Leçon 6. Savoir compter

Cette leçon est une introduction aux questions de dénombrements. Il s'agit, d'une part, de compter certains objets mathématiques (éléments, parties, applications, ...) et, d'autre part, de comparer les *tailles* de certains ensembles finis ou infinis.

1. Préliminaires

Voici la façon naturelle (au sens du dénombrement) de comparer deux ensembles A et B:

Définition: On dit que A et B sont *équipotents* s'il existe une bijection f de A vers B.

En d'autres termes: on dit que A et B ont *même taille* si l'on peut mettre les éléments de A en correspondance avec les éléments de B à l'aide d'une bijection.

Notation: on écrira $A \sim B$ pour A est équipotent à B.

Voici la propriété principale de cette relation:

Propriété: soit E un ensemble. La relation - *être équipotent* à - est une relation d'équivalence sur l'ensemble $P(E)$ des parties de E.

Démo: (1) la relation est réflexive: quelle que soit $A \subset E$, l'application identité $id_A : A \to A : a \mapsto a$ est une bijection, dès lors $A \sim A$.
(2) la relation est symétrique: si $f : A \to B$ est une bijection alors $f^{-1} : B \to A$ est aussi une bijection. Dès lors si $A \sim B$ (i.e. si f existe) alors $B \sim A$ (en prenant pour bijection f^{-1}).
(3) la relation est transitive: si $f : A \to B$ et $g : B \to C$ sont deux bijections, alors $g \circ f : A \to C$ est aussi une bijection. Dès lors, si $A \sim B$ et $B \sim C$ on a aussi $A \sim C$.

2. Ensembles finis

On dit qu'un ensemble est fini s'il a un nombre fini $n \in \mathrm{N}$ d'éléments. Notons $[1, n] = \{1, 2, \ldots, n\}$. Voici une version formelle de la finitude:

Définition: un ensemble non vide E est dit fini de *cardinal* $n \in \mathrm{N} \setminus \{0\}$ s'il est équipotent à $[1, n]$.
Autrement dit: E est fini de cardinal n si l'on peut numéroter ses éléments de 1 à n: si $f : [1, n] \to E$ est une bijection, on a $E = \{f(1), f(2), \ldots, f(n)\}$.
On écrit Card (E) ou encore $\mid E \mid$ pour désigner le cardinal n de E i.e. le nombre de ses éléments. Le vide est de cardinal 0.

La proposition qui suit nous dit que le cardinal d'un ensemble fini détermine sa classe pour la relation 'être équipotent à'.

Proposition 1: 2 ensembles finis E et F sont équipotents (i.e. en bijection) ssi $\mid E \mid = \mid F \mid$.

Démo: supposons $\mid E \mid = \mid F \mid = n$.
On a $E \sim [1, n]$ et $[1, n] \sim F$. D'où, par transitivité, $E \sim F$.
Réciproquement, supposons $E \sim F$ et notons $m = \mid E \mid$, $n = \mid F \mid$.
On a
$$[1, m] \sim E,\ E \sim F,\ F \sim [1, n].$$
Par transitivité, on a donc $[1, m] \sim [1, n]$, i.e. il existe une bijection $f : [1, m] \to [1, n]$.

Mais alors $m = n$: en effet, si $m < n$ au moins l'un des entiers $l \in [1, n]$ n'aurait pas d'antécédent par f et f ne serait pas surjective. De même, si $m > n$, l'un des entiers $l \in [1, n]$ aurait au moins 2 antécédents par f et f ne serait pas injective.

Proposition 2: soient 2 ensembles finis E et F de même cardinal et $f : E \to F$ une application. Alors les assertions suivantes
(1) f est injective (2) f est surjective (3) f est bijective
sont équivalentes.

Démo: par définition, (3) implique (1) et (2). Pour voir que (1) implique (2) et (3), observer que si f est injective, $f : E \to f(E)$ est une bijection sur son image $f(E)$, i.e. E est équipotent à $f(E)$. Dès lors, $f(E)$ est une partie de F qui a même cardinal que F. On doit avoir $f(E) = F$ i.e. f est surjective et donc bijective (car elle est injective). Pour voir que (2) implique (1) (et dès lors (3)), on peut argumenter par contraposée: si f n'était pas injective, on aurait $\mid f(E) \mid < \mid E \mid = \mid F \mid$ et f ne pourrait être surjective.

La propriété qui suit est évidente (1 pomme par poche = 2 pommes):
Proposition 3: supposons E et F finis et disjoints ($E \cap F = \emptyset$). Alors $E \cup F$ est fini et

$$\mid E \cup F \mid = \mid E \mid + \mid F \mid .$$

Démo: si $f : [1, m] \to E$ et $g : [1, n] \to F$ sont 2 bijections (i.e. 2 numérotations) alors l'application $h : [1, m + n] \to E \cup F$ définie par

$$h(i) = f(i) \text{ pour } 1 \leq i \leq m, \quad h(m + j) = g(j) \text{ pour } 1 \leq j \leq n,$$

est une bijection (i.e. une numérotation).

Proposition 3 pour n ensembles: si A_j, $1 \leq j \leq n$, sont des ensembles finis deux à deux disjoints, i.e. tels que $A_i \cap A_j = \emptyset$ pour $i \neq j$, alors la réunion $\bigcup_{1 \leq j \leq n} A_j$ est un ensemble fini de cardinal

$$\mid \bigcup_{1 \leq j \leq n} A_j \mid = \sum_{j=1}^{n} \mid A_j \mid .$$

Démo: par récurrence sur $n \geq 2$. C'est vrai pour $n = 2$. Supposons l'assertion vraie pour n ensembles finis et montrons qu'elle est vraie pour $n + 1$ ensembles finis.

On commence par observer que par distributivité de l'intersection sur la réunion on a

$$(\bigcup_{1 \leq j \leq n} A_j) \cap A_{n+1} = \bigcup_{1 \leq j \leq n} (A_j \cap A_{n+1}) = \emptyset.$$

Dès lors

$$\begin{aligned}
\mid \bigcup_{1 \leq j \leq n+1} A_j \mid &= \mid (\bigcup_{1 \leq j \leq n} A_j) \cup A_{n+1} \mid \\
&= \mid \bigcup_{1 \leq j \leq n} A_j \mid + \mid A_{n+1} \mid \qquad \text{(car c'est vrai pour 2 ensembles disjoints)} \\
&= (\sum_{j=1}^{n} \mid A_j \mid) + \mid A_{n+1} \mid \qquad \text{(par hypothèse de récurrence)} \\
&= \sum_{j=1}^{n+1} \mid A_j \mid
\end{aligned}$$

Corollaire (de la proposition 3): Si E et F sont 2 ensembles finis, alors le produit cartésien $E \times F$ est un ensemble fini et
$$| E \times F |=| E | \cdot | F | .$$

Démo:
$$E \times F = \{(a,b),\, a \in E \text{ et } b \in F\} = \bigcup_{b \in F} E \times \{b\}.$$

Pour $b \neq b'$ on a

$$(E \times \{b\}) \cap (E \times \{b'\}) = \emptyset \quad \text{(2 couples de secondes composantes distinctes sont distincts)}$$

Par la proposition 3, le produit est fini de cardinal

$$| E \times F |= \sum_{b \in F} | E \times \{b\} |= \sum_{b \in F} | E |=| E | \cdot | F | .$$

Une récurrence sur $n \geq 2$ montre aussi que si $A_j, 1 \leq j \leq n$, sont des ensembles finis, on a

$$| A_1 \times A_2 \times \cdots \times A_n |=| A_1 | \cdot | A_2 | \cdots | A_n | .$$

Application au dictionnaire:
Soit D_n l'ensemble des mots de longueur n en l'alphabet $A = \{a, b\}$. Par exemple,

$$D_1 = A, \quad D_2 = \{aa, ab, ba, bb\}, \quad D_3 = \{a_i a_j a_k, a_i, a_j, a_k \in \{a, b\}\}.$$

L'application
$$A^n \to D_n : (a_{i_1}, a_{i_2}, \ldots, a_{i_n}) \mapsto a_{i_1} a_{i_2} \cdots a_{i_n}$$
est une bijection. Dès lors
$$| D_n |=| A^n |= (| A |)^n = 2^n,$$
i.e. il y a 2^n mots de longueur n dont les lettres sont a et b.

- Le principe d'inclusion-exclusion: si E et F sont 2 ensembles finis, alors $E \cup F$ est fini de cardinal

$$| E \cup F |=| E | + | F | - | E \cap F | .$$

Démo: pour rappel $E \setminus F = \{x \in E,\, x \notin F\}$. L'ensemble $E \cup F$ est réunion de 3 parties 2 à 2 disjointes:
$$E \cup F = (E \setminus F) \cup (E \cap F) \cup (F \setminus E).$$

D'où
$$| E \cup F |=| E \setminus F | + | E \cap F | + | F \setminus E | .$$

D'autre part, en écrivant E comme réunion de 2 parties disjointes:

$$E = (E \setminus F) \cup (E \cap F),$$

on a
$$| E \setminus F |=| E | - | E \cap F | .$$

De même on a $\mid F\setminus E\mid=\mid F\mid-\mid E\cap F\mid$.

- L'inclusion-exclusion pour 3 ensembles finis A, B, C:

$$\mid A\cup B\cup C\mid=\mid A\mid+\mid B\mid+\mid C\mid-\mid A\cap B\mid-\mid A\cap C\mid-\mid B\cap C\mid+\mid A\cap B\cap C\mid.$$

Démo:

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

Proposition: soient 2 ensembles finis E et F. Il y a $\mid F\mid^{|E|}$ applications $f: E\to F$.

Voici une preuve différente de celle faite en amphi: désignons par F^E l'ensemble des applications de E vers F. Notons $n=\mid E\mid$ et écrivons $E=\{a_1,\ldots,a_n\}$. Tout $n-$ uplet $(b_1,b_2,\ldots,b_n)\in F^n$ définit une application $f: E\to F$ en posant

$$f(a_i)=b_i,\quad 1\le i\le n.$$

Réciproquement, toute application $f: E\to F$ définit le $n-$ uplet $(f(a_1),f(a_2),\ldots,f(a_n))\in F^n$. Dès lors, l'application

$$\Phi: F^E\to F^n: f\mapsto(f(a_1),\ldots,f(a_n))$$

est une bijection et on a

$$\mid F^E\mid=\mid F^n\mid=\mid F\mid^{|E|}.$$

Proposition: soit E un ensemble fini de cardinal n. Il y a $n!$ bijections $f: E\to E$.

Démo: cf travaux dirigés.

Nombres de parties d'un ensemble fini E de cardinal n.

Pour un entier $p\in\mathrm{N}$, $0\le p\le n$, désignons par $N(p,n)$ le nombre de parties de E de cardinal p. Le résultat qui suit est important:

Théorème:

$$N(p,n)=\binom{n}{p}=\frac{n!}{p!(n-p)!}$$

où, pour $k\in\mathrm{N}\setminus\{0\}$, $k!=k(k-1)(k-2)\cdots1$ et par convention $0!=1$.

Démo: par récurrence sur $n\ge0$. C'est vrai pour $n=0$: $E=\emptyset$, $P(E)=\{\emptyset\}$, $N(0,0)=1=\binom{0}{0}$
C'est aussi vrai pour $n=1$ (même type de vérification).
Supposons vrai pour E de cardinal n et tout $p\le n$ et montrons vrai pour E de cardinal $n+1$ et tout $p\le n+1$:
lorsque $p=0$, $N(0,n+1)=1$ car le vide est la seule partie de cardinal 0 et on a bien $\binom{n+1}{0}=1$.
Lorsque $p=n+1$, $N(n+1,n+1)=1$ car E est la seule partie de cardinal $n+1$ et on a bien $\binom{n+1}{n+1}=1$.
Il nous reste à considérer les cas $1\le p\le n$. Pour cela, choisissons un élément $x\in E$. On va compter séparément les parties $P\subset E$ contenant x et celles ne contenant pas x:

- toute partie P de cardinal p contenant x est de la forme $P = \{x\} \cup P'$ où $P' \subset E \setminus \{x\}$ est une partie de cardinal $p-1$ de $E \setminus \{x\}$ qui est de cardinal n. Il y a donc $N(p-1, n)$ choix pour P' ce qui, par hypothèse de récurrence, vaut $\binom{n}{p-1}$.
- toute partie P de cardinal p ne contenant pas x est incluse dans $E \setminus \{x\}$ qui est de cardinal n. Il y a donc $N(p, n)$ choix pour P, ce qui, par hypothèse de récurrence, vaut $\binom{n}{p}$.
Conclusion: le nombre de parties de cardinal p de E est donné par

$$\begin{aligned}
N(p, n+1) &= \binom{n}{p-1} + \binom{n}{p} \\
&= \frac{n!}{(p-1)!(n-(p-1))!} + \frac{n!}{p!(n-p)!} \\
&= \frac{n!}{(p-1)!(n-(p-1))!}\frac{p}{p} + \frac{n!}{p!(n-p)!}\frac{n-p+1}{n-p+1} \\
&= \frac{n!}{p!(n-p+1)!}(p + (n-p+1)) \\
&= \frac{(n+1)!}{p!(n+1-p)!} \\
&= \binom{n+1}{p}
\end{aligned}$$

Remarque: La formule que nous venons d'obtenir est connue sous le nom de *formule du triangle de Pascal* bien qu'elle fut découverte plusieurs siècles avant Pascal par des mathématiciens chinois. Elle permet de calculer les coefficients du binôme de proche en proche (cf le diagramme triangulaire en amphi).

On a aussi la symétrie: pour $m \leq n$, $\binom{n}{m} = \binom{n}{n-m}$ qui est immédiate à vérifier. On peut aussi la comprendre sans vérification en observant que toute partie $P \subset E$ de cardinal m admet une partie complémentaire $E \setminus P$ de cardinal $n-m$.

Application: soit $m \leq n$. Le nombre de listes strictement croissantes de m entiers entre 1 et n est égal à $\binom{n}{m}$. En effet, chaque liste de m entiers: $1 \leq a_1 < a_2 < \ldots < a_m \leq n$ équivaut au choix de la partie $\{a_1, a_2, \ldots, a_m\} \subset \{1, 2, \ldots, n\}$.

Formule du binôme de Newton: quelques soient les nombres complexes a et b et l'entier $n \in \mathrm{N}$, on a

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

avec la convention $a^0 = 1$.

Pour une preuve par récurrence sur $n \geq 0$ voir les travaux dirigés.

Corollaire (de la formule du binôme): soit E un ensemble fini de cardinal n. Alors $P(E)$ est fini de cardinal 2^n.

Démo: on compte les parties par cardinal: par le théorème, il y a $\binom{n}{k}$ parties de cardinal k, $0 \leq k \leq n$. Dès lors, le nombre total de parties de E vaut

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = \sum_{k=0}^{n} \binom{n}{k}.$$

Par la formule du binôme pour $a = 1 = b$, on a

$$\sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n.$$

3. Ensembles infinis.

Comme dans la langue française, un ensemble est dit infini s'il n'est pas fini. Depuis Cantor, on distingue en mathématique divers types d'ensembles infinis.

3.1 Ensembles dénombrables

Les ensembles infinis les plus simples sont ceux qui sont équipotents à l'ensemble des entiers N.

Définition: On dit qu'un ensemble infini E est dénombrable s'il est équipotent à N, i.e. s'il existe une bijection

$$f : \mathrm{N} \to E.$$

Dire que E est dénombrable signifie donc que l'on peut faire la liste de ses éléments en les énumérant à l'aide de f:

$$E = \{f(0), f(1), f(2), \ldots\}.$$

Exemple 1: l'ensemble des entiers relatifs Z est dénombrable.
En effet, l'application $f : \mathrm{N} \to \mathrm{Z}$ définie par

$$f(n) = -\frac{n}{2} \quad \text{si } n \text{ est pair }, \quad f(n) = \frac{n+1}{2} \quad \text{si } n \text{ est impair },$$

est une bijection dont la réciproque $f^{-1} : \mathrm{Z} \to \mathrm{N}$ est l'application

$$f^{-1}(l) = -2l \quad \text{si } l \leq 0, \quad f^{-1}(l) = 2l - 1 \quad \text{si } l > 0.$$

Il est instructif d'observer que

$$f(0) = 0,\ f(1) = 1, f(2) = -1,\ f(3) = 2, f(4) = -2, \ldots,$$

si bien que l'application f compte les entiers relatifs en les regroupant par paire $+n, -n,\ n \in \mathrm{N}\backslash\{0\}$.

L'énoncé qui suit peut surprendre:

Théorème: Toute partie infinie $P \subset \mathrm{N}$ est équipotente à N.

Démo: la preuve consiste à faire la liste des éléments de P en prenant les minima successifs comme suit: on crée une suite $a_0, a_1, a_2, \ldots$ en posant

$$a_0 = min(P), \quad , a_1 = min(P \setminus \{a_0\}), \ldots, a_{n+1} = min(P \setminus \{a_0, a_1, \ldots, a_n\}), \ldots$$

On va montrer que l'application

$$f : \mathrm{N} \to P : n \mapsto f(n) = a_n$$

est bijective.

- f est injective: par construction, quel que soit $n \in$ N, on a $a_n < a_{n+1}$.

- f est surjective: on procède par l'absurde. Supposons qu'il existe un élément $p \in P$ tel que pour tout $n \in$ N, $p \neq a_n$. La partie

$$Q = \{n \in \mathrm{N},\, p < a_n\}$$

serait alors non vide (sinon P serait finie). Posons

$$m = min(Q).$$

On a $m > 0$ car $a_0 = min(P)$ et, par définition du minimum, $a_{m-1} < p < a_m$. Mais alors on aurait $a_m \neq min(P \setminus \{a_0, a_1, \ldots, a_{m-1}\})$, ce qui contredit notre construction de la suite.

Exemples: les nombres pairs 2N et les nombres impairs 2N + 1 sont 2 parties infinies de N. De plus, elles sont strictement incluses dans N. Pourtant, par le théorème, elles sont toutes deux en bijections avec N. *Il y a autant de nombres pairs (impairs) que d'entiers naturels.*

L'ensemble $P \subset$ N des nombres premiers est infini (cf arithmétique). Par le théorème, P est en bijection avec N. *Il y a autant de nombres premiers que d'entiers naturels.*

Corollaire: soit E un ensemble infini. S'il existe une application injective $f : E \to$ N alors E est équipotent à N.

Démo: Puisque f est injective, l'application $f : E \to f(E) \subset$ N est une bijection de E sur son image $f(E)$ qui est une partie infinie de N. On a donc $E \sim f(E)$ et, par le théorème, $f(E) \sim N$. D'où $E \sim N$.

Exemple important:

- le produit cartésien N × N est dénombrable.

Démo 1: on utilise le corollaire: pour commencer, N × N est infini car l'application

$$\mathrm{N} \to \mathrm{N} \times \mathrm{N} : n \mapsto (n, n)$$

est injective. D'autre part, par l'unicité de la décomposition en facteurs premiers, l'application

$$\mathrm{N} \times \mathrm{N} \to \mathrm{N} : (m, n) \mapsto 2^m 3^n$$

est injective. Le corollaire assure alors que N × N $\sim$ N.

Démo 2: on peut aussi expliciter une bijection. L'application

$$f : \mathrm{N} \times \mathrm{N} \to \mathrm{N} : (a, b) \mapsto f(a, b) = \frac{(a + b)(a + b + 1)}{2} + b$$

est une bijection. Pour la vérification, voir les travaux dirigés. Observer que cela revient à énumérer les couples d'entiers suivant les diagonales:

$$(0, 0), \quad (0, 1), (1, 0), \quad (0, 2), (1, 1), (2, 0), \quad \ldots$$

3.2 Ensembles non dénombrables

Le lemme qui suit est du à Cantor. Il est à la fois simple et fondamental.

Lemme de Cantor: soit E un ensemble. Il n'existe pas d'application surjective $f : E \to P(E)$.

Démo: pour une application $f : E \to P(E) : x \mapsto f(x)$, on pose

$$A = \{x \in E,\, x \notin f(x)\} \subset E.$$

On va montrer que $A \in P(E)$ n'admet pas d'antécédent par f.
Supposons, par l'absurde, qu'il existe $a \in E$ tel que $f(a) = A$. Pour cet élément on a soit $a \in A$, soit $a \notin A$.
Si $a \in A$, alors $a \notin f(a) = A$. Contradiction.
Si $a \notin A$, alors $a \in f(a) = A$. Contradiction.

Conclusion: un tel élément a ne peut exister i.e. A ne peut admettre d'antécédent par f.

Voici une conséquence immédiate et fondamentale du lemme de Cantor:

Corollaire: Il n'existe pas de bijection $f : \mathrm{N} \to P(\mathrm{N})$.

Démo: toute bijection serait en particulier surjective.

L'ensemble des parties $P(\mathrm{N})$ est infini car l'application

$$\mathrm{N} \to P(\mathrm{N}) : n \mapsto \{n\}$$

est injective. Par contre, $P(\mathrm{N})$ n'est pas équipotent à N. Il est *infini non dénombrable.* Vous verrez plus tard que $P(\mathrm{N})$ est équipotent à l'ensemble des réels.