Université Bordeaux 1
Licence de Sciences, Technologies, Santé
Mathématiques, Informatique, Sciences de la Matière et Ingénierie
M1MI1002 Fondamentaux pour les Mathématiques et l'Informatique

Fondamentaux pour les Mathématiques et l'Informatique :

Résumés de cours

Table des matières

1 Rudiments de logique **5**
- 1.1 Opérations logiques . . . 5
- 1.2 Notion d'ensemble . . . 7
- 1.3 Quantificateurs . . . 7
- 1.4 Démonstration d'une implication . . . 7
- 1.5 Démonstration de la négation d'une implication . . . 8
- 1.6 Démonstration d'une équivalence . . . 8
- 1.7 Raisonnement par la contraposée . . . 9
- 1.8 Raisonnement par l'absurde . . . 9
- 1.9 Raisonnement par récurrence . . . 10

2 Théorie des ensembles **11**
- 2.1 Ensembles . . . 11
  - 2.1.1 Ensembles et parties d'un ensemble . . . 11
  - 2.1.2 Opérations sur les ensembles . . . 12
- 2.2 Applications . . . 13
  - 2.2.1 Définitions : . . . 13
  - 2.2.2 Image directe, image réciproque . . . 14
  - 2.2.3 Composition des applications et des fonctions . . . 15
  - 2.2.4 Applications injectives, surjectives, bijectives . . . 16
  - 2.2.5 Composition des applications injectives, surjectives, bijectives . . . 18
- 2.3 Relations binaires sur un ensemble . . . 19
  - 2.3.1 Relations d'ordre . . . 19
  - 2.3.2 Relations d'équivalence. . . . 20

3 Cardinaux et dénombrements **23**
- 3.1 Ensembles finis . . . 23
- 3.2 Dénombrement . . . 24
  - 3.2.1 Principes de base . . . 24
  - 3.2.2 k-listes . . . 24
  - 3.2.3 Arrangements . . . 25
  - 3.2.4 Combinaisons, coefficients binômiaux, formule du binôme . . . 25

Chapitre 1

Rudiments de logique

1.1 Opérations logiques

Une *proposition logique*, concernant divers objets mathématiques, est un énoncé qui doit être ou bien vrai (ce que l'on note V) ou bien faux (ce que l'on note F).

On construit avec ces propositions (ou "variables propositionnelles") des *formules propositionnelles* en utilisant les connecteurs logiques suivants

1. La négation "**non**", notée $\neg$
2. La disjonction logique "**ou**", notée $\vee$
3. La conjonction logique "**et**", notée $\wedge$
4. L'**implication**, notée $\Rightarrow$
5. L'**équivalence**, notée $\Leftrightarrow$

La *valeur de vérité* d'une formule propositionnelle, c'est-à-dire l'interprétation de cette formule une fois que l'on s'est fixé des valeurs de vérité de ses variables propositionnelles, est définie par sa *table de vérité*. Ainsi, pour les formules définies par les connecteurs logiques élémentaires, on a les tables suivantes :

p	$\neg p$
F	V
V	F

p	q	$p \vee q$
F	F	F
F	V	V
V	F	V
V	V	V

p	q	$p \wedge q$
F	F	F
F	V	F
V	F	F
V	V	V

p	q	$p \Rightarrow q$
F	F	V
F	V	V
V	F	F
V	V	V

p	q	$p \Leftrightarrow q$
F	F	V
F	V	F
V	F	F
V	V	V

Attention :

1. 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, $p \vee q$ est vraie.
2. Dire que "$p \Rightarrow q$ est vrai" ne signifie pas que l'hypothèse p est vraie mais seulement que *si l'hypothèse p est vraie, alors la conclusion q l'est aussi.* Noter en particulier que, si p est fausse, $p \Rightarrow q$ est vrai...
3. La formule $p \Rightarrow q$ peut s'exprimer à l'aide des symboles de conjonction et de disjonction par l'une ou l'autre des phrases suivantes :
   - $\neg p \vee q$
   - $\neg\,(p \wedge (\neg q))$.

Remarque importante : un abus courant, bien que totalement illégitime, consiste à confondre une *formule propositionnelle* et sa *valeur de vérité*. Ainsi, dans un texte mathématique, on écrira souvent (toujours !) "$p \Rightarrow q$" pour dire "$p \Rightarrow q$ est vraie". Avec cet abus de notation la formule "$p \Rightarrow q$" se dit aussi parfois "si p, alors q", ou bien "p implique q", ou bien "pour que p soit vraie, il faut que q soit vraie", ou encore

— "une **condition suffisante** pour q est p",
— "une **condition nécessaire** pour p est q".

Définition 1.1. On dit que deux formules propositionnelles F et G sont *équivalentes*, et on écrit $F \equiv G$, si elles ont même table de vérité.

Voici quelques exemples importants de formules équivalentes :

- $\neg(p \wedge q) \equiv (\neg p) \vee (\neg q)$.
- $\neg(p \vee q) \equiv (\neg p) \wedge (\neg q)$.
- $(p \wedge (q \vee r)) \equiv ((p \wedge q) \vee (p \wedge r))$.
- $(p \vee (q \wedge r)) \equiv ((p \vee q) \wedge (p \vee r))$.
- $(p \Leftrightarrow q) \equiv ((p \Rightarrow q) \wedge (q \Rightarrow p))$ **(équivalence et double implication).**
- $(p \Rightarrow q) \equiv ((\neg q) \Rightarrow (\neg p))$ **(principe de contraposition).**
- $(\neg(p \Rightarrow q)) \equiv (p \wedge (\neg q))$ **(négation d'une implication).**

Définition 1.2. Une **tautologie** est une formule propositionnelle qui ne prend que la valeur "vrai".

Proposition 1. Les formules suivantes sont des tautologies :

- $p \vee (\neg p)$ (**principe du tiers exclu**).
- $((r \Rightarrow s) \wedge (s \Rightarrow t)) \Rightarrow (r \Rightarrow t)$ (**principe de transitivité de l'implication**).

Remarque : dire que « $F \Leftrightarrow G$ » est une tautologie signifie exactement que F et G sont des formules équivalentes, au sens de la définition précédente (c'est-à-dire ont même table de vérité).

1.2 Notion d'ensemble

Définition 1.3. Un ensemble est une collection d'éléments, donnés dans un ordre indifférent. On note $x \in E$ pour indiquer que x est un élément de l'ensemble E.
Il existe par convention un ensemble ne contenant aucun élément, c'est l'**ensemble vide** noté $\emptyset$. Un ensemble n'ayant qu'un seul élément est un **singleton**.

1.3 Quantificateurs

Définition 1.4. Soit $p(x)$ une proposition dépendant d'une variable x qui appartient à un ensemble E ; on définit deux nouvelles formules, à l'aide des **quantificateurs** $\forall$ et $\exists$:

1. $\forall x \in E,\ p(x)$: "pour tout $x \in E$, on a $p(x)$"
2. $\exists x \in E,\ p(x)$: "il existe $x \in E$, tel que $p(x)$"

La première est vraie si la proposition $p(x)$ est vraie *pour tous* les éléments x de E. La seconde est vraie, s'*il existe (au moins) un* élément x de E pour lequel $p(x)$ est vraie.

Par convention, si E est vide, "$\forall x \in E, p(x)$" est vraie, et "$\exists x \in E, p(x)$" est fausse.

Remarques :

1. Les variables sont muettes : $\forall x,\ p(x)$ et $\forall y,\ p(y)$ désignent la même proposition.
2. La négation de $(\forall x \in E,\ p(x))$ est $(\exists x \in E,\ \neg(p(x)))$.
3. En général, $(\forall x \in E, \exists y \in E, p(x,y))$ et $(\exists y \in E, \forall x \in E, p(x,y))$ sont deux propositions différentes.
4. Pour montrer que "$\exists x \in E, p(x)$" est vraie, il suffit de trouver un x particulier dans l'ensemble E pour lequel $p(x)$ est vraie. Pour montrer que "$\forall x \in E, p(x)$" est vraie, un tel **exemple** ne suffit pas.

   Montrer que "$\forall x \in E, p(x)$" est faux revient à montrer que "$\exists x \in E, \neg p(x)$" est vraie, donc il suffit de trouver un **contre-exemple**, c'est-à-dire un x pour lequel $p(x)$ est faux.

1.4 Démonstration d'une implication

On veut montrer que l'assertion $p \Rightarrow q$ est vraie.

Principe de la démonstration : Pour démontrer que $p \Rightarrow q$ est vraie, on suppose que p est vraie, et par une chaîne d'implications, on montre que q est vraie.

Exemple 1.1. Soient n et p deux entiers. On dit que n est congru à r modulo p (et on écrit $n \equiv r[p]$) si le reste de la division euclidienne de n par p est r. Montrer que $n \equiv 1[p] \Rightarrow n^2 \equiv 1[p]$.

Supposons $n \equiv 1[p]$. Soit $q \in \mathbb{N}$ tel que $n = qp + 1$. Ceci implique $n^2 = (q^2p + 2q)p + 1$, donc $n^2 \equiv 1[p]$.

1.5 Démonstration de la négation d'une implication

Pour montrer que l'assertion $p \Rightarrow q$ est fausse. On utilise la tautologie $(\neg(p \Rightarrow q)) \Leftrightarrow (p \wedge (\neg q))$. Il faut donc démontrer qu'on peut réaliser p vraie et q fausse.

Exemple 1.2. Soient a, b, n des entiers distincts. Montrer que l'implication $\big($ a divise n et b divise n $\big) \Rightarrow \big($ ab divise n $\big)$ est fausse.

Il faut montrer qu'on peut réaliser $\big($ a divise n et b divise n $\big)$ et $\big($ ab ne divise pas n $\big)$. On prend $a = 6$, $b = 9$ et $n = 18$. On a bien 6 divise 18 et 9 divise 18 et 6×9 ne divise pas 54.

1.6 Démonstration d'une équivalence

Principe de la démonstration : Pour démontrer que $p \Leftrightarrow q$ est vraie, on démontre que l'implication $p \Rightarrow q$ est vraie, puis on démontre que la réciproque $q \Rightarrow p$ l'est également.

Exemple 1.3. Si $a, b \in \mathbb{Z}$, on note $a\mathbb{Z} := \{na;\ n \in \mathbb{Z}\}$. On dit que $b\mathbb{Z}$ est inclus dans $a\mathbb{Z}$ (et on note $b\mathbb{Z} \subset a\mathbb{Z}$) si tout élément de $b\mathbb{Z}$ appartient aussi à $a\mathbb{Z}$. Montrer que

$$(a \text{ divise } b) \Leftrightarrow (b\mathbb{Z} \subset a\mathbb{Z}).$$

Démonstration de $(a$ divise $b) \Rightarrow (b\mathbb{Z} \subset a\mathbb{Z})$. Soit $m \in b\mathbb{Z}$. On veut montrer que $m \in a\mathbb{Z}$. Puisque $m \in b\mathbb{Z}$, il existe $n \in \mathbb{Z}$ tel que $m = nb$. Par hypothèse, a divise b. Il existe donc $p \in \mathbb{Z}$ tel que $b = pa$. Par conséquent, $m = nb = npa \in a\mathbb{Z}$ car np est entier.

Démonstration de la réciproque. On suppose $b\mathbb{Z} \subset a\mathbb{Z}$. En particulier, $b \in a\mathbb{Z}$. Il existe donc $p \in \mathbb{Z}$ tel que $b = pa$, ce qui signifie que a divise b.

On peut, dans certains cas, raisonner directement par équivalence.

Exemple 1.4. Soient a, b, c trois complexes tels que $a \neq 0$ et r un complexe tel que $r^2 = b^2 - 4ac$. Montrer que

$$az^2 + bz + c = 0 \quad \Leftrightarrow \quad \Big(\ z = \frac{-b + r}{2a} \quad \text{ou} \quad z = \frac{-b - r}{2a} \ \Big)$$

Démonstration :

$$\begin{aligned}
az^2 + bz + c = 0 \quad &\Leftrightarrow \quad z^2 + \frac{b}{a}z + \frac{c}{a} = 0 \\
&\Leftrightarrow \quad (z + \frac{b}{2a})^2 - \big(\frac{b^2 - 4ac}{4a^2}\big) = 0 \\
&\Leftrightarrow \quad (z + \frac{b}{2a})^2 - \big(\frac{r^2}{4a^2}\big) = 0 \\
&\Leftrightarrow \quad (z + \frac{b}{2a} - \frac{r}{2a})(z + \frac{b}{2a} - \frac{r}{2a}) = 0 \\
&\Leftrightarrow \quad z = \frac{-b + r}{2a} \quad \text{ou} \quad z = \frac{-b - r}{2a}
\end{aligned}$$

1.7 Raisonnement par la contraposée

Principe : Soient p et q deux propositions. Supposons que l'on veuille prouver que la proposition $p \Rightarrow q$ est vraie. Le principe de **contraposition** assure qu'il est équivalent de démontrer que la proposition $(\neg q) \Rightarrow (\neg p)$ est vraie, que l'on appelle la **contraposée** de $p \Rightarrow q$.

Attention : Ne pas confondre la contraposée de $p \Rightarrow q$, qui est $\neg q \Rightarrow \neg p$, avec sa **réciproque** "$q \Rightarrow p$". La contraposée est équivalente à la proposition de départ, la réciproque ne l'est en général pas.

Exemple 1.5. Soient x et y deux réels. Montrer que

$$x \neq y \quad \Rightarrow \quad (x+1)(y-1) \neq (x-1)(y+1).$$

Pour cela, montrons la contraposée de cette implication, qui est

$$(x+1)(y-1) = (x-1)(y+1) \quad \Rightarrow \quad x = y.$$

Supposons donc que $(x+1)(y-1) = (x-1)(y+1)$. En développant, on obtient $xy + y - x - 1 = xy - y + x - 1$. Après simplification, $x = y$.

1.8 Raisonnement par l'absurde

Le **raisonnement par l'absurde** est un principe de démonstration fondé sur le principe logique du **tiers exclu**. Ce principe affirme que

$$p \vee \neg(p)$$

est une tautologie.

Principe de la démonstration par l'absurde : Supposons que l'on veuille prouver que la proposition p est vraie. On suppose que $\neg(p)$ est vraie (ou que p est fausse), et l'on exhibe (en utilisant notre système d'axiomes et/ou les règles de déduction logique) une contradiction. On en conclut alors que l'hypothèse faite sur p est fausse, donc que p est vraie.

Exemple 1.6. On admet que tout entier peut se décomposer en produit de facteurs premiers. Montrons par l'absurde qu'il existe une infinité de nombres premiers. Supposons que cette proposition est fausse, i.e. il existe un nombre fini de nombres premiers, disons $p_1, \ldots, p_n$. Alors l'entier $p := (p_1 \times \ldots \times p_n + 1)$ n'est divisible par aucun des entiers p_i. Mais ceci constitue une contradiction. La proposition initiale est donc valide.

1.9 Raisonnement par récurrence

L'ensemble $\mathbb{N}$ des *entiers naturels* vérifie les trois propriétés caractéristiques suivantes :

(N1) Toute partie non vide de $\mathbb{N}$ possède un plus petit élément.

(N2) Toute partie non vide et *majorée* de $\mathbb{N}$ possède un plus grand élément.

(N3) L'ensemble $\mathbb{N}$ lui-même n'est pas majoré.

Ces propriétés sont à la bases du raisonnement par récurrence, dont le principe est rappelé dans le théorème suivant :

Théorème 2. Soit n_0 un entier, et $\mathcal{P}(n)$ une propriété de l'entier n, définie pour tout $n \geq n_0$. On fait les hypothèses suivantes :

(R1) La propriété $\mathcal{P}(n_0)$ est vraie.

(R2) $\forall n \geq n_0$, $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ est vraie.

Alors, la propriété $\mathcal{P}(n)$ est vraie pour tout $n \geq n_0$.

Preuve. Par l'absurde, on suppose que l'ensemble $E := \{m \geq n_0 \mid \mathcal{P}(m) \text{ fausse } \}$ est non vide. Il admet alors un plus petit élement n par (N1), qui est strictement plus grand que n_0 à cause de (R1). Par suite $n-1 \notin E$ et $\mathcal{P}(n-1)$ est vraie. Mais n est *strictement* supérieur à n_0 donc $n-1 \geq n_0$ et $\mathcal{P}(n)$ est donc vraie à cause de (R2), contradiction. □

Variante (*"Récurrence forte"*) : dans le théorème précédent, on peut remplacer (R2) par l'hypothèse (R3) suivante

(R3) Si $\mathcal{P}(k)$ est vraie pour tout $n_0 \leq k \leq n$, alors $\mathcal{P}(n+1)$ est vraie.

La conclusion est alors la même.

Chapitre 2

Théorie des ensembles

2.1 Ensembles

2.1.1 Ensembles et parties d'un ensemble

Définition 2.1. Si chaque élément d'un ensemble E est également élément de l'ensemble F on dit que E **est inclus** dans F, ou que E est **une partie** de F et on note $E \subset F$. On a donc
$E \subset F$ si et seulement si $\forall x \in E, x \in F$.
En particulier, toute ensemble est contenu dans lui-même ($E \subset E$) et l'ensemble vide est inclus dans tous les ensembles ($\emptyset \subset E$).

Remarque : la notation $E \subset F$ signifie que E est inclus dans F « au sens large », c'est-à-dire que E est *éventuellement* égal à F. Pour distinguer inclusion *au sens strict* et *au sens large*, on introduit parfois les notations $E \subseteq F$ (E est inclus dans ou égal à F) et $E \subsetneq F$ (E est inclus dans F strictement). Les notations $E \subset F$ et $E \subseteq F$ signifient donc *exactement la même chose*.

On peut décrire un ensemble **en extension** en donnant tous ses éléments entre accolades (par exemple : $E = \{1, 3, 7, 5, 2\}$).
On peut aussi décrire un sous-ensemble E d'un ensemble F **en compréhension**, c'est-à-dire en donnant une propriété qui caractérise ses éléments : $E = \{x \in F / \, p(x)\}$ est l'ensemble de tous les éléments de F pour lesquels la propriété $p(x)$ est vraie (par exemple :
$\{x \in \mathbb{Z} / \, x^2 = 4\} = \{-2, 2\}$).
Enfin, on définit souvent un ensemble en donnant une manière de construire chacun de ses éléments ; par exemple $\{n^2, n \in \mathbb{N}\} = \{m \in \mathbb{N} / \, \exists n \in \mathbb{N}, m = n^2\}$.
Attention un ensemble peut avoir pour élément des ensembles... Ainsi $\{\emptyset\}$ est un ensemble contenant un élément, l'ensemble vide. Ce n'est donc pas l'ensemble vide : $\{\emptyset\} \neq \emptyset$.

Proposition 3. Si A, B et C sont trois ensembles, on a l'implication
$(A \subset B)$ et $(B \subset C) \Rightarrow A \subset C$.

Définition 2.2. L'ensemble des parties d'un ensemble E, noté $\mathcal{P}(E)$ est formé de tous les ensembles inclus dans E. En particulier, il contient toujours $\emptyset$ et E.

Exemple : $\mathcal{P}(\{0,1\}) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$.

2.1.2 Opérations sur les ensembles

Définition 2.3. Soient E et F deux ensembles. La **réunion** de E et F notée $E \cup F$ est formée des éléments qui appartiennent à E ou à F. On a donc
$x \in E \cup F \Leftrightarrow (x \in E \text{ ou } x \in F)$

Définition 2.4. Soient E et F deux ensembles. L'**intersection** de E et F notée $E \cap F$ est formée des éléments qui appartiennent à E et à F. On a donc
$x \in E \cap F \Leftrightarrow (x \in E \text{ et } x \in F)$
Si $E \cap F = \emptyset$ on dit que E et F sont **disjoints**.

Proposition 4. Si E, F, G sont trois ensembles, on a les égalités suivantes :

- Commutativité : $E \cup F = F \cup E$ et $E \cap F = F \cap E$
- Associativité : $(E \cup F) \cup G = E \cup (F \cup G)$ et $(E \cap F) \cap G = E \cap (F \cap G)$
- Distributivité 1 : $E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$
- Distributivité 2 : $E \cap (F \cup G) = (E \cap F) \cup (E \cap G)$.
- $E \cup \emptyset = E$ et $E \cap \emptyset = \emptyset$
- $E \cap E = E \cup E = E$

Définition 2.5. Soit E un ensemble et F une partie de E. Le **complémentaire** de F dans E noté $\complement_E F$ (ou parfois F^c) est l'ensemble des éléments de E qui n'appartiennent pas à F. On a donc $\complement_E F = \{x \in E / x \notin F\}$.
En particulier, $\complement_E F \cup F = E$ et $\complement_E F \cap F = \emptyset$.

Définition 2.6. Soient F et G deux parties d'un ensemble E. L'ensemble $F \backslash G$ est l'ensemble formé des éléments de E qui appartiennent à F et pas à G. On a donc
$F \backslash G = F \cap (\complement_E G)$.
En particulier, $E \backslash F = \complement_E F$, $E \backslash \emptyset = E$

Proposition 5. Soient E un ensemble et A et B deux parties de E. On a alors
$\complement_E \left(\complement_E A\right)$, $\complement_E(A \cap B) = \complement_E A \cup \complement_E B$, et $\complement_E(A \cup B) = \complement_E A \cap \complement_E B$.

Remarque : L'union, l'intersection et le complémentaire sont la traduction en terme d'appartenance à un ensemble des opérations logiques "et", "ou" et "non".

Définition 2.7. Une partition d'un ensemble E est la donnée d'une famille de parties de E $(F_i)_{i \in I}$ non vides, deux-à-deux disjointes, et telles que $\cup_{i \in I} F_i = E$.

Exemple 2.1. $\{0\}, \{1,3\}$ et $\{2\}$ forment une partition de $\{0,1,2,3\}$.

Définition 2.8. Soient E et F deux ensembles. Le produit cartésien de E et F noté $E \times F$ est l'ensemble des couples (x, y) tels que x est éléments de E et y est élément de F.

Exemple 2.2. $\{0,1\} \times \{0,1\} = \{(0,0),(0,1),(1,0),(1,1)\}$
$\{0,1\} \times \{2,3\} = \{(0,2),(0,3),(1,2),(1,3)\}$

Remarque : l'ordre dans un couple est important : $(0,1) \neq (1,0)$.

2.2 Applications

Dans toute cette section, E, F et G désigneront des ensembles.

2.2.1 Définitions :

Définition 2.9. On appelle **fonction** d'un ensemble E dans un ensemble F la donnée des ensembles E, F et d'une correspondance entre les éléments de E et ceux de F telle qu'à tout élément x de E corresponde au plus un élément y de F.

Définition 2.10. Désignons par f une fonction de E dans F.
- y, s'il existe, est appelé l'**image** de x par f, et est noté $f(x)$.
- x est appelé un **antécédent** de y par f.
- E est l'**ensemble de départ** de f.
- F est l'**ensemble d'arrivée** de f.
- On appelle **domaine de définition** de f l'ensemble des éléments de E qui ont une image par f. On note cet ensemble D_f, $Dom(f)$ ou $Dom\ f$.
- On appelle **graphe de** f l'ensemble $G_f = \big\{ (x, f(x));\ x \in Dom(f) \big\}$.

Définition 2.11. Une fonction f de E dans F dont le domaine de définition est E, s'appelle une **application** de E dans F. Tout élément $x \in E$ a donc une image par f.

On note : $f : \begin{array}{ccc} E & \to & F \\ x & \mapsto & f(x) \end{array}$

Remarques :

1. La correspondance qui définit une fonction mathématique **n'est pas nécessairement un algorithme de calcul** : par exemple, la fonction "racine carrée" de $\mathbb{R}$ vers $\mathbb{R}$.

2. Inversement, un algorithme de calcul est un moyen d'obtenir un résultat à partir de données, mais il ne définit pas une fonction mathématique : encore faut-il préciser les ensembles de départ et d'arrivée.
   On dit qu'une « fonction » d'un langage de programmation **implémente** la fonction mathématique $f : E \longrightarrow F$ si, pour toute valeur $x \in D_f$, elle retourne $f(x)$: par exemple, la fonction `doubler` définie en Python par

```
def doubler(x):
    return x + x
```

est une implémentation de la fonction $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ définie par $f(x) = 2x$. Mais `doubler(x)` peut retourner un résultat même si `x` n'est pas dans l'ensemble de départ de f : par exemple, `doubler(1.4)` retourne `1.8`.

3. On appelle identité de E, et on note Id_E, la fonction définie par :

$$\begin{array}{rccc} Id_E : & E & \to & E \\ & x & \mapsto & x \end{array}$$

4. Une fonction dont l'ensemble de départ E est un produit cartésien de n ensembles

$$E = E_1 \times E_2 \times \ldots \times E_n$$

est appelée une **fonction de n variables** (les implémentations sont alors des « fonctions » à n paramètres)

Définition 2.12. Soient une fonction f d'un ensemble E dans un ensemble F, et A une partie de E. On appelle **restriction** de f à A la fonction de A dans F, notée $f_{|A}$, qui à tout élément x de A fait correspondre, s'il existe, $f(x)$.

Remarque : Soit une fonction f d'un ensemble E dans un ensemble F. La restriction de f à D_f est une application de D_f dans F.

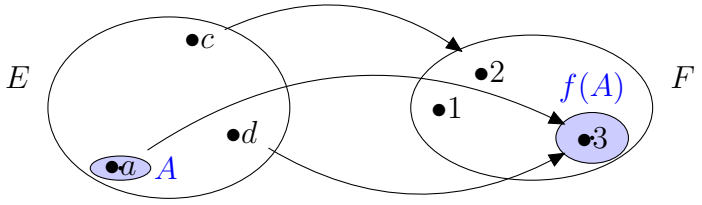
Par exemple : la restriction à $[0, +\infty[$ de la fonction "racine carrée" de $\mathbb{R}$ dans $\mathbb{R}$ est une application de $[0, +\infty[$ dans $\mathbb{R}$.

2.2.2 Image directe, image réciproque

Définition 2.13. Soit f une application de l'ensemble E dans l'ensemble F. Pour toute partie A de E, on appelle **image directe** de A et on note $f_\star(A)$, ou plus simplement $f(A)$, le sous-ensemble de F formé des images des éléments de A.
Autrement dit :

$$f(A) := \{f(a)\,;\, a \in A\}$$

Exemple :



Remarques :

— $f(A) = \{y \in F\,;\, \exists a \in A \text{ tel que } y = f(a)\}\,.$

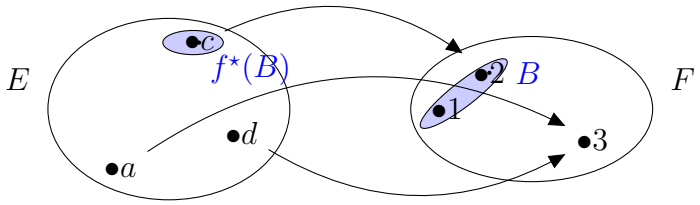
— $y \in f(A) \iff (\, y \in F \text{ et } \exists a \in A \text{ tel que } y = f(a)\,)$

Cas particulier : $A = E$
$f(E)$ est l'ensemble des éléments de F qui ont un antécédent par f. On l'appelle **image** de f, ou **ensemble des valeurs** de f. $f(E)$ se note aussi $Im(f)$ ou $Im\ f$.

Définition 2.14. Soit f une application de l'ensemble E dans l'ensemble F. Pour toute partie B de F, on appelle **image réciproque** de B et on note $f^{-1}(B)$ le sous-ensemble de E défini par

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

Exemple :



Exemple : Considérons l'application : $\mathbb{R} \to \mathbb{R}$ définie par $f(x) = x^2$. On a $f(1) = 1$ et $f(2) = 4$. Pour les images de parties, on a $f([1,2]) = [1,4]$, $f([-1,1]) = [0,1]$, $f\big(\{1,2\}\big) = \{1,4\}$ et $f\big(\{2\}\big) = \{4\}$. Pour les images réciproques de parties, on a $f^{-1}\big([1,4]\big) = [1,2] \cup [-2,1]$, $f^{-1}\big(\{1,4\}\big) = \{1,2,-1,-2\}$ et $f^{-1}\big(\{4\}\big) = \{2,-2\}$. On ne définit pas, pour l'instant $f^{-1}(4)$.

2.2.3 Composition des applications et des fonctions

Définition 2.15. Soient deux applications $f : A \to B$, et $g : C \to D$ vérifiant la condition

$$f(A) \subset C \tag{2.1}$$

On appelle **application composée** de g avec f, et on note $g \circ f$, l'application de E dans G définie par :

$$\begin{array}{rccc} g \circ f : & A & \to & D \\ & x & \mapsto & g(f(x)) \end{array}$$

Remarques :

— La condition (2.1), est automatiquement vérifiée si $B = C$, ce qui sera le plus souvent le cas dans les exemples étudiés.

— Pour définir la composition de deux *fonctions* g et f, on n'a pas besoin de condition du type (2.1), maisle domaine de définition de $g \circ f$ peut être éventuellement vide.

Propriétés de la composition :

— En général $g \circ f \neq f \circ g$
— $\forall x \in E,\ h((g \circ f)(x)) = (h \circ g)(f(x))$
Cette égalité permet de définir $h \circ g \circ f$:
$\forall x \in E,\ (h \circ g \circ f)(x) = h((g \circ f)(x))$

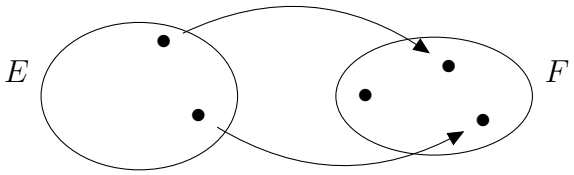
2.2.4 Applications injectives, surjectives, bijectives

Définition 2.16. Une application $f : E \to F$ est **injective** (on dit que c'est une injection) si tout élément y de F a au plus un antécédent dans E.

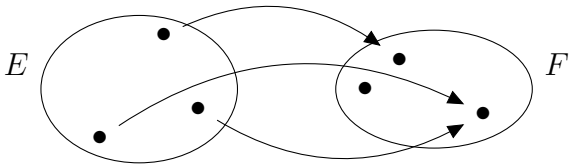
Remarque : Une application $f : E \to F$ est injective si et seulement si l'une des propositions suivantes est vraie :
— Pour tout $y \in F$ l'équation $f(x) = y$ admet au plus une solution x dans F.
— $\forall x \in E\,,\ \forall x' \in E\,,\ (f(x) = f(x')) \Longrightarrow (x = x')$
— ou encore par contraposée : $\forall x \in E\,,\ \forall x' \in E\,,\ (x \neq x') \Longrightarrow (f(x) \neq f(x'))$

Exemples :

Une application injective :



Une application non injective :



1. L'application $f : \mathbb{R} \longrightarrow \mathbb{R}$ définie par $f(x) = x^2$ n'est pas injective (des nombres opposés, 1 et -1 par exemple, ont même image par f).

2. L'application $g : \mathbb{N} \longrightarrow \mathbb{R}$ définie par $g(x) = \sqrt{x}$ est injective (en effet, si $y = g(x)$, nécessairement $x = y^2$).

3. Quand $E \subset F$, l'application définie par : $\begin{array}{ccc} E & \to & F \\ x & \mapsto & x \end{array}$
est appelée injection canonique de E dans F.

Remarque : La notion d'injection est la formalisation d'un concept qui apparaît constamment en informatique : la représentation symbolique des objets que l'on se propose d'étudier. Par exemple, un individu sera représenté par un numéro d'identité, un compte en banque par un numéro de compte, un fichier sur disque par un chemin d'accés : dans tous ces cas, la représentation est une injection d'un ensemble d'objets réels dans l'ensemble des chaines de caractères.

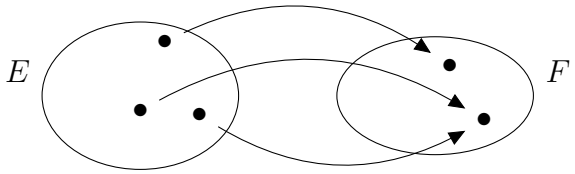
Définition 2.17. Une application $f : E \to F$ est **surjective** (on dit que c'est une surjection) si tout élément y de F a au moins un antécédent dans E.

Remarque : Une application $f : E \to F$ est surjective si et seulement si l'une des propositions suivantes est vraie :

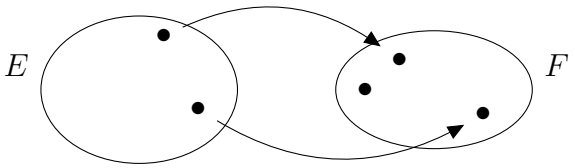
- $f(E) = F$
- Pour tout $y \in F$ l'équation $f(x) = y$ admet au moins une solution x dans E
- $\forall y \in F\,,\ \exists x \in E\,, y = f(x)$

Exemples :

Une application surjective :



Une application non surjective :



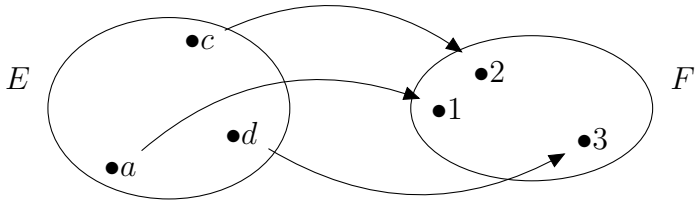
1. L'application $f : \mathbb{R} \longrightarrow \mathbb{R}$ définie par $f(x) = x + 1$ est surjective (tout réel y admet $y - 1$ comme antécédent).
2. L'application $g : \mathbb{N} \longrightarrow \mathbb{N}$ définie par $g(x) = x + 1$ n'est pas surjective (0 n'a pas d'antécédent par g).

Définition 2.18. Une application $f : E \to F$ est **bijective** (on dit que c'est une bijection) si elle est à la fois injective et surjective.

Remarque : Une application $f : E \to F$ est bijective si et seulement si l'une des propositions suivantes est vraie :

- Tout élément y de F a un et un seul antécédent dans E.
- Pour tout $y \in F$ l'équation $f(x) = y$ admet une solution unique x dans E.
- $\forall y \in F\,,\ \exists !\, x \in E\,, y = f(x)$

Exemples :

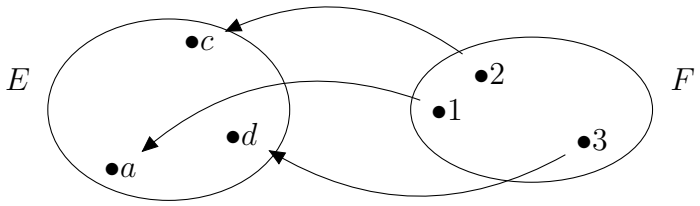


1. L'application $f : \mathbb{R} \longrightarrow \mathbb{R}$ définie par $f(x) = 2x + 5$ est bijective (tout réel y admet $\frac{1}{2}(y - 5)$ comme unique antécédent).
2. La fonction qui à un point d'un plan associe ses coordonnées dans un repère est une bijection de l'ensemble des points du plan sur $\mathbb{R}^2$ ($\mathbb{R}^3$ pour les points de l'espace).

Définition 2.19. Si l'application $f : E \to F$ est bijective on peut définir une application de F dans E qui à $y \in F$ associe son unique antécédent $x \in E$. On appelle cette application **l'application réciproque** de f et on la note f^{-1}.
Le graphe de f^{-1} est l'ensemble $G_{f^{-1}} = \{(y, f^{-1}(y);\ y \in F\} = \{(f(x), x);\ x \in E\}$.

Exemples :

l'application réciproque de la bijection précédente :



1. L'application réciproque de la bijection $f : \mathbb{R} \longrightarrow \mathbb{R}$ définie par $f(x) = 2x + 5$ est l'application $f^{-1} : \mathbb{R} \longrightarrow \mathbb{R}$ définie par $f^{-1}(y) = \frac{1}{2}(y - 5)$.

Proposition 6. Soit $f : E \to F$ bijective. On a alors :

- $y = f(x) \iff x = f^{-1}(y)$
- $f \circ f^{-1} = Id_F$ et $f^{-1} \circ f = Id_E$
- f^{-1} est bijective et on a : $\left(f^{-1}\right)^{-1} = f$.

Théorème 7. Soit $f : E \to F$ une application. Pour que f soit bijective, il faut et il suggit qu'il existe une application $g : F \to E$ telle que $f \circ g = Id_F$ et $g \circ f = Id_E$.

Remarque : l'application g du théorème précédent, quand elle existe, est unique, et elle est égale à la bijection réciproque f^{-1} de f.

2.2.5 Composition des applications injectives, surjectives, bijectives

Proposition 8. Soient deux applications $f : E \to F$, et $g : F \to G$.

- Si f et g sont injectives, alors $g \circ f$ est injective.
- Si f et g sont surjectives, alors $g \circ f$ est surjective.
- Si f et g sont bijectives, alors $g \circ f$ est bijective, et on a $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

2.3 Relations binaires sur un ensemble

De façon informelle, une relation binaire sur un ensemble E est une proposition qui lie entre eux certains éléments de cet ensemble. Plus proprement, une *relation binaire* $\mathcal{R}$ sur un ensemble E est définie par une partie $\mathcal{G}$ de $E \times E$. Si $(x, y) \in \mathcal{G}$ on dit que x est en relation avec y et on le note "$x\mathcal{R}y$".

On s'intéresse dans la suite à deux types de relations que l'on retrouve dans un grand nombre de situations, à savoir les *relations d'ordre* et les *relations d'équivalence*. Pour définir ces notions, on introduit un peu de vocabulaire

— une relation binaire $\mathcal{R}$ sur un ensemble E est *réflexive* si

$$\forall x \in E \qquad x\mathcal{R}x \tag{2.2}$$

— une relation binaire $\mathcal{R}$ sur un ensemble E est transitive si

$$\forall x, y, z \in E, \qquad (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z \tag{2.3}$$

— une relation binaire $\mathcal{R}$ sur un ensemble E est symétrique si

$$\forall x, y \in E, \qquad (x\mathcal{R}y) \Rightarrow (y\mathcal{R}x) \tag{2.4}$$

— une relation binaire $\mathcal{R}$ sur un ensemble E est antisymétrique si

$$\forall x, y \in E, \qquad (x\mathcal{R}y \text{ et } y\mathcal{R}x) \Rightarrow x = y \tag{2.5}$$

2.3.1 Relations d'ordre

Définition 2.20. Une relation binaire $\mathcal{R}$ sur un ensemble E qui est réflexive, transitive et antisymétrique est appelée relation d'ordre sur E.

La plupart des relations d'ordre sont notées $\leq$ ou $\preceq$ (à l'exception notable de l'inclusion et de la divisibilité). Un ensemble E muni d'une relation d'ordre $\preceq$ est dit *ordonné*, et on utilise la notation $(E, \preceq)$ pour s'y référer. Deux éléments x et y d'un ensemble E muni d'une relation d'ordre $\preceq$ sont dits *comparables* si $x \preceq y$ ou $y \preceq x$. Si tous les éléments de E sont deux à deux comparables la relation d'ordre est dite *totale*.

Exemples

1. la relation d'ordre usuelle sur $\mathbb{R}$ (ou sur $\mathbb{Q}$).
2. la relation de divisibilité dans $\mathbb{N}^*$ (ou dans $\mathbb{Z}^*$) : $m \mid n$ si il existe $q \in \mathbb{N}^*$ (resp. $\mathbb{Z}^*$) tel que $n = qm$.
3. la relation d'inclusion entre parties d'un ensemble E.

Les deux derniers exemples ne sont pas des ordres totaux.

On définit maintenant les notions (cruciales) de *majorant*, *minorant*, *borne supérieure* et *borne inférieure*.

Définition 2.21. Soient $(E, \preceq)$ un ensemble ordonné et A une partie de E.

1. Un élément m de E est un *minorant* de A si $\forall x \in A, m \preceq x$.
2. Un élément M de E est un *majorant* de A si $\forall x \in A, x \preceq M$.

Une partie admettant un majorant (resp. minorant) est dite majorée (resp. minorée). Une partie majorée et minorée est dite bornée.

Un élément d'une partie A de E est le *plus grand élément* (ou le *maximum*) de A s'il majore tous les éléments de A. De même, un élément d'une partie A de E est le *plus petit élément* (ou le *minimum*) de A s'il minore tous les éléments de A.

Définition 2.22. Soient $(E, \preceq)$ en ensemble ordonné et A une partie de E.

— Si l'ensemble des majorants de A admet un plus petit élément, cet élément est appelé *borne supérieure* et est noté $\sup A$.

— Si l'ensemble des minorants de A admet un plus grand élément, cet élément est appelé *borne inférieure* et est noté $\inf A$.

Remarque. Si A admet un maximum, alors il admet une borne supérieure et $\max A = \sup A$. De même, si A admet un minimum, alors il admet une borne inférieure et $\min A = \inf A$. Les réciproques sont fausses !

2.3.2 Relations d'équivalence.

Définition 2.23. Une relation d'équivalence $\mathcal{R}$ sur un ensemble E est une relation binaire qui est à la fois réflexive, symétrique et transitive.

Définition 2.24. La classe d'équivalence d'un élément x de E , notée $\mathrm{Cl}_{\mathcal{R}}(x)$, est l'ensemble des éléments de E qui sont en relation avec x.

$$\mathrm{Cl}_{\mathcal{R}}(x) = \{y \in E \mid x \mathcal{R} y\}.$$

Proposition 9.

1. $\forall x \in E, \quad x \in \mathrm{Cl}_{\mathcal{R}}(x)$.
2. $\mathrm{Cl}_{\mathcal{R}}(y) = \mathrm{Cl}_{\mathcal{R}}(x)$ ssi y appartient à $\mathrm{Cl}_{\mathcal{R}}(x)$.
3. Si $y \notin \mathrm{Cl}_{\mathcal{R}}(x)$ alors $\mathrm{Cl}_{\mathcal{R}}(y) \cap \mathrm{Cl}_{\mathcal{R}}(x) = \emptyset$.

On déduit de ce qui précède que l'ensemble des classes d'équivalence de E forme une partition de E. Inversement, toute partition d'un ensemble définit une relation d'équivalence.

Définition 2.25. L' ensemble quotient de E par la relation d'équivalence $\mathcal{R}$, noté $E/\mathcal{R}$, est l'ensemble des classes d'équivalence de E suivant $\mathcal{R}$:

$$E/\mathcal{R} = \{\mathrm{Cl}_{\mathcal{R}}(x) \mid x \in E\}$$

Exemples

1. Sur un ensemble de personnes, la relation *"être de même sexe"* est une relation d'équivalence (2 classes d'équivalence).
2. Sur un ensemble de mots, la relation *"commencer par la même lettre"* (26 classes).
3. L'égalité sur un ensemble quelconque est une relation d'équivalence.
4. Le parallélisme sur un ensemble de droites (dans un plan) est une relation d'équivalence.
5. Sur l'esnsmble des parties finies de $\mathbb{N}$, la relation "avoir même cardinal" est un relation d'équivalence (il y a une infinité de classes d'équivalence).
6. Si f est une application d'un ensemble E dans un ensemble F, alors la relation $\mathcal{R}$ définie par :
$$\forall\ (x,y) \in E^2, [x\mathcal{R}y] \Leftrightarrow [f(x) = f(y)]$$
est une relation d'équivalence sur E. Ainsi toute application induit une relation d'équivalence sur son ensemble de départ.

Un exemple fondamental : les congruences.

Définition 2.26. Soit n un entier naturel non nul. On dit que deux entiers relatifs a et b sont *congrus modulo* n ou encore que a est *congru* à b *modulo* n si n divise $a - b$. On notera $a \equiv b \bmod n$ ou $a \equiv b\ [n]$.

Théorème 10. Si $n \in \mathbb{N}^*$ et si a, b et c appartiennent à $\mathbb{Z}$ alors :

$$a \equiv a \bmod n$$
$$a \equiv b \bmod n \iff b \equiv a \bmod n$$
$$a \equiv b \bmod n \text{ et } b \equiv c \bmod n \Rightarrow a \equiv c \bmod n$$

Autrement dit la relation de congruence est une **relation d'équivalence** sur l'ensemble des entiers. La classe d'équivalence d'un entier k est l'ensemble $k+n\mathbb{Z} := \{k + nq, q \in \mathbb{Z}\}$

Définition 2.27. L'ensemble quotient pour la relation de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$.

Proposition 11. Chaque classe de congruence modulo n admet un unique représentant $r \in \{0, 1, \ldots, n-1\}$. En particulier, on a

$$\mathbb{Z}/n\mathbb{Z} = \{\mathbb{Z}, 1 + \mathbb{Z}, \ldots, (n-1) + \mathbb{Z}\}$$

Si le contexte ne prête pas à confusion, on pourra adopter la notation $\bar{k}$ pour la classe de k modulo n, auquel cas l'ensemble quotient peut s'écrire

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

Proposition 12. Soit n un entier naturel non nul. On note a, b, a' et b' quatre entiers relatifs. On a les propriétés suivantes : si $a \equiv b \bmod n$ et $a' \equiv b' \bmod n$ alors

$$a + a' \equiv b + b' \bmod n \qquad a - a' \equiv b - b' \bmod n \qquad aa' \equiv bb' \bmod n$$

Chapitre 3

Cardinaux et dénombrements

3.1 Ensembles finis

Définition 3.1. Un ensemble E est fini s'il est vide ou bien s'il existe un entier positif n et une bijection de E sur l'ensemble $\{1, 2, ..., n\}$.

Théorème 13. Si E est un ensemble fini non vide il existe un unique entier positif n pour lequel il existe une bijection de E sur $\{1, 2, ..., n\}$. Cet entier s'appelle le cardinal de E. Le cardinal de l'ensemble vide est 0. Le cardinal d'un ensemble fini E se note $\operatorname{Card} E$ ou $|E|$ et c'est le nombre d'éléments de l'ensemble.

Proposition 14. Toute partie A d'un ensemble fini E est finie et $\operatorname{Card} A \leq \operatorname{Card} E$

Proposition 15. Soient E et F des ensembles finis non vides. Il existe une bijection de E sur F si et seulement si $\operatorname{Card} E = \operatorname{Card} F$.

Proposition 16. Soient E et F deux ensembles finis non vides de cardinaux respectifs n et p et $f : E \to F$ une application.
• Si f est injective alors $n \leq p$.
• Si f est surjective alors $n \geq p$.

Proposition 17. Soient E et F deux ensembles finis non vides de même nombre d'éléments, et $f : E \to F$ une application. Alors :

$$f \text{ injective} \iff f \text{ surjective} \iff f \text{ bijective}$$

3.2 Dénombrement

3.2.1 Principes de base

Proposition 18. Soient E et F deux ensembles finis.

1. *"Principe de la somme".* Si E et F sont disjoints, alors

$$\mathrm{Card}(E \cup F) \;=\; \mathrm{Card}E \;+\; \mathrm{Card}F.$$

2. *"Principe du produit" :* $\mathrm{Card}(E \times F) \;=\; \mathrm{Card}E \;\times\; \mathrm{Card}F$

Plus généralement :

1. Si des ensembles $A_1, \ldots, A_n$ constituent une partition d'en ensemble fini E, on a

$$\mathrm{Card}\, E = \sum_{i=1}^{n} \mathrm{Card}\, A_i = \mathrm{Card}\, A_1 + \cdots + \mathrm{Card}\, A_n.$$

2. Le cardinal d'un produit cartésien $E_1 \times \cdots \times E_n$ d'ensembles finis est donné par

$$\mathrm{Card}\,(E_1 \times \cdots \times E_n) = \prod_{i=1}^{n} \mathrm{Card}\, E_i = \mathrm{Card}\, E_1 \times \cdots \times \mathrm{Card}\, E_n.$$

Corollaire 19.
1. Si A est une partie d'un ensemble fini E, on a $\mathrm{Card}\, \complement_E A = \mathrm{Card}\, E - \mathrm{Card}\, A$.
2. Si E et F sont deux ensembles finis, non nécessairement disjoints, on a

$$\mathrm{Card}(E \cup F) \;=\; \mathrm{Card}E \;+\; \mathrm{Card}F \;-\; \mathrm{Card}(E \cap F).$$

3.2.2 k-listes

Définition 3.2. Soit $k \in \mathbb{N}^*$, et E un ensemble. Une **k-liste (ou liste de longueur k)** de E est un k-uplet d'éléments de E, c'est-à-dire un élément de E^k.

Proposition 20.
1. Si E est un ensemble de cardinal n, le nombre de k-listes de E ($k \in \mathbb{N}^*$) est égal à n^k.
2. Le nombre d'applications d'un ensemble de cardinal k vers un ensemble de cardinal n est égal à n^k.

3.2.3 Arrangements

Définition 3.3. Soit $k \in \mathbb{N}^*$. Un **k-arrangement** est une liste de k éléments deux à deux distincts d'un ensemble donné. Si E est un ensemble de cardinal n, le nombre de k-arrangements que l'on peut former avec les éléments de E est noté A_n^k.

Par convention, on posera $A_n^0 = 1$ pour tout n, ce qui est cohérent avec les formules de la proposition suivante.

Proposition 21. Soient $0 \leq k \leq n$ deux entiers naturels.

1. On a $A_n^k = n(n-1)\dots(n-k+1) = \dfrac{n!}{(n-k)!}$.
2. Si E et F sont deux ensembles finis non vides de cardinaux respectifs k et n, le nombre d'injections de E dans F est égal à A_n^k.

Remarque : si $k > n$, on peut également convenir de poser $A_n^k = 0$, auquel cas la proposition212 reste vraie. Autrement dit :

Proposition 22. Si E et F sont des ensembles finis avec $\operatorname{Card} E > \operatorname{Card} F$, alors il n'existe pas d'injection de E dans F.

Cette proposition est une formulation sophistiquée d'un principe connu sous le nom de *principe des tiroirs* (ou *principe des tiroirs de Dirichlet*, ou bien encore *pigeonhole principle* en anglais) que l'on peut énoncer de la façon suivante :

> *Si n chaussettes occupent m tiroirs, et si $n > m$, alors au moins un tiroir doit contenir strictement plus d'une chaussette...*

3.2.4 Combinaisons, coefficients binômiaux, formule du binôme

Définition 3.4. Soit $k \in \mathbb{N}^*$. Une **combinaison de k éléments parmi** n est une partie à k éléments d'un ensemble de cardinal n. Le nombre de combinaison de k éléments parmi n est noté $\binom{n}{k}$ ou C_n^k.

Proposition 23.

1. Pour tout $n \in \mathbb{N}$ on a $\binom{n}{0} = \binom{n}{n} = 1$.
2. Pour tout $n \in \mathbb{N}$ et tout $k \in \mathbb{N}$ tel que $0 \leq k \leq n$, on a : $\binom{n}{k} = \binom{n}{n-k}$.
3. Si $0 < k < n$, on a : $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

La propriété 233 est à la base du "triangle de Pascal" dont les premières lignes sont représentées sur la figure 3.1

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & \\
1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1
\end{array}
$$

FIGURE 3.1 – Triangle de Pascal

Proposition 24. Si $0 \leq k \leq n$ sont deux entiers naturels, on a :

$$\binom{n}{k} = \frac{A_n^k}{k!} = \frac{n!}{k!(n-k)!}.$$

Proposition 25. (Formule du binôme) Soient x et y deux réels (ou deux complexes) et n un entier naturel. On a

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Corollaire 26. Si E est un ensemble fini de cardinal n, le nombre de parties de E est égal à 2^n.