Chapitre 1

Logique

Un scientifique étudie des objets, à propos desquels il énonce des faits (ou propositions). La logique manipule de façon formelle les propositions. Elle permet de modéliser les bases élémentaires du raisonnement.

Il est important de souligner que la logique est utile dans toute démarche scientifique. En revanche, dans le langage courant (dit langage vernaculaire), la logique ne s'applique pas toujours. Cela peut poser problème car les livres et les articles scientifiques (ainsi que les copies des étudiants !) sont rédigés en langage vernaculaire, et pas dans un langage formel. Il faut donc s'efforcer d'être parfaitement clair quand on rédige un texte scientifique.

Définition. En logique, une **proposition** (ou assertion) est une phrase à laquelle on peut attribuer une valeur de vérité (vrai ou faux).

On note 1 le vrai, et 0 le faux.

Exemple. « π est un nombre entier » est une assertion fausse. « 18 est divisible par 3 » est une assertion vraie.

Remarque. a) La phrase « cette assertion est fausse » n'est ni vraie, ni fausse. Ce n'est donc pas une assertion logique. Ce paradoxe est comparable à un individu affirmant « je mens » : il est logiquement impossible de savoir si cet individu dit ou non la vérité. C'est le paradoxe du menteur.

b) Mentionnons aussi le paradoxe de Berry : soit E l'ensemble des entiers naturels descriptibles par une phrase (en français) de quinze mots ou moins. Alors E est un ensemble fini (il n'y a qu'un nombre fini de phrases de quinze mots ou moins). Soit n_0 le plus petit entier n'appartenant pas à E. Alors n_0 est défini de façon unique par la phrase

« Le plus petit entier non descriptible par une phrase de moins de quinze mots ».

Or cette phrase comporte 14 mots, donc n_0 appartient à E, ce qui constitue un paradoxe. Celui-ci ne dévoile aucune incohérence des mathématiques, mais prouve tout simplement que n'importe quelle phrase ne peut être considérée comme une assertion mathématique.

1.1 Connecteurs logiques

Soient P et Q deux propositions. Les connecteurs logiques sont :

1) La conjonction : « et » (notée $\wedge$)
$P \wedge Q$ signifie que P est vraie et Q est vraie.

2) La disjonction : « ou » (notée $\vee$)
   $P \vee Q$ signifie que au moins l'une des deux propositions P ou Q est vraie.
3) La négation : « non » (notée $\neg$)
   $\neg P$ signifie que P est fausse.
4) L'implication (notée $\Rightarrow$)
   $P \Rightarrow Q$ signifie que si P est vraie, alors Q est vraie.
5) L'équivalence (notée $\Leftrightarrow$)
   $P \Leftrightarrow Q$ signifie que P et Q ont même valeur de vérité.

Remarque. a) Dans le langage courant, « ou » a en général un sens exclusif (fromage « ou » dessert). En mathématiques, le « ou » est toujours inclusif : si P et Q sont toutes les deux vraies, alors $P \vee Q$ est vraie.

b) Le seul cas où $P \Rightarrow Q$ est fausse se produit quand P est vraie et Q est fausse. En mathématiques, un résultat vrai n'implique jamais un résultat faux.

c) En revanche, si P est fausse, alors $P \Rightarrow Q$ est toujours vraie, quelle que soit la valeur de vérité de Q.

On raconte, qu'intrigué par ce résultat, un philosophe interpella ainsi Bertrand Russell : « Voulez-vous dire que si $2 = 1$, alors vous êtes le pape ? ». « Bien sûr », répondit Russell. « En effet, le pape et moi sont deux personnes distinctes et deux égale un, donc le pape et moi sont la même personne ».

Les connecteurs logiques permettent de combiner des assertions données $P, Q, R, \ldots$ pour construire de nouvelles assertions, dites **composées**, dont on peut déterminer la valeur de vérité à partir des valeurs de vérité de $P, Q, R, \ldots$.

1.2 Tables de vérité

Pour manipuler une assertion composée, on peut tout simplement parcourir la liste complète des valeurs de vérité possibles des assertions qui ont servi à la construire, qui n'est en général pas très longue. Ceci permet de remplacer un raisonnement par une simple vérification mécanique, exécutable par ordinateur.

Les tables ci-dessous, qui décrivent les connecteurs logiques, servent de point de départ à ces vérifications.

P	Q	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$	$P \Leftrightarrow Q$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

P	$\neg P$
0	1
1	0

Exemple. Si P et Q sont deux assertions, alors $P \Rightarrow Q$ est équivalente à $(\neg P) \vee Q$. En effet, on peut vérifier cela à l'aide d'une table de vérité :

P	Q	$P \Rightarrow Q$	$\neg P$	$(\neg P) \vee Q$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	1	0	1

Ainsi l'assertion $(P \Rightarrow Q) \Leftrightarrow ((\neg P) \vee Q)$ est toujours vraie, quelles que soient les valeurs de vérité rattachées aux assertions P et Q. On qualifie un tel énoncé de **tautologie**.

1.3 Règles logiques

Il existe en logique un certain nombre de règles qui établissent un calcul des propositions, semblable au calcul algébrique. Après application de l'une de ces règles sur une assertion, on obtient une assertion équivalente, c'est-à-dire ayant la même valeur de vérité.

Propriété. Soient P, Q et R trois assertions. Alors :

1. $(\neg(\neg P)) \Leftrightarrow P$
2. $(P \wedge P) \Leftrightarrow P$ et $(P \vee P) \Leftrightarrow P$
3. $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$
4. $\neg(P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q)$
5. $\neg(P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q)$
6. $\neg(P \Rightarrow Q) \Leftrightarrow (P \wedge \neg Q)$
7. $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$
8. $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$

Démonstration. Ces règles sont des tautologies, qui se vérifient avec une table de vérité. □

Remarque. a) Étant donnée une implication $P \Rightarrow Q$, on dit que :

- l'implication $Q \Rightarrow P$ est sa **réciproque** ;
- l'implication $\neg Q \Rightarrow \neg P$ est sa **contraposée**.

La règle 3. affirme qu'une implication est équivalente à sa contraposée. Par contre, il n'y a en général aucun lien logique entre une implication et sa réciproque : il se peut que l'une soit vraie et l'autre fausse.

b) Les règles 4. et 5. sont appelées lois de De Morgan en l'honneur du mathématicien britannique Augustus De Morgan (1806-1871).

c) La règle 6. est très importante à retenir, car elle permet d'écrire la négation d'une implication.

1.4 Quantificateurs

Définition. Un **prédicat** (ou formule à une variable) sur un ensemble E est un procédé qui associe à chaque élément de E une assertion.

Exemple. La phrase « x est pair » est un prédicat sur l'ensemble $\mathbb{N}$ des entiers naturels. Ce prédicat associe à l'entier 4 une assertion vraie, et à l'entier 5 une assertion fausse.

Pour transformer un prédicat en proposition, on utilise un quantificateur. Soient E un ensemble, et P un prédicat sur E.

(1) Quantificateur universel : $\forall x \in E, P(x)$ signifie que, pour tout élément x de E, l'assertion $P(x)$ est vraie.

(2) Quantificateur existentiel : $\exists x \in E, P(x)$ signifie qu'il existe au moins un élément x de E tel que $P(x)$ soit vraie.

Il convient également de signaler le quantificateur « d'existence et d'unicité », d'usage moins courant que les deux précédents.

(3) $\exists! x \in E, P(x)$ signifie qu'il existe un unique élément x de E tel que $P(x)$ soit vraie.

Remarque. Les variables quantifiées sont muettes, c'est-à-dire que $\forall x \in E, P(x)$ est la même assertion que $\forall \beta \in E, P(\beta)$.

Exemple. L'assertion (vraie) « Tout nombre réel strictement positif a une racine cubique réelle strictement positive » s'écrit :

$$\forall x \in]0, +\infty[, \exists y \in]0, +\infty[, y^3 = x$$

Attention à l'ordre des quantificateurs. En effet :

$$\exists y \in]0, +\infty[, \forall x \in]0, +\infty[, y^3 = x$$

est une assertion tout à fait différente de la précédente (et fausse).

Remarque. a) Si E est vide, alors $\forall x \in E, P(x)$ est vraie, et $\exists x \in E, P(x)$ est fausse.

b) Si $E = \{x_1, \ldots, x_n\}$ est un ensemble fini, alors $\forall x \in E, P(x)$ est équivalente à $P(x_1) \wedge \cdots \wedge P(x_n)$. De même, $\exists x \in E, P(x)$ est équivalente à $P(x_1) \vee \cdots \vee P(x_n)$.

c) Une assertion de la forme $\exists x \in E, P(x)$ peut être vraie sans qu'on ait aucun moyen de construire effectivement un élément x de E tel que $P(x)$ soit vraie. Par exemple, l'assertion « il existe des banquiers honnêtes » ne constitue pas une information très substantielle, car elle ne permet pas, à elle seule, de fournir un exemple.

1.5 Négation et quantificateurs

Propriété. Soient E un ensemble, et P un prédicat sur E. Alors :

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

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

Exemple. L'assertion $\neg(\exists x \in \mathbb{R}, x^2 = -1)$ peut se réécrire $(\forall x \in \mathbb{R}, x^2 \neq -1)$.

Le quantificateur universel pouvant être vu comme une généralisation de la conjonction et le quantificateur existentiel pouvant être vu comme une généralisation de la disjonction, ces règles de négation des quantificateurs généralisent les lois de De Morgan.

1.6 Démonstrations

En mathématiques, démontrer un résultat, c'est se convaincre de sa validité par application des règles logiques, en s'appuyant sur les axiomes de la théorie considérée ainsi que sur les théorèmes déjà existants.

1.6.1 Démonstration directe

L'énoncé d'un théorème est souvent de la forme $P \Rightarrow Q$ (des hypothèses impliquent une conclusion). Une démonstration directe de cette implication est une suite finie $P_1, \ldots, P_n$ de propositions telles que :

(1) $P_1 \Leftrightarrow P$ et $P_n \Leftrightarrow Q$

(2) Pour tout $i \in \{1, \ldots, n\}$, $P_i \Rightarrow P_{i+1}$.

Il est clair que la donnée d'une telle suite d'assertions constitue bien une démonstration de l'énoncé de départ.

1.6.2 Raisonnement par l'absurde

On souhaite démontrer une certaine proposition P. Pour cela on suppose que $\neg P$ est vraie, puis on en déduit, par le raisonnement, un résultat faux (souvent sous forme de contradiction). Ceci montre que l'hypothèse de départ est fausse, donc que P est vraie.

Exemple (Euclide)**.** Il existe une infinité de nombres premiers.

Démonstration. On suppose connu que tout entier strictement supérieur à 1 possède au moins un diviseur premier. Supposons (par l'absurde) que l'ensemble des nombres premiers soit fini, disons égal à $\{p_1, \ldots, p_n\}$. Considérons alors l'entier :

$$m = (p_1 \times \cdots \times p_n) + 1$$

Alors m est strictement supérieur à 1, donc admet au moins un diviseur premier p. D'autre part, m n'est divisible par aucun des p_i. Donc p n'appartient pas à l'ensemble $\{p_1, \ldots, p_n\}$, contradiction.

Exemple. Il n'existe pas de solution réelle au système d'équations ($y = x^2 + 1$ et $x + y = 0$).

Démonstration. Supposons qu'il existe un couple (x, y) de réels qui soit solution du système. Alors, en reportant, on voit que x est solution de l'équation $x^2 + x + 1 = 0$. Donc cette équation a un discriminant positif, c'est-à-dire que l'on a : $-3 \geq 0$, ce qui est faux. Cela montre que le système n'a pas de solution.

1.6.3 Démonstration par disjonction des cas

Soient E un ensemble, et P un prédicat sur E. On veut démontrer que $\forall x \in E, P(x)$ est vraie. Une démonstration par disjonction des cas consiste à trouver des sous-ensembles $E_1, \ldots, E_n$ de E tels que :

(1) $E = E_1 \cup \cdots \cup E_n$.

(2) pour tout $i \in \{1, \ldots, n\}$, l'assertion $\forall x \in E_i, P(x)$ est vraie,

Alors l'assertion $\forall x \in E, P(x)$ est vraie.

Dans la pratique, cette méthode consiste à montrer que $P(x)$ est vraie quand x vérifie certaines hypothèses supplémentaires, puis que chaque élément de E vérifie l'une au moins de ces hypothèses.

Exemple. Il existe deux irrationnels a et b tels que a^b soit rationnel.

Démonstration. On suppose connue l'irrationnalité de $\sqrt{2}$. Alors deux cas se présentent : ou bien $\sqrt{2}^{\sqrt{2}}$ est un nombre rationnel, auquel cas le résultat est démontré, ou bien $\sqrt{2}^{\sqrt{2}}$ est un nombre irrationnel. Dans ce cas, on peut écrire

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2$$

d'où le résultat en prenant $a = \sqrt{2}^{\sqrt{2}}$ et $b = \sqrt{2}$.

Exemple. Pour tout entier naturel n, $n^3 - n$ est pair.

Démonstration. On peut toujours écrire :

$$n^3 - n = n(n^2 - 1) = n(n + 1)(n - 1)$$

Si n est pair, alors le produit est pair (car n est facteur). Si n est impair, alors $n + 1$ est pair donc le produit est pair. Comme n est forcément pair ou impair et que la propriété est montrée dans les deux cas, alors elle est montrée pour tout n.

1.6.4 Le principe de récurrence

Récurrence simple

Soit P un prédicat sur $\mathbb{N}$, et soit n_0 un entier naturel. Supposons que l'on ait les propriétés suivantes :

(1) $P(n_0)$ est vraie.

(2) Pour tout $n \geq n_0$, $P(n) \Rightarrow P(n+1)$.

Alors l'assertion $\forall n \geq n_0, P(n)$ est vraie.

Récurrence forte

Soit P un prédicat sur $\mathbb{N}$, et soit n_0 un entier naturel. Supposons que l'on ait les propriétés suivantes :

(1) $P(n_0)$ est vraie.

(2) Pour tout $n \geq n_0$,
$$(P(n_0) \wedge \cdots \wedge P(n-1) \wedge P(n)) \Rightarrow P(n+1)$$

Alors l'assertion $\forall n \geq n_0, P(n)$ est vraie.

Remarque. Une récurrence forte fonctionne exactement de la même façon qu'une récurrence, mais il faut faire attention à l'initialisation. Si par exemple on a besoin d'utiliser l'hypothèse au rang $n-1$ et au rang n pour montrer qu'elle est vraie au rang $n+1$, alors on devra vérifier au départ que $P(n_0)$ et $P(n_0+1)$ sont vraies.

Exemple. Soit (u_n) la suite définie par $u_0 = 1$, $u_1 = 1$ et $u_{n+1} = u_n + u_{n-1}$. Alors cette suite est à valeurs entières strictement positives.

Démonstration. Ici le prédicat qui nous intéresse est « $u_n > 0$ ». La propriété est vraie pour $n = 0$ et $n = 1$. Soit $n \geq 1$ un entier. On suppose que $P(m)$ est vraie pour tout m tel que $0 \leq m \leq n$. En particulier, $P(n-1)$ et $P(n)$ sont vraies. C'est-à-dire que u_{n-1} et u_n sont des entiers strictement positifs. Mais alors, en considérant la formule $u_{n+1} = u_n + u_{n-1}$, on voir que u_{n+1} est un entier strictement positif. Donc l'assertion $\forall n \in \mathbb{N}, u_n > 0$ est vraie.

Chapitre 2

Ensembles

L'objectif des mathématiques est d'explorer l'intuition que nous avons d'un certain nombre d'objets abstraits (comme les nombres ou les fonctions continues), ce qui nous permet d'en déduire de nouvelles propriétés de ces objets.

Il existe bien sûr une grande variété d'objets mathématiques, dont certains sont de nature ensembliste, et d'autres non. Cependant, il est agréable de constater que la théorie des ensembles fournit un cadre universel d'étude pour tous ces objets. C'est ainsi qu'on peut représenter les nombres entiers, rationnels, ou réels, par des ensembles.

2.1 Notion d'ensemble

Définition. (1) Un **ensemble** est une collection d'objets.

(2) Les objets appartenant à un ensemble donné sont appelés ses **éléments**.

Si E est un ensemble et si x est un objet mathématique, alors :

« $x \in E$ » signifie que x appartient à E.

« $x \notin E$ » signifie que x n'appartient pas à E.

Exemple. a) L'ensemble n'ayant aucun élément s'appelle l'ensemble vide, noté $\emptyset$.

b) Si x est un objet, on note $\{x\}$ l'ensemble dont le seul élément est x. On appelle un tel ensemble un singleton.

c) Plus généralement, si $x, y, \ldots$ est une liste finie d'objets, on note $\{x, y, \ldots\}$ l'ensemble de ces objets. On dit qu'un tel ensemble est **défini en extension**.

d) Quand on définit un ensemble en extension, l'ordre des objets et les redondances ne comptent pas : $\{0, 1\} = \{1, 0\} = \{1, 0, 1\}$.

Un ensemble est entièrement caractérisé par la collection des éléments qui lui appartiennent, ce qui se traduit par la propriété suivante, connue sous le nom d'extensionnalité :

Propriété (extensionnalité)**.** Deux ensembles sont égaux si et seulement s'ils ont les mêmes éléments.

2.2 Sous-ensembles

Définition. Soient A et B deux ensembles. On dit que A est inclus dans B, et on note $A \subseteq B$, si tout élément de A est élément de B.

On dit aussi que A est une partie de B, ou que A est un sous-ensemble de B.

Propriété (transitivité de l'inclusion)**.** Si $A \subseteq B$ et si $B \subseteq C$, alors $A \subseteq C$.

Propriété. Si E est un ensemble, et si P est un prédicat sur E, alors l'ensemble des éléments de E satisfaisant P est une partie de E, que l'on note $\{x \in E \mid P(x)\}$. On dit qu'un tel ensemble est **défini en compréhension**.

On peut souvent décrire un ensemble de plusieurs façons : par exemple, $\{2, 3, 5\}$ est l'ensemble des nombres premiers inférieurs à 6.

Définition. Si E est un ensemble, on note $\mathfrak{P}(E)$ l'ensemble des parties de E.

Notons que l'ensemble vide est toujours contenu dans E, c'est-à-dire : $\emptyset \in \mathfrak{P}(E)$.

Exemple.

$$\mathfrak{P}(\{0,1\}) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$$

2.3 Opérations sur les ensembles

Soient A et B deux parties d'un ensemble E. Les opérations ensemblistes sont :

1) L'intersection : $A \cap B$ est l'ensemble des éléments qui appartiennent à la fois à A et à B

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

2) La réunion : $A \cup B$ est l'ensemble des éléments qui appartiennent à A ou à B

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

3) Le complémentaire : $\complement_E A$ est l'ensemble des éléments de E qui n'appartiennent pas à A :

$$\complement_E A = \{x \in E \mid x \notin A\}$$

4) La différence : $A \backslash B$ est l'ensemble des éléments qui appartiennent à A mais n'appartiennent pas à B :

$$A \setminus B = \{x \in E \mid x \in A \text{ et } x \notin B\} = A \cap \complement_E B$$

On constate une analogie entre ces opérations et les connecteurs logiques. En poursuivant cette analogie, on peut dresser une liste de propriétés pour les opérations ensemblistes.

Propriété. Soient A, B et C trois parties de E. Alors :

1. $\complement_E(\complement_E A) = A$
2. $A \cap A = A$ et $A \cup A = A$
3. $A \subseteq B \Leftrightarrow \complement_E B \subseteq \complement_E A$
4. $\complement_E(A \cap B) = \complement_E A \cup \complement_E B$
5. $\complement_E(A \cup B) = \complement_E A \cap \complement_E B$
6. $A \nsubseteq B \Leftrightarrow A \cap \complement_E B \neq \emptyset$
7. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
8. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Remarque. L'analogie entre connecteurs logiques et opérations ensemblistes peut s'expliquer de plusieurs façons :

a) Il revient au même de se donner un prédicat (à équivalence près) sur E ou une partie de E. En effet, si P est un prédicat sur E on lui associe l'ensemble $\{x \in E \mid P(x)\}$, et inversement si A est une partie de E on lui associe le prédicat $x \in A$. Dans cette correspondance :

$$\wedge \text{ devient } \cap, \quad \vee \text{ devient } \cup, \quad \neg \text{ devient } \complement_E, \quad \Rightarrow \text{ devient } \subseteq$$

b) Dans le cas ensembliste comme dans le cas logique, les opérations que nous avons introduites définissent une algèbre de Boole.

2.4 Couples et produit d'ensembles

Soient E et F deux ensembles.

Définition. A partir de deux éléments $x \in E$ et $y \in F$, on construit le **couple** (x, y), qui satisfait la propriété fondamentale :

$$(x, y) = (a, b) \Leftrightarrow (x = a) \wedge (y = b)$$

pour tous x, a dans E et y, b dans F.

Définition. Le **produit** des ensembles E et F, noté $E \times F$, est l'ensemble des couples de la forme (x, y) avec $x \in E$ et $y \in F$.

Autrement dit :

$$E \times F = \{(x, y) \mid x \in E \text{ et } y \in F\}$$

Remarque. a) Le produit d'ensembles est parfois appelé produit cartésien, en l'honneur de René Descartes (1596-1650) qui fut le premier à identifier le plan euclidien avec $\mathbb{R} \times \mathbb{R}$.

b) Attention à l'ordre des facteurs : $E \times F$ n'est pas égal à $F \times E$ en général.

c) Si l'un des deux ensembles est vide, alors leur produit est vide.

Soit G un troisième ensemble. Étant donnés $x \in E$, $y \in F$ et $z \in G$, on peut construire le **triplet** (x, y, z) de façon analogue au couple. L'ensemble des triplets est noté $E \times F \times G$.

On identifie le couple $((x, y), z)$ avec le triplet (x, y, z). De même, on identifie $(x, (y, z))$ avec (x, y, z). Compte-tenu de ces identifications, on peut écrire :

$$(E \times F) \times G = E \times (F \times G) = E \times F \times G$$

Plus généralement, si $E_1, \ldots, E_n$ sont n ensembles, on note le produit $E_1 \times \cdots \times E_n$ sans parenthèses, et les éléments de ce produit sont appelés des n-uplets.

Si $n \geq 1$ est un entier, le produit de n copies de E est noté E^n. C'est l'ensemble des n-uplets d'éléments de E.

Exemple. a) $\mathbb{R}^2$ s'identifie au plan, $\mathbb{R}^3$ s'identifie à l'espace. Plus généralement, $\mathbb{R}^n$ s'appelle l'espace à n dimensions.

b) Si $A = \{\text{As}, \text{Roi}, \text{Dame}, \text{Valet}, 10, 9, 8, 7, 6, 5, 4, 3, 2\}$ et $B = \{\text{pique}, \text{cœur}, \text{carreau}, \text{trèfle}\}$, alors $A \times B$ s'identifie à un jeu classique de 52 cartes.

Chapitre 3

Applications

3.1 Notion d'application

Définition. Soient E et F deux ensembles. Une application f de E dans F (notée $f : E \to F$) est un procédé qui permet d'associer, à chaque élément x de E, un unique élément de F, que l'on note $f(x)$.

Vocabulaire

- E est **l'ensemble de départ** de f
- F est **l'ensemble d'arrivée** de f
- $f(x)$ est **l'image** de x par f
- Si y est un élément de F, un **antécédent** de y par f est un élément x de E tel que $f(x) = y$
- Le **graphe** de f est l'ensemble $G(f)$ défini par :

$$\begin{aligned} G(f) &= \{(a, b) \in E \times F \mid f(a) = b\} \\ &= \{(a, f(a)) \mid a \in E\}. \end{aligned}$$

Pour définir une application f, on utilise parfois la notation

$$\begin{aligned} f : E &\longrightarrow F \\ x &\longmapsto f(x) \end{aligned}$$

ce qui est pratique quand $f(x)$ est donné par une formule en la variable x.

Exemple. Soit E un ensemble.

a) Il existe une unique application $\emptyset \to E$. Il n'existe aucune application $E \to \emptyset$, à moins que E soit vide.

b) On appelle identité de E l'application

$$\begin{aligned} \mathrm{id}_E : E &\longrightarrow E \\ x &\longmapsto x \end{aligned}$$

c) Si A est une partie de E, on appelle injection canonique de A dans E l'application

$$\begin{aligned} i_A : A &\longrightarrow E \\ x &\longmapsto x \end{aligned}$$

d) Si F est un autre ensemble, les applications

$$\begin{aligned} \mathrm{pr}_1 : E \times F &\longrightarrow E \\ (x, y) &\longmapsto x \end{aligned} \qquad\qquad \begin{aligned} \mathrm{pr}_2 : E \times F &\longrightarrow F \\ (x, y) &\longmapsto y \end{aligned}$$

sont appelées respectivement première et deuxième projection.

Remarque. Attention, une application n'est pas toujours définie par une formule explicite. Par exemple, l'application $\mathbb{N}^* \to \mathbb{N}^*$ qui à un entier $n \geq 1$ associe le n-ième nombre premier.

Dans tous les cas, il est important de souligner que **la donnée de l'ensemble de départ et de l'ensemble d'arrivée font partie de la donnée d'une application**, ce qui se traduit par la propriété suivante :

Propriété. Deux applications sont égales si et seulement si elles ont même ensemble de départ, même ensemble d'arrivée, et même graphe.

L'ensemble des applications de E dans F est noté F^E. Cette notation correspond au point de vue suivant : une application $E \to F$ est une famille d'éléments de F indexée par E. Par exemple, la donnée d'une application $f : \{1, 2\} \to \mathbb{R}$ équivaut à la donnée du couple $(f(1), f(2))$, ce qui signifie que $\mathbb{R}^{\{1,2\}}$ s'identifie à $\mathbb{R}^2$.

3.2 Image directe, image réciproque

Soit $f : E \to F$ une application.

Image directe

Si A est une partie de E, on appelle image directe de A par f, et on note $f(A)$, le sous-ensemble de F défini par :

$$\begin{aligned} f(A) &= \{y \in F \mid \exists a \in A, y = f(a)\} \\ &= \{f(a) \mid a \in A\}. \end{aligned}$$

On appelle image de f, et on note $\operatorname{Im} f$, l'ensemble $f(E)$.

Image réciproque

Si B est une partie de F, on appelle image réciproque de B par f, et on note $f^{-1}(B)$, le sous-ensemble de E défini par :

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

Exemples et dessins

Remarque. a) La notation $f^{-1}(A)$ prête à confusion : on dirait que l'on a « inversé » l'application f, ce qui n'est pas du tout le cas.

b) Pour toute partie A de E, $A \subseteq f^{-1}(f(A))$.

c) Pour toute partie B de F, $f(f^{-1}(B)) \subseteq B$.

3.3 Composition des applications

Définition. Soient $f : E \to F$ et $g : F \to G$ deux applications. On définit l'application composée de f par g, que l'on note $g \circ f$, en posant

$$\begin{aligned} g \circ f : E &\longrightarrow G \\ x &\longmapsto g(f(x)) \end{aligned}$$

Remarque. a) Si $f : E \to F$ est une application, alors $f \circ \mathrm{id}_E = f$ et $\mathrm{id}_F \circ f = f$.

b) Dans notre définition, on ne peut composer f et g que si l'ensemble de départ de g est égal à l'ensemble d'arrivée de f. Dans la pratique, il y a bien d'autres situations dans lesquelles l'application $x \mapsto g(f(x))$ a un sens, à condition de modifier les ensembles de départ et d'arrivée de f [1]. Cependant l'ensemble de départ et l'ensemble d'arrivée sont des données importantes dans l'étude d'une application ; c'est pourquoi nous évitons ici d'aborder de telles situations.

Propriété. Si f, g et h sont trois applications composables, alors :

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

On dit que la loi de composition est **associative**.

Remarque. La loi de composition n'est pas commutative : même si $g \circ f$ et $f \circ g$ ont tous les deux un sens, il est en général faux que $g \circ f = f \circ g$. Par exemple, soient

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto x^2 \end{aligned} \qquad\qquad \begin{aligned} g : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto x + 1 \end{aligned}$$

Alors :

$$\begin{aligned} g \circ f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto x^2 + 1 \end{aligned} \qquad\qquad \begin{aligned} f \circ g : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto (x+1)^2 \end{aligned}$$

3.4 Restriction, prolongement

Restriction

Soit $f : E \to F$ une application, et soit A une partie de E. La restriction de f à A, notée $f_{|A}$, est l'application de A dans F qui à tout élément x de A associe l'élément $f(x)$ de F.

Remarque. a) La restriction de f à A est l'application qui prend les mêmes valeurs que f, mais avec A comme ensemble de départ au lieu de E.

b) On observe que $f_{|A}$ est la composée de f et de l'injection canonique $i_A : A \to E$, autrement dit $f_{|A} = f \circ i_A$.

c) Le graphe de $f_{|A}$ se déduit du graphe de f par la formule :

$$G(f_{|A}) = G(f) \cap (A \times F)$$

1. Par exemple, si $f(E)$ est contenu dans F, alors $x \mapsto g(f(x))$ est une application de F dans G. Plus généralement, on peut choisir une partie A de E telle que $f(A)$ soit contenu dans F, et alors $x \mapsto g(f(x))$ est une application de A dans G.

Corestriction

La corestriction est l'opération analogue sur une partie B de l'ensemble d'arrivée F, mais si on veut que celle-ci reste une application, il faut que B contienne $f(E)$.

On obtient alors une application qui a même ensemble de départ et même graphe, mais pas même ensemble d'arrivée.

Prolongement

Soient deux applications $f : E \to F$ et $g : A \to B$. On dit que f est un prolongement de g si A est une partie de E, B est une partie de F, et $G(g) \subseteq G(f)$.

3.5 Injections, surjections et bijections

Soit $f : E \to F$ une application. On est amené naturellement à se poser deux questions : la donnée de $f(x)$ permet-elle de retrouver x ? Un élément de F est-il l'image par f d'un élément de E ? Plusieurs cas peuvent se présenter.

Définition. (1) On dit que f est injective si tout élément de F admet au plus un antécédent par f, c'est-à-dire :

$$\forall (x, x') \in E^2, f(x) = f(x') \Longrightarrow x = x'$$

ce qui s'écrit aussi :

$$\forall (x, x') \in E^2, x \neq x' \Longrightarrow f(x) \neq f(x')$$

(2) On dit que f est surjective si tout élément de F admet au moins un antécédent par f, c'est-à-dire :

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

(3) On dit que f est bijective si elle est à la fois injective et surjective.

Exemple.

$\mathbb{R} \longrightarrow \mathbb{R}$ $x \longmapsto x^2$	n'est ni injective, ni surjective
$\mathbb{R} \longrightarrow \mathbb{R}$ $x \longmapsto e^x$	est injective, non surjective
$\mathbb{R} \longrightarrow \mathbb{R}$ $x \longmapsto x(x-1)(x+1)$	est surjective, non injective
$\mathbb{R} \longrightarrow \mathbb{R}$ $x \longmapsto x^3$	est bijective

Remarque. a) Une application injective est un processus qui conserve l'information : la donnée de $f(x)$ permet de retrouver x.

b) Une application $f : E \to F$ est surjective si et seulement si $f(E) = F$.

c) Si on modifie l'ensemble de départ ou d'arrivée, on modifie les propriétés d'injectivité ou de surjectivité de l'application, comme on voit sur les exemples ci-dessus.

Pour exprimer l'injectivité d'une application $E \to F$ on utilise parfois le symbole $E \hookrightarrow F$, et pour la surjectivité le symbole $E \twoheadrightarrow F$.

Proposition. *(1) La composée de deux injections est une injection.*

(2) La composée de deux surjections est une surjection.

(3) La composée de deux bijections est une bijection.

Démonstration. La démonstration est laissée au lecteur. □

3.6 Réciproque d'une application bijective

Définition. Si $f : E \to F$ est bijective, on note

$$f^{-1} : F \to E$$

l'application qui à $y \in F$ associe l'unique $x \in E$ tel que $f(x) = y$. On l'appelle l'application réciproque de f.

Proposition. *Supposons que $f : E \to F$ soit bijective. Alors*

(1) Pour tout $x \in E$ et tout $y \in F$,

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

(2) $f \circ f^{-1} = \mathrm{id}_F$.

(3) $f^{-1} \circ f = \mathrm{id}_E$.

Démonstration. (1) C'est vrai par définition de f^{-1}. (2) Soit $y \in F$, alors $f^{-1}(y)$ est l'unique x tel que $f(x) = y$, donc :

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

(3) Soit $x \in E$, alors $f^{-1}(f(x))$ est l'unique antécédent de $f(x)$ par f, donc est égal à x. □

Remarque. Si $f : E \to F$ est bijective, et si B est une partie de F, alors l'image réciproque de B par f est égale à l'image directe de B par f^{-1}. La notation $f^{-1}(B)$ peut donc être utilisée sans ambiguïté.

Théorème. *Soient $f : E \to F$ et $g : F \to E$ deux applications telles que $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$. Alors f et g sont bijectives et réciproques l'une de l'autre.*

Démonstration. Par symétrie du problème, il suffit de montrer que f est bijective et que g est sa réciproque. Montrons que f est injective : soient x et x' dans E tels que $f(x) = f(x')$, alors $g(f(x)) = g(f(x'))$, donc $x = x'$ puisque $g \circ f = \mathrm{id}_E$. Montrons que f est surjective : soit $y \in F$, alors $f(g(y)) = y$, ce qui montre que $g(y)$ est un antécédent de y par l'application f. On a donc bien montré que f est bijective, et que g est sa réciproque. □

Corollaire. *Si $f : E \to F$ est bijective, alors $f^{-1} : F \to E$ est également bijective, et*

$$(f^{-1})^{-1} = f$$

Démonstration. En effet, on sait que $f^{-1} \circ f = \mathrm{id}_E$ et $f \circ f^{-1} = \mathrm{id}_F$, donc d'après le théorème précédent f^{-1} est bijective, de réciproque f. □

Chapitre 4

Relations d'équivalence

Dans tout le chapitre, E désigne un ensemble.

4.1 Notion de relation

Définition. Une relation sur l'ensemble E est un prédicat sur $E \times E$.

Autrement dit, une relation est une assertion qui dépend de deux variables prises dans E. Intuitivement, une relation sur E est un procédé qui permet de comparer deux éléments de l'ensemble E.

Pour exprimer que deux éléments x et y de E satisfont la relation $\mathcal{R}$, on notera $x\mathcal{R}y$ au lieu de $\mathcal{R}(x, y)$.

Exemple. a) Sur tout ensemble E, l'égalité est une relation.

b) Sur $\mathbb{R}$, « $x < y$ » est une relation.

c) Sur $\mathbb{N}$, « p divise q » est une relation.

4.2 Relations d'équivalence

Définition. Soit $\mathcal{R}$ une relation sur E. On dit que $\mathcal{R}$ est une relation d'équivalence si les propositions suivantes sont vérifiées :

(1) $\mathcal{R}$ est réflexive : $\forall x \in E, x\mathcal{R}x$

(2) $\mathcal{R}$ est symétrique : $\forall (x, y) \in E^2, x\mathcal{R}y \Rightarrow y\mathcal{R}x$

(3) $\mathcal{R}$ est transitive : $\forall (x, y, z) \in E^3, (x\mathcal{R}y \wedge y\mathcal{R}z) \Rightarrow x\mathcal{R}z$

Une relation d'équivalence a des propriétés semblables à la relation d'égalité. On peut voir une telle relation comme étant un « critère de ressemblance » entre deux objets.

Exemple. a) Sur l'ensemble des mots de la langue française, la relation « x et y commencent par la même lettre » est une relation d'équivalence.

b) Sur l'ensemble des êtres humains, la relation « x et y ont le même âge » est une relation d'équivalence.

c) Soit D une partie de $\mathbb{R}$, et soit $x_0 \in \overline{D}$. Sur l'ensemble des fonctions $D \to \mathbb{R}$, la relation « $f \sim_{x_0} g$ » est une relation d'équivalence.

4.3 Classes d'équivalence, ensemble quotient

Si une relation d'équivalence constitue un critère de ressemblance, alors il est naturel de regrouper en paquets les éléments qui se ressemblent.

Définition. Soit $\mathcal{R}$ une relation d'équivalence sur E, et soit $x \in E$. On appelle classe d'équivalence de x pour $\mathcal{R}$, et on note $\mathrm{Cl}_{\mathcal{R}}(x)$, l'ensemble $\{y \in E \mid x\mathcal{R}y\}$.

Quand il n'y aura pas de confusion possible, on notera $\mathrm{Cl}(x)$ au lieu de $\mathrm{Cl}_{\mathcal{R}}(x)$.

Lemme. *Soit $\mathcal{R}$ une relation d'équivalence sur E. Alors :*

$$\forall (x, y) \in E^2, \quad x\mathcal{R}y \Leftrightarrow \mathrm{Cl}_{\mathcal{R}}(x) = \mathrm{Cl}_{\mathcal{R}}(y).$$

Démonstration. Supposons que x et y sont deux éléments de E tels que $x\mathcal{R}y$. Soit $z \in \mathrm{Cl}(y)$. Alors $y\mathcal{R}z$, d'où par transitivité $x\mathcal{R}z$, donc $z \in \mathrm{Cl}(x)$. Ceci montre que $\mathrm{Cl}(y) \subseteq \mathrm{Cl}(x)$. D'autre part, $y\mathcal{R}x$ car $\mathcal{R}$ est symétrique. Le raisonnement ci-dessus montre alors que $\mathrm{Cl}(x) \subseteq \mathrm{Cl}(y)$, d'où $\mathrm{Cl}(x) = \mathrm{Cl}(y)$. Réciproquement, si $\mathrm{Cl}(x) = \mathrm{Cl}(y)$, alors y (qui, par réflexivité de $\mathcal{R}$, est dans $\mathrm{Cl}(y)$) appartient à $\mathrm{Cl}(x)$, donc $x\mathcal{R}y$. □

Définition. Une partition de E est la donnée d'un ensemble de parties non vides de E, deux à deux disjointes, dont la réunion est égale à E.

Théorème. *Soit $\mathcal{R}$ une relation d'équivalence sur E. Alors l'ensemble des classes d'équivalence d'éléments de E pour $\mathcal{R}$ forme une partition de E.*

Démonstration. Tout d'abord, pour tout $x \in E$, l'ensemble $\mathrm{Cl}(x)$ est non vide, car il contient x. Soient x et y dans E tels que $\mathrm{Cl}(x) \cap \mathrm{Cl}(y) \neq \emptyset$, alors $\mathrm{Cl}(x) = \mathrm{Cl}(y)$. En effet, supposons qu'il existe $z \in \mathrm{Cl}(x) \cap \mathrm{Cl}(y)$, alors $x\mathcal{R}z$ et $y\mathcal{R}z$ sont vrais. Par symétrie et transitivité, nous obtenons $x\mathcal{R}y$. Mézalor, d'après le lemme, $\mathrm{Cl}(x) = \mathrm{Cl}(y)$. Ceci prouve que les classes d'équivalence sont deux à deux disjointes. D'autre part, leur réunion est égale à E, puisque chaque élément de E appartient à sa propre classe. □

Exemple. La partition de l'ensemble des mots en classes d'équivalence pour la relation « x et y commencent par la même lettre » coïncide avec le découpage des dictionnaires.

Remarque. Il est clair que $x\mathcal{R}y \Leftrightarrow y \in \mathrm{Cl}_{\mathcal{R}}(x)$. Donc la donnée des classes d'équivalences pour $\mathcal{R}$ permet de retrouver $\mathcal{R}$. En fait, se donner une partition de E est la même chose que se donner une relation d'équivalence sur E.

Définition. Soit $\mathcal{R}$ une relation d'équivalence sur E.

(1) On appelle ensemble quotient de E par $\mathcal{R}$, et on note $E/\mathcal{R}$, l'ensemble des classes d'équivalence d'éléments de E pour $\mathcal{R}$.

(2) On appelle surjection canonique associée à $\mathcal{R}$ l'application

$$\begin{aligned} E &\longrightarrow E/\mathcal{R} \\ x &\longmapsto \mathrm{Cl}_{\mathcal{R}}(x) \end{aligned}$$

Comme son nom l'indique, la surjection canonique associée à $\mathcal{R}$ est... surjective !

Exemple. Le quotient de l'ensemble des mots par la relation « x et y commencent par la même lettre » s'identifie avec l'alphabet. La surjection canonique associée s'identifie alors à l'application qui à un mot associe la première lettre de ce mot.

4.4 Théorème de factorisation

Théorème. *Soit $f : E \to F$ une application.*

(1) *La relation $\mathcal{R}_f$ sur l'ensemble E définie par :*

$$x\mathcal{R}_f y \Leftrightarrow f(x) = f(y)$$

est une relation d'équivalence.

(2) *L'application*

$$\begin{aligned} \overline{f} : E/\mathcal{R}_f &\longrightarrow \operatorname{Im} f \\ \operatorname{Cl}(x) &\longmapsto f(x) \end{aligned}$$

est bien définie, et bijective.

Démonstration. Il est immédiat que $\mathcal{R}_f$ est une relation d'équivalence. Montrons que l'application $\overline{f}$ est bien définie. Soient x et y deux éléments tels que $\operatorname{Cl}(x) = \operatorname{Cl}(y)$. Alors $x\mathcal{R}_f y$ (d'après le lemme), donc $f(x) = f(y)$. La définition de $\overline{f}$ ne dépend donc pas du choix du représentant de la classe d'équivalence. En outre, $\overline{f}$ est surjective, car si $y \in \operatorname{Im} f$, alors $y \in \operatorname{Im} \overline{f}$. Enfin, $\overline{f}$ est injective, car si $\operatorname{Cl}(x)$ et $\operatorname{Cl}(y)$ sont deux éléments de $E/\mathcal{R}_f$ tels que $\overline{f}(\operatorname{Cl}(x)) = \overline{f}(\operatorname{Cl}(y))$, alors $f(x) = f(y)$, ce qui montre que $x\mathcal{R}y$, donc que $\operatorname{Cl}(x) = \operatorname{Cl}(y)$ d'après le lemme. □

Corollaire. *Soit $f : E \to F$ une application. Alors f se décompose de la façon suivante :*

$$E \to E/\mathcal{R}_f \to \operatorname{Im} f \to F$$

où la première flèche est la surjection canonique, la seconde est l'application $\overline{f}$, et la troisième est l'injection canonique.

Ainsi, toute application f est « canoniquement » la composée d'une injection, d'une bijection, et d'une surjection.

4.5 Congruences dans $\mathbb{Z}$

Définition. Soit $n > 0$ un entier naturel. Si a et b sont deux entiers relatifs, on dit que a est congru à b modulo n, et on note

$$a \equiv b \pmod{n}$$

si $a - b$ est divisible par n.

Proposition. *Soit $n > 0$ un entier naturel fixé. Alors la relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.*

Démonstration. Réflexivité : soit a un entier, alors $a \equiv a \pmod{n}$ car $a - a = 0$ est divisible par n. Symétrie : soient a et b tels que $a \equiv b \pmod{n}$, alors $a - b$ est divisible par n, donc $b - a$ est divisible par n, c'est-à-dire que $b \equiv a \pmod{n}$. Transitivité : soient a, b et c trois entiers tels que $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$. Alors $a - b$ et $b - c$ sont divisibles par n, donc leur somme $a - c$ est divisible par n, c'est-à-dire que $a \equiv c \pmod{n}$. □

Quelques notations : l'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n se note $\mathbb{Z}/n\mathbb{Z}$. Si a est un entier relatif, on note $\overline{a}$ la classe de a modulo n. On vérifie aisément à partir des définitions que :

$$\overline{a} = \{a + nk \mid k \in \mathbb{Z}\} = a + n\mathbb{Z}$$

On peut décrire explicitement $\mathbb{Z}/n\mathbb{Z}$ sous la forme :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

Remarque. On vérifie facilement que la congruence modulo n est compatible avec l'addition et la multiplication de $\mathbb{Z}$. On peut donc additionner, soustraire et multiplier les classes d'équivalence modulo n. Autrement dit, $\mathbb{Z}/n\mathbb{Z}$ est un anneau.

4.6 Congruences dans $\mathbb{R}$

Définition. Soit $\omega > 0$ un réel. Si a et b sont deux réels, on dit que a est congru à b modulo ω, et on note

$$a \equiv b \pmod{\omega}$$

si $a - b$ est de la forme ωk, avec $k \in \mathbb{Z}$.

Proposition. *Soit $\omega > 0$ un réel fixé. Alors la relation de congruence modulo ω est une relation d'équivalence sur $\mathbb{R}$.*

Démonstration. En exercice. □

L'ensemble quotient de $\mathbb{R}$ par la relation se note $\mathbb{R}/\omega\mathbb{Z}$. On vérifie que $\mathbb{R}/\omega\mathbb{Z}$ est en bijection avec l'intervalle $[0, \omega[$. Dans le cas particulier où $\omega = 2\pi$, l'ensemble $\mathbb{R}/2\pi\mathbb{Z}$ s'identifie au cercle trigonométrique.

Remarque. La congruence modulo ω est compatible avec l'addition de $\mathbb{R}$: on peut additionner et soustraire les classes d'équivalence modulo ω. Par contre, on ne peut pas les multiplier.

Chapitre 5

Combinatoire, dénombrements

5.1 Ensembles finis

Étant donné un entier $n \in \mathbb{N}$, rappelons que l'on note :

$$\{1, \dots, n\} = \{i \in \mathbb{N} \mid 1 \leq i \leq n\}.$$

Dans le cas particulier où $n = 0$, on constate que $\{1, \dots, n\} = \emptyset$. Intuitivement, il est clair que le nombre d'éléments de l'ensemble $\{1, \dots, n\}$ est égal à n.

Définition. Soit $n \in \mathbb{N}$ un entier. On dit qu'un ensemble E est fini à n éléments, ou fini de cardinal n, et l'on note $\mathrm{card}(E) = n$, s'il existe une application bijective $\{1, \dots, n\} \to E$.

Autrement dit, E est fini de cardinal n si l'on peut écrire E sous la forme

$$E = \{x_1, x_2, \dots, x_n\}$$

où les x_i sont deux à deux distincts.

Lemme. *Soient E et F deux ensembles finis. Alors* $\mathrm{card}(E) = \mathrm{card}(F)$ *si et seulement s'il existe une bijection entre E et F.*

Démonstration. Soient E et F deux ensembles finis, et soit $f : E \to F$ une bijection. Soit d'autre part $n = \mathrm{card}(E)$, et soit $\sigma : \{1, \dots, n\} \to E$ une application bijective. Alors la composée $f \circ \sigma : \{1, \dots, n\} \to F$ est bijective, donc $\mathrm{card}(F) = n$, ce qu'on voulait. Réciproquement, soient E et F deux ensembles finis ayant même cardinal n, alors on dispose de deux bijections $\sigma : \{1, \dots, n\} \to E$ et $\tau : \{1, \dots, n\} \to F$, d'où une bijection $\tau \circ \sigma^{-1} : E \to F$. □

5.2 Injections et surjections entre ensembles finis

Proposition. *Soit X un ensemble fini, et soit A une partie de X. Alors :*

(1) L'ensemble A est fini, et $\mathrm{card}(A) \leq \mathrm{card}(X)$ *;*

(2) Si $\mathrm{card}(A) = \mathrm{card}(X)$ *alors $A = X$.*

Démonstration. Se démontre par récurrence sur le cardinal de X. □

La propriété (2) ci-dessus est intuitive, mais elle est loin d'être triviale. En fait, elle est fausse si l'on considère un ensemble X infini (voir plus loin).

Proposition. *Soient X et Y deux ensembles finis. Alors :*

(1) Les ensembles $X \cup Y$ et $X \cap Y$ sont finis, et

$$\mathrm{card}(X \cup Y) = \mathrm{card}(X) + \mathrm{card}(Y) - \mathrm{card}(X \cap Y)$$

(2) L'ensemble $X \times Y$ est fini, et

$$\mathrm{card}(X \times Y) = \mathrm{card}(X) \cdot \mathrm{card}(Y)$$

Démonstration. Se montre par récurrence sur le cardinal de X (ou celui de Y). □

Avant de continuer, faisons l'observation suivante. Si $f : X \to Y$ est une application surjective, alors on peut choisir au hasard, pour tout $y \in Y$, un antécédent $g(y)$ de y par f. On obtient ainsi une application $g : Y \to X$ telle que $f \circ g = \mathrm{id}_Y$. Il est immédiat qu'une telle application g est injective ; on dit que g est une **section** de f.

Proposition. *Soit $f : X \to Y$ une application entre deux ensembles finis.*

(1) Si f est injective, alors $\mathrm{card}(X) \leq \mathrm{card}(Y)$ *;*

(2) Si f est surjective, alors $\mathrm{card}(X) \geq \mathrm{card}(Y)$*.*

Démonstration. (1) Si $f : X \to Y$ est injective, alors X est en bijection avec $\mathrm{Im}\, f$. Donc $\mathrm{card}(X) = \mathrm{card}(\mathrm{Im}\, f)$. Mais $\mathrm{Im}\, f$ est une partie de Y, donc, d'après ce qui précède $\mathrm{card}(\mathrm{Im}\, f) \leq \mathrm{card}(Y)$, d'où le résultat. (2) Si f est surjective, alors f admet une section $g : Y \to X$ qui est injective, et on applique le résultat (1). □

De la propriété (1) découle le « principe des tiroirs » : si $n+1$ chaussettes sont rangées dans n tiroirs, alors l'un des tiroirs contient au moins deux chaussettes (n étant ici un entier naturel non nul). En effet, nier ce résultat reviendrait à affirmer l'existence d'une application injective de l'ensemble des chaussettes (de cardinal $n+1$) dans l'ensemble des tiroirs (de cardinal n), contredisant ainsi (1).

Théorème. *Soit $f : X \to Y$ une application entre deux ensembles finis de même cardinal. Alors les propriétés suivantes sont équivalentes :*

(i) f est injective

(ii) f est surjective

(iii) f est bijective

Démonstration. $(i) \Rightarrow (ii)$ Supposons que l'application $f : X \to Y$ est injective, alors X est en bijection avec $\mathrm{Im}\, f$. Donc $\mathrm{card}(X) = \mathrm{card}(\mathrm{Im}\, f)$. Mais alors, X et Y ayant même cardinal, $\mathrm{Im}\, f$ est une partie de Y telle que $\mathrm{card}(\mathrm{Im}\, f) = \mathrm{card}(Y)$. Donc $Y = \mathrm{Im}\, f$, c'est-à-dire que f est surjective. $(ii) \Rightarrow (iii)$ Supposons que f est surjective, alors f admet une section $g : Y \to X$ telle que $f \circ g = \mathrm{id}_Y$. Sachant que g est injective et que $(i) \Rightarrow (ii)$, g est surjective, donc bijective. Par conséquent, l'application réciproque g^{-1} existe et on peut écrire :

$$f = f \circ g \circ g^{-1} = \mathrm{id}_Y \circ g^{-1} = g^{-1}$$

ce qui montre que f est bijective. $(iii) \Rightarrow (i)$ C'est une tautologie. □

Dans le cas particulier où $f : X \to X$ est une application d'un ensemble fini X dans lui-même, il revient au même d'affirmer l'injectivité, la surjectivité, ou la bijectivité de f. Dans ce cas, on dira que f est une permutation de X.

5.3 Applications entre ensembles finis

Proposition. *Soient X et Y deux ensembles finis. Alors l'ensemble Y^X des applications de X dans Y est fini, et*

$$\mathrm{card}(Y^X) = \mathrm{card}(Y)^{\mathrm{card}(X)}.$$

Remarque. a) Cet énoncé justifie *a posteriori* la notation Y^X.

b) Cet énoncé permet d'expliquer pourquoi $0^0 = 1$. En effet, 0^0 est le nombre d'application de l'ensemble vide dans lui-même.

Démonstration. Se montre par récurrence sur le cardinal de X. □

Comment compter le nombre de parties d'un ensemble donné ? Si X est un ensemble quelconque (fini ou infini), on dispose d'une application naturelle

$$\begin{aligned} \mathfrak{P}(X) &\longrightarrow \{0,1\}^X \\ A &\longmapsto \mathbf{1}_A \end{aligned}$$

qui à une partie A de X associe sa fonction caractéristique, notée $\mathbf{1}_A$. On vérifie facilement que cette application $A \mapsto \mathbf{1}_A$ est une bijection, dont la réciproque est l'application qui à une fonction $f : X \to \{0,1\}$ associe l'ensemble des $x \in X$ tels que $f(x) = 1$.

Corollaire. *Soit X un ensemble fini, alors :*

$$\mathrm{card}(\mathfrak{P}(X)) = 2^{\mathrm{card}(X)}.$$

Démonstration. L'ensemble $\mathfrak{P}(X)$ est en bijection avec $\{0,1\}^X$, et la proposition précédente permet de calculer le cardinal de $\{0,1\}^X$. □

5.4 Arrangements, combinaisons

Définition. Soit X un ensemble, et soit p un entier naturel.

(1) Un p-arrangement de X est un p-uplet $(x_1, \ldots, x_p)$ d'éléments de X tel que les x_i soient deux à deux distincts.

(2) Une p-combinaison de X est une partie à p éléments de X.

Remarque. La donnée d'un p-arrangement de X équivaut à la donnée d'une application injective de $\{1, \ldots, p\}$ dans X.

Définition. Soient n et p deux entiers naturels.

(1) On note A_n^p le nombre de p-arrangements d'un ensemble à n éléments.

(2) On note $\binom{n}{p}$ le nombre de p-combinaisons d'un ensemble à n éléments.

Remarque. a) Il découle de la définition de $\binom{n}{p}$ que :

$$2^n = \sum_{p=0}^{n} \binom{n}{p}.$$

En effet, pour compter le nombre de parties d'un ensemble à n éléments, on doit compter le nombre de parties à p éléments pour tout p compris entre 0 et n.

b) Si n et p sont deux entiers naturels tels que $p \leq n$, alors

$$\binom{n}{p} = \binom{n}{n-p}.$$

En effet, si X est un ensemble à n éléments, alors l'application $A \mapsto \complement_X A$ est une bijection de l'ensemble des parties à p éléments de X dans l'ensemble des parties à $n-p$ éléments de X.

c) Si n et p sont deux entiers naturels tels que $p \leq n$, alors

$$\binom{n+1}{p+1} = \binom{n}{p+1} + \binom{n}{p}.$$

En effet, soit X un ensemble à $n+1$ éléments, et soit x_0 un élément de X. Alors une partie à $p+1$ éléments de X est ou bien une partie de $X \setminus \{x_0\}$, ou bien une partie de X contenant x_0. Or, le nombre de parties à $p+1$ éléments de $X \setminus \{x_0\}$ est $\binom{n}{p+1}$, et le nombre de parties à $p+1$ éléments contenant x_0 est égal au nombre de parties à p éléments de $X \setminus \{x_0\}$, c'est-à-dire $\binom{n}{p}$. D'où le résultat.

Proposition. *Soient n et p deux entiers naturels.*

(i) Si $p > n$, alors $A_n^p = 0$.

(ii) Si $p \leq n$, alors $A_n^p = \dfrac{n!}{(n-p)!}$.

Démonstration. (i) Si $p > n$, alors il est impossible de choisir p éléments distincts dans un ensemble à n éléments, donc $A_n^p = 0$. (ii) Soit X un ensemble à n éléments. Pour choisir un p-arrangement $(x_1, \ldots, x_p)$ de X, il faut d'abord choisir x_1, pour lequel il y a n choix possibles, puis x_2 qui doit être différent de x_1, donc pour lequel il y a $n-1$ choix possibles, puis x_3 pour lequel il y a $n-2$ choix possibles, ainsi de suite jusqu'à x_p, pour lequel il reste $n-p+1$ choix possibles. Le nombre total de choix possibles pour $(x_1, \ldots, x_p)$ est donc :

$$n(n-1)(n-2)\ldots(n-p+1) = \frac{n!}{(n-p)!}$$

ce qu'on voulait. □

Remarque. a) On déduit de la formule précédente que le nombre d'applications bijectives d'un ensemble à n éléments dans lui-même — c'est-à-dire le nombre de permutations de n éléments — est égal à $n!$.

b) Le point a) explique pourquoi $0! = 1$. En effet, il existe une unique application de l'ensemble vide dans lui-même, qui est bijective.

Proposition. *Soient n et p deux entiers naturels.*

(i) Si $p > n$, alors $\binom{n}{p} = 0$.

(ii) Si $p \leq n$, alors $\binom{n}{p} = \dfrac{A_n^p}{p!} = \dfrac{n!}{p!(n-p)!}$.

Démonstration. (i) S'il existe une partie à p éléments dans un ensemble à n éléments, alors $p \leq n$. Donc $p > n$ entraîne $\binom{n}{p} = 0$. (ii) Soit X un ensemble à n éléments. Pour choisir un p-arrangement de X, on peut d'abord choisir une partie à p éléments de X (pour laquelle il y a, par définition, $\binom{n}{p}$ choix possibles), puis ordonner ces p éléments. Or il y a $p!$ façons d'ordonner p éléments. Donc

$$A_n^p = \binom{n}{p} \times p!$$

ce qu'on voulait. □