Chapitre 17

Dénombrement

Conformément au programme, nous nous contenterons d'une notion intuitive de cardinal et nous admettrons certaines propriétés particulièrement intuitives. Pour ceux que ça intéresse, tout est défini et démontré rigoureusement dans la partie V (qui est HP et donc que nous ne lirons pas en classe).

I Cardinal d'un ensemble fini

I.1 Définition, premières propriétés

Définition. Un ensemble fini est un ensemble contenant un nombre fini d'éléments. Le nombre d'éléments d'un ensemble fini est appelé son cardinal. Il est noté $\text{card}(E)$, $|E|$ ou encore $\#E$.

Bonjour la rigueur !

Exemples :

- $\text{card}(\varnothing) = 0$
- $\text{card}(\{0\}) = 1$
- $\text{card}(\llbracket 1\,;\,n\rrbracket) = n$

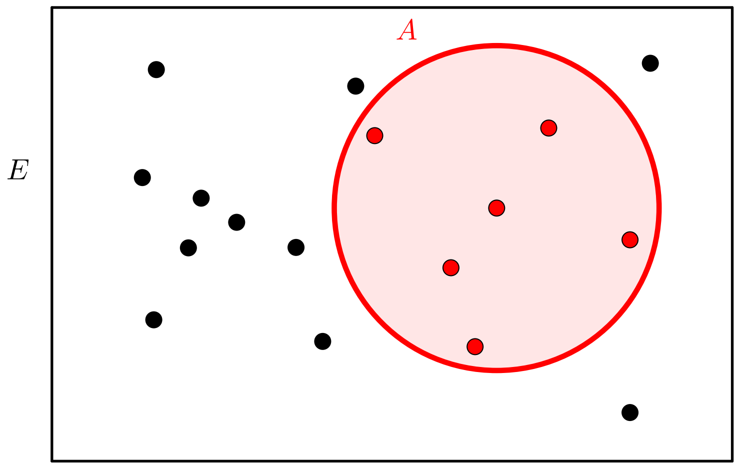
Plus généralement :

- l'ensemble vide est le seul ensemble de cardinal nul.
- un singleton est un ensemble de cardinal 1.
- un ensemble est de cardinal n si et seulement s'il est en bijection avec $\llbracket 1\,;\,n\rrbracket$, cf. paragraphes I.3 et V.

Rappel : Un élément appartient ou n'appartient pas à un ensemble, il n'y a pas de notion de « multiplicité ».

Exemple : $\text{card}(\{R;I;C;H;E;L;I;E;U\}) = \text{card}(\{R;I;C;H;E;L;U\}) = 7$

Théorème. Soit E un ensemble fini et soit A une partie de E. Alors A est un ensemble fini, et $\text{card}(A) \leqslant \text{card}(E)$, avec égalité si et seulement si $A = E$.

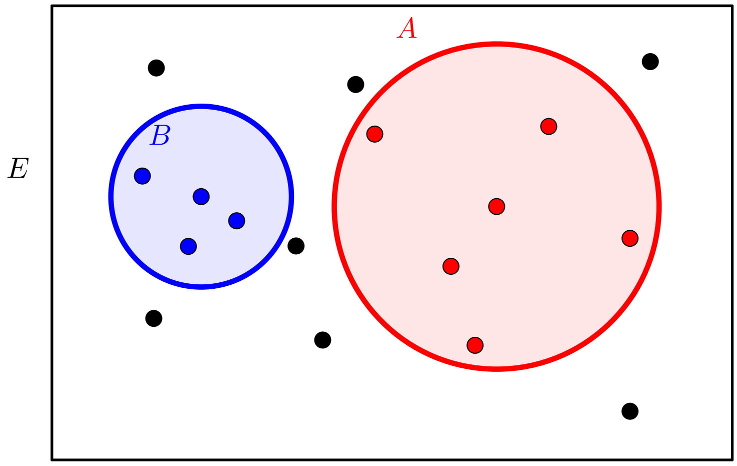


Corollaire. Une intersection d'ensembles finis est un ensemble fini.

Démonstration. Soit $(A_i)_{i\in I}$ une famille quelconque d'ensembles finis. Soit $i_0 \in I$. Alors $\displaystyle\bigcap_{i\in I} A_i \subset A_{i_0}$ qui est un ensemble fini ce qui permet de conclure.

Remarque : Comme on vient de le voir, il suffit même que l'un des ensembles soit fini.

Théorème. Soient A et B deux ensembles finis disjoints. Alors $A\cup B$ est fini et $\text{card}(A\cup B) = \text{card}(A) + \text{card}(B)$.



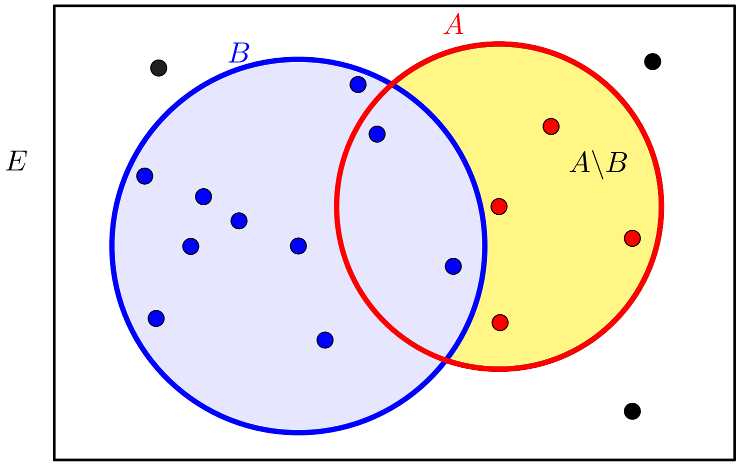
Théorème. Soient A et B deux ensembles finis. Alors $A\backslash B$ et $A\cup B$ sont finis et :

1. $\text{card}(A\backslash B) = \text{card}(A) - \text{card}(A\cap B)$.
2. $\text{card}(A\cup B) = \text{card}(A) + \text{card}(B) - \text{card}(A\cap B)$. En particulier, $\text{card}(A\cup B) \leqslant \text{card}(A) + \text{card}(B)$.

Le dernier point est intuitif : si on veut compter les éléments de $A\cup B$, on compte ceux de A, ceux de B, et on enlève ceux de $A\cap B$ car on les a comptés deux fois. Il faudra sans cesse faire attention, dans les exercices de dénombrement, à ne pas compter les objets plusieurs fois.

DÉMONSTRATION.

1. $A\backslash B$ est fini car inclus dans A qui est fini. De plus, $A = (A\backslash B)\cup (A\cap B)$ et cette union est disjointe.



Le théorème précédent permet de conclure.

2. $A\cup B = (A\backslash B)\cup B$ et cette union est disjointe. Le résultat précédent et le théorème précédent permettent de conclure.

Remarque : Si $B\subset A$, alors $\text{card}(A\backslash B) = \text{card}(A) - \text{card}(B)$.

Corollaire.

1. Si A est une partie d'un ensemble fini E, alors $\overline{A}$ est fini et $\text{card}\left(\overline{A}\right) = \text{card}(E) - \text{card}(A)$.
2. Si $(A_1, \dots, A_n)$ sont des ensembles finis, alors $A_1\cup\cdots\cup A_n$ est un ensemble fini et :

$$\text{card}\left(\bigcup_{i=1}^n A_i\right) \leqslant \sum_{i=1}^n \text{card}(A_i)$$

De plus, si les A_i sont deux à deux disjoints, il y a égalité.

DÉMONSTRATION. 1. $\overline{A} = E \backslash A$.

2. Par récurrence sur n : ⇝ EXERCICE.

Remarque : En d'autres termes, une union finie d'ensembles finis est un ensemble fini. C'est faux avec une union infinie. Par exemple, tout ensemble est l'union (disjointe) de ses éléments donc, en particulier, si E est un ensemble infini, alors $E = \displaystyle\bigcup_{e \in E} \{e\}$: E est une union d'ensembles finis (à un élément) mais n'est pas un ensemble fini.

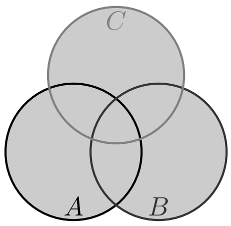
Léger abus de langage : un ensemble est l'union disjointe des singletons formés par ses éléments. Mais ça sonne moins bien...

Remarque : On dispose d'une formule générale pour $\text{card}(A_1 \cup \cdots \cup A_n)$, mais elle est HP. Donnons-la tout de même pour $n = 3$ en guise d'entraînement (cf. exercice 50 pour la formule générale).

Théorème (Formule du crible ou de Poincaré (HP)). Soient A_1, A_2, A_3 trois ensembles finis. Alors $A_1 \cup A_2 \cup A_3$ est fini et :

$$\begin{aligned} \text{card}(A_1 \cup A_2 \cup A_3) \quad = \quad & \text{card}(A_1) + \text{card}(A_2) + \text{card}(A_3) \\ & - \text{card}(A_1 \cap A_2) - \text{card}(A_1 \cap A_3) - \text{card}(A_2 \cap A_3) \\ & + \text{card}(A_1 \cap A_2 \cap A_3) \end{aligned}$$

C'est tout aussi intuitif que pour deux ensembles : on compte tous les éléments de A_1, de A_2, de A_3. Seulement, certains ont été comptés plusieurs fois : ceux des diverses intersections, dont on retire donc le cardinal. Mais alors, les éléments de $A_1 \cap A_2 \cap A_3$ ont été comptés trois fois puis retirés trois fois : il faut donc les rajouter, sinon on ne les compte pas du tout. Je vous laisse mettre des points dans le dessin ci-contre vous-mêmes...



$A \cup B \cup C$

DÉMONSTRATION. $\text{card}(A_1 \cup A_2 \cup A_3) = \text{card}(A_1 \cup A_2) + \text{card}(A_3) - \text{card}((A_1 \cup A_2) \cap A_3)$. Or, l'intersection est distributive par rapport à l'union donc

$$(A_1 \cup A_2) \cap A_3 = (A_1 \cap A_3) \cup (A_2 \cap A_3)$$

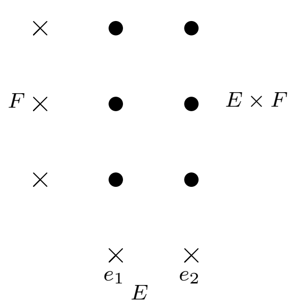
D'où :

$$\begin{aligned} \text{card}(A_1 \cup A_2 \cup A_3) \quad = \quad & \text{card}(A_1) + \text{card}(A_2) - \text{card}(A_1 \cap A_2) \\ & + \text{card}(A_3) - \text{card}(A_1 \cap A_3) - \text{card}(A_2 \cap A_3) \\ & + \text{card}(A_1 \cap A_3 \cap A_2 \cap A_3) \end{aligned}$$

Or, $A_1 \cap A_3 \cap A_2 \cap A_3 = A_1 \cap A_2 \cap A_3$ ce qui permet de conclure. □

Théorème. Soient E et F deux ensembles finis. Alors $E \times F$ est fini et $\text{card}(E \times F) = \text{card}(E) \times \text{card}(F)$.

Remarque : Ce théorème est intuitif (et donc sera admis, cf. paragraphe V pour une démonstration) si on représente $E \times F$ sous forme de tableau :



À chaque élément de E correspond « une copie conforme » de F et donc on a « autant de copies de F que d'éléments de E » : $\text{card}(E \times F) = \text{card}(E) \times \text{card}(F)$.

Corollaire. Si $E_1, \dots, E_k$ sont des ensembles finis, alors $E_1 \times \cdots \times E_k$ est fini, de cardinal $\text{card}(E_1) \times \cdots \times \text{card}(E_k)$. En particulier, si E est fini alors, pour tout $k \in \mathbb{N}^*$, E^k est fini et $\text{card}\left(E^k\right) = (\text{card}(E))^k$.

En d'autres termes, un produit fini d'ensembles finis est un ensemble fini.

Démonstration. Par récurrence : $\rightsquigarrow$ Exercice.

Exemple : $\text{card}\left(\llbracket 1\,;6\rrbracket^2\right) = 36$.

I.2 Cas particulier des parties de $\mathbb{N}$ ou de $\mathbb{Z}$

Théorème.

1. Une partie de $\mathbb{N}$ est finie si et seulement si elle est majorée.
2. Une partie de $\mathbb{Z}$ est finie si et seulement si elle est bornée.

Là aussi, ce théorème étant totalement intuitif, nous l'admettons, et nous renvoyons au paragraphe V pour une démonstration.

Remarque : Puisqu'on manipule souvent des suites, le premier point sera très souvent utilisé (et on ne s'est pas privé de le faire dans le chapitre 12). Rappelons que, si A est une partie de $\mathbb{N}$, l'assertion « A est majorée » s'écrit :

$$\exists n_0 \in \mathbb{N}, \forall n \in A, n < n_0$$

Dès lors, sa négation s'écrit :

$$\forall n_0 \in \mathbb{N}, \exists n \in A, n \geqslant n_0$$

et on vient de voir que cette assertion est équivalente à : « A est infinie ». C'est intuitif : une partie A de $\mathbb{N}$ est infinie si et seulement si, pour tout entier n_0, A contient un entier qui lui est supérieur.

Donnons une application très classique de ce résultat. On parle parfois de la limite inférieure ou de la limite supérieure d'une suite $(A_n)_{n\in\mathbb{N}}$ d'ensembles (par exemple dans l'exercice 19 du chapitre 4), que l'on définit de la façon suivante :

$$\liminf_{n\in\mathbb{N}} A_n = \bigcup_{n\in\mathbb{N}} \bigcap_{k\geqslant n} A_k \qquad \text{et} \qquad \limsup_{n\in\mathbb{N}} A_n = \bigcap_{n\in\mathbb{N}} \bigcup_{k\geqslant n} A_k$$

Dès lors, un élément x appartient à $\limsup_{n\in\mathbb{N}} A_n$ si et seulement si :

$$\forall n \in \mathbb{N}, \exists k \geqslant n, x \in A_k$$

En d'autres termes, un élément x appartient à $\limsup_{n\in\mathbb{N}} A_n$ si et seulement si l'ensemble A des entiers k pour lesquels $x \in A_k$ n'est pas majoré. D'après ce qui précède : un élément x appartient à $\limsup_{n\in\mathbb{N}} A_n$ si et seulement s'il appartient à une infinité de A_k ! Bien comprendre cela permet de mieux visualiser cet ensemble, et permet de mieux comprendre certaines démonstrations (voir par exemple le lemme de Borel-Cantelli, un grand classique que vous verrez probablement l'année prochaine).

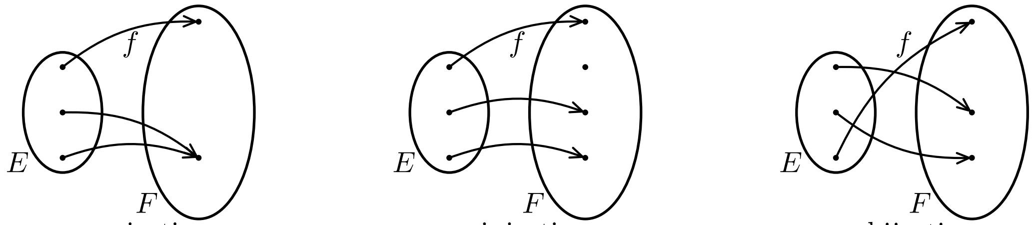
Pour la limite inf, c'est plus simple : un élément x appartient à $\liminf_{n\in\mathbb{N}} A_n$ si et seulement si il existe n tel que, pour tout $k \geqslant n$, $x \in A_k$: en d'autres termes, $x \in \liminf_{n\in\mathbb{N}} A_n$ lorsque x appartient à tous les A_k à partir d'un certain rang.

I.3 Applications entre deux ensembles finis

Théorème. Soient E et F deux ensembles finis.

- Il existe une application $f : E \to F$ injective si et seulement si $\text{card}(E) \leqslant \text{card}(F)$.
- Il existe une application $f : E \to F$ surjective si et seulement si $\text{card}(E) \geqslant \text{card}(F)$.
- Il existe une application $f : E \to F$ bijective si et seulement si $\text{card}(E) = \text{card}(F)$.

Remarque : Là aussi, ce théorème est très intuitif et sera prouvé dans la partie V. Il se voit très bien sur des patatoïdes :



surjective injective bijective

Attention de ne faire par dire à ce théorème ce qu'il ne dit pas : il ne dit PAS que si $f : E \to F$ et si $\text{card}(E) \leqslant \text{card}(F)$ alors f est injective (ou toute autre joyeuseté du même genre), il suffit de prendre f constante pour s'en convaincre.

Corollaire. Soient E et F deux ensembles finis et soit $f : E \to F$.

- Si f est injective, alors $\text{card}(E) \leqslant \text{card}(F)$.
- Si f est surjective, alors $\text{card}(E) \geqslant \text{card}(F)$.
- Si f est bijective, alors $\text{card}(E) = \text{card}(F)$.

Remarque : Ainsi, un moyen simple de prouver que deux ensembles finis ont le même cardinal consiste à exhiber une bijection entre eux, même si l'utilisation de bijections dans les problèmes de dénombrement n'est pas un attendu du programme. On peut généraliser les deux derniers points de ce résultat au cas où F n'est pas forcément fini.

Théorème. Soient E et F deux ensembles avec E fini. Soit $f : E \to F$.

- Si f est injective, alors F est infini ou $\text{card}(E) \leqslant \text{card}(F)$.
- Si f est surjective, alors F est fini et $\text{card}(E) \geqslant \text{card}(F)$.
- Si f est bijective, alors F est fini et $\text{card}(E) = \text{card}(F)$.

Attention, si f est injective, F n'a aucune raison d'être fini !

Remarque : La contraposée du premier résultat est : « si $\text{card}(E) > \text{card}(F)$ (y compris si E est infini et F fini) alors f n'est pas injective ». Ce résultat est connu sous le nom de « principe des tiroirs » (de Dirichlet) : si on a plus de paires de chaussettes que de tiroirs (y compris si on a un nombre infini de paires de chaussettes et un nombre fini de tiroirs), alors il existe un tiroir qui contient au moins deux paires de chaussettes (et même un nombre infini de paires dans le cas d'un nombre infini de paires de chaussettes et d'un nombre fini de tiroirs).

Il est appelé « pigeon-hole principle » en anglais : si on a plus de pigeons que de trous, alors il existe un trou contenant au moins deux pigeons.

Exemple : Utilisons ce résultat pour « finir le boulot » concernant l'équation de Pell-Fermat vue dans le DS n° 1 de l'année 2021/2022. Prouvons que, dans le cas où d n'est pas un carré parfait, il existe une solution $(x, y) \in \mathbb{N}^2$ non triviale (i.e. avec $y \neq 0$) à l'équation $x^2 - dy^2 = 1$. Tout découle du résultat suivant, obtenu dans la partie IV du DS : « il existe une infinité de rationnels p/q avec $p, q > 0$ (que l'on peut prendre premiers entre eux) tels que $\left|\sqrt{d} - \dfrac{p}{q}\right| < \dfrac{1}{q^2}$ ». Prouvons à l'aide de ce résultat et d'une utilisation judicieuse du principe des tiroirs que l'équation admet une solution non triviale.

L'exemple ci-contre est plutôt difficile (et est un exercice d'ENS, au passage). Nous verrons des exemples plus simples en TD.

- Soit p/q un rationnel qui convient. Alors, en multipliant par $q > 0$:

$$-\frac{1}{q} < q\sqrt{d} - p < \frac{1}{q}$$

  En particulier, $-\dfrac{1}{q} < q\sqrt{d} - p$ donc $0 < p + q\sqrt{d} < \dfrac{1}{q} + 2q\sqrt{d}$ (l'inégalité de gauche vient du fait que p et q sont strictement positifs).

- Puisque $|p - q\sqrt{d}| < 1/q$, avec l'inégalité $|p + q\sqrt{d}| < \dfrac{1}{q} + 2q\sqrt{d}$ du point précédent, par produit, il vient que

$$|p^2 - dq^2| < \frac{1}{q^2} + 2\sqrt{d} \leqslant 1 + 2\sqrt{d}$$

si bien que $-1 - 2\sqrt{d} < p^2 - dq^2 < 1 + 2\sqrt{d}$.

- Il existe donc une infinité de couples (p,q) d'entiers premiers entre eux (les chaussettes) vérifiant l'inégalité $-1-2\sqrt{d} < p^2 - dq^2 < 1+2\sqrt{d}$. Or, il y a un nombre fini d'entiers dans cet intervalle (les tiroirs). D'après le principe des tiroirs, il existe un entier k (un tiroir) dans l'intervalle précédent tel qu'il existe une infinité de couples (p,q) (les chaussettes) avec p et q premiers entre eux, tels que $p^2 - dq^2 = k$. On s'intéresse uniquement à ces couples (p,q) dans la suite (et, encore une fois, il y en a une infinité).

Il y en a au plus $2\left\lfloor 1+2\sqrt{d}\right\rfloor + 1$ si on veut être précis.

- Puisque $\sqrt{d}$ est irrationnel, alors k n'est pas nul. Il n'y a qu'un nombre fini de congruences modulo k (les tiroirs) donc il existe une infinité de couples (p,q) tels que tous les p aient la même congruence modulo k.
- Parmi tous ces couples avec les p ayant la même congruence modulo k (une infinité de chaussettes), on regarde la congruence de q modulo k : il n'y a qu'un nombre fini de congruences possibles (des sous-tiroirs si on veut) et donc, encore une fois, il existe une infinité de couples (p,q) tels que tous les q aient la même congruence modulo k.
- Résumons : il existe une infinité de couples (p,q) d'entiers premiers entre eux vérifiant $p^2 - dq^2 = k$ avec tous les p ayant la même congruence modulo k et tous les q ayant aussi la même congruence modulo k. Soient alors (p_1,q_1) et (p_2,q_2) deux éléments distincts de cet ensemble. On a :

$$ {p_1}^2 - d{q_1}^2 = {p_2}^2 - d{q_2}^2 = k, \qquad p_1 \equiv p_2[k] \qquad \text{et} \qquad q_1 \equiv q_2[k]$$

Alors $p_1q_2 - p_2q_1$ est divisible par k. Or :

$$\begin{aligned}(p_1p_2 - dq_1q_2)^2 - d(p_1q_2-p_2q_1)^2 &= {p_1}^2{p_2}^2 + d^2{q_1}^2{q_2}^2 - d{p_1}^2{q_2}^2 - d{p_2}^2{q_1}^2 \\ &= \left({p_1}^2 - d{q_1}^2\right) \times \left({p_2}^2 - d{q_2}^2\right) \\ &= k^2\end{aligned}$$

On a simplifié les doubles produits.

et puisque k divise $p_1q_2 - p_2q_1$, alors k^2 divise $d(p_1q_2-p_2q_1)^2$ donc k^2 divise $(p_1p_2 - dq_1q_2)^2$. D'après l'exercice 15 du chapitre 6 (il faut regarder la décomposition en produit de facteurs premiers), il en découle que k divise $p_1p_2 - dq_1q_2$. Il en découle finalement que

$$(x,y) = \left(\frac{|p_1p_2 - dq_1q_2|}{k}, \frac{|p_1q_2 - p_2q_1|}{k}\right)$$

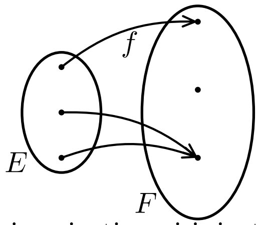
est une solution non triviale de l'équation. En effet, ce couple est solution (on divise par k^2 la dernière égalité ci-dessus), la deuxième coordonnée est non nulle car les couples (p_1,q_1) et (p_2,q_2) sont distincts et (p_1,q_1) sont premiers entre eux, ainsi que (p_2,q_2). Ouf !

Remarque : On peut faire le raisonnement inverse : si on sait que $\text{card}(E) = \text{card}(F)$, alors on peut se demander ce que cela implique pour une fonction $f : E \to F$. Elle n'a aucune raison d'être injective ou surjective (prendre une application constante), mais on se convainc assez facilement de la validité du théorème suivant avec des patatoïdes :

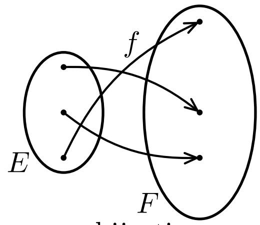
Théorème. Soient E et F deux ensembles **finis de même cardinal** et soit $f : E \to F$. Alors :

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

En particulier, si f va d'un ensemble **fini** dans lui-même, elle est injective si et seulement si elle est surjective, si et seulement si elle est bijective.



ni surjective ni injective



bijective

Remarque : Ce théorème est d'une grande aide lorsqu'on connaît les cardinaux des ensembles que l'on manipule (et qu'ils sont égaux) : parfois, prouver la surjectivité est difficile. Pour prouver que f est bijective, il suffit de prouver qu'elle est injective, ce qui est souvent plus facile.

I.4 Introduction aux cardinaux infinis (HP)

On généralise les résultats de la partie précédente aux cas des ensembles infinis.

Définition. Soient E et F deux ensembles infinis.

- S'il existe une application $f : E \to F$ injective, on dit que $\text{card}(E) \leqslant \text{card}(F)$.
- S'il existe une application $f : E \to F$ surjective, on dit que $\text{card}(E) \geqslant \text{card}(F)$.
- S'il existe une application $f : E \to F$ bijective, on dit que $\text{card}(E) = \text{card}(F)$.

C'est une définition !

Remarque : Cette définition est totalement intuitive. Dans le cas d'ensembles finis, on a vu que des ensembles finis ont le même nombre d'éléments quand il y a une bijection entre les deux. On veut définir proprement le fait que deux ensembles infinis ont « le même nombre d'éléments » et on prend donc cette définition : deux ensembles infinis ont « le même nombre d'éléments », ont « la même taille » lorsqu'il existe une bijection de l'un dans l'autre. On peut se dire que cette notion n'a aucun intérêt car, de toute façon, « l'infini c'est l'infini« ou « ils ont tous la même taille : une taille infinie » ou « ils ont tous le même nombre d'éléments : une infinité ». Rien ne saurait être plus faux ! Il existe « des infinis plus gros que d'autres » !

S'il existe une bijection de E dans F, on dit que E et F sont équipotents, et on a vu dans le chapitre 16 que cela définit une relation d'équivalence.

It is a little wrong to say a tomato is a vegetable. It is very wrong to say it's a suspension bridge.

Exemples :

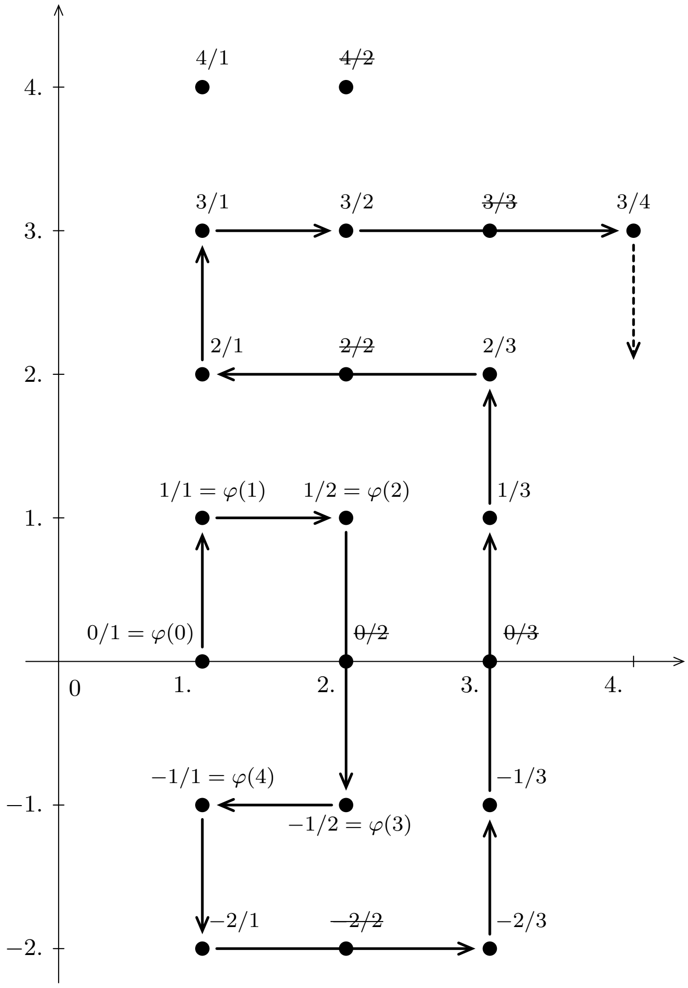
- On a vu dans le chapitre 4 qu'il existe une bijection de $\mathbb{N}$ dans $\mathbb{N}^*$. Ainsi, $\mathbb{N}$ et $\mathbb{N}^*$ ont le même cardinal.
- On a vu dans l'exercice 44 du chapitre 4 qu'il existe une bijection de $\mathbb{N}$ dans $\mathbb{Z}$. Ainsi, $\mathbb{N}$ et $\mathbb{Z}$ ont le même cardinal. Cela peut paraître surprenant à première vue, on pourrait se dire que $\mathbb{Z}$ « a deux fois plus d'éléments » que $\mathbb{N}$ mais, pour s'en convaincre, il suffit de représenter $\mathbb{N}$, $\mathbb{Z}$ et φ de la façon suivante :

$$\begin{array}{cccccccc}
\mathbb{N} & 0 & 1 & 2 & 3 & 4 & \cdots \\
\Big\downarrow \varphi & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
\mathbb{Z} & 0 & -1 & 1 & -2 & 2 & \cdots
\end{array}$$

Cette représentation justifie la cohérence de la définition, que deux ensembles (même infinis) sont de même taille lorsqu'il existe une bijection de l'un dans l'autre. En anglais, d'ailleurs, une bijection est parfois appelée « one-to-one function ».

- On a vu dans l'exercice 20 du chapitre 4 qu'il existe toujours une injection de E dans $\mathscr{P}(E)$ mais aucune bijection ! Par conséquent, la définition ci-dessus a un intérêt, tous les ensembles infinis ne font pas la même taille ! Un ensemble des parties est toujours « strictement plus gros » que l'ensemble ! Terminons par deux exemples classiques.
- Il existe une bijection entre $\mathbb{N}$ et $\mathbb{Q}$. On se contente d'une illustration du même type que ci-dessus. Pour cela, on écrit $\mathbb{Q}$ sous forme de tableau (numérateur en ordonnée, dénominateur en abscisse) dont on supprime les termes apparaissant plusieurs fois.

Expliquons un peu ce dessin (encore une fois, nous nous contenterons de ce dessin et d'une approche intuitive). Nous avons représenté tous les rationnels : le numérateur en ordonnée et le dénominateur en abscisse. Puisque les ordonnées parcourent $\mathbb{Z}$ et les abscisses $\mathbb{N}^*$, on obtient bien tous les rationnels. Certains sont atteints plusieurs fois : par exemple, $1 = 1/1 = 2/2 = 3/3$.



On veut construire une bijection de $\mathbb{N}$ dans $\mathbb{Q}$. Pour cela, on part de $0/1$ puis on fait le chemin ci-contre : quand on rencontre un rationnel qu'on a déjà vu, on le passe (et celui-ci est barré). Il est clair (encore une fois, on raisonne avec les mains) qu'on atteindra tous les rationnels et qu'on ne les atteindra qu'une fois car on passe ceux qu'on a déjà vus. En posant $\varphi(0) = 0/1, \varphi(1) = 1/1, \varphi(2) = 2/1, \varphi(3) = -1/2, \varphi(4) = -1/1$ etc., on construit une fonction définie sur $\mathbb{N}$, à valeurs dans $\mathbb{Q}$, et qui atteint une et une seule fois chaque rationnel : on a donc construit une bijection de $\mathbb{N}$ dans $\mathbb{Q}$.

- Enfin, montrons qu'il n'existe pas de bijection de $\mathbb{N}$ dans $\mathbb{R}$. Plus précisément, montrons qu'il n'existe pas de surjection de $\mathbb{N}$ dans $\mathbb{R}$. Soit $\varphi : \mathbb{N} \longrightarrow \mathbb{R}$, montrons que φ n'est pas surjective. Écrivons tous les $(\varphi(p))_{p\in\mathbb{N}}$ sous forme décimale : (les n_i appartiennent à $\mathbb{Z}$ et les d_{ij} à $[\![0\,;9]\!]$) :

> Le procédé de construction de y utilisé ci-contre est appelé procédé diagonal de Cantor (c'est Cantor qui, le premier, a montré qu'il n'existait pas de bijection entre $\mathbb{N}$ et $\mathbb{R}$).

$$\begin{array}{lclccccccc}
\varphi(0) & = & n_0, & d_{00} & d_{01} & d_{02} & \dots & d_{0p} & \dots \\
\varphi(1) & = & n_1, & d_{10} & d_{11} & d_{12} & \dots & d_{1p} & \dots \\
\varphi(2) & = & n_2, & d_{20} & d_{21} & d_{22} & \dots & d_{2p} & \dots \\
\vdots & & & & & & \ddots & & \\
\varphi(p) & = & n_p, & d_{p0} & d_{p1} & d_{p2} & \dots & d_{pp} & \dots \\
\vdots & & & & & & & & \ddots
\end{array}$$

Construisons un réel y de développement décimal $y = 0, y_0y_1y_2 \dots y_p \dots$ défini par :

- ⋆ $y_0 = 0$ si $d_{00} \neq 0$ et $y_0 = 1$ si $d_{00} = 0$.
- ⋆ $y_1 = 0$ si $d_{11} \neq 0$ et $y_1 = 1$ si $d_{11} = 0$.
- ⋆ Plus généralement, $y_p = 0$ si $d_{pp} \neq 0$ et $y_p = 1$ si $d_{pp} = 0$.

Alors $y \in \mathbb{R}$ mais $y \neq \varphi(p)$ pour tout $p \in \mathbb{N}$ car ces deux réels ont leur p-ième décimale distincte : y n'a aucun antécédent par φ donc φ n'est pas surjective. En conclusion, il n'y a aucune surjection donc aucune bijection de $\mathbb{N}$ dans $\mathbb{R}$: en conclusion, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ont le même cardinal, mais $\mathbb{R}$ a un cardinal strictement plus grand.

> Vous direz en deuxième année qu'un ensemble en bijection avec $\mathbb{N}$ (donc qui a le même cardinal que $\mathbb{N}$, on dit aussi : équipotent à $\mathbb{N}$) est dénombrable. Ainsi, $\mathbb{Z}$ et $\mathbb{Q}$ sont dénombrables, mais $\mathbb{R}$ ne l'est pas.

II Les trois commandements du dénombrement

Les résultats des paragraphes précédents sont surtout utiles pour justifier de façon théorique les raisonnements que l'on fait en pratique, et dont on parle plus en détails ci-dessous.

II.1 Compter par caractérisation

Je cite : « l'utilisation de bijections dans les problèmes de dénombrement n'est pas un attendu du programme ». Cependant (comme pour le lemme des bergers ci-dessous), on utilisera souvent sans le dire des bijections et le fait que cela préserve le cardinal, les résultats théoriques ci-dessus servant à justifier les raisonnements que l'on fera en pratique.

Le principe est simple : chercher ce qui caractérise un élément, chercher par quoi un élément est entièrement déterminé, et compter le nombre d'éléments en question. Nous utiliserons sans arrêt cette méthode, sans rappeler le résultat théorique sous-jacent. Par exemple, si on cherche le nombre de couples d'éléments de E (un ensemble fini) dont les deux coordonnées sont identiques, il suffit de voir qu'un tel couple est entièrement déterminé par sa première coordonnée, l'autre lui étant égale. Il y a donc $\text{card}(E)$ possibilités donc il y a $\text{card}(E)$ tels couples.

Rigoureusement, cela vient du fait que F, l'ensemble des couples d'éléments de E dont les deux coordonnées sont identiques, est en bijection avec E grâce à $\varphi : e \mapsto (e,e)$ donc E et F ont le même cardinal mais, comme on vient de le voir, en pratique, inutile de justifier autant.

II.2 Le principe additif

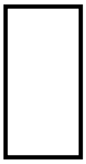
Principe additif : Si on a différents cas de figure deux à deux incompatibles, alors le nombre total de possibilités est la somme des nombres de possibilités dans chaque cas de figure. Cela vient du fait que le cardinal d'une union disjointe (elle l'est car les cas de figure sont deux à deux incompatibles) est la somme des cardinaux.

Exemples :

- On a 15 bonbons verts et 5 bonbons rouges. On a donc $15 + 5 = 20$ bonbons.
- Donnons un exemple moins trivial. Soit $n \geqslant 1$. Donnons le nombre de façons de paver un damier de taille $n \times 2$ avec des dominos de taille 1×2.

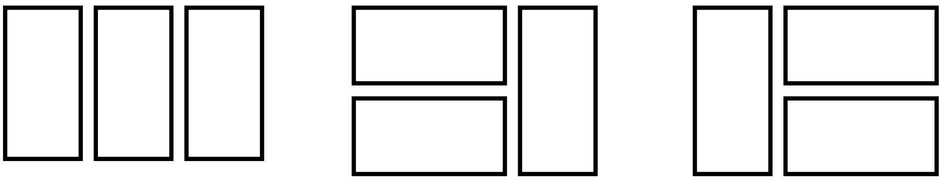
  Notons u_n le nombre recherché. Faisons un dessin pour de petites valeurs de n :

  ⋆ Dans le cas où $n = 1$, il y a une seule façon.



  ⋆ Dans le cas où $n = 2$, il y a deux façons :

  ⋆ Dans le cas où $n = 3$, il y a trois façons de faire :



  Supposons donc $n \geqslant 4$. Il y a deux cas de figure : soit le domino occupant la case en haut à gauche est vertical, soit il est horizontal.

  ⋆ Dans le cas où ce domino est vertical, on se retrouve dans la configuration ci-dessous :

Il reste à remplir le reste, c'est-à-dire un damier de taille $2 \times (n-1)$: on sait qu'il y a pour cela u_{n-1} façons de faire.

- Dans le cas où ce domino est horizontal, le coin inférieur gauche ne peut pas être recouvert par un domino vertical (il n'y a pas la place en hauteur), il l'est donc forcément par un domino horizontal, si bien qu'on est dans la configuration ci-dessous :

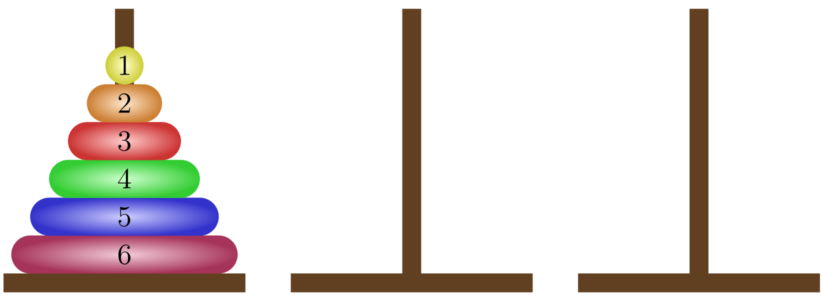
Il reste à remplir le reste, c'est-à-dire un damier de taille $2 \times (n-2)$: on sait qu'il y a pour cela u_{n-2} façons de faire.

Ces deux cas étant incompatibles, on applique le principe additif, c'est-à-dire que $u_n = u_{n-1} + u_{n-2}$. On reconnaît une suite récurrente linéaire d'ordre 2. On reconnaît même la même relation de récurrence que pour la suite de Fibonacci $(F_n)_{n\in\mathbb{N}}$, et puisque $u_1 = 1 = F_2$ et $u_2 = 2 = F_3$, alors $u_n = F_{n+1}$ pour tout $n \geqslant 1$, c'est-à-dire que le nombre recherché est

$$u_n = \frac{1}{\sqrt{5}} \times \left[\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right]$$

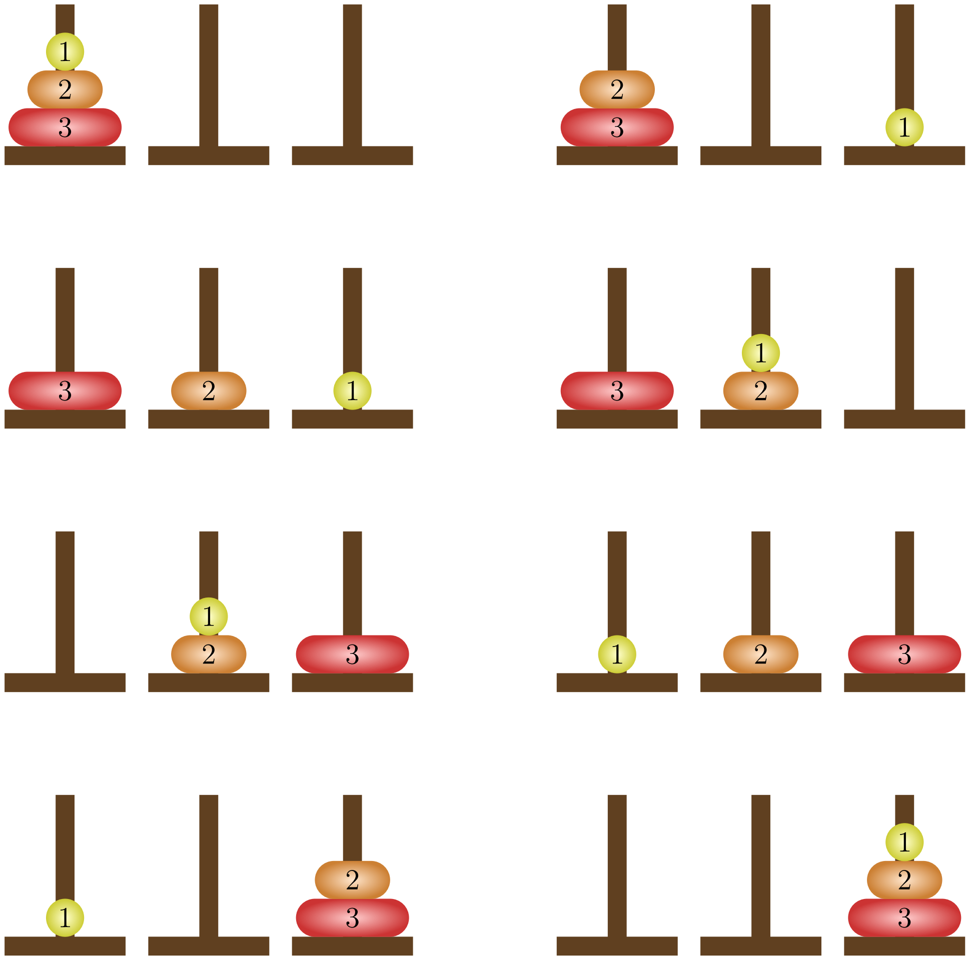
Remarque : Ce dernier exemple (pas forcément simple) est un exemple de raisonnement par récurrence, c'est-à-dire qu'on trouve un nombre grâce à une relation de récurrence en se ramenant au cas précédent. Ce genre de raisonnement est fréquent en combinatoire (et également en informatique, pour des calculs de complexité, en particulier pour des algorithmes récursifs ou de type « diviser pour régner »). Bien que cela n'utilise pas le principe additif, donnons un exemple classique de raisonnement combinatoire par récurrence : celui des tours de Hanoï.

Exemple : On dispose de n tores, numérotés de 1 à n, de diamètres croissants. On se donne également trois piquets, numérotés de A à C. Initialement, tous les tores sont enfilés sur le premier piquet, le plus grand étant à la base, le plus petit au sommet, comme sur la figure ci-dessous.



Le but du jeu est d'amener tous les tores sur le troisième piquet, en suivant les règles suivantes :

- déplacer les tores un à un d'un piquet à un autre.
- un tore ne doit jamais être posé sur un disque de diamètre inférieur. Ci-dessous une résolution du jeu lorsque $n = 3$.



On cherche le nombre u_n **minimal** de mouvement à effectuer pour terminer le jeu. Le cas $n = 1$ est trivial : il n'y a qu'une étape. Supposons $n \geqslant 2$ et là aussi, essayons de nous ramener à un rang inférieur.

On cherche le nombre minimal de mouvements, car on pourrait très bien décider de tourner en rond un long moment avant de s'y mettre sérieusement : mettre le plus petit tore sur le piquet B, puis le remettre sur le piquet A, puis à nouveau sur le piquet B etc. ce qui ferait grimper assez artificiellement le nombre de mouvements.

- Pour terminer le jeu, il faut bouger le plus grand tore sur le poteau C, et cela n'est possible que s'il n'y a plus aucun tore au dessus, c'est-à-dire qu'il faut avoir déplacé les $n-1$ autres tores. Ceux-ci sont donc forcément sur le poteau B car, s'ils sont sur le poteau C, on ne peut pas placer le grand tore par dessus. On peut y arriver en u_{n-1} mouvements pour les déplacer, et un mouvement supplémentaire pour mettre le n-ième tore sur le poteau C.
- Il faut ensuite replacer les $n-1$ tores restants sur le poteau C, et on peut y arriver en u_{n-1} mouvements.
- En d'autres termes, il est **possible** de terminer le jeu en $2u_{n-1}+1$ mouvements, c'est-à-dire que $u_n \leqslant 2u_{n-1}+1$. En effet, ce n'est pas (encore) une égalité puisque u_n est le nombre minimal : $2u_{n-1}+1$ mouvements suffisent, mais on pourrait faire mieux.
- Il faut prouver pour conclure qu'on ne peut pas y arriver en (strictement) moins de mouvements. Mais il suffit d'adapter la démonstration ci-dessus : il faut obligatoirement déplacer les $n-1$ premiers tores pour accéder au dernier, ce qui prend au moins u_{n-1} mouvements, puis il faut obligatoirement 1 mouvement pour déplacer le grand tore, et encore une fois il faut obligatoirement mettre les $n-1$ tores restants

au-dessus du grand sur le poteau C : encore au moins u_{n-1} mouvements, c'est-à-dire que $u_n \geqslant 2u_{n-1}+1$.

En conclusion, pour tout $n \geqslant 2$, $u_n = 2u_{n-1}+1$: on reconnaît une suite arithmético-géométrique, et puisque $u_1 = 1$, on trouve facilement que, pour tout n, $u_n = 2^n - 1$.

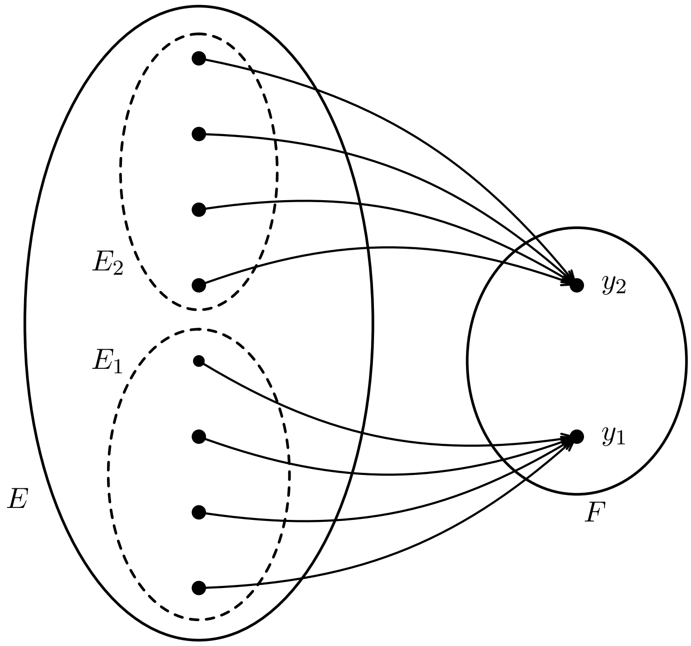
Pour la petite histoire, ce problème a été introduit par Edouard Lucas : cf. Wikipédia !

II.3 Le principe multiplicatif

II.3.a Fondement théorique : le lemme des bergers

Lemme (lemme des bergers). Soient E et F deux ensembles finis et $f : E \to F$ surjective. Soit enfin $k \in \mathbb{N}^*$. Si tout élément de F admet exactement k antécédents par f, alors $\text{card}(E) = k \times \text{card}(F)$.

Si un berger a n moutons (non amputés) alors il a $4n$ pattes de mouton dans son troupeau.



Démonstration. Notons $F = \{y_1; \dots ; y_p\}$ (et donc $\text{card}(F) = p$). Pour tout $i \in [\![1\,;\,p]\!]$, notons $E_i = f^{-1}(\{y_i\})$ l'ensemble des antécédents de y_i. Par hypothèse, pour tout i, $\text{card}(E_i) = k$. De plus, les E_i sont deux à deux disjoints et $E = \displaystyle\bigcup_{i=1}^{p} E_i$ donc

$$\begin{aligned} \text{card}(E) &= \sum_{i=1}^{p} \text{card}(E_i) \\ &= \sum_{i=1}^{p} k \\ &= k \times p \\ &= k \times \text{card}(F) \end{aligned}$$

□

Exemple : Soit E un ensemble fini à au moins deux éléments. Donnons le nombre de couples formés d'éléments de E distincts. Notons F l'ensemble des couples d'éléments distincts. Soit

$$f : \left\{ \begin{array}{ccc} F & \to & E \\ (e_1, e_2) & \mapsto & e_1 \end{array} \right.$$

Alors f est surjective. En effet, pour tout $e \in E$, il existe $e' \neq e$ (car E a au moins deux éléments) donc $f(e, e') = e$. De plus, les antécédents de e par f sont exactement les éléments de la forme (e, e') avec $e' \neq e$: un antécédent de e est entièrement déterminé par sa seconde coordonnée, un élément de E différent de E : il y a $\mathrm{card}(E) - 1$ choix donc e a $\mathrm{card}(E) - 1$ antécédents. D'après le lemme des bergers, $\mathrm{card}(F) = \mathrm{card}(E) \times (\mathrm{card}(E) - 1)$.

II.3.b Le principe multiplicatif :

Principe multiplicatif : On choisit successivement plusieurs éléments. Si, à chaque étape, le nombre de possibilités de l'élément qu'on choisit ne dépend pas des éléments choisis précédemment, alors le nombre total de possibilités est égal au produit du nombre de possibilités à chaque étape. Ce principe repose sur le lemme des bergers (il peut aussi reposer, selon les cas, sur le résultat donnant le cardinal d'un produit d'ensembles finis), voyons comment faire en pratique pour éviter une formalisation excessive comme dans l'exemple précédent.

Le nombre de possibilités ne varie pas mais les possibilités, elles, peuvent varier ! Avec le premier exemple ci-contre, le nombre de livres ne dépend pas du sac choisi, mais les livres eux-mêmes, si ! Heureusement, cela ne change rien pour l'application du principe multiplicatif.

Exemples :

- Exemple trivial : on a 3 sacs contenant chacun 10 livres. On a donc $3 \times 10 = 30$ livres. Ici, il ne faut pas additionner le nombre de sacs et le nombre de livres, car on choisit un sac <u>puis</u> un livre (et non pas un sac <u>ou</u> un livre comme dans l'exemple précédent), et pour chaque choix de sac possible, il y a 10 choix de livres possibles : le nombre de livres ne dépend pas du sac choisi donc on peut appliquer le principe multiplicatif.
- Reprenons l'exemple du paragraphe précédent et donnons encore le cardinal de F. Un élément de F est entièrement déterminé :
  - ⋆ par sa première coordonnée : $\mathrm{card}(E)$ choix possibles.
  - ⋆ par sa seconde coordonnée : pour tout choix de la première coordonnée, il y a $\mathrm{card}(E) - 1$ choix possibles (toutes sauf la première).

  D'après le principe multiplicatif, il y a bien $\mathrm{card}(E) \times (\mathrm{card}(E) - 1)$ choix possibles.
- Soit $n \geqslant 2$. Donnons le nombre de diviseurs positifs de n. Notons $n = {p_1}^{\alpha_1} \times \cdots \times {\alpha_k}^{p_k}$ la décomposition de n en produit de facteurs premiers. Alors (cf. chapitre 6) un entier d divise n si et seulement s'il s'écrit sous la forme $d = {p_1}^{\beta_1} \times \cdots \times {p_k}^{\beta_k}$ avec, pour tout i, $\beta_i \in [\![0\,; \alpha_i]\!]$. d est donc entièrement déterminé par :
  - ⋆ β_1 : $\alpha_1 + 1$ choix possibles.
  - ⋆ β_2 : $\alpha_2 + 1$ choix possibles.

    $\vdots$
  - ⋆ β_k : $\alpha_k + 1$ choix possibles.

  D'après le principe multiplicatif, il y a $(\alpha_1 + 1) \times \cdots \times (\alpha_k + 1)$ choix possibles donc n admet $(\alpha_1 + 1) \times \cdots \times (\alpha_k + 1)$ diviseurs.

Remarque : Quand utiliser le principe additif et quand utiliser le principe multiplicatif ? Il suffit de se demander si on prend l'un des deux (principe additif) ou l'un puis l'autre (principe multiplicatif) : toujours penser en terme de bonbons ou en terme de sacs et de livres. Pour faire simple :

- On choisit SOIT ça SOIT ça (en faisant attention d'avoir des choix incompatibles) : principe additif.
- On choisit ça PUIS ça (en faisant attention que le nombre de choix ne dépend pas de l'élément choisi) : principe multiplicatif.

Exemple : On a une urne contenant $2n$ boules numérotées de 1 à $2n$. Combien y a-t-il de façons possibles de tirer les $2n$ boules sans remise pour qu'une boule paire soit toujours suivie d'une boule impaire, et qu'une boule impaire soit toujours suivie d'une boule paire ?

Tout dépend en fait de la première boule tirée : soit elle est paire, soit elle est impaire. Si elle est paire, alors les $2n$ tirages seront : pair - impair - pair - impair - $\cdots$ - pair - impair, et ce sera l'alternance contraire si la première boule est impaire.

Supposons la première boule paire.

- Il y a n choix possibles (les numéros $2, 4, 6, \dots, 2n$) pour cette boule.
- Il y a n choix possibles pour la seconde boule (les numéros $1, 3, 5, \dots, 2n-1$).
- Pour la troisième boule, il a $n-1$ choix possibles : tous les numéros pairs sauf le numéro de la première boule.
- Idem pour la quatrième boule : il y a $n-1$ choix possibles, tous les numéros impairs sauf le numéro de la deuxième boule.
- et ainsi de suite jusqu'aux deux dernières boules, où il n'y a qu'un choix possible : le numéro pair restant (pour l'avant-dernière boule) et le numéro impair restant (pour la dernière).

Le nombre de possibilités ne dépend pas des boules tirées précédemment, même si les boules disponibles, elles, dépendent évidemment des tirages précédents.

Ainsi, dans le cas où la première boule est paire, par principe multiplicatif, il y a $n \times n \times (n-1) \times (n-1) \times \cdots \times 1 \times 1 = n!^2$. De même dans le cas d'une première boule impaire : $n!^2$ possibilités. Puisque la première boule est soit paire soit impaire, par principe additif, il y a $n!^2 + n!^2 = 2 \times (n!)^2$ tirages possibles.

III Listes et combinaisons

On se donne dans cette partie un entier $n \geqslant 1$ et E un ensemble fini de cardinal n.

III.1 p-listes.

Définition. Soit $p \geqslant 1$. On appelle p-liste (ou p-uplet) d'éléments de E toute famille de p éléments de E i.e. un élément de E^p.

Remarque : ⚠ On rappelle (cf. chapitre 3) qu'une famille n'est pas un ensemble : l'ordre compte et on peut avoir plusieurs fois le même élément dans une p-liste. Par exemple, $(1,2,2)$ et $(2,1,2)$ sont deux 3-listes distinctes de $E = \llbracket 1\,;\,6 \rrbracket$. Les listes sont par exemple utilisées en probabilités pour modéliser des tirages **successifs** (l'ordre compte) et **avec remise** (on peut avoir plusieurs fois le même élément). Par exemple, si on tire successivement et avec remise p boules dans une urne contenant n boules numérotées de 1 à n, alors les numéros des boules tirées forment une p-liste d'éléments de $\llbracket 1\,;\,n \rrbracket$.

Remarque : On peut avoir $p \geqslant n$ puisque les éléments d'une p-liste ne sont pas forcément distincts.

Proposition. Soit $p \geqslant 1$. Il y a n^p p-listes dans un ensemble à n éléments.

Démonstration. Il suffit de voir que $\mathrm{card}(E^p) = \mathrm{card}(E)^p = n^p$.

III.2 p-listes d'éléments distincts

III.2.a Nombre de p-listes d'éléments distincts

Une p-liste d'éléments distincts est parfois appelée un arrangement.

On s'intéresse dans ce paragraphe aux p-listes d'éléments distincts de E. On a alors forcément $p \leqslant n$ car on ne peut pas avoir plus d'éléments distincts qu'il y a d'éléments dans E. Attention, l'ordre compte toujours. Ainsi, $(1,2,3)$ et $(1,3,2)$ sont deux 3-listes distinctes (d'éléments distincts) de $\llbracket 1\,;\,6 \rrbracket$. Les listes d'éléments distincts (ou arrangements) sont par exemple utilisées en probabilités pour modéliser des tirages **successifs** (l'ordre compte) et **sans remise** (on ne peut pas avoir plusieurs fois le même élément). Par exemple, si on tire successivement et sans remise p boules dans une urne contenant n boules numérotées de 1 à n (avec forcément $p \leqslant n$), alors les numéros des boules tirées forment une p-liste d'éléments distincts de $\llbracket 1\,;\,n \rrbracket$.

Proposition. Soit $p \leqslant n$. Il y a $\dfrac{n!}{(n-p)!}$ p-listes d'éléments distincts dans un ensemble à n éléments.

Démonstration. Découle du principe multiplicatif : il y a n choix pour le premier élément, puis $n-1$ choix pour le deuxième (tous sauf le premier) et ainsi de suite jusqu'au p-ième, pour lequel il y a $n-(p-1) = n-p+1$ choix possibles (tous sauf les $p-1$ premiers). Dès lors, il y a bien

$$n \times (n-1) \times \cdots \times (n-p+1) = \frac{n!}{(n-p)!}$$

□

choix possibles.

Exemple : Le tiercé. Il y a 15 chevaux au départ. Combien y a-t-il de tiercés, quartés, quintés différents ?

Un cheval ne peut apparaître qu'une seule fois dans le classement, et l'ordre compte. Il y a donc :

- $15 \times 14 \times 13$ tiercés possibles.
- $15 \times 14 \times 13 \times 12$ quartés possibles.
- $15 \times 14 \times 13 \times 12 \times 11$ quintés possibles.

III.2.b Application aux injections et aux bijections/permutations

On peut se demander l'utilité d'une telle notion, ou se dire qu'une p-liste ne se rencontre pas très souvent au coin d'une rue (idem pour les urnes et les boules). Il faut en fait bien comprendre que ces objets sont en quelque sorte des modèles permettant de modéliser des situations extrêmement fréquentes (comme le tiercé dans le paragraphe précédent). Une p-liste représente une succession d'éléments avec ordre et avec répétition, et une p-liste d'éléments distincts représente une succession d'éléments avec ordre et sans répétition. Dès qu'on rencontre une situation de ce type, on peut donc la modéliser par une p-liste (d'éléments distincts ou non), ce qui permet de donner le nombre d'objets auxquels on s'intéresse. Donnons deux exemples très importants (et au programme).

Ce sera la même chose pour une combinaison dans le paragraphe suivant.

Rappelons qu'une p-liste, et une famille en général, est une fonction (cf. chapitre 4). Par exemple, si $E = \{x_1; \dots; x_p\}$ et si $F = \{y_1; \dots; y_n\}$, alors une p-liste d'éléments de F $(z_1, \dots, z_p)$ peut être vue comme l'application de E dans F suivante

$$\begin{tikzcd}
x_1 \arrow[d] & x_2 \arrow[d] & \cdots & x_k \arrow[d] \\
z_1 & z_2 & \cdots & z_k
\end{tikzcd}$$

On en déduit le résultat suivant :

Corollaire. Si E et F sont deux ensembles finis, alors il y a F^E est fini de cardinal $\text{card}(F)^{\text{card}(E)}$. En particulier, il y a n^p applications d'un ensemble à p éléments dans un ensemble à n éléments.

Remarque : Encore une fois, cela se voit très bien avec le principe multiplicatif : s'il y a n éléments dans F et p éléments dans E, alors une application de E dans F est entièrement déterminée par l'image de $x_1, \dots, x_p$ (les éléments de E) et il y a n choix pour l'image de x_1, n choix pour l'image de x_2 etc. jusqu'à x_p donc il y a $n \times \cdots \times n = n^p$ choix possibles donc n^p fonctions de E dans F.

De la même manière, une p-liste d'éléments distincts d'un ensemble à n éléments peut être vue comme une application injective d'un ensemble E à p éléments dans un ensemble

F à n éléments. En effet, si $E = \{x_1; \dots; x_p\}$ et si $F = \{y_1; \dots; y_n\}$, alors une p-liste d'éléments distincts de F $(z_1, \dots, z_p)$ peut être vue comme l'application de E dans F ci-dessus (injective car les z_k sont distincts). On en déduit le résultat suivant :

Corollaire. Si $p \leqslant n$, alors il y a $\dfrac{n!}{(n-p)!}$ injections d'un ensemble de cardinal p dans un ensemble de cardinal n.

Nous en reparlerons dans le paragraphe suivant.

Remarque : Cela se voit encore une fois très bien avec le principe multiplicatif : n choix pour l'image de x_1, $n-1$ pour l'image de x_2 etc.

cf. exercice 28 pour le nombre de surjections.

Définition. Soit E un ensemble non vide. On appelle permutation de E toute bijection de E dans lui-même.

Remarques :

- On se restreindra dans ce chapitre au cas d'un ensemble fini, mais cette définition est plus générale et permet de définir le groupe des permutations d'un ensemble non vide quelconque, cf. chapitre 18.
- En généralisant les remarques précédentes, une bijection ou permutation d'un ensemble à n éléments dans lui-même n'est rien d'autres qu'un n-uplets d'éléments distincts de cet ensemble. Par exemple, si $E = \{x_1; x_2; x_3\}$, alors on peut assimiler la n-liste (d'éléments distincts) (x_2, x_1, x_3) à la bijection

$$\begin{array}{ccc} x_1 & x_2 & x_3 \\ \downarrow & \downarrow & \downarrow \\ x_2 & x_1 & x_3 \end{array}$$

- Nous garderons le terme « bijection » pour les ensembles infinis, nous parlerons plutôt de permutation quand nous manipulerons des ensembles finis (et, surtout quand nous manipulerons le groupe symétrique S_n, nous les écrirons sous forme de n-uplets, cf. chapitre 32).

Corollaire. Il y a $n!$ permutations d'un ensemble à n éléments.

Il y a donc $n!$ bijections d'un ensemble de cardinal n dans lui-même.

Remarque : Une permutation d'un ensemble à n éléments $E = \{x_1, \dots, x_n\}$ est une manière d'ordonner, de classer ces n éléments (d'où le nom de permutation) : il y a donc $n!$ manières d'ordonner n éléments. Par exemple, si $n = 3$, on peut ordonner x_1, x_2 et x_3 de 6 façons différentes :

- x_1, x_2, x_3
- x_1, x_3, x_2
- x_2, x_1, x_3
- x_2, x_3, x_1
- x_3, x_1, x_2
- x_3, x_2, x_1

De la même façon, il y a 46! façons de classer les élèves de la classe, c'est-à-dire qu'il y a 46! classements possibles au DS.

Autre exemple : si vous avez 100 chansons dans une playlist, il y a 100! ordres de lecture possibles : c'est un nombre tellement énorme que l'ordre de lecture peut être considéré comme totalement aléatoire, et que vous ne tombiez jamais deux fois sur la même.

III.3 Parties/Combinaisons d'un ensemble à n éléments

Rappel : Un élément appartient ou non à un ensemble, il ne peut pas appartenir plusieurs fois. Par exemple, $\{1; 1; 2\} = \{1; 2\}$. De plus, l'ordre des éléments ne compte pas : $\{1; 2\} = \{2; 1\}$. On ne confondra pas une famille ou une liste (dans lesquelles l'ordre compte) et un ensemble ou une partie, dans lesquels l'ordre ne compte pas.

Proposition. Soit $k \in \llbracket 0 ; n \rrbracket$. Il y a $\displaystyle\binom{n}{k}$ parties à k éléments dans un ensemble à n éléments.

Le fait (cf. chapitre 3) que, par définition, $\binom{n}{p}$ soit nul si $p < 0$ ou $p > n$ n'est donc pas si surprenant, et est cohérent avec le résultat ci-contre : il n'y a aucune partie à -2 ou à 17 éléments dans un ensemble à 5 éléments.

Exemple : Dans un ensemble E à n éléments :

- Il y a $\displaystyle\binom{n}{0} = 1$ partie à 0 éléments : l'ensemble vide.
- Il y a $\displaystyle\binom{n}{1} = n$ parties à 1 éléments : les singletons.
- Il y a $\displaystyle\binom{n}{n} = 1$ partie à n éléments : E lui-même.

Démonstration. Notons C_n^k le nombre cherché. Un arrangement à k éléments (ou une k-liste d'éléments distincts) d'un ensemble à n éléments est entièrement déterminé par :

- l'ensemble de ces k éléments (l'ordre n'étant pas encore fixé). Il y a donc C_n^k choix possibles.
- l'ordre des éléments choisis. Pour chaque ensemble de k éléments, il y a $k!$ façons de les ordonner (nombre de permutations dans un ensemble à k éléments).

Par principe multiplicatif, $A_n^k = C_n^k \times k!$ donc

$$\begin{aligned} C_n^k &= \frac{A_n^k}{k!} \\ &= \frac{n!}{k! \times (n-k)!} \\ &= \binom{n}{k} \end{aligned}$$

$\square$

Remarque : On dit parfois que la donnée de k éléments de E sans notion d'ordre ou de répétition est une combinaison à k éléments (ou k-combinaison), d'où la notation C_n^k (qui est parfois utilisée à la place de $\displaystyle\binom{n}{k}$ dans les sujets plus anciens).

Remarque : ⚠ On rappelle (voir ci-dessus) qu'un ensemble n'est pas une famille : l'ordre ne compte pas et on ne peut pas avoir plusieurs fois le même élément dans une p-liste. Les parties (ou combinaisons) sont par exemple utilisées en probabilités pour modéliser des tirages **simultanés** (l'ordre ne compte pas) et **sans remise** (on ne peut pas avoir plusieurs fois le même élément). Par exemple, si on tire de façon simultanée (pas d'ordre et pas de remise) p boules dans une urne contenant n boules numérotées de 1 à n, alors les numéros des boules tirées forment une p-combinaison d'éléments de $\llbracket 1 ; n \rrbracket$: il y en a donc $\displaystyle\binom{n}{p}$.

Exemple : À l'Euromillion, il faut choisir 5 numéros parmi 50 et deux étoiles parmi 12 : même si les tirages sont successifs, l'ordre ne compte pas. Dès lors, il y a $\displaystyle\binom{50}{5}$ choix possibles pour les numéros, et $\displaystyle\binom{12}{2}$ choix possibles pour les étoiles. Par principe multiplicatif, il y a :

$$\binom{50}{5} \times \binom{12}{2} = \frac{50 \times 49 \times 48 \times 47 \times 46}{120} \times \frac{12 \times 11}{2} \approx 140 \times 10^6$$

combinaisons différentes.

Corollaire. Soit E un ensemble fini de cardinal n. Alors $\mathscr{P}(E)$ est un ensemble fini de cardinal 2^n.

DÉMONSTRATION. Soit $k \in \llbracket 0\,;n \rrbracket$. D'après ce qui précède, il y a $\binom{n}{k}$ parties de E à k éléments. Or une partie de E a 0 élément ou 1 élément ou ... ou n éléments. Les différents cas de figure sont incompatibles donc, par principe additif,

$$\begin{aligned}\operatorname{card} \mathscr{P}(E) &= \sum_{k=0}^{n} \binom{n}{k} \\ &= 2^n\end{aligned}$$

□

Remarque : De même, il y a (de même que dans le chapitre 3 : faire la somme et la différence) $\displaystyle\sum_{\substack{k=0\\k \text{ pair}}}^{n} \binom{n}{k} = 2^{n-1}$ parties de E de cardinal pair et $\displaystyle\sum_{\substack{k=0\\k \text{ impair}}}^{n} \binom{n}{k} = 2^{n-1}$ parties de E de cardinal pair. Un ensemble contient donc autant de parties de cardinal pair que de parties de cardinal impair

Exemple : Soit $n \geqslant 1$ et soit $m \in \llbracket 0\,;n \rrbracket$. Notons P_m l'ensemble des parties de $\llbracket 1\,;n \rrbracket$ à m éléments. Soient enfin $x_1, \dots, x_n$ des réels. Soit $1 \leqslant i \leqslant n$ un entier naturel. Montrer que

$$\sum_{A \in P_m} \sum_{i \in A} x_i = \binom{n-1}{m-1} \sum_{i=1}^{n} x_i$$

Réponse : Notons $S = \displaystyle\sum_{A \in P_m} \sum_{i \in A} x_i$. Tout d'abord, $S = \displaystyle\sum_{A \in P_m} \sum_{\substack{i=1\\i \in A}}^{n} x_i$. On peut intervertir les deux sommes, ce qui donne $S = \displaystyle\sum_{i=1}^{n} \sum_{\substack{A \in P_m\\A \text{ contenant } i}} x_i$. Or, dans la seconde somme, on somme sur les parties A (en poussant un peu, on pourrait dire que A est l'indice de sommation) : x_i est indépendant de A, on peut donc le considérer comme un terme constant, et on sait que la somme d'un terme constant est le terme constant multiplié par le nombre de termes, si bien que

$$\sum_{\substack{A \in P_m\\A \text{ contenant } i}} x_i = x_i \times \operatorname{card}\left(A \in P_m | i \in A\right) = x_i \times \binom{n-1}{m-1}$$

En effet, une partie A de P_m contenant i est entièrement déterminée par les $m-1$ (rappelons que A a m éléments) autres éléments de A, choisis parmi les $n-1$ éléments de $\llbracket 1\,;n \rrbracket$ distincts de i. Il y a $\binom{n-1}{m-1}$ choix donc il y a $\binom{n-1}{m-1}$ parties de A de cardinal m contenant i, ce qui permet de conclure.

Représentons les entiers $i \in \llbracket 1\,;n \rrbracket$ et les parties $A \in P_m$ sous forme d'un tableau comme ci-dessus :

$$\begin{array}{c} \\ A_1 \\ A_2 \\ A_3 \\ \vdots \end{array} \begin{array}{c} \begin{array}{ccc} 1 & 2 & \dots \end{array} \\ \begin{pmatrix} X & & \dots \\ & & \dots \\ X & X & \dots \\ & \vdots & \vdots \end{pmatrix} \end{array}$$

où l'on a mis une croix si i appartient à la partie A écrite à gauche. Le principe de Fubini dit que nous pouvons sommer indifféremment selon les lignes ou les colonnes. Si nous sommons selon les lignes, pour chaque partie $A \in P_m$, nous sommons sur les entiers i appartenant à A, tandis que si nous sommons les colonnes, pour chaque entier $i \in \llbracket 1\,;n \rrbracket$, nous sommons sur les parties A auxquelles i appartient. D'où l'égalité

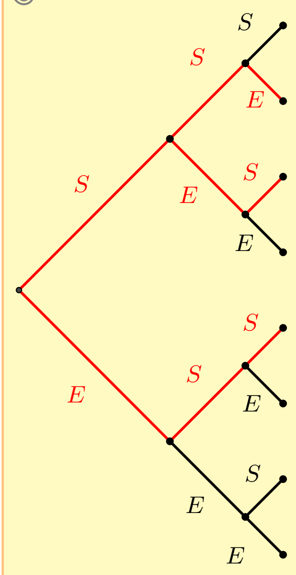
$$\sum_{A \in P_m} \sum_{i \in A} = \sum_{i=1}^{n} \sum_{\substack{A \in P_m\\A \text{ contenant } i}}$$

III.4 Un peu de combinatoire avec des coefficients binomiaux

Encore une fois, les objets (listes, combinaisons) que nous manipulons sont des modèles qui permettent de modéliser des situations très fréquentes. Ici, les combinaisons cherchent à compter des objets sans notion d'ordre ou de répétition. Un cas de figure se présente souvent :

Cadre : Soit $n \geqslant 1$. On réalise n fois une expérience où deux issues sont possibles : succès et échec. On représente la répétition de ces expériences sous forme d'un arbre, voir ci-dessous.

Proposition. Soit $k \in [\![0\,;n]\!]$. Il y a $\dbinom{n}{k}$ chemins réalisant k succès parmi les n réalisations d'une expérience, l'ordre ne comptant pas.



Remarque : De façon équivalente : il y a $\dbinom{n}{k}$ façons d'obtenir k succès parmi n réalisations, l'ordre ne comptant pas.

Exemple : Ci-contre, il y a deux chemins comportant exactement deux succès (en rouge) et on a bien $\dbinom{3}{2} = 3$.

Démonstration. Un chemin à k succès est entièrement déterminé par les instants auxquels ont lieu les succès (les autres instants donnant obligatoirement lieu à des échecs). En d'autres termes, un chemin à k succès est entièrement déterminé par la partie à k éléments de $[\![1\,;n]\!]$ formée des instants auxquels ont lieu des succès (par exemple, sur le dessin ci-dessus la partie $\{2;3\}$ correspond au chemin ayant des succès aux instants 2 et 3 et un échec à l'instant 1). Il y a donc autant de chemins à k succès que de parties à k éléments, ce qui permet de conclure.

Là aussi, on manipule une bijection sans le dire : la bijection envoyant un chemin sur la partie formée des instants auxquels ont lieu les succès.

Rappelons les résultats suivants, vus au chapitre 3 :

Théorème.
Soient $n \in \mathbb{N}^*$ et $p \in [\![0\,;n]\!]$.

1. $\dbinom{n}{n} = \dbinom{n}{0} = 1$.
2. Si $n \in \mathbb{N}^*$, alors $\dbinom{n}{n-1} = \dbinom{n}{1} = n$.
3. Symétrie des coefficients binomiaux : $\dbinom{n}{p} = \dbinom{n}{n-p}$.
4. Formule de Pascal : si $p \in [\![1\,;n-1]\!]$, alors $\dbinom{n}{p} = \dbinom{n-1}{p-1} + \dbinom{n-1}{p}$.

Démonstration. On a prouvé ces résultats grâce à la définition des coefficients binomiaux (celle avec des factorielles). Donnons à présent une démonstration combinatoire de ces résultats.

1. Il y a un seul chemin avec uniquement des succès, tout comme il y a un seul chemin avec uniquement des échecs.
2. Il y a n façons d'obtenir exactement un succès. En effet, un tel chemin est entièrement déterminé par le temps d'apparition du succès (n choix possibles) : les autres expériences donnent lieu à des échecs. Il en découle que $\dbinom{n}{1} = n$. De même pour $\dbinom{n}{n-1}$.
3. Les échecs et les succès jouant le même rôle, il y a autant de chemins avec k succès que de chemins avec k échecs. Or, obtenir k échecs revient à obtenir $n-k$ succès.
4. On suppose qu'on réalise $n+1$ répétitions d'une expérience. Soit $k \in [\![0\,;n-1]\!]$. Soit la première expérience est un succès, soit c'est un échec :
   On cherche le nombre de façons d'obtenir $k+1$ succès :
   - Si la première expérience est un succès, obtenir $k+1$ succès revient à obtenir k succès parmi les n expériences restantes : il y a donc $\dbinom{n}{k}$ choix possibles.
   - Si la première expérience est un échec, obtenir $k+1$ succès revient à obtenir $k+1$ succès parmi les n expériences restantes : il y a donc $\dbinom{n}{k+1}$ choix possibles.

Ces deux cas de figures sont incompatibles : par principe additif, le nombre de façons d'obtenir $k+1$ succès est égal à $\binom{n}{k}+\binom{n}{k+1}$. Or, il est par définition égal à $\binom{n+1}{k+1}$. D'où le résultat.

Rappelons également la formule du binôme de Newton :

Théorème (Formule du binôme de Newton). Soient $n \in \mathbb{N}$ et $(a,b) \in \mathbb{C}^2$.

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

DÉMONSTRATION. Donnons une démonstration combinatoire de ce résultat. $(a+b)^n$ n'est rien d'autre que l'écriture condensée de

$$\underbrace{(a+b)\times\cdots\times(a+b)}_{n \text{ fois}}$$

□

Pour développer, il faut prendre exactement un a ou un b par parenthèse. Si $k \in [\![0\,;n]\!]$, il y a $\binom{n}{k}$ façons d'obtenir k fois a (et on obtient automatiquement $n-k$ fois b), donc il y a $\binom{n}{k}$ termes de la forme $a^k b^{n-k}$. Ceci étant valable pour $k=0,\ldots,k=n$, on a le résultat voulu.

Terminons par deux formules HP mais classiques (cf. par exemple exercices 37 et 41 du chapitre 3, ou l'exercice 52 du chapitre 14) :

Proposition. Si $p \neq 0$, alors $p\binom{n}{p} = n\binom{n-1}{p-1}$.

DÉMONSTRATION. On peut démontrer cette formule par un calcul direct, mais nous allons en donner une démonstration combinatoire. On cherche à faire une équipe de p personnes prises parmi n personnes, et à désigner un chef (d'où le nom de cette formule) dans cette équipe. On peut le faire de deux façons différentes :

- on peut soit choisir d'abord les p personnes formant l'équipe ($\binom{n}{p}$ choix possibles) puis choisir un chef (p choix possibles) ce qui donne $p\times\binom{n}{p}$ choix possibles.
- on peut soit choisir la personne qui sera le chef (n choix possibles) puis choisir les $p-1$ personnes restantes qui intégreront l'équipe, et celles-ci sont à choisir parmi les $n-1$ personnes restantes, toutes sauf le chef ($\binom{n-1}{p-1}$ choix possibles) ce qui donne finalement $n\times\binom{n-1}{p-1}$ choix possibles.

Ces deux façons de faire donnant le même nombre de possibilités, les deux nombres de possibilités sont égaux, ce qui est le résultat voulu.

Cette démonstration justifie le joli nom (personnel !) que j'aime donner à cette formule : la formule du chef.

Proposition. Soit $n \in \mathbb{N}$. Alors :

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

Démonstration. On se donne $2n$ objets. Il y a $\binom{2n}{n}$ façons de choisir n objets parmi ces $2n$ objets. Mais on peut aussi faire comme suit : pour tout $k \in [\![0\,;\,n]\!]$, on peut d'abord choisir k objets parmi les n premiers puis $n-k$ objets parmi les n restants, ce qui donne, par principe multiplicatif, $\binom{n}{k} \times \binom{n}{n-k}$. Or, toutes ces possibilités, pour chaque valeur de k, sont incompatibles puisque dans chaque cas de figure, on aura un nombre d'objets différents parmi les n premiers, si bien que par principe additif, le nombre de façons de choisir ces objets est

$$\sum_{k=0}^{n} \binom{n}{k} \times \binom{n-k}{k}$$

□

Cette somme est égale à celle de l'énoncé par symétrie des coefficients binomiaux, et elle est donc égale à $\binom{2n}{n}$.

Remarques :

- Plus généralement, si $(n,p,q) \in \mathbb{N}^3$, on a la formule de Vandermonde (dont la démonstration est analogue et laissée en exo) :

$$\sum_{k=0}^{q} \binom{n}{k} \times \binom{p}{q-k} = \binom{n+p}{q}$$

- Attention, dans l'exemple précédent, il ne faut pas raisonner comme suit : « Il y a $(n+1)$ façons de choisir le nombre d'objets parmi les n premiers (entre 0 et n) puis, une fois ce nombre k choisi, il y a $\binom{n}{k}$ façons pour choisir ces k objets, puis $\binom{n}{n-k}$ façons de choisir les objets restants donc, par principe multiplicatif, il y a $(n+1) \times \binom{n}{k} \times \binom{n}{n-k}$ façons de choisir les objets ». Où est l'erreur ? Tout d'abord, dans la rédaction finale, k n'est pas défini, donc cela n'a aucun sens ! Mais, plus généralement, il faut bien comprendre le principe multiplicatif : à chaque étape, le nombre de choix ne doit pas dépendre des choix précédents. En particulier, si le nombre de choix (comme ici) dépend du choix précédent (du choix de k dans notre exemple), le principe multiplicatif ne s'applique pas ! On peut commencer par dénombrer le nombre de possibilités pour k mais, si on se rend compte que cela change quelque chose pour le nombre de possibilités, alors c'est qu'il ne faut pas appliquer le principe multiplicatif et se demander s'il ne faut pas plutôt appliquer le principe additif.

Bilan : Lorsqu'on veut choisir p éléments dans un ensemble à n éléments, il faut se poser les deux questions suivantes : l'ordre compte-t-il ? peut-on avoir plusieurs fois le même élément ?

- Avec ordre, et avec répétitions : p-listes.
- Avec ordre, et sans répétitions : p-listes d'éléments distincts/arrangements.
- Sans ordre, et sans répétitions : parties à p éléments, ou p-combinaisons.

Le cas sans ordre et avec répétitions n'est pas au programme, nous en parlerons dans l'exercice 26

Attention, parfois, parler d'ordre est ambigu quand il n'y a aucune notion de temporalité. Si on a un doute, on se demande si, en intervertissant les deux objets, on a la même chose. Par exemple, si on cherche la façon d'avoir deux paires quand on joue au poker (cf. exercice 23), on peut se dire qu'il y a 13 valeurs pour la valeur de la première paire (disons, une paire de dames) puis 12 valeurs pour la valeur de la deuxième paire (disons une paire de valets), ce qui fait 13×12 possibilités pour les valeurs des deux paires

Il reste à choisir les couleurs et la cinquième carte : cf. exercice 23.

Mais cette façon de faire est erronée : on a introduit une notion d'ordre, on a pris d'abord une paire et ensuite une autre. En d'autres termes : les deux paires n'ont pas le même rôle, si on les intervertit on n'a pas le même jeu. Ou encore en d'autres termes : une paire de dames puis une paire de valets, ce n'est pas la même chose qu'une paire de valets puis une paire de dames, ce qui est évidemment faux. Les deux paires jouant un rôle symétrique, on est en présence d'une combinaison ou d'une partie : il y a $\binom{13}{2}$ façons de choisir les valeurs des deux paires, c'est-à-dire $\dfrac{13 \times 12}{2}$.

On peut aussi voir les choses de la façons suivante : en prenant le lemme des bergers « à l'envers », si on a regroupés des objets par paquets, pour connaître le nombre de paquets, on divise par le nombre d'éléments par paquets. En d'autres termes (et nous ferons ça souvent) : « on divise par le nombre d'éléments donnant le même paquet pour qu'ils ne comptent que pour un ».

Donnons un exemple simple : donnons le nombre d'anagrammes (ayant un sens ou non) du mot « menteuse ». Une anagramme est un mot obtenu en changeant l'ordre des lettres. Il y a donc autant d'anagrammes (enfin, presque, voir la suite) que de façons d'ordonner les lettres du mot, donc que de permutations des 8 lettres : il y a donc 8! façons d'ordonner les 8 lettres du mot. On pourrait donc se dire qu'il y a 8! anagrammes... mais il faut se rendre compte que plusieurs permutations donnent le même mot ! Par exemple, si les lettres sont notées de 1 à 8, la permutation $(1, 2, 3, 4, 5, 6, 7, 8)$, c'est-à-dire quand on ne change aucune lettre de place, donne le même mot que la permutation $(1, 2, 3, 4, 8, 6, 7, 5)$, c'est-à-dire la permutation qui consiste à échanger les deux derniers e. Combien de permutations donnent le même mot ?

Je précise qu'anagramme est un nom féminin !

On voit que la seule lettre présente plusieurs fois est le e donc il y a autant de permutations qui donnent le même mot que de façons de permuter entre eux les lettres e. Puisqu'il y a trois e, il y a 3! façons de permuter les e au sein d'un même mot, donc pour chaque mot, il y a 3! permutations des e qui donnent ce mot, donc il y a 3! permutations qui donnent le même mot, qui ne comptent que pour un mot. Pour avoir le nombre total d'anagrammes, il faut donc diviser par 3!, si bien qu'il y a 8!/3! anagrammes du mot « menteuse ».

IV Activité de synthèse : les nombres de Catalan

IV.1 Définition et relation de récurrence

Soit $n \geqslant 0$. On note C_n le nombre de façons d'écrire n parenthèses gauches et n parenthèses droites de sorte que le mot obtenu soit bien parenthésé (avec la convention selon laquelle, lorsqu'il n'y a pas de parenthèse, il n'y a qu'une façon de les ordonner, en ne faisant rien... donc $C_0 = 1$). Par exemple, pour $n = 3$, les 5 possibilités sont `((()))`, `(()())`, `(())()`, `()(())` et `()()()`. Les nombres C_n sont appelés nombres de Catalan. Donner une relation de récurrence vérifiée par la suite $(C_n)_{n\geqslant 1}$.

Un tel parenthésage est appelé un bon parenthésage, ou un parenthésage admissible.

Ils sont nommés ainsi en l'honneur d'Eugène Catalan, mathématicien belge... ce ne sont pas des nombres qui aiment passer leurs vacances à Barcelone !

Il suffit de regarder quand fermera la première parenthèse. Puisque le mot est bien parenthésé, toutes les parenthèses ouvertes après la premières sont refermées avant la première, si bien qu'il y a un nombre pair de parenthèses fermées entre la première parenthèse et la parenthèse qui la ferme. Notons $2k$ le nombre de parenthèses entre celles-ci : k peut prendre n'importe quelle valeur entre 0 (s'il n'y en a aucune) et $n - 1$ (si toutes les autres parenthèses se retrouvent entre celles-ci). Il y a alors C_k façons de bien les ordonner. Il reste $2n - 2k - 2 = 2(n - k - 1)$ parenthèses à placer ensuite, et il y a C_{n-k-1} façons de les ordonner. En d'autres termes, on a une situation de la forme suivante :

Le -2 vient de la première parenthèse et de sa parenthèse fermante, qu'il ne faut pas oublier.

$$\underbrace{(}_{\substack{\text{première}\\ \text{parenthèse}}} \quad \underbrace{\cdots}_{\substack{2k \text{ parenthèses restantes}\\ C_k \text{ manières}\\ \text{de les ordonner}}} \quad \underbrace{)}_{\substack{\text{parenthèse}\\ \text{fermant}\\ \text{la première}}} \quad \underbrace{\cdots}_{\substack{2n-2k-2 \text{ parenthèses restantes}\\ C_{n-k-1} \text{ manières}\\ \text{de les ordonner}}}$$

En d'autres termes, pour tout $k \in [\![0\,;\, n-1]\!]$, il y a C_k façons d'ordonner les $2k$ parenthèses entre la première parenthèse et celle qui la ferme, et C_{n-k-1} façons d'ordonner celles qui suivent donc, par principe multiplicatif, il y a $C_k \times C_{n-k-1}$ façons d'ordonner toutes les parenthèses, et ceci est valable lorsqu'il y a $2k$ parenthèses entre la première parenthèse et celle qui la ferme. Or, soit k vaut 0, soit k vaut 1 etc. soit k vaut $n - 1$ et donc, par principe additif :

$$C_n = \sum_{k=0}^{n-1} C_k \times C_{n-1-k}$$

Lorsqu'il y a 2 parenthèses, il n'y a qu'une façon de les ordonner : `()`, donc $C_1 = 1$. Avec la relation ci-dessus, on trouve successivement :

- $C_2 = C_0C_1 + C_1C_0 = 2$.
- $C_3 = C_0C_2 + C_1C_1 + C_2C_0 = 5$.
- $C_4 = C_0C_3 + C_2C_1 + C_1C_2 + C_0C_3 = 14$.

IV.2 Chemins de Bernoulli

On munit le plan d'un repère orthonormé direct. Soient n et k des entiers tels que $0 < n$. On appelle chemin de Bernoulli allant de $(0,0)$ à (n,k) une ligne polygonale dans le plan joignant le point de coordonnées $(0,0)$ au point de coordonnées (n,k) en ne faisant que des montées (déplacement selon le vecteur $(1,1)$) et des descentes (déplacement selon le vecteur $(1,-1)$).

Ci-dessus un exemple d'un chemin allant de $(0,0)$ à (n,k) avec $n = 20$ et $k = 2$. Il est constitué de deux montées successives, puis d'une descente, puis de trois montées successives, puis de deux descentes successives, etc.
On cherche le nombre de chemins de Bernoulli reliant $(0,0)$ à (n,k). Puisqu'un chemin de Bernoulli ne peut aller que dans deux directions (vers le haut ou vert le bas, toujours vers la droite), un chemin est entièrement déterminé par les instants auxquels il va vers le haut (il ira obligatoirement vers le bas aux autres instants). Par exemple, ci-dessus, pour caractériser entièrement notre chemin, il suffit de savoir qu'il va vers le haut aux instants $0, 1, 3, 4, 5, 8, 13, 16, 17, 18, 19$.

Il suffit donc de savoir à quels instants, entre 0 et $n-1$ (ce qui fait n instants) il a été vers le haut. Notons n_h le nombre de fois où il est allé vers le haut, et n_b le nombre de fois où il est allé vers le bas. On a évidemment $n_h + n_b = n$ mais on a aussi $n_h - n_b = k$ puisqu'il se retrouve « à l'altitude k » : il a donc effectué k pas vers le haut de plus (ou de moins si $k < 0$) qu'il n'a fait de sauts vers le bas. Dès lors, $n_h = \dfrac{n+k}{2}$. On en déduit deux choses :

- Si $n + k$ est impair i.e. si n et k sont de parités différentes, alors le problème n'a pas de solution, il n'est pas possible d'aller du point $(0,0)$ au point (n,k).
- Si $n + k$ est pair, alors un tel chemin est entièrement déterminé par l'ensemble des instants où il est allé vers le haut. Il y en a $n_h = \dfrac{n+k}{2}$ si bien que le nombre de chemins recherché est

$$\binom{n}{\frac{n+k}{2}}$$

Essayez d'aller du point $(0,0)$ au point $(2,1)$!

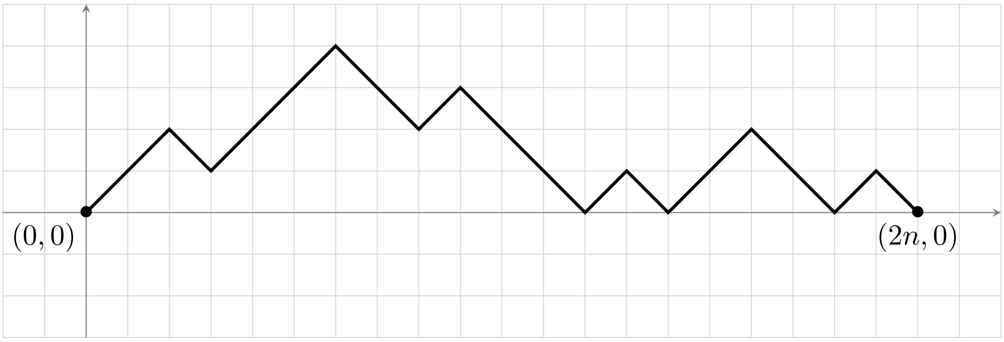
Remarque : On pourrait se dire qu'un chemin est tout aussi bien caractérisé par l'ensemble des instants où il va vers le bas. On trouve alors que le nombre de chemins est

$$\binom{n}{n_b} = \binom{n}{\frac{n-k}{2}}$$

ce qui est la même chose par symétrie des coefficients binomiaux puisque $n_b = n - n_h$. Ouf !

IV.3 Chemins de Dyck et valeur des nombres de Catalan

Si $n \geqslant 1$, on appelle chemin de Dick de longueur $2n$ un chemin de Bernoulli joignant les points de coordonnées $(0,0)$ et $(2n,0)$ « qui ne descend jamais sous l'horizon » c'est-à-dire qui ne prend que des ordonnées positives ou nulles.



Montrons que le nombre de chemins de Dick de longueur $2n$ est égal à C_n, le n-ième nombre de Catalan. Il suffit d'exhiber une bijection entre l'ensemble des parenthésages admissibles et l'ensemble des chemins de Dick. Il suffit de voir qu'un parenthésage est admissible si et seulement si, lorsqu'on le parcourt de la gauche vers la droite, il y a toujours au moins autant de parenthèses gauches que de parenthèses droites, et qu'il y a autant de parenthèses gauche que de parenthèses droites dans le parenthésage final.

Puisqu'un chemin est de Dick lorsqu'il ne descend jamais sous l'horizon, un chemin est de Dyck lorsqu'il y a toujours au moins autant de montées que de descentes, et qu'il y a autant de montées que de descentes dans le chemin final (puisqu'on arrive à une altitude nulle). Dès lors, la bijection est immédiate : on passe d'un bon parenthésage à un chemin de Dick en associant à une parenthèse gauche une montée, et à une parenthèse droite une descente.

La bijectivité est immédiate :

- si deux parenthésages ont la même image, i.e. le même chemin, alors ils sont égaux car ils ont des parenthèses gauches au même endroit (là où le chemin monte) et des parenthèses droites au même endroit (là où le chemin descend), d'où l'injectivité.
- tout chemin a un antécédent, le parenthésage avec des parenthèses gauches là où le chemin monte, et des parenthèses droites là où le chemin descend.

Par exemple, le parenthésage associé au chemin de Dyck ci-dessus est :

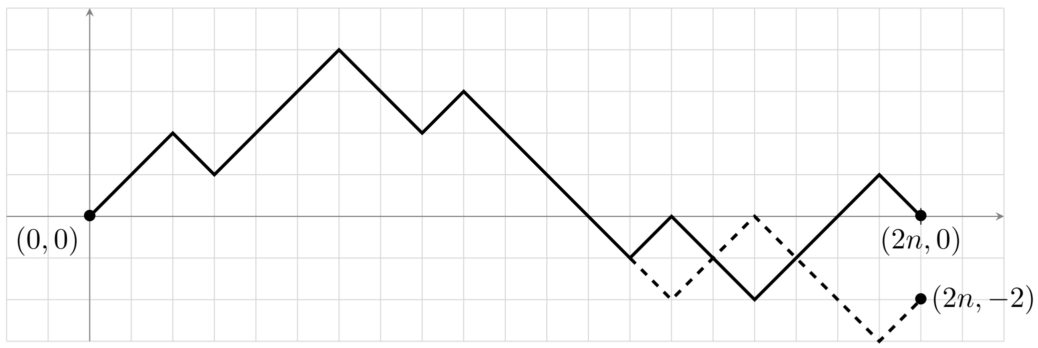
$$( ) ((( )) ( ))) ( ) (( )) ( )$$

Puisque deux ensembles en bijection ont le même cardinal, il en découle que l'ensemble des chemins de Dyck a le même cardinal que l'ensemble des parenthésages admissibles, donc que le nombre de chemins de Dyck est égal à C_n.

Donnons à présent la valeur exacte de C_n. Puisqu'on connaît le nombre de chemins reliant $(0,0)$ à $(2n,0)$ d'après le paragraphe précédent, il suffit de connaître le nombre de chemins qui ne sont pas des chemins de Dyck. Or, un chemin n'est pas un chemin de Dyck si et seulement s'il prend des valeurs négatives, si et seulement s'il atteint la valeur -1 (inutile d'invoquer le TVI ici, c'est assez évident comme cela, et on fait certains raisonnements « avec les mains » quand on fait de la combinatoire).

Dans ce paragraphe, sauf indication contraire, par exemple quand il reliera $(0,0)$ à $(2n,-2)$, un chemin sera un chemin reliant $(0,0)$ à $(2n,0)$.

À un tel chemin, on associe son chemin « miroir » à partir du moment où il atteint -1 c'est-à-dire le chemin qui descend quand il monte, et qui monte quand il descend, à partir du premier moment où il atteint -1.



Montrons que l'on construit ainsi une bijection de l'ensemble des chemins qui ne sont pas des chemins de Dyck vers l'ensemble des chemins reliant $(0, 0)$ à $(2n, -2)$:

- si deux chemins (qui ne sont pas des chemins de Dyck) ont la même image, alors ils sont égaux car ils coïncident avec le chemin reliant $(0, 0)$ à $(2n, -2)$ jusqu'au premier instant où il vaut -1, et font les mouvements contraires ensuite, donc ils sont bien égaux entre eux. D'où l'injectivité.
- tout chemin reliant $(0, 0)$ à $(2n, -2)$ a un antécédent, le chemin qui coïncide avec lui premier instant où il vaut -1, et qui fait tous les mouvements contraires ensuite (et qui va bien jusqu'en $(2n, 0)$). D'où la surjectivité.

Dessinez un chemin reliant $(0, 0)$ à $(2n, -2)$ et donnez son unique antécédent : vous verrez que vous n'avez pas le choix !

Il en découle qu'il y a autant de chemins qui ne sont pas des chemins de Dyck que de chemins joignant $(0, 0)$ à $(2n, -2)$. Or :

- un chemin joignant $(0, 0)$ à $(2n, 0)$ est entièrement déterminé par l'ensemble des instants où il va vers le haut, et il y en a n. Il y a donc $\binom{2n}{n}$ tels chemins, et il y a donc $\binom{2n}{n} - C_n$ chemins qui ne sont pas des chemins de Dyck.
- un chemin joignant $(0, 0)$ à $(2n, -2)$ est entièrement déterminé par l'ensemble des instants où il va vers le haut, et il y en a $n - 1$ (et $n + 1$ instants où il va vers le bas). Il y a donc $\binom{2n}{n-1} = \binom{2n}{n+1}$ tels chemins.

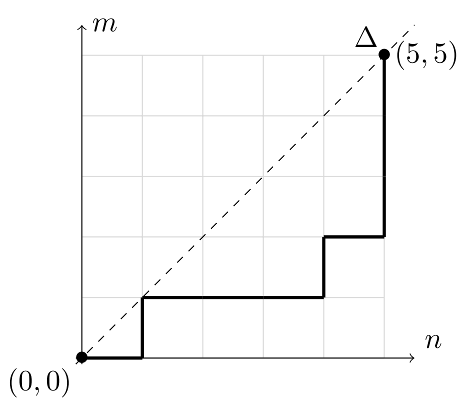
On refait le raisonnement du paragraphe précédent.

Ces deux nombres étant égaux d'après ce qui précède, on retrouve la valeur des nombres de Catalan vue dans l'exercice 31 du chapitre 3 et dans l'exercice 34 du chapitre 10 :

$$C_n = \binom{2n}{n} - \binom{2n}{n+1} = \frac{\binom{2n}{n}}{n+1}$$

IV.4 Chemins sous-diagonaux

On appelle chemin sous-diagonal de longueur $2n$ un chemin reliant $(0, 0)$ à (n, n) qui ne peut aller que vers la droite ou vers le haut en restant sous la diagonale, comme sur le dessin ci-dessous.



On met facilement en bijection un tel chemin avec un chemin de Dyck en faisant correspondre les déplacements vers la droite (pour les chemins sous-diagonaux) aux montées (pour les chemins de Dyck), et les déplacements vers le haut (pour les chemins sous-diagonaux) aux descentes (pour les chemins de Dyck). En effet, un chemin est sous-diagonal si et seulement si, en le parcourant, on a toujours plus de déplacements vers la droite que de montées, et si on a autant de l'un que de l'autre à la fin.

La bijectivité est immédiate : essayez de la prouver comme ci-dessus, ou essayez de trouver le chemin de Dyck associé au chemin sous-diagonal ci-dessus, vous verrez que vous n'avez pas beaucoup le choix !

Il y a donc autant de chemins sous-diagonaux que de chemins de Dyck : il y a donc C_n chemins sous-diagonaux de longueur $2n$.

Remarque : Les nombres de Catalan sont sans doute les nombres les plus importants en combinatoire. Ils comptent encore bon nombre d'objets : le nombre de façon de trianguler un polygone à n côtés, le nombre d'arbres binaires à n noeuds, le nombre de partitions de $[\![1\,;\,n]\!]$ non croisées...

V Démonstrations (HP)

Le but de cette partie est de tout définir et de tout démontrer correctement. En particulier, la notion même de cardinal n'est pas supposée connue. Nous n'utiliserons donc aucun des résultats de ce chapitre, même lorsqu'ils semblent particulièrement intuitifs.

V.1 Préliminaires

Lemme. Soit$p \geqslant 2$. Soit $c \in [\![1\,;\,p]\!]$. Alors il existe une bijection de $[\![1\,;\,p]\!]\backslash\{c\}$ dans $[\![1\,;\,p-1]\!]$.

Démonstration. L'application « tassement » $f : [\![1\,;\,p]\!]\backslash\{c\} \mapsto [\![1\,;\,p-1]\!]$ définie par :

$$f : x \mapsto \begin{cases} x & \text{si } x \leqslant c-1 \\ \\ x-1 & \text{si } x \geqslant c+1 \end{cases}$$

□

convient. En effet :

- soient $x_1 \neq x_2$ dans $[\![1\,;\,p]\!]\backslash\{c\}$. Si x_1 et x_2 sont tous les deux inférieurs ou égaux à $c-1$ alors $f(x_1) = x_1 \neq x_2 = f(x_2)$. De même si x_1 et x_2 sont tous les deux supérieurs ou égaux à $c+1$. Enfin, si $x_1 \leqslant c-1$ et $x_2 \geqslant c+1$ alors $f(x_1) = x_1 \leqslant c-1$ et $f(x_2) = x_2 - 1 \geqslant c$ donc $f(x_1) \neq f(x_1)$: f est injective.
- Soit $y \in [\![1\,;\,p-1]\!]$. Si $y \leqslant c-1$ alors $f(y) = y$ donc y est un antécédent de y. Si $y \geqslant c$ alors $y = f(y+1)$ donc $y+1$ est un antécédent de y. Dans tous les cas, y admet un antécédent par f : f est surjective.

Proposition. Soient n et p deux entiers naturels non nuls. S'il existe une injection de $[\![1\,;\,n]\!]$ dans $[\![1\,;\,p]\!]$ alors $n \leqslant p$.

La réciproque étant immédiate (prendre l'injection canonique, cf. chapitre 4), c'est donc une équivalence.

Démonstration. Raisonnons par récurrence sur n.

- Si $n \geqslant 1$, notons H_n : « Pour tout $p \geqslant 1$, s'il existe une injection de $[\![1\,;\,n]\!]$ dans $[\![1\,;\,p]\!]$ alors $n \leqslant p$ ».
- Il n'y a rien à prouver pour $n = 1$ puisqu'on prend $p \geqslant 1$: H_1 est vraie.
- Soit $n \geqslant 1$. Supposons H_n vraie et prouvons que H_{n+1} est vraie. Soit $p \geqslant 1$ et supposons qu'il existe une injection de $[\![1\,;\,n+1]\!]$ dans $[\![1\,;\,p]\!]$. Notons $c = f(n+1)$ et g la restriction de f à $[\![1\,;\,n]\!]$. g est encore injective de $[\![1\,;\,n]\!]$ dans $[\![1\,;\,p]\!]\backslash\{c\}$. Soit h une bijection de $[\![1\,;\,p]\!]\backslash\{c\}$ dans $[\![1\,;\,p-1]\!]$ (qui existe d'après le lemme précédent). Alors $h \circ g$ est une injection (car composée d'injections) de $[\![1\,;\,n]\!]$ dans $[\![1\,;\,p-1]\!]$. Par hypothèse de récurrence, $n \leqslant p-1$ donc $n+1 \leqslant p$: H_{n+1} est vraie.
- D'après le principe de récurrence, H_n est vraie pour tout $n \geqslant 1$.

On montre de même que s'il existe une surjection de $[\![1\,;\,n]\!]$ dans $[\![1\,;\,p]\!]$ alors $n \geqslant p$.

Corollaire. Soit $(n,p) \in \mathbb{N}^2$. S'il existe une bijection entre $\llbracket 1\,;\, n \rrbracket$ et $\llbracket 1\,;\, p \rrbracket$ alors $n = p$.

Là aussi, en prenant l'identité, la réciproque est immédiate.

Démonstration. L'image d'un ensemble non vide étant non vide, il n'existe pas de bijection entre un ensemble vide et un ensemble non vide. Dès lors, s'il existe une bijection entre $\llbracket 1\,;\, n \rrbracket$ et $\llbracket 1\,;\, p \rrbracket$ avec $n = 0$ ou $p = 0$, l'autre est obligatoirement nul donc $n = p = 0$. Supposons à présent qu'il existe une bijection f entre $\llbracket 1\,;\, n \rrbracket$ et $\llbracket 1\,;\, p \rrbracket$ avec n et p non nuls. Alors f est injective donc, d'après ce qui précède, $n \leqslant p$, et f^{-1} est une injection de $\llbracket 1\,;\, p \rrbracket$ dans $\llbracket 1\,;\, n \rrbracket$ donc $p \leqslant n$ ce qui permet de conclure.

Proposition. Soit $n \in \mathbb{N}^*$. Alors une injection de $\llbracket 1\,;\, n \rrbracket$ dans lui-même est une bijection.

Démonstration. Là aussi, raisonnons par récurrence.

- Si $n \geqslant 1$, notons H_n : « une injection de $\llbracket 1\,;\, n \rrbracket$ dans lui-même est une bijection ».
- La seule application de $\{1\}$ dans lui-même est l'identité qui est injective et bijective donc H_1 est vraie.
- Soit $n \geqslant 1$. Supposons H_n vraie et prouvons que H_{n+1} est vraie. Soit $f : \llbracket 1\,;\, n+1 \rrbracket \to \llbracket 1\,;\, n+1 \rrbracket$ injective. Notons $c = f(n+1)$ et g la restriction de f à $\llbracket 1\,;\, n \rrbracket$. g est encore injective de $\llbracket 1\,;\, n \rrbracket$ dans $\llbracket 1\,;\, n+1 \rrbracket \backslash \{c\}$. Soit h une bijection de $\llbracket 1\,;\, n+1 \rrbracket \backslash \{c\}$ dans $\llbracket 1\,;\, n \rrbracket$ (qui existe d'après le lemme ci-dessus avec $p = n+1$). Alors $h \circ g$ est une injection (car composée d'injections) de $\llbracket 1\,;\, n \rrbracket$ dans $\llbracket 1\,;\, n \rrbracket$. Par hypothèse de récurrence, $h \circ g$ est bijective. En composant par h^{-1} qui est une bijection de $\llbracket 1\,;\, n \rrbracket$ dans $\llbracket 1\,;\, n+1 \rrbracket \backslash \{c\}$, par composition, $g = h^{-1} \circ (h \circ g)$ est une bijection de $\llbracket 1\,;\, n \rrbracket$ dans $\llbracket 1\,;\, n+1 \rrbracket \backslash \{c\}$ donc est surjective : pour tout $y \in \llbracket 1\,;\, n+1 \rrbracket \backslash \{c\}$, il existe $x \in \llbracket 1\,;\, n \rrbracket$ tel que $y = g(x) = f(x)$ puisque g est la restriction de f à $\llbracket 1\,;\, n \rrbracket$. En d'autres termes, tout élément de $\llbracket 1\,;\, n+1 \rrbracket \backslash \{c\}$ admet un antécédent par f, et puisque $c = f(n+1)$, c a aussi un antécédent par f : f est surjective donc bijective, c'est-à-dire que H_{n+1} est vraie.
- D'après le principe de récurrence, H_n est vraie pour tout $n \geqslant 1$.

V.2 Ensembles finis et cardinal

Définition. Soit E un ensemble. On dit qu'il est fini s'il existe $n \in \mathbb{N}$ tel que E soit en bijection avec $\llbracket 1\,;\, n \rrbracket$. Si ce n'est pas le cas, E est dit infini.

Remarques :

- Le vide est fini car il est en bijection avec lui-même.
- La relation « être en bijection avec » est une relation d'équivalence (cf. chapitre 16).

Proposition/Définition. Soit E un ensemble fini. L'entier n tel que E soit en bijection avec $\llbracket 1\,;\, n \rrbracket$ est unique et est appelé cardinal de E. On le note $\text{card}(E)$, $|E|$ ou $\#E$.

En particulier, le vide est de cardinal 0.

Démonstration. Soient n et p tels que E soit en bijection avec $\llbracket 1\,;\, n \rrbracket$ et $\llbracket 1\,;\, p \rrbracket$. Par transitivité (c'est une relation d'équivalence), $\llbracket 1\,;\, n \rrbracket$ et $\llbracket 1\,;\, p \rrbracket$ sont en bijection donc $n = p$ d'après le paragraphe précédent.

V.3 Parties de $\mathbb{N}$

Théorème. Une partie non vide de $\mathbb{N}$ est finie si et seulement si elle est majorée.

Démonstration. Montrons par récurrence que toute partie de $\mathbb{N}$ de cardinal n est majorée.

- Si $n \geqslant 1$, notons H_n : « toute partie de $\mathbb{N}$ de cardinal n est majorée ».
- Soit A une partie de $\mathbb{N}$ de cardinal 1 i.e. A est en bijection avec $\{1\}$. Soit $f : A \to \{1\}$ une bijection. Alors f^{-1} est une bijection de $\{1\}$ dans A c'est-à-dire que $A = \{f^{-1}(1)\}$: A est bien majorée, H_1 est vraie.
- Soit $n \geqslant 1$. Supposons H_n vraie et prouvons que H_{n+1} est vraie. Soit donc A une partie de $\mathbb{N}$ de cardinal $n+1$: soit $f : A \to [\![1\,;n+1]\!]$ une bijection, si bien que $A = \{f^{-1}(1); \dots ; f^{-1}(n+1)\}$. $B = \{f^{-1}(1); \dots ; f^{-1}(n)\}$ est de cardinal n donc, par hypothèse, B est majorée : soit M un majorant de B. Alors $\max(M, f^{-1}(n+1)\}$ est un majorant de A : A est majorée, H_{n+1} est vraie.
- D'après le principe de récurrence, H_n est vraie pour tout $n \geqslant 1$.

Finalement, toute partie finie de $\mathbb{N}$ est majorée. Montrons la réciproque, c'est-à-dire que toute partie majorée de $\mathbb{N}$ est finie. Puisqu'une partie majorée de $\mathbb{N}$ admet un plus grand élément, il suffit de prouver par récurrence que, pour tout p, toute partie de plus grand élément p est finie. Là aussi, raisonnons par récurrence.

- Si $p \geqslant 1$, notons H_p : « toute partie non vide de $\mathbb{N}$ de plus grand élément p est finie ».
- Si A est de plus grand élément 0 alors $A = \{0\}$ qui est finie car en bijection avec $[\![1\,; n]\!] = \{1\}$: H_0 est vraie.
- Soit $p \geqslant 0$. Supposons $H_0, \dots, H_p$ vraies (récurrence forte) et prouvons que H_{p+1} est vraie. Soit donc A une partie non vide de $\mathbb{N}$ de plus grand élément $p+1$. Soit $B = A \backslash \{p+1\}$. Si B est vide alors $A = \{p+1\}$ donc est fini car en bijection avec $\{1\}$. Si B est non vide alors B admet un plus grand élément inférieur ou égal à p : par hypothèse de récurrence, B est fini i.e. il existe n et f tel que f soit une bijection de B dans $\mathbb{N}$. On pose $f(p+1) = n+1$. Il est alors facile de prouver que f est une bijection de A dans $[\![1\,; n+1]\!]$ ce qui clôt la récurrence.

Corollaire. Toute partie B d'une partie finie A de $\mathbb{N}$ est finie.

Démonstration. $B \subset A$ et A est finie donc majorée donc B est majorée donc finie.

Corollaire. Une intersection de parties finies de $\mathbb{N}$ est une partie finie de $\mathbb{N}$.

Corollaire. L'union de deux parties finies de $\mathbb{N}$ est une partie finie de $\mathbb{N}$.

Démonstration. Si A et B sont deux parties finies de $\mathbb{N}$, alors elles sont majorées, disons par a et b. Alors $A \cup B$ est majorée par $\max(a, b)$ donc est finie.

Corollaire. Le complémentaire d'une partie finie de $\mathbb{N}$ est infini.

Démonstration. Soit A une partie finie de $\mathbb{N}$. Si $\overline{A}$ est fini, alors $N = A \cup \overline{A}$ est fini car union de deux parties finies de $\mathbb{N}$ ce qui est absurde car $\mathbb{N}$ est infini car non majoré.

V.4 Retour aux ensembles finis

Théorème. Soit E un ensemble fini et soit A une partie de E. Alors A est un ensemble fini, et $\text{card}(A) \leqslant \text{card}(E)$, avec égalité si et seulement si $A = E$.

Démonstration. Si A est vide, alors A est finie. Supposons A non vide. Notons $n = \text{card}(E)$ et $g : E \to [\![1\,;\, n]\!]$ une bijection. Alors la restriction de g à A est injective et est une surjection sur $g(A)$ qui est une partie de $[\![1\,;\, n]\!]$ donc qui est un ensemble fini (voir le premier corollaire ci-dessus). On en déduit que g est une bijection de A sur $g(A)$ et qu'il existe p tel que $g(A)$ soit en bijection avec $[\![1\,;\, p]\!]$. Par transitivité, A est en bijection avec $[\![1\,;\, p]\!]$ donc A est finie (et de cardinal p).

Puisque A est incluse dans E, il existe une injection de A dans E (l'injection canonique $x \mapsto x$ que l'on note i). Il existe également une bijection h de $[\![1\,;\, p]\!]$ dans A et rappelons qu'il existe une bijection g de E dans $[\![1\,;\, n]\!]$ si bien qu'on a la succession d'applications injectives suivantes :

$$[\![1\,;\, p]\!] \xrightarrow{h} A \xrightarrow{i} E \xrightarrow{g} [\![1\,;\, n]\!]$$ □

Par composition, $g \circ i \circ h$ est une injection de $[\![1\,;\, p]\!]$ dans $[\![1\,;\, n]\!]$ donc $p \leqslant n$ si bien que $\text{card}(A) \leqslant \text{card}(E)$. Si $\text{card}(A) = \text{card}(E)$ alors $p = n$ donc $g \circ i \circ h$ est une injection de $[\![1\,;\, n]\!]$ dans lui-même donc est une bijection. En composant à gauche par h^{-1} et à droite par g^{-1}, $i = h^{-1} \circ (h \circ i \circ g) \circ g^{-1}$ est une bijection car composée de bijections. En particulier, $i(A) = E$. Or, $i(A) = A$ donc $A = E$. La réciproque est immédiate.

Théorème. Soient E et F deux ensembles finis.

- Il existe une application $f : E \to F$ injective si et seulement si $\text{card}(E) \leqslant \text{card}(F)$.
- Il existe une application $f : E \to F$ surjective si et seulement si $\text{card}(E) \geqslant \text{card}(F)$.
- Il existe une application $f : E \to F$ bijective si et seulement si $\text{card}(E) = \text{card}(F)$.

Démonstration. Notons $n = \text{card}(E)$ et $p = \text{card}(F)$. Soient $f : E \to [\![1\,;\, n]\!]$ et $g : F \to [\![1\,;\, p]\!]$ bijectives. Supposons que $\text{card}(E) \leqslant \text{card}(F)$. Alors l'injection canonique $i : [\![1\,;\, n]\!] \mapsto [\![1\,;\, p]\!]$ est injective, et $g^{-1} \circ i \circ f$ est une injection (car composée d'injections) de E dans F. Réciproquement, supposons qu'il existe une injection φ de E dans F. Alors $g \circ \varphi \circ f^{-1}$ est une injection de $[\![1\,;\, n]\!]$ dans $[\![1\,;\, p]\!]$ donc $n \leqslant p$ i.e. $\text{card}(E) \leqslant \text{card}(F)$. Les deux autres équivalences se prouvent de façon analogue.

Théorème. Soient A et B deux ensembles finis disjoints. Alors $A \cup B$ est fini et $\text{card}(A \cup B) = \text{card}(A) + \text{card}(B)$.

On généralise à une union finie quelconque par récurrence.

Démonstration. Notons $n = \text{card}(A)$ et $p = \text{card}(B)$. Tout d'abord, $[\![n+1\,;\, n+p]\!]$ est fini de cardinal p (la fonction $x \mapsto x - n$ est une bijection entre cet ensemble et $[\![1\,;\, p]\!]$) donc $\text{card}(B) = \text{card}([\![n+1\,;\, n+p]\!])$: il existe donc une bijection g entre ces ensembles, ainsi qu'une bijection entre A et $[\![1\,;\, n]\!]$. Soit h la fonction définie sur $A \cup B$ par :

$$h : x \mapsto \begin{cases} f(x) & \text{si } x \in A \\ \\ g(x) & \text{si } x \in B \end{cases}$$ □

Tout d'abord, h est bien définie car A et B sont disjoints : il n'y a pas de problème de définition. De plus, f étant à valeurs dans $[\![1\,;\, n]\!]$ et g dans $[\![n+1\,;\, n+p]\!]$, h est à valeurs dans $[\![1\,;\, n+p]\!]$. On montre aisément que h est une bijection entre $A \cup B$ et $[\![1\,;\, n+p]\!]$ (exo) ce qui permet de conclure : $A \cup B$ est fini de cardinal $n + p = \text{card}(A) + \text{card}(B)$.

Théorème. Soient E et F deux ensembles finis. Alors $E \times F$ est fini et $\text{card}(E \times F) = \text{card}(E) \times \text{card}(F)$.

Démonstration. Notons $E = \{x_1; \dots; x_n\}$ (c'est-à-dire que E est de cardinal n). Pour tout $i \in [\![1\,;\, n]\!]$, la fonction

$$f_i : \left\{ \begin{array}{ccc} \{x_i\} \times F & \to & F \\ & & \\ (x_i, y) & \mapsto & y \end{array} \right.$$

est une bijection (exo) donc $\text{card}(\{x_i\} \times F) = \text{card}(F)$. Finalement, $E \times F$ est l'union disjointe des $\{x_i\} \times F$ donc

$$\begin{aligned} \text{card}(E \times F) &= \sum_{i=1}^{n} \text{card}(\{x_i\} \times F) \\ &= \sum_{i=1}^{n} \text{card}(F) \\ &= n\,\text{card}(F) \\ &= \text{card}(E) \times \text{card}(F) \end{aligned} \qquad \square$$

Théorème. Soient E et F deux ensembles **finis de même cardinal** et soit $f : E \to F$. Alors :

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

Démonstration. Supposons f injective. Alors f est une bijection de E sur $f(E)$ (une injection est une bijection sur son image) donc $\text{card}(f(E)) = \text{card}(E)$. Si f n'est pas surjective, alors il existe $a \in F \backslash f(E)$ donc $f(E) \cup \{a\} \subset F$ et c'est une union disjointe si bien que

$$\text{card}(F) \geqslant \text{card}(f(E) \cup \{a\}) = \text{card}(f(E)) + 1 = \text{card}(E) + 1 \qquad \square$$

ce qui est absurde. On en déduit que f est surjective. Réciproquement, supposons f surjective. Si f n'est pas injective, alors il existe $x_1 \neq x_2$ tel que $f(x_1) = f(x_2)$. Dès lors, $F = f(E) = f(E \backslash \{x_1\})$ si bien que f est une surjection de $E \backslash \{x_1\}$ dans F donc $\text{card}(F) \leqslant \text{card}(E \backslash \{x_1\}) = \text{card}(E) - 1$ ce qui est absurde.