



Mathématiques fondamentales

Préparation au CAPES de mathématiques

Jérôme LAURENS



Copyright © 2019 Jérôme LAURENS

Éditeur inconnu

www.inconnu.com

Sous licence Creative Commons Attribution-NonCommercial 3.0 Unported (la «Licence»). Vous ne pouvez pas utiliser ce fichier sauf en conformité avec la licence. Vous pouvez obtenir une copie de la licence sur <http://creativecommons.org/licenses/by-nc/3.0>. Sauf disposition contraire de la loi applicable ou accord écrit, les logiciels distribués sous licence sont distribués sur la base de «tel quel», sans garantie ou condition d'aucune sorte, expresse ou implicite. Voir la licence pour la langue spécifique régissant les autorisations et les limitations sous la licence.

Jamais imprimé, Janvier 2019

Table des matières

Introduction

| | | |
|----------|---------------------|----------|
| 1 | Présentation | 9 |
|----------|---------------------|----------|

I

Cours

| | | |
|------------|---------------------------------|-----------|
| 2 | Raisonnements | 15 |
| 2.1 | Éléments de logique | 15 |
| 2.1.1 | Bases | 15 |
| 2.1.2 | Implications | 18 |
| 2.1.3 | Équivalences | 18 |
| 2.2 | Quantificateurs | 27 |
| 2.3 | Types de raisonnements | 29 |
| 2.3.1 | Modus ponens | 29 |
| 2.3.2 | Contraposition ou modus tollens | 29 |
| 2.3.3 | Par l'absurde | 29 |
| 2.3.4 | Séparation | 29 |
| 2.3.5 | Contre-exemple | 30 |
| 2.3.6 | Disjonction des cas | 30 |
| 2.3.7 | Syllogisme | 30 |
| 2.3.8 | Syllogisme disjonctif | 30 |
| 2.3.9 | Déduction | 30 |
| 2.3.10 | Récurrence | 30 |

| | | |
|------------|--|-----------|
| 2.3.11 | Descente | 30 |
| 2.3.12 | Abduction | 30 |
| 2.3.13 | Induction | 31 |
| 3 | Ensembles | 33 |
| 3.1 | Éléments de théorie des ensembles | 33 |
| 3.1.1 | Égalité | 33 |
| 3.1.2 | Éléments de théorie des ensembles | 33 |
| 4 | Applications | 41 |
| 4.1 | Applications | 41 |
| 4.1.1 | Généralités | 41 |
| 4.1.2 | Injection | 42 |
| 4.1.3 | Surjection | 44 |
| 4.1.4 | Bijection | 44 |
| 4.1.5 | Composition | 45 |
| 5 | Nombres entiers naturels | 49 |
| 5.1 | Nombres entiers naturels | 49 |
| 5.1.1 | Présentation axiomatique | 49 |
| 5.1.2 | Addition des entiers naturels | 54 |
| 5.1.3 | Ordre | 55 |
| 5.1.4 | Soustraction | 62 |
| 5.1.5 | Multiplication | 63 |
| 5.1.6 | Division | 64 |
| 6 | Nombres entiers relatifs | 65 |
| 6.1 | Entiers relatifs | 65 |
| 6.1.1 | Définition | 65 |
| 6.1.2 | Addition | 66 |
| 6.1.3 | Soustraction | 68 |
| 6.1.4 | Produit | 68 |
| 7 | Relations | 71 |
| 7.1 | Relations | 71 |
| 7.1.1 | Généralités | 71 |
| 7.1.2 | Ordre | 72 |
| 7.1.3 | Équivalence | 72 |
| 8 | Nombres rationnels | 75 |
| 9 | Corps totalement ordonné | 77 |

| | | |
|-------------|--------------------------------------|------------|
| 10 | Nombres réels | 79 |
| 11 | Nombres décimaux | 81 |
| 12 | Nombres complexes | 83 |
| 13 | Dénombrement | 85 |
| 13.1 | Dénombrement | 85 |
| 13.1.1 | Ensembles finis ou infinis | 85 |
| 13.1.2 | Cardinal | 90 |
| 14 | Combinatoire | 97 |
| 14.1 | Combinatoire | 97 |
| 14.1.1 | Factorielle | 97 |
| 14.1.2 | Listes et application | 100 |
| 14.1.3 | Arrangements et injections | 101 |
| 14.1.4 | Bijections et permutations. | 102 |
| 14.1.5 | Combinaisons | 103 |
| 15 | Groupes | 113 |
| 16 | Arithmétique | 115 |
| 17 | Congruences | 117 |
| 18 | Polynômes | 119 |
| 19 | Suites réelles | 121 |
| 20 | Fonctions de variable réelle | 123 |
| 21 | Suites et séries de fonctions | 125 |
| 22 | Calcul intégral | 127 |
| 23 | Intégrale de Riemann | 129 |
| 24 | Équations différentielles | 131 |
| 25 | Analyse asymptotique | 133 |
| 26 | Espaces vectoriels | 135 |

| | |
|---|------------|
| 27 Applications linéaires | 137 |
| 28 Matrices et déterminants | 139 |
| 29 Systèmes linéaires | 141 |
| 30 Applications multi linéaires | 143 |
| 31 Espaces euclidiens | 145 |
| 32 Topologie d'un EVN de dimension finie | 147 |
| 33 Applications linéaires continues | 149 |
| 34 Calcul différentiel | 151 |
| 35 Probabilités | 153 |
| 35.1 Probabilités | 153 |
| 35.1.1 Prérequis, rappels et précautions | 153 |
| 35.1.2 Généralités. | 153 |
| 35.1.3 Probabilités composées | 161 |
| 36 Variables aléatoires | 165 |
| 36.1 Variables aléatoires | 165 |
| 36.1.1 Variables aléatoires discrètes | 165 |
| 36.1.2 Exemples de lois discrètes | 170 |
| 36.1.3 Variables aléatoires à densité | 173 |
| 36.1.4 Théorèmes limites | 175 |
| 36.1.5 Fluctuation. Estimation. | 177 |
| 37 Familles | 181 |



1. Présentation

Première épreuve d'admissibilité

Programme de l'option mathématiques

Raisonnement et vocabulaire ensembliste.

Opérateurs logiques et quantificateurs. Vocabulaire de la théorie des ensembles. Applications, relations d'ordre et relations d'équivalence.

Nombres complexes.

Module et argument. Racines n^{mes} de l'unité. Exponentielle complexe, trigonométrie. Application à la géométrie plane. Équation du second degré.

Fonctions d'une variable réelle.

Continuité, théorème des valeurs intermédiaires. Dérivabilité, théorème de Rolle, inégalité des accroissements finis. Extension aux fonctions à valeurs complexes. Fonctions à valeurs dans \mathbf{R}^2 . Courbes paramétrées.

Calcul intégral et Équations différentielles.

Intégrale d'une fonction continue sur un segment, sommes de Riemann. Calculs de primitives. Intégration par parties, changement de variable. Formule de Taylor avec reste intégral. Intégrales généralisées. Équations différentielles linéaires du premier ordre, du premier ordre à variables séparables, linéaires du second ordre à coefficients constants.

Nombres réels et suites réelles.

Construction de \mathbf{N} , \mathbf{Z} et \mathbf{Q} . Présentation axiomatique de \mathbf{R} , bornes supérieure et inférieure. Valeurs approchées, nombres décimaux. Limite d'une suite réelle, théorèmes d'existence. Suites extraites. Extension aux suites à valeurs complexes. Séries numériques, séries à termes positifs, séries absolument convergentes, séries de références (séries géométriques, séries de Riemann).

Suites et séries de fonctions.

Convergence simple, convergence uniforme. Théorèmes de régularité. Convergence normale des séries de fonctions. Séries entières, rayon de convergence. Développement en série entière des fonctions usuelles.

Analyse asymptotique.

Relations de comparaisons des suites et des fonctions. Développements limités.

Algèbre linéaire.

Systèmes linéaires, algorithme du pivot de Gauss-Jordan. Espaces vectoriels de dimension finie, familles libres, familles génératrices, bases. Applications linéaires. Homothéties, projections et symétries. Rang d'une application linéaire. Représentations matricielles d'un endomorphisme. Réduction des endomorphismes et des matrices carrées : éléments propres, diagonalisation, trigonalisation.

Matrices et déterminants.

Calcul matriciel, matrices inversibles, transposition. Matrices et applications linéaires, changement de bases. Équivalence, similitude. Déterminant d'une matrice carrée, d'un endomorphisme d'un espace vectoriel de dimension finie.

Dénombrement.

Cardinal d'un ensemble fini, listes, combinaisons, factorielles, formule du binôme.

Arithmétique des entiers.

Arithmétique des entiers : nombres premiers, PGCD, PPCM, algorithme d'Euclide. Sous-groupes de \mathbf{Z} . Congruences. Anneaux $\mathbf{Z}/n\mathbf{Z}$. Théorème des restes chinois, petit théorème de Fermat.

Polynômes.

Arithmétique des polynômes à coefficients réels ou complexes. Racines. Décomposition dans $\mathbf{R}[X]$ et $\mathbf{C}[X]$.

Groupes.

Sous-groupes, morphismes de groupes. Groupes monogènes et groupes cycliques : groupes $\mathbf{Z}/n\mathbf{Z}$, groupe des racines n -ièmes de l'unité ; générateurs, indicatrice d'Euler. Ordre d'un élément. Groupes symétriques. Exemples de groupes agissant sur un ensemble, exemples de groupes laissant invariante une partie du plan ou de l'espace.

Produit scalaire et espaces euclidiens.


Produit scalaire sur un espace de dimension finie, norme associée, orthogonalité. Bases orthonormées. Projections orthogonales. Orientation. Groupes des isométries vectorielles d'un espace euclidien, des isométries affines d'un espace euclidien, des similitudes d'un espace euclidien. Isométries vectorielles d'un espace euclidien de dimension 2 ou 3. Isométries affines du plan euclidien.

Probabilités.

Espaces probabilisés finis. Probabilités conditionnelles, conditionnement et indépendance. Variable aléatoires sur un univers fini : lois usuelles (lois uniformes, lois binomiales), variables aléatoires indépendantes, espérance, variance et écart-type. Variables aléatoires discrètes : espérance et variance, lois de Poisson, lois géométriques, lois exponentielles.



| | | |
|-----------|--|------------|
| 17 | Congruences | 117 |
| 18 | Polynômes | 119 |
| 19 | Suites réelles | 121 |
| 20 | Fonctions de variable réelle | 123 |
| 21 | Suites et séries de fonctions | 125 |
| 22 | Calcul intégral | 127 |
| 23 | Intégrale de Riemann | 129 |
| 24 | Équations différentielles . | 131 |
| 25 | Analyse asymptotique | 133 |
| 26 | Espaces vectoriels | 135 |
| 27 | Applications linéaires | 137 |
| 28 | Matrices et déterminants | 139 |
| 29 | Systèmes linéaires | 141 |
| 30 | Applications multi linéaires | 143 |
| 31 | Espaces euclidiens | 145 |
| 32 | Topologie d'un EVN de dimension finie | 147 |
| 33 | Applications linéaires continues | 149 |
| 34 | Calcul différentiel | 151 |
| 35 | Probabilités | 153 |
| 35.1 | Probabilités | |
| 36 | Variables aléatoires | 165 |
| 36.1 | Variables aléatoires | |
| 37 | Familles | 181 |



2. Raisonnements

2.1 Éléments de logique

On utilise la définition d'ensemble ainsi que les calculs algébriques sur les petits entiers. On présente un peu de calcul propositionnel.

2.1.1 Bases

Axiome 2.1.1 — Proposition. **vrai** et **faux** sont deux objets mathématiques dénommés valeurs logiques.

Vocabulaire 2.1.1

- valeur de vérité est synonyme de valeur logique.
- **V** et 1 sont synonymes de **vrai**.
- **F** et 0 sont synonymes de **faux**.

En particulier, **faux** = 1 – **vrai** , **faux** < **vrai**.

Définition 2.1.1 — Proposition. Une proposition est un objet mathématique auquel est associée une valeur logique

Définition 2.1.2

- **vrai** est une proposition à laquelle est associée la valeur logique **vrai**.
- **faux** est une proposition à laquelle est associée la valeur logique **faux**.

Notation 2.1.1 $vl(P)$ désigne la valeur logique de la proposition P .

En particulier, $vl = vl^2$ ou $vl \times (1 - vl) = 0$

Définition 2.1.3 — Théorie. Une théorie est un ensemble de propositions.

Définition 2.1.4 — contraire, et, ou. Si P et Q sont des propositions,

- **non** P est une proposition appelée contraire de P , aussi notée $\neg P$ ou \bar{P} ,
- P **et** Q est une proposition appelée conjonction de P et Q , aussi notée $P \wedge Q$,
- P **ou** Q est une proposition appelée disjonction de P et Q , aussi notée $P \vee Q$.

Vocabulaire 2.1.2 — Propositions composées, atomiques. Une proposition est complexe signifie qu'elle est sous une des formes **non** P , P **et** Q ou P **ou** Q . Une proposition est atomique signifie qu'elle n'est pas sous l'une de ces formes.

Définition 2.1.5 — Priorité. Par ordre de priorité décroissante des opérateurs, il vient **non**, puis **et** et **ou**.

R à rapprocher de certains langages informatiques.

Définition 2.1.6 — Table de vérité. Soit P une proposition construite à partir d'un nombre fini de propositions atomiques Q_i . La table de vérité de P est l'application qui associe à chaque combinaison possible des valeurs de vérité des Q_i une valeur de vérité à P correspondante.

Axiome 2.1.2 — Tables de vérité de la négation, de la conjonction et de la disjonction.

| P | $\neg P$ | P | Q | $P \wedge Q$ | P | Q | $P \vee Q$ |
|---|----------|---|---|--------------|---|---|------------|
| V | F | V | V | V | V | V | V |
| V | F | V | F | F | V | F | V |
| F | V | F | V | F | F | V | V |
| | | F | F | F | F | F | F |

R De manière synthétique, on a

| P | Q | $\neg P$ | $P \wedge Q$ | $P \vee Q$ |
|---|---|----------|--------------|------------|
| V | V | F | V | V |
| V | F | F | F | V |
| F | V | V | F | V |
| F | F | V | F | F |

En termes de valeur logique :

$$vl(\neg P) = 1 - vl(P)$$

$$vl(P \wedge Q) = vl(P).vl(Q)$$

$$vl(P \vee Q) = vl(P) + vl(Q) - vl(P).vl(Q)$$

Définition 2.1.7 — Tautologie, antinomie. Une tautologie est une proposition qui n'a que la valeur logique **vrai**, une antinomie est une proposition qui n'a que la valeur logique **faux**.

Théorème 2.1.3 Soit P et Q des propositions. Si P est une tautologie, alors P **ou** Q est une tautologie. Si en plus Q est une tautologie, alors P **et** Q est une tautologie.

Si P est une antinomie, alors P **et** Q est une antinomie. Si en plus Q est une antinomie, alors P **ou** Q est une tautologie.

Démonstration. Dans le premier cas, cela correspond aux deux premières lignes du tableau précédent. Uniquement la première dans le deuxième cas. ■

De manière symétrique.

Théorème 2.1.4 Soit P et Q des propositions. Si P est une antinomie, alors P **et** Q est une antinomie. Si en plus Q est une antinomie, alors P **ou** Q est une antinomie.

Démonstration. Dans le premier cas, ce sont les deux dernières lignes du tableau précédent. Uniquement la dernière dans le deuxième cas. ■

Théorème 2.1.5 — Tiers exclu. P **ou non** P est une tautologie.

Théorème 2.1.6 — Non contradiction. P **et non** P est une antinomie.

Démonstration. On a regroupé ci-dessous les tables de vérités de P **et non** P et P **ou non** P.

| P | $\neg P$ | $P \wedge \neg P$ | $P \vee \neg P$ |
|----------|----------|-------------------|-----------------|
| V | F | F | V |
| F | V | F | V |

On peut le lire dans le tableau précédent, mais on a aussi

$$\begin{aligned} vl(P \wedge \neg P) &= vl(P).vl(\neg P) \\ &= vl(P).(1 - vl(P)) \\ &= 0 \end{aligned}$$

$$\begin{aligned} vl(P \vee \neg P) &= vl(P) + vl(\neg P) - vl(P).vl(\neg P) \\ &= vl(P) + 1 - vl(P) - vl(P).(1 - vl(P)) \\ &= 1 \end{aligned}$$

■

2.1.2 Implications

Définition 2.1.8 — Implication. Si P et Q sont des propositions, on pose :

$$(P \Rightarrow Q) \stackrel{\text{déf}}{=} ((\text{non } P) \text{ ou } Q)$$

$$(Q \Leftarrow P) \stackrel{\text{déf}}{=} (P \Rightarrow Q)$$

\Rightarrow est lu «implique» ou entraîne. \Leftarrow est lu «est impliqué par» ou «est entraîné par». La proposition complexe $P \Rightarrow Q$ est une implication. P est la prémisse, Q est la conclusion.

2.1.3 Équivalences

Définition 2.1.9 — Équivalence. Si P et Q sont des propositions, on pose

$$P \Leftrightarrow Q \stackrel{\text{déf}}{=} (P \text{ et } Q) \text{ ou } ((\text{non } P) \text{ et } (\text{non } Q))$$

Vocabulaire 2.1.3 P et Q sont équivalentes signifie que $P \Leftrightarrow Q$ est vraie. De même pour P équivaut à Q . Les équivalences sont les propositions complexes de la forme $P \Leftrightarrow Q$.

Théorème 2.1.7 — Tautologies. Si P et Q sont des propositions, les équivalences suivantes sont des tautologies :

- $(\text{non}(\text{non } P)) \Leftrightarrow P$
- $(P \text{ et } P) \Leftrightarrow P$,
- $(P \text{ ou } P) \Leftrightarrow P$
- $(P \text{ et } Q) \Leftrightarrow (Q \text{ et } P)$
- $\text{non}(P \text{ et } Q) \Leftrightarrow ((\text{non } P) \text{ ou } (\text{non } Q))$
- $\text{non}(P \text{ ou } Q) \Leftrightarrow \text{non } P \text{ et } \text{non } Q$

Démonstration. Pour les deux premières lignes :

| P | P | $\neg P$ | $\neg(\neg P)$ | $P \wedge P$ | $P \vee P$ |
|-----|-----|----------|----------------|--------------|------------|
| 1 | 1 | 0 | 1 | 1 | 1 |
| 0 | 0 | 1 | 0 | 0 | 0 |

Il est facile de voir à partir de leurs définitions que **et** et **ou** sont commutatifs par équivalence. Pour leurs négations :

| P | $\neg P$ | Q | $\neg Q$ | $P \wedge Q$ | $\neg(P \wedge Q)$ | $\neg P \vee \neg Q$ | $P \vee Q$ | $\neg(P \vee Q)$ | $\neg P \wedge \neg Q$ |
|-----|----------|-----|----------|--------------|--------------------|----------------------|------------|------------------|------------------------|
| 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |

| P | $\neg P$ | Q | $\neg Q$ | $P \wedge Q$ | $\neg P \wedge \neg Q$ | $P \Leftrightarrow Q$ | $P \Rightarrow Q$ | $Q \Rightarrow P$ | $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ |
|---|----------|---|----------|--------------|------------------------|-----------------------|-------------------|-------------------|--|
| 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |



Définition 2.1.10 Étant donné P et Q deux propositions. $P \Leftrightarrow Q$ signifie que $\text{vl}(P) = \text{vl}(Q)$. $P \Leftrightarrow Q$ est lu «P équivaut à Q» ou «P est équivalent à Q».

Démonstration. Par la table de vérité :

| P | Q | $P \Leftrightarrow Q$ | $\text{vl}(P) = \text{vl}(Q)$ |
|---|---|-----------------------|-------------------------------|
| 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 1 |

et par le calcul :

$$\begin{aligned}
 \text{vl}(P \Leftrightarrow Q) &= \text{vl}((P \wedge Q) \vee (\neg P \wedge \neg Q)) \\
 &= \text{vl}(P \wedge Q) + \text{vl}(\neg P \wedge \neg Q) - \text{vl}(P \wedge Q) \cdot \text{vl}(\neg P \wedge \neg Q) \\
 &= \text{vl}(P) \cdot \text{vl}(Q) + \text{vl}(\neg P) \cdot \text{vl}(\neg Q) - \text{vl}(P) \cdot \text{vl}(Q) \cdot \text{vl}(\neg P) \cdot \text{vl}(\neg Q) \\
 &= \text{vl}(P) \cdot \text{vl}(Q) + (1 - \text{vl}(P)) \cdot (1 - \text{vl}(Q)) \\
 &= 1 + 2 \cdot \text{vl}(P) \cdot \text{vl}(Q) - \text{vl}(P) - \text{vl}(Q) \\
 &= 1 + 2 \cdot \text{vl}(P) \cdot \text{vl}(Q) - \text{vl}^2(P) - \text{vl}^2(Q) \\
 &= 1 - (\text{vl}(P) - \text{vl}(Q))^2
 \end{aligned}$$



Théorème 2.1.8 — Substitution. Dans une proposition complexe, on peut remplacer une proposition argument d'un des opérateurs par une proposition qui lui est équivalente et obtenir ainsi une nouvelle proposition qui est équivalente à la celle de départ.

Démonstration. On pourrait le démontrer modulo un formalisme adapté, mais c'est lourd...



R Dans la suite, on n'utilise plus **V** et **F**, seulement 1 et 0.

Théorème 2.1.9 — Tautologies. Si P et Q sont des propositions, les propositions suivantes sont des tautologies :

- $P \Rightarrow P$,
- $P \Rightarrow (P \text{ ou } Q)$

Démonstration.

| P | Q | $\neg P$ | $(\neg P) \vee P$ | $P \vee Q$ | $(\neg P) \vee (P \vee Q)$ |
|---|---|----------|-------------------|------------|----------------------------|
| 1 | 1 | 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 1 |
| 0 | 1 | 1 | 1 | 1 | 1 |
| 0 | 0 | 1 | 1 | 0 | 1 |

Théorème 2.1.10 Si P et Q sont des propositions, la valeur de vérité de $P \Rightarrow Q$ est **vrai** si et seulement si la valeur de vérité de P est inférieure à celle de Q . En plus court, $(P \Rightarrow Q) \Leftrightarrow (vl(P) \leq vl(Q))$ est une tautologie.

Démonstration.

| P | Q | $\neg P$ | $(\neg P) \vee Q$ | $vl(P) \leq vl(Q)$ |
|---|---|----------|-------------------|--------------------|
| 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 | 1 |
| 0 | 0 | 1 | 1 | 1 |

Théorème 2.1.11 Pour montrer qu'une implication est une tautologie, il suffit de la démontrer dans le cas particulier où la prémisse est vraie.

Théorème 2.1.12 — Simplification de et. Si P et Q sont des propositions, $(P \text{ et } Q) \Rightarrow P$ est une tautologie.

Démonstration.

| P | Q | $P \wedge Q$ | $\neg(P \wedge Q)$ | $\neg(P \wedge Q) \vee P$ |
|---|---|--------------|--------------------|---------------------------|
| 1 | 1 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 1 | 1 |
| 0 | 0 | 0 | 1 | 1 |

Théorème 2.1.13 — Syllogisme disjonctif. Si P et Q sont des propositions, $P \text{ ou } Q \text{ et non } P \Rightarrow Q$ est une tautologie.

Démonstration.

| P | Q | $P \vee Q$ | $\neg P$ | $(P \vee Q) \vee \neg P$ |
|---|---|------------|----------|--------------------------|
| 1 | 1 | 1 | 0 | 0 |
| 1 | 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 1 | 1 |
| 0 | 0 | 0 | 1 | 0 |

Avec l'associativité de **ou** vue ci-dessous, on a

$$\begin{aligned}
 ((P \vee Q) \wedge \neg P \Rightarrow Q) &\Leftrightarrow \neg((P \vee Q) \wedge \neg P) \vee Q \\
 &\Leftrightarrow (\neg(P \vee Q) \vee P) \vee Q \\
 &\Leftrightarrow \neg(P \vee Q) \vee (P \vee Q)
 \end{aligned}$$

■

Théorème 2.1.14 — Tautologies. Si P et Q sont des propositions, les propositions complexes suivantes sont toutes des tautologies :

- $(P \Leftrightarrow Q) \Leftrightarrow ((P \Rightarrow Q) \text{ et } (Q \Rightarrow P))$
- $(P \Leftrightarrow Q) \Leftrightarrow (Q \Leftrightarrow P)$
- $\text{non}(P \Leftrightarrow Q) \Leftrightarrow ((\text{non } P) \Leftrightarrow Q)$
- $\text{non}(P \Leftrightarrow Q) \Leftrightarrow (P \Leftrightarrow (\text{non } Q))$
- $\text{non}(P \Rightarrow Q) \Leftrightarrow (P \text{ et non } Q)$

Démonstration. Par substitution,

$$\begin{aligned}
 ((P \Rightarrow Q) \text{ et } (Q \Rightarrow P)) &\Leftrightarrow ((\text{vl}(P) \leq \text{vl}(Q)) \text{ et } (\text{vl}(Q) \leq \text{vl}(P))) \\
 &\Leftrightarrow (\text{vl}(P) = \text{vl}(Q))
 \end{aligned}$$

on termine en utilisant la commutativité par équivalence de **et** ainsi que la caractérisation de l'équivalence par la valeur logique.

Pour la deuxième ligne,

| P | $\neg P$ | Q | $\neg Q$ | $P \Leftrightarrow Q$ | $\neg(P \Leftrightarrow Q)$ | $(\neg P) \Leftrightarrow Q$ | $P \Leftrightarrow (\neg Q)$ |
|---|----------|---|----------|-----------------------|-----------------------------|------------------------------|------------------------------|
| 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 |
| 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |

Pour finir, par substitutions successives :

$$\begin{aligned}
 \neg(P \Rightarrow Q) &\Leftrightarrow \neg(\neg P \vee Q) \\
 &\stackrel{\text{subs}}{\Leftrightarrow} (\neg(\neg P) \wedge \neg Q) \\
 &\stackrel{\text{subs}}{\Leftrightarrow} (P \wedge \neg Q)
 \end{aligned}$$

■

Théorème 2.1.15 — Contraposition. Si P et Q sont des propositions, on a les tautologies :

$$(P \Leftrightarrow Q) \Leftrightarrow ((\text{non } P) \Leftrightarrow (\text{non } Q))$$

$$(P \Rightarrow Q) \Leftrightarrow ((\text{non } Q) \Rightarrow (\text{non } P))$$

Démonstration.

| P | $\neg P$ | Q | $\neg Q$ | $P \Leftrightarrow Q$ | $\neg P \Leftrightarrow \neg Q$ | $P \Rightarrow Q$ | $\neg Q \Rightarrow \neg P$ |
|---|----------|---|----------|-----------------------|---------------------------------|-------------------|-----------------------------|
| 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |

■

En fait, il y a 16 combinaisons possibles pour des opérations binaires :

| P | Q | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|-----------------|------------|-----------------|-----|-----------------|-----|---------------------------------|--------------|--------------------|-----------------------------|-----|-----------------------------|----------|-----------------------------|------------------|-------------------|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| | | $P \vee \neg P$ | $P \vee Q$ | $P \vee \neg Q$ | P | $\neg P \vee Q$ | Q | $\neg P \Leftrightarrow \neg Q$ | $P \wedge Q$ | $\neg(P \wedge Q)$ | $\neg(P \Leftrightarrow Q)$ | Q | $\neg(P \Leftrightarrow Q)$ | $\neg P$ | $\neg(Q \Leftrightarrow P)$ | $\neg(P \vee Q)$ | $P \wedge \neg P$ |

R On peut introduit l'opérateur binaire **ou bien** aussi noté $\vee\vee$ en sorte que $\neg(P \Leftrightarrow Q)$ et $P \vee\vee Q$ sont équivalents.

Théorème 2.1.16 — \Leftrightarrow est une relation d'équivalence. L'équivalence des propositions définit une relation d'équivalence entre les propositions.

Démonstration.

- Réflexivité :

$$P \Leftrightarrow P \stackrel{\text{déf}}{=} (P \text{ et } P) \text{ ou } ((\text{non } P) \text{ et } (\text{non } P))$$

$$\stackrel{\text{subs}}{\Leftrightarrow} (P \text{ ou } (\text{non } P))$$

- Symétrie : c'est la première tautologie du théorème précédent.

- Transitivité :

| P | Q | R | $P \Leftrightarrow Q$ | $Q \Leftrightarrow R$ | $(P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R)$ | $P \Leftrightarrow R$ |
|---|---|---|-----------------------|-----------------------|--|-----------------------|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 |
| 1 | 0 | 1 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 |



- R** On peut écrire les suites d'équivalence en ligne.

Théorème 2.1.17 — Associativités. Soient P, Q et R des propositions, on a les tautologies :

- $(P \text{ et } (Q \text{ et } R)) \Leftrightarrow ((P \text{ et } Q) \text{ et } R)$
- $(P \text{ ou } (Q \text{ ou } R)) \Leftrightarrow ((P \text{ ou } Q) \text{ ou } R)$
- $(P \Leftrightarrow (Q \Leftrightarrow R)) \Leftrightarrow ((P \Leftrightarrow Q) \Leftrightarrow R)$
- $(P \Rightarrow (Q \Rightarrow R)) \Rightarrow ((P \Rightarrow Q) \Rightarrow R)$

- A** \Rightarrow n'est pas associatifs !

- R** (moyen presque mnémotechnique) commutatif donne associatif.

Démonstration.

| P | Q | R | $Q \wedge R$ | $P \wedge (Q \wedge R)$ | $P \wedge Q$ | $(P \wedge Q) \wedge R$ |
|---|---|---|--------------|-------------------------|--------------|-------------------------|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |

On en déduit :

$$\begin{aligned} \neg(P \vee (Q \vee R)) &\Leftrightarrow \neg P \wedge \neg(Q \vee R) \Leftrightarrow \neg P \wedge (\neg Q \wedge \neg R) \Leftrightarrow \dots \\ \dots &\Leftrightarrow (\neg P \wedge \neg Q) \wedge \neg R \Leftrightarrow \neg(P \vee Q) \wedge \neg R \Leftrightarrow \neg((P \vee Q) \vee R) \end{aligned}$$

Pour les deux dernières lignes :

| P | Q | R | $Q \Leftrightarrow R$ | $P \Leftrightarrow (Q \Leftrightarrow R)$ | $P \Leftrightarrow Q$ | $(P \Leftrightarrow Q) \Leftrightarrow R$ |
|---|---|---|-----------------------|---|-----------------------|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| 0 | 0 | 1 | 0 | 1 | 1 | 1 |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 |

| P | Q | R | $Q \Rightarrow R$ | $P \Rightarrow (Q \Rightarrow R)$ | $P \Rightarrow Q$ | $(P \Rightarrow Q) \Rightarrow R$ |
|---|---|---|-------------------|-----------------------------------|-------------------|-----------------------------------|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 |

■

Théorème 2.1.18 — Distributivités et ou. Soient P, Q et R des propositions, on a les tautologies :

- $(P \text{ ou } (Q \text{ et } R)) \Leftrightarrow ((P \text{ ou } Q) \text{ et } (P \text{ ou } R))$
- $(P \text{ et } (Q \text{ ou } R)) \Leftrightarrow ((P \text{ et } Q) \text{ ou } (P \text{ et } R))$

Démonstration.

| P | Q | R | $Q \wedge R$ | $P \vee (Q \wedge R)$ | $P \vee Q$ | $P \vee R$ | $(P \vee Q) \wedge (P \vee R)$ |
|---|---|---|--------------|-----------------------|------------|------------|--------------------------------|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

On pourrait faire le même tableau en échangeant les deux opérateurs, on peut aussi utiliser la négation :

$$\begin{aligned}
\neg(P \wedge (Q \vee R)) &\Leftrightarrow \neg P \vee \neg(Q \vee R) \\
&\Leftrightarrow \neg P \vee (\neg Q \wedge \neg R) \\
&\Leftrightarrow (\neg P \vee \neg Q) \wedge (\neg P \vee \neg R) \\
&\Leftrightarrow \neg(P \wedge Q) \wedge \neg(P \wedge R) \\
&\Leftrightarrow \neg((P \wedge Q) \vee (P \wedge R))
\end{aligned}$$

■

Théorème 2.1.19 — Distributivités à gauche de \Rightarrow . Soient P, Q et R des propositions, on a les tautologies :

- $(P \Rightarrow (Q \text{ et } R)) \Leftrightarrow ((P \Rightarrow Q) \text{ et } (P \Rightarrow R))$
- $(P \Rightarrow (Q \text{ ou } R)) \Leftrightarrow ((P \Rightarrow Q) \text{ ou } (P \Rightarrow R))$

Démonstration. Par la définition de l'implication et le théorème précédent,

$$\begin{aligned}
\neg(P \vee (Q \wedge R)) &\Leftrightarrow (\neg P \vee Q) \wedge (\neg P \vee R) \\
\neg P \vee (Q \vee R) &\Leftrightarrow ((\neg P \vee Q) \vee (\neg P \vee R))
\end{aligned}$$

On a terminé en utilisant associativité et commutativité de \vee . ■

Théorème 2.1.20 — Séparation. Soient P, Q et R des propositions, on a les tautologies :

- $((P \text{ et } Q) \Rightarrow R) \Leftrightarrow (P \Rightarrow (Q \Rightarrow R))$
- $((P \text{ ou } Q) \Rightarrow R) \Leftrightarrow ((P \Rightarrow R) \text{ et } (Q \Rightarrow R))$

Démonstration. Par la définition de l'implication et l'associativité de **ou**,

$$\begin{aligned}
((P \wedge Q) \Rightarrow R) &\Leftrightarrow \neg(P \wedge Q) \vee R \\
&\Leftrightarrow (\neg P \vee \neg Q) \vee R \\
&\Leftrightarrow \neg P \vee (\neg Q \vee R) \\
&\Leftrightarrow \neg P \vee (Q \Rightarrow R) \\
&\Leftrightarrow (P \Rightarrow (Q \Rightarrow R))
\end{aligned}$$

et par la définition de l'implication et le théorème ??,

$$\begin{aligned}
((P \vee Q) \Rightarrow R) &\Leftrightarrow \neg(P \vee Q) \vee R \\
&\Leftrightarrow (\neg P \wedge \neg Q) \vee R \\
&\Leftrightarrow (\neg P \vee R) \wedge (\neg Q \vee R) \\
&\Leftrightarrow (P \Rightarrow R) \wedge (Q \Rightarrow R)
\end{aligned}$$

■

Théorème 2.1.21 Soient P, Q et R des propositions.

- $(P \Leftrightarrow (Q \text{ et } R)) \Leftarrow ((P \Leftrightarrow Q) \text{ et } (P \Leftrightarrow R))$
- $(P \Leftrightarrow (Q \text{ ou } R)) \Rightarrow ((P \Leftrightarrow Q) \text{ ou } (P \Leftrightarrow R))$

R Ce ne sont pas des équivalences !

Démonstration. Pour la première implication, on compare les colonnes en gras :

| P | Q | R | $Q \wedge R$ | $P \Leftrightarrow (Q \wedge R)$ | $P \Leftrightarrow Q$ | $P \Leftrightarrow R$ | $(P \Leftrightarrow Q) \wedge (P \Leftrightarrow R)$ |
|---|---|---|--------------|----------------------------------|-----------------------|-----------------------|--|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 |
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |

Les cases grises montrent qu'il n'y a pas d'équivalences. Pour la deuxième implication, sont équivalentes :

- $(P \Leftrightarrow (Q \wedge R)) \Leftarrow ((P \Leftrightarrow Q) \wedge (P \Leftrightarrow R))$
- $\neg((P \Leftrightarrow Q) \wedge (P \Leftrightarrow R)) \Rightarrow \neg(P \Leftrightarrow (Q \wedge R))$
- $(\neg(P \Leftrightarrow Q) \vee \neg(P \Leftrightarrow R)) \Rightarrow (\neg P \Leftrightarrow \neg(Q \wedge R))$
- $((\neg P \Leftrightarrow \neg Q) \vee (\neg P \Leftrightarrow \neg R)) \Rightarrow (\neg P \Leftrightarrow (\neg Q \vee \neg R))$

Il suffit de substituer à chaque proposition sa négation. ■

Théorème 2.1.22 — Ordre. \Rightarrow est une relation d'ordre à équivalence près.

Démonstration. À équivalence près signifie que c'est une relation d'ordre sur les classes d'équivalence.

Soient P, Q et R des propositions.

- \Rightarrow est réflexive : Par définition, $P \Rightarrow P$ est la tautologie (**non** P) **ou** P.
- \Rightarrow est anti-symétrique à équivalence près : on a déjà vu la tautologie

$$(P \Rightarrow Q \text{ et } P \Leftarrow Q) \Leftrightarrow (P \Leftrightarrow Q)$$

- \Rightarrow est transitive :

| P | Q | R | $P \Rightarrow Q$ | $Q \Rightarrow R$ | $(P \Rightarrow Q) \wedge (Q \Rightarrow R)$ | $P \Rightarrow R$ |
|---|---|---|-------------------|-------------------|--|-------------------|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 |
| 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 0 | 1 | 0 | 0 | 1 |
| 0 | 0 | 1 | 1 | 1 | 0 | 1 |
| 0 | 0 | 0 | 1 | 1 | 0 | 1 |



2.2 Quantificateurs

Cette partie repose sur la notion d'ensembles détaillée au chapitre suivant.

Axiome 2.2.1 — Quantificateurs existentiel et universel. Pour tout ensemble E , les propositions suivantes sont des tautologies

- $E \neq \emptyset \Leftrightarrow \exists x(x \in E)$
- $E = \emptyset \Leftrightarrow \forall x(x \notin E)$

- R** Ce ne sont pas des définitions car la notion d'ensemble est pré-requise, qui utilise elle-même les quantificateurs.

Définition 2.2.1 — Quantificateurs. Étant donné un ensemble Ω et une proposition dont l'écriture dépend formellement d'un paramètre x notée $P(x)$,

- $\exists x \in \Omega (P(x)) \stackrel{\text{déf}}{\Leftrightarrow} \exists x (x \in \Omega \text{ et } P(x))$
- $\forall x \in \Omega (P(x)) \stackrel{\text{déf}}{\Leftrightarrow} \text{non}(\exists x \in \Omega (\text{non } P(x)))$

Communication 2.2.1 $\exists x \in \Omega \dots$ est lu « il existe \square élément de (ou dans) Ω tel que \dots ». $\forall x \in \Omega \dots$ est lu « quel que soit x élément de (ou dans) Ω tel que \dots » ou « pour tout x élément de (ou dans) Ω tel que \dots ».

- R** En fait ce n'est pas une seule définition mais un gabarit de définitions. Cela permet de donner autant de définitions que de Ω et $P(x)$ possibles.

Théorème 2.2.2 Étant donné un ensemble Ω et une proposition dont l'écriture dépend formellement d'un paramètre x notée $P(x)$, on a les tautologies

- $\exists x \in \Omega P(x) \Leftrightarrow \{z \in \Omega / P(z)\} \neq \emptyset \Rightarrow \Omega \neq \emptyset$

- $\forall x \in \Omega (P(x)) \Leftrightarrow \{z \in \Omega / \neg P(z)\} = \emptyset \Leftrightarrow \{z \in \Omega / P(z)\} = \Omega$

Démonstration. Avec le quantificateur existentiel, c'est une application directe de l'axiome ci-dessus sachant que

$$x \in \{z \in \Omega / P(z)\} \stackrel{\text{déf}}{\Leftrightarrow} x \in \Omega \text{ et } P(x)$$

Avec le quantificateur universel, on utilise les négations. On a

$$\exists x \in \Omega (\neg P(x)) \Leftrightarrow \{z \in \Omega / \neg P(z)\} \neq \emptyset$$

d'où

$$\forall x \in \Omega (P(x)) \Leftrightarrow \neg(\exists x \in \Omega (\neg P(x))) \Leftrightarrow \{z \in \Omega / \neg P(z)\} = \emptyset$$

■

Théorème 2.2.3 Étant donné un ensemble Ω et une proposition dont l'écriture dépend formellement d'un paramètre notée $P(\square)$. Les ensembles $\{z \in \Omega / P(z)\}$ et $\{z \in \Omega / \neg P(z)\}$ forment une partition de Ω , en particulier

$$\{z \in \Omega / P(z)\} = \Omega \Leftrightarrow \{z \in \Omega / \neg P(z)\} = \emptyset$$

Démonstration. On a pour tout x ,

$$x \in \{z \in \Omega / P(z)\} \cap \{z \in \Omega / \neg P(z)\} \Leftrightarrow x \in \Omega \text{ et } P(x) \text{ et } \neg P(x) \Leftrightarrow x \in \emptyset$$

et

$$x \in \{z \in \Omega / \neg P(z)\} \cup \{z \in \Omega / P(z)\} \Leftrightarrow x \in \Omega \text{ et } (P(x) \text{ ou } \neg P(x)) \Leftrightarrow x \in \Omega$$

■

Théorème 2.2.4 — Distributivité. Étant donné un ensemble Ω , une proposition dont l'écriture dépend formellement d'un paramètre \square notée $P(\square)$, et une proposition Q , on a

$$(\exists x \in \Omega P(x)) \text{ et } Q \Leftrightarrow \exists x \in \Omega (P(x) \text{ et } Q)$$

et par contraposition et négation

$$(\forall x \in \Omega P(x)) \text{ ou } Q \Leftrightarrow \forall x \in \Omega (P(x) \text{ ou } Q)$$

De plus,

$$(\exists x \in \Omega P(x)) \text{ ou } Q \Leftarrow \exists x \in \Omega (P(x) \text{ ou } Q)$$

et par contraposition et négation

$$(\forall x \in \Omega P(x)) \text{ et } Q \Rightarrow \forall x \in \Omega (P(x) \text{ et } Q)$$

Si en plus Ω n'est pas vide, les deux dernières implications sont des équivalences.

Démonstration. Soit x_0 tel que $P(x_0)$. Si Q est vrai alors la proposition $P(x_0)$ **et** Q aussi d'où $\exists x \in \Omega (P(x) \text{ et } Q)$. Inversement, soit x_0 tel que $P(x_0)$ **et** Q est vrai. Alors $P(x_0)$ est vrai donc $\exists x \in \Omega P(x)$ l'est aussi aussi.

Soit x_0 tel que $P(x_0)$ **ou** Q . On a

$$P(x_0) \Rightarrow (\exists x \in \Omega P(x)) \Rightarrow (\exists x \in \Omega P(x)) \text{ ou } Q$$

$$Q \Rightarrow (\exists x \in \Omega P(x)) \text{ ou } Q$$

Par le théorème ?? :

$$P(x_0) \text{ ou } Q \Rightarrow (\exists x \in \Omega, P(x)) \text{ ou } Q$$

Inversement, supposons $\exists x \in \Omega P(x)$ vrai, soit donc x_0 tel que $P(x_0)$. On a $P(x_0)$ **ou** Q donc $\exists x \in \Omega (P(x) \text{ ou } Q)$ est vrai. Supposons maintenant Q vrai et Ω non vide. Soit x_0 un élément de Ω , on a encore $P(x_0)$ **ou** Q d'où le résultat. ■

2.3 Types de raisonnements

2.3.1 Modus ponens

$$(P \text{ et } (P \Rightarrow Q)) \Rightarrow Q$$

2.3.2 Contraposition ou modus tollens

$$(\neg Q \Rightarrow \neg P) \Rightarrow (P \Rightarrow Q)$$

2.3.3 Par l'absurde

$$P \text{ et } ((P \text{ et } \neg Q) \Rightarrow \text{faux}) \Rightarrow Q$$

2.3.4 Séparation

Le principe repose sur le théorème ?? :

$$((P \text{ et } Q) \Rightarrow R) \Leftrightarrow (P \Rightarrow (Q \Rightarrow R))$$

$$((P \text{ ou } Q) \Rightarrow R) \Leftrightarrow ((P \Rightarrow R) \text{ et } (Q \Rightarrow R))$$

2.3.5 Contre-exemple

Sachant que

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

pour montrer que $\forall x \in \Omega, P(x)$ est fausse, il suffit de trouver $x_0 \in \Omega$ tel que $P(x_0)$ est faux. x_0 est le contre-exemple.

2.3.6 Disjonction des cas

Le principe repose sur

$$\forall x \in \bigcup_{i \in I} \Omega_i P(x) \Leftrightarrow \bigwedge_{i \in I} (\forall x \in \Omega_i P(x))$$

La démonstration est adaptée à l'ensemble Ω_i étudié.

2.3.7 Syllogisme

$$\forall x (x \in \Omega \text{ et } \Omega \subset \Omega' \Rightarrow x \in \Omega')$$

2.3.8 Syllogisme disjonctif

$$((P \text{ ou } Q) \text{ et } \neg P) \Rightarrow Q$$

2.3.9 Dédution

À compléter...


2.3.10 Récurrence

À compléter...

2.3.11 Descente

À compléter...

2.3.12 Abduction

 Ce n'est pas du tout une règle d'inférence logique mais c'est fondamental.

$$((P \Rightarrow Q) \text{ et } Q) \Rightarrow P$$

L'argument pour justifier un tel raisonnement est le suivant : si Q est une proposition complexe et s'il y a très peu de prémisses simples qui l'impliquent, il y a de forte chance que P soit vrai.

2.3.13 Induction

R Ce n'est pas du tout une règle d'inférence logique.


Passer du cas particulier au cas général : voir conjecturer...

$$\exists x \in \Omega, P(x) \Rightarrow \forall x \in \Omega P(x)$$

Extension :

$$\exists \Omega' \subset \Omega, \Omega' \neq \emptyset, \text{ et } \forall x \in \Omega' P(x) \Rightarrow \forall x \in \Omega P(x)$$

Cette proposition est vraie si $\Omega' = \Omega$, pas toujours dans le cas contraire. Dans le doute, on peut se baser sur ce schéma si Ω' est suffisamment grand. Cela peut être une aide pour trouver un raisonnement mathématique rigoureux, ou bien une aide à la prise de décision sans raisonnement mathématique rigoureux. Ce dernier cas intervient de manière essentielle dans la construction du raisonnement chez l'enfant et l'adolescent.



3. Ensembles

3.1 Éléments de théorie des ensembles

Vocabulaire de la théorie des ensembles.

3.1.1 Égalité

Axiome 3.1.1 — Principe de Leibnitz. $P(.)$ étant un prédicat d'une variable

$$\forall x, y, (x = y) \Rightarrow (P(x) \Leftrightarrow P(y))$$

- R** Cela fait un axiome par prédicat... pour pouvoir remplacer dans n'importe quelle expression un objet par un autre qui lui est égal.

3.1.2 Éléments de théorie des ensembles

a Axiomes ZFC (de Zermelo, Fraenkel et du choix)

Pour la culture, voici une liste d'axiomes qui permettent de bâtir correctement la théorie des ensembles. À partir de là, on peut construire l'ensemble des entiers naturels puis les autres ensembles de nombres, avec d'autres axiomes éventuellement.

En général, la rédaction est descriptive puis symbolique. Au début, tous les objets sont des ensembles.

Axiome 3.1.2 — Extensionnalité. Si deux ensembles ont les mêmes

éléments, alors ils sont égaux.

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

- R** C'est bien un axiome et pas une définition car les éléments étant eux-mêmes des ensembles, parler des « mêmes éléments » utilise implicitement l'égalité des ensembles. La réciproque vient simplement du principe de substitution.

Axiome 3.1.3 — Ensemble vide. Il existe un ensemble sans élément. Il est noté \emptyset .

Lemme 3.1.4 L'ensemble vide est unique.

Démonstration. Si x et y sont des ensembles vides, pour tout z on a

$$z \in x \Leftrightarrow \text{faux} \Leftrightarrow z \in y$$

Donc tous les ensembles vides ont les mêmes éléments : ils sont égaux. ■

Axiome 3.1.5 — Paire. Si x et y sont des ensembles, alors il existe un ensemble contenant x et y , et eux seuls comme éléments. Il est noté $\{x, y\}$. $\forall x (\forall y (\forall z (z \in \{x, y\} \Rightarrow (z = x \text{ ou } z = y))))$.

- A** En théorie des ensembles, une paire peut avoir un seul élément : on n'a pas supposé que x et y étaient distincts.

Définition 3.1.1 — Singleton. Un **singleton** est une paire $\{x, x\}$ où x est un ensemble, il est noté $\{x\}$.

Lemme 3.1.6 Un singleton n'est pas vide.

Démonstration. Par définition, $x \in \{x\}$. ■

Théorème 3.1.7 Si x est un ensemble, on a

$$\forall y ((y \in \{x\}) \Rightarrow (y = x)),$$

et

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

Démonstration. Par l'axiome de la paire,

$$\forall y (y \in \{x, x\} \Rightarrow (y = x \text{ ou } y = x) \Rightarrow (y = x))$$

$$\forall y, y' ((y \in \{x\} \text{ et } y' \in \{x\}) \Rightarrow (y = x \text{ et } y' = x) \Rightarrow (y = y')).$$

■

Théorème 3.1.8 Un ensemble non vide E est un singleton si

- 1) $\exists x (\forall y ((y \in E) \Rightarrow (y = x)))$ ou
 2) $\forall y, y' ((y \in E \text{ et } y' \in E) \Rightarrow (y = y'))$

Un ensemble E est un singleton si $\exists! x (x \in E)$.

Démonstration. À compléter.

1) La première proposition entraîne

$$\forall y ((y \in E) \Rightarrow (y = x) \Rightarrow (y \in \{x\}))$$

Avec y_0 dans E , elle entraîne aussi $y_0 = x$, ce qui donne $x \in E$ puis

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

Par l'axiome d'extensionnalité, on obtient $E = \{x\}$.

2) Soit y_0 dans E , la deuxième proposition donne

$$\forall y ((y \in E) \Rightarrow (y = y_0))$$

qui est la première proposition. E est non vide et l'unicité signifie exactement la dernière proposition. ■

Axiome 3.1.9 — Réunion. Pour tout ensemble x , il existe un ensemble qui contient tous les éléments des éléments de x et eux seuls, il est noté $\bigcup_{y \in x} y$:

$$\forall x \left(\forall z \left(z \in \bigcup_{y \in x} y \Leftrightarrow \exists y (z \in y \text{ et } y \in x) \right) \right)$$

Axiome 3.1.10 — Ensemble des parties. Pour tout ensemble x , il existe un ensemble dont les éléments sont les sous-ensembles de x et eux seuls. Il est noté $\mathcal{P}(x)$.

$$\forall x \left(\forall y (y \in \mathcal{P}(x) \Leftrightarrow \forall z (z \in y \Rightarrow z \in x)) \right)$$

Axiome 3.1.11 — Infini. Il existe un ensemble Ω qui contient \emptyset et tel que pour chacun de ses éléments x , Ω contient $x \cup \{x\}$.

$$\exists \Omega ((\emptyset \in \Omega) \text{ et } (\forall x (x \in \Omega \Rightarrow x \cup \{x\} \in \Omega)))$$

Axiome 3.1.12 — Schéma de compréhension. Pour tout ensemble E et toute proposition dont l'écriture dépend formellement d'un paramètre x notée $P(x)$, il existe un ensemble dont les éléments sont les

éléments de E vérifiant P.

$$\forall E \left(\forall P(x) \left(\exists F \left(\forall x \left(x \in F \Leftrightarrow (x \in E \text{ et } P(x)) \right) \right) \right) \right)$$

Terminologie 3.1.1 On le note $\{x \in E \mid P(x)\}$, lu «ensemble des x éléments de E tels que P(x)».

Axiome 3.1.13 — Schéma de remplacement. Pour tout ensemble E et toute relation fonctionnelle \mathcal{R} , formellement définie comme une proposition $x \mathcal{R} y$ et telle que $x \mathcal{R} y$ et $x \mathcal{R} y'$ entraîne $y = y'$, il existe un ensemble contenant les images par \mathcal{R} des éléments de l'ensemble d'origine E et elles seules.

$$\left(\forall E \left(\forall x \mathcal{R} y \left(\forall x \left(\forall y \left(\forall y' \left(x \mathcal{R} y \text{ et } x \mathcal{R} y' \Rightarrow y = y' \right) \right) \right) \right) \Rightarrow \dots \right. \right. \\ \left. \dots \Rightarrow \left(\exists \Omega \left(\forall y \left((y \in \Omega) \Leftrightarrow \exists x \left((x \in E) \text{ et } (x \mathcal{R} y) \right) \right) \right) \right) \right) \right)$$

Axiome 3.1.14 — Fondation. Tout ensemble E non vide contient un élément x qui ne contient aucun élément de E.

$$\forall E \left(\left(\exists x (x \in E) \right) \Rightarrow \left(\exists x \left(\forall y (y \in x \Rightarrow y \notin E) \right) \right) \right)$$

Axiome 3.1.15 — Choix. Étant donné un ensemble E d'ensembles non vides mutuellement disjoints, il existe un ensemble qui contient exactement un élément de chaque élément de E.

La formulation symbolique est laissée en exercice.

R E et F sont des ensembles.

b Comparaison

Définition 3.1.2 — Inclusion des ensembles.

$$E \subset F \stackrel{\text{déf}}{\Leftrightarrow} F \supset E \stackrel{\text{déf}}{\Leftrightarrow} \forall x (x \in E \Rightarrow x \in F)$$

On dit : E est un **sous-ensemble** de F, E est **inclus dans** F ou F **contient** E. **Partie** est synonyme de sous-ensemble.

Définition 3.1.3 — Égalité des ensembles.

$$E = F \stackrel{\text{déf}}{\Leftrightarrow} \forall x (x \in E \Leftrightarrow x \in F)$$

R C'est en réalité un axiome de la théorie des ensembles, voir l'axiome 3.1.2 d'extensionnalité.

Théorème 3.1.16 — Double inclusion.

$$E = F \iff E \subset F \text{ et } F \subset E$$

Démonstration. On a $(x \in E \iff x \in F) \iff ((x \in E \Rightarrow x \in F) \text{ et } (x \in F \Rightarrow x \in E))$.

À compléter... ■

Définition 3.1.4 — Partie stricte.

$$E \subsetneq F \stackrel{\text{déf}}{\iff} F \supsetneq E \stackrel{\text{déf}}{\iff} \forall x (x \in E \Rightarrow x \in F) \text{ et } \exists y (y \notin E \text{ et } y \in F)$$

On dit : E est un **sous-ensemble strict** de F, E est **inclus strictement** dans F ou F **contient strictement** E.

Lemme 3.1.17 Il n'existe pas de partie stricte de \emptyset .

Démonstration. De la définition précédente, on déduit

$$(\forall x (x \in E \Rightarrow x \in F) \text{ et } \exists y (y \notin E \text{ et } y \in F)) \Rightarrow \exists y (y \in F) \Rightarrow F \neq \emptyset$$

d'où le résultat par contraposition. ■

c Opérations binaires

Définition 3.1.5 — Union et intersection. Pour tout x

$$x \in E \cup F \stackrel{\text{déf}}{\iff} x \in E \text{ ou } x \in F$$

$$x \in E \cap F \stackrel{\text{déf}}{\iff} x \in E \text{ et } x \in F$$

\cup se lit **union** ou **réunion**, \cap se lit **inter** ou **intersection**. «L'union (ou la réunion) de E et F» désigne $E \cup F$, «l'intersection de E et F» désigne $E \cap F$.

R Pour des définitions en compréhension, on a

$$\{x \in E \mid P(x)\} \cup \{x \in E \mid P'(x)\} = \{x \in E \mid P(x) \text{ ou } P'(x)\}$$

$$\{x \in E \mid P(x)\} \cap \{x \in E \mid P'(x)\} = \{x \in E \mid P(x) \text{ et } P'(x)\}$$

Théorème 3.1.18 Pour tout ensemble E et toute proposition dont l'écriture dépend formellement d'un paramètre x notée P(x),

$$\{x \in E \mid P(x)\} \cup \{x \in E \mid \text{non } P(x)\} = E$$

$$\{x \in E \mid P(x)\} \cap \{x \in E \mid \text{non } P(x)\} = \emptyset$$

Démonstration. On a

$$\begin{aligned} x \in \{x \in E \mid P(x)\} \cup \{x \in E \mid \neg P(x)\} &\Leftrightarrow (x \in E \wedge P(x)) \vee (x \in E \wedge \neg P(x)) \\ &\Leftrightarrow x \in E \wedge (P(x) \vee \neg P(x)) \\ &\Leftrightarrow x \in E \end{aligned}$$

$$\begin{aligned} x \in \{x \in E \mid P(x)\} \cap \{x \in E \mid \neg P(x)\} &\Leftrightarrow (x \in E \wedge P(x)) \wedge (x \in E \wedge \neg P(x)) \\ &\Leftrightarrow x \in E \wedge (P(x) \wedge \neg P(x)) \\ &\Leftrightarrow x \in \emptyset \end{aligned}$$

■

Théorème 3.1.19 — Propriétés. \cup et \cap sont des opérations commutatives et associatives. $E \cap F = F \cap E$ et $E \cup F = F \cup E$. $E \cap (F \cap G) = (E \cap F) \cap G$ et $E \cup (F \cup G) = (E \cup F) \cup G$

1) \emptyset est élément neutre de \cup et élément absorbant de \cap ,

2) \cup est distributive par rapport à \cap :

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

3) \cap est distributive par rapport à \cup :

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

4) \cup et \cap sont croissantes par rapport à chacun de leurs arguments :

$$F \subset G \Rightarrow (E \cap F \subset E \cap G \text{ et } E \cup F \subset E \cup G)$$

Démonstration.

1) Pour la commutativité de la réunion : pour tout x

$$x \in E \cup F \stackrel{\text{déf}}{\Leftrightarrow} x \in E \text{ ou } x \in F \Leftrightarrow x \in F \text{ ou } x \in E \stackrel{\text{déf}}{\Leftrightarrow} x \in F \cup E$$

De même pour l'intersection par commutativité de **et**.

2) Pour l'associativité de la réunion : pour tout x

$$\begin{aligned} x \in E \cup (F \cup G) &\Leftrightarrow x \in E \text{ ou } x \in F \cup G \\ &\Leftrightarrow x \in E \text{ ou } (x \in F \text{ ou } x \in G) \\ &\Leftrightarrow (x \in E \text{ ou } x \in F) \text{ ou } x \in G \\ &\Leftrightarrow x \in E \cup F \text{ ou } x \in G \\ &\Leftrightarrow x \in (E \cup F) \cup G \end{aligned}$$

De même pour l'intersection par associativité de **et**

3) Élément neutre : pour tout x

$$x \in E \cup \emptyset \stackrel{\text{déf}}{\iff} x \in E \text{ **ou** } x \in \emptyset \iff x \in E$$

On rappelle que $x \in \emptyset$ est toujours **faux**.

4) Élément absorbant : pour tout x

$$x \in E \cap \emptyset \stackrel{\text{déf}}{\iff} x \in E \text{ **et** } x \in \emptyset \iff x \in \emptyset$$

5) Distributivités : deux versions en prenant d'abord l'opérateur au dessus, puis celui qui est dessous. Pour tout x

$$\begin{aligned} x \in E \cup (F \cap G) &\iff x \in E \text{ **ou** } x \in F \cap G \\ &\iff x \in E \text{ **ou** } (x \in F \text{ **et** } x \in G) \\ &\iff (x \in E \text{ **ou** } x \in F) \text{ **et** } (x \in E \text{ **ou** } x \in G) \\ &\iff x \in E \cup F \text{ **et** } x \in E \cup G \\ &\iff x \in (E \cup F) \cap (E \cup G) \end{aligned}$$

6) Croissance : même convention que ci-dessus. On suppose $F \subset G$. Pour tout x

$$x \in E \cap F \implies x \in E \text{ **et** } x \in F \implies x \in E \text{ **et** } x \in G \implies x \in E \cap G$$

■

Définition 3.1.6 — Partition. Une partition de E est une partie P de $\mathcal{P}(E)$ dont les éléments sont non vides, mutuellement disjoints et ont pour réunion E , *id est*

- 1) $\forall F \in P, F \neq \emptyset$
- 2) $\forall F, G \in P, (F \neq G) \implies (F \cap G = \emptyset)$
- 3) $E = \bigcup_{F \in P} F.$

Les éléments de P sont ses **composantes**.

Définition 3.1.7 — Différence. Pour tout x

$$x \in E \setminus F \stackrel{\text{déf}}{\iff} x \in E \text{ **et** } x \notin F$$

Si E contient F , $E \setminus F$ est le **complémentaire** de F dans E .

d Produit cartésien

Définition 3.1.8 — Couple, composante. Pour tous x et y , (x, y) est un **couple**. x et y en sont les **composantes**, x en est la **première composante** et y en est la **deuxième composante**. Pour tous x' et y' ,

$$(x, y) = (x', y') \stackrel{\text{déf}}{\iff} x = x' \text{ **et** } y = y'$$

Dans le contexte de la géométrie, l'abscisse est synonyme de la première composante et l'ordonnée est synonyme de la deuxième composante.

- R** En théorie des ensembles avancée, on a $(x, y) \stackrel{\text{déf}}{=} \{\{x\}, \{x, y\}\}$. L'existence du deuxième membre repose sur l'*axiome de la paire*, son unicité repose sur l'*axiome d'extensionnalité*.

Définition 3.1.9 — Produit cartésien. E et F étant des ensembles, le **produit cartésien** de E par F, noté $\mathbf{E} \times \mathbf{F}$, est l'ensemble de tous les couples dont la première composante est dans E et la deuxième dans F.

Exercice 1. Montrer que le produit cartésien est associatif, mais pas commutatif.

4. Applications

4.1 Applications

4.1.1 Généralités

Dans la suite E, F, G, \dots désignent des ensembles quelconques dont les propriétés sont précisées selon les besoins.

Définition 4.1.1 — Application. Une **application** f est la donnée de

- un ensemble E , l'**ensemble de départ**,
- un ensemble F , l'**ensemble d'arrivée**,
- une partie Γ de $E \times F$, le **graphe**, telle que

$$\forall x \in E, \exists ! y \in F, (x; y) \in \Gamma$$

Pour $(x; y)$ de Γ , y est l'**image** de x par f , notée $f(x)$. x est un **antécédent** de y par f , l'ensemble de tous les antécédents de y est noté $f^{-1}(y)$, c'est l'**image réciproque** ou **pré image** de y par f . y est **associé** à x par f .

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

Définition 4.1.2 L'ensemble des applications de E dans F est noté F^E .

$f : E \rightarrow F$ désigne une application de E dans F nommée f . On peut rencontrer la notation $f : E \hookrightarrow F$.

$$\begin{array}{ccc} f : E & \longrightarrow & F \\ x & \longmapsto & \text{une formule} \end{array}$$

désigne l'application de E dans F nommée f qui à x associe une formule.

Théorème 4.1.1 Il n'existe qu'une seule application de \emptyset dans F , son graphe est \emptyset . On la désigne par **application vide**.

Démonstration. En exercice... ■

Théorème 4.1.2 — Application de choix. Étant donnée une partition P de E , il existe une application de choix $\varphi : P \rightarrow E$ telle que pour tout F de P , on a $\varphi(F) \in F$.

Démonstration. L'axiome du choix appliqué à la partition P donne un ensemble G qui contient un seul élément par composante de la partition. $\{(x; y) \mid x \in P \text{ et } y \in x \cap E\}$ est un graphe qui répond à la question. À détailler... ■

Définition 4.1.3 — Prolongement, restriction. Soit $f : E \rightarrow F$ et $g : G \rightarrow F$, de graphes respectifs Γ_f et Γ_g . f est une **restriction** de g ou g est un **prolongement** de f signifie que $E \subset G$ et $\Gamma_f \subset \Gamma_g$. g est aussi notée $f|_G$, lu « f restreinte à G ».

R On garde le même ensemble d'arrivée.

4.1.2 Injection

Définition 4.1.4 — Injection. E et F étant des ensembles, une application f de E dans F est **injective** ou de manière synonyme une **injection** signifie que

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

ou par contraposition

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

L'ensemble des injections de E dans F est noté $I(E; F)$.

Théorème 4.1.3 Une application vide est injective.

Démonstration. En exercice... ■

Théorème 4.1.4 Toute restriction d'une injection est une injection.

Démonstration. En exercice... ■

Définition 4.1.5 — Image réciproque. E et F étant des ensembles, f une application de E dans F. Pour un ensemble G, l'**image réciproque** de G par f est $\{x \in E | \exists y \in G, y = f(x)\}$, notée $f^{-1}(G)$.

R $f^{-1}(G)$ est $f^{-1}(y)$ si G est le singleton $\{y\}$.

Théorème 4.1.5 — Image réciproque. E et F étant des ensembles, f une application de E dans F. Pour un ensemble G,

$$\{x \in E | \exists y \in G, y = f(x)\} = \bigcup_{y \in G} f^{-1}(y)$$

C'est l'**image réciproque** ou **pré image** de G par f , notée $f^{-1}(G)$, c'est aussi $f^{-1}(y)$ si G est le singleton $\{y\}$.

Démonstration. En exercice... ■

Théorème 4.1.6 Une application f est une injection si et seulement si pour tout y , $f^{-1}(y)$ est vide ou un singleton.

Démonstration. S'il n'est pas vide, $f^{-1}(y)$ contient x_0 et par définition de l'image réciproque, $y = f(x_0)$. Comme f est injective, en particulier

$$\forall x \in E, (x \in f^{-1}(y) \xrightarrow{\text{déf}} f(x) = y \Rightarrow x = x_0)$$

d'où $f^{-1}(y)$ est le singleton $\{x_0\}$. ■

Définition 4.1.6 — Injection canonique. Étant donné $F \subset E$, l'**injection canonique** de F dans E est l'application qui à tout élément associe lui-même.

Définition 4.1.7 L'injection canonique est une injection.

Démonstration. En exercice... ■

Définition 4.1.8 — Ensemble infini. Un ensemble E est infini s'il existe une injection de lui-même dans un de ses sous-ensembles stricts :

$$E \text{ est infini} \stackrel{\text{déf}}{\iff} \exists F \subsetneq E, \exists \Phi : E \hookrightarrow F$$

Définition 4.1.9 — Ensemble dénombrable). Un ensemble E est **dénombrable** signifie qu'il existe une injection de E dans \mathbb{N} .

Exercice 4.1 \mathbb{N}^2 est dénombrable, on vérifie que $(m, n) \mapsto 2^m 3^n$ est une injection de \mathbb{N}^2 dans \mathbb{N} . Généraliser à \mathbb{N}^k , $k \in \mathbb{N}$. \mathbb{R} et $\mathbb{N}^{\mathbb{N}}$ ne sont pas dénombrables. ■

4.1.3 Surjection

Définition 4.1.10 — Surjection. E et F étant des ensembles, une application f de E dans F est **surjective**, ou de manière synonyme une **surjection**, signifie que $\forall y \in F, \exists x \in E, y = f(x)$.

R Pour une formulation textuelle : tout élément de l'ensemble d'arrivée a au moins un antécédent.

Théorème 4.1.7 L'application vide de \emptyset dans lui-même est surjective.

Démonstration. En exercice... ■

Théorème 4.1.8 Une application f est une surjection si et seulement si pour tout y de son ensemble d'arrivée, $f^{-1}(y)$ n'est pas vide.

Démonstration. On a $\exists x \in E, y = f(x) \stackrel{\text{déf}}{\iff} f^{-1}(y) \neq \emptyset$. ■

Proposition 4.1.9 Tout prolongement d'une surjection est une surjection.

Démonstration. En exercice... ■

Définition 4.1.11 — Image. Soit $G \subset E$ et $f : E \rightarrow F, \{y \in F | \exists x \in G, y = f(x)\}$ est l'**image** de G par f , noté $f(G)$. L'**image** de f est $f(E)$ aussi notée $\mathcal{I}f$.

Théorème 4.1.10 Une application f de E dans F est surjective si et seulement si $\mathcal{I}f = F$.

Démonstration. En exercice... ■

4.1.4 Bijection

Définition 4.1.12 — Bijection. E et F étant des ensembles, une application f de E dans F est **bijjective** ou de manière synonyme une **bijection** si

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

Théorème 4.1.11 L'application vide de \emptyset dans lui-même est bijective.

Démonstration. En exercice... ■

Théorème 4.1.12 L'application de E dans E qui à tout élément associe lui-même est une bijection, elle est notée Id_E .

Démonstration. À compléter... ■

Définition 4.1.13 E et F sont en bijection, ou **équipotents**, signifie qu'il existe une bijection de E sur F .

Théorème 4.1.13 Une application f est une bijection si et seulement si pour tout y de son ensemble d'arrivée, $f^{-1}(y)$ est un singleton.

Démonstration. On a $\exists ! x \in E, y = f(x) \iff f^{-1}(y)$ est un singleton. ■

Théorème 4.1.14 Toute injection induit une bijection sur son image.

Démonstration. Soit $f : E \rightarrow F$. Son graphe Γ , en tant que partie de $E \times \mathcal{I}f$, définit une application de E dans $\mathcal{I}f$, qui est une bijection. À compléter... ■

Théorème 4.1.15 Une application est une bijection si et seulement si c'est une injection et une surjection.

Démonstration. C'est une application des lemmes ?? et ??. ■

Théorème 4.1.16 Étant donnés a et b de E ,

$$\begin{aligned} \tau : E &\longrightarrow E \\ x &\longmapsto \begin{cases} a & \text{si } x = b \\ b & \text{si } x = a \\ x & \text{sinon} \end{cases} \end{aligned}$$

τ est une bijection.

Démonstration. En exercice... ■

4.1.5 Composition

Définition 4.1.14 — Composition. E , F et G étant des ensembles, f étant une application de E dans F et g une application de F dans G , l'application $x \mapsto g(f(x))$ est notée $g \circ f$, c'est l'application **composée**.

de g par f .

Théorème 4.1.17 La composition est associative : $(h \circ g) \circ f = h \circ (g \circ f)$.

Démonstration. On a $(h \circ g) \circ f(x) = (h \circ g)(f(x)) = h(g(f(x))) = h((g \circ f)(x)) = h \circ (g \circ f)(x)$. ■

R La composition n'est pas commutative. En général, on a trois ensembles de départ ou d'arrivée mutuellement différents, pour avoir la commutativité, il en faut nécessairement deux au total et pas plus.

Théorème 4.1.18 1) La composée de deux applications injectives est injective.

2) La composée de deux applications surjectives est surjective.

3) La composée de deux applications bijectives est bijective.

Démonstration.

1) On a $x \neq y \Rightarrow f(x) \neq f(y) \Rightarrow g(f(x)) \neq g(f(y))$.

2) Avec les notations de la définition de composition, on a $\forall z \in G, \exists y_z \in F, z = g(y_z)$ et $\forall y \in F, \exists x_y \in E, y = f(x_y)$. En particulier, $z = g \circ f(x_{y_z})$.

3) Par les points précédents ainsi que la proposition ??.

Définition 4.1.15 — Application réciproque, à gauche, à droite.

E et F étant des ensembles, f étant une application de E dans F et g une application de F dans E .

1) g est **réciproque à gauche** de f signifie que $g \circ f = \text{Id}_E$.

2) g est **réciproque à droite** de f signifie que $f \circ g = \text{Id}_F$.

3) g est **réciproque** de f signifie g est à la fois réciproque à gauche et réciproque à droite de f .

Théorème 4.1.19 1) Toute application injective admet une réciproque à gauche.

2) Toute application surjective admet une réciproque à droite.

3) Toute application bijective admet une réciproque, qui est unique et à la fois réciproque à gauche et à droite.

Démonstration. On note $f : E \rightarrow F$, $g : F \rightarrow E$, Γ_f le graphe de f et Γ_g celui de g . Soit $G \stackrel{\text{déf}}{=} \{(y; x) \mid (x; y) \in \Gamma_f\}$. On laisse en exercice le cas où l'un des deux ensembles est vide. À compléter...

1) Si f est injective. Soit $x_0 \in E$ et $G' \stackrel{\text{déf}}{=} \{(y; x_0) \mid y \notin \mathcal{I}F\}$, $G \cup G'$ est le graphe d'une application réciproque à gauche de f . À compléter...

2) Si f est surjective. Par l'axiome du choix, il existe une application φ qui à tout y associe l'un de ses éléments. L'application φ est un inverse à droite de f .

Si E est dénombrable, il peut être muni d'une relation d'ordre total¹ ce qui permet d'éviter l'axiome du choix : on prend $\varphi : y \mapsto \min f^{-1}(y)$.
 3) Si f est bijective, on a une réciproque à gauche et une réciproque à droite : $g \circ f = \text{Id}_E$ et $f \circ g' = \text{Id}_F$. Par associativité, $g = g \circ (f \circ g') = (g \circ f) \circ g' = g'$, donc g est réciproque de f , mais aussi réciproque à gauche et à droite. L'unicité vient de $g \circ f = h \circ f = \text{Id} \Rightarrow (g \circ f) \circ g = (h \circ f) \circ g \Rightarrow g \circ (f \circ g) = h \circ (f \circ g) \Rightarrow g = h$. ■

Définition 4.1.16 On note f^{-1} la réciproque de f .

Théorème 4.1.20 1) Si $g \circ f$ est injective alors f est injective.

2) Si $g \circ f$ est surjective, alors g est surjective.

3) Si $g \circ f$ est bijective, $g|_{\mathcal{I}f}$ est une bijection.

Démonstration.

1) Si f n'est pas injective, on a $f(x) = f(x')$ avec $x \neq x'$, d'où $g \circ f(x) = g \circ f(x')$ et $g \circ f$ n'est pas injective. On a le résultat par contraposition.

2) Notons $f : E \rightarrow F$ et $g : G \rightarrow H$. Si $g \circ f$ est surjective, on a $g(f(E)) = H$. Comme on a $f(E) \subset F$, on a aussi $g(f(E)) \subset g(F)$. Cela donne $H \subset g(F) \subset H$ puis $g(F) = H$ et la surjectivité de g .

3) Par 1, f est injective, soit f_b la bijection qu'elle induit sur $\mathcal{I}f$. On a $g \circ f = g|_{\mathcal{I}f} \circ f_b$ et $g|_{\mathcal{I}f} = (g \circ f) \circ f_b^{-1}$ qui est la composée de deux bijections. ■

Théorème 4.1.21 1) Toute application qui admet une réciproque à gauche est injective.

2) Toute application qui admet une réciproque à droite est surjective.

3) Toute application qui admet une réciproque est bijective.

Démonstration. Si on a $g \circ f = \text{Id}_E$, sachant que Id_E est à la fois injective et surjective, g est surjective et f injective. Si on a en plus $f \circ g = \text{Id}_F$, g est aussi injective et f surjective, les deux sont des bijections. ■

Théorème 4.1.22 Une réciproque à gauche est surjective, une réciproque à droite injective.

Démonstration. En exercice... ■

1. À détailler...

5. Nombres entiers naturels

5.1 Nombres entiers naturels

Construction de \mathbb{N} .

5.1.1 Présentation axiomatique

a Définition

Définition 5.1.1 \mathbb{N} est un ensemble dont les éléments sont appelés **entiers naturels**.

Axiome 5.1.1 — de Peano.

P1) 0 est un entier naturel, lu « zéro ».

P2) Tout entier naturel n a un unique **successeur** noté n_+ .

P3) Aucun entier naturel n'a 0 pour successeur.

P4) Deux entiers naturels ayant même successeur sont égaux.

P5) Récurrence. Si un ensemble d'entiers naturels contient 0 et contient le successeur de chacun de ses éléments alors cet ensemble est égal à \mathbb{N} .

$$\left\{ \begin{array}{l} E \subset \mathbb{N} \\ 0 \in E \\ \forall n \in \mathbb{N}, n \in E \Rightarrow n_+ \in E \end{array} \right. \Rightarrow E = \mathbb{N}$$

R On peut reformuler ces axiomes en utilisant la notion d'application.

Définition 5.1.2 $\mathbb{N}^* \stackrel{\text{déf}}{=} \mathbb{N} \setminus \{0\}$, lu « n étoile ».

Définition 5.1.3 **Suivant** est synonyme de **successeur**. p **succède à** q signifie que p est le successeur de q .

Définition 5.1.4 — Nombres.

- $1 \stackrel{\text{déf}}{=} 0_+$, lu « un »,
- $2 \stackrel{\text{déf}}{=} 1_+$, lu « deux »,
- $3 \stackrel{\text{déf}}{=} 2_+$, lu « trois »,
- $4 \stackrel{\text{déf}}{=} 3_+$, lu « quatre »,
- $5 \stackrel{\text{déf}}{=} 4_+$, lu « cinq »,
- $6 \stackrel{\text{déf}}{=} 5_+$, lu « six »,
- $7 \stackrel{\text{déf}}{=} 6_+$, lu « sept »,
- $8 \stackrel{\text{déf}}{=} 7_+$, lu « huit »,
- $9 \stackrel{\text{déf}}{=} 8_+$, lu « neuf ».

Notation 5.1.1 n_+ est noté $n + 1$

b Principe de récurrence

Si un ensemble E inclus dans \mathbb{N} est donné en compréhension, *id est* $E \stackrel{\text{déf}}{=} \{n \in \mathbb{N} \mid P(n)\}$, E contient n signifie $P(n)$ est vraie : on spécialise l'axiome P5.

Axiome 5.1.2 — Récurrence. Si $P(0)$ est vraie et si pour tout entier naturel n , $P(n) \Rightarrow P(n + 1)$ est vraie alors pour tout entier naturel n , $P(n)$ est vraie.



Ceci n'est pas un théorème, c'est exactement l'axiome P5 dans le cas particulier des ensembles définis en compréhension.

Théorème 5.1.3 Pour démontrer $\forall n \in \mathbb{N}, P(n)$,

- 1) on démontre $P(0)$, c'est **l'initialisation**,
- 2) on démontre $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n + 1)$, c'est **l'hérédité**.

Théorème 5.1.4 — Récurrence à deux niveaux. Si

- 1) $P(0)$ est vraie,
 - 2) $P(1)$ est vraie et
 - 3) pour tout entier naturel n , on a $P(n)$ **et** $P(n + 1) \Rightarrow P(n + 2)$ est vraie
- alors pour tout entier naturel n , $P(n)$ est vraie.

Démonstration. Soit $Q(n) \stackrel{\text{déf}}{=} P(n)$ et $P(n + 1)$. On a $Q(0) = P(0)$ et $P(1)$,
 $(P(n) \text{ et } P(n + 1) \Rightarrow P(n + 2)) \Leftrightarrow (P(n) \text{ et } P(n + 1) \Rightarrow P(n + 1) \text{ et } P(n + 2))$

ainsi que $\forall k \in \mathbb{N}, P(n) \Leftrightarrow \forall k \in \mathbb{N}, Q(n)$. Donc les deux formulations de récurrence sont équivalentes. ■

R Les récurrences à plus de niveaux sont laissées en exercice.

Si nous anticipons sur la définition de la relation d'ordre, nous avons

Théorème 5.1.5 — Récurrence forte. Si $P(0)$ est vraie et si pour tout entier naturel n , $(\forall 0 \leq k \leq n, P(k)) \Rightarrow P(n+1)$ est vraie alors pour tout entier naturel n , $P(n)$ est vraie.

Démonstration. Soit $Q(n) \stackrel{\text{déf}}{=} (\forall 0 \leq k \leq n, P(k))$. On a $Q(0) = P(0)$,

$$\begin{aligned} (\forall 0 \leq k \leq n, P(k)) &\Rightarrow P(n+1) \\ &\Leftrightarrow (\forall 0 \leq k \leq n, P(k)) \Rightarrow (\forall 0 \leq k \leq n+1, P(k)) \\ &\Leftrightarrow Q(n) \Rightarrow Q(n+1) \end{aligned}$$

ainsi que $(\forall n \in \mathbb{N}, P(n)) \Leftrightarrow (\forall n \in \mathbb{N}, Q(n))$. Donc les deux formulations de récurrence sont équivalentes. ■

Définition 5.1.5 Un prédécesseur de n est un entier naturel, noté n_- , dont le successeur est n .

Théorème 5.1.6 Tout entier naturel n admet au plus un prédécesseur.

Démonstration. Par définition, deux prédécesseurs de n ont le même successeur n . Par l'axiome P4 ils sont égaux. ■

Théorème 5.1.7 Tout entier naturel est le prédécesseur de son successeur.

$$\forall n \in \mathbb{N}, n = (n_+)_-$$

Corollaire 5.1.8 En particulier, tout successeur admet un prédécesseur.

Démonstration. Par définition du prédécesseur on a $((n_+)_-)_+ = n_+$, ainsi n et $(n_+)_-$ ont pour successeur n_+ , ils sont donc égaux par l'axiome P4. ■

Théorème 5.1.9 Les entiers naturels non nuls sont les successeurs.

Corollaire 5.1.10 En particulier, tout entier naturel non nul admet un prédécesseur.

Démonstration. Soit E l'ensemble des entiers naturels successeurs et $F \stackrel{\text{déf}}{=} \{0\} \cup E$. Par l'axiome P2, tout élément de F admet un successeur qui est dans E et *a fortiori* dans F . Ainsi, F est une partie de \mathbb{N} qui contient 0 et le successeur de chacun de ses éléments, c'est donc \mathbb{N} lui-même par l'axiome P5. Par l'axiome P3, E ne contient pas 0, donc $\mathbb{N} \setminus \{0\} = (\{0\} \cup E) \setminus \{0\} = \emptyset \cup (E \setminus \{0\}) = E$. ■

Théorème 5.1.11 Tout entier naturel non nul est le successeur de son prédécesseur.

$$\forall n \in \mathbb{N}^*, n = (n_-)_+$$

Démonstration.

C'est une application directe de la définition et des lemmes précédents. ■

Théorème 5.1.12 L'application $n \mapsto n_+$ est une bijection de \mathbb{N} sur \mathbb{N}^* , elle est **nommée décalage à droite**. Sa réciproque est nommée **décalage à gauche**.

Démonstration. Immédiat. À préciser... ■

Définition 5.1.6 Soit E une partie de \mathbb{N} , p est un **élément minimal** de E signifie qu'il appartient à E et que son prédécesseur, s'il existe, n'appartient pas à E .

E admet un élément minimal signifie qu'il existe un élément minimal de E .

► Exemples 5.1

- 1) Si E contient 0, celui-ci est minimal.
- 2) Dans l'ensemble des entiers naturels pairs, tout entier est minimal. ▲

Théorème 5.1.13 Toute partie non vide de \mathbb{N} contient un élément minimal.

Démonstration. Soit E une telle partie. Si E contient 0, c'est immédiat. Sinon le complémentaire de E contient 0, mais n'est pas \mathbb{N} : par l'axiome P5 il ne peut pas contenir le successeur de chacun de ses éléments. Il existe donc un entier qui n'appartient pas à E mais dont le successeur appartient à E . Ce successeur est un élément minimal de E . ■



Le théorème suivant est **fondamental** ! Il est utilisé notamment pour les suites récurrentes. La preuve de l'unicité est facile, celle de l'existence est plus technique sans être réellement difficile.

Théorème 5.1.14 — Définition par récurrence. Soit un ensemble E qui contient a et $H : \mathbb{N} \times E \rightarrow E$. Il existe une application f de \mathbb{N} dans E , et une seule, telle que

- 1) $f(0) = a$
- 2) $\forall n \in \mathbb{N}, f(n_+) = H(n, f(n))$.

Démonstration.

1) Unicité. Soient f_1 et f_2 de telles applications et

$$F \stackrel{\text{déf}}{=} \{n \in \mathbb{N} \mid f_1(n) = f_2(n)\}$$

Par la propriété 1) du théorème, $f_1(0) = a = f_2(0)$ donc F contient 0. Par la propriété 2),

$$f_1(n) = f_2(n) \Rightarrow H(n, f_1(n)) = H(n, f_2(n)) \Rightarrow f_1(n_+) = f_2(n_+)$$

et F contient le successeur de chacun de ses éléments. Par l'axiome de récurrence, F vaut \mathbb{N} et $f_1 = f_2$.

2) Existence : par construction du graphe. On considère les parties M de $\mathbb{N} \times E$ qui ont les deux propriétés suivantes :

- $(0, a) \in M$
- $(n, y) \in M \Rightarrow (n_+, H(n, y)) \in M$.

$\mathbb{N} \times E$ est un tel ensemble. L'intersection Γ de tous ces ensembles a encore ces propriétés et c'est le plus petit sous-ensemble de $\mathbb{N} \times E$ qui les a. Montrons que c'est le graphe d'une application.

On considère $F \stackrel{\text{déf}}{=} \{n \in \mathbb{N} \mid \exists y \in E, (n, y) \in \Gamma\}$. F contient 0 puisque $(0, a) \in \Gamma$. Si F contient n , alors $(n, y) \in \Gamma$ pour un certain y de E et par la propriété 2) on a $(n_+, H(n, y)) \in \Gamma$, donc F contient n_+ . Ainsi, F vaut \mathbb{N} et $\forall n \in \mathbb{N}, \exists y \in E, (n, y) \in \Gamma$.

On considère maintenant

$$F \stackrel{\text{déf}}{=} \{n \in \mathbb{N} \mid \exists y, z \in E, y \neq z, (n, y) \in \Gamma, (n, z) \in \Gamma\}.$$

Si F contient 0, on a $(0, x) \in \Gamma$ avec $x \neq a$. $\Gamma \setminus \{(0, x)\}$ a les deux propriétés ci-dessus et il est strictement inclus dans Γ , ce qui contredit la minimalité de Γ . Donc F ne contient pas 0.

Si F n'est pas vide, il admet un élément minimal non nul p . Comme p_- n'est pas dans F , il existe un unique t tel que $(p_-, t) \in \Gamma$. Comme p est dans F , on a $(p, x) \in \Gamma$ avec $x \neq H(p_-, t)$. Puisque $(0, a) \neq (p, x)$, $\Gamma \setminus \{(p, x)\}$ contient $(0, a)$. De plus, si $\Gamma \setminus \{(p, x)\}$ contient (n, y) alors on a

$$(n_+, H(n, y)) = (p, z) \Rightarrow \begin{cases} n = p_- \\ y = t \\ z \neq x \end{cases}$$

c'est-à-dire $\Gamma \setminus \{(p, x)\}$ contient $(n_+, H(n, y))$. $\Gamma \setminus \{(p, x)\}$ a les deux propriétés ci-dessus et il est strictement inclus dans Γ , cela contredit la minimalité de Γ .

Donc F est vide et Γ est le graphe d'une application f de \mathbb{N} dans E pour laquelle on a bien $f(0) = a$, $f(n_+) = H(n, f(n))$ pour chaque entier n . ■

Théorème 5.1.15 — Intervalles entiers. Il existe une unique application de \mathbb{N} dans $\mathcal{P}(\mathbb{N})$, notée $n \mapsto \llbracket 0; n \rrbracket$ telle que

- 1) $\llbracket 0; 0 \rrbracket = \{0\}$,
- 2) $\forall n \in \mathbb{N}, \llbracket 0; n_+ \rrbracket = \llbracket 0; n \rrbracket \cup \{n_+\}$.

Démonstration. On applique le théorème de définition par récurrence à $a = \{0\}$, $E = \mathcal{P}(\mathbb{N})$ et $H(n, y) \stackrel{\text{déf}}{=} y \cup \{n_+\}$. ■

Lemme 5.1.16 $\mathbb{N} = \bigcup_{n=0}^{\infty} \llbracket 0; n \rrbracket$

Démonstration. C'est immédiat. ■

5.1.2 Addition des entiers naturels

a Définition

Théorème 5.1.17 Pour tout entier naturel n , il existe une unique application de \mathbb{N} dans \mathbb{N} , notée $p \mapsto +_n(p)$ telle que

- 1) $+_n(0) = n$,
- 2) $\forall p \in \mathbb{N}, +_n(p_+) = (+_n(p))_+$.

Démonstration. C'est une définition par récurrence. À compléter. ■

Proposition 5.1.18

- 1) $\forall p \in \mathbb{N}, +_0(p) = p$,
- 2) $\forall p \in \mathbb{N}, +_1(p) = p_+ = p + 1$,

Démonstration. À compléter. ■

Définition 5.1.7 — addition des entiers naturels.

$$\forall n, p \in \mathbb{N}, n + p \stackrel{\text{déf}}{=} +_n(p)$$

b Propriétés

Théorème 5.1.19

- 1) Élément neutre : $\forall n \in \mathbb{N}, n + 0 = 0 + n = n$
- 2) Successeur : $\forall n \in \mathbb{N}, n_+ = n + 1 = 1 + n$
- 3) Associativité : $\forall p, q, r \in \mathbb{N}, (p + q) + r = p + (q + r)$
- 4) Commutativité : $\forall p, q \in \mathbb{N}, p + q = q + p$
- 5) $\forall p, q \in \mathbb{N}, p + q = 0 \Leftrightarrow p = q = 0$

6) Régularité : $\forall p, q, r \in \mathbb{N}, p + r = q + r \Rightarrow p = q$

R

- Par 1), 2), 4) et 6), $(\mathbb{N}, +)$ est un **monoïde régulier commutatif**.
- Par 2), la notation 5.1.1 est consistante avec la définition ??

Démonstration.

1) Par le théorème 5.1.17, pour tout entier naturel n , on a $n + 0 = n$. L'autre égalité se montre par récurrence. On a $0 + 0 = 0$ et $0 + n = n \Rightarrow n_+ = (0 + n)_+ = 0 + n_+$

2) Pour la première égalité, $n_+ = (n + 0)_+ = n + (0_+) = n + 1$. Par récurrence pour la deuxième, $0 + 1 = 1 + 0 = 1$ et

$$n + 1 = 1 + n \Rightarrow (n + 1) + 1 = (1 + n) + 1 = 1 + (n + 1)$$

3) Par récurrence sur r . Initialisation : $(p + q) + 0 = p + q = p + (q + 0)$. Hérédité : si on a $(p + q) + r = p + (q + r)$, alors

$$(p + q) + r_+ = ((p + q) + r)_+ = (p + (q + r))_+ = p + (q + r)_+ = p + (q + r_+)$$

4) Par récurrence sur p à n fixé. Initialisation : voir 1) ci-dessus. Hérédité : si on a $n + p = p + n$, alors

$$n + (p + 1) = (n + p) + 1 = (p + n) + 1 = p + (n + 1) = p + (1 + n) = (p + 1) + n$$

5) $0 + 0 = 0$ donne un sens de l'équivalence. Par ailleurs, si q est un successeur, $p + q$ aussi. Par contraposition, si $p + q$ est nul alors q aussi. Il en va de même pour p par commutativité.

6) Par récurrence sur r . Initialisation : immédiat. Hérédité : essentiellement

$$p + (r + 1) = q + (r + 1) \Rightarrow (p + r) + 1 = (q + r) + 1 \Rightarrow p + r = q + r.$$

■

Proposition 5.1.20 On obtient une égalité vraie en ajoutant membre à membre des égalités vraies.

Démonstration. Par le principe de Leibnitz,

$$\begin{cases} a = b \\ c = d \\ a + c = a + c \end{cases} \Rightarrow \begin{cases} a = b \\ a + c = a + d \end{cases} \Rightarrow a + c = b + d$$

■

5.1.3 Ordre

a Définitions

Définition 5.1.8 Pour tous entiers p et q

- 1) $p \leq q$ signifie $\exists \delta \in \mathbb{N}, p + \delta = q$,
 - 2) $p < q$ signifie en plus $\delta \neq 0$,
 - 3) $q \geq p$ signifie $p \leq q$ et
 - 4) $q > p$ signifie $p < q$.
- 1) et 3) sont des **inégalités larges**, les autres sont des **inégalités strictes**.
 - 1) et 2) sont des inégalités de **sens croissant**, les deux autres sont des inégalités de **sens décroissant**.
 - p **minore** q , p **est minorant de** q sont des synonymes de $p \leq q$.
 - p **majore** q , p **est majorant de** q sont des synonymes de $p \geq q$.
 - $p \leq q \leq r$ signifie $p \leq q$ **et** $q \leq r$. De même avec des inégalités strictes, et avec des inégalités dans l'autre sens.

Définition 5.1.9

- p est **positif ou nul** signifie $0 \leq p$.
- p est **positif** signifie $0 < p$.
- p est **néгатif ou nul** signifie $p \leq 0$.
- p est **néгатif** signifie $p < 0$.

b Propriétés

Proposition 5.1.21 Tout entier naturel est positif ou nul.

Démonstration. Pour tout entier naturel p , on a $0 + p = p$, c'est la définition de $0 \leq p$ avec $\delta = p$. ■

Théorème 5.1.22 Pour tous entiers naturels p et q , $p \leq p + q$. Si en plus q n'est pas nul, $p < p + q$. En particulier $p < p + 1$

Démonstration.

On a $p + q = p + q$, c'est la définition de $p \leq p + q$ ou $p < p + q$ avec $\delta = q$. ■

Théorème 5.1.23 Pour tous entiers p et q ,

- 1) $p \leq q \Leftrightarrow p < q$ ou $p = q$
- 2) $p < q \Leftrightarrow \exists \delta \in \mathbb{N}, p + \delta + 1 = q$.

Démonstration.

1) On a par définitions $p \leq q \iff p < q \text{ ou } p = q$. De plus,

$$\begin{aligned}
 p \leq q \text{ et } p \neq q &\implies \exists \delta \in \mathbb{N}, p + \delta = q, p \neq q \\
 &\implies \exists \delta \in \mathbb{N}, (\delta = 0, p + \delta = q, p \neq q) \\
 &\quad \text{ou } (\delta \neq 0, p + \delta = q, p \neq q) \\
 &\implies \exists \delta \in \mathbb{N}, (\delta = 0, p = q, p \neq q) \\
 &\quad \text{ou } (\delta \neq 0, p + \delta = q, p \neq q) \\
 &\implies \exists \delta \in \mathbb{N}, \delta \neq 0, p + \delta = q \\
 &\implies p < q
 \end{aligned}$$

2) On a

$$\begin{aligned}
 \exists \delta \in \mathbb{N}, \delta \neq 0, p + \delta = q \\
 &\iff \exists \delta \in \mathbb{N}, \exists \delta' \in \mathbb{N}, \delta = \delta' + 1, p + \delta = q \\
 &\iff \exists \delta \in \mathbb{N}, \exists \delta' \in \mathbb{N}, \delta = \delta' + 1, p + (\delta' + 1) = q \\
 &\iff \exists \delta' \in \mathbb{N}, p + (\delta' + 1) = q, \exists \delta \in \mathbb{N}, \delta = \delta' + 1 \\
 &\iff \exists \delta' \in \mathbb{N}, p + (\delta' + 1) = q
 \end{aligned}$$

■

Lemme 5.1.24 Pour tout entier naturel p , on a $p \leq p$.

Démonstration.

On a $p + 0 = p$, c'est la définition de $p \leq p$ avec $\delta = 0$.

■

Théorème 5.1.25 Pour tous entiers naturels p et q , on a $p \leq q \text{ et } q \leq p \implies p = q$.

Démonstration.

$$\begin{aligned}
 p \leq q \text{ et } q \leq p &\implies \exists \delta \in \mathbb{N}, p + \delta = q \text{ et } \exists \delta' \in \mathbb{N}, q + \delta' = p \\
 &\implies \exists \delta, \delta' \in \mathbb{N}, p + \delta = q, (p + \delta) + \delta' = p \\
 &\implies \exists \delta, \delta' \in \mathbb{N}, p + \delta = q, p + (\delta + \delta') = p \\
 &\implies \exists \delta, \delta' \in \mathbb{N}, p + \delta = q, \delta + \delta' = 0 \\
 &\implies \exists \delta, \delta' \in \mathbb{N}, p + \delta = q, \delta = \delta' = 0 \\
 &\implies \exists \delta, \delta' \in \mathbb{N}, p + 0 = q, \delta = \delta' = 0 \\
 &\implies p + 0 = q, \exists \delta, \delta' \in \mathbb{N}, \delta = \delta' = 0 \\
 &\implies p = q
 \end{aligned}$$

■

Théorème 5.1.26 Pour tous entiers naturels p , q et r , on a $p \leq q \text{ et } q \leq r \implies p \leq r$.

Démonstration.

$$\begin{aligned}
 p \leq q \text{ et } q \leq r \text{ et } r \leq p \\
 \Rightarrow \exists \delta, \delta', \delta'' \in \mathbb{N}, p + \delta = q \text{ et } q + \delta' = r \text{ et } r + \delta'' = p \\
 \Rightarrow \exists \delta, \delta', \delta'' \in \mathbb{N}, \begin{cases} ((p + \delta) + \delta') + \delta'' = p \\ p + \delta = q \text{ et } q + \delta' = r \text{ et } r + \delta'' = p \end{cases}
 \end{aligned}$$

Or,

$$\begin{aligned}
 ((p + \delta) + \delta') + \delta'' = p &\Rightarrow p + ((\delta + \delta') + \delta'') = p \\
 &\Rightarrow ((\delta + \delta') + \delta'') = 0 \\
 &\Rightarrow \delta + \delta' = 0, \delta'' = 0 \\
 &\Rightarrow \delta = \delta' = \delta'' = 0
 \end{aligned}$$

Cela donne directement le résultat après

$$\begin{aligned}
 p \leq q \text{ et } q \leq r \text{ et } r \leq p \\
 \Rightarrow \exists \delta, \delta', \delta'' \in \mathbb{N}, \% \begin{cases} \delta = \delta' = \delta'' = 0 \\ p + \delta = q \text{ et } q + \delta' = r \text{ et } r + \delta'' = p \end{cases} \\
 \Rightarrow \exists \delta, \delta', \delta'' \in \mathbb{N}, \begin{cases} \delta = \delta' = \delta'' = 0 \\ p = q \text{ et } q = r \text{ et } r = p \end{cases}
 \end{aligned}$$

■

Lemme 5.1.27 Pour tous entiers naturels p, q et r , on a $p \leq q \text{ et } q \leq r \text{ et } r \leq p \Rightarrow p = q = r$

Démonstration.

$$\begin{aligned}
 p \leq q \text{ et } q \leq r \text{ et } r \leq p &\Rightarrow p \leq q \text{ et } q \leq r \text{ et } p \leq r \text{ et } r \leq p \\
 &\Rightarrow p \leq q \text{ et } q \leq r \text{ et } p = r \\
 &\Rightarrow p \leq q \text{ et } q \leq p \text{ et } p = r \\
 &\Rightarrow p = q \text{ et } p = r
 \end{aligned}$$

■

Lemme 5.1.28 Pour tous entiers naturels p, q et r , on a

- $p < q \text{ et } q \leq r \Rightarrow p < r$,
- $p \leq q \text{ et } q < r \Rightarrow p < r$.

Démonstration.

$$\begin{aligned}
 p < q \text{ et } q \leq r &\Rightarrow p < q \text{ et } p \leq q \text{ et } q \leq r \\
 &\Rightarrow p < q \text{ et } q \leq r \text{ et } p \leq r \\
 &\Rightarrow p < q \text{ et } q \leq r \text{ et } p = r \text{ ou } p < q \text{ et } q \leq r \text{ et } p < r \\
 &\Rightarrow r < q \text{ et } q \leq r \text{ ou } p < r \\
 &\Rightarrow r \neq q \text{ et } r \leq q \text{ et } q \leq r \text{ ou } p < r \\
 &\Rightarrow r \neq q \text{ et } r = q \text{ ou } p < r \\
 &\Rightarrow p < r
 \end{aligned}$$

■

Lemme 5.1.29 Pour tous entiers p et q , on a $p < q$ ou bien $p = q$ ou bien $q < p$.

Démonstration. On montre par récurrence que pour tout entier naturel p , on a

$$\forall q \in \mathbb{N}, p < q \text{ ou } p = q \text{ ou } q < p.$$

- Initialisation : sachant que tout entier est positif ou nul, avec le lemme précédent, nous avons $\forall q \in \mathbb{N}, 0 < q \text{ ou } 0 = q$.
- Hérédité : on a d'après ce qui précède

$$\begin{aligned}
 p < q &\Rightarrow p + 1 \leq q \Rightarrow (p + 1 < q \text{ ou } p + 1 = q), \\
 p = q &\Rightarrow p + 1 > q \\
 q < p &\Rightarrow q < p < p + 1 \Rightarrow q < p + 1
 \end{aligned}$$

On a le résultat par combinaison de **ou** par rapport à \Rightarrow .

■

1

Théorème 5.1.30 \leq et \geq sont des relations d'ordre total.

Démonstration.

Voir ce qui précède.

■

Théorème 5.1.31 Pour tous entiers naturels p et q ,

$$(p < q) \Leftrightarrow (p + 1 \leq q) \Leftrightarrow (p \leq q_-)$$

Démonstration.

$$\begin{aligned}
 p < q &\stackrel{\text{déf}}{\Leftrightarrow} \exists \delta \in \mathbb{N}^*, p + \delta = q \\
 &\Leftrightarrow \exists \delta' \in \mathbb{N}, p + (\delta' + 1) = q \\
 &\Leftrightarrow \exists \delta' \in \mathbb{N}, (p + 1) + \delta' = q \\
 &\stackrel{\text{déf}}{\Leftrightarrow} p + 1 \leq q
 \end{aligned}$$

1. $((A \Rightarrow B) \text{ ou } (C \Rightarrow D)) \Rightarrow ((A \text{ ou } C) \Rightarrow (B \text{ ou } D))$

$$\begin{aligned}
\exists \delta' \in \mathbb{N}, p + (\delta' + 1) = q &\Leftrightarrow \exists \delta' \in \mathbb{N}, (p + \delta') + 1 = q \\
&\Leftrightarrow \exists \delta' \in \mathbb{N}, p + \delta' = q_- \\
&\Leftrightarrow p \leq q_-.
\end{aligned}$$

■

Théorème 5.1.32 Pour tout entier naturel n ,

$$\llbracket 0 ; n \rrbracket = \{k \in \mathbb{N} \mid 0 \leq k \leq n\}.$$

Démonstration. On a $\llbracket 0 ; 0 \rrbracket = \{0\} = \{k \in \mathbb{N} \mid 0 \leq k \leq 0\}$ sachant que $0 \leq k \leq 0 \Leftrightarrow k = 0$. Pour tout k

$$k \leq n + 1 \Leftrightarrow k < n + 1 \text{ ou } k = n + 1 \Leftrightarrow k \leq n \text{ ou } k = n + 1,$$

$$\begin{aligned}
\{k \in \mathbb{N} \mid 0 \leq k \leq n + 1\} &= \{k \in \mathbb{N} \mid 0 \leq k \text{ et } (k \leq n \text{ ou } k = n + 1)\} \\
&= \{k \in \mathbb{N} \mid 0 \leq k \leq n\} \cup \{n + 1\}
\end{aligned}$$

Cela fait deux suites définies par la même récurrence : elles sont égales.

■

Définition 5.1.10 Soit A une partie de \mathbb{N} .

1) m **minore** A , m est un **minorant** de A , signifient que m **minore** tout élément de A .

2) m **majore** A , m est un **majorant** de A , signifient que m **majore** tout élément de A .

3) m est un **plus petit élément** de A , m est un **minimum** de A , signifient que m est un minorant de A appartenant à A .

4) m est un **plus grand élément** de A , m est un **maximum** de A , signifient que m est un majorant de A appartenant à A .

5) A est **majorée** si elle admet un majorant.

Lemme 5.1.33 Pour tout entier naturel n , $\llbracket 0 ; n \rrbracket$ a pour maximum n . \mathbb{N} n'est pas majoré.

Démonstration. Immédiat par la proposition 5.1.32 ou les définitions.

■

Théorème 5.1.34 1) Un minorant d'un minorant est un minorant.

2) Un majorant d'un majorant est un majorant.

3) Un minorant de A minore tout partie de A .

4) Un majorant de A majore tout partie de A .

5) Quand il existe, un minimum est unique. *Idem* pour un maximum.

Démonstration.

1) Immédiat.

- 2) Immédiat.
- 3) Immédiat.
- 4) Immédiat.
- 5) Si m et m' sont deux minima, on a $m \leq m' \leq m$, donc $m = m'$. *Idem* dans l'autre sens.

■

Théorème 5.1.35 Toute partie non vide de \mathbb{N} admet un minimum unique.

Démonstration.

- Unicité : immédiat.
- Existence. Soit A une partie de \mathbb{N} contenant a et M l'ensemble de ses minorants. M contient 0. Si M contenait le successeur de chacun de ses éléments, ce serait \mathbb{N} et il contiendrait $a + 1$ qui ne minore pas a . Donc il existe un entier naturel m dans M tel que $m + 1$ n'est pas dans M . Or

$$\begin{aligned}
 m \in M \text{ et } m + 1 \notin M &\Rightarrow m \in M \text{ et } \exists p \in A, m + 1 > p \\
 &\Rightarrow \exists p \in A, m \geq p \text{ et } m \leq p \\
 &\Rightarrow \exists p \in A, m = p \\
 &\Rightarrow m \in A
 \end{aligned}$$

Donc m est un minimum de A .

■

Théorème 5.1.36 Toute partie non vide majorée de \mathbb{N} admet un maximum unique.

Démonstration. Soit A une partie de \mathbb{N} contenant a et majorée par m , M l'ensemble de ses majorants. M , contenant m , n'est pas vide : soit m' son minimum. Si m' n'appartient pas à A , cela signifie que $a < m'$, ou $a \leq m'_-$, et de même pour tout autre élément de A . m'_- est un maximum de A qui contredit la minimalité de m' . Ainsi, m' est dans A : c'est un maximum.

■

Définition 5.1.11 — Intervalles entiers naturels. Pour tous entiers naturels p et q , on pose

- $\llbracket p ; q \rrbracket \stackrel{\text{déf}}{=} \{n \in \mathbb{N} \mid p \leq n \leq q\},$
- $\llbracket p ; q \llbracket \stackrel{\text{déf}}{=} \{n \in \mathbb{N} \mid p \leq n < q\},$
- $\llbracket p ; q \rrbracket \stackrel{\text{déf}}{=} \{n \in \mathbb{N} \mid p < n \leq q\},$
- $\llbracket p ; q \llbracket \stackrel{\text{déf}}{=} \{n \in \mathbb{N} \mid p < n < q\},$
- $\llbracket p ; \infty \rrbracket \stackrel{\text{déf}}{=} \{n \in \mathbb{N} \mid p \leq n\},$
- $\llbracket p ; \infty \llbracket \stackrel{\text{déf}}{=} \{n \in \mathbb{N} \mid p < n\}.$

R $\llbracket p; p \rrbracket = \{p\}$, $\llbracket p; p \rrbracket = \emptyset \dots$

Théorème 5.1.37 — Récurrence décalée. Si un sous-ensemble de \mathbb{N} contient un entier naturel n et contient le successeur de chacun de ses éléments, alors elle contient $\llbracket n; \infty \rrbracket$.

Démonstration. Notons cette partie A . Par l'absurde, si $\llbracket n; \infty \rrbracket \setminus A$ n'est pas vide, soit m son minimum. On a $n \leq m$, $n \neq m$ qui garantit $m > 0$. Par minimalité, $m - 1 \notin \llbracket n; \infty \rrbracket \setminus A$, donc $m - 1 \in A$ et $m \in A$ par succession. Contradiction. ■

Théorème 5.1.38 — Récurrence finie. Si $u_0 = v_0$ et si pour tout $0 \leq i < n$, on a $u_i = v_i \Rightarrow u_{i+1} = v_{i+1}$ alors pour tout $0 \leq i \leq n$, on a $u_i = v_i$.

Démonstration. Par récurrence sur n , en exercice... ■

5.1.4 Soustraction

a Définition

Théorème 5.1.39 Pour tout entier naturel n , $+_n$ est une bijection de \mathbb{N} sur $\llbracket n; \infty \rrbracket$ (voir 5.1.7).

Démonstration. L'injectivité vient de la régularité de l'addition. La surjectivité vient de la définition de l'ordre. ■

Définition 5.1.12 — Soustraction des entiers naturels. $\forall p, q \in \mathbb{N}$, $q \geq p$,

$$q - p \stackrel{\text{déf}}{=} +_p^{-1}(q).$$

b Propriétés

Théorème 5.1.40

$$\forall n \in \mathbb{N}, n_- = n - 1$$

Démonstration. C'est une réécriture de la définition du prédécesseur. ■

Théorème 5.1.41

- $\forall p, q \in \mathbb{N}, q \geq p, (q - p) + p = q$
- $\forall p, q \in \mathbb{N}, (p + q) - q = p$

Démonstration. C'est une réécriture de $+_p +_p^{-1}$ et $+_q^{-1} +_q$. ■

5.1.5 Multiplication

a Définition

Lemme 5.1.42 Pour tout entier naturel n , il existe une unique application de \mathbb{N} dans \mathbb{N} , notée $p \mapsto \times_n(p)$ telle que

- 1) $\times_n(0) = 0$,
- 2) $\forall p \in \mathbb{N}, \times_n(p_+) = \times_n(p) + n$.

Démonstration. C'est une définition par récurrence. À compléter. ■

Définition 5.1.13 — multiplication des entiers naturels.

$$\forall n, p \in \mathbb{N}, n \times p \stackrel{\text{déf}}{=} \times_n(p)$$

R On pourra omettre le signe \times s'il n'y a pas d'ambiguïté.

A La multiplication est prioritaire devant l'addition.

b Propriétés

Théorème 5.1.43

- 1) Élément absorbant : $\forall n \in \mathbb{N}, n \times 0 = 0 \times n = 0$
- 2) Élément neutre : $\forall n \in \mathbb{N}, n \times 1 = n = 1 \times n$
- 3) Distributivités : $\forall p, q, r \in \mathbb{N}, (p + q) \times r = p \times r + q \times r$
 $\forall p, q, r \in \mathbb{N}, p \times (q + r) = p \times q + p \times r$
- 4) Associativité : $\forall p, q, r \in \mathbb{N}, (p \times q) \times r = p \times (q \times r)$
- 5) Commutativité : $\forall p, q \in \mathbb{N}, p \times q = q \times p$
- 6) Intégrité : $\forall p, q \in \mathbb{N}, p \times q = 0 \Leftrightarrow p = 0 \text{ ou } q = 0$
- 7) Régularité : $\forall p, q, r \in \mathbb{N}, p \times r = q \times r \Rightarrow p = q$

Démonstration.

1) La première égalité est immédiate. La deuxième est prouvée par récurrence. Initialisation : immédiat. Hérédité :

$$0 \times n = 0 \Rightarrow 0 \times (n + 1) = 0 \times n + 0 = 0 + 0 = 0$$

2) On a $n \times 1 = n \times 0 + n = 0 + n = n$. Par récurrence pour la deuxième égalité. Initialisation : voir i). Hérédité :

$$n = 1 \times n \Rightarrow n + 1 = 1 \times n + 1 = 1 \times (n + 1)$$

3) Par récurrence sur r pour prouver les deux égalités. Initialisation : $(p + q) \times 0 = 0 = 0 + 0 = p \times 0 + q \times 0$. Hérédité : si $(p + q)r = pr + qr$

$$\begin{aligned} (p + q)(r + 1) &= (p + q)r + (p + q) \\ &= (pr + qr) + (p + q) \\ &= (pr + p) + (qr + q) \\ &= p(r + 1) + q(r + 1) \end{aligned}$$

Initialisation : $p(q + 0) = pq = pq + 0 = pq + p \times 0$. Hérédité : si $p(q + r) = pq + pr$,

$$\begin{aligned} p(q + (r + 1)) &= p((q + r) + 1) \\ &= p(q + r) + p \\ &= (pq + pr) + p \\ &= pq + (pr + p) \\ &= pq + p(r + 1) \end{aligned}$$

4) Par récurrence sur r . Initialisation : on a $p \times (q \times 0) = p \times 0 = 0 = (p \times q) \times 0$. Hérédité :

$$(pq) \times (r + 1) = (pq) \times r + (pq) = p \times (qr) + (pq) = p \times (qr + q) = p \times (q \times (r + 1))$$

5) Par récurrence sur q . Initialisation : voir 1). Hérédité : si $p \times q = q \times p$ alors

$$p \times (q + 1) = p \times q + p = q \times p + p = q \times p + 1 \times p = (q + 1) \times p$$

6) Déjà 1) donne un sens de l'équivalence, l'autre est montré par contraposition. Si p et q ne sont pas nuls, ce sont des successeurs, donc on a

$$p \times q = (p_- + 1) \times q = p_- \times q + q = p_- \times q + (q_- + 1) = (p_- \times q + q_-) + 1$$

et leur produit est aussi un successeur : il n'est pas nul.

7) Si on a $p < q$ alors $q = p + \delta_+$ et $qr_+ = (p + \delta_+)r_+ = pr_+ + \delta_+r_+$ donc $qr_+ < pr_+$. Par contraposition puis échange de p et q on obtient la régularité. ■

Théorème 5.1.44 — Puissances entières. Pour tout entier naturel p , il existe une unique application de \mathbb{N} dans \mathbb{N} , notée $n \mapsto p^n$ telle que

1) $p^0 = 1$,

2) $\forall n \in \mathbb{N}, p^{n+1} = p^n \times p$.

Démonstration. On applique le théorème de définition par récurrence à $a = 1$, $E = \mathbb{N}$ et $H(n, y) \stackrel{\text{déf}}{=} y \times p$. ■

5.1.6 Division

Le problème de la division est traité dans le chapitre d'arithmétique.

6. Nombres entiers relatifs

6.1 Entiers relatifs

Construction de \mathbb{Z} .

6.1.1 Définition

Définition 6.1.1 On définit sur \mathbb{N}^2 la relation \mathcal{R} par :

$$\forall (a; b), (c; d) \in \mathbb{N}^2, (a; b) \mathcal{R} (c; d) \stackrel{\text{déf}}{\iff} a + d = c + b.$$

Théorème 6.1.1

$$\forall n \in \mathbb{N}, (n; n) \mathcal{R} (0; 0)$$

Démonstration. On a $n + 0 = 0 + n$. ■

Théorème 6.1.2 \mathcal{R} est une relation d'équivalence sur \mathbb{N}^2 .

Démonstration.

1) Réflexivité : $a + b = a + b$ donc $(a; b) \mathcal{R} (a; b)$.

2) Symétrie : $(a; b) \mathcal{R} (c; d) \stackrel{\text{déf}}{\iff} a + d = c + b \iff c + b = a + d \stackrel{\text{déf}}{\iff} (c; d) \mathcal{R} (a; b)$

3) Transitivité :

$$\begin{aligned} a + d = c + b \text{ et } c + f = d + e &\implies (a + d) + (c + f) = (c + b) + (d + e) \\ &\implies (a + f) + (d + c) = (b + e) + (d + c) \\ &\implies a + f = b + e \end{aligned}$$
■

Définition 6.1.2

$$\mathbb{Z} \stackrel{\text{déf}}{=} \mathbb{N}^2 / \mathcal{R}$$

C'est l'ensemble des **entiers relatifs**.

6.1.2 Addition

a Définition

Définition 6.1.3 — Addition dans \mathbb{Z} . Pour tous $(a, b), (c, d) \in \mathbb{N}^2$, on pose : $(a, b) +_{\mathbb{N}^2} (c, d) \stackrel{\text{déf}}{=} (a + c, b + d)$.

Proposition 6.1.3 Soient $(a; b), (a'; b'), (c; d), (c'; d') \in \mathbb{N}^2$.

$$(a; b) \mathcal{R} (a'; b') \text{ et } (c; d) \mathcal{R} (c'; d') \implies ((a; b) + (c; d)) \mathcal{R} ((a'; b') + (c'; d'))$$

R L'addition est compatible avec la relation d'équivalence.

Démonstration.

$$\begin{aligned} a + b' &= a' + b \text{ et } c + d' = c' + d \\ \implies (a + b') + (c + d') &= (a' + b) + (c' + d) \\ \implies (a + c) + (b' + d') &= (a' + c') + (b + d) \end{aligned}$$

■

Définition 6.1.4 Soient $p, q \in \mathbb{Z}$, on pose :

$$p +_{\mathbb{Z}} q \stackrel{\text{déf}}{=} p' +_{\mathbb{N}^2} q' \text{ où } p' \in p \text{ et } q' \in q.$$

b Propriétés

Théorème 6.1.4 $(\mathbb{N}^2, +_{\mathbb{N}^2})$ est un monoïde régulier commutatif.

Démonstration. En tant que carré de $(\mathbb{N}, +)$. L'élément neutre est $(0; 0)$.

■

Théorème 6.1.5 $(\mathbb{Z}, +_{\mathbb{Z}})$ est un groupe abélien.

Démonstration. L'addition dans \mathbb{Z} est associative, commutative et admet $(0; 0)$ comme élément neutre, cela se déduit de la proposition précédente appliquée aux représentants. Symétrie : soit $(a; b) \in \mathbb{Z}$, on a

$$\overline{(a, b)} + \overline{(b, a)} \stackrel{\text{déf}}{=} \overline{(a + b, a + b)} = \overline{(0; 0)}$$

donc $\overline{(a, b)}$ est symétrique de $\overline{(b, a)}$.

■

Terminologie 6.1.1 Dans \mathbb{Z} , symétrique et **opposé** sont synonymes. L'opposé de p est noté $-p$.

R On rappelle que par unicité de l'opposé, on a $-(-p) = p$.

Théorème 6.1.6 L'application $f : \mathbb{N} \rightarrow \mathbb{Z}$ définie par $f(a) = \overline{(a, 0)}$ est un homomorphisme injectif de monoïdes.

Démonstration. On a $f(a + b) = \overline{(a + b, 0)} = \overline{(a, 0)} +_{\mathbb{Z}} \overline{(b, 0)} = f(a) +_{\mathbb{Z}} f(b)$. L'injectivité vient de

$$f(a) = f(b) \Rightarrow \overline{(a; 0)} \mathcal{R} \overline{(b; 0)} \Rightarrow a + 0 = 0 + b \Rightarrow a = b \quad \blacksquare$$

R On identifie \mathbb{N} à son image par f dans \mathbb{Z} : pour tout entier naturel a , on a $a = \overline{(a, 0)}$. De plus, f étend l'addition dans \mathbb{N} , on ne fait plus de différence entre $+$ et $+_{\mathbb{Z}}$.

Définition 6.1.5 $-\mathbb{N}$ désigne l'ensemble des entiers relatifs opposés des entiers naturels.

Théorème 6.1.7

- 1) $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$
- 2) $\mathbb{N} \cap (-\mathbb{N}) = \{0\}$

Démonstration.

1) Soit $\overline{(a, b)} \in \mathbb{Z}$.

- Si $a \geq b$, on a $\overline{(a; b)} = \overline{(a - b; 0)}$, c'est un entier naturel.
- Si $a \leq b$, on a $\overline{(a; b)} = \overline{(0; b - a)} = -\overline{(b - a; 0)}$, c'est l'opposé d'un entier naturel.

2) Pour des entiers naturels a et b , on a

$$a = -b \Leftrightarrow \overline{(a, 0)} = \overline{(0, b)} \Leftrightarrow a + b = 0 \Leftrightarrow a = b = 0. \quad \blacksquare$$

Définition 6.1.6 — Valeur absolue et signe. Pour tout entier relatif p , la **valeur absolue** de p est p s'il est entier naturel et $-p$ sinon, elle est notée $|p|$ ou $|p|$.

Définition 6.1.7 Le **signe** de p est 0 si p est nul, 1 si p est entier naturel non nul et -1 sinon, il est noté $\text{sgn}(p)$.

Lemme 6.1.8 Pour tout p entier relatif, $p = \text{sgn}(p) \times |p|$.

Théorème 6.1.9 Pour p et q entiers relatifs, on a $|-p| = |p|$, $||p|| = |p|$ et $|p \times q| = |p| \times |q|$.

Démonstration. Si p est entier naturel, on a $|p| = p$ et $|-p| = -(-p) = p$, sinon, on a $|p| = -p$ et $|-p| = -p$. Dans tous les cas, $|p|$ est entier naturel donc $||p|)| = |p|$. Si p et q sont dans \mathbb{N} , $p \times q$ aussi et $|p \times q| = p \times q = |p| \times |q|$. Si p est dans \mathbb{N} , mais pas q , on a

$|p \times q| = |-(p \times (-q))| = |p \times (-q)| = |p| \times |-q| = |p| \times |q|$. *Idem* pour q est dans \mathbb{N} , mais pas p . Si p et q ne sont pas dans \mathbb{N} , on a

$$|p \times q| = |-(p \times (-q))| = |(-p) \times (-q)| = |-p| \times |-q| = |p| \times |q| \quad \blacksquare$$

6.1.3 Soustraction

Définition 6.1.8 — Soustraction. Soient $p, q \in \mathbb{Z}$, on pose :

$$p - q \stackrel{\text{déf}}{=} p + (-q).$$

Théorème 6.1.10 Soient $p, q \in \mathbb{Z}$, on a $p - q = -(q - p)$.

Démonstration. $(p - q) + (q - p) = (p + (-q)) + (q + (-p)) = (p + (-p)) + (q + (-q)) = 0 + 0 = 0$. \blacksquare

6.1.4 Produit

Définition 6.1.9 Soient $\overline{(a; b)}$ et $\overline{(c; d)}$ de \mathbb{Z} on pose :

$$\overline{(a; b)} \times \overline{(c; d)} \stackrel{\text{déf}}{=} \overline{(ac + bd; ad + bc)}$$

Théorème 6.1.11 Pour p et q entiers relatifs, on a

- 1) $0 \times p = 0$,
- 2) $1 \times p = p$,
- 3) $(-1) \times p = -p$, en particulier $(-1) \times (-1) = 1$,
- 4) $p \times q = q \times p$ (\times est **commutatif** dans \mathbb{Z}) et
- 5) $p \times (-q) = (-p) \times q = -(p \times q)$.

Démonstration.

$$1) \ 0 \times \overline{(a; b)} = \overline{(0; 0)} \times \overline{(a; b)} = \overline{(0 \times a + 0 \times b; 0 \times b + 0 \times a)} = \overline{(0; 0)} = 0$$

$$2) \ 1 \times \overline{(a; b)} = \overline{(1; 0)} \times \overline{(a; b)} = \overline{(1 \times a + 0 \times b; 1 \times b + 0 \times a)} = \overline{(a; b)}$$

$$3) \ (-1) \times \overline{(a; b)} = \overline{(0; 1)} \times \overline{(a; b)} = \overline{(0 \times a + 1 \times b; 0 \times b + 1 \times a)} = \overline{(b; a)} = -\overline{(a; b)}. \text{ En particulier, } (-1) \times (-1) = -(-1) = 1$$

$$4) \ \overline{(a; b)} \times \overline{(c; d)} \stackrel{\text{déf}}{=} \overline{(ac + bd; ad + bc)} = \overline{(ca + db; cb + da)} \stackrel{\text{déf}}{=} \overline{(c; d)} \times \overline{(a; b)}$$

$$5) \text{ On a } \overline{(a; b)} \times \overline{(c; d)} = -\overline{(ad + bc; ac + bd)} = \overline{(a; b)} \times \overline{(d; c)} = \overline{(a; b)} \times \overline{-(c; d)}. \text{ Dans cette dernière égalité on échange } \overline{(a; b)} \text{ et } \overline{(c; d)} \text{ puis on utilise deux fois la commutativité de 4) : } \overline{(a; b)} \times \overline{(c; d)} = \overline{-(a; b)} \times \overline{(c; d)}. \quad \blacksquare$$

Théorème 6.1.12 Pour p et q entiers relatifs, on a $\text{sgn}(-p) = -\text{sgn}(p)$, $\text{sgn}(\text{sgn}(p)) = \text{sgn}(p)$ et $\text{sgn}(p \times q) = \text{sgn}(p) \times \text{sgn}(q)$, en particulier si p n'est pas nul, $\text{sgn}(p^2) = 1$ ^a.

a. Attention à la définition du carré.

Démonstration.

- Si p est nul, on a $\text{sgn}(-0) = 0 = -0 = -\text{sgn}(0)$, $\text{sgn}(\text{sgn}(0)) = \text{sgn}(0)$ et $\text{sgn}(0 \times q) = \text{sgn}(0) = 0 = 0 \times \text{sgn}(q) = \text{sgn}(0) \times \text{sgn}(q)$.
- Si p est entier naturel, on a $\text{sgn}(-p) = -1 = -\text{sgn}(p)$ et $\text{sgn}(\text{sgn}(p)) = \text{sgn}(1) = 1 = \text{sgn}(p)$, sinon, on a $\text{sgn}(-p) = 1 = -(-1) = -\text{sgn}(p)$ et $\text{sgn}(\text{sgn}(p)) = \text{sgn}(-1) = -1 = \text{sgn}(p)$.
- Si p et q sont dans \mathbb{N} , on a $\text{sgn}(p \times q) = 1 = 1 \times 1 = \text{sgn}(p) \times \text{sgn}(q)$.
- Si p est dans \mathbb{N} , mais pas q , on a $\text{sgn}(p) \times \text{sgn}(q) = -1$ $\text{sgn}(p \times q) = \text{sgn}(-(p \times (-q))) = -\text{sgn}(p \times (-q)) = -\text{sgn}(p) \times \text{sgn}(-q) = -1$, $\text{sgn}(p) = 1$ et $\text{sgn}(1) = 1$, sinon, on a $\text{sgn}(p) = -1$ et $\text{sgn}(-1) = -1$.
- *Idem* pour q est dans \mathbb{N} , mais pas p .
- Si p et q ne sont pas dans \mathbb{N} , on a $\text{sgn}(p) \times \text{sgn}(q) = (-1) \times (-1) = 1$. $\text{sgn}(p \times q) = \text{sgn}(-(p \times (-q))) = \text{sgn}((-p) \times (-q)) = 1$.
- Si p est dans \mathbb{N} , $\text{sgn}(p^2) = 1^2 = 1$ sinon $\text{sgn}(p^2) = (-1)^2 = 1$. ■

Théorème 6.1.13 $(\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire.

a Ordre

Théorème 6.1.14 Pour tous a et b dans \mathbb{N} , on a $a \leq b \Leftrightarrow b - a \in \mathbb{N}$.

Démonstration. Dans \mathbb{Z} , on a $b = a + (b - a)$. À compléter... ■

Définition 6.1.10 Pour tous a et b dans \mathbb{Z} , on pose

- $a \leq b \stackrel{\text{déf}}{\Leftrightarrow} b - a \in \mathbb{N}$,
- $a < b \stackrel{\text{déf}}{\Leftrightarrow} a \leq b$ **et** $a \neq b$,
- $a \geq b \stackrel{\text{déf}}{\Leftrightarrow} b \leq a$, $a > b \stackrel{\text{déf}}{\Leftrightarrow} b < a$.

Théorème 6.1.15

- $p \leq q$ **et** $p' \leq q' \Rightarrow p + p' \leq q + q'$,
- $p \leq q$ **et** $0 \leq r \Rightarrow pr \leq qr$,
- $p \leq q$ **et** $0 \geq r \Rightarrow pr \geq qr$.

Démonstration. À compléter... ■

Théorème 6.1.16

- Toute partie non vide majorée de \mathbb{Z} admet un maximum.
- Toute partie non vide minorée de \mathbb{Z} admet un minimum.

Démonstration. À compléter... ■

Définition 6.1.11 — Intervalles entiers relatifs. Pour tous entiers relatifs p et q , on pose

- $\llbracket p; q \rrbracket \stackrel{\text{déf}}{=} \{n \in \mathbb{Z} \mid p \leq n \leq q\},$
- $\llbracket p; q[\stackrel{\text{déf}}{=} \{n \in \mathbb{Z} \mid p \leq n < q\},$
- $\llbracket]p; q \rrbracket \stackrel{\text{déf}}{=} \{n \in \mathbb{Z} \mid p < n \leq q\},$
- $\llbracket]p; q[\stackrel{\text{déf}}{=} \{n \in \mathbb{Z} \mid p < n < q\},$
- $\llbracket p; +\infty[\stackrel{\text{déf}}{=} \{n \in \mathbb{Z} \mid p \leq n\},$
- $\llbracket]p; +\infty[\stackrel{\text{déf}}{=} \{n \in \mathbb{Z} \mid p < n\},$
- $\llbracket -\infty; q \rrbracket \stackrel{\text{déf}}{=} \{n \in \mathbb{Z} \mid n \leq q\},$
- $\llbracket -\infty; q[\stackrel{\text{déf}}{=} \{n \in \mathbb{Z} \mid n < q\}.$

R $\llbracket p; p \rrbracket = \{p\}, \llbracket p; p[= \emptyset \dots$

Terminologie 6.1.2 Si n est négatif, son successeur est $n + 1$ et son prédécesseur est $n - 1$.

R Cela étend les définitions éponymes dans \mathbb{N} de manière formellement homogène.

Théorème 6.1.17 — Récurrence décalée. Si une partie de \mathbb{Z} contient un entier relatif n et contient le successeur de chacun de ses éléments, alors elle contient $\llbracket n; +\infty[$.

Démonstration. Notons cette partie A . Par l'absurde, si $\llbracket n; \infty[\setminus A$ n'est pas vide, soit m son minimum. On a $n \leq m$, $n \neq m$ qui garantit $m > 0$. Par minimalité, $m - 1 \notin \llbracket n; \infty[\setminus A$, donc $m - 1 \in A$ et $m \in A$ par succession. Contradiction. (*Idem* cas \mathbb{N}). ■

Théorème 6.1.18 — Récurrence décalée. Si une partie de \mathbb{Z} contient un entier relatif n et contient le prédécesseur de chacun de ses éléments, alors elle contient $\llbracket -\infty; n \rrbracket$.

Démonstration. On se ramène au théorème précédent en prenant les opposés. ■

7. Relations

7.1 Relations

Relations d'ordre et relations d'équivalence.

7.1.1 Généralités

Définition 7.1.1 — Relation binaire. Une **relation binaire** \mathcal{R} sur un ensemble E est donnée par une partie Γ de $E \times E$. Pour deux éléments x et y de E , $x\mathcal{R}y$ signifie que le couple (x, y) est dans Γ .

$x\mathcal{R}y$ est lu : « x est en relation avec y par \mathcal{R} ». On omettra « par \mathcal{R} » si le contexte est suffisamment clair.

Définition 7.1.2 — Relation binaire réciproque. À toute relation binaire \mathcal{R} sur un ensemble E est associée la relation binaire réciproque \mathcal{R}' définie par

$$x\mathcal{R}'y \stackrel{\text{déf}}{\iff} y\mathcal{R}x$$

Définition 7.1.3 — Réflexivité. Une relation binaire \mathcal{R} sur un ensemble E est **réflexive** signifie que

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

Définition 7.1.4 — Symétrie. Une relation binaire \mathcal{R} sur un ensemble E est **symétrique** signifie que

$$\forall (x, y) \in E^2 (x\mathcal{R}y \implies y\mathcal{R}x).$$

Terminologie 7.1.1 Dans le cas d'une relation symétrique, $x\mathcal{R}y$ peut être lu « x et y sont en relation par \mathcal{R} ».

Définition 7.1.5 — Antisymétrie. Une relation binaire \mathcal{R} sur un ensemble E est **antisymétrique** signifie que

$$\forall (x, y) \in E^2 \ (x\mathcal{R}y \text{ et } y\mathcal{R}x \implies x = y).$$

Définition 7.1.6 — Transitivité. Une relation binaire \mathcal{R} sur un ensemble E est **transitive** signifie que

$$\forall (x, y, z) \in E^3 \ (x\mathcal{R}y \text{ et } y\mathcal{R}z \implies x\mathcal{R}z).$$

7.1.2 Ordre

Voir le chapitre sur les corps totalement ordonnés.

7.1.3 Équivalence

a Définitions

Définition 7.1.7 — Équivalence. Une relation binaire est une **relation d'équivalence** signifie qu'elle est réflexive, symétrique et transitive.

Terminologie 7.1.2 — Classe d'équivalence. Soit \mathcal{R} une relation d'équivalence sur E , et x un élément de E . La **classe d'équivalence** de x **modulo** \mathcal{R} est $\{y \in E \mid x\mathcal{R}y\}$.

Elle est notée \dot{x} . On pourra omettre «**modulo** \mathcal{R} » s'il n'y a pas ambiguïté. Un élément d'une classe d'équivalence en est un **représentant**.

b Propriétés

Théorème 7.1.1 La classe d'équivalence d'un élément contient au moins cet élément. En particulier, elle n'est pas vide.

Démonstration. Immédiat par la réflexivité. ■

Théorème 7.1.2 Pour une même relation d'équivalence, deux classes sont disjointes ou bien confondues.

Démonstration. Soit \mathcal{R} une relation d'équivalence sur E , x_0 et y_0 deux éléments de E . On a

$$\dot{x}_0 \cap \dot{y}_0 = \emptyset \text{ ou bien } \dot{x}_0 \cap \dot{y}_0 \neq \emptyset$$

Si $\dot{x}_0 \cap \dot{y}_0 \neq \emptyset$, soit z_0 élément commun. On a $x_0\mathcal{R}z_0$ et $y_0\mathcal{R}z_0$ donc $x_0\mathcal{R}y_0$. Pour tout x de \dot{x}_0 , on a $x\mathcal{R}x_0$ et $x_0\mathcal{R}y_0$ donc $x\mathcal{R}y_0$, x est dans \dot{y}_0 . Pour tout représentant y de \dot{y}_0 , on a $y\mathcal{R}y_0$ et $y_0\mathcal{R}x_0$ donc $y\mathcal{R}x_0$, y est dans \dot{x}_0 . Ainsi, deux classes non disjointes sont confondues.

Inversement, deux classes confondues ne sont pas disjointes puisqu'elles ne sont pas vides, ce qui donne

$$\dot{x}_0 \cap \dot{y}_0 \neq \emptyset \Leftrightarrow \dot{x}_0 = \dot{y}_0$$

et le résultat. ■

Théorème 7.1.3 Toute classe d'équivalence est la classe d'équivalence de chacun de ses éléments.

Démonstration. Soit \mathcal{R} une relation d'équivalence sur E , et x_0 un élément de E . Pour tout x de \dot{x}_0 , \dot{x} et \dot{x}_0 ont en commun x donc sont confondues. ■

Lemme 7.1.4 Soit \mathcal{R} une relation d'équivalence sur E , deux éléments de E sont en relation si et seulement s'ils ont la même classe d'équivalence.

Démonstration. On a $x \mathcal{R} y \Leftrightarrow (x \in \dot{x} \text{ et } y \in \dot{y}) \Leftrightarrow \dot{x} = \dot{y}$. ■

c Projection canonique

Définition 7.1.8 — Ensemble quotient. Soit \mathcal{R} une relation d'équivalence sur E . L'ensemble des classes d'équivalence est l'**ensemble quotient** de E par \mathcal{R} , noté E / \mathcal{R} . L'application de E dans E / \mathcal{R} qui à tout élément de E associe sa classe d'équivalence est l'**application** (ou **projection**) **canonique**.

Théorème 7.1.5 La projection canonique est surjective.

Démonstration. En exercice... ■

- R** les propriétés de \square qui ne dépendent que de la classe d'équivalence se transportent à l'ensemble quotient.

d Partitions

Théorème 7.1.6 Soit \mathcal{R} une relation d'équivalence sur E . Les classes d'équivalence définissent une partition de E .

Démonstration. Par les lemmes 7.1.1 et 7.1.2, les classes d'équivalences sont non vides et mutuellement disjointes. Comme tout élément de E est dans sa classe d'équivalence, la réunion des classes est E . ■

Proposition 7.1.7 Toute partition de E définit sur E une relation d'équivalence dont les classes coïncident avec les éléments de la partition.

Démonstration. Soit P une partition de \square . On pose

$$x \mathcal{R} y \stackrel{\text{déf}}{\iff} \exists F \in P, (x \in F \text{ et } y \in F)$$

À finir en exercice... ■

Théorème 7.1.8 — Relation et application. Étant donnée une application f de E dans F ,

$$x \mathcal{R} y \stackrel{\text{déf}}{\iff} f(x) = f(y)$$


est une relation d'équivalence dans E .

Démonstration. Pour appliquer le résultat précédent : $\bigcup_{y \in f(E)} f^{-1}(y)$ est une partition de E .

- 1) Tout y de $f(E)$ est un $f(x)$, donc $f^{-1}(y)$ contient x et $f^{-1}(y) \neq \emptyset$.
 - 2) Tout x de E est dans $f^{-1}(f(x))$. Or $f(x)$ est dans $f(E)$, donc $\bigcup_{y \in f(E)} f^{-1}(y)$, qui est une partie de E , contient $f^{-1}(f(x))$ et x . Donc $E = \bigcup_{y \in f(E)} f^{-1}(y)$.
 - 3) Pour tous y et y' de $f(E)$, si $f^{-1}(y) \cap f^{-1}(y')$ contient x alors $f(x) = y = y'$. Par contraposition, si y et y' sont différents, $f^{-1}(y) \cap f^{-1}(y')$ est vide.
-



8. Nombres rationnels



9. Corps totalement ordonné



10. Nombres réels



11. Nombres décimaux



12. Nombres complexes

13. Dénombrement

Dans la suite G , F et E désignent des ensembles.

13.1 Dénombrement

Cardinal d'un ensemble fini.

13.1.1 Ensembles finis ou infinis

a Définitions

Définition 13.1.1

1) Un ensemble E est **infini** signifie qu'il existe une injection de E dans une partie stricte de E .

2) Un ensemble E est **fini** signifie qu'il n'est pas infini.

Théorème 13.1.1

1) Un ensemble dont une partie est infinie est infini.

2) Toute partie d'un ensemble fini est finie.

Démonstration.

1) Si $E \subset G$ et $\varphi : E \rightarrow E$ est une injection. L'application

$$\begin{aligned} \psi : G &\rightarrow G \\ x &\mapsto \begin{cases} x & \text{si } x \in G \setminus E \\ \varphi(x) & \text{sinon} \end{cases} \end{aligned}$$

est une injection dont l'image est $\text{Im } \varphi \cup G \setminus E$, qui est une partie stricte de G dès que $\text{Im } \varphi$ est une partie stricte de G .

2) Par contraposition de ce qui précède. ■

Théorème 13.1.2 Un ensemble infini privé d'un seul élément est encore infini.

Démonstration. Soit $F \subsetneq E$, φ une injection de E dans F et $x \in E$. Soit τ la transposition qui échange x et $\varphi(x)$. $\tau(F)$ est une partie stricte de E car elle ne contient pas $\tau(E \setminus F)$. $\tau \circ \varphi$ est une injection de E dans $\tau(F)$ telle que $\tau \circ \varphi(x) = x$. Elle induit une injection de $E \setminus \{x\}$ dans $\tau(F) \setminus \{x\}$ où $\tau(F) \setminus \{x\} \subsetneq E \setminus \{x\}$. Donc $E \setminus \{x\}$ est infini. ■

b Intervalles entiers

Théorème 13.1.3 Soit $n \in \mathbb{N}$, $\llbracket 1; n \rrbracket$ est un ensemble fini.

Démonstration. Soit E l'ensemble des entiers tels que $\llbracket 1; n \rrbracket$ est infini. Supposons par l'absurde que E n'est pas vide. E ne contient pas 0 car $\llbracket 1; 0 \rrbracket = \emptyset$ et il n'existe pas de partie stricte de $\llbracket 1; 0 \rrbracket$ donc il n'existe pas d'injection d'une partie stricte de $\llbracket 1; 0 \rrbracket$ dans $\llbracket 1; 0 \rrbracket$. Le minimum de E , non nul, est noté m . Comme $\llbracket 1; m \rrbracket$ est infini, et $\llbracket 1; m \rrbracket = \llbracket 1; m-1 \rrbracket \cup \{m\}$, par le lemme précédent, $\llbracket 1; m-1 \rrbracket$ est infini, ce qui contredit la minimalité de m . ■

Théorème 13.1.4 Soient $n, m \in \mathbb{N}$.

- 1) S'il existe une injection de $\llbracket 1; n \rrbracket$ dans $\llbracket 1; m \rrbracket$ alors $n \leq m$.
- 2) S'il existe une surjection de $\llbracket 1; n \rrbracket$ sur $\llbracket 1; m \rrbracket$ alors $n \geq m$.

Démonstration.

1) Par récurrence sur n .

- Initialisation. Pour $n = 0$, comme $m \in \mathbb{N}$, $n = 0 \leq m$.
- Hérédité. On montre d'abord que s'il existe une injection, notée φ , de $\llbracket 1; n+1 \rrbracket$ dans $\llbracket 1; m+1 \rrbracket$ alors il existe une injection de $\llbracket 1; n \rrbracket$ dans $\llbracket 1; m \rrbracket$.

Si $m+1 \notin \text{Im } \varphi$, $\varphi|_{\llbracket 1; n \rrbracket}$ est une injection $\llbracket 1; n \rrbracket$ dans $\llbracket 1; m \rrbracket$.

Si $m+1 \in \text{Im } \varphi$, soit τ la transposition qui échange $n+1$ et $\varphi^{-1}(m+1)$, $\varphi \circ \tau|_{\llbracket 1; n \rrbracket}$ est une injection de $\llbracket 1; n \rrbracket$ dans $\llbracket 1; m \rrbracket$.

On combine avec une hypothèse de récurrence pour obtenir $n \leq m$ et $n+1 \leq m+1$, ce qui donne l'hérédité.

2) Par récurrence sur m .

- Initialisation. Pour $m = 0$, comme $n \in \mathbb{N}$, $n \geq 0 = m$.

- **Hérédité.** On montre d'abord que s'il existe une surjection, notée φ , de $\llbracket 1; n+1 \rrbracket$ sur $\llbracket 1; m+1 \rrbracket$ alors il existe une surjection de $\llbracket 1; n \rrbracket$ sur $\llbracket 1; m \rrbracket$.

Si $\varphi(n+1) \neq m+1$, l'application

$$\begin{aligned} \psi : \llbracket 1; n \rrbracket &\longrightarrow \llbracket 1; m \rrbracket \\ i &\longmapsto \begin{cases} \varphi(n+1) & \text{si } \varphi(i) = m+1 \\ \varphi(i) & \text{sinon} \end{cases} \end{aligned}$$

est une surjection. En effet, il existe i de $\llbracket 1; n+1 \rrbracket$ tel que $\varphi(i) = m+1$. Par hypothèse, $i \neq n+1$, d'où $\psi(i) = \varphi(n+1)$, donc $\varphi(n+1) \in \text{Im } \psi$. De plus, pour tout entier j de $\llbracket 1; m \rrbracket$ autre que $\varphi(n+1)$, il existe i de $\llbracket 1; n+1 \rrbracket$ tel que $\varphi(i) = j$. Comme on a $j \neq \varphi(n+1)$, on a $i \neq n+1$. Comme on a $j \neq m+1$, on a $\varphi(i) \neq m+1$ et par définition de ψ , $\varphi(i) = \psi(i)$. Ainsi $j \in \text{Im } \psi$ et ψ est surjective.

Si $\varphi(n+1) = m+1$, l'application

$$\begin{aligned} \psi : \llbracket 1; n \rrbracket &\longrightarrow \llbracket 1; m \rrbracket \\ i &\longmapsto \begin{cases} 1 & \text{si } \varphi(i) = m+1 \\ \varphi(i) & \text{sinon} \end{cases} \end{aligned}$$

est une surjection. En effet, pour tout entier j de $\llbracket 1; m \rrbracket$, il existe i de $\llbracket 1; n+1 \rrbracket$ tel que $\varphi(i) = j$. Comme on a $j \neq m+1$, on a $i \neq n+1$ et d'où $\psi(i) = \varphi(i) = j$. Ainsi $j \in \text{Im } \psi$ et ψ est surjective. ■

Théorème 13.1.5 S'il existe une bijection entre $\llbracket 1; n \rrbracket$ et $\llbracket 1; m \rrbracket$ alors $n = m$.

Démonstration. S'il existe une bijection entre $\llbracket 1; n \rrbracket$ et $\llbracket 1; m \rrbracket$ alors en particulier :

- 1) il existe une injection de $\llbracket 1; n \rrbracket$ dans $\llbracket 1; m \rrbracket$, et $n \leq m$,
- 2) il existe une surjection de $\llbracket 1; n \rrbracket$ sur $\llbracket 1; m \rrbracket$, et $m \leq n$.

Par conséquent, $n = m$. ■

Théorème 13.1.6

- 1) Toute injection de $\llbracket 1; n \rrbracket$ dans lui-même est une bijection.
- 2) Toute surjection de $\llbracket 1; n \rrbracket$ sur lui-même est une bijection.

Démonstration.

- 1) Par récurrence sur n .

- Initialisation. Toute application de \emptyset dans lui-même est une bijection.

- Hérédité. Soit φ une injection de $\llbracket 1; n+1 \rrbracket$ dans lui-même.

Si $n+1 = \varphi(n+1)$, $\varphi|_{\llbracket 1; n \rrbracket}$ est une injection de $\llbracket 1; n \rrbracket$ dans $\llbracket 1; n+1 \rrbracket$ qui n'atteint pas $n+1$, c'est donc une injection de $\llbracket 1; n \rrbracket$ dans lui-même.

Par hypothèse de récurrence, c'est une bijection, donc une surjection. Ainsi $\mathcal{I}\varphi$, qui contient $\mathcal{I}\varphi_{\llbracket 1; n \rrbracket}$, contient $\llbracket 1; n \rrbracket$. Comme il contient par ailleurs $n + 1$, il contient $\llbracket 1; n + 1 \rrbracket$ donc φ est surjective : c'est une bijection.

Si $n + 1 \neq \varphi(n + 1)$, l'application τ de $\llbracket 1; n + 1 \rrbracket$ dans lui-même qui échange $n + 1$ et $\varphi(n + 1)$ est une bijection :

$$\begin{aligned} \tau : \llbracket 1; n + 1 \rrbracket &\longrightarrow \llbracket 1; n + 1 \rrbracket \\ i &\longmapsto \begin{cases} n + 1 & \text{si } i = \varphi(n + 1) \\ \varphi(n + 1) & \text{si } i = n + 1 \\ i & \text{sinon} \end{cases} \end{aligned}$$

On a $\tau \circ \varphi(n + 1) = n + 1$ et $\tau \circ \varphi$ est une injection, par le point précédent, $\tau \circ \varphi$ est aussi une bijection. Par conséquent, $\tau \circ \tau \circ \varphi$, qui vaut φ , en est aussi une.

2) Par récurrence sur n .

- Initialisation. Toute application de \emptyset dans lui-même est une bijection, ainsi que toute application de $\llbracket 1; 1 \rrbracket$ dans lui-même.
- Hérédité. Pour tout $n \geq 0$, soit φ une surjection de $\llbracket 1; n + 1 \rrbracket$ dans lui-même.

Si $n + 1 = \varphi(n + 1)$. Pour tout \square de $\llbracket 1; n \rrbracket$, $\varphi^{-1}(\square)$ est une partie non vide de $\llbracket 1; n + 1 \rrbracket$ qui ne contient pas $n + 1$, c'est donc une partie non vide de $\llbracket 1; n \rrbracket$. Donc $\varphi_{\llbracket 1; n \rrbracket}$ a pour image $\llbracket 1; n \rrbracket$ et par hypothèse de récurrence, elle induit une bijection de $\llbracket 1; n \rrbracket$ dans lui-même. Cela fait de φ une bijection de $\llbracket 1; n + 1 \rrbracket$ dans lui-même.

Si $n + 1 \neq \varphi(n + 1)$, on a $\tau \circ \varphi(n + 1) = n + 1$ et $\tau \circ \varphi$ est une surjection, par le point précédent, $\tau \circ \varphi$ est aussi une bijection. Par conséquent, $\tau \circ \tau \circ \varphi$, qui vaut φ , en est aussi une. ■

Théorème 13.1.7 \mathbb{N} est infini.

Démonstration. Soit

$$\begin{aligned} \varphi : \mathbb{N} &\longrightarrow \mathbb{N}^* & \psi : \mathbb{N}^* &\longrightarrow \mathbb{N} \\ n &\longmapsto n + 1' & n &\longmapsto n - 1 \end{aligned}$$

On a $\forall n \in \mathbb{N}$, $\psi \circ \varphi(n) = \psi(n + 1) = n$. Donc, φ est une injection de \mathbb{N} dans \mathbb{N}^* qui est une partie stricte de \mathbb{N} . ■

c Cas général

Théorème 13.1.8 L'ensemble E est infini si et seulement s'il existe une injection de \mathbb{N} dans E .

Démonstration. Si φ est une injection de \mathbb{N} dans E , l'application

$$\begin{aligned} \psi : E &\longrightarrow E \\ x &\longmapsto \begin{cases} x & \text{si } x \notin \text{Im } \varphi \\ \varphi(1 + \varphi^{-1}(x)) & \text{sinon} \end{cases} \end{aligned}$$

est une injection de E dans $E \setminus \{\varphi(0)\}$. ■

Théorème 13.1.9 Soit $f : E \rightarrow F$.

- 1) Si $f(E)$ est infini alors E est infini.
- 2) Si E est fini alors $f(E)$ est fini.
- 3) Si f est injective, alors E est infini si et seulement si $f(E)$ est infini.
- 4) Si f est injective, alors E est fini si et seulement si $f(E)$ est fini.

Démonstration.

- 1) Soit $\varphi : \mathbb{N} \rightarrow f(E)$ une injection. On sait que f induit une surjection de E sur $f(E)$, encore notée f , qui admet une réciproque à droite, notée $g : f(E) \rightarrow E$, injective et telle que $f \circ g = \text{Id}_{f(E)}$. $g \circ \varphi$ est une injection de \mathbb{N} dans E .
- 2) C'est la contraposée du point précédent.
- 3) Si $\varphi : \mathbb{N} \rightarrow E$ est une injection, alors $f \circ \varphi : \mathbb{N} \rightarrow f(E)$ est une injection : si E est infini, $f(E)$ aussi. Avec i) on a l'équivalence.
- 4) C'est la contraposée du point précédent. ■

Théorème 13.1.10 Il existe une injection de \mathbb{N} dans E si et seulement si pour tout entier naturel n il existe une injection de $\llbracket 1; n \rrbracket$ dans E .

Démonstration.

- 1) Condition nécessaire. Soit φ une injection de \mathbb{N} dans E . Alors, pour tout $n \in \mathbb{N}$, $\varphi_{\llbracket 1; n \rrbracket}$ est une injection de $\llbracket 1; n \rrbracket$ dans E (y compris $n = 0$).
- 2) Condition suffisante. Soit φ_n l'injection de $\llbracket 1; n \rrbracket$ dans E . On définit l'injection de \mathbb{N} dans E par récurrence. On pose $e_1 \stackrel{\text{déf}}{=} \varphi_1(1)$. Pour $n > 1$, si e_1, \dots, e_n sont mutuellement distincts, on n'a pas $\text{Im } \varphi_{n+1} \subset \{e_1, \dots, e_n\}$ sinon $\{e_i \mapsto i\} \circ \varphi_{n+1}$ serait une injection de $\llbracket 1; n+1 \rrbracket$ dans $\llbracket 1; n \rrbracket$. Ainsi, il existe un élément de E différent de e_1, \dots, e_n , c'est e_{n+1} . À préciser. ■

Théorème 13.1.11 Un ensemble E est fini s'il existe une bijection de E vers $\llbracket 1; n \rrbracket$ où $n \in \mathbb{N}$.

Démonstration. Par l'absurde, soit φ_n une bijection de E vers $\llbracket 1; n \rrbracket$ et ψ une injection de E vers F où $F \subsetneq E$. L'application $\varphi_n^{-1} \circ \psi \circ \varphi_n$ est injective. Son image est incluse dans $\varphi_n^{-1}(F)$, c'est donc une partie stricte de $\llbracket 1; n \rrbracket$. Contradiction avec la finitude de $\llbracket 1; n \rrbracket$. ■

13.1.2 Cardinal

a Définition

Lemme 13.1.12 Soit E un ensemble. L'ensemble des entiers naturels n tels qu'il existe une injection de $\llbracket 1; n \rrbracket$ dans E est non vide, s'il est majoré alors E est fini, s'il n'est pas majoré alors E est infini.

Démonstration. Notons A l'ensemble des entiers naturels en question. Pour $n = 0$, on a $\llbracket 1; 0 \rrbracket = \emptyset$ et l'unique application de \emptyset dans E est injective. Ainsi, A est non vide.

Si A est majoré, notons m son maximum et φ_m une injection correspondante. Si φ_m n'est pas surjective, $E \setminus \text{Im } \varphi_m$ contient un élément y et l'application

$$\begin{aligned} \psi : \llbracket 0; m+1 \rrbracket &\longrightarrow E \\ n &\longmapsto \begin{cases} y & \text{si } n = m+1 \\ \varphi_m(n) & \text{sinon} \end{cases} \end{aligned}$$

est injective, ce qui contredit la maximalité de m . Donc φ_m est une bijection et par le lemme 13.1.11, E est fini.

Si A n'est pas majoré alors pour tout $n \in \mathbb{N}^*$ il existe une injection de $\llbracket 1; n \rrbracket$ dans E avec $n \leq m$, qui par restriction, donne une injection de $\llbracket 1; m \rrbracket$ dans E . Par le lemme 13.1.10 il y a une injection de \mathbb{N} dans E et par le lemme 13.1.8 E est infini. ■

Définition 13.1.2 Soit E un ensemble fini. n est le **cardinal**, ou **nombre d'éléments**, de E signifie qu'il existe une bijection de $\llbracket 1; n \rrbracket$ dans E . Il est noté $\text{card}(E)$, ou $|E|$.

Vocabulaire 13.1.1

- E a n éléments signifie $\text{card}(E) = n$.
- E a au moins, ou plus de, n éléments signifie $\text{card}(E) \geq n$.
- E a strictement plus de n éléments signifie $\text{card}(E) > n$.
- E a au plus, ou moins de, n éléments signifie $\text{card}(E) \leq n$.
- E a strictement moins de n éléments signifie $\text{card}(E) < n$.

On peut remplacer «a» par «possède», «contient» et autres synonymes.

Théorème 13.1.13

$$|\emptyset| = 0$$

Démonstration. L'application vide est une bijection de $\llbracket 1; 0 \rrbracket$ dans \emptyset . ■

Théorème 13.1.14 Le cardinal d'un singleton est 1.

Démonstration. Soit $\{x\}$ le singleton, l'unique application de $\llbracket 1; 1 \rrbracket$ dans $\{x\}$ est une bijection. ■

b Applications et cardinal

Théorème 13.1.15 Soient E et F deux ensembles finis. Il existe une bijection de E dans F si et seulement si $\text{card}(E) = \text{card}(F)$.

Démonstration. E et F sont finis donc il existe une bijection f de $\llbracket 1; |E| \rrbracket$ dans E et une bijection g de $\llbracket 1; |F| \rrbracket$ dans F .

Si h est une bijection de E vers F , alors $g^{-1} \circ h \circ f$ est une bijection de $\llbracket 1; |E| \rrbracket$ vers $\llbracket 1; |F| \rrbracket$, donc, $\text{card}(E) = \text{card}(F)$.

Si $\text{card}(E) = \text{card}(F)$, $g \circ f^{-1}$ est une bijection de E vers F . ■

Théorème 13.1.16

1) S'il existe une injection de E dans F fini, E est fini et $\text{card}(E) \leq \text{card}(F)$.

2) S'il existe une surjection de E fini sur F , F est fini et $\text{card}(E) \geq \text{card}(F)$.

Démonstration.

1) Si φ est une injection de E dans F , $g^{-1} \circ \varphi \circ f$ est une injection de $\llbracket 1; |E| \rrbracket$ dans $\llbracket 1; |F| \rrbracket$, donc $\text{card}(E) \leq \text{card}(F)$.

2) Si φ est une surjection de E sur F , $g^{-1} \circ \varphi \circ f$ est une surjection de $\llbracket 1; |E| \rrbracket$ sur $\llbracket 1; |F| \rrbracket$, donc $\text{card}(E) \geq \text{card}(F)$. ■

Théorème 13.1.17 Soient E et F deux ensembles finis de même cardinal.

1) Toute injection de E dans F est une bijection.

2) Toute surjection de E sur F est une bijection.

Démonstration. Soit n le cardinal commun, f une bijection de $\llbracket 1; n \rrbracket$ dans E , g une bijection de $\llbracket 1; n \rrbracket$ dans F et $\varphi : E \rightarrow F$.

1) $g^{-1} \circ \varphi \circ f$ est une injection de $\llbracket 1; n \rrbracket$ dans lui-même, c'est une bijection, donc φ aussi puisque $\varphi = g \circ (g^{-1} \circ \varphi \circ f) \circ f^{-1}$.

2) $g^{-1} \circ \varphi \circ f$ est une surjection de $\llbracket 1; n \rrbracket$ dans lui-même, c'est une bijection, donc φ aussi puisque $\varphi = g \circ (g^{-1} \circ \varphi \circ f) \circ f^{-1}$. ■

Théorème 13.1.18 Soit E un ensemble fini et F une partie de E , alors $\text{card}(F) \leq \text{card}(E)$ avec égalité si et seulement si E et F sont égaux.

Démonstration. On applique le lemme à l'injection canonique pour obtenir l'inégalité. En cas d'égalité des cardinaux, l'injection canonique est aussi une surjection et son image vaut à la fois E et F . ■

Théorème 13.1.19 Soit $f : E \rightarrow F$. Si E est fini alors $\text{card}(f(E)) \leq \text{card}(E)$ avec égalité si et seulement si f est injective

Démonstration. Comme f induit une surjection de E sur $f(E)$ on a l'inégalité. On a égalité si et seulement si f induit une bijection de E sur $f(E)$, id est f injective. ■

c Opérations binaires

Théorème 13.1.20 Étant donnés E et F deux ensembles finis dis-joints, $E \cup F$ est fini et $\text{card}(E \cup F) = \text{card}(E) + \text{card}(F)$.

Démonstration. E étant fini, il existe une bijection f de $\llbracket 1; |E| \rrbracket$ dans E . De même, il existe une bijection g de $\llbracket 1; |F| \rrbracket$ dans F . Les applications

$$\begin{aligned} h : \llbracket 1; |E| + |F| \rrbracket &\longrightarrow E \cup F \\ i &\longmapsto \begin{cases} f(i) & \text{si } 1 \leq i \leq |E| \\ g(i - |E|) & \text{si } |E| < i \leq |E| + |F| \end{cases} \end{aligned}$$

et

$$\begin{aligned} k : E \cup F &\longrightarrow \llbracket 1; |E| + |F| \rrbracket \\ x &\longmapsto \begin{cases} f^{-1}(x) & \text{si } x \in E \\ |E| + g^{-1}(x) & \text{si } x \in F \end{cases} \end{aligned}$$

sont bien définies.

Pour h , d'une part $\llbracket 1; |E| \rrbracket$ et $\llbracket |E|; |E| + |F| \rrbracket$ sont les deux composantes d'une partition de $\llbracket 1; |E| + |F| \rrbracket$ et d'autre part, si $1 \leq i \leq |E|$, f est définie en i et $f(i) \in E \cup F$ et si $|E| < i \leq |E| + |F|$, on a $0 < i - |E| \leq |F|$, g définie en $i - |E|$ et $g(i - |E|) \in E \cup F$.

Pour k , d'une part E et F sont les deux composantes d'une partition de $E \cup F$ et d'autre part, si on a $x \in E$, f^{-1} est définie en x et on a $f^{-1}(x) \in \llbracket 1; |E| + |F| \rrbracket$ et si $x \in F$, g^{-1} est définie en x et on a $\llbracket 1; |E| + |F| \rrbracket$.

Montrons que h et k sont réciproques l'une de l'autre.

- On a $\forall i \in \llbracket 1; |E| + |F| \rrbracket$, $k \circ h(i) = i$.

Si $1 \leq i \leq |E|$ alors $h(i) \in E$, car $h(i) \stackrel{\text{déf}}{=} f(i)$ et $f(i) \in E$, d'où $k(f(i)) = f^{-1}(f(i)) = i$.

Si $|E| < i \leq |E| + |F|$ alors $h(i) \in F$, car $h(i) \stackrel{\text{déf}}{=} g(i - |E|)$ et $g(i - |E|) \in F$, d'où il vient $k(g(i - |E|)) = |E| + g^{-1}(g(i - |E|)) = |E| + i - |E| = i$.

- On a $\forall x \in E \cup F$, $h \circ k(x) = x$.

Si $x \in E$ alors $k(x) \in \llbracket 1; |E| \rrbracket$, car $k(x) \stackrel{\text{déf}}{=} f^{-1}(x)$ et $f^{-1}(x) \in \llbracket 1; |E| \rrbracket$, d'où il vient $h \circ k(x) = h(f^{-1}(x)) = f(f^{-1}(x)) = x$.

Si $x \in F$ alors $k(x) \in \llbracket |E|; |E| + |F| \rrbracket$, $k(x) \stackrel{\text{déf}}{=} |E| + g^{-1}(x)$ et $g^{-1}(x) \in \llbracket 1; |F| \rrbracket$, d'où il vient $h \circ k(x) = h(|E| + g^{-1}(x)) = g(|E| + g^{-1}(x) - |E|) = g(g^{-1}(x)) = x$.

Ainsi h est bijective et $\text{card}(E \cup F) = \text{card}(E) + \text{card}(F)$. ■

Théorème 13.1.21 Soit F partie de E fini, on a $\text{card}(E \setminus F) = \text{card}(E) - \text{card}(F)$.

Démonstration. Sachant que $E = (E \setminus F) \cup F$ et $(E \setminus F) \cap F = \emptyset$, on applique la proposition précédente d'où $\text{card}(E) = \text{card}(E \setminus F) + \text{card}(F)$. ■

Théorème 13.1.22 Soient E et F deux ensembles finis. $E \cup F$ et $E \cap F$ sont finis et $\text{card}(E \cup F) = \text{card}(E) + \text{card}(F) - \text{card}(E \cap F)$.

Démonstration. $E \cap F$ et $E \setminus F$ sont finis en tant que parties de E qui est fini. De plus, on a $E \cup F = (E \setminus F) \cup F$ avec $(E \setminus F) \cap F = \emptyset$. Par ce qui précède, $E \cup F$ est fini et $\text{card}(E \cup F) = \text{card}(E \setminus F) + \text{card}(F)$. Par ailleurs, on a $E = (E \setminus F) \cup (E \cap F)$ avec $(E \setminus F) \cap (E \cap F) = \emptyset$, d'où par ce qui précède $\text{card}(E) = \text{card}(E \setminus F) + \text{card}(E \cap F)$. En combinant, il vient le résultat. ■

d Principe des bergers

Théorème 13.1.23 Soit $(E_i)_{i \in I}$ avec I fini, telle que

1) $\forall i \in I, E_i$ est fini,

2) $\forall i, j \in I, i \neq j \Rightarrow E_i \cap E_j = \emptyset$

alors $\text{card}\left(\bigcup_{i \in I} E_i\right) = \sum_{i \in I} \text{card}(E_i)^a$.

a. Où sont définies les unions, intersections, sommes et produits finis ?

Démonstration. Par récurrence sur le cardinal de I .

- Initialisation. Si $|I| = 0$, c'est-à-dire I est vide, d'une part la réunion est vide, donc son cardinal est 0, et d'autre part la somme est vide, donc vaut aussi 0.
- Hérédité. Si $|I| = n + 1$, I n'est pas vide et contient i_0 . On a

$$I = I \setminus \{i_0\} \cup \{i_0\} \text{ et } I \setminus \{i_0\} \cap \{i_0\} = \emptyset$$

d'après ce qui précède,

$$n + 1 = |I| = |I \setminus \{i_0\}| \cup |\{i_0\}| = |I \setminus \{i_0\}| + 1$$

d'où $|I \setminus \{i_0\}| = n$.

Par ailleurs,

$$\bigcup_{i \in I} E_i = E_{i_0} \cup \left(\bigcup_{i \in I \setminus \{i_0\}} E_i \right)$$

et

$$E_{i_0} \cap \left(\bigcup_{i \in I \setminus \{i_0\}} E_i \right) = \bigcup_{i \in I \setminus \{i_0\}} (E_{i_0} \cap E_i) = \bigcup_{i \in I \setminus \{i_0\}} \emptyset = \emptyset,$$

donc $\left| \bigcup_{i \in I} E_i \right| = |E_{i_0}| + \left| \bigcup_{i \in I \setminus \{i_0\}} E_i \right| = |E_{i_0}| + \sum_{i \in I \setminus \{i_0\}} |E_i| = \sum_{i \in I} |E_i|$. ■

Lemme 13.1.24 — des bergers. Soit E un ensemble et E_1, \dots, E_r une partition de E . Si $\text{card } E_1 = \dots = \text{card } E_r = p$ alors $\text{card } E = r \times p$.

Démonstration. $\text{card } E = \text{card} \left(\bigcup_{i=1}^r E_i \right) = \sum_{i=1}^r \text{card}(E_i) = p \sum_{i=1}^r 1 = r \times p$ ■

Théorème 13.1.25 — des bergers. Soient E, F deux ensembles finis et $f : E \rightarrow F$ une application surjective telle que tout élément de F a exactement n antécédents dans E . Alors on a $\text{card}(E) = n \times \text{card}(F)$.

Démonstration. On sait que $\bigcup_{y \in f(E)} \bar{f}^{-1}(y)$ est une partition¹ de E et par surjection $f(E) = F$, donc

$$|E| = \left| \bigcup_{y \in F} \bar{f}^{-1}(y) \right| = \sum_{y \in F} \left| \bar{f}^{-1}(y) \right| = n \sum_{y \in F} 1 = n \times |F|. \quad \blacksquare$$

Théorème 13.1.26 Soit $f : E \rightarrow F$ avec E fini.

$$\text{card}(E) = \sum_{y \in F} \text{card}(\bar{f}^{-1}(y))$$

Démonstration. C'est une partie de la preuve précédente. ■

e Produit cartésien

Théorème 13.1.27 Soient G et F deux ensembles finis alors $G \times F$ est fini et

$$\text{card}(G \times F) = \text{card}(G) \times \text{card}(F)$$

Démonstration. Soit g une bijection de $\llbracket 1; |G| \rrbracket$ dans G et f une bijection de $\llbracket 1; |F| \rrbracket$ dans F . Les applications

$$\begin{aligned} h : \llbracket 1; |G| \rrbracket \times \llbracket 1; |F| \rrbracket &\longrightarrow G \times F \\ (i; j) &\longmapsto (g(i); f(j)) \end{aligned}$$

et

$$\begin{aligned} k : G \times F &\longrightarrow \llbracket 1; |G| \rrbracket \times \llbracket 1; |F| \rrbracket \\ (x; y) &\longmapsto (g^{-1}(x); f^{-1}(y)) \end{aligned}$$

sont bien définies et réciproques l'une de l'autre car

$$\forall (i; j) \in \llbracket 1; |G| \rrbracket \times \llbracket 1; |F| \rrbracket,$$

$$k \circ h(i; j) = k(g(i), f(j)) = (g^{-1} \circ g(i), f^{-1} \circ f(j)) = (i; j)$$

1. Voir le chapitre sur les relations d'équivalence.

$$\forall (i; j) \in \llbracket 1; |G| \rrbracket \times \llbracket 1; |F| \rrbracket,$$

$$k \circ h(i; j) = k(g(i), f(j)) = (g^{-1} \circ g(i), f^{-1} \circ f(j)) = (i; j)$$

$$\forall (x, y) \in G \times F,$$

$$h \circ k(x, y) = h(g^{-1}(x), f^{-1}(y)) = (g \circ g^{-1}(x), f \circ f^{-1}(y)) = (x, y)$$

Cela montre que h est bijective, donc $G \times F$ et $\llbracket 1; |G| \rrbracket \times \llbracket 1; |F| \rrbracket$ sont équipotents.

De plus, les applications

$$\begin{aligned} h : \llbracket 1; |G| \rrbracket \times \llbracket 1; |F| \rrbracket &\longrightarrow \llbracket 1; |G| \times |F| \rrbracket \\ (i; j) &\longmapsto (i-1)|F| + j \end{aligned}$$

et

$$\begin{aligned} k : \llbracket 1; |G| \times |F| \rrbracket &\longrightarrow \llbracket 1; |G| \rrbracket \times \llbracket 1; |F| \rrbracket \\ n &\longmapsto (1 + (n-1) \div |F|; 1 + (n-1) \% |F|) \end{aligned}$$

sont bien définies et réciproques l'une de l'autre. Pour h , l'ensemble d'arrivée est justifié par

$$1 \leq i \leq |G| \text{ et } 1 \leq j \leq |F| \Rightarrow 1 \leq (i-1)|F| + j \leq (|G|-1)|F| + |F| = |G||F|$$

et pour g , l'ensemble d'arrivée est justifié par

$$\begin{aligned} 1 \leq n \leq |G||F| &\Rightarrow 0 \leq n-1 \leq |G||F|-1 \Rightarrow 0 \leq (n-1) \div |F| \leq |G|-1 \\ &\Rightarrow 1 \leq 1 + (n-1) \div |F| \leq |G| \end{aligned}$$

$$\text{et } 0 \leq (n-1) \% |F| \leq |F|-1 \Rightarrow 1 \leq 1 + (n-1) \% |F| \leq |F|.$$

Pour la réciprocité, on a

$$\begin{aligned} k \circ h(i; j) &= k((i-1)|F| + j) \\ &= (1 + ((i-1)|F| + j - 1) \div |F|; 1 + ((i-1)|F| + j - 1) \% |F|) \\ &= (1 + (i-1) + (j-1) \div |F|; 1 + (j-1) \% |F|) \\ &= (i; j) \end{aligned}$$

sachant que

$$1 \leq j \leq |F| \Rightarrow 0 \leq j-1 \leq |F|-1 \Rightarrow (j-1) \div |F| = 0$$

et $(j-1) \div |F| = j-1$ et

$$\begin{aligned} h \circ k(n) &= h((1 + (n-1) \div |F|; 1 + (n-1) \% |F|)) \\ &= (1 + (n-1) \div |F| - 1)|F| + 1 + (n-1) \% |F| \\ &= 1 + ((n-1) \div |F|)|F| + (n-1) \% |F| \end{aligned}$$

qui fait apparaître la division euclidienne de $n-1$ par $|F|$ et donne $h \circ k(n) = h$.

Ainsi k est bijective, donc $\llbracket 1; |G| \rrbracket \times \llbracket 1; |F| \rrbracket$ est fini et son cardinal est $|G||F|$. Comme il est équipotent à $G \times F$, ce dernier est fini et de même cardinal. ■

Théorème 13.1.28 Pour tout $j \in \mathbb{N}^*$, $\text{card}(E^j) = (\text{card}(E))^j$.

Démonstration. Par récurrence sur j dans \mathbb{N}^* .

- Initialisation. Pour $j = 1$, on a $\text{card}(E^1) = \text{card}(E) = (\text{card}(E))^1$.
- Hérédité. Par ce qui précède, $|E^{j+1}| = |E^j \times E| = |E^j||E| = |E|^j|E| = |E|^{j+1}$.



14. Combinatoire

14.1 Combinatoire

Listes, combinaisons, factorielles, formule du binôme.

14.1.1 Factorielle

a Définition et propriétés

Définition 14.1.1 — Factorielle. $(n!)_{n \geq 0}$ désigne la suite bien définie par $0! = \text{déf}1$ et $\forall n \in \mathbb{N}, (n+1)! = (n+1) \times n$.

R c'est aussi la définition¹ de $n! = \prod_{i=1}^n i$. Pour $n = 0$ on obtient un produit vide qui vaut donc 1. En extension $n! = n \times (n-1) \times (n-2) \dots 2 \times 1$.

Proposition 14.1.1 $\sum_{k=0}^{\infty} \frac{x^k}{k!}$ converge normalement sur toute partie bornée de \mathbb{C} vers $x \mapsto e^x$. En particulier $\sum_{k=0}^{\infty} \frac{1}{k!} = e$.

Démonstration. En utilisant la règle de d'Alembert, comme on a $\limsup_{n \rightarrow +\infty} \left| \frac{x^{n+1}}{(n+1)!} \right| = 0$, le rayon de convergence de la série est $+\infty$. Par le lemme d'Abel, on en déduit que la série converge normalement sur toute partie bornée de \mathbb{C} .

Que la limite soit l'exponentielle dépend de la façon dont celle-ci est définie.

Une autre preuve de la convergence de $\sum_{k=0}^{\infty} \frac{1}{k!}$. On montre par récurrence que $\forall n \in \mathbb{N}, (n+1)! \geq 2^n$.

1. Où sont définis les produits ?

1) Initialisation. $1! = 1$ et $2^0 = 1$.

2) Hérédité. $(n+2)! = (n+1)!(n+2) \geq 2^n \times 2 = 2^{n+1}$.

Donc à partir du rang 1, on a $\frac{1}{n!} \leq \frac{1}{2^{n-1}}$. $\sum_{k=0}^{\infty} \frac{1}{k!}$ est une série à termes positifs, dont les termes sont majorés par ceux d'une série géométrique convergente, elle est donc convergente. ■

Théorème 14.1.2

$$\forall n \in \mathbb{N}, \int_0^{+\infty} e^{-t} t^n dt = n!$$

Démonstration. Par récurrence sur k .

1) Initialisation.

$$\int_{t=0}^{+\infty} e^{-t} dt = \lim_{A \rightarrow +\infty} \int_{t=0}^A e^{-t} dt = \lim_{A \rightarrow +\infty} [-e^{-t}]_{t=0}^A = 1$$

2) Hérédité. On intègre par parties (à vérifier...)

$$\begin{aligned} \int_{t=0}^{+\infty} e^{-t} t^{n+1} dt &= \lim_{A \rightarrow +\infty} \int_{t=0}^A e^{-t} t^{n+1} dt \\ &= \lim_{A \rightarrow +\infty} [e^{-t} t^{n+1}]_0^A + \lim_{A \rightarrow +\infty} (n+1) \int_{t=0}^A e^{-t} t^n dt \\ &= (n+1) \int_{t=0}^{+\infty} e^{-t} t^n dt = (n+1)! \end{aligned}$$

b Formule de Stirling

Théorème 14.1.3 — Stirling.

$$n! \underset{n \rightarrow +\infty}{\sim} n^n e^{-n} \sqrt{2\pi n}$$

Démonstration. En trois lemmes. ■

Lemme 14.1.4 Il existe une constante C positive telle que $n! \sim C n^n e^{-n} \sqrt{n}$.

Démonstration. Posons $u_n \stackrel{\text{déf}}{=} \ln \left(\frac{n!}{n^n e^{-n} \sqrt{n}} \right)$. On a

$$\begin{aligned} u_n &= \ln(n!) - \ln(n^n) - \ln(e^{-n}) - \ln(\sqrt{n}) \\ &= \ln(n!) - n \ln(n) + n - \frac{1}{2} \ln(n) \\ &= \ln(n!) - \left(n + \frac{1}{2}\right) \ln n + n \end{aligned}$$

et

$$\begin{aligned} u_{n+1} - u_n &= \ln((n+1)!) - \left(n+1 + \frac{1}{2}\right) \ln(n+1) + n+1 \\ &\quad - \left(\ln n! - \left(n + \frac{1}{2}\right) \ln(n) + n\right) \\ &= 1 - \left(n + \frac{1}{2}\right) \ln \frac{n+1}{n} \end{aligned}$$

D'après la formule de Taylor-Young, au voisinage de 0,

$$\ln(1+x) = x - \frac{x^2}{2} + O(x^3).$$

Par conséquent quand n est grand :

$$u_{n+1} - u_n = 1 - \left(n + \frac{1}{2}\right) \left(\frac{1}{n} - \frac{1}{2n^2} + O\left(\frac{1}{n^3}\right)\right) = O\left(\frac{1}{n^2}\right)$$

La série de terme général $u_{n+1} - u_n$ est donc absolument convergente et la suite u_n admet une limite notée c . Ainsi, $\frac{n!}{n^n e^{-n} \sqrt{n}}$ tend vers e^c qui est la constante cherchée. ■

Lemme 14.1.5 Soient les intégrales de Wallis définies par

$$\forall n \in \mathbb{N}, I_n \stackrel{\text{déf}}{=} \int_{x=0}^{\pi/2} \cos^n x \, dx.$$

On a

$$I_n \underset{n \rightarrow +\infty}{\sim} \sqrt{\frac{\pi}{2n}}$$

Démonstration. En intégrant par parties, on montre que pour tout entier n , $(n+2)I_{n+2} = (n+1)I_n$.

$$\begin{aligned} I_{n+2} &= \int_{x=0}^{\pi/2} \cos^{n+2} x \, dx = \int_{x=0}^{\pi/2} (\cos^{n+1} x)(\sin x)' \, dx \\ &= [\cos^{n+1} x \sin x]_{x=0}^{\pi/2} - \int_{x=0}^{\pi/2} (\cos^{n+1} x)' \sin x \, dx \\ &= \int_{x=0}^{\pi/2} (n+1) \sin x \cos^n x \sin x \, dx \\ &= (n+1) \int_{x=0}^{\pi/2} \cos^n x \sin^2 x \, dx = (n+1) \int_{x=0}^{\pi/2} \cos^n x (1 - \cos^2 x) \, dx \\ \text{phantom} I_{n+2} &= (n+1) \int_{x=0}^{\pi/2} \cos^n x - \cos^{n+2} x \, dx = (n+1)(I_n - I_{n+2}) \end{aligned}$$

D'où, $(n+2)I_{n+2} = (n+1)I_n$, puis $(n+2)I_{n+1}I_{n+2} = (n+1)I_nI_{n+1}$ et $(n+1)I_nI_{n+1}$ ne dépend pas de n . Comme par ailleurs $I_0 = \int_{x=0}^{\pi/2} dx = \frac{\pi}{2}$ et $I_1 = \int_{x=0}^{\pi/2} \cos x \, dx = 1$, on a $(n+1)I_nI_{n+1} = I_1I_0 = \frac{\pi}{2}$.

En intégrant $0 < \cos^{n+1} x \leq \cos^n x$ sur $[0, \pi/2[$, on trouve que $0 < I_{n+1} \leq I_n$ et par conséquent $\frac{I_{n+1}}{I_n} \leq 1$. Par la relation de récurrence ci-dessus, on a $\frac{I_{n+1}}{I_n} = \frac{n+1}{n+2} \frac{I_{n+1}}{I_{n+2}} \geq \frac{n+1}{n+2}$, ce qui donne $\frac{n+1}{n+2} \leq \frac{I_{n+1}}{I_n} \leq 1$. Le théorème des gendarmes donne $I_{n+1} \underset{n \rightarrow +\infty}{\sim} I_n$ puis $(n+1)I_nI_{n+1} \underset{n \rightarrow +\infty}{\sim} nI_n^2$ d'où le résultat. ■

Lemme 14.1.6 Pour tout entier naturel p , on a $I_{2p} = \frac{\pi}{2} \frac{(2p)!}{2^{2p} p!^2}$.

Démonstration. Par récurrence sur p .

1) Initialisation. $I_0 = \frac{\pi}{2}$ et $\frac{\pi}{2} \frac{0!}{2^0 0!^2} = \frac{\pi}{2}$

2) Hérédité.

$$I_{2(p+1)} = \frac{2p+1}{2p+2} I_{2p} = \frac{2p+2}{2p+2} \times \frac{2p+1}{2p+2} \times \frac{\pi}{2} \frac{(2p)!}{2^{2p} p!^2} = \frac{\pi}{2} \times \frac{(2(p+1))!}{2^{2p+2} ((p+1)!)^2}$$

Pour finir $I_{2p} \underset{p \rightarrow +\infty}{\sim} \sqrt{\frac{\pi}{4p}}$ on a donc par i)

$$\sqrt{\frac{\pi}{4p}} \underset{p \rightarrow +\infty}{\sim} \frac{\pi}{2} \frac{(2p)!}{2^{2p} p!^2} \underset{p \rightarrow +\infty}{\sim} \frac{\pi}{2} \frac{C(2p)^{2p} e^{-2p} \sqrt{2p}}{2^{2p} (Cp^p e^{-p} \sqrt{p})^2} \underset{p \rightarrow +\infty}{\sim} \frac{\pi}{2} \frac{\sqrt{2}}{C\sqrt{p}}$$

qui donne $C = \sqrt{2\pi}$. ■

14.1.2 Listes et application

Définition 14.1.2 — Liste. F étant un ensemble, une **liste** de p éléments de F est une application de $\llbracket 1; p \rrbracket$ dans F . Elle peut être notée $(x_i)_{1 \leq i \leq p}$. La **longueur** de la liste est p .

R on rencontre souvent p -liste pour signifier liste de longueur p , même si ce n'est pas très heureux. La notion d'ordre des éléments est primordiale.

► **Exemple 14.1** Si $F = \{y_1, y_2, y_3\}$, il y a neuf listes de deux éléments de F qui sont : (y_1, y_1) , (y_1, y_2) , (y_1, y_3) , (y_2, y_2) , (y_2, y_1) , (y_2, y_3) , (y_3, y_3) , (y_3, y_2) , (y_3, y_1) . ▲

Théorème 14.1.7 Soient E et F deux ensembles finis, l'ensemble F^E des applications de E dans F est fini et son cardinal est $(\text{card } F)^{\text{card } E}$.

Démonstration. Si E et F sont vides, comme il n'existe qu'une seule application de \emptyset dans lui-même, $\text{card}(\emptyset^\emptyset) = 1 = 0^0$. Si F est vide mais pas E , il n'existe aucune application de E dans \emptyset et $\text{card}(\emptyset^E) = 0 = 0^{\text{card}(E)}$. Si F n'est pas vide, on montre le théorème par récurrence sur le cardinal de E .

1) Initialisation : déjà vu ci-dessus.

2) Hérédité. Considérons E de cardinal $p + 1$. N'étant pas vide, soit x l'un de ses éléments et $E' = E \setminus \{x\}$. E' est fini, de cardinal p . Considérons

$$\begin{aligned} \varphi : F^E &\longrightarrow F^{E'} \times F \\ f &\longmapsto (f|_{E'}; f(x)) \end{aligned}$$

C'est une injection car si on a $(f|_{E'}; f(x)) = (g|_{E'}; g(x))$ alors $f(z) = g(z)$ si $z = x$ et $f(z) = f|_{E'}(z) = g|_{E'}(z) = g(z)$ sinon. C'est une

surjection car un élément $(g; y)$ de $F^{E'} \times F$ a pour antécédent

$$\begin{aligned} f : E &\longrightarrow F \\ z &\longmapsto \begin{cases} g(z) & \text{si } z \in E' \\ y & \text{sinon} \end{cases} \end{aligned}$$

Ainsi, φ est une bijection et

$$\text{card}(F^E) = \text{card}(F^{E'}) \times |F| = |F|^p \times |F| = |F|^{p+1} = \text{card}(F)^{\text{card}(E)}. \quad \blacksquare$$

Théorème 14.1.8 Soit F un ensemble fini de cardinal n . Le nombre de listes d'éléments de F de longueur p est n^p .

Démonstration. On applique ce qui précède à $E = \llbracket 1; p \rrbracket$. \blacksquare

14.1.3 Arrangements et injections

Définition 14.1.3 F étant un ensemble, un **arrangement** de p éléments de F est une liste de p éléments de F sans répétition *id est* une application injective de $\llbracket 1; p \rrbracket$ dans F .

► **Exemple 14.2** Si $F = \{y_1, y_2, y_3\}$, il y a six arrangements de deux éléments qui sont : (y_1, y_2) , (y_1, y_3) , (y_2, y_1) , (y_2, y_3) , (y_3, y_2) , (y_3, y_1) .
▲

Théorème 14.1.9 Soient les ensembles finis E de cardinal p et F de cardinal n . Le nombre d'injections de E dans F est A_n^p où

$$A_n^p = \prod_{i=n-p+1}^n i.$$

R Pseudo preuve non rigoureuse.

- il y a n possibilités de choisir le premier élément,
- il y a $(n-1)$ possibilités de choisir le deuxième élément (car les éléments doivent être mutuellement distincts),
- ...
- il y a $(n - (p - 1))$ possibilités de choisir le p^{e} élément.

Il y a donc $n \times (n-1) \times \dots \times (n - (p-1)) = \frac{n!}{(n-p)!} = A_n^p$ possibilités d'arrangements de p éléments dans n .

Démonstration. Remarque préliminaire. S'il existe une injection de E dans F alors on a $\text{card}(E) \leq \text{card}(F)$. Par contraposition, si $\text{card}(F) < \text{card}(E)$, *id est* $n < p$, il n'y a pas d'injection de E dans F . Dans ce cas, on a $n - p + 1 \leq 0 \leq n$, donc le produit contient 0 et $\prod_{i=n-p+1}^n i = 0 = A_n^p$.

Par récurrence sur p , n étant fixé.

1) Initialisation. L'application vide est l'unique application injective de \emptyset dans F , donc $A_n^0 = 1$. De plus $\prod_{i=n+1}^n i = 1$ car c'est un produit vide.

2) Hérédité. La remarque préliminaire donne l'hérédité pour $n \leq p$ car toute implication de conclusion vraie est vraie. Il reste à montrer que pour $p < n$ on a

$$A_n^p = \prod_{i=n-p+1}^n i \Rightarrow A_n^{p+1} = \prod_{i=n-(p+1)+1}^n i$$

ou plus simplement, $A_n^{p+1} = (n-p)A_n^p$. Pour cela, considérons E de cardinal $p+1$. N'étant pas vide, soit x l'un de ses éléments et $E' = E \setminus \{x\}$. E' est fini, de cardinal p . Considérons aussi

Cette application est bien définie puisque toute restriction d'une application injective est injective. Soit g de $I(E'; F)$, considérons

$$\psi_g : \begin{array}{ccc} \bar{\varphi}^{-1}(g) & \longrightarrow & F \\ f & \longmapsto & f(x) \end{array}$$

Cette application est injective, car on a $f(x) = f'(x)$ **et** $f|_{E'} = f'|_{E'} \Rightarrow f = f'$.

Par conséquent on a $\text{Im } \psi_g \subset F \setminus \text{Im } g$. Pour tout y de $F \setminus \text{Im } g$, l'application

$$f_y : \begin{array}{ccc} E & \longrightarrow & F \\ z & \longmapsto & \begin{cases} y \text{ si } z = x \\ g(z) \text{ sinon} \end{cases} \end{array}$$

est dans $\bar{\varphi}^{-1}(g)$. À compléter...

Ainsi, on a $\text{Im } \psi_g = F \setminus \text{Im } g$. De là, ψ_g est une bijection entre $\bar{\varphi}^{-1}(g)$ et $F \setminus \text{Im } g$ et

$$\text{card} \left(\bar{\varphi}^{-1}(g) \right) = \text{card} (F \setminus \text{Im}(g)) = |F| - |\text{Im}(g)| = n - |E'| = n - p.$$

Par le lemme des bergers,

$$A_n^{p+1} = \text{card} (I(E; F)) = (n-p) \text{card} (I(E'; F)) = (n-p)A_n^p.$$

■

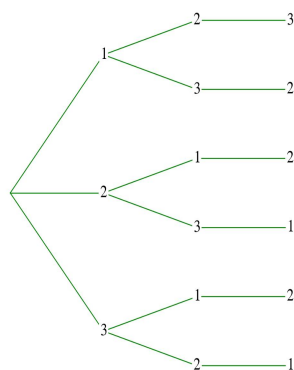
Théorème 14.1.10 Si $p \leq n$ alors $A_n^p = \frac{n!}{(n-p)!}$.

Démonstration. En exercice...

■

R le nombre d'arrangements de p éléments d'un ensemble de cardinal n est A_n^p .

14.1.4 Bijections et permutations.



Proposition 14.1.11 — Nombre de bijections. Soient E et F deux ensembles finis de même cardinal n . Le nombre de bijections de E sur F est n .

Démonstration. À cause du cardinal commun, les bijections de E sur F sont les injections de E dans F , il y en a donc A_n^n or on a $A_n^n = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!$. ■

Définition 14.1.4 — Permutation. Soit F un ensemble. Une **permutation** de F désigne une bijection de F sur F . L'ensemble des permutations de F est noté \mathfrak{S}_F .

Théorème 14.1.12 Si F est fini et ordonné, une permutation de F est entièrement déterminée par une liste ordonnée de $|F|$ éléments de F , à ce titre, c'est un arrangement de $|F|$ éléments de F .

Démonstration. À compléter... ■

► **Exemple 14.3** Soit $F = \{1; 2; 3\}$. Faisons un arbre des différentes possibilités :

Les permutations de F sont : $(1; 2; 3)$, $(1; 3; 2)$, $(2; 1; 3)$, $(2; 3; 1)$, $(3; 1; 2)$, $(3; 2; 1)$. (Refaire le dessin) ▲

Théorème 14.1.13 — Nombre de permutations. Le nombre de permutations d'un ensemble à n éléments est $n!$.

Démonstration. C'est le théorème ci-dessus avec $E = F$. ■

14.1.5 Combinaisons

a Combinaison et coefficient binomial

Définition 14.1.5 Une combinaison de p éléments de E désigne toute partie de E contenant p éléments.

Théorème 14.1.14 Le nombre de combinaisons de p éléments est le même pour tous les ensembles de même cardinal, il est noté $\binom{n}{p}$ et lu « p parmi n ».

Démonstration. En exercice... ■

Théorème 14.1.15 On a

$$\binom{n}{p} = \begin{cases} \frac{n!}{p!(n-p)!} & \text{si } 0 \leq p \leq n \\ 0 & \text{sinon.} \end{cases}$$

Démonstration. Toute partie d'un ensemble fini a moins d'élément que l'ensemble. Par contraposition, il n'y a aucune partie avec strictement plus d'éléments. Cela donne le résultat si $p > n$.

Pour $0 \leq p \leq n$, soit F de cardinal n . Notons $\mathcal{P}_p(F) = \{A \subset F \mid \text{card}(A) = p\}$ et considérons

$$\begin{array}{ccc} \varphi_p : I(\llbracket 1; p \rrbracket; F) & \longrightarrow & \mathcal{P}_p(F) \\ f & \longmapsto & \text{Im } f \end{array}$$

Pour A de $\mathcal{P}_p(F)$, on a

$$\bar{\varphi}_p^{-1}(A) = \{f : \llbracket 1; p \rrbracket \rightarrow F \mid f \text{ injective et } \text{Im}(f) = A\}$$

donc $\bar{\varphi}_p^{-1}(A)$ est équipotent à l'ensemble des bijections de $\llbracket 1; p \rrbracket$ dans A et son cardinal vaut $p!$. On obtient $\text{card}(I(\llbracket 1; n \rrbracket; F)) = p! \times \text{card}(\mathcal{P}_p(F))$ par le principe des bergers, d'où il vient $\binom{n}{p} = \text{card}(\mathcal{P}_p(F)) = \frac{A_n^p}{p!} = \frac{n!}{p!(n-p)!}$. ■

Lemme 14.1.16 Soient $n, p \in \mathbb{N}$. Alors $n!p! \mid (n+p)!$.

Démonstration. On a $\binom{n+p}{p} = \frac{(n+p)!}{p!(n+p-p)!} = \frac{(n+p)!}{n!p!}$ donc $n!p! \binom{n+p}{p} = (n+p)!$ avec $\binom{n+p}{p} \in \mathbb{N}$, ce qui démontre le résultat. ■

b Formule de Pascal

Théorème 14.1.17 — Formule de Pascal.

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

Démonstration. Soient E un ensemble de cardinal $n+1$ éléments, $a \in E$ et $E' = E \setminus \{a\}$, qui a n éléments. Il y a deux sortes différentes de parties de E ayant p éléments :

1) celles qui ne contiennent pas a : ce sont des parties à p éléments dans E' , il y en a donc $\binom{n}{p}$,

2) celles qui contiennent a : elles sont de la forme $\{a\} \cup A'$ avec A' une partie à $p-1$ éléments de E' . Il y en a $\binom{n}{p-1}$.

Par somme, cela donne le résultat.

D'une autre manière, on a :

$$\begin{aligned} \binom{n+1}{p} - \left(\binom{n}{p} + \binom{n}{p-1} \right) &= \frac{(n+1)!}{p!(n+1-p)!} - \left(\frac{n!}{p!(n-p)!} + \frac{n!}{(p-1)!(n-p+1)!} \right) \\ &= \frac{n!}{p!(n+1-p)!} ((n+1) - (n+1-p) - p) = 0 \quad \blacksquare \end{aligned}$$

c Triangle de Pascal

Chaque entrée du triangle de Pascal est la somme du nombre situé au-dessus à gauche et de celui situé au-dessus dans la même colonne, ce qui se traduit bien par la formule vue précédemment.

| $p \setminus n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Σ |
|-----------------|---|---|----|----|----|----|----|---|---|-------------|
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $1 = 2^0$ |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $2 = 2^1$ |
| 2 | 1 | 2 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | $4 = 2^2$ |
| 3 | 1 | 3 | 3 | 1 | 0 | 0 | 0 | 0 | 0 | $8 = 2^3$ |
| 4 | 1 | 4 | 6 | 4 | 1 | 0 | 0 | 0 | 0 | $16 = 2^4$ |
| 5 | 1 | 5 | 10 | 10 | 5 | 1 | 0 | 0 | 0 | $32 = 2^5$ |
| 6 | 1 | 6 | 15 | 20 | 15 | 6 | 1 | 0 | 0 | $64 = 2^6$ |
| 7 | 1 | 7 | 21 | 35 | 35 | 21 | 7 | 1 | 0 | $128 = 2^7$ |
| 8 | 1 | 8 | 28 | 56 | 70 | 56 | 28 | 8 | 1 | $256 = 2^8$ |

d Propriétés

Théorème 14.1.18 Pour tous n et p entiers naturels tels que $0 \leq p \leq n$, on a

$$\begin{aligned} \binom{n}{p} &= \binom{n}{n-p}, \quad \binom{n}{0} = \binom{n}{n} = 1 \\ \binom{n}{1} &= \binom{n}{n-1} = n \text{ et } n \binom{n-1}{k-1} = k \binom{n}{k} \end{aligned}$$

Démonstration.

$$\binom{n}{n-p} = \frac{n!}{(n-p)!(n-(n-p))!} = \frac{n!}{p!(n-p)!} = \binom{n}{p}$$

$$\binom{n}{0} = \binom{n}{n-0} = \frac{n!}{0!n!} = 1$$

$$\binom{n}{n-1} = \binom{n}{1} = \frac{n!}{1!(n-1)!} = n$$

$$\begin{aligned}
n \binom{n-1}{k-1} - k \binom{n}{k} &= \frac{n(n-1)!}{(k-1)!(n-k)!} - \frac{kn!}{k!(n-k)!} \\
&= \frac{n!}{(k-1)!(n-k)!} - \frac{n!}{(k-1)!(n-k)!} = 0. \quad \blacksquare
\end{aligned}$$

e Formule du binôme

Théorème 14.1.19 Soient x et y deux éléments d'un anneau qui commutent. Pour tout entier naturel n , on a

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

Démonstration. Par récurrence sur n .

1) Initialisation. Sachant que $z^0 = 1$,

$$\sum_{k=0}^0 \binom{0}{k} x^k y^{0-k} = \binom{0}{0} x^0 y^0 = 1$$

et $(x + y)^0 = 1$.

2) Hérédité.

$$\begin{aligned}
(x + y)^{n+1} &= (x + y)(x + y)^n \\
&= (x + y) \sum_{k=0}^n \binom{n}{k} x^k y^{n-k} \\
&= \sum_{k=0}^n \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=0}^n \binom{n}{k} x^k y^{n+1-k} \\
&= x^{n+1} + \sum_{k=0}^{n-1} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=1}^n \binom{n}{k} x^k y^{n+1-k} + y^{n+1} \\
&= x^{n+1} + \sum_{k=0}^{n-1} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=0}^{n-1} \binom{n}{k+1} x^{k+1} y^{n-k} + y^{n+1} \\
&= x^{n+1} + \sum_{k=0}^{n-1} \left(\binom{n}{k} + \binom{n}{k+1} \right) x^{k+1} y^{n-k} + y^{n+1} \\
&= x^{n+1} + \sum_{k=0}^{n-1} \binom{n+1}{k+1} x^{k+1} y^{n-k} + y^{n+1} \\
&= x^{n+1} + \sum_{k=1}^n \binom{n+1}{k} x^k y^{n+1-k} + y^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} x^k y^{n+1-k}
\end{aligned}$$

Autre démonstration avec les polynômes. $(X + y)^{n+1}$ est un polynôme en X à coefficients dans $\mathbb{Z}[y]$. Son polynôme dérivé est $(n+1)(X + y)^n$ donc

$$\begin{aligned}(X + y)^{n+1} &= y^{n+1} + \sum_{k=0}^n \binom{n}{k} \frac{X^{k+1}}{k+1} y^{n-k} \\ &= y^{n+1} + \sum_{k=0}^n \binom{n+1}{k+1} X^{k+1} y^{n-k} \\ &= y^{n+1} + \sum_{k=1}^{n+1} \binom{n+1}{k} X^k y^{n+1-k} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} X^k y^{n+1-k}\end{aligned}$$

■

Théorème 14.1.20 Pour tout entier naturel n , on a

$$\sum_{k=0}^n \binom{n}{k} = 2^n \text{ et } \sum_{k=0}^n (-1)^k \binom{n}{k} = 0.$$

Démonstration.

$$\begin{aligned}2^n &= (1 + 1)^n = \sum_{k=0}^n \binom{n}{k} 1^k 1^{n-k} = \sum_{k=0}^n \binom{n}{k} \\ 0 &= 0^n = (-1 + 1)^n = \sum_{k=0}^n \binom{n}{k} (-1)^k 1^{n-k} = \sum_{k=0}^n (-1)^k \binom{n}{k}\end{aligned}$$

■

Théorème 14.1.21 Si $\text{card}(E) = n$ alors $\text{card}(\mathcal{P}(E)) = 2^n$.

Démonstration. Pour $0 \leq k \leq n$, $\mathcal{P}_k(E)$ désigne l'ensemble des parties de E de cardinal k . Ces ensembles forment une partition de $\mathcal{P}(E)$ donc

$$\text{card}(\mathcal{P}(E)) = \sum_{k=0}^n \text{card}(\mathcal{P}_k(E)) = \sum_{k=0}^n \binom{n}{k} = 2^n.$$

Autre preuve. $\mathcal{P}(E)$ est équipotent à $\{0; 1\}^E$. À compléter... ■

Théorème 14.1.22 — Formule de Vandermonde. Soit m , n et p trois entiers naturels, on a $\sum_{k=0}^p \binom{m}{k} \binom{n}{p-k} = \binom{m+n}{p}$

Démonstration. Soient E et F deux ensembles disjoints de cardinal m et n , respectivement. Alors $\text{card}(E \cup F) = m + n$ et il y a en tout $\binom{m+n}{p}$ parties de $E \cup F$ de cardinal p .

Une telle partie se compose de k éléments de E et $p - k$ éléments de F , où $0 \leq k \leq p$. Pour k fixé, on obtient $\binom{m}{k} \binom{n}{p-k}$ parties de $E \cup F$ de cette sorte. Comme les parties de $E \cup F$ ainsi obtenues sont distinctes, le nombre total de parties de $E \cup F$ de cardinal p est $\sum_{k=0}^p \binom{m}{k} \binom{n}{p-k}$. D'où l'égalité.

Autre preuve. Dans $\mathbb{Z}[X]$, on a $(1 + X)^m (1 + X)^n = (1 + X)^{m+n} = \sum_{p=0}^{m+n} \binom{m+n}{p} X^p$ et par ailleurs,

$$\begin{aligned} (1 + X)^m (1 + X)^n &= \left(\sum_{i=0}^m \binom{m}{i} X^i \right) \left(\sum_{j=0}^n \binom{n}{j} X^j \right) \\ &= \sum_{i=0}^m \sum_{j=0}^n \binom{m}{i} \binom{n}{j} X^{i+j} \\ &= \sum_{p=0}^{m+n} \sum_{\substack{0 \leq i, j \\ i+j=p}} \binom{m}{i} \binom{n}{j} X^{i+j}. \end{aligned}$$

Par identification des coefficients de degré p , on obtient le résultat. ■

Théorème 14.1.23 — Formule de Chu. Soient p et n deux entiers naturels tels que $0 \leq p \leq n$, on a

$$\sum_{k=p}^n \binom{k}{p} = \binom{n+1}{p+1}$$

Démonstration.

$$\begin{aligned} \sum_{k=p}^n \binom{k}{p} &= \sum_{k=p}^n \left(\binom{k+1}{p+1} - \binom{k}{p+1} \right) \\ &= \sum_{j=p+1}^{n+1} \binom{j}{p+1} - \sum_{k=p}^n \binom{k}{p+1} \\ &= \binom{n+1}{p+1} - \binom{p}{p+1} \\ &= \binom{n+1}{p+1} \end{aligned}$$

f Application aux développements en séries entières

Théorème 14.1.24 Pour tout $k \in \mathbb{N}$ et $z \in \mathbb{C}$ avec $|z| < 1$, on a

$$\frac{1}{(1 - z)^{k+1}} = \sum_{n \geq 0} \binom{n+k}{k} z^n$$

Démonstration. Par récurrence.

1) Initialisation. $\sum_{n \geq 0} \binom{n}{0} z^n = \sum_{n \geq 0} z^n = \frac{1}{1-z}$.

2) Hérédité. On utilise la formule de Chu dans

$$\begin{aligned} \frac{1}{(1-z)^{k+1}} &= \sum_{n \geq 0} \binom{n+k-1}{k-1} z^n \times \sum_{n \geq 0} z^n \\ &= \sum_{n \geq 0} \sum_{p+q=n} z^p \binom{q+k-1}{k-1} z^q \\ &= \sum_{n \geq 0} \left(\sum_{q=0}^n \binom{q+k-1}{k-1} \right) z^n \\ &= \sum_{n \geq 0} \binom{n+k}{k} z^n \end{aligned}$$

■

Définition 14.1.6 — Coefficient binomial généralisé. Pour tout entier naturel p et tout nombre α on pose

$$\binom{\alpha}{p} \stackrel{\text{déf}}{=} \frac{\prod_{i=0}^{p-1} \alpha - i}{p!}$$

Théorème 14.1.25 — Dérivées successives des puissances.

$$(x \mapsto x^\alpha)^{(p)} = p! \binom{\alpha}{p} (x \mapsto x^{\alpha-p})$$

Démonstration. Par récurrence sur p . À compléter... ■

Théorème 14.1.26 — Majoration des coefficients binomiaux.

Pour $|\alpha| < \ln p$, on a $\left| \binom{\alpha}{p} \right| \leq 3^{\lceil |\alpha| \rceil} \lceil |\alpha| \rceil^{\lceil |\alpha| \rceil} p^{\lceil |\alpha| \rceil}$.

Démonstration. Pour α entier naturel, le coefficient binomial vaut 0. Pour $-1 < \alpha < p$ et α non entier naturel, on a

$$\begin{aligned} \left| \prod_{i=0}^{p-1} \alpha - i \right| &= \left(\prod_{i=0}^{\lceil \alpha \rceil - 1} \alpha - i \right) \times \left(\prod_{i=\lceil \alpha \rceil}^{p-1} i - \alpha \right) \\ &< \left(\prod_{i=0}^{\lceil \alpha \rceil - 1} \lceil \alpha \rceil - i \right) \times \left(\prod_{i=\lceil \alpha \rceil}^{p-1} i - \lfloor \alpha \rfloor \right) \\ &= \left(\prod_{i=1}^{\lceil \alpha \rceil} i \right) \times \left(\prod_{i=1}^{p-1-\lceil \alpha \rceil} i \right) \\ &= \lceil \alpha \rceil! (p - \lceil \alpha \rceil)! \end{aligned}$$

donc on a

$$\begin{aligned} \left| \binom{\alpha}{p} \right| &\leq \frac{[\alpha]!(p - [\alpha])!}{p!} = \frac{[\alpha]!}{\prod_{i=p-[\alpha]+1}^p i} \\ &\leq \frac{[\alpha]!}{\prod_{i=p-[\alpha]+1}^p (p - [\alpha] + 1)} \\ &\leq \frac{[\alpha]!}{(p - [\alpha])^{[\alpha]}} \end{aligned}$$

ce qui donne pour $-1 < \alpha < \ln p$

$$\left| \binom{\alpha}{p} \right| \leq \frac{1}{p^{[\alpha]}} \frac{[\alpha]!}{(1 - \ln p / p)^{[\alpha]}} \leq \frac{1}{p^{[\alpha]}} \frac{[\alpha]!}{(1 - 1/e)^{[\alpha]}} \leq \frac{3^{[\alpha]} [\alpha]!}{p^{[\alpha]}}$$

Pour $\alpha \leq -1$ et α non entier naturel,

$$\begin{aligned} \left| \prod_{i=0}^{p-1} \alpha - i \right| &= \prod_{i=0}^{p-1} i - \alpha = \prod_{i=0}^{p-1} i + (-\alpha) \\ &< \prod_{i=0}^{p-1} i + [-\alpha] = \prod_{i=[-\alpha]+1}^{p+[-\alpha]} i \\ &= \frac{(p + [-\alpha])!}{[-\alpha]!} \end{aligned}$$

donc

$$\left| \binom{\alpha}{p} \right| \leq \frac{(p + [-\alpha])!}{p! [-\alpha]!} = \frac{\prod_{i=p+1}^{p+[-\alpha]} i}{[-\alpha]!} \leq \frac{(p + [-\alpha])^{[-\alpha]}}{[-\alpha]!} \leq \frac{[-\alpha]^{[-\alpha]}}{[-\alpha]!} p^{[-\alpha]}$$

En compilant les deux cas, on obtient au pire

$$\left| \binom{\alpha}{p} \right| \leq \max(3^{[\alpha]} [\alpha]!, [|\alpha|]^{[|\alpha|]}) p^{[|\alpha|]}$$

d'où le résultat. ■

Théorème 14.1.27

$$\binom{\alpha}{p} = (-1)^p \binom{p - \alpha - 1}{p}.$$

Démonstration. On a $\prod_{i=0}^{p-1} \alpha - i = \prod_{i=0}^{p-1} \alpha - (p - 1 - i) = \prod_{i=0}^{p-1} i + \alpha - p + 1 \dots$ ■

R On a

$$\begin{aligned} (1 + z)^{-k-1} &= \sum_{n \geq 0} (-1)^n \binom{n+k}{n} z^n \\ &= \sum_{n \geq 0} (-1)^n \binom{n+k}{n} z^n = \sum_{n \geq 0} \binom{-k-1}{n} z^n \end{aligned}$$

Théorème 14.1.28 Pour tout $\alpha \in \mathbb{R}$ et $z \in \mathbb{C}$ avec $|z| < 1$, on a

$$(1+z)^\alpha = \sum_{p \geq 0} \binom{\alpha}{p} z^p.$$

Démonstration. Le cas complexe est admis. Pour α entier naturel, c'est une conséquence directe de la formule du binôme. Pour α entier relatif négatif, avec $k+1 = -\alpha$ dans le développement précédent et le lemme ci-dessus, on obtient

$$\begin{aligned} (1+z)^\alpha &= \sum_{n \geq 0} (-1)^n \binom{n-\alpha-1}{-\alpha-1} z^n \\ &= \sum_{n \geq 0} (-1)^n \binom{n-\alpha-1}{n} z^n = \sum_{n \geq 0} \binom{\alpha}{n} z^n. \end{aligned}$$

Pour z réel uniquement, la formule de Taylor avec reste intégral donne pour $\alpha \leq n+1$,

$$(1+x)^\alpha = \sum_{p=0}^n \binom{\alpha}{p} x^p + R_n(x)$$

avec

$$R_n(x) = (n+1)x^{n+1} \binom{\alpha}{n+1} \int_{t=0}^1 \frac{(1-t)^n}{(1+tx)^{n+1-\alpha}} dt$$

On a

$$\begin{aligned} |R_n(x)| &\leq (n+1)|x|^{n+1} \left| \binom{\alpha}{n+1} \right| \max_{0 \leq t \leq 1} (1+tx)^{\alpha-1} \int_{t=0}^1 \frac{(1-t)^n}{(1+tx)^{n+2}} dt \\ &\leq \frac{|x|^{n+1}}{1+x} (n+1)^{|\alpha|} 3^{|\alpha|} [|\alpha|]^{|\alpha|} \max_{0 \leq t \leq 1} (1+tx)^{\alpha-1} \end{aligned}$$

On a posé $s = \frac{1-t}{1+tx}$ dans l'intégrale puis on a utilisé un lemme précédent. Par les théorèmes de comparaison, cela montre que le reste tend uniformément vers 0 sur tout segment de $] -1; 1[$.

Squelette d'une autre preuve. D'abord, la fonction $x \mapsto (1+x)^\alpha$ est l'unique solution sur $] -1; +\infty[$ de l'équation différentielle ordinaire $(1+x)y' - \alpha y = 0$, qui vaut 1 en 0. Ensuite, la série entière $x \mapsto \sum_{p \geq 0} \binom{\alpha}{p} x^p$ a pour rayon de convergence 1 et elle vérifie l'équation différentielle sur $] -1; 1[$ avec la même condition initiale. Ces deux fonctions coïncident sur $] -1; 1[$. À détailler... ■



15. Groupes



16. Arithmétique



17. Congruences



18. Polynômes



19. Suites réelles



20. Fonctions de variable réelle



21. Suites et séries de fonctions



22. Calcul intégral



23. Intégrale de Riemann



24. Équations différentielles



25. Analyse asymptotique



26. Espaces vectoriels



27. Applications linéaires



28. Matrices et déterminants



29. Systèmes linéaires

A close-up photograph of a red, textured fabric or material, possibly a piece of clothing or a decorative element. The texture is fibrous and uneven, with some areas appearing more saturated in red than others. The lighting is soft, highlighting the intricate details of the material's surface.

30. Applications multi linéaires



31. Espaces euclidiens




32. Topologie d'un EVN de dimension fin



33. Applications linéaires continues



34. Calcul différentiel



35. Probabilités

35.1 Probabilités

Espaces probabilisés finis. Probabilités conditionnelles, conditionnement et indépendance.

35.1.1 Prérequis, rappels et précautions

On suppose connus les notions élémentaires de la théorie des ensembles ainsi que le vocabulaire afférent. En particulier, on utilisera les notions de réunion et d'intersection de familles d'ensembles rappelées au chapitre II.

35.1.2 Généralités.

Le cas des variables aléatoires qui suivent la loi de Poisson ne rentre pas dans le cadre de probabilités finies car l'ensemble des événements est infini : il faut étendre le programme au cas dénombrable. De là au cas général, il n'y a souvent qu'un pas. On donne les définitions essentielles en faisant apparaître, quand c'est nécessaire, les trois situations :

1. cas fini,
2. cas dénombrable,
3. cas général.

Ce sont les définitions mathématiques, pas les définitions pragmatiques utilisées dans l'enseignement secondaire.

a Univers

Terminologie 35.1.1 En théorie des probabilités, **univers** est synonyme de **ensemble**, **issue** est synonyme de **élément**. L'univers est noté en général Ω . Dans ce contexte, un autre synonyme moins fréquent de issue est éventualité.

Dans toute la suite Ω désigne un univers fini, dénombrable ou général selon le cas.

b Événements

Définition 35.1.1 — Événements, Tribu, cas général. Une **tribu sur Ω** est un ensemble non vide de parties de Ω stable par passage au complémentaire et par union dénombrable. Elle est notée en général \mathcal{T} . Les éléments de la tribu sont appelés **événements**. (Ω, \mathcal{T}) est un **espace probabilisable**.

- R** Si Ω est dénombrable, $\mathcal{P}(\Omega)$ est la tribu choisie par défaut, ce qui permet une définition simplifiée des événements. Ce choix recouvre en réalité toutes les possibilités.

Définition 35.1.2 — Événements, cas fini ou dénombrable. Les parties de Ω sont appelés **événements**.

- R**
- Dans les deux cas, un événement est un ensemble d'issues.
 - Il ne faut pas confondre l'événement avec sa description. Par exemple, « tirer un nombre multiple de 3 » n'a pas du tout la même signification selon que le dé a quatre, six ou huit faces. D'ailleurs, la probabilité n'est pas la même.

Définition 35.1.3 Le **contraire** d'un événement E est le complémentaire $\Omega \setminus E$ de E dans Ω . Il est noté \bar{E} , qui peut être lu « E barre ». Deux événements sont **contraires** si l'un est le contraire de l'autre.

- R** contraire et complémentaire sont deux termes synonymes en mathématique mais pas en français.

Dans le cas fini, \emptyset et Ω sont des événements par définition, mais dans le cas général, on a la

Proposition 35.1.1 \emptyset et Ω sont des événements. Cela équivaut à dire que toute tribu contient \emptyset et Ω .

Démonstration. Par définition d'une tribu. Il existe au moins un événement E . Le contraire \bar{E} , $E \cap \bar{E}$ et $E \cup \bar{E}$ sont aussi des événements. Or $E \cap \bar{E} = \emptyset$ et $E \cup \bar{E} = \Omega$. ■

Théorème 35.1.2 Toute tribu est stable par intersection dénombrable.

Démonstration. C'est immédiat dans le cas fini ou dénombrable. On sait que l'intersection est le complémentaire de la réunion des complémentaires : pour toute famille dénombrable d'événements $(E_i)_{i \in I}$, $(\bar{E}_i)_{i \in I}$ est aussi une famille dénombrable d'événements, la réunion est un événement ainsi que son contraire. ■

Définition 35.1.4 — Issues possibles. Les éléments d'un événement sont les **issues possibles** de l'événement. Si l'événement n'est pas spécifié, il s'agit de Ω .

Définition 35.1.5 — Événement incompatibles. Deux événements sont **incompatibles** signifie que leur intersection est vide. Un événement est **incompatible** avec un autre s'ils sont incompatibles.

R Tout événement est incompatible avec son contraire.

Terminologie 35.1.2 Incompatible est synonyme de **disjoint**, qui appartient plutôt au vocabulaire ensembliste.

Théorème 35.1.3 L'événement \emptyset est incompatible avec tout événement. Il est le seul incompatible avec lui-même.

Démonstration. Pour tout événement E , on a $\emptyset \cap E = \emptyset$ et si $E \cap E = \emptyset$ alors $E = \emptyset$. puisque $E \cap E = E$. ■

Théorème 35.1.4 Soit E, F deux événements, on a

$$E \subset F \iff E \cap \bar{F} = \emptyset$$

id est E est inclus dans F si et seulement si E et \bar{F} sont incompatibles.

Théorème 35.1.5 Soit E, F deux événements, on a

$$(E \cap F) \cap (E \cap \bar{F}) = \emptyset \text{ et } E = (E \cap F) \cup (E \cap \bar{F}).$$

$\{E \cap F; E \cap \bar{F}\}$ est une partition de E .

Démonstration. Par associativité de l'intersection, on a $(E \cap F) \cap (E \cap \bar{F}) = E \cap (F \cap \bar{F}) = E \cap \emptyset = \emptyset$. Par distributivité, on a $(E \cap F) \cup (E \cap \bar{F}) = E \cap (F \cup \bar{F}) = E \cap \Omega = E$ ■

Définition 35.1.6 — et, ou. Soit E, F deux événements, l'événement $E \cap F$ est noté **E et F**, l'événement $E \cup F$ est noté **E ou F**.

c Probabilité

Définition 35.1.7 — Probabilité. Une **loi de probabilité** est une application \mathbb{P}

- 1) qui à tout événement associe un nombre dans $[0; 1]$.
 2) telle que $\mathbb{P}(\Omega) = 1$
 3) et
 a) cas fini : si deux événements E et F sont incompatibles, on a $\mathbb{P}(E \cup F) = \mathbb{P}(E) + \mathbb{P}(F)$,
 b) autres cas : pour toute famille dénombrable $(E_i)_{i \in I}$ d'événements deux à deux incompatibles $\mathbb{P}(\bigcup_{i \in I} E_i) = \sum_{i \in I} \mathbb{P}(E_i)$
 Selon le cas, (Ω, \mathbb{P}) ou $(\Omega, \mathcal{T}, \mathbb{P})$ est appelé **espace probabilisé**.
 Loi de probabilité, **mesure de probabilité**, et **probabilité** sont synonymes l'un de l'autre.

R Pour information, la propriété 3-b ci-dessus est la σ -additivité de \mathbb{P} .

Dans la suite de la section, (Ω, \mathbb{P}) ou $(\Omega, \mathcal{T}, \mathbb{P})$ est un espace probabilisé, selon le cas.

Théorème 35.1.6 — Probabilité du contraire. Pour tout événement E , $\mathbb{P}(\bar{E}) = 1 - \mathbb{P}(E)$.

Démonstration. Pour tout événement E , on a $E \cap \bar{E} = \emptyset$ et $E \cup \bar{E} = \Omega$ donc $1 = \mathbb{P}(\Omega) = \mathbb{P}(E \cup \bar{E}) = \mathbb{P}(E) + \mathbb{P}(\bar{E})$. ■

Théorème 35.1.7 On a $\mathbb{P}(\emptyset) = 0$.

Démonstration. On applique le théorème précédent au cas particulier $E = \Omega$. D'une autre façon, on a $\emptyset \cap \emptyset = \emptyset$ et $\emptyset \cup \emptyset = \emptyset$ donc $\mathbb{P}(\emptyset) = \mathbb{P}(\emptyset \cup \emptyset) = \mathbb{P}(\emptyset) + \mathbb{P}(\emptyset)$ et par régularité $0 = \mathbb{P}(\emptyset)$. ■

Théorème 35.1.8 — de l'intersection. Pour des événements E et F on a

$$\mathbb{P}(E \cap F) + \mathbb{P}(E \cup F) = \mathbb{P}(E) + \mathbb{P}(F)$$

Démonstration. On a $(E \cap F) \cup (\bar{E} \cap F) = (E \cup \bar{E}) \cap F = \Omega \cap F = F$ et

$$(E \cap F) \cap (\bar{E} \cap F) = (E \cap \bar{E}) \cap F = \emptyset \cap F = \emptyset$$

donc $\mathbb{P}(\bar{E} \cap F) = \mathbb{P}(F) - \mathbb{P}(E \cap F)$. De plus

$$E \cup (\bar{E} \cap F) = (E \cup \bar{E}) \cap (E \cup F) = \Omega \cap (E \cup F) = E \cup F$$

et

$$E \cap (\bar{E} \cap F) = (E \cap \bar{E}) \cap F = \emptyset \cap F = \emptyset$$

donc $\mathbb{P}(E \cup F) = \mathbb{P}(E) + \mathbb{P}(\bar{E} \cap F) = \mathbb{P}(E) + \mathbb{P}(F) - \mathbb{P}(E \cap F)$. ■

R on pouvait traiter E et F de manière symétrique mais c'est un peu plus long.

Définition 35.1.8 — Événements certains, possible, impossible.

Un événement est **certain** quand sa probabilité vaut 1. Un événement est **impossible** quand sa probabilité vaut 0, il est **possible** sinon.



- L'univers des possibles est un événement certain, mais selon cette terminologie, ce n'est pas le seul.
- Dans le langage courant, improbable peut correspondre à une probabilité faible, mais pas nulle : voir «hautement improbable».

Théorème 35.1.9 — Croissance. Soit E, F deux événements, on a $E \subset F \Rightarrow \mathbb{P}(E) \leq \mathbb{P}(F)$.

Démonstration. On a $F = E \cup (F \setminus E)$ et $E \cap (F \setminus E) = \emptyset$ donc $\mathbb{P}(F) = \mathbb{P}(E) + \mathbb{P}(F \setminus E) \geq \mathbb{P}(E)$. ■

Théorème 35.1.10 — Continuité. Si $(E_n)_{n \in \mathbb{N}}$ est une suite d'événements mutuellement incompatibles, $\mathbb{P}(\bigcup_{i=0}^n E_i) \xrightarrow{n \rightarrow \infty} \mathbb{P}(\bigcup_{i=0}^{\infty} E_i)$.



Ce théorème n'a d'intérêt que pour un univers infini.

Démonstration. C'est une conséquence immédiate de

$$\mathbb{P}\left(\bigcup_{i=0}^n E_i\right) = \sum_{i=0}^n \mathbb{P}(E_i), \quad \mathbb{P}\left(\bigcup_{i=0}^{\infty} E_i\right) = \sum_{i=0}^{\infty} \mathbb{P}(E_i)$$

et

$$\sum_{i=0}^n \mathbb{P}(E_i) \xrightarrow{n \rightarrow \infty} \sum_{i=0}^{\infty} \mathbb{P}(E_i). \quad \blacksquare$$

Théorème 35.1.11 — Continuité monotone.

1) Si $(E_n)_{n \in \mathbb{N}}$ est une suite croissante d'événements,

$$\mathbb{P}(E_n) \xrightarrow{n \rightarrow \infty} \mathbb{P}\left(\bigcup_{i \in \mathbb{N}} E_i\right).$$

2) Si $(E_n)_{n \in \mathbb{N}}$ est une suite décroissante d'événements,

$$\mathbb{P}(E_n) \xrightarrow{n \rightarrow \infty} \mathbb{P}\left(\bigcap_{i \in \mathbb{N}} E_i\right).$$

Démonstration. Dans le cas fini, c'est immédiat car une suite monotone est constante à partir d'un certain rang.

1) On définit la suite d'événements $(F_n)_{n \in \mathbb{N}}$ par

$$F_0 \stackrel{\text{déf}}{=} E_0, \quad \forall n \in \mathbb{N}^*, \quad F_n \stackrel{\text{déf}}{=} E_n \setminus E_{n-1}$$

Ces événements sont deux à deux disjoints : pour $0 < m < n$

$$\begin{aligned} F_m \cap F_n &= (E_m \setminus E_{m-1}) \cap (E_n \setminus E_{n-1}) \\ &= (E_m \cap \overline{E_{m-1}}) \cap (E_n \cap \overline{E_{n-1}}) \\ &= E_m \cap \overline{E_{n-1}} \subset E_m \cap \overline{E_m} = \emptyset \end{aligned}$$

On peut montrer par récurrence que $\forall n \in \mathbb{N}, E_n = \bigcup_{i=0}^n F_i$. L'initialisation est immédiate. L'hérédité vient de

$$\begin{aligned} \bigcup_{i=0}^{n+1} F_i &= \bigcup_{i=0}^n F_i \cup F_{n+1} = E_n \cup (E_{n+1} \setminus E_n) \\ &= (E_n \cap E_{n+1}) \cup (E_{n+1} \setminus E_n) = E_{n+1} \end{aligned}$$

On peut appliquer le théorème précédent pour obtenir la première proposition.

2) la deuxième proposition se déduit de la première par passage au contraire. En effet, si $(E_n)_{n \in \mathbb{N}}$ est une suite décroissante d'événements, alors $(\overline{E}_n)_{n \in \mathbb{N}}$ est une suite croissante d'événements¹ donc

$$\mathbb{P}(\overline{E}_n) \xrightarrow{n \rightarrow \infty} \mathbb{P}\left(\bigcup_{i \in \mathbb{N}} \overline{E}_i\right) \text{ et } 1 - \mathbb{P}(\overline{E}_n) \xrightarrow{n \rightarrow \infty} 1 - \mathbb{P}\left(\bigcup_{i \in \mathbb{N}} \overline{E}_i\right).$$

Or

$$1 - \mathbb{P}(\overline{E}_n) = \mathbb{P}(E_n) \text{ et } 1 - \mathbb{P}\left(\bigcup_{i \in \mathbb{N}} \overline{E}_i\right) = \mathbb{P}\left(\bigcap_{i \in \mathbb{N}} E_i\right). \quad \blacksquare$$

d Cas des espaces finis ou dénombrables

Dans cette section Ω est fini ou dénombrable.

Événements élémentaires

Définition 35.1.9 — Événement élémentaire. Un événement est **élémentaire** signifie qu'il n'est pas vide et qu'il n'est pas la réunion de deux événements incompatibles et non vides.

Théorème 35.1.12 Deux événements élémentaires différents sont incompatibles.

1. Le passage au complémentaire définit une application décroissante des parties d'un ensemble.

Démonstration. Soit E, F deux événements élémentaires, on a

$$E = (E \cap F) \cup (E \cap \bar{F}) \text{ et } \emptyset = (E \cap F) \cap (E \cap \bar{F}),$$

Donc $\emptyset = E \cap F$ ou bien $\emptyset = E \cap \bar{F}$ et d'une manière symétrique $\emptyset = E \cap F$ ou bien $\emptyset = \bar{E} \cap F$. Si les événements ne sont pas incompatibles, alors $\emptyset = E \cap \bar{F} = \bar{E} \cap F$ d'où $E \subset F$ et $E \supset F$ et l'égalité des événements. ■

Théorème 35.1.13 Dans le cas dénombrable, toute issue appartient à un unique événement élémentaire.

Démonstration. Si x est une issue, les événements qui contiennent x sont en nombre dénombrable, donc leur intersection est un événement qui contient x , noté ici E_x . Si on a $E_x = E \cup F$ avec $\emptyset = E \cap F$, alors $x \in E$ ou bien $x \in F$. Dans le premier cas, on obtient $E_x \subset E$ par définition de E_x et $E \subset E_x$ par définition de E . On en déduit $E_x = E$ et $\emptyset = E \cap \bar{E} = (E \cup F) \cap \bar{E} = (E \cap \bar{E}) \cup (F \cap \bar{E}) = \emptyset \cup (F \cap \bar{E}) = F \cap \bar{E}$. Ainsi $F \subset E$ et $F = F \cap E = \emptyset$, donc E_x est élémentaire. ■

Théorème 35.1.14 Dans le cas dénombrable, tout événement est la réunion des événements élémentaires qu'il contient. En particulier, l'univers est la réunion de tous les événements élémentaires.

Démonstration. Par définition, tout événement contient les événements élémentaires qu'il contient, donc leur réunion. L'inclusion réciproque vient de la proposition précédente. ■

Théorème 35.1.15 Si toutes les parties sont des événements, les événements élémentaires sont les singletons.

Démonstration. Tout singleton est un événement élémentaire. En effet, c'est une partie de l'univers, or toutes ses parties sont des événements, donc c'est un événement. Les parties de $\{x\}$ étant \emptyset et $\{x\}$, il n'existe pas deux événements différents et non vides dans $\{x\}$.

Si un événement E contient une paire $\{x, y\}$, alors

$$E = (E \cap \{x\}) \cup (E \cap \overline{\{x\}}) = \{x\} \cup (E \cap \overline{\{x\}}).$$

y est dans E mais pas $\{x\}$, il est donc dans $E \cap \overline{\{x\}}$. Ainsi E n'est pas élémentaire. Par contraposition, si un événement est élémentaire, alors il ne contient pas de paire. Comme il n'est pas vide, c'est un singleton. ■

R on pouvait définir les singletons comme événements élémentaires, la définition ci-dessus devenant du coup un théorème.

Théorème 35.1.16 Une loi de probabilités est entièrement déterminée par la probabilité de chaque événement élémentaire, sauf éventuellement un. La somme des probabilités de tous les événements élémentaires vaut 1.

Démonstration. En exercice... ■

Cas des espaces finis

Dans cette section Ω est fini.

Définition 35.1.10 — Loi uniforme. On appelle loi uniforme toute loi de probabilités qui donne à chaque événement élémentaire la même probabilité.

Théorème 35.1.17 Dans le cas d'une loi uniforme sur un espace fini Ω , la probabilité de chaque événement élémentaire est $\frac{1}{|\Omega|}$.

Démonstration. Soit p la probabilité commune à tous les événements élémentaires. On a

$$1 = \mathbb{P}(\Omega) = \mathbb{P}\left(\bigcup_{x \in \Omega} \{x\}\right) = \sum_{x \in \Omega} \mathbb{P}(\{x\}) = p \sum_{x \in \Omega} 1 = p |\Omega| \quad \blacksquare$$

Théorème 35.1.18 Dans le cas d'une loi uniforme, la probabilité d'un événement est le nombre de cas favorables sur le nombre de cas possibles.

Démonstration.

$$\mathbb{P}(E) = \mathbb{P}\left(\bigcup_{x \in E} \{x\}\right) = \sum_{x \in E} \mathbb{P}(\{x\}) = \frac{1}{|\Omega|} \sum_{x \in E} 1 = \frac{|E|}{|\Omega|} \quad \blacksquare$$

e Indépendance

Définition 35.1.11 — Indépendance. Deux événements E et F sont **indépendants** signifie que

$$\mathbb{P}(E \cap F) = \mathbb{P}(E) \times \mathbb{P}(F)$$

On dit aussi que E est **indépendant** de F .

R il n'y a pas de notation symbolique pour deux événements indépendants. On pourrait noter par exemple $E \perp F$.

Lemme 35.1.19 Tout événement est indépendant d'un événement certain.

Démonstration. E et F deux événements, on a $E = (E \cap F) \cup (E \cap \bar{F})$ et $(E \cap F) \cup (E \cap \bar{F}) = \emptyset$, d'où $\mathbb{P}(E) = \mathbb{P}(E \cap F) + \mathbb{P}(E \cap \bar{F})$. Si F est certain, $\mathbb{P}(F) = 1$ et $\mathbb{P}(\bar{F}) = 0$, et $\mathbb{P}(E \cap \bar{F}) = 0$ puisque $E \cap \bar{F} \subset \bar{F}$. Donc $\mathbb{P}(E \cap F) = \mathbb{P}(E) = \mathbb{P}(E) \times \mathbb{P}(F)$. ■

Théorème 35.1.20 Tout événement est indépendant d'un événement impossible.

Démonstration. E et F deux événements, F étant impossible. Comme $(E \cap F) \subset F$ et $0 \leq \mathbb{P}(E \cap F) \leq \mathbb{P}(F) = 0$, on a $\mathbb{P}(E \cap F) = 0$. Bien sûr, $\mathbb{P}(E) \times \mathbb{P}(F) = 0$. ■

Proposition 35.1.21 Soit E et F deux événements. Sont équivalents

- E et F sont indépendants
- F et E sont indépendants
- E et \bar{F} sont indépendants

Démonstration. Comme $E \cap F = F \cap E$, on a $\mathbb{P}(E \cap F) = \mathbb{P}(F \cap E)$ d'où l'équivalence des deux premières propositions.

De plus, $E = (E \cap F) \cup (E \cap \bar{F})$ et $\emptyset = (E \cap F) \cap (E \cap \bar{F})$, donc $\mathbb{P}(E) = \mathbb{P}(E \cap F) + \mathbb{P}(E \cap \bar{F})$ et

$$\begin{aligned} \mathbb{P}(E \cap F) - \mathbb{P}(E) \times \mathbb{P}(F) &= \mathbb{P}(E) - \mathbb{P}(E \cap \bar{F}) - \mathbb{P}(E) \times \mathbb{P}(F) \\ &= \mathbb{P}(E) \times (1 - \mathbb{P}(F)) - \mathbb{P}(E \cap \bar{F}) \\ &= \mathbb{P}(E) \times \mathbb{P}(\bar{F}) - \mathbb{P}(E \cap \bar{F}) \end{aligned}$$

ce qui donne les autres équivalences. ■

► **Exemple 35.1** Deux événements contraires et possibles ne sont pas indépendants. ▲

35.1.3 Probabilités composées

a Restriction.

On peut changer d'univers en prenant une sous-tribu. À compléter.

b Probabilités produit dans le cas fini.

Cela permet de modéliser des combinaisons d'expériences aléatoires indépendantes, comme des répétitions par exemple.

Si (Ω_1, \mathbb{P}_1) et (Ω_2, \mathbb{P}_2) sont deux univers probabilisés finis, alors $\Omega_1 \times \Omega_2$ est un univers fini, ses événements élémentaires sont les singletons.

Théorème 35.1.22 — Probabilité produit. L'application qui à tout événement élémentaire $\{(x_1, x_2)\}$ de $\Omega_1 \times \Omega_2$ associe le nombre $\mathbb{P}_1(\{x_1\}) \times \mathbb{P}_2(\{x_2\})$ définit bien une loi de probabilités sur $\Omega_1 \times \Omega_2$. C'est la **loi produit**.

Démonstration. On a

$$\sum_{(x_1, x_2) \in \Omega_1 \times \Omega_2} \mathbb{P}_1(\{x_1\}) \times \mathbb{P}_2(\{x_2\}) = \sum_{x_1 \in \Omega_1} \mathbb{P}_1(\{x_1\}) \sum_{x_2 \in \Omega_2} \mathbb{P}_2(\{x_2\})$$

qui vient de

$$\sum_{(i,j) \in I \times J} p_i q_j = \sum_{i \in I} p_i \sum_{j \in J} q_j \quad \blacksquare$$

- R** Pour les répétitions d'une même expérience modélisée par (Ω, \mathbb{P}) une infinité dénombrable de fois, on a aussi une probabilité produit sur $\Omega^{\mathbb{N}}$. Les événements de références ne sont pas les événements élémentaires mais des cylindres, c'est-à-dire des suites d'événements de Ω qui valent Ω à partir d'un certain rang. À compléter...

c Probabilités conditionnelles

La notion est générale, on ne l'appliquera qu'aux espaces dénombrables.

$(\Omega, \mathcal{T}, \mathbb{P})$ est un espace probabilisé.

Théorème 35.1.23 — Probabilité conditionnelle. Si A est un événement possible, l'application $E \mapsto \mathbb{P}(E \cap A)/\mathbb{P}(A)$ définit une loi de probabilités sur (Ω, \mathcal{T}) qui est notée \mathbb{P}_A .

Démonstration. Pour tout événement E , $E \cap A \subset A$, donc $\mathbb{P}(E \cap A) \leq \mathbb{P}(A)$. Comme $\mathbb{P}(A) \neq 0$, $0 \leq \frac{\mathbb{P}(E \cap A)}{\mathbb{P}(A)} \leq 1$. Ensuite $\frac{\mathbb{P}(\Omega \cap A)}{\mathbb{P}(A)} = \frac{\mathbb{P}(A)}{\mathbb{P}(A)} = 1$. Pour une famille d'événements $(E_i)_{i \in I}$ mutuellement incompatibles, les événements $(E_i \cap A)_{i \in I}$ sont aussi mutuellement incompatibles car $(E_i \cap A) \cap (E_j \cap A) = (E_i \cap E_j) \cap A$. de plus, on a $(\bigcup_{i \in I} E_i) \cap A = (\bigcup_{i \in I} E_i \cap A)$, ce qui donne

$$\mathbb{P}\left(\bigcup_{i \in I} (E_i \cap A)\right) = \sum_{i \in I} \mathbb{P}(E_i \cap A)$$

d'où la σ -additivité en divisant par $\mathbb{P}(A)$. ■

Théorème 35.1.24 Deux événements possibles E et F sont indépendants si et seulement si $\mathbb{P}(E) = \mathbb{P}_F(E)$ ou de manière symétrique $\mathbb{P}(F) = \mathbb{P}_E(F)$.

Démonstration. C'est une application directe de la définition de l'indépendance. ■

Définition 35.1.12 — Système complet d'événements. Une famille dénombrable $(E_i)_{i \in I}$ d'événements est un **système complet** d'événements signifie que

- 1) ils sont mutuellement incompatibles : $\forall i, j \in I, i \neq j \Rightarrow E_i \cap E_j = \emptyset$,
- 2) leur réunion est l'univers : $\bigcup_{i \in I} E_i = \Omega$,
- 3) ils sont tous possibles : $\forall i \in I, \mathbb{P}(E_i) \neq 0$.

❶ Dans le contexte dénombrable, les événements élémentaires forment un système complet d'événements. Un tel système peut être utilisé pour restreindre l'ensemble des événements et simplifier le modèle.

Théorème 35.1.25 — des probabilités totales. Pour un système complet d'événements $(E_i)_{i \in I}$ et un événement E , on a

$$\mathbb{P}(E) = \sum_{i \in I} \mathbb{P}(E_i) \mathbb{P}_{E_i}(E).$$

Démonstration. D'une part

$$E = E \cap \Omega = E \cap \bigcup_{i \in I} E_i = \bigcup_{i \in I} E \cap E_i$$

et d'autre part les $E \cap E_i$ sont mutuellement incompatibles car si $i \neq j$ dans I , $(E \cap E_i) \cap (E \cap E_j) = E \cap (E_i \cap E_j) = E \cap \emptyset = \emptyset$. Donc

$$\begin{aligned} \mathbb{P}(E) &= \mathbb{P}\left(\bigcup_{i \in I} E \cap E_i\right) \\ &= \sum_{i \in I} \mathbb{P}(E \cap E_i) \\ &= \sum_{i \in I} \mathbb{P}(E_i) \frac{\mathbb{P}(E \cap E_i)}{\mathbb{P}(E_i)} \\ &= \sum_{i \in I} \mathbb{P}(E_i) \mathbb{P}_{E_i}(E). \end{aligned}$$

■

Théorème 35.1.26 — de Bayes. Pour un système complet d'événements $(E_i)_{i \in I}$ et un événement E possible, on a

$$\mathbb{P}_E(E_i) = \frac{\mathbb{P}(E_i) \mathbb{P}_{E_i}(E)}{\sum_{j \in I} \mathbb{P}(E_j) \mathbb{P}_{E_j}(E)}.$$

Démonstration. C'est quasi immédiat avec la formule des probabilités totales :

$$\mathbb{P}_E(E_i) \stackrel{\text{déf}}{=} \frac{\mathbb{P}(E \cap E_i)}{\mathbb{P}(E)} = \frac{\mathbb{P}(E_i) \mathbb{P}_{E_i}(E)}{\sum_{j \in I} \mathbb{P}(E_j) \mathbb{P}_{E_j}(E)}$$

■



cette formule est tellement simple qu'on ne la retient pas, on la retrouve selon les besoins.

36. Variables aléatoires

36.1 Variables aléatoires

Variable aléatoires sur un univers fini : lois usuelles (lois uniformes, lois binomiales), variables aléatoires indépendantes, espérance, variance et écart-type. Variables aléatoires discrètes : espérance et variance, lois de Poisson, lois géométriques. Lois exponentielles, loi faible des grands nombres.

On rappelle que $\mathbb{1}_E$ est l'indicatrice de l'ensemble E qui vaut 1 sur E et 0 sur son complémentaire.

36.1.1 Variables aléatoires discrètes

a Définitions

Un espace probabilisé $(\Omega, \mathcal{T}, \mathbb{P}_\Omega)$ et un espace mesurable (Ω', \mathcal{E}) étant donnés.

Cas général

Définition 36.1.1 — Variable aléatoire. Une **variable aléatoire** est une application X de Ω dans Ω' telle que la préimage par X de toute partie mesurable est un événement.

R De manière équivalente : la préimage par X de tout élément de \mathcal{E} est un élément de \mathcal{T} .

Théorème 36.1.1 — Loi de la variable aléatoire. L'application qui à tout élément E de \mathcal{E} associe $\mathbb{P}_\Omega(X^{-1}(E))$ est une mesure de probabilités sur (Ω', \mathcal{E}) , elle est notée \mathbb{P}_X .
C'est la **loi de la variable aléatoire** X

Démonstration. On a :

$$1) 0 \leq \mathbb{P}_X(E) = \mathbb{P}_\Omega(X^{-1}(E)) \leq 1$$

$$2) \mathbb{P}_X(\Omega') = \mathbb{P}_\Omega(X^{-1}(\Omega')) = \mathbb{P}_\Omega(\Omega) = 1$$

3) Si $(E_i)_{i \in I}$ est une famille dénombrable d'éléments de \mathcal{E} deux à deux disjoints, alors $(X^{-1}(E_i))_{i \in I}$ est une famille dénombrable d'événements de Ω deux à deux disjoints. En effet, par contraposition :

$$\begin{aligned} X^{-1}(E_i) \cap X^{-1}(E_j) \neq \emptyset &\implies \exists \omega, \omega \in X^{-1}(E_i) \text{ et } \omega \in X^{-1}(E_j) \\ &\implies \exists \omega, X(\omega) \in E_i \text{ et } X(\omega) \in E_j \\ &\implies \exists x, x \in E_i \text{ et } x \in E_j \\ &\implies E_i \cap E_j \neq \emptyset \end{aligned}$$

ainsi,

$$\begin{aligned} \mathbb{P}_X\left(\bigcup_{i \in I} E_i\right) &= \mathbb{P}_\Omega\left(X^{-1}\left(\bigcup_{i \in I} E_i\right)\right) = \mathbb{P}_\Omega\left(\bigcup_{i \in I} X^{-1}(E_i)\right) \\ &= \sum_{i \in I} \mathbb{P}_\Omega(X^{-1}(E_i)) = \sum_{i \in I} \mathbb{P}_X(E_i) \end{aligned} \quad \blacksquare$$

Terminologie 36.1.1 Sont synonymes

- $\mathbb{P}(X \in E)$, $\mathbb{P}_X(E)$ et $\mathbb{P}_\Omega(X^{-1}(E))$.
- $\mathbb{P}(X = x)$ et $\mathbb{P}_X(\{x\})$ et $\mathbb{P}_\Omega(X^{-1}(\{x\}))$.

R Ce n'est plus une notation fonctionnelle mais c'est pratique d'un certain point de vue car cela permet de cacher Ω et de se consacrer à l'essentiel.

Terminologie 36.1.2 Si X prend des valeurs réelles, sont synonymes

- $\mathbb{P}(X < a)$ et $\mathbb{P}(X \in]-\infty, a[)$,
- $\mathbb{P}(X \leq a)$ et $\mathbb{P}(X \in]-\infty, a])$,
- $\mathbb{P}(X > a)$ et $\mathbb{P}(X \in]a, -\infty[)$,
- $\mathbb{P}(X \geq a)$ et $\mathbb{P}(X \in [a, -\infty[)$,
- $\mathbb{P}(a < X < b)$ et $\mathbb{P}(X \in]a, b[)$,
- $\mathbb{P}(a < X \leq b)$ et $\mathbb{P}(X \in]a, b])$,
- $\mathbb{P}(a \leq X < b)$ et $\mathbb{P}(X \in [a, b[)$,
- $\mathbb{P}(a \leq X \leq b)$ et $\mathbb{P}(X \in [a, b])$.

Variables aléatoires sur des espaces dénombrables

Définition 36.1.2 Si Ω et Ω' sont **dénombrables**, avec événements ou ensembles mesurables par défaut, une **variable aléatoire** est une application de Ω dans Ω' .

Théorème 36.1.2 L'application qui à tout événement élémentaire $\{x\}$ de Ω' associe $\mathbb{P}_\Omega(X^{-1}(x))$ définit bien une loi de probabilités sur Ω' , elle est notée \mathbb{P}_X .

Démonstration. Les préimages par X des événements élémentaires de Ω' forment un système complet d'événements. À compléter... ■

Dans la suite, Δ désigne une **partie dénombrable** de \mathbb{R} .

Définition 36.1.3 — Variable aléatoire discrète. Une **variable aléatoire discrète** est une application de Ω dans Δ telle que la préimage de tout nombre est un événement.

R une variable aléatoire discrète prend ses valeurs dans une partie dénombrable de \mathbb{R} , pas une partie discrète de \mathbb{R} .

Dans les deux contextes précédent ci-dessus, on a le

Théorème 36.1.3 — Loi d'une variable aléatoire discrète. L'application qui à tout événement élémentaire $\{x\}$ de Δ associe $\mathbb{P}_\Omega(X^{-1}(x))$ définit bien une loi de probabilités sur Δ , elle est notée \mathbb{P}_X .

Démonstration. On a :

$$1) 0 \leq \mathbb{P}_X(x) = \mathbb{P}_\Omega(X^{-1}(x)) \leq 1$$

2) $(X^{-1}(x))_{x \in \Delta}$ est une famille dénombrable d'événements de Ω deux à deux disjoints. En effet, par contraposition :

$$\begin{aligned} X^{-1}(x) \cap X^{-1}(x') \neq \emptyset &\Rightarrow \exists \omega, \omega \in X^{-1}(x) \text{ et } \omega \in X^{-1}(x') \\ &\Rightarrow \exists \omega, X(\omega) = x \text{ et } X(\omega) = x' \\ &\Rightarrow x = x' \end{aligned}$$

ainsi,

$$\mathbb{P}_\Omega\left(\bigcup_{x \in \Delta} X^{-1}(x)\right) = \sum_{x \in \Delta} \mathbb{P}_\Omega(X^{-1}(x)) = \sum_{x \in \Delta} \mathbb{P}_X(x) = 1 \quad \blacksquare$$

Dans la suite, les variables aléatoires discrètes ont leurs valeurs dans Δ .

b Opérations algébriques

Théorème 36.1.4 Si X et Y sont deux variables aléatoires discrètes définies sur Ω , λ et μ deux réels.

- $\lambda X + \mu$, $X + Y$ et $X \times Y$ sont aussi des variables aléatoires discrètes définies sur Ω .

- Si Y ne s'annule pas, X/Y est aussi une variable aléatoire discrète définie sur Ω .

Démonstration. À préciser... ■

c Espérance

Définition 36.1.4 — Espérance. L'espérance d'une variable aléatoire discrète X est

- le nombre $\sum_{x \in X(\Omega)} x \mathbb{P}(X = x)$ si $X(\Omega)$ est fini,
- la somme de la série $\sum_{i \in \mathbb{N}} x_i \mathbb{P}(X = x_i)$ si $X(\Omega) = \{x_i, i \in \mathbb{N}\}$ et s'il y a convergence absolue
- non définie sinon.

Elle est notée $\mathbb{E}(X)$ ou \bar{X} . **Moyenne (arithmétique)** est synonyme d'espérance.

- R** On ne peut pas définir une notion d'espérance si la série est semi-convergente car la somme dépend alors de l'ordre des termes.

Théorème 36.1.5 — Linéarité de l'espérance. Si X et Y sont deux variables aléatoires discrètes définies sur Ω , λ et μ deux réels, alors $\mathbb{E}(\lambda X + \mu Y) = \lambda \mathbb{E}(X) + \mu \mathbb{E}(Y)$ dès que deux des trois espérances sont bien définies.

Démonstration. À préciser... ■

Théorème 36.1.6 — Croissance de l'espérance. Si elle existe, l'espérance d'une variable aléatoire discrète à valeurs positives est positive.

Démonstration. À préciser... ■

d Variance

Définition 36.1.5 — Variance, écart type. La variance d'une variable aléatoire discrète X est $\mathbb{E}((X - \mathbb{E}(X))^2)$ si elle existe. Elle est notée $\mathbb{V}(X)$. L'écart-type est la racine carrée de la variance, il est noté $\sigma(X)$.

- R** L'écart-type est traduit en anglais par "standard deviation" dont la première lettre correspond à \mathbb{V} en grec.

Théorème 36.1.7 — de König.

$$\mathbb{E}((X - \mathbb{E}(X))^2) = \mathbb{E}(X^2) - \mathbb{E}(X)^2$$

Démonstration. À compléter... ■

Théorème 36.1.8 — Homogénéité. Pour une variable aléatoire discrète X , λ et μ deux nombres réels, on a $\mathbb{V}(\lambda X + \mu) = \lambda^2 \mathbb{V}(X)$ et $\sigma(\lambda X + \mu) = |\lambda| \sigma(X)$, quand c'est bien défini.

R on dit que la variance est homogène de degré 2, l'écart-type de degré 1.

Démonstration. À préciser... ■

Théorème 36.1.9 — Normalisation. Pour une variable aléatoire discrète X d'espérance μ et d'écart-type σ , $\frac{X-\mu}{\sigma}$ a pour espérance 0 et pour écart-type 1.

Démonstration. À préciser... ■

Théorème 36.1.10 — Sous additivité. Si X et Y sont deux variables aléatoires discrètes définies sur Ω , on a $\sigma(X + Y) \leq \sigma(X) + \sigma(Y)$.

Démonstration. À préciser... ■

e Indépendance

Théorème 36.1.11 — Loi jointe, lois marginales. Si (X, Y) est un couple de variables aléatoires discrètes définies sur Ω , à valeurs respectivement dans Δ_X et Δ_Y . L'application qui à tout événement élémentaire $\{(x, y)\}$ de $\Delta_X \times \Delta_Y$ associe $\mathbb{P}_\Omega(X^{-1}(x) \cap Y^{-1}(y))$ définit bien une loi de probabilités sur $\Delta_X \times \Delta_Y$. C'est la **loi jointe** du couple, les lois de X et de Y en sont les **lois marginales**. On note

$$\mathbb{P}_{X,Y}(E \times F) \stackrel{\text{déf.}}{=} \mathbb{P}(X \in E, Y \in F) \stackrel{\text{déf.}}{=} \mathbb{P}_\Omega(X^{-1}(E) \cap Y^{-1}(F)).$$

Lemme 36.1.12 Dans le contexte ci-dessus, $\{X^{-1}(x) \cap Y^{-1}(y) \mid (x, y) \in \Delta_X \times \Delta_Y\}$ forme un système complet d'événements de Ω .

Démonstration. Pour le lemme, on a

- 1) pour tout issue ω de Ω , on a $\omega \in X^{-1}(X(\omega)) \cap Y^{-1}(Y(\omega))$,
- 2) si $(x, y) \neq (x', y')$, on a $x \neq x'$ ou $y \neq y'$, par conséquent $X^{-1}(x) \cap X^{-1}(x') = \emptyset$ ou $Y^{-1}(y) \cap Y^{-1}(y') = \emptyset$. En tout cas, $X^{-1}(x) \cap Y^{-1}(y) \cap X^{-1}(x') \cap Y^{-1}(y') = \emptyset$.

Pour le théorème, il suffit de vérifier que la somme éventuellement infinie des probabilités des événements élémentaires vaut 1. D'après le lemme précédent, on a un système complet d'événement dénombrable, cela suffit. ■

Définition 36.1.6 Deux variables aléatoires discrètes X et Y définies sur Ω , à valeurs respectivement dans Δ_X et Δ_Y sont **indépendantes** signifie que pour tout événement élémentaire $\{(x, y)\}$ de $\Delta_X \times \Delta_Y$ on

a

$$\mathbb{P}_{X,Y}(\{(x, y)\}) = \mathbb{P}_X(\{x\}) \times \mathbb{P}_Y(\{y\})$$

ou de manière synonyme

$$\mathbb{P}(X = x, Y = y) = \mathbb{P}(X = x) \times \mathbb{P}(Y = y).$$

Lemme 36.1.13 Si X et Y sont deux variables aléatoires discrètes indépendantes définies sur Ω , pour toutes paires de fonctions réelles d'une variable réelle f et g , on a $\mathbb{E}(f(X) \times g(Y)) = \mathbb{E}(f(X)) \times \mathbb{E}(g(Y))$, si ces quantités sont bien définies.

Démonstration. À compléter... ■

Proposition 36.1.14 Si X et Y sont deux variables aléatoires discrètes indépendantes définies sur Ω , alors $\mathbb{E}(X \times Y) = \mathbb{E}(X) \times \mathbb{E}(Y)$ et $\mathbb{V}(X + Y) = \mathbb{V}(X) + \mathbb{V}(Y)$, si toutes ces quantités sont bien définies.

Démonstration. À compléter... ■

Terminologie 36.1.3 Indépendance et **corrélacion** sont contraires, tout comme indépendant et **corrélé**.

36.1.2 Exemples de lois discrètes

a Lois uniformes discrètes

C'est la transposition de l'équiprobabilité.

b Épreuve de Bernoulli

Définition 36.1.7 — Épreuve de Bernoulli. «succès» et «échec» désignant deux objets différents, une **épreuve de Bernoulli** est une expérience aléatoire modélisée par l'univers $\Omega = \{\text{succès}, \text{échec}\}$, ainsi que $\mathbb{P}(\{\text{succès}\}) = p$ et $\mathbb{P}(\{\text{échec}\}) = 1 - p$, où p est un paramètre réel de $[0, 1]$.

L'application qui à succès associe 1 et à échec associe 0 définit une variable aléatoire discrète particulière.

Définition 36.1.8 — Loi de Bernoulli. Une variable aléatoire X discrète suit la loi de Bernoulli de paramètre p , réel de $[0, 1]$, si $\mathbb{P}(X = 1) = p$ et $\mathbb{P}(X = 0) = 1 - p$.

On note $X \sim \mathcal{B}(p)$, qui est lu « X suit la loi $\mathcal{B}(p)$ » ou « X suit la loi de Bernoulli de paramètre p ». On peut aussi trouver les notations $X \sim \mathcal{B}(p)$ et $X \hookrightarrow \mathcal{B}(p)$.

Théorème 36.1.15 — Espérance, variance, écart-type. Si $X \sim \mathcal{B}(p)$, $\mathbb{E}(X) = p$, $\mathbb{V}(X) = p(1-p)$ et $\sigma(X) = \sqrt{p(1-p)}$.

c Lois géométriques

Modèle

Une suite d'épreuves de Bernoulli mutuellement indépendantes : occurrence du premier succès.

Formule

Définition 36.1.9 — Loi géométrique. Une variable aléatoire X discrète suit la loi de géométrique de paramètre p , réel de $[0, 1]$, si $\mathbb{P}(X = k) = p(1-p)^{k-1} \mathbb{1}_{\mathbb{N}}(k)$.

Propriétés

Théorème 36.1.16 — Espérance, variance, écart-type. Si une variable aléatoire X discrète suit la loi de géométrique de paramètre p , réel de $]0, 1]$, $\mathbb{E}(X) = \frac{1}{p}$, $\mathbb{V}(X) = \frac{1-p}{p^2}$.

Démonstration. À compléter... ■

d Lois binomiales

Modèle

Le nombre de succès parmi n épreuves de Bernoulli de même paramètre p de $[0, 1]$ et deux à deux indépendantes.

Formule

Définition 36.1.10 — Loi binomiale. Une variable aléatoire S discrète suit la loi de binomiale de paramètres n entier naturel et p , réel de $[0, 1]$, si $\mathbb{P}(S = k) = \binom{n}{k} p^k (1-p)^{n-k} \mathbb{1}_{\mathbb{N}}(k)$.

On note $S \sim \mathcal{B}(n, p)$, qui est lu « S suit la loi $\mathcal{B}(n, p)$ » ou « S suit la loi binomiale de paramètres n et p ».

R $\mathcal{B}(p)$ et $\mathcal{B}(1, p)$ sont les mêmes lois.

Propriétés

Théorème 36.1.17 Si n variables aléatoires deux à deux indépendantes suivent la loi $\mathcal{B}(p)$ alors leur somme suit la loi $\mathcal{B}(n, p)$.

Démonstration. À compléter... ■

Théorème 36.1.18 — Espérance, variance, écart-type. Si $S \sim \mathcal{B}(n, p)$, $\mathbb{E}(S) = np$, $\mathbb{V}(S) = np(1 - p)$ et $\sigma(S) = \sqrt{np(1 - p)}$.

Démonstration. À compléter de deux manières : avec la linéarité et par le calcul direct ■

e Lois de Poisson

Modèle

On modélise un nombre d'occurrences par unité lorsque la moyenne est connue.

Formule

Définition 36.1.11 — Loi de Poisson. Une variable aléatoire X discrète suit la loi de Poisson de paramètre λ , notée $\mathcal{P}(\lambda)$ avec λ réel strictement positif, si $\mathbb{P}(X = k) = \frac{\lambda^k}{k!} e^{-\lambda} \mathbb{1}_{\mathbb{N}}(k)$.

On note $X \sim \mathcal{P}(\lambda)$, qui est lu « X suit la loi $\mathcal{P}(\lambda)$ » ou « X suit la loi de Poisson de paramètre λ ».

Propriétés

Théorème 36.1.19 — Espérance, variance, écart-type. Si $X \sim \mathcal{P}(\lambda)$, $\mathbb{E}(X) = \lambda$, $\mathbb{V}(X) = \lambda$ et $\sigma(X) = \sqrt{\lambda}$.

Théorème 36.1.20 Si $X \sim \mathcal{P}(\lambda)$ et $Y \sim \mathcal{P}(\mu)$, X et Y étant indépendantes, alors $X + Y \sim \mathcal{P}(\lambda + \mu)$.

Démonstration. Pour tout entier naturel k , l'événement $X + Y = k$ est la réunion disjointe de tous les événements $(X = i \text{ et } Y = k - i)$ lorsque i varie entre 0 et k .

$$\begin{aligned} \mathbb{P}(X + Y = k) &= \sum_{i=0}^k \mathbb{P}(X = i, Y = k - i) \\ &= \sum_{i=0}^k \mathbb{P}(X = i) \mathbb{P}(Y = k - i) \\ &= \sum_{i=0}^k \frac{\lambda^i}{i!} e^{-\lambda} \frac{\mu^{k-i}}{(k-i)!} e^{-\mu} \\ &= \frac{(\lambda + \mu)^k}{k!} e^{-(\lambda + \mu)} \lambda^i \mu^{k-i} \end{aligned}$$

On a utilisé l'indépendance pour obtenir la deuxième ligne. ■

36.1.3 Variables aléatoires à densité

a Définitions

Définition 36.1.12 — fonction de densité. Une **(fonction de) densité** est une fonction réelle de variable réelle, positive, continue par morceaux, croissante et d'intégrale 1.

Définition 36.1.13 — variables aléatoires à densité. Une variable aléatoire X est à densité f signifie que pour tous réels a et b , on a

$$\mathbb{P}(a \leq X) = \int_{x=a}^{+\infty} f(x) \, dx$$

$$\mathbb{P}(X \leq b) = \int_{x=-\infty}^b f(x) \, dx$$

Corollaire 36.1.21 Dans le même contexte,

$$\mathbb{P}(a \leq X \leq b) = \int_{x=a}^b f(x) \, dx$$



- les intégrales impropres ne sont pas au programme de l'enseignement secondaire. Elles sont définies comme des limites d'intégrales propres lorsque les bornes tendent vers l'infini de manière indépendante. Il se pose la question de la convergence...
- En fait on a pour tout ensemble mesurable E , $\mathbb{P}(X \in E) = \int_E f(x) \, dx$.

Proposition 36.1.22 Si la variable aléatoire réelle X est à densité f , pour tout réel a on a $\mathbb{P}(X = a) = 0$.

Démonstration. $\mathbb{P}(X = a) = \mathbb{P}(a \leq X \leq a) = \int_{x=a}^a f(x) \, dx = 0$ ■

b Loi uniforme continue

Définition 36.1.14 — Loi uniforme continue. Une variable aléatoire réelle X suit la **loi uniforme** sur l'intervalle $[a, b]$, avec $a < b$, signifie qu'elle a pour densité

$$x \mapsto \frac{1}{b-a} \mathbb{1}_{[a,b]}(x)$$

Théorème 36.1.23 Soit X une variable aléatoire réelle qui suit la loi uniforme sur l'intervalle $[a, b]$, avec $a < b$. $\mathbb{E}(X) = \frac{a+b}{2}$, $\mathbb{V}(X) = \frac{(b-a)^2}{12}$ et $\sigma(X) = \frac{b-a}{2\sqrt{3}}$.

Démonstration. À compléter... ■

c Loi exponentielle

Définition 36.1.15 — Loi exponentielle. Une variable aléatoire réelle X suit la **loi exponentielle** de paramètre λ , avec $\lambda > 0$, si elle a pour densité

$$x \mapsto \lambda e^{-\lambda x} \mathbb{1}_{[0, +\infty[}(x)$$

Théorème 36.1.24 Soit X une variable aléatoire réelle qui suit la loi exponentielle de paramètre λ , avec $\lambda > 0$. $\mathbb{E}(X) = \frac{1}{\lambda}$, $\mathbb{V}(X) = \frac{1}{\lambda^2}$ et $\sigma(X) = \frac{1}{\lambda}$.

Démonstration. À compléter... ■

Théorème 36.1.25 — Vieillessement. Soit X une variable aléatoire réelle qui suit une loi exponentielle, on a

$$\forall t, t' \in \mathbb{R}_+, \mathbb{P}_{X \geq t}(X \geq t + t') = \mathbb{P}(X \geq t').$$

- R** Si X modélise une durée de vie, alors la probabilité de vivre encore t' ne dépend pas de l'âge déjà atteint *id est* du vieillissement.

Démonstration. C'est une réécriture de la propriété fonctionnelle de l'exponentielle.

À compléter... ■

- R** La somme de variables aléatoires indépendantes qui suivent une loi exponentielle ne suit pas une loi exponentielle mais une loi dite gamma. En revanche, c'est le cas pour leur minimum.

d Loi normale

Définition 36.1.16 — Loi normale. Une variable aléatoire X suit la **loi normale** de paramètres μ réel et σ réel strictement positif signifie qu'elle a pour densité

$$x \mapsto \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

On note $X \sim \mathcal{N}(\mu, \sigma)$, qui est lu « X suit la loi $\mathcal{N}(\mu, \sigma)$ » ou « X suit la loi normale de paramètres μ et σ ». On peut trouver la notation $X \sim \mathcal{N}(\mu, \sigma^2)$.

Théorème 36.1.26 — Espérance et variance de la loi normale. Si $X \sim \mathcal{N}(\mu, \sigma)$ alors $\mathbb{E}(X) = \mu$ et $\mathbb{V}(X) = \sigma^2$.

Démonstration. À compléter... ■

En particulier, pour $\mu = 0$ et $\sigma = 1$ on a la

Définition 36.1.17 — Loi normale centrée réduite. Une variable aléatoire X suit la **loi normale centrée réduite**, signifie qu'elle a pour densité

$$x \mapsto \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}$$

On note $X \sim \mathcal{N}(0, 1)$, qui est lu comme ci-dessus ou « X suit la loi normale centrée réduite».

Théorème 36.1.27 — Valeurs remarquables. Pour tout α de $[0, 1[$, il existe un unique réel u_α tel que

$$\frac{1}{\sqrt{2\pi}} \int_{x=-u_\alpha}^{u_\alpha} e^{-\frac{x^2}{2}} dx = \alpha$$

En particulier :

| α | u_α |
|--------------|------------|
| $\geq 99 \%$ | 2,58 |
| $\geq 95 \%$ | 1,96 |
| $\geq 90 \%$ | 1,65 |

Démonstration. Dans une feuille de calcul, mettre en colonne A les nombres de 1,64 à 2,58 avec un pas de 0,01. Mettre en B1 la formule $= 1 - 2 * \text{NORM.S.DIST}(A1; 1)$ puis étendre vers le bas. À compléter...

Définition 36.1.18 — Plages de normalité. Si $X \sim \mathcal{N}(\mu, \sigma)$ alors

$$\mathbb{P}(X \in [\mu - \sigma, \mu + \sigma]) \cong 68 \%$$

$$\mathbb{P}(X \in [\mu - 2\sigma, \mu + 2\sigma]) \cong 95\%$$

$$\mathbb{P}(X \in [\mu - 3\sigma, \mu + 3\sigma]) \cong 99 \%$$

Ces intervalles sont les **plages de normalité** à niveau de confiance de 68 %, 95 %, 99,7 %.

36.1.4 Théorèmes limites

a Loi faible des grands nombres

Théorème 36.1.28 — Inégalité de Bienaymé-Tchebychev. Soit X une variable aléatoire réelle avec espérance et variance.

$$\forall \varepsilon \in]0, +\infty[, \mathbb{P}(|X - \mathbb{E}(X)| \geq \varepsilon) \leq \frac{\mathbb{V}(X)}{\varepsilon^2}$$

Démonstration. À compléter...

Théorème 36.1.29 — Loi faible des grands nombres. Soit $(X_n)_{n \in \mathbb{N}^*}$ une suite de variables aléatoires réelles définies sur le même espace probabilisé, deux à deux indépendantes, suivant la même loi d'espérance μ et d'écart-type σ .

$$\forall \varepsilon \in]0, +\infty[, \mathbb{P} \left(\left| \frac{X_1 + X_2 + \dots + X_n}{n} - \mu \right| \geq \varepsilon \right) \xrightarrow{n \rightarrow \infty} 0$$

Démonstration. On applique l'inégalité de Bienaymé-Tchebychev à la moyenne $\frac{X_1 + X_2 + \dots + X_n}{n}$. Sachant que

$$\mathbb{E} \left(\frac{X_1 + X_2 + \dots + X_n}{n} \right) = \mu \text{ et } \mathbb{V} \left(\frac{X_1 + X_2 + \dots + X_n}{n} \right) = \frac{\sigma^2}{n}$$

on obtient :

$$\mathbb{P} \left(\left| \frac{X_1 + X_2 + \dots + X_n}{n} - \mu \right| \geq \varepsilon \right) \leq \frac{\sigma^2}{n\varepsilon^2}$$

d'où le résultat. ■

Corollaire 36.1.30 Dans le même contexte,

$$\forall \varepsilon \in]0, +\infty[, \mathbb{P} \left(-\varepsilon < \frac{X_1 + X_2 + \dots + X_n}{n} - \mu < \varepsilon \right) \xrightarrow{n \rightarrow \infty} 1$$

Démonstration. Il suffit de passer au complémentaire.

$$\mathbb{P} \left(-\varepsilon < \frac{X_1 + X_2 + \dots + X_n}{n} - \mu < \varepsilon \right) = 1 - \mathbb{P} \left(\left| \frac{X_1 + X_2 + \dots + X_n}{n} - \mu \right| \geq \varepsilon \right) \quad \blacksquare$$

- R** La loi faible des grands nombres est précisée par le théorème central limite ci-dessous.

b Théorème central limite

Hors programme mais pas de beaucoup, en tout cas absolument indispensable à la compréhension.

Théorème 36.1.31 — Central limite. Soit $(X_n)_{n \in \mathbb{N}^*}$ une suite de variables aléatoires réelles définies sur le même espace probabilisé, deux à deux indépendantes, suivant la même loi d'espérance μ et d'écart-type σ non nul. Pour tout nombre t ,

$$\mathbb{P} \left(\frac{X_1 + X_2 + \dots + X_n - n\mu}{\sigma\sqrt{n}} \leq t \right) \xrightarrow{n \rightarrow \infty} \frac{1}{\sqrt{2\pi}} \int_{-\infty}^t e^{-\frac{x^2}{2}} dx$$

- R** C'est un théorème très puissant car on ne connaît de la loi commune à toutes les variables aléatoires que la moyenne et l'écart type, et rien d'autre.

Démonstration. Hors programme. ■

Théorème 36.1.32 — Théorème de Moivre-Laplace. Soit $(S_n)_{n \in \mathbb{N}^*}$ une suite de variables aléatoires réelles telles que $S_n \sim \mathcal{B}(n, p)$, avec p dans $]0, 1[$. Pour tous réels a et b tels que $a \leq b$, on a

$$\mathbb{P} \left(a \leq \frac{S_n - np}{\sqrt{np(1-p)}} \leq b \right) \xrightarrow{n \rightarrow \infty} \frac{1}{\sqrt{2\pi}} \int_a^b e^{-\frac{x^2}{2}} dx$$

Démonstration. Hors programme. ■

- R** On retrouve le théorème central limite si $S_n = X_1 + X_2 + \dots + X_n$ et si les X_n suivent une loi de Bernoulli de paramètre p . Au passage : peut-on toujours obtenir une telle décomposition de S_n ? À préciser...

c Autre convergence

Théorème 36.1.33 Si pour tout entier naturel n on a $S_n \sim \mathcal{B}(n, p_n)$, avec $n p_n \xrightarrow{n \rightarrow +\infty} \lambda$ alors

$$\mathbb{P}(S_n = k) \xrightarrow{n \rightarrow \infty} \frac{\lambda^k}{k!} e^{-\lambda}$$

Démonstration. À compléter... ■

36.1.5 Fluctuation. Estimation.

La fluctuation : on connaît la loi de l'échantillon, on connaît la fréquence, on mesure la cohérence des deux.

L'estimation : on connaît le type de loi de l'échantillon, on connaît la fréquence, on estime la moyenne.

a Intervalle de fluctuation en 2^{de}

Présentation

Le programme de 2^{de} suggère de présenter aux élèves le résultat suivant : pour des échantillons de taille n supérieure ou égale à 25 et des proportions p du caractère comprises entre 0,2 et 0,8 : si f désigne la fréquence du caractère dans l'échantillon, f appartient à l'intervalle $[p - 1/\sqrt{n}, p + 1/\sqrt{n}]$ avec une probabilité d'au moins 0,95.

Justification asymptotique

Pour $0,2 \leq p \leq 0,8$, on obtient $0,4 \leq \sqrt{p(1-p)} \leq 0,5$, d'où

$$-\frac{1,96\sqrt{p(1-p)}}{\sqrt{n}} \leq \frac{S_n}{n} - p \leq \frac{1,96\sqrt{p(1-p)}}{\sqrt{n}} \implies -\frac{1}{\sqrt{n}} \leq \frac{S_n}{n} - p \leq \frac{1}{\sqrt{n}}.$$

Sous réserve que la limite existe, on retrouve bien l'estimation de la classe de seconde

$$\lim_{n \rightarrow +\infty} \mathbb{P} \left(-\frac{1}{\sqrt{n}} \leq \frac{S_n}{n} - p \leq \frac{1}{\sqrt{n}} \right) \geq 95\%$$

R Dans ce programme, il est conseillé de s'assurer que $n \geq 25$ et $0,2 \leq p \leq 0,8$. En classe terminale, on prendra plutôt $n \geq 30$, $np \geq 5$ et $n(1-p) \geq 5$. Mais à la limite !

Justification

On sait que nf suit la loi (n, p) , ce qui nous permet d'avoir une idée beaucoup plus précise du seuil de tolérance. Dans le tableau suivant, on a indiqué pour différentes valeurs de n pour les lignes et p pour les colonnes la probabilité d'avoir f dans l'intervalle indiqué ci-dessus, avec 4 chiffres après la virgule.

| $n \setminus p$ | 0,2 | 0,25 | 0,3 | 0,35 | 0,4 | 0,45 |
|-----------------|--------|--------|--------|--------|--------|--------|
| 25 | 0,9944 | 0,9822 | 0,9736 | 0,9649 | 0,9774 | 0,9569 |
| 26 | 0,9891 | 0,9791 | 0,9678 | 0,9608 | 0,9569 | 0,9526 |
| 27 | 0,9866 | 0,9741 | 0,9807 | 0,9589 | 0,9508 | 0,9682 |
| 28 | 0,9832 | 0,9855 | 0,9636 | 0,9728 | 0,9673 | 0,9443 |
| 29 | 0,9915 | 0,9817 | 0,9763 | 0,9692 | 0,9438 | 0,9618 |
| 30 | 0,9893 | 0,9678 | 0,9737 | 0,9467 | 0,9616 | 0,9354 |
| 40 | 0,9906 | 0,9837 | 0,9766 | 0,9703 | 0,9655 | 0,9625 |
| 50 | 0,9925 | 0,9790 | 0,9805 | 0,9633 | 0,9707 | 0,9545 |
| 100 | 0,9916 | 0,9852 | 0,9786 | 0,9729 | 0,9685 | 0,9657 |
| 1000 | 0,9873 | 0,9786 | 0,9703 | 0,9633 | 0,9580 | 0,9548 |
| 10000 | 0,9880 | 0,9797 | 0,9717 | 0,9649 | 0,9598 | 0,9566 |

On a utilisé la symétrie $p \leftrightarrow 1-p$ pour restreindre p entre 0,2 et 0,5, ainsi que la formule suivante

$$\begin{aligned} &= \text{BINOM.DIST}(\text{FLOOR}(n * p + \text{SQRT}(n)); n; p; 1) - \dots \\ &\dots - \text{BINOM.DIST}(\text{CEILING}(n * p - \text{SQRT}(n)) - 1; n; p; 1) \end{aligned}$$

qui vient du

Lemme 36.1.34

$$\mathbb{P} \left(-\frac{1}{\sqrt{n}} \leq f - p \leq \frac{1}{\sqrt{n}} \right) = \mathbb{P}(nf \leq \lfloor np + \sqrt{n} \rfloor) - \mathbb{P}(nf < \lfloor np - \sqrt{n} \rfloor)$$

Démonstration. On a

$$-\frac{1}{\sqrt{n}} \leq f - p \leq \frac{1}{\sqrt{n}} \Leftrightarrow np - \sqrt{n} \leq nf \leq np + \sqrt{n}$$

donc

$$\mathbb{P}\left(-\frac{1}{\sqrt{n}} \leq f - p \leq \frac{1}{\sqrt{n}}\right) = \mathbb{P}(nf \leq np + \sqrt{n}) - \mathbb{P}(nf < np - \sqrt{n}).$$

Comme nf est un entier,

$$\begin{aligned} nf \leq np + \sqrt{n} &\Leftrightarrow nf \leq \lfloor np + \sqrt{n} \rfloor, \\ nf < np - \sqrt{n} &\Leftrightarrow nf < \lfloor np + \sqrt{n} \rfloor. \end{aligned}$$

■

R si on fait une étude avec plus de données, on observe que pour avoir effectivement un seuil plus grand que 0,95, il faut prendre $n \geq 49$. Ce n'est pas du tout $n \geq 25$! C'est ce qui fait la différence entre un intervalle de fluctuation et un intervalle de fluctuation asymptotique.

b Intervalle de fluctuation en terminale.

Théorème 36.1.35 Si la variable aléatoire S_n suit la loi $\mathcal{B}(n, p)$, alors, pour tout α dans $[0, 1[$ on a,

$$\mathbb{P}\left(-u_\alpha \leq \frac{S_n - np}{\sqrt{np(1-p)}} \leq u_\alpha\right) \xrightarrow{n \rightarrow \infty} \alpha$$

ou de manière équivalente

$$\mathbb{P}\left(\frac{S_n}{n} \in I_n^\alpha(p)\right) \xrightarrow{n \rightarrow \infty} \alpha, \text{ avec } I_n^\alpha(p) \stackrel{\text{déf}}{=} p + u_\alpha \sqrt{\frac{p(1-p)}{n}} [-1, 1]$$

u_α étant la valeur remarquable associée à α .

Démonstration. Application du théorème de Moivre-Laplace. À compléter... ■

Pour appliquer ce théorème, on a la

Méthode 36.1.1 Soit $(X_n)_{n \in \mathbb{N}^*}$ une suite de variables aléatoires réelles deux à deux indépendantes qui suivent la même loi de Bernoulli. Soit f_n une réalisation de $\frac{X_1 + X_2 + \dots + X_n}{n}$.

- Si $f_n \in I_n^\alpha(p)$, on décidera que le paramètre de la loi de Bernoulli est p au seuil asymptotique $1 - \alpha$. Le risque asymptotique d'erreur dépend du paramètre réel de la loi.
- Si $f_n \notin I_n^\alpha(p)$, on décidera que le paramètre de la loi de Bernoulli n'est pas p au seuil asymptotique $1 - \alpha$. Le risque asymptotique d'erreur est de α .

C Estimation

Avec les notations précédentes, on observe que d'une certaine manière,

$$p + u_\alpha \sqrt{\frac{\frac{S_n}{n} \left(1 - \frac{S_n}{n}\right)}{n}} [-1, 1] \xrightarrow{n \rightarrow \infty} p + u_\alpha \sqrt{\frac{p(1-p)}{n}} [-1, 1]$$

comme par ailleurs

$$\frac{S_n}{n} \in p + u_\alpha \sqrt{\frac{\frac{S_n}{n} \left(1 - \frac{S_n}{n}\right)}{n}} [-1, 1] \Leftrightarrow p \in \frac{S_n}{n} + u_\alpha \sqrt{\frac{\frac{S_n}{n} \left(1 - \frac{S_n}{n}\right)}{n}} [-1, 1]$$

on en déduit d'une certaine manière le

Théorème 36.1.36 — Estimation de paramètre.

$$\mathbb{P}(p \in J_n^\alpha) \xrightarrow{n \rightarrow \infty} \alpha, \text{ avec } J_n^\alpha \stackrel{\text{déf}}{=} \frac{S_n}{n} + u_\alpha \sqrt{\frac{\frac{S_n}{n} \left(1 - \frac{S_n}{n}\right)}{n}} [-1, 1]$$

u_α étant la valeur remarquable associée à α .

Démonstration. Hors programme... ■



37. Familles