Le langage mathématique

Lycée Berthollet, MPSI^2 2023-24

I Introduction

Le but des mathématiques (et des sciences en général) est la recherche de la *vérité* : on cherche à établir certains faits à l'aide de preuves. La plupart du temps, dans le monde mathématique réel (celui des chercheurs), on ne sait pas au départ si tel résultat est vrai ou non. On parle alors de problème *ouvert* ("$\sqrt{2}$ est-il rationnel ?"), par opposition aux problèmes fermés souvent rencontrés dans l'enseignement ("montrer que $\sqrt{2}$ est irrationnel"). Dans le premier cas, on doit *conjecturer* le résultat, puis tenter de le prouver, quitte à changer d'avis en cours de route, souvent suite à l'apparition, au cours de la recherche de la preuve, de *contrexemples* qui nous permettent de modifier la conjecture. Dans tous les cas, la résolution n'est achevée qu'une fois établie la *démonstration* du résultat.

Deux phases alternent, souvent assez rapidement, lors de ce processus scientifique : la phase de création, pour imaginer une conjecture, des contrexemples, des preuves, et la phase de validation qui consiste en la production d'une preuve *rigoureuse* et sa vérification. Les qualités requises au cours de ces deux phases sont presque antagonistes : introduire trop de rigueur bride la créativité et l'intuition. Il est donc nécessaire, au cours de cette alternance de savoir exactement à chaque instant dans quelle phase on est. Lors de l'écriture de la démonstration, on ne laissera aucun point dans l'ombre, ce qui nécessite *rigueur* et *honnêteté intellectuelle*, pour être "certain" du résultat obtenu. Lors des phases de créativité, il faut laisser libre cours à son imagination, se "lâcher", utiliser des analogies, des *métaraisonnements*, éviter l'autocensure.

Un exemple de métaraisonnement fréquent est l'étude des "petits" cas : si une propriété $P(n)$ est vraie pour $n = 0$, 1, 2, ..., 50, on peut conjecturer qu'elle est vraie pour tout entier n. Deux conjectures célèbres de ce type n'ont toujours pas été prouvées, après des siècles de recherche mathématique :

- La conjecture de Goldbach : tout entier pair strictement plus grand que 3 peut s'écrire comme somme de deux nombres premiers.
- La conjecture des nombres premiers jumeaux : il existe une infinité de couples de nombres premiers jumeaux, c'est-à-dire du type $(n, n+2)$.

Ces deux conjectures ont été vérifiées par ordinateur jusqu'à des rangs gigantesques (voir Wikipedia pour les dernières bornes, qui évoluent fréquemment). Elles peuvent cependant être fausses...

Activité 1 (*Problème des pizzas.*) On découpe une pizza de la manière suivante : on choisit n points au bord de manière "générique" (c'est-à-dire sans particularité) et on découpe la pizza suivant toutes les cordes reliant ces points. Conjecturer le nombre de parts de pizza.

La généricité s'exprime ici par le fait que trois cordes ne sont jamais concourantes en un point strictement intérieur au disque. Noter que la résolution complète de ce problème nécessite des formules qui seront vues dans un chapitre ultérieur, qu'on peut fournir dès maintenant aux plus motivés.

Exercice 2 On trace n droites dans le plan sans que trois de ces droites ne concourent jamais en un même point ni qu'on ait de droites parallèles. Combien cela délimite-t-il de "régions" (finies ou infinies) du plan ?

Pour expérimenter la démarche mathématique, on propose les trois activités suivantes.

Activité 3 (*Énigme géométrique japonaise.*) Étant donné trois cercles deux-à-deux tangents extérieurement et tous trois tangents à une même droite, montrer que leurs rayons R, R' et r vérifient l'identité $\frac{1}{\sqrt{r}} = \frac{1}{\sqrt{R}} + \frac{1}{\sqrt{R'}}$.

On voit à cette occasion que des mathématiques *élémentaires* peuvent mener à des problèmes *difficiles*, même lorsque la solution est elle-même élémentaire et relativement courte.

Activité 4 (*Sur le principe du tiers exclus.*) En utilisant uniquement le fait que $\sqrt{2}$ est irrationnel, montrer qu'il existe deux irrationnels a et b tels que a^b soit rationnel.

On évoque à cette occasion la notion de démonstration *constructive*, c'est-à-dire qui prouve l'existence d'objets mathématiques en les exhibant effectivement.

Activité 5 (*Questionnement de la preuve.*) On présente au tableau une preuve géométrique du fait que $90 = 91$ et on laisse la parole à la classe.

Il ressort de cette dernière activité qu'un *cadre rigoureux* est nécessaire pour définir la notion de démonstration.

II La démarche formelle

L'activité du mathématicien consiste à prouver des *théorèmes*, c'est-à-dire des résultats mathématiques qu'on considère comme avérés à condition qu'on en ait donné des *démonstrations* (on dit aussi des *preuves*). À partir de ces théorèmes, on peut en prouver de nouveaux et construire ainsi l'édifice mathématique. Il n'est cependant pas possible de bâtir cet édifice sans fondations : certains résultats (considérés comme "naturels") sont posés comme vrais au départ, on les appelle des *axiomes* (ou parfois *postulats*). Cette démarche axiomatique et démonstrative remonte à l'antiquité (*cf* par exemple les *Éléments de géométrie* d'Euclide). Elle s'est en général accompagnée d'un souci de *formalisation*, d'une part pour lever au maximum les ambiguïtés des énoncés et d'autre part pour faciliter la validation des démonstrations. Cette démarche de formalisation a connu son apogée à la fin du XIX$^{\text{e}}$ et au début du XX$^{\text{e}}$ siècle, lorsque plusieurs mathématiciens ont voulu exprimer toutes les mathématiques dans un unique langage entièrement formel (on parle de *système formel*). Cela a permis de construire une axiomatique commune à la très grande majorité des mathématiciens actuels, la "théorie des ensembles", dont nous donnons un aperçu dans la section suivante.

Cependant, le but ultime recherché à l'époque était, pour chaque énoncé mathématique, de pouvoir le prouver ou prouver sa négation et ainsi décider de sa véracité. Ce dernier but n'a non

seulement pas été atteint, mais le logicien Kurt Gödel a prouvé dans les années trente que cela était inatteignable : dans tout système formel non contradictoire permettant d'exprimer les propriétés des entiers naturels (ce qui semble un minimum pour faire des mathématiques) il existe des énoncés *indécidables*, c'est-à-dire pour lesquels il n'existe ni démonstrations, ni démonstrations de leurs négations. Ce résultat, même s'il a été en son temps un choc pour le monde mathématique, est plutôt un bonne nouvelle puisqu'il montre qu'aucune automatisation complète des mathématiques n'est possible et qu'il restera donc toujours une place pour l'homme et sa créativité dans ce domaine.

Cependant, tous les énoncés que nous considérerons dans la suite de ce cours seront **décidables** et nous nous poserons la question de savoir s'ils sont vrais ou faux.

III Axiomatique de Zermelo-Fraenkel

Actuellement, la plupart des mathématiciens travaillent implicitement dans le système formel de Zermelo-Fraenkel (ZF) conçu au début du XX^{e} siècle. Les preuves qu'ils produisent ne sont cependant pas entièrement écrites en langage formel car elles seraient peu compréhensibles par l'homme. Toutefois, ils restent persuadés que ces preuves seraient formalisables et donc que leurs résultats sont bien des théorèmes (ce qui n'est parfois pas le cas...). Pour comprendre le langage mathématique "courant", il est utile d'avoir une petite idée du langage formel qu'il est censé représenter.

Les objets de base du système formel ZF sont les **ensembles**, c'est pourquoi on l'appelle aussi la "théorie des ensembles". Pour décrire ZF, il faut d'abord définir la syntaxe des énoncés mathématiques : il comprennent des variables (x, y, z,...), des parenthèses ("(", ")"), des connecteurs logiques ($\neg$ ("non"), $\wedge$ ("et"), $\vee$ ("ou"), $\Longrightarrow$ ("implique"), $\Longleftrightarrow$ ("est équivalent à")), des quantificateurs ($\forall$ ("pour tout") et $\exists$ ("il existe")) et des relations ($=$ ("égale"), $\in$ ("appartient à")). À cela s'ajoutent au fur et à mesure de la construction de nouveaux symboles qui permettent des *abréviations* des énoncés (par exemple $\subset$, $\cup$, $\cap$, $\{x,y\}$,... mais encore 0, 1, $+$, $\times$, 3.14159, cos,...). On notera ici ces abréviations à l'aide de la notation "deux point égale" : par exemple dans cette théorie, le nombre 3 est défini comme un ensemble (tous les objets de la théorie des ensembles sont des ensembles !) de la manière suivante :

$$3 := \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}.$$

On a aussi par exemple $a \subset b \ := \forall x, (x \in a \Longrightarrow x \in b)$. Il y a ensuite des règles qui permettent de définir les énoncés "bien formés" (par exemple, si A et B sont bien formés, alors $A \vee B$ est bien formé,...) qu'on ne donnera pas *in extenso* ici.

Remarquons que, dans la suite du cours de mathématiques, pour simplifier la lecture, nous remplacerons dans les énoncés formels les trois connecteurs logiques $\neg$, $\wedge$, $\vee$ par les mots "non", "et","ou".

Voici quelques énoncés bien formés de ZF :

$$\exists \varepsilon \in \mathbb{R}_+^\star, \exists q \in \mathbb{Q}, ((q > x - \varepsilon) \text{ et } (q < x + \varepsilon))$$

$$\exists n_0 \in \mathbb{N}, \forall p \in \mathbb{N}^\star, ((\forall q \in \mathbb{N}^\star, ((\exists k \in \mathbb{N}^\star, qk = p) \Longrightarrow (q = 1 \text{ ou } q = p))) \Longrightarrow (p \leq n_0))$$

Les suites suivantes de symboles ne sont pas des énoncés bien formés :

$$\exists \varepsilon \in \mathbb{R}_+^\star, \exists q \in \mathbb{Q}, ((q > x - \varepsilon) \text{ et } (q < x + \varepsilon)$$

$$\exists \varepsilon \in \mathbb{R}_+^\star, ((q > x - \varepsilon) \text{ et } (q < x + \varepsilon)), \forall q \in \mathbb{Q}$$

Les suites suivantes sont des *termes*. Ils sont censés représenter des objets de la théorie, mais ne forment pas un énoncé, tout comme en français les groupes nominaux ne sont pas des phrases :

$$(1+2) \times 3$$

$$x + \varepsilon$$

$$\sum_{i=1}^{n} i^2$$

Pour énoncer les axiomes et plus généralement comprendre les énoncés mathématiques, il est nécessaire de distinguer les occurrences de variables "liées" à une quantification de celles qui ne le sont pas : dans un énoncé formel, pour une variable x fixée, lors d'une quantification $\forall x$ ou $\exists x$, le plus petit sous-énoncé bien formé qui la suit est le *champ* de cette quantification. Toute **occurrence** de la variable x située dans le champ d'un quantificateur $\forall x$ ou $\exists x$ est dite *liée*. Toute occurrence de la variable x qui n'est ni quantifiée ni liée est dite *libre*. Par exemple, dans l'énoncé suivant :

$$(\forall q \in \mathbb{N}^\star, ((\exists k \in \mathbb{N}^\star, qk = p) \Longrightarrow (q = 1 \text{ ou } q = p))) \Longrightarrow (p \leq q)$$

la première occurrence de q est quantifiée, les trois suivantes sont liées et la dernière est libre, toutes les occurrences de p sont libres et les deux occurrences de k sont l'une quantifiée et l'autre liée.

Un fait très important en pratique est que dans une quantification, si l'on remplace l'occurrence quantifiée de la variable quantifiée ainsi que toutes ses occurrences liées correspondant à cette quantification par n'importe quelle variable n'apparaissant pas dans le champ de la quantification, on obtient un énoncé mathématiquement équivalent (en fait plus que cela, c'est en quelque sorte le "même" énoncé). On parle dans ce cas de variable *muette*. Par exemple, l'énoncé $\forall x \in \mathbb{R},\ f(x) > 0$ peut être remplacé par $\forall y \in \mathbb{R},\ f(y) > 0$, car la variable x est muette. Mais attention, les énoncés $f(x) > 0$ et $f(y) > 0$ ne sont eux pas interchangeables, comme on peut le voir en comparant $\forall x \in \mathbb{R},\ f(x) > 0$ et $\forall x \in \mathbb{R},\ f(y) > 0$. On retrouve cette notion de variable muette dans les sommes et les intégrales : $\sum_{k=1}^{n} k^2 = \sum_{i=1}^{n} i^2$, $\int_a^b f(x)\,\mathrm{d}x = \int_a^b f(u)\,\mathrm{d}u$. Elle est analogue à la notion de variable locale en informatique.

Un énoncé avec n variables $x_1, \ldots, x_n$ ayant des occurrences libres est appelé un *prédicat* à n places et souvent noté $P(x_1, \ldots, x_n)$. Voici des exemples de prédicats :

$$2^k > k, \quad x \leq y, \quad x^n + y^n = z^n$$

Un énoncé sans occurrences libres de variables est appelé un énoncé *clos*. Par exemple :

$$\forall x \in \mathbb{R}, \forall \varepsilon \in \mathbb{R}_+^\star, \exists q \in \mathbb{Q}, ((q > x - \varepsilon) \text{ et } (q < x + \varepsilon))$$

Il y a ensuite deux règles qui permettent la démonstration des théorèmes, la première, largement utilisée dans l'enseignement secondaire est appelée le *modus ponens :* si l'énoncé A et l'énoncé $A \Longrightarrow B$ sont des théorèmes, alors B est un théorème. La deuxième, plus technique, est la règle de *généralisation :* si A est un théorème et x une variable, alors $\forall x, A$ est un théorème.

Pour finir de décrire ZF, il ne reste alors plus qu'à donner les axiomes, ce qu'on fait à titre indicatif en appendice.

Un texte mathématique classique suit à peu près ce schéma : on définit des objets, on énonce des résultats (théorèmes, lemmes, propositions,...) qu'on démontre, on en donne des exemples et contrexemples, on donne de nouvelles définitions et ainsi de suite... Les énoncés sont donnés soit en langage formel, soit en français, mais on évite les mélanges (à quelques exceptions près qu'on décrira *in situ*). Si une partie d'un énoncé ou d'une démonstration en français est écrite en langage formel, on la sépare nettement, par exemple avec des parenthèses ou des crochets. **Tous les énoncés sont clos**, c'est-à-dire que toute occurrence de variable doit être quantifiée ou liée, et dans les démonstrations **tout objet utilisé doit avoir été préalablement introduit**.

Dans les deux sections suivantes, on présente tout ce qu'il est utile de savoir au mathématicien débutant sur la logique et la théorie des ensembles. Le lecteur exigeant pourra vérifier que tout cela est compatible avec les axiomes donnés en appendice.

IV Logique

Les premiers axiomes de ZF régissent le rôle des connecteurs logiques. Une autre manière de décrire ces connecteurs est de les définir par tables de vérité (c'est-à-dire en parcourant tous les cas possibles), ce que nous allons faire ici. La logique obtenue est alors **identique** à celle définie axiomatiquement dans ZF. Les lettres A, B et C, A_1, …, A_n, désignent ici des énoncés.

Donnons par exemple les tables de vérité des connecteurs "non" et "et", en représentant *vrai* par la lettre V et *faux* par la lettre F :

A	non A
V	F
F	V

A	B	A et B
V	V	V
V	F	F
F	V	F
F	F	F

Activité 6 On fait construire par la classe les tables de vérité suivantes, en suscitant autant que possible le débat :

A	B	A ou B
V	V	
V	F	
F	V	
F	F	

A	B	$A \Longrightarrow B$
V	V	
V	F	
F	V	
F	F	

A	B	$A \Longleftrightarrow B$
V	V	
V	F	
F	V	
F	F	

Remarque 7 (**Formulations de l'implication**)

Il y a de nombreuses manières de formuler en français l'*implication* $A \Longrightarrow B$:

— "A implique B" ;
— "Si A, alors B" ;
— "B si A" ;
— "Pour avoir B, il *suffit* d'avoir A" ;
— "A est une condition *suffisante* pour B" ;
— "Pour avoir A, il est *nécessaire* d'avoir B" ;
— "B est une condition *nécessaire* pour A" ;

— “Pour avoir A, il *faut* avoir B”.

Remarque 8 (**Formulations de l’équivalence**)
On formule aussi l’*équivalence* $A \iff B$ de différentes manières :
— “B est une condition *nécessaire et suffisante* pour A” ;
— “Pour avoir A, *il faut et il suffit* que B soit vérifiée” ;
— “*A si et seulement si B*”.

Remarque 9 Dans les énoncés en français, nous nous autoriserons parfois l’abréviation “ssi” pour “si et seulement si”, mais il serait **fautif** de mettre à la place le symbole $\iff$.

Remarque 10 (**Priorité des opérateurs logiques**)
Pour alléger les écritures des opérations logiques, on convient, comme pour les opérations arithmétiques, de priorités sur les opérations logiques :
— le “non” est prioritaire sur tous les autres opérateurs ;
— le “et” est prioritaire sur le “ou”.
Par exemple, $[A$ ou non B et non $C]$ signifie $[A$ ou $((\text{non } B)$ et $(\text{non } C))]$.

Activité 11 (*Exemple de démonstration mathématique*)
Pour x réel, montrer que

$$\left[x^2 \leq 4 \iff (x \leq 2 \text{ et } x \geq -2)\right].$$

On y voit différents types de raisonnements.

Plus généralement, on utilise souvent les “méthodes” suivantes :

Principes logiques de démonstration
— Pour montrer $[A$ et $B]$, on montre A et on montre B.
— Pour montrer $[A$ ou $B]$, on peut supposer non A et montrer B.
— Pour montrer $A \Longrightarrow B$, on peut supposer A et montrer B, ou alors supposer non B et montrer non A (**raisonnement par contraposition**).
— Pour montrer $A \iff B$, on montre $A \Longrightarrow B$ et on montre $B \Longrightarrow A$.
— Pour montrer $(A$ ou $B) \Longrightarrow C$, il suffit de montrer $A \Longrightarrow C$ et montrer $B \Longrightarrow C$ (**principe de disjonction des cas**).
— non $(A$ et $B) \iff (\text{non } A$ ou non $B)$ (**loi de De Morgan**)
— non $(A$ ou $B) \iff (\text{non } A$ et non $B)$ (**loi de De Morgan**)

Pour montrer que ces méthodes sont valides, on peut raisonner par tables de vérités en utilisant les deux lemmes naturels suivants, qu’on admet :

Lemme 12 *Si deux opérations logiques $P(A_1,\ldots,A_k)$ et $Q(A_1,\ldots,A_k)$ ont les mêmes tables de vérité, elles sont équivalentes.*

Lemme 13 *Si on remplace, dans un énoncé, une partie de cet énoncé qui est lui même un énoncé par un énoncé équivalent à ce sous-énoncé, on obtient un énoncé équivalent à l’énoncé initial.*

Activité 14 On demande de valider certaines des méthodes précédentes par tables de vérité et notamment l’une des lois de De Morgan :

A	B	A ou B	non (A ou B)	non A	non B	non A et non B
V	V					
V	F					
F	V					
F	F					

Pour la deuxième loi de De Morgan, on peut utiliser la première, ainsi que les équivalences suivantes, qu'on pourrait aussi montrer par table de vérité, et qui sont à la fois très naturelles et très utiles :

Proposition 15 *(Équivalences simples)*
non non $A \iff A$
$(A \iff B) \iff (B \iff A)$
$(\text{non } A \iff \text{non } B) \iff (A \iff B)$

Les deux résultats suivants sont à savoir restituer sans hésitation :

Proposition 16 *(Reformulation et négation de l'implication)*
$(A \Longrightarrow B) \iff (\text{non } A \text{ ou } B)$
non $(A \Longrightarrow B) \iff (A \text{ et non } B)$

Démonstration: en exercice, le premier résultat se démontre par tables de vérité et le deuxième en utilisant une loi de De Morgan. □

On se sert souvent de cette proposition pour démontrer qu'un résultat $A \Longrightarrow B$ est faux en exhibant un contrexemple qui vérifie l'hypothèse A mais pas la conclusion B.

Exemple 17 L'énoncé $\big(\forall x \in \mathbb{R}, (x^2 > 1 \Longrightarrow x > 1)\big)$ est faux. En effet le réel -2 vérifie $(-2)^2 > 1$, mais il est faux que $-2 > 1$.

Enfin, il est utilse de connaître les résultats suivants :

Proposition 18 *(Propriétés du "et" et du "ou")*
$(A \text{ et } B) \iff (B \text{ et } A)$ *(Commutativité du "et")*
$(A \text{ ou } B) \iff (B \text{ ou } A)$ *(Commutativité du "ou")*
$(A \text{ et } (B \text{ et } C)) \iff ((A \text{ et } B) \text{ et } C)$ *(Associativité du "et")*
$(A \text{ ou } (B \text{ ou } C)) \iff ((A \text{ ou } B) \text{ ou } C)$ *(Associativité du "ou")*
$(A \text{ et } (B \text{ ou } C)) \iff (A \text{ et } B \text{ ou } A \text{ et } C)$ *(Distributivité de "et" par rapport à "ou")*
$(A \text{ ou } B \text{ et } C) \iff ((A \text{ ou } B) \text{ et } (A \text{ ou } C))$ *(Distributivité de "ou" par rapport à "et")*

Démonstration: En exercice, par tables de vérité. Pour l'associativité du "et", on remplira la table de vérité suivante, puis on procèdera de manière analogue pour les autres résultats.

A	B	C	B et C	A et $(B$ et $C)$	A et B	$(A$ et $B)$ et C
V	V	V				
V	V	F				
V	F	V				
V	F	F				
F	V	V				
F	V	F				
F	F	V				
F	F	F				

□

Voici un exercice récapitulatif sur les connecteurs logiques et le raisonnement :

Exercice 19 Lors d'une réunion pédagogique, on entend les affirmations suivantes, dont chacune est soit vraie, soit fausse :

— Chris : "$4+2\times 5=\frac{48}{12}+\frac{28}{4}+19$."
— Smarty : "J'ai mangé un beignet à midi."
— Fred : "Smarty ment."
— J.-B. : "Si Fred dit la vérité, alors Chris aussi."

1. Combien y a-t-il d'affirmations fausses parmi les trois premières ?
2. Montrer qu'il y a exactement une phrase fausse parmi celles de J.-B. et de Fred.

On entend alors une cinquième affirmation, elle aussi vraie ou fausse :

— Denise : "Il y a exactement trois affirmations fausses parmi ces cinq."

3. J.-B. dit-il la vérité ?
4. Que peut-on en déduire sur Fred, Smarty et Denise ?

V Ensembles et quantificateurs

1 Premiers ensembles et appartenance

Certaines "collections" non ordonnées d'objets (mathématiques) sont des *ensembles*. Il sont en général représentés par des lettres majuscules (à ne pas confondre avec les énoncés mathématiques des sections précédentes) pour aider la distinction entre un ensemble et ses éléments (représentés en général par des lettres minuscules).

Ensembles de nombres

Activité 20 Décrivez les **ensembles de nombres** suivants :

$$\mathbb{N}\subset\mathbb{Z}\subset\mathbb{D}\subset\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}.$$

Leur définition nécessite cependant l'introduction d'un très grand nombre d'axiomes et d'abréviations de ZF.

Ensembles finis

Toute collection **finie** (non ordonnée) d'objets est un ensemble (par les axiomes de la paire et de la réunion) et on peut le représenter en mettant ces objets entre accolades :

$$\{a,b,c\},\ \{5,1,3\},\ \emptyset := \{\},\ \{\emptyset\},\ \{\emptyset,\{\emptyset\}\},\ \{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\}$$

Définition 21 (*cf* axiome d'extensionnalité) On dit que deux ensembles A et B sont *égaux* si et seulement s'ils ont les mêmes éléments (*i.e.* pour tout objet x, x est élément de A si et seulement si c'est un élément de B).

Exemple 22 $\{5,1,3\} = \{1,3,5\}$

On autorise dans la notation entre accolades la répétition, surtout pour le cas on ne connaît pas d'éventuelles égalités entre les éléments de l'ensemble. Cependant, à cause de la définition précédente, le nombre d'occurrences de l'élément n'a aucune importance (chaque élément n'appartient "qu'une fois" à l'ensemble) :

$$\{2,2,2,3,1,1\} = \{1,2,3\}$$

Appartenance et sélection d'éléments d'un ensemble

Relation d'appartenance : On note $x \in E$ pour dire que l'objet x est un élément de l'ensemble E :

$$a \in \{a,b,c\},\ c \in \{a,b,c\}, 4 \notin \{1,3,5\},\ \emptyset \notin \emptyset, \{\emptyset\} \in \{\emptyset,\{\emptyset\}\}$$

On **admet** qu'on peut construire un ensemble en **sélectionnant** dans un ensemble E les éléments qui vérifient une certaine propriété mathématique $P(x)$ (*cf* axiome de compréhension), qu'on note

$$\{x \in E \mid P(x)\}$$

et qu'on lit : "l'ensemble des éléments x de E tels que $P(x)$ (soit vérifiée)".

Remarque 23 Il est nécessaire de sélectionner **dans un ensemble**, sous peine d'arriver à des paradoxes, par exemple celui de Russell : si $E = \{x \mid x \notin x\}$ est un ensemble, alors si $E \in E$, $E \notin E$ et si $E \notin E$, $E \in E$. Dans les deux cas, on aboutit à une contradiction (analogue en théorie des ensembles du paradoxe du menteur).

Exemples 24 On peut ainsi définir les intervalles réels ($[-1,2[= \{x \in \mathbb{R} \mid -1 \leq x < 2\},]-\infty,2[= \{x \in \mathbb{R} \mid x < 2\}$), les intervalles entiers ($[\![2,13]\!] = \{n \in \mathbb{N} \mid 2 \leq n \leq 13\}$) ou encore l'ensemble des nombres premiers.

Exercice 25 Écrire en langage formel la propriété $\mathcal{A}(p)$:="p est un nombre premier", puis montrer que la collection des nombres premiers forme un ensemble.

2 Quantificateurs

Lorsqu'une propriété $P(x)$ est vraie **pour tout élément** x d'un ensemble E, on note

$$\forall x \in E, P(x)$$

Lorsqu'une propriété $P(x)$ est vraie **pour au moins un élément** x d'un ensemble E, on note

$$\exists x \in E, P(x)$$

Exemples 26 $(\exists x \in \mathbb{R}, x > 0)$, $(\forall x \in \mathbb{R}, x^2 \geq 0)$, $(\forall z \in \mathbb{C}, z^2 \in \mathbb{R}_+)$.

Remarque 27 Attention, à la différence de la pratique des quantificateurs dans ZF, **on imposera** que tout quantificateur soit suivi d'une relation d'appartenance à un ensemble comme ci-dessus. Cela permet de savoir quel est le "type" de l'objet qu'on manipule (comme dans certain langages informatiques (par exemple *C*), où toute variable doit être déclarée et typée).

Il est cependant utile de garder en mémoire les définitions formelles des énoncés mathématiques avec quantification "dans un ensemble", qui sont :

$$(\forall x \in E, P(x)) := (\forall x, (x \in E \Longrightarrow P(x)))$$

$$(\exists x \in E, P(x)) := (\exists x, (x \in E \text{ et } P(x)))$$

En effet ces définitions permettent de prouver l'"'algorithme" de négation de phrases quantifiées que nous verrons plus tard. Par ailleurs, il découle directement de ces définitions que, pour une propriété quelconque $P(x)$ de la variable x :

$$(\forall x \in \emptyset, P(x)) \text{ est vraie}$$

$$(\exists x \in \emptyset, P(x)) \text{ est fausse}$$

Remarque 28 Les quantificateurs sont à placer impérativement **avant** d'utiliser les variables quantifiées, sous peine de graves ambiguïtés : ils "vont devant". On pourra, par exemple, donner plusieurs "interprétations" de la suite de symboles suivante **qui ne forme pas un énoncé mathématique correct** :

$$\exists m \in \mathbb{N}, n \leq m, \forall n \in \mathbb{N}.$$

Abus de notation : en vue d'alléger les notations, nous noterons $\forall x, y \in E$ au lieu de $\forall x \in E, \forall y \in E$ et de même avec le quantificateur existentiel. Cet abus ne pose pas de problème si toute quantification est suivie d'une appartenance (ce que nous avons convenu) puisqu'alors le quantificateur marque le début de la liste d'objets considérés et l'appartenance en marque la fin, ce qui donne donc une notation non ambiguë.

Définition 29 (*Existence unique*) Lorsqu'il existe un unique $x \in E$ qui vérifie une propriété $P(x)$, on note cela avec un point d'exclamation :

$$\exists\, !x \in E,\ P(x)$$

Cette notation très pratique remplace une suite de symboles formels qu'il serait pénible d'écrire à chaque fois qu'on veut exprimer cette unicité et qu'on laisse au lecteur le soin de détailler en exercice (très instructif) :

Exercice 30 Exprimer formellement l'énoncé $(\exists\, !x \in E,\ P(x))$ sans point d'exclamation.

3 Inclusion et ensemble des parties d'un ensemble

On définit la relation d'*inclusion* :

Définition 31 Pour A et B deux ensembles, on note $(A \subset B)$ la propriété $(\forall x \in A, x \in B)$ et on dit que A est inclus dans (ou est une partie de) B.

Deux ensembles sont alors égaux s'il y a "double inclusion" :

Proposition 32 *Pour A et B deux ensembles,*

$$A = B \iff (A \subset B \text{ et } B \subset A)$$

On **admet** que la collection des parties d'un ensemble E forme un **ensemble** noté $\mathcal{P}(E)$ (*cf* axiome de l'ensemble des parties).

Exemple 33 $\mathcal{P}(\{1,3,5\}) = \{\emptyset, \{1\}, \{3\}, \{5\}, \{1,3\}, \{3,5\}, \{5,1\}, \{1,3,5\}\}$

4 Opérations sur les ensembles

Intersection

Les *intersections* (finies ou non) d'ensembles sont des ensembles par sélection :

Définition 34 Pour deux ensembles A et B, $A \cap B := \{x \in A \mid x \in B\}$ est l'ensemble des objets appartenant à A **et** à B.

On définit alors par récurrence "évidente", $A_1 \cap A_2 \cap \ldots \cap A_n$, pour n ensembles A_i, $i \in [\![1,n]\!]$.

Activité 35 Dessiner un diagramme de Venn ("en patates") de trois ensembles et identifier les intersections deux à deux et l'intersection des trois.

Plus généralement, si $\mathcal{A}$ est un ensemble non vide d'ensembles et A_0 un de ses éléments, on peut définir l'intersection des éléments de $\mathcal{A}$, **qui ne dépend pas du choix de** A_0, ainsi :

Définition 36 $\displaystyle\bigcap_{\mathcal{A}} = \bigcap_{A \in \mathcal{A}} A := \{x \in A_0 \mid \forall A \in \mathcal{A}, x \in A\}$

Exemple 37 Si $\mathcal{A} = \left\{I \subset \mathbb{R} \mid \exists n \in \mathbb{N}^\star, I = [0, \frac{1}{n}[\right\}$, alors $\displaystyle\bigcap_{I \in \mathcal{A}} I = \bigcap_{n \in \mathbb{N}^\star} [0, \frac{1}{n}[= \{0\}$.

Remarque 38 On dit que deux ensembles A et B sont *disjoints* ssi $A \cap B = \emptyset$. Par exemple l'ensemble des entiers pairs et celui des entiers impairs sont disjoints.

Réunion

À l'aide de l'axiome de la réunion, on peut aussi définir les réunions (finies ou non) :

Définition 39 $\bigcup_{\mathcal{A}} = \bigcup_{A\in\mathcal{A}} A$ est l'ensemble formé des éléments de tous les ensembles A appartenant à un ensemble $\mathcal{A}$ donné (si $\mathcal{A}=\emptyset$, on a donc $\bigcup_{\mathcal{A}} = \emptyset$).

En particulier pour deux ensembles A et B, $A\cup B = \bigcup_{\{A,B\}}$ est l'ensemble des objets appartenant à A **ou** à B.

On définit de même $A_1\cup A_2\cup\ldots\cup A_n$, pour n ensembles A_i, $i\in[\![1,n]\!]$.

Activité 40 Dessiner un diagramme de Venn de trois ensembles et identifier les réunions deux à deux et la réunion des trois.

Remarque 41 Lorsque A et B sont disjoints, on parle de *réunion disjointe* et on note alors cette réunion $A\sqcup B$.

Par exemple, $\mathbb{Z}$ est réunion disjointe de l'ensemble P des entiers pairs et de l'ensemble I des entiers impairs : $\mathbb{Z} = P\sqcup I$.

Pour les réunions quelconques, on a la définition suivante :

Définition 42 Une réunion est dite *disjointe* ssi les ensembles qu'on réunit sont deux-à-deux disjoints. On la note alors avec un symbole $\bigsqcup$.

Exemple 43 Par exemple, prenons E un ensemble quelconque et $\mathcal{S}$ l'ensemble des singletons formés à partir des éléments de E. Alors la réunion $\bigcup_{A\in\mathcal{S}} A$ est disjointe, car deux singletons différents sont disjoints, et vaut E, ce qu'on note

$$E = \bigsqcup_{A\in\mathcal{S}} A.$$

Notion de famille d'ensembles

On utilisera dès maintenant la notion de *famille d'ensembles* sans la définir formellement (cela devrait intervenir plus tard dans le développement théorique) pour se l'approprier progressivement. Pour définir une telle famille, on prend un ensemble d'indices I, qui est un ensemble quelconque (fini ou infini), et on fait correspondre à chaque indice $i\in I$ un ensemble qu'on note A_i. La famille est alors notée $(A_i)_{i\in I}$.

Dans le cas où I est fini, c'est souvent une intervalle d'entiers de la forme $[\![1,n]\!]$ et on peut utiliser les différentes notations suivantes :

$$(A_i)_{i\in[\![1,n]\!]} = (A_i)_{1\leq i\leq n} = (A_i)_{i=1}^n = (A_1,A_2,\ldots,A_n).$$

Cependant, dans le cas général, l'ensemble I n'est supposé ni fini, ni même ordonné.

On peut définir l'intersection d'une telle famille lorsque I est **non vide** : $\bigcap_{i\in I} A_i$ est l'ensemble des objets mathématiques x tels que $\forall i\in I,\ x\in A_i$.

On peut aussi définir la réunion d'une telle famille pour I quelconque : $\bigcup_{i\in I} A_i$ est l'ensemble des objets mathématiques x tels que $\exists i\in I,\ x\in A_i$.

Exemple 44 On reformule l'exemple 43 en définissant la famille des singletons $(\{x\})_{x\in E}$ et on a alors

$$E = \bigsqcup_{x\in E} \{x\}\,.$$

Remarquons que l'ensemble des indices est ici E.

Partitions et recouvrements

Définition 45 Lorsqu'un ensemble E est réunion disjointe d'une famille de parties non vides de E, on dit que cette famille est une *partition*.

Exemples 46

1. Dans un exemple précédent, (P,I) est une partition de $\mathbb{Z}$.
2. Pour tout ensemble E, la famille des singletons de ses éléments est une partition de E. Par exemple, $(\{n\})_{n\in\mathbb{N}}$ est une partition de $\mathbb{N}$.
3. Les $\{j+4k;\ k\in\mathbb{Z}\}$, pour $j\in\{0,1,2,3\}$, forment une partition de $\mathbb{Z}$.

Définition 47 On dit qu'une famille d'ensembles $(A_i)_{i\in I}$ est un *recouvrement* d'un ensemble E ssi $X\subset\bigcup_{i\in I} A_i$.

Exemple 48 En particulier, une partition d'un ensemble en est un recouvrement disjoint.

Différence

Définition 49 Pour deux ensembles A et B on appelle *différence* de A par B l'ensemble $A\setminus B := \{x\in A \mid x\notin B\}$ des éléments qui sont dans A et non dans B.

Remarque 50 On ne requiert pas que $B\subset A$ pour calculer $A\setminus B$.

Activité 51 Dessiner un diagramme de Venn de deux ensembles et identifier les deux différences ensemblistes possibles.

Définition 52 Si A et E sont deux ensembles tels que $A\subset E$, on définit le *complémentaire* de A dans E, $E\setminus A$, parfois noté $\overline{A}$ ou A^c si l'ensemble E est sous-entendu (par exemple en probabilités).

Différence symétrique

Définition 53 La *différence symétrique* de deux ensembles A et B est $A\triangle B := (A\cup B)\setminus(A\cap B) = (A\setminus B)\cup(B\setminus A)$

Activité 54 Décrire en français $A\triangle B$, puis la dessiner sur un diagramme de Venn.

5 Propriétés des opérations

Ces opérations vérifient de nombreuses propriétés. On en donne quelques unes.

Définition 55 On dit qu'une opération $\star$ sur les ensembles est *associative* ssi, pour tous ensembles A, B et C,

$$A \star (B \star C) = (A \star B) \star C$$

On dit qu'elle est *commutative* ssi, pour tous ensembles A et B,

$$A \star B = B \star A$$

Enfin, on dit que l'opération $\star$ est distributive par rapport à une autre opération $\diamond$ ssi, pour tous ensembles A, B et C,

$$A \star (B \diamond C) = (A \star B) \diamond (A \star C) \quad \text{et} \quad (A \diamond B) \star C = (A \star C) \diamond (B \star C)$$

Proposition 56
La réunion, l'intersection et la différence symétrique sont associatives et commutatives.
L'intersection est distributive par rapport à la réunion et vice-versa.

Démonstration: les faire en exercice, mis à part celle de l'associativité de la différence symétrique qui se fait beaucoup plus aisément en utilisant les propriétés du prochain paragraphe et les tables de vérité. □

Voici aussi deux autres propriétés très utiles, dont on laisse les démonstrations en exercice.

Proposition 57 *(“Croissances” de l'intersection et de la réunion avec un ensemble)*
Pour tous A, B, C ensembles,

$$A \subset B \Longrightarrow A \cap C \subset B \cap C \quad \text{et} \quad A \subset B \Longrightarrow A \cup C \subset B \cup C.$$

Proposition 58 *Le passage au complémentaire échange union et intersection.*
Plus généralement, pour tous A, B, C ensembles,

$$C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B) \quad \text{et} \quad C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B).$$

Voici un exercice récapitulatif sur les opérations ensemblistes :

Exercice 59 Soient les ensembles suivants : $E = \{a,b,c,d,e,f\}$, $A = \{a,\{b,c\}\}$, $B = \{\{a,d\},\{\{b,c\},\{e,f\}\}\}$, $C = \{\{a,d\},\{e,f\}\}$.

1. Calculer $A \cup B \cup C$.
2. Est-ce que $B = E$?
3. Est-ce que $A \subset B$?
4. Est-ce que $A \subset \mathcal{P}(E)$? $B \subset \mathcal{P}(E)$? $C \subset \mathcal{P}(E)$?
5. Comparer $\bigcup_{X \in B} X$ et E. Que dire de $\bigcup_{X \in C} X$ et E ?
6. Exprimer $\mathcal{P}(B)$.
7. Calculer $B \setminus A$ et $B \setminus C$.
8. Quel relation y a-t-il entre C et $\mathcal{P}(\mathcal{P}(E))$?

6 Lien avec les connecteurs logiques

En voici quelques exemples sous forme d'exercices.

Exercice 60 Soit E un ensemble, P et Q deux propriétés mathématiques d'une variable x, $A = \{x \in E \mid P(x)\}$ et $B = \{x \in E \mid Q(x)\}$. Exprimer les ensembles suivants en fonction de A et B :
- $\{x \in E \mid P(x) \text{ et } Q(x)\}$
- $\{x \in E \mid P(x) \text{ ou } Q(x)\}$
- $\{x \in E \mid \text{non } P(x)\}$
- $\{x \in E \mid P(x) \text{ et non } Q(x)\}$
- $\{x \in E \mid P(x) \Longrightarrow Q(x)\}$

Comment reconnaître que $(\forall x \in E, (P(x) \Longrightarrow Q(x)))$?

Exercice 61 Soient A, B et C trois ensembles et $P(x) := (x \in A)$, $Q(x) := (x \in B)$ et $R(x) := (x \in C)$. Exprimer une propriété équivalente à la propriété $(x \in A \triangle B)$ en utilisant $P(x)$ et $Q(x)$.

On note cette propriété $P(x)$ xou $Q(x)$. Définir plus généralement le connecteur logique "xou" ("ou" exclusif) en donnant la table de vérité de S xou T, pour S, T deux variables logiques quelconques.

En déduire l'associativité de la différence symétrique à l'aide de tables de vérité.

7 Produit cartésien

Définition 62 (**Couple**)
Un *couple* d'objets (a,b) est la donnée de deux objets a et b, éventuellement égaux, dans un ordre précis (l'un étant la première composante du couple et l'autre la seconde).

Remarque 63 Le couple (a,b) est donc différent de la paire $\{a,b\}$ (et aussi du couple (b,a) si $a \neq b$).

Remarque 64 On peut définir précisément cela en théorie des ensembles par $(a,b) = \{\{a\}, \{a,b\}\}$, ce qui ne nécessite aucun axiome autre que celui de la paire, déjà utilisé plus haut.

Définition 65 Le produit cartésien de deux ensembles A et B est l'ensemble des couples dont la première composante est élément de A et la seconde est élément de B, ce qu'on note aussi :

$$A \times B = \{(x,y); x \in A, y \in B\}$$

Remarque 66 En fait, à l'aide de la définition ensembliste de couple vue plus haut, le produit cartésien $A \times B$ est défini par sélection dans l'ensemble $\mathcal{P}(\mathcal{P}(A \cup B))$. Écrivez-le.

Exemples 67 $\mathbb{R}^2$, $\mathbb{R}_+ \times [0, 2\pi[$ (coordonnées polaires), $\mathbb{R} \times \mathbb{N}$ (le représenter graphiquement).

Exercice 68 Soient A, B, C et D quatre ensembles. Montrer par double inclusion que $(A \times C) \setminus (B \times D) = ((A \setminus B) \times C) \cup ((A \cap B) \times (C \setminus D))$ et que cette réunion est disjointe.

Ces définitions se généralisent au cas de plus de deux objets :

Définition 69 Un n-uplet $(x_1, \ldots, x_n)$ est la donnée de n objets dans un certain ordre. Le produit cartésien de n ensembles $A_1, \ldots, A_n$ est l'ensemble des n-uplets suivant :

$$A_1 \times \ldots \times A_n = \{(x_1, \ldots, x_n); \forall i \in [\![1,n]\!], x_i \in A_i\}$$

Exemples 70 $\mathbb{R}^3$, $\mathbb{R}^n$.

8 Négation d'un énoncé quantifié

On cherche ici à exprimer la négation d'un énoncé quantifié sous une forme équivalente qui ne contienne pas de négation d'une partie "complexe" de l'énoncé. Cela se fait en "faisant sauter" la négation par dessus chaque quantificateur, à l'aide des règles suivantes, qu'on admet après les avoir élaborées à partir d'exemples concrets en langage usuel. :

Proposition 71 *Pour tout prédicat P et tout ensemble E, on a les deux équivalences :*

$$(\text{non } (\forall x \in E, P(x))) \iff (\exists x \in E, (\text{non } P(x)))$$

$$(\text{non } (\exists x \in E, P(x))) \iff (\forall x \in E, (\text{non } P(x)))$$

Exercice 72 Nier les énoncés mathématiques suivants :

1. $\forall x \in \mathbb{R}, \forall \varepsilon \in \mathbb{R}_+^\star, \exists q \in \mathbb{Q}, ((q > x - \varepsilon) \text{ et } (q < x + \varepsilon))$
2. $\exists (a,b) \in (\mathbb{R}_+^\star \setminus \mathbb{Q})^2, a^b \in \mathbb{Q}$
3. $\forall \varepsilon > 0, \exists \alpha > 0, \forall x \in \mathbb{R}, (|x-a| \leq \alpha \Longrightarrow |f(x) - \ell| \leq \varepsilon)$
4. $\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, \forall p \in \mathbb{N}, (((n \geq N) \text{ et } (p \geq N)) \Longrightarrow |u_n - u_p| \leq \varepsilon)$
5. $\exists n_0 \in \mathbb{N}, \forall p \in \mathbb{N}^\star, ((\forall q \in \mathbb{N}^\star, ((\exists k \in \mathbb{N}^\star, qk = p) \Longrightarrow (q = 1 \text{ ou } q = p))) \Longrightarrow (p \leq n_0))$
6. La fonction f est décroissante au sens large sur $\mathbb{R}$.

VI Différents types de raisonnement

1 Raisonnement direct

C'est le plus fréquent. On utilise le *modus ponens* : on sait que $(A \Longrightarrow B)$ est vraie, on montre A et on en déduit B. Dans les raisonnements en français, cela se traduit par le mot "donc" ou un autre mot exprimant la conséquence :

On sait que $A \Longrightarrow B$, or A est vérifiée, **donc** B aussi.

La référence à l'implication $A \Longrightarrow B$ est souvent implicite lorsque cette implication est un résultat bien connu : supposons qu'on ait deux réels x et y dont on sait qu'ils vérifient $x \leq y$. On pourra dire

$x \leq y$ et $\pi \geq 0$, donc $\pi x \leq \pi y$

Le résultat sous-jacent serait ici : $\forall a,b,c \in \mathbb{R}, ((a \leq b \text{ et } c \geq 0) \Longrightarrow ac \leq bc)$, qui est une propriété de base de la relation $\leq$ sur $\mathbb{R}$.

Lorsque les implications des *modus ponens* successifs sont toutes implicites, le raisonnement prend alors la forme d'une suite de conséquences : On a A_1, donc A_2, donc A_3, *etc*. Il est **impératif** de ne pas remplacer le mot "donc" par le symbole $\Longrightarrow$, ce qui serait une faute de logique. En effet, le fait que $A \Longrightarrow B$ ne dit rien *a priori* sur la véracité de A ou de B.

2 Raisonnement par disjonction des cas

On a déjà vu plusieurs fois ce raisonnement dans ce qui précède. Il repose sur le fait suivant : si $A_1 \Rightarrow B$ et $A_2 \Rightarrow B$... et $A_n \Rightarrow B$, alors $(A_1$ ou $A_2 \dots$ ou $A_n) \Rightarrow B$.

Autrement dit, si au cours d'un raisonnement, plusieurs cas se présentent et que l'on montre le résultat voulu dans chacun de ces cas, alors on a montré le résultat.

Remarque 73 Malgré le vocable "disjonction", les différents cas considérés n'ont aucun besoin d'être exclusifs comme le montre l'exemple suivant.

Exemple 74 (*Distributivité de l'intersection par rapport à la réunion.*) Pour montrer que pour trois ensembles quelconques A, B et C, on a $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$, on prend un élément x de $A \cap (B \cup C)$ et on dit que $x \in B$ ou $x \in C$. Dans le premier cas, $x \in A \cap B$ donc $x \in (A \cap B) \cup (A \cap C)$ et de manière analogue pour le second cas. Il se peut cependant que $x \in B$ et $x \in C$ soient vraies simultanément si B et C ont une intersection non vide. Les deux cas ne sont donc pas "disjoints".

3 Raisonnement par contraposée

Il repose sur le fait que

$$(A \Rightarrow B) \iff ((\text{non } B) \Rightarrow (\text{non } A)).$$

On verra plus tard qu'une fonction f est *injective* ssi deux éléments différents de son ensemble de définition D_f ont forcément des images différentes, *i.e.*

$$\forall x, y \in D_f, (x \neq y \Rightarrow f(x) \neq f(y)).$$

En pratique, pour montrer l'injectivité, on prend en général deux éléments quelconques x et y de D_f ayant la même image, et on montre qu'ils sont égaux, *i.e.*

$$\forall x, y \in D_f, (f(x) = f(y) \Rightarrow x = y).$$

4 Raisonnement par l'absurde

Si supposer A et $(\text{non } B)$ entraîne une contradiction, alors $A \Rightarrow B$.

Remarque 75 Il arrive souvent qu'il n'y ait pas de proposition A (on peut alors prendre pour A n'importe quelle proposition vraie) : si $(\text{non } B)$ entraîne une contradiction, alors B est vraie, comme dans les deux exemples classiques suivants, qui remontent à l'antiquité.

Théorème 76 $\sqrt{2} \notin \mathbb{Q}$.

Démonstration: Raisonnons par l'absurde et supposons que $\sqrt{2} \in \mathbb{Q}$. Comme $\sqrt{2} > 0$, il s'écrit donc $\sqrt{2} = \frac{p}{q}$, avec $p, q \in \mathbb{N}^\star$. Quitte à diviser simultanément par 2, éventuellement plusieurs fois, les nombres p et q jusqu'à ce que l'un des deux soit impair, on peut supposer dès le départ p et q non tous deux pairs. En élevant au carré l'égalité $\sqrt{2} = \frac{p}{q}$, puis en multipliant par q^2, on obtient $p^2 = 2q^2$, donc p^2 est pair. Or le carré d'un nombre impair est impair (si $k \in \mathbb{N}$, $(2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$), donc par contraposition, p est pair. Il s'écrit donc $p = 2p'$ avec $p' \in \mathbb{N}^\star$ et l'égalité précédente s'écrit $4p'^2 = 2q^2$, donc $q^2 = 2p'^2$. Par le même raisonnement que ci-dessus, q est pair. Comme p et q sont tous deux pairs, on a une contradiction. □

Théorème 77 *Il existe une infinité de nombres premiers.*

Démonstration: On admet ici le fait intuitif que tout nombre entier supérieur ou égal à 2 admet au moins un diviseur premier (l'étudiant exigeant pourra réfléchir à une vraie preuve de ce fait).

Raisonnons par l'absurde et supposons qu'il n'y ait qu'un nombre fini de nombres premiers $p_1, p_2, \ldots, p_n$. On définit $N = p_1 \cdot p_2 \cdots p_n + 1$. Il est clair que $N \in \mathbb{N}$ et $N \geq 2$. D'après le résultat admis, N admet un diviseur premier p_k, pour un certain $k \in [\![1, n]\!]$. On a alors, comme différence positive de deux entiers, $\frac{1}{p_k} = \frac{N}{p_k} - \frac{p_1 \cdot p_2 \cdots p_n}{p_k} \in \mathbb{N}$, ce qui est impossible car $p_k \geq 2$, p_k étant premier. □

5 Raisonnement par Analyse-Synthèse

On veut trouver tous les objets vérifiant une certaine propriété. On peut le faire par le raisonnement en deux étapes suivant :
Analyse : soit x un tel objet. En faisant certaines déductions, on en déduit que x appartient à un certain ensemble E de solutions possibles.
Synthèse : on vérifie que certains des éléments de E conviennent et d'autres non.

Un cas particulier important est celui où l'on veut prouver l'existence et l'unicité d'un objet vérifiant une certaine propriété.
Analyse : soit x un tel objet. En faisant certaines déductions, on en déduit que $x = x_0$.
Synthèse : on vérifie que x_0 convient.

Voici un exemple très classique de ce raisonnement :

Proposition 78 *Toute fonction définie sur $\mathbb{R}$ se décompose de manière unique comme somme d'une fonction paire et d'une fonction impaire.*

Démonstration: Soit f une fonction définie sur $\mathbb{R}$.
Analyse. **Soient deux fonctions p paire et i impaire définies sur $\mathbb{R}$ telles que $f = p + i$.**

Pour $x \in \mathbb{R}$, on a, en utilisant la parité de p et l'imparité de i, le système d'égalités suivant :

$$\begin{cases} f(x) &= p(x) &+i(x) \\ f(-x) &= p(x) &-i(x) \end{cases}.$$

Par addition d'une part, et soustraction d'autre part, de ces deux égalités, puis division par 2, on obtient

$$\boxed{\forall x \in \mathbb{R}, \begin{cases} p(x) &= \frac{f(x)+f(-x)}{2} \\ i(x) &= \frac{f(x)-f(-x)}{2}. \end{cases}}$$

Ainsi, si la décomposition existe, **elle est unique**.
Synthèse. **On définit alors deux fonctions p et i par les formules suivantes :**

$$\forall x \in \mathbb{R}, \begin{cases} p(x) &= \frac{f(x)+f(-x)}{2} \\ i(x) &= \frac{f(x)-f(-x)}{2}. \end{cases}$$

et on montre que ces deux fonctions conviennent bien, à savoir :

1. p est paire ;
2. i est impaire ;
3. $p+i=f$.

Pour $x\in\mathbb{R}$, on a $p(-x)=\frac{f(-x)+f(-(-x))}{2}=\frac{f(-x)+f(x)}{2}=p(x)$ et $i(-x)=\frac{f(-x)-f(-(-x))}{2}=\frac{f(-x)-f(x)}{2}=-i(x)$, donc $\boxed{p \text{ est paire et } i \text{ est impaire.}}$

Pour $x\in\mathbb{R}$, $p(x)+i(x)=\frac{f(x)+f(-x)}{2}+\frac{f(x)-f(-x)}{2}.=f(x)$, donc $\boxed{p+i=f.}$

On a donc montré **l'existence de la décomposition**.

□

6 Raisonnement par récurrence

Activité 79 *Théorème des deux couleurs :* si on prend n droites dans le plan, on peut colorier avec deux couleurs les régions ainsi définies de telle manière que deux régions contiguës ne soient jamais de la même couleur.

Activité 80 On montre par récurrence que tous les élèves de la classe auront la même note au prochain DS, ou que tout ensemble fini de points du plan est inclus dans une droite. Où est le problème ?

On met ainsi évidence les étapes-clés d'un raisonnement par récurrence (précision de la variable par rapport à laquelle on fait la récurrence (en général n mais pas toujours) et du rang de départ (n_0), assertion de récurrence, initialisation, hérédité avec mise en valeur de l'utilisation de l'hypothèse de récurrence) et la rédaction appropriée (l'assertion de récurrence $P(n)$ ou P_n **ne contient pas de quantification en n** et l'hérédité commence par l'*hypothèse de récurrence* : "Soit $n\geq n_0$ tel que que P_n soit vraie." ou "Supposons que P_n soit vraie pour un certain $n\geq n_0$.").

Exemple 81 On veut montrer que : $\quad\forall n\in\mathbb{N},\ \sum_{k=1}^{n}k^3=\left(\frac{n(n+1)}{2}\right)^2$.

Pour cela on raisonne par récurrence sur n à partir du rang 0. On définit, pour tout $n\in\mathbb{N}$, l'assertion de récurrence

$$\mathcal{P}_n:\quad\sum_{k=1}^{n}k^3=\left(\frac{n(n+1)}{2}\right)^2.$$

Initialisation. L'assertion $\mathcal{P}_0$ est vérifiée :

$$\sum_{k=1}^{0}k^3=0=\left(\frac{0\times(0+1)}{2}\right)^2.$$

Hérédité. Soit $n\in\mathbb{N}$ tel que l'assertion $\mathcal{P}_n$ soit vérifiée. Montrons $\mathcal{P}_{n+1}$:

$$\sum_{k=1}^{n+1}k^3=\sum_{k=1}^{n}k^3+(n+1)^3$$

donc, par l'hypothèse de récurrence $\mathcal{P}_n$,

$$\sum_{k=1}^{n+1}k^3=\left(\frac{n(n+1)}{2}\right)^2+(n+1)^3=\frac{(n+1)^2}{4}\left(n^2+4(n+1)\right)=\frac{(n+1)^2}{4}(n+2)^2=\left(\frac{(n+1)(n+2)}{2}\right)^2$$

et $\underline{\mathcal{P}_{n+1} \text{ est vérifiée}}$.

Par récurrence, on a donc $\boxed{\forall n \in \mathbb{N},\ \sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2.}$

La validité du raisonnement par récurrence repose sur le principe suivant :

Proposition 82 *(Principe de récurrence)*
Soit $P(n)$ une propriété mathématique dépendant d'un entier naturel n.
Si $P(0)$ et $(\forall n \in \mathbb{N},\ (P(n) \Rightarrow P(n+1)))$, alors $(\forall n \in \mathbb{N}, P(n))$.

Démonstration: On démontre ce principe en **admettant** la propriété suivante : *toute partie non vide de $\mathbb{N}$ admet un plus petit élément.*

On suppose alors que $P(0)$ (initialisation) et $(\forall n \in \mathbb{N},\ (P(n) \Rightarrow P(n+1)))$ (hérédité) et on raisonne par l'absurde : s'il existait un entier n tel que $P(n)$ soit fausse, alors l'ensemble $E = \{n \in \mathbb{N} \mid \text{non } P(n)\}$ serait non vide et, comme c'est une partie de $\mathbb{N}$, il admettrait un plus petit élément n_0. Par l'initialisation, $0 \notin E$, donc $n_0 > 0$. Ainsi $n_0 - 1 \in \mathbb{N}$ et, par minimalité de n_0, $n_0 - 1 \notin E$, donc $P(n_0 - 1)$, puis $P((n_0 - 1) + 1)$ par l'hérédité, *i.e.* $P(n_0)$, ce qui contredirait le fait que $n_0 \in E$. □

Remarque 83 En pratique, il arrive souvent que la récurrence commence à un rang n_0 : $P(n_0)$ est vraie et l'hérédité est vérifiée à partir du rang n_0. On en déduit alors que $\forall n \geq n_0, P(n)$.

Exercice 84 Montrer que pour tout entier naturel n, $2^n > n$.

Remarque 85 Il y a des variantes qui découlent facilement du principe de récurrence :
- Récurrence double : Si $P(0)$, $P(1)$ et $(\forall n \geq 2, ((P(n-2) \text{ et } P(n-1)) \Rightarrow P(n)))$, alors $\forall n \in \mathbb{N}, P(n)$.
- Récurrence multiple en généralisant la récurrence double.
- Récurrence forte : si $P(0)$ et $(\forall n \in \mathbb{N}, ((\forall k \in [\![0,n]\!], P(k)) \Rightarrow P(n+1)))$, alors $\forall n \in \mathbb{N}, P(n)$.

Exemple 86 La récurrence forte permet de démontrer que tout nombre entier plus grand que 2 se décompose en produit de facteurs premiers.

Exercice 87 On considère la fameuse suite de Fibonacci définie par $F_0 = 0$ et $F_1 = 1$ et, pour tout $n \geq 2$, $F_n = F_{n-1} + F_{n-2}$.

1. Montrer par récurrence double que pour tout $n \geq 1$, $F_n > 0$. En déduire que la suite est strictement croissante à partir du rang 2.
2. Montrer par récurrence simple que, pour tout $n \in \mathbb{N}$, $0 \leq F_n \leq F_{n+1}$.

Exercice 88

1. Montrer par récurrence forte que tout $n \in \mathbb{N}^\star$ s'écrit sous la forme $n = 2^p(2q+1)$, avec $(p,q) \in \mathbb{N}^2$.
2. Montrer par l'absurde que ce couple est unique.

Exercice 89 Démontrer le principe de récurrence forte à partir du principe de récurrence usuel.

Remarque 90 On peut aussi formuler le principe de récurrence forte ainsi :

Si $(\forall n \in \mathbb{N}, ((\forall k \in [\![0,n-1]\!], P(k)) \Rightarrow P(n)))$, alors $\forall n \in \mathbb{N}, P(n)$.

Où est passée l'initialisation ?

Appendice : Axiomatique de Zermelo-Fraenkel

Les premiers axiomes permettent de régir les opérateurs logiques (c'est ce qu'on appelle le *calcul des propositions*). Il y a plusieurs manières de voir les choses. On en donne une ici : les connecteurs $\neg$ et $\vee$ sont des symboles de base et on "définit" alors les deux connecteurs $\wedge$ et $\Longrightarrow$ comme des abréviations de la façon suivante : pour A et B des énoncés bien formés,

$$[A \wedge B] := [\neg(\neg A \vee \neg B)] \quad \text{et} \quad [A \Longrightarrow B] := [B \vee \neg A].$$

Puis on donne un des jeux d'axiomes logiques possibles. Pour tous les énoncés bien formés A, B et C, les énoncés suivants sont des axiomes :

1. $(A \vee A) \Longrightarrow A$
2. $A \Longrightarrow (A \vee B)$
3. $(A \vee B) \Longrightarrow (B \vee A)$
4. $(A \Longrightarrow B) \Longrightarrow ((A \vee C) \Longrightarrow (B \vee C))$

Viennent ensuite des axiomes régissant le rôle des quantificateurs (en ajoutant cela au calcul des propositions, on accède ainsi à la *logique du premier ordre*). Il est d'usage de noter $A(x)$ un énoncé A pour spécifier qu'on s'intéresse aux occurrences libres de la variable x dans A, puis de noter $A(t)$ l'énoncé obtenu en remplaçant chaque occurrence libre de x dans A par le terme t. On peut alors énoncer les deux schémas d'axiomes régissant les quantificateurs. Pour toute variable x et tous énoncés bien formés A et $B(x)$, tels que A ne contienne aucune occurrence libre de x, et tout terme t, les énoncés suivants sont des axiomes :

5. $(\forall x, (A \Longrightarrow B(x))) \Longrightarrow (A \Longrightarrow (\forall x, B(x)))$
6. $(\forall x, B(x)) \Longrightarrow B(t)$, lorsque x n'a pas d'occurrence libre dans $B(x)$ qui soit dans le champ d'une quantification $\forall t$.

Un axiome et un schéma d'axiomes permettent de régir l'égalité :

7. (Réflexivité) $\forall x, x = x$
8. (Schéma d'axiomes de substitution)

$$\forall a_1, \forall a_2, \ldots, \forall a_p, \forall x, \forall y, (x = y \Longrightarrow (P(x, a_1, \ldots, a_p) \Longrightarrow P(y, a_1, \ldots, a_p)))$$

où $P(x, a_1, \ldots, a_p)$ est un énoncé ne contenant pas d'occurrence libre de variables autres que $x, a_1, \ldots, a_p$.

Enfin, les axiomes concernant la théorie des ensembles proprement dite. On définit l'*inclusion* par $[a \subset b] := [\forall x, (x \in a \Longrightarrow x \in b)]$ et on pose :

9. (Extensionnalité) $\forall a, \forall b, (((a \subset b) \wedge (b \subset a)) \Longrightarrow (a = b))$
10. (Axiome de la paire) $\forall a, \forall b, \exists c, \forall x, ((x \in c) \iff ((x = a) \vee (x = b)))$
11. (Axiome de la réunion) $\forall a, \exists b, \forall c, ((c \in b) \iff (\exists d, ((c \in d) \wedge (d \in a))))$
12. (Axiome de l'ensemble des parties) $\forall e, \exists p, \forall a, ((a \in p) \iff (a \subset e))$

Ces axiomes s'interprètent ainsi : deux ensembles sont égaux si et seulement s'ils ont les mêmes éléments ; quels que soient deux objets a et b de la théorie des ensembles (en fait des ensembles !), éventuellement égaux, il existe un ensemble, alors noté $\{a, b\}$, formé de ces seuls éléments ; on peut obtenir un ensemble, noté $\bigcup_a$, en réunissant tous les ensembles appartenant à un ensemble a donné et, pour tout ensemble e, il existe un autre ensemble $\mathcal{P}(e)$ dont les éléments sont exactement les sous-ensembles (ou parties) du premier ensemble.

Pour construire l'ensemble des entiers naturels, on introduit :

13. (Axiome de l'infini) $\exists a, ((\exists y, ((\forall z, z \notin y) \wedge (y \in a))) \wedge (\forall x, ((x \in a) \Longrightarrow (x \cup \{x\} \in a))))$

On note alors $\emptyset$ l'ensemble y et $0 := \emptyset$, $1 := \{\emptyset\}$, $2 := \{\emptyset, \{\emptyset\}\}$, *etc*.

Le prochain schéma d'axiomes permet de *sélectionner* dans un ensemble a tous les éléments x vérifiant une propriété mathématique donnée $P(x)$ et d'en faire un ensemble noté $\{x \in a \mid P(x)\}$.

14. (Schéma d'axiomes de compréhension)

$$\forall a_1, \forall a_2, \ldots, \forall a_p, \forall a, \exists b, \forall x, ((x \in b) \iff ((x \in a) \wedge P(x, a_1, \ldots, a_p)))$$

où $P(x, a_1, \ldots, a_p)$ est un énoncé ne contenant pas d'occurrence libre de variables autres que $x, a_1, \ldots, a_p$.

Tous ces axiomes forment la théorie de Zermelo, si l'on exclut l'axiome du choix de cette dernière. Pour accéder à ZF, on rajoute un schéma d'axiomes et un axiome plus techniques :

15. (Schéma d'axiomes de remplacement)
$\forall a_1, \forall a_2, \ldots, \forall a_p,$
$((\forall x, \forall y, \forall y', (P(x, y, a_1, \ldots, a_p) \wedge P(x, y', a_1, \ldots, a_p)) \Rightarrow (y = y'))$
$\Rightarrow (\forall a, \exists b, \forall y, ((y \in b) \iff (\exists x, ((x \in a) \wedge P(x, y, a_1, \ldots, a_p))))))$
où $P(x, y, a_1, \ldots, a_p)$ est un énoncé ne contenant pas d'occurrence libre de variables autres que $x, y, a_1, \ldots, a_p$.
16. (Axiome de fondation, optionnel) $\forall x, ((x \neq \emptyset) \Longrightarrow (\exists y, ((y \in x) \wedge (y \cap x = \emptyset))))$

A la théorie ZF, on peut rajouter le fameux

17. (Axiome du choix) : Étant donné un ensemble e d'ensembles non vides, il existe une *fonction de choix* f définie sur e permettant de choisir un élément dans chaque élément de e : $\forall x \in e, f(x) \in x$.

qui permet de démontrer l'existence de beaucoup d'objets mathématiques de manière non constructive, ce qui rend certains mathématiciens circonspects quant à son emploi. Il nécessite d'avoir défini proprement la notion de "fonction" (en fait d'*application*).