

Mathématiques discrètes, 1ère année

Laurent Regnier

25 octobre 2010

Chapitre 1

Étudier les mathématiques

Comment doit on apprendre les mathématiques? Il n'y a évidemment pas une réponse unique mais voici quelques pistes (qui du reste ne sont pas propres aux mathématiques, mais valables pour toutes les disciplines).

Faire les exercices. Les mathématiques sont abstraites et difficiles. Il est très important de se familiariser avec les objets, les définitions, les démonstrations pour se les approprier et se tester soi-même : dominer les mathématiques et ne pas se laisser dominer. La technique la plus efficace pour cela est de faire des exercices. On en trouve toujours, dans le cours, dans les livres, dans les annales d'examens...

Les exercices doivent être *préparés*, c'est à dire que l'on doit passer un certain temps à chercher la solution, mais il n'est pas nécessaire de la trouver toujours. Il est par contre extrêmement utile de *faire des erreurs et de les comprendre*, c'est pourquoi les exercices doivent être discutés avec d'autres, les différentes solutions trouvées doivent être comparées et corrigées.

Ce cours est divisé en séances de cours magistral (souvent en amphi) et séances de TD (en groupes plus restreints). L'enseignant chargé de TD fournit chaque semaine la liste des exos à traiter pour la semaine suivante. Les exercices *doivent tous avoir été préparés avant la séance*, le TD consiste à discuter et corriger les solutions trouvées, à répondre aux éventuelles questions sur le cours, et à approfondir certains points du cours.

Apprendre son cours. En mathématiques apprendre le cours est souvent synonyme de le comprendre. En effet lorsque l'on a bien compris on peut reconstruire tout le cours, même si on a tout oublié. Les formules trigonométriques sont un excellent exemple de cela : si on a bien compris la formule de Moivre $e^{ix} = \cos x + i \sin x$, on peut toutes les retrouver facilement.

Il est donc rare que l'on doive apprendre par cœur. La manière la plus simple de comprendre son cours est de sortir de séance en ayant tout compris! Pour cela *il faut être concentré pendant le cours*, les mathématiques comme toutes les disciplines de la pensée, demandent beaucoup de concentration (le cerveau étant l'organe du corps humain qui consomme le plus de calories, on peut considérer que la concentration en cours est un sport).

Il est plus important de comprendre pendant le cours, que de prendre des notes. Donc si on commence à se sentir dépassé, on cesse de prendre des notes pour se concentrer sur ce que dit le ou la prof. On pourra toujours soit récupérer les notes d'un camarade, soit relire le poly, soit trouver un livre.

Un principe important : ne jamais croire ce que dit le ou la prof, on ne croit que ce que l'on comprend. Ne pas hésiter à poser des questions en cours lorsque l'on commence à ne pas comprendre.

Lorsque le cours est bien compris on peut passer directement aux exercices; de toute façon on le relira en faisant les exos car il y a *toujours* des points que l'on a mal assimilés ou oubliés; d'où l'importance de faire des exos. Autrement dit faire les exos est la 2ème méthode la plus efficace pour apprendre son cours.

Travailler à plusieurs. C'est une bonne manière de se motiver à travailler. Idéalement on travaille à 2 ou 3. Si on n'ose pas aller vers les autres, on peut demander au chargé de TD d'organiser des binômes.

La troisième méthode la plus efficace pour apprendre son cours c'est de le refaire à un camarade. Si on a tout compris on trouve quelqu'un qui n'a rien compris et on lui explique tout (et réciproquement). C'est un exercice qui sera autant bénéfique à l'un qu'à l'autre.

Le cas le plus fréquent toutefois est quand on n'a pas tout compris, mais pas rien non plus. Se mettre à deux ou trois est alors excellent car ce ne sont souvent pas les mêmes choses sur lesquelles les uns et les autres butent.

De même pour préparer les exos avant les séances de TD, le mieux est de les faire à plusieurs. D'abord ça motive.

Même si on pense ne pas avoir besoin d'aide pour y arriver, il est excellent d'expliquer les solutions que l'on a trouvées à ses camarades. Et par contre il ne faut jamais croire que l'on est trop nul pour travailler avec d'autres. L'expérience montre que souvent un étudiant très fort s'associe avec un étudiant très faible, pour le plus grand bénéfice des deux.

Interagir avec les enseignants. Il faut savoir que les enseignants sont en général heureux que l'on pose des questions : cela signifie que l'on s'intéresse, cela leur donne un retour sur la manière dont leur cours est reçu, ça met de la vie... Par vocation un mathématicien aime parler de mathématiques donc si on lui en donne l'occasion il sera intarissable (trop peut-être).

Donc ne pas hésiter à poser des questions, en cours, en TD et si vraiment on est trop timide on peut passer voir l'enseignant à la fin du cours, ou tenter de le trouver dans son bureau hors des heures de cours, lui envoyer un mail, etc.

Chapitre 2

Le langage mathématique

En mathématiques, après un raisonnement ou un calcul on se pose (presque) toujours deux questions :

1. a-t-on bien utilisé toutes les hypothèses du problème ?
2. ne pourrait-on pas améliorer le raisonnement ou le calcul en supprimant l'une des hypothèses ?
Ou plus modestement, ne pourrait-on pas reformuler certaines hypothèses de manière moins restrictive pour obtenir un raisonnement plus général ?

Il arrive souvent que la deuxième question ait une réponse positive mais que cela ne soit pas facile à voir ; de très grands développements mathématiques ont découlé de cette seconde question, qui est tout à fait fondamentale.

EXEMPLE.

« Les médiatrices d'un triangle *rectangle* se coupent en un seul point : le centre du cercle circonscrit. »
C'est vrai mais l'hypothèse que le triangle est rectangle est inutile puisque les médiatrices de *tout* triangle se coupent au centre du cercle circonscrit. Cette hypothèse superflue peut même nous induire en erreur : par exemple on pourrait chercher (longtemps) à utiliser Pythagore.

Lorsque l'on résout un exercice et que l'on découvre à la fin que l'une des hypothèses n'a servi à rien, il y a deux cas de figure :

1. on s'est trompé, l'hypothèse inutilisée était nécessaire et le calcul ou raisonnement est faux ; c'est le cas le plus probable ;
2. le concepteur de l'exercice s'est trompé, ou alors il a cherché à nous enduire d'horreur. Ça arrive.

2.1 LES OBJETS MATHÉMATIQUES

Les objets mathématiques sont abstraits, on ne peut pas les toucher. Parfois on peut les représenter par un dessin, par exemple en géométrie, mais il faut toujours faire attention car les dessins peuvent être trompeurs ; par exemple si on dessine un triangle sans faire attention, on a toutes les chances de tomber sur un triangle particulier (un triangle rectangle, ou isocèle). Si après on se fie au dessin, on risque d'utiliser une propriété du triangle dessiné qui n'est pas une hypothèse du problème : si notre triangle semble rectangle sur le dessin on pourrait tenter de démontrer que deux médiatrices se coupent au centre d'un côté (ce qui n'est vrai que pour les triangles rectangles).

Cela étant dit les dessins sont souvent d'une aide précieuse pour se figurer les objets mathématiques.

Types d'objets mathématiques. Si on prend le mot *objet* en un sens suffisamment large, il y a beaucoup d'objets mathématiques (vraiment beaucoup). Pour s'y retrouver on les classe en différents *types*. Il est très important lorsque l'on a affaire à un énoncé mathématique, de savoir typer chacun des objets dont il est question. En particulier lorsque l'on compare deux objets, ils sont *toujours* de même type : dire que la

fonction x^2 sur \mathbb{R} est égale à l'ensemble des réels positifs n'a pas de sens ; il faut dire que la fonction x^2 est à valeur dans les réels positifs.

Voici les types d'objets les plus courants que l'on trouvera dans ce cours :

Nombres : c'est le seul type *simple*, c'est à dire qui ne dépend d'aucun autre type. Il y a plusieurs types de nombres mais on peut toujours comparer deux nombres : les *entiers naturels*, 0, 1, 2, ... ; les *entiers relatifs* qui sont les naturels auxquels on ajoute leurs opposés -1, -2, ... ; les rationnels qui s'expriment par des fractions entre entiers relatifs ; les *réels*, les *complexes*.

Ensembles : il en sera à nouveau question dans le chapitre suivant. Il s'agit d'un type complexe : un ensemble est toujours un ensemble *de* quelque chose, par exemple un ensemble de nombres, ou un ensemble de fonctions, voire même un ensemble... d'ensembles.

On connaît déjà plusieurs ensembles : l'ensemble des entiers naturels est noté \mathbb{N} , des relatifs noté \mathbb{Z} , des rationnels noté \mathbb{Q} , des réels noté \mathbb{R} , des complexes noté \mathbb{C} ... Les ensembles sont toujours des ensembles *de* quelque chose : ensemble de nombres, ensemble de fonctions, ensemble d'ensembles, etc.

Fonctions ou applications : dans ce cours les deux termes « fonction » et « application » sont synonymes. Un autre type complexe : une fonction est toujours définie *sur* un ensemble appelé *ensemble de départ* ou *domaine de définition* et à valeurs *dans* un ensemble appelé *ensemble d'arrivée*. On note cela $f : X \rightarrow Y$ ce qui se lit « la fonction f définie sur l'ensemble X , à valeurs dans l'ensemble Y ». On dit aussi que f est *de* X *dans* Y .

Des exemples de fonctions sont : la fonction factorielle sur les entiers naturels à valeurs dans les entiers naturels, la fonction x^2 sur les réels, la fonction cosinus sur les réels, la fonction exponentielle sur les complexes, etc.

Tuples ou uplets : les tuples sont des suites finies d'objets ; encore une fois il s'agit d'un type complexe paramétré par le type des objets contenus : un tuple d'entiers, un tuple de fonctions... Par exemple les vecteurs de \mathbb{R}^3 sont des triplets de réels.

Les *couples* sont des 2-uplets, les *triplets* sont des 3-uplets...

Suites : ce sont encore des cas de fonctions, une suite est une fonction sur les entiers ; par exemple une suite (x_n) de réels est une fonction de \mathbb{N} dans \mathbb{R} qui à chaque entier n associe un réel x_n .

Relations : on les retrouvera également au chapitre suivant. Les relations ne sont pas à proprement parler des objets mathématiques mais plutôt les briques de base pour construire des énoncés mathématiques. Elles sont pourtant typées et c'est la raison pour laquelle on les mentionne ici.

La plupart des relations intéressantes (en commençant par la plus intéressante de toutes : l'égalité) sont binaires, c'est à dire qu'elles portent sur deux objets. Par exemple la relation d'ordre \leq entre les nombres est binaire puisqu'elle permet de comparer *deux* nombres. Toutefois il existe aussi des relations ternaires ou plus. Par exemple l'équation $x^2 + y^2 + z^2 = 1$ qui définit la sphère unité dans \mathbb{R}^3 , est une relation ternaire entre les 3 coordonnées x , y et z des points de \mathbb{R}^3 .

Comme les fonctions les relations sont le plus souvent sur un ensemble, par exemple la relation \leq sur les entiers, ou sur les réels, la relation \subset sur l'ensemble des parties de \mathbb{N} .

La plupart des relations en mathématiques sont homogènes, c'est à dire que les deux objets comparés par la relation sont de même type : par exemple on écrit des égalités entre nombres, entre vecteurs, entre ensembles, entre fonctions mais ça n'a pas de sens d'écrire une égalité entre une fonction et un nombre. Il existe toutefois des relations hétérogènes, la plus connue étant la relation d'appartenance \in qui exprime qu'un objet appartient à un ensemble.

Surcharge¹ des notations. Les mathématiques utilisent une symbolique riche mais finie ; aussi on est amené à utiliser les mêmes symboles pour nommer des objets différents. Par exemple on note toujours 0 l'élément neutre de l'addition, qu'il s'agisse de l'addition d'entiers, de relatifs, de complexes, de vecteurs, de

1. Ce terme de *surcharge* est emprunté à l'informatique, et plus particulièrement à la programmation objet où la surcharge désigne le fait de donner le même nom à plusieurs fonctions lorsqu'elles ont des types suffisamment différents pour éviter toute ambiguïté.

matrices, d'opérateurs sur un espace de Banach... De même on note (presque) toujours 1 l'élément neutre de la multiplication.

Toutefois ça n'est pas parce que deux objets portent le même nom qu'ils sont égaux ; le vecteur 0 de \mathbb{R}^3 est distinct de l'entier 0, ce sont deux objets qui n'ont pas le même type (les vecteurs de \mathbb{R}^3 sont des triplets de réels, les entiers sont des nombres). Sans parler de la fonction 0 sur les réels qui à chaque x associe la valeur 0 et qui n'est évidemment ni un nombre, ni un triplet.

En général le contexte d'utilisation d'un symbole suffit à déterminer le type du symbole. Par exemple si on sait que x est un vecteur de \mathbb{R}^3 alors dans l'expression $x + 0$, le symbole $+$ désigne l'addition de vecteurs (et non l'addition de nombres) et le symbole 0 désigne le vecteur nul de \mathbb{R}^3 c'est à dire le triplet $(0, 0, 0)$. Par contre si f est une fonction de \mathbb{R} dans \mathbb{R} , lorsque l'on écrit $f \neq 0$, le symbole 0 représente la fonction nulle.

EXEMPLE.

Considérons l'énoncé : « si x et y sont des vecteurs de \mathbb{R}^3 alors $x.y = 0$ ssi $x = 0$ ou $y = 0$ (ou $x.y$ est le produit scalaire de x et y) ». Par définition x et y sont des triplets de réels. On nous dit que $x.y$ est le produit scalaire de x et y ; il faut se souvenir que le produit scalaire est à valeurs dans \mathbb{R} , donc $x.y$ est un nombre réel. Par conséquent le symbole 0 dans l'égalité $x.y = 0$ représente le nombre 0. Par contre le même symbole 0 dans les expressions $x = 0$ et $y = 0$ représente cette fois le vecteur nul ; ça ne peut être le nombre 0 car ça n'a pas de sens de comparer un vecteur avec un nombre.

Exercice 1 Donner les types de tous les symboles et expressions utilisés dans les énoncés suivants :

- Soient a et b deux réels ; si $f : [a, b] \rightarrow \mathbb{R}$ est continue et si $f(a) < 0$ et $f(b) > 0$ alors il existe $x_0 \in [a, b]$ tel que $f(x_0) = 0$.
- soient $f : \mathbb{R} \rightarrow \mathbb{R}$; supposons que f est partout dérivable, que $f'(x) = 0$ pour tout x et qu'il existe x_0 tel que $f(x_0) = 0$; alors $f = 0$.
- Si X est un ensemble d'entiers naturels, alors X admet un plus petit élément x_0 .
- Soit $f : \mathbb{N} \rightarrow \mathbb{N}$ une fonction sur les entiers. Il existe un entier n_0 tel que $f(n_0)$ est minimum, c'est à dire tel que pour tout n on a $f(n_0) \leq f(n)$.
- $\forall \epsilon > 0, \exists \alpha > 0, \forall x$ si $|x - x_0| < \alpha$ alors $|f(x) - f(x_0)| < \epsilon$

Exercice 2 Donner le type de chaque variable et expression dans l'énoncé suivant :

Soit \mathcal{T} une topologie sur un ensemble X . Une fonction $f : X \rightarrow X$ est dite *continue en x* si pour tout $V \in \mathcal{T}$ tel que $f(x) \in V$, on a $f^{-1}(V) \in \mathcal{T}$.

Vous n'avez pas besoin de savoir précisément ce qu'est une topologie. Sachez seulement que $f^{-1}(V)$ est défini comme l'ensemble des x tels que $f(x) \in V$.

Exercice 3 Donner le type de chaque variable dans l'énoncé suivant :

Soit x une fonction sur h dérivable en f , il existe une fonction π sur \mathbb{R} qui tend vers 0 en 0 et telle que $x(f + R) = x(f) + R.x'(f) + R.\pi(R)$ pour tout R tel que $f + R \in h$.

2.2 NOTATIONS USUELLES

Jusqu'à la renaissance, les mathématiques n'utilisaient aucune symbolique spéciale et s'écrivaient en langage savant (grec, arabe, latin). On ne disait pas « le *nombre d'or* est la (plus grande) solution de l'équation $x^2 - x - 1 = 0$ » mais « le *nombre d'or* est le plus grand dont le carré est égal à lui-même plus un ».

La notation mathématique moderne a commencé à apparaître vers le 15ème siècle, où Viète invente l'utilisation de lettres pour désigner des inconnues ou des paramètres d'une équation ; elle s'est à peu près fixée dans sa forme actuelle au 17ème siècle où Leibnitz et Newton notamment introduisent une bonne partie de la symbolique moderne. Elle est souvent très utile pour exprimer précisément les propriétés mathématiques. Elle utilise les lettres des alphabets latin et grec (et même hébreux) et aussi un certain nombre de symboles dédiés, à commencer par les célèbres \forall (pour tout) et \exists (il existe).

2.2.1 Variables.

Une variable est un nom, en général une unique lettre, que l'on donne à un objet. Une variable doit toujours être *introduite* avant d'être utilisée : il faut dire quel objet on nomme et quel nom on lui donne. Une variable a également une *portée* ou *durée de vie* : c'est la portion de texte où elle est définie.

Il arrive en pratique que l'on n'explique pas l'introduction des variables, car il est lourd d'écrire sans cesse « Soit $x...$ ». Toutefois pour chaque symbole mathématique apparaissant dans un texte, on doit pouvoir répondre à la question : que représente ce symbole ? Si on ne peut pas c'est qu'il s'agit d'une variable qui n'a pas été (implicitement ou explicitement) introduite, c'est à dire une variable dont on ne sait pas ce qu'elle représente.

EXEMPLE.

Dans la phrase « soit n un entier ; si n est pair alors il existe un entier k tel que $n = 2k$ », la variable n qui est introduite au début porte sur toute la phrase, alors que la variable k porte uniquement sur la partie de la phrase qui vient après le « alors ».

EXEMPLE.

Considérons la phrase « si a et b sont tels que $p = ab$ alors $a = 1$ ou $b = 1$ » (qui définit le fait que p est premier). Ici aucune des trois variables a , b et p n'est explicitement introduite mais on voit bien que les variables a et b sont introduites implicitement car la phrase peut facilement se compléter en « si a et b sont deux entiers tels que $p = ab$ alors... ». La variable p par contre, même si on voit qu'elle représente un entier, n'est pas introduite par la phrase et doit avoir été définie avant dans le texte.

La question de la portée des variables a et b est un peu subtile : apparemment elles sont introduites dans la partie *si* de la phrase, mais on les mentionne également dans la partie *alors*. Ici aussi il faut reformuler la phrase sans en changer le sens pour bien tirer au clair ce qui se passe : « Soient a et b deux entiers ; si $p = ab$ alors $a = 1$ ou $b = 1$ ».

Parfois on introduit les variables après leur usage, au moyen des locutions *où* ou *pour*. Par exemple la définition d'entier pair pourrait s'écrire : « n est un entier pair si $n = 2k$ pour un entier k ».

Exercice 4 Dans les énoncés suivant donner le statut de chaque variable (introduite dans l'énoncé ou pas), et donner la portée de chaque variable introduite.

- i) Si n est un entier tel que $n = 2k$ pour un entier k alors n est pair.
- ii) Il existe deux entiers q et r tels que $a = bq + r$ et $0 \leq r < b$.
- iii) Le PGCD de a et b est l'entier d tel que : d divise a et b et $d' \leq d$ pour tout entier d' qui divise a et b .
- iv) Si x est un réel positif non nul alors $x = nx'$ où n est un entier et x' un réel positif tel que $x' < 1$.
- v) Soient I un intervalle de \mathbb{R} , $x_0 \in I$ et f une fonction de I dans \mathbb{R} ; on dit que f est continue en x_0 si pour tout $\epsilon > 0$, il existe $\alpha > 0$ tel que pour tout $x \in I$, si $|x - x_0| < \alpha$ alors $|f(x) - f(x_0)| < \epsilon$.

Il arrive que la portée d'une variable dépasse la phrase où elle est introduite ; par exemple lorsque la phrase est « Soit f une fonction réelle. », il est clair que la portée de la variable f ne se limite pas à la phrase puisque celle-ci ne dit rien de f ; par défaut la portée de la variable est alors le paragraphe courant. Toutefois le texte peut expliciter une autre portée au moyen d'expression du genre « Dans cette section on appellera $x...$ » ou « Pour les besoins de la démonstration on notera G le groupe... ».

Par exemple on peut dire « Dans ce cours on notera \mathbb{N} l'ensemble des entiers naturels » ; ici on introduit le nom \mathbb{N} et l'on en indique explicitement la portée : tout le cours. En règle général un symbole introduit dans une définition a pour portée tout le reste du cours.

Quantificateurs. Le langage mathématique prévoit de nombreuses manières d'introduire des variables, notamment par l'utilisation des quantificateurs \forall et \exists .

Le quantificateur \forall introduit le nom d'un objet *quelconque*, ou *générique*, ou *arbitraire*, c'est à dire un objet sur lequel on ne fait aucune hypothèse ; il sert donc à exprimer une propriété qui sera valable pour tout objet. Le quantificateur \forall a de nombreux avatars, le plus courant étant l'usage du verbe être au subjonctif : « soit » ou « soient » pour introduire plusieurs noms, qui sont des abréviations pour « quel que soit » ou « quels que soient ».

EXEMPLE.

« Soit n un entier naturel ; si n est pair alors $n+1$ est impair ». Dans cette phrase on commence par introduire un objet dont on dit qu'il s'agit d'un entier naturel que l'on va appeler n . À part le type de l'objet on ne fait aucune hypothèse sur cet objet. Le reste de la phrase exprime une propriété de l'objet appelé n . Le même énoncé pourrait s'écrire plus symboliquement : « $\forall n \in \mathbb{N}$, si n pair alors $n+1$ impair ».

Le quantificateur \exists sert à introduire le nom d'un objet dont on affirme l'existence. Par exemple : « il existe un entier n tel que n est égal à la somme de ses diviseurs », ce que l'on peut écrire aussi $\exists n \in \mathbb{N}, n = \sum_{\substack{d|n \\ d \neq n}} d$.

2.2.2 Sommes et produits

Le signe \sum permet d'exprimer une somme d'un nombre déterminé de termes tous de la même forme. Chaque terme dépend d'un paramètre appelé *indice de sommation* pour lequel on explicite l'ensemble des valeurs possibles. La forme la plus générale est donc

$$\sum_{i \in I} x_i$$

où I est un ensemble et les x_i sont des nombres ; on dit que la somme est *indexée par I* .

REMARQUE

L'indice de sommation est une variable introduite par le signe somme ; la portée de cette variable est limitée à l'expression sous le signe somme.

Somme vide. Dans le cas particulier où I est vide, on parle d'une somme vide. Par convention la somme vide est égale à 0 (l'élément neutre de l'addition).

Très souvent I est l'ensemble des entiers compris entre 1 et n pour une valeur n fixée. Dans ce cas on écrit :

$$\sum_{1 \leq i \leq n} x_i = \sum_{i=1}^n x_i$$

Dans le cas particulier où l'on a choisi une valeur de n plus petite que 1, par exemple si $n = 0$, on a affaire à une somme vide, dont la valeur est donc 0.

EXEMPLE.

La somme $1 + 2 + \dots + n$ s'écrira $\sum_{k=1}^n k$. Le signe somme introduit une variable, ici la variable k , nommée *indice de sommation* et indique toutes les valeurs prises par cette variable, ici toutes les valeurs comprises entre 1 et n .

EXEMPLE.

$\sum_{i=0}^n 2^i$ introduit l'indice de sommation i qui prend toutes les valeurs entières comprises entre 0 (inclus) et n (inclus). En développant on obtient donc :

$$\sum_{i=0}^n 2^i = 2^0 + 2^1 + \dots + 2^n$$

La valeur de la somme ne dépend pas du nom que l'on a choisi pour l'indice de sommation ; autrement dit $\sum_{k=0}^n 2^k = \sum_{i=0}^n 2^i = \sum_{\alpha=0}^n 2^\alpha$.

Produit. On peut de même exprimer un produit d'un nombre déterminé de facteurs au moyen du symbole \prod .

Exercice 5 Dans chacune des expressions suivantes, dire quel est l'indice de sommation et réécrire la même expression en changeant le nom de l'indice de sommation :

i) $\sum_{i=1}^k i^k$;

ii) $\prod_{1 \leq k \leq n} k$

Exercice 6 À quoi est égal la somme $\sum_{n=1}^p 1$?

Changement de variable. Une opération très courante sur les sommes indexées est le changement de variable. Par exemple on l'utilise pour rénuméroter : $\sum_{i=1}^{n+1} x_i = \sum_{j=0}^n x_{j+1}$.

Exercice 7 On note $S_n = \sum_{k=1}^n k$. Montrer, par le changement de variable de k en $n+1-k$ que $S_n = n(n+1) - S_n$.

Somme multi-indexée. Pour faire des sommes de sommes, on est amené à manipuler des sommes avec plusieurs indices de sommation.

EXEMPLE.

$$\begin{aligned} \sum_{\substack{0 \leq i \leq n \\ 0 \leq j \leq p}} 2^{i+j} &= \sum_{i=0}^n \sum_{j=0}^p 2^{i+j} \\ &= \sum_{i=0}^n 2^i \sum_{j=0}^p 2^j \\ &= \sum_{i=0}^n 2^i (2^{p+1} - 1) \\ &= (2^{p+1} - 1) \sum_{i=1}^n 2^i \\ &= (2^{p+1} - 1)(2^{n+1} - 1) \end{aligned}$$

Exercice 8 Soient $f(x) = \sum_{i=0}^n a_i x^i$ et $g(x) = \sum_{j=0}^p b_j x^j$ deux fonctions polynomiales. Calculer $f(x)g(x)$.

2.3 LES ÉNONCÉS MATHÉMATIQUES

Les énoncés parlent d'objets mathématiques (les entiers, les réels, les fonctions, les vecteurs, ...) et expriment des propriétés de ces objets. Par exemple « p est un nombre premier » est un énoncé exprimant une propriété de l'objet nommé p .

Exercice 9 Écrire en français les énoncés :

- i) $\exists k \in \mathbb{N}, n = 2k$;
- ii) $\forall n, p \in \mathbb{N}$, si $\exists k, l \in \mathbb{N}$ tel que $n = 2k$ et $p = 2l$ alors $\exists m \in \mathbb{N}$ tel que $n + p = 2m$;
- iii) $\forall a, b, c \in \mathbb{C}, \exists z \in \mathbb{C}$ tel que $az^2 + bz + c = 0$.

Exercice 10 Écrire de façon complètement formelle les énoncés suivants :

- i) Le carré de la somme de deux nombres est égal à la somme des carrés de ces deux nombres augmentée du double de leur produit.
- ii) Le sinus de la somme de deux angles est la somme des produits du sinus de l'un par le cosinus de l'autre.
- iii) Si une fonction dérivable sur un intervalle prend la même valeur en deux points distincts de cet intervalle, alors sa dérivée s'annule entre ces deux points.

iv) On dit qu'une suite de réels tend vers un point si, pour tout intervalle ouvert contenant ce point, elle prend toutes ses valeurs dans cet intervalle à partir d'un certain rang.

v) De toute suite réelle à valeurs dans un intervalle fermé on peut extraire une sous-suite convergente.

Exercice 11 On définit la relation \leq sur \mathbb{N}^2 en posant que $(x, y) \leq (x', y')$ si $x = x'$ et $y \leq y'$. Dire si les propriétés suivantes sont vraies :

- i) $\forall x, y \in \mathbb{N}, (x, y) \leq (x, y)$;
- ii) $\forall x, y, x', y' \in \mathbb{N}$, si $(x, y) \leq (x', y')$ et $(x', y') \leq (x, y)$ alors $x = x'$ et $y = y'$;
- iii) $\forall x, y, x', y', x'', y'' \in \mathbb{N}$, si $(x, y) \leq (x', y')$ et $(x', y') \leq (x'', y'')$ alors $(x, y) \leq (x'', y'')$;
- iv) $\forall x, y, x', y'$, soit $(x, y) \leq (x', y')$ soit $(x', y') \leq (x, y)$.

2.3.1 Définitions

Les définitions sont des énoncés un peu particuliers puisqu'ils ne sont ni vrai ni faux mais servent à introduire de nouvelles notions et notations. Ces notions et notations seront ensuite utilisées dans les théorèmes et les définitions qui suivent.

Comme les objets mathématiques sont abstraits on ne peut pas les définir en les montrant. Pour définir un objet mathématique on a essentiellement 2 méthodes :

- tout d'abord on peut se fier à l'intuition ; par exemple on ne va pas définir les *nombre entiers* ni les *ensembles* dans ce cours, on va se fier à l'idée qu'on a. Toutefois cette méthode atteint rapidement ses limites, d'une part on se fait parfois des idées fausses ou contradictoires, d'autre part quand les objets deviennent plus compliqués il faut leur donner une définition précise sinon on ne peut pas travailler avec.
- La deuxième méthode, qui est massivement utilisée en mathématique consiste donc à *lister les propriétés de l'objet que l'on définit*. Autrement dit on décrit très précisément comment l'objet peut être utilisé, quelles relations il entretient avec les autres objets déjà définis, etc.

EXEMPLE.

« On appelle nombre *composé* un entier qui peut s'écrire comme produit de deux entiers différents de 1. »

Ici la notion introduite est celle de nombre composé, ce qui est clairement indiqué par la mise en italique du mot « composé » ; il n'y a pas de notation associée. On peut formuler la même définition de façon plus symbolique : «1 Un nombre entier n est dit *composé* si il existe deux entiers a et b tels que : $a \neq 1, b \neq 1$ et $n = ab$ ».

Les noms que l'on donne aux objets n'ont aucune importance, ce qui compte est la notion introduite.

EXEMPLE.

Une formulation strictement équivalente à la précédente (et encore plus symbolique) est : « $\alpha \in \mathbb{N}$ est *composé* ssi $\exists n, p \in \mathbb{N}, n \neq 1, p \neq 1$ et $\alpha = np$ ».

Exercice 12

- i) Vue la définition de nombre composé, 0 est-il composé ? et 1 ?, et 2 ? et 3 ? et 4 ? et 5 ? et 6 ?
- ii) Le nombre π est-il composé ? Et $\sqrt[3]{8}$?
- iii) Soit n un nombre entier. Le nombre $n!$ est-il composé ?

Une fois qu'une notion est définie on peut l'utiliser dans d'autres définitions.

EXEMPLE.

Voici par exemple la définition de nombre premier, utilisant la notion de nombre composé qui vient d'être introduite : « Un nombre entier est premier s'il est différent de 1 et n'est pas composé ».

Exercice 13 Écrire la définition de nombre premier de manière complètement symbolique.

Exercice 14 0 est-il premier? et 1?, et 2? et 3? et 4? et 5? et 6?

Une définition peut également introduire une notation (et même plusieurs) pour la notion introduite qui pourra ensuite être utilisée dans des formulations symboliques.

EXEMPLE.

« Soit a et b deux entiers non nuls. On appelle *plus grand commun diviseur* de a et de b et on note $\text{pgcd}(a, b)$ ou $a \wedge b$ le plus grand entier d tel que d divise a et d divise b . »

Cette définition introduit deux notations pour la même chose.

2.3.2 Théorèmes

Le mot *théorème* désigne un énoncé mathématique dont on sait qu'il est vrai car on en connaît (au moins) une *démonstration* ; il existe également des énoncés mathématiques dont on *pense* qu'ils sont vrais mais dont on ne connaît pas de démonstration : ce sont des *conjectures*. Enfin il existe des énoncés mathématiques dont on pense qu'ils sont vrais mais qui finalement s'avèrent faux : ce sont des erreurs (et en un certain sens ce sont les plus intéressants).

Le mot théorème a plusieurs synonymes : *proposition*, *lemme*, *corollaire*, ... Une proposition est un énoncé (prouvé) qui ne mérite pas le titre un peu pompeux de théorème, soit parce que la démonstration est trop facile, soit parce que la proposition n'est pas très utile en pratique (pour démontrer d'autres théorèmes). Un lemme est un résultat intermédiaire qui sert dans la démonstration d'un théorème. Un corollaire est un théorème qui se déduit facilement d'un autre théorème.

2.4 LES DIFFÉRENTS TYPES D'ÉNONCÉS MATHÉMATIQUES

Les énoncés mathématiques se construisent en combinant des énoncés simples (des propriétés élémentaires comme des (in)égalités) au moyen de constructions logiques ; Il y a essentiellement trois types de constructions qu'il faut savoir reconnaître :

Implication ce sont les énoncés de la forme « si ... alors ... » ;

Existence énoncés de la forme « il existe ... tel que ... » ;

Équivalence énoncés de la forme « ... ssi ... ».

Pour comprendre un énoncé mathématique il faut tout d'abord en saisir la structure logique, puis décomposer l'énoncé en sous-énoncés plus simples (les ... ci-dessus) ; on recommence avec chacun des sous-énoncés, et ainsi de suite jusqu'à arriver à des énoncés dont on comprend tous les termes.

2.4.1 Implications.

Les implications forment la grande majorité des énoncés mathématiques ; du reste on verra que les existences sont souvent des formes particulières d'implications, et les équivalences sont des combinaisons d'implications.

EXEMPLE.

« Si p est un nombre premier supérieur ou égal à 3 alors p est impair ». Cette implication exprime une propriété vraie de *tous* les nombres premiers plus grand que 3. Autrement dit on pourrait écrire cette implication : « Pour tout nombre entier p , si p est premier et supérieur à 3 alors p est impair ». Ou un peu plus symboliquement : « $\forall p \in \mathbb{N}$, si p est premier et $p \geq 3$ alors p est impair ».

« Si x et y sont deux nombres réels, alors $x^2 + y^2$ est un nombre réel positif ou nul ». Cette implication parle de tous les nombres réels ; une autre manière de l'écrire serait : « pour tous x, y , si x et y sont des nombres réels alors $x^2 + y^2 \geq 0$ », ou même « pour tous nombres réels x et y , $x^2 + y^2 \geq 0$ ».

Comme on voit une implication exprime en général une propriété de toute une classe d'objets. Implicitement une implication commence (presque) toujours par une série de « pour tout », ce qui s'exprime de plusieurs manières :

- au travers de l'article indéfini « un » : « si p est *un* nombre premier... » signifie que cette implication commence implicitement par « pour tout $p \in \mathbb{N}$, si p est premier... » ;
- au travers l'emploi des adjectifs « quelconque » ou « arbitraire » : « si p est une nombre premier *arbitraire*... » ;
- au travers l'emploi de l'adjectif « tout » : « Tout nombre premier p est tel que... » ;
- etc.

Différentes manières d'écrire les implications. Les implications ne s'écrivent pas toujours sous la forme « si ... alors ... » mais il faut savoir les reconnaître malgré tout.

EXEMPLE.

Les deux implications précédentes peuvent s'écrire : « tout nombre premier supérieur à 3 est impair » et « la somme des carrés de deux réels est positive ou nulle ».

Il est fondamental de savoir reconnaître la partie *si*, les *hypothèses* de l'implication, de la partie *alors*, la *conclusion* de l'implication. Prenons par exemple le théorème de Bezout :

Si a et b sont deux entiers et d est le pgcd de a et b alors il existe deux entiers u et v tels que $ua + vb = d$.

Dans cet énoncé les hypothèses sont :

- a et b sont deux entiers,
- d est le pgcd de a et b ;

et la conclusion est : il existe deux entiers u et v tels que $ua + vb = d$. On peut écrire cela complètement symboliquement :

$$\forall a, b \in \mathbb{N}, \exists u, v \in \mathbb{N}, ua + vb = \text{pgcd}(a, b)$$

On peut aussi, en se rappelant du vocabulaire de l'algèbre linéaire, se débarrasser complètement de la symbolique : « étant donnés deux entiers, ils ont une combinaison linéaire à coefficients entiers égale à leur pgcd ».

Voici plusieurs autres formulations de ce théorème :

- Soient a et b deux entiers et d leur pgcd. Il existe deux entiers u et v tels que $ua + vb = d$.
- Étant donnés deux entiers a et b et d leur pgcd, il existe deux entiers u et v tels que $ua + vb = d$.
- Pour tous entiers a et b , il existe des entiers u et v tels que $ua + vb = d$ où d est le pgcd de a et b .
- Soit d le pgcd de deux entiers quelconques a et b . Il existe deux entiers u et v tels que $ua + vb = d$.
- Si d est le pgcd des entiers a et b alors il existe u et v tels que $ua + vb = d$.
- Il suffit que d soit le pgcd de a et b pour qu'il existe deux entiers a et b tels que $ua + vb = d$.
- Il existe deux entiers u et v tels que $ua + vb = d$ pour tous entiers a et b , où d est le pgcd de a et de b .
- L'existence de deux entiers u et v tels que $ua + vb = d$ est nécessaire pour que d soit le pgcd de deux entiers a et b

Les deux dernières formulations sont correctes mais très maladroites puisqu'elles semblent inverser les hypothèses et la conclusion. Notons au passage que « B est nécessaire pour A » est une manière correcte de dire « si A alors B ».

REMARQUE

Il n'est pas nécessaire de comprendre les termes d'une implication pour reconnaître quelles sont ses hypothèses et quelle est sa conclusion :

Soit A une algèbre de Banach et Ω un ouvert de \mathbb{C} . Supposons que $x \in A_\Omega$ et $f \in H(\Omega)$. Alors $\sigma(\tilde{f}(x)) = f(\sigma(x))$.

Ce théorème (appelé théorème d'*application spectrale* et qui est l'un des fondements de la théorie spectrale) est incompréhensible pour qui ne sait pas ce qu'est une algèbre de Banach, ce que dénote A_Ω , etc. Mais sa structure si ... alors ... est claire ; on peut écrire ce théorème plus symboliquement :

$$\forall A \text{ algèbre de Banach, } \forall \Omega \text{ ouvert de } \mathbb{C}, \forall x \in A_\Omega, \forall f \in H(\Omega), \sigma(\tilde{f}(x)) = f(\sigma(x))$$

Les hypothèses de ce théorème sont donc :

- A est une algèbre de Banach ;
- Ω est un ouvert de \mathbb{C} ;
- x est un élément de A_Ω ;
- f est un élément de $H(\Omega)$.

et la conclusion est l'égalité : $\sigma(\tilde{f}(x)) = f(\sigma(x))$.

Pour expliciter les hypothèses et la conclusion d'un théorème, il est souvent nécessaire d'introduire des notations.

EXEMPLE.

«Les médiatrices d'un triangle se coupent en un seul point, le centre du cercle circonscrit ». Ce théorème exprime une propriété de tous les triangles. Pour bien en dégager les hypothèses et la conclusion, on va le réécrire en donnant des noms aux objets : « soient A, B, C trois points du plan, a la médiatrice du segment $[BC]$, b la médiatrice du segment $[AC]$ et c celle du segment $[AB]$. Alors les trois droites a, b , et c se coupent en un seul point O . De plus le point O est le centre du cercle circonscrit (cercle passant pas les trois sommets du triangle ABC) ».

Exercice 15 Quelles sont les hypothèses et la conclusion des énoncés suivant :

- i) Soit p un nombre premier. Si a n'est pas divisible par p alors $a^{p-1} \equiv 1(p)$.
- ii) Dans un triangle rectangle, la somme des carrés des côtés adjacents à l'angle droit est égal au carré de l'hypoténuse.
- iii) Tout polynôme du second degré a deux racines complexes.
- iv) L'ordre d'un sous-groupe divise l'ordre du groupe.

Implication fausse. Une implication est vraie si chaque fois que les hypothèses sont vérifiées la conclusion l'est aussi. Tous les exemples d'implications ci-dessus sont vrais. Une implication est réfutée dès que l'on trouve un exemple où *toutes* les hypothèses sont vraies, mais la conclusion est fausse.

EXEMPLE.

Reprenons le premier exemple mais en oubliant l'une des hypothèses : « si p est un nombre premier alors p est impair ». Cette implication est fausse car si on prend $p = 2$ alors p est un nombre premier mais p n'est pas impair.

De même si on transforme un petit peu la seconde implication en : « si x et y sont des nombres complexes (et non pas réels) alors $x^2 + y^2 \geq 0$ », on obtient un énoncé faux ; en effet si on prend $x = 0$ et $y = i$ alors $x^2 + y^2 = 0^2 + i^2 = 0 - 1 = -1$ n'est pas positif.

Implication réciproque et contraposée. Il faut faire attention à ne pas confondre les deux ; la contraposée d'une implication est une autre implication qui a le même sens que la première ; en particulier, si l'implication est vraie sa contraposée l'est également. La réciproque d'une implication par contre est un nouvel énoncé qui signifie tout autre chose ; la réciproque d'une implication vraie est rarement vraie.

EXEMPLE.

Reprenons par exemple la première implication : « si p est un nombre premier plus grand que 3 alors p est impair ». Sa réciproque est « si p est impair alors p est un nombre premier plus grand que 3 » qui est visiblement fausse puisque 1 est impair mais n'est pas un nombre premier supérieur à 3 (exercice : trouver un autre contre-exemple).

La contraposée est « si p n'est pas impair alors p n'est pas un nombre premier supérieur à 3 », autrement dit « si p est pair alors p n'est pas un nombre premier supérieur à 3 » ; la contraposée ne dit rien d'autre que l'implication de départ.

EXEMPLE.

(Cet exemple est emprunté au livre *Mathématiques L1* [BBE⁺07]) Considérons l'énoncé : « soit n un entier, si n^2 est impair alors n est impair ». Lorsque l'on a à l'esprit que la négation de « n est impair » est « n est pair », on voit que la contraposée de cet énoncé est « soit n un entier, si n est pair alors n^2 est pair ».

Remarquons que pour cet exemple, la réciproque est également vraie : « si n est impair alors n^2 est impair ».

Quand une hypothèse est fausse, l'implication est vraie. C'est un principe logique sur l'implication à bien avoir en tête. Pour s'en convaincre considérer l'énoncé : « si n est un multiple de 4 alors n est pair »² Cet énoncé est vrai, et il l'est pour *n'importe quel* n , en particulier pour $n = 1$ par exemple ; mais dans ce cas n n'est pas un multiple de 4. Pourtant l'énoncé « si 1 est un multiple de 4 alors 1 est pair » est vrai. Cette remarque logique a une conséquence intéressante : les éléments de l'ensemble vide satisfont toutes les propriétés. Par exemple tout élément de l'ensemble vide est pair. En effet cet énoncé dit que « si x appartient à l'ensemble vide alors x est pair ». Mais « x appartient à l'ensemble vide » est toujours faux puisque l'ensemble vide... est vide ! Donc l'implication est toujours vraie.

2.4.2 Énoncés d'existence

Les énoncés d'existence expriment l'existence d'un objet possédant une certaine propriété.

EXEMPLE.

« l'opération d'addition sur les entiers naturels admet un élément neutre » ; autrement dit : « il existe un entier z tel que pour tout entier n on a $n + z = z + n = n$ », ce qui est évidemment vrai, il suffit de prendre $z = 0$.

Les énoncés d'existence prennent souvent la forme : « pour tout ... il existe ... ».

EXEMPLE.

« Tout nombre réel non nul a un inverse », c'est à dire : « pour tout nombre réel x , si x est non nul alors il existe un nombre réel y tel que $xy = yx = 1$ ».

On voit qu'un énoncé d'existence est souvent un cas particulier d'implication.

Existence et unicité. Il arrive souvent qu'un énoncé d'existence soit renforcé en un énoncé d'existence et d'*unicité*. Un énoncé d'existence et unicité se décompose toujours en deux énoncés : l'un exprimant l'existence, l'autre l'unicité.

EXEMPLE.

« L'addition sur les entiers naturels admet un *unique* élément neutre ». « Tout nombre réel non nul admet un unique inverse ».

Symboliquement l'existence et unicité se note $\exists!$.

2. Cet exemple est emprunté à l'excellent livre de logique de Daniel Lascar et René Cori [LC93].

EXEMPLE.

« $\exists! z \in \mathbb{N}, \forall n \in \mathbb{N}, n + z = z + n = n$ », « $\forall x \in \mathbb{R}, \text{ si } x \neq 0 \text{ alors } \exists! y \in \mathbb{R} \text{ tel que } xy = yx = 1$ ».

L'unicité d'un objet s'exprime par une implication : si deux objets quelconques satisfont la propriété pour laquelle il y a unicité, alors ils sont égaux.

EXEMPLE.

L'unicité de l'élément neutre est : si z et z' sont deux entiers neutres pour l'addition alors $z = z'$. Si on écrit symboliquement l'existence et l'unicité de l'élément neutre, on obtient :

$$\exists z \in \mathbb{N} (\forall n \in \mathbb{N}, n + z = z + n = n \text{ et } \forall z' \in \mathbb{N} \text{ si } \forall n \in \mathbb{N}, n + z' = z' + n = n \text{ alors } z' = z)$$

Autrement dit il y a un entier z tel que : z est neutre pour l'addition et pour tout z' si z' est neutre pour l'addition, alors $z' = z$.

L'unicité de l'inverse s'exprime : si x est un réel non nul et y et y' sont deux inverses de x , alors $y = y'$. Si on développe symboliquement l'existence et unicité de l'inverse sur les réels on obtient :

$$\forall x \in \mathbb{R}, \text{ si } x \neq 0 \text{ alors } \exists y \in \mathbb{R} \text{ tel que } (xy = yx = 1 \text{ et } \forall y' \in \mathbb{R} \text{ si } xy' = y'x = 1 \text{ alors } y' = y)$$

Exercice 16 Montrer ces deux propriétés d'unicité.

2.4.3 Équivalence

L'implication exprime une causalité : « si A alors B » dit que à chaque fois que l'on a A , on a nécessairement B aussi (« B est nécessaire pour A »). On a vu que même quand une implication est vraie sa réciproque ne l'est pas forcément mais il arrive que ça soit le cas, et on parle alors d'*équivalence* : on ne peut jamais avoir A sans B ni B sans A .

Une équivalence est donc une combinaison de deux implications : « A ssi B » est une abbréviation pour « A si B et si A alors B », c'est à dire « si B alors A » et « si A alors B ».

On dit également « A est une condition nécessaire et suffisante pour B ».

Exercice 17 Expliciter chacun des énoncés suivants en faisant clairement apparaître : la structure logique de l'énoncé, les hypothèses et la conclusion, le ou les (classes d') objets dont il est question.

- i) Les diagonales d'un losange sont orthogonales.
- ii) La somme de deux entiers est paire dès que les deux entiers ont la même parité.
- iii) Quand l'un de deux entiers est pair, leur produit l'est également.
- iv) Tout nombre réel positif a une racine carrée.
- v) La limite des sommes de termes de la suite géométrique de raison $0 \leq \rho < 1$ existe et est $1/(1 - \rho)$.
- vi) L'image par une fonction continue d'une suite convergente est une suite convergente et la limite de l'image de la suite est l'image de la limite de la suite.
- vii) Une fonction continue sur un intervalle et prenant des valeurs de signes différents aux extrémités de l'intervalle a (au moins) un zéro.
- viii) Tout nombre entier se décompose de manière unique en un produit fini de puissances de nombres premiers.

2.5 DÉMONSTRATIONS

Il n'existe pas de technique universelle de démonstration (heureusement pour les mathématiciens d'ailleurs). Chaque théorème nécessite une ou plusieurs idées qui lui sont propres pour être démontré et il n'y a pas de moyen automatique d'obtenir cette ou ces idées.

Pour faire une démonstration il faut d'abord avoir les idées claires sur ce qu'il faut démontrer, c'est à dire procéder à l'analyse logique complète du théorème, bien repérer quelles sont les hypothèses, quelle est la conclusion, décomposer les hypothèses en énoncés simples en utilisant les définitions, etc.

Il y a plusieurs formes logique de raisonnement que l'on retrouve et qu'il faut connaître.

2.5.1 Architecture d'un raisonnement

Pour démontrer une implication, on commence par supposer que les hypothèses sont réalisées, et on cherche à en déduire la conclusion. Au cours du raisonnement on peut être amené à démontrer un ou plusieurs résultats intermédiaires dont la combinaison mènera au résultat final. Et lorsque l'on démontre un résultat intermédiaire, qui est en général une implication, on pose des hypothèses intermédiaires et on démontre la conclusion intermédiaire.

À tout instant au cours d'une démonstration on a donc un certain nombre d'hypothèses : celles du théorème qui sont valides pendant tout le raisonnement et celles du résultat intermédiaire qui ne sont valides que pendant la démonstration du résultat intermédiaire.

Par exemple lorsque l'on fait une démonstration par récurrence il y a toujours deux étapes intermédiaires : démontrer que la propriété est vraie quand $n = 0$; pendant que l'on démontre cela, on a l'hypothèse supplémentaire que $n = 0$. Puis démontrer que si la propriété est vraie pour n elle l'est pour $n + 1$. Pendant cette étape on ne suppose plus que $n = 0$ mais par contre on suppose que la propriété est vraie pour n .

Lorsque ces deux résultats intermédiaires sont prouvés, on en déduit, par récurrence sur n que la propriété est vraie pour tout n .

2.5.2 Raisonnement équationnel ou calcul

Utilisé en général pour démontrer une égalité, mais pas seulement, il s'agit d'une suite d'équations aboutissant au résultat cherché. Chacune des équations est justifiée par l'une ou plusieurs des équations précédentes et par une propriété connue ou par une hypothèse du théorème.

EXEMPLE.

Montrons l'unicité de l'élément neutre de l'addition sur les entiers : soient donc z et z' deux éléments neutres c'est à dire deux entiers tels que pour tout entier n on a $z + n = n + z = n$ et $z' + n = n + z' = n$. En particulier on a :

$$\begin{aligned} z &= z + z' && \text{car } z' \text{ est neutre à droite} \\ &= z' && \text{car } z \text{ est neutre à gauche} \end{aligned}$$

EXEMPLE.

Montrons que $\cos(x + y) = \cos x \cos y - \sin x \sin y$. La formule de Moivre nous dit que $e^{ix} = \cos x + i \sin x$ pour tout réel x . On a donc : $e^{i(x+y)} = \cos(x + y) + i \sin(x + y)$ mais également :

$$\begin{aligned} e^{i(x+y)} &= e^{ix} e^{iy} && \text{propriété bien connue de l'exponentielle} \\ &= (\cos x + i \sin x)(\cos y + i \sin y) && \text{en appliquant deux fois la formule de Moivre} \\ &= \cos x \cos y - \sin x \sin y + i(\cos x \sin y + \sin x \cos y) && \text{en développant et réorganisant le produit} \end{aligned}$$

Donc les deux nombres complexes $\cos(x+y) + i \sin(x+y)$ et $\cos x \cos y - \sin x \sin y + i(\cos x \sin y + \sin x \cos y)$ sont égaux ce qui implique que leurs parties réelles et imaginaires sont égales, soit :

$$\begin{aligned} \cos(x + y) &= \cos x \cos y - \sin x \sin y \\ \sin(x + y) &= \cos x \sin y + \sin x \cos y \end{aligned}$$

Exercice 18

- i) Démontrer que si x, y et z sont des entiers relatifs tels que $x + z = y + z$ alors $x = y$.
- ii) Quelle hypothèse manque dans l'énoncé suivant : si x, y et z sont des rationnels tels que $xz = yz$ alors $x = y$?
- iii) Démontrer que la somme de deux entiers pairs est paire et que la somme de deux entiers impairs est paire.
- iv) Démontrer l'unicité de l'inverse sur les réels.

2.5.3 Raisonnement par cas, tiers-exclus

Le tiers-exclus est un principe logique qui dit que, en mathématiques, tout énoncé est soit vrai, soit faux. On peut utiliser ce principe dans une démonstration en ajoutant une hypothèse supplémentaire et en considérant deux cas : celui où cette hypothèse est vraie, celui où l'hypothèse est fautive. Si on parvient à démontrer la conclusion dans les deux cas, alors celle-ci est toujours vraie et le théorème est démontré.

EXEMPLE.

Voici un exemple de raisonnement par cas. On va montrer que pour tout entier naturel a le produit $a(a^2 - 1)$ est un multiple de 3. Soit donc un entier a quelconque. On commence par remarquer que au moins l'un des trois entiers a , $a + 1$ ou $a + 2$ est un multiple de 3.

Si a est un multiple de 3 alors $a = 3a'$ pour un certain a' , donc $a(a^2 - 1) = 3a'(a^2 - 1) = 3(a'(a^2 - 1))$ est un multiple de 3.

Si $a + 1$ est un multiple de 3 alors $a + 1 = 3a'$ pour un certain a' , donc $a = 3a' - 1$, $a^2 = 9a'^2 - 6a' + 1$ et $a^2 - 1 = 9a'^2 - 6a' = 3(3a'^2 - 2a')$ est un multiple de 3. Donc $a(a^2 - 1)$ est également un multiple de 3.

Si $a + 2$ est un multiple de 3 alors $a + 2 = 3a'$ pour un certain a' . Donc $a = 3a' - 2$, $a^2 = 9a'^2 - 12a' + 4$ et $a^2 - 1 = 9a'^2 - 12a' + 3 = 3(a'^2 - 4a' + 1)$; c' est encore un multiple de 3 donc $a(a^2 - 1)$ est un multiple de 3.

Comme on est forcément dans un de ces trois cas, le théorème est démontré pour tout a .

Exercice 19 Montrer que si a est un entier quelconque alors l'un des entiers a , $a + 1$ ou $a + 2$ est un multiple de 3.

EXEMPLE.

Voici maintenant un exemple d'application du tiers-exclus. On montre qu'il existe deux nombres irrationnels a et b tels que a^b est rationnel (un nombre est irrationnel si il n'est pas rationnel).

Considérons le nombre $x = \sqrt{2}^{\sqrt{2}}$. Ce nombre est soit rationnel, soit irrationnel (tiers-exclus).

Si x est rationnel alors on choisit $a = b = \sqrt{2}$; comme $\sqrt{2}$ est irrationnel, a et b sont irrationnels et $a^b = x$ est rationnel par hypothèse.

Si x est irrationnel alors on choisit $a = x$ et $b = \sqrt{2}$. Dans ce cas $a^b = x^{\sqrt{2}} = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2$ est donc rationnel. Mais a est irrationnel par hypothèse et b également puisque $b = \sqrt{2}$.

Dans les deux cas on a bien trouvé a et b irrationnels tels que a^b est rationnel. Le théorème est démontré.

Exercice 20 Montrer que $\sqrt{2}$ est irrationnel.

2.5.4 Raisonnement par l'absurde, ou par contraposition

Pour montrer une propriété, on la suppose fautive et on en déduit une contradiction. Lorsque la propriété est une implication, ceci revient à raisonner par contraposition : on suppose que la conclusion de l'implication est fautive et on en déduit que l'une des hypothèses est fautive.

2.5.5 Raisonnement par récurrence.

Il s'agit d'une méthode très puissante pour démontrer les propriétés des entiers. Un raisonnement par récurrence est toujours en 2 parties : on commence par démontrer la propriété dans le cas où $n = 0$ (ou pour $n = 1$) ; puis on procède à l'étape de récurrence : on suppose la propriété vraie pour n et on démontre qu'alors elle est aussi pour $n + 1$.

EXEMPLE.

Voici un exemple de théorème que l'on démontre par l'absurde (et par récurrence) : tout ensemble non vide d'entiers naturels a un plus petit élément. Écrit symboliquement : $\forall X \subset \mathbb{N}$, si $X \neq \emptyset$ alors $\exists n_0 \in X$ tel que $\forall n \in X$, $n_0 \leq n$.

Preuve. Supposons que X soit non vide et n'ait pas de plus petit élément. On va démontrer par récurrence sur n que pour tout entier n et pour tout $p < n$, p n'appartient pas à X . De là on déduit que X est vide ce qui contredit l'hypothèse.

REMARQUE

Il s'agit bien d'une contraposition. On démontre que si X n'a pas de plus petit élément alors X est vide, ce qui est la contraposée du théorème.

Cas de base de la récurrence, $n = 0$; il n'y a aucun entier naturel $p < n$, donc tout $p < n$ n'appartient pas à X (on applique ici le principe vu 15 qu'une implication est vraie dès que l'une de ses hypothèses est fausse).

Pour l'étape de récurrence, supposons que pour tout $p < n$, $p \notin X$. Alors $n \notin X$ sinon n serait le plus petit élément de X et on a supposé qu'il n'y en avait pas. Donc pour tout $p < n + 1$ on a $p \notin X$, ce qui achève la récurrence.

Chapitre 3

Ensembles et fonctions

Essentiellement tout objet mathématique est soit un nombre, soit un ensemble, soit une fonction. Dans ce chapitre on va s'attacher à voir les propriétés élémentaires des deux derniers.

3.1 ENSEMBLES

Avec les nombres, les ensembles sont les objets les plus primitifs des mathématiques (certains les considèrent même comme plus primitifs que les nombres). Leur définition précise est assez complexe (et abstraite) et est à la base de la très belle *théorie des ensembles*.

Pour ce cours on va se contenter d'une définition intuitive sans trop chercher à aller dans les détails : un ensemble est une collection *non ordonnée* et *sans répétitions* d'objets. Si X est un ensemble et x un objet on note $x \in X$ pour « x appartient à X », ce que l'on peut dire aussi « x est un *élément* de X ».

Un ensemble est défini si on sait répondre à coup sûr à la question : tel objet x appartient-il à l'ensemble ? Il y a deux manières de définir un ensemble.

En extension : on donne la liste complète de ses éléments ; on note alors les éléments entre accolades : $\{1, 2, 3\}$ est l'ensemble dont les éléments sont les nombres 1, 2 et 3. Pour pouvoir définir des ensembles infinis de cette manière, on utilise les points de suspensions : $\{1, 2, 3, \dots\}$ est l'ensemble de tous les entiers positifs.

En compréhension : on donne une propriété caractéristique qui est satisfaite par les éléments de l'ensemble et seulement ceux-là¹. L'ensemble $\{1, 2, 3\}$ se définit en compréhension comme l'ensemble des entiers compris entre 1 et 3 (inclus) ce que l'on note $\{n \in \mathbb{N}, 1 \leq n \leq 3\}$.

Égalité entre ensembles. Deux ensembles sont égaux si ils ont les mêmes éléments. Donc $\{1, 2, 3\} = \{n \in \mathbb{N}, 1 \leq n \leq 3\} = \{3, 1, 2\}$.

Exercice 1 Écrire toutes les formes en extension de l'ensemble $\{n \in \mathbb{N}, n^2 \leq 12\}$. Cet ensemble est-il égal à $\{n \in \mathbb{N}, n^3 \leq 34\}$? et à $\{n \in \mathbb{N}, n \text{ divise } 6\}$?

Intervalles d'entiers. Ce sont des ensembles que l'on utilisera beaucoup dans ce cours. Si n et p sont des entiers, l'intervalle $[n, p]$ est par définition l'ensemble $\{k \in \mathbb{Z} \text{ tel que } n \leq k \leq p\} = \{n, n+1, \dots, p\}$. Par exemple l'ensemble $\{1, 2, 3\}$ est l'intervalle $[1, 3]$.

Il y a deux cas particuliers intéressants à cette définition :

– si $n = p$ alors l'intervalle $[n, p] = [n, n]$ est le *singleton* (ensemble à un seul élément) $\{n\}$;

1. il faut faire un peu attention avec les définitions en compréhension qui peuvent donner lieu à des paradoxes ; historiquement c'est la découverte de ces paradoxes qui a motivé le développement de la théorie des ensembles. En pratique les définitions en compréhension ne posent pas de problème (sauf dans des cas tordus comme le célèbre paradoxe de Russel : l'ensemble de tous les ensembles qui ne s'appartiennent pas à eux-même).

– si $p < n$ alors l'intervalle $[n, p]$ est l'ensemble vide.

REMARQUE

Encore une fois on utilise une notation connue par ailleurs : $[a, b]$ désigne d'habitude l'intervalle fermé des réels compris entre a et b . Dans ce cours et sauf mention explicite du contraire, cette notation ne désignera que des intervalles d'entiers.

Inclusion. On dit qu'un ensemble X est *inclus* ou *contenu* dans un ensemble Y (notation : $X \subset Y$) quand tout élément de X est aussi élément de Y . Quand X est différent de Y on dit que l'inclusion est *stricte* (notation : $X \subsetneq Y$).

Exercice 2 Soient X, Y . Montrer que $X = Y$ ssi $X \subset Y$ et $Y \subset X$.

REMARQUE

On utilise très fréquemment cette propriété pour montrer que deux ensembles sont égaux.

3.1.1 Constructions élémentaires

Ensemble vide. L'ensemble vide, noté \emptyset ne contient aucun élément ; autrement dit, à la question $x \in \emptyset ?$, la réponse est toujours non. On peut définir l'ensemble vide en compréhension par : $\emptyset = \{x, x \neq x\}$.

Exercice 3 Montrer que l'ensemble vide est inclus dans tout ensemble.

Singleton. Un ensemble contenant un unique élément est appelé un singleton.

Complémentaire. Soit X un ensemble et Y un sous-ensemble de X ; le complémentaire de Y dans X est le sous-ensemble de X défini par : $Y^c = \{x \in X \text{ tel que } x \notin Y\}$.

REMARQUE

On a défini le complémentaire de Y dans X , pourtant la notation Y^c ne mentionne pas X . Lorsque l'on parle de complémentaire, il y a *toujours* un ensemble référent même si celui-ci est laissé implicite dans la notation.

Réunion. Soient X et Y deux ensembles.

L'*union* ou *réunion* de X et Y est l'ensemble des objets appartenant soit à X , soit à Y : $X \cup Y = \{x, x \in X \text{ ou } x \in Y\}$.

Exercice 4 Soient X et Y deux ensembles. Montrer que X et Y sont inclus dans $X \cup Y$ et que si Z contient X et Z contient Y alors Z contient $X \cup Y$.

Exercice 5 Montrer que $X \subset Y$ ssi $X \cup Y = Y$.

Soient n un entier positif et X_1, \dots, X_n des ensembles. La réunion des X_i est notée $X_1 \cup \dots \cup X_n$ ou encore $\bigcup_{i=1}^n X_i$. Dans le cas particulier où $n = 0$, la réunion des X_i est l'ensemble vide : $\bigcup_{i=1}^0 X_i = \emptyset$.

Intersection. L'*intersection* de X et Y est l'ensemble des objets appartenant à X et à Y : $X \cap Y = \{x, x \in X \text{ et } x \in Y\}$.

Exercice 6 Montrer que $X \cap Y$ est contenu dans X et dans Y , et que tout ensemble contenu dans X et dans Y est contenu dans $X \cap Y$.

Exercice 7 Montrer que $X \subset Y$ ssi $X \cap Y = X$.

Soient n un entier non nul et X_1, \dots, X_n des ensembles. L'intersection des X_i est notée $X_1 \cap \dots \cap X_n$ ou encore $\bigcap_{i=1}^n X_i$.

Ensembles disjoints. Si X et Y sont deux ensembles qui n'ont aucun élément en commun, c'est à dire tels que $X \cap Y = \emptyset$, on dit que X et Y sont disjoints.

Soustraction. On note $X \setminus Y$ l'ensemble des éléments de X qui ne sont pas dans Y . Symboliquement : $X \setminus Y = \{x \in X, x \notin Y\}$.

Exercice 8 Montrer que $X \setminus Y \cap Y = \emptyset$ et $X \setminus Y \cup Y = X \cup Y$.

Exercice 9 Montrer que si $Y \subset X$ alors $X \setminus Y$ est le complémentaire de Y dans X .

Si x est un élément de X alors $X \setminus \{x\}$ est l'ensemble des éléments de X différents de x ; on oublie souvent les accolades et on le note $X \setminus x$. Si X est un ensemble de nombres (\mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} ou \mathbb{C}), l'ensemble $X \setminus 0$ est également noté X^* .

Parties. Une *partie* de X est un sous-ensemble de X , c'est à dire un ensemble inclus dans X . L'ensemble de toutes les parties de X est noté $\mathcal{P}(X)$.

Exercice 10 Soient X un ensemble et Y, Y' deux parties de X .

- i) Montrer que $(Y \cup Y')^c = Y^c \cap Y'^c$ et que $(Y \cap Y')^c = Y^c \cup Y'^c$.
- ii) Montrer que les propositions suivantes sont équivalentes :
 - $Y \subset Y'$;
 - $Y \cap Y' = Y$;
 - $Y \cup Y' = Y'$;
 - $Y \cap Y'^c = \emptyset$;
 - $Y^c \cup Y' = X$
- iii) Montrer que $Y \setminus Y' = Y \cap Y'^c$.

Partition. Soit X un ensemble non vide; une partition de X est un ensemble non vide P de parties non vides de X deux à deux disjointes et dont la réunion est X tout entier :

- si $A, B \in P$, $A \neq B$ alors $A \cap B = \emptyset$;
- pour tout $x \in X$, il existe un $A \in P$ tel que $x \in A$.

Les éléments de P sont appelés les *classes* de la partition.

EXEMPLE.

Si on prend $X = \mathbb{N}$ alors on peut partitionner X en deux classes : les pairs et les impairs. Dans ce cas on a $P = \{\{2n, n \in \mathbb{N}\}, \{2n + 1, n \in \mathbb{N}\}\}$. Plus généralement, si p est un entier naturel non nul, on peut partitionner \mathbb{N} en p classes : les multiples de p , leurs successeurs, les successeurs de leurs successeurs, etc. : $P = \{\{kp, k \in \mathbb{N}\}, \{kp + 1, k \in \mathbb{N}\}, \dots, \{kp + p - 1, k \in \mathbb{N}\}\}$.

On peut par exemple partitionner l'ensemble des fonctions de \mathbb{N} dans \mathbb{N} selon la valeur des fonctions en 0 : $P = \{\{f : \mathbb{N} \rightarrow \mathbb{N}, f(0) = 0\}, \{f : \mathbb{N} \rightarrow \mathbb{N}, f(0) = 1\}, \{f : \mathbb{N} \rightarrow \mathbb{N}, f(0) = 2\}, \dots\}$.

Exercice 11 Écrire toutes les partitions de l'ensemble $\{1, 2\}$, puis de l'ensemble $\{1, 2, 3\}$.

3.2 FONCTIONS

On l'a déjà dit : dans ce cours les termes « fonction » et « application » sont synonymes.

Une fonction est définie par trois choses : son *ensemble de définition*, appelé également son *ensemble de départ* ou simplement son *domaine*, son *ensemble d'arrivée* et la donnée pour chaque élément x de l'ensemble de définition d'une *image* de x , également appelée *valeur* de la fonction en x , dans l'ensemble d'arrivée. On dit que f est définie *sur* D et à valeurs dans A et on note $f : D \rightarrow A$; la valeur de f en x est notée $f(x)$.

EXEMPLE.

La fonction factorielle : $\mathbb{N} \rightarrow \mathbb{N}$ qui prend la valeur $n! = n(n-1)\dots 2$ pour chaque $n \in \mathbb{N}$, la fonction carré : $\mathbb{R} \rightarrow \mathbb{R}$ qui prend la valeur x^2 pour chaque réel x , etc.

La fonction *nulle* $0 : \mathbb{R} \rightarrow \mathbb{R}$ qui à chaque réel associe la valeur $0 : 0(x) = 0$ pour tout $x \in \mathbb{R}$.

Les ensembles de définition D et d'arrivée A d'une fonction constitue son type (en informatique on appelle cela la *signature* de la fonction). Une fonction a *toujours* un type bien déterminé.

Égalité de fonctions. Deux fonctions $f : D \rightarrow A$ et $f' : D' \rightarrow A'$ sont égales si elles ont le même type, c'est à dire si $D = D'$ et $A = A'$ et si pour chaque $x \in D$ les valeurs de x par f et f' sont égales, c'est à dire $f(x) = f'(x)$.

REMARQUE

Il y a souvent une ambiguïté sur l'ensemble d'arrivée d'une fonction. Par exemple la fonction cosinus peut-être vue soit comme une fonction réelle à valeurs dans \mathbb{R} , soit comme une fonction réelle à valeurs dans l'intervalle $[-1, 1]$; dans les deux cas on parle de *la* fonction cosinus mais il s'agit bien de deux fonctions distinctes (encore un exemple de surcharge).

Fonction vide. Si D est l'ensemble vide, il existe une fonction de D dans A appelée la *fonction vide* et que l'on note aussi parfois \emptyset .

REMARQUE

Par contre si A est vide il n'existe aucune fonction de D dans A , sauf si D est vide aussi.

REMARQUE

On retrouve l'ambiguïté relevée précédemment : on parle de *la* fonction vide, alors qu'en réalité pour chaque ensemble A , il y a une fonction vide à valeurs dans A et toutes ces fonctions vides sont distinctes.

Fonction identité. Soit X un ensemble; la fonction identité sur X est la fonction $\text{Id}_X : X \rightarrow X$ définie par $\text{Id}_X(x) = x$ pour tout $x \in X$.

REMARQUE

Très souvent on oublie de mettre X en indice et on note Id l'identité sur X .

REMARQUE

Voici un autre exemple de deux fonctions qui ne diffèrent que par leur ensemble d'arrivée : soit X et Y deux ensembles tels que $X \subset Y$. Comme $X \subset Y$ on peut définir la fonction *d'inclusion* $i : X \rightarrow Y$ par $i(x) = x$ pour tout $x \in X$. Si X et Y sont égaux, cette fonction est égale à l'identité sur X (les deux fonction ont même ensemble de départ, même ensemble d'arrivée et même valeur en tout point de l'ensemble de départ). Mais si $X \neq Y$ alors ces deux fonctions sont différentes.

Ensemble des fonctions. L'ensemble des fonctions de D dans A est noté A^D (la raison de cette notation apparaîtra bientôt).

REMARQUE

Si D est vide il y a exactement une fonction de D dans A , la fonction vide. Dans ce cas A^D est un singleton.

3.2.1 Constructions élémentaires

Soient $f : D \rightarrow A$ une fonction.

Image d'un ensemble. Si E est un sous-ensemble de D l'*image de E par f* est l'ensemble des images des éléments de $E : f(E) = \{f(x), x \in E\}$. En particulier l'image de D (qui est un sous-ensemble de lui-même) est appelée l'image de f et parfois notée $\text{im } f$.

REMARQUE

On utilise le terme « image » pour désigner soit l'image d'un élément de D , c'est à dire la valeur de f en cet élément, soit l'image d'un sous-ensemble de D .

De même la notation f désigne soit une fonction de D dans A , soit une fonction de $\mathcal{P}(D)$ dans $\mathcal{P}(A)$. En toute rigueur comme il s'agit de fonctions différentes on devrait leur donner des noms différents, par exemple \bar{f} pour celle définie sur les ensembles.

Cela dit il n'y a pas de confusion possible entre les deux : si on écrit $f(x)$ où $x \in D$ on parle clairement de la première, et si on écrit $f(x)$ où $x \subset D$, il s'agit de la seconde. Dans un souci d'économie des notations, on utilisera donc le même nom pour les deux fonctions.

Exercice 12 Quelle est l'image de l'ensemble vide ?

Image réciproque. Si B est un sous-ensemble de A , on note $f^{-1}(B)$ l'*image réciproque* de B , c'est à dire le sous-ensemble de D constitué des $x \in D$ dont l'image est dans B : $f^{-1}(B) = \{x \in D, f(x) \in B\}$.

Exercice 13 Soit $f : D \rightarrow A$ une fonction.

- i) Montrer que $f^{-1}(A) = D$.
- ii) Soit E un sous-ensemble de A ; se peut-il que $f^{-1}(E) = \emptyset$?
- iii) Montrer que si $y \neq y' \in A$ alors $f^{-1}(\{y\}) \cap f^{-1}(\{y'\}) = \emptyset$.

REMARQUE

Cet exercice démontre que l'ensemble $\{f^{-1}(\{y\}), y \in A\}$ (duquel on a retiré l'ensemble vide) est une *partition* de D .

Exercice 14 Soit $f : D \rightarrow A$ une fonction, E un sous-ensemble de D et F un sous-ensemble de A .

- i) Montrer que $E \subset f^{-1}(f(E))$. Trouver un exemple où l'inclusion est stricte.
- ii) Montrer que $f(f^{-1}(F)) \subset F$. Trouver un exemple où l'inclusion est stricte.

Restriction. Si E est un sous-ensemble de D la restriction de f à E est la fonction $f|_E : E \rightarrow A$ définie par $f|_E(x) = f(x)$ pour tout $x \in E$.

Composition. Soient $f : A \rightarrow B$ et $g : B \rightarrow C$; la composée de f et g est la fonction $g \circ f : A \rightarrow C$ définie par $g \circ f(x) = g(f(x))$.

REMARQUE

Attention à la notation : la composée de f et g se note $g \circ f$ et non pas $f \circ g$.

Exercice 15 Pour chacune des fonctions f et g de \mathbb{R} dans \mathbb{R} suivantes, donner les valeurs de $f \circ f(x)$, $g \circ g(x)$, $f \circ g(x)$, $g \circ f(x)$:

- i) $f(x) = -x$, $g(x) = |x|$;
- ii) $f(x) = \sqrt{|x|}$, $g(x) = x^2$.
- iii) $f(x) = x^3$, $g(x) = 2x + 1$;
- iv) $f(x) = 1/(x^2 + 1)$, $g(x) = x^2 + 1$.

Exercice 16 Soit $f : A \rightarrow B$ une fonction.

- i) Montrer que $f \circ \text{Id}_A = \text{Id}_B \circ f = f$.
- ii) Montrer que la composition est *associative* : si $g : B \rightarrow C$ et $h : C \rightarrow D$ sont deux autres fonctions alors $h \circ (g \circ f) = (h \circ g) \circ f$.

Itération. Soit $f : A \rightarrow A$ une fonction sur A et n un entier naturel. On définit l'itérée n fois de f par récurrence sur n : $f^0 = \text{Id}_A$ et $f^{n+1} = f \circ f^n$.

Exercice 17 Notons f_n la fonction sur A définie par récurrence par : $f_0 = \text{Id}_A$ et $f_{n+1} = f_n \circ f$. Montrer que pour tout n on a $f \circ f_n = f_{n+1}$. En déduire que $f_n = f^n$ pour tout n .

3.2.2 Propriétés élémentaires des fonctions

Injection. Soit $f : D \rightarrow A$ une fonction. On dit que f est injective si les éléments de D ont des images deux à deux distinctes. Symboliquement :

$$f : D \rightarrow A \text{ est injective ssi } \forall x, y \in D, \text{ si } x \neq y \text{ alors } f(x) \neq f(y)$$

On peut contraposer cet énoncé et obtenir une définition équivalente :

$$f : D \rightarrow A \text{ est injective ssi } \forall x, y \in D, \text{ si } f(x) = f(y) \text{ alors } x = y$$

C'est souvent cette définition que l'on utilise dans les démonstrations.

Exercice 18 La fonction vide de \emptyset dans \mathbb{N} est-elle injective ?

Exercice 19

- i) Trouver une fonction injective $f : \mathbb{N} \rightarrow \mathbb{N}$ telle que pour tout $k \in \mathbb{N}$ on ait $f(2k+1) < 2k+1$.
- ii) Soit $f : \mathbb{N} \rightarrow \mathbb{N}$. On suppose que f vérifie : pour tout $n \in \mathbb{N}$ si $n > 0$ alors $f(n) < n$. Montrer que f n'est pas injective.

Exercice 20 Soit $f : D \rightarrow A$ une fonction.

- i) Montrer que si f est injective et $E \subset D$ alors la fonction $f|_E$ est injective.
- ii) Montrer que si f est injective alors pour tout sous-ensemble E de D on a $f^{-1}(f(E)) = E$.
- iii) Montrer la réciproque : si $f^{-1}(f(E)) = E$ pour tout sous-ensemble E de D , alors f est injective.

Exercice 21 Montrer que si les fonctions $f : A \rightarrow B$ et $g : B \rightarrow C$ sont injectives alors $g \circ f$ est injective.

Exercice 22 Soit $f : A \rightarrow B$ une fonction ; montrer que f est injective ssi pour toutes parties X et Y de A on a $f(X \cap Y) = f(X) \cap f(Y)$.

Surjection. Une fonction $f : D \rightarrow A$ est surjective si l'image de D est égale à A . Autrement dit pour tout élément y de A il existe un $x \in D$ tel que $y = f(x)$. On dit alors que f est une surjection de D sur A .

Exercice 23 Montrer l'équivalence entre ces deux définitions.

Exercice 24 La fonction vide de \emptyset dans \mathbb{N} est-elle surjective ?

Exercice 25 Montrer que si les fonctions $f : A \rightarrow B$ et $g : B \rightarrow C$ sont surjectives alors $g \circ f$ est surjective.

Exercice 26

- i) Montrer que pour tout $n \in \mathbb{N}^*$ (c'est à dire pour tout entier naturel non nul) il existe un unique entier k tel que $2^k \leq n < 2^{k+1}$.
- ii) On définit la fonction $\log_2 : \mathbb{N}^* \rightarrow \mathbb{N}$ par $\log_2(n) = k$ tel que $2^k \leq n < 2^{k+1}$. Montrer que \log_2 est surjective.

Exercice 27 Soit $f : X \rightarrow Y$ une fonction.

- i) Notons f' la fonction $Y \rightarrow \mathcal{P}(X)$ définie par $f'(y) = f^{-1}(\{y\})$ pour chaque $y \in Y$. Montrer que si f est surjective alors f' est injective.
- ii) À quelle condition sur f la fonction $f^{-1} : \mathcal{P}(Y) \rightarrow \mathcal{P}(X)$ est-elle injective ?
- iii) À quelle condition sur f la fonction $f^{-1} : \mathcal{P}(Y) \rightarrow \mathcal{P}(X)$ est-elle surjective ?

Bijection. Une fonction qui est à la fois injective et surjective est une bijection.

3.1 Théorème

Une fonction $f : A \rightarrow B$ est bijective ssi il existe une fonction $\varphi : B \rightarrow A$ telle que $\varphi \circ f = \text{Id}_A$ et $f \circ \varphi = \text{Id}_B$. Dans ce cas la fonction φ est uniquement déterminée par f (ce qui signifie que si $\psi : B \rightarrow A$ est une fonction telle que $\psi \circ f = \text{Id}_A$ et $f \circ \psi = \text{Id}_B$ alors $\psi = \varphi$). On la note f^{-1} et on l'appelle l'inverse de f (beaucoup d'auteurs appellent également f^{-1} la fonction réciproque de f). La fonction f^{-1} est bijective de B dans A et son inverse est f (c'est à dire que $(f^{-1})^{-1} = f$).

Si de plus $g : B \rightarrow C$ est également bijective alors $g \circ f$ est bijective et l'inverse de $g \circ f$ est $f^{-1} \circ g^{-1}$.

REMARQUE

Une fois de plus (et ça n'est pas la dernière) on utilise la même notation pour deux choses différentes : si B_0 est un sous-ensemble de B alors $f^{-1}(B_0)$ désigne l'image réciproque de B_0 qui est un sous-ensemble de A . Si y désigne un élément de B , alors $f^{-1}(y)$ désigne l'antécédent de y obtenu par la fonction inverse de f . Remarquons que on n'a besoin d'aucune hypothèse particulière sur f pour définir $f^{-1}(B_0)$ alors que $f^{-1}(y)$ n'est défini que si f est bijective.

Attention à la terminologie un peu particulière de ce cours. Il est fréquent d'appeler fonction réciproque ce que l'on appelle ici fonction inverse. D'autre part lorsque f est une fonction réelle qui ne s'annule pas, la fonction $1/f$ est souvent appelée fonction inverse de f . Cette terminologie, courante dans d'autres contextes, ne sera pas utilisée dans ce cours où l'on s'en tiendra à ce qui est défini ci-dessus.

REMARQUE

Un ensemble quelconque X est toujours en bijection avec lui-même puisque la fonction Id_X est une bijection de X sur X .

Exercice 28 Quelle est la fonction inverse de Id_X ?

3.2 Théorème

Soit $f : A \rightarrow B$ une fonction injective ; notons $B_0 = f(A)$ l'image par f de A et soit $f_0 : A \rightarrow B_0$ la fonction définie par $f_0(x) = f(x)$ pour tout $x \in A$. Alors f_0 est bijective.

En particulier si A est non vide, il existe une fonction surjective $g : B \rightarrow A$ telle que $g \circ f = \text{Id}_A$.

Preuve. La première partie du théorème est immédiate. Quant à la seconde, on remarque que comme f est injective, pour tout $y \in B$ il y a au plus un $x \in A$ tel que $f(x) = y$. On choisit un $x_0 \in A$ et on définit $g : B \rightarrow A$ par $g(y) =$ le x tel que $f(x) = y$ si il y en a un, x_0 sinon. On a donc $g(f(x)) = x$ pour tout $x \in A$. De plus g est surjective puisque pour tout $x \in A$ il y a un $y \in B$ tel que $g(y) = x$; il suffit de prendre $y = f(x)$.

REMARQUE

On applique très souvent ce théorème sous la forme suivante : si $f : A \rightarrow B$ est injective alors on dit que f est une bijection entre A et $f(A)$. En toute rigueur il ne s'agit pas de la même fonction f (puisque elles n'ont pas le même ensemble d'arrivée) mais ici aussi on utilise le même nom pour deux objets (pas très) différents.

Exercice 29 Pourquoi faut-il l'hypothèses $A \neq \emptyset$ dans la 2ème partie du théorème ?

3.3 Théorème

Soit $f : A \rightarrow B$ une surjection. Il existe une fonction injective $g : B \rightarrow A$ telle que $f \circ g = \text{Id}_B$.

Preuve. Comme f est surjective, pour chaque $y \in B$ l'ensemble $f^{-1}(\{y\}) = \{x \in A \text{ tel que } f(x) = y\}$ est non vide.

Soit x_y un élément de cet ensemble; définissons $g : B \rightarrow A$ par $g(y) = x_y$. Alors $f \circ g(y) = f(x_y)$. Mais par définition $x_y \in f^{-1}(\{y\})$. Donc $f(x_y) = y$ et on a montré que $f \circ g(y) = y$ pour tout $y \in B$.

De plus si $y \neq y'$ alors $f^{-1}(\{y\}) \cap f^{-1}(\{y'\}) = \emptyset$ donc $x_y \neq x_{y'}$ ce qui montre que g est injective.

Lorsqu'il existe une bijection entre deux ensembles A et B on dit que A et B sont en bijection ou qu'ils sont *équipotents*.

Le théorème suivant résume quelques propriétés utiles des fonctions.

3.4 Théorème

Soient $f : A \rightarrow B$ et $g : B \rightarrow C$ deux fonctions.

Si f est bijective alors $g \circ f$ est injective (resp. surjective, bijective) ssi g est injective (resp. surjective, bijective).

Si g est bijective alors $g \circ f$ est injective (resp. surjective, bijective) ssi f est injective (resp. surjective, bijective).

Exercice 30 Pour chacune des fonctions suivantes, dire si elle est injective, surjective et/ou bijective. Dans le cas où la fonction est bijective on donnera sa fonction inverse :

$$\begin{array}{cccccc}
 f_1 : \mathbb{N} \rightarrow \mathbb{N} & f_2 : \mathbb{N} \rightarrow \mathbb{N} & f_3 : \mathbb{N} \rightarrow \mathbb{Z} & f_4 : \mathbb{N} \rightarrow \mathbb{N} & f_5 : \mathbb{Z} \rightarrow \mathbb{Z} & f_6 : \mathbb{Z} \rightarrow \mathbb{Z} \\
 x \mapsto 0 & x \mapsto x & x \mapsto x & x \mapsto x + 1 & x \mapsto x + 1 & x \mapsto -x \\
 \\
 f_7 : \mathbb{Z} \rightarrow \mathbb{Z} & f_8 : \mathbb{Z} \rightarrow \mathbb{N} & f_9 : \mathbb{Z} \rightarrow \mathbb{Z} & f_{10} : \mathbb{Q} \rightarrow \mathbb{Q} & f_{11} : \mathbb{Q}^* \rightarrow \mathbb{Q}^* \\
 x \mapsto |x| & x \mapsto |x| & x \mapsto 2x & x \mapsto 2x & x \mapsto 1/x \\
 \\
 f_{12} : \mathbb{Q} \rightarrow \mathbb{Q}^+ & f_{13} : \mathbb{Q}^+ \rightarrow \mathbb{Q}^+ & f_{14} : \mathbb{R} \rightarrow \mathbb{R}^+ & f_{15} : \mathbb{R}^+ \rightarrow \mathbb{R}^+ & f_{16} : \mathbb{R} \rightarrow \mathbb{R} \\
 x \mapsto x^2 & x \mapsto x^2 & x \mapsto x^2 & x \mapsto x^2 & x \mapsto x^3 \\
 \\
 f_{17} : \mathbb{R} \rightarrow \mathbb{R} & f_{18} : \mathbb{R} \rightarrow [-1, 1] & f_{19} : [-\pi/2, \pi/2] \rightarrow \mathbb{R} & f_{20} : [-\pi/2, \pi/2] \rightarrow [-1, 1] \\
 x \mapsto \sin x & x \mapsto \sin x & x \mapsto \sin x & x \mapsto \sin x
 \end{array}$$

Exercice 31 Pour chacune des fonctions suivantes, dire si elle est injective, surjective et/ou bijective. Dans le cas où la fonction est bijective on donnera sa fonction inverse.

- i) $f : \mathbb{N} \rightarrow \mathbb{N}$ définie par :
 - $f(n) = n/2$ si n est pair ;
 - $f(n) = (n - 1)/2$ si n est impair.
- ii) $f : \mathbb{Z} \rightarrow \mathbb{N}$ définie par :
 - $f(n) = 2n$ si $n \geq 0$;
 - $f(n) = -2n - 1$ si $n < 0$.
- iii) $f : \mathbb{N} \rightarrow \mathbb{N}$ définie par :
 - $f(n) = n$ si n est un multiple de 3 ;
 - $f(n) = n + 1$ si n est de la forme $3k + 1$;
 - $f(n) = n - 1$ si n est de la forme $3k + 2$.
- iv) $f : \mathbb{N}^2 \rightarrow \mathbb{N}$ définie par $f(n, p) = (n + p)(n + p + 1)/2 + p$.
- v) $f : \mathbb{N} \rightarrow \mathbb{N}$ définie par :
 - $f(0) = 0$;
 - si $10^k \leq n < 10^{k+1}$ alors $f(n) = b_1 + b_2 10 + \dots + b_k 10^{k-1} + b_0 10^k$ où les b_i sont les chiffres de l'écriture de n en base 10, c'est à dire que $n = b_0 + b_1 10 + \dots + b_k 10^k$.

3.2.3 Constructions avec ensembles et fonctions

3.5 Théorème

Si X_1 et X_2 sont deux ensembles en bijection, et Y_1 et Y_2 sont deux autres ensembles en bijection alors :

Produit $X_1 \times Y_1$ est en bijection avec $X_2 \times Y_2$; pour tout entier naturel k , X_1^k est en bijection avec X_2^k .

Parties $\mathcal{P}(X_1)$ est en bijection avec $\mathcal{P}(X_2)$.

Fonctions $Y_1^{X_1}$ est en bijection avec $Y_2^{X_2}$

Preuve. On ne montre que la dernière propriété (fonctions), les autres sont laissées en exercice. Soit $\varphi : X_1 \rightarrow X_2$ une bijection et $\psi : Y_1 \rightarrow Y_2$ une autre bijection ; les deux existent par hypothèse. Soit maintenant $f \in Y_1^{X_1}$ une fonction de X_1 dans Y_1 . Alors $\psi \circ f \circ \varphi^{-1}$ est une fonction de X_2 dans Y_2 , c'est à dire un élément de $Y_2^{X_2}$. Notons $\Phi : Y_1^{X_1} \rightarrow Y_2^{X_2}$ la fonction définie par $\Phi(f) = \psi \circ f \circ \varphi^{-1}$. On définit de même $\Psi' : Y_2^{X_2} \rightarrow Y_1^{X_1}$ par $\Psi'(g) = \psi^{-1} \circ g \circ \varphi$. Mais alors on a $\Psi'(\Phi(f)) = \Psi'(\psi \circ f \circ \varphi^{-1}) = \psi^{-1} \circ \psi \circ f \circ \varphi^{-1} \circ \varphi = f$ et de même $\Phi(\Psi'(g)) = g$. La fonction Ψ' est donc l'inverse de Φ , qui est donc une bijection.

Fonctions caractéristiques. Soit E un ensemble non vide. Toute partie F de E détermine une unique fonction $\chi_F : E \rightarrow \{0, 1\}$ appelée *fonction caractéristique* de F dans E et définie par : $\chi_F(x) = 1$ si $x \in F$, 0 sinon.

Exercice 32

- i) Quelle est la fonction caractéristique de l'ensemble vide ? de l'ensemble E tout entier ?
- ii) Supposons que $E = \mathbb{N}$ est l'ensemble des entiers naturels. Quelle est la fonction caractéristique de l'ensemble des entiers pairs ? de l'ensemble des carrés parfaits ?
- iii) Soient F et G deux sous-ensembles de E et χ_F, χ_G leurs fonctions caractéristiques. Quelles sont, en fonction de χ_F et χ_G , les fonctions caractéristiques de F^c ? de $F \cup G$? de $F \cap G$.

Réciproquement étant donnée une fonction $\chi : E \rightarrow \{0, 1\}$, celle-ci détermine une unique partie de E de E définie par : $E_\chi = \{x \in E \text{ tel que } \chi(x) = 1\}$. Par conséquent si on note D l'ensemble $\{0, 1\}$, il y a une bijection de D^E (ensemble des fonctions de E dans D) dans $\mathcal{P}(E)$.

Produit cartésien. Soient X_1, \dots, X_n des ensembles. Le produit cartésien des X_i noté $X_1 \times \dots \times X_n$ est l'ensemble des fonctions $c : [1, n] \rightarrow X_1 \cup \dots \cup X_n$ telles que pour $i = 1, \dots, n$ on ait $c(i) \in X_i$. Une telle fonction est appelée un *n-uplet* ; si $c(i) = x_i$ pour $i = 1, \dots, n$, le *n-uplet* c est noté (x_1, \dots, x_n) .

REMARQUE

Si l'un des X_i est vide il n'existe aucune fonction c telle que $c(i) \in X_i$, donc le produit cartésien $X_1 \times \dots \times X_n$ est vide.

REMARQUE

Si $n = 0$ la définition fonctionne toujours : le produit cartésien de 0 ensemble est l'ensemble des fonctions de $[1, 0]$ dans l'ensemble vide (car la réunion des X_i est l'ensemble vide) mais comme $[1, 0]$ est également l'ensemble vide, le produit cartésien est réduit à l'unique fonction de \emptyset dans \emptyset . Cette unique fonction est notée $()$.

Si $n = 2$, les éléments du produits cartésien $X_1 \times X_2$ sont appelés des *couples*. Si $n = 3$ ce sont des *triplets*. Si $X_1 = \dots = X_n = X$ le produit cartésien $X_1 \times \dots \times X_n$ est noté X^n .

Exercice 33 Soient n et p deux entiers naturels.

- i) Montrer que $[1, n] \times [1, p]$ est en bijection avec $[1, np]$.
- ii) On note $[1, n] + [1, p]$ l'ensemble $\{0\} \times [1, n] \cup \{1\} \times [1, p]$. Montrer que $[1, n] + [1, p]$ est en bijection avec $[1, n + p]$.

Fonctions de plusieurs variables. Le produit cartésien est une opération très utilisée, au moins implicitement, car il permet de définir des fonctions de plusieurs variables. Une fonction de plusieurs variables est simplement une fonction définie sur un produit cartésien d'ensembles. Par exemple une fonction de deux variables réelles est une fonction définie sur \mathbb{R}^2 .

REMARQUE

Les opérations comme l'addition sur les entiers ou le produit scalaire de vecteurs sont des fonctions de deux variables : l'addition sur les entiers est définie sur \mathbb{N}^2 , le produit scalaire de vecteurs de \mathbb{R}^2 est défini sur $(\mathbb{R}^2)^2$.

Fonctions surjectives et partitions. Soient $f : X \rightarrow Y$ une fonction surjective. Alors l'ensemble des images réciproques des éléments de Y forme une partition de $X : \{f^{-1}(\{y\}), y \in Y\}$.