30 | Dénombrement

L'objectif de ce chapitre est purement pratique : APPRENDRE À COMPTER. Il était temps !

Dénombrer un ensemble d'objets consiste à déterminer le cardinal de cet ensemble. Le dénombrement se base souvent sur la combinatoire, qui est l'étude des configurations possibles d'un ensemble d'objets, soit l'étude de la structuration d'un ensemble, passant éventuellement par une description décomposée des objets (construction par choix successifs) ou un tri des objets suivant certains critères (partition).

La clé du dénombrement combinatoire est la notion de bijection : si je peux construire une correspondance biunivoque entre les objets d'un ensemble E et les objets d'un ensemble F (c'est-à-dire une bijection de E sur F), alors E a autant d'objets que F. C'est d'ailleurs comme cela que l'on définit la notion de cardinal d'un ensemble fini E, par comparaison avec un ensemble $[\![1\,,n]\!]$, correspondant à une énumération des éléments de E (l'action de compter).

Par la suite, il est souvent maladroit de revenir systématiquement à la définition, en comparant à un ensemble $[\![1\,,n]\!]$, et on recherche plutôt la mise en bijection avec des ensembles de référence bien connus.

1 Cardinal d'un ensemble fini, combinatoire des ensembles

1.1 Définition du cardinal

La définition suivante formalise la notion intuitive de nombre d'éléments d'un ensemble fini.

Définition-théorème 1 – Ensemble fini/infini, cardinal d'un ensemble fini

- Un ensemble E est dit *fini* lorsqu'il est vide ou lorsque, pour un certain entier $n \in \mathbb{N}^*$, il existe une bijection de l'ensemble $[\![1\,,n]\!]$ sur E. Dans le cas contraire, l'ensemble E est dit *infini*.
- Si E est un ensemble fini non vide, l'entier n de la définition précédente est unique, appelé le *cardinal de* E ou *nombre d'éléments de* E, et noté $|E|$ ou $\mathrm{Card}(E)$. Par convention, l'ensemble vide est de cardinal 0.

Démonstration. Cf. annexe A. ■

Se donner une telle bijection entre un enesemble E et $[\![1\,,n]\!]$ revient à énumérer les éléments de E et permet d'écrire $E = \{x_1, \dots, x_n\}$.

Exemple 2 Pour tous $m, n \in \mathbb{Z}$, avec $m \leqslant n$, l'ensemble $[\![m\,,n]\!]$ est fini de cardinal $n - m + 1$.

En effet, la fonction $k \longmapsto k + m - 1$ est une bijection de $[\![1\,,n-m+1]\!]$ sur $[\![m\,,n]\!]$, de réciproque $k \longmapsto k - m + 1$.

Théorème 3 – Équipotence et cardinal

Soit E et F deux ensembles. Si E est fini et s'il existe une bijection de E sur F, alors F est fini et $|F| = |E|$.

Démonstration. Si E est vide, F l'est nécessairement aussi. Dans le cas où E est non vide, nous pouvons nous donner une bijection f de $[\![1\,,|E|]\!]$ sur E et une bijection g de E sur F. L'application $g \circ f$ est alors bijective de $[\![1\,,|E|]\!]$ sur F, ainsi d'une part F est fini et d'autre part $|F| = |E|$, par unicité du cardinal. ■

Théorème 4 – Partie d'un ensemble fini

Soit E un ensemble fini. Si A une partie de E, alors A est finie et $|A| \leqslant |E|$, avec égalité si et seulement si $A = E$.

Démonstration. Cf. annexe A. ■

✎ **En pratique** ✎ Ainsi, pour établir que deux ensembles FINIS sont égaux, au lieu de montrer la double inclusion $A \subset B$ et $B \subset A$, on peut se contenter de montrer, grâce au résultat précédent, l'inclusion $A \subset B$ et l'égalité d'entiers $|A| = |B|$. On notera l'analogie avec l'argument de dimension pour l'égalité de deux sous-espaces vectoriels de dimension finie.

1.2 Règles de calcul sur les cardinaux

Par la suite, pour indiquer qu'une union est disjointe, on utilisera le symbole « $\sqcup$ » en lieu et place de « $\cup$ ».

Théorème 5 – Cardinal d'une union, d'une différence, d'un complémentaire, d'un produit cartésien

Soit A, B, $A_1, \dots, A_n$ des ensembles finis.

- **Union.** $|A \cup B| = |A| + |B| - |A \cap B|$. En particulier, si A et B sont disjoints : $|A \sqcup B| = |A| + |B|$.
  Plus généralement, si $A_1, \dots, A_n$ sont deux à deux disjoints : $\left|\bigsqcup_{k=1}^{n} A_k\right| = \sum_{k=1}^{n} |A_k|$.
- **Différence.** $|A \backslash B| = |A| - |A \cap B|$.
  Complémentaire. En particulier, si $B \subset A$: $\left|\overline{B}\right| = |A \backslash B| = |A| - |B|$.
- **Produit cartésien.** $|A \times B| = |A| \times |B|$. Plus généralement, $|A_1 \times \cdots \times A_n| = \prod_{k=1}^{n} |A_k|$.

En effet, pour calculer $|A \cup B|$, on additionne $|A|$ et $|B|$ pour tenir compte des éléments de A et de ceux de B, mais de ce fait on compte deux fois les éléments de l'intersection $A \cap B$, ce qui nécessite de retrancher $|A \cap B|$.

Démonstration. Cf. annexe A. ∎

Remarque 6 – Formule d'inclusion-exclusion ou du crible de Poincaré† (HP)

La formule donnant le cardinal d'une union quelconque de deux ensembles finis se généralise également à une union finie quelconque d'ensembles finis. Précisément, si $A_1, \dots, A_n$ sont des ensembles finis, alors

$$\left|\bigcup_{k=1}^{n} A_k\right| = \sum_{k=1}^{n} \left((-1)^{k-1} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} |A_{i_1} \cap \cdots \cap A_{i_k}| \right) = \sum_{\substack{I \subset [\![1,n]\!] \\ I \neq \varnothing}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right|.$$

Nous donnerons une preuve efficace de cette formule à l'exemple 9 du chapitre 32.

1.3 Cardinaux *vs* injection/surjection

Théorème 7 – Effet d'une application sur le cardinal

Soit E et F deux ensembles et $f : E \longrightarrow F$ une application.

(i) Si f est injective et si F est fini, alors E aussi est fini et $|E| \leqslant |F|$, avec égalité si et seulement si f est bijective.

(ii) Si f est surjective et si E est fini, alors F aussi est fini et $|F| \leqslant |E|$, avec égalité si et seulement si f est bijective.

(iii) Si E et F sont FINIS DE MÊME CARDINAL, alors

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

En effet,

- Dire que f est injective, c'est dire que deux points distincts de E sont envoyés par f sur deux points distincts de F, *i.e.* que $f(E)$ est comme une copie de E dans F. Une telle copie n'est possible que si F est « plus gros » que E, *i.e.* si $|E| \leqslant |F|$ – assertion **(i)**.
- Dire que f est surjective, c'est dire qu'à travers f, E couvre F en totalité. Une telle couverture n'est possible que si E est « plus gros » que F, *i.e.* si $|F| \leqslant |E|$ – assertion **(ii)**.

Démonstration.

(i) Si f est injective, alors f induit une bijection de E sur $f(E)$, or $f(E)$ est un sous-ensemble de F qui est fini, on conclut alors grâce au théorème 4.

(ii) Par surjectivité de f, on peut considérer $X \subset E$ tel que tout élément de F admet un unique antécédent par f dans X. Ainsi F est en bijection avec X et on conclut à nouveau grâce au théorème 4.

(iii) Conséquence des deux points précédents. ∎

†. Henri Poincaré (1854 Nancy – 1912 Paris) est un mathématicien, physicien théoricien et philosophe des sciences français. Ses contributions majeures à l'étude du problème des trois corps en font un fondateur de l'étude qualitative des systèmes d'équations différentielles et de la théorie du chaos. Il est aussi un précurseur majeur de la théorie de la relativité restreinte et de la théorie des systèmes dynamiques.

Remarque 8 Le point **(iii)** du théorème précédent est totalement analogue à l'énoncé caractérisant les bijections entre deux espaces vectoriels de même dimension finie.

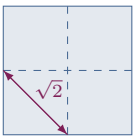
Corollaire 9 – Principe des tiroirs de Dirichlet[†]

Si $n+1$ chaussettes doivent être rangées dans n tiroirs, alors deux chaussettes au moins se retrouvent dans le même tiroir.

Démonstration. Ranger $n+1$ chaussettes dans n tiroirs revient à se donner une application d'un ensemble de cardinal $n+1$ (l'ensemble des chaussettes) dans un ensemble de cardinal n (l'ensemble des tiroirs). Or, puisque $n+1 > n$, une telle application ne saurait être injective. ■

Plus formellement, le principe des tiroirs énonce que si E et F sont deux ensembles finis tels que $|E| > |F|$, alors il n'existe pas d'injection de E dans F.

Exemple 10 Étant donné 5 points dans un carré d'arête 2, on peut toujours en trouver deux distants d'au plus $\sqrt{2}$.



En effet, coupons simplement notre carré en quatre comme indiqué ci-contre. Un des quatre carrés ainsi formés contient nécessairement deux des cinq points. Or ces quatre carrés ont des diagonales de longueur $\sqrt{2}$.

2 Combinatoire des ensembles d'applications

Dans l'ensemble de cette section, E et F désignent deux ensembles finis.

2.1 Applications quelconques, p-listes

Définition-théorème 11 – p-liste

Soit $p \in \mathbb{N}^*$.

- On appelle *p-liste d'éléments de F* tout p-uplet d'éléments de F, *i.e.* tout élément de F^p.
- Le nombre de p-listes d'éléments de F est $|F|^p$.

Démonstration. Le nombre de p-listes d'éléments de F est $|F^p| = |F|^p$ (théorème 5). ■

Remarque 12

- Dans une liste, l'ordre des éléments compte (une p-liste étant un p-uplet et non un ensemble) et un même élément peut figurer plusieurs fois dans une liste.
- Les listes sont utilisées pour modéliser des tirages SUCCESSIFS AVEC REMISE : les tirages sont successifs, puisque l'ordre des éléments d'une p-liste compte, et avec remise, puisque les répétitions sont autorisées.

Exemple 13 Il y a 52^5 $(= 380\,204\,032)$ façons de tirer 5 cartes successivement avec remise dans un jeu de 52 cartes.

Observons que la donnée d'une p-liste d'éléments de F, *i.e.* d'un p-uplet $(x_i)_{1\leqslant i\leqslant p}$ d'éléments de F, équivaut à se donner une application de $[\![1\,,p]\!]$ dans F (définie par $i \longmapsto x_i$) et que, réciproquement, la donnée d'une application de $E = \{e_1, \dots, e_p\}$ dans F est équivalente à la donnée de la p-liste $(f(e_1), \dots, f(e_p))$ de F.

Théorème 14 – Nombre d'applications entre deux ensembles finis

$\left|F^E\right| = |F|^{|E|}$, où l'on rappelle que F^E désigne l'ensemble des applications de E dans F.

Remarque 15 Le théorème précédent reste valable dans les cas où l'un des ensembles E ou F est l'ensemble vide.

†. Johann Peter Gustav Lejeune Dirichlet (1805 à Düren – 1859 à Göttingen) est un mathématicien prussien qui apporta de profondes contributions à la théorie des nombres, en créant le domaine de la théorie analytique des nombres, et à la théorie des séries de Fourier. On lui attribue la définition formelle moderne d'une fonction.

2.2 Lemme du berger

Le résultat suivant permet de donner de la rigueur à tous les arguments combinatoires reposant sur des choix successifs.

Théorème 16 – Lemme du berger ou Principe multiplicatif

Si l'application $f : E \longrightarrow F$ est surjective et s'il existe un entier $k \in \mathbb{N}^*$ tel que, pour tout $y \in F$, $\left|f^{-1}(\{y\})\right| = k$ (tous les éléments de F ont le même nombre k d'antécédents par f), alors $|E| = k|F|$.

Démonstration. Il suffit de considérer la partition $\left\{f^{-1}(\{y\}) \mid y \in F\right\}$ de E définie par la surjection f pour laquelle le nombre de parts est $|F|$ et chaque part est de cardinal k. ■

Ce principe affirme essentiellement que si tout mouton a quatre pattes, un berger possédant n moutons possède aussi $4n$ pattes de moutons ! La fonction f étant ici la fonction associant à une patte donnée le mouton auquel elle est rattachée.

✎ **En pratique** ✎ Le lemme du berger permet de formaliser la notion de « choix successifs » et est souvent utilisé de façon implicite dans les raisonnements. Il faut essentiellement en retenir que lorsque l'on fait des choix successifs, et qu'à chaque étape le nombre de possibilité ne dépend pas de la situation dans laquelle on se trouve (c'est-à-dire des choix précédents), alors le nombre total de possibilités s'obtient en faisant le produit du nombre de possibilités à chaque étape.

La formalisation d'un tel choix par le lemme du berger se fait en considérant la fonction qui à un choix possible associe la situation à l'étape précédente permettant ce choix. Le calcul du nombre de p-arrangements d'un ensemble fini est un exemple typique d'utilisation du lemme du berger (cf. section suivante).

Exemple 17 Il y a $n(n-1)$ couples (x, y) dans $[\![1\,,n]\!]^2$ tels que $x \neq y$.

En effet, construire un tel couple revient par exemple à commencer par choisir x, puis à choisir y. Il y a alors n valeurs possibles pour x et, pour chacune de ces n valeurs, $n-1$ valeurs restantes pour y, soit en tout $n(n-1)$ couples possibles. Formellement, la surjection f est ici la projection de la première coordonnée :

$$f : [\![1\,,n]\!]^2 \backslash \{(i,i) \mid i \in [\![1\,,n]\!]\} \longrightarrow [\![1\,,n]\!], (x,y) \longmapsto x.$$

Exemple 18 À partir d'un alphabet de p lettres, on peut former $p(p-1)^{n-1}$ mots de n lettres qui ne contiennent jamais deux lettres consécutives identiques.

En effet, pour la première lettre, on peut choisir n'importe quelle lettre de l'alphabet (p possibilités), mais pour chacune des suivantes, on n'a plus que $p-1$ choix possibles pour éviter que deux lettres consécutives soient identiques.

Exemple 19 Une urne contient $2n$ boules numérotées de 1 à $2n$ que l'on tire toutes successivement sans remise. Il y a $2 \times n!^2$ tirages pour lesquels un numéro pair est toujours suivie d'un numéro impair et réciproquement.

En effet, les tirages à dénombrer sont de deux types disjoints : ceux qui commencent par un numéro pair et ceux qui commencent par un numéro impair. Pour un tirage commençant par un numéro pair, on tire une boule paire (n possibilités), puis une boule impaire (n possibilités), puis une boule paire ($n-1$ possibilités), puis une boule impaire ($n-1$ possibilités), etc. – soit un total de $n^2(n-1)^2 \dots 2^2 1^2 = n!^2$ tirages. De la même façon, on en dénombre autant à commencer par un numéro impair.

Exemple 20 Il y a 4×26^3 $(= 70\,304)$ mots de 7 lettres contenant le mot « OUPS ».

En effet, lorsque le mot « OUPS » apparait dans un mot de 7 lettres, il n'y apparait qu'une fois. Pour construire un tel mot, on peut donc :

- d'abord choisir la position du sous-mot « OUPS », soit 4 possibilités pour le « O » initial qui ne peut occuper que les positions 1, 2, 3 et 4 ;
- puis choisir arbitrairement les trois lettres restantes, *i.e.* une 3-liste de l'alphabet, soit 26^3 possibilités.

2.3 Injections, p-listes d'éléments distincts

Définition-théorème 21 – Arrangement

Soit $p \in \mathbb{N}^*$.
On pose $n = |F|$.

- On appelle *p-arrangement de F* toute p-liste d'éléments DISTINCTS de F.
- Il existe $\dfrac{n!}{(n-p)!}$ p-arrangements de F si $p \leqslant n$, et il n'en existe pas si $p > n$.

Démonstration. Construire un p-arrangement de F, avec $p \leqslant n$, revient à choisir un premier élément dans F (n possibilités), puis un deuxième élément distinct du premier ($n-1$ possibilités), ... et enfin un p^{e} élément distinct des précédents ($n-(p-1)$ possibilités) ; d'où un total de $n \times (n-1) \times \ldots \times (n-p+1) = \dfrac{n!}{(n-p)!}$ p-arrangements de F. ■

Remarque 22 Les arrangements sont utilisés pour modéliser des tirages SUCCESSIFS SANS REMISE (sans remise puisque les répétitions sont exclues).

Exemple 23 Il y a $\dfrac{52!}{47!}$ $(= 311\,875\,200)$ façons de tirer 5 cartes successivement sans remise dans un jeu de 52 cartes.

Exemple 24 De combien de façons peut-on asseoir n personnes sur un banc rectiligne ? autour d'une table ronde ?

- **Banc rectiligne.** En numérotant les personnes à asseoir de 1 à n, les asseoir sur un banc rectiligne revient alors à se donner un n-arrangement de $[\![1\,,n]\!]$, soit un total de $n!$ configurations.
- **Table ronde.** La différence entre un banc rectiligne et une table ronde réside notamment en l'absence d'une première place autour de cette dernière – par exemple, on ne change pas la configuration des places assises si l'on demande à chaque convive de se déplacer d'une place sur sa droite. Pour asseoir n personnes autour d'une table ronde :
  - × on peut donc commencer par asseoir arbitrairement la personne numérotée n ;
  - × puis lui donner des voisins de proche en proche par la droite en se donnant un $(n-1)$-arrangement quelconque de $[\![1\,,n-1]\!]$, soit $(n-1)!$ possibilités ;

  et finalement un total de $(n-1)!$ configurations possibles.

On peut à nouveau faire le lien avec le dénombrement des applications ; les arrangements étant aux listes ce que les injections sont aux applications.

Théorème 25 – Nombres d'injections et de permutations

(i) Injections. On pose $p = |E|$ et $n = |F|$. L'ensemble des applications injectives de E dans F est vide si $p > n$ et de cardinal $\dfrac{n!}{(n-p)!}$ si $p \leqslant n$.

(ii) Permutations. On appelle *permutations de E* toute bijection de E sur E et on note classiquement $\mathfrak{S}_E$ l'ensemble des permutations de E. Si l'on pose $n = |E|$, alors $|\mathfrak{S}_E| = n!$.

Démonstration. Pour **(ii)**, il suffit de rappeler qu'une application entre deux ensembles finis DE MÊME CARDINAL est bijective si et seulement si elle est injective (théorème 7). Le calcul de $|\mathfrak{S}_E|$ est dès lors une conséquence de **(i)**, obtenue pour $p = n$. ■

Exemple 26 Soit $n \geqslant 3$. Il y a $(n-2)!$ permutations de $[\![1\,,n]\!]$ qui envoient 1 sur 2 et 2 sur 3.

En effet, construire une telle permutation revient à choisir l'image de 3 ($n-2$ possibilités), puis celle de 4 ($n-3$ possibilités),... et enfin celle de n (1 possibilité) ; d'où un total de $(n-2) \times (n-3) \times \ldots \times 1 = (n-2)!$ possibilités.

Remarque 27 – Surjections Dénombrer les surjections est une tâche plus délicate. On pourra se reporter aux exercices 22 et 23 de la feuille de TD.

3 Sous-ensembles et coefficients binomiaux

Définition-théorème 28 – Combinaison

Soit E un ensemble et $p \in \mathbb{N}$.

- On appelle *p-combinaison de E* toute partie de E de cardinal p.
- Si E est fini de cardinal n, alors le nombre de p-combinaisons de E est $\binom{n}{p}$.

Démonstration. Notons, pour $p \leqslant n$, C_n^p le nombre de p-combinaisons de E.

On souhaite établir que $C_n^p = \dfrac{n!}{p!(n-p)!}$, *i.e.* que $\dfrac{n!}{(n-p)!} = p! \times C_n^p$ et on reconnait à gauche de cette égalité le nombre de p-arrangements de E. Or choisir un p-arrangement de E revient à :

- choisir p éléments dans E, *i.e.* une p-combinaison, soit C_n^p possibilités ;
- puis à ordonner ces p éléments, *i.e.* choisir un premier élément (p possibilités), puis un deuxième ($p-1$ possibilités), ... et enfin un p^{e} (1 possibilité), soit au total $p!$ choix (en pratique, on a construit une permutation des p éléments !) ;

soit finalement un total de $p! \times C_n^p$ p-arrangements de E. ■

Exemple 29 Les 2-combinaisons de l'ensemble $\{1,2,3,4\}$ sont ces $\binom{4}{2} = 6$ sous-ensembles à deux éléments :

$$\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\} \text{ et } \{3,4\}.$$

Remarque 30

- Dans une combinaison, qui est un ENSEMBLE et non un p-uplet, les éléments sont donnés sans ordre. Si l'on décide de numéroter les éléments d'une combinaison, le choix de la numérotation est totalement arbitraire, la combinaison en tant que telle n'ayant pas un premier élément, un deuxième élément, etc.
- Les combinaisons sont utilisées pour modéliser des tirages SIMULTANÉS, l'ordre des éléments n'ayant pas d'importance.

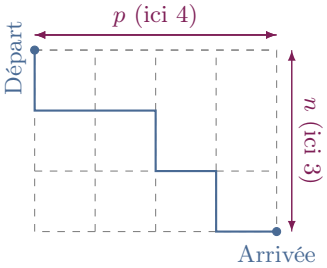
Exemple 31 Il y a $\binom{52}{5} = \dfrac{52 \times 51 \times 50 \times 49 \times 48}{5!}$ $(= 2\,598\,960)$ façons de tirer 5 cartes simultanément dans un jeu de 52 cartes.

Théorème 32 – p-listes strictement croissantes de $[\![1\,,n]\!]$

Pour tout $p \in [\![1\,,n]\!]$, il existe $\binom{n}{p}$ p-listes d'entiers $(i_1, \ldots, i_p)$ telles que $1 \leqslant i_1 < \ldots < i_p \leqslant n$.

Démonstration. Choisir une famille $(i_1, \ldots, i_p)$ d'entiers tels que $1 \leqslant i_1 < \ldots < i_p \leqslant n$ revient à choisir une p-combinaison de $[\![1\,,n]\!]$ ($\binom{n}{p}$ possibilités), puisqu'il n'y a ensuite qu'une seule manière d'en ranger les éléments dans l'ordre croissant. ■

Exemple 33 Un pion se promène le long d'un grillage plan de taille $n \times p$ dont chaque arête est de longueur 1. Combien de chemins de longueur minimale peut-il emprunter pour gagner le point d'arrivée depuis son point de départ ?



Un chemin de longueur minimale est ici entièrement déterminé par la donnée de n déplacements élémentaires vers le bas et p vers la droite. Tout chemin peut donc être identifié avec un mot quelconque de $n+p$ lettres dont n « B » (bas) et p « D » (droite). Or il existe autant de tels mots que de façons d'y placer les « D », soit $\binom{n+p}{p}$.

Exemple 34 On appelle *anagramme* d'un mot tout autre mot composé des mêmes lettres avec multiplicité mais dans un ordre quelconque. Le mot « MSCOIONIBNA » est une anagramme du mot « COMBINAISON ». Combien d'anagrammes le mot « INITIATIVE » possède-t-il ?

En effet, on souhaite dénombrer les mots de 10 lettres formés à partir de 4 « I », 2 « T », 1 « N », 1 « A », 1 « V » et 1 « E ». Pour construire de façon quelconque un tel mot, on peut choisir :

- d'abord la position des « I », soit $\binom{10}{4} = 210$ possibilités ;
- puis la position des « T », soit $\binom{10-4}{2} = 15$ possibilités ;
- puis la position du « N », soit $\binom{4}{1} = 4$ possibilités ;
- puis la position du « A », soit $\binom{3}{1} = 3$ possibilités ;
- puis la position du « V », soit $\binom{2}{1} = 2$ possibilités ;
- et enfin la position du « E », soit $\binom{1}{1} = 1$ possibilité ;

d'où un total de $210 \times 15 \times 4 \times 3 \times 2 = 75\,600$ anagrammes possibles.

On aurait évidemment pu choisir la position des lettres dans un ordre différent - par exemple, le « A », puis les « T », puis le « V », le « E », le « N » et enfin les « I », ce qui mène naturellement au même résultat, mais obtenu différemment :

$$\binom{10}{1} \times \binom{9}{2} \times \binom{7}{1} \times \binom{6}{1} \times \binom{5}{1} \times \binom{4}{4} = 10 \times 36 \times 7 \times 6 \times 5 \times 1 = 75\,600.$$

Exemple 35 Soit $n \geqslant 2$. Le nombre de surjections de $[\![1\,,n]\!]$ sur $[\![1\,,n-1]\!]$ est $(n-1)!\binom{n}{2}$.

En effet, se donner une surjection de $[\![1\,,n]\!]$ sur $[\![1\,,n-1]\!]$ revient à

- commencer par se donner une paire d'éléments $\{x,y\}$ de $[\![1\,,n]\!]$, soit $\binom{n}{2}$ possibilités ;
- puis à se donner une bijection de $[\![1\,,n]\!]\backslash\{x\}$ sur $[\![1\,,n-1]\!]$ (ensemble de même cardinaux), soit $(n-1)!$ possibilités.

Théorème 36 – Nombre de parties d'un ensemble fini

Si E un ensemble fini, alors $|\mathscr{P}(E)| = 2^{|E|}$.

Démonstration. *Preuve 1.* Pour dénombrer les parties d'un ensemble fini à $n = |E|$ éléments, il suffit d'en dénombrer les parties à k éléments, pour $0 \leqslant k \leqslant n$. Précisément, si $\mathscr{P}_k(E)$ est l'ensemble des k-combinaisons de E, alors $\mathscr{P}(E)$ est la réunion DISJOINTE des ensembles $\mathscr{P}_0(E)$, ..., $\mathscr{P}_n(E)$ et ainsi

$$|\mathscr{P}(E)| = \sum_{k=0}^{n} |\mathscr{P}_k(E)| = \sum_{k=0}^{n} \binom{n}{k} = 2^n = 2^{|E|}.$$

Preuve 2. D'après l'exemple 75 du chapitre 3, $\mathscr{P}(E)$ est en bijection avec $\{0,1\}^E$ qui est de cardinal $2^{|E|}$ (théorème 14). ■

Exemple 37 $|\mathscr{P}(\{0,1,2\})| = 8 = 2^3 = 2^{|\{0,1,2\}|}$.

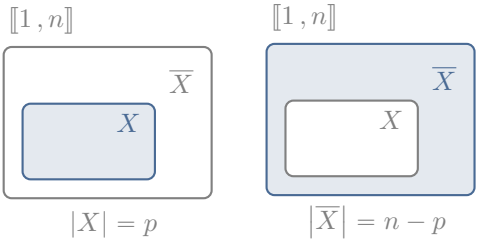
En effet,

$$\mathscr{P}(\underbrace{\{0,1,2\}}_{\text{3 éléments}}) = \Big\{ \underbrace{\varnothing}_{\substack{\binom{3}{0}=1 \text{ partie} \\ \text{à 0 élément}}}, \underbrace{\{0\},\{1\},\{2\}}_{\substack{\binom{3}{1}=3 \text{ parties} \\ \text{à 1 élément}}}, \underbrace{\{0,1\},\{0,2\},\{1,2\}}_{\substack{\binom{3}{2}=3 \text{ parties} \\ \text{à 2 éléments}}}, \underbrace{\{0,1,2\}}_{\substack{\binom{3}{3}=1 \text{ partie} \\ \text{à 3 éléments}}} \Big\}.$$

✎ **En pratique** ✎ **Double comptage.** Pour établir certaines égalités « $n = m$ », avec $m, n \in \mathbb{N}$, on peut parfois procéder par *double comptage*, *i.e.* montrer qu'un certain ensemble est de cardinal m via un certain mode d'énumération et de cardinal n selon un autre. Nous avons déjà fait usage de ce principe lors de la démonstration du théorème 28. Les deux exemples qui suivent illustrent également cette démarche dans trois situations bien connues.

Exemple 38 – Formule de Symétrie Pour tous $n, p \in \mathbb{N}$, avec $0 \leqslant p \leqslant n$, $\binom{n}{p} = \binom{n}{n-p}$.

On souhaite établir cette égalité sans calcul par un raisonnement purement combinatoire. Pour cela il suffit simplement d'observer que se donner une p-combinaison X de $[\![1\,,n]\!]$ ($\binom{n}{p}$ possibilités) équivaut à se donner son complémentaire $\overline{X}$ (puisque $X = \overline{\overline{X}}$) qui est une $(n-p)$-combinaison de $[\![1\,,n]\!]$ ($\binom{n}{n-p}$ possibilités).



Formellement, on exprime le fait que l'application $X \longrightarrow \overline{X}$ est une bijection de l'ensemble $\mathscr{P}_p([\![1\,,n]\!])$ des p-combinaisons de $[\![1\,,n]\!]$ sur l'ensemble $\mathscr{P}_{n-p}([\![1\,,n]\!])$ des $(n-p)$-combinaisons de $[\![1\,,n]\!]$. En effet, cette application est sa « propre » réciproque, à l'échange près des ensembles de départ et d'arrivée. Ainsi, comme voulu,

$$|\mathscr{P}_p([\![1\,,n]\!])| = |\mathscr{P}_{n-p}([\![1\,,n]\!])|.$$

Exemple 39 – Formule comité-président Pour tous $n, p \in \mathbb{N}^*$, avec $1 \leqslant p \leqslant n$, $\quad p\binom{n}{p} = n\binom{n-1}{p-1}$.

À nouveau, on souhaite établir cette égalité sans calcul par un raisonnement purement combinatoire. L'idée consiste à dénombrer le nombre de sous-ensembles de cardinal p (comités) dans lesquels on a distingué un élément (président). Suivant que l'on choisit d'abord le comité qui élit son président (on se donne une p-combinaison de $[\![1\,,n]\!]$, puis on choisit un élément de cette p-combinaison) ou que l'on choisit d'abord le président qui s'entoure ensuite d'un comité à son goût (on choisit un élément de $[\![1\,,n]\!]$, puis une $(p-1)$-combinaison de $[\![1\,,n-1]\!]$), on obtient les deux expressions voulues.

Exemple 40 – Formule comité-président généralisée Pour tous $n, p \in \mathbb{N}^*$, avec $1 \leqslant j \leqslant p \leqslant n$,

$$\binom{p}{j}\binom{n}{p} = \binom{n}{j}\binom{n-j}{p-j}.$$

On procède selon la même idée : on dénombre le nombre de sous-ensembles de cardinal p (comités) dans lesquels on distingue un sous-ensemble de cardinal de j (directoire). Suivant que l'on choisit d'abord le comité qui élit son directoire (on se donne une p-combinaison de $[\![1\,,n]\!]$, puis on choisit une j-combinaison de cette p-combinaison) ou que l'on choisit d'abord le directoire qui s'entoure ensuite d'un comité à son goût (on choisit une j-combinaison de $[\![1\,,n]\!]$, puis une $(p-j)$-combinaison de $[\![1\,,n-j]\!]$), on obtient les deux expressions voulues.

Exemple 41 – Formule de Pascal Pour tous $n, p \in \mathbb{N}^*$, avec $1 \leqslant p \leqslant n$, $\quad \binom{n}{p-1} + \binom{n}{p} = \binom{n+1}{p}$.

À nouveau, on souhaite établir cette égalité sans calcul par un raisonnement purement combinatoire. Il suffit alors ici de distinguer deux types de p-combinaisons de $[\![1\,,n+1]\!]$ – celles qui contiennent l'élément $n+1$ et celles qui ne le contiennent pas :

- Les p-combinaisons de $[\![1\,,n+1]\!]$ qui contiennent $n+1$ sont moralement des $(p-1)$-combinaisons quelconques de $[\![1\,,n]\!]$ auxquelles on ajoute $n+1$ et il y en a $\binom{n}{p-1}$.
- Les p-combinaisons de $[\![1\,,n+1]\!]$ qui ne contiennent pas $n+1$ sont exactement les p-combinaisons de $[\![1\,,n]\!]$ et il y en a $\binom{n}{p}$.

Formellement, on a partitionné l'ensemble $\mathscr{P}_p([\![1\,,n+1]\!])$ en deux sous-ensembles (disjoints donc) de p-combinaisons particulières.

4 Bilan pratique

Les questions de dénombrement peuvent s'avérer compliquées, toutefois on pourra s'efforcer de se ramener aux trois modèles de base suivants :

Tirages successifs AVEC REMISE	Tirages successifs SANS REMISE	Tirages SIMULTANÉS
=	=	=
LISTES	**ARRANGEMENTS**	**COMBINAISONS**

- soit directement ;
- soit en découpant l'ensemble à dénombrer en parties disjointes auxquelles s'appliquent ces modèles ;
- soit en dénombrant le complémentaire de l'ensemble à étudier et en utilisant la formule $\left|\overline{B}\right| = |A| - |B|$;
- soit en mettant en bijection l'ensemble à dénombrer avec un autre ensemble plus facile à structurer.

5 Ensembles dénombrables (programme de 2e année)

Les ensembles usuels de nombres $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{R}$ sont qualifiés d'*infinis*, dans la mesure où ils ne sont pas en bijection avec un intervalle d'entiers de la forme $[\![1\,,n]\!]$, avec $n \in \mathbb{N}^*$ – autrement dit ils n'ont pas un nombre fini d'éléments.

Naturellement, il n'est plus possible de définir le cardinal d'un ensemble ayant une infinité d'éléments comme son nombre d'éléments. Toutefois, on peut s'efforcer d'établir une comparaison entre les tailles des ensembles infinis via la définition suivante.

Définition 42 – Cardinal d'un ensemble, équipotence

Deux ensembles E et F sont dits *équipotents* ou *de même cardinal* lorsqu'il existe une bijection entre E et F.

Cette définition prolonge celle énoncée pour le cardinal d'un ensemble fini (définition 1). L'existence d'une bijection de E sur F garantit que l'on peut faire se correspondre parfaitement les éléments de E et ceux de F, en associant à tout élément de F un et un seul élément de E et inversement. Dire que F est équipotent à E revient ainsi à dire que F a exactement la même quantité d'éléments que E.

Intuitivement, de même, l'existence d'une injection de E dans F signifie qu'il y a moins d'éléments dans E que dans F – éventuellement autant – puisque l'on peut dans ce cas trouver dans F une copie de E qui peut ne pas être F tout entier. Quant à l'existence d'une surjection f de E sur F, elle indique au contraire que l'ensemble E a plus d'éléments que F – éventuellement autant – puisque l'on peut associer à tout élément de F au moins un antécédent, peut-être plusieurs, ce qui fait qu'en un sens E couvre F via f.

À ce titre, le théorème de Cantor-Bernstein[†] est totalement naturel.

Théorème 43 – Cantor-Bernstein

S'il existe une injection de E dans F et une injection de F dans E, alors les ensembles E et F sont équipotents.

Démonstration. Cf. exercice 33. ■

Exemple 44 Les ensembles $\mathbb{N}$ et $\mathbb{N}^*$ sont équipotents.

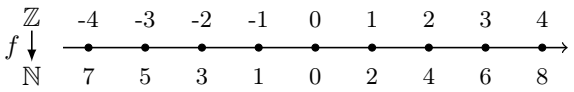
En effet, l'application de décalage vers la droite $f : \mathbb{N} \longrightarrow \mathbb{N}^*, n \longmapsto n+1$ est clairement une bijection de $\mathbb{N}$ sur $\mathbb{N}^*$, sa réciproque étant $f^{-1} : \mathbb{N}^* \longrightarrow \mathbb{N}, n \longmapsto n-1$.

Le résultat de l'exemple précédent semble surprenant, puisqu'il indique que $\mathbb{N}^*$, une partie *propre* de $\mathbb{N}$, *i.e.* une partie strictement incluse dans $\mathbb{N}$, a autant d'éléments que $\mathbb{N}$. En effet, du point de vue de l'inclusion, $\mathbb{N}^*$ est strictement plus « petit » que $\mathbb{N}$. Cependant, du point de vue de la notion d'équipotence, les ensembles infinis $\mathbb{N}$ et $\mathbb{N}^*$ ont la même « quantité » d'éléments.

Remarque 45 Il s'agit là d'une propriété caractéristique des ensembles infinis : un ensemble E est infini si et seulement s'il est en bijection avec une de ses parties propres, *i.e.* une partie strictement incluse dans E.

Exemple 46 Les ensembles $\mathbb{Z}$ et $\mathbb{N}^2$ sont équipotents à $\mathbb{N}$.

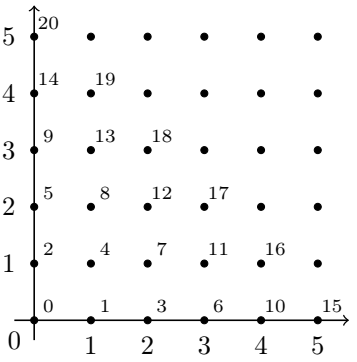
En effet, les figures ci-dessous donnent une idée des bijections que l'on peut établir entre ces ensembles.



Cette bijection entre $\mathbb{Z}$ et $\mathbb{N}$ s'obtient en associant 0 à 0, -1 à 1, 1 à 2 et ainsi de suite en alternant entre entiers positifs et négatifs. De façon explicite

$$f(n) = \begin{cases} 2n & \text{si } n \geqslant 0, \\ -2n-1 & \text{sinon.} \end{cases}$$

Les points de $\mathbb{N}^2$ sont numérotés diagonale par diagonale. En pratique, cela revient à associer à un élément (i,j) de $\mathbb{N}^2$ l'entier $(i+j)(i+j+1)/2 - j$.



Les deux bijections de l'exemple précédent consistent à numéroter les éléments respectifs de $\mathbb{Z}$ et $\mathbb{N}^2$, autrement dit les énumérer. Elles soulignent l'intérêt pour un ensemble E d'être en bijection avec $\mathbb{N}$: les éléments de E peuvent être énumérés, *i.e.* il est possible d'écrire $E = \{x_n \mid n \in \mathbb{N}\}$. De cette manière, on a « ordonné » E – dorénavant x_0 est le « premier » élément de E, x_1 le « deuxième », etc. Évidemment cet ordonnancement est arbitraire, mais en structurant

ainsi E de nouveaux procédés de calculs deviennent accessibles, tels des sommes infinies d'éléments de E par exemple. Il est par conséquent naturel de nommer cette classe d'ensembles.

Définition 47 – Ensemble dénombrable/au plus dénombrable

- Un ensemble E est dit *dénombrable* lorsqu'il est équipotent à $\mathbb{N}$, *i.e.* il existe une bijection de $\mathbb{N}$ sur E.
- Un ensemble E est dit *au plus dénombrable* lorsqu'il est fini ou dénombrable.

La propriété essentielle des ensembles au plus dénombrables est donc la possibilité d'énumérer leurs éléments, *i.e.* les représenter sous la forme des valeurs d'une suite : $\{x_n \mid n \in \mathbb{N}\}$.

Théorème 48 – Propriétés des ensembles (au plus) dénombrables

(i) Tout sous-ensemble d'un ensemble au plus dénombrable est au plus dénombrable.

(ii) Soit E et F deux ensembles.
- S'il existe une injection de E dans F et si F est au plus dénombrable, alors E est au plus dénombrable.
- S'il existe une surjection de E sur F et si E est au plus dénombrable, alors F est au plus dénombrable.

(iii) Un produit cartésien fini d'ensemble au plus dénombrables est au plus dénombrable.

(iv) Une union au plus dénombrable d'ensembles au plus dénombrables est au plus dénombrable.

Démonstration.

(i) II suffit de démontrer qu'un sous-ensemble E de $\mathbb{N}$, qui n'est pas fini, peut être mis en bijection avec $\mathbb{N}$. Pour tout $x \in E$, posons $\varphi(x) = |\{y \in X \mid y < x\}|$. Si x_0 est le plus petit élément de E, on a $\varphi(x_0) = 0$, ce qui montre que $\varphi(E)$ contient 0. Si $\varphi(x) = n$, et x' est le plus petit élément de E strictement supérieur à x, on a $\varphi(x') = n+1$, ce qui prouve que φ est surjective. Par ailleurs, φ est injective car strictement croissante. En effet, si $x_1 < x_2$, alors $\{y \in X \mid y < x_2\}$ contient $\{y \in X \mid y < x_1\}$ et x_1. Ceci permet de conclure.

(ii) Si $\varphi : E \longrightarrow F$ est injective, alors φ réalise une bijection de E sur $\varphi(E)$, qui est au plus dénombrable comme sous-ensemble d'un ensemble au plus dénombrable, et E est donc au plus dénombrable.
Si $\varphi : E \longrightarrow F$ est surjective, on peut choisir (cela demande l'axiome du choix), pour tout $y \in F$, un antécédent $s(y) \in E$ de y par φ. Alors l'application $s : F \longrightarrow E$ ainsi construite est injective puisque $s(y_1) = s(y_2)$ implique $y_1 = \varphi(s(y_1)) = \varphi(s(y_2)) = y_2$, et donc F est au plus dénombrable si E l'est, d'après ce qui précède.

(iii) Soient $E_1, \dots, E_k$ des ensembles au plus dénombrables, $E = E_1 \times \dots \times E_k$, et $p_1, \dots, p_k$ des nombres premiers distincts. Soit $\varphi_i : E_i \longrightarrow \mathbb{N}$ injective, pour tout $i \in \{1, \dots, k\}$. Alors $\varphi : E \longrightarrow \mathbb{N}$, définie par $\varphi(x_1, \dots, x_k) = p_1^{\varphi_1(x_1)} \cdots p_k^{\varphi_k(x_k)}$ est injective d'après le théorème de factorisation première (unicité de la factorisation d'un entier naturel non nul en produit de nombres premiers).

(iv) Soit $(E_i)_{i \in I}$, avec I au plus dénombrable et chacun des E_i aussi. Soit $\varphi_i : E_i \longrightarrow \mathbb{N}$ des applications injectives, pour $i \in I$, et soit $F \subset I \times \mathbb{N}$ l'ensemble des couples $(i, \varphi_i(x))$, pour $i \in I$ et $x \in E_i$.
Alors F est au plus dénombrable comme sous-ensemble de l'ensemble au plus dénombrable $I \times \mathbb{N}$, et l'application $(i, y) \longmapsto \varphi_i^{-1}(y)$ de F dans $\bigcup_{i \in I} E_i$ est surjective, ce qui prouve que $\bigcup_{i \in I} E_i$ est au plus dénombrable. ∎

Corollaire 49

Soit $d \in \mathbb{N}^*$. Les ensembles $\mathbb{Z}$, $\mathbb{N}^d$, $\mathbb{Z}^d$ et $\mathbb{Q}$ sont dénombrables.

Démonstration. L'application $(a, b) \mapsto a - b$ est une surjection de $\mathbb{N} \times \mathbb{N}$ sur $\mathbb{Z}$, et comme $\mathbb{N} \times \mathbb{N}$ est dénombrable, en tant que produit fini d'ensembles dénombrables, il en est de même de $\mathbb{Z}$. Les ensembles $\mathbb{N}^d, \mathbb{Z}^d$ sont dénombrables puisque ce sont des produits finis d'ensembles dénombrables. Enfin, $(a, b) \mapsto a/b$ induit une surjection de $\mathbb{Z} \times \mathbb{Z}^*$ sur $\mathbb{Q}$ qui de ce fait est dénombrable, $\mathbb{Z}$ et $\mathbb{Z}^*$ l'étant. ∎

Remarque 50 Il est possible de construire des énumérations explicites de l'ensemble des rationnels (cf. exercice 32).

✖ **Attention !** ✖ L'ensemble $\{0, 1\}^{\mathbb{N}}$, qui peut être assimilé à un produit cartésien dénombrable d'ensembles au plus dénombrables n'est pas dénombrable (cf. exercice 27).

†. Georg Cantor (1845 à Saint-Pétersbourg – 1918 à Halle) est un mathématicien allemand, créateur de la théorie des ensembles, qu'il introduisit pour étudier l'infini.
Felix Bernstein (1878 à Halle – 1956 à Zurich) est un mathématicien allemand, étudiant de Cantor, qui contribua également à la théorie des ensembles.

Il n'en va pas de même en revanche pour $\mathbb{R}$, dont les éléments ne sauraient être énumérés. Ce résultat est dû à Georg Cantor (1874) et nous en donnons une démonstration basée sur l'*argument diagonal (de Cantor)*.

Théorème 51 – Caractère indénombrable de $\mathbb{R}$ (Cantor)

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

Démonstration. Raisonnons par l'absurde, en supposant $\mathbb{R}$ dénombrable. Par conséquent, l'intervalle $[0\,,1[$, qui est un sous-ensemble de $\mathbb{R}$, devrait l'être aussi. Il est alors possible d'énumérer les éléments de $[0\,,1[$, *i.e.* les représenter sous la forme des termes d'une suite. Par exemple :

$$\begin{aligned} x_1 &= 0,\mathbf{0}000\ldots0\ldots \\ x_2 &= 0,5\mathbf{0}45\ldots7\ldots \\ x_3 &= 0,014\mathbf{3}\ldots8\ldots \\ &\ldots \\ x_{147} &= 0,1464\ldots\mathbf{9}\ldots \\ &\ldots \end{aligned}$$

où les réels sont représentés via leur développement décimal (propre).
La contradiction va alors surgir de la construction d'un réel $\alpha \in [0\,,1[$ qui n'appartient pas à la suite précédente. En l'occurrence, on définit α via son développement décimal de la façon suivante : la n-ième décimale de α est 0 si la n-ième décimale de x_n est non nulle et vaut 1 sinon. Ainsi, avec l'exemple ci-dessus, $\alpha = 0,110\ldots$
Puisque α est un élément de $[0\,,1[$ par construction, il existe un rang N tel que $\alpha = x_N$. La N-ième décimale de α est alors soit 0 soit 1. Or, s'il s'agit de 0, cela implique à la fois que la N-ième décimale de x_N est 0 et est non nulle – contradiction. S'il s'agit de 1, cela implique à la fois que la N-ième décimale de x_N est 1 et 0 – contradiction à nouveau. ■

Exemple 52 On peut montrer que $\mathbb{R}$, $\mathbb{R}^2$ (soit $\mathbb{C}$), $\mathbb{R}^3$ et plus généralement $\mathbb{R}^n$, avec $n \in \mathbb{N}^*$, sont équipotents. Il y a donc autant de points sur une droite ou sur un plan que dans notre espace à trois dimensions.

Exemple 53 Tout intervalle de $\mathbb{R}$ non vide et non réduit à un point est équipotent à $\mathbb{R}$.
Par exemple, la fonction exponentielle réalise une bijection de $\mathbb{R}$ sur $\mathbb{R}_+^*$ et la fonction tangente réalise une bijection de $\left]-\frac{\pi}{2}\,,\frac{\pi}{2}\right[$ sur $\mathbb{R}$. Ainsi la longueur d'un intervalle n'est pas reliée à son nombre de points.

Ainsi, du point de vue des cardinaux, les ensembles $\mathbb{Q}$ et $\mathbb{R}$ sont fondamentalement différents – le second ayant une infinité d'éléments d'un ordre supérieur au premier. Se pose alors la question naturelle : existe-t-il un ensemble infini de cardinal supérieur à $\mathbb{R}$? La réponse est positive, comme l'indique le théorème suivant, également dû à Cantor.

Théorème 54 – Absence de surjection de E sur $\mathscr{P}(E)$ (Cantor)

Il n'existe pas de surjection de E sur $\mathscr{P}(E)$.

Démonstration. Cf. exercice 28. ■

Ainsi l'ensemble $\mathscr{P}(E)$ a toujours un cardinal strictement supérieur à celui de E, dans la mesure où l'application $x \longmapsto \{x\}$ réalise une injection de E dans $\mathscr{P}(E)$. Il découle de ceci un procédé simple de construction d'infinis de tailles différentes toujours plus grandes : $\mathbb{N}$, $\mathscr{P}(\mathbb{N})$, $\mathscr{P}(\mathscr{P}(\mathbb{N}))$, ... Au passage, il est possible de montrer que $\mathbb{R}$ et $\mathscr{P}(\mathbb{N})$ sont équipotents.

En 1878 Georg Cantor émis l'hypothèse qu'il n'existe pas d'infini de taille intermédiaire entre $\mathbb{N}$ et $\mathscr{P}(\mathbb{N})$ (*hypothèse du continu*), sans parvenir à le démontrer. En 1938, Kurt Gödel[‡] montre que l'hypothèse du continu ne réfute pas le cadre traditionnel des mathématiques, appelé ZF ou ZFC (axiomatique de Zermelo-Fraenkel de la théorie des ensembles avec ou sans l'axiome du choix), *i.e.* si l'on ajoute aux axiomes usuels de ZFC l'hypothèse du continu, la théorie obtenue n'est ni plus ni moins contradictoire que la théorie usuelle ZFC. Le dernier résultat majeur concernant l'hypothèse du continu date de 1963 et est dû à Paul Cohen[§] qui montra que l'hypothèse du continu n'est pas démontrable dans le cadre de ZFC, cette hypothèse est *indécidable*.

‡. Kurt Gödel (1906 à Brno – 1978 à Princeton) est un logicien et mathématicien autrichien, naturalisé américain. Il démontra ces résultats majeurs (les deux théorèmes d'incomplétude) en 1931.

§. Paul Cohen (1934 à Long Branch – 2007 à Stanford) est un logicien et mathématicien américain, principalement connu pour avoir démontrer l'indépendance de l'hypothèse du continu et de l'axiome du choix vis-à-vis des axiomes de la théorie des ensembles ZF, travaux pour lesquels il reçut la médaille Fields en 1966.

Compétences à acquérir

- Structurer et décomposer (via le principe multiplicatif, des partitions et des mises en bijection) des ensembles d'objets à dénombrer : exercices 2 à 14.
- Obtenir des identités par double comptage : 20 à 24.
- Montrer qu'un ensemble est (au plus) dénombrable : exercices 29 et 31.

Quelques résultats classiques :

- Formule d'inclusion-exclusion ou du crible de Poincaré (remarque 6).
- Formule comité-président généralisée (exemple 40).
- Formule de Vandermonde (exercice 24).
- Nombre de fonctions croissantes de $[\![1\,,p]\!]$ dans $[\![1\,,n]\!]$ (exercice 10).
- Nombre de surjections entre deux ensembles finis (exercices 22 et 23).
- Bijections entre $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{N}^2$ (exemple 46).
- L'ensemble $\mathbb{R}$ n'est pas dénombrable (théorème 51).
- Absence de surjection de E sur $\mathscr{P}(E)$ (exercice 28).
- Théorème de Cantor-Bernstein (exercice 33).
- L'ensemble des points de discontinuité d'une fonction monotone est au plus dénombrable (exercice 29).

A Annexe (HP)

Démonstration du second point du théorème 1.
Il suffit d'établir par récurrence, pour tout $n \in \mathbb{N}^*$, la propriété

$$\mathscr{P}(n) : \text{« Pour tout } m \in \mathbb{N}^*, \text{ si } [\![1\,,n]\!] \text{ et } [\![1\,,m]\!] \text{ sont en bijection alors } m = n \text{ ».}$$

- *Initialisation.* $\mathscr{P}(1)$ est claire.
- *Hérédité.* Soit $n \in \mathbb{N}^*$. Supposons $\mathscr{P}(n)$ vraie et montrons que $\mathscr{P}(n+1)$ l'est aussi.
  Considérons $m \in \mathbb{N}^*$ et supposons que f réalise une bijection de $[\![1\,,n+1]\!]$ sur $[\![1\,,m]\!]$. Puisque $n+1 \geqslant 2$, $m = 1$ est exclu. En outre f induit une bijection de $[\![1\,,n]\!]$ sur $[\![1\,,m]\!]\backslash\{f(n+1)\}$ lui-même en bijection avec $[\![1\,,m-1]\!]$ (il suffit de décaler les entiers compris entre $f(n+1)+1$ et m). Alors, par hypothèse de récurrence, $n = m-1$, soit $n+1 = m$.
  Finalement $\mathscr{P}(n+1)$ est vraie et la propriété $\mathscr{P}$ est héréditaire.
- *Conclusion.* La propriété $\mathscr{P}$ étant vraie au rang 1 et héréditaire, elle est vraie pour tout $n \in \mathbb{N}^*$, par principe de récurrence.

Démonstration du théorème 4.
Le théorème est clair si E est vide. Sinon, sans perte de généralité, on peut supposer que $E = [\![1\,,n]\!]$, avec $n \in \mathbb{N}^*$, et on procède à nouveau par récurrence sur n.

- *Initialisation.* $\mathscr{P}(1)$ est claire.
- *Hérédité.* Soit $n \in \mathbb{N}^*$. Supposons $\mathscr{P}(n)$ vraie et montrons que $\mathscr{P}(n+1)$ l'est aussi.
  Soit A une partie stricte de $[\![1\,,n+1]\!]$. Il existe donc un entier $a \in [\![1\,,n+1]\!]$ tel que $A \subset [\![1\,,n+1]\!]\backslash\{a\}$. Considérons alors la bijection f de $[\![1\,,n+1]\!]$ sur lui-même définie par

$$\forall x \in [\![1\,,n+1]\!], \quad f(x) = \begin{cases} n+1 & \text{si } x = a \\ a & \text{si } x = n+1 \\ x & \text{sinon.} \end{cases}$$

  L'image de A par f est ainsi une partie de $[\![1\,,n]\!]$, par conséquent, par hypothèse de récurrence, $f(A)$ est un ensemble fini et $|f(A)| \leqslant n$. Il en va donc de même de A, puisque f induit une bijection de A sur $f(A)$.
  Finalement $\mathscr{P}(n+1)$ est vraie et la propriété $\mathscr{P}$ est héréditaire.
- *Conclusion.* La propriété $\mathscr{P}$ étant vraie au rang 1 et héréditaire, elle est vraie pour tout $n \in \mathbb{N}^*$, par principe de récurrence.

Démonstration du théorème 5.

- **Union disjointe.** Soit A et B disjoints avec $m = |A|$ et $n = |B|$. Il existe, par définition, deux bijections $f : [\![1\,,m]\!] \longrightarrow A$ et $g : [\![1\,,n]\!] \longrightarrow B$. En outre, on peut considérer une bijection $h : [\![1\,,n]\!] \longrightarrow [\![m+1\,,m+n]\!]$ (cf. exemple 2). On obtient alors une bijection φ de $[\![1\,,m+n]\!]$ sur $A \sqcup B$ via

$$\varphi : x \longmapsto \begin{cases} f(x) & \text{si } x \leqslant m \\ g(h^{-1}(x)) & \text{si } x > m. \end{cases}$$

  La formule plus générale pour $\left|\bigsqcup_{k=1}^{n} A_k\right|$ s'en déduit bien sûr par récurrence.
- **Différence.** D'une part, $A \cap B$ et $A\backslash B$ sont finis en tant que sous-ensemble de l'ensemble fini A.
  D'autre part, $A = (A\backslash B) \sqcup (A \cap B)$ et on conclut d'après le point précédent.
- **Union quelconque.** Il suffit de remarquer que

$$A \cup B = (A\backslash B) \sqcup (A \cap B) \sqcup (B\backslash A)$$

  les deux points précédents permettant de conclure.
- **Produit cartésien.** Pour tout $a \in A$, $b \longmapsto (a,b)$ est clairement une bijection de B sur $\{a\} \times B$, ainsi $|\{a\} \times B| = |B|$. Or

$$A \times B = \bigsqcup_{a \in A} \{a\} \times B$$

  et ainsi, d'après le premier point,

$$|A \times B| = \left|\bigsqcup_{a \in A} \{a\} \times B\right| = \sum_{a \in A} |\{a\} \times B| = \sum_{a \in A} |B| = |A| \times |B|.$$

  La formule plus générale pour $|A_1 \times \cdots \times A_n|$ s'obtient à nouveau par récurrence.