Chapitre 4 : Ensembles

PTSI B Lycée Eiffel

15 octobre 2013

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 sur le principe de récurrence et ses variantes qui contiendra également en guise d'application des calculs de sommes et de produits ; une petite partie consacrée aux rudiments de l'arithmétique ; et une partie théorique sur les notions d'applications injective et sujective, permettant de vraiment comprendre la notion essentielle en mathématiques de bijection. 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 chapîtres d'algèbre et d'analyse que nous aborderons ensuite.

Objectifs du chapitre :

- 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
- maîtriser les notions d'application injective et surjective, y compris pour des applications autres que celles de $\mathbb{R}$ dans $\mathbb{R}$

1 Récurrence, sommes et produits

1.1 Compléments sur les ensembles

Définition 1. 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 2. 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 Démonstration par récurrence

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

Remarque 4. Ce résultat fondamental pour la structure de l'ensemble $\mathbb{N}$ est plus un axiome qu'un réel théorème.

Proposition 1. 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 5. 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.

1.3 Sommes classiques

Définition 3. 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 6.

- 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 2. 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 7. 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 3. 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.

□

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 :
$\sum_{1 \leqslant j \leqslant i \leqslant n} 3j = 3\sum_{i=1}^{i=n} \sum_{j=1}^{j=i} = 3\sum_{i=1}^{i=n} \frac{i(i+1)}{2} = \frac{3}{2}\sum_{i=1}^{i=n} i^2 + i = \frac{3}{2}\left(\frac{n(n+1)(2n+1)}{6} + \frac{n(n+1)}{2}\right) = \frac{n(n+1)(2n+1)+3n(n+1)}{4} = \frac{(n+1)(2n^2+n+3n)}{4} = \frac{n(n+1)(n+2)}{2}$.

1.4 Produits

Définition 4. 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 5. On appelle **factorielle** de l'entier naturel n, et on note $n!$, le nombre $n! = \prod_{i=1}^{i=n} i$.

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

Proposition 4. 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 8. 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. $P = \prod_{i=1}^{i=n} 3i = \prod_{i=1}^{i=n} 3 \times \prod_{i=1}^{i=n} i = 3^n n!$

2 Arithmétique

Définition 6. Soient n et p deux entiers relatifs, n est **divisible par** p (ou p divise n) s'il existe un troisième entier k tel que $n = kp$.

Remarque 9. La relation de divisibilité est une relation d'ordre sur $\mathbb{N}^*$ mais pas sur $\mathbb{Z}^*$, où elle n'est pas pas antisymétrique. En effet, deux entiers relatifs qui se divisent l'un l'autre sont soit égaux soit opposés.

Théorème 2. Division euclidienne.
Soit $n \in \mathbb{Z}$ et $p \in \mathbb{N}^*$, alors il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $n = pq + r$, et $0 \leqslant r < p$. L'entier q est appelé **quotient** de la division euclidienne de n par p, et l'entier r **reste** de cette même division.

Exemple : Pour effectuer en pratique une division euclidienne, on peut revenir à ses classiques du primaire en posant la division (et en s'arrêtant avant d'obtenir un quotient décimal). Ainsi, on aura par exemple $207 = 14 \times 14 + 11$.

Démonstration. Commençons par prouver l'existence du couple (q, r), en supposant $n > 0$ (sinon, ce n'est pas beaucoup plus compliqué). Comme $\mathbb{R}$ est archimédien, il existe certainement un entier a à partir duquel $ap > n$, notons donc $q = \max\{a \in \mathbb{N} \mid ap \leqslant n\}$, et $r = n - pq$. Par définition, $pq \leqslant n$, donc $r \geqslant 0$. De plus, par maximalité de q, on doit avoir $(q+1)p > n$, soit $pq + p - n > 0$, ou encore $p > n - pq = r$. Enfin, par définition de r, $n = pq + r$, l'existence du couple est donc prouvée.

Démontrons désormais l'unicité en supposant comme d'habitude qu'il y a deux couples convenables (q, r) et (q', r'). On a alors $pq + r = pq' + r' = n$, donc $p(q - q') = r' - r$. En particulier $r' - r$ divise p, alors que $-p < r' - r < p$. Ce n'est possible que si $r' - r = 0$, soit $r' = r$, ce qui implique $p(q' - q) = 0$, donc $q = q'$. Les deux couples sont alors identiques. □

Définition 7. Soit n et p deux entiers naturels non nuls. Le **plus grand commun diviseur** (ou pgcd) de n et p est, comme son nom l'indique, le plus grand entier divisant simultanément n et p. On le note parfois $n \wedge p$. Le **plus petit commun multiple** (ou ppcm) est le plus petit entier naturel que divisent n et p.

Proposition 5. Quels que soient les nombres entiers n et p, le produit du pgcd et du ppcm de n et de p est égal à np.

Définition 8. Un entier naturel n est **premier** s'il n'est divisible que par 1 et par lui-même. Deux entiers n et p sont premiers entre eux si leu pgcd est égal à 1.

Remarque 10. Par convention, le nombre 1 n'est pas considéré comme un nombre premier.

Remarque 11. Il n'existe pas de méthode extrêmement simple pour savoir si un entier donné est premier ou non. Pour faire la liste des nombres premiers inférieurs à un entier donné, le plus simple est encore d'utiliser le **crible d'Eratosthène** : on place dans un tableau tous les entiers inférieurs à n (à partir de 2), et à chaque étape on garde le plus petit entier disponible (qui sera nécessairement prémier), et on raye tous ses multiples.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Les nombres restants : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 et 97 sont tous premiers. il y a donc 25 nombres premiers inférieurs ou égaux à 100. On peut démontrer plus généralement (mais c'est très compliqué) que le nombre de nombres premiers inférieurs à n devient proche de $\ln(n)$ (c'est-à-dire que le quotient des deux tend vers 1), lorsque n tend vers $+\infty$.

Théorème 3. Théorème de Bezout.
Deux entiers n et p sont premiers entre eux si et seulement s'il existe un couple d'entiers $(a, b) \in \mathbb{Z}^2$ tels que $an + bp = 1$. Plus généralement, il existe toujours un couple d'entiers relatifs tels que $an + bp = n \wedge p$.

Démonstration. Ce théorème étant à la lisière du programme, on ne démontrera que la deuxième partie. Les deux entiers n et p engendrent dans $\mathbb{Z}$ les sous-groupes $n\mathbb{Z}$ et $p\mathbb{Z}$. Le sous-groupe G engendré par n et p est quant à lui composé de tous les entiers de la forme $an + bp$, pour a et b parcourant $\mathbb{Z}$ (en effet, un sous-groupe contenant n et p contient nécessairement tout ces éléments puisqu'il eststable par somme, et cet ensemble est bien un sous-groupe de $\mathbb{Z}$). Or, c'est un sous-groupe de $\mathbb{Z}$, donc il est de la forme $k\mathbb{Z}$. Comme $n \in G$ et $p \in G$, les deux entiers n et p sont divisibles par k, qui divise donc nécessairement le pgcd de n et p. Autrement dit, $n \wedge p \in G$, ce qui prouve l'existence de deux entiers tels que $an + bp = n \wedge p$. □

Théorème 4. Il existe une infinité de nombres premiers.

Démonstration. On va un tout petit peu anticiper sur le dernier résultat du paragraphe. Faisons un raisonnement par l'absurde : il existerait donc une liste finie p_1, p_2, …, p_k de nombres premiers. Notons alors $p = \prod_{i=1}^{k} p_i + 1$. Cet entier n'est sûrement pas divisible par p_1 (puisque l'entier qui le précède l'est et que $p_1 \geqslant 2$), ni par aucun des p_i. Soit il est lui-même premier (mais distinct des autres, ce qui est absurde), soit il est divisible par un entier premier (c'est là qu'on utilise la décomposition), qui n'est lui-même aucun des p_i. Dans tous les cas, on aboutit à une contradiction. □

Théorème 5. Décomposition en facteurs premiers.
Tout nombre entier $n \geqslant 2$ peut se décomposer de façon unique à l'ordre des facteurs près sous la forme $n = \prod_{i=1}^{i=k} p_i^{\alpha_i} = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$, où p_1, p_2, …, p_k sont des nombres premiers, et $(\alpha_1, \ldots, \alpha_k) \in (\mathbb{N}^*)^k$.

Démonstration. La démonstration de ce théorème n'est pas au programme, on va s'en dispenser. On peut la faire par récurrence, mais c'est un peu technique. □

Exemple : La décomposition du nombre 384 est $2^7 \times 3$ (il suffit de diviser par 2 jusqu'à ce que ce ne soit plus possible, de recommencer avec 3, etc), et celle de 660 est $2^2 \times 3 \times 5 \times 11$. Il est assez facile ensuite de calculer le pgcd et le ppcm. Pour le pgcd, il suffit d'élever chaque facteur premier apparaissant à la fois dans la décomposition de n et de p à la puissance égale au minimum des puissances des deux décompositions. Ici, $384 \wedge 660 = 2^2 \times 3 = 12$. Ensuite, le ppcm est égal au produit des deux entiers divisé par le pgcd, ou au produit des facteurs premiers apparaissant dans au moins une des deux décompositions, élevés à la puissance égale au maximum des deux puissances. Ici, $\text{ppcm}(384, 660) = 2^7 \times 3 \times 5 \times 11 = \dfrac{34 \times 660}{12} = 21\ 120$.

3 Applications

3.1 Définitions

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 9. 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 12. 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.

Remarque 13. L'ensemble de toutes les application de E dans F peut être noté F^E. Ainsi, la notation $\mathbb{R}^{\mathbb{N}}$ désigne l'ensemble de toutes les suites réelles.

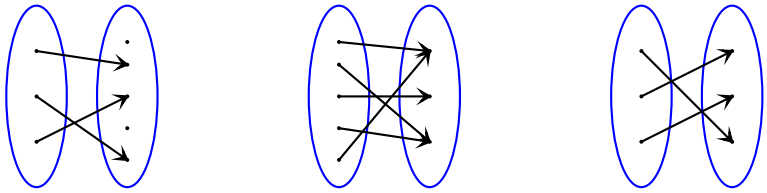
Définition 10. Soit $f : E \to F$ une application et E' un sous-ensemble de E. L'application $g : E' \to F$ définie par $\forall x \in E'$, $g(x) = f(x)$ est appelée **restriction** de f au sous-ensemble E' et notée $f_{|E'}$. On dit egalement que f est un **prolongement** de g à E.

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 11. Soit $A \subset E$, la **fonction caractéristique** du sous-ensemble A est l'application $\mathbb{1}_A : E \to \{0, 1\}$ définie par $\mathbb{1}_A(x) = 1$ si $x \in A$ et $\mathbb{1}_A(x) = 0$ si $x \notin A$.

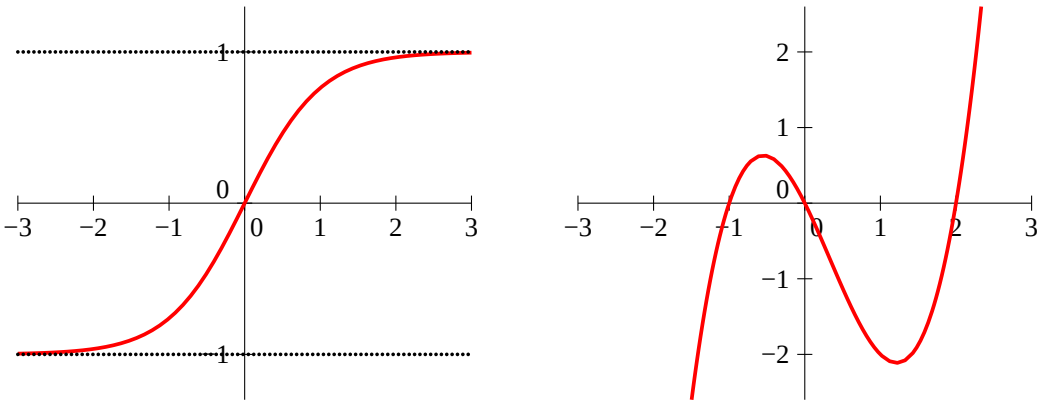
3.2 Injections, surjections, bijections

Définition 12. 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 $\qquad$ f surjective $\qquad$ 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 14. 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 6. 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 15. La réciproque de ces propriétés est totalement fausse, voir la feuille d'exercices pour quelques exemples.

Proposition 7. 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 16. 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 $\frac{1}{f}$. 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 17. 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 $g : x \mapsto \frac{1}{3}x - 2$. En effet, $g \circ f(x) = \frac{1}{3}(3x+6) - 2 = x$ et $f \circ g(x) = 3\left(\frac{1}{3}x - 2\right) + 6 = x$.

Proposition 8. 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 13. 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 18. 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 $f([2;5]) = [4;25]$; $f([-1;3]) = [0;9]$; $f^{-1}([4;9]) = [-3;-2] \cup [2;3]$.

Proposition 9. L'application $\varphi : \left\{ \begin{array}{ccc} \mathcal{P}(E) & \to & \{0,1\}^E \\ A & \mapsto & \mathbb{1}_A \end{array} \right.$ est une bijection.

Démonstration. Cette propriété explique bien le nom de fonction caractéristique puisqu'il s'agit de caractériser un sous-ensemble de E par une application de E dans $\{0,1\}$. En particulier, elle explique pourquoi, dans le cas d'un ensemble fini E à n éléments, $\mathcal{P}(E)$ contiendra 2^n éléments. Prouvons séparément l'injectivité et la surjectivité :

- prouver l'injectivité revient, par contraposée, à prouver que $A \neq B \Rightarrow \mathbb{1}_1 \neq \mathbb{1}_B$. Dire que $A \neq B$ revient à dire qu'il existe un élément x appartenant à A mais pas à B (ou le contraire, les conséquences étant complètement symétriques). On a alors, par définition de la fonction caractéristique, $\mathbb{1}_A(x) = 1$ et $\mathbb{1}_B(x) = 0$, ce qui implique certainement que $\mathbb{1}_A \neq \mathbb{1}_B$.
- choisissons maintenant une application f de E dans $\{0,1\}$ quelconque et notons $A = f^{-1}(\{1\})$. Par définition, on a donc, $\forall x \in A$, $f(x) = 1$, et $\forall x \notin A$, $f(x) \neq 1$, c'est-à-dire $f(x) = 0$ puisque f ne prend que les valeurs 0 et 1. Autrement dit, $f = \mathbb{1}_A$, et f admet donc l'ensemble A comme antécédent par l'application φ, qui est bien surjective.

□

3.3 Relations d'équivalence

Nous avons déjà étudié il y a quelques semaines les relations d'ordre sur un ensemble, dont le but est en gros de classer les éléments d'un ensemble. Les relations d'équivalence procèdent sur le même principe, mais en tentant de regrouper les éléments en paquets d'élements « qui se ressemblent ».

Définition 14. Une **relation d'équivalence** R sur un ensemble E est :

- réflexive : $\forall x \in E$, xRx
- symétrique : $\forall (x,y) \in E^2$, $xRy \Leftrightarrow yRx$.
- transitive : $\forall (x,y,z) \in E^3$, xRy et yRZ impliquent xRz.

Exemple : La relation d'équivalence la plus simple possible sur un ensemble quelconque E est la relation d'égalité (mais elle ne présente aucun intérêt !). Quelques exemples moins triviaux :

- la relation de congruence modulo 2π sur $\mathbb{R}$ (qui consiste à identifier les réels correspondant au même point sur le cercle trigonométrique)
- la relation de parallélisme sur l'ensemble de toutes les droites du plan (en considérant deux droites confondues comme parallèles).

Définition 15. Soit $x \in E$ et R une relation d'équivalence sur E, la **classe d'équivalence** de x pour la relation R est l'ensemble $C_x = \{y \in E \mid xRy\}$.

Définition 16. Soit E un ensemble, une liste de sous-ensembles $(A_1, A_2, \ldots, A_n)$ de E forme une **partition** de E si :

- $\forall (i,j) \in \{1,n\}^2$, $i \neq j \Rightarrow A_i \cap A_j = \emptyset$.
- $\bigcup_{i=1}^{n} A_i = E$.

Remarque 19. Autrement dit, tout élément $x \in E$ appartient à exactement un des sous-ensembles A_i. Cette notion de partition est essentielle en probabilités, comme nous le verrons en fin d'année.

Proposition 10. Si R est une relation sur E, l'ensemble des classes d'équivalence de R forme une partition de l'ensemble E.

Démonstration. En effet, supposons que deux classes C_x et C_y ne soient pas disjointes, il existe donc un z tel que xRz et zRy, ce qui implique par transitivité que xRy. Les classes d'équivalence de x et de y sont alors les mêmes. Par ailleurs, tout élement de E appartient certainement à une classe d'équivalence : la sienne ! □

Exemples : Pour la relation de parallélisme sur l'ensemble des droites du plan, la classe d'équivalence d'une droite donnée est constituée de toutes les droites du plan qui lui sont parallèles. On l'appelle **direction** de la droite.
La relation définie sur $\mathbb{C}$ par xRy si $|x| = |y|$ est une relation d'équivalence, et ses classes d'équivalence sont, dans le plan complexe, tous les cercles concentriques centrés en l'origine du repère.