, et ceci choqua bon nombre de mathématiciens qui le rejetèrent. Cependant, d'autres théorèmes, dont les énoncés paraissaient vraisemblables à la communauté mathématique nécessitent l'axiome du choix. En voici quelques-uns :

❑ Soit E et F deux ensembles. Alors ou bien il existe une injection de E dans F ou bien il existe une injection de F dans E. (**Théorème de Cantor**, équivalent à l'axiome du choix)
❑ Soit E un espace vectoriel. Alors il existe une base sur E.
❑ Tout ensemble inductif admet un élément maximal. (Un ensemble est **inductif** si toute partie totalement ordonnée est majorée). (**Théorème de Zorn**, équivalent à l'axiome du choix).

Certains résultats cependant sont prouvés au moyen de l'axiome du choix et fortement contraires à l'intuition :
❑ Lebesgue a développé une théorie de l'intégration très puissante. Toutes les fonctions usuelles sont mesurables au sens de Lebesgue. Les seuls exemples non mesurables qui ont été découverts nécessitent l'axiome du choix.
❑ La sphère unité peut être décomposée en quatre parties isométriques A, B, C, D avec D également isométrique à $A \cup B$. (D est donc à la fois le quart et la moitié de la sphère). (**Théorème de Hausdorf**, extrêmement choquant. Le paradoxe se lève du fait qu'il n'est pas possible d'attribuer une aire à ces parties).
❑ Dans le même ordre d'idée, deux ensembles bornés quelconques de $\mathbb{R}^3$ d'intérieur non vide peuvent être partitionnés en deux familles finies respectives (A_i) et (B_i) de façon que A_i soit isométrique à B_i. (**Théorème de Banach-Tarski**).
❑ Il existe des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ telle que $f(x + y) = f(x) + f(y)$, avec f différente des fonctions linéaires ax. Cependant aucune de ces fonctions ne peut être explicitée.

La nature de l'axiome du choix est donc complexe. Affirmant l'existence d'un objet, il ne peut cependant définir explicitement cet objet. Bien plus, une telle explicitation est impossible puisque le rejet de l'axiome (qui est possible) supprimerait la seule possibilité de valider son existence.

Ces questions sont liées à la nature de la notion de l'existence en mathématiques. Il y a deux notions différentes, l'une est l'existence explicite, fournissant le moyen de construire l'objet (par exemple, étant donnés deux entiers, on peut déterminer explicitement le plus petit multiple commun de ces deux entiers), l'autre est une existence purement formelle ne fournissant aucun moyen de définir explicitement l'objet (des exemples ont été donnés précédemment). Les mathématiques usuelles ne font aucune distinction entre ces deux notions d'existence, ce qu'on peut juger regrettable car l'existence formelle a une utilité et une efficacité bien moins grande que l'existence explicite. Avouons cependant que les branches des mathématiques cherchant à apporter une distinction entre ces deux notions d'existence (logique intuitionniste, analyse constructive) sont difficiles à aborder. Selon un mot d'Hermann Weyl, l'existence formelle consiste à savoir qu'il y a un trésor dans une île. L'existence effective consiste à savoir qu'il y a un trésor dans un île et en posséder une carte.

On peut néanmoins reconnaître cette qualité à l'existence formelle : elle prouve qu'il est vain de dépenser ces efforts à montrer l'inexistence de l'objet considéré. Considérons par exemple une propriété donnée sur les entiers dont on ignore actuellement si elle est vraie ou fausse, par exemple, celle d'être un nombre impair **parfait** (i.e. égal à la somme de ses diviseurs autres que lui-même. 6 et 28 sont parfaits mais ils sont pairs) et posons-nous la question de savoir si cette propriété est vérifiée par au moins un entier. Il y a alors trois possibilités.

i) Aucun entier ne vérifie la propriété.

ii) Il existe au moins un entier vérifiant la propriété et on peut donner sa valeur (existence explicite).

iii) Il existe au moins un entier vérifiant la propriété mais on ne peut donner sa valeur (existence formelle), soit parce que cette valeur est trop grande pour pouvoir être calculée, soit parce qu'on ignore un procédé de calcul de cette valeur, soit même parce que cette existence repose sur un axiome. Si on se trouve dans ce dernier cas, cela montre qu'il est inutile de chercher à prouver i).

3- Sur le principe de récurrence

Le principe de récurrence ne se prouve pas. On indique dans L1/ARITHMTQ.PDF qu'il s'agit d'un axiome, supposé par définition être vérifié par les entiers. Cependant, on trouve parfois dans la littérature mathématiques des tentatives de justification. En voici deux exemples :

Le premier est un extrait d'un livre paru en 1993[2] :

> *Le principe de récurrence s'énonce informellement ainsi ; si une certaine propriété sur les nombres entiers est vraie pour* 0 *et si la propriété est vraie pour le successeur d'un nombre dès qu'elle est vraie pour ce nombre, alors cette propriété est vraie pour tous les nombres. Formellement : soit* P(*n*) *une propriété qui dépend d'un entier n. Si les phrases suivantes sont vraies :*
>
> 1. P(0) *est vraie,*
> 2. *si* P(*n*) *est vraie, alors* P(*n* + 1) *est vraie,*
>
> *alors* P(*n*) *est vraie pour tout n.*
>
> *Ce principe est en fait évident : les deux propriétés demandées par le principe de récurrence permettent facilement de démontrer la propriété* P *pour toute valeur entière. Par exemple, supposons que* P *vérifie les deux propriétés et qu'on veuille démontrer que* P *est vraie pour* 2. *Puisque* P *est vraie pour* 0, *elle est vraie pour son successeur* 1. *Mais puisque* P *est vraie pour* 1, *elle est vraie pour son successeur, donc elle est vraie pour* 2. *Il est clair que ce raisonnement se poursuit sans problème pour tout nombre entier fixé à l'avance.*

Contrairement à ce que dit ce texte, on prendra conscience que le principe de récurrence n'est pas une évidence en soi. Ainsi, Gödel (1906-1978) dans les années 1930 a présenté un prédicat[3] stupéfiant P(*n*) tel que :

pour tout *n*, il existe une démonstration de P(*n*)
il n'existe pas de démonstration de $\forall$ *n*, P(*n*)

En effet, la réunion de toutes les démonstrations de P(*n*) n'est pas une démonstration de $\forall$ *n*, P(*n*), car cette réunion est infinie, or une démonstration se doit d'être finie. C'est cette objection qui rend invalide la tentative de justification du texte ci-dessus. Le principe de récurrence consiste justement à décider d'accepter comme démonstration valide une démarche qui nécessiterait une infinité de pas. C'est un élargissement de la notion de démonstration qui est ainsi proposé.

Le deuxième exemple est tiré de la revue *Tangente* de décembre 1987 (n° 2). Il affirme démontrer trois principes, dont le principe de récurrence. Or il n'en est rien. Il y a une faille[4] dans le raisonnement qui n'échappera pas à un esprit sagace.

---

[2] Le langage CAML, Weis et Leroy, InterEditions.

[3] Ce prédicat est par exemple exposé dans le livre grand public de Douglas Hofstader, *Gödel, Escher, Bach*, InterEditions (1985), p.507.

[4] La faille réside dans le fait que la relation $x_n \leq x_0 - n$ se montre évidemment par récurrence !! Le principe de récurrence est donc supposé valide pour pouvoir montrer le principe de descente infini de Fermat.

Premièrement : Le principe de descente infinie de Fermat. Il ne peut exister de suite infinie strictement décroissante d'entiers naturels.

Démonstration : si (x_n) *était une telle suite, on aurait* $x_{n+1} < x_n$ *pour tout n entier naturel, donc* $x_{n+1} \leq x_n - 1$. *En appliquant ceci à* $n = 0, 1, 2, ...,$ *on trouve successivement :* $x_1 \leq x_0 - 1$, $x_2 \leq x_1 - 1$, *etc. On en déduit :* $x_2 \leq x_0 - 2$, $x_3 \leq x_0 - 3, ...,$ $x_n \leq x_0 - n$. *En prenant* $n = x_0 + 1$, *on obtient* $x_n < -1$, *ce qui contredit le fait que la suite* x_n *est composée d'entiers naturels.*

Deuxièmement : Le principe du bon ordre. Tout ensemble non vide X *d'entiers naturels comporte un plus petit élément.*

Démonstration : Si X *n'avait pas de plus petit élément, alors pour chaque élément de* X, *il y en aurait un autre, strictement plus petit. Partant d'un élément donné a appartenant à* X, *on pourrait fabriquer ainsi une suite strictement décroissante :* $x_0 = a$, $x_1 < x_0$, $x_2 < x_1$, *etc, infinie, composée d'éléments de* X, *ce qui contredit le principe précédent.*

Troisièmement : Le principe de récurrence. Soit X *un ensemble d'entiers naturels contenant* 0 *qui vérifie la propriété suivante : pour tout x appartenant à* X, *alors* $x + 1$ *appartient à* X. *On peut en conclure que* X *est l'ensemble de tous les entiers naturels.*

Démonstration : Si X *n'était pas l'ensemble de tous les entiers naturels, soit* Y *l'ensemble des entiers naturels y non éléments de* X. *D'après le principe du bon-ordre, cet ensemble* Y *aurait un plus petit élément* y_0 *qui ne serait pas égal à* 0, *puisque* 0 *appartient à* X. *Donc* $y_0 \geq 1$ *et par suite* $y_0 - 1$ *appartient à* $\mathbb{N}$. *Si* $y_0 - 1$ *appartient à* X, *on a de par la propriété de* X *:* $(y_0 - 1) + 1$ *appartient à* X, *soit* y_0 *appartient à* X, *ce qui est impossible. Si* $y_0 - 1$ *n'appartient pas à* X, *on a* $y_0 - 1$ *dans* Y, *impossible encore car* y_0 *est le plus petit élément de l'ensemble* Y.

4- Analyse non standard

Le principe de récurrence est donc un axiome. Or comme tout axiome, la décision de l'adopter ne relève pas d'une évidence en soi, mais d'un choix arbitrairement fait, essentiellement pour des raisons de commodité ou d'efficacité.

De même que le rejet de l'axiome d'Euclide conduit aux géométries non-euclidiennes, que se passe-t-il si l'on décide de *rejeter l'axiome de récurrence* ? On obtient alors une nouvelle théorie mathématique totalement étrangère à tout ce à quoi nous sommes habitués, mais tout aussi cohérente que la théorie usuelle (si tant est que celle-ci le soit, ce qu'on ignore). Que signifie rejeter le principe de récurrence ? Cela signifie que, dans notre nouvel ensemble d'entiers, il existe un prédicat P tel que l'on ait *simultanément* les *trois* propriétés suivantes :

P(0) est vrai

$\forall\, n$, P(n) $\Rightarrow$ P($n + 1$)

$\exists\, n$, non P(n)

Quel sens donner à un tel prédicat P ? Est-ce concevable ? Comment définir une propriété vraie pour 0, vraie pour $n + 1$ si elle est vraie pour n, et cependant fausse pour un certain entier. Voici une possibilité. Les entiers n vérifiant la propriété P seront qualifiés d'accessibles, de limités, ou de **standard**. Les entiers n ne vérifiant pas la propriété P seront qualifiés d'inaccessibles, d'illimités, ou de **non standard**. Ainsi, 0 est accessible. Si n est accessible, alors $n + 1$ l'est aussi. Cependant, il existe des entiers qui nous sont inaccessibles. Finalement, cette position n'est peut-être pas si

incroyable que cela. Après tout, la propriété P ainsi définie ne correspond-elle pas à la réalité ? Cette position a été développée par Nelson dans les années 1960. Il définit l'analyse non standard de la façon suivante :

- On se place dans le cadre de la théorie des ensembles de Zermelo-Fraenkel (celle que nous pratiquons tous sans le savoir, comme M. Jourdain).
- Les objets ou les ensembles définis par cette théorie seront qualifiés d'**internes** ou **classiques**.
- On introduit un nouveau prédicat, *étranger à la théorie de Zermelo-Fraenkel*, et qui s'applique sur les ensembles internes. Un tel ensemble ou objet pourra être qualifié de **standard** ou de **non standard**. Ce prédicat est une notion primitive au même titre que la notion d'ensemble ou d'appartenance.
- On définit trois règles – que nous ne détaillerons pas ici – permettant de manipuler ce nouveau prédicat.

Pour comprendre cette démarche, faisons un parallélisme avec ce que vivent les élèves de Terminale lorsqu'ils découvrent les nombres complexes :
- Ils se placent dans le cadre des nombres rencontrés jusqu'en Première.
- De tels nombres sont qualifiés de **réels**.
- On introduit un nombre, *étranger aux réels*, baptisé ***i***.
- On définit les règles de calcul relatives à i (essentiellement $i^2 = -1$)

Une fois cette démarche adoptée, on dispose d'une théorie mathématique plus riche qu'avant. (Il faut bien sûr s'assurer que l'on a pas introduit d'incohérence). Pour en revenir à l'analyse non standard, le principe de récurrence continuera à s'appliquer aux prédicats internes. En particulier, la somme des n premiers entiers continuera à valoir $\frac{n(n+1)}{2}$. Mais le principe de récurrence *ne peut pas* s'appliquer aux entiers non standard, car le fait d'être standard ou non n'est pas une propriété interne. 0 est standard. Si n est standard, alors $n + 1$ est standard, **mais** il existe néanmoins des entiers non standard. Ceci est déroutant (mais peut-être tout autant que d'admettre qu'il existe un nombre de carré –1 !!).

A quoi peut bien servir cette théorie ? Il y a deux types d'applications :
- Il a été établi qu'un énoncé interne, possédant une démonstration dans le cadre de l'analyse non standard, était vrai dans le cadre des mathématiques classiques. La situation est tout à fait comparable aux calculs numériques réels qui donnent un résultat réel valide, même si, transitoirement, on a utilisé les nombres complexes.
- L'analyse non-standard permet en outre de manipuler les concepts nouveaux de nombre infiniment petit ou d'infiniment grand qui ont posé tant de problèmes aux mathématiciens et qui avaient été bannis de l'analyse. Elle est donc plus générale, de même que l'analyse complexe est plus générale que l'analyse réelle.

Exercices

1- Enoncés

Exo.1) Comparer les ensembles suivants :

a) $A \cup (B - C)$

b) $(A \cup B) - (C - A)$

c) $(A \cup B) - C$
d) $(A \cup B) - (C - (A \cap B))$

Exo.2) Soient U et V deux parties d'un ensemble E. Que signifient les énoncés suivants ?
a) $(\forall\, x \in U, x \notin V)$ ou $(\forall\, x \in V, x \notin U)$
b) $\forall\, x$, non $(x \in U \Leftrightarrow x \in V)$
c) $\exists\, x\ (x \in U \Leftrightarrow x \notin V)$

Exo.3) Soit E un ensemble non vide et f une application de E dans E telle que :

$$\forall\, A \subset E,\ f(A) \subset A \Rightarrow A = \varnothing \text{ ou } A = E.$$

Montrer que E est fini.
(Indication : si on pose $f^0 = Id$ et $f^n = f \circ f \circ ... \circ f$ n fois, on pourra considérer, pour x dans E, $A = \{f^n(x), n \geq 0\}$ et $B = \{f^n(x), n > 0\}$)

Exo.4) Soient A et B deux parties données d'un ensemble E. On considère l'application suivante :

$$\begin{aligned} f : \mathcal{P}(E) &\to \mathcal{P}(A) \times \mathcal{P}(B) \\ X &\to (A \cap X, B \cap X) \end{aligned}$$

où $\mathcal{P}(E)$ désigne l'ensemble des parties de E. A quelle condition nécessaire et suffisante portant sur A et B a-t-on :
a) f injective ?
b) f surjective ?
c) Si f est bijective, expliciter f^{-1}.

Exo.5) X et Y étant deux ensembles, on pose :

$$\begin{aligned} p : X \times Y &\to X \\ (x, y) &\to x \\ q : X \times Y &\to Y \\ (x, y) &\to y \end{aligned}$$

Soit $f : X \to Y$ de graphe G, A une partie de X, B une partie de Y. Identifier les ensembles $q(G \cap (A \times Y))$ et $p(G \cap (X \times B))$.

Exo.6) Soit $(A_i)_{i \in I}$ une famille de parties d'un ensemble E. Comparer :

a) $\bigcap_{i \in I} \mathcal{P}(A_i)$ et $\mathcal{P}(\bigcap_{i \in I} A_i)$

b) $\bigcup_{i \in I} \mathcal{P}(A_i)$ et $\mathcal{P}(\bigcup_{i \in I} A_i)$

Exo.7) a) Soit f la fonction définie de $\mathbb{R}$ dans $\mathbb{R}$ par $f(x) = x^2$ et g la fonction définie de $\mathbb{R}$ dans $\mathbb{R}$ par $g(x) = e^x$. Trouver deux parties A et B de $\mathbb{R}$ telles que $f(A) = B$ et $g(B^c) = A^c$ (les complémentaires étant pris dans $\mathbb{R}$).

b) Même question avec le même f, mais avec $g(x) = \sin(x)$.

Exo.8) Soit $f : E \to F$, S inclus dans F et U contenant $f^{-1}(S)$. Soit $V = \complement_F f(\complement_E U)$, où $\complement_E$ et $\complement_F$ désignent respectivement les complémentaires dans E et dans F. Montrer que $S \subset V$ et que $f^{-1}(S) \subset f^{-1}(V) \subset U$.

Exo.9) Une relation $\mathcal{R}$ sur un ensemble E est **circulaire** si :

$$\forall\, x, \forall\, y, \forall\, z,\ x\ \mathcal{R}\, y \text{ et } y\ \mathcal{R}\, z \Rightarrow\ z\ \mathcal{R}\, x.$$

Montrer qu'il y a équivalence entre :

(i) $\mathcal{R}$ est circulaire et réflexive.

(ii) $\mathcal{R}$ est une relation d'équivalence.

Exo.10) Soit f une application d'un ensemble E dans un ensemble F. Soit $\mathcal{R}$ la relation binaire définie sur E par $x\ \mathcal{R}\, y \Leftrightarrow f(x) = f(y)$. Vérifier qu'il s'agit d'une relation d'équivalence. On note C(x) la classe de x. Soit S une partie de E. Montrer que :

$$[\ \forall\, x \in \mathrm{S},\ \mathrm{C}(x) \subset \mathrm{S}\ ] \Leftrightarrow\ f^{-1}(f(\mathrm{S})) = \mathrm{S}$$

Exo.11) Soient $\mathcal{R}$ et $\mathcal{S}$ deux relations d'équivalences (respectivement relations d'ordre) sur un ensemble E. Les relations définies par "$x\ \mathcal{R}\, y$ et $x\ \mathcal{S}\, y$", puis "$x\ \mathcal{R}\, y$ ou $x\ \mathcal{S}\, y$" sont-elles des relations d'équivalences (respectivement relations d'ordre) ?

Exo.12) Pour tout couple de réels (a, b), on pose : $a * b = a + b + ab$.

a) ($\mathbb{R}$, *) est-il un groupe ?

b) Déterminer une partie G de $\mathbb{R}$, telle que (G, $*$) soit un groupe.

c) Que vaut $a_1 * a_2 * \ldots * a_n$?

Exo.13) La notation choisie pour désigner l'image et l'image réciproque d'une partie n'est pas très heureuse. Dans cette exercice, on préfère les noter de la façon suivante. Soit $f : \mathrm{E} \to \mathrm{F}$ une fonction. A chaque partie A de E, on associe son image directe D(A) = $\{f(x),\ x \in \mathrm{A}\}$. On définit ainsi une application D de $\mathcal{P}$(E) dans $\mathcal{P}$(F).

a) Montrer que f est injective si et seulement si D est injective.

b) Montrer que f est surjective si et seulement si D est surjective.

On note maintenant R(B) = $\{x \in \mathrm{E},\ f(x) \in \mathrm{B}\}$ l'image réciproque d'une partie B de F. On définit également ainsi une application de $\mathcal{P}$(F) dans $\mathcal{P}$(E).

c) Montrer que R est injective si et seulement si f est surjective.

d) Montrer que R est surjective si et seulement si f est injective.

Exo.14) Soit E un ensemble de cardinal n.

a) Combien y a-t-il de relations réflexives ?

b) Combien y a-t-il de relations symétriques ?

2- Solutions

Sol.1) a) $x \in \mathrm{A} \cup (\mathrm{B} - \mathrm{C}) \Leftrightarrow x \in \mathrm{A}$ ou ($x \in \mathrm{B}$ et $x \notin \mathrm{C}$)

b) $x \in (\mathrm{A} \cup \mathrm{B}) - (\mathrm{C} - \mathrm{A}) \Leftrightarrow x \in \mathrm{A} \cup \mathrm{B}$ et $x \notin (\mathrm{C} - \mathrm{A})$

$\Leftrightarrow x \in \mathrm{A} \cup \mathrm{B}$ et non ($x \in (\mathrm{C} - \mathrm{A})$)

$\Leftrightarrow x \in \mathrm{A} \cup \mathrm{B}$ et non ($x \in \mathrm{C}$ et $x \notin \mathrm{A}$)

$\Leftrightarrow x \in \mathrm{A} \cup \mathrm{B}$ et ($x \notin \mathrm{C}$ ou $x \in \mathrm{A}$)

$\Leftrightarrow$ ($x \in \mathrm{A} \cup \mathrm{B}$ et $x \notin \mathrm{C}$) ou $x \in \mathrm{A}$

$\Leftrightarrow (x \in B$ et $x \notin C)$ ou $x \in A$

donc (a) = (b)

c) Dans la démonstration précédente, on a vu que :

$(A \cup B) - (C - A) = ((A \cup B) - C) \cup A$

Or $(A \cup B) - C \subset B - C$, donc (c) $\subset$ (b). Il n'y a pas toujours égalité. Par exemple, prenons A = B = C non vide. Alors $(A \cup B) - C = \varnothing$ alors que $(A \cup B) - (C - A) = A$.

d) $x \in (A \cup B) - (C - (A \cap B)) \Leftrightarrow x \in A \cup B$ et $x \notin (C - (A \cap B))$

$\Leftrightarrow x \in A \cup B$ et non $(x \in C - (A \cap B))$

$\Leftrightarrow x \in A \cup B$ et non $(x \in C$ et $x \notin A \cap B)$

$\Leftrightarrow x \in A \cup B$ et $(x \notin C$ ou $x \in A \cap B)$

$\Leftrightarrow (x \in A \cup B$ et $x \notin C)$ ou $x \in A \cap B$

$\Leftrightarrow (x \in (A \cup B) - C)$ ou $x \in A \cap B$

Donc $(A \cup B) - (C - (A \cap B)) = ((A \cup B) - C) \cup (A \cap B)$. On a vu que :

(b) = $((A \cup B) - C) \cup A$

donc (c) $\subset$ (d) $\subset$ (b).

Il n'y a pas toujours égalité. Par exemple, C = {1, 2}, A = C, B = {1}. On a :

(c) = $\varnothing$

(d) = B

(b) = A

Sol.2) a) La proposition $(\forall\ x \in U,\ x \notin V)$ et la proposition $(\forall\ x \in V,\ x \notin U)$ sont en fait équivalentes. On passe de l'une à l'autre par contraposition dans l'implication $\forall\ x, x \in U \Rightarrow x \notin V$. La conjonction des deux est inutile. Elles sont toutes deux équivalentes à $U \subset V^c$, $V \subset U^c$ ou encore $U \cap V = \varnothing$.

b) La proposition équivaut successivement aux propositions suivantes :

$\forall\ x$, (non $((x \in U \Rightarrow x \in V)$ et $(x \in V \Rightarrow x \in U)))$

$\forall\ x$, (non $(x \in U \Rightarrow x \in V)$ ou non $(x \in V \Rightarrow x \in U))$

$\forall\ x$, $((x \in U$ et $x \notin V)$ ou $(x \in V$ et $x \notin U))$

$\forall\ x$, $(x \in U \cap V^c$ ou $x \in V \cap U^c)$

$\forall\ x, x \in (U \cap V^c) \cup (V \cap U^c)$

tout x appartient à une et une seule des parties U ou V

U et V sont complémentaires

c) La proposition équivaut successivement aux propositions suivantes :

$\exists\ x\ ((x \in U \Rightarrow x \notin V)$ et $(x \notin V \Rightarrow x \in U))$

$\exists\ x\ ((x \notin U$ ou $x \notin V)$ et $(x \in V$ ou $x \in U))$

$\exists\ x\ (x \in U^c \cup V^c$ et $x \in U \cup V)$

$\exists\ x\ (x \in (U \cap V)^c$ et $x \in U \cup V)$

$\exists\ x\ (x \notin U \cap V$ et $x \in U \cup V)$

$U \Delta V \neq \varnothing$

$U \neq V$

Sol.3) On a $f(A) = \{f^{n+1}(x),\ n \geq 0\} = \{f^n(x),\ n \geq 1\} = B \subset A$. Or $A \neq \varnothing$, donc A = E. On montre de même que B = E. Donc A = B. Comme $x \in A$ (pour $n = 0$), $x \in B$ et il existe $n > 0$, $f^n(x) = x$. Mais alors les images itérées de x bouclent circulairement et les éléments de A se réduisent à x, $f(x)$, $f^2(x)$, ..., $f^{n-1}(x)$.

Sol.4) a) Si $A \cup B = E$, alors f est injective. En effet, soient X et X' tels que $f(X) = f(X')$. Alors on a $(A \cap X, B \cap X) = (A \cap X', B \cap X')$ donc on a $(A \cap X) \cup (B \cap X) = (A \cap X') \cup (B \cap X')$. Mais $(A \cap X) \cup (B \cap X) = X$ et $(A \cap X') \cup (B \cap X') = X'$. Donc $X = X'$
Réciproquement, si $A \cup B \neq E$, alors $E \setminus (A \cup B) \neq \varnothing$ et f n'est pas injective car on a $f(\varnothing) = f(E \setminus (A \cup B))$.
b) Si $A \cap B = \varnothing$ alors f est surjective car, pour toute partie A' de A et B' de B, on a $f(A' \cup B') = (A', B')$.
Réciproquement, si $A \cap B \neq \varnothing$, f n'est pas surjective car $(\varnothing, A \cap B)$ n'a pas d'antécédent. En effet, un tel antécédent X devrait vérifier $A \cap X = \varnothing$ donc être disjoint de A mais être tel que $B \cap X = B \cap A$. On aurait alors $B \cap A = B \cap A \cap A = B \cap X \cap A = B \cap \varnothing = \varnothing$ contraitement à l'hypothèse.
c) f est bijective si et seulement si A et B sont complémentaire l'un de l'autre et alors l'antécédent de (A', B') est $A' \cup B'$.

Sol.5) $z \in q(G \cap (A \times Y)) \Leftrightarrow \exists\, (x, y) \in G \cap (A \times Y)$ et $z = q(x, y)$
$\Leftrightarrow \exists\, (x, y) \in G \cap (A \times Y)$ et $z = y$
$\Leftrightarrow \exists\, x, (x, z) \in G \cap (A \times Y)$
$\Leftrightarrow \exists\, x \in A, (x, z) \in G$
$\Leftrightarrow \exists\, x \in A, z = f(x)$
$\Leftrightarrow z \in f(A)$
$q(G \cap (A \times Y))$ est l'image directe de A par f. Dans l'ensemble $X \times Y$, on intersecte $A \times Y$ par le graphe de f puis on projette sur Y.
$z \in p(G \cap (X \times B)) \Leftrightarrow \exists\, (x, y) \in G \cap (X \times B)$ et $z = p(x, y)$
$\Leftrightarrow \exists\, (x, y) \in G \cap (X \times B)$ et $z = x$
$\Leftrightarrow \exists\, y, (z, y) \in G \cap (X \times B)$
$\Leftrightarrow \exists\, y \in B, (z, y) \in G$
$\Leftrightarrow \exists\, y \in B, y = f(z)$
$\Leftrightarrow f(z) \in B$
$\Leftrightarrow z \in f^{-1}(B)$
$p(G \cap (X \times B))$ est l'image réciproque de B par f. Dans l'ensemble $X \times Y$, on intersecte $X \times B$ par le graphe de f puis on projette sur X.

Sol.6) a) $B \in \bigcap_{i \in I} \mathcal{P}(A_i) \Leftrightarrow \forall\, i, B \in \mathcal{P}(A_i) \Leftrightarrow \forall\, i, B \subset A_i \Leftrightarrow B \subset \bigcap_{i \in I} A_i \Leftrightarrow B \in \mathcal{P}(\bigcap_{i \in I} A_i)$

Donc $\bigcap_{i \in I} \mathcal{P}(A_i) = \mathcal{P}(\bigcap_{i \in I} A_i)$.

b) $B \in \bigcup_{i \in I} \mathcal{P}(A_i) \Leftrightarrow \exists\, i, B \in \mathcal{P}(A_i) \Leftrightarrow \exists\, i, B \subset A_i \Rightarrow B \subset \bigcup_{i \in I} A_i \Leftrightarrow B \in \mathcal{P}(\bigcup_{i \in I} A_i)$

Donc $\bigcup_{i \in I} \mathcal{P}(A_i) \subset \mathcal{P}(\bigcup_{i \in I} A_i)$. Mais la réciproque est fausse. En effet, si $B \subset \bigcup_{i \in I} A_i$ cela ne signifie pas que B est inclus dans l'un des A_i. Exemple, $A_1 = \{1\}$, $A_2 = \{2\}$. $\mathcal{P}(A_1) = \{\varnothing, \{1\}\}$, $\mathcal{P}(A_2) = \{\varnothing, \{2\}\}$ donc $\bigcup_{i \in I} \mathcal{P}(A_i) = \{\varnothing, \{1\}, \{2\}\}$.

Mais $A_1 \cup A_2 = \{1, 2\}$, donc $\mathcal{P}(\bigcup_{i \in I} A_i) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\} \neq \bigcup_{i \in I} \mathcal{P}(A_i)$

Sol.7) a) Prendre par exemple A =]–∞, 0] ∪ [1, +∞[, dont l'image par f est [0, +∞[= B. On a alors B^c =]–∞, 0[dont l'image par g est]0, 1[
b) Prendre A =]–∞, –1[∪]1, +∞[dont l'image par f est B =]1, +∞[. On a alors B^c =]–∞, 1] dont l'image par g est [–1, 1].

Sol.8) $f^{-1}(S) \subset U$ donc $\complement_E U \subset \complement_E f^{-1}(S) = f^{-1}(\complement_F S)$ donc $f(\complement_E U) \subset f(f^{-1}(\complement_F S)) \subset \complement_F S$ donc $S \subset \complement_F f(\complement_E U) = V$
Donc $f^{-1}(S) \subset f^{-1}(V)$ or $f^{-1}(V) \subset f^{-1}(\complement_F f(\complement_E U)) = \complement_E(f^{-1}(f(\complement_E U))) \subset U$ car $f^{-1}(f(\complement_E U)) \supset \complement_E U$.

Sol.9) (ii) ⇒ (i) est laissé au lecteur. Montrons que (i) ⇒ (ii).
La relation étant réflexive, en prenant $y = x$ dans la propriété de circularité, on obtient $x \mathcal{R} z \Rightarrow z \mathcal{R} x$. Donc la relation est symétrique.
Etant symétrique, la propriété de circularité donne alors :

$$\forall x, \forall y, \forall z, x \mathcal{R} y \text{ et } y \mathcal{R} z \Rightarrow z \mathcal{R} x \Rightarrow x \mathcal{R} z$$

donc la relation est transitive.

Sol.10) Le fait que la relation est d'équivalence est laissé au lecteur. Montrons l'équivalence :
(⇒) Soit $x \in f^{-1}(f(S))$. Alors $f(x) \in f(S)$, donc $\exists\, y \in S$, $f(x) = f(y)$. Mais alors $x \mathcal{R} y$ donc $C(x) = C(y)$. Comme $y \in S$, on a d'après l'hypothèse $C(y) \subset S$, donc $C(x) \subset S$, et comme $x \in C(x)$, $x \in S$. On a montré que $f^{-1}(f(S)) \subset S$. L'inclusion inverse $S \subset f^{-1}(f(S))$ est vraie pour toute partie et toute fonction sans hypothèse particulière.
(⇐) Soit $x \in S$ et $y \in C(x)$. Il s'agit de montrer que $y \in S$. Or $y \in C(x) \Rightarrow f(x) = f(y) \Rightarrow f(y) \in f(S) \Rightarrow y \in f^{-1}(f(S)) = S$ donc $y \in S$.

Sol.11) Oui avec le "et", pas nécessairement avec le "ou".
Par exemple, prenons dans $\mathbb{Z}$ les relations d'équivalence :

$x \mathcal{R} y \Leftrightarrow 2$ divise $x - y$ (relation de congruence modulo 2)

$x \mathcal{S} y \Leftrightarrow 3$ divise $x - y$ (relation de congruence modulo 3)

On a alors :

$x \mathcal{R} y$ et $x \mathcal{S} y \Leftrightarrow 2$ et 3 divisent $x - y \Leftrightarrow 6$ divise $x - y$

qui est bien une relation d'équivalence (congruence modulo 6).
Mais on a $2 \mathcal{R} 6$ (donc $2 \mathcal{R} 6$ ou $2 \mathcal{S} 6$)et $6 \mathcal{S} 9$ (donc $6 \mathcal{R} 9$ ou $6 \mathcal{S} 9$) mais on n'a ni $2 \mathcal{R} 9$ ni $2 \mathcal{S} 9$ donc on n'a pas $2 \mathcal{R} 9$ ou $2 \mathcal{S} 9$. $\mathcal{R}$ ou $\mathcal{S}$ n'est pas transitive.

Sol.12) a) La loi $*$ est associative. En effet :

$$(a * b) * c = (a + b + ab) * c = (a + b + ab) + c + (a + b + ab)c$$
$$= a + b + c + ab + ac + bc + abc$$

et on vérifiera que $a * (b * c)$ donne le même résultat. La loi est aussi commutative.
e est neutre si et seulement si, pour tout a, $a * e = e * a = a$ ce qui est équivalent à $e + ea = 0$. Il suffit de prendre $e = 0$.
a admet un symétrique a' si et seulement si $a * a' = a' * a = e = 0$, ce qui est équivalent à :

$a + a' + aa' = 0$

ou à $a'(1 + a) = -a$. On constate que $a = -1$ ne peut avoir de symétrique.

Prenons donc G = $\mathbb{R} \setminus \{-1\}$. Vérifions que $*$ reste une loi interne à G. Soit $a \neq -1$ et $b \neq -1$. Vérifions que $a * b \neq -1$. Dans le cas contraire, on aurait :

$a * b = -1$

$\Leftrightarrow$ $a + b + ab = -1$

$\Leftrightarrow$ $a + b + ab + 1 = 0$

$\Leftrightarrow$ $(a + 1)(b + 1) = 0$

ce qui est absurde puisque $a + 1 \neq 0$ et $b + 1 \neq 0$.

Dans G, la loi continue à être associative et le neutre est toujours 0. Le symétrique de a est :

$$a' = -\frac{a}{1 + a}$$

Il est bien élément de G puisque $a' = -1$ conduit à la relation absurde $a = 1 + a$.

c) Vérifier par récurrence que $a_1 * a_2 * ... * a_n = \prod_{i=1}^{n} (1 + a_i) - 1$

Sol.13) a) Soit f injective, et A et B tels que D(A) = D(B). Soit x élément de A. Alors :

$f(x) \in$ D(A) donc $f(x) \in$ D(B) donc $\exists\, y \in$ B, $f(x) = f(y)$

Par injectivité de f, on en déduit que $x = y$ et $x \in$ B. Donc A $\subset$ B. De même B $\subset$ A. Ainsi A = B et D est injective.

Réciproquement, soit D injective et x et y tels que $f(x) = f(y) = z$. Alors :

D($\{x\}$) = $\{z\}$ = D($\{y\}$) donc $\{x\} = \{y\}$ par injectivité de D donc $x = y$

et f est injective.

b) Soit f surjective, et B $\subset$ F. Soit A = $\{x \in$ E, $f(x) \in$ B$\}$. Alors D(A) = B et D est surjective. La surjectivité de f est utilisée pour l'inclusion B $\subset$ D(A).

Réciproquement, soit D surjective, et $y \in$ F. D étant surjective, il existe A tel que D(A) = $\{y\}$. Soit x élément de A. Alors $f(x) = y$, et f est surjective.

c) Supposons f surjective. On a donc D(E) = F. Soit A et B deux parties de F telles que R(A) = R(B). On a :

D(R(A)) = D(R(B)) or D(R(A)) = $\{y = f(x) \mid x \in$ R(A)$\}$ = $\{y \in$ A $\cap$ D(E)$\}$ = A $\cap$ D(E)

donc A $\cap$ D(E) = B $\cap$ D(E)

donc A $\cap$ F = B $\cap$ F

donc A = B et on a montré que R est injective.

Réciproquement, (par l'absurde), si f n'est pas surjective, il existe y qui ne possède pas d'antécédent. Soit A = $\{y\}$ et B = $\varnothing$. Alors A $\neq$ B et pourtant, R(A) = R(B) = $\varnothing$ donc R n'est pas injective.

d) Supposons f injective. Soit A une partie de E. Alors, montrons que A = R(B) avec B = D(A), ce qui prouvera que R est surjective. En effet :

$x \in$ R(B)

$\Leftrightarrow$ $f(x) \in$ B

$\Leftrightarrow$ $f(x) \in$ D(A)

$\Leftrightarrow$ $\exists\, x' \in$ A, $f(x) = f(x')$

or f est injective, donc, $x = x'$ avec x' dans A donc $x \in$ A. Et réciproquement, si $x \in$ A, on a $f(x) \in$ D(A) = B donc $x \in$ R(B).

Réciproquement, supposons R surjective. Soient x et y tels que $z = f(x) = f(y)$. Il existe deux ensembles X et Y tels que $\{x\} = R(X)$ et $\{y\} = R(Y)$, d'après la surjectivité de R. Cela implique que $X = \{f(x)\} = \{z\} = \{f(y)\} = Y$. Donc $\{x\} = R(X) = R(Y) = \{y\}$ et $x = y$.

Sol.14) a) Pour définir une relation réflexive, on choisit ou pas de mettre chaque couple (a, b) en relation pour $a \neq b$, et obligatoirement tous les couples (a, a). Comme il y a $n(n-1)$ couples (a, b) avec $a \neq b$ et deux choix possibles pour chaque couple, il y a $2^{n(n-1)}$ relations réflexives.
b) Pour définir une relation symétrique, pour tout a, on choisit ou pas de mettre (a, a) en relation, et pour tout $a \neq b$, on choisit ou pas de mettre (a, b) et (b, a) en relation. Il y a donc $n + \frac{n(n-1)}{2} = \frac{n(n+1)}{2}$ décisions à prendre, avec deux choix possibles par décision. Le nombre de relations symétriques est donc $2^{n(n+1)/2}$.

◆