

# Entiers naturels - dénombrement

## Table des matières

|   |          |
|---|----------|
| <b>1 Généralités, principe de récurrence</b>  | <b>2</b> |
| 1.1 L'ensemble $\mathbb{N}$   | 2        |
| 1.2 Principe de récurrence  | 2        |
| 1.3 Suites définies par récurrence  | 3        |
| 1.4 Symboles $\sum$ et $\prod$  | 3        |
| 1.5 Division euclidienne  | 4        |
| <b>2 Cardinal d'un ensemble fini</b>  | <b>4</b> |
| 2.1 Ensembles finis   | 4        |
| 2.2 Injections et surjections de $\llbracket 1, p \rrbracket$ dans $\llbracket 1, q \rrbracket$ | 4        |
| 2.3 Définition du cardinal d'un ensemble fini   | 5        |
| 2.4 Quelques propriétés élémentaires  | 5        |
| <b>3 Dénombrement</b>   | <b>6</b> |
| 3.1 Cardinal d'une réunion  | 6        |
| 3.2 Cardinal d'un produit cartésien   | 6        |
| 3.3 Quelques cardinaux remarquables   | 6        |
| 3.4 Coefficients binomiaux  | 8        |

# 1 Généralités, principe de récurrence

## 1.1 L'ensemble $\mathbb{N}$

On admet l'existence d'un ensemble, noté  $\mathbb{N}$ , dont les éléments sont les entiers naturels "que l'on connaît depuis longtemps". Cet ensemble est muni d'une loi d'ordre total<sup>1</sup>  $\leq$  telle que :

- $\mathbb{N}$  contient un plus petit élément, noté 0 ;
- toute partie non vide de  $\mathbb{N}$  majorée admet un plus grand élément ;
- toute partie non vide de  $\mathbb{N}$  minorée admet un plus petit élément.

$\mathbb{N}$  est par ailleurs muni de deux lois de composition interne  $+$  et  $\cdot$  "qui ont les propriétés que l'on sait".

## 1.2 Principe de récurrence

**THÉORÈME 1** Principe de récurrence

Soit  $P$  une proposition dépendant de  $n \in \mathbb{N}$ . On suppose :

- $P(0)$  est vérifiée ;
- pour tout  $n \in \mathbb{N}$ ,  $P(n)$  implique  $P(n+1)$  (on dit alors que "la propriété est héréditaire").

Alors  $P(n)$  est vérifiée pour tout entier  $n \in \mathbb{N}$ .

**PREUVE :** On considère l'ensemble  $A$  des entiers  $n$  tels que  $P(n)$  n'est pas vérifié. On veut montrer que  $A = \emptyset$ . Par l'absurde, on va supposer que  $A \neq \emptyset$ .  $A$  possède alors un plus petit élément  $n_0$ . Puisque  $P(0)$  est vérifié,  $n_0 \neq 0$ . Mais alors,  $n_0 - 1$  est un entier qui n'est pas dans  $A$ , donc  $P(n_0 - 1)$  est vérifiée, et comme la propriété est héréditaire,  $P(n_0)$  est vérifiée également : contradiction avec la définition de  $n_0$ . ■

**REMARQUES 1**

- On peut survivre (taupinalement s'entend) sans connaître la démonstration précédente, mais il est par contre essentiel de bien comprendre les hypothèses de ce principe d'induction.
- Pour vérifier la deuxième hypothèse du principe d'induction, il faut fixer  $n$ , et montrer  $P(n) \Rightarrow P(n+1)$ , ce qui ne veut pas dire montrer  $P(n)$ , ou bien montrer  $P(n+1)$ , mais montrer que si  $P(n)$  est vrai, alors  $P(n+1)$  également. En pratique, on fixe donc  $n \in \mathbb{N}$  tel que  $P(n)$  est vérifié, et on montre  $P(n+1)$ . On rappelle que lorsqu'on a montré  $A \Rightarrow B$ , on ne sait toujours pas si  $A$  est vrai, pas plus que  $B$ .
- Supposer  $P(n)$  vrai pour tout  $n$  (ce qui arrive en général implicitement si on ne fixe pas  $n$ ) revient tout simplement à supposer ce que l'on veut montrer... On ne verra donc JAMAIS : "supposons  $P(n)$  vérifiée pour tout  $n$ , et montrons  $P(n+1)$ "...
- Selon le contexte, on pourra adapter l'énoncé (et sa démonstration) au cas d'une proposition définie seulement pour  $n \geq n_0$ , ou bien  $n \in \llbracket n_1, n_2 \rrbracket$ . Dans ces cas là, on fera TRES attention lors de l'initialisation comme lors de l'hérédité à bien préciser les valeurs de  $n$ ...

**EXERCICE 1** Montrer que pour tout  $n \in \mathbb{N}$ ,  $10^n - 1$  est divisible par 9.

On commencera par donner un sens précis à "est divisible par".

On a parfois besoin, pour montrer  $P(n+1)$ , de supposer  $P(k)$  vérifiée pour tout  $k \in \llbracket 0, n \rrbracket$ , et non simplement  $P(n)$ . Dans ce cas, on peut encore "raisonner par récurrence", grâce au résultat suivant, plus fort (en apparence) que le précédent, puisque les hypothèses à vérifier sont plus faibles, si on y réfléchit bien (et calmement) :

**THÉORÈME 2** Principe de récurrence avec prédécesseurs

Soit  $P$  une proposition dépendant de  $n \in \mathbb{N}$ . On suppose :

- $P(0)$  est vérifiée ;
- pour tout  $n \in \mathbb{N}$ ,  $(P(0) \text{ et } P(1) \text{ et } P(2) \dots \text{ et } P(n))$  implique  $P(n+1)$ .

Alors  $P(n)$  est vérifiée pour tout entier  $n \in \mathbb{N}$ .

<sup>1</sup>Rappel : une relation binaire  $R$  est un *ordre* lorsqu'elle est réflexive ( $xRx$  pour tout  $x$ ), antisymétrique (si  $xRy$  et  $yRx$ , alors  $x=y$ ), et transitive (si  $xRy$  et  $yRz$ , alors  $xRz$ ). Lorsque pour tout  $x, y$  on a  $xRy$  ou  $yRx$ , on dit que l'ordre est *total*.

PREUVE : On peut raisonner comme dans la preuve du principe de récurrence “de base”, ou bien appliquer ce principe de récurrence à la proposition  $Q(n)$  : “ $P(0)$  et  $P(1)$  et ... et  $P(n-1)$  et  $P(n)$ ”. ■

EXERCICE 2 Montrer que tout entier  $n \in \mathbb{N}$  peut s'écrire comme le produit d'entiers premiers. On rappelle que  $p \in \mathbb{N}$  est dit premier s'il n'est pas divisible par un entier naturel autre que 1 et lui-même.

### 1.3 Suites définies par récurrence

Si  $f$  est une application de  $E$  dans  $E$  ( $E \subset \mathbb{C}$ ) et  $x \in E$ , on admettra qu'il existe une unique suite réelle  $u$  telle que  $u_0 = x$  et  $u_{n+1} = f(u_n)$  pour tout  $n \in \mathbb{N}$ .

S'il convient de justifier une définition de la forme  $u_0 \in [0, 1]$  et  $u_{n+1} = \sqrt{1 - u_n}$ , on peut appliquer le résultat précédent à l'application  $f : [0, 1] \rightarrow [0, 1]$ ,  $t \mapsto \sqrt{1 - t}$ . Si  $f$  est une application définie seulement sur une partie  $E$  de  $\mathbb{R}$  (ex :  $u_{n+1} = 10 + \ln u_n$ ), il convient de trouver une partie  $F$  de  $E$  qui contient  $u_0$  et qui est  $f$ -stable. On peut alors justifier l'existence et la localisation des  $u_n$ .

Si  $g$  est cette fois une application de  $E \times \mathbb{N}$  dans  $E$  et  $x \in E$ , il existe également une unique suite telle que  $u_0 = x$  et  $u_{n+1} = f(u_n, n)$  pour tout  $n \in \mathbb{N}$ .

EXEMPLE 1 Soit  $f : \mathbb{R} \times \mathbb{N} \rightarrow \mathbb{R}$ ,  $(x, n) \mapsto (n+1)x$  et  $u_n$  l'unique suite telle que  $u_0 = 1$  et  $u_{n+1} = f(u_n, n)$  pour tout  $n \in \mathbb{N}$ .  $u_n$  est par définition  $n!$

### 1.4 Symboles $\sum$ et $\prod$

#### DÉFINITION 1

Si  $(a_i)_{1 \leq i \leq n}$  est une famille de réels (ou de complexes), on définit  $\sigma_n = \sum_{i=1}^n a_i$  (resp.  $\pi_n = \prod_{i=1}^n a_i$ ) par :  $\sigma_0 = 0$  (resp.  $\pi_0 = 1$ ), et  $\sigma_{k+1} = \sigma_k + a_{k+1}$  (resp.  $\pi_{k+1} = a_{k+1}\pi_k$ ) pour tout  $k \in \llbracket 0, n-1 \rrbracket$ .

#### REMARQUES 2

- Il sera bien utile d'écrire  $a_1 + \dots + a_n$  et  $a_1 a_2 \dots a_n$  à la place de  $\sum a_k$  et  $\prod a_k$ . Cela permet de voir de quoi on parle...
- Dans la notation  $\sum_{i=1}^n a_i$ , on peut remplacer  $i$  par  $j$  voire *toto* : on dit que  $i$  est une *variable muette*.
- Il est essentiel de comprendre pourquoi on a :

$$\sum_{k=1}^n a_k = \sum_{k=0}^{n-1} a_{k+1} = \sum_{k=2}^{n+1} a_{k-1} = \sum_{k=0}^{n-1} a_{n-k}.$$

Tout “théorème” concernant les changements d'indice est du verbiage. Par contre, il est essentiel de savoir pratiquer ces changements d'indice.

- D'après sa définition, on a  $n! = \prod_{i=1}^n i$ .
- Bien entendu (et heureusement!), on a :

$$\sum_{i=1}^n (\lambda a_i + b_i) = \lambda \sum_{i=1}^n a_i + \sum_{i=1}^n b_i.$$

EXERCICE 3 Soient  $n \in \mathbb{N}$ ,  $r \in \mathbb{R}$  et  $q \in \mathbb{R} \setminus \{1\}$ . Montrer :

$$\sum_{k=1}^n k = \frac{n(n+1)}{2} \quad \text{et} \quad \sum_{k=0}^n q^k = \frac{q^{n+1} - 1}{q - 1}.$$

**REMARQUE 3** On retient les formules précédentes comme on veut... mais on les retient, *et sans erreurs...* On a le droit de retenir des formules plus compliquées (de  $n_1$  à  $n_2...$ ) tant que les formules de base sont connues. Un moyen efficace peut être de savoir refaire la démonstration instantanément.

**EXERCICE 4** Montrer à nouveau (et différemment que dans l'exercice 2) que si  $n \in \mathbb{N}$ , alors  $10^n - 1$  est divisible par 9.

## 1.5 Division euclidienne

**THÉORÈME 3** Soient  $a \in \mathbb{N}$  et  $b \in \mathbb{N}^*$ . Il existe un unique couple d'entiers  $(q, r)$  tels que  $a = bq + r$  et  $0 \leq r < b$ .  $q$  (resp.  $r$ ) s'appelle le quotient (resp. reste) dans la division euclidienne de  $a$  par  $b$

**PREUVE :** On pourra raisonner par récurrence sur  $a$  (énoncer soigneusement (c'est-à-dire en quantifiant et en précisant ce qui est fixé...) la proposition), ou bien considérer l'ensemble des  $x \in \mathbb{N}$  tels que  $xb \leq a$ . ■

**EXERCICE 5** Effectuer à la main la division euclidienne de 1515 par 16.  
Refaire la même chose à la calculatrice en justifiant la méthode.

## 2 Cardinal d'un ensemble fini

Les résultats de cette partie doivent être connus, bien que leurs preuves ne soit pas exigibles (des indications sont données ici, mais à titre informatif).

### 2.1 Ensembles finis

#### DÉFINITION 2

Un ensemble  $E$  sera dit fini s'il existe une bijection entre  $E$  et  $\llbracket 1, n \rrbracket$ , pour un certain  $n \in \mathbb{N}$ .

**REMARQUE 4** Si  $E$  est un ensemble fini de cardinal  $n$ , alors en notant  $x_i = \varphi(i)$ , où  $\varphi$  est une bijection de  $\llbracket 1, n \rrbracket$  sur  $E$ , les  $x_i$  sont distincts, et on peut écrire  $E = \{x_1, \dots, x_n\}$ .

**EXERCICE 6** Montrer que l'ensemble des élèves de 843 est fini.

Il y a-t-il unicité de la bijection ? et de  $n$  tel que cet ensemble est en bijection avec  $\llbracket 1, n \rrbracket$  ?

Avec les notations de la définition 2, il est trop tôt pour déclarer  $n$  comme le cardinal de  $E$  : il faut d'abord établir l'unicité d'un tel  $n$ . Quel serait en effet le cardinal d'un ensemble en bijection avec  $\llbracket 1, 1515 \rrbracket$  et  $\llbracket 1, 1789 \rrbracket$  ?

### 2.2 Injections et surjections de $\llbracket 1, p \rrbracket$ dans $\llbracket 1, q \rrbracket$

**PROPOSITION 1** S'il existe une injection de  $\llbracket 1, p \rrbracket$  dans  $\llbracket 1, q \rrbracket$ , alors  $p \leq q$ .

**PREUVE :** Raisonner par récurrence (soignée) sur  $p$ . Si  $\varphi$  est une injection de  $\llbracket 1, p+1 \rrbracket$  dans  $\llbracket 1, q \rrbracket$ , on pourra commencer par traiter le cas où  $\varphi(p+1) = q$ . ■

**COROLLAIRE 1** S'il existe une surjection de  $\llbracket 1, p \rrbracket$  dans  $\llbracket 1, q \rrbracket$ , alors  $p \geq q$ .

**PREUVE :** Si on dispose d'une surjection de  $E$  sur  $F$ , on peut construire une injection de  $F$  dans  $E$ ... ■

**COROLLAIRE 2** S'il existe une bijection de  $\llbracket 1, p \rrbracket$  dans  $\llbracket 1, q \rrbracket$ , alors  $p = q$ .

**COROLLAIRE 3** Si  $E$  est en bijection avec  $\llbracket 1, p \rrbracket$  et  $\llbracket 1, q \rrbracket$ , alors  $p = q$ .

**PREUVE :** On construit une bijection de  $\llbracket 1, p \rrbracket$  sur  $\llbracket 1, q \rrbracket$  : il suffit de prendre  $\varphi = \varphi_2 \circ \varphi_1^{-1}$ , où  $\varphi_1$  et  $\varphi_2$  sont des bijections de  $E$  sur  $\llbracket 1, p \rrbracket$  et  $\llbracket 1, q \rrbracket$ . ■

## 2.3 Définition du cardinal d'un ensemble fini

### DÉFINITION 3

Soit  $E$  un ensemble fini. Grâce à la définition et aux résultats précédents, il existe un unique  $N \in \mathbb{N}$  tel que  $E$  soit en bijection avec  $\llbracket 1, N \rrbracket$ . Cet entier s'appelle le cardinal de  $E$ . On le note  $|E|$ , ou  $\text{card } E$ , voire encore  $\#E$ .

**EXERCICE 7** Soient  $E$  et  $F$  deux ensembles finis. Montrer qu'il existe une injection (resp. surjection, bijection) de  $E$  vers  $F$  si et seulement si  $|E| \leq |F|$  (resp.  $|E| \geq |F|$ ,  $|E| = |F|$ ). On pourra s'inspirer du diagramme suivant, où  $\varphi_1$  (resp.  $\varphi_2$ ) est une bijection de  $E$  (resp.  $F$ ) sur  $\llbracket 1, N_1 \rrbracket$  (resp.  $\llbracket 1, N_2 \rrbracket$ ) :

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ \varphi_1 \downarrow & & \downarrow \varphi_2 \\ \llbracket 1, N_1 \rrbracket & \xrightarrow[\varphi_2 \circ f \circ \varphi_1^{-1}]{} & \llbracket 1, N_2 \rrbracket \end{array}$$

## 2.4 Quelques propriétés élémentaires

### PROPOSITION 2

- Si  $E_1$  et  $E_2$  sont deux ensembles finis **disjoints**, alors leur réunion est finie, de cardinal  $|E_1| + |E_2|$ .
- Si  $F$  est fini et  $E \subset F$ , alors  $E$  est fini de cardinal  $\leq |F|$ , avec égalité si et seulement si  $E = F$ .

**PREUVE** : Le point délicat est ici de montrer que si  $F$  est fini et  $E \subset F$ , alors  $E$  est fini. On pourra le faire par récurrence sur  $|F|$ . Très franchement, ça n'est ni exaltant, ni essentiel, ni même vraiment formateur : on pourra passer sans état d'âme à la suite. . . ■

Le résultat suivant aura un analogue très important dans le chapitre sur les espaces vectoriels de dimension finie.

**THÉORÈME 4** Soient  $E$  et  $F$  deux ensembles finis de même cardinal (c'est en particulier le cas si  $E = F$ ) et  $f$  une application de  $E$  dans  $F$ . Alors les trois propositions suivantes sont équivalentes :

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

**PREUVE** : Pour l'implication (2)  $\Rightarrow$  (1), on pourra établir la contraposée après avoir montré le :

**LEMME 1** Si  $A$  est fini et  $f : A \rightarrow B$ , alors  $f(A)$  est fini et  $|f(A)| \leq |A|$  (récurrence sur  $|A|$ ).

On montrera ensuite (1)  $\Rightarrow$  (2) grâce au résultat suivant :

**LEMME 2** Si  $A$  est fini et  $f : A \rightarrow B$  est injective, alors  $|f(A)| = |A|$  (récurrence sur  $|A|$ ).

Les détails sont pour le lecteur. . . ■

**REMARQUE 5**  $n \mapsto n + 1$  établit une injection non surjective de  $\mathbb{N}$  dans lui-même, alors que  $n \mapsto \text{Max}(n - 1, 0)$  établit une surjection non injective de  $\mathbb{N}$  dans lui-même.

### 3 Dénombrement

#### 3.1 Cardinal d'une réunion

PROPOSITION 3 Soient  $E$  et  $F$  deux ensembles finis. Alors  $E \cup F$  et  $E \cap F$  sont finis, avec de plus :

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

PREUVE : Faire un dessin et se ramener à des réunions d'ensembles disjoints. ■

EXERCICE 8 Soient  $E, F, G$  trois ensembles finis. Montrer :

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

On verra dans la feuille d'exercices une formule exprimant le cardinal d'une réunion de  $N$  ensembles à partir du cardinal des différentes intersections. . .

#### 3.2 Cardinal d'un produit cartésien

PROPOSITION 4 Soient  $E$  et  $F$  deux ensembles finis. Alors  $E \times F$  est fini, de cardinal  $|E| |F|$ .

PREUVE : Récurrence sur  $|E|$ , par exemple. . . ■

#### 3.3 Quelques cardinaux remarquables

EXERCICE 9 Un pâtre Corse<sup>2</sup> compte le nombre de pattes des ses moutons. Il en trouve 24. Combien a-t-il de moutons ?

Le résultat suivant "généralise" (!) la technique de l'exercice précédent : quand on veut prouver un peu mieux qu'avec les mains les résultats usuels concernant les cardinaux, c'est un lemme utile. Ici, il n'est donné qu'à titre culturel.

PROPOSITION 5 Lemme des bergers

- Soit  $E$  un ensemble tel qu'il existe une partition<sup>3</sup> de  $E$  par  $N$  ensembles finis de cardinal commun  $k$ . Alors  $E$  est fini de cardinal  $Nk$ .
- Soit  $E$  un ensemble tel qu'il existe  $k \in \mathbb{N}^*$  et une application  $f : E \rightarrow F$ , avec  $F$  fini, de sorte que tout  $y \in F$  admet exactement  $k$  antécédents dans  $E$  par  $f$ . Alors  $E$  est fini, de cardinal  $k|F|$ .

PREUVE : On peut montrer les deux propositions de façon indépendante, ou bien montrer l'une, puis en déduire l'autre. ■

PROPOSITION 6

1. Si  $E$  et  $F$  sont deux ensembles finis, l'ensemble des applications de  $E$  dans  $F$  est fini, de cardinal  $|F|^{|E|}$ .
2. Si  $E$  est un ensemble fini, alors  $\mathcal{P}(E)$  est fini de cardinal  $2^{|E|}$ .
3. Si  $p$  et  $n$  sont deux entiers  $\geq 1$  le nombre d'injections de  $[[1, p]]$  dans  $[[1, n]]$ , noté  $A_n^p$ , vaut  $\frac{n!}{(n-p)!}$ .
4. Si  $n \in \mathbb{N}^*$ , le nombre de bijections de  $[[1, n]]$  sur lui-même vaut  $n!$ .
5. Si  $n \in \mathbb{N}^*$  et  $0 \leq k \leq n$ , le nombre de parties de  $[[1, n]]$  à  $k$  éléments, noté  $C_n^k$  ou  $\binom{n}{k}$ , vaut  $\frac{n!}{k!(n-k)!}$ .

<sup>2</sup>cette dernière hypothèse n'est pas indispensable, mais en tout cas, et c'est essentiel, ses moutons doivent avoir le nombre de pattes réglementaire

<sup>3</sup>une partition de  $E$  est la donnée d'ensembles **disjoints** dont la réunion est  $E$

## REMARQUES 6

- On appelle un “arrangement sans répétition de  $p$  éléments de  $\llbracket 1, n \rrbracket$ ” un  $p$ -uplet  $(x_1, \dots, x_p)$  où les  $x_i$  sont des éléments distincts de  $\llbracket 1, n \rrbracket$ . Cela correspond à une injection de  $\llbracket 1, p \rrbracket$  dans  $\llbracket 1, n \rrbracket$ ; il y en a donc  $A_n^p$ .
- Si  $E$  et  $F$  sont finis de cardinaux respectifs  $p$  et  $n$ , le nombre d’injections de  $E$  dans  $F$  est encore  $A_n^p$ .
- Si  $E$  est fini de cardinal  $n$ , le nombre de parties de  $E$  est  $2^n$ , alors que le nombre de bijections de  $E$  sur lui-même est  $n!$

PREUVE : On donne des idées de preuve. A chaque fois, on peut écrire une preuve précise (généralement par récurrence) ou bien “expliquer les choses avec les mains”, ce qui n’empêche pas d’être rigoureux<sup>4</sup>. Dans la suite,  $E$  est de cardinal  $n$ , avec  $E = \{x_1, x_2, \dots, x_n\}$ .

1. - Pour construire  $f : E \rightarrow F$ , on choisit  $f(x_1)$  ( $|F|$  possibilités), puis **de façon indépendante**  $f(x_2)$ , etc. . . , et enfin  $f(x_n)$ ; d’où  $|F|^n$  possibilités.
  - On raisonne par récurrence sur  $|E|$ , et on montre que l’application  $f \mapsto (f|_{\llbracket 1, n-1 \rrbracket}, f(n))$  établit une bijection de  $F^{\llbracket 1, n \rrbracket}$  sur  $F^{\llbracket 1, n-1 \rrbracket} \times F$ .
2. - Pour construire une partie  $A$  de  $E$ , on décide si oui ou non on place  $x_1$  dans  $A$  (deux possibilités), puis de façon indépendante, si on place  $x_2$ , etc. . . ; d’où  $2^n$  possibilités.
  - On peut utiliser le fait que  $\mathcal{P}(E)$  est en bijection avec l’ensemble des applications de  $E$  dans  $\llbracket 0, 1 \rrbracket$  (via les fonctions caractéristiques), et utiliser le résultat précédent.
3. - Pour construire une injection  $f : \llbracket 1, p \rrbracket \rightarrow \llbracket 1, n \rrbracket$ , on choisit  $f(1)$  ( $n$  possibilités), puis  $f(2)$  ( $n-1$  possibilités, puisqu’il faut exclure  $f(1)$ ), puis  $f(3)$  ( $n-2$  possibilités, puisqu’il faut exclure  $f(1)$  et  $f(2)$ ), etc. . . , et enfin  $f(n)$  ( $n-p+1$  possibilités); d’où  $n(n-1) \dots (n-p+1) = \frac{n!}{(n-p)!}$  possibilités.
  - Récurrence sur  $p$  : on applique le lemme des bergers à l’application :

$$\varphi : I(p, n) \longrightarrow I(p-1, n), \quad f \longmapsto f|_{\llbracket 1, p-1 \rrbracket}$$

( $I(p, n)$  désigne le nombre d’injections de  $\llbracket 1, p \rrbracket$  dans  $\llbracket 1, n \rrbracket$ ). Cette application est surjective et, plus précisément, chaque injection de  $\llbracket 1, p-1 \rrbracket$  dans  $\llbracket 1, n \rrbracket$  peut être prolongée de  $n-p+1$  façons différentes en une injection de  $\llbracket 1, p \rrbracket$  dans  $\llbracket 1, n \rrbracket$ , ce qui signifie que les éléments de  $I(p-1, n)$  admettent  $n-p+1$  antécédents par  $f$ . On peut alors appliquer le lemme des bergers.

4. Pour les applications de  $\llbracket 1, n \rrbracket$  dans lui-même, il y a équivalence entre l’injectivité et la bijectivité (applications entre deux ensembles finis de même cardinal); on applique alors le résultat précédent.
5. Déjà, en bon physicien, on regardera les “cas limites”  $k \in \{0, 1, n-1, n\}$ .
  - Pour construire une partie à  $p$  éléments, on peut choisir les éléments les uns après les autres, ce qui revient à choisir un  $p$ -uplet  $(x_1, \dots, x_p)$ , puis considérer l’ensemble de ses éléments. Mais un même ensemble  $\{y_1, \dots, y_p\}$  peut être décrit par les  $p!$   $p$ -uplets  $(y_{\sigma(1)}, \dots, y_{\sigma(p)})$ , où  $\sigma$  est une bijection de  $\llbracket 1, p \rrbracket$  sur lui-même. Il y a donc  $\frac{A_n^p}{p!}$  telles parties.
  - Considérons l’application  $\Phi$  qui à une injection de  $\llbracket 1, p \rrbracket$  dans  $\llbracket 1, n \rrbracket$  associe son image (qui est donc une partie à  $p$  éléments de  $\llbracket 1, n \rrbracket$ ). On montre que chaque pré-image<sup>5</sup> est de cardinal  $p!$ , et on applique le lemme des bergers.

■

EXERCICE 10 Déterminer le nombre de surjections de  $\llbracket 1, n+1 \rrbracket$  dans  $\llbracket 1, n \rrbracket$ .

SOLUTION : On commence par choisir les deux éléments qui auront la même image, soit  $C_n^2$  possibilités, puis l’image commune de ces éléments ( $n$  choix), puis on établit une bijection entre les  $n-1$  éléments restant un départ et à l’arrivée. Le nombre de surjections est donc :  $\frac{n(n+1)}{2}n(n-1)!$ .

<sup>4</sup>ceux qui grognent, bien souvent, ne savent pas ce qu’est une preuve, au sens formel du terme, et, en tout cas, sont très certainement incapables d’en faire une de plus de trois lignes, alors bon. . .

<sup>5</sup>une pré-image est l’ensemble des antécédents par  $\Phi$  d’un élément donné de l’ensemble d’arrivée de  $\Phi$

**EXERCICE 11** Quelle est la probabilité pour qu'au moins deux personnes parmi 40 aient la même date anniversaire ? On supposera que les dates anniversaires sont équiréparties parmi 365 dates possibles.

Evaluer à la calculatrice. Surpris ?

### 3.4 Coefficients binomiaux

On donne ici trois résultats élémentaires concernant les coefficients binomiaux. On verra plus tard des résultats "autour du binôme". Tout d'abord, on peut étendre la définition des  $C_n^k$  aux cas où  $k < 0$  ou bien  $k > n$ , en posant  $C_n^k = 0$ .  $C_n^k$  reste d'ailleurs le nombre de parties à  $k$  éléments de  $\llbracket 1, n \rrbracket$  dans ces cas un peu dégénérés.

#### PROPOSITION 7

1. Si  $n \in \mathbb{N}^*$  et  $p \in \llbracket 0, n \rrbracket$ , alors  $C_n^{n-p} = C_n^p$ .
2. Si  $n \in \mathbb{N}^*$  et  $p \in \llbracket 1, n-1 \rrbracket$ , on a :  $C_n^p = C_{n-1}^{p-1} + C_{n-1}^p$ .
3. Si  $n \in \mathbb{N}^*$ , on a  $\sum_{k=0}^n C_n^k = 2^n$ .

PREUVE : On donne dans chaque cas une preuve combinatoire et une preuve calculatoire.

1. - L'application  $A \mapsto \llbracket 1, n \rrbracket \setminus A$  induit une bijection entre les parties de  $\llbracket 1, n \rrbracket$  à  $p$  éléments et celles à  $n-p$  éléments.
  - Si  $p \in \llbracket 1, n-1 \rrbracket$  :  $C_n^{n-p} = \frac{n!}{(n-p)!(n-(n-p))!} = \frac{n!}{(n-p)!p!} = C_n^p$ .
2. - Les parties à  $p$  éléments de  $\llbracket 1, n \rrbracket$  sont incluses dans  $\llbracket 1, n-1 \rrbracket$  (il y en a  $C_{n-1}^p$ ) ou bien (ou exclusif) de la forme  $\{n\} \cup E$ , où  $E$  est une partie à  $p-1$  éléments de  $\llbracket 1, n-1 \rrbracket$  (il y en a  $C_{n-1}^{p-1}$ ). D'où le résultat.
  - On peut également écrire :

$$\begin{aligned} C_{n-1}^{p-1} + C_{n-1}^p &= \frac{(n-1)!}{(p-1)!(n-p)!} + \frac{(n-1)!}{p!(n-p-1)!} \\ &= \frac{(n-1)!}{p!(n-p)!} (p + (n-p)) = \frac{n!}{p!(n-p)!} = C_n^p. \end{aligned}$$

3. - Les parties de  $\llbracket 1, n \rrbracket$  sont au nombre de  $2^n$ . Mais celles-ci ont un cardinal compris entre 0 et  $n$ , et, pour un cardinal  $k$  donné, il y a  $C_n^k$  parties à  $k$  éléments.
  - On peut également appliquer la formule du binôme de Newton<sup>6</sup>, en notant que  $2^n = (1+1)^n$ . ■

**REMARQUE 7** Pour établir les formules sommatoires concernant les  $C_n^k$ , on s'efforcera, dans la mesure du possible, de donner des preuves combinatoires.

**EXERCICE 12** Soit  $n \in \mathbb{N}^*$ . Montrer :  $C_{2n}^n = \sum_{k=0}^n (C_n^k)^2$ .

**SOLUTION** : Dénombrons les parties de  $\llbracket 1, 2n \rrbracket$  à  $n$  éléments. D'une part, on sait qu'il y a  $C_{2n}^n$  telles parties. D'autre part, ces parties sont de la forme  $E_1 \cup E_2$ , où  $E_1$  et  $E_2$  sont des parties de  $\llbracket 1, n \rrbracket$  et  $\llbracket n+1, 2n \rrbracket$ .

On peut commencer par choisir le nombre  $k \in \llbracket 0, n \rrbracket$  d'éléments de  $E_1$ . Ensuite, pour un  $k$  donné, il faut choisir la partie  $E_1$  ( $C_n^k$  choix) et indépendamment, la partie  $E_2$ , constitué de  $n-k$  éléments parmi  $n$ , soit  $C_n^{n-k} = C_n^k$  choix. On en déduit la formule annoncée. ■

<sup>6</sup>cf terminale, ou bien le chapitre sur les anneaux, à venir