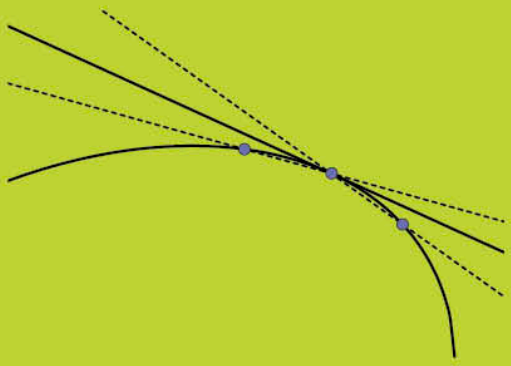
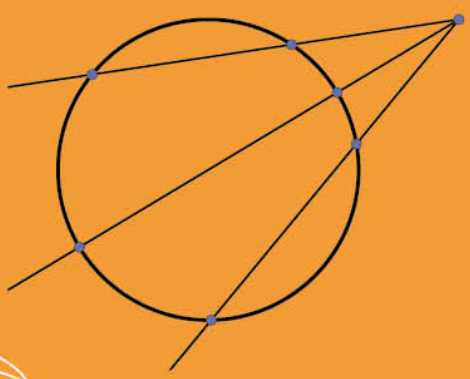


PREMIÈRE
SPÉCIALITÉ

LES MATHS EN PROFONDEUR

Fabien Besnard

- Cours développé
- Démonstrations
- Questions d'élèves
- Exercices corrigés



ellipses

Chapitre 1

Ensembles et applications

1.1 Préliminaires : symbole de sommation

Nous allons commencer ce chapitre en introduisant une notation qui sera très utile par la suite. On est souvent amené à considérer des sommes, comme par exemple :

$$S_n = 1^2 + 2^2 + 3^2 + \ldots + n^2. \tag{1.1}$$

On peut écrire cette somme de la façon suivante :

$$S_n = \sum_{k=1}^{n} k^2 \tag{1.2}$$

Le symbole $\sum$, qui est la lettre grecque sigma majuscule, se lit « somme », et k s'appelle *l'indice de sommation*. On voit que l'indice k va de 1 à n. Pour chacune de ces valeurs on ajoute k^2 au total de la somme, qui au départ vaut 0 par convention.

Cette notation fonctionne exactement comme l'algorithme suivant :
$S_0 = 0$,
Pour k allant de 1 à n faire : $S_n \leftarrow S_n + k^2$.

Je trouve quand même l'écriture (1.1) plus lisible.

C'est certain, mais la notation (1.2) a l'avantage d'être compacte, et permet certaines manipulations, comme les changements d'indices. Par exemple, la même somme peut s'écrire

$$S_n = \sum_{j=0}^{n-1} (j+1)^2 \tag{1.3}$$

En effet, on passe de (1.2) à (1.3) en posant $j = k - 1$. Lorsque k varie de 1 à n, j varie de 0 à $n - 1$, mais la somme reste le même. Remarquez que la lettre désignant l'indice de sommation n'a aucune importance en dehors de la somme, et

on pourrait très bien la réemployer dans une autre somme. On dit que c'est une *variable muette*[1]. On peut par exemple écrire :

$$T_n = \sum_{k=1}^{n} k^2 - \sum_{k=1}^{n} (k+1)^2 \tag{1.4}$$

Exercice 1.1.1 Montrer que T_n vaut $1-(n+1)^2$ en développant les sommes. Retrouver ce résultat à l'aide d'un changement d'indices.

Remarque 1.1.1 Au lieu d'écrire les bornes entre lesquelles varie l'indice de sommation, on peut écrire un encadrement pour k. Par exemple

$$S_n = \sum_{1 \leq k \leq n} k^2 \tag{1.5}$$

Cette façon d'écrire peut se généraliser en remplaçant l'encadrement par n'importe quelle condition portant sur k. Par exemple, la notation

$$R_n = \sum_{\substack{1 \leq k \leq n \\ k \text{ premier}}} k^2 \tag{1.6}$$

désigne la somme des carrés de tous les nombres premiers compris entre 1 et n.

Pour montrer l'intérêt du symbole de sommation (et aussi parce que c'est utile), démontrons l'identité remarquable suivante qui généralise « $a^2 - b^2$ ».

Théorème 1.1.1 *Pour tous réels a, b et tout entier $n \in \mathbb{N}^*$, on a*

$$a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-1-k} \tag{1.7}$$

Aïe, aïe, aïe, je ne comprends même pas l'énoncé !

Si c'est difficile à « décortiquer », donnez une valeur à n. Pour $n = 3$ vous devez obtenir $a^3 - b^3 = (a-b)(b^2 + ab + a^2)$. Vous vous habituerez très vite ! Passons à la démonstration.

Démonstration : On a

$$\begin{aligned}
(a-b) \sum_{k=0}^{n-1} a^k b^{n-1-k} &= \big(a \sum_{k=0}^{n-1} a^k b^{n-1-k}\big) - b \sum_{k=0}^{n-1} a^k b^{n-1-k} \\
&= \sum_{k=0}^{n-1} a^{k+1} b^{n-1-k} - \sum_{k=0}^{n-1} a^k b^{n-k} \\
&= a^n + \sum_{k=0}^{n-2} a^{k+1} b^{n-1-k} - b^n - \sum_{k=1}^{n-1} a^k b^{n-k}
\end{aligned}$$

1. C'est identique aux variables locales en informatique.

où, à la dernière étape, on a isolé le terme correspondant à $k = n-1$ dans la première somme et celui correspondant à $k = 0$ dans la seconde. Il ne reste plus qu'à démontrer que

$$\sum_{k=0}^{n-2} a^{k+1} b^{n-1-k} = \sum_{k=1}^{n-1} a^k b^{n-k} \tag{1.8}$$

Pour cela, posons $j = k-1$ dans la somme de droite. On obtient :

$$\sum_{k=1}^{n-1} a^k b^{n-k} = \sum_{j=0}^{n-2} a^{j+1} b^{n-j-1}$$

L'équation (1.8) est donc bien vérifiée, puisque k et j sont des variables muettes.□

Si vous n'avez rien compris à la démonstration précédente, pas d'inquiétude : respirez un grand coup et reprenez-la calmement, en développant toutes les sommes et en prenant une valeur pour n (par exemple $n = 4$). Puis relisez la démonstration : ça devrait s'éclairer.

Théorème 1.1.2 (Produit de deux sommes) *On a*

$$\Big(\sum_{i=1}^{n} a_i\Big)\Big(\sum_{j=1}^{m} b_j\Big) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j \tag{1.9}$$

Démonstration : La propriété à démontrer est en fait évidente, mais la démonstration sera l'occasion de travailler les factorisations dans les sommes. On a

$$\begin{aligned}\sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j &= \sum_{i=1}^{n} a_i \Big(\sum_{j=1}^{m} b_j\Big), \\ &= \Big(\sum_{i=1}^{n} a_i\Big)\Big(\sum_{j=1}^{m} b_j\Big)\end{aligned}$$

où on a factorisé : à la première étape par a_i (qui ne dépend pas de j) dans la somme $\displaystyle\sum_{j=1}^{m} a_i b_j$, et à la deuxième étape par $\displaystyle\sum_{j=1}^{m} b_j$ (qui ne dépend pas de i) dans la somme $\displaystyle\sum_{i=1}^{n} a_i \Big(\sum_{j=1}^{m} b_j\Big)$. □

On peut aussi développer les sommes pour démontrer (1.9) : à gauche on a $(a_1 + \ldots + a_n)(b_1 + \ldots + b_m)$, donc il est clair qu'en développant ce produit on obtiendra la somme de tous les produits du type $a_i b_j$ avec $1 \le i \le n$ et $1 \le j \le m$, c'est-à-dire exactement le membre de droite !

Exercice 1.1.2 Montrer que $(a_1+a_2+a_3)^2 = a_1^2+a_2^2+a_3^2+2a_1a_2+2a_2a_3+2a_1a_3$. Généraliser.

1.2 Principe de récurrence

Le principe de récurrence est un type de raisonnement fréquent, dont nous allons rapidement avoir besoin. Pour comprendre de quoi il s'agit, voyons un exemple.

Exemple 1.2.1 Soit x un réel positif et n un entier naturel. On veut montrer que

$$(1+x)^n \geq 1+nx \tag{1.10}$$

Notons cette inégalité P_n car elle dépend de n. On peut montrer sans difficulté que P_0, P_1, P_2 sont vraies (faites-le !). Cependant, on ne peut pas se contenter de ces exemples puisqu'on veut démontrer l'inégalité P_n pour tout entier n. Il existe bien une formule générale pour développer $(1+x)^n$ mais nous ne la connaissons pas encore... On peut cependant faire la remarque suivante : si on suppose que $(1+x)^n \geq 1+nx$ pour un certain entier n, alors en multipliant de part et d'autre par $1+x$ on ne change pas le sens de l'inégalité car $1+x>0$. On obtient donc $(1+x)^{n+1} \geq (1+nx)(1+x)$. Or $(1+nx)(1+x) = 1+(n+1)x+nx^2 \geq 1+(n+1)x$, puisque $nx^2 \geq 0$. On a donc démontré que si P_n est vraie, alors P_{n+1} aussi. Or on sait que déjà que P_2 est vraie, donc on en déduit que P_3 est vraie aussi, et par conséquent P_4, et ainsi de suite. Finalement P_n est vraie pour tout $n \in \mathbb{N}$.

L'exemple précédent peut être érigé en principe. Si on veut démontrer qu'une assertion P_n, dont la valeur de vérité dépend de l'entier $n \in \mathbb{N}$, est vraie pour tout $n \in \mathbb{N}$, on peut procéder ainsi :

1. On montre que P_0 est vraie (c'est l'initialisation).
2. On montre que pour tout $n \in \mathbb{N}$, l'implication $P_n \Rightarrow P_{n+1}$ est vraie (on dit qu'on prouve *l'hérédité* de P_n)

On peut alors conclure que P_n est vraie pour tout $n \in \mathbb{N}$, et on dit qu'on l'a démontrée par *récurrence sur n*.

Quand on montre que $P_n \Rightarrow P_{n+1}$, est-ce qu'on ne suppose pas déjà que P_n est vraie ? Autrement dit, on suppose ce que l'on doit démontrer...

Non, et c'est très important de le comprendre ! Ce qu'on démontre dans la partie « hérédité », c'est une chaîne infinie d'implications :

$$P_0 \Rightarrow P_1 \Rightarrow P_2 \Rightarrow P_3 \Rightarrow \dots \tag{1.11}$$

Or, rappelez-vous du cours de seconde, l'implication $A \Rightarrow B$ est toujours vraie quand A est fausse ! Pour démontrer l'implication $P_n \Rightarrow P_{n+1}$ on peut donc supposer que P_n est vraie (on dit que c'est *l'hypothèse de récurrence*), c'est rendu très clairement par les mots « montrons que si P_n est vraie alors P_{n+1} est vraie ». Mais la conclusion de cette étape n'est pas que P_n est vraie ! C'est seulement que la chaîne d'implications (1.11) est vraie.

Et cette chaîne peut être vraie sans que P_n le soit ?

Absolument. Prenons l'exemple de la propriété suivante :

$$P_n \ : \ n = n + 1 \tag{1.12}$$

Il est clair que P_n est fausse pour tout $n \in \mathbb{N}$. Pourtant, il suffit d'ajouter 1 de chaque côté pour passer de P_n à P_{n+1}. Ainsi l'implication $P_n \Rightarrow P_{n+1}$ est vraie pout tout n, mais P_n est fausse pour tout n! Cela montre bien l'importance de la phase d'initialisation. Bien sûr, on n'est pas obligé d'initialiser à $n = 0$: si P_0 est fausse mais que P_1 est vraie et que la propriété P_n est héréditaire, alors elle sera vraie pour tout $n \geq 1$. Notons enfin qu'il existe une variante de la propriété d'hérédité : au lieu de montrer que $P_n \Rightarrow P_{n+1}$, on peut montrer que (P_0 et P_1 et ... et P_n) $\Rightarrow P_{n+1}$.

Le principe de récurrence semble logique. Mais peut-on le démontrer ?

Oui, et on peut donc en faire un théorème.

Théorème 1.2.1 *Soit P_n une assertion dépendant de n et telle que :*

1. *P_0 est vraie,*
2. *$\forall n \in \mathbb{N}$, $P_n \Rightarrow P_{n+1}$.*

Alors $\forall n \in \mathbb{N}$, P_n est vraie.

Démonstration : Soit $F = \{n \in \mathbb{N} | P_n \text{ est fausse }\}$. Un entier n appartient donc à F ssi P_n est fausse. Le but est de montrer que F est vide. Supposons que F soit non vide. Alors, d'après le théorème I-3.4.3, F possède un plus petit élément n_0. Comme P_0 est vraie, on a $n_0 \geq 1$. Ainsi $n_0 - 1 \in \mathbb{N}$. Donc $P_{n_0-1} \Rightarrow P_{n_0}$ est vraie, et comme P_{n_0} est fausse, il en résulte que P_{n_0-1} est fausse. Donc $n_0 - 1 \in F$, or c'est absurde car n_0 est le plus petit élément de F. Donc F est vide. □

Remarque 1.2.1 Il ne faut pas faire tout un plat du principe de récurrence. Comme le montre la démonstration du théorème 1.2.1, ce n'est qu'un corollaire du théorème, admis en seconde, qui stipule que tout sous-ensemble non vide de $\mathbb{N}$ possède un plus petit élément (théorème I-3.4.3). Il est d'ailleurs parfois nécessaire d'utiliser directement ce théorème, lorsque la propriété que l'on souhaite démontrer ne se prête pas à une récurrence : on raisonne par l'absurde en considérant le plus petit entier ne vérifiant pas la propriété. C'est ainsi que nous avons démontré au théorème I-3.1.5, en suivant Euclide, qu'il existe une infinité de nombres premiers.

Exercice 1.2.1 Démontrer que pour tout entier $n \geq 3$, on a $\left(\frac{1}{1+\frac{1}{n}}\right)^n \geq \frac{1}{n}$. En déduire que $n^{n+1} \geq (n+1)^n$ pour tout entier $n \geq 3$.

1.3 Ensemble des parties

Dans le livre de seconde, nous avons présenté une version simplifiée de la théorie des ensembles, et introduit les opérations d'intersection, d'union, etc. Ce paragraphe, très court, complète cette présentation avec une dernière opération.
Soit E un ensemble. L'un des axiomes de la théorie des ensembles nous autorise à construire l'ensemble de ses parties, c'est-à-dire l'ensemble de ses sous-ensembles.

On note $\mathcal{P}(E)$ l'ensemble des parties (i.e. sous-ensembles) de E. On a donc par définition, et pour tout ensemble X :

$$X \subset E \Leftrightarrow X \in \mathcal{P}(E) \tag{1.13}$$

Le vide étant inclus dans tout ensemble, c'est toujours un élément de $\mathcal{P}(E)$, quel que soit E.

Exemple 1.3.1 $E = \{1; 2\}$. $\mathcal{P}(E) = \{\emptyset; \{1\}; \{2\}; E\}$.

Exercice 1.3.1 Soient A et B deux points sur la droite d. Parmi les assertions suivantes, lesquelles sont vraies ? $[AB] \subset \mathcal{P}(d)$, $[AB] \in \mathcal{P}(d)$, $[AB] \in d$, $[AB] \subset d$.

1.4 Dénombrements

Dans cette section, E et F sont des ensembles finis. On rappelle que le *cardinal* de E, noté $|E|$, désigne le nombre d'éléments de E. Les *dénombrements* sont la partie des mathématiques qui consiste à compter (dénombrer) les éléments de certains ensembles finis. On utilise les dénombrements dans le calculs des probabilités, ainsi que pour mesurer la complexité de certains algorithmes. Nous allons donner cette année les éléments de base permettant de mener à bien ces calculs. Nous connaissons déjà le premier, que nous avons vu dans le cours de seconde.

Théorème 1.4.1 *On a* $|E \cup F| = |E| + |F| - |E \cap F|$.

Démonstration : Voir exercice I-11.2.9. □

Remarque 1.4.1 Ce théorème admet une généralisation, nommée « formule du crible ». Voir exercice 5.1.21.

Le second est évident : le nombre de couples $(x; y)$ avec $x \in E$ et $y \in F$, c'est-à-dire le nombre d'éléments du produit cartésien $E \times F$, est égal au cardinal de E multiplié par celui de F. On peut généraliser sans problème ce principe aux multiplets, et on obtient :

Théorème 1.4.2 *Soit* $k \in \mathbb{N}^*$*, et soient* $E_1, \dots E_k$ *des ensembles finis. Alors* $|E_1 \times \dots \times E_k| = |E_1| \times \dots \times |E_k|$*. En particulier, on a* $|E^k| = |E|^k$*.*

Ce résultat simple nous permet de dénombrer les applications d'un ensemble fini dans un autre.

Théorème 1.4.3 (Nombre d'applications) *Si* $|E| = p$ *et* $|F| = n$*, alors il y a* n^p *applications de* E *dans* F*.*

Démonstration : Notons $e_1, \dots, e_p$ les différents éléments de E. Définir une application f de E dans F, revient à donner le p-uplet $(f(e_1), \dots, f(e_p))$. Or il y a $|F^p| = n^p$ tels p-uplets. □

Remarque 1.4.2 À cause de ce théorème, les mathématiciens ont inventé la notation F^E pour l'ensemble des applications de E dans F. Cette notation s'étend aux ensembles infinis. Par exemple $\mathbb{R}^{\mathbb{N}}$ est l'ensemble de toutes les applications de $\mathbb{N}$ dans $\mathbb{R}$.

Le nombre d'applications intervient dans chaque situation où l'on choisi des objets dans un certain ordre parmi une collection finie, sans les éliminer de la collection quand on les choisit (pioche avec remise). Par exemple, si on veut former des mots de 5 lettres (ayant un sens ou non) avec l'alphabet latin, il faut choisir la première lettre parmi 26, la deuxième lettre parmi 26, etc. Cela revient à définir une application de l'ensemble $E = \{1; 2; 3; 4; 5\}$ dans l'alphabet, qui est un ensemble F de cardinal 26. Il y a donc 26^5 façons de s'y prendre.
Pour énoncer le théorème suivant, il faut introduire une notation.

Définition 1.4.1 *Soit $n \in \mathbb{N}^*$. On note $n!$ le produit de tous les entiers de 1 jusqu'à n, c'est-à-dire le nombre*

$$n! = 1 \times 2 \times \ldots \times n$$

Si $n = 0$ on pose $0! = 1$.

Le nombre $n!$ se lit « n factorielle » ou « factorielle n ». C'est un nombre qui devient rapidement gigantesque. Par exemple, 100! s'écrit avec 158 chiffres !

Théorème 1.4.4 (Nombre d'injections) *Si $|E| = p$ et $|F| = n$ avec $p \leq n$, alors il y a $\dfrac{n!}{(n-p)!}$ applications injectives de E dans F.*

C'est quoi déjà une application injective ?

C'est une application telle que les images des éléments de l'ensemble de départ soient toutes différentes. Pour plus de détails, voir le paragraphe I-7.1.4.

Démonstration : Comme dans la démonstration du théorème 1.4.3, définir f revient à choisir $(f(e_1), \ldots, f(e_p))$. La seule différence est que $f(e_2)$ ne peut pas être égal à $f(e_1)$: il y a donc seulement $n-1$ choix pour $f(e_2)$. De même $f(e_3)$ ne peut être égal ni à $f(e_1)$ ni à $f(e_2)$: il reste donc $n-2$ possibilités, et ainsi de suite. Au final il y a $n \times (n-1) \times \ldots (n-p+1) = \dfrac{n!}{(n-p)!}$ possibilités pour l'application f. □

Le nombre d'injections intervient lorsqu'on pioche sans remise des objets distincts et que l'ordre est important. Supposons par exemple qu'on dispose de 9 cartons portant les chiffres de 1 à 9. Combien de nombres de 3 chiffres différents peut-on écrire avec ces cartons ? On pioche trois cartons qu'on dispose de gauche à droite : cela revient à choisir une injection de l'ensemble $\{1; 2; 3\}$ (représentant les 1re, 2e et 3e places) dans l'ensemble $\{1; 2; \ldots; 9\}$. La réponse est donc $\dfrac{9!}{6!} = 9 \times 8 \times 7$ nombres différents en tout.

Pourquoi doit-on supposer $p \leq n$ dans l'énoncé du théorème 1.4.4 ?

Exercice 1.4.1 Répondez à la question de Natacha !

Un cas particulier du théorème 1.4.4 mérite qu'on s'y attarde : lorsque $n = p$, une injection de E dans F est nécessairement une bijection. En effet, les images

$f(e_1), \ldots, f(e_n)$ étant toutes distinctes, il y a en n, donc tous les éléments de F sont des images, et f est ainsi surjective. L'application du théorème 1.4.4 fournit donc le corollaire suivant.

Corollaire 1.4.5 (Nombre de bijections) *Soit $n \in \mathbb{N}$. Il y a $n!$ bijections d'un ensemble à n éléments dans un ensemble à n éléments.*

Notons qu'une bijection d'un ensemble dans lui-même est appelé une *permutation*. Il y a donc $n!$ permutations d'un ensemble à n éléments.
Le nombre de bijections est aussi le nombre de façons d'ordonner des objets distincts. En effet, ordonner n objets c'est décider lequel sera le numéro 1, lequel sera le numéro 2, etc. C'est donc réaliser une bijection de l'ensemble de ces n objets sur l'ensemble $\{1; 2; \ldots; n\}$.

Exercice 1.4.2 Combien y a-t-il d'anagrammes (ayant ou non un sens) du mot « surjection » ?

Posons-nous maintenant la question suivante : combien y a-t-il de façons de choisir p objets parmi n sans tenir compte de l'ordre ? On peut par exemple se demander combien il y a de mains différentes de 5 cartes prises parmi un jeu de 32. On peut compter les injections de $\{1; \ldots; 5\}$ dans l'ensemble C des cartes, mais on tient alors compte de l'ordre (on a la carte numéro 1, la numéro 2, etc.). La question devient alors : combien de fois a-t-on compté la même main ?


5! fois, puisqu'il y a 5! façons d'ordonner 5 objets !

Il y a donc en tout...


$\frac{32!}{(32-5)!}$ divisé par 5!, soit $\frac{32!}{27!5!}$ mains de 5 cartes différentes !

Et plus généralement, si on prend p objets distincts parmi n, on a $\frac{n!}{(n-p)!}$ façons de le faire en tenant compte de l'ordre, nombre qu'il faut diviser par les $p!$ façons d'ordonner les p objets. On obtient ainsi qu'il y a $\frac{n!}{(n-p)!p!}$ façons de choisir p objets distincts mais non ordonnées pris parmi n objets. On peut redire ça de la façon suivante :

Théorème 1.4.6 *On pose $|E| = n$ et $p \in \mathbb{N}$. On note $\binom{n}{p}$ le nombre de sous-ensembles de E à p éléments. Alors on a*

$$\binom{n}{p} = \frac{n!}{p!(n-p)!} \tag{1.14}$$


On ne devrait pas dire que $p \leq n$ dans la formule (1.14) ?

Si, vous avez raison. Si $p > n$ il n'y a pas de sous-ensemble à p éléments dans E, donc dans ce cas $\binom{n}{p}$ vaut 0 par définition.
Les nombres $\binom{n}{p}$ sont appelés *coefficients binomiaux* en raison d'une application extrêmement importante que nous allons maintenant voir. Il s'agit de généraliser