Applications et dénombrement

Table des matières

1 Applications

1.1 Généralités

Définition. Une fonction f d'un ensemble E dans un ensemble F est un triplet $f = (E, F, \Gamma)$, où E et F sont des ensembles et où Γ est une relation binaire sur $E \times F$ telle que $\forall x \in E,\ \forall y, z \in F,\ (x\ \Gamma\ y) \wedge (x\ \Gamma\ z) \Longrightarrow (y = z)$, c'est-à-dire telle que pour tout $x \in E$, il existe au plus un $y \in F$ en relation avec x.
On note alors "$y = f(x)$ " au lieu de $x\ \Gamma\ y$ ou bien $(x, y) \in \Gamma$.

- Le domaine de définition de f est $\{x \in E / \exists y \in F,\ x\ \Gamma\ y\}$. On le notera $\mathcal{D}_f$.
- Une application de E dans F est une fonction telle que $\mathcal{D}_f = E$.
- E s'appelle l'ensemble de départ de f et F l'ensemble d'arrivée.
- Γ s'appelle le graphe de f. $\Gamma = \{(x, y) \in E \times F / x\ \Gamma\ y\} = \{(x, f(x)) / x \in \mathcal{D}_f\}$.
- Lorsque $y = f(x)$, où $x \in E$ et $y \in F$,
  - on dit que y est l'image de x par f et
  - que x est un antécédent de y par f.

Remarque. En pratique, on confond souvent les deux notions d'application et de fonction, lorsque le domaine de définition est connu sans ambiguité. La suite de ce chapitre est essentiellement consacrée aux applications, ce qui évite d'étudier précisément les problèmes de domaines de définition.

Propriété. Soit f une fonction d'un ensemble E vers un ensemble F et soit g une fonction d'un ensemble E' vers un ensemble F'.
Alors $f = g$ si et seulement si $E = E'$, $F = F'$, $\mathcal{D}_f = \mathcal{D}_g$
et pour tout $x \in \mathcal{D}_f$, $f(x) = g(x)$.

Démonstration.
Notons $f = (E, F, \Gamma)$ et $g = (E', F', \Gamma')$. Supposons que $f = g$. Alors $E = E'$ et $F = F'$.
Soit $x \in \mathcal{D}_f$. Il existe $y \in F$ tel que $(x, y) \in \Gamma$. Alors $(x, y) \in \Gamma'$. Ainsi $x \in \mathcal{D}_g$ et $y = f(x) = g(x)$ ...
Réciproquement, supposons que $E = E'$, $F = F'$, $\mathcal{D}_f = \mathcal{D}_g$
et pour tout $x \in \mathcal{D}_f$, $f(x) = g(x)$.
Soit $(x, y) \in \Gamma$. Alors $x \in \mathcal{D}_f$, donc $x \in \mathcal{D}_g$ et $f(x) = g(x) = y$, donc $(x, y) \in \Gamma'$. □

Exemple. La fonction $f : x \longmapsto \frac{1}{x}$ de $\mathbb{R}$ dans $\mathbb{R}$ a pour domaine de définition $\mathbb{R}^*$ et pour graphe $\{(x, \frac{1}{x}) / x \in \mathbb{R}^*\}$.

Remarque. C'est pour garantir cette propriété qu'une fonction est définie comme un triplet (E, F, Γ). Ainsi, si deux fonctions f et g sont telles que $\mathcal{D}_f = \mathcal{D}_g$ et
$\forall x \in \mathcal{D}_f,\ f(x) = g(x)$, elles sont tout de même différentes dès lors qu'elles ont des ensembles de départ ou d'arrivée différents.

Définition. Soit E et I deux ensembles. La famille $(e_i)_{i \in I}$ d'éléments de E indexée par I est l'unique application de I dans E dont le graphe est $\{(i, e_i) / i \in I\}$. Il s'agit d'une autre façon de noter une application, parfois mieux adaptée.

Définition. Une *suite* est une famille d'éléments indexée par $\mathbb{N}$, ou éventuellement par $\{n \in \mathbb{N}/n \geq n_0\}$ (où $n_0 \in \mathbb{N}$).

Définition.
- Lorsque E et F sont deux ensembles, le triplet $(E, F, \emptyset)$ est une fonction, appelée la fonction vide de E dans F, dont le domaine de définition est vide.
- Si F est un ensemble, le triplet $(\emptyset, F, \emptyset)$ est appelé l'application vide, à valeurs dans F.
- Cette application vide est égale à la famille vide à valeurs dans F, parfois notée $(e_i)_{i\in\emptyset}$.

Notation. L'application identité sur E est définie par : $\forall x \in E,\ \ Id_E(x) = x$.

Définition. Soit E un ensemble et A une partie de E. L'indicatrice de A dans E est l'unique application, notée $\mathbf{1}_A$, de E dans $\{0, 1\}$ telle que $\mathbf{1}_A(x) = 1$ si $x \in A$ et $\mathbf{1}_A(x) = 0$ si $x \in E \setminus A$.

Propriété. Soit E un ensemble et A et B deux parties de E. En définissant naturellement la somme, la différence et le produit de deux applications de E dans $\mathbb{R}$, on vérifie que : $\mathbf{1}_{E\setminus A} = \mathbf{1}_E - \mathbf{1}_A$, $\mathbf{1}_{A\cap B} = \mathbf{1}_A.\mathbf{1}_B$ et $\mathbf{1}_{A\cup B} = \mathbf{1}_A + \mathbf{1}_B - \mathbf{1}_A.\mathbf{1}_B$.

Remarque. Il est important de bien distinguer une fonction f, par exemple la fonction exponentielle $exp\ :\ x \longmapsto e^x$ de $\mathbb{R}$ dans $\mathbb{R}$, de la quantité $f(x)$ pour x donné. Ainsi $exp \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ alors que pour $x \in \mathbb{R}$, $exp(x) = e^x$ est un réel.

Définition. Soit f une application d'un ensemble E vers un ensemble F. On suppose que F est muni d'une relation d'ordre $\preceq$. Soit A une partie de E.
- Soit $m \in F$. On dit que m est un majorant (resp : minorant) de f sur A si et seulement si m est un majorant (resp : minorant) de $f(A)$.
- On dit que f est majorée (resp : minorée, bornée) sur A si et seulement si $f(A)$ est une partie majorée (resp : minorée, bornée) de F.
- Lorsque $f(A)$ possède un maximum (resp : minimum), on dit que f possède un maximum (resp : un minimum) sur A et on note $\max\limits_{x\in A} f(x) = \max(f(A))$ (resp : ...).
- Lorsque $f(A)$ possède une borne supérieure (resp : inférieure), on dit que f possède un sup sur A (resp : un inf) et on note $\sup\limits_{x\in A} f(x) = \sup(f(A))$ (resp : ...).

Exemple. Déterminer le maximum de l'application $x \longmapsto x(1 - x)$ sur $[0, 1]$.
Solution : Notons f cette fonction. On pourrait la dériver et tracer son tableau de variations. De façon plus élémentaire, pour tout $x \in [0, 1]$,
$f(x) = x - x^2 = -(x - \frac{1}{2})^2 + \frac{1}{4} \leq \frac{1}{4}$, donc $\frac{1}{4}$ majore f sur $[0, 1]$.
De plus, $f(\frac{1}{2}) = \frac{1}{4}$, donc $\max\limits_{x\in[0,1]} f(x) = f(\dfrac{1}{2}) = \dfrac{1}{4}$.

Exemple. De manière élémentaire, déterminer la borne supérieure de $x \longmapsto \dfrac{x-1}{x+1}$ sur $[1, +\infty[$.

Solution : Notons f cette application. Pour tout $x \in [1, +\infty[$,
$0 \leq f(x) < \dfrac{x+1}{x+1} = 1$, donc 1 est un majorant de f sur $[1, +\infty[$.
Soit $a < 1$. Pour tout $x \in [1, +\infty[$, $x + 1 > 0$,
donc $f(x) > a \iff x - 1 > a(x+1) \iff x(1-a) > a+1$, or $1 - a > 0$,
donc $f(x) > a \iff x > \dfrac{a+1}{1-a}$. Cette inéquation possède des solutions, donc 1 est le plus petit des majorants. On a montré, sans recourir à des arguments d'analyse, que $\sup_{x \in [1,+\infty[} f(x)$ est défini et qu'il vaut 1.

C'est cependant plus rapide avec un peu d'analyse : $f'(x) = \dfrac{2}{(x+1)^2} \geq 0$, donc f est croissante. Ainsi, d'après le théorème de la limite monotone, $f(x) \underset{x \to +\infty}{\longrightarrow} \sup_{t \in [1,+\infty[} f(t)$, or on sait que $f(x) \underset{x \to +\infty}{\longrightarrow} 1$ et le principe d'unicité de la limite permet de conclure.

Définition. Soit I un ensemble quelconque et soit $(f_i)_{i \in I}$ une famille d'éléments d'un ensemble F. On suppose que F est muni d'une relation d'ordre $\preceq$.

- Soit $m \in F$. On dit que m est un majorant (resp : minorant) de la famille $(f_i)_{i \in I}$ si et seulement si m est un majorant (resp : minorant) de $\{f_i / i \in I\}$.
- On dit que la famille (f_i) est majorée (resp : minorée, bornée) si et seulement si $\{f_i / i \in I\}$ est une partie majorée (resp : minorée, bornée) de F.
- Lorsque $\{f_i / i \in I\}$ possède un maximum (resp : minimum), on dit que la famille (f_i) possède un maximum (resp : un minimum)
  et on note $\max_{i \in I} f_i = \max(\{f_i / i \in I\})$ (resp : ...).
- Lorsque $\{f_i / i \in I\}$ possède une borne supérieure (resp : inférieure), on dit que la famille (f_i) possède un sup (resp : un inf)
  et on note $\sup_{i \in I} f_i = \sup(\{f_i / i \in I\})$ (resp : ...).

Exemple. Pour tout $n \in \mathbb{N}^*$, posons $x_n = \dfrac{n-1}{n+1}$. En adaptant l'exemple précédent, on peut montrer que $\sup_{n \in \mathbb{N}^*} x_n = 1$.

Notation. On note $\mathcal{F}(E, F)$ ou bien F^E l'ensemble des applications de E dans F. F^I est donc aussi l'ensemble des familles indexées par I d'éléments de l'ensemble F

Définition. Soient E et F deux ensembles, E' une partie de E et F' une partie de F.

- Soit f une application de E dans F.
  Si $E' \subset E$, la restriction de f à E' est l'unique application de E' dans F telle que $\forall x \in E', \ f|_{E'}(x) = f(x)$.
- Soit f une application de E' dans F. On appelle prolongement de f sur E toute application g de E dans F telle que $g|_{E'} = f$.
- Si F' est une partie de F telle que, pour tout $x \in E$, $f(x) \in F'$, la corestriction de f à F' est l'unique application de E dans F' telle que : pour tout $x \in E$, $f|^{F'}(x) = f(x)$.

— Si $E' \subset E$ et $F' \subset F$, lorsque pour tout $x \in E'$, $f(x) \in F'$, on désigne par $f|_{E'}^{F'}$ l'unique application de E' dans F' telle que, pour tout $x \in E'$, $f|_{E'}^{F'}(x) = f(x)$.

Définition. Soit f une application d'un ensemble E *dans lui-même*. Une partie A de E est stable par f si et seulement si $[\forall x \in A,\ \ f(x) \in A]$, c'est-à-dire si et seulement si $f|_A^A$ est définie.

Définition. Soit f une application de E dans F et g une application de F dans G. La composée de g et de f est l'unique application $g \circ f$ de E dans G définie par : $\forall x \in E,\ \ (g \circ f)(x) = g(f(x))$.

Remarque. Pour considérer $g \circ f$, on doit être dans la situation $E \xrightarrow{f} F \xrightarrow{g} G$: il y a donc inversion de l'ordre.

Exemple. Si $\begin{array}{rccc} f : & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \sin x \end{array}$ et $\begin{array}{rccc} g : & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & x^3 \end{array}$, alors $(f \circ g)(x) = \sin(x^3)$ et $(g \circ f)(x) = \sin^3 x$.

Associativité de la composition : Soit f une application de E dans F, g une application de F dans G et h une application de G dans H. Alors $h \circ (g \circ f) = (h \circ g) \circ f$. On peut donc noter $h \circ g \circ f$ cette fonction.

Démonstration.
Pour tout $x \in E$, $[h \circ (g \circ f)](x) = h[(g \circ f)(x)] = h[g(f(x))]$
et $[(h \circ g) \circ f](x) = (h \circ g)(f(x)) = h(g(f(x)))$. □

1.2 Applications croissantes et décroissantes

Définition. Soit f une application d'un ensemble ordonné $(E, \leq_E)$ dans un ensemble ordonné $(F, \leq_F)$.

— f est croissante si et seulement si $[\forall x, y \in E,\ \ x \leq_E y \Longrightarrow f(x) \leq_F f(y)]$.
— f est strictement croissante si et seulement si
$\forall x, y \in E,\ \ x <_E y \Longrightarrow f(x) <_F f(y)$.
— f est décroissante si et seulement si elle est croissante de $(E, \leq_E)$ dans $(F, \geq_F)$.
— f est strictement décroissante si et seulement si
$\forall x, y \in E,\ \ x <_E y \Longrightarrow f(x) >_F f(y)$.
— f est monotone si et seulement si f est croissante ou décroissante.
— f est strictement monotone si et seulement si f est strictement croissante ou strictement décroissante.

Exemples :

— L'application $x \longmapsto x^2$ est strictement croissante sur $\mathbb{R}_+$, strictement décroissante sur $\mathbb{R}_-$, donc sur $\mathbb{R}$, elle n'est pas monotone.
— L'application partie entière est croissante sur $\mathbb{R}$.
En effet, si $x, y \in \mathbb{R}$ avec $x < y$, alors $\{k \in \mathbb{Z} / k \leq x\} \subset \{k \in \mathbb{Z} / k \leq y\}$.
— L'application $\begin{array}{ccc} (\mathbb{N}^*, |) & \longrightarrow & (\mathbb{N}^*, |) \\ n & \longmapsto & n^2 \end{array}$ est strictement croissante.

— Si E est un ensemble, l'application $\begin{array}{ccc}(\mathcal{P}(E),\subset) & \longrightarrow & (\mathcal{P}(E),\subset)\\ A & \longmapsto & \overline{A}\end{array}$ est strictement décroissante.

— Notons $\mathbb{N}^{(\mathbb{P})}$ l'ensemble des familles $(v_p)_{p\in\mathbb{P}}$ d'entiers naturels telles que $\{p\in\mathbb{N}/v_p\neq 0\}$ est de cardinal fini. Il s'agit des suites *presque nulles* indexées par $\mathbb{P}$. On munit $\mathbb{N}^{(\mathbb{P})}$ de l'ordre produit :

$$(v_p)_{p\in\mathbb{P}}\leq(w_p)_{p\in\mathbb{P}}\Longleftrightarrow[\forall p\in\mathbb{P},\ \ v_p\leq w_p].$$

Alors l'application $\begin{array}{ccc}\mathbb{N}^{(\mathbb{P})} & \longrightarrow & \mathbb{N}^*\\ (v_p)_{p\in\mathbb{P}} & \longmapsto & \displaystyle\prod_{p\in\mathbb{P}}p^{v_p}\end{array}$ est une bijection (d'après le théorème sur la décomposition primaire d'un entier) qui est strictement croissante si l'on munit $\mathbb{N}^*$ de la relation de divisiblité.

Remarque. On a vu qu'il existe des fonctions qui ne sont ni décroissantes, ni croissantes. Ainsi, si l'on suppose qu'une application f n'est pas croissante, on ne peut pas affirmer qu'elle est décroissante.

Propriété.
— La composée de deux applications croissantes est croissante.
— La composée de deux applications décroissantes est croissante.
— La composée d'une application croissante et d'une application décroissante est décroissante.

Propriété. Soit f et g deux fonctions d'un ensemble ordonné $(E,\leq)$ dans $\mathbb{R}$.
— Si f et g sont croissantes, alors $f+g$ est croissante.
— Si f et g sont décroissantes, alors $f+g$ est décroissante.
— Si f est croissante, $-f$ est décroissante.
— Si f et g sont à valeurs positives et croissantes (resp : décroissantes), alors fg est croissante (resp : décroissante).
— Si f et g sont à valeurs strictement positives et sont strictement croissantes (resp : strictement décroissantes), alors fg est strictement croissante (resp : strictement décroissante).

Démonstration.
Démontrons seulement la dernière propriété dans le cas strictement décroissant.
Soit $x,y\in E$ tels que $x<y$. On a $0<f(y)<f(x)$ et $0<g(y)<g(x)$, donc $(fg)(y)=f(y)g(y)<f(x)g(y)<f(x)g(x)$. Ainsi fg est strictement décroissante. □

Exemple. Pour tout $x\in[0,\frac{\pi}{2}]$, posons $f(x)=\cos(\sin x)+\sin(\cos x)$.
cos est une application décroissante de $[0,\frac{\pi}{2}]$ dans $[0,1]$ et sin est croissante de $[0,\frac{\pi}{2}]$ dans $[0,1]$. Ainsi, par composition, $x\longmapsto\cos(\sin x)$ et $x\longmapsto\sin(\cos x)$ sont décroissantes, ce qui montre, sans dériver, que f est décroissante.

Définition. Soit f et g deux applications d'un ensemble E dans un ensemble ordonné $(F,\leq)$. On écrit $f\leq g$ si et seulement si , pour tout $x\in E$, $f(x)\leq g(x)$.
On définit ainsi une relation d'ordre sur $\mathcal{F}(E,F)$.

Exemple. Sur $\mathbb{R}_+$, $\sin\leq Id_{\mathbb{R}_+}$.

1.3 Images directes et réciproques

Définition. Soit f une application de E dans F.

— Si A est une partie de E, l'image directe de A par f est $f(A) \triangleq \{f(x)/x \in A\}$.
Ainsi, $\forall y \in F,\ y \in f(A) \iff [\exists x \in A,\ y = f(x)]$.
$f(A)$ est l'ensemble des images par f des éléments de A.

— Si B est une partie de F, l'image réciproque de B par f est
$f^{-1}(B) \triangleq \{x \in E/f(x) \in B\}$. Ainsi, $\forall x \in E,\ x \in f^{-1}(B) \iff f(x) \in B$.
$f^{-1}(B)$ est l'ensemble des antécédents par f des éléments de B.

Remarque. La notation $f(A)$ est pratique, mais curieuse, car dès que f est une application de E dans F, cette notation fait également de f une application de $\mathcal{P}(E)$ dans $\mathcal{P}(F)$.

Exemple. $\exp(\mathbb{R}) = \mathbb{R}_+^*$, $\cos([0, \frac{\pi}{2}]) = [0, 1]$, $\sin(\mathbb{R}) = [-1, 1]$.
$(\mathbf{1}_A)^{-1}(\{1\}) = A$, $\exp^{-1}([1, +\infty[) = \mathbb{R}_+$, $\sin^{-1}(\{1, -1\}) = \{\frac{\pi}{2} + k\pi/k \in \mathbb{Z}\}$.
Si $f\ :\ x \longmapsto x^2$, $f^{-1}([1, 2[) =]-\sqrt{2}, -1] \cup [1, \sqrt{2}[$.

Propriétés des images directes : Soit f une application de E dans F, $(A_i)_{i\in I}$ une famille de parties de E, A et A' deux parties de E.

— $A \subset A' \Longrightarrow f(A) \subset f(A')$.

— $f\Big(\bigcup_{i\in I} A_i\Big) = \bigcup_{i\in I} f(A_i)$.

— $f\Big(\bigcap_{i\in I} A_i\Big) \subset \bigcap_{i\in I} f(A_i)$, mais l'inclusion réciproque est fausse en général.

— $f(E \setminus A) \supset f(E) \setminus f(A)$, mais l'inclusion réciproque est fausse en général.

Démonstration.

— Soit $y \in F$.
$$\begin{aligned} y \in f\Big(\bigcup_{i\in I} A_i\Big) &\iff \exists x \in \bigcup_{i\in I} A_i,\ y = f(x) \\ &\iff \exists x \in E, \exists i \in I,\ x \in A_i \wedge y = f(x) \\ &\iff \exists i \in I,\ \exists x \in A_i,\ y = f(x) \\ &\iff \exists i \in I,\ y \in f(A_i) \\ &\iff y \in \bigcup_{i\in I} f(A_i). \end{aligned}$$

— Soit $y \in f\Big(\bigcap_{i\in I} A_i\Big)$. Il existe $x \in \bigcap_{i\in I} A_i$ tel que $y = f(x)$.
Pour tout $i \in I$, $x \in A_i$, donc $y = f(x) \in f(A_i)$. Ainsi $y \in \bigcap_{i\in I} f(A_i)$.
DONC, $f\Big(\bigcap_{i\in I} A_i\Big) \subset \bigcap_{i\in I} f(A_i)$.
Lorsque f est l'application valeur absolue sur $\mathbb{R}$, en prenant $A_1 = \mathbb{R}_+$ et $A_2 = \mathbb{R}_-$, $f(A_1 \cap A_2) = f(\{0\}) = \{0\}$ et $f(A_1) \cap f(A_2) = \mathbb{R}_+$. Ainsi, l'inclusion réciproque peut être fausse.

— Soit $y \in f(E) \setminus f(A)$. Il existe $x \in E$ tel que $y = f(x)$. Si $x \in A$, alors $y = f(x) \in f(A)$ ce qui est faux. Ainsi $x \in E \setminus A$, donc $y \in f(E \setminus A)$.
— Toujours avec l'application valeur absolue, si $A = \mathbb{R}_+$, alors $f(\mathbb{R} \setminus A) = \mathbb{R}_+^*$ et $f(\mathbb{R}) \setminus f(A) = \emptyset$. Dans ce cas, $f(E \setminus A) \not\subset f(E) \setminus f(A)$.

□

Propriétés des images réciproques : Soit f une application de E dans F, $(B_i)_{i\in I}$ une famille de parties de F, B et B' deux parties de F.

— $B \subset B' \Longrightarrow f^{-1}(B) \subset f^{-1}(B')$.
— $f^{-1}\Big(\bigcup_{i\in I} B_i\Big) = \bigcup_{i\in I} f^{-1}(B_i)$.
— $f^{-1}\Big(\bigcap_{i\in I} B_i\Big) = \bigcap_{i\in I} f^{-1}(B_i)$.
— $f^{-1}(F \setminus B) = E \setminus f^{-1}(B)$.

Démonstration.

— Soit $x \in f^{-1}\Big(\bigcup_{i\in I} B_i\Big)$. Alors $f(x) \in \bigcup_{i\in I} B_i$, donc il existe $i_0 \in I$ tel que $f(x) \in B_{i_0}$. Alors $x \in f^{-1}(B_{i_0}) \subset \bigcup_{i\in I} f^{-1}(B_i)$.
Réciproquement, soit $x \in \bigcup_{i\in I} f^{-1}(B_i)$. Il existe $i_0 \in I$ tel que $x \in f^{-1}(B_{i_0})$. Alors $f(x) \in B_{i_0} \subset \bigcup_{i\in I} B_i$, donc $x \in f^{-1}\Big(\bigcup_{i\in I} B_i\Big)$.
— De même, on montre que $f^{-1}\Big(\bigcap_{i\in I} B_i\Big) = \bigcap_{i\in I} f^{-1}(B_i)$.
— Soit $x \in E$. $x \in f^{-1}(F \setminus B) \iff f(x) \in F \setminus B \iff \neg(f(x) \in B)$, donc $x \in f^{-1}(F \setminus B) \iff \neg(x \in f^{-1}(B)) \iff x \in E \setminus f^{-1}(B)$.

□

Propriété. Avec les notations de la propriété précédente,
$A \subset f^{-1}(f(A))$ et $f(f^{-1}(B)) \subset B$, mais les inclusions réciproques peuvent être fausses.

Démonstration.

◇ Soit $x \in A$. $f(x) \in f(A)$, or $x \in f^{-1}(f(A)) \iff f(x) \in f(A)$, donc $x \in f^{-1}(f(A))$.
◇ Soit $y \in f(f^{-1}(B))$. Il existe $x \in f^{-1}(B)$ tel que $y = f(x)$. Mais $x \in f^{-1}(B)$, donc $f(x) \in B$. On en déduit que $y \in B$.
◇ Reprenons pour f l'application valeur absolue de $\mathbb{R}$ dans $\mathbb{R}$.
Avec $A = \mathbb{R}_+$, $f(A) = \mathbb{R}_+$ donc $f^{-1}(f(A)) = \mathbb{R}$ (ensemble des antécédents de réels positifs). Avec $B = \mathbb{R}$, $f^{-1}(B) = \mathbb{R}$ puis $f(f^{-1}(B)) = \mathbb{R}_+$. □

1.4 Injectivité et surjectivité

Définition. Soit f une application de E dans F.
On dit que f est injective si et seulement si $\forall x, y \in E,\ [f(x) = f(y) \Longrightarrow x = y]$.
f est injective si et seulement si, pour tout couple d'éléments distincts de E, leurs images sont différentes.
f est injective si et seulement si tout élément de F possède au plus un antécédent.

Exemple. L'application qui à chaque individu associe son prénom n'est pas injective. Celle qui associe à tout individu ses empreintes digitales est injective.

Interprétation graphique.

Propriété. Soit f une application d'un ensemble ordonné $(E, \leq_E)$ dans un ensemble ordonné $(F, \leq_F)$.
Si $\leq_E$ est total et si f est strictement monotone, alors f est injective.

Définition. Soit f une application de E dans F.
On dit que f est surjective si et seulement si $\forall y \in F,\ \exists x \in E,\ y = f(x)$.
f est surjective si et seulement si $f(E) = F$.
f est surjective si et seulement si tout élément de F possède au moins un antécédent.

Exemple. L'application $(x, y) \longmapsto x$ de $\mathbb{R}^2$ dans $\mathbb{R}$ est surjective.

Définition. On dit que f est bijective si et seulement si f est injective et surjective, c'est-à-dire si et seulement si tout élément de l'ensemble d'arrivée possède un unique antécédent dans l'ensemble de départ.

Exemple. L'application $(x, y) \longmapsto (x+y, x-y)$ est une bijection de $\mathbb{R}^2$ dans lui-même.

Remarque. On évitera de confondre l'injectivité de f avec la pseudo-injectivité : f est pseudo-injective si et seulement si $\forall x, y \in E,\ [x = y \Longrightarrow f(x) = f(y)]$, ce qui est ...toujours vrai.
De même, on évitera de confondre la surjectivité de f avec la pseudo-surjectivité : f est pseudo-surjective si et seulement si $\forall x \in E,\ \exists y \in F,\ y = f(x)$, ce qui est ...toujours vrai. On pourrait également dire que f est pseudo-surjective si et seulement si $\forall y \in f(E),\ \exists x \in E,\ y = f(x)$.

Propriété. Si l'on considère une application quelconque, il existe une manière naturelle de lui associer une bijection : soit f une application de E dans F. C'est déjà une surjection si l'on remplace F par $f(E)$.
Sur E, on définit la relation binaire R par : $xRy \Longleftrightarrow f(x) = f(y)$. R est une relation d'équivalence. Alors l'application $\begin{array}{rccc} \overline{f} : & E/R & \longrightarrow & f(E) \\ & \overline{x} & \longmapsto & f(x) \end{array}$ est une bijection.

Démonstration.
Il faut d'abord montrer que $\overline{f}$ est correctement définie, c'est-à-dire que $f(x)$ est effectivement une fonction de $\overline{x}$, ou encore que si $\overline{x} = \overline{y}$, alors $f(x) = f(y)$, ce qui est évident.
On vérifie ensuite la surjectivité et l'injectivité. □

Propriété. La composée de deux injections est une injection.
La composée de deux surjections est une surjection.
La composée de deux bijections est une bijection.

Démonstration.
Soit f une application de E dans F et g une application de F dans G.
$\diamond$ Supposons que f et g sont injectives. Soit $x, y \in E$ tels que $(g \circ f)(x) = (g \circ f)(y)$. On a $g(f(x)) = g(f(y))$, or g est injective, donc $f(x) = f(y)$, puis $x = y$ car f est injective. Ceci démontre que $g \circ f$ est injective.
$\diamond$ Supposons que f et g sont surjectives. Soit $z \in G$. g étant surjective, il existe $y \in F$ tel que $z = g(y)$. f est aussi surjective, donc il existe $x \in E$ tel que $y = f(x)$. Alors $z = (g \circ f)(x)$. Ceci prouve la surjectivité de $g \circ f$. $\square$

Propriété. (hors programme) Soient E, F et G trois ensembles.
- Soit $f : F \longrightarrow G$ et g et h deux applications de E dans F.
  Si f est injective, alors $fg = fh \Longrightarrow g = h$: on dit que f est simplifiable (ou régulière) à gauche.
- Soit $f : E \longrightarrow F$ et g et h deux applications de F dans G.
  Si f est surjective, alors $gf = hf \Longrightarrow g = h$: on dit que f est simplifiable (ou régulière) à droite.

Démonstration.
$\diamond$ Supposons que f est injective et que $fg = fh$.
Soit $x \in E$. On a $f(g(x)) = f(h(x))$ et f est injective, donc $g(x) = h(x)$.
$\diamond$ Supposons que f est surjective et que $gf = hf$.
Soit $y \in F$. Il existe $x \in E$ tel que $y = f(x)$. Alors $g(y) = g(f(x)) = h(f(x)) = h(y)$.
$\square$

Propriété. Soit f une application de E dans F et g une application de F dans G.
Si $g \circ f$ est injective, alors f est injective.
Si $g \circ f$ est surjective, alors g est surjectif.

Définition et propriété :
$\diamond$ Soit f une bijection de E dans F.
Pour tout $y \in F$, notons $f^{-1}(y)$ l'unique antécédent de y par f.
Alors f^{-1} est une bijection de F dans E, appelée la bijection réciproque de f.
$\diamond$ On vérifie que $f \circ f^{-1} = Id_F$ et $f^{-1} \circ f = Id_E$.
$\diamond$ Réciproquement, s'il existe une application g de F dans E telle que $f \circ g = Id_F$ et $g \circ f = Id_E$, alors f et g sont des bijections et $g = f^{-1}$.
$\diamond$ $(f^{-1})^{-1} = f$.

Démonstration.
$\diamond$ Soit $y \in F$. Posons $x = f^{-1}(y)$. C'est l'unique antécédent de y par f, donc $f(x) = y$.
Ainsi $(f \circ f^{-1})(y) = y$, pour tout $y \in F$, donc $f \circ f^{-1} = Id_F$.
$\diamond$ Soit $x \in E$. Posons $y = f(x)$. x est un antécédent de y par f,
donc $x = f^{-1}(y) = f^{-1}(f(x))$. Ainsi, $f^{-1} \circ f = Id_E$.

◇ Id_E et Id_F étant bijectives, la propriété précédente permet d'en déduire que f^{-1} est une bijection de F dans E.
◇ Supposons qu'il existe une application g de F dans E telle que $f \circ g = Id_F$ et $g \circ f = Id_E$. La propriété précédente prouve à nouveau que f et g sont bijectives.
Enfin, $g = g \circ Id_F = g \circ (f \circ f^{-1}) = (g \circ f) \circ f^{-1} = Id_E \circ f^{-1} = f^{-1}$. □

Exemple. La bijection réciproque de la bijection $(x, y) \longmapsto (x + y, x - y)$ de $\mathbb{R}^2$ dans lui-même est l'application $(a, b) \longmapsto (\frac{a+b}{2}, \frac{a-b}{2})$.

Remarque. La dernière partie de cette propriété fournit une méthode souvent efficace pour prouver la bijectivité d'une application : il suffit de trouver g telle que $f \circ g = Id_F$ et $g \circ f = Id_E$.
Par exemple, l'application $\begin{array}{ccc} (\mathcal{P}(E), \subset) & \longrightarrow & (\mathcal{P}(E), \subset) \\ A & \longmapsto & \overline{A} \end{array}$ est une bijection car, composée avec elle-même, elle donne l'identité.
Une application f telle que $f \circ f = Id_E$ s'appelle une involution sur E.

Propriété. Soit f une bijection de E dans F. Soit B une partie de F. Alors l'image directe de B par f^{-1} coïncide avec l'image réciproque de B par f.
C'est heureux car ils sont tous les deux notés $f^{-1}(B)$.

Démonstration.
Notons A_1 l'image directe de B par f^{-1} et A_2 l'image réciproque de B par f.
Soit $x \in E$. $x \in A_1 \iff \exists y \in B,\ \ x = f^{-1}(y)$
et $x \in A_2 \iff f(x) \in B \iff \exists y \in B,\ \ f(x) = y$. □

Propriété. Soit f une bijection de E dans F et g une bijection de F dans G.
Alors $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Démonstration.
On sait déjà que $g \circ f$ est bien une bijection.
De plus, $(g \circ f) \circ (f^{-1} \circ g^{-1}) = gff^{-1}g^{-1} = Id_G$ et $(f^{-1}g^{-1})(gf) = Id_E$. □

Remarque. La notation f^{-1}, pour une application f, est utilisée selon deux sens *différents*, qu'il est important de bien distinguer :
- Lorsque f est une application *quelconque* de E dans F, si B est une partie de F, alors $f^{-1}(B) = \{x \in E / f(x) \in B\}$.
- Lorsque f est une *bijection* de E dans F, pour tout $y \in F$, $f^{-1}(y)$ est l'unique antécédent de y par f.

En particulier, dès que l'on utilise une expression de la forme $f^{-1}(y)$ où y est un *élément* de l'ensemble d'arrivée de f, on suppose nécessairement que f est une bijection.
Lorsque $y \in F$, il importe de bien distinguer $f^{-1}(y)$ qui représente, pour une bijection f, l'unique antécédent de y, et $f^{-1}(\{y\})$ qui représente, pour une application f quelconque, l'ensemble des antécédents de y. Cet ensemble peut être vide lorsque f n'est pas surjective, il peut contenir plus de deux éléments lorsque f n'est pas injective.

> **Exercice.** Soit f une application de E dans F.
> Lorsque f est surjective, montrer que, pour toute partie B de F, $f(f^{-1}(B)) = B$.
> Lorsque f est injective, montrer que, pour toute partie A de E, $f^{-1}(f(A)) = A$.

Propriété. Soit f une bijection de E dans F.
Pour toute partie B de F, $f(f^{-1}(B)) = B$.
Pour toute partie A de E, $f^{-1}(f(A)) = A$.

Propriété. (hors programme)
Soit f une application de E dans F. On suppose que $E \neq \emptyset$.
Alors f est injective si et seulement si il existe $g : F \longrightarrow E$ telle que $g \circ f = Id_E$,
et f est surjective si et seulement si il existe $g : F \longrightarrow E$ telle que $f \circ g = Id_F$.

Démonstration.
$\diamond$ Supposons qu'il existe $g : F \longrightarrow E$ telle que $g \circ f = Id_E$. Alors $g \circ f$ est injective, donc on sait que f est injective.
Réciproquement, supposons que f est injective. $E \neq \emptyset$, donc on peut choisir $e \in E$.
$f|^{f(E)} = h$ est une bijection de E dans $f(E)$, donc on peut poser, pour tout $y \in F$, $g(y) = h^{-1}(y)$ lorsque $y \in f(E)$ et $g(y) = e$ lorsque $y \in F \setminus f(E)$.
Soit $x \in E$. Alors $f(x) \in f(E)$, donc $g \circ f(x) = g(f(x)) = h^{-1}(f(x)) = x$. Ainsi, $g \circ f = Id_E$.
$\diamond$ Supposons qu'il existe $g : F \longrightarrow E$ telle que $f \circ g = Id_F$. Alors $f \circ g$ est surjective, donc on sait que f est surjective.
Réciproquement, supposons que f est surjective. Pour tout $y \in F$, choisissons (on utilise l'axiome du choix) un antécédent de y par f, que l'on notera $g(y)$: son existence est assurée car f est surjective. Par construction, pour tout $y \in F$, $f(g(y)) = y$, donc $f \circ g = Id_F$. $\square$

1.5 Lois internes

Définition. Une loi interne sur E est une application f de $E \times E$ dans E. Dans ce contexte la notation *préfixe* "$f(x, y)$" est remplacée par la notation *infixe* "$x\ f\ y$", où $x, y \in E$.
On dit que (E, f) est un magma (hors programme).

Exemple. L'addition et la multiplication sont des lois internes sur $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$.

Définition. Soit Δ une loi interne sur E. Δ est associative si et seulement si pour tout $x, y, z \in E$, $(x\ \Delta\ y)\ \Delta\ z = x\ \Delta\ (y\ \Delta\ z)$.
Dans ce cas, pour tout $x, y, z \in E$, cette quantité est notée sans parenthèses : $x\ \Delta\ y\ \Delta z$.
On dit alors que (E, Δ) est un magma associatif.

Notation. Soit Δ une loi interne associative sur un ensemble E.
Soit $n \in \mathbb{N}^*$ et $x_1, \ldots, x_n \in E$. Pour tout $p \in \{1, \ldots, n\}$, on définit par récurrence la quantité $x_1\ \Delta\ x_2\ \Delta\ \cdots\ \Delta\ x_p = y_p$ en convenant que
$y_1 = x_1$ et pour tout $p \in \{1, \ldots, n-1\}$, $y_{p+1} = y_p\ \Delta\ x_{p+1}$.

Propriété. Avec ces notations, l'hypothèse d'associativité garantit que la quantité $x_1\ \Delta\ x_2\ \Delta\ \cdots\ \Delta\ x_p$ ne dépend pas de la façon dont elle est parenthésée.

Démonstration.
Soit $n \in \mathbb{N}^*$. Soit E un ensemble muni d'une loi Δ associative. On note $R(n)$ l'assertion suivante : pour tout $x_1, \dots, x_n \in E$, toute expression correctement parenthésée de $x_1 \Delta x_2 \Delta \cdots \Delta x_n$ donne le même résultat.
$R(n)$ est évidente pour $n = 1$ et $n = 2$, elle résulte de l'associativité pour $n = 3$.
Soit $n \geq 3$, supposons $R(k)$ pour tout $k \in \{1, \dots, n\}$.
Soit $x_1, \dots, x_{n+1} \in E$. Soit $p \in \{1, \dots, n\}$. Posons $y = x_1 \Delta \cdots \Delta x_p$ (qui ne dépend pas du choix du parenthésage d'après l'hypothèse de récurrence) et $z = x_{p+1} \Delta \cdots \Delta x_{n+1}$.
Il suffit de montrer que $y \Delta z = x_1 \Delta \cdots \Delta x_{n+1}$, car toute expression correctement parenthésée de $x_1 \Delta x_2 \Delta \cdots \Delta x_{n+1}$ peut s'écrire sous la forme $y \Delta z$ pour un certain p.
Premier cas : Supposons que $p = n$. Alors il n'y a rien à démontrer, car par définition de $x_1 \Delta x_2 \Delta \cdots \Delta x_{n+1}$, on a $y \Delta z = x_1 \Delta x_2 \Delta \cdots \Delta x_{n+1}$.
Second cas : On suppose que $p \leq n - 1$. Par définition de z,
$y \Delta z = y \Delta ((x_{p+1} \Delta \cdots \Delta x_n) \Delta x_{n+1})$, donc par associativité,
$y \Delta z = (y \Delta (x_{p+1} \Delta \cdots \Delta x_n)) \Delta x_{n+1}$. D'après l'hypothèse de récurrence,
$y \Delta z = (x_1 \Delta x_2 \Delta \cdots \Delta x_n) \Delta x_{n+1} = x_1 \Delta x_2 \Delta \cdots \Delta x_{n+1}$, ce qui prouve $R(n+1)$. □

Définition. Soit Δ une loi interne sur E et soit $e \in E$. On dit que e est un élément neutre de (E, Δ) si et seulement si, pour tout $x \in E$, $x \Delta e = e \Delta x = x$.
Si E possède un élément neutre, il est unique. On peut donc parler de *l'*élément neutre.
On dit alors que (E, Δ) est un magma unitaire, ou bien unifère.

Démonstration.
Supposons que e est neutre à droite, c'est-à-dire que pour tout $x \in E$, (1) : $x \Delta e = x$ et que f est neutre à gauche, c'est-à-dire que pour tout $x \in F$, (2) : $f \Delta x = x$.
Alors d'après (2), $e = f \Delta e$, puis d'après (1), $f \Delta e = f$, donc $e = f$. □

Définition. On dit que (E, Δ) est un monoïde si et seulement si E est un ensemble et Δ est une loi interne associative sur E qui possède un élément neutre.
On dit que le monoïde est commutatif, ou abélien, si et seulement si,
pour tout $x, y \in E$, $x \Delta y = y \Delta x$.

Remarque. Un monoïde est donc un magma unitaire et associatif.

Remarque. l'usage est de confondre le monoïde (E, Δ) et l'ensemble sous-jacent E.

Exemple. Si A est un ensemble, alors $(\mathcal{P}(A), \cup)$ est un monoïde commutatif dont l'élément neutre est $\emptyset$. Qu'en est-il de $(\mathcal{P}(A), \cap)$?

Exemple. Si A est un ensemble, dont les éléments sont appelés des lettres, on note A^* l'ensemble des mots écrits avec l'alphabet A. Plus formellement, $A^* = \bigsqcup_{n \in \mathbb{N}} A^n$, en convenant que A^0 désigne le singleton contenant le mot vide.
La concaténation entre mots structure A^* comme un monoïde.

Notation. Soit (E, Δ) un monoïde dont l'élément neutre est noté e.
Soit $n \in \mathbb{N}^*$ et $x_1, \dots, x_n \in E$. Pour tout $p \in \{1, \dots, n\}$, on a défini par récurrence la quantité $x_1 \ \Delta \ x_2 \ \Delta \ \cdots \ \Delta \ x_p = y_p$. On convient de plus que $y_0 = e$, c'est-à-dire que

$$x_1 \ \Delta \ x_2 \ \Delta \ \cdots \ \Delta \ x_p = e, \quad \text{lorsque } p = 0.$$

Définition. Soit $(E, \times)$ un monoïde et $x \in E$.
On dit que x est inversible à droite si et seulement si il existe $y \in E$ tel que $yx = 1_E$.
On dit que x est inversible à gauche si et seulement si il existe $y \in E$ tel que $xy = 1_E$.
Lorsque x est inversible à gauche et à droite, alors il existe un unique $y \in E$ tel que $xy = yx = 1_E$. Dans ce cas, on dit que x est inversible dans E et que y est le symétrique de x. Le symétrique de x est noté x^{-1} (en notation multiplicative).

Propriété. Soit $(E, \times)$ un monoïde et $x, y \in E$.
Si x et y sont inversibles dans E, alors xy est aussi inversible et

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Définition. Un groupe est un monoïde dans lequel tout élément est inversible.

Remarque. On aurait très bien pu continuer à noter Δ la loi de G et e son élément neutre, avec Δ et e substituable par n'importe quel autre symbole, mais l'usage restreint la notation de la loi interne d'un groupe à seulement deux notations : la notation multiplicative, que l'on vient de voir, et la notation additive, réservée aux groupes commutatifs. Ainsi, $(G, +)$ est la notation générique d'un groupe commutatif. Son élément neutre est alors noté 0 ou 0_G et le symétrique de x est alors noté $-x$.

Remarque. On dit qu'un groupe est abélien si et seulement si il est commutatif.

Exemple. $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$ sont des groupes commutatifs.
$(\mathbb{Q}^*, \times)$ est un groupe commutatif mais $(\mathbb{Z}^*, \times)$ n'est pas un groupe.

Définition. On appelle ***anneau*** tout triplet $(A, +, .)$, où A est un ensemble et où "+" et "." sont deux lois internes sur A telles que
- $(A, +)$ est un groupe abélien (l'élément neutre étant noté 0 ou 0_A),
- "." est une loi associative, admettant un élément neutre noté 1 ou 1_A,
- la loi "." est ***distributive*** par rapport à la loi "+", c'est-à-dire que
$\forall (x, y, z) \in A^3 \ \ x.(y + z) = (x.y) + (x.z)$ et $(x + y).z = (x.z) + (y.z)$.

2 Dénombrement

Remarque. Ce chapitre utilise seulement la théorie des ensembles et les propriétés de $\mathbb{N}$.
En effet, les autres notions utilisées sont uniquement bâties sur la théorie des ensembles et des entiers : injections, surjections et bijections, relations d'équivalence, monoïdes etc.

2.1 Cardinal d'un ensemble

Lemme : Soit $n, m \in \mathbb{N}$. S'il existe une injection de $\mathbb{N}_n$ dans $\mathbb{N}_m$, alors $n \leq m$.

Démonstration.
Pour tout $n \in \mathbb{N}$, notons $R(n)$ l'assertion : pour tout $m \in \mathbb{N}$, s'il existe une injection de $\mathbb{N}_n$ dans $\mathbb{N}_m$, alors $n \leq m$.
Si $n = 0$, pour tout $m \in \mathbb{N}$, on a bien $m \geq 0 = n$, donc $R(0)$ est vraie.
Pour $n \geq 0$, supposons $R(n)$. Soit $m \in \mathbb{N}$.
Supposons qu'il existe une injection g de $\mathbb{N}_{n+1}$ dans $\mathbb{N}_m$.
Posons $k = g(n+1)$. $k \in \mathbb{N}_m$, donc $m \geq 1$.

- Si $k < m$, on note $g' = \tau \circ g$, où τ est la bijection de $\mathbb{N}_m$ dans $\mathbb{N}_m$ qui échange k et m.
- Si $k = m$, on pose $g' = g$.

Dans tous les cas, $g'(n+1) = m$.
De plus g' est une injection en tant que composée d'injections.
Notons h l'application de $\mathbb{N}_n$ dans $\mathbb{N}_{m-1}$ définie par restriction de g' :
$\forall a \in \mathbb{N}_n,\ \ h(a) = g'(a)$.
h est bien à valeurs dans $\mathbb{N}_{m-1}$ car pour tout $a \in \mathbb{N}_n$, $h(a) = g'(a) \in \mathbb{N}_m$ et d'après l'injectivité de g', $g'(a) \neq g'(n+1) = m$.
h est clairement injective, par restriction d'une application injective.
Alors, d'après $R(n)$, $n \leq m-1$, donc $n+1 \leq m$, ce qui prouve $R(n+1)$. □

Définition. Soit E un ensemble. S'il existe $n \in \mathbb{N}$ tel que $\mathbb{N}_n$ est en bijection avec E, alors n est unique. On dit que n est le cardinal de E. Il est noté $\mathrm{card}(E)$ ou bien $\#E$, ou encore $|E|$.
En cas d'inexistence d'un tel entier n, on dit que E est infini.

Démonstration.
Supposons qu'il existe $n, m \in \mathbb{N}$, une bijection f de E dans $\mathbb{N}_n$ et une bijection g de E dans $\mathbb{N}_m$. Montrons que $n = m$.
L'application $f \circ g^{-1}$ est une bijection, donc une injection de $\mathbb{N}_m$ dans $\mathbb{N}_n$, donc d'après le lemme $m \leq n$. Mais $[f \circ g^{-1}]^{-1}$ est une injection de $\mathbb{N}_n$ dans $\mathbb{N}_m$, donc $n \leq m$, puis $n = m$. □

Exemple. $\emptyset = \mathbb{N}_0$ est de cardinal nul.
Pour tout $n \in \mathbb{N}$, $\mathbb{N}_n$ est de cardinal n.

Exemple. Pour tout $n, m \in \mathbb{Z}$, notons $[\![n, m]\!] = \{k \in \mathbb{N} / n \leq k \leq m\}$.
Lorsque $m < n$, $[\![n, m]\!] = \emptyset$. Supposons maintenant que $m \geq n$.
Alors l'application $\begin{array}{rccc} f : & [\![n, m]\!] & \longrightarrow & \mathbb{N}_{m-n+1} \\ & k & \longmapsto & k - n + 1 \end{array}$ est une bijection, donc

$$\text{Card}([\![n, m]\!]) = m - n + 1.$$

Remarque. Lorsque A est de cardinal n, si f est une bijection de $\mathbb{N}_n$ dans A, en posant $a_i = f(i)$, on a $A = \{a_1, \ldots, a_n\}$. Ainsi une bijection de $\mathbb{N}_n$ dans A donne une manière de numéroter les éléments de A.
Mais réciproquement, lorsqu'on écrit $B = \{b_1, \ldots, b_n\}$, on n'affirme pas que les b_i sont deux à deux distincts.

Propriété. Soit A un ensemble de cardinal $n \in \mathbb{N}$ et soit B un ensemble quelconque. B est fini de cardinal n si et seulement si il existe une bijection de A sur B.

Lemme : Soit $n \in \mathbb{N}$. Soit K une partie de $\mathbb{N}_n$. Alors K est un ensemble fini et $|K| \leq n$, avec égalité si et seulement si $K = \mathbb{N}_n$.

Démonstration.
Notons $R(n)$ cette propriété.
Supposons que $n = 0$. Soit K une partie de $\mathbb{N}_0 = \emptyset$. Alors $K = \emptyset = \mathbb{N}_0$, donc $|K| = 0$. Ceci prouve $R(0)$.
Pour $n \geq 0$, supposons $R(n)$. Soit K une partie de $\mathbb{N}_{n+1}$.
Premier cas : Supposons que $n + 1 \notin K$. Alors d'après $R(n)$, K est un ensemble fini et $|K| \leq n < n + 1$. De plus $K \neq \mathbb{N}_{n+1}$.
Second cas : Supposons que $n + 1 \in K$. Posons $H = K \setminus \{n + 1\}$. H est une partie de $\mathbb{N}_n$, donc d'après $R(n)$, H est un ensemble fini et $|H| \leq n$. Posons $h = |H|$.
Par définition du cardinal, il existe une bijection f de H dans $\mathbb{N}_h$.
Posons $f(n+1) = h+1$. Alors f est prolongée en une application de K dans $\mathbb{N}_{h+1}$, pour laquelle tout élément de $\mathbb{N}_{h+1}$ possède un unique antécédent. C'est donc une bijection de K dans $\mathbb{N}_{h+1}$, ce qui prouve que K est un ensemble fini avec $|K| = h + 1 \leq n + 1$.
De plus, si $|K| = n + 1$, alors $h = n$, donc d'après $R(n)$, $H = \mathbb{N}_n$, puis $K = \mathbb{N}_{n+1}$.
Réciproquement, si $K = \mathbb{N}_{n+1}$, on a bien sûr $|K| = n + 1$, donc on a prouvé $R(n + 1)$.
□

Propriété. Soit A un ensemble fini de cardinal $n \in \mathbb{N}$. Soit B une partie de A.
Alors B est un ensemble fini et $|B| \leq |A|$, avec égalité si et seulement si $B = A$.

Démonstration.
Il existe une bijection f de A dans $\mathbb{N}_n$.
◇ $f|_B$ réalise une bijection de B dans $f(B)$. $f(B)$ est une partie de $\mathbb{N}_n$ donc d'après le lemme précédent, $f(B)$ est un ensemble fini de $\mathbb{N}_n$ et $|f(B)| \leq n$. On en déduit que B est fini et que $|B| = |f(B)| \leq n = |A|$.
◇ Supposons que $|B| = |A|$. Alors $|f(B)| = n$, donc d'après le lemme, $f(B) = \mathbb{N}_n$, puis $B = f^{-1}(f(B)) = f^{-1}(\mathbb{N}_n) = A$. □

Remarque. Ainsi, pour montrer l'égalité entre deux ensembles finis, on peut se contenter de montrer une inclusion et l'égalité des cardinaux.

Remarque. Lorsque E est un ensemble fini, aucune partie stricte de E n'est donc en bijection avec E. On peut montrer la réciproque (en TD) : si E est un ensemble infini, alors E est en bijection avec l'une de ses parties strictes. On obtient ainsi une propriété caractéristique d'un ensemble infini.
On peut même montrer que E est infini si et seulement si pour tout $x \in E$, E et $E \setminus \{x\}$ sont en bijection : le fait d'ôter un élément d'un ensemble infini n'en modifie pas le cardinal (en convenant que deux ensembles sont de même cardinal si et seulement si ils sont en bijection). Cette propriété des ensembles infinis est au coeur des mathématiques. Elle permet de remplacer l'affirmation un peu vague "si l'on enlève un élément parmi vraiment beaucoup d'éléments, il en reste à peu près toujours autant" par une propriété d'invariance fondamentale : si on enlève un élément d'un ensemble infini, il en reste toujours exactement autant.
L'existence de l'infini n'est pas démontrée en mathématiques, elle est admise dans les axiomes (axiome de l'infini ou axiomes de Peano). C'est une condition préalable pour faire des mathématiques.

Propriété. Soit A une partie de $\mathbb{N}$. A est finie si et seulement si elle est majorée.
En particulier, $\mathbb{N}$ est infini.

Démonstration.
$\diamond$ Supposons que A est majorée. Il existe $n \in \mathbb{N}$ tel que, pour tout $a \in A$, $a \leq n$. Ainsi $A \subset [\![0, n]\!]$, donc A est finie.
$\diamond$ Notons $R(n)$ l'assertion : si A est de cardinal n, alors A est majorée.
Si A est de cardinal 0, A est vide donc est majorée : $R(0)$ est vraie.
Pour $n \geq 0$, supposons $R(n)$. Soit A une partie de $\mathbb{N}$ de cardinal $n+1$. Il existe une bijection f de $\mathbb{N}_{n+1}$ dans A. Posons $a = f(n+1)$. $f|_{\mathbb{N}_n}$ est une bijection de $\mathbb{N}_n$ dans $A \setminus \{a\}$, donc $A \setminus \{a\}$ est de cardinal n. D'après $R(n)$, il existe $m \in \mathbb{N}$ tel que, pour tout $b \in A \setminus \{a\}$, $b \leq m$.
Si $a \leq m$, alors m majore A.
Si $a > m$, alors a majore A. Ceci démontre $R(n+1)$.
$\diamond$ Si $m \in \mathbb{N}$ était un majorant de $\mathbb{N}$, alors $m+1 \leq m$, ce qui est faux.
$\mathbb{N}$ n'est pas majoré, donc il est infini. $\square$

Exemple. Soit $(x_n)_{n\in\mathbb{N}}$ une suite de réels et $l \in \mathbb{R}$. Alors x_n ne tend pas vers l si et seulement si il existe $\varepsilon > 0$ tel que $\{n \in \mathbb{N} / |x_n - l| > \varepsilon\}$ est infini.

2.2 Cardinaux d'ensembles usuels

Propriété. Pour tout $n \in \mathbb{N}^*$, une réunion *disjointe* de n ensembles finis est finie et son cardinal est égal à la somme des cardinaux de ces ensembles.

Démonstration.
Il suffit d'établir la propriété pour $n = 2$, car une récurrence simple permet alors de conclure.
Soit A et B deux ensembles finis disjoints de cardinaux respectifs n et m.
Il existe des bijections f de A sur $\mathbb{N}_n$ et g de B sur $\mathbb{N}_m$.
Pour tout $x \in A \sqcup B$, posons $h(x) = f(x)$ si $x \in A$ et $h(x) = g(x) + n$ si $x \in B$.
h est ainsi une application de $A \sqcup B$ dans $\mathbb{N}_{n+m}$. On vérifie que h est surjective et injective. □

Exemple. En admettant qu'une femme a au plus 400 000 cheveux et qu'il y a au moins un million de parisiennes, montrer qu'au moins 3 parisiennes ont le même nombre de cheveux.
Solution : Notons f l'application qui à une parisienne associe son nombre de cheveux. En posant $N = 400000$, elle permet de partitionner l'ensemble des parisiennes sous la forme $P = \bigsqcup_{i=0}^{N} P_i$ où P_i est l'ensemble des parisiennes possédant exactement i cheveux.
On raisonne alors par l'absurde : si pour tout $i \in \{0, \dots, N\}$, $|P_i| \leq 2$,
alors $|P| = \sum_{i=0}^{N} |P_i| \leq 2(N+1) < 10^6$, ce qui est faux.

Principe des tiroirs : En adaptant le raisonnement précédent, on montre que, lorsque l'on dispose de T tiroirs et de N objets, avec $T, N \in \mathbb{N}$, si chaque tiroir contient au plus c objets, alors $N \leq cT$. Ainsi, lorsque $N > cT$, il existe un tiroir qui contient au moins $c + 1$ objets.

Principe du "ou exclusif" : Pour dénombrer un ensemble, ce principe consiste à découper celui-ci en plusieurs sous-ensembles disjoints qui sont plus faciles à dénombrer. Le cardinal de l'ensemble global est alors la somme des cardinaux des sous-ensembles.

> **Exercice.** Une urne contient 5 billes blanches et 10 billes noires. On tire *avec remise* 3 billes. Quelle est la probabilité que les 2 premières soient d'une même couleur, et que la dernière soit de l'autre couleur ?
> ***Solution :*** Les probabilités feront l'objet d'un cours ultérieur. On admet que la probabilité cherchée est $P = \dfrac{|A|}{|E|}$, où E est l'ensemble de tous les tirages possibles de 3 billes et où A est la partie de E constituée des tirages pour lesquels les 2 premières billes sont d'une même couleur alors que la dernière est de l'autre couleur.
> Numérotons les billes, $b_1, \dots, b_5$ pour les 5 billes blanches et $n_1, \dots, n_{10}$ pour les 10 billes noires. Posons $B = \{b_1, \dots, b_5\} \cup \{n_1, \dots, n_{10}\}$.
> Comme l'ordre des 3 billes importe, un tirage de trois billes sera formellement un triplet d'éléments de B, donc $E = B^3$.
> Pour construire un élément de E, on choisit d'abord le premier élément, soit 15 choix, puis le second, soit encore 15 choix, puis le dernier. Ainsi $|E| = 15^3$. On

donne plus loin une démonstration plus formelle pour dénombrer plus généralement un produit cartésien.
Pour dénombrer A, on applique le principe du "ou exclusif", car $A = A_1 \sqcup A_2$, où A_1 est l'ensemble des tirages pour lesquels les deux premières billes sont blanches et la dernière noire, et où A_2 est l'ensemble des tirages pour lesquels les deux premières billes sont noires et la dernière blanche.
En raisonnant comme pour le dénombrement de E, on obtient $|A_1| = 5.5.10$ et $|A_2| = 10.10.5$. Ainsi, $P = \dfrac{250 + 500}{15^3} = 0,22 \pm 10^{-2}$.

Propriété. Soit E un ensemble fini et A une partie de E. Alors $|E \setminus A| = |E| - |A|$.

Démonstration.
$E = A \sqcup (E \setminus A)$. □

Principe du passage au contraire : Pour dénombrer une partie d'un ensemble, il est parfois plus simple de dénombrer son complémentaire.

Exemple. Quel est le nombre de surjections de $\mathbb{N}_n$ dans $\mathbb{N}_2$?
Lorsque $n < 2$, ce nombre est nul. Supposons que $n \geq 2$.
Appliquons le principe des contraires en dénombrant la partie A de $\mathcal{F}(\mathbb{N}_n, \mathbb{N}_2)$ constituée des fonctions qui ne sont pas surjectives : Si $f \in A$, l'une des deux valeurs de $\mathbb{N}_2$ n'est pas atteinte, donc f est constante. Ainsi $|A| = 2$.
Pour construire une fonction quelconque de $\mathbb{N}_n$ dans $\mathbb{N}_2$, on choisit pour chaque élément de $\mathbb{N}_n$ son image dans $\mathbb{N}_2$, soit 2 choix à chacune de ces n étapes.
Ainsi, $|\mathcal{F}(\mathbb{N}_n, \mathbb{N}_2)| = 2^n$. On donne plus loin une preuve plus formelle pour dénombrer plus généralement $\mathcal{F}(E, F)$.
En conclusion, le nombre de surjections demandé est $2^n - 2$.

Propriété. Soit E un ensemble fini et R une relation d'équivalence sur E.
Alors E/R est aussi de cardinal fini et $|E/R| \leq |E|$.

Démonstration.
On le démontre par récurrence forte sur le cardinal de E ; pour $n \in \mathbb{N}$, on note $R(n)$ l'assertion suivante : pour tout ensemble E de cardinal n, pour toute relation d'équivalence R sur E, E/R est fini et $|E/R| \leq |E|$.
$R(0)$ est vraie. Soit $n \in \mathbb{N}$. On suppose $R(k)$ pour tout $k \in \{0, \dots, n\}$.
Soit E un ensemble de cardinal $n+1$ et R une relation d'équivalence sur E.
Il existe $a \in E$. Notons $cl_R(a)$ sa classe d'équivalence pour R.
Sur $E' = E \setminus cl_R(a)$, on définit la relation binaire R' par : $xR'y \iff xRy$.
R' est une relation d'équivalence sur E'. $|E'| = |E| - |cl_R(a)|$, or $|cl_R(a)| \geq 1$, donc $|E'| \leq n$. On peut donc appliquer l'hypothèse de récurrence. Ainsi E'/R' est fini et $|E'/R'| \leq |E|$. On vérifie que $E/R = E'/R' \sqcup \{cl_R(a)\}$, donc E/R est fini. On a prouvé $R(n+1)$. □

Formule : Si A et B sont deux ensembles finis, alors $A \cup B$ est fini et

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Démonstration.
$A \cup B$ est la réunion disjointe de $A \setminus (A \cap B)$, $B \setminus (A \cap B)$ et $A \cap B$, donc $A \cup B$ est fini et
$$\begin{aligned} |A \cup B| &= |A \setminus (A \cap B)| + |B \setminus (A \cap B)| + |A \cap B| \\ &= (|A| - |A \cap B|) + (|B| - |A \cap B|) + |A \cap B| \\ &= |A| + |B| - |A \cap B|. \end{aligned}$$
□

Remarque. La formule du crible, hors programme, généralise la formule précédente au cas d'une réunion de n ensembles finis $E_1, \dots, E_n$:
$\left|\bigcup_{i=1}^{n} E_i\right| = \sum_{k=1}^{n} (-1)^{k+1} S_k$, où pour tout $k \in \mathbb{N}_n$, $S_k = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} \left|\bigcap_{j=1}^{k} E_{i_j}\right|$.
En particulier, $S_1 = \sum_{i=1}^{n} |E_i|$, $S_n = \left|\bigcap_{i=1}^{n} E_i\right|$, $S_2 = \sum_{1 \leq i < j \leq n} |E_i \cap E_j|$.
Elle se démontre par récurrence sur n.

Propriété. Pour tout $n \in \mathbb{N}^*$, un produit cartésien de n ensembles finis est fini et son cardinal est égal au produit des cardinaux de ces ensembles.

Démonstration.
Il suffit d'établir la propriété pour $n = 2$, puis on conclut par récurrence.
Soit A et B deux ensembles finis de cardinaux respectifs n et m.
Il existe une bijection f de $\mathbb{N}_m$ dans B. Ainsi $A \times B = \bigsqcup_{i=1}^{m} [A \times \{f(i)\}]$.
Soit $i \in \mathbb{N}_m$. Pour tout $a \in A$, notons $g(a) = (a, f(i))$. g est une bijection de A dans $A \times \{f(i)\}$, donc $A \times \{f(i)\}$ est un ensemble fini dont le cardinal vaut $|A|$.
On en déduit que $A \times B$ est fini et que $|A \times B| = \sum_{i=1}^{m} |A| = m|A|$ par définition de la multiplication (ou par récurrence sur m). □

Principe du "et" : Si le dénombrement d'un ensemble se décompose en une succession de p étapes offrant respectivement $n_1, n_2, \dots, n_p$ possibilités, où chacun des nombres n_i ne dépend que de l'étape i, le nombre total d'issues est égal à $n_1 \times n_2 \times \cdots, \times n_p$ parce que chaque choix d'une étape doit être associé à chaque choix de tout autre étape.

Exemple. Un facteur sanguin est constitué d'un groupe sanguin dans $\{A, B, AB, O\}$ et d'un rhésus dans $\{+; -\}$. Pour constituer un facteur sanguin, il faut un groupe sanguin, ce qui laisse 4 choix, et un rhésus, ce qui laisse 2 choix. Il y a donc $4 \times 2 = 8$ facteurs sanguins distincts.

Exercice. Calculer le nombre de diviseurs dans $\mathbb{N}$ d'un entier $n \in \mathbb{N}^*$.

Solution : La décomposition de n en produit de facteurs premiers s'écrit $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$, donc si $m = \prod_{p \in \mathbb{P}} p^{v_p(m)} \in \mathbb{N}^*$, $m \mid n \iff \forall p \in \mathbb{P},\ v_p(m) \leq v_p(n)$.
Ainsi, pour choisir un diviseur de n, pour chaque $p \in \mathbb{P}$, on choisit un entier

entre 0 et $v_p(n)$, soit $v_p(n)+1$ choix, donc le nombre de diviseurs de n est égal à $\prod_{p\in\mathbb{P}}(v_p(n)+1)$.

Formule : Si E et F sont des ensembles finis, alors $\mathcal{F}(E,F)$ est fini et

$$|\mathcal{F}(E,F)| = |F|^{|E|}.$$

Remarque. Cela explique la notation classique $\mathcal{F}(E,F) = F^E$.

Démonstration.
Notons n le cardinal de E. Il existe une bijection f de $\mathbb{N}_n$ dans E. Notons, pour tout $i \in \mathbb{N}_n$, $e_i = f(i)$.
Pour tout $h \in \mathcal{F}(E,F)$, notons $\varphi(h) = (h(e_1), \dots, h(e_n))$. On définit ainsi une application φ de $\mathcal{F}(E,F)$ dans F^n.
On vérifie que φ est bijective, ce qui permet de conclure. □

Propriété. Si E est de cardinal n, alors $\mathcal{P}(E)$ est de cardinal 2^n.

Démonstration.
Notons $x_1, \dots, x_n$ les éléments deux à deux distincts de E.
Pour construire une partie quelconque F de E, on décide de prendre ou de ne pas prendre x_1 dans F (2 choix), puis on décide de prendre ou de ne pas prendre x_2 dans F (2 choix), et on procède ainsi jusqu'à x_n. Il y a donc 2^n façons de construire ainsi des parties de E. Elles sont toutes distinctes et toute partie de E est ainsi obtenue exactement une fois, donc le cardinal de $\mathcal{P}(E)$ vaut 2^n.
On peut rendre cette preuve plus formelle, en traduisant le procédé de construction mis en évidence sous la forme d'une bijection d'un ensemble d'"ingrédients" dont le cardinal est connu vers $\mathcal{P}(E)$. Ici, il est plus simple d'écrire la bijection réciproque. C'est l'application φ qui à une partie A de E associe son indicatrice.
Notons donc, pour tout $A \in \mathcal{P}(E)$, $\varphi(A)$ l'application de E dans $\{0,1\}$ définie par :
si $x \in A$, $\varphi(A)(x) = 1$ et si $x \in E \setminus A$, $\varphi(A)(x) = 0$.
Montrons que φ est une bijection de $\mathcal{P}(E)$ dans $\mathcal{F}(E,\{0,1\})$.
◇ Soit $A, B \in \mathcal{P}(E)$ tels que $\varphi(A) = \varphi(B)$.
Si $x \in A$, $\varphi(A)(x) = 1$, donc $\varphi(B)(x) = 1$, donc $x \in B$. On établit de même la réciproque, donc $A = B$. On a prouvé que φ est injective.
◇ Soit $f \in \mathcal{F}(E,\{0,1\})$. Posons $A = \{x \in E / f(x) = 1\}$. Alors $\varphi(A) = f$, donc φ est surjective.
φ étant une bijection, on en déduit que $|\mathcal{P}(E)| = |\mathcal{F}(E,\{0,1\})| = 2^n$. □

Remarque. Plus généralement, pour dénombrer un ensemble fini F, on peut rechercher un procédé de construction des éléments de F, qui fournit tous les éléments de F une seule fois. Il n'est pas toujours nécessaire de traduire ce procédé de construction sous la forme d'une bijection.

2.3 Sommes et produits finis

Notation. Lorsque $(G,+)$ est un monoïde commutatif, on a déjà défini la notation $\sum_{i=1}^{n} x_i = x_1 + \cdots + x_n$ pour tout $n \in \mathbb{N}$ et $x_1, \ldots, x_n \in G$.
En notation multiplicative, dans un monoïde commutatif $(G,\times)$, ceci devient :

$$x_1 \times \cdots \times x_n = \prod_{i=1}^{n} x_i.$$

On fixe dans tout ce paragraphe un monoïde *commutatif* $(G,+)$.
Toutes les propriétés qui suivent sont bien sûr valables indépendamment de la façon dont la loi interne est notée. Il sera notamment utile de les traduire en notation multiplicative.

Remarque. Dans l'écriture $S = \sum_{i=1}^{n} x_i$, la variable i est muette, car elle peut être remplacée par toute autre variable : $S = \sum_{j=1}^{n} x_j$.
Au contraire, n n'est pas une variable muette (c'est une variable libre) : si $m \neq n$, a priori $S \neq \sum_{i=1}^{m} x_i$.

En particulier, l'écriture $\sum_{n=1}^{n} x_n$ n'a aucun sens car la variable n devrait être à la fois muette et libre.

Exemples à connaître : (on peut les démontrer par récurrence)

- Pour tout $a \in G$ et $n \in \mathbb{N}$, $\sum_{k=1}^{n} a = na$.
- Pour tout $n \in \mathbb{N}$, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.
- Pour tout $n \in \mathbb{N}$, $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.
- Pour tout $n \in \mathbb{N}$, $\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$.

Notation. Pour tout $n \in \mathbb{N}$, on note $\mathcal{S}_n$ l'ensemble des bijections de $\mathbb{N}_n$ dans lui-même.

Commutativité généralisée : Soit $n \in \mathbb{N}$ et $x_1, \ldots, x_n \in G$. Alors

$$\forall \sigma \in \mathcal{S}_n, \quad \sum_{i=1}^{n} x_i = \sum_{j=1}^{n} x_{\sigma(j)}.$$

Démonstration.
Admis pour le moment car la démonstration utilise des propriétés du groupe symétrique de degré n, égal à $(\mathcal{S}_n, \circ)$. □

Remarque. Nous verrons plus tard que cette propriété *n'est plus valable* dans le cadre des sommes infinies de séries semi-convergentes.

Définition. Soit A un ensemble fini et $(x_a)_{a\in A}$ une famille de G indexée par A.
Notons $n = |A|$. Il existe une bijection f de $\mathbb{N}_n$ dans A. On pose $\sum_{a\in A} x_a \overset{\Delta}{=} \sum_{i=1}^{n} x_{f(i)}$.
Cette quantité ne dépend pas de la bijection f.

Démonstration.
Soit g une seconde bijection de $\mathbb{N}_n$ dans A. Alors $\sum_{i=1}^{n} x_{g(i)} = \sum_{i=1}^{n} x_{f([f^{-1}\circ g](i))} = \sum_{i=1}^{n} y_{\sigma(i)}$,
en posant $\sigma = f^{-1} \circ g$ et $y_j = x_{f(j)}$ pour tout $j \in \mathbb{N}_n$.
$\sigma \in \mathcal{S}_n$, donc d'après la propriété précédente, $\sum_{i=1}^{n} y_{\sigma(i)} = \sum_{i=1}^{n} y_i = \sum_{i=1}^{n} x_{f(i)}$. □

Exemple. Si $n, m \in \mathbb{Z}$, $\sum_{k=m}^{n} x_k = \sum_{a\in[\![m,n]\!]} x_a$, où $[\![m, n]\!] = \{k \in \mathbb{Z}/m \leq k \leq n\}$.
En particulier, lorsque $n < m$, $\sum_{k=m}^{n} x_k = \sum_{k\in\emptyset} x_k = 0$.

Propriété d'additivité : Soit A un ensemble fini, $(x_a)_{a\in A}$ et $(y_a)_{a\in A}$ deux familles d'éléments de G indexées par A. Alors

$$\sum_{a\in A}(x_a + y_a) = \Big(\sum_{a\in A} x_a\Big) + \Big(\sum_{a\in A} y_a\Big).$$

Démonstration.
En utilisant une bijection de $\mathbb{N}_n$ dans A, on se ramène au cas où $A = \{1, \ldots, n\}$, que l'on démontre par récurrence sur n. □

Exemple.
$$\sum_{k=1}^{n} k(k+1) = \sum_{k=1}^{n} k^2 + \sum_{k=1}^{n} k = \frac{n(n+1)(2n+1)}{6} + \frac{n(n+1)}{2} = \frac{n(n+1)(n+2)}{3}.$$

Distributivité généralisée : Soit A un ensemble fini, $\lambda \in \mathbb{C}$ et $(x_a)_{a\in A}$une famille de *complexes* indexée par A. Alors

$$\sum_{a\in A}(\lambda x_a) = \lambda \sum_{a\in A} x_a.$$

Démonstration.
En utilisant une bijection de $\mathbb{N}_n$ dans A, on se ramène au cas où $A = \{1, \dots, n\}$, que l'on démontre par récurrence sur n. □

Remarque. Cette formule est valable dans un contexte plus général, où le produit utilisé est distributif par rapport à l'addition utilisée. C'est notamment le cas lorsque $(G, +, \times)$ est un anneau, avec $\lambda \in G$ et pour tout $a \in A$, $x_a \in G$.

Changement de variable dans une somme finie : Soit B un ensemble fini, $(x_b)_{b\in B}$ une famille d'éléments de G. Soit φ une bijection d'un ensemble A dans B. Alors

$$\sum_{b\in B} x_b = \sum_{a\in A} x_{\varphi(a)}.$$

Lorsqu'on transforme l'une des sommes en l'autre somme, on dit qu'on a posé $b = \varphi(a)$. Il importe en pratique de s'assurer que φ est bien bijective.

Démonstration.
Posons $n = |B| = |A|$. Il existe une bijection f de $\mathbb{N}_n$ dans A. Alors $\varphi \circ f$ est une bijection de $\mathbb{N}_n$ dans B, donc $\sum_{b\in B} x_b = \sum_{i=1}^{n} x_{[\varphi\circ f](i)} = \sum_{i=1}^{n} x_{\varphi(f(i))} = \sum_{a\in A} x_{\varphi(a)}$. □

Exemple. Dans la quantité $S = \sum_{k=0}^{n} k$, on pose $k = n - h$. L'application φ correspondante est la bijection $\begin{array}{rccc} \varphi : & [\![0,n]\!] & \longrightarrow & [\![0,n]\!] \\ & h & \longmapsto & n-h \end{array}$. Ainsi, $S = \sum_{h=0}^{n}(n-h) = n(n+1) - S$, ce qui permet de retrouver que $\sum_{k=0}^{n} k = \dfrac{n(n+1)}{2}$.

Décalage d'indice : Pour tout $m, n, p \in \mathbb{Z}$, $\sum_{k=m}^{n} x_k = \sum_{h=m-p}^{n-p} x_{h+p}$.

Démonstration.
On pose $k = h + p = \varphi(h)$ où φ est bien une bijection de $[\![m-p, n-p]\!]$ dans $[\![m, n]\!]$. □

Remarque. En pratique, le plus souvent, $p = \pm 1$.

Exemple. (à connaître) : calcul d'une somme géométrique .

Soit $q \in \mathbb{C}$ avec $q \neq 1$. Soit $m, n \in \mathbb{N}$ avec $m \leq n$. On souhaite calculer $S = \sum_{k=m}^{n} q^k$.

Par distributivité,

$qS = \sum_{k=m}^{n} q^{k+1} = \sum_{k=m+1}^{n+1} q^k = S - q^m + q^{n+1}$, donc $\boxed{\sum_{k=m}^{n} q^k = \dfrac{q^m - q^{n+1}}{1-q}}$.

Théorème. Soit $(G..)$ un groupe commutatif fini. Alors, pour tout $a \in G$, $a^{\#G} = 1_G$.

Démonstration.
Soit $a \in G$. Notons φ l'application de G dans G définie par $\varphi(g) = ag$. Alors φ est une bijection dont la bijection réciproque est $g \longmapsto a^{-1}g$, donc si l'on pose $S = \prod_{g\in G} g$, on a $S = \prod_{g\in G} \varphi(g) = \prod_{g\in G} ag = a^{\#G}S$, car G est commutatif. En multipliant cette égalité par S^{-1}, on en déduit que $a^{\#G} = 1_G$. □

Lemme : Soit C un ensemble fini. On suppose que $C = A \sqcup B$. Alors, pour toute famille $(x_c)_{c\in C}$ d'éléments de C, $\sum_{c\in C} x_c = \Big(\sum_{a\in A} x_a\Big) + \Big(\sum_{b\in B} x_b\Big)$.

Démonstration.
Posons $n = |A|$ et $m = |B|$.
Il existe des bijections $f : \mathbb{N}_n \longrightarrow A$ et $g : [\![n+1, n+m]\!] \longrightarrow B$,
donc $\sum_{a\in A} x_a = \sum_{i=1}^{n} x_{f(i)}$ et, en posant $b = g(j)$, $\sum_{b\in B} x_b = \sum_{j=n+1}^{n+m} x_{g(j)}$.
En posant $h(k) = f(k)$ lorsque $k \in \mathbb{N}_n$ et $h(k) = g(k)$ lorsque $k \in [\![n+1, n+m]\!]$, on définit une bijection de $\mathbb{N}_{n+m}$ dans $A \sqcup B = C$. Ainsi,
$\Big(\sum_{a\in A} x_a\Big) + \Big(\sum_{b\in B} x_b\Big) = \Big(\sum_{i=1}^{n} x_{h(i)}\Big) + \Big(\sum_{j=n+1}^{n+m} x_{h(j)}\Big)$. On conclut par associativité. □

Sommation par paquets : Soit A un ensemble fini et $(x_a)_{a\in A}$ une famille d'éléments de G. Soit $n \in \mathbb{N}$. On suppose qu'il existe des parties $A_1, \dots, A_n$ de A telles que $A = \bigsqcup_{i=1}^{n} A_i$. Alors

$$\sum_{a\in A} x_a = \sum_{i=1}^{n} \sum_{a\in A_i} x_a.$$

Démonstration.
A partir du lemme, par récurrence. □

Sommation par paquets, seconde formulation : Soit A un ensemble fini et $(x_a)_{a\in A}$ une famille d'éléments de G. On suppose qu'il existe un ensemble fini B et une famille $(A_b)_{b\in B}$ de parties de A telles que $A = \bigsqcup_{b\in B} A_b$. Alors

$$\sum_{a\in A} x_a = \sum_{b\in B} \sum_{a\in A_b} x_a.$$

Démonstration.
On se ramène à la première formulation en considérant une bijection $f : \mathbb{N}_n \longrightarrow B$ et en posant $A'_i = A_{f(i)}$. □

Sommation par paquets, troisième formulation : Soit A un ensemble fini et $(x_a)_{a\in A}$ une famille d'éléments de G. Soit R une relation d'équivalence sur A. Alors

$$\sum_{a\in A} x_a = \sum_{c\in A/R}\sum_{a\in c} x_a.$$

Démonstration.
On sait que dans ces conditions, A/R est fini et que $A = \bigsqcup_{c\in A/R} c$. □

Remarque. En particulier, si l'on prend $x_a = 1$ pour tout $a \in A$, on en déduit que $|A| = \sum_{a\in A} 1 = \sum_{c\in A/R} |c|$.

2.4 Applications et cardinaux

Notation. Considérons une application f de E dans F, où E est de cardinal fini.
On a vu que l'application $\begin{array}{rccc}\overline{f}: & E/R & \longrightarrow & f(E)\\ & \overline{x} & \longmapsto & f(x)\end{array}$ est une bijection, où $\overline{x}$ est la classe d'équivalence de x pour la relation d'équivalence R définie par : $xRy \iff f(x) = f(y)$.
On sait de plus que E/R est fini, donc $f(E)$ est fini et $|E/R| = |f(E)|$.
Par ailleurs, $|E| = \sum_{c\in E/R} |c|$.
Pour tout $c \in E/R$, $|c| \geq 1$, donc $|E| \geq \sum_{c\in E/R} 1 = |E/R|$.
Ainsi, dans tous les cas, $|E| \geq |f(E)|$.
De plus, $|E| = |f(E)|$ si et seulement si $0 = |E| - |f(E)| = \sum_{c\in E/R} (|c| - 1)$, donc si et seulement si pour tout $c \in E/R$, $|c| = 1$. Ainsi $|E| = |f(E)|$ si et seulement si les classes d'équivalence de R sont toutes des singletons, c'est-à-dire si et seulement si R est la relation d'égalité, ou encore si et seulement si f est injective. On peut énoncer :

Propriété. Soit E un ensemble fini et f une application de E dans un ensemble quelconque F. Alors $f(E)$ est fini. De plus,
$|f(E)| \leq |E|$, avec égalité si et seulement si f est injective, et
$|f(E)| \leq |F|$, avec égalité si et seulement si f est surjective.

Remarque. Lorsque F est de cardinal infini, on a bien sûr $|f(E)| \leq +\infty = |F|$.

Propriété. Soit E et F deux ensembles finis *de même cardinal*. Soit f une application de E dans F. Alors f injective $\iff$ f surjective $\iff$ f bijective .

Démonstration.
f injective $\iff |f(E)| = |E| \iff |f(E)| = |F| \iff f$ surjective. □

Remarque. Ainsi, lorsque E est fini, une application de E dans E injective (resp : surjective) est toujours surjective (resp : injective). C'est faux lorsque E est infini. Par

exemple l'application $\begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{N} \\ n & \longmapsto & n+1 \end{array}$ est injective mais 0 n'a aucun antécédent, donc elle n'est pas surjective.
De plus, l'application $f : \mathbb{N} \longrightarrow \mathbb{N}$ définie par $f(2n) = n$ et $f(2n+1) = n$ pour tout $n \in \mathbb{N}$, est surjective sans être injective.

Propriété. Soit A et B deux ensembles.
S'il existe une injection de A dans B et si B est fini, alors A est fini et $|A| \leq |B|$.
S'il existe une surjection de A dans B et si A est fini, alors B est fini et $|A| \geq |B|$.

Démonstration.
◇ Supposons qu'il existe une injection f de A dans B et que B est fini.
f est alors une bijection de A dans $f(A)$ qui est une partie de B. On en déduit que $f(A)$ est finie avec $|f(A)| \leq |B|$, puis que A est fini avec $|A| \leq |B|$.
◇ Sous ces hypothèses, on a vu que $|A| \geq |f(A)| = |B|$. □

Principe des tiroirs : Si l'on doit ranger p objets dans n tiroirs et que $p > n$, alors il existe au moins 2 objets qui seront dans le même tiroir.

Démonstration.
L'application qui à un objet associe le tiroir où il sera rangé n'est pas injective. □

Principe des bergers : Soit E et F des ensembles finis et $f : E \longrightarrow F$ une application. On suppose qu'il existe $k \in \mathbb{N}^*$ tel que, pour tout $y \in F$, $|f^{-1}(\{y\})| = k$. Cela signifie que tout élément de F possède exactement k antécédents par f.
Alors $|E| = k|F|$.

Démonstration.
Nous sommes dans la situation du début de ce paragraphe. Pour tout $x \in E$, la classe d'équivalence de x est $\overline{x} = \{y \in E / f(x) = f(y)\} = f^{-1}(\{f(x)\})$, donc par hypothèse, toutes les classes d'équivalence sont de cardinal k.
Alors $|E| = \sum_{c \in E/R} |c| = |k| \sum_{c \in E/R} 1 = k|E/R| = k|f(E)|$. Enfin, $f(E) = F$, car tout élément de F possède au moins un antécédent. □

2.5 Ensembles dénombrables

Définition.
Un ensemble est dénombrable si et seulement s'il est en bijection avec $\mathbb{N}$.

Exemples. L'ensemble des nombres pairs est dénombrable.

Propriété. Toute partie infinie de $\mathbb{N}$ est dénombrable.

Démonstration.
Soit P une partie infinie de $\mathbb{N}$. On va montrer qu'il existe une unique bijection strictement croissante de $\mathbb{N}$ sur P.
• *U*nicité. Supposons qu'il existe une bijection $\varphi : \mathbb{N} \longrightarrow P$ strictement croissante.
◇ Pour tout $p \in P$, il existe $k \in \mathbb{N}$ tel que $p = \varphi(k)$. Or $\varphi(k) \geq \varphi(0)$, donc pour tout $p \in P$, $p \geq \varphi(0)$, ce qui prouve que (1) : $\varphi(0) = \min(P)$.

◇ Soit $n \in \mathbb{N}^*$. Si $p \in P \setminus \{\varphi(0), \dots, \varphi(n-1)\}$, il existe $k \in \mathbb{N}$ tel que $p = \varphi(k)$.
$k \geq n$, donc $\varphi(k) \geq \varphi(n)$, donc pour tout $p \in P \setminus \{\varphi(0), \dots, \varphi(n-1)\}$, $p \geq \varphi(n)$. De plus $\varphi(n) \in P \setminus \{\varphi(0), \dots, \varphi(n-1)\}$,
donc (2) : $\forall n \in \mathbb{N}^*$ $\boxed{\varphi(n) = \min(P \setminus \{\varphi(0), \dots, \varphi(n-1)\})}$.
Les relations (1) et (2) définissent par récurrence φ de manière unique.

• *E*xistence. Notons φ l'application de $\mathbb{N}$ dans P définie par les relations (1) et (2).
φ est correctement définie, car pour tout $n \in \mathbb{N}^*$, $P \setminus \{\varphi(0), \dots, \varphi(n-1)\}$ est non vide (P est supposé infini), donc il possède un minimum dans $\mathbb{N}$.
Montrons que φ est une bijection strictement croissante.
◇ Soient $p \in P$ et $n \in \mathbb{N}$. Supposons que $p \notin \{\varphi(0), \dots, \varphi(n)\}$.
Si $n = 0$, $p \neq \varphi(0) = min(P)$, donc $p > \varphi(0)$.
Si $n > 0$, $p \in P \setminus \{\varphi(0), \dots, \varphi(n-1)\}$, donc $p \geq min(P \setminus \{\varphi(0), \dots, \varphi(n-1)\}) = \varphi(n)$.
Or $p \neq \varphi(n)$, donc $p > \varphi(n)$.
Ainsi, pour tout $p \in P$ et $n \in \mathbb{N}$, (3) : $p \notin \{\varphi(0), \dots, \varphi(n)\} \Longrightarrow p > \varphi(n)$.
◇ Soit $n \in \mathbb{N}$. D'après (2), $\varphi(n+1) \notin \{\varphi(0), \dots, \varphi(n)\}$,
donc d'après (3), $\varphi(n+1) > \varphi(n)$.
Ainsi φ est strictement croissante. En particulier, elle est injective.
◇ De plus, si $\varphi(n) \geq n$, $\varphi(n+1) > \varphi(n) \geq n$, donc $\varphi(n+1) \geq n+1$. Ainsi, on montre par récurrence que, pour tout $n \in \mathbb{N}$, $\varphi(n) \geq n$.
Soit $p \in P$. $p \leq \varphi(p)$, donc d'après la contraposée de (3) avec $n = p$, $p \in \{\varphi(0), \dots, \varphi(p)\}$.
Ainsi il existe $k \in \mathbb{N}$ tel que $p = \varphi(k)$, ce qui prouve la surjectivité. □

Exemple. L'ensemble $\mathbb{P}$ des nombres premiers est dénombrable et en notant p_n le $n$ième nombre premier, on a $\mathbb{P} = \{p_n / n \in \mathbb{N}^*\}$.

Propriété. On dit qu'un ensemble est au plus dénombrable si et seulement si il est fini ou dénombrable.
Un ensemble est au plus dénombrable si et seulement s'il est en bijection avec une partie de $\mathbb{N}$.

Démonstration.
Supposons que I est un ensemble et qu'il existe une partie P de $\mathbb{N}$ et une bijection $\varphi : P \longrightarrow I$.
Si P est finie, alors I est fini.
Sinon, d'après la propriété précédente, il existe une bijection de $\mathbb{N}$ dans P, donc par composition, il existe une bijection de $\mathbb{N}$ sur I, ce qui prouve que I est dénombrable.
La réciproque est claire. □

Lemme technique :
Un ensemble I est fini ou dénombrable si et seulement s'il existe une suite croissante $(J_n)_{n\in\mathbb{N}}$ de parties finies de I dont la réunion est égale à I.
Dans ce cas, on dira que $(J_n)_{n\in\mathbb{N}}$ est une suite adaptée à I.

Remarque. Dans ce cas, pour tout $n \in \mathbb{N}$, $J_n = \bigcup_{k=0}^{n} J_k$ et $I = \bigcup_{k=0}^{\infty} J_k$, donc, en un certain sens, que l'on ne tentera pas de formaliser, I est la limite des J_n.

Démonstration.
• Supposons que I est fini ou dénombrable.
◇ Si I est fini, on pose, pour tout $n \in \mathbb{N}$, $J_n = I$. La suite (J_n) convient.
◇ Supposons que I est infini. Il existe une bijection f de $\mathbb{N}$ dans I.
Posons $J_n = f([0,n])$. $\bigcup_{n\in\mathbb{N}} J_n = f\Big(\bigcup_{n\in\mathbb{N}} [0,n]\Big) = f(\mathbb{N}) = I$, donc la suite (J_n) convient.
• Supposons qu'il existe une suite croissante $(J_n)_{n\in\mathbb{N}}$ de parties finies de I dont la réunion est égale à I.
◇ Posons $K_0 = J_0$ et, pour tout $n \in \mathbb{N}^*$, $K_n = J_n \setminus J_{n-1}$.
On vérifie que $I = \bigcup_{n\in\mathbb{N}} J_n = \bigcup_{n\in\mathbb{N}} K_n$ par double inclusion : Pour tout $n \in \mathbb{N}$, $K_n \subset J_n$, donc $\bigcup_{n\in\mathbb{N}} K_n \subset \bigcup_{n\in\mathbb{N}} J_n$ et réciproquement, si $x \in \bigcup_{n\in\mathbb{N}} J_n$, il existe $p = \min\{n \in \mathbb{N} \ / \ x \in J_n\}$, donc $x \in J_p \setminus J_{p-1} = K_p$ (en convenant que $J_{-1} = \emptyset$).
Si $n > p$, $K_n \cap K_p \subset (J_n \setminus J_{n-1}) \cap J_{n-1} = \emptyset$. Ainsi, les parties K_n sont deux à deux disjointes. Ainsi, $I = \bigsqcup_{n\in\mathbb{N}} K_n$
◇ Soit $n \in \mathbb{N}$. Notons d_n le cardinal de K_n (notamment, $d_n = 0$ lorsque $K_n = \emptyset$).
Il existe une bijection g_n de K_n dans l'intervalle d'entiers $[\sum_{k=0}^{n-1} d_k, \sum_{k=0}^{n} d_k \ - 1]$.
On note g l'application de I dans $\mathbb{N}$ dont les restrictions aux K_n coïncident avec g_n.
g est injective, car si $i, j \in I$ avec $i \neq j$, on montre facilement que $g(i) \neq g(j)$, donc c'est une bijection de I dans une partie de $\mathbb{N}$.
Ainsi, I est fini ou dénombrable. □

Remarque. S'il existe une suite $(J_n)_{n\in\mathbb{N}}$ de parties finies de I dont la réunion est égale à I, on a encore que I est fini ou dénombrable, car en posant pour tout $n \in \mathbb{N}$, $K_n = \bigcup_{k=0}^{n} J_k$, la suite (K_n) est adaptée à I.

Remarque. Il faut savoir démontrer la partie "$\Longrightarrow$" de ce lemme technique, ce qui est facile. Par contre la partie "$\Longleftarrow$" ne sera pas utile pour les exercices, car elle se déduit simplement des propriétés qui suivent.

Corollaire. $\mathbb{Z}$ est dénombrable.

Démonstration.
$\mathbb{Z} = \bigcup_{n\in\mathbb{N}} ([-n,n] \cap \mathbb{Z})$. □

Corollaire. $\mathbb{N} \times \mathbb{N}$ est dénombrable.

Démonstration.
$\mathbb{N} \times \mathbb{N} = \bigcup_{n\in\mathbb{N}} ([0,n]^2 \cap \mathbb{N}^2)$. □

Corollaire. $\mathbb{Q}$ est dénombrable.

Démonstration.
$\mathbb{Q} = \bigcup_{n\in\mathbb{N}} \{\frac{p}{q}/(p,q) \in ([-n,n]\cap\mathbb{Z}) \times ([1,n]\cap\mathbb{N})\}$. □

Exercice. Montrer que $\mathbb{Q}[X]$ est dénombrable.
Solution. $\mathbb{Q}[X]$ est l'ensemble des polynômes à coefficients rationnels, c'est-à-dire $\mathbb{Q}^{(\mathbb{N})}$, en convenant de noter toute suite $(a_n)_{n\in\mathbb{N}}$ presque nulle de rationnels sous la forme $\sum_{n\in\mathbb{N}} a_n X^n$.
Pour tout $n \in \mathbb{N}^*$, notons
$J_n = \{\sum_{k=0}^{n} \frac{p_k}{q_k} X^k / \forall k \in \{0,\dots,n\}\ \ p_k \in \mathbb{Z}\cap[-n,n] \text{ et } q_k \in \mathbb{N}\cap[1,n]\}$.
On vérifie que J_n est adaptée à $\mathbb{Q}[X]$.

Propriété. Une réunion au plus dénombrable d'ensembles au plus dénombrables est au plus dénombrable.

Démonstration.
On suppose que $A = \bigcup_{i\in I} A_i$, où I est fini ou dénombrable et où, pour tout $i \in I$, A_i est fini ou dénombrable.
Il existe $\varphi : \mathbb{N} \longrightarrow I$ surjective (même si I est fini).
Ainsi, $A = \bigcup_{n\in\mathbb{N}} B_n$, où $B_n = A_{\varphi(n)}$.
Pour tout $n \in \mathbb{N}$, notons $(J_{n,p})_{p\in\mathbb{N}}$ une suite adaptée à B_n. Ainsi,
$A = \bigcup_{n\in\mathbb{N}} \bigcup_{p\in\mathbb{N}} J_{n,p} = \bigcup_{(n,p)\in\mathbb{N}^2} J_{n,p}$.
$\mathbb{N}^2$ est dénombrable, donc il existe une bijection $\Psi : \mathbb{N} \longrightarrow \mathbb{N}^2$.
Ainsi $A = \bigcup_{n\in\mathbb{N}} J_{\Psi(n)}$ et d'après une remarque précédente, A est fini ou dénombrable. □

Propriété. Un produit cartésien fini d'ensembles dénombrables est dénombrable.

Démonstration.
Soit $A_1,\dots,A_p$ p ensembles dénombrables où $p \in \mathbb{N}^*$. Posons $A = A_1 \times \cdots \times A_p$ et montrons que A est dénombrable.
Pour tout $k \in \{1,\dots,p\}$, il existe d'après le lemme technique une suite $(J_{n,k})_{n\in\mathbb{N}}$ adaptée à A_k.
Pour tout $n \in \mathbb{N}$, posons $L_n = J_{n,1} \times \cdots \times J_{n,p}$.
L_n est un ensemble fini en tant que produit cartésien fini d'ensembles finis
et $A = \bigcup_{n\in\mathbb{N}} L_n$:
En effet, si $a = (a_1,\dots,a_p) \in A$, pour tout $k \in \{1,\dots,p\}$, il existe n_k tel que $a_k \in J_{n_k,k}$.
Posons alors $n = \sup_{1\le k\le p} n_k$. Pour tout $k \in \{1,\dots,p\}$, sachant que la suite $(J_{m,k})_{m\in\mathbb{N}}$ est croissante, $a_k \in J_{n_k,k} \subset J_{n,k}$, donc $a \in L_n$.
Ainsi $A \subset \bigcup_{n\in\mathbb{N}} L_n$ et l'inclusion réciproque est claire.

Alors, d'après le lemme technique, A est fini ou dénombrable.
De plus A est infini, car l'application f de A_1 dans A définie par : pour tout $a_1 \in A_1$, $f(a_1) = (a_1, e_2, \dots, e_p)$ où $e_2, \dots, e_p$ sont des éléments fixés dans $A_2, \dots, A_p$, est une injection. □

Remarque. Notons p_n le $n^{\text{ème}}$ nombre premier.
Notons également $\mathbb{N}^{(\mathbb{N})}$ l'ensemble des suites presque nulles d'entier, c'est-à-dire l'ensemble des suites $(n_i)_{i\in\mathbb{N}}$ d'entiers telle que : $\exists N \in \mathbb{N},\ \forall i \geq N\ n_i = 0$.
D'après le théorème d'existence et d'unicité de la décomposition d'un entier comme produit de nombres premiers, l'application $\begin{array}{ccc} \mathbb{N}^{(\mathbb{N})} & \longrightarrow & \mathbb{N} \\ (\alpha_i)_{i\in\mathbb{N}} & \longmapsto & \prod_{i\in\mathbb{N}} p_i^{\alpha_i} \end{array}$ est une injection.
Ceci prouve directement que $\mathbb{N}^{(\mathbb{N})}$ est dénombrable.

Propriété. $\mathbb{R}$ n'est pas dénombrable.

Démonstration.
Supposons que $\mathbb{R}$ est dénombrable. Alors il existe une bijection φ de $\mathbb{N}$ dans $\mathbb{R}$. Pour tout $n \in \mathbb{N}$, posons $\varphi(n) = b_{0,n} + \sum_{k=1}^{+\infty} b_{k,n} 10^{-k}$, où $b_{0,n}$ est la partie entière de $\varphi(n)$ et où la suite $(b_{k,n})_{k\in\mathbb{N}^*}$ est le développement décimal (dans $\mathcal{V}$) de $\varphi(n)$.
Pour tout $n \in \mathbb{N}$, posons $c_n = \begin{cases} 0 \text{ si } b_{n,n} \neq 0 \\ 1 \text{ si } b_{n,n} = 0 \end{cases}$.
Notons $x = c_0 + \sum_{k=1}^{+\infty} c_k 10^{-k}$. x est un réel, donc il existe $n \in \mathbb{N}$ tel que $x = \varphi(n)$. Alors, d'après l'unicité de la partie entière et du développement décimal d'un réel, $c_n = b_{n,n}$, ce qui est faux. □

Remarque. Cette technique de démonstration s'appelle un "argument diagonal". Il est repris dans la démonstration suivante.

Propriété. Hors programme : $\mathcal{P}(\mathbb{N})$ n'est pas dénombrable.

Démonstration.
Sinon, il existe une bijection φ de $\mathbb{N}$ dans $\mathcal{P}(\mathbb{N})$.
Notons $A = \{n \in \mathbb{N} / n \notin \varphi(n)\}$. Il existe $a \in \mathbb{N}$ tel que $A = \varphi(a)$.
Dans ces conditions, $a \in \varphi(a) \iff a \in A \iff a \notin \varphi(a)$, ce qui est impossible. □

Remarque. En adaptant cette démonstration, on voit que plus généralement, aucun ensemble I n'est en bijection avec $\mathcal{P}(I)$.

2.6 Listes et combinaisons

Vocabulaire : Soit E un ensemble et $p \in \mathbb{N}$.
- Une p-liste (aussi appelée un p-uplet) d'éléments de E est un élément de E^p.
- Un p-arrangement d'éléments de E est une p-liste dont les éléments sont deux à deux distincts.

— Une p-combinaison de E est une partie de E de cardinal p.

Lorsque E est de cardinal fini, l'objet de ce chapitre est de dénombrer les p-listes, p-arrangements et p-combinaisons d'éléments de E.
Pour tout ce chapitre, on supposera que E est un ensemble de cardinal fini égal à n.

Propriété. Le nombre de p-listes d'éléments de E est égal à n^p (c'est $|E|^p$).

Choix (ou tirages) successifs avec répétitions éventuelles :
On utilise les p-listes dans les problèmes de choix successifs de p éléments d'un ensemble, avec d'éventuelles répétitions, ou bien de tirages successifs d'éléments d'un ensemble avec remise. Cela permet ainsi de dénombrer le nombre d'issues possibles lorsqu'on effectue p fois indépendamment une même expérience.

Exemple. Le nombre de mots de 4 lettres, ayant un sens ou non, écrits dans notre alphabet de 26 lettres est égal à 26^4 : on peut considérer qu'un tel mot est obtenu par tirages successifs avec remise de 4 lettres parmi les 26 lettres de l'alphabet.
Le nombre d'octets, c'est-à-dire de mots de 8 lettres, écrits dans l'alphabet $\{0,1\}$, est égal à $2^8 = 256$.

Propriété. Soit $p \in \mathbb{N}$. Si $a = (e_1, \dots, e_p)$ est un p-arrangement d'éléments de E, l'application $\begin{array}{rccc} f_a : & \mathbb{N}_p & \longrightarrow & E \\ & i & \longmapsto & e_i \end{array}$ est une injection.
De plus, l'application $a \longmapsto f_a$ est une bijection de l'ensemble des p-arrangements d'éléments de E vers l'ensemble des injections de $\mathbb{N}_p$ dans E.

Démonstration.
Notons $\mathcal{A}_p$ l'ensemble des p-arrangements d'éléments de E et $\mathcal{I}_p$ l'ensemble des injections de $\mathbb{N}_p$ dans E. Notons $\begin{array}{rccc} \varphi : & \mathcal{A}_p & \longrightarrow & \mathcal{I}_p \\ & a & \longmapsto & f_a \end{array}$ et $\begin{array}{rccc} \Psi : & \mathcal{I}_p & \longrightarrow & \mathcal{A}_p \\ & f & \longmapsto & (f(1), \dots, f(p)) \end{array}$.
On vérifie que Ψ est bien à valeurs dans $\mathcal{A}_p$, puis que $\varphi \circ \Psi = Id_{\mathcal{I}_p}$ et $\Psi \circ \varphi = Id_{\mathcal{A}_p}$. □

Remarque. Supposons que $p > n$. Alors il n'existe aucun p-arrangement dans E, ni aucune p-combinaison.
En effet, pour les p-combinaisons, on a vu que toute partie de E est de cardinal inférieur à n, et pour les p-arrangements, d'après la propriété précédente, le nombre de p-arrangements coïncide avec le nombre d'injections de $\mathbb{N}_p$ dans E, que l'on sait être nul lorsque $|\mathbb{N}_p| > |E|$.
Pour toute la suite de ce paragraphe, on suppose que p est un entier compris entre 0 et n.

Notation. Pour tout $n \in \mathbb{N}$, on appelle factorielle (de) n le produit des entiers consécutifs de 1 à n. Elle est notée $n!$. Ainsi,

$$n! = 1 \times 2 \times \cdots (n-1) \times n$$

Conformément à une convention étudiée page 13, on convient que $0! = 1$: c'est un produit vide.

Théorème. Le nombre de p-arrangements d'éléments d'un ensemble de cardinal n est

$$A_{n,p} = n(n-1)\cdots(n-p+1) = \frac{n!}{(n-p)!}.$$

C'est aussi le nombre d'injections d'un ensemble à p éléments vers un ensemble à n éléments.

Démonstration.
$\diamond$ Soit B un ensemble de cardinal p. Il existe une bijection f de $\mathbb{N}_p$ dans B.
Notons $\mathcal{I}_B$ l'ensemble des injections de B dans E.
Alors l'application $\begin{array}{rccc}\varphi : & \mathcal{I}_B & \longrightarrow & \mathcal{I}_p \\ & g & \longmapsto & g\circ f\end{array}$ est une bijection, dont la bijection réciproque est ...
Pour prouver le théorème, il suffit donc de montrer que $|\mathcal{I}_p| = A_{n,p}$. Notons $R(p)$ cette propriété et raisonnons par récurrence finie.
$\diamond$ Lorsque $p = 0$, $\mathbb{N}_p = \emptyset$ et on sait qu'il existe une unique application (vide) de $\mathbb{N}_p$ dans E. C'est une injection, d'où $R(0)$.
Lorsque $0 \leq p < n$, on suppose $R(p)$.
Si g est une injection de $\mathbb{N}_{p+1}$ dans E, sa restriction $g|_{\mathbb{N}_p}$ est une injection de $\mathbb{N}_p$ dans E, donc on peut définir l'application $\begin{array}{rccc}\Psi : & \mathcal{I}_{p+1} & \longrightarrow & \mathcal{I}_p \\ & g & \longmapsto & g|_{\mathbb{N}_p}\end{array}$.
Soit $h \in \mathcal{I}_p$. Pour tout $g \in \mathcal{I}_{p+1}$, $\Psi(g) = h \iff g|_{\mathbb{N}_p} = h$,
donc $\Psi^{-1}(\{h\}) = \{g \in \mathcal{F}(\mathbb{N}_{p+1}, E) / \forall i \in \mathbb{N}_p,\ g(i) = h(i) \text{ et } g(p+1) \in E \setminus h(\mathbb{N}_p)\}$.
On peut mettre cet ensemble en bijection avec $E \setminus h(\mathbb{N}_p)$, donc $|\Psi^{-1}(\{h\})| = n - p \in \mathbb{N}^*$.
D'après le principe des bergers, $|\mathcal{I}_{p+1}| = (n-p)|\mathcal{I}_p|$, d'où $R(p+1)$. $\square$

Exemple. paradoxe des anniversaires : Soit C une classe d'élèves et f l'application qui à tout élément de C associe sa date d'anniversaire. La probabilité que 2 élèves au moins aient la même date d'anniversaire est égal à $p = 1 - \dfrac{N}{\#(\mathcal{F}(C,D))}$, où D est l'ensemble des dates possibles (on simplifie la situation en supposant que $\#D = 365$, c'est-à-dire en oubliant les années bissextiles) et où N est le nombre d'injections de C dans D. Ainsi, $p = 1 - \dfrac{365 \times 364 \times \cdots \times (365-n+1)}{365^n}$, où n est le nombre d'élèves de C. Avec $n = 47$, on obtient $p = 95,5\%$.

Corollaire. Pour tout $n \in \mathbb{N}$, $|\mathcal{S}_n| = n!$.
Plus généralement, *factorielle de n* est le nombre de bijections d'un ensemble de cardinal n dans un autre ensemble de cardinal n.

Choix successifs sans répétition, tirages sans remise :
On utilise les p-arrangements dans les problèmes de choix successifs de p éléments pris parmi n, sans répétition, ou bien de tirages successifs de p éléments dans un ensemble de n éléments sans remise. Ici, l'ordre d'apparition des différents choix ou tirages compte, c'est-à-dire que deux p-arrangements ayant les mêmes éléments dans un ordre différent sont comptabilisés tous les deux.

Cela permet ainsi de dénombrer le nombre d'issues possibles lorsqu'on effectue p fois une expérience, sans possibilité de retrouver un résultat précédemment obtenu.

Exemple. 8 sportifs se présentent pour courir un 100m. Déterminer le nombre de podiums possibles.
Un podium est un 3-arrangement de coureurs, désignant le médaillé d'or, le médaillé d'argent et le médaillé de bronze. Le nombre de podiums est donc $A_{8,3} = 8.7.6 = 336$.

Théorème. Le nombre de p-combinaisons d'éléments d'un ensemble de cardinal n, c'est-à-dire le nombre de parties de p éléments incluses dans un ensemble de cardinal n est égal à

$$\binom{n}{p} \triangleq \frac{A_{n,p}}{p!} = \frac{n!}{(n-p)!p!}.$$

Cette quantité s'appelle le coefficient binomial "p parmi n".

Démonstration.
Notons $\mathcal{C}_p$ l'ensemble des p-combinaisons d'éléments de E et $\begin{array}{rccc}\varphi : & \mathcal{I}_p & \longrightarrow & \mathcal{C}_p \\ & f & \longmapsto & f(\mathbb{N}_p)\end{array}$.
Soit $A \in \mathcal{C}_p$. $f \in \varphi^{-1}(\{A\})$ si et seulement si $f(\mathbb{N}_p) = A$, donc si et seulement si f réalise une bijection de $\mathbb{N}_p$ dans A. Ainsi, pour tout $A \in \mathcal{C}_p$, $|\varphi^{-1}(\{A\})| = p!$ et le principe des bergers permet de conclure. □

Choix simultanés, tirages sans remise où l'ordre est indifférent :
On utilise les p-combinaisons dans les problèmes de choix simultanés de p éléments pris parmi n, ou bien de tirages successifs de p éléments dans un ensemble de n éléments sans remise lorsque l'ordre d'apparition des différents tirages n'intervient pas.

Exercice. Avec un jeu de 32 cartes, quelle est la probabilité qu'une main de 5 cartes comporte au plus 2 piques.
Solution :
◇ Rappelons qu'une carte possède une couleur (pique, coeur, carreau, trèfle) et une valeur (7,8,9,10,valet, dame, roi, as). Dans un jeu de 32 cartes, on dispose donc de 8 cartes de chaque couleur.
Dans un jeu de 52 cartes, on dispose des mêmes couleurs et des valeurs supplémentaires 2,3,4,5,6, soit 13 valeurs au total.
◇ Ici, la condition portant sur la main ne dépend pas de l'ordre des cartes, donc on peut assimiler une main de 5 cartes à une partie de 5 éléments parmi les 32 cartes. Ainsi, le nombre total de mains de 5 cartes est $\binom{32}{5}$.
◇ On applique le principe du "ou exclusif" en fonction du nombre de piques dans la main :

— Le nombre de mains de 5 cartes sans aucun pique est $\binom{24}{5}$,

— Le nombre de mains de 5 cartes comportant exactement un pique est $8 \times \binom{24}{4}$, car pour en construire une, on peut d'abord choisir un pique, soit 8 choix, puis

un ensemble de 4 cartes d'une couleur différente de pique, soit $\binom{24}{4}$ choix. On a donc appliqué le principe du "et".

— De la même façon, il y a $\binom{24}{3} \times \binom{8}{2}$ mains de 5 cartes avec 2 piques exactement.

Ainsi la probabilité demandée est égale à $\dfrac{\binom{24}{5} + \binom{24}{4} \times 8 + \binom{24}{3} \times \binom{8}{2}}{\binom{32}{5}}$.

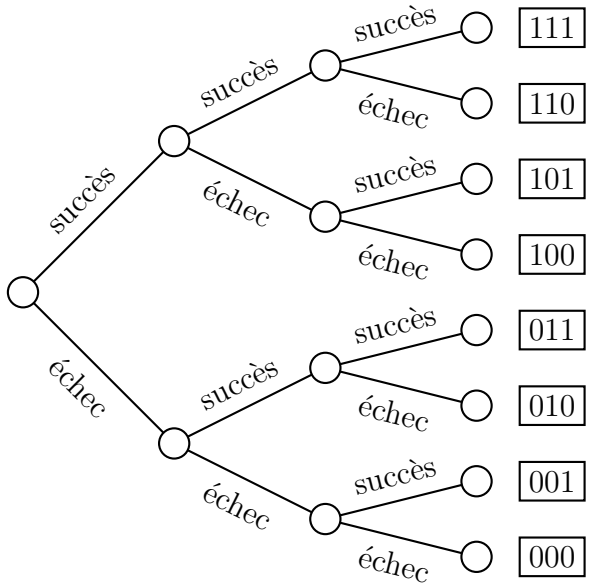
Exercice. Avec un jeu de 32 cartes, quelle est la probabilité qu'une main de 5 cartes comporte au plus 4 piques.
Solution : On peut adapter la solution précédente, mais il est préférable de passer au contraire, en cherchant d'abord à dénombrer les mains comportant uniquement des piques, ce qui est plus simple, car cela revient à choisir 5 éléments parmi les 8 cartes de couleur pique. Ainsi, la probabilité cherchée est
$\dfrac{\binom{32}{5} - \binom{8}{5}}{\binom{32}{5}}$.

Exercice. Combien le mot MISSISSIPPI possède-t-il d'anagrammes, qu'ils aient un sens ou non ?
Solution : On cherche le nombre de mots de 11 lettres possèdant 1 M, 2 P, 4 I et 4 S.
Pour construire un tel mot, on remplit par des lettres 11 cases initialement vides. On choisit d'abord l'emplacement de la lettre M, soit 11 choix, puis les deux emplacements des lettres P parmi les 10 emplacements restants, soit $\binom{10}{2}$ choix etc. Ainsi, le nombre cherché est égal à $N = 11.\binom{10}{2}.\binom{8}{4} = 34650$.
A noter qu'on aurait pu raisonner en classant les 4 lettres M, P, I, et S dans un autre ordre.

2.7 Les coefficients binomiaux

Considérons un ensemble de n éléments, noté $E = \{e_1, \ldots, e_n\}$.
Pour démontrer que $|\mathcal{P}(E)| = 2^n$, on a mis $\mathcal{P}(E)$ en bijection avec $\mathcal{F}(E, \{0,1\})$ en associant à toute partie de E son indicatrice. Mais $\mathcal{F}(E, \{0,1\})$ est aussi l'ensemble des familles $(\varepsilon_i)_{1 \leq i \leq n}$ d'éléments de $\{0,1\}$. On peut donc coder toute partie A de E par une suite binaire de longueur n.
Par exemple, avec $n = 5$, la partie $A = \{e_2, e_3, e_5\}$ de E est codée par la suite 01101.
Cette bijection envoie les parties de E à k éléments sur les suites binaires possédant

exactement k "1". Ainsi $\binom{n}{k}$ est aussi le nombre de suites binaires de longueur n possédant exactement k "1". On peut le retrouver directement en disant que pour construire une telle suite, il suffit de convenir de l'ensemble des k positions des "1" parmi les n positions.
Changeons un peu le vocabulaire, en remplaçant "0" par "échec" et "1" par "succès". On considère un test que l'on peut répéter n fois, comme le fait de lancer une pièce de monnaie et de tester si elle tombe sur le côté "face". Alors $\binom{n}{k}$ est le nombre de réalisations de n tests comportant exactement k succès.
On peut représenter les 2^n réalisations possibles par un arbre :



Ainsi, dans un tel arbre, s'il représente la répétition de n tests, le nombre de chemins réalisant exactement k succès est égal à $\binom{n}{k}$.

Formule : $\forall n, p \in \mathbb{N}$ avec $0 \leq p \leq n$, $\binom{n}{p} = \binom{n}{n-p}$.

Démonstration.
C'est évident avec la formule $\binom{n}{p} = \dfrac{n!}{(n-p)!p!}$, mais on peut aussi en donner une preuve combinatoire : avec les notations de la démonstration précédente, l'application $\begin{array}{ccc} \mathcal{C}_p & \longrightarrow & \mathcal{C}_{n-p} \\ A & \longmapsto & \overline{A} \end{array}$ est une bijection (c'est une involution). □

Formule comité-président : Pour tout $n, k \in \mathbb{N}^*$ avec $k \leq n$,

$$k\binom{n}{k} = n\binom{n-1}{k-1}.$$

Démonstration.
C'est très simple par le calcul, mais on peut aussi en donner une preuve combinatoire, qui permet notamment de retenir la formule :
$k\binom{n}{k}$ est le nombre de comités à k éléments parmi n, où chaque comité est muni d'un président. Formellement, c'est le nombre de couples (a, A) où A est une partie à k éléments d'un ensemble E de cardinal n et où $a \in A$. Mais pour dénombrer ces couples, on peut d'abord choisir le président a, soit n choix, puis le président choisit la composition des autres membres du comité, soit $\binom{n-1}{k-1}$ choix.
On peut alors concevoir une formule "comité à deux présidents" : pour tout $n, k \in \mathbb{N}$ avec $2 \leq k \leq n$, $k(k-1)\binom{n}{k} = n(n-1)\binom{n-2}{k-2}$. Je vous laisse généraliser : □

Formule comité-bureau : Pour tout $p \in \mathbb{N}$, pour tout $n, k \in \mathbb{N}$ avec $p \leq k \leq n$,

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

Formule du triangle de Pascal [1] **:** $\forall n, p \in \mathbb{N}$ avec $1 \leq p < n$,

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

Remarque. Il est souvent pratique de convenir que, pour tout $n, p \in \mathbb{Z}$ tels que $\neg(0 \leq p \leq n)$, $\binom{n}{p} = 0$.
Alors la formule du triangle de Pascal est vraie pour tout $n \geq 1$ et $p \in \mathbb{Z}$ (le raisonnement combinatoire reste valable).

Démonstration.
Là aussi, on peut vérifier cette formule par le calcul : à faire.
De manière combinatoire, distinguons un élément a dans E. On peut alors partitionner l'ensemble des p-combinaisons de E en deux sous-ensembles :

— les p-combinaisons ne contenant pas a, qui sont toutes les p-combinaisons de $E \setminus \{a\}$, au nombre de $\binom{n-1}{p}$,

1. Blaise Pascal, 1623-1662, est un mathématicien, physicien, inventeur, philosophe, moraliste et théologien français. Enfant précoce, il publie un traité de géométrie projective à seize ans et il invente la première machine à calculer (la pascaline) à 19 ans. Après 1654 il se consacre à la réflexion philosophique et religieuse. Ses "pensées" seront publiées après sa mort.

— et les p-combinaisons contenant a, que l'on peut mettre en bijection avec les $(p-1)$-combinaisons de $E \setminus \{a\}$, au nombre de $\binom{n-1}{p-1}$.

□

Représentation graphique du triangle de Pascal.

Remarque. On vient de voir plusieurs exemples de démontrations combinatoires de formules. Le principe général de ce type de preuve, concernant une égalité entre entiers de la forme $a = b$, consiste à interpréter a et b comme le dénombrement d'un même ensemble fini selon deux méthodes différentes.
Par exemple, la formule $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ peut se démontrer en disant que, pour constuire une partie quelconque d'un ensemble à n éléments, on choisit d'abord le nombre k d'éléments de cette partie, puis on choisit k éléments parmi n qui constitueront cette partie.
Cependant cette dernière formule est un cas particulier de la formule du binôme de Newton :

Formule du binôme de Newton [2] : On se place dans un anneau $(A, +, \times)$. Soit a_1 et a_2 deux éléments de A qui commutent, c'est-à-dire tels que $a_1 a_2 = a_2 a_1$. Alors

$$\forall n \in \mathbb{N},\ \ (a_1 + a_2)^n = \sum_{k=0}^{n} \binom{n}{k} a_1^k\ a_2^{n-k}.$$

Démonstration.

- *Première méthode : par récurrence.*

On note $R(n)$ l'assertion $(a_1 + a_2)^n = \sum_{k=0}^{n} \binom{n}{k} a_1^k a_2^{n-k}$. $R(0)$ est vraie.
Pour $n \geq 0$, on suppose $R(n)$.

$$\begin{aligned}(a_1 + a_2)^{n+1} &= (a_1 + a_2) \sum_{k=0}^{n} \binom{n}{k} a_1^k a_2^{n-k} \\ &= a_1^{n+1} + \sum_{k=0}^{n-1} \binom{n}{k} a_1^{k+1} a_2^{n-k} + a_2^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a_1^k a_2^{n-k+1}.\end{aligned}$$

Dans la première somme, posons $h = k + 1$:
l'application $k \longmapsto k+1$ est une bijection de $\{0, \ldots, n-1\}$ dans $\{1, \ldots, n\}$, donc
$\sum_{k=0}^{n-1} \binom{n}{k} a_1^{k+1} a_2^{n-k} = \sum_{k=0}^{n-1} \binom{n}{(k+1)-1} a_1^{k+1} a_2^{n+1-(k+1)} = \sum_{h=1}^{n} \binom{n}{h-1} a_1^h a_2^{n+1-h}$.
L'indice h de cette somme est une variable muette que l'on peut renommer en k, donc

2. Isaac Newton, 1642-1727 est un philosophe, mathématicien, physicien, alchimiste, astronome et théologien britannique. Il a fondé la mécanique classique, dont la théorie de la gravitation universelle. En mathématiques, il est à l'origine avec Leibniz du calcul infinitésimal.

$$\begin{aligned}(a_1+a_2)^{n+1} &= a_1^{n+1} + \sum_{k=1}^{n} \binom{n}{k-1} a_1^k a_2^{n+1-k} + a_2^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a_1^k a_2^{n-k+1} \\ &= a_1^{n+1} + a_2^{n+1} + \sum_{k=1}^{n} (\binom{n}{k-1} + \binom{n}{k}) a_1^k a_2^{n+1-k} \\ &= a_1^{n+1} + a_2^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a_1^k a_2^{(n+1)-k} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} a_1^k a_2^{(n+1)-k}.\end{aligned}$$

Ceci prouve $R(n+1)$.

• *Seconde méthode : combinatoire.* $(a_1+a_2)^n = (a_1+a_2)\times\cdots\times(a_1+a_2)$. Si l'on développe complètement ce produit de n facteurs, où chaque facteur est la somme de deux termes, on obtient une somme de termes où chaque terme est un produit de n facteurs, obtenu en choissant dans chacun des n facteurs a_1+a_2, ou bien a_1, ou bien a_2. Ainsi, (1) : $(a_1+a_2)^n = \sum_{f\in\mathcal{F}(\mathbb{N}_n,\{1,2\})} \prod_{i=1}^{n} a_{f(i)}$: chacun de ces termes est construit en choissant $a_{f(1)}$ dans le premier facteur a_1+a_2, puis $a_{f(2)}$ dans le second facteur a_1+a_2, etc. Plus rigoureusement, on peut démontrer la relation (1) par récurrence sur n, car elle entraîne

$$\begin{aligned}(a_1+a_2)^{n+1} &= a_1 \sum_{f\in\mathcal{F}(\mathbb{N}_n,\{1,2\})} \prod_{i=1}^{n} a_{f(i)} + a_2 \sum_{f\in\mathcal{F}(\mathbb{N}_n,\{1,2\})} \prod_{i=1}^{n} a_{f(i)} \\ &= \sum_{\substack{f\in\mathcal{F}(\mathbb{N}_{n+1},\{1,2\}) \\ \text{tel que } f(n+1)=1}} \prod_{i=1}^{n+1} a_{f(i)} + \sum_{\substack{f\in\mathcal{F}(\mathbb{N}_{n+1},\{1,2\}) \\ \text{tel que } f(n+1)=2}} \prod_{i=1}^{n+1} a_{f(i)} \\ &= \sum_{f\in\mathcal{F}(\mathbb{N}_{n+1},\{1,2\})} \prod_{i=1}^{n+1} a_{f(i)}.\end{aligned}$$

Pour tout $k\in\{0,\dots,n\}$, notons F_k l'ensemble des fonctions f de $\mathcal{F}(\mathbb{N}_n,\{1,2\})$ telles que 1 possède exactement k antécédents. La famille $(F_0,\dots,F_n)$ est une partition de $\mathcal{F}(\mathbb{N}_n,\{1,2\})$ donc, en sommant par paquets, $(a_1+a_2)^n = \sum_{k=0}^{n}\sum_{f\in F_k}\prod_{i=1}^{n} a_{f(i)}$.

Mais si $f\in F_k$, parmi $a_{f(1)},\dots,a_{f(n)}$, on rencontre exactement k fois a_1 et $n-k$ fois a_2, donc $\prod_{i=1}^{n} a_{f(i)} = a_1^k a_2^{n-k}$. Ainsi, $(a_1+a_2)^n = \sum_{k=0}^{n} a_1^k a_2^{n-k} \sum_{f\in F_k} 1 = \sum_{k=0}^{n} a_1^k a_2^{n-k}|F_k|$.

De plus, pour construire une application f de F_k, il suffit d'indiquer quelle est la partie à k éléments de $\mathbb{N}_n$ dont les images par f sont égales à 1, donc $|F_k| = \binom{n}{k}$. □

Formule du multinôme : (Hors programme). Soit $p, n \in \mathbb{N}^*$. Soit $a_1, \dots, a_p$ p éléments d'un anneau A qui commutent deux à deux. Alors

$$(a_1 + \cdots + a_p)^n = \sum_{\substack{i_1,\dots,i_p \in \mathbb{N} \\ \text{tel que } i_1+\cdots+i_p=n}} \frac{n!}{i_1! \times \cdots \times i_p!}\, a_1^{i_1} \times \cdots \times a_p^{i_p}.$$

Exemple. Avec $n = p = 3$, les triplets (i_1, i_2, i_3) d'entiers naturels tels que $i_1 + i_2 + i_3 = 3$ sont $(1,1,1), (1,2,0), (2,1,0), (1,0,2), (2,0,1), (0,1,2), (0,2,1)$, $(3,0,0), (0,3,0)$ et $(0,0,3)$, donc
$(a+b+c)^3 = 6abc + 3(ab^2 + a^2b + ac^2 + a^2c + bc^2 + b^2c) + a^3 + b^3 + c^3$.

Démonstration.
On adapte la démonstration combinatoire.

On obtient d'abord $(a_1 + \cdots + a_p)^n = \sum_{f \in \mathcal{F}(\mathbb{N}_n, \mathbb{N}_p)} \prod_{i=1}^{n} a_{f(i)}$.

Pour tout $(i_1, \dots, i_p) \in \mathbb{N}^p$ tel que $i_1 + \cdots + i_p = n$, on note $F_{i_1,\dots,i_p}$ l'ensemble des $f \in \mathcal{F}(\mathbb{N}_n, \mathbb{N}_p)$ telles que, pour tout $j \in \mathbb{N}_p$, le nombre d'antécédents de j par f est égal à i_j. La famille des $F_{i_1,\dots,i_p}$, lorsque $(i_1, \dots, i_p)$ parcourt tous les p-uplets d'entiers tels que $i_1 + \cdots + i_p = n$, est une partition de $\mathcal{F}(\mathbb{N}_n, \mathbb{N}_p)$, donc en sommant par paquets,

$$(a_1 + \cdots + a_p)^n = \sum_{\substack{i_1,\dots,i_p \in \mathbb{N} \\ \text{tel que } i_1+\cdots+i_p=n}} |F_{i_1,\dots,i_p}| a_1^{i_1} \times \cdots \times a_p^{i_p}.$$

Pour construire une fonction quelconque de $F_{i_1,\dots,i_p}$, on choisit d'abord les i_1 antécédents de 1 parmi les n éléments de $\mathbb{N}_n$, soit $\binom{n}{i_1}$ choix, puis les i_2 antécédents de 2 parmi les $n - i_1$ éléments restants de $\mathbb{N}_n$, soit $\binom{n-i_1}{i_2}$ choix, etc., jusqu'aux choix des i_{p-1} antécédents de $p-1$ parmi les $n - i_1 - \cdots - i_{p-2}$ éléments restants. Ainsi,

$$\begin{aligned} |F_{i_1,\dots,i_p}| &= \binom{n}{i_1}\binom{n-i_1}{i_2}\cdots\binom{n-i_1-\cdots-i_{p-2}}{i_{p-1}} \\ &= \frac{n!}{i_1!(n-i_1)!}.\frac{(n-i_1)!}{i_2!(n-i_1-i_2)!}\cdots\frac{n-i_1-\cdots-i_{p-2}}{i_{p-1}!(n-i_1-\cdots-i_{p-2}-i_{p-1})!} \\ &= \frac{n!}{i_1! \times \cdots \times i_p!}. \end{aligned}$$

□

Remarque. Associons à toute application f de $\mathbb{N}_n$ dans $\mathbb{N}_p$ la suite $(f(1), f(2), \dots, f(n))$, que l'on peut assimiler à un mot de longueur n écrit sur l'alphabet $\{1, \dots, p\}$, ou si l'on préfère au codage d'un mot de longueur n écrit sur l'alphabet $A = \{a_1, \dots, a_p\}$. La fonction qui envoie f sur ce mot est une bijection de $\mathcal{F}(\mathbb{N}_n, \mathbb{N}_p)$ dans A^n, il suffit d'ailleurs de montrer l'injectivité. Donc $F_{i_1,\dots,i_p}$ est aussi le nombre de mots de n lettres comportant i_1 lettres a_1,...,i_p lettres a_p. Cela généralise l'exercice Mississippi.

Petit théorème de Fermat : Soit $p \in \mathbb{P}$ et $n \in \mathbb{N}$. Alors $n^p \equiv n\ [p]$.
En particulier, si $n \notin p\mathbb{Z}$, alors $n^{p-1} \equiv 1\ [p]$.

Démonstration.
◇ Soit $k \in \{1, \dots, p-1\}$. $k! \binom{p}{k} = p(p-1)\cdots(p-k+1)$ est un multiple de p car $k \geq 1$, mais p est premier et $k \leq p-1$, donc $p \wedge (k!) = 1$. Ainsi, d'après le théorème de Gauss, $p \mid \binom{p}{k}$.
◇ Soit $n \in \mathbb{N}$ tel que $n^p \equiv n\ [p]$. Alors, d'après la formule du binôme de Newton, $(n+1)^p = \sum_{k=0}^{p} \binom{p}{k} n^k$, donc d'après le point précédent, modulo p,
$(n+1)^p \equiv n^0 + n^p \equiv n+1$. De plus, $0^p = 0$, donc par récurrence sur n, on montre que $n^p \equiv n\ [p]$.
◇ Supposons maintenant que $n \notin p\mathbb{Z}$. On vient de montrer que $p|(n^p - n) = n(n^{p-1}-1)$, mais $n \wedge p = 1$, donc d'après le théorème de Gauss, $p|(n^{p-1}-1)$. □

La formule suivante est analogue à la formule du binôme de Newton, mais elle concerne la dérivée n-ième d'un produit de deux fonctions :
Formule de Leibniz : Soient f et g deux applications d'un intervalle I dans $\mathbb{R}$. Si f et g sont n fois dérivables sur I, alors fg est n fois dérivable sur I et

$$(fg)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(k)} g^{(n-k)}.$$

Démonstration.
Soit $n \in \mathbb{N}$. Notons $R(n)$ l'assertion suivante : si f et g sont n fois dérivables sur I, fg est n fois dérivable sur I et $(fg)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(k)} g^{(n-k)}$.
Pour $n = 0$, $R(0)$ est vraie.
Pour $n \geq 0$, supposons $R(n)$. On suppose également que f et g sont $n+1$ fois dérivables sur I. D'après $R(n)$, $(fg)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(k)} g^{(n-k)}$.
Pour tout $k \in \{0, \dots, n\}$, $f^{(k)}$ et $g^{(n-k)}$ sont dérivables sur I, donc $f^{(k)} g^{(n-k)}$ est dérivable sur I. On peut donc dériver l'égalité précédente. On obtient :

$$\begin{aligned}
(fg)^{(n+1)} &= \sum_{k=0}^{n} \binom{n}{k} (f^{(k+1)} g^{(n-k)} + f^{(k)} g^{(n-k+1)}) \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} f^{(k)} g^{(n-k+1)} + \sum_{k=0}^{n} \binom{n}{k} f^{(k)} g^{(n-k+1)} \\
&= f^{(n+1)} g^{(0)} + f^{(0)} g^{(n+1)} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) f^{(k)} g^{(n-k+1)} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} f^{(k)} g^{(n-k+1)}.
\end{aligned}$$

Ceci prouve $R(n+1)$.

Ainsi, d'après le principe de récurrence, pour tout $n \in \mathbb{N}$, on a montré $R(n)$. □

Remarque. Lorsque a et b sont des réels, on peut retrouver la formule du binôme de Newton à partir de la formule de Leibniz, en l'appliquant avec $f(t) = e^{ta}$ et $g(t) = e^{tb}$, en $t = 0$. En effet, pour tout $k \in \mathbb{N}$, $\dfrac{d^k}{dt^k}(e^{ta}) = a^k e^{ta}$.

2.8 Sommes et produits : quelques techniques

2.8.1 Télescopage

Propriété. Soit $m, n \in \mathbb{Z}$ avec $m \leq n$. Soit $(u_k)_{m \leq k \leq n+1}$ une famille d'éléments d'un groupe abélien $(G, +)$. Alors $\displaystyle\sum_{k=m}^{n} (u_{k+1} - u_k) = u_{n+1} - u_m$.

De même, $\displaystyle\sum_{k=m+1}^{n+1} (u_{k-1} - u_k) = u_m - u_{n+1}$.

On dit que ces sommes sont télescopiques.

Exemple.

◇ $\displaystyle\sum_{k=1}^{n} \frac{1}{k(k+1)} = \sum_{k=1}^{n} \Big(\frac{1}{k} - \frac{1}{k+1}\Big) = 1 - \frac{1}{n+1} \underset{n\to+\infty}{\longrightarrow} 1$, donc la série $\displaystyle\sum_{k\geq 1} \frac{1}{k(k+1)}$ converge et $\displaystyle\sum_{k=1}^{+\infty} \frac{1}{k(k+1)} = 1$.

◇ $\displaystyle\sum_{k=1}^{n} \ln(1 + \frac{1}{k}) = \sum_{k=1}^{n} (\ln(k+1) - \ln k) = \ln(n+1) - \ln 1 \underset{n\to+\infty}{\longrightarrow} +\infty$, donc la série $\displaystyle\sum_{k\geq 1} \ln(1 + \frac{1}{k})$ diverge (alors que $\ln(1 + \frac{1}{n}) \underset{n\to+\infty}{\longrightarrow} 0$).

◇ $\displaystyle\sum_{k=0}^{n} k(k!) = \sum_{k=0}^{n} ((k+1) - 1)(k!) = \sum_{k=0}^{n} ((k+1)! - k!) = (n+1)! - 1$.

2.8.2 Séparation des indices pairs et impairs

D'après le principe de sommation par paquets, lorsque $(u_k)_{0 \leq k \leq n}$ est une famille d'éléments d'un monoïde commutatif, $\displaystyle\sum_{k=0}^{n} u_k = \sum_{\substack{0\leq k\leq n \\ k \text{ pair}}} u_k + \sum_{\substack{0\leq k\leq n \\ k \text{ impair}}} u_k = \sum_{p=0}^{\lfloor \frac{n}{2} \rfloor} u_{2p} + \sum_{p=0}^{\lfloor \frac{n-1}{2} \rfloor} u_{2p+1}$.

Exemple. $\displaystyle\sum_{k=0}^{2n} (-1)^k k^2 = \sum_{k=0}^{n} (2k)^2 - \sum_{k=0}^{n-1} (2k+1)^2 = 4\sum_{k=0}^{n} k^2 - \sum_{k=0}^{n-1} (4k^2 + 4k + 1)$, donc $\displaystyle\sum_{k=0}^{2n} (-1)^k k^2 = 4n^2 - 4\frac{n(n-1)}{2} - n = 2n^2 + n$.

2.8.3 Fonction génératrice

Soit $m, n \in \mathbb{N}$ avec $m \leq n$ et soit $(u_k)_{m \leq k \leq n}$ une famille de complexes. La fonction génératrice de cette famille est l'application polynomiale $P : x \longmapsto \sum_{k=m}^{n} u_k x^k$.

Si P est connu, on peut en déduire plusieurs sommes : $\sum_{k=m}^{n} u_k = P(1)$, $\sum_{k=m}^{n} k u_k = P'(1)$, $\sum_{k=m}^{n} k(k-1)u_k = P''(1)$, $\sum_{k=m}^{n} \frac{u_k}{k+1} = \int_0^1 P(t)dt$ etc.

Plus tard, vous étudierez la théorie des séries entières, qui sont des applications de la forme $x \longmapsto \sum_{k=m}^{+\infty} u_k x^k$. Cela permet de prolonger la méthode précédente à des calculs de sommes de séries.

Exemple.

◇ Calculer $S = \sum_{k=0}^{n} \binom{n}{k} k$.

$S = P'(1)$, où $P(x) = \sum_{k=0}^{n} \binom{n}{k} x^k = (x+1)^n$ d'après la formule du binôme de Newton, donc $S = n2^{n-1}$.

On peut aussi calculer S en utilisant la formule du comité-président :

$S = \sum_{k=1}^{n} \binom{n-1}{k-1} n = n2^{n-1}$.

◇ Calculer $S = \sum_{k=0}^{n} k2^k$.

$S = 2P'(2)$, où $P(x) = \sum_{k=0}^{n} x^k = \frac{x^{n+1}-1}{x-1}$ (pour $x \neq 1$).

$P'(x) = \frac{(n+1)x^n(x-1) - (x^{n+1}-1)}{(x-1)^2} = \frac{nx^{n+1} - (n+1)x^n + 1}{(x-1)^2}$,

donc $S = 2(n2^{n+1} - (n+1)2^n + 1) = (n-1)2^{n+1} + 2$.

2.8.4 Quelques formules

Somme arithmétique : Soit $r \in \mathbb{C}$. Une suite (u_n) de complexes est arithmétique de raison r si et seulement si elle vérifie la relation de récurrence suivante :
$\forall n \in \mathbb{N},\ u_{n+1} = u_n + r$. Par récurrence, on montre que pour tout $n \in \mathbb{N}$, $u_n = u_0 + nr$.
Soit $m, n \in \mathbb{N}$ avec $m \leq n$ et soit (u_n) une suite arithmétique de raison r. Alors

$$\sum_{k=m}^{n} u_k = \frac{u_m + u_n}{2}(n - m + 1),$$

ce que l'on retient de la manière suivante : une somme arithmétique est égale à la moyenne de ses termes extrèmes multiplié par son nombre de termes.

Démonstration.

$$\begin{aligned} 2\sum_{k=m}^{n} u_k &= u_m + u_{m+1} + \cdots + u_{n-1} + u_n \\ &\quad + u_n + u_{n-1} + \cdots + u_{m+1} + u_m \\ &= (u_m + u_n) + (u_{m+1} + u_{n-1}) + \cdots + (u_{n-1} + u_{m+1}) + (u_n + u_m). \end{aligned}$$

Or, pour tout $k \in \{0, \ldots, n-m\}$, $u_{m+k}+u_{n-k} = 2u_0+r(m+k+n-k) = 2u_0+r(m+n)$, donc il ne dépend pas de k. Ceci permet de conclure. □

Exemple. $\displaystyle\sum_{k=1}^{n}(2k-1) = \frac{(2n-1)+(2-1)}{2} \times n = n^2.$

Formule de Bernoulli : Soit $(A, +, \times)$ un anneau. Soit a et b deux éléments de A qui commutent (i.e $ab = ba$). Alors, pour tout $n \in \mathbb{N}$,

$$a^{n+1} - b^{n+1} = (a-b)\sum_{k=0}^{n} a^k b^{n-k}.$$

Démonstration.

$(a-b)\displaystyle\sum_{k=0}^{n} a^k b^{n-k} = \sum_{k=0}^{n}(a^{k+1}b^{(n+1)-(k+1)} - a^k b^{(n+1)-k})$. Il s'agit d'une somme télescopique, ce qui permet de conclure. □

Remarque. Lorque $n+1$ est impair,

$$a^{n+1} + b^{n+1} = a^{n+1} - (-b)^{n+1} = (a+b)\sum_{k=0}^{n} a^k(-1)^{n-k}b^{n-k}.$$

Exemple. $a^3 - b^3 = (a-b)(a^2+ab+b^2)$.

Somme géométrique : Soit $r \in \mathbb{C}$. Une suite (u_n) de complexes est géométrique de raison r si et seulement si elle vérifie la relation de récurrence suivante :
$\forall n \in \mathbb{N},\ u_{n+1} = ru_n$. Par récurrence, on montre que pour tout $n \in \mathbb{N}$, $u_n = u_0 r^n$.
Soit $m, n \in \mathbb{N}$ avec $m \leq n$ et soit (u_n) une suite géométrique de raison r avec $r \neq 1$. Alors

$$\sum_{k=m}^{n} u_k = \frac{u_{n+1} - u_m}{r-1},$$

ce que l'on retient de la manière suivante : une somme géométrique est égale au terme suivant le dernier moins le premier terme divisé par la raison privée de 1.

Remarque. On a déjà rencontré et démontré ce résultat page 23, mais il est à ce point important qu'il mériterait d'apparaître même une dizaine de fois.

Démonstration.
C'est un cas particulier de la formule de Bernoulli :
$u_{n+1}-u_m = u_0(r^{n+1}-r^m) = u_0 r^m(r^{n+1-m}-1) = u_0 r^m(r-1)\sum_{k=0}^{n-m} r^k = (r-1)\sum_{k=0}^{n-m} u_{m+k}$.
□

Exemple. Soit $n \in \mathbb{N}^*$. Soit ω une racine n-ième différente de 1.
Alors $\sum_{k=0}^{n-1} \omega^k = \frac{\omega^n - 1}{\omega - 1} = 0$.
Ainsi, pour tout $h \in \{1, \dots, n-1\}$, $\sum_{k=0}^{n-1} e^{2i\pi\frac{hk}{n}} = 0$.

2.8.5 Sommes doubles

Soit $m, n, p, q \in \mathbb{N}$ avec $m \leq n$ et $p \leq q$.
Soit $(u_{k,\ell})_{(k,\ell)\in\{m,\dots,n\}\times\{p,\dots,q\}}$ une famille d'éléments d'un monoïde commutatif $(G, +)$.
On peut partitionner $A = \{m, \dots, n\} \times \{p, \dots, q\}$ en la famille $(A_i)_{m\leq i\leq n}$,
où $A_i = \{(i, \ell)/\ell \in \{p, \dots, q\}\}$. Ainsi,
$\sum_{(k,\ell)\in A} u_{k,\ell} = \sum_{i=m}^{n} \sum_{(k,\ell)\in A_i} u_{k,\ell}$. De plus , pour tout $i \in \{m, \dots, n\}$,
l'application $\begin{array}{rccc} \varphi : & \{p, \dots, q\} & \longrightarrow & A_i \\ & \ell & \longmapsto & (i, \ell) \end{array}$ est une bijection, donc on peut poser dans la somme interne, $(k, \ell) = \varphi(\ell')$. Ainsi, $\sum_{(k,\ell)\in A} u_{k,\ell} = \sum_{i=m}^{n}\sum_{\ell'=p}^{q} u_{i,\ell'} = \sum_{k=m}^{n}\sum_{\ell=p}^{q} u_{k,\ell}$, en renommant les indices.
À la place de $\sum_{(k,\ell)\in A} u_{k,\ell}$, on note souvent $\sum_{\substack{m\leq k\leq n \\ p\leq \ell\leq q}} u_{k,\ell}$.
De plus, on peut aussi considérer la partition de A selon la famille $(B_\ell)_{p\leq\ell\leq q}$,
où $B_\ell = \{(k, \ell)/m \leq k \leq n\}$. Ainsi, on a montré que

$$\sum_{\substack{m\leq k\leq n \\ p\leq \ell\leq q}} u_{k,\ell} = \sum_{k=m}^{n}\sum_{\ell=p}^{q} u_{k,\ell} = \sum_{\ell=p}^{q}\sum_{k=m}^{n} u_{k,\ell}.$$

Exemple. $\sum_{\substack{1\leq k\leq n \\ 1\leq \ell\leq q}} (k+l) = \sum_{k=1}^{n}\Big(\sum_{\ell=1}^{q} k + \sum_{\ell=1}^{q} \ell\Big) = \sum_{k=1}^{n}\Big(kq + \frac{q(q+1)}{2}\Big)$,
donc $\sum_{\substack{1\leq k\leq n \\ 1\leq \ell\leq q}} (k+l) = q\frac{n(n+1)}{2} + n\frac{q(q+1)}{2}$.

Propriété. Avec les notations précédentes, on suppose de plus que $(G,+,\times)$ est un anneau et que, pour tout $(k,\ell)\in A$, $u_{k,\ell}=v_kw_\ell$, où $v_k,w_\ell\in G$. Alors

$$\sum_{\substack{m\leq k\leq n\\ p\leq \ell\leq q}} v_kw_\ell=\Big(\sum_{k=m}^{n}v_k\Big)\Big(\sum_{\ell=p}^{q}w_\ell\Big).$$

Démonstration.
$\displaystyle\sum_{\substack{m\leq k\leq n\\ p\leq \ell\leq q}} v_kw_\ell=\sum_{k=m}^{n}\sum_{\ell=p}^{q}v_kw_\ell=\sum_{k=m}^{n}v_k\Big(\sum_{\ell=p}^{q}w_\ell\Big)$. Notons $S=\displaystyle\sum_{\ell=p}^{q}w_\ell$.

Ainsi, $\displaystyle\sum_{\substack{m\leq k\leq n\\ p\leq \ell\leq q}} v_kw_\ell=\sum_{k=m}^{n}(v_kS)=\Big(\sum_{k=m}^{n}v_k\Big)S$. □

2.8.6 Sommes triangulaires

Soit $m,n\in\mathbb{N}$ avec $m\leq n$. Notons $T=\{(k,\ell)/m\leq k\leq\ell\leq n\}$. Si l'on représente T dans le plan $\mathbb{R}^2$, on obtient bien un triangle.
Soit $(u_{k,\ell})_{(k,\ell)\in T}$ une famille d'éléments d'un monoïde commutatif $(G,+)$.
Notons $T'=\{m,\dots,n\}^2\setminus T$ et prolongeons la famille $(u_{k,\ell})$ sur T' en convenant que, pour tout $(k,\ell)\in T'$, $u_{k,\ell}=0_G$. $\{T,T'\}$ étant une partition de $\{m,\dots,n\}^2$, on a
$\displaystyle\sum_{\substack{m\leq k\leq n\\ m\leq \ell\leq n}} u_{k,\ell}=\sum_{(k,\ell)\in T}u_{k,\ell}+\sum_{(k,\ell)\in T'}u_{k,\ell}=\sum_{(k,\ell)\in T}u_{k,\ell}$.
Ainsi, la somme triangulaire $\displaystyle\sum_{(k,\ell)\in T}u_{k,\ell}$ peut être vue comme une somme double en ajoutant des "0". D'après le paragraphe précédent,
$\displaystyle\sum_{(k,\ell)\in T}u_{k,\ell}=\sum_{k=m}^{n}\sum_{\ell=m}^{n}u_{k,\ell}=\sum_{k=m}^{n}\sum_{\ell=k}^{n}u_{k,\ell}$. Le plus souvent, la somme triangulaire est notée $\displaystyle\sum_{m\leq k\leq\ell\leq n}u_{k,\ell}$, ce qui rend la formule précédente naturelle. De même, on peut montrer que $\displaystyle\sum_{m\leq k\leq\ell\leq n}u_{k,\ell}=\sum_{\ell=m}^{n}\sum_{k=m}^{\ell}u_{k,\ell}$.
De même, on a $\displaystyle\sum_{m\leq k<\ell\leq n}u_{k,\ell}=\sum_{k=m}^{n}\sum_{\ell=k+1}^{n}u_{k,\ell}=\sum_{\ell=m}^{n}\sum_{k=m}^{\ell-1}u_{k,\ell}$.

Exemple.
◇ Soit $n\in\mathbb{N}^*$ et $(u_k)_{1\leq k\leq n}$ une famille de réels. D'après la fin du paragraphe précédent, $\Big(\displaystyle\sum_{k=1}^{n}u_k\Big)^2=\sum_{\substack{1\leq k\leq n\\ 1\leq\ell\leq n}}u_ku_\ell$, donc d'après le principe de sommation par paquets,
$\Big(\displaystyle\sum_{k=1}^{n}u_k\Big)^2=\sum_{k=1}^{n}u_k^2+2\sum_{1\leq k<\ell\leq n}u_ku_\ell$.

◇ Notons $S = \sum_{1\leq k<\ell\leq n} \frac{k}{l}$. Ainsi, $S = \sum_{k=1}^{n} k \sum_{\ell=k+1}^{n} \frac{1}{\ell}$, mais pour simplifier S, il est indispensable d'intervertir les deux variables :
$S = \sum_{\ell=1}^{n} \frac{1}{\ell} \sum_{k=1}^{\ell-1} k = \sum_{\ell=1}^{n} \frac{1}{\ell} \frac{\ell(\ell-1)}{2} = \frac{1}{2} \sum_{\ell=1}^{n} (\ell-1) = \frac{n(n-1)}{4}$.

2.8.7 Produits

Toutes les propriétés précédentes, lorsqu'elles étaient valables dans un monoïde commutatif $(G,+)$ sont bien sûr valables en notation multiplicative dans un monoïde commutatif $(G,\times)$, car il ne s'agit que d'un changement de notation de la loi utilisée.
Par exemple, on peut énoncer une propriété de produit par paquets : Soit A un ensemble fini et $(x_a)_{a\in A}$ une famille d'éléments d'un monoïde commutatif $(G,\times)$. Soit $n\in\mathbb{N}$. On suppose qu'il existe des parties $A_1,\dots,A_n$ de A telles que $A = \bigsqcup_{i=1}^{n} A_i$.

Alors $\prod_{a\in A} x_a = \prod_{i=1}^{n} \prod_{a\in A_i} x_a$.

Soit $m,n\in\mathbb{N}$ avec $m\leq n$ et soit $(u_k)_{m\leq k\leq n}$ une famille de réels strictement positifs. Alors $\prod_{k=m}^{n} u_k = \exp\Big(\sum_{k=m}^{n} \ln u_k\Big)$, ce qui permet dans certains cas de ramener l'étude d'un produit à celle d'une somme.

Exemple. Soit $m,n\in\mathbb{N}$ avec $m\leq n$ et soit $(u_k)_{m\leq k\leq n}$ une famille de complexes. Soit $\lambda\in\mathbb{C}$. Alors $\prod_{k=m}^{n} (\lambda u_k) = \lambda^{n-m+1} \prod_{k=m}^{n} u_k$.

Exemple. $\prod_{k=1}^{n} 2k^2(k+1) = 2^n (n!)^2 (n+1)!$.

Exemple. Calcul de $\prod_{\substack{0\leq k\leq 2n\\ k\neq n}} (-1)^k (n-k)$:

$\prod_{\substack{0\leq k\leq 2n\\ k\neq n}} (-1)^k (n-k) = \Big(\prod_{k=0}^{n-1} (-1)^k (n-k)\Big)\Big(\prod_{k=n+1}^{2n} (-1)^k (n-k)\Big)$. Dans le second produit, posons $h = 2n-k$: $\prod_{k=n+1}^{2n} (-1)^k (n-k) = \prod_{h=0}^{n-1} (-1)^h (h-n)$, donc

$\prod_{\substack{0\leq k\leq 2n\\ k\neq n}} (-1)^k (n-k) = (-1)^n \Big(\prod_{k=0}^{n-1} (-1)^k (n-k)\Big)^2 = (-1)^n \prod_{k=0}^{n-1} (n-k)^2 = (-1)^n (n!)^2$.

Exemple de produit télescopique : Si $n \geq 2$, $\displaystyle\prod_{k=2}^{n}\Big(1-\frac{1}{k}\Big) = \prod_{k=2}^{n}\frac{k-1}{k} = \frac{1}{n}$.