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 extrêment 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 même 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 résoud 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 classifie 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 connait 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* quelquechose : 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 $f : X \to Y$ 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 a 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.

Surcharge[1] **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 ambigüité.

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 $f : [a,b] \to \mathbb{R}$ 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 $f : \mathbb{R} \to \mathbb{R}$; 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 $f : \mathbb{N} \to \mathbb{N}$ 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 $f : X \to X$ 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'explicite 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 $1 + 2 + \cdots + n$ 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 :

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

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 *nombres entiers* ni les *ensembles* dans ce cours, on va se fier à l'idée qu'on en 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 utiliser 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 connait (au moins) une *démonstration* ; il existe également des énoncés mathématiques dont on *pense* qu'ils sont vrais mais dont on ne connait 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 entier 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 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 une 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.

« $\exists! z \in \mathbb{N}, \forall n \in \mathbb{N},\ n+z=z+n=n$ », « $\forall x \in \mathbb{R},$ si $x \neq 0$ alors $\exists! y \in \mathbb{R}$ 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'élement 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 vrai 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 fausse. Si on parvient à démontrer la conclusion dans les deux cas, alors celle-ci est toujours vraie et le théorème est démontrée.

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 fausse 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 fausse et on en déduit que l'une des hypothèses est fausse.

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 : $\{1, 2, 3, \ldots\}$ 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-là[1]. 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 $\{k \in \mathbb{Z} \text{ tel que } n \leq k \leq p\} = \{n, n+1, \ldots, p\}$. 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 $X_1, \ldots, X_n$ des ensembles. La réunion des X_i est notée $X_1 \cup \cdots \cup X_n$ ou encore $\bigcup_{i=0}^{n} X_i$. 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 $X_1, \ldots, X_n$ des ensembles. L'intersection des X_i est notée $X_1 \cap \cdots \cap X_n$ ou encore $\bigcap_{i=0}^{n} X_i$.

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

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

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

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

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. : $P = \{\{kp, k \in \mathbb{N}\}, \{kp+1, k \in \mathbb{N}\}, \ldots, \{kp+p-1, k \in \mathbb{N}\}\}$.
>
> On peut par exemple partitionner l'ensemble des fonctions de $\mathbb{N}$ dans $\mathbb{N}$ selon la valeur des fonctions en 0 : $P = \{\{f : \mathbb{N} \to \mathbb{N}, f(0) = 0\}, \{f : \mathbb{N} \to \mathbb{N}, f(0) = 1\}, \{f : \mathbb{N} \to \mathbb{N}, f(0) = 2\}, \ldots\}$.

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 $f : D \to A$; la valeur de f en x est notée $f(x)$.

EXEMPLE.

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

La fonction *nulle* $0 : \mathbb{R} \to \mathbb{R}$ 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 $f : D \to A$ et $f' : D' \to A'$ 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 $\mathrm{Id}_X : X \to X$ définie par $\mathrm{Id}_X(x) = x$ 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* $i : X \to Y$ 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 $f : D \to A$ 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 $\mathrm{im}\, f$.

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 $f : D \to A$ 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 $f : D \to A$ 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 $f|_E : E \to A$ définie par $f|_E(x) = f(x)$ pour tout $x \in E$.

Composition. Soient $f : A \to B$ et $g : B \to C$; la composée de f et g est la fonction $g \circ f : A \to C$ 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 $f : A \to B$ une fonction.

i) Montrer que $f \circ \mathrm{Id}_A = \mathrm{Id}_B \circ f = f$.

ii) Montrer que la composition est *associative* : si $g : B \to C$ et $h : C \to D$ sont deux autres fonctions alors $h \circ (g \circ f) = (h \circ g) \circ f$.

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

Exercice 17 Notons f_n la fonction sur A définie par récurrence par : $f_0 = \mathrm{Id}_A$ 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 $f : D \to A$ une fonction. On dit que f est injective si les éléments de D ont des images deux à deux distinctes. Symboliquement :

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

On peut contraposer cet énoncé et obtenir une définition équivalente :

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

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 $f : \mathbb{N} \to \mathbb{N}$ telle que pour tout $k \in \mathbb{N}$ on ait $f(2k+1) < 2k+1$.

ii) Soit $f : \mathbb{N} \to \mathbb{N}$. 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 $f : D \to A$ 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 $f : A \to B$ et $g : B \to C$ sont injectives alors $g \circ f$ est injective.

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

Surjection. Une fonction $f : D \to A$ 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 $f : A \to B$ et $g : B \to C$ 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 $\log_2 : \mathbb{N}^* \to \mathbb{N}$ par $\log_2(n) = k$ tel que $2^k \leq n < 2^{k+1}$. Montrer que $\log_2$ est surjective.

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

i) Notons f' la fonction $Y \to \mathcal{P}(X)$ 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 $f^{-1} : \mathcal{P}(Y) \to \mathcal{P}(X)$ est-elle injective ?

iii) À quelle condition sur f la fonction $f^{-1} : \mathcal{P}(Y) \to \mathcal{P}(X)$ est-elle surjective ?

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

3.1 Théorème
*Une fonction $f : A \to B$ est bijective ssi il existe une fonction $\varphi : B \to A$ telle que $\varphi \circ f = \mathrm{Id}_A$ et $f \circ \varphi = \mathrm{Id}_B$. Dans ce cas la fonction φ est uniquement déterminée par f (ce qui signifie que si $\psi : B \to A$ est une fonction telle que $\psi \circ f = \mathrm{Id}_A$ et $f \circ \psi = \mathrm{Id}_B$ 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 $g : B \to C$ 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 $f : A \to B$ une fonction injective ; notons $B_0 = f(A)$ l'image par f de A et soit $f_0 : A \to B_0$ 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 $g : B \to A$ telle que $g \circ f = \mathrm{Id}_A$.

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 $g : B \to A$ 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 $f : A \to B$ 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 (puisqu'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 $f : A \to B$ une surjection. Il existe une fonction injective $g : B \to A$ telle que $f \circ g = \mathrm{Id}_B$.

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 $g : B \to A$ 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 $f : A \to B$ et $g : B \to C$ 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 :

$$f_1 : \mathbb{N} \to \mathbb{N},\ x \mapsto 0 \qquad f_2 : \mathbb{N} \to \mathbb{N},\ x \mapsto x \qquad f_3 : \mathbb{N} \to \mathbb{Z},\ x \mapsto x \qquad f_4 : \mathbb{N} \to \mathbb{N},\ x \mapsto x+1 \qquad f_5 : \mathbb{Z} \to \mathbb{Z},\ x \mapsto x+1 \qquad f_6 : \mathbb{Z} \to \mathbb{Z},\ x \mapsto -x$$

$$f_7 : \mathbb{Z} \to \mathbb{Z},\ x \mapsto |x| \qquad f_8 : \mathbb{Z} \to \mathbb{N},\ x \mapsto |x| \qquad f_9 : \mathbb{Z} \to \mathbb{Z},\ x \mapsto 2x \qquad f_{10} : \mathbb{Q} \to \mathbb{Q},\ x \mapsto 2x \qquad f_{11} : \mathbb{Q}^* \to \mathbb{Q}^*,\ x \mapsto 1/x$$

$$f_{12} : \mathbb{Q} \to \mathbb{Q}^+,\ x \mapsto x^2 \qquad f_{13} : \mathbb{Q}^+ \to \mathbb{Q}^+,\ x \mapsto x^2 \qquad f_{14} : \mathbb{R} \to \mathbb{R}^+,\ x \mapsto x^2 \qquad f_{15} : \mathbb{R}^+ \to \mathbb{R}^+,\ x \mapsto x^2 \qquad f_{16} : \mathbb{R} \to \mathbb{R},\ x \mapsto x^3$$

$$f_{17} : \mathbb{R} \to \mathbb{R},\ x \mapsto \sin x \qquad f_{18} : \mathbb{R} \to [-1,1],\ x \mapsto \sin x \qquad f_{19} : [-\pi/2, \pi/2] \to \mathbb{R},\ x \mapsto \sin x \qquad f_{20} : [-\pi/2, \pi/2] \to [-1,1],\ x \mapsto \sin x$$

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) $f : \mathbb{N} \to \mathbb{N}$ définie par :
- $f(n) = n/2$ si n est pair ;
- $f(n) = (n-1)/2$ si n est impair.

ii) $f : \mathbb{Z} \to \mathbb{N}$ définie par :
- $f(n) = 2n$ si $n \geq 0$;
- $f(n) = -2n - 1$ si $n < 0$.

iii) $f : \mathbb{N} \to \mathbb{N}$ 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) $f : \mathbb{N}^2 \to \mathbb{N}$ définie par $f(n, p) = (n + p)(n + p + 1)/2 + p$.

v) $f : \mathbb{N} \to \mathbb{N}$ définie par :
- $f(0) = 0$;
- si $10^k \leq n < 10^{k+1}$ alors $f(n) = b_1 + b_2 10 + \cdots + b_k 10^{k-1} + b_0 10^k$ où les b_i sont les chiffres de l'écriture de n en base 10, c'est à dire que $n = b_0 + b_1 10 + \cdots + b_k 10^k$.

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 $\varphi : X_1 \to X_2$ une bijection et $\psi : Y_1 \to Y_2$ 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 $\Phi : Y_1^{X_1} \to Y_2^{X_2}$ la fonction définie par $\Psi(f) = \psi \circ f \circ \varphi^{-1}$. On définit de même $\Psi' : Y_2^{X_2} \to Y_1^{X_1}$ par $\Psi'(g) = \psi^{-1} \circ g \circ \varphi$. Mais alors on a $\Psi'(\Psi(f)) = \Psi'(\psi \circ f \circ \varphi^{-1}) = \psi^{-1} \circ \psi \circ f \circ \varphi^{-1} \circ \varphi = f$ et de même $\Psi(\Psi'(g)) = g$. La fonction Ψ' est donc l'inverse de Ψ, qui est donc une bijection.

Fonctions caractéristiques. Soit E un ensemble non vide. Toute partie F de E détermine une unique fonction $\chi_F : E \to \{0,1\}$ 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 $\chi : E \to \{0,1\}$, celle-ci détermine une unique partie de E_χ 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, ..., X_n des ensembles. Le produit cartésien des X_i noté $X_1 \times \cdots \times X_n$ est l'ensemble des fonctions $c : [1,n] \to X_1 \cup \cdots \cup X_n$ telles que pour $i = 1, \ldots, n$ on ait $c(i) \in X_i$. Une telle fonction est appelée un *n-uplet* ; si $c(i) = x_i$ pour $i = 1, \ldots, n$, le n-uplet c est noté $(x_1, \ldots, x_n)$.

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 $X_1 \times X_n$ 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 $X_1 = \cdots = X_n = X$ le produit cartésien $X_1 \times \ldots X_n$ 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 variable 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 $f : X \to Y$ une fonction surjective. Alors l'ensemble des images réciproques des éléments de Y forme une partition de X : $\{f^{-1}(\{y\}), y \in Y\}$.

Chapitre 4

Dénombrement, combinatoire élémentaire

On rappelle que la notation $[a, b]$ désigne l'intervalle des *entiers* compris entre a et b.

4.1 Ensembles finis

Dans cette partie on va définir les notions d'ensembles finis, de cardinal d'un ensemble fini et établir quelques propriétés élémentaires des ensembles finis. On passera ensuite aux ensembles infinis en exposant la différence entre le dénombrable et le continu.
On commence par établir quelques propriétés des ensembles d'entiers qui nous seront utiles par la suite.

4.1 Théorème
Soient n et p deux entiers naturels. On a les propriétés suivantes :
- *$n \leq p$ ssi il existe une injection de $[1, n]$ dans $[1, p]$;*
- *$n \geq p$ ssi il existe une surjection de $[1, n]$ dans $[1, p]$;*
- *$n = p$ ssi il existe une bijection de $[1, n]$ dans $[1, p]$;*
- *si $n = p$ et il y a une injection $f : [1, n] \to [1, p]$ alors f est une bijection ;*
- *si $n = p$ et il y a une surjection $f : [1, n] \to [1, p]$ alors f est une bijection ;*

Preuve. Le troisième cas est conséquence des deux précédents. En effet si $n = p$ alors la fonction $\mathrm{Id}_{[1,n]}$ est une bijection sur $[1, n]$ et réciproquement si il existe une fonction $f : [1, n] \to [1, p]$ bijective, alors comme f est injective on a $n \leq p$ et comme f est surjective on a $n \geq p$ par les deux cas précédents, donc $n = p$.

Pour montrer le premier cas supposons $n \leq p$. Dans ce cas l'injection canonique $\iota : [1, n] \to [1, p]$ définie par $\iota(x) = x$ pour $x \in [1, n]$ est une injection.

On montre en même temps la réciproque et la 4ème propriété du théorème. Plus précisément on montre par récurrence sur n que pour tout $p \in \mathbb{N}$, si il existe une injection $f : [1, n] \to [1, p]$ alors $n \leq p$; si de plus $n = p$ alors f est une bijection.

Si $n = 0$ alors $[1, n]$ est l'ensemble vide et f est nécessairement l'application vide qui est injective (pourquoi ?). Si de plus $p = 0$ alors l'application vide est surjective, donc est bien une bijection.

Supposons la propriété vraie pour n et soit $f : [1, n + 1] \to [1, p]$ une fonction injective. Il faut montrer que $n + 1 \leq p$. Remarquons que l'on a nécessairement $p > 0$, sinon $[1, p]$ est l'ensemble vide et il ne saurait y avoir de fonction de $[1, n + 1]$ (qui est non vide) dans $[1, p]$.

Si $f(n + 1) = p$ alors comme f est supposée injective, pour tout $x \in [1, n]$ on a $f(x) \neq p$. Soit $f' = f|_{[1,n]}$ la restriction de f à $[1, n]$. Comme f est injective, f' l'est aussi. De plus comme $f'(x) \neq p$ pour tout $x \in [1, n]$, f' est à valeurs dans $[1, p - 1]$. Autrement dit f' est une injection de $[1, n]$ dans $[1, p - 1]$. Par hypothèse de récurrence on en déduit que $n \leq p - 1$, donc que $n + 1 \leq p$.

Si de plus $n+1=p$ alors $n=p-1$ et l'hypothèse de récurrence nous dit que f' est alors une bijection; en particulier pour tout $y \in [1,p-1]$ il y a un $x \in [1,n]$ tel que $f'(x)=y$. Comme $f'=f|_{1,n]}$ et $f(n+1)=p$, on en déduit que f est surjective, donc bijective.

Supposons pour finir que $f(n+1)=q \neq p$. Soit $\tau : [1,p] \to [1,p]$ la *transposition* de p et q définie par $\tau(x)=x$ si $x \neq p,q$, $\tau(p)=q$ et $\tau(q)=p$ (τ est la fonction qui échange p et q, en laissant tous les autres éléments de $[1,p]$ invariants). On vérifie facilement que $\tau \circ \tau = \mathrm{Id}_{[1,p]}$, c'est à dire que τ est sa propre fonction inverse[1]. On en déduit que τ est une bijection de $[1,p]$ dans $[1,p]$. Soit $f'=\tau \circ f$. Alors f' est une fonction de $[1,n+1]$ dans $[1,p]$ qui est composée de deux fonctions injectives; f' est donc une injection. De plus on a $f'(n+1)=\tau(f(n+1))=\tau(q)=p$. On est donc ramené au cas précédent et on a vu que l'on peut en déduire que $n+1 \leq p$.

Si de plus $p=n+1$ alors on a vu que f' est bijective, mais comme $f'=\tau \circ f$ on obtient $f=\tau \circ f'$ en composant par τ à gauche. Donc f est bijective puisque elle est la composée de deux fonctions bijectives.

Montrons enfin la deuxième et la cinquième propriété. Si $n \geq p$ alors la fonction $f : [1,n] \to [1,p]$ définie par $f(i)=i$ si $i \leq p$ et $f(i)=p$ si $i>p$ est clairement une surjection.

Réciproquement supposons qu'il existe une fonction $f : [1,n] \to [1,p]$ surjective. Soit $g : [1,p] \to [1,n]$ définie par $g(y)$ est le plus petit $x \in [1,n]$ tel que $f(x)=y$. Pour tout $y \in [1,p]$ un tel x existe puisque f est surjective; la fonction g est donc bien définie. Elle est injective; en effet soient $y,y' \in [1,p]$ tels que $g(y)=g(y')$. Par définition de g on a $f(g(y))=y$ et $f(g(y'))=y'$ et comme $g(y)=g(y')$ on en déduit que $y=y'$. Comme $g : [1,p] \to [1,n]$ est injective, on peut appliquer le résultat précédent et en déduire que $p \leq n$.

Si de plus $n=p$ on en déduit que g est bijective, donc admet une fonction inverse g^{-1} qui est également bijective. Mais on a vu que $f \circ g = \mathrm{Id}_{[1,p]}$, donc en composant à droite par g^{-1} on obtient $f=g^{-1}$, et f est donc bijective.

Exercice 1 Soient n et p deux entiers naturels.

i) Montrer les cinq propriétés du théorème mais en considérant cette fois les intervalles $[0,n]$ et $[0,p]$.

ii) Qu'est ce qui devient faux si on considère les intervalles $[2,n]$ et $[2,p]$?

4.1.1 Cardinaux finis

Un ensemble F est fini si il existe un entier naturel n tel que F et $[1,n]$ soient en bijection.

REMARQUE

L'ensemble vide est fini puisqu'il est est égal à l'ensemble $[1,0]$ et que tout ensemble est en bijection avec lui-même.

Exercice 2 Montrer que :

i) Si X est en bijection avec Y et Y est fini alors X est fini.

ii) Pour tous entiers n, p, l'ensemble $[n,p]$ est fini.

iii) Si $X \subset [1,n]$ alors X est fini.

iv) Si $X \subset Y$ et Y est fini alors X est fini.

v) Si il y a une injection de X dans Y et Y est fini alors X est fini.

vi) Si il y a une surjection de X dans Y et X est fini alors Y est fini.

vii) Si X et Y sont finis alors $X \cup Y$ et $X \cap Y$ sont finis.

4.2 Théorème
Si F est en bijection avec $[1,n]$ et avec $[1,p]$ alors $n=p$.

Preuve. Notons $\phi : F \to [1,n]$ la première bijection, et $\psi : F \to [1,p]$ la seconde. Alors $\psi \circ \phi^{-1}$ est une bijection de $[1,n]$ dans $[1,p]$ et le théorème 4.1 nous dit que $n=p$.

1. Une telle fonction, égale à sa fonction inverse, est appelée une *involution*.

Cardinal d'un ensemble fini. Le cardinal de l'ensemble fini F est l'unique entier n tel que F est en bijection avec $[1, n]$; on le note $|F|$.

4.1.2 Propriétés élémentaires des cardinaux finis

4.3 Théorème
Soient F et G deux ensembles finis. On a :
– $|F| \leq |G|$ ssi il existe une injection de F dans G ;
– $|F| \geq |G|$ ssi il existe une surjection de F sur G ;
– $|F| = |G|$ ssi il existe une bijection de F sur G.

Preuve. Notons $n = |F|$ et $p = |G|$. Par définition des cardinaux il existe deux bijections $\phi : F \to [1, n]$ et $\psi : G \to [1, p]$.

Supposons que $|F| \leq |G|$. D'après le théorème 4.1 cela entraîne qu'il existe une injection $f : [1, n] \to [1, p]$. Mais alors $\psi^{-1} \circ f \circ \phi$ est une injection de F dans G.

Réciproquement supposons qu'il existe une injection $f : F \to G$. Alors $\psi \circ f \circ \phi^{-1}$ est une injection de $[1, n]$ dans $[1, p]$ et le théorème 4.1 nous dit que $|F| = n \leq p = |G|$.

Les deux autres cas se démontrent de manière analogue.

Ce théorème a un corollaire souvent utilisé pour montrer que deux ensembles finis sont en bijection.

4.4 Corollaire
Soient X et Y deux ensembles finis. Si il existe une injection de X dans Y et une autre injection de Y dans X alors il existe une bijection de X dans Y.
De même si il existe une surjection de X dans Y et une autre surjection de Y dans X alors il existe une bijection de X dans Y.

Preuve. Si il existe une injection de X dans Y alors on a vu que $|X| \leq |Y|$. De même s'il existe une injection de Y dans X on a $|Y| \leq |X|$. Donc les deux cardinaux sont égaux ce qui entraine qu'il existe une bijection de X dans Y.

Le cas des surjections est analogue.

Voici un théorème qui renforce légèrement le corollaire précédent.

4.5 Théorème
Soient X et Y deux ensembles finis et supposons que $|X| \leq |Y|$:
– si $f : Y \to X$ est une injection, alors f est une bijection ;
– si $g : X \to Y$ est une surjection alors g est une bijection.

Preuve. On sait déjà que l'existence d'une injection de Y dans X entraine que $|Y| \leq |X|$. Donc $|X| = |Y|$, c'est à dire qu'il y a un entier naturel n et deux bijections $\varphi : X \to [1, n]$ et $\psi : Y \to [1, n]$. Par conséquent la composée $\varphi \circ f \circ \psi^{-1}$ est une injection de $[1, n]$ dans $[1, n]$ et c'est donc une bijection d'après le théorème 4.1. On en déduit immédiatement que f est une bijection.

Un raisonnement analogue montre que g est une bijection.

4.6 Théorème
Soient X et Y deux ensembles finis. Alors les ensembles $X \cup Y$, $X \times Y$, Y^X et $\mathcal{P}(X)$ sont finis et on a les relations suivantes :

Somme *Si X et Y sont disjoints alors $|X \cup Y| = |X| + |Y|$.*

Sous-ensemble *Si $Y \subset X$ alors $|Y| + |Y^c| = |X|$.*

Réunion *si X et Y sont quelconques (finis) on a $|X \cup Y| = |X| + |Y| - |X \cap Y|$.*

Produit $|X \times Y| = |X| \,.\, |Y|$.

Puissance *Si k est un entier,* $\left|X^k\right| = |X|^k$

Fonctions $\left|Y^X\right| = |Y|^{|X|}$.

Parties $|\mathcal{P}(X)| = 2^{|X|}$.

Preuve. Puisque X et Y sont supposés finis, notons $n = |X|$ et $p = |Y|$ et soient $\varphi_X : X \to [1, n]$ et $\varphi_Y : Y \to [1, p]$ deux bijections.

Somme. Supposons X et Y disjoints. On définit une fonction $\psi : X \cup Y \to [1, n + p]$ par :
– si $x \in X$ alors $\psi(x) = \varphi_X(x)$;
– sinon puisque $x \notin X$ mais $x \in X \cup Y$, on doit avoir $x \in Y$ et on définit $\psi(x) = \varphi_Y(x) + n$
Soient $x, x' \in X \cup Y$ tels que $\psi(x) = \psi(x')$. Si $\psi(x) \leq n$ alors par définition de ψ les éléments x et x' sont dans X et on a $\varphi_X(x) = \varphi_X(x')$; par injectivité de φ_X on en déduit que $x = x'$.

Si maintenant $\psi(x) > n$ alors par définition de ψ on doit avoir $x, x' \in Y$ et $\psi(x) = \varphi_Y(x)+n$, $\psi(x') = \varphi_Y(x')+n$. Donc $\varphi_Y(x) = \varphi_Y(x')$ et par injectivité de φ_Y on en déduit à nouveau que $x = x'$. La fonction ψ est donc injective.

Soit finalement $i \in [1, n + p]$. Si $i \leq n$ alors il existe $x \in X$ tel que $\varphi_X(x) = i$, donc tel que $\psi(x) = i$. Si $i > n$ alors il existe $x \in Y$ tel que $\varphi_Y(x) = i - n$. Mais comme Y est disjoint de X, x n'est pas dans X et par définition de ψ on a donc $\psi(x) = \varphi_Y(x) + n = i$. Dans les deux cas on a bien trouvé $x \in X \cup Y$ tel que $\psi(x) = i$; la fonction ψ est surjective, et donc bijective.

Sous-ensemble. Supposons que $Y \subset X$; on sait que $Y \cup Y^c = X$ et que Y et Y^c sont disjoints. La relation précédente nous donne le résultat.

Réunion. Notons $Z = X \cap Y$. Soit Z' le complémentaire de Z dans X ; par la relation précédente on a $|Z|+|Z'| = |X|$. Soit Z'' le complémentaire de Z dans Y. On a de même $|Y| = |Z|+|Z''|$. Mais $X \cup Y = Z \cup Z' \cup Z''$ et Z, Z' et Z'' sont deux à deux disjoints. On a donc $|X \cup Y| = |Z| + |Z'| + |Z''|$, d'où le résultat.

Produit On raisonne par récurrence sur n (le cardinal de X). Si $n = 0$ alors X est l'ensemble vide et $X \times Y$ est également l'ensemble vide dont le cardinal est $0 = |X| \, . \, |Y|$.

Supposons $n > 0$ et le résultat vrai pour $n - 1$. Notons $x = \varphi_X^{-1}(n)$ et $X' = X \backslash \{x\}$. On vérifie facilement que $\varphi_X|_{X'}$ est une bijection de X' dans $[1, n - 1]$. Par hypothèse de récurrence on a donc $|X' \times Y| = (n - 1) \, |Y|$.

Mais on a $|\{x\} \times Y| = |Y|$ car la fonction de $\{x\} \times Y$ dans Y qui à (x, y) associe y pour chaque $y \in Y$ est bijective. De plus $X' \times Y$ et $\{x\} \times Y$ sont disjoints et leur réunion est $X \times Y$. Donc $|X \times Y| = |X' \times Y| + |\{x\} \times Y| = (n - 1) \, |Y| + |Y| = n \, |Y|$ et le théorème est démontré.

Puissance Par récurrence sur k. Si $k = 0$ alors on a vu que X^k est un singleton, donc $\left|X^k\right| = 1 = |X|^0$.

Supposons le résultat vrai pour k. Soit $\varphi : X^k \times X \to X^{k+1}$ définie par $\varphi((x_1, \ldots, x_k), x) = (x_1, \ldots, x_k, x)$. On voit facilement que φ est une bijection, donc $\left|X^{k+1}\right| = \left|X^k \times X\right| = \left|X^k\right| \, . \, |X|$ par la propriété de produit démontrée précédemment. Mais $\left|X^k\right| = |X|^k$ par hypothèse de récurrence. On obtient donc finalement $\left|X^{k+1}\right| = |X|^k \, . \, |X| = |X|^{k+1}$.

Fonctions Pour $i = 1, \ldots n$ on note $x_i = \varphi_X^{-1}(i)$. On a donc $X = \{x_1, \ldots, x_n\}$. On définit une fonction $\psi : Y^X \to Y^n$ de la façon suivante : si $f : X \to Y$ est un élément de Y^X alors $\psi(f) = (f(x_1), \ldots, f(x_n))$. On va montrer que ψ est une bijection.

Si $\psi(f) = \psi(f')$ alors $(f(x_1), \ldots, f(x_n)) = (f'(x_1), \ldots, f'(x_n))$ donc $f(x_i) = f'(x_i)$ pour $i = 1, \ldots, n$, donc $f(x) = f'(x)$ pour tout $x \in X$, c'est à dire $f = f'$. La fonction ψ est donc injective.

Soit maintenant $(y_1, \ldots, y_n)$ un élément de Y^n. On définit $f : X \to Y$ par : soit $x \in X$; comme φ_X est une bijection il existe un unique $i \in [1, n]$ tel que $x = x_i$. On pose alors $f(x) = y_i$. On a ainsi bien défini une fonction $f : X \to Y$ et on a par définition de ψ que $\psi(f) = (y_1, \ldots, y_n)$. La fonction ψ est surjective, donc bijective.

Par conséquent $\left|Y^X\right| = |Y^n| = |Y|^n = |Y|^{|X|}$ en vertu de la proposition puissance précédente.

Parties On a vu au chapitre précédent que l'ensemble $\mathcal{P}(X)$ est en bijection avec l'ensemble $\{0, 1\}^X$; ces deux ensembles ont donc même cardinal et comme $|\{0, 1\}| = 2$ on en déduit le résultat.

Exercice 3 Vérifier le théorème 4.6 pour $X = [1, 2]$ et $Y = [1, 3]$.

Exercice 4 Soient X et Y deux ensembles finis disjoints.

i) Calculer le cardinal de l'ensemble $\mathcal{P}(X \cup Y)$.

ii) Calculer le cardinal de l'ensemble $\mathcal{P}(X) \times \mathcal{P}(Y)$.

iii) Qu'en déduire ?

Exercice 5 Soient X et Y deux ensembles finis. D'après le théorème on a que $|\mathcal{P}(X \times Y)| = 2^{|X|.|Y|} = 2^{|X|^{|Y|}} = |\mathcal{P}(X)|^{|Y|} = \left|\mathcal{P}(X)^Y\right|$. Il y a donc une bijection de l'ensemble des parties de $X \times Y$ dans l'ensemble des fonctions de Y dans les parties de X. Construire une telle bijection.

4.1.3 Permutations

Une bijection de $[1, n]$ dans lui-même est appelée une permutation de $[1, n]$. L'ensemble des permutations de $[1, n]$ est notée $\mathfrak{S}_n$. C'est un sous-ensemble de l'ensemble des fonctions de $[1, n]$ dans lui-même, il est donc fini. On note $n!$ (factorielle de n) le cardinal de $\mathfrak{S}_n$, c'est à dire le nombre de permutations de $[1, n]$.

EXEMPLE.

Soient i et j deux éléments de $[1, n]$. On note $\tau_{i,j}$ la *transposition* de i et j, c'est à dire la fonction de $[1, n]$ dans lui-même définie par $\tau_{i,j}(k) = k$ si $k \neq i, j$, $\tau_{i,j}(i) = j$ et $\tau_{i,j}(j) = i$. On vérifie que pour tout $k \in [1, n]$ on a $\tau_{i,j}(\tau_{i,j}(k)) = k$, c'est à dire que $\tau_{i,j} \circ \tau_{i,j} = \mathrm{Id}_{[1,n]}$. Donc $\tau_{i,j}$ est une bijection de $[1, n]$ sur lui-même, c'est donc bien une permutation de $[1, n]$.

REMARQUE

Si σ et σ' sont des permutations de $[1, n]$ alors leur composée $\sigma \circ \sigma'$ est encore une permutation de $[1, n]$. Si σ est une permutation, c'est une bijection de $[1, n]$ dans lui-même et elle admet donc une fonction inverse σ^{-1}. Mais σ^{-1} est également une bijection de $[1, n]$ dans lui-même, c'est donc également une permutation.

Un ensemble comme $\mathfrak{S}_n$ muni d'un opération associative (la composition), d'un élément neutre pour cette opération (la permutation Id qui vérifie bien $\sigma \circ \mathrm{Id} = \mathrm{Id} \circ \sigma = \sigma$) et d'un inverse pour chaque élément (la permutation σ^{-1}) est appelé un *groupe*.

REMARQUE

Si X est un ensemble à n éléments, alors les bijections de X dans X sont appelées des permutations de X. Il y en a $n!$ (pourquoi ?).

4.7 Théorème
Si $n \in \mathbb{N}$ on a $n! = 1.2 \ldots n = \Pi_{i=1}^{n} i$. En particulier $0! = 1$.

Preuve. Par récurrence sur n. Si $n = 0$, $\mathfrak{S}_n$ est l'ensemble de permutations de l'ensemble vide ; il y a exactement une telle permutation, la fonction vide, donc $0! = 1$.

Supposons le résultat vrai pour n. Pour $i \in [1, n+1]$ on note S_i l'ensemble des permutations σ de $[1, n+1]$ telles que $\sigma(n+1) = i$. Remarquons que pour $i, j \in [1, n+1]$, si $\sigma \in S_i \cap S_j$ alors on a $\sigma(n+1) = i = j$. Autrement dit si $i \neq j$ alors S_i et S_j sont disjoints. De plus si σ est une permutation de $[1, n+1]$ alors on a $\sigma \in S_{\sigma(n+1)}$, donc σ appartient à l'un des S_i. Autrement dit la réunion des S_i est égal à $\mathfrak{S}_{n+1}$ (les S_i forment une partition de $\mathfrak{S}_{n+1}$). Comme les S_i sont deux à deux disjoints on en déduit que $|\mathfrak{S}_{n+1}| = |S_1| + \cdots + |S_{n+1}|$.

On va maintenant calculer $|S_i|$, et plus précisément on va montrer que les S_i ont tous le même cardinal. Pour cela soient $i, j \in [1, n+1]$; on rappelle que $\tau_{i,j}$ est la transposition de i et j. Si $\sigma \in \mathfrak{S}_{n+1}$, $\tau_{i,j} \circ \sigma$ est une composition de permutations et est donc une permutation. On définit la fonction $\varphi : \mathfrak{S}_{n+1} \to \mathfrak{S}_{n+1}$ par $\varphi(\sigma) = \tau_{i,j} \circ \sigma$ pour tout $\sigma \in \mathfrak{S}_{n+1}$.

On a donc $\varphi(\varphi(\sigma)) = \varphi(\tau_{i,j} \circ \sigma) = \tau_{i,j} \circ \tau_{i,j} \circ \sigma = \sigma$ (car $\tau_{i,j}$ est une involution). La fonction φ est donc aussi une involution, et en particulier c'est une bijection de $\mathfrak{S}_{n+1}$ dans $\mathfrak{S}_{n+1}$.

Soit maintenant $\sigma \in S_i$; alors on a $\varphi(\sigma)(n+1) = \tau_{i,j} \circ \sigma(n+1) = \tau_{i,j}(i) = j$, donc $\varphi(\sigma) \in S_j$. Mais si on prend $\sigma \in S_j$, alors on a de même $\varphi(\sigma) \in S_i$ et comme $\varphi(\varphi(\sigma)) = \sigma$, on en déduit que $\varphi(\sigma)$ est un antécédent de σ par φ. Tout ceci montre que la fonction $\varphi|_{S_i}$ est à valeurs dans S_j et qu'elle est surjective ; étant la restriction d'une bijection, elle est également injective et c'est donc une bijection de S_i dans S_j ce qui montre que S_i et S_j ont même cardinal.

Par conséquent on a $|\mathfrak{S}_{n+1}| = |S_1| + \cdots + |S_{n+1}| = (n+1)\,|S_{n+1}|$. On va finir en montrant que $|S_{n+1}| = |\mathfrak{S}_n|$. Pour cela on définit une fonction $\psi : S_{n+1} \to \mathfrak{S}_n$ par $\psi(\sigma) = \sigma|_{[1,n]}$. Par définition de S_{n+1}, si $\sigma \in S_{n+1}$ on a $\sigma(n+1) = n+1$, donc $\psi(\sigma)$ est bien une permutation de $[1, n]$. De plus si σ_0 est une permutation de $[1, n]$ soit σ dans S_{n+1} definie par $\sigma(k) = \sigma_0(k)$ pour $k \leq n$ et $\sigma(n+1) = n+1$. On a donc $\sigma \in S_{n+1}$ et $\psi(\sigma) = \sigma_0$, donc

ψ est surjective. Enfin si σ et σ' sont deux permutations distinctes de S_{n+1} alors comme $\sigma(n+1) = \sigma'(n+1)$, il existe un $k \leq n$ tel que $\sigma(k) \neq \sigma'(k)$, donc $\psi(\sigma) \neq \psi(\sigma')$, ce qui montre que ψ est également injective. Donc $|S_{n+1}| = |\mathfrak{S}_n|$.
On peut (enfin) appliquer l'hypothèse de récurrence qui nous dit que $|\mathfrak{S}_n| = n! = 1 \dots n$. Donc $|\mathfrak{S}_{n+1}| = (n+1)! = (n+1)\,|S_{n+1}| = (n+1)\,|\mathfrak{S}_n| = (n+1).n \dots 1$.

Arrangements. Soient n et p deux entiers naturels ; une injection de $[1, p]$ dans $[1, n]$ est appelée un *arrangement* de p parmi n. L'idée derrière cette terminologie est que l'on a choisi p éléments de $[1, n]$ que l'on a *arrangés*, c'est à dire numérotés de 1 à p. On note $\mathcal{A}_n^p$ l'ensemble des arrangements de p parmis n et A_n^p le cardinal de $\mathcal{A}_n^p$.

REMARQUE

Si X est un ensemble à p éléments et Y un ensemble à n éléments alors le nombre d'injections de X dans Y est également A_n^p (pourquoi ?).

4.8 Théorème
Si $n < p$ alors $A_n^p = 0$. Si $n \geq p$ alors $A_n^p = n!/(n-p)!$.

Preuve. Si $n < p$ alors il ne peut y avoir d'injections de $[1, p]$ dans $[1, n]$ (sinon on aurait $p \leq n$). Donc $A_n^p = 0$.
Si $p \leq n$ la preuve est par récurrence sur n et on en donne les grandes lignes. Le cas $n = 0$ est immédiat. Dans le cas $n+1$ on suppose par récurrence que pour $p = 1, \dots, n$ on a $A_n^p = n!/(n-p)!$. Si $p = 0$ alors il y a exactement un arrangement de p parmi $n+1$ (la fonction vide) ce qui satisfait bien la formule $A_{n+1}^0 = (n+1)!/(n+1-0)!$. Si $0 < p \leq n+1$ on raisonne comme pour les permutations en définissant pour chaque $i = 1, \dots, n+1$ l'ensemble A_i constitué des arrangements de p parmi $n+1$ vérifiant $\sigma(p) = i$; les A_i forment alors une partition de $\mathcal{A}_{n+1}^p$ et sont tous de même cardinal si bien que $A_{n+1}^p = \left|\mathcal{A}_{n+1}^p\right| = |A_1| + \dots + |A_{n+1}| = (n+1)\,|A_{n+1}|$. Comme dans chaque A_i on a fixé la valeur de $\sigma(p)$, on voit que les arrangements dans A_i sont en fait des arrangements de $p-1$ parmi n. Par hypothèse de récurrence le cardinal de A_{n+1} est donc $n!/(n-p+1)!$ et on obtient finalement $A_{n+1}^p = (n+1).n!/(n-p+1)! = (n+1)!/(n+1-p)!$ comme attendu.

REMARQUE

Cette démonstration est essentiellement la même que celle pour les permutations. Du reste le théorème généralise celui des permutations ; en effet, dans le cas particulier où $p = n$, un arrangement de n parmi n est une injection de $[1, n]$ dans $[1, n]$, donc une bijection, c'est à dire une permutation de $[1, n]$. Autrement dit $\mathcal{A}_n^n = \mathfrak{S}_n$, donc $A_n^n = n!$ ce que l'on retrouve comme cas particulier du théorème ci-dessus.

4.1.4 Coefficients binomiaux

Soit X un ensemble et p un entier naturel. On note $\mathcal{P}_p(X)$ l'ensemble des parties finies de X dont le cardinal est p.

4.9 Théorème
Soient X et X' deux ensembles finis ; si X et X' ont même cardinal et si p est un entier naturel alors $|\mathcal{P}_p(X)| = |\mathcal{P}_p(X')|$.

REMARQUE

Autrement dit le nombre de parties à p éléments de X ne dépend pas de la nature des éléments de X : il y a exactement autant de manières de choisir p nombres dans un ensemble de n nombres que de manières de choisir p vecteurs dans un ensemble de n vecteurs, etc.

Exercice 6 Démontrer si X est fini alors $|\mathcal{P}_p(X)| = |\mathcal{P}_p(X')|$.

Si X est fini de cardinal n on note $\binom{n}{p}$ (p parmi n) le cardinal de $\mathcal{P}_p(X)$; cette notation est correcte car on vient de voir que le cardinal de $\mathcal{P}_p(X)$ ne dépend que de p et du cardinal de X, mais pas de la nature de X. Pour des raisons explicitées ci-dessous, l'entier $\binom{n}{p}$ est appelé *coefficient binomial* n, p.

Remarque

Le coefficient binomial n, p se note également C_n^p. On prendra garde que dans cette notation les positions respectives de n et p sont inversées par rapport à la notation $\binom{n}{p}$.

Dans le cas où $p = 0$ on voit que $\binom{n}{0} = 1$ car il n'y a qu'une partie à 0 élément (l'ensemble vide). Dans le cas où $p = n$ on voit que $\binom{n}{n} = 1$ également puisque il y a une seule partie à n éléments : X lui même. Finalement dans le cas où $p > n$ on voit que $\binom{n}{p} = 0$ puisqu'il ne peut y avoir un sous-ensemble à p éléments d'un ensemble qui n'en a que n.
La fonction de $\mathcal{P}_p(X)$ dans $\mathcal{P}_{n-p}(X)$ qui à une partie de cardinal p associe son complémentaire de cardinal $n-p$ est une bijection. Donc $\mathcal{P}_p(X)$ et $\mathcal{P}_{n-p}(X)$ ont même cardinal, ce qui s'écrit :

$$\binom{n}{p} = \binom{n}{n-p}$$

4.10 Théorème
Pour tous entiers naturels n et p les coefficients binomiaux satisfont la relation de récurrence :

$$\binom{n+1}{p+1} = \binom{n}{p} + \binom{n}{p+1}$$

On en déduit que :

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

Preuve. La seconde relation se déduit facilement par récurrence de la première. On peut également la justifier intuitivement : on sait que $n!/(n-p)!$ est le nombre d'arrangements de p éléments parmi n. Pour construire un arrangement il faut choisir p éléments parmi n, et il y a $\binom{n}{p}$ façons de faire, et il faut les ordonner, c'est à dire les numéroter de 1 à p. Il y a $p!$ façons de faire. Donc on a $A_n^p = p!\binom{n}{p}$ ce qui donne exactement la seconde relation ci-dessus.

Remarquons que la relation de récurrence est vérifiée dans les cas extrêmes : $p = 0$ ou $p \geq n$. Supposons maintenant que $0 < p < n$. Soit X un ensemble à $n+1$ éléments et $x \in X$. Notons $\mathcal{P}$ l'ensemble des parties à $p+1$ éléments de X qui contiennent x et $\mathcal{P}'$ l'ensemble des parties à $p+1$ éléments de X qui ne contiennent pas x.

Si $P \in \mathcal{P}$ est une partie à $p+1$ éléments contenant x alors $P\backslash\{x\}$ est une partie à p éléments de $X\backslash\{x\}$. On vérifie facilement que la fonction qui à P associe $P\backslash\{x\}$ est une bijection de $\mathcal{P}$ dans $\mathcal{P}_p(X\backslash\{x\})$. Comme $X\backslash\{x\}$ a n éléments, on a donc $|\mathcal{P}| = \binom{n}{p}$.

Si $P \in \mathcal{P}'$ est une partie à $p+1$ éléments ne contenant pas x alors P est aussi une partie de $X\backslash\{x\}$. Clairement la fonction ainsi définie de $\mathcal{P}'$ dans $\mathcal{P}_{p+1}(X\backslash\{x\})$ est également une bijection. Donc $|\mathcal{P}'| = \binom{n}{p+1}$.

Par définition $\mathcal{P}$ et $\mathcal{P}'$ forment une partition de $\mathcal{P}_{p+1}(X)$ (ils sont disjoints et leur réunion est $\mathcal{P}_{p+1}(X)$) ; donc $\binom{n+1}{p+1} = |\mathcal{P}_{p+1}(X)| = |\mathcal{P}| + |\mathcal{P}'| = \binom{n}{p} + \binom{n}{p+1}$.

Remarque

Cette formule de récurrence est à l'origine de la construction du fameux *triangle de Pascal* dans lequel le nombre à la ligne n et colonne p est la somme de celui immédiatement au-dessus (ligne $n-1$, colonne p) et de son voisin de gauche (ligne $n-1$, colonne $p-1$) : :

```
1
1  1
1  2   1
1  3   3    1
1  4   6    4    1
1  5   10   10   5    1
1  6   15   20   15   6    1
1  7   21   35   35   21   7    1
                ...
```

4.11 Théorème (Formule du binôme)
Soient x et y deux nombres (entiers, rationnels, réels, complexes, ...) et n un entier. On a :

$$\begin{aligned}(x+y)^n &= x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-1}xy^{n-1} + y^n \\ &= \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k\end{aligned}$$

Preuve. On raisonne par récurrence sur n. Si $n=0$ alors $(x+y)^n = 1$ et $\sum_{k=0}^{0}(\binom{k}{n}x^{n-k}y^k = \binom{0}{0}x^0y^0 = 1$.

Supposons la formule vraie pour n ; on a

$$\begin{aligned}(x+y)^{n+1} &= (x+y)(x+y)^n \\ &= (x+y)\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k && \text{par hypothèse de récurrence} \\ &= \sum_{k=0}^{n}\binom{n}{k}x^{n+1-k}y^k + \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^{k+1} \\ &= x^{n+1} + \sum_{k=1}^{n}\binom{n}{k}x^{n+1-k}y^k + \sum_{k=0}^{n-1}\binom{n}{k}x^{n-k}y^{k+1} + y^{n+1} \\ &= x^{n+1} + \sum_{k=1}^{n}\binom{n}{k}x^{n+1-k}y^k + \sum_{k=1}^{n}\binom{n}{k-1}x^{n+1-k}y^k + y^{n+1} \\ &= x^{n+1} + \sum_{k=1}^{n}\left(\binom{n}{k-1} + \binom{n}{k}\right)x^{n+1-k}y^k + y^{n+1} \\ &= \binom{n+1}{0}x^{n+1} + \sum_{k=1}^{n}\binom{n+1}{k}x^{n+1-k}y^k + \binom{n+1}{n+1}y^{n+1} \\ &= \sum_{k=0}^{n+1}\binom{n+1}{k}x^{n+1-k}y^k\end{aligned}$$

Exercice 7 Montrer que pour tout entier naturel n on a :

$$\sum_{p=0}^{n}\binom{n}{p} = 2^n$$

Exercice 8 Soit n un entier naturel.

i) Calculer la somme $\sum_{k=0}^{n} 2^k\binom{n}{k}$.

ii) Calculer la somme $\sum_{k=0}^{n} 2^{k-1}3^{n-k+1}\binom{n}{k}$.

iii) Calculer la somme $\sum_{k=0}^{n} k\binom{n}{k}$

Indication : Dériver $(1+x)^n$ de deux manières différentes.

Exercice 9 Démontrer que pour tous entiers naturels n et p tels que $p \le n$ on a :

$$\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1} \qquad \text{si } p \neq 0,$$

$$\binom{n}{p+1} = \frac{n-p}{p+1}\binom{n}{p}$$

Exercice 10 Démontrer que pour tous entiers naturels n et p on a l'égalité :

$$\binom{n+1}{p+1} = \sum_{k=p}^{n} \binom{k}{p}$$

Exercice 11 On note $F_n = \sum_{k=0}^{n} \binom{n-k}{k}$. Montrer que pour tout entier naturel n on a $F_n + F_{n+1} = F_{n+2}$ (on en déduit que les F_n forment la fameuse *suite de Fibonacci*).

Exercice 12 Démontrer que pour tout entier naturel n on a l'égalité :

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$$

Indication : On peut utiliser la formule du binôme et calculer $(x+y)^{2n}$ de deux manières différentes ; on peut également utiliser un raisonnement combinatoire.

4.1.5 Exercices de dénombrement

Exercice 13 Soit P un polygone convexe à n sommets ($n \geq 3$). Une diagonale de P est une droite joignant deux sommets non consécutifs. Combien P a-t-il de diagonales distinctes ?

Exercice 14 Combien y-a-t-il de fonctions caractéristiques sur $\{0,1\}$? sur $\{0,1\}^2$? sur $\{0,1\}^k$ pour $k \in \mathbb{N}$?

Exercice 15 Un joueur lance un dé jusqu'à ce qu'il obtienne un même chiffre pour le deuxième fois. La suite de chiffres obtenue s'appelle un *résultat*.

i) Quel est le maximum de lancers possible ?
ii) Combien y-a-t-il de résultats comportant deux lancers exactement ?
iii) Combien y-a-t-il de résultats comportant trois lancers exactement ?
iv) Combien y-a-t-il de résultats possibles ?

Exercice 16 Soit Σ un ensemble de cardinal 3 ; les éléments de Σ seront appelés des *lettres* et notés a, b et c. Un *mot de longueur n sur Σ* est n-uplet d'éléments de Σ, c'est à dire un élément de Σ^n.

i) Combien y-a-t-il de mots de longueur n ?
ii) Combien y-a-t-il de mots de longueur inférieure ou égale à n ?
iii) Combien y-a-t-il de mots de longueur n tel que chacune des trois lettres apparait au moins un fois ?

4.2 Ensembles infinis

La théorie des ensembles permet de généraliser la définition des cardinaux à tous les ensembles infinis. Il serait toutefois un peu trop long de donner ici cette définition. Il suffit de savoir que deux ensembles ont même cardinal s'ils sont en bijection et que le cardinal d'un ensemble X est plus petit que celui d'un ensemble Y s'il existe une injection de X dans Y.
On va évoquer ici deux cardinaux importants en mathématique : le *dénombrable* et le *continu*. Le dénombrable est le cardinal de l'ensemble des entiers naturels $\mathbb{N}$. On verra que c'est aussi le cardinal des entiers relatifs $\mathbb{Z}$ et des rationnels $\mathbb{Q}$. Le continu est les cardinal de l'ensemble des réels $\mathbb{R}$. C'est également le cardinal de n'importe quel intervalle réel de la forme $[a,b]$ $(a<b)$ ou $]a,b[$ $(a<b)$ et celui des complexes $\mathbb{C}$.
Le point de départ de la théorie des ensembles a été la constation par Cantor (mathématicien du 19ème siècle et inventeur de la théorie des ensembles) qu'il n'y a pas de bijection entre $\mathbb{N}$ et $\mathbb{R}$. Plus précisément il n'existe pas d'injection de $\mathbb{R}$ dans $\mathbb{N}$: le continu est strictement plus grand que le dénombrable.

4.12 Théorème (Cantor)
Il n'existe pas d'injection de $\mathcal{P}(\mathbb{N})$ dans $\mathbb{N}$.

Preuve. On montre qu'il n'y a pas de surjection de $\mathbb{N}$ dans $\mathcal{P}(\mathbb{N})$. De là on déduit qu'il n'y a pas d'injection de $\mathcal{P}(\mathbb{N})$ dans $\mathbb{N}$ grâce au théorème 3.2.

Soit $\varphi : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ une fonction quelconque de $\mathbb{N}$ dans $\mathcal{P}(\mathbb{N})$. On va construire un ensemble $X \subset \mathbb{N}$ qui n'est pas dans l'image de φ. On en déduit que φ n'est pas surjective.

Par définition de φ, pour chaque n, $\varphi(n)$ est un ensemble d'entiers. On définit X de la façon suivante : si n est un entier naturel on pose $n \in X$ ssi $n \notin \varphi(n)$.

L'ensemble d'entiers X ne peut être dans l'image de $\mathbb{N}$ par φ. Sinon il y aurait un entier n_0 tel que $X = \varphi(n_0)$. Mais c'est impossible car on a $n_0 \in X$ ssi $n_0 \notin \varphi(n_0)$ par définition de X, c'est à dire $n_0 \in X$ ssi $n_0 \notin X$.

4.13 Corollaire
Il n'y a pas d'injection de $\mathbb{R}$ dans $\mathbb{N}$.

Preuve. La démonstration précise de ce corollaire demande un peu de connaissances en analyse aussi on n'en donne que les grandes lignes ici. L'idée est d'associer à chaque partie N de $\mathbb{N}$ un nombre réel x_N. Pour cela on prend $x_N = \sum_{k\geq 0} 2\chi_N(k)/3^k$ où $\chi_N : \mathbb{N} \to \{0,1\}$ est la fonction caractéristique de N. On peut alors vérifier que si N et N' sont deux parties distinctes de $\mathbb{N}$ alors $x_N \neq x_{N'}$.

On définit *l'ensemble de Cantor* $\mathcal{C}$ par $\mathcal{C} = \{x \in \mathbb{R}, \exists N \subset \mathbb{N}, x = x_N\}$. Alors $\mathcal{C}$ est en bijection avec $\mathcal{P}(\mathbb{N})$. S'il existait une injection de $\mathbb{R}$ dans $\mathbb{N}$, sa restriction à $\mathcal{C}$ serait également injective, mais comme $\mathcal{C}$ est en bijection avec $\mathcal{P}(\mathbb{N})$, on en déduirait une injection de $\mathcal{P}(\mathbb{N})$ dans $\mathbb{N}$ ce qui ne se peut.

4.2.1 Ensembles dénombrables

Comme on a dit un ensemble est dénombrable s'il est en bijection avec $\mathbb{N}$.

4.14 Théorème
Un ensemble fini n'est pas dénombrable.

Preuve. Il suffit de démontrer que pour tout entier n, il n'existe pas de bijection de $[1,n]$ sur $\mathbb{N}$. En effet par définition un ensemble fini est en bijection avec $[1,n]$; s'il y avait une bijection de l'ensemble sur $\mathbb{N}$, en composant les deux on obtiendrait une bijection de $[1,n]$ sur $\mathbb{N}$.

Soit $\varphi : [1,n] \to \mathbb{N}$ une fonction et $p = \varphi(1) + \varphi(2) + \cdots + \varphi(n) + 1$. Alors pour $i = 1, \ldots, n$ on a $p \neq \varphi(i)$. Autrement dit il n' y a aucun $i \in [1,n]$ tel que $p = \varphi(i)$. Donc φ n'est pas surjective, et a fortiori n'est pas bijective.

Ensemble au plus dénombrable. Un ensemble est au plus dénombrable si il est fini ou dénombrable.

4.15 Théorème
Soit X un sous-ensemble de $\mathbb{N}$; alors X est au plus dénombrable.

Preuve. Supposons que X n'est pas fini ; on va construire une bijection de X dans $\mathbb{N}$. Pour cela on définit par récurrence sur n une suite (x_n) d'entiers et une suite (X_n) de sous-ensembles infinis de X : $X_0 = X$, $x_0 =$ le plus petit élément de X_0, et pour chaque n, $X_{n+1} = X_n \backslash x_n$; comme X_n est un ensemble infini d'entiers naturels, X_{n+1} est également infini (pourquoi ?) et a donc un plus petit élément que l'on note x_{n+1}.

On vérifie facilement par récurrence sur n que l'on a les propriétés suivantes pour tout n :
- $x_n < x_{n+1}$;
- $\{x_0, \ldots, x_n\} \cup X_{n+1} = X$.

Soit $x \in X$. Comme la suite (x_n) est strictement croissante, il existe un N tel que $x_N \geq x$ et donc il y a un *plus petit* N tel que $x_N \geq x$. Donc pour tout $n < N$ on a $x_n < x$. Mais x_N est le plus petit élément de X_N, donc pour tout $y \in X_N$ on a $y \geq x_N \geq x$.

Or on a $\{x_0, \ldots, x_{N-1}\} \cup X_N = X$; comme $x \in X$ et $x \notin \{x_0, \ldots, x_{N-1}\}$, on en déduit que $x \in X_N$. Par conséquent $x \geq x_N$ et donc $x = x_N$. On vient donc de montrer que pour tout $x \in X$ il y a un N tel que $x = x_N$. Si on définit la fonction $\varphi : \mathbb{N} \to X$ par $\varphi(n) = x_n$ alors φ est bijective puisque $n < p$ implique $\varphi(n) = x_n < x_p = \varphi(p)$ et que l'on vient de voir que tout $x \in X$ a un antécédent.

4.16 Théorème
Soit X un ensemble non vide. Les trois conditions suivantes sont équivalentes :

1. *X est au plus dénombrable ;*
2. *il existe une injection de X dans $\mathbb{N}$;*
3. *Il existe une surjection de $\mathbb{N}$ sur X.*

Preuve. Supposons que X est au plus dénombrable. Si X est fini il existe un n et une bijection $\varphi : X \to [1, n]$. Mais $[1, n] \subset \mathbb{N}$ donc cette bijection est aussi une injection de X dans $\mathbb{N}$.

D'autre part φ^{-1} est une bijection de $[1, n]$ dans X. Supposons X non vide et soit $x_0 \in X$. On définit une fonction $f : \mathbb{N} \to X$ par : $f(i) = \varphi^{-1}(i)$ si $i \in [1, n]$, $f(i) = x_0$ sinon. Alors f est une surjection de $\mathbb{N}$ sur X. En effet soit $x \in X$ et posons $i = \varphi(x)$; alors $i \in [1, n]$ si bien que $f(i) = x$.

Si maintenant X est dénombrable, alors par définition il y a une bijection $\varphi : X \to \mathbb{N}$; mais φ est en particulier une injection de X dans $\mathbb{N}$ et φ^{-1} est une bijection, donc en particulier une surjection de $\mathbb{N}$ sur X.

Réciproquement soit $\varphi : X \to \mathbb{N}$ une injection. Alors $\varphi(X)$ qui est un sous-ensemble de $\mathbb{N}$ est fini ou dénombrable (théorème précédent) et $\varphi_0 : X \to \varphi(X)$ définie par $\varphi_0(x) = \varphi(x)$ pour tout $x \in X$ est une bijection.

Si $\varphi(X)$ est fini alors il y a une bijection $\psi : \varphi(X) \to [1, n]$ pour un entier n et la composition $\psi \circ \varphi_0$ est une bijection de X dans $[1, n]$; donc X est fini.

Si $\varphi(X)$ est dénombrable alors il y a une bijection $\psi : \varphi(X) \to \mathbb{N}$ et la composition $\psi \circ \varphi_0$ est une bijection de X dans $\mathbb{N}$; donc X est dénombrable.

Finalement supposons qu'il y a une surjection de $\mathbb{N}$ dans X. D'après le théorème 3.3 cela implique qu'il y a une fonction injective de X dans $\mathbb{N}$ et on est ramené au cas précédent.

Exercice 17 Soit $\varphi : \mathbb{N}^2 \to \mathbb{N}$ définie par $\varphi(n, m) = (n + m)(n + m + 1)/2 + m$.

i) Montrer que φ est bijective.

ii) En déduire que $\mathbb{N}^k$ est dénombrable pour tout entier naturel non nul k.

iii) On note $\mathbb{N}^\omega = \bigcup_{k \geq 1} \mathbb{N}^k$. Montrer que $\mathbb{N}^\omega$ est dénombrable.

iv) On note $\mathcal{P}^\omega$ l'ensemble des parties finies de $\mathbb{N}$. Montrer que $\mathcal{P}^\omega$ est dénombrable.

Exercice 18 Montrer que $\mathbb{Z}$ est dénombrable, puis que $\mathbb{Q}$ est dénombrable.

4.17 Théorème
Soit $(X_n)_{n \geq 0}$ une famille d'ensembles tous dénombrables. Alors $\bigcup_{n \geq 0} X_n$ est dénombrable.

Chapitre 5

Arithmétique

5.1 Notions de base

5.1.1 Divisibilité, nombre premier

Soit n et p deux entiers. On dit que p divise n, et l'on note $p \mid n$, si n est un multiple de p, c'est à dire si il existe un entier k tel que $n = kp$.

Remarque

si $p = 0$ alors p divise n ssi $n = 0$.

Exercice 1 Montrer que si $p \mid n$ alors $p \mid n + kp$ pour tout $k \in \mathbb{Z}$.

Exercice 2 Montrer que si $p \mid m$ et $p \mid n$ alors pour tous $u, v \in \mathbb{Z}$, $p \mid um + vn$.

Exercice 3 Soient m, n, u, v des entiers et d un entier positif. Montrer que si $um + vn = d$ et d divise m et d divise n alors $d = m \wedge n$.

5.1 Théorème
La relation de divisibilité est une relation d'ordre sur les entiers naturels, c'est à dire qu'elle vérifie :

Reflexivité *pour tout entier naturel n, $n \mid n$;*

Antisymétrie *pour tous $m, n \in \mathbb{N}$, si $m \mid n$ et $n \mid m$ alors $m = n$;*

Transitivité *pour tous $m, n, p \in \mathbb{N}$, si $m \mid n$ et $n \mid p$ alors $m \mid p$.*

Exercice 4 Démontrer que la relation divise est une relation d'ordre. Qu'est ce qui devient faux si on considère non pas des entiers naturels mais des entiers ?

Diviseurs de n. Si p divise n alors $-p$ divise n, p divise $-n$ et $-p$ divise $-n$. En particulier p divise n ssi p divise $|n|$. On appelle *diviseurs* de n les entiers strictement positifs qui divisent n.

REMARQUE

Il est en général inutile de spécifier qu'un diviseur est non nul puisque 0 ne divise que 0. La condition est là juste éviter de considérer 0 comme un diviseur de 0.

5.2 Théorème
Soit n un entier non nul. Si d est un diviseur de n alors $d \leq |n|$. En particulier l'ensemble des diviseurs de n est fini.

Preuve. Un diviseur de n est également un diviseur de $|n|$. Il existe donc un $k \in \mathbb{Z}$ tel que $|n| = kd$. Mais comme $|n|$ et d sont positifs, k est également positif ; de plus comme $|n| > 0$ (puisque n est supposé non nul), $k > 0$ également, c'est à dire $k \geq 1$. Donc $kd = n \geq d$.

L'ensemble des diviseurs de n est un ensemble d'entiers naturels majorés par n, il est donc fini.

Nombres premiers. Un entier $n > 1$ a toujours au moins deux diviseurs distincts : n lui même qui est le plus grand, et 1 qui est le plus petit. Si n n'a pas d'autres diviseurs que ces deux là, on dit que n est premier ; plus précisément :

$$n \text{ est premier ssi } n > 1 \text{ et } \forall k \in \mathbb{N}, p \in \mathbb{N} \text{ si } n = kp \text{ alors } p = 1 \text{ ou } p = n$$

REMARQUE

Avec cette définition un nombre négatif n'est pas premier.

Il y a toujours un petit doute sur le nombre 1 : est-il premier ou non ? La réponse que l'on donne ici est que 1 n'est pas premier.

5.3 Théorème
Tout entier $n \geq 2$ admet au moins un diviseur premier.

Preuve. Par récurrence. Si $n = 2$ alors comme 2 est premier et 2 divise n, n admet bien un diviseur premier. Supposons le résultat démontré pour tout entier $m < n$. Si n est premier alors le résultat est démontré. Sinon soit m un diviseur de n différent de 1 et de n. Alors $m < n$ et par récurrence sur m, m admet un diviseur premier p ; mais comme p divise m qui divise n, on a que p divise n qui admet donc un diviseur premier.

REMARQUE

Dans ce raisonnement on applique l'hypothèse de récurrence non pas à $n - 1$ comme il est d'usage, mais à un entier m dont on a montré qu'il est strictement plus petit que n. Il s'agit d'une forme tout à fait licite du raisonnement par récurrence si on pense que le théorème démontré est : pour tout $n \geq 2$, pour tout m tel que $2 \leq m \leq n$, m admet un diviseur premier. Cette énoncé est équivalent au théorème mais c'est celui-là qui nous sert d'hypothèse de récurrence.

5.4 Théorème (Euclide, 300 av. J.-C.)
Il y a une infinité de nombres premiers

Preuve. On montre que pour tout entier naturel n il existe un nombre premier supérieur à n. Ceci entraîne qu'il y a une infinité de nombres premiers.

On considère le nombre $c_n = n! + 1$. Soit d un diviseur de c_n. Si $d \leq n$ alors d divise $n!$, donc d divise également 1 puisque $1 = c_n - n!$. Or 1 n'a qu'un seul diviseur, lui-même, donc $d = 1$. Autrement dit tout diviseur de c_n différent de 1 est strictement plus grand que n.

Comme $c_n \geq 2$, le théorème précédent nous assure qu'il existe un nombre premier p qui divise c_n. Mais si p est premier il est en particulier différent de 1, et comme c'est un diviseur de c_n il est donc strictement supérieur à n. On a donc trouvé un nombre premier plus grand que n comme annoncé.

Exercice 5 Soit n un entier naturel ; montrer que n est premier ssi n n'admet aucun diviseur premier inférieur à $\sqrt{n}$.

5.1.2 PGCD

Soient m et n deux entiers. Le PGCD de m et n, noté PGCD(m,n), ou (m,n) ou encore $m \wedge n$ est le plus grand des diviseurs communs à m et n. Autrement dit $m \wedge n$ est l'entier naturel non nul d qui vérifie :
- $d \mid m$ et $d \mid n$;
- pour tout d', si $d' \mid m$ et $d' \mid n$ alors $d' \leq d$.

Remarque

Dans le cas particulier où $m = n = 0$, le PGCD de m et n n'est pas défini car 0 a une infinité de diviseurs. En règle générale dans tous les énoncés mentionnant le PGCD, on supposera implicitement que les deux entiers dont on prend le PGCD ne sont pas tous les deux nuls.

On peut également remarquer que m et n ont toujours au moins un diviseur commun : 1, si bien que le PGCD de m et n est bien défini dès que l'on suppose que m et n ne sont pas tous les deux nuls.

Entiers premiers entre eux. Si le PGCD de m et n est égal à 1, on dit que m et n sont premiers entre eux. Autrement dit m et n sont premiers entre eux si leur seul diviseur commun est 1.

Remarque

0 n'est premier avec aucun autre entier que 1.

5.1.3 Division euclidienne

5.5 Théorème
Soient n un entier et p un entier naturel non nul ; il existe deux uniques entiers q et r satisfaisant :
- $n = pq + r$;
- $0 \leq r < p$.

La fonction qui au couple (n,p) associe le couple (q,r) (fonction de $\mathbb{Z} \times \mathbb{N}^*$ dans $\mathbb{Z} \times \mathbb{N}$) s'appelle la *division euclidienne*. L'entier q est appelé le *quotient* de n par p et l'entier naturel r est appelé le *reste* de n par p. On dit aussi que r est le *reste de n modulo p* ce que l'on note $n = r\,(p)$.

Preuve. On commence par traiter le cas où $n \geq 0$; on montre l'existence de q et r par récurrence sur n. Si $n = 0$ alors on a $n = 0p + 0$, donc le résultat est démontré en prenant le quotient et le reste tous deux égaux à 0. Supposons qu'il existe deux entiers q et r tels que $n = pq + r$ et $0 \leq r < p$. Puisque $r < p$ on a $r + 1 \leq p$ et on peut distinguer deux cas :
- $r + 1 < p$: dans ce cas on a $n + 1 = pq + r + 1$ et comme $0 \leq r + 1 < p$ le résultat est démontré pour $n + 1$ en prenant q pour le quotient et $r + 1$ pour le reste ;
- $r + 1 = p$: dans ce cas on a $n + 1 = pq + p = p(q + 1)$ et le résultat est démontré pour $n + 1$ en prenant $q + 1$ comme quotient et 0 comme reste.

Si maintenant $n < 0$ alors $-n > 0$ et on vient de voir qu'il existe q et r tels que $-n = pq + r$ et $0 \leq r < p$; donc $n = -pq - r = p(-q) - r$. Si $r = 0$ alors $n = p(-q)$ et le résultat est démontré en prenant $-q$ comme quotient et 0 comme reste. Si $r > 0$ alors $n = p(-q) - r = p(-q - 1) + p - r$ et comme $0 < r < p$ on a $0 < p - r < p$ également, donc le résultat est démontré en prenant $-q - 1$ comme quotient et $p - r$ comme reste.

Montrons maintenant l'unicité : soient q, r, q', r' tels que $n = pq + r = pq' + r'$, $0 \leq r < p$ et $0 \leq r' < p$. Alors on a $pq + r - pq' - r' = p(q - q') + r - r' = 0$. Mais comme r et r' sont tous deux compris entre 0 et p, on a $-p < r - r' < p$, donc $p(q-q') - p < p(q-q') + r - r' < p(q-q') + p$, c'est à dire $p(q-q'-1) < 0 < p(q-q'+1)$. Comme p est positif non nul on obtient $q - q' - 1 < 0 < q - q' + 1$. La première inéquation est équivalente à $q - q' \leq 0$ et la seconde à $q - q' \geq 0$, donc $q - q' = 0$, soit $q = q'$. Comme par hypothèse $pq + r = pq' + r'$ on en déduit que l'on a également $r = r'$.

5.1.4 Théorème de Bezout

5.6 Théorème (Bezout)
Deux entiers m et n sont premiers entre eux ssi il existe des entiers u et v tels que $um + vn = 1$.

Preuve. Supposons qu'il existe u et v tels que $um + vn = 1$ et soit d un diviseur de m et n ; alors d divise 1 donc $d = 1$. Le seul diviseur commun de m et n est 1 donc m et n sont premiers entre eux.

Supposons maintenant que m et n sont premiers entre eux. Notons I l'ensemble des entiers de la forme $um+vn$ pour tous les $u, v \in \mathbb{Z}$. Alors I est non vide et contient des entiers positifs. Soit d le plus petit élément strictement positif de I. Par définition de I il existe des entiers u_0 et v_0 tels que $u_0m + v_0n = d$.

Faisons maitenant la division euclidienne de m par d : on obtient q et r tels que $m = dq + r$, avec $0 \leq r < d$. Donc $r = m - dq = m - (u_0m + v_0n)q = (1 - u_0q)m - v_0qn$ et par conséquent $r \in I$. Mais comme $0 \leq r < d$ et d a été supposé le plus petit élément strictement positif dans I, on doit avoir $r = 0$. Donc d divise m. On peut voir de même que d divise n. Par conséquent, comme m et n sont premiers entre eux on a $d = 1$ et comme $d = u_0m + v_0n$ le théorème est démontré.

5.7 Corollaire
Soit m et n deux entiers et d leur PGCD. Il existe des entiers u et v tels que $um + vn = d$.

Preuve. Comme d divise m il existe m' tel que $m = m'd$; de même il existe n' tel que $n = n'd$. On va voir que m' et n' sont premiers entre eux.

Soit p un diviseur de m' et n' ; on a donc deux entiers k et l tels que $m' = kp$ et $n' = lp$; par conséquent on a $m = kpd$ et $n = lpd$, donc pd divise m et n. Mais d est le PGCD de m et n donc $pd \leq d$ ce qui ne se peut que si $p = 0$ ou $p = 1$. Mais p ne peut être nul car c'est un diviseur, donc $p = 1$. On vient de montrer que le seul diviseur commun de m' et n' est 1, c'est à dire que m' et n' sont premiers entre eux comme annoncé.

On applique le théorème de Bezout à m' et n' ce qui nous donne deux entiers u et v tels que $um' + vn' = 1$, donc $um'd + vn'd = d$, c'est à dire $um + vn = d$ et le corollaire est démontré.

5.8 Corollaire
Si m et n sont deux entiers et si p est un diviseur de m et de n alors p divise le PGCD de m et n.

Preuve. Notons d le PGCD de m et n. Par le théorème de Bezout on sait qu'il existe u et v tels que $um + vn = d$. Comme p divise m et n on en déduit que p divise d.

Exercice 6 Soit m, n, p trois entiers et d leur PGCD, c'est à dire le plus grand diviseurs de à la fois m, n, et p.

i) Montrer que $d = (m \wedge n) \wedge p = m \wedge n \wedge p$.

ii) Montrer qu'il existe des entiers u, v et w tels que $um + vn + wp = d$.

iii) Énoncer et démontrer la généralisation des deux questions précédentes à un nombre quelconques d'entiers.

Exercice 7 Soient m, n et p des entiers. Montrer que $pm \wedge pn = p(m \wedge n)$.

Exercice 8 Montrer que $a \wedge b = a \wedge (b + ax)$ pour tous entiers a, b, x.

Exercice 9 Soient a, b et c trois entiers. Montrer que si $b \wedge c = 1$ alors $ab \wedge c = a \wedge c$.

Exercice 10 Soient m et n deux entiers ; montrer que si u et v sont tels que $um + vn = m \wedge n$ alors u et v sont premiers entre eux.

5.1.5 Décomposition en facteurs premiers

5.9 Théorème
Soient m et n et p trois entiers tels que p divise mn. Si p est premier avec m alors p divise n. En particulier si p est premier alors p divise m ou p divise n.

Preuve. Supposons p premier avec m ; par Bezout il existe u et v tels que $up + vm = 1$. Par conséquent on a $upn + vmn = n$. Mais p divise upn et par hypothèse p divise mn ; donc p divise $upn + vmn$, c'est à dire p divise n.

Supposons maintenant p premier. Si p divise m alors le résultat est démontré ; supposons donc que p ne divise pas m et montrons que p est premier avec m. Soit d un diviseur commun de p et m ; alors d divise en particulier p donc est égal à 1 ou p puisque p est premier ; mais p ne divise pas m, donc $d = 1$. Autrement dit le seul diviseur commun de p et m est 1, c'est à dire que p est premier avec m. On vient de voir qu'alors p divise n.

5.10 Théorème (Décomposition en facteurs premiers)
Soit n un entier naturel non nul. Il existe un unique $k \in \mathbb{N}$ et un unique ensemble de couples $D_n = \{(p_1, \alpha_1), \ldots, (p_k, \alpha_k)\}$ tel que :
– *les p_i sont des nombres premiers deux à deux distincts ;*
– *les α_i sont des entiers naturels non nuls.*
– $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$;

L'ensemble D_n est appelé la décomposition de n en facteurs premiers.

REMARQUE

Si on prend $n = 1$ le théorème est vérifié en prenant $k = 0$ et $D_1 = \emptyset$.

Preuve. On montre l'existence de la décomposition par récurrence sur n. Plus précisément on montre que : pour tout n et pour tout $1 \leq m \leq n$, m admet une décomposition en facteurs premiers. On vient de voir que c'était vrai pour $n = 1$. Soit $n > 1$; notre hypothèse de récurrence est donc que pour tout $m \leq n - 1$, m admet une décomposition en facteurs premiers. Il reste donc à montrer que n admet une décomposition.

Soit p un diviseur premier de n ; il en existe un puisque $n > 1$. Il y a donc un entier n' tel que $n = pn'$. Comme p est premier $p \geq 2$ donc $n \geq 2n'$ et en particulier $n' < n$, c'est à dire $n' \leq n - 1$. Par hypothèse de récurrence on a donc une décomposition $D = \{(p_1, \alpha_1), \ldots, (p_k, \alpha_k)\}$ de n'.

Si p est égal à l'un des p_i, par exemple à p_1 alors $n = pn' = pp_1^{\alpha_1} \ldots p_k^{\alpha_k} = p_1^{\alpha_1+1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$; donc $\{(p_1, \alpha_1 + 1), (p_2, \alpha_2), \ldots, (p_k, \alpha_k)\}$ est une décomposition de n.

Si au contraire p est distinct de tous les p_i alors $n = pn' = p^1 p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ et donc $\{(p, 1), (p_1, \alpha_1), \ldots, (p_k, \alpha_k)\}$ est une décomposition de n. Dans les deux cas on a bien montré l'existence d'une décomposition de n.

Supposons maintenant que n admet deux décompositions $\{(p_1, \alpha_1), \ldots, (p_k, \alpha_k)\}$ et $\{(q_1, \beta_1), \ldots, (q_l, \beta_l)\}$. On va montrer qu'elles sont égales par récurrence sur n ; plus exactement on va montrer par récurrence sur n que pour tout $1 \leq m \leq n$, m a une unique décomposition en facteurs premiers.

Si $n = 1$ alors $k = 0$ et $l = 0$, sinon il y aurait un nombre premier qui divise 1 ce qui ne se peut ; donc les deux décompositions sont égales.

Si $n > 1$ alors soit $n' = p_1^{\alpha_1 - 1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$; on a donc $n = p_1 n'$. Mais p_1 est premier et divise $q_1^{\beta_1} \ldots q_l^{\beta_l}$, donc il y a un i tel que p_1 divise q_i (pourquoi ?). Mais comme q_i est premier, on en déduit que $q_i = p_1$. On a donc $n = p_1 q_1^{\beta_1} \ldots q_i^{\beta_i - 1} \ldots q_l^{\beta_l}$ et par conséquent $n' = q_1^{\beta_1} \ldots q_i^{\beta_i - 1} \ldots q_l^{\beta_l}$. Par récurrence sur n' on en déduit que $\{(p_1, \alpha_1 - 1), \ldots, (p_k, \alpha_k)\} = \{(q_1, \beta_1), \ldots, (q_i, \beta_i - 1), \ldots, (q_l, \beta_l)\}$ ce qui entraîne l'égalité cherchée.

Exercice 11 Montrer que si $n > 4$ alors n divise $(n-1)!$ ssi n n'est pas premier.

5.2 Algorithme d'Euclide

Soient n_0 et n_1 deux entiers naturels tels que $n_0 \geq n_1 > 0$. On construit par récurrence sur k une suite finie $(n_k)_{0 \leq k \leq l}$ d'entiers naturels non nuls.
Supposons n_{k-1} et n_k définis et non nuls. Si n_k divise n_{k-1} alors la suite est terminée ; on a donc $l = k$.
Sinon comme n_k est non nul, on peut effectuer la division euclidienne de n_{k-1} par n_k. On définit n_{k+1} comme le reste de la division euclidienne de n_{k-1} par n_k. Si on note q_k le quotient on a donc

$$n_{k-1} = n_k q_k + n_{k+1}$$

où, par définition de la division euclidienne, $n_{k+1} < n_k$. De plus comme on a supposé que n_k ne divise pas n_{k-1}, n_{k+1} est non nul.

Par construction pour chaque k on a $n_{k+1} < n_k$, la suite construite ainsi est strictement décroissante et comme tous les n_k sont positifs, cette suite est finie. Autrement dit l'algorithme termine.
Cette construction de la suite (n_k) à partir de $n_0 \geq n_1$ s'appelle l'algorithme d'Euclide.

Exercice 12 Construire la suite (n_k) de l'algorithme d'Euclide en partant de $n_0 = 55$ et $n_1 = 34$.

5.11 Théorème
Soient $n_0 \geq n_1 > 0$ deux entiers et $(n_k)_{0\leq k\leq l}$ la suite obtenue à partir de n_0, n_1 par l'algorithme d'Euclide. Pour chaque $k = 1, \ldots, l-1$ on a $n_{k-1} \wedge n_k = n_k \wedge n_{k+1}$. En particulier le PGCD de n_0 et n_1 est égal à n_l.

L'algorithme d'Euclide fournit donc un moyen de calculer le PGCD de deux nombres. On va voir qu'il fait cela de manière très efficace, et d'autre part qu'il permet de faire un peu mieux, à savoir calculer les coefficients u et v du théorème de Bezout.

Preuve. Si $1 \leq k \leq l-1$ on a $n_{k-1} = n_k q_k + n_{k+1}$. Donc si d est un diviseur de n_k et de n_{k+1} alors d divise également n_{k-1}. Réciproquement si d est un diviseur de n_{k-1} et n_k alors comme $n_{k+1} = n_{k-1} - n_k q_k$, d divise également n_{k+1}. Autrement dit n_{k-1} et n_k ont les mêmes diviseurs communs que n_k et n_{k+1} ; en particulier le PGCD de n_{k-1} et n_k est le même que le PGCD de n_k et n_{k+1}.

Par définition de l'algorithme n_l divise n_{l-1} ; donc le PGCD de n_{l-1} et n_l est n_l ; mais c'est le même que celui de n_{l-2} et n_{l-1}, et que celui de n_{l-3} et n_{l-2}, etc. jusqu'à n_0 et n_1.

5.2.1 Une démonstration constructive du théorème de Bezout

La démonstration que l'on a donnée du théorème de Bezout assure l'existence des deux coefficients u et v tels que $um + vn = m \wedge n$, mais elle ne donne aucune indication sur la manière de calculer u et v. L'algorithme d'Euclide permet de résoudre ce problème.
Soient n_0, n_1 tels que $0 < n_1 \leq n_0$ et construisons la suite $(n_k)_{0\leq k\leq l}$ par l'algorithme d'Euclide. Notons $d = n_l$; on sait maintenant que d est le PGCD de n_{k-1} et n_k pour chaque $k = 1, \ldots, l$. Pour $k = l, \ldots, 1$ on va définir des nombres u_k et v_k vérifiant $u_k n_{k-1} + v_k n_k = d$. On aura ainsi redémontré le théorème de Bezout pour n_0 et n_1 et donné une méthode effective pour calculer u_1 et v_1 tels que $u_1 n_0 + v_1 n_1 = d$.
On définit $u_l = 0$ et $v_l = 1$; on a donc bien $u_l n_{l-1} + v_l n_l = n_l = d$. Supposons u_{k+1} et v_{k+1} définis tels que $u_{k+1} n_k + v_{k+1} n_{k+1} = d$. Par définition de l'algorithme d'Euclide, on sait qu'il y a un nombre q_k tel que $n_{k-1} = n_k q_k + n_{k+1}$. Donc $n_{k+1} = n_{k-1} - q_k n_k$ et par conséquent on a $u_{k+1} n_k + v_{k+1}(n_{k-1} - q_k n_k) = d$, soit $v_{k+1} n_{k-1} + (u_{k+1} - q_k) n_k = d$. On pose $u_k = v_{k+1}$ et $v_k = u_{k+1} - q_k$; ainsi on obtient bien $u_k n_{k-1} + v_k n_k = d$, comme annoncé

Exercice 13 On dispose de deux bidons, l'un de 6 litres, l'autre de 11 litres, d'une bassine de plus de 50 litres et d'un robinet d'eau courante. Comment fait-on pour remplir la bassine avec exactement 13 litres d'eau ?

Exercice 14 Appliquer l'algorithme d'Euclide pour trouver les coefficients de Bezout de 55 et 34. Faire de même avec 55 et 36, puis 54 et 35.

Exercice 15 Trouver des entiers x et y tels que :

i) $283x + 1722y = 31$;

ii) $365x + 72y = 18$;

iii) $1111x + 2345y = 66$.

5.2.2 La complexité de l'algorithme de d'Euclide

On va maintenant s'intéresser à la longueur de la suite $(n_k)_{0\leq k\leq l}$ obtenue par l'algorithme d'Euclide, c'est à dire au nombre l. On cherche une majoration de l en fonction de n_0.

Suite de Fibonacci. La suite de Fibonacci est la suite d'entiers naturels $(F_n)_{n\geq 0}$ définie par récurrence sur n : $F_0 = F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$.

Exercice 16 Calculer les 10 premiers termes de la suite de Fibonacci.

Exercice 17 On note $\varphi = (1+\sqrt{5})/2$ et $\bar{\varphi} = (1-\sqrt{5})/2$.

i) Montrer que φ et $\bar{\varphi}$ sont les deux solutions de l'équation $x^2 = x + 1$.

ii) Montrer que pour tout $n \in \mathbb{N}$ on a $F_n = (\varphi^{n+1} - \bar{\varphi}^{n+1})/\sqrt{5}$.

Le nombre réel φ était bien connu des mathématiciens grecs de l'antiquité qui l'appelaient le *nombre d'or*. Comme $0 < \bar{\varphi} < 1$ on voit que dès que n est un peu grand, $\bar{\varphi}^{n+1}$ est presque nul et donc F_n est quasiment égal $\varphi^{n+1}/\sqrt{5}$. On dit que F_n croît exponentiellement avec n.

5.12 Théorème
Soient $n_0 \geq n_1$ deux entiers naturels non nuls et $(n_k)_{0\leq k\leq l}$ la suite obtenue par l'algorithme d'Euclide à partir de n_0 et n_1. Alors $n_0 \geq F_l$.

Preuve. On reprend les notations de la section précédente ; pour $k = 1, \ldots, l$ on a donc $n_{k-1} = n_k q_k + n_{k+1}$; on a vu que $n_{k-1} \geq n_k$, donc $q_k \geq 1$.

On va montrer par récurrence sur k que on a $n_{l-k+1} \geq F_{k-1}$ et $n_{l-k} \geq F_k$ pour $k = 1, \ldots, l$ donc en particulier que $n_0 \geq F_l$ comme annoncé.

Si $k = 1$ alors $n_{l-k+1} = n_l$. Par définition de l'algorithme, on sait que $n_l > 0$ donc $n_l \geq 1 = F_0$. De même $n_{l-k} = n_{l-1}$ est non nul donc $n_{l-1} \geq 1 = F_1$.

Supposons pour la récurrence que $n_{l-k+1} \geq F_{k-1}$ et $n_{l-k} \geq F_k$; il faut voir que $n_{l-k-1} \geq F_{k+1}$. On a $n_{l-k-1} = n_{l-k}q_{l-k} + n_{l-k+1} \geq F_k q_{l-k} + F_{k-1}$. Comme $q_{l-k} \geq 1$ on obtient finalement $n_{l-(k+1)} \geq F_k + F_{k-1} = F_{k+1}$ et le résultat est démontré.

5.13 Corollaire
Il existe des constante réelles positives C et D telles que pour tous entiers naturels non nuls $n_0 \geq n_1$ si $(n_k)_{0\leq k\leq l}$ est la suite obtenue par l'algorithme d'Euclide à partir de n_0 et n_1 alors $l \leq C(\log n_0 + D)$.

Preuve. Soit k le plus petit entier tel que $n_0 < F_k$. D'après le théorème précédent on doit avoir $n_0 \geq F_l$ donc $F_l < F_k$ et comme la suite de Fibonacci est croissante on en déduit que $l \leq k$. Mais comme k est le plus petit tel que $n_0 < F_k$ on a $n_0 \geq F_{k-1}$. Or on a vu que F_{k-1} est équivalent à $\varphi^k/\sqrt{5}$. Donc $n_0 \geq \varphi^k/\sqrt{5}$, et donc $\log n_0 \geq k\log\varphi - \log\sqrt{5}$, c'est à dire $k \leq (\log n_0 + \log\sqrt{5})/\log\varphi$. On a donc $l \leq (\log n_0 + \log\sqrt{5})/\log\varphi \sim 2,07 \times (\log n_0 + 0,8)$.

Le nombre d'étapes de l'algoritme d'Euclide est donc, à une constante près, majoré par le log de n_0. Pour se faire une idée, on peut calculer le PGCD de toute paire d'entiers inférieurs à 1 000 000 avec moins de 30 divisions euclidiennes ; si les entiers sont inférieurs à 10^{100} alors le calcul ci-dessus montre que l'algorithme d'Euclide compte moins de 500 divisions euclidiennes.

Bibliographie

[BBE+07] Hassan Boualem, Robert Brouzet, Bernhard Elsner, Laurent Kaczemarek, and Denis Pennequin. *Mathématiques L1*. Pearson education, 2007.

[LC93] Daniel Lascar and René Cori. *Logique mathématique*. Masson, 1993.