Analyse-Probabilités CAPES Bloc 2

Antoine Boivin

7 septembre 2026

Table des matières

Chapitre 1

Dénombrement et probabilités sur un univers fini

1.1 Dénombrement

1.1.1 Injection, surjection, bijection

Définition 1.1.1.1. Soient X, Y deux ensembles et $f\colon X \to Y$ une fonction. On dit que f est injective (ou est une injection) si

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

Exercice 1. Soient X, Y deux ensembles et $f\colon X \to Y$ une fonction. Montrer qu'une fonction est injective si, et seulement si, pour tout $y \in Y$, l'ensemble $f^{-1}(y)$ contient au plus un élément.

Exemple 1.1.1.2.

— La fonction $x \in \mathbb{R} \mapsto x^2 \in \mathbb{R}$ n'est pas injective ($1^2 = (-1)^2$) mais $x \in \mathbb{R}_{\geq 0} \mapsto x^2 \in \mathbb{R}$ l'est.

— Si $A \subset X$ alors la fonction (dite d'inclusion) $x \in A \mapsto x \in X$ est injective.

— Une fonction strictement monotone $\mathbb{R} \to \mathbb{R}$ est injective.

— La restriction d'une fonction injective est injective.

Exercice 2. Montrer qu'une fonction $f\colon X \to Y$ est injective si, et seulement si, pour tout $A \subset X$, $f^{-1}(f(A)) = A$.

Définition 1.1.1.3. Soient X, Y deux ensembles et $f\colon X \to Y$ une fonction. On dit que f est surjective (ou est une surjection) si

$$\forall y \in Y, \exists x \in X, y = f(x).$$

Exercice 3. Soient X, Y deux ensembles et $f\colon X \to Y$ une fonction. Montrer qu'une fonction est surjective si, et seulement si, pour tout $y \in Y$, l'ensemble $f^{-1}(y)$ contient au moins un élément.

Exemple 1.1.1.4.

— La fonction $x \in \mathbb{R} \mapsto x^2 \in \mathbb{R}$ n'est pas surjective (aucun réel n'est envoyé sur -1 par positivité) mais $x \in \mathbb{R} \mapsto x^2 \in \mathbb{R}_{\geq 0}$ l'est (par le TVI).

— Si $n \in \mathbb{N}_{\geq 2}$ alors la fonction $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto x + n\mathbb{Z}$ est surjective.

— Une fonction polynomiale $\mathbb{R} \to \mathbb{R}$ de degré impaire est surjective.

— La restriction d'une fonction surjective n'est pas nécessairement surjective (il suffit de réduire le domaine de la fonction carré à un unique point).

— Si $f\colon X \to Y$ est une fonction alors sa corestriction $f^{|f(X)}\colon X \to f(X)$ est une surjection.

— Si X, Y sont deux ensembles non-vides, les fonctions de projection $(x, y) \in X \times Y \mapsto x \in X$ et $(x, y) \in X \times Y \mapsto y \in Y$ sont surjectives.

Exercice 4. Montrer qu'une fonction $f\colon X \to Y$ est injective si, et seulement si, pour tout $B \subset Y$, $f(f^{-1}(B)) = B$.

Définition 1.1.1.5. Soient X, Y deux ensembles et $f\colon X \to Y$ une fonction. On dit que f est bijective (ou est une bijection) si elle est injective et surjective.

Exercice 5. Soient X, Y deux ensembles et $f\colon X \to Y$ une fonction. Montrer qu'une fonction est bijective si, et seulement si, pour tout $y \in Y$, l'ensemble $f^{-1}(y)$ contient exactement un élément.

Exemple 1.1.1.6.

1. La fonction $x \in \mathbb{R}_{\geq 0} \mapsto x^2 \in \mathbb{R}_{\geq 0}$ est bijective.
2. Les fonctions $\ln\colon]0, +\infty[\to \mathbb{R}$ et $\exp\colon \mathbb{R} \to]0, +\infty[$ sont des bijections.
3. Si n et m sont premiers entre eux alors $\mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, x + nm\mathbb{Z} \mapsto (x + n\mathbb{Z}, x + m\mathbb{Z})$ est une bijection (par le théorème des restes chinois).
4. La fonction $\mathbb{N} \to \mathbb{N}_{\geq 1}, n \mapsto n + 1$ est une bijection.
5. Si $f\colon X \to Y$ est une fonction injective alors sa corestriction $f^{|f(X)}\colon X \to f(X)$ est une bijection.

Exercice 6. Montrer que la fonction $\mathbb{N}^2 \to \mathbb{N}_{\geq 1}, (n, p) \mapsto 2^n(2p + 1)$ est une bijection.

Exercice 7. Montrer qu'une fonction $f\colon X \to Y$ est bijective si, et seulement si, il existe une fonction $g\colon Y \to X$ telle que $g \circ f = \mathrm{Id}_X$ et $f \circ g = \mathrm{Id}_Y$. Montrer que dans ce cas cette fonction g est unique (c'est la bijection réciproque de f).

Proposition 1.1.1.7. *Soient X, Y, Z trois ensembles et $f\colon X \to Y$, $g\colon Y \to Z$ deux fonctions. Alors*

1. *si f et g sont injectives alors $g \circ f$ est injective ;*
2. *si f et g sont surjectives alors $g \circ f$ est surjective ;*
3. *si f et g sont bijectives alors $g \circ f$ est bijective.*

Démonstration. 1) Supposons f et g injectives. Soient $x, x' \in X$ tels que $g \circ f(x) = g \circ f(x')$. Comme g est injective alors $f(x) = f(x')$. Et comme f est injective, on obtient $x = x'$ et donc que $g \circ f$ est injective.

2) Supposons f et g surjectives. Soit $z \in Z$. Comme g est surjective alors il existe $y \in Y$ tel que $z = g(y)$. Fixons un tel y. Comme f est surjective alors il existe $x \in X$ tel que $y = f(x)$. Pour un tel x, on a :

$$g \circ f(x) = g(y) = z.$$

On en déduit que $g \circ f$ est surjective.

3) Si f et g sont bijectives alors en particulier, elles sont injectives et surjectives. Par les points précédents, $g \circ f$ est injective et surjective et est donc bijective. □

Exercice 8. Soient X, Y, Z trois ensembles et $f\colon X \to Y$, $g\colon Y \to Z$ deux fonctions bijectives. Déterminer la bijection réciproque de $g \circ f$.

Exercice 9. Soient W, X, Y, Z quatre ensembles, et $f\colon W \to X$, $g\colon X \to Y$ et $h\colon Y \to Z$.

1. Montrer que si $g \circ f$ est injective alors f est injective.
2. Montrer que si $g \circ f$ est surjective alors f est surjective.
3. Montrer que $g \circ f$ et $h \circ g$ sont bijectives si, et seulement si, f, g et h sont bijectives.

Exercice 10. Soient X, Y, Z trois ensembles, et $f\colon X \to Y$ et $g\colon Y \to Z$ deux fonctions. Posons $h := g \circ f$.

1. On suppose h injective et f surjective. Montrer que g est injective.
2. On suppose h surjective et g injective. Montrer que h est surjective.

Théorème 1.1.1.8 (Cantor-Bernstein)**.** *Soient X, Y deux ensembles. S'il existe une injection $X \to Y$ et une injection $Y \to X$ alors il existe une bijection $X \to Y$.*

Exercice 11. Montrer que $[0, 1]$ et $[0, 1[$ sont en bijection.

Exercice 12. Montrer que l'ensemble $\mathbb{R}$ et l'ensemble des parties de $\mathbb{N}$ sont en bijection.

1.1.2 Ensembles finis

Notation 1.1.2.1. On pose $E_0 \coloneqq \emptyset$ et pour $n \in \mathbb{N}_{\geq 1}$, $E_n \coloneqq \{1, \dots, n\} = \{k \mid 1 \leq k \leq n\}$.

Proposition 1.1.2.2. *Soient* $m, n \in \mathbb{N}$.

1. *S'il existe une fonction injective* $E_m \to E_n$ *alors* $m \leq n$ *;*
2. *S'il existe une fonction surjective* $E_m \to E_n$ *alors* $m \geq n$ *;*
3. *S'il existe une fonction bijective* $E_m \to E_n$ *alors* $m = n$ *;*

Démonstration. 1) Supposons qu'il existe une fonction injective $E_m \to E_n$. Soit f une telle fonction.
Notons $i_1, \dots, i_m$ les éléments (qui sont tous distincts par injectivité) de $f(E_m)$ où $i_1 < i_2 < \dots < i_m$[1]. On peut remarquer que $i_m \geq m$ (car pour $k \in E_m \setminus \{1\}$, $i_k \geq i_{k-1} + 1$ et $i_1 \geq 1$). De plus, par définition, $i_m \leq n$. On en déduit que $m \leq n$.

2) Supposons qu'il existe une fonction surjective $E_m \to E_n$. Soit f une telle fonction.
Soient $i_1, \dots, i_n \in E_m$ tels que $\forall k \in E_n, f(i_k) = k$. Comme les $(i_k)_{k \in E_n}$ sont tous distincts, on en déduit de la même façon que dans 1) que $n \leq \max(i_k) \leq m$.

3) Supposons qu'il existe une fonction bijective $E_m \to E_n$. En particulier, il existe une fonction injective et une fonction surjective. Par les deux points précédents, $m \leq n$ et $n \leq m$ et donc $m = n$. □

Exercice 13. Énoncer les contraposées de ces énoncés.

Proposition 1.1.2.3. *Soient* $n \in \mathbb{N}_{\geq 1}$ *et* $f \colon E_n \to E_n$ *une fonction. Les assertions suivantes sont équivalentes :*

1. f *est injective ;* 2. f *est surjective ;* 3. f *est bijective.*

Démonstration. Nous allons montrer l'équivalence entre les point 1 et 3. Par définition, si f est bijective alors f est injective.
Supposons f injective. Supposons par l'absurde que f n'est pas surjective. Soit $k \notin f(E_n)$. On définit la fonction

$$\pi_k \colon j \in E_n \mapsto \begin{cases} j & \text{si } j \leq k \\ j-1 & \text{si } j > k \end{cases} \in E_{n-1}$$

Comme $k \notin f(E_n)$ alors la fonction $\pi_k \circ f : E_n \to E_{n-1}$ est toujours injective. Par la proposition précédente, on en déduit que $n \leq n-1$, ce qui est absurde. □

Remarque 1.1.2.4. Si $n = 0$, la fonction est trivialement injective, surjective et bijective.

Exercice 14. En reprenant la démonstration, montrer l'équivalence entre le point 2 et le point 3.

Définition 1.1.2.5. On dit qu'un ensemble X est fini s'il existe un entier $n \in \mathbb{N}$ et une bijection $X \to E_n$.

Exercice 15. Montrer que les ensembles suivants sont finis :

— $\{\diamondsuit, \spadesuit, \clubsuit, \heartsuit\}$; — $\{1, 3, 5, 9, 11\}$; — $\{2k+1 \mid -3 \leq k \leq 9\}$.

Proposition 1.1.2.6. *Le* n *de la définition précédente, s'il existe, est unique.*

Démonstration. Soient $n, m \in \mathbb{N}$ et deux bijections $\varphi \colon X \to E_n$ et $\psi \colon X \to E_m$. Alors $\psi \circ \varphi^{-1} \colon E_n \to E_m$ est une bijection et donc $n = m$. □

Remarque 1.1.2.7. La bijection n'a aucune raison d'être unique.

Définition 1.1.2.8. On appelle cet entier cardinal de l'ensemble X. On le note $\mathrm{Card}(X), \sharp X, |X|$.

Proposition 1.1.2.9. *Soient* X, Y *deux ensembles et* $f \colon X \to Y$ *une fonction.*

1. *Si* Y *est fini et* f *est une injection alors* X *est fini et* $|X| \leq |Y|$.
2. *Si* X *est fini et* f *est une surjection alors* Y *est fini et* $|X| \geq |Y|$.
3. *Si* f *est une bijection alors* X *est fini si, et seulement si,* Y *est fini. De plus,* $|X| = |Y|$.

1. on le fait par induction : $i_1 \coloneqq \min f(E_m)$, $i_2 \coloneqq \min(f(E_m) \setminus \{i_1\})$ et ainsi de suite.

Démonstration. 1) Supposons que Y est fini (considérons $\varphi\colon Y \to E_{|Y|}$ une bijection) et que f est une injection. Posons $g \coloneqq \varphi \circ f\colon X \to E_{|Y|}$. C'est aussi une injection. La corestriction $g^{|g(X)}\colon X \to g(X)$ est une bijection. Soient $i_1, \dots, i_k$ les éléments de $g(X) \subset E_{|Y|}$ (on a $k \leq |Y|$). On obtient ainsi une bijection $i\colon E_k \to g(X)$ définie par $k \mapsto i_k$ et donc une bijection $i^{-1} \circ g^{|g(X)}\colon X \to E_k$. On en déduit que X est fini et de cardinal $|X| = k \leq |Y|$.

2) Supposons que X est fini (considérons $\psi\colon X \to E_{|X|}$ une bijection) et que f est une surjection. Alors $f \circ \psi^{-1}\colon E_{|X|} \to Y$ est une surjection. Pour chaque $y \in Y$, on choisit un antécédent $e_y \in E_{|X|}$. Ainsi, on a une bijection $e\colon Y \to \{e_y \mid y \in Y\}$ définie par $y \mapsto e_y$.

Soient $i_1, \dots, i_k \in E_{|X|}$ (ainsi $k \leq |X|$) tels que $i_1 < i_2 < \dots < i_k$ et $\{i_1, \dots, i_k\} = \{e_y \mid y \in Y\}$ (on a ordonné l'ensemble des e_y). On obtient ainsi une bijection $a\colon E_k \to \{e_y \mid y \in Y\}$ définie par $j \mapsto i_j$ et donc une bijection $a^{-1} \circ e\colon Y \to E_k$. On en déduit que Y est fini et $|Y| = k \leq |X|$.

3) On utilise les points précédents avec f et f^{-1} pour montrer le résultat. □

Proposition 1.1.2.10 (Principe des tiroirs)**.** *Soient X, Y deux ensembles. Si $|X| > |Y|$ alors il n'existe pas d'injection $X \to Y$.*

Démonstration. C'est la contraposée de 1.1.2.2. □

Exercice 16.

1. Montrer qu'il existe deux personnes en France qui ont exactement le même nombre de cheveux.
2. Montrer que, dans un groupe d'au moins deux personnes, il existe toujours deux personnes possédant le même nombre d'amis dans ce groupe.
3. Montrer que parmi 101 nombres entiers distincts, il existe toujours onze d'entre eux dont la somme est divisible par 11
4. On choisit dix nombres entre 1 et 100. Montrer qu'il existe deux sous-ensembles disjoints non vides de ces dix nombres ayant la même somme.
5. Soient $n > 1$ et E un ensemble d'au moins $n + 1$ nombres entiers différents. Montrer qu'il existe deux nombres différents dans E dont la différence est divisible par n.

Exercice 17. Soient X, Y deux ensembles finis de même cardinal et $f\colon X \to Y$ une fonction. Montrer que les assertions suivantes sont équivalentes :

1. f est injective ; 2. f est surjective ; 3. f est bijective.

Proposition 1.1.2.11. *Soient X, Y deux ensembles finis. Alors $X \cup Y$ et $X \cap Y$ sont finis et*

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

Démonstration. — Supposons que $X \cap Y = \emptyset$. Soient $\varphi\colon X \to E_{|X|}$ et $\psi\colon X \to E_{|Y|}$ deux bijections. On définit la fonction $f\colon E_{|X|+|Y|} \to X \cup Y$ par

$$\forall j \in E_{|X|+|Y|}, f(j) \coloneqq \begin{cases} \varphi^{-1}(j) \text{ si } j \leq |X| \\ \psi^{-1}(j - |X|) \text{ si } j > |X| \end{cases}$$

Comme X et Y sont disjoints et que φ^{-1} et ψ^{-1} sont injectives alors f est injective. Montrons que f est surjective. Soit $x \in X \cup Y$. Si $x \in X$ alors $x = f(\varphi(x))$ et si $x \in Y$ alors $x = f(|X| + \psi(x))$. On en déduit que f est une bijection et que $|X \cup Y| = |X| + |Y|$.

— De la formule précédente, on en déduit que si $A \subset X$ alors $|X \setminus A| = |X| - |A|$. On a ensuite l'égalité $X \cup Y = (X \cap Y) \cup (X \setminus (X \cap Y)) \cup (Y \setminus (X \cap Y))$. Par construction, ces trois ensembles sont disjoints et donc[2]

$$\begin{aligned} |X \cup Y| &= |X \cap Y| + |X \setminus (X \cap Y)| + |Y \setminus (X \cap Y)| \\ &= |X \cap Y| + (|X| - |X \cap Y|) + (|Y| - |X \cap Y|) = |X| + |Y| - |X \cap Y|. \end{aligned}$$

□

Exercice 18. Existe-t-il deux ensembles A et B tels que $|A| = 42$, $B = |17|$ et $|C| = 1000$?

Exercice 19. Soient X, Y, Z trois ensembles. Déterminer $|X \cup Y \cup Z|$.

Exercice 20. Soient $(X_i)_{1 \leq i \leq n}$ n ensembles tels que $\forall i \neq j, X_i \cap X_j = \emptyset$. Montrer que

$$\left| \bigcup_{i=1}^{n} X_i \right| = \sum_{i=1}^{n} |X_i|.$$

2. on utilise deux fois l'égalité précédente

Exercice 21. Soient $(X_i)_{1\leq i\leq n}$ n ensembles. Montrer que

$$\left|\bigcup_{i=1}^{n} X_i\right| \leq \sum_{i=1}^{n} |X_i|.$$

Exercice 22. Soit $n \in \mathbb{N}$.

1. Combien y a-t-il de paires d'entiers naturels (x, y) tels que $x + y = n$?
2. Combien y a-t-il de paires d'entiers naturels (x, y) tels que $x < y \leq n$?
3. Combien y a-t-il de paires d'entiers naturels (x, y) tels que $x, y \leq n$ et $|x - y| \leq 1$?

Exercice 23 (Principe des tiroirs II)**.** Soit $f\colon X \to Y$ une fonction entre deux ensembles finis tels que $|X| > n|Y|$. Montrer qu'il existe $y \in Y$ tel que $f^{-1}(y) > n$.

Exercice 24. Combien de personnes faut-il pour être sûr que trois d'entre elles aient le même anniversaire ?

Proposition 1.1.2.12. *Soient X, Y deux ensembles finis. Alors $X \times Y$ est fini et*

$$|X \times Y| = |X||Y|.$$

Démonstration. Soient $\varphi\colon X \to E_{|X|}$ et $\psi\colon Y \to E_{|Y|}$ deux bijections. Comme $(\varphi, \psi)\colon X \times Y \to E_{|X|} \times E_{|Y|}, (x, y) \mapsto (\varphi(x), \psi(y))$ est une bijection alors il suffit de montrer que $E_{|X|} \times E_{|Y|}$ et $E_{|X||Y|}$ sont en bijection. Soit $f\colon E_{|X|} \times E_{|Y|} \to E_{|X||Y|}$ la fonction définie par :

$$\forall (k, \ell) \in E_{|X|} \times E_{|Y|}, f(k, l) \coloneqq k + (\ell - 1)|X|$$

On remarque que $f - 1\colon E_{|X|} \times E_{|Y|} \to \{0, \ldots, |X||Y| - 1\}$ est une écriture de la division euclidienne. Grâce à l'existence et l'unicité de celle-ci, on en déduit que $f - 1$ est une bijection et donc f aussi. □

Exercice 25. Soient X un ensemble fini et $n \in \mathbb{N}_{\geq 1}$. Calculer le cardinal de $|X^n|$. En déduire le cardinal $X^Y \coloneqq \{f\colon Y \to X\}$ où X et Y sont deux ensembles finis non-vides.

Exercice 26. Soit X un ensemble fini. Calculer le cardinal de $\mathcal{P}(X) \coloneqq \{E \subset X\}$.

Définition 1.1.2.13. Soient $n \in \mathbb{N}_{\geq 1}$ et X un ensemble fini. On appelle n-liste de X un élément de X^n.

Proposition 1.1.2.14 (Principe multiplicatif)**.** *Soient X et Y deux ensembles finis, $(\mathcal{P}(x))_{x\in X}$, $(\mathcal{Q}(x, y))_{x\in X, y\in Y}$ deux familles d'assertions. Supposons qu'il existe un entier naturel n tel que pour tous $x \in X, y \in Y$, si $\mathcal{P}(x)$ est vraie alors $|\{y \in Y \mid \mathcal{Q}(x, y)\}| = n$. Alors*

$$|\{(x, y) \in X \times Y \mid \mathcal{P}(x), \mathcal{Q}(x, y)\}| = n|\{x \in X \mid \mathcal{P}(x)\}|.$$

Démonstration. On a

$$\{(x, y) \in X \times Y \mid \mathcal{P}(x), \mathcal{Q}(x, y)\} = \bigcup_{x \text{ tq } \mathcal{P}(x)} \{y \in Y \mid \mathcal{Q}(x, y)\}$$

et donc comme les ensembles $\{(x, y) \in X \times Y \mid \mathcal{Q}(x, y)\}$ sont disjoints, on a :

$$|\{(x, y) \in X \times Y \mid \mathcal{P}(x), \mathcal{Q}(x, y)\}| = \sum_{x \text{ tq } \mathcal{P}(x)} \{(x, y) \in X \times Y \mid \mathcal{Q}(x, y)\}.$$

On en déduit que

$$|\{(x, y) \in X \times Y \mid \mathcal{P}(x), \mathcal{Q}(x, y)\}| = \sum_{x \text{ tq } \mathcal{P}(x)} n = n|\{x \in X \mid \mathcal{P}(x)\}.$$

□

Remarque 1.1.2.15. On peut donner un énoncé avec un nombre quelconque d'ensembles mais cela alourdirait significativement l'écriture.

Exercice 27. Un cadenas possède un code à 3 chiffres (allant de 0 à 9)

1. Combien de codes différents sont possibles en tout ?
2. Combien de codes contiennent au moins un chiffre 7 ?

Exercice 28.

1. Un code est composé de quatre chiffres suivis d'une lettre (de l'alphabet latin). Combien y a-t-il de possibilités de combinaisons ?
2. Même question mais la lettre n'est plus nécessairement à la fin du code.

Exercice 29. Une plaque d'immatriculation française comporte deux lettres, puis trois chiffres, puis deux lettres. Les lettres "O", "I" et "U" sont exclues (pour éviter la confusion avec "0", "1"et "V"). Combien de plaques différentes sont possibles ?

1.1.3 Permutations, arrangements, combinaisons

1.1.3.1 Permutations

Définition 1.1.3.1. Soit $n \in \mathbb{N}$. Une permutation de n objets est une bijection $E_n \to E_n$. On note $\mathfrak{S}_n$ (ou S_n, Σ_n) l'ensemble des permutations.

Exercice 30. Montrer que si X et Y sont de cardinal n alors l'ensemble des bijections de X dans Y est en bijection avec $\mathfrak{S}_n$.

Théorème 1.1.3.2. *Soit $n \in \mathbb{N}$. Le cardinal de $\mathfrak{S}_n$ est $n!$ où $0! \coloneqq 1$ et pour tout $n \in \mathbb{N}$, $(n+1)! \coloneqq (n+1)n!$.*

Démonstration. On remarque tout d'abord que

$$\mathfrak{S}_n = \bigcup_{k=1}^{n} \underbrace{\{\sigma \in \mathfrak{S}_n \mid \sigma(n) = k\}}_{=:A_{k,n}}.$$

Comme les $A_{k,n}$ sont disjoints alors

$$|\mathfrak{S}_n| = \sum_{k=1}^{n} |A_{k,n}|.$$

On remarque ensuite que si $\sigma \in \mathfrak{S}_n$ alors la restriction-corestriction $\sigma_{E_{n-1}}^{E_n \setminus \{\sigma(n)\}}$ est aussi une bijection. On en déduit que $A_{k,n}$ est en bijection avec l'ensemble des bijections $E_{n-1} \to E_n \setminus \{k\}$. On en déduit ainsi que $|A_{k,n}| = |\mathfrak{S}_{n-1}|$ et donc

$$|\mathfrak{S}_n| = n|\mathfrak{S}_{n-1}|$$

Comme $|\mathfrak{S}_0| = |\{\emptyset \to \emptyset\}| = 1$ alors on en conclut que $|\mathfrak{S}_n| = n!$.

□

Exercice 31.

1. Combien y-a-t-il d'anagrammes (on ne demande pas que les mots obtenues aient du sens) au mot "PROBA" ?
2. Combien y-a-t-il d'anagrammes commençant par la lettre "B" ?
3. Combien y-a-t-il d'anagrammes commençant par une consonne ?

Exercice 32. Trois groupes de personnes (constitué, respectivement, de quatre, six et huit personnes) arrivent dans un restaurant. Chaque groupe est dirigé vers une table avec exactement le bon nombre de places. Combien y a-t-il de plans de table possibles ?

1.1.3.2 Arrangements et Combinaisons

Définition 1.1.3.3. Soient X un ensemble fini et $p \in \mathbb{N}_{\geq 1}$. Un arrangement de p éléments de X est une p-liste d'éléments distincts de X

Remarque 1.1.3.4. Un arrangement de $|X|$ éléments de X définit une bijection de X.

Exercice 33. Montrer que l'ensemble des arrangements de p éléments de X est en bijection avec l'ensemble des injections $E_p \to X$ (que l'on note $\mathrm{Inj}(E_p, X)$)

Proposition 1.1.3.5. *Soient $p, n \in \mathbb{N}$ avec $n \geq p$. Il y a $\frac{n!}{(n-p)!}$ arrangements de p éléments de E_n.*

Démonstration. Considérons la fonction res: $\mathfrak{S}_n \to \mathrm{Inj}(E_p, E_n)$ définie par $\sigma \mapsto \sigma_{|E_p}$. On remarque que pour tout $i \in \mathrm{Inj}(E_p, E_n)$, l'image réciproque de i par res s'écrit :

$$\mathrm{res}^{-1}(i) = \{\sigma \in \mathfrak{S}_n \mid \forall j \in E_p, \sigma(j) = i(j)\}$$

On en déduit que cet ensemble est en bijection avec l'ensemble des bijections $E_n \setminus E_p \to E_n \setminus i(E_p)$ par restriction-corestriction. On en déduit que $|\mathrm{res}^{-1}(i)| = (n-p)!$. De plus,

$$\mathfrak{S}_n = \bigcup_{i \in \mathrm{Inj}(E_p, E_n)} \mathrm{res}^{-1}(i)$$

et donc, comme les images réciproques sont disjointes,

$$n! = |\mathfrak{S}_n| = \sum_{i \in \mathrm{Inj}(E_p, E_n)} |\mathrm{res}^{-1}(i)| = \sum_{i \in \mathrm{Inj}(E_p, E_n)} (n-p)! = (n-p)!|\mathrm{Inj}(E_p, E_n)|,$$

ce qui permet de conclure. □

Définition 1.1.3.6. On note cet entier A_n^p.

Exercice 34. Combien y a-t-il de nombres à 8 chiffres contenant aucun "1" et dont tous les chiffres sont distincts ?

Exercice 35. Dans une course de Formule 1, il y a vingt pilotes. Combien de podiums (premier, deuxième, troisième) différents sont possibles ?

Définition 1.1.3.7. Soient X un ensemble fini et $p \in \mathbb{N}$, $p \leq |X|$. Un combinaison de p éléments de X est une partie de X à p éléments.

Remarque 1.1.3.8. La différence entre arrangement et combinaison réside dans le fait d'un arrangement est une partie **ordonnée** d'éléments de X.

Proposition 1.1.3.9. *Soient* $p, n \in \mathbb{N}$ *avec* $n \geq p$. *Il y a* $\frac{n!}{(n-p)!p!}$ *combinaisons de* p *éléments de* E_n.

Démonstration. On considère la fonction Im: $\mathrm{Inj}(E_p, E_n) \to \mathscr{P}_p(n) \coloneqq \{E \in \mathscr{P}(E_n) \mid |E| = p\}$ définie par $i \mapsto i(E_p)$. Pour chaque $E \in \mathscr{P}_k(n)$, l'image réciproque de E est l'ensemble des injections $E_p \to E_n$ d'image E qui est donc par corestriction en bijection avec l'ensemble des bijections $E_p \to E$ et est donc de cardinal $p!$. Ainsi, comme

$$\mathrm{Inj}(E_p, E_n) = \bigcup_{E \in \mathscr{P}_p(n)} \mathrm{Im}^{-1}(E)$$

et que les images réciproques sont disjointes :

$$\frac{n!}{(n-p)!} = |\mathrm{Inj}(E_p, E_n)| = \sum_{E \in \mathscr{P}_p(n)} |\mathrm{Im}^{-1}(E)| = \sum_{E \in \mathscr{P}_p(n)} p! = |\mathscr{P}_p(n)|p!,$$

ce qui permet de trouver le résultat. □

Notation 1.1.3.10. On note $\binom{n}{k}$ (ou C_n^k) le nombre de combinaisons de k éléments dans E_n.

Proposition 1.1.3.11. *Soient* $k, n \in \mathbb{N}_{\geq 1}$ *tels que* $n \geq k$. *Alors*

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

Démonstration. On a les égalités suivantes :

$$\begin{aligned}\mathscr{P}_k(n+1) &= \{E \in \mathscr{P}_k(n+1) \mid n+1 \in E\} \cup \{E \in \mathscr{P}_k(n+1) \mid n+1 \notin E\} \\ &= \{E \in \mathscr{P}_k(n+1) \mid n+1 \in E\} \cup \mathscr{P}_k(n).\end{aligned}$$

L'ensemble $\{E \in \mathscr{P}_k(n+1) \mid n+1 \in E\}$ est en bijection avec $\mathscr{P}_{k-1}(n)$ par la fonction $E \mapsto E \cap E_n$ (d'inverse $F \mapsto F \cup \{n+1\}$). On en déduit donc que

$$\begin{aligned}\binom{n+1}{k} = |\mathscr{P}_k(n+1)| &= |\{E \in \mathscr{P}_k(n+1) \mid n+1 \in E\}| + |\mathscr{P}_k(n)| \\ &= |\mathscr{P}_{k-1}(n)| + |\mathscr{P}_k(n)| = \binom{n}{k-1} + \binom{n}{k}.\end{aligned}$$

□

Exercice 36. Retrouver ce résultat par calcul.

Exercice 37. Dénombrer les anagrammes des mots suivants : "PIZZA", "PROBABILITES", "PEPITE".

Exercice 38. Une main au poker est formée de 5 cartes extraites d'un jeu de 52 cartes. Traditionnellement,trèfle, carreau, coeur, pique sont appelées couleurs et les valeurs des cartes sont rangées dans l'ordre : as, roi, dame, valet, 10, 9, 8, 7, 6, 5, 4, 3, 2, de la plus forte à la plus faible. Dénombrer les mains suivantes :

1. quinte flush : main formée de 5 cartes consécutives de la même couleur (ici, la suite as, 2, 3, 4 et 5 est une quinte flush).
2. carré : main contenant 4 cartes de la même valeur (quatre as par exemple).
3. full : main formée de trois cartes de la même valeur et de deux autres cartes de même valeur (par exemple, trois as et deux rois).
4. suite : main formée de 5 cartes consécutives et qui ne sont pas toutes de la même couleur.
5. brelan : main comprenant trois cartes de même valeur et qui n'est ni un carré, ni un full (par exemple, trois as, un valet, un dix).

Exercice 39. Déterminer le nombre de diagonales d'un polygône à n côtés.

Exercice 40. Soient $n, k \in \mathbb{N}_{\geq 1}$ deux entiers naturels.

1. Déterminer le nombre de k-uplets $(x_1, \ldots, x_k)$ d'entiers naturels non-nuls tels que $x_1 + \ldots + x_k = n$.
2. Déterminer le nombre de k-uplets $(x_1, \ldots, x_k)$ d'entiers naturels tels que $x_1 + \ldots + x_k = n$.

Exercice 41. Montrer combinatoirement les égalités suivantes :

1. $\forall k, n \in \mathbb{N}, k \leq n, \binom{n}{k} = \binom{n}{n-k}$;
2. $2^n = \sum_{k=0}^{n} \binom{n}{k}$;
3. $\forall k, n \in \mathbb{N}_{\geq 1}, k \leq n, k\binom{n}{k} = n\binom{n-1}{k-1}$ et en déduire $\sum_{k=1}^{n} k\binom{n}{k}$;
4. Déduire du premier point que $\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$.

Proposition 1.1.3.12. *Soit A un anneau commutatif (par exemple, $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$). Soient $a, b \in A$ et $n \in \mathbb{N}$. Alors*

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

Démonstration. On montre ce résultat par récurrence sur n :

— pour $n = 0$, $(a+b)^0 = 1 = \sum_{k=0}^{0} \binom{n}{k} a^k b^{0-k}$

— Soit $n \in \mathbb{N}$ et supposons la propriété vraie au rang n. Alors

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \overset{HR}{=} (a+b) \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1} \\
&\overset{\text{chgt de var}}{=} \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n-k+1} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1} \\
&= a^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k b^{n-k+1} + b^{n+1} \\
&= a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n-k+1} + b^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}
\end{aligned}$$

□

Exercice 42. Retrouver ce résultat par un argument combinatoire.

1.2 Probabilités sur un univers fini

1.2.1 Espaces probabilisés

1.2.1.1 Premières définitions

Définition 1.2.1.1. Un espace probabilisé fini est un couple (Ω, p) où Ω est un ensemble fini et $p\colon \Omega \to [0,1]$ une fonction telle que

$$\sum_{\omega\in\Omega} p(\omega) = 1.$$

On appelle Ω *univers* et une telle fonction est appelée *germe de probabilité sur* Ω.

Exemple 1.2.1.2. Soit $f \in \{2,4,6,8,10,12,20,100\}$. Pour modéliser le lancer d'un dé équilibré à f faces[3], on peut poser $\Omega \coloneqq \{1,\dots,f\}$ et définir p par :

$$\forall \omega \in \Omega, p(\omega) \coloneqq \frac{1}{f}.$$

On a bien $\sum_{\omega\in\Omega} p(\omega) = 1$.

Toutes les issues ont la même probabilité, on dit alors qu'elles sont équiprobables.

Exemple 1.2.1.3. Dans le cas où on veut modéliser $d \geq 1$ lancers de dés équilibrés à f faces, on peut poser $\Omega \coloneqq \{1,\dots,f\}^d$ et définir p par :

$$\forall \omega \in \Omega, p(\omega) \coloneqq \frac{1}{f^d}.$$

Exemple 1.2.1.4. Pour modéliser une urne avec des boules ayant V boules vertes et R boules rouges, on peut prendre $\Omega \coloneqq \{v, r\}$ et définir p par :

$$p(v) \coloneqq \frac{1}{V} \text{ et } p(r) \coloneqq \frac{1}{R}$$

Définition 1.2.1.5. Soit (Ω, p) un espace probabilisé fini. On appelle *événement* une partie de Ω.

Exercice 43. Soit Ω un ensemble fini et soient A, B, C trois événements de Ω. Traduire en termes ensemblistes (en utilisant uniquement les symboles d'union, d'intersection et de passage au complémentaire, ainsi que A, B et C) les événements suivants :

1. Seul A se réalise ;
2. A et B se réalisent, mais pas C.
3. les trois événements se réalisent ;
4. au moins l'un des trois événements se réalise ;
5. au moins deux des trois événements se réalisent ;
6. aucun ne se réalise ;
7. au plus l'un des trois se réalise ;
8. exactement deux des trois se réalisent ;

Définition 1.2.1.6. Soit (Ω, p) un espace probabilité fini. La *mesure de probabilité de germe* p est la fonction $\mathbb{P}\colon \mathscr{P}(\Omega) \to [0,1]$ définie par

$$\forall A \in \mathscr{P}(\Omega), \mathbb{P}(A) \coloneqq \sum_{\omega\in A} p(\omega).$$

Exemple 1.2.1.7. Dans le cas équiprobable,

$$\forall B \in \mathscr{P}(\Omega), \mathbb{P}(B) = \frac{|B|}{|\Omega|}.$$

Proposition 1.2.1.8. *Soit Ω un ensemble fini. La fonction qui associe à un germe de probabilité sur Ω sa mesure de probabilité est une bijection entre l'ensemble des fonctions $p\colon \Omega \to [0,1]$ vérifiant $\sum_{\omega\in\Omega} p(\omega) = 1$ et l'ensemble des fonctions $\mathbb{P}\colon \mathscr{P}(\Omega) \to [0,1]$ vérifiant*

3. notons que le lancer d'un dé à deux faces est équivalent à un lancer de pièce

— $\mathbb{P}(\Omega) = 1$;

— *Si* $A_1, \dots, A_n$ *sont des parties disjointes de* Ω *(i.e. pour tout* $i \neq j$, $A_i \cap A_j = \emptyset$*) alors*

$$\mathbb{P}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} \mathbb{P}(A_i).$$

Démonstration. On vérifie tout d'abord que la fonction $\mathbb{P}$ obtenue vérifie bien les conditions désirées :

— $\mathbb{P}(\Omega) = \sum_{\omega\in\Omega} p(\omega) = 1$;

— Soient $A_1, \dots, A_n$ des parties disjointes de Ω. Alors

$$\mathbb{P}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{\omega\in\bigcup_{i=1}^{n} A_i} p(\omega) = \sum_{i=1}^{n} \sum_{\omega\in A_i} p(\omega) = \sum_{i=1}^{n} \mathbb{P}(A_i)$$

(la deuxième égalité vient du fait que les parties sont disjointes)
On remarque ensuite que l'on retrouve la fonction p en posant

$$\forall \omega \in \Omega, p(\omega) \coloneqq \mathbb{P}(\{\omega\})$$

fournissant ainsi la bijection réciproque (car les fonctions $\mathbb{P}$ vérifient $\mathbb{P}(A) = \sum_{\omega\in A} \mathbb{P}(\{\omega\})$).

□

Remarque 1.2.1.9. Autrement dit, la donnée du germe ou la donnée de la mesure de probabilité associée sont équivalentes. On écrira de façon interchangeable (Ω, p) ou $(\Omega, \mathbb{P})$.

Proposition 1.2.1.10. *Soit* $(\Omega, \mathbb{P})$ *un espace probabilisé fini. Soient* A, B *deux événements. Alors*

1. *Si* $A \subset B$ *alors* $\mathbb{P}(B \setminus A) = \mathbb{P}(B) - \mathbb{P}(A)$. *En particulier,* $\mathbb{P}(A) \leq \mathbb{P}(B)$
2. $\mathbb{P}(A^c) = 1 - \mathbb{P}(A)$;
3. $\mathbb{P}(\emptyset) = 0$;
4. $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$.

Démonstration.
1. Comme $B \setminus A$ et A sont disjoints alors $\mathbb{P}(B) = \mathbb{P}(A \cup (B \setminus A)) = \mathbb{P}(A) + \mathbb{P}(B \setminus A)$. La deuxième partie vient de la positivité de la mesure de probabilité ;
2. Par le point précédent, en prenant $B = \Omega$;
3. Par le premier point, on a : $\mathbb{P}(\emptyset) = \mathbb{P}(A \setminus A) = \mathbb{P}(A) - \mathbb{P}(A) = 0$;
4. Se fait comme 1.1.2.11.

□

Exercice 44. Soit $n \geq 1$. On lance n fois un dé à six faces parfaitement équilibré. Quelle est la probabilité d'obtenir

1. au moins une fois le chiffre 6 ?
2. au moins deux fois le chiffre 6 ?
3. au moins $k \in \{0, \dots, n\}$ fois le chiffre 6 ?

Exercice 45. On jette 3 fois un dé à 4 faces, et on note a, b et c les résultats successifs obtenus. On pose $Q \coloneqq aX^2 + bX + c$. Déterminer la probabilité pour que :

— Q ait deux racines réelles distinctes ;

— Q ait une racine réelle double ;

— Q n'ait pas de racines réelles.

Exercice 46. Donner la probabilité pour que, dans une assemblée de n personnes, deux au moins aient la même date d'anniversaire. Faire le calcul numérique lorsque $n = 23$.

Exercice 47. On dispose d'un dé pipé à huit faces tel que la probabilité d'obtenir la face k soit k fois celle d'obtenir 1.

1. Donner un espace probabilisé modélisant l'expérience aléatoire. *On pourra se demander quelle est la probabilité de faire* 1.
2. Quelle est la probabilité d'obtenir un chiffre pair ? premier ?

1.2.1.2 Probabilités conditionnelles

Définition 1.2.1.11. Soient $(\Omega, \mathbb{P})$ un espace probabilisé fini et A un événement tels que $\mathbb{P}(A) \neq 0$. Pour tout événement B, la probabilité conditionnelle de B sachant A, noté $\mathbb{P}(B \mid A)$, est définie par :

$$\mathbb{P}(B \mid A) \coloneqq \frac{\mathbb{P}(B \cap A)}{\mathbb{P}(A)}$$

Lemme 1.2.1.12. *Soient $(\Omega, \mathbb{P})$ un espace probabilisé fini et A un événement tel que $\mathbb{P}(A) \neq 0$. Alors $\mathbb{P}(\cdot \mid A)$ est une mesure de probabilité dont la germe associée $p_A : \Omega \to \mathbb{R}$ est*

$$\forall \omega \in \Omega, p_A(\omega) \coloneqq \begin{cases} \frac{\mathbb{P}(\{\omega\})}{\mathbb{P}(A)} & \text{si } \omega \in A \\ 0 & \text{sinon.} \end{cases}$$

Démonstration. On remarque que la fonction p_A vérifie

$$\sum_{\omega \in \Omega} p_A(\omega) = \sum_{\omega \in A} p_A(\omega) = \sum_{\omega \in A} \frac{P(\{\omega\})}{\mathbb{P}(A)} = \frac{P(A)}{P(A)} = 1.$$

De plus,

$$\forall B \in \mathscr{P}(\Omega), \sum_{\omega \in B} p_A(\omega) = \sum_{\omega \in B \cap A} p_A(\omega) = \sum_{\omega \in B \cap A} \frac{\mathbb{P}(\{\omega\})}{\mathbb{P}(A)} = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(A)} = \mathbb{P}(B \mid A).$$

La proposition 1.2.1.8 permet de conclure. □

Remarque 1.2.1.13. Une conséquence de ce résultat est que la restriction sur les parties de A d'une situation d'équiprobabilité sachant A est une situation d'équiprobabilité sur A.

Définition 1.2.1.14. Soient $(\Omega, \mathbb{P})$ un espace probabilisé et A, B deux événements. On dit que A et B sont *indépendants* si $\mathbb{P}(B \mid A) = P(B)$, ce qui est équivalent à $\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B)$.

Exercice 48. Soient A, B deux événements indépendants. Montrer que A^c et B sont indépendants. En déduire que A et B^c, et A^c et B^c sont indépendants.

Exercice 49.

1. Une urne contient 12 boules numérotées de 1 à 12. On en tire une hasard, et on considère les événements

   $$A = \text{"tirage d'un nombre pair"},$$

   $$B = \text{"tirage d'un multiple de 3"}.$$

   Les événements A et B sont-ils indépendants ?
2. Reprendre la question avec une urne contenant 13 boules.

Définition 1.2.1.15. Une famille finie $(A_i)_{1 \leq i \leq n}$ d'événements d'un espace probabilisé $(\Omega, \mathbb{P})$ est un *système complet d'événements* si

1. Les A_i sont deux-à-deux disjoints.
2. $\mathbb{P}\left(\bigcup_{i=1}^{n} A_i\right) = 1$.

Remarque 1.2.1.16. Une partition de Ω est un système complet d'événements.

Proposition 1.2.1.17 (Formule des probabilités totales)**.** *Soit $(\Omega, \mathbb{P})$ un espace probabilisé fini. Soit $(A_1, \ldots, A_n)$ un système complet d'événements. Pour tout événement B, on a :*

$$\mathbb{P}(B) = \sum_{i=1}^{n} \mathbb{P}(B \cap A_i) = \sum_{i=1}^{n} \mathbb{P}(B \mid A_i)\mathbb{P}(A_i)$$

où par convention $\mathbb{P}(B \mid A_i)\mathbb{P}(A_i) = 0$ si $\mathbb{P}(A_i) = 0$

Démonstration. Soit B un événement. Posons $C \coloneqq \bigcup_{i=1}^{n} A_i$. Par hypothèse, $\mathbb{P}(C) = 1$ et donc $\mathbb{P}(\Omega \setminus C) = 0$. Comme $B \cap C \subset B$ alors $\mathbb{P}(B \cap C) \leq \mathbb{P}(B)$ et

$$\mathbb{P}(B) = \mathbb{P}((B \cap C) \cup (B \cap (\Omega \setminus C)) = \mathbb{P}(B \cap C) + \mathbb{P}(B \cap (\Omega \setminus C)) \leq \mathbb{P}(B \cap C) + \mathbb{P}(\Omega \setminus C) = \mathbb{P}(B \cap C)$$

(la deuxième égalité vient $(B \cap C) \cap (B \cap (\Omega \setminus C) = \emptyset$). On en déduit donc que $\mathbb{P}(B) = \mathbb{P}(B \cap C)$. Ainsi, comme les A_i sont disjoints, on obtient :

$$\mathbb{P}(B) = \mathbb{P}(B \cap C) = \mathbb{P}\left(\bigcup_{i=1}^{n} B \cap A_i\right) = \sum_{i=1}^{n} \mathbb{P}(B \cap A_i).$$

La deuxième égalité vient de la définition de probabilité conditionnelle. □

Corollaire 1.2.1.18 (Formule de Bayes)**.** *Soit* $(A_1, \ldots, A_n)$ *un système complet d'événements. Pour tout événement* B *tel que* $\mathbb{P}(B) \neq 0$ *et tout* $j \in \{1, \ldots, n\}$*,*

$$\mathbb{P}(A_j \mid B) = \frac{\mathbb{P}(B \mid A_j)\mathbb{P}(A_j)}{\sum_{i=1}^{n} \mathbb{P}(B \mid A_i)\mathbb{P}(A_i)}.$$

où par convention $\mathbb{P}(B \mid A_i)\mathbb{P}(A_i) = 0$ *si* $\mathbb{P}(A_i) = 0$

Démonstration. Soient B un événement tel que $\mathbb{P}(B) \neq 0$ et $j \in \{1, \ldots, n\}$. Alors

$$\mathbb{P}(A_j \mid B)\mathbb{P}(B) = \mathbb{P}(A_j) = \mathbb{P}(B \mid A_j)\mathbb{P}(A_j)$$

et donc

$$\mathbb{P}(A_j \mid B) = \frac{\mathbb{P}(B \mid A_j)\mathbb{P}(A_j)}{\mathbb{P}(B)} = \frac{\mathbb{P}(B \mid A_j)\mathbb{P}(A_j)}{\sum_{i=1}^{n} \mathbb{P}(B \mid A_i)\mathbb{P}(A_i)}$$

(la deuxième égalité venant de la formule des probabilités totales

□

Exemple 1.2.1.19. On estime qu'une ligne de production sort un produit défectueux une fois sur 10000. Le contrôle qualité permet d'exclure 99% d'entre eux mais aussi 2% de non-défectueux. Un article est déclaré "défectueux". Calculons la probabilité qu'il le soit vraiment.

Notons D l'événement "le produit défectueux" et P l'événement "le produit est exclu". Par hypothèse, on a les égalités suivantes :

$$\mathbb{P}(D) = \frac{1}{10000},\ \mathbb{P}(P \mid D) = 0.99,\ \mathbb{P}(P \mid D^c) = 0.02$$

Alors, par la formule de Bayes, on a :

$$\mathbb{P}(D \mid P) = \frac{\mathbb{P}(P \mid D)\mathbb{P}(D)}{\mathbb{P}(P \mid D)\mathbb{P}(D) + \mathbb{P}(P \mid D^c)\mathbb{P}(D^c)} \approx 4.93 \times 10^{-3}.$$

Proposition 1.2.1.20 (Formule des probabilités composées)**.** *Soit* $(\Omega, \mathbb{P})$ *un espace probabilisé fini. Soient* $A_1, \ldots, A_n$ *des événement de* Ω *tels que* $\mathbb{P}\left(\bigcap_{i=1}^{n-1} A_i\right) \neq 0$*. Alors*

$$\mathbb{P}\left(\bigcap_{i=1}^{n} A_i\right) = \mathbb{P}(A_1) \prod_{k=2}^{n} \mathbb{P}\left(A_k \mid \bigcap_{i=1}^{k-1} A_i\right)$$

Démonstration. Si $k \leq n$ alors $\bigcap_{i=1}^{n-1} A_i \subset \bigcap_{i=1}^{k-1} A_i$ et donc

$$0 < \mathbb{P}\left(\bigcap_{i=1}^{n-1} A_i\right) \leq \mathbb{P}\left(\bigcap_{i=1}^{k-1} A_i\right).$$

On en déduit que la formule donnée a un sens. Ensuite, on remarque que

$$\mathbb{P}\left(A_k \mid \bigcap_{i=1}^{k-1} A_i\right) = \frac{\mathbb{P}\left(\bigcap_{i=1}^{k} A_i\right)}{\mathbb{P}\left(\bigcap_{i=1}^{k-1} A_i\right)}.$$

Par télescopage, on obtient que

$$\prod_{k=2}^{n} \mathbb{P}\left(A_k \mid \bigcap_{i=1}^{k-1} A_i\right) = \frac{\mathbb{P}\left(\bigcap_{i=1}^{n} A_i\right)}{\mathbb{P}(A_1)},$$

ce qui permet de conclure. □

Exercice 50. On considère une urne contenant quatre boules blanches et trois boules noires. On tire une à une et sans remise trois boules de l'urne. Quelle est la probabilité pour que la première boule tirée soit blanche, la seconde blanche et la troisième noire ?

Exercice 51. On dispose de 100 dés à six faces dont 25 sont pipés. Pour chaque dé pipé, la probabilité d'obtenir le chiffre 6 lors d'un lancer vaut $1/2$.

1. On tire un dé au hasard parmi les 100 dés. On lance ce dé et on obtient 6. Quelle est la probabilité que ce dé soit pipé ?
2. Soit $n \geq 1$. On tire un dé au hasard parmi 100 dés. On lance ce dé n fois et on obtient n fois le chiffre 6. Quelle est la probabilité p_n pour que ce dé soit pipé. Interpréter le résultat.

Exercice 52. Soit $n \geq 1$. Deux urnes U_1 et U_2 contiennent chacune $3n$ boules blanches et n boules rouges. On effectue dans l'ordre les deux étapes suivantes :

i) On tire une boule dans l'urne U_1 puis on la place dans l'urne U_2 sans regarder sa couleur ;

ii) On tire au hasard une boule dans chacune des deux urnes U_1 et U_2.

On note A l'événement « la boule tirée dans U_1 lors de la première étape est blanche »et B l'événement « les deux boules tirées lors de la deuxième étape sont blanches ».

1. Déterminer $\mathbb{P}(B \mid A)$ et $\mathbb{P}(B \mid A^c)$.
2. En déduire $\mathbb{P}(B)$.

Exercice 53. Soit $n \geq 1$. On effectue n tirages successifs dans une urne contenant des boules rouges et des boules noires. Au départ, l'urne contient une boule de chaque couleur. Après chaque tirage, on remet dans l'urne la boule tirée plus deux autres boules de la même couleur. Soit $k \in \{0, \dots, n\}$.

1. Calculer la probabilité de tirer d'abord k boules rouges, puis $n-k$ boules noires.
2. Calculer la probabilité de tirer une boule rouge, puis une boule noire, puis $k-1$ boules rouges, puis $n-k-1$ boules noires.
3. Calculer la probabilité de tirer k boules rouges (dans un ordre quelconque).
4. En déduire la formule suivante :

$$4^n = \sum_{k=0}^{n} \binom{2k}{k} \binom{2n-2k}{n-k}.$$

1.2.2 Variables aléatoires sur un univers fini

1.2.2.1 Généralités

Définition 1.2.2.1. Soit $(\Omega, \mathbb{P})$ un espace probabilisé fini. On appelle *variable aléatoire* une fonction $X \colon \Omega \to \mathbb{R}$.

Notation 1.2.2.2. Soient $(\Omega, \mathbb{P})$ un espace probabilisé fini, X, Y deux variables aléatoires et B, C deux parties de $\mathbb{R}$. On note

— $\{X \in B\} \coloneqq X^{-1}(B) = \{\omega \in \Omega \mid X(\omega) \in B\} \in \mathscr{P}(\Omega)$;

— $\mathbb{P}(X \in B) \coloneqq \mathbb{P}(\{X \in B\})$;

— $\{X \in B, Y \in C\} \coloneqq \{X \in B\} \cap \{Y \in C\}$.

Définition 1.2.2.3. Soient $(\Omega, \mathbb{P})$ un espace probabilisé fini et $X \colon \Omega \to \mathbb{R}$ une variable aléatoire. On appelle loi de X la famille $(\mathbb{P}(X = x))_{x \in X(\Omega)}$.

Lemme 1.2.2.4. *Soient $(\Omega, \mathbb{P})$ un espace probabilisé fini et $X \colon \Omega \to \mathbb{R}$ une variable aléatoire.*

1. *Les événements $(\{X = x\})_{x \in X(\Omega)}$ forment un système complet.*
2. *Pour toute partie B de $\mathbb{R}$, on a :*

$$\mathbb{P}(X \in B) = \sum_{x \in B \cap X(\Omega)} \mathbb{P}(X = x)$$

Démonstration. 1. Pour tout $x \neq y \in X(\Omega)$, $\{X = x\} \cap \{X = y\} = X^{-1}(x) \cap X^{-1}(y) = X^{-1}(\{x\} \cap \{y\}) = X^{-1}(\emptyset) = \emptyset$. De plus,

$$\bigcup_{x \in X(\Omega)} \{X = x\} = \bigcup_{x \in X(\Omega)} X^{-1}(x) = X^{-1}\left(\bigcup_{x \in X(\Omega)} \{x\}\right) = X^{-1}(X(\Omega)) = \Omega.$$

2. Soit B une partie de $\mathbb{R}$. Alors $P(X \in B \cap X(\Omega)) \leq \mathbb{P}(X \in B)$ (car $B \cap X(\Omega) \subset B$) et

$$\mathbb{P}(X \in B) = \mathbb{P}(X \in B \cap X(\Omega)) + \mathbb{P}(X \in B \cap X(\Omega)^c) \leq \mathbb{P}(X \in B \cap X(\Omega)) + \mathbb{P}(X \in X(\Omega)^c) = \mathbb{P}(X \in B \cap X(\Omega)) + \mathbb{P}(\emptyset) = \mathbb{P}(X \in B \cap X(\Omega)).$$

On en déduit que $P(X \in B \cap X(\Omega)) = \mathbb{P}(X \in B)$, ce qui permet de conclure.

□

Lemme 1.2.2.5. *Soient $\mathcal{X}$ une partie finie de $\mathbb{R}$ et $p\colon \mathcal{X} \to \mathbb{R}$ un germe de probabilité sur $\mathcal{X}$ (i.e. une famille $(p(x))_{x \in \mathcal{X}}$ telle que $\sum_{x \in \mathcal{X}} p(x) = 1$). Il existe un espace probabilisé fini $(\Omega, \mathbb{P})$ et une variable aléatoire $X\colon \Omega \to \mathbb{R}$ dont la loi est $(p(x))_{x \in \mathcal{X}}$.*

Démonstration. On prend $\Omega := \mathcal{X}$, $X\colon \Omega \to \mathbb{R}$ l'inclusion de $\Omega = \mathcal{X}$ dans $\mathbb{R}$ et $\mathbb{P}$ la mesure de probabilité définie par le germe p. □

Remarque 1.2.2.6. Ces deux résultats permettent de simplifier l'explicitation d'une variable aléatoire en se contentant de donner sa loi.

1.2.2.2 Exemples usuels

Définition 1.2.2.7 (loi uniforme)**.** On dit qu'une variable aléatoire X suit une loi uniforme sur un ensemble fini $A \subset \mathbb{R}$ si

$$\forall a \in A, \mathbb{P}(X = a) = \frac{1}{|A|}.$$

i.e. X prend chaque valeur de A de façon équiprobable.
Ainsi, pour toute partie B de A, on a

$$\mathbb{P}(X \in B) = \frac{|B|}{|A|}.$$

Définition 1.2.2.8 (loi de Bernoulli)**.** On dit qu'une variable aléatoire suit la loi de Bernoulli de paramètre p, notée $\mathscr{B}(p)$, si

$$\mathbb{P}(X = 0) = 1 - p;\ \mathbb{P}(X = 1) = p$$

La variable aléatoire X modélise une expérience à deux issues ; la valeur 1 représente un succès et la valeur 0 représente un échec (on pourra penser à un pile ou face)

Définition 1.2.2.9 (loi binomiale)**.** On dit qu'une variable aléatoire suit une loi binomiale $\mathscr{B}(n, p)$ si

$$\forall k \in \{0, \ldots, n\}, \mathbb{P}(X = k) = \binom{n}{k} p^k (1-p)^{n-k}$$

Remarque 1.2.2.10. Par le binôme de Newton, on voit que cela définit bien entièrement X :

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

Exercice 54. On lance $n \geq 1$ fois une pièce parfaitement équilibrée. Quelle est la probabilité d'obtenir strictement plus de piles que de faces ?

Remarque 1.2.2.11. Si X suit une loi de Bernoulli $\mathscr{B}(p)$ alors elle suit une loi binomiale $\mathscr{B}(1, p)$. On verra dans 1.2.2.18 que la somme de n variables aléatoires indépendantes suivant la loi de Bernoulli $\mathscr{B}(p)$ suit une loi binomiale $\mathscr{B}(n, p)$. Ainsi, on peut modéliser un décompte de nombre de succès d'une répétition d'une expérience à deux issues par une loi binomiale.

Remarque 1.2.2.12. Soient $X_1, \ldots, X_n\colon \Omega \to \mathbb{R}$ des variables aléatoires. On peut construire une nouvelle loi grâce à n'importe quelle fonction $f\colon \mathbb{R}^n \to \mathbb{R}$ et en prenant la variable aléatoire donnée par la composée $f(X_1, \ldots, X_n)\colon \Omega \to \mathbb{R}$. En particulier, on considéra la somme, le produit, le maximum, le minimum,... de variables aléatoires.

1.2.2.3 Indépendance

Définition 1.2.2.13. Soient $(\Omega, \mathbb{P})$ un espace probabilisé fini et $X, Y \colon \Omega \to \mathbb{R}$ deux variables aléatoires. On dit que X, Y sont indépendantes si

$$\forall A, B \in \mathscr{P}(\mathbb{R}), \mathbb{P}(X \in A, Y \in B) = \mathbb{P}(X \in A)\mathbb{P}(Y \in B)$$

Autrement dit, si toutes les paires d'événements $(\{X \in A\}, \{Y \in B\})$ sont indépendantes.

Remarque 1.2.2.14. Avec $n \geq 2$ variables aléatoires $X_1, \ldots, X_n$, on a aussi une notion d'indépendance qui s'écrit :

$$\forall A_1, \ldots, A_n \in \mathscr{P}(\mathbb{R}), \mathbb{P}\left(\bigcap_{i=1}^{n} \{X_i \in A_i\}\right) = \prod_{i=1}^{n} \mathbb{P}(X_i \in A_i)$$

Exercice 55. Soient $(\Omega, \mathbb{P})$ un espace probabilisé fini. Soient $X, Y \colon \Omega \to \mathbb{R}$ deux variables aléatoires indépendantes. Soient $f, g \colon \mathbb{R} \to \mathbb{R}$ deux fonctions. Montrer que $f(X)$ et $g(Y)$ sont indépendantes.

Exercice 56. Soient $(\Omega, \mathbb{P})$ un espace probabilisé fini. Soient X, Y deux variables aléatoires telles qu'il existe deux fonctions $f, g \colon \mathbb{R} \to \mathbb{R}$ telles que :

$$\forall (x, y) \in \Omega^2, \mathbb{P}(X = x, Y = y) = f(x)g(y).$$

Montrer que X et Y sont indépendantes et qu'il existe $c > 0$ telle que

$$\forall x \in \Omega, \mathbb{P}(X = x) = cf(x) \text{ et } \forall y \in \Omega, \mathbb{P}(Y = y) = \frac{1}{c} g(y).$$

Proposition 1.2.2.15. *Soient $(\Omega, \mathbb{P})$ un espace probabilisé fini et $X, Y \colon \Omega \to \mathbb{R}$ deux variables aléatoires. Les variables aléatoires X et Y sont indépendantes si, et seulement si,*

$$\forall x \in X(\Omega), \forall y \in Y(\Omega), \mathbb{P}(X = x, Y = y) = \mathbb{P}(X = x)\mathbb{P}(Y = y)$$

Démonstration. Le sens directe est immédiat. Montrons la réciproque. Supposons que

$$\forall x \in X(\Omega), \forall y \in Y(\Omega), \mathbb{P}(X = x, Y = y) = \mathbb{P}(X = x)\mathbb{P}(Y = y).$$

Soient A, B deux parties de $\mathbb{R}$. Alors

$$\mathbb{P}(X \in A, Y \in B) = \mathbb{P}\left(\bigcup_{a \in A} \{X = a\} \cap \bigcup_{b \in B} \{Y = b\}\right) = \mathbb{P}\left(\bigcup_{a \in A} \bigcup_{b \in B} \{X = a\} \cap \{Y = b\}\right) = \mathbb{P}\left(\bigcup_{a \in A} \bigcup_{b \in B} \{X = a, Y = b\}\right)$$

Comme les ensembles $\{X = a, Y = b\}$ sont disjoints pour tout $(a, b) \in A \times B$, alors

$$\mathbb{P}(X \in A, Y \in B) = \sum_{a \in A} \sum_{b \in B} \mathbb{P}\left(\{X = a, Y = b\}\right)$$

Par hypothèse, $\mathbb{P}\left(\{X = a, Y = b\}\right) = \mathbb{P}(X = a)\mathbb{P}(Y = b)$ pour tout a, b. Donc

$$\mathbb{P}(X \in A, Y \in B) = \sum_{a \in A} \sum_{b \in B} \mathbb{P}(X = a)\mathbb{P}(Y = b) = \sum_{a \in A} \mathbb{P}(X = a) \sum_{b \in B} \mathbb{P}(Y = b) = \mathbb{P}(X \in A)\mathbb{P}(Y \in B).$$

□

Remarque 1.2.2.16. Avec $n \geq 2$ variables aléatoires $X_1, \ldots, X_n$, le critère qui s'écrit :

$$\forall (x_1, \ldots, x_n) \in \prod_{i=1}^{n} X_i(\Omega), \mathbb{P}\left(\bigcap_{i=1}^{n} \{X_i = x_i\}\right) = \prod_{i=1}^{n} \mathbb{P}(X_i = x_i)$$

Exemple 1.2.2.17. Soient X, Y deux variables aléatoires indépendantes de loi uniforme sur $\{1, \ldots, n\}$. Alors

$$\forall k \in \{1, \ldots, 2n\}, \mathbb{P}(X + Y = k) = \sum_{i=1}^{n} \mathbb{P}(X = i, Y = k - i)$$

$$= \begin{cases} \displaystyle\sum_{i=1}^{k-1} \mathbb{P}(X = i, Y = k - i) = \sum_{i=1}^{k-1} \mathbb{P}(X = i)\mathbb{P}(Y = k - i) = \frac{k-1}{n^2} & \text{si } k \leq n \\ \displaystyle\sum_{i=k-n}^{n} \mathbb{P}(X = i, Y = k - i) = \sum_{i=k-n}^{n} \mathbb{P}(X = i)\mathbb{P}(Y = k - i) = \frac{2n-k+1}{n^2} & \text{sinon} \end{cases}$$

Exercice 57. Vérifier ce calcul en calculant $\sum_{k=0}^{2n} \mathbb{P}(X+Y=k)$.

Exercice 58. Soit $n \geq 1$. Soient X, Y deux variables aléatoires indépendantes suivant la loi uniforme $\{1,\dots,n\}$. Donner la loi des variables aléatoires $\min(X,Y)$ et $\max(X,Y)$. Ces deux lois sont-elles indépendantes ?

Exemple 1.2.2.18. Soient $n \geq 1$ et $p \in [0,1]$. Soient $X_1,\dots,X_n$ n variables aléatoires de loi binomiale $\mathscr{B}(p)$. Soit $k \in \{0,\dots,n\}$. Posons $A_k := \{(a_1,\dots,a_n) \in \{0,1\}^n \mid \sum_{i=1}^n a_i = k\}$. On remarque tout d'abord que (en utilisant l'indépendance des X_i)

$$\mathbb{P}(X_1+\dots+X_n=k) = \sum_{(a_1,\dots,a_n)\in A_k} \mathbb{P}(X_1=a_1,\dots,X_n=a_n) = \sum_{(a_1,\dots,a_n)\in A_k} \prod_{i=1}^n \mathbb{P}(X_i=a_i)$$

Si $(a_1,\dots,a_n) \in A_k$ alors il y a k a_i qui valent 1 et $n-k$ qui valent 0. Ainsi

$$\forall (a_1,\dots,a_n) \in A_k, \prod_{i=1}^n \mathbb{P}(X_i=a_i) = p^k(1-p)^{n-k}$$

et donc

$$\mathbb{P}(X_1+\dots+X_n=k) = p^k(1-p)^{n-k} \sum_{(a_1,\dots,a_n)\in A_k} 1 = p^k(1-p)^{n-k}|A_k|$$

Comme A_k est en bijection avec $\mathscr{P}_k(E_n)$ par la fonction $(a_1,\dots,a_n) \mapsto \{i \in E_n \mid a_i = 1\}$ (sa réciproque étant $A \mapsto (a_1,\dots,a_n)$ où $a_i = 1$ si $i \in A$ et 0 sinon), on en déduit que

$$\mathbb{P}(X_1+\dots+X_n=k) = p^k(1-p)^{n-k}|\mathscr{P}_k(n)| = p^k(1-p)^{n-k}\binom{n}{k}.$$

Autrement dit, la somme $X_1+\dots+X_n$ suit la loi binomiale $\mathscr{B}(n,p)$.

1.2.2.4 Espérance

Définition 1.2.2.19. Soient $(\Omega,\mathbb{P})$ un espace probabilisé fini et $X\colon \Omega \to \mathbb{R}$ une variable aléatoire. On appelle *espérance de* X, que l'on note $\mathbb{E}(X)$, le nombre réel défini par :

$$\mathbb{E}(X) := \sum_{x\in X(\Omega)} x\mathbb{P}(X=x)$$

Remarque 1.2.2.20. On remarque que l'espérance dépend uniquement de la loi de X.

Proposition 1.2.2.21. *Soient* $(\Omega,\mathbb{P})$ *un espace probabilisé fini et* $X\colon \Omega \to \mathbb{R}$ *une variable aléatoire. Alors*

$$\mathbb{E}(X) = \sum_{\omega\in\Omega} X(\omega)\mathbb{P}(\{\omega\})$$

Démonstration. La famille $(\{\omega\})_{\omega\in\Omega}$ est une partition de Ω et donc est un système complet d'événements. On en déduit donc que

$$\mathbb{E}(X) = \sum_{x\in X(\Omega)} x\mathbb{P}(X=x) = \sum_{x\in X(\Omega)} x \sum_{\omega\in\Omega} \mathbb{P}(\{X=x\}\cap\{\omega\}) = \sum_{x\in X(\Omega)} \sum_{\omega\in\Omega} x\mathbb{P}(\{X=x\}\cap\{\omega\})$$

Pour tout $x \in X(\Omega)$ et $\omega \in \Omega$, $\{X=x\}\cap\{\omega\}$ est non-vide si, et seulement si, $X(\omega)=x$ et vaut alors $\{\omega\}$. Ainsi,

$$\mathbb{E}(X) = \sum_{\omega\in\Omega} X(\omega)\mathbb{P}(\{\omega\})$$

□

Exercice 59. Soient $n \geq 1$ et $p \in [0,1]$. Soient X une variable aléatoire suivant la loi uniforme sur $\{1,\dots,n\}$, Y une variable aléatoire suivant une loi de Bernoulli $\mathscr{B}(p)$ et Z une variable aléatoire suivant une loi binomiale $\mathscr{B}(n,p)$. Calculer l'espérance de X, Y et Z.

Exercice 60. On reprend les notations de l'exercice 58. Calculer l'espérance de $\min(X,Y)$ et $\max(X,Y)$.

Exercice 61. Soit $n \geq 1$. Soit X une variable aléatoire suivant une loi uniforme sur $\{1, \ldots, n\}$. On suppose que $\mathbb{E}(X) = 51$. Déterminer n.

Exercice 62. Soit $n \geq 1$. Soit X une variable aléatoire prenant ses valeurs dans $\{0, \ldots, n\}$. Montrer que

$$\mathbb{E}(X) = \sum_{k=0}^{n-1} \mathbb{P}(X > k).$$

Les trois résultats suivants permettent de calculer des espérances sans expliciter les lois des variables concernées.

Proposition 1.2.2.22 (Linéarité de l'espérance)**.** *Soient* $(\Omega, \mathbb{P})$ *un espace probabilisé fini,* $X, Y \colon \Omega \to \mathbb{R}$ *deux variables aléatoires et* $\lambda \in \mathbb{R}$*. Alors*

$$\mathbb{E}(X + \lambda Y) = \mathbb{E}(X) + \lambda \mathbb{E}(Y).$$

Démonstration. Par la formule précédente, on a :

$$\mathbb{E}(X+\lambda Y) = \sum_{\omega \in \Omega} (X+\lambda Y)(\omega)\mathbb{P}(\{\omega\}) = \sum_{\omega \in \Omega} (X(\omega)+\lambda Y(\omega))\mathbb{P}(\{\omega\}) = \sum_{\omega \in \Omega} X(\omega)\mathbb{P}(\{\omega\}) + \lambda \sum_{\omega \in \Omega} Y(\omega))\mathbb{P}(\{\omega\}) = \mathbb{E}(X) + \lambda \mathbb{E}(Y)$$

□

Exercice 63. On utilise avec un jeu de 52 cartes et on attribue 4 points à un As, 3 à un Roi, 2 à une Dame et 1 pour un Valet (et 0 pour toutes les autres cartes).

1. Soit X la variable aléatoire décrivant cette expérience. Déterminer la loi de X et son espérance.
2. Un joueur pioche 13 cartes dans le jeu de 52, on note Y le nombre de points contenu dans son jeu.
   (a) Montrer que $Y = X_1 + \ldots + X_{13}$ où les X_i sont des variables aléatoires de même loi que Y. *On pourra commencer par se convaincre de ce résultat en remplaçant* 13 *par* 2*.*
   (b) En déduire $\mathbb{E}(Y)$.

Proposition 1.2.2.23 (Formule de transfert)**.** *Soient* $(\Omega, \mathbb{P})$ *un espace probabilisé fini,* $X \colon \Omega \to \mathbb{R}$ *une variable aléatoire et* $f \colon \mathbb{R} \to \mathbb{R}$*. Alors*

$$\mathbb{E}(f(X)) = \sum_{x \in X(\Omega)} f(x)\mathbb{P}(X = x).$$

Démonstration. On a les égalités suivantes :

$$\mathbb{E}(f(X)) = \sum_{y \in f(X)(\Omega)} y\mathbb{P}(f(X) = y) = \sum_{x \in f(X)(\Omega)} y\mathbb{P}(X \in f^{-1}(y)) = \sum_{y \in f(X)(\Omega)} y \sum_{x \in f^{-1}(y)} \mathbb{P}(X = x) = \sum_{y \in f(X)(\Omega)} \sum_{x \in f^{-1}(y)} f(x)\mathbb{P}(X = x)$$

Comme $X(\Omega) = \bigcup_{y \in f(X(\Omega))} f^{-1}(y)$, on en déduit

$$\mathbb{E}(f(X)) = \sum_{y \in X(\Omega)} f(x)\mathbb{P}(X = x)$$

□

Exercice 64. On reprend l'étude du dé de l'exercice 47. Soit X la variable aléatoire décrivant la face obtenue avec ce dé. Soit Y la variable aléatoire définie par $Y := \frac{1}{X}$.

1. Rappeler la loi de X et Y
2. Calculer l'espérance de X et de Y. A-t-on $\mathbb{E}(Y) = \frac{1}{\mathbb{E}(X)}$?

Proposition 1.2.2.24. *Soient* $(\Omega, \mathbb{P})$ *un espace probabilisé fini et* $X, Y \colon \Omega \to \mathbb{R}$ *deux variables aléatoires* ***indépendantes****. Alors*

$$\mathbb{E}(XY) = \mathbb{E}(X)\mathbb{E}(Y).$$

Démonstration. On a :

$$\mathbb{E}(XY) = \sum_{z\in XY(\Omega)} z\mathbb{P}(XY=z) = \sum_{z\in XY(\Omega)} z \sum_{xy=z} \mathbb{P}(\{X=x, Y=y\}) = \sum_{z\in XY(\Omega)} \sum_{(x,y)\in X(\Omega)\times Y(\Omega), xy=z} xy\mathbb{P}(X=x, Y=y)$$

Comme $X(\Omega)\times Y(\Omega) = \bigcup_{z\in XY(\Omega)}\{(x,y)\in X(\Omega)\times Y(\Omega) \mid xy=z\}$, on en déduit que

$$\mathbb{E}(XY) = \sum_{x\in X(\Omega)} \sum_{y\in Y(\Omega)} xy\mathbb{P}(X=x, Y=y)$$

Par indépendance de X et Y, on obtient :

$$\mathbb{E}(XY) = \sum_{x\in X(\Omega)} \sum_{y\in Y(\Omega)} xy\mathbb{P}(X=x)\mathbb{P}(Y=y) = \sum_{x\in X(\Omega)} x\mathbb{P}(X=x) \sum_{y\in Y(\Omega)} y\mathbb{P}(Y=y) = \mathbb{E}(X)\mathbb{E}(Y).$$

□

Exercice 65. Reprendre l'exercice 58. Calculer l'espérance des deux variables aléatoires et en conclure à nouveau que les deux lois sont dépendantes.

Remarque 1.2.2.25. On a aussi un énoncé pour n variables aléatoires indépendantes $X_1, \dots, X_n$:

$$\mathbb{E}\left(\prod_{i=1}^{n} X_i\right) = \prod_{i=1}^{n} \mathbb{E}(X_i).$$

Exercice 66. Soient $(\Omega, \mathbb{P})$ un espace probabilisé fini et $X, Y\colon \Omega \to \mathbb{R}$ deux variables aléatoires. Montrer que

1. Si $X \geq 0$ alors $\mathbb{E}(X) \geq 0$ avec égalité si, et seulement si, $\mathbb{P}(X=0)=1$;
2. Si $X \geq Y$ alors $\mathbb{E}(X) \geq \mathbb{E}(Y)$ avec égalité si, et seulement si, $\mathbb{P}(X=Y)=1$;
3. $|\mathbb{E}(X)| \leq \mathbb{E}(|X|)$.

Proposition 1.2.2.26 (Inégalité de Cauchy-Schwarz)**.** *Soient $(\Omega, \mathbb{P})$ un espace probabilisé fini et $X, Y\colon \Omega \to \mathbb{R}$ deux variables aléatoires. Alors*

$$|\mathbb{E}(XY)| \leq \sqrt{\mathbb{E}(X^2)\mathbb{E}(Y^2)}.$$

avec égalité si, et seulement si, il existe $(a,b)\in\mathbb{R}^2\setminus\{(0,0)\}$, $\mathbb{P}(aX+bY=0)=1$.

Démonstration. Soient $\varphi\colon t\in\mathbb{R}\mapsto \mathbb{E}((X+tY)^2)$. Cette fonction est positive car $(X+tY)^2\geq 0$. De plus, par linéarité de l'espérance, on a :

$$\forall t\in\mathbb{R}, \mathbb{E}((X+tY)^2) = \mathbb{E}(X^2) + 2t\mathbb{E}(XY) + t^2\mathbb{E}(Y^2)$$

Ainsi, φ est une fonction polynomiale de degré au plus 2.

— Si $\mathbb{E}(Y^2)=0$ alors Y^2 est nul avec probabilité 1 et donc Y aussi. On en déduit que XY est alors nul avec probabilité 1, ce qui permet d'obtenir l'inégalité voulue. C'est même une égalité et on a $\mathbb{P}(0X+1\cdot Y=0)=1$.

— Sinon, comme φ est positive et de degré 2, on en déduit que son discriminant est négatif. Ainsi,

$$0 \geq 4\mathbb{E}(XY)^2 - 4\mathbb{E}(X^2)\mathbb{E}(Y^2)$$

d'où le résultat. Il y a égalité si ce discriminant est nul. La fonction φ a une racine t_0 i.e. $\mathbb{E}((X+t_0Y)^2)=0$ et donc $X+t_0Y=0$ avec probabilité 1.

□

Proposition 1.2.2.27 (Inégalité de Markov)**.** *Soient $(\Omega, \mathbb{P})$ un espace probabilisé fini et $X\colon \Omega\to\mathbb{R}$ une variable aléatoire positive. Alors*

$$\forall \varepsilon > 0, \mathbb{P}(X > \varepsilon) \leq \frac{\mathbb{E}(X)}{\varepsilon}.$$

Démonstration. Soit $\varepsilon > 0$. Alors

$$\begin{aligned}\mathbb{E}(X) &= \sum_{\omega\in\Omega} X(\omega)\mathbb{P}(\{\omega\}) = \sum_{\omega\in\Omega, X(\omega)>\varepsilon} \underbrace{X(\omega)}_{>\varepsilon}\mathbb{P}(\{\omega\}) + \sum_{\omega\in\Omega, X(\omega)\leq\varepsilon} \underbrace{X(\omega)}_{\geq 0}\underbrace{\mathbb{P}(\{\omega\})}_{\geq 0} \\ &\geq \sum_{\omega\in\Omega, X(\omega)>\varepsilon} \varepsilon\mathbb{P}(\{\omega\}) = \varepsilon \sum_{\omega\in\Omega, X(\omega)>\varepsilon} \mathbb{P}(\{\omega\}) = \varepsilon\mathbb{P}(X>\varepsilon)\end{aligned}$$

□

Exercice 67. Soient X une variable aléatoire réelle finie à valeurs positive et $f\colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{>0}$ une fonction croissante. Démontrer que

$$\forall \varepsilon > 0, \mathbb{P}(X \geq a) \leq \frac{\mathbb{E}(f(X))}{f(\varepsilon)}$$

Exercice 68. Soient $n \geq 1$ et $p \in [0,1]$. Soit X une variable aléatoire suivant une loi binomiale $\mathscr{B}(n,p)$. Montrer que

$$\mathbb{P}\left(\left|\frac{X}{n} - p\right| \geq \varepsilon\right) \leq \frac{\sqrt{p(1-p)}}{\varepsilon\sqrt{n}}.$$

1.2.2.5 Variance

Définition 1.2.2.28. Soient $(\Omega, \mathbb{P})$ un espace probabilisé fini et $X\colon \Omega \to \mathbb{R}$ une variable aléatoire. La *variance de* X est le réel défini par

$$\mathbb{V}(X) \coloneqq \inf_{c \in \mathbb{R}} \mathbb{E}((X-c)^2)$$

Remarque 1.2.2.29. Cette borne inférieure existe car $\mathbb{E}((X-c)^2) \geq 0$ pour tout $c \in \mathbb{R}$ (et car $\mathbb{R}$ est non-vide).

Remarque 1.2.2.30. La variance a pour but de minimiser la distance[4] entre la variable aléatoire et une variable aléatoire constante.

Proposition 1.2.2.31. *Soient* $(\Omega, \mathbb{P})$ *un espace probabilisé fini et* $X\colon \Omega \to \mathbb{R}$ *une variable aléatoire. Alors*

$$\mathbb{V}(X) = \mathbb{E}((X - \mathbb{E}(X))^2) = \mathbb{E}(X^2) - \mathbb{E}(X)^2$$

Démonstration. Soit $\varphi\colon c \in \mathbb{R} \mapsto \mathbb{E}((X-c)^2) = \mathbb{E}(X^2) - 2c\mathbb{E}(X) + c^2$. C'est une fonction polynomiale de degré 2. Son minimum est donc atteint en $\frac{-(-2\mathbb{E}(X))}{2} = \mathbb{E}(X)$ et donc $\mathbb{V}(X) = \mathbb{E}((X - \mathbb{E}(X))^2)$. En développant, on obtient :

$$\mathbb{V}(X) = \mathbb{E}(X^2) - 2\mathbb{E}(X)\mathbb{E}(X) + \mathbb{E}(X)^2 = \mathbb{E}(X^2) - \mathbb{E}(X)^2.$$

□

Corollaire 1.2.2.32. *La variance d'une variable aléatoire ne dépend que de la loi de celle-ci.*

Démonstration. Cela vient du fait que l'espérance ne dépend que de la loi et de la formule de transfert. □

Exercice 69. Soient $(\Omega, \mathbb{P})$ un espace probabilisé fini et $X\colon \Omega \to \mathbb{R}$ une variable aléatoire. Alors

1. $\mathbb{V}(X) \geq 0$ avec égalité si, et seulement si, $\mathbb{P}(X = \mathbb{E}(X)) = 1$.
2. $\forall a, b \in \mathbb{R}, \mathbb{V}(aX + b) = a^2\mathbb{V}(X)$

Exercice 70. Soient $n \geq 1$ et $p \in [0,1]$. Soient X une variable aléatoire suivant la loi uniforme sur $\{1, \ldots, n\}$, Y une variable aléatoire suivant une loi de Bernoulli $\mathscr{B}(p)$ et Z une variable aléatoire suivant une loi binomiale $\mathscr{B}(n,p)$. Calculer la variance de X, Y et Z.

Exercice 71. Reprendre l'exercice 58. Calculer la variance des deux variables aléatoires.

Exercice 72. Soient $X_1, X_2, ..., X_n$ des variables aléatoires indépendantes de même espérance m et de même variance σ^2. On considère les variables aléatoires $\overline{X} \coloneqq \frac{1}{n}\sum_{i=1}^{n} X_i$ et $Z \coloneqq \frac{1}{n-1}\sum_{i=1}^{n-1}(X_i - \overline{X})^2$.

1. Calculer $\mathbb{E}(\overline{X}), \mathbb{V}(\overline{X})$.
2. Montrer que $\mathbb{V}(X_i - \overline{X}) = \sigma^2\left(1 - \frac{1}{n}\right)$ et en déduire $\mathbb{E}(Z)$.

Proposition 1.2.2.33 (Inégalité de Bienaymé-Tchebychev)**.** *Soient* $(\Omega, \mathbb{P})$ *un espace probabilisé fini et* $X\colon \Omega \to \mathbb{R}$ *une variable aléatoire. Alors*

$$\forall \varepsilon > 0, \mathbb{P}(|X - \mathbb{E}(X)| > \varepsilon) \leq \frac{\mathbb{V}(X)}{\varepsilon^2}.$$

4. on étudie $|X-c|$ qui est une variable aléatoire donc en prenant l'espérance, on pourrait minimiser $\mathbb{E}|X-c|$ mais la distance choisie ici a des meilleurs propriétés (celle d'être induite par un produit scalaire)

Démonstration. Soit $\varepsilon > 0$. Alors, par l'inégalité de Markov, on a :

$$\mathbb{P}(|X - \mathbb{E}(X)| > \varepsilon) = \mathbb{P}(|X - \mathbb{E}(X)|^2 > \varepsilon^2) \leq \frac{\mathbb{E}(|X - \mathbb{E}(X)|^2)}{\varepsilon^2} = \frac{\mathbb{V}(X)}{\varepsilon^2}$$

□

Exercice 73. On jette 10 fois un dé équilibré à 6 faces. Minorer la probabilité que le nombre d'apparitions du numéro 1 soit compris entre 20 et 50.

Exercice 74. Une population présente une propriété dans une proportion inconnue $p \in]0,1[$ que l'on souhaite estimer. On choisit un échantillon de $n \geq 1$ personnes et l'on pose $X_i = 1$ si le i-ème individu présente la propriété étudiée, 0 sinon. On considère que les variables aléatoires X_i ainsi définies sont indépendantes et suivent chacune une loi de Bernoulli de paramètre p. Enfin, on pose $S_n \coloneqq \sum_{i=1}^{n} X_i$.

1. Établir
$$\forall \varepsilon > 0, \mathbb{P}\left(\left|\frac{S_n}{n} - p\right| > \varepsilon\right) \leq \frac{1}{4n\varepsilon^2}.$$
2. Quelle valeur de n peut-on choisir pour que $\frac{S_n}{n}$ constitue une valeur approchée de p à $0,05$ près avec une probabilité supérieure à 95 % ?

Exercice 75. On souhaite estimer l'équilibre d'une pièce. On note p la probabilité (inconnue) que la pièce tombe côté face lors d'un lancer. On lance $n \geq 1$ fois la pièce et l'on définit F_n à la fréquence de lancers ayant donné face.

1. Calculer $\mathbb{E}(F_n)$. Vérifier $\mathbb{V}(F_n) \leq \frac{1}{4n}$.
2. À partir de combien de lancers peut-on supposer que F_n est une approximation de p à $\frac{1}{100}$ près avec une probabilité supérieure à 95 % ?

Exercice 76. Soit $(X_n)_{n\in\mathbb{N}}$ une suite de variables aléatoires telle que, pour tout $n \in \mathbb{N}$, X_n suit une loi binomiale de paramètres n et $p \in]0,1[$. Soit $k \in \mathbb{N}$. Montrer que $\lim\limits_{n\to\infty} \mathbb{P}(X_n \leq k) = 0$.

Définition 1.2.2.34. Soient $(\Omega, \mathbb{P})$ un espace probabilisé fini et $X, Y \colon \Omega \to \mathbb{R}$ deux variables aléatoires. La covariance des variables aléatoires X et Y est le réel, noté $\mathbb{C}\mathrm{ov}(X,Y)$, défini par :

$$\mathbb{C}\mathrm{ov}(X,Y) \coloneqq \mathbb{E}((X - \mathbb{E}(X))(Y - \mathbb{E}(Y))).$$

Exercice 77. Soient $(\Omega, \mathbb{P})$ un espace probabilisé fini et $X, Y, Z \colon \Omega \to \mathbb{R}$ trois variables aléatoires. Montrer que :

1. $\mathbb{V}(X) = \mathbb{C}\mathrm{ov}(X,X)$
2. $\forall a, b \in \mathbb{R}, \mathbb{C}\mathrm{ov}(aX + bY, Z) = a\,\mathbb{C}\mathrm{ov}(X,Z) + b\,\mathbb{C}\mathrm{ov}(Y,Z)$.

Proposition 1.2.2.35. *Soient $(\Omega, \mathbb{P})$ un espace probabilisé fini et $X, Y \colon \Omega \to \mathbb{R}$ deux variables aléatoires. Alors*

$$\mathbb{C}\mathrm{ov}(X,Y) = \mathbb{E}(XY) - \mathbb{E}(X)\mathbb{E}(Y) = \frac{1}{2}(\mathbb{V}(X+Y) - \mathbb{V}(X) - \mathbb{V}(Y))$$

Démonstration. On a :

$$\mathbb{C}\mathrm{ov}(X,Y) = \mathbb{E}((X - \mathbb{E}(X))(Y - \mathbb{E}(Y)) = \mathbb{E}(XY - \mathbb{E}(X)Y - \mathbb{E}(Y)X + \mathbb{E}(X)\mathbb{E}(Y)) = \mathbb{E}(XY) - 2\mathbb{E}(X)\mathbb{E}(Y) + \mathbb{E}(X)\mathbb{E}(Y) = \mathbb{E}(XY) - \mathbb{E}(X)\mathbb{E}(Y).$$

De plus,

$$\mathbb{V}(X+Y) = \mathbb{E}((X+Y)^2) - \mathbb{E}(X+Y)^2 = \mathbb{E}(X^2 + 2XY + Y^2) - \mathbb{E}(X)^2 - 2\mathbb{E}(X)\mathbb{E}(Y) + \mathbb{E}(Y)^2 = \mathbb{V}(X) + \mathbb{V}(Y) + 2\,\mathbb{C}\mathrm{ov}(X,Y)$$

□

Remarque 1.2.2.36. En particulier, si X et Y sont indépendants alors $\mathbb{C}\mathrm{ov}(X,Y)$ est nulle. Mais ce n'est pas une condition nécessaire et suffisante.

Exercice 78. Soit X une variable aléatoire définie par :

$$\mathbb{P}(X = 0) = \mathbb{P}(X = 1) = \mathbb{P}(X = -1) = \frac{1}{3}.$$

Soit Y la variable aléatoire valant 0 si X est non-nul et 1 sinon. Montrer que $\mathbb{C}\mathrm{ov}(X, Y) = 0$ mais que X et Y ne sont pas indépendantes.

Exercice 79. Soient $(\Omega, \mathbb{P})$ un espace probabilisé fini et $X, Y \colon \Omega \to \mathbb{R}$ deux variables aléatoires. Montrer que :

$$|\mathbb{C}\mathrm{ov}(X, Y)| \leq \sqrt{\mathbb{V}(X)\mathbb{V}(Y)}$$

avec égalité si, et seulement si, il existe $(a, b, c) \in (\mathbb{R}^2 \setminus \{0\}) \times \mathbb{R}$ tel que $\mathbb{P}(aX + bY = c) = 1$.

Chapitre 2

Ensembles dénombrables

2.1 Construction des ensembles usuels

2.1.1 Construction de $\mathbb{N}$: Axiomes de Peano

Axiome 2.1.1.1 (de Peano)**.** Il existe un ensemble $\mathbb{N}$ et une fonction $s : \mathbb{N} \to \mathbb{N}$ (appelée fonction successeur) tels que :

- $\mathbb{N}$ est non-vide et contient un élément noté 0.
- $0 \notin s(\mathbb{N})$ (il n'existe pas d'entier naturel avec comme successeur 0).
- La fonction s est injective (si deux entiers ont le même successeur alors ils sont égaux).
- Si A est un sous-ensemble de $\mathbb{N}$ tel que $0 \in A$ et $s(A) \subset A$ alors $A = \mathbb{N}$ (un sous-ensemble de $\mathbb{N}$ contenant 0 et tel que si $a \in A$ alors $s(a) \in A$ est $\mathbb{N}$ tout entier).

On se fixe un tel couple $(\mathbb{N}, s)$ pour le reste du cours. Les éléments de $\mathbb{N}$ sont appelés « entiers naturels ».

Théorème 2.1.1.2 (Récurrence)**.** *Soit $(\mathscr{P}_n)_{n\in\mathbb{N}}$ une suite d'assertions. Supposons que $\mathscr{P}_0$ soit vraie et que pour tout $n \in \mathbb{N}$, si $\mathscr{P}_n$ est vraie alors $\mathscr{P}_{s(n)}$ est vraie. Alors $\mathscr{P}_n$ est vraie pour tout $n \in \mathbb{N}$.*

Démonstration. On considère l'ensemble

$$A \coloneqq \{n \in \mathbb{N} \mid \mathscr{P}_n \text{ est vraie}\}.$$

C'est un sous-ensemble de $\mathbb{N}$ qui contient 0 ($\mathscr{P}_0$ est vraie) et pour tout $n \in A$, $s(n) \in A$. On en déduit donc que $A = \mathbb{N}$ et donc pour tout $n \in \mathbb{N}$, l'assertion $\mathscr{P}_n$ est vraie. □

Exemple 2.1.1.3. Soit (u_n) une suite dans $\mathbb{N}$ telle que $u_0 = 0$ et telle que pour tout $n \in \mathbb{N}$, $u_{s(n)} = s(u_n)$.

Montrons par récurrence que $\forall n \in \mathbb{N}, u_n = n$.

Notons, pour $n \in \mathbb{N}$, $\mathscr{P}_n$ l'assertion « $u_n = n$ ».

Initialisation : pour $n = 0$, on a $u_0 = 0$ par définition. L'assertion $\mathscr{P}_0$ est vraie.

Hérédité : Soit $n \in \mathbb{N}$ et supposons l'assertion $\mathscr{P}_n$ vraie i.e. $u_n = n$. Alors

$$u_{s(n)} = s(u_n) \overset{HR}{=} s(n)$$

On a donc montré que pour tout $n \in \mathbb{N}$, $\mathscr{P}_n$ implique $\mathscr{P}_{s(n)}$.

Conclusion : Par le principe de récurrence, on a :

$$\forall n \in \mathbb{N}, u_n = n.$$

On a ainsi montré que tout élément de $\mathbb{N}$ s'écrit comme une composée de la fonction successeur appliquée à 0.

Avertissement 2.1.1.4. — Ne pas oublier l'initialisation.

— Ne pas écrire « Supposons que $\mathscr{P}_n$ est vraie pour tout n » ou « Supposons qu'il existe n tel que $\mathscr{P}_n$ est vraie ».

Dans les deux cas, le raisonnement par récurrence est faux quoi qu'il arrive.

— Il faut utiliser l'hypothèse de récurrence (i.e. le fait que $\mathscr{P}_n$ soit vraie) quelque part dans l'hérédité. Sinon, le raisonnement par récurrence est superflu et un raisonnement direct fonctionne.

— Une récurrence se fait sur $\mathbb{N}$ (ou un de ses sous-ensembles) pas sur $\mathbb{R}$ ou sur un autre ensemble.

Remarque 2.1.1.5. On peut commencer une récurrence à un rang n_0 (i.e. vérifier l'initialisation pour $n = n_0$). Si on note $(\mathscr{P}_n)_{n\geq n_0}$ la suite d'assertions que l'on veut montrer, on peut considérer la suite auxiliaire $(\mathscr{R}_n)$ définie par

$$\mathscr{R}_n = \begin{cases} \text{« } 0 = 0 \text{ »} & \text{si } n < n_0 \\ \mathscr{P}_n & \text{si } n \geq n_0 \end{cases}$$

et montrer par récurrence que $\mathscr{R}_n$ est vraie pour tout $n \in \mathbb{N}$ (si P et Q sont deux assertions vraies alors $P \Rightarrow Q$ est vraie aussi).

Remarque 2.1.1.6. Pour définir une suite (u_n) de E, il y a deux possibilités :

— pour tout $n \in \mathbb{N}$, se donner un élément de E ;

— se donner u_0 et pour tout $n \in \mathbb{N}$, une façon de calculer $u_{s(n)}$ en fonction de u_n

Définition 2.1.1.7. On appelle addition la fonction $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ définie par

— $\forall a \in \mathbb{N}, a + 0 \coloneqq a$

— pour tout $a \in \mathbb{N}$, on note u_b la suite définie par

  — $u_0 \coloneqq a$;

  — $\forall b \in \mathbb{N}, u_{s(b)} \coloneqq s(u_b)$

  On définit alors $a + b \coloneqq u_b$.

On appelle multiplication la fonction $\times : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ définie par :

— $\forall a \in \mathbb{N}, a \times 0 \coloneqq 0$

— pour tout $a \in \mathbb{N}$, on note u_b la suite définie par

  — $u_0 \coloneqq 0$;

  — $\forall b \in \mathbb{N}, u_{s(b)} \coloneqq u_b + a$

  On définit alors $a \times b \coloneqq u_b$.

Remarque 2.1.1.8. Si on note 1 le successeur de 0 alors $a + 1 = s(a)$. Dans la suite, on notera $a + 1$ le successeur de a ($a + 2$ le successeur de $a + 1$,...).

Exercice 80. Montrer que $2 + 2 = 2 \times 2 = 4$ (où 2 est le successeur du successeur de 0 et 4 est le successeur du successeur de 2).

Notation 2.1.1.9. La multiplication s'écrit aussi $a \cdot b$ ou ab (si le contexte est clair).

Proposition 2.1.1.10. *Soient* $p, q, r \in \mathbb{N}$. *Alors*

— $p + q = q + p$ *(commutativité de* $+$*)* ;

— $p + (q + r) = (p + q) + r$ *(associativité de* $+$*)* ;

— $p + 0 = p$ *(0 est l'élément neutre de* $+$*)* ;

— $p(q + r) = pq + pr$ *(distributivité de* $\times$ *par rapport à* $+$*)* ;

— $p(qr) = (pq)r$ *(associativité de* $\times$*)* ;

— $p \times 1 = 1 \times p = p$ *(1 est l'élément neutre de* $\times$*)*

— $pq = qp$ *(commutativité de* $\times$*)* ;

Remarque 2.1.1.11. On dit que les couples $(\mathbb{N}, +)$ et $(\mathbb{N}, \times)$ sont des monoïdes.

Exercice 81. Montrer que $\forall p \in \mathbb{N}, p+1 = 1+p$. En déduire que $+$ est commutative.

Exercice 82. Montrer que 1 est l'élément neutre de $\times$ et en déduire la commutativité de $\times$.

Définition 2.1.1.12. Soient $a, b \in \mathbb{N}$. On dit que a est supérieur à b, on note $a \geq b$, s'il existe $n \in \mathbb{N}$ tel que $a = b+n$. L'entier a est strictement supérieur à b si $a \geq b$ et $a \neq b$. On note alors $a > b$. On dit que a est inférieur (resp. strictement inférieur) à b si $b \geq a$ (resp. $b > a$).

Proposition 2.1.1.13. *Soient $a, b, c, d \in \mathbb{N}$ tels que $a \geq c$ et $b \geq d$. Alors*

1. $a+b \geq c+d$;
2. $ab \geq cd$.

Démonstration. Soient $n, m \in \mathbb{N}$ tels que $a = c+n$ et $b = d+m$. Alors

$$a+b = (c+d) + \underbrace{n+m}_{\in\mathbb{N}}$$

et

$$ab = (c+n)(d+m) = cd + \underbrace{cm+nd+nm}_{\in\mathbb{N}}$$

□

Corollaire 2.1.1.14 (Récurrence double)**.** *Soit $(\mathscr{P}_n)_{n\in\mathbb{N}}$ une suite d'assertions. Supposons que $\mathscr{P}_0$ et $\mathscr{P}_1$ soient vraies et que pour tout $n \in \mathbb{N}$, si $\mathscr{P}_n$ et $\mathscr{P}_{n+1}$ sont vraies alors $\mathscr{P}_{n+2}$ est vraie. Alors $\mathscr{P}_n$ est vraie pour tout $n \in \mathbb{N}$.*

Démonstration. Pour $n \in \mathbb{N}$, on note $\mathscr{R}_n$ l'assertion « $\mathscr{P}_n$ et $\mathscr{P}_{n+1}$ sont vraies ». On peut remarquer que si pour tout $n \in \mathbb{N}$, $\mathscr{R}_n$ est vraie alors en particulier, pour tout $n \in \mathbb{N}$, $\mathscr{P}_n$ est vraie.

On va montrer par récurrence (simple) que $\mathscr{R}_n$ est vraie pour tout $n \in \mathbb{N}$.

Initialisation : Comme $\mathscr{P}_0$ et $\mathscr{P}_1$ sont vraies par hypothèse alors $\mathscr{R}_0$ est vraie

Hérédité : Soit $n \in \mathbb{N}$ et supposons l'assertion $\mathscr{R}_n$ vraie i.e. $\mathscr{P}_n$ et $\mathscr{P}_{n+1}$ est vraie.

Par hypothèse, le fait que $\mathscr{P}_n$ et $\mathscr{P}_{n+1}$ est vraie implique que $\mathscr{P}_{n+2}$, et donc que $\mathscr{R}_{n+1}$ est vraie puisqu'on a déjà supposé que $\mathscr{P}_{n+1}$ était vraie.

Conclusion : Par le principe de récurrence, on a montré que pour tout $n \in \mathbb{N}$, $\mathscr{R}_n$ est vraie et donc $\mathscr{P}_n$ est vraie aussi. □

Corollaire 2.1.1.15 (Récurrence forte)**.** *Soit $(\mathscr{P}_n)_{n\in\mathbb{N}}$ une suite d'assertions. Supposons que $\mathscr{P}_0$ soit vraie et que pour tout $n \in \mathbb{N}$, si $\mathscr{P}_k$ est vraie pour tout $k < n+1$ alors $\mathscr{P}_{n+1}$ est vraie. Alors $\mathscr{P}_n$ est vraie pour tout $n \in \mathbb{N}$.*

Démonstration. Pour $n \in \mathbb{N}$, on note $\mathscr{R}_n$ l'assertion « $\mathscr{P}_k$ est vraie pour $k < n+1$ ». On peut remarquer que si pour tout $n \in \mathbb{N}$, $\mathscr{R}_n$ est vraie alors en particulier, pour tout $n \in \mathbb{N}$, $\mathscr{P}_n$ est vraie.

On va montrer par récurrence (simple) que $\mathscr{R}_n$ est vraie pour tout $n \in \mathbb{N}$.

Initialisation : Comme $\mathscr{P}_0$ est vraie par hypothèse alors $\mathscr{R}_0$ est vraie

Hérédité : Soit $n \in \mathbb{N}$ et supposons l'assertion $\mathscr{R}_n$ vraie i.e. $\mathscr{P}_k$ est vraie pour $k < n+1$.

Par hypothèse, cela implique que $\mathscr{P}_{n+1}$ est vraie, cela implique ainsi que $\mathscr{R}_{n+1}$ est vraie puisqu'on a déjà supposé que $\mathscr{P}_k$ était vraie pour $k < n+1$.

Conclusion : Par le principe de récurrence, on a montré que pour tout $n \in \mathbb{N}$, $\mathscr{R}_n$ est vraie et donc $\mathscr{P}_n$ est vraie aussi. □

Théorème 2.1.1.16. *Toute partie non vide A de $\mathbb{N}$ admet un minimum, noté* $\min A$. *On a ainsi $\forall a \in A, a \geq \min A$.*

Démonstration. Soit A un sous-ensemble non vide de $\mathbb{N}$. Supposons par l'absurde que A n'ait pas de minimum.
On va maintenant en déduire que cela entraîne que A est vide. Pour cela, montrons par récurrence forte que l'assertion $\mathscr{P}_n : n \notin A$ est vraie pour tout $n \in \mathbb{N}$:

Initialisation : Si $0 \in A$ alors comme $A \subset \mathbb{N}$, on a en particulier, $\forall n \in A, a \geq 0$ i.e. $0 = \min(A)$. On en déduit donc que $0 \notin A$.

Hérédité : Soit $n \in \mathbb{N}$ et supposons que pour $k < n+1$, $\mathscr{P}_k$ est vraie i.e. $\forall k < n+1, k \notin A$. En particulier, cela veut dire que pour tout $a \in A$, $a \geq n+1$. Ainsi, si $n+1 \in A$ alors on aurait $\min(A) = n+1$. Ce qui est impossible donc $n+1 \notin A$ et donc $\mathscr{P}_{n+1}$ est vraie.

Conclusion : On en déduit que pour tout $n \in \mathbb{N}$, $\mathscr{P}_n$ est vraie et donc A est vide. □

Exercice 83. Établir les formules ou assertions suivantes par récurrence.

1. $\forall n \in \mathbb{N} \setminus \{0\},\ 1+2+...+n = \frac{n(n+1)}{2}$.
2. $\forall n \in \mathbb{N} \setminus \{0\},\ 1+3+...+(2n-1) = n^2$.

3. $\forall n \in \mathbb{N} \setminus \{0\},\ 1^3 + 2^3 + ... + n^3 = \frac{n^2(n+1)^2}{4}$.
4. Pour tout $n \in \mathbb{N}$, 3 divise $n^3 - n$.
5. $\forall n \in \mathbb{N},\ 2^0 + 2^1 + ... + 2^n = 2^{n+1} - 1$.
6. $\forall n \in \mathbb{N} \setminus \{0\},\ \sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}$.
7. Pour tout $n \in \mathbb{N} \setminus \{0\}$, tout produit de n entiers consécutifs est divisible par $n!$.
8. Quels que soient $k, n \in \mathbb{N}$, $(k+1)^n - kn - 1$ est divisible par k^2.
9. $\forall n \in \mathbb{N} \setminus \{0\}, \sum_{k=1}^{n} k(n+1-k) = \frac{n(n+1)(n+2)}{6}$

Exercice 84. Soit (u_n) la suite définie par $u_0 = 1$, $u_1 = 3$ et $u_{n+2} = 3u_{n+1} - 2u_n$ pour tout $n \geq 1$.

1. Calculer u_2, u_3, u_4, puis deviner une formule générale pour u_n.
2. Démontrer la formule par une récurrence double.

Exercice 85. Soit (u_n) la suite définie par $u_0 = 1$ et $u_{n+1} = 1 + u_0 + \cdots + u_n$ pour tout $n \geq 1$.

1. Calculer u_1, u_2, u_3, puis deviner une formule générale pour u_n.
2. Démontrer la formule par une récurrence forte.

Exercice 86. L'argument par récurrence suivant est-il correct ?

On note, pour tout $n \geq 1$, P_n la proposition suivante : Si une trousse contient n stylos, alors les n stylos sont de la même couleur.

Montrons par récurrence que pour tout $n \geq 1$, P_n est vraie.
Initialisation : Pour $n = 1$, P_1 est vraie puisqu'il n'y a qu'un stylo.
Hérédité : Soit $n \in \mathbb{N} \setminus \{0\}$. On suppose que P_n est vraie, montrons que P_{n+1} l'est aussi.
Prenons une trousse qui a $n+1$ stylos, on en enlève 1, il en reste donc n qui sont de la même couleur par l'hypothèse de récurrence. On en enlève encore 1 dans la trousse puis on remet le premier : il y a à nouveau n stylos : ils sont donc de la même couleur. Donc le premier stylo enlevé a la même couleur que les n autres.

Donc P_{n+1} est vraie.

Exercice 87. Soit $(u_n)_{n\in\mathbb{N}}$ la suite définie par $u_0 = 0$, $u_1 = 1$ et

$$\forall n \in \mathbb{N},\ u_{n+2} = u_{n+1} + u_n \quad \text{(suite de Fibonacci)}.$$

1. Montrer que $\forall n \in \mathbb{N} \setminus \{0\},\ u_{n+1}u_{n-1} - u_n^2 = (-1)^n$ et en déduire que $\forall n \in \mathbb{N} \setminus \{0\}$, $\mathrm{PGCD}(u_n, u_{n+1}) = 1$.
2. Montrer que $\forall n \in \mathbb{N}, \forall m \in \mathbb{N} \setminus \{0\}, u_{m+n} = u_m u_{n+1} + u_{m-1}u_n$ et en déduire que $\mathrm{PGCD}(u_m, u_n) = u_{\mathrm{PGCD}(m,n)}$ pour m et n non nuls.

2.1.2 Interlude : relations d'ordres et d'équivalence

Définition 2.1.2.1. Soit E un ensemble. Une *relation binaire* de E est un sous-ensemble de $E \times E$. Si $\mathscr{R}$ est une relation binaire, on écrira $x\mathscr{R}y$ au lieu d'écrire $(x, y) \in \mathscr{R}$.

Exemple 2.1.2.2.

1. Pour tout ensemble E, l'égalité est une relation binaire sur E ($\Delta_E \coloneqq \{(x, x) \mid x \in E\} \subset E \times E$).
2. Les ordres usuels $\leq, \geq, <, >$ sont des relations binaires sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ (par exemple $\{(x, y) \in \mathbb{Z}^2 \mid x \leq y\} \subset \mathbb{Z}^2$).
3. La divisibilité est une relation binaire sur $\mathbb{N}$, $\mathbb{Z}$ ou sur $\mathbb{K}[X]$.
4. Le graphe d'une fonction $E \to E$ est une relation binaire sur E.
5. Soit $n \in \mathbb{N}_{\geq 1}$. L'ensemble $\equiv_n \coloneqq \{(x, y) \in \mathbb{Z}^2 \mid x \equiv y \mod n\}$ est une relation binaire sur $\mathbb{Z}$.

6. Soit $B \in \mathbb{K}[X] \setminus \{0\}$. L'ensemble $\equiv_B := \{(P, Q) \in \mathbb{K}[X] \mid P \equiv Q \mod B\}$ est une relation binaire dans $\mathbb{K}[X]$.
7. On peut définir une relation sur les suites réelles :

$$u_n \sim v_n \text{ si } \forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, (1-\varepsilon)u_n \leq v_n \leq (1+\varepsilon)u_n.$$

8. Soit $A \subset \mathbb{R}$ et $a \in \mathbb{R}$ un point adhérent de A. On peut définir une relation sur l'ensemble des fonctions $A \to \mathbb{R}$:

$$f \sim_a g \text{ si } \exists \eta > 0, \exists \varepsilon :]a-\eta, a+\eta[\to \mathbb{R}, \forall x \in]a-\eta, a+\eta[\cap A, f(x) = (1+\varepsilon(x))g(x) \text{ et } \lim_{x \to a} \varepsilon(x) = 0$$

9. Si $\mathscr{R}$ est une relation binaire sur E et $F \subset E$ alors $\mathscr{R}_{|F} := \mathscr{R} \cap F \times F$ est une relation binaire sur F.

Définition 2.1.2.3. Une relation binaire $\mathscr{R}$ sur un ensemble E est dite

— *réflexive* si pour tout $a \in E$, $a\mathscr{R}a$ (i.e. $\Delta_E \subset \mathscr{R}$) ;

— *symétrique* si pour tous $a, b \in E$, $a\mathscr{R}b \Rightarrow b\mathscr{R}a$;

— *antisymétrique* si pour tous $a, b \in E$, $a\mathscr{R}b$ et $b\mathscr{R}a \Rightarrow a = b$;

— *transitive* si pour tous $a, b, c \in E$, ($a\mathscr{R}b$ et $b\mathscr{R}c$) $\Rightarrow a\mathscr{R}c$.

Exemple 2.1.2.4.

— L'égalité est une relation réflexive, symétrique, antisymétrique, transitive.

— Les relations $\equiv_n, \equiv_B$ ainsi que l'équivalence de suites ou de fonctions sont des relations réflexives, symétriques et transitives.

— Les relations $\leq, \geq$ sont des relations réflexives, antisymétriques et transitives sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

— La divisibilité est réflexive et transitive. Sur $\mathbb{N}$, elle est aussi antisymétrique (car deux entiers naturels associés sont égaux) mais ne l'est pas sur $\mathbb{Z}$ ou $\mathbb{K}[X]$.

— Le graphe d'une fonction est réflexive si la fonction est la fonction identité, symétrique si $f \circ f = \mathrm{id}_E$ et transitive si $f \circ f = f$.

— Si $\mathscr{R}$ est une relation réflexive (resp. symétrique, antisymétrique, transitive) sur E et F est une partie de E alors $\mathscr{R}_{|F}$ aussi.

Avertissement 2.1.2.5. L'égalité n'est pas la seule relation symétrique et anti-symétrique : l'ensemble $\{(x, y) \in \mathbb{N}^2 \mid x = y\} \subset \mathbb{Z}^2$ est une relation symétrique et antisymétrique de $\mathbb{Z}$ qui n'est pas l'égalité.

Exercice 88. Soit $\mathscr{R}$ une relation symétrique et antisymétrique d'un ensemble E. Si une des projections $\mathscr{R} \subset E \times E \to E$ est surjective (en particulier, si $\mathscr{R}$ est surjective) alors $\mathscr{R} = \{(x, x) \mid x \in E\}$ i.e. $\mathscr{R}$ est l'égalité de E.

Exercice 89. Dire si les relations suivantes sont réflexives, symétriques, antisymétriques, transitives :

1. si $E = \mathbb{Q}$ et $x\mathscr{R}y$ si $y = -x$;
2. si $E = \mathbb{R}$ et $x\mathscr{R}y$ si $\cos^2(x) + \sin^2(y) = 1$;
3. si $E = \mathbb{N}$ et $x\mathscr{R}y$ si $\exists p, q \in \mathbb{N}_{\geq 1}, y = px^q$.

Exercice 90. La relation d'orthogonalité entre deux droites du plan est-elle symétrique ? réflexive ? transitive ?

Définition 2.1.2.6. Une relation binaire est

— une *relation d'équivalence* si elle est réflexive, symétrique et transitive ;

— une *relation d'ordre* si elle réflexive, antisymétrique et transitive.

Exercice 91. Parmi les relations de l'exercice 89, lesquelles sont des relations d'ordre ? des relations d'équivalence ?

Exemple 2.1.2.7. — L'égalité est la seule relation qui soit d'équivalence et d'ordre.

— Les relations $\leq, \geq$ sont des relations d'ordre.

— La divisibilité est une relation d'ordre sur $\mathbb{N}$ mais pas sur $\mathbb{Z}$ ou $\mathbb{K}[X]$.

— Les relations $\sim, \sim_a, \equiv_n, \equiv_B$ sont des relations d'équivalence.

Exercice 92. Soient A, B deux ensembles non-vides, $\sim_1$ une relation d'équivalence sur A, $\sim_2$ une relation d'équivalence sur B. Montrer que la relation $\sim$ définie sur $A \times B$ par

$$(a, b) \sim (a', b') \text{ si } a \sim_1 a' \text{ et } b \sim_2 b'$$

est une relation d'équivalence. On la notera $\sim_1 \times \sim_2$.

Définition 2.1.2.8. Soit E un ensemble non-vide et $\sim$ une relation d'équivalence sur E.

— Soit $x \in E$. La *classe d'équivalence de* x pour la relation d'équivalence $\sim$ est l'ensemble des $y \in E$ tel que $x \sim y$. On la notera $\overline{x}$.

— L'*ensemble quotient* de E par $\sim$ est l'ensemble des classes d'équivalences pour $\sim$ que l'on notera $E/\sim$.

Remarque 2.1.2.9. Il existe une fonction naturelle $\pi\colon E \to E/\sim$ définie par $\pi(x) \coloneqq \overline{x}$. Elle est surjective par construction de $E/\sim$.

Exemple 2.1.2.10. — $\mathbb{Z}/\equiv_n = \mathbb{Z}/n\mathbb{Z}$ (ainsi les deux notations $\overline{x}$ coïncident).

— $\mathbb{R}[X]/\equiv_{X^2+1} = \{\overline{a + bX} \mid a, b \in \mathbb{R}\}$

— Pour un ensemble E, $E/= \ = E$

Théorème 2.1.2.11. *Soient E un ensemble non-vide et $\sim$ une relation d'équivalence sur E. Pour tout ensemble F et toute fonction $f : E \to F$ telle que*

$$\forall x, y \in E, x \mathscr{R} y \Rightarrow f(x) = f(y),$$

il existe une unique fonction $\widetilde{f}\colon E/\sim \to F$ telle que $\widetilde{f} \circ \pi = f$.

On dit qu'une telle fonction f passe au quotient.

Démonstration. Soient F un ensemble et $f : E \to F$ une fonction telle que $\forall x, y \in E, x \mathscr{R} y \Rightarrow f(x) = f(y)$. Alors pour tout $x \in E$, on peut définir $\widetilde{f}(\overline{x}) \coloneqq f(x)$. Cela est bien défini car pour tout élément $y \in \overline{x}$, $f(y) = f(x)$. Cela définit donc une fonction $E/\sim \to F$ et par définition, qui vérifie bien $\widetilde{f} \circ \pi = f$. Par construction de $E/\sim$, c'est la seule façon de définir $\widetilde{f}$. □

Exemple 2.1.2.12.

— Les fonctions $(p, q) \in \mathbb{Z}^2 \mapsto \overline{p + q} \in \mathbb{Z}/n\mathbb{Z}$ et $(p, q) \in \mathbb{Z}^2 \mapsto \overline{pq} \in \mathbb{Z}/n\mathbb{Z}$ passent au quotient pour la relation d'équivalence produit $\equiv_n \times \equiv_n$ à gauche . On obtient ainsi les lois $\overline{+}$ et $\overline{\times}$.

— Le somme et le produit de $\mathbb{R}[X]$ descendent au quotient sur $\mathbb{R}[X]/\equiv_{X^2+1}$. En particulier, le produit vérifie :

$$(\overline{a + bX})(\overline{c + dX}) = \overline{ac + (bc + ad)X + bdX^2} = \overline{(ac - bd) + (bc + ad)X}$$

En particulier, $\overline{a}\,\overline{b} = \overline{ab}$ et $\overline{X}^2 = \overline{-1}$.
Ainsi, $\mathbb{R}[X]/\equiv_{X^2+1}$ est une façon de construire $\mathbb{C}$.

Exercice 93. Soient A, B deux ensembles non-vides. On définit sur $A \times B$ la relation suivante :

$$(a, b) \sim (a', b') \text{ si } a = a'$$

1. Montrer que $\sim$ est une relation d'équivalence.
2. Montrer que la fonction $\overline{(a, b)} \in A \times B/\sim \mapsto b \in B$ est bien définie et est une bijection.

Exercice 94. Soit $k \in \mathbb{N}$. On définit sur l'ensemble des fonctions $]-1,1[\to \mathbb{R}$ de classe $\mathscr{C}^k$ la relation suivante :

$$f \sim g \text{ si } \forall \ell \leq k, f^{(\ell)}(0) = g^{(\ell)}(0)$$

1. Montrer que $\sim$ est une relation d'équivalence.
2. Montrer que la fonction associant une classe d'équivalence de fonctions vers son polynôme de Taylor est bien définie et est une bijection $\mathscr{C}^k(]-1,1[,\mathbb{R})/\sim \to \mathbb{R}[X]_{\leq k}$.

Exercice 95. On note $\mathbb{S}^1$ le cercle unité dans le plan complexe[1]. On définit sur $\mathbb{S}^1 \times \mathbb{S}^1$ la relation suivante :

$$(z,w) \sim (z',w') \text{ si } \exists \theta \in \mathbb{R}, z = e^{i\theta}z' \text{ et } w = e^{i\theta}w'$$

1. Montrer que cela définit une relation d'équivalence.
2. Justifier que l'ensemble $\mathbb{S}^1 \times \mathbb{S}^1/\sim$ permet de définir ce qu'est un « angle ».

2.1.3 Construction de $\mathbb{Z}$

Exercice 96. Montrer que la relation binaire sur $\mathbb{N} \times \mathbb{N}$ définie par

$$(a,b)\mathscr{R}(c,d) \text{ si } a+c = b+d$$

est une relation d'équivalence.

Définition 2.1.3.1. L'ensemble $\mathbb{Z}$ est le quotient $\mathbb{N} \times \mathbb{N}/\mathscr{R}$ où $\mathscr{R}$ est la relation d'équivalence de l'exercice 96. On appelle *entier relatif* un élément de $\mathbb{Z}$.

Exercice 97. Montrer que la fonction $\iota\colon \mathbb{N} \to \mathbb{Z}$ définie par

$$\forall n \in \mathbb{N}, \iota(n) \coloneqq \overline{(n,0)}$$

est une injection.

Notation 2.1.3.2. On notera n la classe d'équivalence de $(n,0)$ pour $n \in \mathbb{N}$. Ainsi, on pourra écrire $\mathbb{N} \subset \mathbb{Z}$.

Exercice 98. Montrer que les fonctions $(\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}) \to \mathbb{Z}$ suivantes passent au quotient pour la relation $\mathscr{R} \times \mathscr{R}$:

— $((a,b),(c,d)) \mapsto \overline{(a+c,b+d)}$;

— $((a,b),(c,d)) \mapsto \overline{(bd+ac,bc+ad)}$;

On notera (par abus) $+$ et $\times$ les deux lois sur $\mathbb{Z}$ ainsi obtenues.

Exercice 99. Montrer que $(\mathbb{Z},+)$ et $(\mathbb{Z},\times)$ vérifient les mêmes énoncés (mutatis mutandis) que dans la proposition 2.1.1.10 (les éléments neutres étant aussi 0 et 1).

Proposition 2.1.3.3. *Le couple $(\mathbb{Z},+)$ est un groupe abélien.*

Démonstration. Par l'exercice 99, il suffit de montrer que chaque élément de $\mathbb{Z}$ a un inverse pour $+$. Soit $N = \overline{(a,b)} \in \mathbb{Z}$. Alors $N + \overline{(b,a)} = \overline{(a+b,a+b)} = \overline{(0,0)} = 0$.

Notons que cet inverse ne dépend pas du représentant de N qui a été choisi : si $N = \overline{(c,d)}$ alors $\overline{(d,c)} = \overline{(b,a)}$. □

Remarque 2.1.3.4. En combinant l'exerice 99 et la proposition 2.1.3.3, on a montré que $(\mathbb{Z},+,\times)$ est un anneau.

Notation 2.1.3.5. Si $N \in \mathbb{Z}$ alors on notera $-N$ son inverse.

Proposition 2.1.3.6. *L'égalité suivante est vérifiée :*

$$\mathbb{Z} = \mathbb{N} \cup \{-n \mid n \in \mathbb{N}\}.$$

On peut alors écrire pour tout $a,b \in \mathbb{N}$, $\overline{(a,b)} = b + (-a) =: b - a$

1. on n'a pas besoin de le voir ainsi mais cela facilite les calculs.

Démonstration. L'inclusion $\supset$ a déjà été démontrée. Montrons l'autre. Soit $N = \overline{(a,b)} \in \mathbb{Z}$. Si $a \geq b$ (et donc $a = b+n$ avec $n \in \mathbb{N}$) alors $N = \overline{(n,0)} = n \in \mathbb{N}$ (on note que cela ne dépend pas du représentant choisi) sinon $b = a+m$ avec $m \in \mathbb{N}$ et donc $N = \overline{(0,m)} = -m \in \{-n \mid n \in \mathbb{N}\}$. □

Remarque 2.1.3.7. Les deux ensembles ont une intersection non-vide $\{0\}$.

Remarque 2.1.3.8. Avec cette écriture, on obtient une justification de la formule du produit :

$$\overline{(a,b)} \times \overline{(c,d)} = (a-b) \times (c-d) = (ac+bd) - (bc+ad) = \overline{(bd+ac, bc+ad)}$$

Exercice 100. Montrer que la fonction $f\colon \mathbb{Z} \to \mathbb{N}$ définie par

$$\forall n \in \mathbb{Z}, f(n) \coloneqq \begin{cases} 2n & \text{si } n \in \mathbb{N}; \\ 2(-n)+1 & \text{si } n \in \mathbb{Z} \setminus \mathbb{N}. \end{cases}$$

est une bijection. Donner sa bijection réciproque.

On peut définir une fonction $|\cdot| : \mathbb{Z} \to \mathbb{N}$, appelée valeur absolue, par

$$\forall n \in \mathbb{Z}, |n| \coloneqq \begin{cases} n & \text{si } n \in \mathbb{N} \\ -n & \text{sinon} \end{cases}$$

Remarque 2.1.3.9. On remarque que si $-n \in \mathbb{N}$ alors $n = \overline{(0,|n|)}$.

Proposition 2.1.3.10. *La règle des signes est vérifiée :*

1. $\forall a, b \in \mathbb{N}, ab = |a||b|$;
2. $\forall a \in \mathbb{N}, \forall b \in \mathbb{Z} \setminus \mathbb{N}, ab = -|a||b|$;
3. $\forall a \in \mathbb{Z} \setminus \mathbb{N}, \forall b \in \mathbb{N}, ab = -|a||b|$;
4. $\forall a, b \in \mathbb{Z} \setminus \mathbb{N}, ab = |a||b|$;

Démonstration.

1. Le premier point est immédiat.
2. Soient $a \in \mathbb{N}$ et $b \in \mathbb{Z} \setminus \mathbb{N}$. Alors
$$ab = (|a|,0)(0,|b|) = (0,|a||b|) = -|a||b|.$$
3. Soient $a \in \mathbb{Z} \setminus \mathbb{N}$ et $b \in \mathbb{N}$. Alors
$$ab = (0,|a|)(|b|,0) = (0,|a||b|) = -|a||b|.$$
4. Soient $a \in \mathbb{Z} \setminus \mathbb{N}$ et $b \in \mathbb{Z} \setminus \mathbb{N}$. Alors
$$ab = (0,|a|)(0,|b|) = (|a||b|,0) = |a||b|.$$

□

Notation 2.1.3.11. Soit $a, b \in \mathbb{Z}$. On note $a \geq b$ (resp. $a > b$) si $a-b \in \mathbb{N}$ (resp. $a-b \in \mathbb{N} \setminus \{0\}$) et $a \leq b$ (resp. $a < b$) si $b-a \in \mathbb{N}$ (resp. $b-a \in \mathbb{N} \setminus \{0\}$).

Remarque 2.1.3.12. En particulier, pour $a \in \mathbb{Z}$, $a \geq 0$ si, et seulement si, $a \in \mathbb{N}$ et donc $a \in \mathbb{N}$ si, et seulement si, $-a \leq 0$.

Exercice 101. Montrer que, pour tout $n \in \mathbb{Z}$, $|n| = \max(n,-n)$.

Exercice 102. Résoudre dans $\mathbb{Z}$ l'équation $n^2 - 5|n| + 6 = 0$.

Exercice 103. Résoudre dans $\mathbb{Z}$ l'équation $||n^2-4| - 2n - 4 = 0$

Proposition 2.1.3.13. *Soient* $a, b, c, d \in \mathbb{Z}$ *tels que* $a \leq b$ *et* $c \leq d$. *Alors* $a+c \leq b+d$ *et si* $a, c \in \mathbb{N}$ *alors* $ac \leq bd$ *et si* $b, d \leq 0$ *alors* $ac \geq bd$.

Démonstration. Soient $a, b, c, d \in \mathbb{Z}$ tels que $a \leq b$ et $c \leq d$. Alors $b-a \in \mathbb{N}$ et $d-c \in \mathbb{N}$ et donc $b-a+d-c \in \mathbb{N}$. Autrement dit, $b+d \geq a+c$.
Pour la multiplication, on va commencer par supposer $c = d$. Alors si $c \geq 0$, on a $c(b-a) \in \mathbb{N}$ et donc $ca \geq bc$ et si $c \leq 0$ alors $c(a-b) \in \mathbb{N}$ et donc $cb \leq ca$.
Pour $d \geq c \geq 0$ alors $c(b-a) + b(d-c) \in \mathbb{N}$ et donc $ac \geq bd$ et si $0 \geq d \geq c$ alors $c(a-b) + b(c-d) \in \mathbb{N}$ et donc $ca \geq bd$. □

Exercice 104. Résoudre dans $\mathbb{Z}$ l'inéquation $n(n-5) \leq 0$.

Définition 2.1.3.14. Un ensemble $A \subset \mathbb{Z}$ est dit minoré (resp. majoré) s'il existe $m \in \mathbb{Z}$ tel que $m \leq a$ (resp. $a \leq m$) pour tout $a \in A$.

Proposition 2.1.3.15. *Toute partie minorée de $\mathbb{Z}$ admet un minimum. Toute partie majorée A de $\mathbb{Z}$ admet un maximum.*

Démonstration. Supposons $A \subset \mathbb{Z}$ minorée par m. Alors $A - m \coloneqq \{a - m \mid a \in A\}$ est une partie de $\mathbb{N}$ qui est minorée, donc $A - m$ admet un plus petit élément $\min(A-m)$. Alors $m + \min(A-m)$ est le plus petit élément de A. En effet, il existe un $a \in A$ tel que $a - m = \min(A-m)$, donc pour tout $b \in A$, on a $a = m + \min(A-m) \leq m + b - m = b$, donc $a = \min A$. Si b est aussi le plus petit élément de A alors $a \leq b$ et $b \leq a$, donc $a = b$. La deuxième affirmation se fait de la même façon. □

Exercice 105. Montrer l'existence de la division euclidienne i.e.

$$\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z} \setminus \{0\}, \exists (q, r) \in \mathbb{Z}^2, a = bq + r \text{ et } 0 \leq r < |b|.$$

Exercice 106. Montrer (sans récurrence) qu'une suite décroissante d'entiers finit par être négative.

2.1.4 Construction de $\mathbb{Q}$

Exercice 107. Montrer que la relation binaire sur $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ définie par

$$(a, b) \mathscr{R} (c, d) \text{ si } ad = bc$$

est une relation d'équivalence.

Définition 2.1.4.1. L'ensemble $\mathbb{Q}$ est le quotient $\mathbb{Z} \times \mathbb{Z} \setminus \{0\} / \mathscr{R}$ où $\mathscr{R}$ est la relation d'équivalence de l'exercice 107. On appelle *nombre rationnel* un élément de $\mathbb{Q}$.

Remarque 2.1.4.2. On enlève $\mathbb{Z} \times \{0\}$ car sinon le quotient serait réduit à un point : tous les éléments seraient équivalents à $(0, 0)$.

Exercice 108. Montrer que la fonction $\iota \colon \mathbb{Z} \to \mathbb{Q}$ définie par

$$\forall n \in \mathbb{Z}, \iota(n) \coloneqq \overline{(n, 1)}$$

est une injection.

Exercice 109. Soit $x \in \mathbb{Q}$. Montrer qu'il existe une unique paire $(p, q) \in \mathbb{Z} \times (\mathbb{N} \setminus \{0\})$ telle que $p \wedge q = 1$ et $x = \frac{p}{q}$.

On pourra commencer par montrer que si $s \in \mathbb{Z} \setminus \{0\}$ alors pour tout $(p, q) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$, $\overline{(sp, sq)} = \overline{(p, q)}$.

Définition 2.1.4.3. On appelle cette écriture *représentation irréductible de x*.

Notation 2.1.4.4. On notera n la classe d'équivalence de $(n, 1)$ pour $n \in \mathbb{Z}$. Ainsi, on pourra écrire $\mathbb{Z} \subset \mathbb{Q}$. On notera $\frac{p}{q}$ la classe d'équivalence $\overline{(p, q)}$.

Exercice 110. Montrer que $\mathbb{N}$ et $\mathbb{Q}$ sont en bijection.
On pourra utiliser Cantor-Bernstein.

Exercice 111. Montrer que les fonctions $(\mathbb{Z} \times \mathbb{Z} \setminus \{0\}) \times (\mathbb{Z} \times \mathbb{Z} \setminus \{0\}) \to \mathbb{Q}$ suivantes passent au quotient pour la relation $\mathscr{R} \times \mathscr{R}$:

— $((a, b), (c, d)) \mapsto \overline{(ad + bc, bd)}$;

— $((a, b), (c, d)) \mapsto \overline{(ac, bd)}$;

On notera (par abus) $+$ et $\times$ les deux lois sur $\mathbb{Q}$ ainsi obtenues qui s'écrivent donc

$$\frac{p}{q} + \frac{r}{s} = \frac{ps + qr}{qs} \text{ et } \frac{p}{q} \times \frac{r}{s} = \frac{pr}{qs}.$$

Exercice 112. Montrer que $(\mathbb{Q}, +)$ et $(\mathbb{Q} \setminus \{0\}, \times)$ vérifient les mêmes énoncés (mutatis mutandis) que dans la proposition 2.1.1.10 (les éléments neutres étant aussi 0 et 1).

Proposition 2.1.4.5. *Les couples* $(\mathbb{Q}, +)$ *et* $(\mathbb{Q} \setminus \{0\}, \times)$ *sont des groupes abéliens.*

Démonstration. Par l'exercice 112, il suffit de montrer que chaque élément de $\mathbb{Q}$ a un inverse pour $+$ et que chaque élément de $\mathbb{Q} \setminus \{0\}$ a un inverse pour $\times$.

- Soit $N = \overline{(p, q)} \in \mathbb{Q}$. Alors $N + \overline{(-p, q)} = \overline{(pq - qp, pq)} = \overline{(0, q^2)} = \overline{(0, 1)} = 0$.
  Notons que cet inverse ne dépend pas du représentant de N qui a été choisi : si $N = \overline{(c, d)}$ alors $\overline{(-c, d)} = \overline{(-p, q)}$.
- Soit $N = \overline{(p, q)} \in \mathbb{Q} \setminus \{0\}$. Alors $N \times \overline{(q, p)} = \overline{(pq, pq)} = \overline{(1, 1)} = 1$ Notons que cet inverse a un sens car $p \neq 0$ (par hypothèse) et ne dépend pas du représentant de N qui a été choisi : si $N = \overline{(c, d)}$ alors $\overline{(d, c)} = \overline{(b, a)}$.

□

Remarque 2.1.4.6. En combinant l'exercice 112 et la proposition 2.1.4.5, on a montré que $(\mathbb{Q}, +, \times)$ est un corps commutatif.

Définition 2.1.4.7. On dit qu'un nombre rationnel x est *décimal* s'il existe $n \in \mathbb{N}$ et $a \in \mathbb{Z}$ tels que

$$x = \frac{a}{10^n}.$$

On notera $\mathbb{D}$ l'ensemble des nombres décimaux.

Exercice 113. Montrer que la somme et le produit de deux nombres décimaux est décimal.

Exercice 114. Montrer que $\frac{1}{3} \notin \mathbb{D}$.

Remarque 2.1.4.8. Cela montre que $(\mathbb{D}, +, \times)$ est un sous-anneau de $(\mathbb{Q}, +, \times)$ (car 0 et 1 sont décimaux).

Proposition 2.1.4.9. *Soit* $x \in \mathbb{Q}$ *de représentation irréductible* $\frac{p}{q}$. *Alors* $x \in \mathbb{D}$ *si, et seulement si, il existe* $a, b \in \mathbb{N}$ *tels que* $q = 2^a 5^b$.

Démonstration. Soit $x \in \mathbb{Q}$. Supposons qu'il existe $a, b \in \mathbb{N}$ tels que $q = 2^a 5^b$. Fixons-les. Posons $n \coloneqq \max(a, b)$ (ainsi $n - a, n - b \in \mathbb{N}$). Alors

$$x = \frac{p}{q} = \frac{2^{n-a}5^{n-b}p}{2^{n-a}5^{n-b}q} = \frac{2^{n-a}5^{n-b}p}{2^n 5^n} = \frac{2^{n-a}5^{n-b}p}{10^n} \in \mathbb{Q}.$$

Réciproquement, supposons que $x \in \mathbb{D}$. Soit $n \in \mathbb{Z}$ et $a \in \mathbb{Z}$ tel que $x = \frac{a}{10^n}$. Alors $10^n p = aq$. Comme p et q sont premiers entre eux alors par le lemme de Gauß, q divise $10^n = 2^n 5^n$. Par unicité de la décomposition en facteurs premiers, q s'écrit comme un produit de puissance de 2 et de 5. □

Exercice 115. Soit $x \in \mathbb{Q}$. Donner une condition nécessaire et suffisante pour que $x \in \mathbb{D}$ et $x^{-1} \in \mathbb{D}$.