

DÉNOMBREMENT

Les énoncés et parties suivis du symbole [✗] ne seront pas traités en cours.

A. Cardinal d'un ensemble fini	3
A. 1. Énumération et cardinal	3
A. 2. Cardinal d'une partie	4
A. 3. Cardinal d'une réunion	5
A. 4. Cardinal du complémentaire	8
A. 5. Cardinal d'un produit cartésien	9
B. Choix successifs	10
B. 1. Listes	10
B. 2. Listes sans répétition (arrangements)	11
B. 3. Permutations	12
C. Choix simultanés	13
C. 1. Coefficients binomiaux	13
C. 2. Combinaisons	14
C. 3. Ensemble des combinaisons	15
D. Applications entre ensembles finis	16
D. 1. Injection, surjection, bijection et cardinal	16
D. 2. Applications entre ensembles finis de même cardinal	17
D. 3. Dénombrement d'applications entre ensembles finis	18
E. Comparaison des ensembles infinis [✗]	19
E. 1. Subpotence et équivalence	19
E. 2. Dénombrabilité	22



Prérequis

Revoir les chapitres sur :

- les nombres ;
- les sommes et produits ;
- la théorie des applications.

Dans ce cours, les lettres E, F, G, H, A, B, \dots désignent des ensembles.

Rappelons que, pour tout entier naturel n , la notation $\llbracket 1; n \rrbracket$ désigne l'ensemble \emptyset si $n = 0$ et l'ensemble $\{1; 2; \dots; n\}$ si $n \geq 1$.

Plus généralement, la notation $\llbracket m; n \rrbracket$ désigne l'ensemble vide \emptyset lorsque $n < m$ et l'ensemble $\{m; m + 1; m + 2; \dots; n\}$ lorsque $n \geq m$.

Les trois lettres AQT signifient « Âne Qui Trotte » et sont utilisées pour désigner une démonstration facile laissée au lecteur.

A. Cardinal d'un ensemble fini

A.1. Enumération et cardinal

Pour compter des objets, dans la vie courante, on procède à une énumération de ces objets : « un, deux, trois, ... », attribuant arbitrairement le numéro 1 à un objet, puis le numéro 2, etc. Lorsque l'énumération s'arrête, au numéro n , on en conclut naturellement qu'il y a n objets.

Pour le mathématicien, une question se pose cependant : si l'on avait compté les objets dans un autre ordre, aurait-on également trouvé n objets ? Je vous rassure tout de suite, la réponse est positive et nous allons le démontrer, fondant ainsi proprement la notion de cardinal d'un ensemble.

Commençons par dire qu'une énumération d'un ensemble E consiste à attribuer à chaque objet de E , de façon univoque, un numéro dans $\llbracket 1; n \rrbracket$. Autrement dit, pour le mathématicien, une énumération de E est une bijection entre $\llbracket 1; n \rrbracket$ et E .

On peut alors donner la définition suivante du cardinal d'un ensemble.

Définition 1

Un ensemble E est dit **fini** s'il existe $n \in \mathbb{N}$ tel que $\llbracket 1; n \rrbracket$ soit en bijection avec E . Il y a alors unicité d'un tel entier n : on l'appelle le **cardinal** de E et on le note $\text{card } E$ (ou $|E|$ ou $\#E$).

Un ensemble qui n'est pas fini est dit **infini**.

Déterminer le cardinal d'un ensemble, c'est **dénombrer** cet ensemble.

■ Il faut prouver l'unicité de n .

S'il existe une bijection φ entre $\llbracket 1; n \rrbracket$ et E et une bijection ψ entre $\llbracket 1; m \rrbracket$ et E , alors l'application $\psi^{-1} \circ \varphi$ est une bijection de $\llbracket 1; n \rrbracket$ vers $\llbracket 1; m \rrbracket$. Pour conclure, il suffit donc de démontrer que s'il existe une bijection de $\llbracket 1; n \rrbracket$ dans $\llbracket 1; m \rrbracket$, alors nécessairement $n = m$.

Pour cela, on procède par récurrence. Pour $n \in \mathbb{N}$, on pose

\mathcal{P}_n : Pour tout $m \geq 0$, si $\llbracket 1; n \rrbracket$ est en bijection avec $\llbracket 1; m \rrbracket$ alors $n = m$.

Initialisation : La propriété \mathcal{P}_0 est vraie car l'ensemble vide n'est en bijection qu'avec lui-même.

Héritéité : Fixons $n \geq 0$ tel que \mathcal{P}_n est vraie et démontrons \mathcal{P}_{n+1} . Soit $m \geq 0$ tel qu'il existe une bijection φ entre $\llbracket 1; n+1 \rrbracket$ et $\llbracket 1; m \rrbracket$. Démontrons que $n+1 = m$. Distinguons deux cas :

▷ 1er cas : $\varphi(n+1) = m$: Dans ce cas, φ induit une bijection entre $\llbracket 1; n \rrbracket$ et $\llbracket 1; m-1 \rrbracket$ et l'hypothèse de récurrence permet d'en déduire que $n = m-1$, c'est-à-dire $n+1 = m$.

▷ 2ème cas : $\varphi(n+1) \neq m$: Posons $a = \varphi(n+1)$ et considérons σ l'application de $\llbracket 1; m \rrbracket$ dans lui-même qui échange a et m et laisse fixe les autres points. Comme σ est bijective (c'est une involution), l'application $\psi = \varphi \circ \sigma$ est aussi une bijection (comme composée de deux bijections) entre $\llbracket 1; n+1 \rrbracket$ et $\llbracket 1; m \rrbracket$ telle que $\psi(n+1) = m$. On est donc ramené au cas précédent.

Dans les deux cas, on a donc démontré que \mathcal{P}_{n+1} est vraie.

Conclusion : D'après le principe de récurrence, la propriété \mathcal{P}_n est vraie pour tout $n \in \mathbb{N}$. ■

On gardera à l'esprit que, derrière l'habillage abstrait de cette définition (nécessaire à la rigueur), se cache le concept très simple de « nombre d'éléments d'un ensemble ».

Exemples :

- L'ensemble vide \emptyset est un ensemble fini de cardinal 0.
- L'ensemble $\{\spadesuit, \heartsuit, \diamondsuit, \clubsuit\}$ est de cardinal 4.
- Si $n \in \mathbb{N}$, l'ensemble $\llbracket 1; n \rrbracket$ est fini et de cardinal n .
Si $m \leq n$, alors $\llbracket m; n \rrbracket$ est un ensemble fini de cardinal $n - m + 1$ (attention au +1 !!).
- Une bijection de $\llbracket 1; n \rrbracket$ dans E permet d'indexer les éléments de E et d'écrire l'ensemble en extension : $E = \{x_1, x_2, \dots, x_n\}$.
Mais attention, réciproquement, si $E = \{x_1, x_2, \dots, x_n\}$, on ne peut pas en déduire que $\text{card}(E) = n$ mais seulement que $\text{card}(E) \leq n$ puisque certains x_k peuvent être égaux.

A.2. Cardinal d'une partie

L'énoncé suivant est élémentaire mais fondamental. Nous verrons une propriété analogue portant sur les dimensions en algèbre linéaire.

Proposition 1

Soit E un ensemble fini. Si A est une partie de E , alors A est fini et l'on a $\text{card } A \leq \text{card } E$ avec égalité si, et seulement si, $A = E$.

- On procède par récurrence. Pour $n \in \mathbb{N}$, on appelle \mathcal{P}_n la propriété « si E est fini de cardinal n et A est une partie de E alors A est finie et $\text{card } A \leq n$ avec égalité si, et seulement si, $A = E$ ».

Initialisation: La propriété \mathcal{P}_0 est vraie car la seule partie de l'ensemble vide est l'ensemble vide.

Héritéité: Fixons $n \geq 0$ tel que \mathcal{P}_n est vraie et démontrons \mathcal{P}_{n+1} . Considérons E un ensemble fini de cardinal $n+1$ et A une partie de E . On veut démontrer que A est fini et que $\text{card } A \leq n+1$ avec égalité si, et seulement si, $A = E$. Cela revient au même de démontrer que ou bien A est fini et $\text{card } A \leq n$, ou bien $A = E$.

Si $A = E$, il n'y a donc rien à faire.

Si $A \neq E$, on introduit $b \in E \setminus A$. Comme E est fini de cardinal $n+1$, on sait que l'on peut introduire une bijection φ entre $\llbracket 1; n+1 \rrbracket$ et E . Quitte à composer ψ par l'application σ de $\llbracket 1; n+1 \rrbracket$ dans lui-même qui échange $\varphi(n+1)$ et b et laisse fixe les autres points (comme nous l'avons déjà fait pour la démonstration de l'unicité du cardinal), on peut supposer que $\varphi(n+1) = b$. Dès lors, φ induit une bijection entre $\llbracket 1; n \rrbracket$ et $E \setminus \{b\}$, ce qui signifie que $\text{card}(E \setminus \{b\}) = n$. Comme A est une partie de $E \setminus \{b\}$, l'hypothèse de récurrence implique que A est fini et $\text{card}(A) \leq n$.

On a ainsi démontré que \mathcal{P}_{n+1} est vraie.

Conclusion: D'après le principe de récurrence, la propriété \mathcal{P}_n est vraie pour tout $n \in \mathbb{N}$. ■



Habituellement, pour démontrer l'égalité de deux ensembles, on procède par double-inclusion. Cette proposition nous dit que, dans le cadre des ensembles finis, il suffit de démontrer une seule des deux inclusions dès lors que l'on sait que les deux ensembles sont de même cardinal.

C'est un prototype de résultats que je surnomme les « théorèmes Bonux » : avec la condition de cardinalité, on ne fait que la moitié du travail, l'autre moitié est offerte en cadeau dans le paquet !

Le résultat de cette proposition montre qu'il est impossible qu'un ensemble fini E soit en bijection avec l'une de ses parties strictes (c'est-à-dire toutes les parties de E sauf E lui-même).

Par conséquent, la bijection $n \mapsto 2n$ entre l'ensemble des entiers naturels \mathbb{N} et l'ensemble des nombres pairs $2\mathbb{N}$ montre que \mathbb{N} est infini. Elle montre aussi qu'il est possible qu'un ensemble infini soit en bijection avec l'une de ses parties strictes. Pour tout dire, c'est même une caractérisation des ensembles infinis !

A.3. Cardinal d'une réunion

Proposition 2

Si E et F sont deux ensembles finis **disjoints**, alors $E \cup F$ est fini et l'on a

$$\text{card}(E \cup F) = \text{card } E + \text{card } F.$$

Plus généralement, si E_1, \dots, E_p sont des ensembles finis **disjoints deux à deux**, alors

$$\text{card}(E_1 \cup \dots \cup E_p) = \sum_{k=1}^p \text{card } E_k.$$

■ Soient E, F deux ensembles finis et disjoints, de cardinaux respectifs n et m . Il existe alors une bijection φ entre $\llbracket 1; n \rrbracket$ et E et une bijection ψ entre $\llbracket 1; m \rrbracket$ et F . L'application $\chi : \llbracket 1; n+m \rrbracket \longrightarrow E \cup F$ telle que

$$\forall k \in \llbracket 1; n \rrbracket, \quad \chi(k) = \varphi(k) \quad \text{et} \quad \forall k \in \llbracket n+1; n+m \rrbracket, \quad \chi(k) = \psi(k-n)$$

réalise alors une bijection entre $\llbracket 1; n+m \rrbracket$ et $E \cup F$ (l'injectivité découle de la disjonction de E et F et la surjectivité est évidente). Il en résulte que $\text{card}(E \cup F) = n+m = \text{card } E + \text{card } F$.

La deuxième formule se démontre par récurrence sur p . ■

Cette proposition est la base d'un premier principe de dénombrement décrit ci-dessous.

Le principe du « ou »

Souvent, pour dénombrer un ensemble, on découpe celui-ci en plusieurs sous-ensembles complémentaires et disjoints qui sont faciles à dénombrer individuellement. Le cardinal de l'ensemble global est alors la somme des cardinaux des sous-ensembles.

Dans la rédaction d'une solution de ce type, on doit proprement distinguer chacun des cas en les séparant par des « ou bien ».

Exemples :

- Pour dénombrer les mains de 5 cartes ayant au plus deux piques, on dénombre séparément les mains ayant 0 pique, celles avec 1 pique et celles avec 2 piques puis on ajoute les résultats.

Si un ensemble T est partitionné en m parties de même cardinal p , la proposition 2 nous dit que $\text{card}(T) = mp$. Mais « pourquoi ces notations T , m et p ? » me direz-vous. Et bien, parce qu'on a l'habitude d'imaginer que T est un troupeau de m moutons ayant chacun p pattes ! On obtient ainsi un second principe de dénombrement (un cas particulier du principe du « ou »).

Lemme des berger

Pour compter ses moutons, un berger, paresseusement allongé sur l'herbe, compte les pattes de ses ovins et divise par 4. Aussi élémentaire qu'il soit, ce principe peut être utile : il est parfois plus simple de compter chaque configuration p fois puis de diviser par p .

Attention aux vilains canards planqués au milieu du troupeau ! Autrement dit, si les différentes configurations n'ont pas le même cardinal, il est impossible d'utiliser le lemme des berger.

Autre avertissement : éviter le plus possible l'utilisation du lemme des berger ! Autrement dit, lorsque vous dénombrez des objets, essayez toujours de ne compter chaque objet qu'une seule fois. En effet, bien souvent, lorsque l'individu moyen^(†) compte chaque configuration plusieurs fois, il oublie la division finale du principe des berger...

[†] Je ne parle évidemment pas de toi, lecteur... Toi, ô roseau d'argent de la finesse, tu es exceptionnel !

Lorsque les ensembles ne sont pas disjoints, on doit utiliser la formule de Poincaré pour deux ensembles ou sa généralisation pour un plus grand nombre d'ensembles : la formule du crible.

Proposition 3

Si E et F sont deux ensembles finis, alors $E \cup F$ est fini et on a la [formule de Poincaré](#)

$$\text{card}(E \cup F) = \text{card } E + \text{card } F - \text{card}(E \cap F).$$

Plus généralement, si E_1, \dots, E_p sont des ensembles finis, alors $E_1 \cup \dots \cup E_p$ est fini et on a la [formule du crible](#)

$$\text{card}(E_1 \cup \dots \cup E_p) = \sum_{k=1}^p (-1)^{k-1} \underbrace{\sum_{1 \leq i_1 < \dots < i_k \leq p} \text{card}(E_{i_1} \cap \dots \cap E_{i_k})}_{\binom{p}{k} \text{ termes}}.$$

■ En appliquant le résultat de la proposition 2 au couple d'ensembles disjoints $(E; F \setminus E)$ dont la réunion est $E \cup F$, on obtient que $E \cup F$ est fini et

$$\text{card}(E \cup F) = \text{card}(E \cup (F \setminus E)) = \text{card } E + \text{card}(F \setminus E).$$

En appliquant une seconde fois le résultat de la proposition 2, cette fois au couple d'ensembles disjoints $(F \setminus E, E \cap F)$ dont la réunion est F , on obtient

$$\text{card } F = \text{card}((F \setminus E) \cup (E \cap F)) = \text{card}(F \setminus E) + \text{card}(E \cap F).$$

En remplaçant dans la première égalité la quantité $\text{card}(F \setminus E)$ par son expression donnée par la seconde égalité, on obtient la formule de Poincaré.

[P] La démonstration de la formule du crible est hors-programme. Elle est donc présentée ci-dessous à titre purement culturel...
Démontrons par récurrence la propriété P_p , définie pour tout $p \in N^*$, par

$$P_p : \quad \forall E_1, \dots, E_p, \quad \text{card}(E_1 \cup \dots \cup E_p) = \sum_{k=1}^p (-1)^{k-1} \sum^{(p)} \text{card}(E_{i_1} \cap \dots \cap E_{i_k}),$$

où le symbole $\sum^{(p)}$ désigne la somme étendue sur les k -uplets (i_1, \dots, i_k) tels que $1 \leq i_1 < \dots < i_k \leq p$.

Initialisation : La formule est claire pour $p = 1$. C'est la formule de Poincaré pour $p = 2$.

Héritéité : Soit $p \geq 2$. Supposons que P_p est vraie et démontrons P_{p+1} . Soient E_1, \dots, E_p, E_{p+1} une famille de $p+1$ ensembles finis. L'ensemble $E_1 \cup \dots \cup E_p$ est fini (par H.R) donc, d'après la formule de Poincaré, $E_1 \cup \dots \cup E_p \cup E_{p+1}$ l'est aussi et l'on a

$$\begin{aligned} \text{card}(E_1 \cup \dots \cup E_p \cup E_{p+1}) &= \text{card}(E_1 \cup \dots \cup E_p) + \text{card}(E_{p+1}) - \text{card}((E_1 \cup \dots \cup E_p) \cap E_{p+1}) \\ &= \text{card}(E_1 \cup \dots \cup E_p) + \text{card}(E_{p+1}) - \text{card}((E_1 \cap E_{p+1}) \cup \dots \cup (E_p \cap E_{p+1})). \end{aligned}$$

En appliquant deux fois l'hypothèse de récurrence, on a

$$\begin{aligned} \text{card}(E_1 \cup \dots \cup E_p) &= \sum_{k=1}^p (-1)^{k-1} \sum^{(p)} \text{card}(E_{i_1} \cap \dots \cap E_{i_k}) \\ &= \text{card}(E_1) + \text{card}(E_2) + \dots + \text{card}(E_p) + \sum_{k=2}^p (-1)^{k-1} \sum^{(p)} \text{card}(E_{i_1} \cap \dots \cap E_{i_k}) \end{aligned}$$

et

$$\begin{aligned} \text{card}((E_1 \cap E_{p+1}) \cup \dots \cup (E_p \cap E_{p+1})) &= \sum_{k=1}^p (-1)^{k-1} \sum^{(p)} \text{card}((E_{i_1} \cap E_{p+1}) \cap \dots \cap (E_{i_k} \cap E_{p+1})) \\ &= \sum_{k=1}^p (-1)^{k-1} \sum^{(p)} \text{card}(E_{i_1} \cap \dots \cap E_{i_k} \cap E_{p+1}). \end{aligned}$$

Donc

$$\begin{aligned} \text{card}(E_1 \cup \dots \cup E_{p+1}) &= \text{card}(E_1) + \dots + \text{card}(E_p) + \sum_{k=2}^p (-1)^{k-1} \sum^{(p)} \text{card}(E_{i_1} \cap \dots \cap E_{i_k}) \\ &\quad + \text{card}(E_{p+1}) \\ &\quad - \sum_{k=1}^p (-1)^{k-1} \sum^{(p)} \text{card}(E_{i_1} \cap \dots \cap E_{i_k} \cap E_{p+1}) \\ &= \text{card}(E_1) + \dots + \text{card}(E_p) + \text{card}(E_{p+1}) + \sum_{k=2}^{p+1} (-1)^k \sum^{(p+1)} \text{card}(E_{i_1} \cap \dots \cap E_{i_k}) \\ &= \sum_{k=1}^{p+1} (-1)^k \sum^{(p+1)} \text{card}(E_{i_1} \cap \dots \cap E_{i_k}), \end{aligned}$$

ce qui démontre P_{p+1} .

Conclusion : Le principe de récurrence permet de conclure. ■

Dans le calcul de $\text{card}(E \cup F)$, en ajoutant $\text{card } E$ et $\text{card } F$, on compte deux fois les éléments de $E \cap F$. C'est pourquoi, il faut retrancher une fois le cardinal de cette intersection.

La formule du crible peut paraître affreuse à première vue. Elle n'est en fait pas si compliquée que cela.

La formule du crible, c'est pas si dur !

La formule du crible est en apparence compliquée. On peut en fait la décrire de manière assez simple. Pour calculer $\text{card}(E_1 \cup \dots \cup E_p)$, on effectue les étapes suivantes :

- on ajoute les cardinaux de chaque ensemble, c'est-à-dire

$$\sum_{1 \leq i \leq p} \text{card}(E_i) = \text{card}(E_1) + \dots + \text{card}(E_p);$$

- on retranche les cardinaux de toutes les intersections de deux ensembles, c'est-à-dire

$$\begin{aligned} \sum_{1 \leq i_1 < i_2 \leq p} \text{card}(E_{i_1} \cap E_{i_2}) &= \text{card}(E_1 \cap E_2) + \text{card}(E_1 \cap E_3) + \dots + \text{card}(E_1 \cap E_p) \\ &\quad + \text{card}(E_2 \cap E_3) + \dots + \text{card}(E_2 \cap E_p) \\ &\quad + \dots \\ &\quad + \text{card}(E_{p-1} \cap E_p); \end{aligned}$$

- on ajoute les cardinaux de toutes les intersections de trois ensembles ;
- etc (en alternant les « on ajoute » et les « on retranche » tout en augmentant d'une unité à chaque étape le nombre d'ensembles intersectés).

Exemples :

- Dans le cas $n = 3$, la formule du crible donne

$$\begin{aligned} \text{card}(A \cup B \cup C) &= \text{card}(A) + \text{card}(B) + \text{card}(C) \\ &\quad - \text{card}(A \cap B) - \text{card}(B \cap C) - \text{card}(C \cap A) \\ &\quad + \text{card}(A \cap B \cap C). \end{aligned}$$

- Dans le cas $n = 4$, on obtient

$$\begin{aligned} \text{card}(A \cup B \cup C \cup D) &= \text{card}(A) + \text{card}(B) + \text{card}(C) + \text{card}(D) \\ &\quad - \text{card}(A \cap B) - \text{card}(A \cap C) - \text{card}(A \cap D) \\ &\quad - \text{card}(B \cap C) - \text{card}(B \cap D) - \text{card}(C \cap D) \\ &\quad + \text{card}(A \cap B \cap C) + \text{card}(A \cap B \cap D) \\ &\quad + \text{card}(A \cap C \cap D) + \text{card}(B \cap C \cap D) \\ &\quad - \text{card}(A \cap B \cap C \cap D). \end{aligned}$$

a.4. Cardinal du complémentaire

Proposition 4

Soient E un ensemble fini et A, B deux parties de E . Alors

- (i) $\text{card}(E \setminus A) = \text{card } E - \text{card } A$;
- (ii) $\text{card}(B \setminus A) = \text{card } B - \text{card}(A \cap B)$.

- (i) En appliquant la formule de Poincaré aux ensembles disjoints A et $E \setminus A$ dont la réunion est E , on obtient

$$\text{card } E = \text{card } (A \cup (E \setminus A)) = \text{card } A + \text{card}(E \setminus A),$$

ce qui donne immédiatement le résultat.

- (ii) En appliquant la formule de Poincaré aux ensembles disjoints $B \setminus A$ et $A \cap B$ dont la réunion est B , on obtient

$$\text{card } B = \text{card } ((B \setminus A) \cup (A \cap B)) = \text{card}(B \setminus A) + \text{card}(A \cap B),$$

ce qui donne immédiatement le résultat. ■

La première de ces deux formules est généralement écrite en utilisant la notation \bar{A} pour désigner le complémentaire de A dans E , ce qui donne

$$\text{card } \bar{A} = \text{card } E - \text{card } A.$$

Cette formule est à la base d'un nouveau principe de dénombrement exposé ci-dessous.

Passage au contraire

Pour dénombrer une partie d'un ensemble, il est parfois plus simple de dénombrer son complémentaire. Le cardinal de la partie considérée est alors la différence entre le cardinal de l'ensemble global et celui du complémentaire de cette partie.

Exemples :

- Pour dénombrer les mains de 5 cartes ayant au plus quatre piques, il est fastidieux de dénombrer les mains ayant 0 pique, celles avec 1 pique, celles avec 2 piques, celles avec 3 piques et celles avec 4 piques. On préférera dénombrer les mains avec 5 piques et soustraire le cardinal trouvé du nombre total de mains de 5 cartes.

A.5. Cardinal d'un produit cartésien

Proposition 5

Si E et F sont deux ensembles finis, alors $E \times F$ est fini et

$$\text{card}(E \times F) = \text{card } E \times \text{card } F.$$

Plus généralement, si E_1, \dots, E_p sont des ensembles finis, alors $E_1 \times \dots \times E_p$ est fini et

$$\text{card}(E_1 \times \dots \times E_p) = \prod_{k=1}^p \text{card } E_k.$$

■ Posons $E = \{x_1, \dots, x_p\}$ et $F = \{y_1, \dots, y_n\}$. On peut alors représenter les éléments du produit cartésien $E \times F$ sous forme d'un tableau à p lignes et n colonnes :

$\begin{array}{c} F \\ \diagdown \\ E \end{array}$	y_1	y_2	\dots	y_n
x_1	(x_1, y_1)	(x_1, y_2)	\dots	(x_1, y_n)
x_2	(x_2, y_1)	(x_2, y_2)	\dots	(x_2, y_n)
\vdots	\vdots	\vdots	\ddots	\vdots
x_p	(x_p, y_1)	(x_p, y_2)	\dots	(x_p, y_n)

En apparence, cela semble nous permettre de conclure. En effet, on sait bien qu'un tableau à p lignes et n colonnes possède pn cases, ce qui démontre que $\text{card}(E \times F) = pn = \text{card } E \times \text{card } F$.

Mais voilà, à bien y réfléchir, la recette « un tableau à p lignes et n colonnes possède pn cases » est précisément ce que l'on souhaite démontrer. Le raisonnement précédent est donc un « joli » cercle vicieux.

Plus proprement, on constate que $E \times F$ est la réunion disjointe des lignes du tableau, c'est-à-dire

$$E \times F = (\{x_1\} \times F) \cup (\{x_2\} \times F) \cup \dots \cup (\{x_n\} \times F)$$

Or, pour tout $k \in \llbracket 1; p \rrbracket$, on vérifie aisément que l'application $\varphi_k : \llbracket 1; n \rrbracket \longrightarrow \{x_k\} \times F$ définie par $\forall \ell \in \llbracket 1; n \rrbracket, \varphi_k(\ell) = (x_k, y_\ell)$ est une bijection, ce qui donne

$$\text{card}(\{x_k\} \times F) = n.$$

On en déduit, d'après la proposition 2, que $E \times F$ est fini et que

$$\text{card}(E \times F) = \sum_{k=1}^p \text{card}(\{x_k\} \times F) = \sum_{k=1}^p n = pn = \text{card } E \times \text{card } F.$$

La deuxième formule se démontre par récurrence sur p . ■

Ce résultat permet d'énoncer l'un des plus importants principes de dénombrement.

Le principe du « et »

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

Dans la rédaction d'une solution de ce type, on dénombre chacune des étapes en les séparant par des « et ».

Exemples :

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

B. Choix successifs

B.1. Listes

Définition 2

Soit E un ensemble fini. Une p -liste de E est un p -uplet d'éléments de E .

Une p -liste de E est donc la donnée successive de p éléments pris parmi les n éléments de E : l'ordre des éléments compte et il peut y avoir des répétitions.

Exemples :

- $(1; 3; 5; 3)$ et $(3; 5; 4; 2)$ sont deux 4-listes de $\llbracket 1; 5 \rrbracket$.
- $(1; 2; 2)$ et $(2; 2; 1)$ sont deux 3-listes distinctes.

La proposition suivante donne le nombre de listes de p éléments pris parmi n .

Proposition 6

Soit E est un ensemble fini de cardinal n . Le nombre de p -listes de E vaut n^p .

■ Pour dénombrer les p -listes (x_1, \dots, x_p) de E , on commence par choisir x_1 parmi les n éléments de E , puis on choisit x_2 parmi les n éléments de E , ..., puis on choisit x_p parmi les n éléments de E distincts de x_1, x_2, \dots, x_{p-1} . D'après le principe du « et », il y a donc n^p p -listes de E .

Autre preuve : L'ensemble des p -listes est E^p et $\text{card}(E^p) = (\text{card } E)^p = n^p$ d'après le corollaire 5. ■

Choix successifs avec répétitions éventuelles

On utilise les p -listes dans les problèmes de choix successifs de p éléments d'un ensemble, avec d'éventuelles répétitions.

Cela permet ainsi de dénombrer le nombre d'issues possibles lorsqu'on effectue p fois indépendamment une même expérience.

Dans la pratique, on invoque rarement le fait que l'on utilise une liste : on préfère expliquer les choix successifs que l'on effectue et appliquer le principe du « et ».

Exemples :

- Déterminons le nombre de mots de 3 lettres (ayant un sens ou non). Pour en constituer un, on choisit successivement :

- * une première lettre dans l'alphabet : 26 choix ;
- * une deuxième lettre dans l'alphabet : 26 choix ;
- * une troisième lettre dans l'alphabet : 26 choix ;

Il y a donc $26^3 = 17\,576$ mots distincts de 3 lettres. Ce sont en fait les éléments de l'ensemble $\{A, B, C, \dots, Z\}^3$ dont le cardinal est bien 26^3 .

- Un octet est une unité de mémoire informatique constituée d'une succession de huit chiffres binaires (c'est-à-dire 0 ou 1). Pour constituer un octet, on choisit successivement :

- * un premier chiffre dans $\{0; 1\}$: 2 choix ;
- * un deuxième chiffre dans $\{0; 1\}$: 2 choix ;
- ⋮
- * un huitième chiffre dans $\{0; 1\}$: 2 choix ;

Il y a donc $2^8 = 256$ octets différents. Ce sont en fait les éléments de l'ensemble $\{0; 1\}^8$ dont le cardinal est bien 2^8 .

B.2. Listes sans répétition (arrangements)

Définition 3

Soit E un ensemble fini. Une p -liste sans répétition (ou p -arrangement) de E est une p -liste constituée d'éléments de E qui sont distincts deux à deux.

Dans une p -liste sans répétition, l'ordre des éléments compte et il ne peut pas y avoir de répétition.

Exemples :

- $(1; 2; 5)$ et $(1; 5; 2)$ sont deux 3-listes sans répétition distinctes de $\llbracket 1; 5 \rrbracket$.
- $(1; 3; 1)$ n'est pas une 3-liste sans répétition car 1 est répété deux fois.

La proposition suivante donne le nombre de listes sans répétition de p éléments pris parmi n .

Proposition 7

Soit E un ensemble fini de cardinal n . Le nombre de p -listes sans répétition de E vaut $n(n - 1)(n - 2) \cdots (n - p + 1)$. En particulier, il est nul si $p > n$.

■ Pour dénombrer les p -listes (x_1, \dots, x_p) de E dont les éléments sont distincts deux à deux, on commence par choisir x_1 parmi les n éléments de E , puis on choisit x_2 parmi les $n - 1$ éléments de E distincts de x_1 , puis on choisit x_3 parmi les $n - 2$ éléments de E distincts de x_1 et x_2 , ..., puis on choisit x_p parmi les $n - p + 1$ éléments de E distincts de x_1, x_2, \dots, x_{p-1} . Il y a donc $n(n - 1)(n - 2) \cdots (n - p + 1)$ p -listes sans répétition de E , ce qui démontre le résultat. ■

La quantité $n(n - 1)(n - 2) \cdots (n - p + 1)$, quelquefois appelée coefficient d'arrangement, peut s'exprimer à l'aide de factorielles :

$$n(n - 1)(n - 2) \cdots (n - p + 1) = \begin{cases} \frac{n!}{(n - p)!} & \text{si } 0 \leq p \leq n, \\ 0 & \text{si } p > n. \end{cases}$$

Choix successifs sans répétition

On utilise les p -listes sans répétition dans les problèmes de choix successifs de p éléments pris parmi n , sans répétition.

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

On utilise rarement les listes sans répétition : on préfère décrire les choix successifs effectués. La notion de liste sans répétition n'est d'ailleurs pas étudiée chez les anglo-saxons : pour eux, ce n'est qu'un cas particulier de l'application du « et ».

Exemples :

- Pour déterminer le nombre de podiums dans une course de 100 m, on choisit le médaillé d'or : 8 choix, puis celui d'argent : 7 choix et enfin celui de bronze : 6 choix. Le nombre de podiums possibles vaut donc $8 \times 7 \times 6 = 336$.

B.3. Permutations

Définition 4

Soit E un ensemble fini de cardinal n . Une **permutation** de E est une n -liste sans répétition (constituée par conséquent des n éléments de E).

Une permutation d'un ensemble E est donc une liste sans répétition de tous les éléments de E : chaque élément apparaît exactement une fois et l'ordre compte.

Exemples :

- $(1; 2; 3)$ et $(1; 3; 2)$ sont deux permutations de $\{1; 2; 3\}$ mais pas de $\{1; 2; 3; 4\}$.
- $(5; 3; 4; 2; 5)$ n'est pas une permutation car 5 se répète deux fois.

La proposition suivante donne le nombre de permutations des éléments d'un ensemble fini.

Proposition 8

Soit E un ensemble fini de cardinal n . Le nombre de permutations de E est égal à $n!$

- Une permutation est une n -liste sans répétition. Il y en a donc $n(n - 1)(n - 2) \cdots (n - n + 1) = n!$ ■

Permutations

Les permutations interviennent dans les problèmes où l'on veut ordonner tous les éléments d'un ensemble (sans répétition).

Pour justifier un dénombrement de permutations, on utilise généralement le verbe « permute » (tout bêtement).

Exemples :

- Le nombre de façons de permute les 7 nains dans leurs 7 petits lits vaut $7!$

2 h 30

C. Choix simultanés

C.1. Coefficients binomiaux

Nous avons déjà rencontré les coefficients binomiaux dans la formule du binôme. Nous les retrouvons ici comme outil de dénombrement.

Définition 5

Soient $n \in \mathbb{N}$ et $p \in \mathbb{Z}$. Le coefficient binomial $\binom{n}{p}$, qui se lit « p parmi n », est défini par

$$\binom{n}{p} = \begin{cases} \frac{n!}{p!(n-p)!} & \text{si } 0 \leq p \leq n, \\ 0 & \text{si } p > n \text{ ou } p < 0. \end{cases}$$

Nous verrons que sur un arbre représentant une série de n épreuves de Bernoulli, le coefficient binomial $\binom{n}{p}$ est le nombre de chemins conduisant à p succès. C'est d'ailleurs ainsi que vous aviez défini les coefficients binomiaux en Première.

Exemples :

- $\binom{n}{0} = \binom{n}{n} = 1$
- Pour calculer $\binom{n}{p}$, on peut retenir le principe suivant :

$$\boxed{\binom{n}{p} = \frac{\text{« }p\text{ qui descendent depuis }n\text{ »}}{\text{« }p\text{ qui montent depuis }1\text{ »}}}$$

ce qui donne, par exemple,

$$\binom{n}{1} = n, \quad \binom{n}{2} = \frac{n(n-1)}{2} \quad \text{et} \quad \binom{n}{3} = \frac{n(n-1)(n-2)}{6}.$$

Les principales propriétés des coefficients binomiaux sont rappelées dans l'énoncé suivant.

Proposition 9

Pour $n \in \mathbb{N}$ et $p \in \mathbb{Z}$, on a

$$\binom{n}{p} = \binom{n}{n-p} \quad (\text{formule de symétrie}),$$

$$\binom{n}{p} = \frac{n}{p} \binom{n-1}{p-1} \quad (\text{formule du pion}, \quad n, p \neq 0),$$

$$\binom{n}{p} = \binom{n-1}{p} + \binom{n-1}{p-1} \quad (\text{relation de Pascal}, \quad n \neq 0).$$

■ AQT ■

Rappelons que la relation de Pascal permet de calculer par récurrence les coefficients binomiaux en les disposant en pyramide : c'est le triangle de Pascal.

C.2. Combinaisons

Définition 6

Soit E un ensemble fini. Une p -combinaison de E est une partie de E de cardinal p .

Alors que les listes sont notées entre parenthèses pour tenir compte de l'ordre des éléments, les combinaisons sont notées entre accolades, comme les ensembles, et l'ordre des éléments ne compte pas. Il est également impossible d'y répéter un élément.

Exemples :

- $\{1; 3; 5\}$ et $\{2; 3; 4; 5\}$ sont deux combinaisons de $\llbracket 1; 5 \rrbracket$.
- $\{1; 2; 3\}$ et $\{1; 3; 2\}$ sont deux 3-combinaisons identiques.
- $\{1; 3; 1\}$ est une 2-combinaison que l'on écrit $\{1; 3\}$ car la répétition du 1 n'est pas utile.

La proposition suivante donne le nombre de combinaisons de p éléments pris parmi n .

Proposition 10

Soit E un ensemble fini de cardinal n . Le nombre de p -combinaisons de E est égal à $\binom{n}{p}$. En particulier, il est nul si $p > n$.

■ Une combinaison permet de fabriquer des listes sans répétition par permutation de ses éléments. Pour chaque p -combinaison, on fabrique ainsi $p!$ p -listes sans répétition. Il y a donc $p!$ fois plus de p -listes sans répétition que de p -combinaisons. Comme le nombre de p -listes sans répétition vaut $n(n-1) \cdots (n-p+1)$, le nombre de p -combinaisons est donc $n(n-1) \cdots (n-p+1)/p! = \binom{n}{p}$ d'après le lemme des bergers. ■

Choix simultanés

On utilise les p -combinaisons dans les problèmes de choix simultanés de p éléments pris parmi n (sans considération d'ordre et sans répétition).

Exemples :

- À l'ancien loto, on choisissait 6 numéros dans $\llbracket 1; 49 \rrbracket$, d'où $\binom{49}{6} = 13\,983\,816$ grilles possibles.
- Pour écrire une anagramme de MISSISSIPPI, on doit choisir successivement :
 - * 1 emplacement parmi les 11 possibles pour le M, ce qui laisse $\binom{11}{1} = 11$ possibilités ;
 - * 4 emplacements parmi les 10 restants pour les I, ce qui laisse $\binom{10}{4} = 210$ possibilités ;
 - * 4 emplacements parmi les 6 restants pour les S, ce qui laisse $\binom{6}{4} = 15$ possibilités ;
 - * 2 emplacements parmi les 2 restants pour les P, ce qui laisse $\binom{2}{2} = 1$ possibilité.

On trouve finalement $11 \times 210 \times 15 \times 1 = 34\,650$ anagrammes différentes de MISSISSIPPI.

- Choisir, dans un paquet de n bonbons, les p que l'on va manger revient à choisir les $n - p$ que l'on ne mangera pas. Donc $\binom{n}{p} = \binom{n}{n-p}$ ce qui (re)démontre la formule de symétrie.
- À la Star Ac', il y a n candidats dont k qui passent à la télé et 1 gagnant. On choisit d'abord les k candidats pour la télé puis le gagnant parmi ces k -là : $\binom{n}{k} \binom{k}{1}$ possibilités. Mais la Star Ac', c'est truqué ! Le gagnant est choisi dès le départ (parmi les n candidats), puis on choisit $k - 1$ perdants (parmi $n - 1$ candidats) pour passer à la télé à ses côtés : $\binom{n}{1} \binom{n-1}{k-1}$ possibilités. En égalant les deux résultats, on obtient la formule du pion.
- Dans le développement de $(a + b)^n$, le nombre de termes de la forme $a^k b^{n-k}$, où $k \in \llbracket 0; n \rrbracket$, est égal au nombre de façons de choisir k facteurs a parmi n facteurs puis $n - k$ facteurs b parmi les $n - k$ facteurs restants. Il y a donc $\binom{n}{k} \binom{n-k}{n-k} = \binom{n}{k}$ termes de la forme $a^k b^{n-k}$, où $k \in \llbracket 0; n \rrbracket$, dans le développement de $(a + b)^n$. Cela (re)démontre la formule du binôme.

C.3. Ensemble des combinaisons

Rappelons que l'ensemble $\mathcal{P}(E)$ désigne l'ensemble de tous les sous-ensembles de E . Dans le cas où E est fini, on peut reformuler la définition de $\mathcal{P}(E)$ de la façon suivante.

Définition 7

Soit E un ensemble fini. On note $\mathcal{P}(E)$ l'ensemble de toutes les combinaisons de E .

Exemples :

- $\mathcal{P}(\{a; b; c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{c, a\}, \{a, b, c\}\}$.

La proposition suivante donne le cardinal de $\mathcal{P}(E)$.

Proposition 11

Soit E est un ensemble fini de cardinal n . Le cardinal de l'ensemble $\mathcal{P}(E)$ de toutes les combinaisons de E est donné par

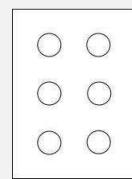
$$\text{card } \mathcal{P}(E) = 2^n.$$

■ Deux démonstrations pour le prix d'une.

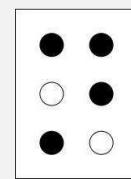
- ▷ Pour obtenir toutes les combinaisons de E , il suffit de réunir les 0-combinaisons, qui sont au nombre de $\binom{n}{0}$, les 1-combinaisons, qui sont au nombre de $\binom{n}{1}$, ..., les n -combinaisons, qui sont au nombre de $\binom{n}{n}$. Donc $\text{card } \mathcal{P}(E) = \binom{n}{0} + \dots + \binom{n}{n} = 2^n$, d'après la formule du binôme de Newton.
- ▷ Notons $E = \{x_1, \dots, x_n\}$. Pour fabriquer une combinaison de E , on doit décider successivement si l'on y met x_1 : 2 choix, si l'on y met x_2 : 2 choix, ..., si l'on y met x_n : 2 choix. Il y a donc 2^n combinaisons de E . ■

Exemples :

- Le nombre de poignées (différentes) de bonbons que l'on peut piocher dans un paquet de n bonbons est le nombre de combinaisons dans un ensemble de cardinal n . Il vaut donc 2^n .
- Un caractère de l'écriture Braille, destinée aux aveugles, est formé de points en relief obtenus en piquant une feuille de papier à travers au moins un des six points disposés sur un rectangle de 2 points de large sur 3 points de haut, comme l'illustrent les figures ci-dessous :



grille Braille



lettre N

Déterminons le nombre de caractères Braille.

On applique le « principe du ou » en distinguant les cas suivants :

Pour un caractère Braille avec 1 point, on choisit 1 point parmi 6 : $\binom{6}{1}$ possibilités.

Pour un caractère Braille avec 2 points, on choisit 2 points parmi 6 : $\binom{6}{2}$ possibilités.

⋮

Pour un caractère Braille avec 6 points, on choisit 6 points parmi 6 : $\binom{6}{6}$ possibilités.

Ainsi, le nombre de caractères Braille vaut $\sum_{k=1}^6 \binom{6}{k} = \sum_{k=0}^6 \binom{6}{k} - \binom{6}{0} = 2^6 - 1 = 63$.

D. Applications entre ensembles finis

D.1. Injection, surjection, bijection et cardinal

Le théorème suivant fait le lien entre la notion de cardinal et les notions d'injection, de surjection et de bijection.

Théorème 1

Soient E et F deux ensembles finis.

- (i) Il existe une injection de E dans F si, et seulement si, $\text{card } E \leq \text{card } F$.
- (ii) Il existe une surjection de E sur F si, et seulement si, $\text{card } E \geq \text{card } F$.
- (iii) Il existe une bijection entre E et F si, et seulement si, $\text{card } E = \text{card } F$.

- (i) Supposons qu'il existe une injection f de E dans F . Notons $E = \{x_1, \dots, x_p\}$ de sorte que l'on ait $f(E) = \{f(x_1), \dots, f(x_p)\}$. Comme f est injective, les éléments $f(x_1), \dots, f(x_p)$ sont deux à deux distincts, ce qui implique que $\text{card } f(E) = p = \text{card } E$. Comme $f(E) \subset F$, on en déduit bien que $\text{card } F \geq \text{card } E$.
Supposons que $\text{card } E \leq \text{card } F$. Notons alors $E = \{x_1, \dots, x_p\}$ et $F = \{y_1, \dots, y_q, y_{q+1}, \dots, y_q\}$ avec donc $p \leq q$. L'application $f : E \rightarrow F$ définie par $\forall i \in [1; p], f(x_i) = y_i$ est alors une injection de E dans F .
- (ii) Supposons qu'il existe une surjection f de E sur F . Notons $F = \{y_1, \dots, y_q\}$. Comme f est surjective, on peut affirmer que, pour tout $j \in [1; q]$, il existe $x_j \in E$ tel que $f(x_j) = y_j$. Les éléments x_1, \dots, x_q sont alors q éléments de E qui sont distincts (puisque leurs images sont distinctes), d'où $\text{card } E \geq q = \text{card } F$.
Supposons que $\text{card } E \geq \text{card } F$. Notons alors $E = \{x_1, \dots, x_q, x_{q+1}, \dots, x_p\}$ et $F = \{y_1, \dots, y_q\}$ avec donc $p \geq q$. L'application $f : E \rightarrow F$ définie par $\forall i \in [1; q], f(x_i) = y_i$ d'une part et $\forall i \in [q+1; p], f(x_i) = y_1$ d'autre part est alors une surjection de E sur F .
- (iii) Supposons qu'il existe une bijection f entre E et F . Alors f est une injection d'où $\text{card } E \leq \text{card } F$ d'après (i) et f est une surjection d'où $\text{card } E \geq \text{card } F$ d'après (ii). Donc $\text{card } E = \text{card } F$.
Supposons que $\text{card } E = \text{card } F$. Notons alors $E = \{x_1, \dots, x_p\}$ et $F = \{y_1, \dots, y_p\}$. L'application $f : E \rightarrow F$ définie par $\forall i \in [1; p], f(x_i) = y_i$ est alors une bijection entre E et F . ■



On utilise parfois le (iii) de ce théorème pour dénombrer un ensemble E dont le cardinal est difficile à déterminer : on met E en bijection avec un ensemble F dont il est plus simple de compter les éléments et on en déduit que $\text{card } E = \text{card } F$.

On notera qu'un énoncé du même type existe pour les ensembles infinis : un ensemble en bijection avec un ensemble infini est infini. Nous allons y revenir.

Selon la propriété (ii) du théorème 1, si l'ensemble d'arrivée est plus petit que l'ensemble de départ, l'application ne peut être injective : il existe donc nécessairement deux éléments qui ont la même image. Cela fournit un nouveau principe de dénombrement.

Principe des tiroirs

Si l'on doit ranger p objets dans n tiroirs et que $p > n$, alors il existe au moins deux objets qui sont dans le même tiroir. Sous son air d'évidence, ce principe permet de démontrer des propriétés qui ne le sont pas toujours.

Exemples :

- Nous avons déjà utilisé le principe des tiroirs pour justifier qu'un rationnel possède nécessairement une écriture décimale périodique.
- Parmi le million de parisiennes, il en existe au moins 3 qui ont le même nombre de cheveux puisqu'une femme a (au plus) 400 000 cheveux.

D.2. Applications entre ensembles finis de même cardinal

Lemme 1

Soit $f : E \rightarrow F$ une application entre deux ensembles finis E et F . Alors $\text{card } f(E) \leq \text{card } E$ avec égalité si, seulement si, f est injective.

■ Notons $E = \{x_1, \dots, x_p\}$ de sorte que $f(E) = \{f(x_1), \dots, f(x_p)\}$. On constate donc bien que $f(E)$ possède au plus p éléments distincts et qu'il en possède exactement p si, et seulement si, $f(x_1), \dots, f(x_p)$ sont deux à deux distincts, c'est-à-dire si, et seulement si, f est injective. ■

Le théorème suivant est très utile dans la pratique pour vérifier la bijectivité d'une application. C'est un **théorème Bonux** pour le cadeau offert par la condition de cardinalité.

Théorème 2

Soient E et F deux ensembles finis de **même cardinal**.

- (i) Toute injection de E dans F est une bijection entre E et F .
- (ii) Toute surjection de E sur F est une bijection entre E et F .

Autrement dit, pour des applications entre ensembles finis de même cardinal, les mots « injectif », « surjectif » et « bijectif » sont synonymes.

- (i) Soit f une injection de E dans F . Il découle du lemme précédent que $f(E)$ est un ensemble fini de même cardinal que E et donc de même cardinal que F . Comme $f(E) \subset F$, on en déduit que $f(E) = F$ et donc que f est surjective. Ainsi f est bijective.
■ (ii) Soit f une surjection de E sur F de sorte que $f(E) = F$. Comme $\text{card } E = \text{card } F$, on en déduit que $\text{card } E = \text{card } f(E)$. Le lemme précédent permet d'en déduire que f est injective. Donc f est bijective. ■

Nous verrons une propriété analogue portant sur les dimensions en algèbre linéaire.

Exemples :

- L'ensemble des bijections entre un ensemble fini E et un autre ensemble fini F de même cardinal est aussi l'ensemble des injections de E dans F . Nous nous servirons de cette remarque pour dénombrer les bijections entre E et F .
- Dans le cas où les ensembles ne sont pas finis, le théorème précédent tombe en défaut. Ainsi, l'application $s : n \mapsto n + 1$ est une application injective mais non surjective de \mathbb{N} dans \mathbb{N} (puisque 0 n'a pas d'antécédent).

D.3. Dénombrement d'applications entre ensembles finis

Se donner une application f d'un ensemble fini $E = \{x_1, \dots, x_p\}$ dans un autre ensemble F revient à se donner la p -liste $(f(x_1), \dots, f(x_p))$ de F . Il est donc logique que les résultats de dénombrement établis pour les listes permettent de dénombrer certains ensembles d'applications.

On commence par le nombre total d'applications entre deux ensembles finis.

Proposition 12

Soient E, F deux ensembles finis. Alors F^E est un ensemble fini et

$$\text{card } F^E = (\text{card } F)^{\text{card } E}.$$

■ Soit $E = \{e_1; e_2; \dots; e_p\}$. L'application f est déterminée de manière univoque par la donnée du p -uplet $(f(e_1), \dots, f(e_p))$. Il y a donc autant d'application f de E dans F que de p -uplets dans F , c'est-à-dire $\text{card}(F^E) = \text{card}(F^p) = (\text{card } F)^p = (\text{card } F)^{\text{card } E}$. ■

Ce résultat nous explique pourquoi l'ensemble des applications de E dans F est noté F^E .

Exemples :

- Si E est vide, on retrouve le fait qu'il n'existe qu'une seule application du vide vers un autre ensemble (l'injection canonique) puisque $n^0 = 1$ même si $n = 0$.

On poursuit avec le nombre d'injections entre deux ensembles finis.

Proposition 13

Soient E et F deux ensembles finis de cardinaux respectifs p et n . Le nombre d'injections de E dans F est égal à $n(n - 1) \cdots (n - p + 1)$.

■ Le résultat est clair si $p > n$. On suppose donc que $p \leq n$. Posons $E = \{e_1; e_2; \dots; e_p\}$. L'application f est déterminée de manière univoque par la donnée du p -uplet $(f(e_1), \dots, f(e_p))$ et elle est injective si, et seulement si, les éléments de ce p -uplet sont distincts deux à deux. Il y a donc autant d'applications injectives de E dans F que de p -uplets sans répétition dans F , c'est-à-dire $n(n - 1) \cdots (n - p + 1)$. ■

Exemples :

- Si $\text{card}(E) > \text{card}(F)$, le nombre d'injections de E dans F est nul. On retrouve qu'il n'y a pas d'injection d'un ensemble dans un autre plus petit.

On termine avec le nombre de bijections entre deux ensemble finis. Le théorème 1 nous dit qu'il faut nécessairement que les deux ensembles aient le même cardinal.

Proposition 14

Soient E et F deux ensembles finis de même cardinal n . Le nombre de bijections de E dans F est égal à $n!$

■ Comme E et F sont finis, une application de E vers F est bijective si, et seulement si, elle est injective. Le nombre de bijections de E dans F est ainsi le nombre d'injections de E dans F , c'est-à-dire le nombre de n listes sans répétitions de n éléments pris parmi n qui vaut $n(n - 1) \cdots 1 = n!$ ■

Exemples :

- Si E est fini, on retrouve que l'ensemble \mathfrak{S}_E des permutations de E est de cardinal $n!$

Dénombrer les surjections entre ensembles finis est nettement plus difficile.

E. Comparaison des ensembles infinis [✚]

Pour comparer la taille d'ensembles finis, il suffit de comparer leurs cardinaux. Il n'en va pas de même pour les ensembles infinis qui ont tous le même cardinal : $+\infty$. Pourtant, tous les ensembles infinis ne sont pas de la même taille ; il y a de plus ou moins gros infinis !

E.1. Subpotence et équipotence

Dans le cadre des ensembles finis, nous avons vu que l'existence d'une injection de E dans F (ou d'une surjection de F sur E) est équivalente au fait que E est plus petit que F et que l'existence d'une bijection entre E et F est équivalente au fait que E est de la même taille que F .

Les notions d'injection, de surjection et de bijection apparaissent donc naturellement comme un outil permettant, au delà du caractère fini ou non des ensembles, de comparer les tailles d'iceux.

Définition 8

Soient E et F deux ensembles (finis ou infinis, peu importe!).

Il est équivalent de dire qu'il existe une injection de E dans F ou de dire qu'il existe une surjection de F sur E . Dans l'une ou l'autre de ces situations, on dit que E est **subpotent** à F .

On dit que E est **équipotent** à F lorsqu'il existe une bijection entre E et F .

■ Il faut démontrer que l'existence d'une injection de E dans F est équivalente à l'existence d'une surjection de F sur E .

Le cas où $E = \emptyset$ ou $F = \emptyset$ est facile. Dans le cas contraire, on raisonne par double-implication.

\Rightarrow Supposons qu'il existe une injection f de E dans F . Tout élément $y \in F$ possède alors au plus un antécédent par f . Si cet antécédent existe, on le note $g(y)$ et s'il n'existe pas, on pose $g(y) = a$ où a est un élément quelconque de E . On obtient ainsi une application g de F dans E qui est surjective puisque tout élément x de E est l'image par g d'au moins un élément de F , à savoir $f(x)$.

\Leftarrow Réciproquement, supposons qu'il existe une surjection g de F sur E . Tout élément $x \in E$ possède au moins un antécédent $y_x \in F$ par g . Posons $f(x) = y_x$. On obtient ainsi une application f de E vers F (c'est l'axiome du choix qui le dit) qui est injective puisque si x_1 et x_2 sont deux éléments de E tels que $f(x_1) = f(x_2)$, on a $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$. ■

L'équipotence est la garantie de l'existence d'une correspondance univoque entre les éléments des ensembles considérés. Autrement dit, lorsque deux ensembles sont équipotents, ils ont bien le même nombre d'éléments, qu'ils soient finis ou non !

La subpotence permet, quant à elle, de comparer des ensembles de tailles différentes : si E est subpotent à F , cela signifie qu'il y a moins (au sens large) de points dans E que dans F .

Exemples :

- Si E et F sont équipotents, alors E est subpotent à F et F est subpotent à E .
- Soient E et F deux ensembles finis. Le théorème 1 dit que:
 - E est subpotent à F si, et seulement si, $\text{card}(E) \leq \text{card } F$,
 - E est équipotent à F si, et seulement si, $\text{card}(E) = \text{card } F$
- La fonction th réalise une bijection (elle est continue et strictement croissante) entre \mathbb{R} et $]-1; 1[$. Par conséquent, \mathbb{R} est équipotent à $]-1; 1[$.
Plus généralement (c'est technique mais pas bien difficile), on peut démontrer que \mathbb{R} est équipotent à tous ses intervalles (sauf \emptyset et les singlétions).
On constate donc qu'un ensemble peut très bien être équipotent à l'une de ses parties strictes. Dans le cas de \mathbb{R} et de $]-1; 1[$, c'est tout de même surprenant : ils n'ont pas la même longueur mais ont le même nombre de points (ils sont juste plus serrés dans $]-1; 1[$).

L'énoncé suivant rassemble les propriétés élémentaires de l'équipotence.

Proposition 15

Sur un ensemble d'ensembles donné, l'équipotence est une relation d'équivalence.

La subpotence est réflexive et transitive mais n'est pas antisymétrique (c'est un préordre).

- Tout ensemble est toujours équipotent (respectivement subpotent) à lui-même puisque l'identité est une bijection (respectivement une injection).

Si E est équipotent à F alors F est équipotent à E car la réciproque d'une bijection est une bijection.

Comme une composée de bijections (respectivement injections) est encore une bijection (respectivement une injection), si E est équipotent (respectivement subpotent) à F et si F est équipotent (respectivement subpotent) à G , alors E est équipotent (respectivement subpotent) à G . ■

Reste une question à éclaircir à propos de la subpotence et de l'équipotence : si E est plus petit que F et si F est plus petit que E , est-il bien vrai que E et F sont de la même taille ? Le théorème suivant répond positivement à cette angoissante question. C'est le [théorème de Cantor–Bernstein](#).

Théorème 3

Si E est subpotent à F et si F est subpotent à E alors E et F sont équipotents.

- Cette démonstration, difficile, n'est pas du tout au programme de MPSI. Ni tout ce que l'on raconte dans cette section de toute façon ...

Supposons qu'il existe une injection f de E dans F et une injection g de F dans E et construisons une bijection entre E et F . L'idée consiste à effectuer une partition de E et une partition de F en introduisant la notion de chaîne d'un élément puis de montrer que chaque sous-ensemble de la partition de E peut être mis en bijection avec l'un des morceaux de la partition de F .

Soit $a \in E$. Si $a \notin g(F)$, nous définissons la chaîne de a en posant $\text{Ch}(a) = (a)$. Si, au contraire, $a \in g(F)$, on considère l'unique antécédent de a par g que l'on note a_1 (avec $a_1 \in F$). On distingue alors à nouveau deux cas : si $a_1 \notin f(E)$, on pose $\text{Ch}(a) = (a, a_1)$ et si $a_1 \in f(E)$, on introduit l'unique antécédent $a_2 \in E$ de a_1 par f auquel on fait subir la même dichotomie : si $a_2 \notin g(F)$, la chaîne de a s'arrête avec a_2 et l'on pose $\text{Ch}(a) = (a, a_1, a_2)$ et si $a_2 \in g(F)$, on poursuit le processus ...

On obtient au final une partition de E en trois sous-ensembles :

$$E = E_E \cup E_F \cup E_\infty \quad \text{où} \quad \begin{cases} E_E = \{a \in E : \text{Ch}(a) \text{ se termine dans } E\} \\ E_F = \{a \in E : \text{Ch}(a) \text{ se termine dans } F\} \\ E_\infty = \{a \in E : \text{Ch}(a) \text{ ne se termine pas}\}. \end{cases}$$

On peut, de la même manière, définir la chaîne de n'importe quel élément de F et obtenir ainsi une partition de F du même type :

$$F = F_E \cup F_F \cup F_\infty \quad \text{où} \quad \begin{cases} F_E = \{b \in F : \text{Ch}(b) \text{ se termine dans } E\} \\ F_F = \{b \in F : \text{Ch}(b) \text{ se termine dans } F\} \\ F_\infty = \{b \in F : \text{Ch}(b) \text{ ne se termine pas}\}. \end{cases}$$

Démontrons alors que la restriction \hat{f} de f à l'ensemble E_E réalise une bijection entre E_E et F_E .

Si $a \in E_E$, alors $f(a)$ est un élément de F dont la chaîne se termine dans E (puisque la chaîne de $f(a)$ est celle de a à laquelle on a concaténé à gauche l'élément $f(a)$), donc $f(E_E) \subset F_E$.

Par ailleurs, si $b \in F_E$, alors b possède au moins un antécédent a par f dans E (sinon sa chaîne serait réduite à $\{b\}$ et ne se terminerait pas dans E) et l'on a $a \in E_E$ (puisque la chaîne de a est celle de $f(a)$ à laquelle on a retiré $f(a)$). On a donc $f(E_E) = F_E$, ce qui assure la surjectivité de \hat{f} et donc aussi sa bijectivité puisque l'injectivité se conserve par restriction.

On démontre de même que la restriction \hat{g} de g à F_F réalise une bijection entre F_F et E_F et que la restriction \tilde{f} de f à E_∞ est une bijection entre E_∞ et F_∞ (sa réciproque est la restriction \tilde{g} de g à F_∞).

Dès lors, l'application φ qui coïncide avec \hat{f} sur E_E , avec \hat{g}^{-1} sur E_F et avec \tilde{f} sur E_∞ est une bijection entre E et F . ■

La proposition suivante, appelée **antinomie de Cantor**, donne un exemple où la relation de subpotence est stricte.

Proposition 16

Tout ensemble E est subpotent, mais jamais équivalent, à son ensemble de parties $\mathcal{P}(E)$

- On nous demande de démontrer qu'il existe au moins une injection de E dans $\mathcal{P}(E)$ mais aucune surjection de E sur $\mathcal{P}(E)$.

L'application $i : x \mapsto \{x\}$ est une injection de E dans $\mathcal{P}(E)$ (pour $a, b \in E$, si $\{a\} = \{b\}$ alors $a = b$).

Pour démontrer qu'il n'existe aucune surjection de E sur $\mathcal{P}(E)$, on raisonne par l'absurde en supposant l'existence d'une telle surjection s . On introduit alors l'ensemble $A = \{x \in E : x \notin s(x)\}$. Comme $A \in \mathcal{P}(E)$, la surjectivité de s assure l'existence de $c \in E$ tel que $A = s(c)$. Mézalors, si $c \in A$, on a $c \notin s(c)$, c'est-à-dire $c \notin A$ ce qui est contradictoire et si $c \notin A$, alors $c \in s(c)$ donc $c \in A$, ce qui est aussi une contradiction. Il n'existe donc pas de surjection de E sur $\mathcal{P}(E)$. ■

Exemples :

- Si E est fini de cardinal $n \geq 0$, le résultat précédent implique que $\text{card } E < \text{card } \mathcal{P}(E)$, c'est-à-dire $n < 2^n$. On obtiendrait évidemment ce résultat très simplement par récurrence.
- La proposition précédente montre, par exemple, que \mathbb{N} et $\mathcal{P}(\mathbb{N})$ n'ont pas la même taille et illustre ainsi le fait que tous les ensembles infinis ne sont pas équivalents. Nous allons préciser cette remarque dans la section suivante.

E.2. Dénombrabilité

Définition 9

On dit qu'un ensemble E est **dénombrable** lorsqu'il existe une injection de E dans \mathbb{N} ou, ce qui revient au même, une surjection de \mathbb{N} sur E , c'est-à-dire lorsque E est subotent à \mathbb{N} .

Une injection de E dans \mathbb{N} (ou une surjection de \mathbb{N} sur E) correspond tout simplement à une façon de numérotier les éléments à l'aide des entiers naturels. Un ensemble est donc dénombrable lorsqu'on peut indexer successivement ses éléments, c'est-à-dire le représenter comme une suite (éventuellement finie).

Vous verrez l'an prochain que la dénombrabilité joue un rôle important en probabilités.

Exemples :

- Tout ensemble fini est dénombrable.
- Évidemment, \mathbb{N} est dénombrable.
En fait, toute partie de \mathbb{N} est dénombrable (prendre l'injection canonique).
En particulier, l'ensemble des nombres pairs (respectivement impairs) est dénombrable.
- \mathbb{Z} est dénombrable puisqu'on a l'application $i : \mathbb{Z} \rightarrow \mathbb{N}$ telle que

$$\forall m \in \mathbb{N}, \quad i(m) = 2m \quad \text{et} \quad \forall m \in \mathbb{Z} \setminus \mathbb{N}, \quad i(m) = -(2m - 1)$$

est une injection (y réfléchir!).

- Le produit cartésien $\mathbb{N} \times \mathbb{N}$ est dénombrable. En effet, pour numérotier les couples d'entiers naturels, il suffit de représenter classiquement le graphe de $\mathbb{N} \times \mathbb{N}$ sous forme d'un tableau à double entrée et d'attribuer un numéro aux couples en les parcourant en diagonale :

(0; 0) ₁	(0; 1) ₃	(0; 2) ₆	...
(1; 0) ₂	(1; 1) ₅	(1; 2)	...
(2; 0) ₄	(2; 1)	(2; 2)	...
:	:	:	⋮

- L'ensemble $\mathcal{P}(\mathbb{N})$ n'est pas dénombrable d'après la proposition 16.

Il en découle un procédé de construction simple d'ensembles infinis de tailles différentes toujours plus grandes : \mathbb{N} , $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, etc

À la fin de 19ème siècle, Cantor a émis l'hypothèse, dite **hypothèse du continu**, qu'il n'existe pas entre \mathbb{N} et $\mathcal{P}(\mathbb{N})$ un infini de taille intermédiaire. Il n'a cependant jamais pu démontrer que cette hypothèse était vraie ou fausse...

Et pour cause ! Gödel (1938) et Cohen (1963) ont prouvé que, dans la théorie axiomatique de Zermelo-Fraenkel avec l'axiome du choix (dite théorie ZFC), cette propriété est indécidable, c'est-à-dire qu'elle est impossible à prouver et impossible à réfuter !

Dans la théorie ZFC, on peut démontrer que tout ensemble infini contient une partie dénombrable. En ce sens, les ensembles dénombrables infinis sont donc les plus petits ensembles infinis.

Attention, certains auteurs appellent « dénombrables » les ensembles qui sont équipotents à \mathbb{N} . Cela a pour conséquence que les ensembles finis ne sont pas dénombrables. Ce n'est pas vraiment pas très pratique...

La proposition suivante dresse la liste des premières propriétés de la dénombrabilité.

Proposition 17

La dénombrabilité satisfait les propriétés de stabilité suivantes :

- (i) Si E est dénombrable et si F s'injecte dans E , alors F est dénombrable. En particulier, si E est dénombrable et si F est inclus dans E alors F est dénombrable.
- (ii) Si E et F sont dénombrables, alors $E \times F$ l'est aussi.
- (iii) Toute réunion dénombrable d'ensembles dénombrables est dénombrable.

■ (i) AQT

- (ii) Si f désigne une injection de E dans \mathbb{N} et si g est une injection de F dans \mathbb{N} , alors l'application définie par $(a; b) \mapsto (f(a); g(b))$ est une injection de $E \times F$ dans $\mathbb{N} \times \mathbb{N}$. Comme $\mathbb{N} \times \mathbb{N}$ est dénombrable, la propriété (i) implique que $E \times F$ l'est aussi.
- (iii) Soit $(E_i)_{i \in I}$ une famille dénombrable (c'est-à-dire que I est dénombrable) d'ensembles dénombrables (c'est-à-dire que chaque E_i est dénombrable). On peut introduire une injection φ de I dans \mathbb{N} et, pour tout $i \in I$, une injection ψ_i de E_i dans \mathbb{N} . Pour tout $x \in \bigcup_{i \in I} E_i$, on note $p(x)$ le plus petit des entiers $f(i)$ pour lesquels $x \in E_i$ et l'on choisit un $i_x \in I$ tel que $f(i_x) = p(x)$. On constate alors que l'application $x \mapsto (p(x); \psi_{i_x}(x))$ définit une injection de $\bigcup_{i \in I} E_i$ dans $\mathbb{N} \times \mathbb{N}$ puisque si $(p(x); \psi_{i_x}(x)) = (p(x'); \psi_{i_{x'}}(x'))$ alors x et x' sont dans la même partie et ont le même numéro dans cette partie donc sont égaux. ■

On peut généraliser la propriété (ii) : tout produit cartésien d'un nombre fini d'ensembles dénombrables est dénombrable. Par contre, ce résultat n'est plus vrai si le produit cartésien porte sur un nombre infini d'ensembles dénombrables (même si ce nombre d'ensembles est lui-même dénombrable). Ainsi, le procédé diagonal de Cantor (exposé ci-dessous pour démontrer l'indénombrabilité de \mathbb{R}) permet de justifier que $\{0; 1\}^{\mathbb{N}}$ n'est pas dénombrable.

Exemples :

- L'ensemble des nombres rationnels \mathbb{Q} est dénombrable puisque l'application

$$\left\{ \begin{array}{ccc} \mathbb{Z} \times \mathbb{N}^* & \longrightarrow & \mathbb{Q} \\ (p, q) & \longmapsto & \frac{p}{q} \end{array} \right.$$

est une surjection sur \mathbb{Q} de l'ensemble $\mathbb{Z} \times \mathbb{N}^*$, qui est dénombrable en tant que produit cartésien d'ensembles dénombrables.

- L'ensemble des nombres réels \mathbb{R} n'est pas dénombrable.

Nous allons le prouver en raisonnant par l'absurde et en utilisant le [procédé diagonal de Cantor](#). Supposons donc que \mathbb{R} est dénombrable. Dès lors, l'intervalle $[0; 1[$ l'est aussi, ce qui permet de représenter $[0; 1[$ comme une suite $(x_n)_{n \in \mathbb{N}}$. Pour chaque $n \in \mathbb{N}$, on introduit le développement décimal propre de x_n sous la forme $x_n = \overline{0, a_{n,1}a_{n,2}\dots a_{n,p}\dots}$ et on considère le nombre $y = \overline{0, b_1b_2\dots b_p\dots}$ où chaque b_p est choisi dans $\llbracket 1; 8 \rrbracket \setminus \{a_{p,p}\}$ (on évite le 9 pour être certain d'avoir un développement décimal propre). Dès lors, on constate que $y \in [0; 1[$ et qu'il est pourtant distinct de tous les x_n . Absurde !

- Comme \mathbb{R} n'est pas dénombrable et que \mathbb{Q} l'est, on en déduit que l'ensemble des nombres irrationnels $\mathbb{R} \setminus \mathbb{Q}$ n'est pas dénombrable. Il y a ainsi beaucoup plus d'irrationnels que de rationnels.
- L'ensemble \mathbb{C} n'est pas dénombrable puisqu'il contient \mathbb{R} . En fait, il est assez simple de voir que \mathbb{C} est équivalent à \mathbb{R} (Y réfléchir).

6 h 45