Ensembles

PTSI B Lycée Eiffel

22 décembre 2012

La vie n'est bonne qu'à étudier et à enseigner les mathématiques.

Blaise Pascal.

Ne tenez pour certain que ce qui est démontré.

Isaac Newton.

Introduction

Ce chapître est un peu fourre-tout, la notion (extrêmement générale) d'ensemble étant prétexte à regrouper trois parties de cours assez indépendantes : une partie théorique sur les notions d'applications injective et sujective, permettant de vraiment comprendre la notion essentielle en mathématiques de bijection ; une partie consacrée au principe de récurrence et à ses variantes, il est évidemment essentiel de maîtriser parfaitement cette technique de démonstration fondamentale. Cette partie contiendra également quelques notions sur les calculs de sommes, là aussi un outil qu'on recroisera souvent. Enfin, la dernière partie de ce chapitre est consacrée au dénombrement, qui sert un peu moins pour nous que pour vos camarades ayant des probabilités à leur programme, mais qui permet tout de même d'introduire quelques outils de calculs très importants, au premier rang desquels les coefficients binomiaux. Même si ce chapître ne sera pas celui qui fera l'objet du plus grand nombre d'interrogations dans l'immédiat, il serait vraiment très malvenu de le négliger, son contenu étant nécessaire pour fixer les bases des premiers chapîtres d'algèbre et d'analyse que nous aborderons ensuite.

Objectifs du chapitre :

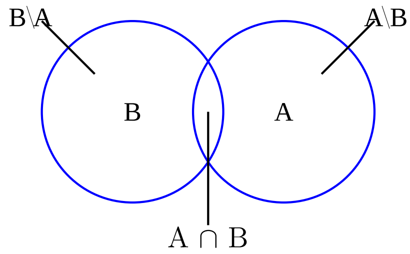
- maîtriser les notions d'application injective et surjective, y compris pour des applications autres que celles de $\mathbb{R}$ dans $\mathbb{R}$
- comprendre réellement le principe de récurrence, et savoir l'appliquer dans toutes les situations où on peut en avoir besoin
- maîtriser les calculs de sommes faisant intervenir les sommes classiques
- savoir effectuer des dénombrements d'ensembles non triviaux, maitriser les calculs faisant intervenir les coefficients binomiaux

1 Ensembles et applications

1.1 Ensembles

On suppose connues les notions d'**ensemble**, **sous-ensemble**, **inclusion**, **appartenance**, **ensemble vide** (qui sont rappelées dans notre premier chapître sur les fonctions usuelles), ainsi que les opérations d'**union** et d'**intersection** et leurs propriétés élémentaires, notamment la distributivité de l'une par rapport à l'autre (dans les deux sens). Signalons simplement la possibilité d'effectuer des unions ou intersections infinies, qu'on notera sous la forme $\bigcup_{i \in I} A_i$ et $\bigcap_{i \in I} A_i$.

Définition 1. Soit A un sous-ensemble d'un ensemble E. On définit le **complémentaire** de A dans E par $\overline{A} = \{x \in E \mid x \notin A\}$. Plus généralement, si B est un autre sous-ensemble de E, on peut définir le complémentaire de A dans B (aussi appelé différence de B et de A) par $B \backslash A = \{x \in B \mid x \notin A\}$.



Exemple : Soit $E = \mathbb{R}$ et $A = [-3; 5]$, alors $\overline{A} =]-\infty; 3[\cup]5; +\infty[$.

Proposition 1. Lois de Morgan. Deux propriétés symétriques à retenir :
- $\overline{A \cup B} = \overline{A} \cap \overline{B}$
- $\overline{A \cap B} = \overline{A} \cup \overline{B}$

Démonstration. Ne pas appartenir à A ou à B est équivalent à n'appartenir ni à A, ni à B. C'est juste ceci que retranscrit la première loi de Morgan. La deuxième est similaire. □

Définition 2. Le **produit cartésien** de deux ensembles E et F est l'ensemble constitué de tous les couples d'éléments (x, y), avec $x \in E$ et $y \in F$. On le note $E \times F$.

Remarque 1. Les notations sont très importantes : l'ensemble $\{2; 3\}$ est constitué de deux éléments (les entiers 2 et 3), alors que l'ensemble $\{(2, 3)\}$ est constitué d'un seul élément, la paire d'entiers $(2, 3)$.

Remarque 2. Encore une fois, on généralise facilement à plus de deux ensembles.

Remarque 3. Lorsque $E = F$, on note E^2 plutôt que $E \times E$, et plus généralement $\underbrace{E \times E \times \cdots \times E}_{n \text{ fois}} = E^n$.

Définition 3. L'ensemble des parties d'un ensemble E, noté $\mathcal{P}(E)$, est l'ensemble dont les éléments sont les sous-ensembles de E.

Exemple : Si $E = \{1; 2; 3\}$, $\mathcal{P}(E) = \{\emptyset; \{1\}; \{2\}; \{3\}; \{1; 2\}; \{1; 3\}; \{2; 3\}; \{1; 2; 3\}\}$.

1.2 Applications

Une application est un cas particulier de ce que vous avez l'habitude d'appeler une fonction. La différence est qu'une application doit être définie sur tout son ensemble de départ, alors qu'on parle par exemple de fonction de $\mathbb{R}$ dans $\mathbb{R}$ pour la fonction inverse (mais on peut très bien parler de l'application inverse de $\mathbb{R}^*$ dans $\mathbb{R}$).

Définition 4. Une **application** f est la donnée d'un ensemble E, appelé ensemble de départ de l'application, d'un ensemble F appelé ensemble d'arrivée, et pour chaque élément x de E, d'un unique élément de F noté $f(x)$. On appelle $f(x)$ l'**image** de l'élément x par f, et si $y \in E$, les éléments x de E vérifiant $f(x) = y$ sont appelés **antécédents** de y par f (un élément y peut très bien ne pas avoir d'antécédent, ou au contraire en avoir plusieurs).

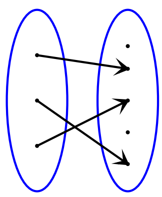
Exemple : L'application $x \to x$, définie sur un ensemble quelconque E, est appelée application **identité**, souvent notée id (ou id_E si on veut bien préciser l'ensemble de départ). La fonction $x \mapsto \dfrac{3}{x-2}$ est une application de $\mathbb{R} \backslash \{2\}$ dans $\mathbb{R}$.

Remarque 4. Deux applications sont identiques si elles ont même ensemble de départ, même ensemble d'arrivée et envoient un même élément sur une même image. Par exemple, les fonctions d'une variable réelle $f : x \mapsto x - 4$ et $g : x \mapsto \dfrac{x^2 - 5x + 4}{x - 1}$ sont différentes, même si elles coïncident sur $\mathbb{R} \backslash \{1\}$: elles n'ont pas le même ensemble de définition.

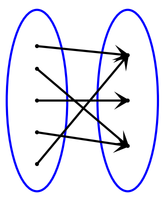
Définition 5. Soit $f : E \to F$ une application et E' un sous-ensemble de E. L'application $g : E' \to F$ définie par $\forall x \in E'$, $g(x) = f(x)$ est appelée **restriction** de f au sous-ensemble E' et notée $f_{|E'}$. On dit egalement que f est un **prolongement** de g à E.

Exemple : La fonction $x \to x \ln x$, définie sur R_+^*, peut se prolonger en une fonction $\tilde{f}$ définie et continue sur R_+ en posant $\tilde{f}(0) = 0$. En pratique, on utilise souvent la même notation pour désigner le prolongement que pour la fonction d'origine, même si c'est un abus de notation.

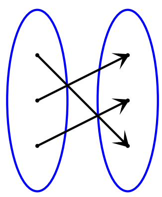
Définition 6. Soit $f : E \to F$ une application, f est dite **injective** si $\forall (x, x') \in E^2, f(x) = f(x') \Rightarrow x = y$; f est dite **surjective** si $\forall y \in F, \exists x \in E, f(x) = y$; enfin, f est dite **bijective** si elle est à la fois injective et surjective.



f injective

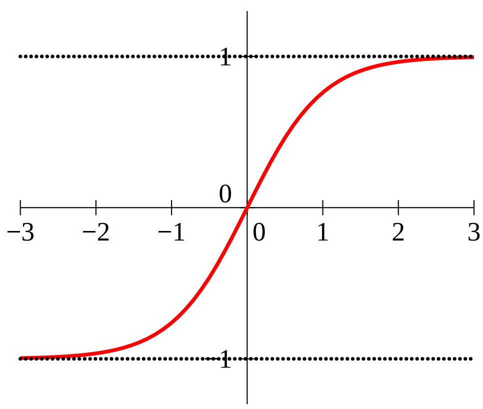


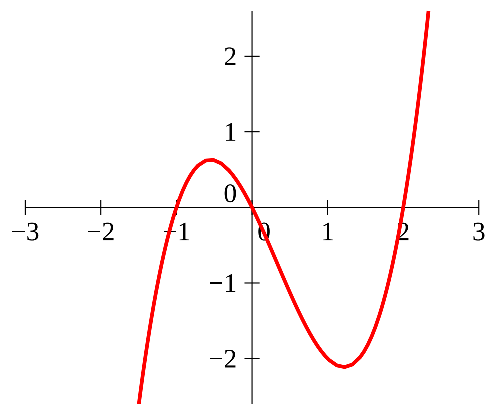
f surjective



f bijective

Et pour ceux qui préfèrent avec des fonctions, un exemple de fonction de $\mathbb{R}$ dans $\mathbb{R}$ injective mais pas surjective (à gauche, on voit que les valeurs supérieures à 1 par exemple n'ont pas d'anctécédent), et un de fonction surjective mais pas injective à droite (par exemple 0 a trois antécédents par cette fonction) :





Remarque 5. Autrement dit, f est injective si tout élément de F a au plus un antécédent par f, surjective si tout élément de F a au moins un antécédent de F, et bijective si tout élément de F a exactement un antécédent par f. On peut aussi définir une application injective de la façon suivante : $x \neq x' \Rightarrow f(x) \neq f(x')$.

Exemples : L'application $x \mapsto x^2$, qui va de $\mathbb{R}$ dans $\mathbb{R}_+$, est surjective (tout réel positif admet une racine carrée) mais pas injective car par exemple 2 et -2 ont la même image par f. L'application racine carrée est par contre bijective de $\mathbb{R}_+$ dans lui-même.

Proposition 2. Soient $f : E \to F$ et $g : F \to G$ deux applications. Si f et g sont injectives alors $g \circ f$ est injective. Si f et g sont surjectives, alors $g \circ f$ est surjective.

Démonstration. Supposons g et f injectives, et soient $x, x' \in E^2$ tels que $g(f(x)) = g(f(x'))$. Par injectivité de g, on a alors nécessairement $f(x) = f(x')$, puis par injectivité de f, $x = x'$, ce qui prouve l'injectivité de $g \circ f$. Supposons désormais g et f surjectives et soit $z \in G$. Par surjectivité de g, $\exists y \in F$, $z = g(y)$, puis par surjectivité de f, $\exists x \in E$, $y = f(x)$. Mais alors $z = g \circ f(x)$, donc z a un antécédent par $g \circ f$, ce qui prouve sa surjectivité. □

Remarque 6. La réciproque de ces propriétés est totalement fausse, voir la feuille d'exercices pour quelques exemples.

Proposition 3. Une application $f : E \to F$ est bijective si et seulement si il existe $g : F \to E$ telle que $g \circ f = id_E$ et $f \circ g = id_F$. L'application g est alors appelée **bijection réciproque** de f (ou réciproque tout court) et notée f^{-1}.

Remarque 7. Cette réciproque, bien que notée f^{-1}, n'a rien à voir avec la fonction inverse de f, que pour cette raison nous noterons toujours $\dfrac{1}{f}$. Notons au passage que f^{-1} est effectivement bijective, de réciproque f (c'est évident une fois le théorème démontré).

Démonstration. Supposons f bijective et soit $y \in F$. Il existe un unique antécédent x de y par f, on pose $g(y) = x$. On a alors par construction $f \circ g(x) = x$, donc $f \circ g = id_F$. De plus, si $x \in E$, $g(f(x))$ est un antécédent de $f(x)$, mais comme il n'y en qu'un ça ne peut être que x, donc on a aussi $g \circ f = id_E$.
Réciproquement, si $g \circ f = id_E$ et $f \circ g = id_F$, considérons x et x' tels que $f(x) = f(x')$, on a alors $g \circ f(x) = g \circ f(x')$, donc $x = x'$, ce qui prouve l'injectivité de f. Soit maintenant $y \in F$, alors $g(y)$ est un antécédent de y par f puisque $f \circ g(y) = y$, donc f est sujective. L'application f est donc bijective. □

Remarque 8. Vous connaissez déjà quelques exemples classiques de bijections réciproques, notamment ln (bijective de $\mathbb{R}_+^*$ dans $\mathbb{R}$) et exp (bijective réciproque de ln de $\mathbb{R}$ dans $\mathbb{R}_+^*$). Vous savez également que les représentations graphiques de ces deux fonctions sont symétriques par rapport à la droite d'équation $y = x$. C'est une propriété générale des fonctions réciproques.

Exemple : L'application $f : x \mapsto 3x + 6$ est bijective de $\mathbb{R}$ dans $\mathbb{R}$ et son application réciproque est l'application $g : x \mapsto \dfrac{1}{3}x - 2$. En effet, $g \circ f(x) = \dfrac{1}{3}(3x+6) - 2 = x$ et $f \circ g(x) = 3\left(\dfrac{1}{3}x - 2\right) + 6 = x$.

Proposition 4. Soient $f : E \to F$ et $g : F \to G$ deux applications bijectives, alors $g \circ f : E \to G$ est une application bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Démonstration. f et g étant à la fois injectives et surjectives, $g \circ f$ est à la fois injective et surjective (cf plus haut) donc bijective. De plus, $\forall x \in E$, $f^{-1} \circ g^{-1} \circ g \circ f(x) = f^{-1}((g^{-1} \circ g)(f(x))) = f^{-1}(f(x)) = x$ et de même $\forall x \in G$, $g \circ f \circ f^{-1} \circ g^{-1}(x) = x$. □

Définition 7. Soit $f : E \to F$ une application et $A \subset E$. On appelle **image** (directe) de A l'ensemble des images des éléments de A : $f(A) = \{y \in F \mid \exists x \in A, f(x) = y\}$. Soit maintenant $B \subset F$, on appelle **image réciproque** de B par F l'ensemble des antécédents d'élements de B : $f^{-1}(B) = \{x \in E \mid f(x) \in B\}$.

Remarque 9. La deuxième notation n'a pas été choisie de façon contradictoire avec la définition d'application réciproque (encore heureux). Si f est bijective, l'image réciproque d'une partie B de F est confondue avec son image directe par f^{-1}.

Exemple : Considérons l'application $f : x \mapsto x^2$ de $\mathbb{R}$ dans $\mathbb{R}$, alors $f([2;5]) = [4;25]$; $f([-1;3]) = [0;9]$; $f^{-1}([4;9]) = [-3;-2] \cup [2;3]$.

2 Récurrence, sommes et produits

2.1 Démonstration par récurrence

Théorème 1. Tout sous-ensemble non vide de $\mathbb{N}$ admet un plus petit élément.

Remarque 10. Ce résultat fondamental pour la structure de l'ensemble $\mathbb{N}$ est plus un axiome qu'un réel théorème.

Proposition 5. Principe de récurrence.
Soit $(P_n)_{n\in\mathbb{N}}$ une suite de propriétés. Si P_0 est vraie, et si $\forall n \in \mathbb{N}$, $P_n \Rightarrow P_{n+1}$, alors toutes les propriétés P_n sont vraies.

Démonstration. C'est en fait équivalent au théorème énoncé précédemment. Notons $A = \{n \in \mathbb{N} \mid P_n \text{est fausse}\}$. On procède par l'absurde, supposons donc que les propriétés ne sont pas toutes vraies, ce qui revient à dire que l'ensemble A n'est pas vide. D'après le théorème précédent, il y a donc un entier n_0 qui est le plus petit élément de l'ensemble A. Cet entier ne peut pas être nul puisque P_0 est supposée vrai, on en déduit que $n_0 - 1 \in \mathbb{N}$. La propriété P_{n_0-1} est vraie puisque n_0 est le plus petit élément de A, mais P_{n_0} est fausse. C'est impossible à cause de l'hypothèse $P_n \Rightarrow P_{n+1}$, l'ensemble A est donc vide, et les propriétés sont toutes vraies. □

Cette propriété sert également de pense-bête pour bien structurer la rédaction d'une démonstration par récurrence. On procède théoriquement en quatre étapes :

- **Énoncé** clair et précis des propriétés P_n et du fait qu'on va réaliser une récurrence.
- **Initialisation** : on vérifie que P_0 est vraie (habituellement un calcul très simple).
- **Hérédité** : on suppose P_n vraie pour un entier n quelconque (c'est l'hypothèse de récurrence) et on prouve P_{n+1} à l'aide de cette hypothèse (si on n'utilise pas l'hypothèse de récurrence, c'est qu'on n'avait pas besoin de faire une récurrence !).
- **Conclusion** : En invoquant le principe de récurrence, on peut affirmer avoir démontré P_n pour tout entier n.

Exemple : On considère la suite numérique définie de la façon suivante : $u_0 = 4$ et $\forall n \in \mathbb{N}$, $u_{n+1} = \dfrac{1}{u_n - 2} + 2$. On souhaite prouver que cette suite est minorée par 2, c'est-à-dire que $\forall n \in \mathbb{N}$, $u_n > 2$. Nous allons pour cela, bien évidemment, procéder par récurrence :

- **Énoncé** : Nous allons prouver par récurrence la propriété P_n : $u_n > 2$.
- **Initialisation** : $u_0 = 4 > 2$, donc la propriété P_0 est vérifiée.
- **Hérédité** : Supposons désormais P_n vraie, c-est-à-dire que $u_n > 2$, et essayons de prouver que $u_{n+1} > 2$. C'est en fait assez simple en partant de l'hypothèse de récurrence : $u_n > 2 \Rightarrow u_n - 2 > 0 \Rightarrow \dfrac{1}{u_n - 2} > 0 \Rightarrow \dfrac{1}{u_n - 2} + 2 > 2 \Rightarrow u_{n+1} > 2$.
- **Conclusion** : D'après le principe de récurrence, la propriété P_n est vrai pour tout entier n.

Remarque 11. Variations du principe de récurrence :
Le monde mathématique n'étant pas parfait, une récurrence classique n'est hélas pas toujours suffisante pour montrer certaines propriétés. Il faut donc être capable de modifier légèrement la structure dans certains cas :

- si on ne cherche à montrer P_n que lorsque $n \geqslant n_0$ (n_0 étant un entier fixe dépendant du contexte), on peut toujours procéder par récurrence, mais en initialisant à n_0.

- il est parfois nécessaire que l'hypothèse de récurrence porte non pas sur une valeur de n, mais sur deux valeurs consécutives. On peut alors effectuer une récurrence double : on vérifie P_0 et P_1 lors de l'étape d'initialisation, et on prouve P_{n+2} à l'aide de P_n et P_{n+1} lors de l'hérédité (on peut de même effectuer des récurrences triples, quadruples, etc. en faisant une initialisation triple ou plus, et en prenant une hypothèse de récurrence triple ou plus ; dans tous les cas on ne démontre qu'une seule propriété lors de l'hérédité).
- on peut même avoir besoin pour prouver l'hérédité que la propriété soit vérifiée pour **tous** les entiers inférieurs. Dans ce cas, on parle de récurrence forte : le plus simple est de modifier la définition de la propriété P_n pour lui donner un énoncé commençant par $\forall k \leqslant n$. Ainsi, lorsqu'on suppose P_n vérifiée, on a une relation vraie pour toutes les valeurs de k inférieures ou égales à n (les plus malins d'entre vous noteront d'ailleurs qu'on peut toujours rédiger une récurrence sous forme de récurrence forte, ça ne demande pas plus de travail et ça ne peut pas être moins efficace ; c'est toutefois un peu plus lourd et déconseillé sauf nécessité).

Exemple : On considère la suite définie par $u_0 = 0$, $u_1 = 1$ et $\forall n \in \mathbb{N}$, $u_{n+2} = 5u_{n+1} - 6u_n$, et on veut déterminer une expression du terme général de la suite (u_n). Pour cela (ce n'est pas forcément la meilleure méthode, mais la plus simple pour nous pour l'instant), on calcule les termes suivants de la suite : $u_2 = 5$, $u_3 = 19$, $u_4 = 65$. Une inspiration soudaine nous fait conjecturer que $u_n = 3^n - 2^n$ (si on ne devine pas la formule, on ne pourra jamais faire de récurrence), ce qu'on va prouver par récurrence double. La formule est vraie pour u_0 : $3^0 - 2^0 = 1 - 1 = 0$ et pour u_1 : $3^1 - 2^1 = 1$. Supposons-là vérifiée pour u_n et u_{n+1}, alors $u_{n+2} = 5u_{n+1} - 6u_n = 5(3^{n+1} - 2^{n+1}) - 6(3^n - 2^n) = 15 \times 3^n - 10 \times 2^n - 6 \times 3^n + 5 \times 2^n = 9 \times 3^n - 4 \times 2^n = 3^{n+2} - 2^{n+2}$. La formule est donc vérifiée au rang $n + 2$, le principe de récurrence double permet de conclure.

2.2 Sommes

Définition 8. Le symbole $\sum$ signifie « somme ». Plus précisément, la notation $\sum_{i=1}^{i=n} a_i$ se lit par exemple « somme pour i variant de 1 à n de a_i » et peut se détailler de la façon suivante : $\sum_{i=1}^{i=n} a_i = a_1 + a_2 + \cdots + a_n$.

Remarque 12.

- La lettre i est une variable muette, autrement dit on peut la changer par n'importe quelle autre lettre sans changer la valeur de la somme. On choisit traditionnellement les lettres i, j, k, etc. pour les indices de sommes.
- Dans une somme, la variable muette prend toujours **toutes** les valeurs entières comprises entre la valeur initiale et la valeur finale.

Exemple : Si a est une constante, $\sum_{i=2}^{i=n} a = (n-1)a$ (faites bien attention au nombre de termes que contient la somme...).

Proposition 6. Règles de calcul sur les sommes. On a le droit d'effectuer les opérations suivantes :

- factoriser par une constante : $\sum_{i=0}^{i=n} ka_i = k \sum_{i=0}^{i=n} a_i$
- séparer ou regrouper des sommes de mêmes indices : $\sum_{i=0}^{i=n} a_i + b_i = \sum_{i=0}^{i=n} a_i + \sum_{i=0}^{i=n} b_i$
- séparer les indices en deux (relation de Chasles) : $\sum_{i=1}^{i=n} a_i = \sum_{i=1}^{i=p} a_i + \sum_{i=p+1}^{i=n} a_i$
- faire un changement d'indice : $\sum_{i=1}^{i=n} a_i = \sum_{j=0}^{j=n-1} a_{j+1}$ (on a posé $j = i - 1$)

Remarque 13. Tenter de simplifier d'une façon ou d'une autre une somme de la forme $\sum_{i=0}^{i=n} a_i b_i$ est par contre une très bonne manière de s'attacher la rancoeur tenace de votre professeur ; les sommes et produits ne font pas bon ménage.

Proposition 7. Sommes classiques.

- $\forall n \in \mathbb{N}, \sum_{i=0}^{i=n} i = \frac{n(n+1)}{2}$
- $\forall n \in \mathbb{N}, \sum_{i=0}^{i=n} i^2 = \frac{n(n+1)(2n+1)}{6}$
- $\forall n \in \mathbb{N}, \sum_{i=0}^{i=n} i^3 = \frac{n^2(n+1)^2}{4} = \left(\sum_{i=1}^{i=n} i\right)^2$
- $\forall q \neq 1, \forall n \in \mathbb{N}, \sum_{k=0}^{k=n} q^k = \frac{1-q^{n+1}}{1-q}$

Démonstration.

- Nous allons démontrer par récurrence que la propriété $P_n : \sum_{i=0}^{i=n} i = \frac{n(n+1)}{2}$ est vraie pour tout entier n. Pour $n = 0$, nous avons $\sum_{i=0}^{i=n} i = 0$ et $\frac{0(0+1)}{2} = 0$, donc P_0 est vraie. Supposons P_n vraie pour un entier n quelconque, c'est-à-dire que $\sum_{i=0}^{i=n} i = \frac{n(n+1)}{2}$. On peut alors effectuer le calcul suivant : $\sum_{i=0}^{n+1} i = \sum_{i=0}^{i=n} i + n + 1 = \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$, ce qui prouve P_{n+1}. D'après le principe de récurrence, nous pouvons donc affirmer que, $\forall n \in \mathbb{N}, \sum_{i=0}^{i=n} i = \frac{n(n+1)}{2}$.

- Nous allons prouver par récurrence la propriété $P_n : \sum_{i=0}^{i=n} i^2 = \frac{n(n+1)(2n+1)}{6}$. Pour $n = 0$, nous avons $\sum_{i=0}^{i=n} i^2 = 0^2 = 0$, et $\frac{0(0+1)(2 \times 0+1)}{6} = 0$, donc P_0 est vérifiée. Supposons désormais P_n vraie pour un entier n quelconque, on peut alors écrire $\sum_{i=0}^{i=n+1} i^2 = \sum_{i=0}^{i=n} i^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} = \frac{(n+1)(n(2n+1) + 6n + 6)}{6} = \frac{(n+1)(2n^2 + 7n + 6)}{6} = \frac{(n+1)(n+2)(2n+3)}{6} = \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}$, donc P_{n+1} est vérifiée. D'après le principe de récurrence, on peut conclure que P_n est vraie pour tout entier naturel n.

- Nous allons prouver par récurrence la propriété $P_n : \sum_{i=0}^{i=n} i^3 = \frac{n^2(n+1)^2}{4}$. Pour $n = 0$, nous avons $\sum_{i=0}^{i=n} i^3 = 0^3 = 0$, et $\frac{0^2(0+1)^2}{4} = 0$, donc P_0 est vérifiée. Supposons désormais P_n vraie pour un entier n quelconque, on peut alors écrire $\sum_{i=0}^{i=n+1} i^3 = \sum_{i=0}^{i=n} i^3 + (n+1)^3 = \frac{n^2(n+1)^2}{4} + (n+1)^3 = \frac{n^2(n+1)^2 + 4(n+1)^3}{4} = \frac{(n+1)^2(n^2+4n+4)}{4} = \frac{(n+1)^2(n+2)^2}{4}$, donc P_{n+1} est vérifiée. D'après le principe de récurrence, on peut conclure que P_n est vraie pour tout entier naturel n.

- Nous allons prouver par récurrence la propriété P_n : $\sum_{k=0}^{k=n} q^k = \frac{1-q^{n+1}}{1-q}$. Pour $n = 0$, nous avons $\sum_{k=0}^{k=n} q^k = q^0 = 1$, et $\frac{1-q^1}{1-q} = 1$, donc P_0 est vérifiée. Supposons désormais P_n vraie pour une entier n quelconque, on peut alors écrire $\sum_{k=0}^{k=n+1} q^k = \sum_{k=0}^{k=n} q^k + q^{n+1} = \frac{1-q^{n+1}}{1-q} + q^{n+1} = \frac{1-q^{n+1}+q^{n+1}-q^{n+2}}{1-q} = \frac{1-q^{n+2}}{1-q}$, donc P_{n+1} est vérifiée. D'après le principe de récurrence, on peut conclure que P_n est vraie pour tout entier naturel n.

$\square$

Exemple : La technique de la somme télescopique consiste à constater que la différence de deux sommes ayant beaucoup de termes communs comporte en fait nettement moins de termes que ce qu'elle n'en a l'air au départ. Considérons $S = \sum_{i=1}^{i=n} \frac{1}{i(i+1)}$. A priori pas évident à calculer, du moins tant qu'on a pas constaté que $\frac{1}{i} - \frac{1}{i+1} = \frac{i+1-i}{i(i+1)} = \frac{1}{i(i+1)}$. On peut alors faire le calcul suivant :
$\sum_{i=1}^{i=n} \frac{1}{i(i+1)} = \sum_{i=1}^{i=n} \frac{1}{i} - \sum_{i=1}^{i=n} \frac{1}{i+1} = \sum_{i=1}^{i=n} \frac{1}{i} - \sum_{j=2}^{j=n+1} \frac{1}{j} = 1 + \sum_{i=2}^{i=n} \frac{1}{i} - \sum_{j=2}^{j=n} \frac{1}{j} - \frac{1}{n+1} = 1 - \frac{1}{n+1}$
Si la fin du calcul ne vous semble pas claire, on peut aussi voir les choses ainsi :
$\sum_{i=1}^{i=n} \frac{1}{i} - \frac{1}{i+1} = 1 - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \cdots + \frac{1}{n} - \frac{1}{n+1} = 1 - \frac{1}{n+1}$.

Rien ne nous interdit de mettre une somme à l'intérieur d'une autre somme. Dans ce cas, il est toutefois très important d'utiliser deux indices différents pour les deux sommes, sous peine de confusion totale. Plusieurs notations sont possibles pour exprimer des sommes doubles : $\sum_{i=1}^{i=n} \sum_{j=1}^{j=n} i\sqrt{j} = \sum_{j=1}^{j=n} \sum_{i=1}^{i=n} i\sqrt{j} = \sum_{1 \leqslant i,j \leqslant n} i\sqrt{j}$. Cette somme est constituée de n^2 termes qu'on peut par exemple représenter dans un tableau contenant n lignes et n colonnes. L'ordre dans lequel on place les deux sommes est indifférent (d'où également la possibilité de n'utiliser qu'une seule somme), on a donc intérêt à les placer dans l'ordre le plus pratique pour le calcul, ici par exemple :
$\sum_{1 \leqslant j \leqslant i \leqslant n} 3j = 3 \sum_{i=1}^{i=n} \sum_{j=1}^{j=i} = 3 \sum_{i=1}^{i=n} \frac{i(i+1)}{2} = \frac{3}{2} \sum_{i=1}^{i=n} i^2 + i = \frac{3}{2} \left(\frac{n(n+1)(2n+1)}{6} + \frac{n(n+1)}{2} \right) = \frac{n(n+1)(2n+1) + 3n(n+1)}{4} = \frac{(n+1)(2n^2+n+3n)}{4} = \frac{n(n+1)(n+2)}{2}$.

2.3 Produits

Définition 9. Le symbole $\prod$ signifie « produit ». Par exemple, $\prod_{i=1}^{i=n} a_i = a_1 \times a_2 \times \cdots \times a_n$.

Définition 10. On appelle **factorielle** de l'entier naturel n, et on note $n!$, le nombre $n! = \prod_{i=1}^{i=n} i$.

Exemples : $\prod_{i=1}^{i=n} a = a^n$; $\quad \dfrac{(n+1)!}{n!} = \dfrac{\prod_{i=1}^{i=n+1} i}{\prod_{i=1}^{i=n} i} = n+1$.

Proposition 8. Les règles de calcul suivantes peuvent être utiles quand on manipule des produits :

- séparer ou regrouper des produits ayant les mêmes indices : $\prod_{i=1}^{i=n} a_i \times \prod_{i=1}^{i=n} b_i = \prod_{i=1}^{i=n} a_i b_i$
- séparer les indices (relation de Chasles) : $\prod_{i=1}^{i=n} a_i = \prod_{i=1}^{i=p} a_i \times \prod_{i=p+1}^{i=n} a_i$
- faire un changement d'indice : $\prod_{i=2}^{i=n+1} a_i = \prod_{j=1}^{j=n} a_{j+1}$

Remarque 14. Bien entendu, tenter de simplifier $\prod_{i=1}^{i=n}(a_i + b_i)$ serait une grave erreur que, j'en suis certain, vous ne commettrez pas deux fois (ni même une seule, si possible).

Exemple : Un petit calcul de produit pour finir ce paragraphe. $P = \prod_{i=1}^{i=n} 3i = \prod_{i=1}^{i=n} 3 \times \prod_{i=1}^{i=n} i = 3^n n!$

3 Dénombrement

3.1 Cardinaux

Définition 11. Un ensemble E est **fini** s'il est en bijection avec l'ensemble $\{1; 2; \dots ; n\}$, pour un entier naturel n. Cet entier n est alors unique. Il est appelé **cardinal** de l'ensemble E, et on le note $card(E)$, ou $|E|$, ou encore $\sharp E$.

Remarque 15. Cela correspond bien à la notion intuitive d'ensemble dont on peut compter les éléments. En effet, une bijection de E vers $\{1; \dots ; n\}$ est simplement une façon d'étiquetter les éléments de E avec les numéros 1, 2, …, n.

Démonstration. La seule chose nécessitant une preuve est l'unicité du cardinal. Supposons donc qu'un même ensemble soit à la fois en bijection avec $\{1; \dots ; n\}$ et avec $\{1; \dots ; p\}$ pour deux entiers distincts n et p. Quitte à composer les deux bijections, il existe alors une bijection de $\{1; \dots ; n\}$ dans $\{1; \dots ; p\}$. Notons donc n le plus petit entier naturel pour lequel $\{1; \dots ; n\}$ est en bijection avec un ensemble de la forme $\{1; \dots ; p\}$, où $p > n$. On veut prouver que cet entier n ne peut pas exister. Notons f la bijection supposée, $f(n) = k$ est alors un entier inférieur ou égal à p ayant un unique antécédent (en l'occurence n) par f. On construit désormais une application $g : \{1; \dots ; p-1\} \to \{1; \dots ; n-1\}$ de la façon suivante : $\forall i < k$, $g(i) = f^{-1}(i)$, et si $i > k$, $g(i) = f^{-1}(i+1)$. Cette application est bien définie, est à valeurs dans $\{1; \dots ; n-1\}$ (puisqu'on a soigneusement évité la valeur $f^{-1}(k)$ dans notre définition), et elle est bijective (linjectivité découle immédiatement de celle de f^{-1}, la surjectivité n'est pas difficile non plus en utilisant celle de f^{-1}, on prend toutes les valeurs prises par f^{-1} sauf n). On en déduit que $\{1; \dots ; n-1\}$ est en bijection avec $\{1; \dots ; p-1\}$, avec $p-1 > n-1$ puisque $p > n$. Ceci contredit la minimalité de l'entier n et achève notre démonstration. □

Proposition 9. Soit E un ensemble fini et F un sous-ensmble de E, alors F est un ensemble fini, et $|F| \leqslant |E|$, avec égalité si et seulement si $E = F$.

Démonstration. Cette propriété, comme souvent en ce qui concerne les ensembles finis, est assez évidente d'un point de vue intuitif, mais pas si simple à démontrer correctement. Contentons-nous de constater sur un cas particulier de constater que le principe est proche de la démonstration précédente. Soit F le sous-ensemble de E obtenu en enlevant à l'ensemble E un seul de ses éléments, qu'on notera x. Il existe par hypothèse, si $|E| = n$, une bijection $f : E \to \{1; \dots ; n\}$. On peut alors construire $g : \{1; \dots ; n-1\} \to F$ de la façon suivante : en notant $k = f(x)$, on pose $g(i) = f^{-1}(i)$ si $i < k$, et $g(i) = f^{-1}(k+1)$ si $i \geqslant k$. On vérifie sans trop de difficulté que g est bijective, et on prouve ainsi que $|E \backslash \{x\}| = n - 1$. Le cas général utilise une récurrence. $\square$

Proposition 10. Soient E et F deux ensembles finis. Si E et F sont en bijection l'un avec l'autre, ils ont même cardinal.

Démonstration. Il existe par hypothèse une bijection f de E vers F. De plus, F étant fini, notons n son cardinal, il existe alors une bijection g de F dans $\{1; \dots ; n\}$. L'application $g \circ f : E \to \{1; \dots ; n\}$ est une composée d'applications bijectives, donc est bijective, ce qui prouve que E est de cardinal n. $\square$

Proposition 11. Soient A et B deux sous-ensembles d'un même ensemble fini E. Alors $|A \cup B| = |A| + |B| - |A \cap B|$.

Démonstration. Commençons par constater que dans le cas où les deux ensembles A et B sont disjoints, on a $|A \cup B| = |A| + |B|$. Vous voulez une démonstration ? Soit f une bijection de A dans $\{1; \dots ; n\}$ et g une bijection de B dans $\{1; \dots ; p\}$, n et p étant les cardinaux respectifs de A et de B. On peut alors construire une bijection h de $A \cup B$ vers $\{1; \dots ; n+p\}$ en posant $\forall x \in A$, $h(x) = f(x)$ et $\forall x \in B$, $h(x) = g(x) + p$ (intuitivement, cela revient à garder pour les éléments de A la numérotation donnée par l'application f, et à décaler pour les éléments de B la numérotation donnée par g, de façon à ne pas utiliser deux fois les mêmes numéros). La démonstration de la bijectivité de h est laissée au lecteur. Une fois ce fait admis, constatons que $A \cup B$ est l'union disjointe des trois ensembles $A \backslash B$, $B \backslash A$ et $A \cap B$. On a donc, en utilisant le résultat que nous venons de démontrer, $|A \cup B| = |A \backslash B| + |B \backslash A| + |A \cap B|$. Or, A étant union disjointe de $A \backslash B$ et de $A \cap B$, on a également $|A| = |A \backslash B| + |A \cap B|$, ou encore $|A \backslash B| = |A| - |A \cap B|$. De même, $|B \backslash A| = |B| - |A \cap B|$, donc on obtient $|A \cup B| = |A| - |A \cap B| + |B| - |A \cap B| + |A \cap B|$, ce qui donne bien la formule annoncée. $\square$

Théorème 2. Formule du crible de Poincaré.
Soient A_1, A_2, ..., A_n des sous-ensembles finis d'un même ensemble E, alors

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{k=1}^{n} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} (-1)^{k+1} |A_{i_1} \cap \cdots \cap A_{i_k}|$$

Proposition 12. La formule de Poincaré étant assez peu lisible, voici ce que ça donne pour $n = 3$ et $n = 4$:

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

$|A \cup B \cup C \cup D| = |A| + |B| + |C| + |D| - |A \cap B| - |A \cap C| - |A \cap D| - |B \cap C| - |B \cap D| - |C \cap D| + |A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D| - |A \cap B \cap C \cap D|$

Démonstration. La preuve de la formule générale, assez technique, se fait par récurrence forte en utilisant le cas $n = 2$ (démontré plus haut). La formule est certainement vraie pour $n = 2$ (et $n = 1$ accessoirement). Supposons-la vraie au rang n, alors $\left| \bigcup_{i=1}^{n+1} A_i \right| = \left| \left(\bigcup_{i=1}^{n} A_i \right) \cup A_{n+1} \right| = \left| \bigcup_{i=1}^{n} A_i \right| + |A_{n+1}| - \left| \left(\bigcup_{i=1}^{n} A_i \right) \cap A_{n+1} \right| = \sum_{k=1}^{n} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} (-1)^{k+1} |A_{i_1} \cap \cdots \cap A_{i_k}| + |A_{n+1}| - \sum_{k=1}^{n} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} (-1)^{k+1} |A_{i_1} \cap \cdots \cap A_{i_k} \cap A_{n+1}|$ (on utilise simplement les propriétés élémentaires de l'union et de l'intersection pour faire rentrer le A_{n+1} dans la somme de droite). Il ne reste plus qu'à constater que tous les termes présents dans ce développement correspondent à ceux de la formule au rang $n+1$: tous les termes ne faisant pas intervenir A_{n+1} sont dans la somme de gauche, tous ceux faisant intervenir A_{n+1} pour $k \geqslant 2$ sont dans celle de droite (et on a bien un $(-1)^{k+2}$ devant la somme intérieure quitte à changer le signe $-$ devant la somme, ce qui correspond au nombre d'ensemble dont on prend l'intersection une fois qu'on a ajouté A_{n+1}). Enfin, le seul terme faisant intervenir A_{n+1} pour $k=1$ est $|A_{n+1}|$, qui est bien présent entre nos deux sommes. Bref, ça marche. □

Exemple : Dans un lycée de 300 élèves, 152 savent jouer au poker, 83 au tarot et 51 au bridge. De plus, 24 savent jouer à la fois au poker et au tarot, 14 au poker et au bridge, et 8 au tarot et au bridge. Enfin, 3 élèves maitrisent les trois jeux de cartes. Le nombre d'élèves jouant aux cartes est alors de $152+83+51-24-14-8+3=237$.

Proposition 13. Soit A un sous-ensemble fini d'un ensemble fini E, alors $|\bar{A}| = |E| - |A|$.

Démonstration. C'est une conséquence de la formule pour une union : E est union disjointe de A et de $\bar{A}$, donc $|E| = |A| + |\bar{A}|$. □

Proposition 14. Soient E et F deux ensembles finis, alors $E \times F$ est fini, et $|E \times F| = |E| \times |F|$.

Démonstration. C'est intuitivement évident en plaçant tous les éléments du produit cartésien dans un tableau :

	e_1	e_2	$\dots$	e_n
f_1	(e_1, f_1)	(e_2, f_1)	$\dots$	(e_n, f_1)
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
f_p	(e_1, f_p)	(e_2, f_p)	$\dots$	(e_n, f_p)

Pour une preuve rigoureuse, il faut constater que $\forall i \in \{1; \dots; n\}$, $F_p = \{e_i\} \times F$ a pour cardinal p (ce n'est pas difficile, il suffit d'envoyer (e_i, f_j) sur l'image de f_j par une bijection entre F et $\{1; \dots; p\}$. Ensuite, E est la réunion disjointe pour i variant entre 1 et n est ensembles précédents, donc $|E| = \sum_{i=1}^{i=n} p = np$. □

3.2 Listes, arrangements et combinaisons

Définition 12. Soit E un ensemble fini de cardinal n, et $p \in \mathbb{N}$. Une **p-liste** d'éléments de E, ou p-uplet d'éléments de E, est simplement un élément de E^p.

Remarque 16. On peut très bien avoir plusieurs fois le même élément dans une p-liste. Par ailleurs, l'ordre des éléments de la p-liste est important.

Proposition 15. Le nombre de p-listes dans un ensemble de cardinal n vaut n^p.

Démonstration. C'est une conséquence de la formule de cardinal du produit vue un peu plus haut : comme $|E \times F| = |E| \times |F|$, on a $|E^p| = |E|^p$, ce qui prouve bien la propriété. □

Définition 13. Soit E un ensemble à n éléments et $p \in \mathbb{N}$, on appelle **arrangement** de p éléments de E une p-liste d'éléments distincts de E.

Remarque 17. L'ordre des éléments est toujours important, par contre on ne peut plus avoir de répétition d'élément dans un arrangement.

Définition 14. Soient n et p deux entiers tels que $p \leqslant n$, on note $A_{n,p} = \dfrac{n!}{(n-p)!} = n(n-1)(n-2)\dots(n-p+1)$.

Proposition 16. Le nombre d'arrangements de p éléments dans un ensemble à n éléments vaut $A_{n,p}$.

Démonstration. Contentons-nous de l'idée intuitive : lorsqu'on construit un arrangement, on a n choix pour le premier élément, $n-1$ pour le deuxième, ..., $n-p+1$ pour le $p$ème, soit au total $n(n-1) \times (n-p+1) = \dfrac{n(n-1)\dots(n-p+1)(n-p)\dots 2 \times 1}{n(n-1)\dots 2 \times 1} = \dfrac{n!}{(n-p)!}$. □

Définition 15. Un arrangement de n éléments dans un ensemble à n éléments est aussi appelé **permutation**. Il y a donc $n!$ permutations dans un ensemble à n éléments.

Exemple 1 : Le nombre de façons d'asseoir 6 personnes autour d'une table ronde est $6! = 720$.

Exemple 2 : Le nombre d'anagrammes d'un mot peut se calculer à l'aide de permutations. Il faut simplement diviser le nombre total du permutations du mot par $k!$ chaque fois qu'une même lettre apparait k fois dans le mot (ainsi, s'il y a trois E dans le mot, on divise par $3!$ car les permutations qui se contentent d'échanger les E entre eux ne modifient pas l'anagramme). Par exemple, le nombre d'anagrammes du mot DENOMBREMENT est $\dfrac{12!}{3! \times 2! \times 2!}$.

Remarque 18. Le nombre de permutations d'un ensemble à n éléments est le nombre d'applications bijectives de cet ensemble dans lui-même.

Proposition 17. $\forall n \in \mathbb{N}$, $(n+1)! = n! \times (n+1)$

Pour les plus curieux, j'ajoute le résutat (hors programme) suivant, connu sous le nom de formule de Stirling : $\dfrac{n!}{\sqrt{2\pi n}(\frac{n}{e})^n} = 1$.

Définition 16. Une **combinaison** de p éléments dans un ensemble fini E à n éléments est un sous-ensemble à p éléments de E.

Définition 17. Soient n et p deux entiers tels que $p \leqslant n$, on appelle **coefficient binomial** d'indices n et p le nombre $\dbinom{n}{p} = \dfrac{n!}{p!(n-p)!}$. On le lit « p parmi n » (comme un raccourci signifiant que le nombre de façon de choisir p objets parmi n objets au total).

Remarque 19. On pose souvent $\dbinom{n}{p} = 0$ si $p > n$.

Proposition 18. Le nombre de sous-ensembles à p éléments d'un ensemble à n éléments est $\dbinom{n}{p}$.

Démonstration. En effet, une combinaison n'est rien d'autre qu'un arrangement dans lequel on a enlevé l'importance de l'ordre. Autrement dit, chaque combinaison apparait $p!$ fois quand on dénombre les arrangements (puisqu'il y a $p!$ façons d'ordonner un ensemble à p éléments), donc le nombre de combinaisons à p éléments vaut $\dfrac{A_{n,p}}{p!} = \dbinom{n}{p}$. □

Exemple : Les combinaisons apparaitront dans les calculs dès qu'on travaillera avec des tirages simultanés, c'est-à-dire quand l'ordre n'est pas important. Ainsi, le nombre de trinomes de colle différents qu'on peut constituer dans une classe de 45 élèves vaut $\dbinom{45}{3} = \dfrac{45 \times 44 \times 43}{3 \times 2 \times 1} = 14190$.

3.3 Propriétés des coefficients binomiaux

Proposition 19. Quelques propriétés des coefficients binomiaux, utiles pour les calculs :

- $\forall n \geqslant 2$, $\dbinom{n}{0} = 1$; $\dbinom{n}{1} = n$; $\dbinom{n}{2} = \dfrac{n(n-1)}{2}$.

- $\forall k \leqslant n$, $\binom{n}{k} = \binom{n}{n-k}$ (propriété de symétrie).
- $\forall 1 \leqslant k \leqslant n$, $k\binom{n}{k} = n\binom{n-1}{k-1}$.
- $\forall 1 \leqslant k \leqslant n$, $\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$ (relation de Pascal).

Démonstration. Pour le premier point, il suffit de reprendre la définition des coefficients binomiaux : $\binom{n}{0} = \dfrac{n!}{0!n!} = 1$; $\binom{n}{1} = \dfrac{n!}{(n-1)!} = n$ et $\binom{n}{2} = \dfrac{n!}{2!(n-2)!} = \dfrac{n(n-1)}{2}$.

La propriété de symétrie est facile aussi : $\binom{n}{n-k} = \dfrac{n!}{(n-k)!(n-(n-k))!} = \dfrac{n!}{(n-k)!k!} = \binom{n}{k}$. Il y a également une interprétation combinatoire de ce résultat : choisir un sous-ensemble de k éléments dans un ensemble à n éléments est équivalent à choisir son complémentaire, qui est constitué de $n-k$ éléments, donc il y a autant de sous-ensembles à k éléments et à $n-k$ éléments dans un ensemble à n éléments.

Pour la troisième, $k\binom{n}{k} = \dfrac{k \times n!}{k!(n-k)!} = \dfrac{n!}{(k-1)!(n-k)!}$, et $n\binom{n-1}{k-1} = \dfrac{n \times (n-1)!}{(k-1)!(n-1-k+1)!} = \dfrac{n!}{(k-1)!(n-k)!}$, les deux quantités sont bien égales.

Enfin, la formule de Pascal : $\binom{n-1}{k} + \binom{n-1}{k-1} = \dfrac{(n-1)!}{k!(n-1-k)!} + \dfrac{(n-1)!}{(k-1)!(n-k)!}$ $= \dfrac{(n-k) \times (n-1)! + k \times (n-1)!}{k!(n-k)!} = \dfrac{n \times (n-1)!}{k!(n-k)!} = \binom{n}{k}$. La encore, il y a une interprétation combinatoire. Soit E un ensemble à n éléments et x un élément fixé de E. Les sous-ensembles de E à k éléments, au nombre de $\binom{n}{k}$, se répartissent en deux catégories : ceux qui contiennent x, qui sont au nombre de $\binom{n-1}{k-1}$ puisqu'il reste $k-1$ éléments à choisir parmi les $n-1$ restants dans E une fois x choisi ; et ceux qui ne contiennent pas x, qui sont au nombre de $\binom{n-1}{k}$ puisqu'il reste cette fois-ci k éléments à choisir parmi les $n-1$ restants (on n'en a encore choisi aucun). D'où la formule. □

Triangle de Pascal : La relation de Pascal permet de calculer les valeurs des coefficients binomiaux par récurrence, en les répartissant sous forme d'un tableau triangulaire :

	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	$k=8$
$n=0$	1								
$n=1$	1	1							
$n=2$	1	2	1						
$n=3$	1	3	3	1					
$n=4$	1	4	6	4	1				
$n=5$	1	5	10	10	5	1			
$n=6$	1	6	15	20	15	6	1		
$n=7$	1	7	21	35	35	21	7	1	
$n=8$	1	8	28	56	56	56	28	7	1

Pour obtenir un coefficient du tableau, on fait la somme de celui qui est au-dessus de lui, et de celui qui est à gauche de celui-ci.

Théorème 3. Formule du binôme de Newton.
Soient a et b deux réels, et $n \in \mathbb{N}$, alors $(a+b)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

Remarque 20. On peut obtenir à partir de cette formule le développement d'une différence : $(b-a)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k a^k b^{n-k}$. En pratique, il suffit d'alterner les signes.

Exemple : $(a+b)^6 = a^6 + 6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 + b^6$. L'ordre est inversé par rapport à celui de la formule, mais c'est la façon habituelle d'écrire le développement. Autre exemple : $(1-2x)^5 = 1 - 5 \times 2x + 10 \times (2x)^2 - 10 \times (2x)^3 + 5 \times (2x)^4 - (2x)^5 = 1 - 10x + 40x^2 - 80x^3 + 80x^5 - 32x^5$.

Démonstration. On va procéder par récurrence sur l'entier n. Pour $n = 0$, la formule du binome dit simplement que $(a+b)^0 = \binom{0}{0} a^0 b^0$, ce qui est vrai (on a 1 de chaque côté). Supposons la formule vraie au rang n, on a alors $(a+b)^{n+1} = (a+b)(a+b)^n = (a+b) \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ par hypothèse de récurrence, donc en développant le $a+b$ et en le faisant rentrer dans la somme, on obtient $(a+b)^{n+1} = \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k}$. Effectuons un changement d'indice en remplaçant k par $k+1$ dans la première somme (on ne touche à rien dans la deuxième) : $(a+b)^{n+1} = \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} = \binom{n}{n} a^{n+1} b^0 + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k b^{n+1-k} + \binom{n}{0} a^0 b^{n+1}$ (on a isolé un terme dans chaque somme pour pouvoir regrouper les sommes). Maintenant, on reconnait la formule de Pascal dans la somme, donc $(a+b)^{n+1} = a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n+1-k} + b^{n+1}$. Il ne reste plus qu'à remettre les deux termes isolés dans la somme pour obtenir la formule au rang $n+1$, ce qu'on peut faire puisqu'ils sont justement égaux aux termes manquants pour $k = 0$ et $k = n+1$. □

Proposition 20. Soit E un ensemble fini de cardinal n. Alors $\mathcal{P}(E)$ est fini, de cardinal 2^n.

Démonstration. Le cardinal de $\mathcal{P}(E)$ est le nombre de sous-ensembles de E. Or, on sait que, pour tout entier k, il y a $\binom{n}{k}$ sous-ensembles de E à k éléments, ce qui fait au total $\sum_{k=0}^{n} \binom{n}{k}$ sous-ensembles. Cette somme n'est rien d'autre qu'un cas particulier de formule du binôme, pour $a = b = 1$, donc elle vaut $(1+1)^n = 2^n$.

Une façon plus combinatoire de voir les choses : choisir un sous-ensemble A de l'ensemble E revient à choisir, pour chaque élément de E, si celui-ci appartient à A ou non. On a ainsi deux possibilités pour chaque élément de E, ce qui fait au total 2^n possibilités pour construire le sous-ensemble A. Autre façon de décrire les choses pour les plus formalistes d'entre vous : pour chaque sous-ensemble A de E, on définit une application $\chi_A : E \to \{0;1\}$, telle que $\chi_A(x) = 1$ si $x \in A$, et $\chi_A(x) = 0$ si $x \notin A$ (cette application χ_A est appelée application caractéristique de l'ensemble A, car elle décrit les éléments appartenant à l'ensemble A). On peut prouver que toutes applications de E vers $\{0;1\}$ sont des applications caractéristiques d'un sous-ensemble de E, et que deux sous-ensembles distincts de E ont des applications caractéristiques différentes. Autrement dit, il y a une bijection entre $\mathcal{P}(E)$ et l'ensemble des applications de E dans $\{0;1\}$. Or, comme on l'a vu plus haut (après la définition des p-listes), il y a 2^n applications de E dans $\{0;1\}$. □