Université Paris 1 Panthéon-Sorbonne

Licence MIASHS 1

Cours de Fondement des Mathématiques

Antoine Mandel

Année Universitaire 2014-2015

Syllabus

Cours: Fondement des Mathématiques.

Enseignant: Antoine Mandel.

Email antoine.mandel@univ-paris1.fr

Objectif du cours: Découvrir les bases des mathématiques contemporaines que sont la logique et la théorie des ensembles. Apprendre à utiliser les objets mathématiques de base et à rédiger des énoncés et des preuves mathématiques dans les règles de l'art.

Méthode de travail: Les objets mathématiques de base sont introduits en cours par des définitions (qu'on veut les plus générales possibles et qui sont donc souvent très abstraites). Les propriétés structurelles de ces objets et les relations qu'ils entretiennent sont ensuite établies dans le cadre de propositions, lemmes, théorèmes, corollaires qui se déduisent des définitions suivant les règles de la logique. La compréhension véritable de ces objets mathématiques se fait cependant par la pratique: c'est en les manipulant qu'on vérifie le bien-fondé de leur définition et qu'on comprend véritablement leur nature et leur utilité. Cet apprentissage pratique commence en cours par l'étude de certains exemples mais se fait principalement en TD en résolvant les problèmes proposés. Il s'agit d'acquérir de l'expérience: le seul moyen d'y parvenir est de résoudre effectivement les exercices par vous-même. Se contenter de suivre la correction de votre chargé de TD revient à essayer d'apprendre à nager en regardant les poissons.

Assiduité: La présence aux travaux dirigés est obligatoire. Un étudiant inscrit en contrôle continu absent à plus de trois séances sera considéré comme défaillant (et ne validera donc ni la matière, ni le semestre ni l'année). La présence en cours n'est pas contrôlée mais suivre le cours activement (c'est à dire en essayant de comprendre les démonstrations lorsqu'elles sont faites au tableau) est le moyen le plus efficace pour apprendre les mathématiques.

Notation: Excepté pour les étudiants inscrits en contrôle terminal, la note finale à la matière est la moyennes des notes de contrôle continu et d'examen final. Pour le contrôle continu il y aura deux interrogations en amphithéâtre et une série de micro-interrogations en TD. Chacune comptera pour un tiers de la note.

Contenu du cours:

1. **Logique.**
   Propositions. Notion de connecteur logique (négation, et, ou, implication). Prédicat. Quantificateurs logiques. Implication, condition nécessaire, condition suffisante, équivalence, contraposition, réciproque. Notion de contre- exemple.

2. **Ensembles.**
   Notions d'ensemble et opérations sur les ensembles. Sous-ensembles, ensemble des parties d'un ensemble. Produit cartésien d'ensembles. Familles indicées d'ensemble et opérations.

3. **Fonctions.**
   Injections, surjections, bijections, fonctions réciproques. Image directe et réciproque d'un ensemble par une fonction. Graphe d'une fonction.

4. **Relations.**
   Relations binaires. Relation d'équivalence. Relation d'ordre. Majorant, minorant, plus grand élément, plus petit élément. Bornes supérieure et inférieure.

5. **Ensemble de nombres.**
   Rappel sur les nombres entiers, démonstration par récurrence. Nombres rationnels. Nombres réels. Nombres complexes. Les notions de groupes, anneaux, corps ne seront pas traités en cours mais pourront faire l'objet d'exercices.

6. **Polynômes.**
   Polynômes irréductibles sur R. Décomposition d'un polynôme dans R[X] et C[X]. Enoncé du théorème fondamental de l'algèbre.

7. **Exemple d'élaboration d'une théorie mathématique : des systèmes d'équations linéaires aux espaces vectoriels.**
   Système homogène, système de Cramer. Résolution d'un système triangulaire. Résolution d'un système par la méthode du pivot de Gauss.

Bibliographie:

- Dixmier, J. *Cours de mathématiques du premier cycle, première année*, Dunod. Chapitres 1, 5 et 9.

1 Logique

1.1 Propositions

En mathématiques, on s'intéresse à des énoncés spécifiques, les propositions, auxquels on peut appliquer les règles du raisonnement logique. On utilisera la définition naïve suivante:

Definition 1 *Une proposition est un énoncé dont on peut déterminer si il est vrai ou faux.*

Exemple 1 *Ci-dessous quelques énoncés qui sont des propositions:*

- *"2+2=4" (vrai)*
- *"La somme des angles d'un triangle vaut 200°" (faux)*
- *"$\forall x \in \mathbb{R},\ x^2 \geq 0$" (vrai)*
- *"$\forall x \in \mathbb{C},\ x^2 \geq 0$" (faux)*
- *"Toutes les fonctions continues sont dérivables" (faux)*
- *"L'ours est un mammifère " (vrai)*
- *"Paris est la capitale de la Pologne" (faux)*

Exemple 2 *Ci-dessous quelques énoncés qui ne sont pas des propositions:*

- *"Quelle heure est-il ?" (une question n'est ni vraie ni fausse)*
- *" Cette phrase est fausse" (on ne peut détermine si cet énoncé est vrai ou faux)*
- *Dans un village où le barbier rase tous les hommes du village qui ne se rasent pas eux-mêmes, et seulement ceux-là, l'énoncé "le barbier se rase lui-même" n'est ni vrai ni faux.*
- *"$\forall x \in \mathbb{R},\ x^2$" (bien qu'écrit avec des formules mathématiques, cet énoncé n'a pas de sens.)*

Généralement une théorie mathématique se construit autour d'un certain nombre de propositions simples qu'on suppose vraies (les axiomes) et à partir desquels on essaie de déduire d'autres énoncés plus complexes. Ces énoncés complexes se construisent à l'aide de connecteurs logiques. En voici quelques exemples importants:

Definition 2 *Etant donnés des propositions p et q :*

- *La proposition $\neg p$, appelée négation de p ou "non p " est vraie si et seulement si p est fausse.*
- *La proposition $p \wedge q$, appelée conjonction de p et q ou "p et q", est vraie si et seulement si p et q sont toutes les deux vraies.*
- *La proposition $p \vee q$ appelée disjonction de p et q ou "p ou q", est vraie si et seulement si p est vraie ou q est vraie.*
- *La proposition $p \Rightarrow q$, appelée implication de q par p ou "p implique q" est la proposition $\neg p \vee q$ qui est vraie sauf si p est vraie et q fausse.*
- *La proposition $p \Leftrightarrow q$, appelée équivalence de p et q est vraie si et seulement si $p \Rightarrow q$ et $q \Rightarrow p$ sont vraies.*

Definition 3 *Quand "$p \Rightarrow q$'"est vraie, p est dite être une condition suffisante pour q et q une condition nécessaire pour p.*

De manière plus générale, un connecteur logique $n-$aire forme une nouvelle proposition à partir de n propositions simples. Pour le définir formellement, on a souvent recours à une table de vérité.

Definition 4 *La table de vérité du connecteur logique n-aire $\mathcal{C}$ est un tableau à $n+1$ colonnes et 2^n lignes qu'on construit en indiquant dans les n premières colonnes les 2^n combinaisons possibles de valeurs de vérité pour les n propositions initiales $p_1, \cdots, p_n$ et dans la $n+1$ème colonne la valeur de la proposition $\mathcal{C}(p_1, \cdots, p_n)$.*

Exemple 3 *Tables de vérité (on note 1 pour vrai et 0 pour faux)*

- *Négation:*

p	$\neg p$
0	1
1	0

- *Conjonction:*

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

- *Disjonction:*

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

- *Implication:*

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

- *Equivalence:*

p	q	$p \Leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Remarque 1 *La définition de l'implication peut sembler contre-intuitive puisque "une proposition fausse implique n'importe quoi". POur comprendre l'intérêt de cette définition, il peut être utile de remarquer que:*

- *On utilise l'implication pour déduire une proposition d'une autre, i.e. si p est vraie et $p \Rightarrow q$ vraie alors q est vraie. Rajouter d'autres contraintes modifierait le sens de l'implication.*
- *$p \Rightarrow q$ est fausse si p est vraie et q fausse, i.e. $\neg(p \Rightarrow q) \Leftrightarrow p \wedge \neg q$*

Exemple 4 *On peut ensuite composer ces tables de vérité pour établir les valeurs de vérité de proposition plus complexes:*

p	q	r	$p \wedge q$	$(p \wedge q) \vee r$
0	0	0	0	0
0	0	1	0	1
0	1	0	0	0
0	1	1	0	1
1	0	0	0	0
1	0	1	0	1
1	1	0	1	1
1	1	1	1	1

p	q	r	$p \vee r$	$q \vee r$	$(p \vee r) \wedge (q \vee r)$
0	0	0	0	0	0
0	0	1	1	1	1
0	1	0	0	1	0
0	1	1	1	1	1
1	0	0	1	0	0
1	0	1	1	1	1
1	1	0	1	1	1
1	1	1	1	1	1

Les tables de vérité peuvent notamment servir à démontrer que certaines propositions sont des tautologies, i.e elles sont toujours vraies (l'usage du mot tautologie en mathématiques est donc différent de celui du langage courant). Notamment, on obtient ainsi les règles de distributivité et d'associativité pour les opérateurs logiques:

Propriété 1 *Les propositions suivantes sont des tautologies:*

1. $(p \wedge q) \vee r \Leftrightarrow (p \vee r) \wedge (q \vee r)$
2. $(p \vee q) \wedge r \Leftrightarrow (p \wedge r) \vee (q \wedge r)$
3. $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$
4. $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$
5. $\neg(p \Rightarrow q) \Leftrightarrow p \wedge \neg q$
6. $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$
7. $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$

Démonstration: *On vient de prouver* 1 *en montrant que* $(p \wedge q) \vee r$ *et* $(p \vee r) \wedge (q \vee r)$ *avaient les mêmes tables de vérité. Les autres propriétés seront démontrées en TD.*

Les principes du raisonnement mathématiques se formalisent également en montrant que ces principes sont vraies indépendamment du contexte.

Théorème 1 *Quelles que soient les propositions* p, q, r*, les propositions suivantes sont des tautologies:*

- *Modus ponens:* $[p \wedge (p \Rightarrow q)] \Rightarrow q$
- *Raisonnement par contraposée:* $[p \Rightarrow q] \Leftrightarrow [\neg q \Rightarrow \neg p]$
- *Raisonnement par l'absurde:* $[(p \Rightarrow q) \wedge \neg q] \Rightarrow \neg p$
- *Raisonnement par disjonction des cas:* $[(p \vee q) \wedge (p \Rightarrow r) \wedge (q \Rightarrow r)] \Rightarrow r$
- *Transitivité de l'implication:* $[(p \Rightarrow r) \wedge (q \Rightarrow r)] \Rightarrow [p \Rightarrow r]$
- *Raisonnement par double implication:* $[(p \Rightarrow q) \wedge (q \Rightarrow p)] \Leftrightarrow [p \Leftrightarrow q]$

Démonstration: *voir TD.*

Remarque 2 *Ces propriétés s'utilisent en pratique comme suit:*

- *Modus ponens: ce principe est à la base du raisonnement mathématique. On se donne une hypothèse p qu'on suppose vraie et pour en déduire qu'une conclusion q est vraie, on montre $p \Rightarrow q$.*
- *Raisonnement par contraposée: pour montrer que $p \Rightarrow q$, il suffit de montrer $\neg q \Rightarrow \neg p$.*
- *Raisonnement par l'absurde: pour montrer que p est fausse, on suppose p vraie et on montre que cela conduit a une contradiction $(q \wedge \neg q)$.*
- *Raisonnement par disjonction des cas: pour montrer que r est vraie lorsqu'on sait que soit p soit q est vraie, il suffit de montrer que p implique r et que q implique r*
- *Transitivité de l'implication: pour montrer que p implique r, il suffit de montrer que p implique q, et que q implique r.*
- *Raisonnement par double implication: pour montrer que deux propositions p et q sont équivalentes, il suffit de montrer que p implique q et que q implique p. Plus généralement, pour montrer que p, q et r sont équivalentes (i.e $p \Leftrightarrow q \Leftrightarrow r$), il suffit de montrer que p implique q, que q implique r, et que r implique p*

Remarque 3 *Ne pas confondre la contraposée $\neg q \Rightarrow \neg p$ et la réciproque $q \Rightarrow p$ de la proposition $p \Rightarrow q$. La contraposée est vraie si et seulement si la proposition initiale l'est, la réciproque peut être vraie ou fausse indépendamment de la valeur de vérité de la proposition initiale.*

1.2 Une approche un peu moins naïve

On peut définir plus formellement, la logique des propositions comme étant constitué de trois éléments: un alphabet, une syntaxe et une sémantique.

Definition 5 *L'alphabet est la liste des symboles utilise, il est constitué:*

- *de symboles/lettres représentant les propositions considérées comme données:* $p, q, A, B, \cdots$
- *de symboles représentant les connecteurs logiques:* $\vee,\ \wedge,\ ,\neg,\ ,\Rightarrow, \cdots$
- *de séparateurs : parenthèses* $()$*, accolades* $\{\}$*,* $\cdots$

Definition 6 *La syntaxe est l'ensemble des règles définissant quelles sont les formules donnant des propositions valides:*

- *Tous les propositions sont des formules valides.*
- *Si* ϕ *est une formule valide, alors* $\neg\phi$ *est une formule valide*
- *Si* ϕ *et* ψ *sont des formules valides, alors* $(\phi \vee \psi)$ $(\phi \wedge \psi)$ $(phi \Rightarrow \psi)$ *sont des formules valides*

N.B: on peut définir d'autres même connecteurs logiques mais cela est redondant.

Definition 7 *La sémantique donne un sens au formule du langage. Dans le cadre de la logique des propositions, elle est définie par:*

- *La valeur de vérité des propositions de base du langage.*
- *L'algorithme de calcul de la valeur de vérité des propositions (i.e. les tables de vérité).*

1.3 Quantificateurs universels et existentiels

On s'intéresse maintenant aux énoncés dont la valeur de vérité dépend d'une ou plusieurs variables.

Definition 8 *Un prédicat (unaire) p sur un ensemble A est une expression qui associe à chaque élément x de A une proposition $p(x)$.*

Exemple 5 *Exemples de prédicats:*

- $p(x)$: "$x \geq 2$" *est un prédicat sur* $\mathbb{R}$.
- $q(n)$: *"n est un nombre premier" est un prédicat sur* $\mathbb{N}$.

On peut de manière similaire définir un prédicat portant sur deux variables

Definition 9 (Prédicat binaire) *Etant donné deux ensembles A et B, un prédicat p sur $A \times B$ est une expression qui associe à chaque paire d'éléments $(a, b) \in A \times B$, une proposition $p(a, b)$.*

Exemple 6 *Exemples de prédicats binaires:*

- $p(x, y)$: "$x = y$" *est un prédicat binaire sur* $\mathbb{R}$.
- $q(n, m)$: *"m divise n" est un prédicat sur* $\mathbb{N} \times \mathbb{N}$.

Remarque 4 *On peut de manière similaire définir des prédicats portant sur un nombre arbitraire de variables. On appelé prédicat n-aire un prédicat portant sur n variables. Plus précisément un prédicat n-aire sur $A_1 \times A_2 \times \cdots \times A_n$, est une expression qui associe à chaque élément $(x_1, \cdots, x_n)$ de $A_1 \times A_2 \times \cdots \times A_n$, une proposition $p(x_1, \cdots, x_n)$.*

Deux propositions qu'on peut former à partir d'un prédicat sont d'un intérêt particulier.

Definition 10 (Quantification universelle) *Etant donné le prédicat $p(x)$ sur A, l'énoncé "$\forall x \in A,\ p(x)$", est la* ***proposition*** *qui est vraie si et seulement si $p(x)$ est vraie pour tout élément x de A.*

Remarque 5 *Quelle démarche adopter face à un quantificateur universel ? Pour montrer qu'une proposition de la forme "$\forall x \in A,\ p(x)$" est vraie, vous devez considérer un élément quelconque de A et prouver que $p(x)$ est vraie. N.B: Par quelconque, on entend un élément dont la seule propriété qu'on utilise est l'appartenance à A.*

Exemple 7 *Exemples de propositions formées par quantification universelle:*

- $\forall x \in \mathbb{R},\ x^2 \geq 0$ *est une proposition vraie.*
- $\forall x \in \mathbb{R},\ x \geq 0$ *est fausse*

Definition 11 (Quantification existentielle) *Etant donné le prédicat $p(x)$ sur A, l'énoncé "$\exists x \in A,\ p(x)$", est la* ***proposition*** *qui est vraie si et seulement si $p(x)$ est vraie pour au moins un élément x de A.*

Remarque 6 *Quelle démarche adopter face à un quantificateur existentiel ? Pour montrer qu'une proposition de la forme "$\exists x \in A,\ p(x)$" est vraie, il suffit d'exhiber un élément particulier de A pour lequel $p(x)$ est vraie.*

Exemple 8 *Exemples de propositions formées par quantification existentielle:*

- "$\exists x \in \mathbb{R}\ x^2 > 1000$" *est une proposition vraie.*
- "$\exists x \in \mathbb{N}\ x < 0$" *est une proposition fausse.*

Definition 12 (Négation des énoncés quantifiés) *La négation des propositions quantifiés se fait selon les règles suivantes:*

1. $\neg(\forall x \in A\ p(x)) \Leftrightarrow \exists x \in A\ \neg p(x)$
2. $\neg(\exists x \in A\ p(x)) \Leftrightarrow \forall x \in A\ \neg p(x)$

Remarque 7 *Cette règle est notamment utile pour prouver que l'énoncé "$\forall x \in A\ p(x)$" est faux: il suffit de prouver que "$\exists x \in A\ \neg p(x)$", c'est à dire un élément a de A tel que $p(a)$ soit faux. C'est ce qu'on appelle un contre-exemple.*

Exemple 9 *On a:*

$$\neg(\forall x \in \mathbb{R}\ x^2 + x + 1 \geq 0) \Leftrightarrow \exists x \in \mathbb{R}\ x^2 + x + 1 < 0$$

1.4 Quantification des prédicats complexes

A partir de prédicats complexes, on peur former des prédicats plus simples et des propositions par quantification. Par exemple, étant donné un prédicat binaire $p(x, y)$ sur $A \times B$, et Q_A et Q_B des quantificateurs ($\forall$ ou $\exists$), on a que:

- un énoncé de la forme:

$$Q_A \ x \in A \ p(x, y)$$

  est un prédicat unaire sur B (on peut le noter $r(y)$).

- Un énoncé de la forme

$$Q_B \ y \in B \ p(x, y)$$

  est un prédicat unaire sur A (on peut le noter $s(x)$).

- Un énoncé de la forme

$$Q_A \ x \in A \ \ Q_B \ y \in B \ p(x, y)$$

  ou

$$Q_B \ y \in B \ Q_A \ x \in A \ p(x, y)$$

  est une proposition.

Plus généralement, étant donné un prédicat $p(x_1, \cdots, x_n)$ sur $A_1 \times A_2 \times \cdots \times A_n$, et $Q_1, \cdots, Q_n$ des quantificateurs, une expression de la forme

$$Q_1 x_1 \in A_1, \ Q_2 x_2 \in A_2, \cdots, \ Q_n x_n \in A_n, \ p(x_1, x_2, \cdots, x_n)$$

est une proposition.

Remarque 8 *Dans un énoncé complexe de la forme*

$$Q_1 x_1 \in A_1, \ Q_2 x_2 \in A_2, \cdots, \ Q_m x_m \in A_m, \ p(x_1, x_2, \cdots, x_n)$$

les variables quantifiés $x_1, \cdots, x_m$ sont dites liées, les autres dites libres.

Exemple 10 *Exemples d'énoncés formés par quantification de prédicats:*

- $p(y) = \forall x \in \mathbb{R} \ x \geq y$ *est un prédicat sur* $\mathbb{R}$ *(la variable libre est y).*
- $q(z) = \forall x \in \mathbb{R} \ \exists y \in \mathbb{R} \ x = y + z$ *est un prédicat sur* $\mathbb{R}$.

- $r = \exists y \in \mathbb{R}\ \forall x \in \mathbb{R}\ x \geq y$ *est une proposition qui est fausse (car il n'existe pas de réel plus petit que tous les autres).*

- $s = \forall x \in \mathbb{R}\ \exists y \in \mathbb{R}\ x \geq y$ *est une proposition qui est vraie (car pour tout réel, il existe un réel plus petit).*

Les exemples précédents montrent que les propositions "$\exists y \in B\, \forall x \in A\, p(x,y)$" et "$\forall x \in A\ \exists y \in B\ \ p(x,y)$" ne sont pas équivalentes en général. Ainsi, dans un énoncé quantifié **l'ordre des quantificateurs importe.** Plus précisément, l'énoncé "$\exists y \in B\ \forall x \in A\ p(x,y)$" est plus fort que l'énoncé "$\forall x \in A\ \exists y \in B\ \ p(x,y)$" puisque le premier énonce l'existence d'un y qui vérifie la propriété $p(x,y)$ pour tous les x tandis que le second dit que pour chaque x on peut trouver un y vérifiant la propriété $p(x,y)$. Dans le premier cas, on doit pouvoir choisir y indépendamment de x, dans le second cas un y différent peut-être choisi pour chaque x. Formellement, on a :

Théorème 2 *La propriété suivante est toujours vraie:*

$$\exists y \in B,\ \forall x \in A,\ p(x,y)\ \Rightarrow \forall x \in A, \exists y \in B,\ p(x,y)$$

Démonstration: *On suppose* $\exists y \in B,\ \forall x \in A,\ p(x,y)$. *On note plus précisément* $\overline{y}$ *l'élément de* B *tel que* $\forall x \in A,\ p(x,\overline{y})$.

On cherche ensuite à montrer que $\forall x \in A, \exists y \in B,\ p(x,y)$. *Soit alors un élément* x *de* A *choisi arbitrairement. D'après ce qui précède, on sait qu'il existe* $y = \overline{y}$ *tel que* $p(x,\overline{y})$ *est vraie. On a donc bien* $\forall x \in A \exists y \in B,\ p(x,y)$.

Remarque 9 *On peut remarkr que lorsque les quantificateurs sont identiques, l'ordre n'importe pas. On a notamment:*

$$\forall y \in B, \forall x \in A, p(x,y) \Leftrightarrow \forall x \in A,\ \forall y \in B, p(x,y)$$
$$\exists y \in B, \exists x \in A,\ \ p(x,y) \Leftrightarrow \exists x \in A,\ \exists y \in B,\ p(x,y)$$

Remarque 10 (Négation des énoncés complexes) *La négation des propositions construites à partir de prédicats complexes se fait par application successive de la règle vue plus haut pour les prédicats unaires. On obtient ainsi:*

$$\neg[\forall x \in A, \exists y \in B, p(x,y)] \Leftrightarrow \exists x \in A, \neg[\exists y \in B, p(x,y)]$$

puis

$$\neg[\forall x \in A, \exists y \in B, p(x,y)] \Leftrightarrow \exists x \in A, \forall y \in B, \neg p(x,y).$$

En pratique, pour obtenir la négation d'un énoncé quantifié $Q_1x_1 \in A_1,\ Q_2x_2 \in A_2, \cdots,\ Q_mx_m \in A_m,\ p(x_1, x_2, \cdots, x_n)$, *on inverse tous les quantificateurs (i.e on remplace* $\forall$ *par* $\exists$ *et* $\exists$ *par* $\forall$*) et on remplace le prédicat* $p(x_1, x_2, \cdots, x_n)$ *par sa négation* $\neg p(x_1, x_2, \cdots, x_n)$.

Remarque 11 *La compréhension d'énoncés quantifiés complexes est l'une des principales compétences que vous devez acquérir pour réussir vos études en mathématiques. Voici quelques exemples d'énoncés importants de ce type:*

- *Tout sous-ensemble de* $\mathbb{N}$ *a un plus petit élément:*

$$\forall A \subset \mathbb{N},\ \exists a \in A,\ \forall x \in A,\ x \geq a.$$

- *La suite numérique* $(u_n)_{n\in\mathbb{N}}$ *converge vers* ℓ :

$$\forall \epsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, |u_n - \ell| < \epsilon$$

- *L'addition des entiers est associative:*

$$\forall a \in \mathbb{N}, \forall b \in \mathbb{N}, \forall c \in \mathbb{N}, (a + b) + c = a + (b + c)$$

2 Théorie naïve des ensembles

2.1 Ensembles et sous-ensembles

Definition 13 (Définition naïve d'un ensemble) *Un ensemble est une collection bien-définie d'objets. Ces objets sont appelés les éléments de l'ensemble. On note $a \in A$, le fait que a soit un élément de A.*

Des exemples importants d'ensembles sont les ensembles usuels de nombres, notamment:

- $\mathbb{N} = \{0, 1, 2, ..., n, ...\}$, l'ensemble des entiers naturels.
- $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, ..., n, -n, ...\}$, l'ensemble des entiers.
- $\mathbb{Q}$, l'ensemble des nombres rationnels.
- $\mathbb{R}$, l'ensemble des nombres réels.

Ces ensembles de nombres seront étudiés plus en détail à la section 5 mais on considère leur existence comme acquise. Un autre ensemble important est l'ensemble qui ne contient aucun élément, appelé l'ensemble vide et noté $\emptyset$.

On peut définir un ensemble de deux façons:

- Par extension ou de manière extensive, c'est-à-dire en listant tous ses éléments.
- Par compréhension ou de manière compréhensive, en caractérisant les éléments de l'ensemble par une propriété.

Exemple 11 *Ensembles définis de manière extensive:*

- $\{1\}$
- $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$
- $\{a, b, c\}$

Exemple 12 *Ensembles définis de manière compréhensive:*

- $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$
- $\{n \in \mathbb{N} \mid n \text{ est pair}\} = \{n \in \mathbb{N} \mid \exists p \in \mathbb{N}, n = 2p\}$
- *Ensemble des étudiants de Paris 1 dont le nom commence par Z.*

La définition sous forme extensive a un champ d'application limité, en particulier elle ne permet de définir que des ensembles finis, mais elle ne prête à aucune ambiguïté. La définition sous forme compréhensive est nécessaire pour définir des ensembles complexes, en particulier les ensembles infinis comme $\mathbb{R}$, mais elle peut donner lieu à des paradoxes. Par exemple, si on considère la propriété $p(x)$:="x est un nombre entier pouvant se définir par une phrase française de moins de cent caractères" et l'ensemble A des nombres entiers satisfaisant $p(x)$. Comme il y a un nombre fini de phrases de moins de cent caractères, l'ensemble A a un nombre fini d'éléments et donc un plus grand élément. Soit alors N le plus petit entier n'appartenant pas à A. N n'est pas dans A pourtant on vient de le définir par une phrase de moins de cent caractères, il est donc dans A. On aboutit donc à une contradiction.

C'est pour exclure ce genre de paradoxes (le précédent est appelé paradoxe de Berry), qu'on a précisé dans la définition 13 qu'un ensemble était une collection **bien définie**. Un sens précis à cette notion de "collection bien définie" peut être donnée dans le cadre de la théorie axiomatique des ensembles de Zermelo-Fraenkel (voir ci)dessous). Il nous faut néanmoins mentionner un axiome clé de cette théorie qui énonce que deux ensembles sont égaux si et seulement si ils ont les mêmes éléments.

Axiome 1 (d'extensionnalité) *Deux ensembles sont égaux si ils ont les mêmes élément. Soit:*

$$\forall A\ \forall B\ [(\forall x\ x \in A \Leftrightarrow x \in B) \Rightarrow A = B]$$

Remarque 12 *Notamment, lorsqu'un ensemble est donné sous forme extensive, sa définition n'eut pas modifiée si un même élément est mentionné plusieurs fois. Par exemple, on a:*

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

La relation fondamentale entre ensemble est l'inclusion:

Definition 14 *Un ensemble A est un sous-ensemble d'un ensemble B si tout élément de A est un élément de B. On dit alors que A est inclus dans B et on note $A \subset B$.*

Remarque 13 *Ainsi, on a $A = B$ si et seulement si $A \subset B$ et $B \subset A$.*

Exemple 13 *Exemple de sous-ensembles:*

- *l'ensemble vide $\emptyset$ est un sous-ensemble de chaque ensemble.*

- $\emptyset \subset \{0\}$
- $\{0\} \subset \{0,1\}$
- $\{0,1\} \subset \mathbb{N}$
- $\mathbb{N} \subset \mathbb{R}$

Propriété 2 *La relation d'inclusion est transitive, i.e:*

$$[(A \subset B) \wedge (B \subset C)] \Rightarrow A \subset C$$

Démonstration: *On veut montrer que* $\forall x x \in A \Rightarrow x \in C$. *Soit donc* $x \in A$. *Comme* $A \subset B$, *on a* $x \in B$. *Comme* $B \subset C$, *on a alors* $x \in C$.

2.2 Opérations sur ensembles

Definition 15 *Il existe deux opérations binaires fondamentales sur les ensembles:*

- *L'intersection de* A *et* B *défini par:*

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

- *L' union de* A *et* B *défini par:*

$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

Exemple 14 *Exemples d'opérations sur les ensembles*

- $\{1,2\} \cup \{3\} = \{1,2,3\}$
- $\{1,2\} \cup \mathbb{N} = \mathbb{N}$
- $\{1,2\} \cup \emptyset = \{1,2\}$
- $\{1,2\} \cap \{1\} = \{1\}$
- $\mathbb{N} \cap \mathbb{R} = \mathbb{N}$
- $\{1,2\} \cap \{3,4\} = \emptyset$

Remarque 14 *Lorsque* $A \cap B = \emptyset$, *les ensembles* A *et* B *sont dits disjoints.*

Definition 16 *Le complémentaire d'un sous-ensemble A de U est l'ensemble des éléments de U n'appartenant pas à A :*

$$A^c := \{x \in U \mid x \notin A\}$$

N.B: U est souvent donné de manière implicite lorsqu'il est fait référence au complémentaire d'un sous-ensemble de U.

On a les propriétés suivantes pour les opérations ensemblistes:

Propriété 3 *Soient A et B des sous-ensembles d'un ensemble U, on a*

- *Idempotence:*

$$A \cup A = A \qquad\qquad A \cap A = A$$

- *Associativité:*

$$(A \cup B) \cup C = A \cup (B \cup C) \qquad\qquad (A \cap B) \cap C = A \cap (B \cap C)$$

- *Commutativité:*

$$A \cup B = B \cup A \qquad\qquad A \cap B = B \cap A$$

- *Distributivité*

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \qquad\qquad A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

- *Elément neutre*

$$A \cup \emptyset = A \qquad\qquad A \cap U = A$$

- *Elément absorbant*

$$A \cup U = U \qquad\qquad A \cap \emptyset = \emptyset$$

- *Lois du complémentaire*

$$A \cup A^c = U \qquad\qquad A \cap A^c = \emptyset$$
$$(A^c)^c = A \qquad\qquad U^c = \emptyset$$

- *Lois de Morgan*

$$(A \cup B)^c = A^c \cap B^c \qquad\qquad (A \cap B)^c = A^c \cup B^c$$

Démonstration: *voir TD*

Remarque 15 *Deux autres opérations utiles, mais moins usuelles, sur les ensembles sont la différence:*

$$A \setminus B = \{x \mid x \in A \wedge x \notin B\}.$$

et la différence symétrique:

$$A \Delta B = (A \cup B) \setminus (A \cap B).$$

2.3 Produit cartésien d'ensembles

On s'intéressera fréquemment aux ensembles formés par des listes ordonnées d'éléments. Formellement, on a:

Definition 17 *Une paire (a, b) d'éléments $a \in A$ et $b \in B$ consiste en deux objets (éventuellement identiques) et un ordre, de telle sorte que l'un d'entre eux "a" soit le premier et l'autre "b" le second.Plus précisément deux paires (a_1, b_1) et (a_2, b_2) d'éléments sont égales si et seulement si $a_1 = a_2$ et $b_1 = b_2$.*

Le produit cartésien de deux ensembles A et B, noté $A \times B$ est l'ensemble des paires ordonnées (a, b) où $a \in A$ et $b \in B$, soit;

$$A \times B = \{(a, b) \mid a \in A \wedge \ b \in B\}.$$

Exemple 15 *Exemple de produits cartésiens et de leurs éléments:*

- $\{1, 2\} \times \emptyset = \emptyset$
- $\{1, 2\} \times \{1\} = \{(1, 1); (2, 1)\}$
- $\{1, 2\} \times \{3, 4\} = \{(1, 3); (1, 4); (2, 3); (2, 4)\}$
- $\mathbb{N} \times \mathbb{R} = \{(n, x) \mid n \in \mathbb{N} \wedge x \in \mathbb{R}\}$

Remarque 16 (Définiton formelle de la paire)

De manière similaire, on définit le produit cartésien de n ensembles dont les éléments sont appelés n-uplets.

Definition 18 *Un n-uplet, $(a_1, \cdots, a_n)$ d'éléments $a_1 \in A_1, a_2 \in A_2, \cdots, a_n \in A_n$, consiste en n objets/éléments et en un ordre de telle sorte que a_1, est la première coordonnée, a_2 la deuxième et ainsi de suite. En particulier, deux n-uplets $(a_1, a_2, \cdots, a_n)$ et $(b_1, b_2, \cdots, b_n)$ sont égaux si et seulement ils ont exactement les mêmes coordonnées. C'est-à-dire que $a_1 = b_1$, $a_2 = b_2$, $\cdots$,$a_n = b_n$.*

Le produit cartésien de n ensembles, $A_1, \cdots, A_n$, noté $A_1 \times A_2 \times \cdots \times A_n$ ou $\Pi_{i=1}^{n} A_i$ est l'ensemble des n-uplets, $(a_1, \cdots, a_n)$ d'élements $a_1 \in A_1, a_2 \in A_2, \cdots, a_n \in A_n$.

Exemple 16 *Exemple de produits cartésiens de plus de deux ensembles*

- $\mathbb{N} \times \mathbb{R} \times \emptyset = \emptyset$

- $\{1,2\} \times \{1\} \times \{3,4\} = \{(1,1,2);(2,1,3);(2,1,2);(2,1,3)\}$
- $\mathbb{N} \times \mathbb{R} \times \mathbb{R} = \{(n,x,y) \mid n \in \mathbb{N} \wedge x \in \mathbb{R} \wedge y \in \mathbb{R}\}$

Remarque 17 *On note généralement A^n le produit cartésien de n fois l'ensemble A. Par exemple $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$.*

2.4 Ensemble des parties d'un ensemble

Definition 19 *L'ensemble des parties d'un ensemble A, noté $\mathcal{P}(A)$ ou 2^A est l'ensemble dont les éléments sont les sous-ensembles de A.*

Exemple 17 *Exemple d'ensemble des parties:*

- $\mathcal{P}(\emptyset) = \{\emptyset\}$ *(l'ensemble vide a un sous-ensemble: lui-même)*
- $\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$
- $\mathcal{P}(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

2.5 Quelques éléments sur la théorie axiomatique des ensembles.

Dans la théorie axiomatique (comme Zermelo-Fraenkel), les ensembles sont définis de manière explicite par un ensemble d'axiome (en plus de l'axiome d'extensionalité) qui énoncent quels sont les ensembles valides. La série d'axiomes suivants permet de construire l'univers des ensembles considérés en mathématiques en utilisant les règles de la logique

Axiome 2 (de la paire) *Si E et F sont deux ensembles, il existe un ensemble paire, noté $\{E, F\}$ dont les uniques éléments sont E et F.*

Axiome 3 (de la réunion) *Si E est un ensemble, il existe un ensemble $\cup E$ dont les éléments sont les éléments des élément de E.*

Notamment si $E = \{A, B\}$, $\cup E$ correspond à l'union classique $A \cup B$.

Axiome 4 (des parties) *Si E est un ensemble, il existe un ensemble $\mathcal{P}(E)$ dont les éléments sont les sous-ensembles (parties) de E*

Axiome 5 (Existence) *Il existe au moins un ensemble.*

Axiome 6 (schéma d'axiomes de compréhension) *Si E est un ensemble et P une propriété (la définition exacte d'une propriété est plus complexe et non abordée ici), alors les éléments de E satisfaisants P forment un ensemble.*

En utilisant l'axiome de l'existence et la propriété $x \notin x$, on en déduit l'existence de l'ensemble vide

$$\emptyset = \{x \in E \mid x \neq x\}$$

Axiome 7 (de l'infini) *Il existe un ensemble E tel que*

- $\emptyset \in E$
- *Si x est un élément de E alors $x \cup \{x\} \in E$.*

Cet ensemble est infini (c'est en fait l'ensemble des nombres entiers, voir ci-dessous)L.

3 Fonctions

3.1 Generalitiés

Definition 20 (Définition naïve d'une fonction) *Une fonction f d'un ensemble A dans un ensemble B, notée $f : A \to B$, associe à chaque élément $a \in A$ un unique element $f(a) \in B$.*

A est appelé le domaine de f; si $f(a) = b$, b est appelé image de a et a l'antécédent de b par f;

Definition 21 *Le graphe d'une fonction $f : A \to B$ est le sous-ensemble de $A \times B$, défini par $Graphf = \{(a, b) \in A \times B \mid b = f(a)\}$.*

Definition 22 (Définition formelle d'une fonction) *Une fonction f (de A dans B) est un triplet (A, B, G) où A et B sont deux-ensembles et G un sous-ensemble de $A \times B$ tel que pour tout $a \in A$, il existe un unique $b \in B$ tel que $(a, b) \in G$.*

G est appelé le graphe de f.

Remarque 18 *Dans ce cours, les termes fonctions et applications seront utilisés comme synonymes.*

Remarque 19 *De cette définition formelle, on peut déduire que deux fonctions f et g de A dans B sont égales si pour tout $a \in A$, on a $f(a) = g(a)$.*

Exemple 18 *Exemple de fonctions:*

- $f : \{1, 2, 3\} -> \{a, b, c, \}$ *définie par* $f(1) = a, f(2) = b, f(3) = c$.
- $f : \{1, 2, 3\} -> \{a, b, c\}$ *définie par* $f(1) = a, f(2) = a, f(3) = c$.
- $f : \{1\} -> \mathbb{R}$ *définie par* $f(1) = 0$
- $f : \mathbb{R} -> \mathbb{R}$ *définie par* $f(x) = -x^3$

Definition 23 *La fonction identité de A notée Id_A, est la fonction de A dans A définie par $Id_A(a) = a$ pour tout $a \in A$.*

Definition 24 *Une fonction $f : A \to B$ est constante si pour tout a_1 et a_2 éléments de A, on a $f(a_1) = f(a_2)$. En d'autres termes: $\exists b_0 \in B \ \forall a \in A \ f(a) = b$.*

Remarque 20 *On notera A^B ou $\mathcal{F}(A, B)$ l'ensemble des fonction de A dans B.*

3.2 Images directe et réciproque

Dans ce qui suit f désigne une fonction de A dans B.

Definition 25 *L'image d'un sous-ensemble D de A par f est l'ensemble des éléments qui sont l'image d'un élément de D,soit:*

$$f(D) = \{b \in B \mid \ \exists a \in D \ b = f(a)\}.$$

Exemple 19 *exemples d'image directe*

- *pour $f : \{1,2,3\} -> \{a,b,c\}$ tel que $f(1) = a, f(2) = a, f(3) = b$ on a $f(\{1\}) = \{a\}$, $f(\{1,2\}) = \{a,b\}$, $f(\{1,2,3\}) = \{a,b\}$.*
- *pour $f : \mathbb{R} \to \mathbb{R}$ tel que $f(x) = x^2$, on a $f([0,2]) = [0,4]$, $f([-2,2]) = [0,4]$,$f([-3,2]) = [0,9]$, $f(\mathbb{R}) = \mathbb{R}_+$*

Proposition 1 *Soient $E \subset F$ deux sous -ensembles de A, on a $f(E) \subset f(F)$*

Démonstration: *Soit $y \in f(E)$. Par définition, il existe $x \in E$ tel que $f(x) = y$. Comme $E \subset F$, on a $x \in F$ et donc il existe $x \in F$ tel que $f(x) = y$. On a bien montré que $f(E) \subset f(F)$*

Proposition 2 *Etant donnés deux ensembles A_1 et A_2, on a:*

1. *$f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$*
2. *$f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$.*

Démonstration: *1. On raisonne par double inclusion. Montrons d'abord que $f(A_1 \cup A_2) \subset f(A_1) \cup f(A_2)$. Soit $y \in f(A_1 \cup A_2)$. Par définition, il existe $x \in A_1 \cup A_2$ tel que $f(x) = y$. Or comme $x \in A_1 \cup A_2$, on a soit $x \in A_1$ soit $x \in A_2$. Si $x \in A_1$, on a bien, puisque $f(x) = y$, $y \in f(A_1)$, d'où on déduit $y \in f(A_1) \cup f(A_2)$. De même si $x \in A_2$, on montrerait que $y \in f(A_2) \subset f(A_1) \cup f(A_2)$. D'où on déduit que $f(A_1 \cup A_2) \subset f(A_1) \cup f(A_2)$.*

Réciproquement, montrons que $f(A_1) \cup f(A_2) \subset f(A_1 \cup A_2)$. Soit $y \in f(A_1) \cup f(A_2)$. On a soit $y \in f(A_1)$ soit $y \in f(A_2)$. Dans les deux cas, on déduit de la proposition 1 que $y \in f(A_1 \cup A_2)$. On a donc bien $f(A_1) \cup f(A_2) \subset f(A_1 \cup A_2)$, ce qui conclut la démonstration.

2. *Soit $y \in f(A_1 \cap A_2)$, il existe $x \in A_1 \cap A_2$ tel que $f(x) = y$. Comme $x \in A_1$, on en déduit que $y \in f(A_1)$. Comme $x \in A_2$, on en déduit que $y \in f(A_2)$. On a donc bien $y \in f(A_1) \cap f(A_2)$, ce qui achève la démonstration.*

Remarque 21 *N.B: On a pas forcément $f(A_1) \cap f(A_2) \subset f(A_1 \cap A_2)$. (exercice: trouver un contre-exemple).*

Definition 26 *L'image réciproque d'un sous-ensemble $C \subset B$ par $f : A \to B$, noté $f^{-1}(C)$, est l'ensemble des éléments de A qui sont l'antécédent d'un élément de C, soit:*

$$f^{-1}(C) = \{a \in A \mid f(a) \in C\}$$

Exemple 20 *exemples d'image réciproque:*

- *pour $f : \{1, 2, 3\} - > \{a, b, c\}$ tel que $f(1) = a, f(2) = a, f(3) = b$ on a $f^{-1}(\{a\}) = \{1, 2\}$, $f^{-1}(\{a, b\}) = \{1, 2, 3\}$, $f^{-1}(\{a, b, c\}) = \{1, 2, 3\}$.*
- *pour $f : \mathbb{R} \to \mathbb{R}$ tel que $f(x) = x^2$, on a $f^{-1}([-3, 0]) = \{0\}$, $f^{-1}([0, 4]) = [-2, 2]$, $f^{-1}(\mathbb{R}_+) = \mathbb{R}$.*

Proposition 3 *Soit $f : A \to B$ et $E \subset F$ deux sous -ensembles de B, on a $f^{-1}(E) \subset f^{-1}(F)$*

Démonstration: *Soit $x \in f^{-1}(E)$. Il existe $y \in E$ tel que $f(x) = y$. Comme $E \subset F$, on aussi $y \in F$. Donc $\exists y \in F$ $f(x) = y$, c'est-à-dire $x \in f^{-1}(F)$. Ce qui achève la démonstration.*

Proposition 4 *Soit $f : A \to B$ et B_1, B_2 des sous-ensembles de B, on a :*

- $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$
- $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

Démonstration:

- *On procède par double inclusion. Soit $x \in f^{-1}(B_1 \cup B_2)$. Il existe $y \in B_1 \cup B_2$ tel que $f(x) = y$. On a donc, soit $y \in B_1$, d'où $x \in f^{-1}(B_1) \subset f^{-1}(B_1) \cup f^{-1}(B_2)$, soit $y \in B_2$, d'où $x \in f^{-1}(B_2) \subset f^{-1}(B_1) \cup f^{-1}(B_2)$. Donc, par disjonction des cas, on a bien montré que $x \in f^{-1}(B_1) \cup f^{-1}(B_2)$, et donc $f^{-1}(B_1 \cup B_2) \subset f^{-1}(B_1) \cup f^{-1}(B_2)$.*

  Réciproquement, on a $B_1 \subset B_1 \cup B_2$, d'où $f^{-1}(B_1) \subset f^{-1}(B_1 \cup B_2)$, et $B_2 \subset B_1 \cup B_2$, d'où $f^{-1}(B_2) \subset f^{-1}(B_1 \cup B_2)$. On en déduit que $f^{-1}(B_1) \cup f^{-1}(B_2) \subset f^{-1}(B_1 \cup B_2)$ ce qui achève la démonstration.

- *exercice.*

Definition 27 *Soient $f : A \to B$ et $g : C \to D$, telles que $f(A) \subset C$. La composée de f par g est la focntion $g \circ f : A \to D$ définie par*
$g \circ f(a) = g(f(a))$ pour tout $a \in A$.

3.3 Fonctions injectives et surjectives

Definition 28 *Une fonction $f : A \to B$ est dite surjective si tout élément de B admet un antécédent par f. Formellement f est surjective si*

$$f(A) = B \text{ ou encore } \forall y \in B \ \exists x \in A \ f(x) = y$$

Exemple 21 *Etude de la subjectivité de quelques fonctions:*

- $\begin{array}{rccc} f & : & \mathbb{R} & \to & \mathbb{R}_+ \\ & & x & \mapsto & x^2 \end{array}$ *est surjective.*
- $\begin{array}{rccc} f & : & \mathbb{R} & \to & \mathbb{R} \\ & & x & \mapsto & x^2 \end{array}$ *n'est pas surjective.*
- *Pour tout ensemble A, $id_A : A \to A$ est surjective.*

Definition 29 *Une fonction $f : A \to B$ est dite injective si chaque élément de A a une image distincte par f. Soit formellement:*

$$a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2) \text{ ou par contraposée } f(a_1) = f(a_2) \Rightarrow a_1 = a_2.$$

Exemple 22 *Etude de l'injectivité de quelques fonctions:*

- $\begin{array}{rccc} f & : & \mathbb{R} & \to & \mathbb{R}_+ \\ & & x & \mapsto & x^2 \end{array}$ *n'est pas injective.*
- $\begin{array}{rccc} f & : & \mathbb{R}_+ & \to & \mathbb{R}_+ \\ & & x & \mapsto & x^2 \end{array}$ *est injective.*
- *Pour tout ensemble A, $id_A : A \to A$ est surjective.*

Definition 30 *Une fonction $f : A \to B$ est dite bijective si elle est à la fois surjective et injective.*

Remarque 22 *On remark que f est bijective si et seulement si tout élément de B admet un unique antécédent par f.*

Definition 31 *Une fonction $f : A \to B$ est dite inversible si il existe une fonction $g : B \to A$ telle que:*

- *$g \circ f = Id_A$ and $f \circ g = Id_B$.*
- *On note alors $g := f^{-1}$ et $f^{-1} : B \to A$ est appelée inverse de f.*

On a alors:

Proposition 1 *Une fonction $f : A \to B$ est bijective si et seulement si elle est inversible.*

Démonstration: *N.B la locution "si et seulement si" indique qu'on doit montrer une équivalence. On procède donc par double inclusion.*

Supposons d'abord que $f : A \to B$ est bijective. On cherche à montrer que son inverse existe. Considérons dès lors $y \in B$ quelconque. Comme f est bijective, il existe un unique x tel que $f(x) = y$ (cf. remark 22). On pose alors $g(y) = x$. On a bien $g \circ f(x) = x$ et $f \circ g(y) = y$. On a donc montré que f est inversible.

Réciproquement, on considère que $f : A \to B$ est inversible et on montre qu'elle est bijective (i.e injective et surjective). Pour l'injectivité, on considère $x_1, x_2 \in A$ tels que $f(x_1) = f(x_2)$. On applique f^{-1} pour obtenir $f^{-1} \circ f(x_1) = f^{-1} \circ f(x_2)$ soit $x_1 = x_2$, ce qui démontre l'injectivité. Pour la subjectivité, on considère $y \in B$ et on pose $x = f^{-1}(y)$. On a alors $f(x) = y$ ce qui prouve que f est surjective.

3.4 Suites et familles

Les suites sont en fait des fonctions particulières:

Definition 32 *Une suite est une application dont le domaine est $\mathbb{N}$ Une suite d'éléments de X associe à chaque élément $n \in \mathbb{N}$ un élément $x_n \in X$ et se note $(x_n)_{n\in\mathbb{N}}$.*

On utilise une notation spécifique pour souligner qu'on s'intéresse principale aux éléments de l'image (les x_n) alors que les entiers servent principalement à distinguer ces différents éléments et sont appelés les indices de la suite.

Exemple 23 *Exemples de suites:*

- *La suite $(u_n)_{n\in\mathbb{N}}$ à valeurs dans $\mathbb{R}$ définie pour tout $n \in \mathbb{N}$ par $u_n = \dfrac{1}{n+1}$.*
- *La suite de fonctions numériques $(f_n)_{n\in\mathbb{N}}$ définie pour tout $n \in \mathbb{N}$ par*
$$\begin{array}{rccc} f_n & : & \mathbb{R}_+ & \to & \mathbb{R}_+ \\ & & x & \mapsto & x^n \end{array}$$
- *La suite de sous-ensembles de $\mathbb{R}$ définie pour tout $n \in \mathbb{N}$ par $A_n = [-n, n]$*

On peut généraliser la notion de suite en celle de famille indicée ou le domaine (i.e les indices) sont choisies dans un ensemble quelconque.

Definition 33 *Une famille indicée par un ensemble d'indices I est une application dont le domaine est I. . Une famille d'éléments de X indicée par I associe à chaque élément $i \in I$ un élément $x_i \in X$ et se note $(x_i)_{i\in I}$ ou $\{x_i\}_{i\in I}$.*

Exemple 24 *Exemples de familles indicées:*

- *La famille de vecteurs de $\mathbb{R}^3$ $(v_x)_{x\in\mathbb{R}}$ définie pour tout $x \in \mathbb{R}$ par $v_x = (x, 2x, 3x)$.*
- *La famille de fonctions numériques $(f_a)_{a\in\ \mathbb{R}}$ définie pour tout $a \in \mathbb{R}$ par* $\begin{array}{rccc} f_a & : & \mathbb{R}_+ & \to & \mathbb{R}_+ \\ & & x & \mapsto & x+a \end{array}$
- *La famille de sous-ensembles $(F_t)_{t\in\mathbb{R}}$ de sous-ensembles de fonctions de $\mathbb{R}$ dans $\mathbb{R}$ définie par $F_t = \{f : \mathbb{R} \to \mathbb{R} \mid \forall x \in \mathbb{R}\ f(x) \leq t\}$*

La notion de famille indicée sera utilisée en particulier pour les ensembles et l'on a une extension naturelle des opérations ensemblistes aux familles indicées.

Definition 34 *Une famille d'ensembles indicée par I consiste en la donnée d'un ensemble $E_i$pour tout $i \in I$. On note une telle famille $\{E_i\}_{i\in I}$*

Definition 35 *Soit $(E_i)_{i\in I}$ une famille indicée d'ensembles. On pose:*

$$\cap_{i\in I}E_i := \{x \mid \forall i \in I\ x \in E_i\}$$

$$\cup_{i\in I}E_i := \{x \mid \exists i \in I\ x \in E_i\}$$

Exemple 25 *Exemples d'opérations sur les familles indicées.*

- *Soit pour tout $n \in \mathbb{N}$, $E_n = [-n, n]$, on a $\cap_{n\in\mathbb{N}}E_n = \{0\}$ et $\cup_{n\in\mathbb{N}}E_n = \mathbb{R}$*
- *Soit pour tout $x \in \mathbb{R}_+^*$, $E_x = [0, \frac{1}{x+1}[$, on a $\cap_{x\in\mathbb{R}_+^*}E_x = \{0\}$ et $\cup_{x\in\mathbb{R}_+^*}E_x = [0, 1]$.*

On a les propriétés suivantes pour les opérations ensemblistes sur les familles indicées d'ensembles:

Proposition 5 *Soit $(E_i)_{i\in I}$ et F un ensemble. On a:*

1. $F \cap (\cap_{i \in I} E_i) = \cap_{i \in I}(F \cap E_i)$
2. $F \cup (\cap_{i \in I} E_i) = \cap_{i \in I}(F \cup E_i)$
3. $F \cap (\cup_{i \in I} E_i) = \cup_{i \in I}(F \cap E_i)$
4. $F \cup (\cup_{i \in I} E_i) = \cup_{i \in I}(F \cup E_i)$
5. $(\cap_{i \in I} E_i)^c = \cup_{i \in I} E_i^c$
6. $(\cup_{i \in I} E_i)^c = \cap_{i \in I} E_i^c$

Démonstration: *voir td.*

4 Relations

4.1 Generalités

Naïvement, une relation est un symbole (e.g $=, >$) représentant le fait qu'une paire (x, y) de variables satisfaisant une certaine propriété. Cette idée peut se formaliser grâce à la définition suivante:

Definition 36 *Soient E et F deux ensembles, une relation binaire de E dans F est un sous-ensemble $\mathcal{R}$ de $E \times F$. On note généralement $x\mathcal{R}y$ plutôt que $(x, y) \in \mathcal{R}$. Lorque $E = F$, $\mathcal{R}$ est dit être une relation dans E.*

Remarque 23 *En pratique, une relation $\mathcal{R}$ de E dans F est souvent définie en énonçant les propriétés que doivent vérifier deux éléments pour être liés par la relation. Dans ce cas, on appelle graphe de $\mathcal{R}$ le sous-ensemble de $E \times F$ constitué des paires $(x, y) \in E \times F$ telles que $x\mathcal{R}y$.*

Exemple 26 *exemple de relations:*

- *La relation $\geq$ dans $\mathbb{N}$ dont le graphe est:*
  $\geq = \{(i, j) \in \mathbb{N}^2 \mid \exists k \in \mathbb{N}/\{0\}\ i = j + k\}$
- *La relation $\mathcal{D}$ dans $\mathbb{N}$ définie par $p\mathcal{D}q$ si et seulement si p divise q, dont le graphe est:*
  $\mathcal{D} := \{(p, q) \in \mathbb{N}^2 \mid \exists a \in \mathbb{N} \mid q = ap\}$
- *Etant donné une fonction $f : E \to F$, la relation de E dans F, $\mathcal{R}_f$, définie par $x\mathcal{R}_f y$ si et seulement si $y = f(x)$. Cet exemple montre en particulier que les fonctions sont des cas particuliers de relation.*
- *Etant donné un ensemble E la relation d'appartenance $\in$ est une relation binaire de $\mathcal{E}$ dans $\mathcal{P}(E)$ sont le graphe est*
  $\in_E := \{(a, A)\ \in E \times \mathcal{P}(E) \mid a \in A\}$

On distingue les propriétés suivantes des relations:

Definition 37 *Une relation $\mathcal{R}$ dans E est dite:*

- *réflexive si: $\forall x \in E \in x\mathcal{R}x$*
- *transitive si: $\forall x, y, z \in E\ [x\mathcal{R}y \wedge y\mathcal{R}z] \Rightarrow x\mathcal{R}z$*
- *symétrique si: $\forall x, y \in E\ x\mathcal{R}y \Leftrightarrow y\mathcal{R}x$*
- *anti-symétrique si: $\forall x, y \in E\ [x\mathcal{R}y \wedge y\mathcal{R}x] \Rightarrow x = y$.*
- *totale (ou complète) si: $\forall x, y \in E\ x\mathcal{R}y \vee y\mathcal{R}x$*

4.2 Relations d'équivalence

Definition 38 *Une relation d'équivalence sur E est une relation dans E qui est symmètrique, réflexive et transitive.*

Exemple 27 *exemples de relations d'équivalence:*

- *La relation d'égalité sur $\mathcal{E}$*
- *Dans l'ensemble D des droites du plan la relation $d\mathcal{P}d'$ si et seulement si d et d' sont parallèles.*
- *Les relation de congruence. Par exemple la relation de congruence modulo 3 est une relation d'équivalence sur $\mathbb{N}$ définie par $x \equiv_3 y$ si et seulement si x et y ont même reste dans la division par 3.*
- *Etant donné une fonction $u : E \to \mathbb{R}$, la relation sur E définie par $x\mathcal{R}_u y$ si et seulement si $u(x) = u(y)$. En économie, lorsque x et y représentent des paniers de biens et u une fonction d'utilité, cette relation est appelée relation d'indifférence.*

On peut structurer un ensemble à partir d'une relation d'équivalence en utilisant les propriétés suivantes:

Definition 39 *Soit $\mathcal{R}$ une relation d'équivalence sur E et $x \in E$, la classe d'équivalence de x est l'ensemble:*

$$\mathcal{R}_x = \{y \in E \mid x\mathcal{R}y\}$$

Definition 40 *Une partition $\mathcal{P}$ d'un ensemble E est un ensemble de parties de E (i.e $\mathcal{P}$ est un sous-ensemble de $\mathcal{P}(E)$) telle que*

- $\cup_{P\in\mathcal{P}} P = E$
- *Si $P \in \mathcal{P}$ et $Q \in \mathcal{P}$ sont tels que $P \neq Q$ alors $P \cap Q = \emptyset$.*

Proposition 2 *Soit $\mathcal{R}$ une relation d'équivalence sur E, l'ensemble des classes d'équivalence de $\mathcal{R}$ est une partition de E.*

Démonstration: *On suppose donc que $\mathcal{R}$ est une relation d'équivalence sur E et on note $\mathcal{Q}$ l'ensemble des classes d'équivalence de $\mathcal{R}$. Pour montrer que $\cup_{Q\in\mathcal{Q}} Q = E$, il suffit de remarkr que tout élément x de E appartient à sa propre classe d'équivalence $\mathcal{R}_x$ et que par définition $\mathcal{R}_x \in \mathcal{Q}$. On a donc bien $x \in \mathcal{R}_x \in \cup_{Q\in\mathcal{Q}} Q = E$. D'où on déduit $E \subset \cup_{Q\in\mathcal{Q}} Q$, ce qui conclut la première partie de la démonstration puisqu'il est évident que $\cup_{Q\in\mathcal{Q}} Q \subset E$.*

Pour démontrer le second point, on considère P, Q deux éléments de $\mathcal{Q}$ tels que $P \cap Q \neq \emptyset$ et on montre que $P = Q$. Par définition, il existe $x, y \in E$ tels que $P = \mathcal{R}_x$ et $Q = \mathcal{R}_y$. Comme alors $\mathcal{R}_x \cap \mathcal{R}_y \neq \emptyset$, il existe un élément $z \in \mathcal{R}_x \cap \mathcal{R}_y$, tel que $x\mathcal{R}z$ et $y\mathcal{R}z$. Par transitivité, on a alors $x\mathcal{R}y$. On en déduit alors, par transitivité à nouveau, que pour tout élément $w \in \mathcal{R}_y$, on a $x\mathcal{R}w$, soit $w \in \mathcal{R}_x$, ce qui montre que $\mathcal{R}_y, \subset \mathcal{R}_x$, soir $Q \subset P$. On prouve de manière symétrique que $P \subset Q$ et on conclut.

Réciproquement, on a:

Proposition 3 *Soit $\mathcal{P}$ une partition de E. La relation*

$$x\mathcal{R}_{\mathcal{P}}y \Leftrightarrow \exists P \in \mathcal{P},\ x \in P \wedge\ y \in P$$

est une relation d'équivalence sur E.

Démonstration: *Il faut vérifier que la relation $\mathcal{R}_{\mathcal{P}}$ est symétrique, réflexive et transitive. La démonstration est laissée en exercice.*

4.3 Ensembles ordonnés

Les relations d'ordre seront fondamentales dans votre cours d'analyse. Comme le dit le grand mathématicien Jean Dieudonné *"Le Calcul infinitésimal, [...], est l'apprentissage du maniement des inégalités bien plus que des égalités, et on pourrait le résumer en trois mot : majorer, minorer, approcher."*

Definition 41 *Un préordre (ou relation de préordre) sur E est une relation dans E qui est réflexive et transitive.*

Exemple 28 *Exemples de relation de préordre*

- *Etant donné une fonction $u : E \to \mathbb{R}$, (penser à une fonction d'utilité), la relation dans E définie par $x\mathcal{R}y$ si et seulement si $u(x) \geq u(y)$est un préordre.*
- *les relations d'ordre sont des relations de préordre (voir ci-dessous)*

Remarque 24 *Etant donné une relation de préordre $\succeq$ on E, la relation $\sim$ dans E définie by $x \sim y$ si et seulement si $x \succeq y$ et $y \succeq x$ est une relation d'équivalence.*

Definition 42 *Une relation d'ordre sur E est une relation binaire dans E qui est réflexive, transitive et anti-symétrique. Un ensemble ordonné est un couple $(E, \mathcal{R})$ où E est un ensemble et $\mathcal{R}$ une relation d'ordre sur E.*

Exemple 29 *Exemples de relations d'ordre:*

- *L'ordre naturel sur* $\mathbb{N}$, $\mathbb{Z}$ *ou* $\mathbb{R}$.
- *L'ordre lexicographique sur* $\mathbb{R}^2$, *défini par* $(x_1, x_2) \succeq_L (y_1, y_2)$ *si:* $[(x_1 > y_1) \vee ((x_1 = y_1) \wedge (x_2 \geq y_2))]$ *On peut définir de manière similaire un ordre lexicographique sur* $\mathbb{R}^n$
- *L'ordre sur* $\mathbb{R}^2$ *définie par* $(x_1, x_2) \succeq' (y_1, y_2)$ *si* $x_1 \geq y_1$ *et* $x_2 \geq y_2$. *Noter que cet ordre n'est pas total.*
- *La relation d'inclusion entre ensembles est un ordre qui n'est pas total.*
- *La relation de divisibilité dans* $\mathbb{N}$ *est un ordre qui n'est pas total.*

En référence à la citation de Jean Dieudonné ci-dessus: lorsqu'un ensemble est muni d'une bonne relations d'ordre, on va pouvoir les parties de cet ensemble par des éléments particuliers (ses "bornes") et raisonner sur ces éléments particuliers plutôt que sur l'ensemble. Cela est particulièrement important lorsqu'on se ramène ainsi du cas infini au cas fini. Pour mettre en oeuvre cette approche, il faut pouvoir définir correctement les bornes dun ensemble.

Definition 43 *Soit* $\preceq$ *une relation d'ordre totale sur* E *(i.e une relation d'ordre qui est totale) et* X *un sous-ensemble de* E.

- $m \in E$ *est un minorant de* X *pour* $\preceq$ *si pour tout élément* $x \in X$ *on a* $m \preceq x$. *On dit alors aussi que* X *est minoré (par* m*).*
- $M \in E$ *est un majorant de* X *pour* $\preceq$ *si pour tout élément* $x \in X$ *on a* $x \preceq M$. *On dit alors aussi que* X *est majoré (par* M*).*

Exemple 30 *Exemples de minorants et majorants:*

1. *Dans* $\mathbb{R}$, *pour l'ordre naturel,* -1 *est un minorant de* $X = [0, 2]$. *En fait tout élément de* $]-\infty, 0]$ *est un minorant de* X.
2. *Dans* $\mathbb{R}$, *pour l'ordre naturel,* 3 *est un majorant de* $X = [0, 2]$. *En fait tout élément de* $[2, +\infty[$ *est un majorant de* X.
3. *Dans* $\mathbb{N}$, *pour l'ordre naturel,* 2 *(et tout élément plus grand que* 2*) est un majorant de* $\{0, 1, 2\}$
4. *Soit* E *un ensemble et* X *un sous-ensemble de* $\mathcal{P}(E)$. E *est un majorant de* X *pour al relation d'inclusion entre ensembles.*

La notion de minorant/majorant n'est malheureusement pas assez fine pour bien caractériser un ensemble. Dans les cas simples, on peut parler de minimum et de maximum

Definition 44 *Soit $\preceq$ une relation d'ordre totale sur E (i.e une relation d'ordre qui est totale) et X un sous-ensemble de E.*

- *$m \in E$ est un minimum de X pour $\preceq$ si*
  1. *m est un minorant de X.*
  2. *$m \in X$.*
- *$M \in E$ est un maximum de X pour $\preceq$ si*
  1. *M est un majorant de X*
  2. *$M \in X$.*

Remarque 25 *On utilise souvent "plus petit élément" comme synonyme de minimum et "plus grand élément" comme synonyme de maximum.*

Exemple 31
1. *Dans $\mathbb{R}$, pour l'ordre naturel, 0 est un minimum et 2 un maximum de $X = [0, 2]$.*
2. *Dans $\mathbb{R}$, pour l'ordre naturel, $Y =]0, 2[$ n'a ni minimum ni maximum.*
3. *Dans $\mathbb{N}$, pour l'ordre naturel, l'ensemble des nombres pairs admet 0 comme minimum mais n'a pas de maximum.*

Remarque 26 *On remark qu'un sous-ensemble même minoré n'admet pas forcément de minimum et qu'un sous-ensemble même majoré n'admet pas forcément de maximum*

Definition 45 *Un ensemble E muni d'une relation d'ordre totale $\mathcal{R}$ telle que tout sous-ensemble de E a un plus petit élément est dit bien ordonné.*

En particulier, la construction de $\mathbb{N}$ (voir chapitre suivant) permettra d'affirmer que

Proposition 6 *$\mathbb{N}$ muni de son ordre naturel est un ensemble bien ordonné.*

D'autre part, on a:

Proposition 4 *Tous sous-ensemble majoré de $\mathbb{N}$ admet un plus grand élément (pour l'ordre naturel).*

Dans le cas de $Y =]0, 2[$ on serait de "borner" l'ensemble par 0 et 2 bien que ces derniers ne soient pas le minimum ou le maximum de l'ensemble. On utilise en fait le concept de borne suivant:

Definition 46 *Soit $\preceq$ une relation d'ordre totale sur E, et $X \subset E$,*

- *On appelle (lorsqu'elle existe) borne inférieure de X et on note* $\inf(X)$ *le plus grand minorant de X (i.e le plus grand élément de l'ensemble de ses minorants).*
- *On appelle (lorsqu'elle existe) borne supérieure de X et on note* $\sup(X)$ *le plus petit majorant de X (i.e le plus petit élément de l'ensemble de ses majorants).*

La notion de borne supérieure/inférieure étend bien celle de maximum/minimum:

Proposition 7 *Soit $\preceq$ une relation d'ordre totale sur E, et $X \subset E$,*

- *Un maximum de X est une borne supérieure.*
- *Un minimum de X est une borne inférieure.*

Démonstration: *On fait la démonstration dans le cas du minimum. Soit m un minimum de X. Par définition m est bien un minimum de X. De plus si m' est un minorant de m, on a par définition $\forall x \in X \; m' \leq x$. Comme en particulier $m \in X$, on a bien $m' \leq m$. m est donc bien le plus grand des minorants de X, i.e une borne inférieure.*

Exemple 32

1. *Dans $\mathbb{R}$, pour l'ordre naturel, 0 est la borne inférieure et 2 la borne supérieure de $X = [0, 2]$.*
2. *Dans $\mathbb{R}$, pour l'ordre naturel, 0 est la borne inférieure et 2 la borne supérieure de $X =]0, 2[$.*
3. *Dans $\mathbb{Q}$, pour l'ordre naturel, l'ensemble $\{x \in \mathbb{Q} \mid x^2 < 2\}$ n'a pas de borne supérieure.*

Comme nous le verrons au chapitres suivant $\mathbb{R}$ est en fait construit pour s'assurer que toute partie minorée (resp. majorée) admet une borne inférieure (resp. supérieure):

Proposition 5 *Pour l'ordre naturel*

- *Tout sous-ensemble majoré de $\mathbb{R}$ admet une borne supérieure*
- *Tout sous-ensemble minoré de $\mathbb{R}$ admet une borne inférieure*

5 Ensemble de nombres

Rappel sur les nombres entiers, démonstration par récurrence. Nombres rationnels. Nombres réels. Nombres complexes. Les notions de groupes, anneaux, corps ne seront pas traités en cours mais pourront faire l'objet d'exercices.

$$\mathbb{N}^* \to \mathbb{N} \to \mathbb{Z} \to \mathbb{D} \to \mathbb{Q} \to \mathbb{R}$$

5.1 Les nombres entiers

5.1.1 Les axiomes de Peano

On s'intéresse dans cette section à la construction axiomatique de l'ensemble des nombres entiers[1]. Cette construction est basée sur les axiomes de Peano, introduits par le mathématicien italien Giuseppe Peano en 1889.

Axiome 8 (de Peano) *Il existe un ensemble appelé ensemble des entiers naturels est noté* $\mathbb{N}$, *un élément* $0 \in \mathbb{N}$ *appelé zéro et une application* $s : \mathbb{N} \to \mathbb{N}$ *appelée successeur, vérifiant les propriétés suivantes:*

1. $0 \notin s(\mathbb{N})$ *(*0 *n'est le successeur d'aucun entier).*
2. s *est injective (deux entiers ayant le même successeur sont égaux)*
3. *Si* $A \subset \mathbb{N}$ *est telle que* $0 \in A$ *et* $\forall n \in A\ s(n) \in A$ *alors* $A = \mathbb{N}$ *(principe de récurrence).*

On pose ensuite $1 = s(0)$, $2 = s(1)$, etc. On va démontrer les principales propriétés de $\mathbb{N}$ à partir des axiomes de Peano.

Théorème 3 (Principe de la démonstration par récurrence) *Soir* $P(n)$ *un prédicat sur* N *telle que:*

1. $P(0)$ *est vraie.*
2. *Pour tout* $n \in \mathbb{N}$ $P(n) \Rightarrow P(s(n))$.

Alors $P(n)$ *est vraie pour tout* $n \in \mathbb{N}$.

Démonstration: *Il suffit d'appliquer le principe de récurrence (troisième axiome de Peano) à l'ensemble* $A = \{n \in \mathbb{N} \mid P(n)\ vraie\}$.

[1]Pour approfondir le sujet le lecteur pourra consulter http://www.math.u-psud.fr/ perrin/CAPES/arithmetique/EntiersCAPES.pdf

Proposition 8 (Définition de l'addition) *Il existe une application de* $\mathbb{N}\times\mathbb{N}\to\mathbb{N}$, *appelée addition, qui au couple* (n,p) *associe l'entier* $n+p$ *et qui est définie en posant pour tout* $n\in\mathbb{N}$:

1. $n+0=n$
2. $\forall p\in\mathbb{N}\ n+s(p)=s(n+p)$

Démonstration: *Pour montrer que l'addition est bien définie, il suffit de montrer que* $n+p$ *est bien définie pour tout entier* $p\in\mathbb{N}$, *c'est-à-dire que l'ensemble* A *des entiers* p *pour lesquels* $n+p$ *est définie est égal à* $\mathbb{N}$. *Ceci est immédiat d'après le principe de récurrence.*

Remarque 27 *On a* $1=s(0)$, *donc pour tout* $n\in\mathbb{N}$, $n+1=s(n+0)=s(n)$.

Proposition 9
1. *L'addition est associative:* $\forall a,b,c\in\mathbb{N}a+(b+c)=(a+b)+c$
2. *L'addition est commutative* $\forall a,b\in\mathbb{N}\ a+b=b+a$
3. *On a la règle de simplification:* $\forall a,b,c\in\mathbb{N}\ a+b=a+c\Rightarrow b=c$.

Démonstration:
1. *Soient* a,b *deux entiers fixés. On va montrer par récurrence que la propriété est vraie pour tout* $c\in\mathbb{N}$.
   - *Au rang* 0, *on a* $a+(b+0)=a+(b)=a+b=(a+b)+0$.
   - *Supposons que la propriété est vraie au rang* n. *On a alors:*
   $$a+(b+s(n))=a+s(b+n)=s(a+(b+n)).$$
   En utilisant la propriété de récurrence au rang n, *on en déduit que*
   $$a+(b+s(n))=s((a+b)+n)=(a+b)+s(n)$$
   Ce qui achève la démonstration.
2. *Montrons ensuite la commutativité de l'addition.*
   - *Montrons d'abord par récurrence que pour tout* $a\in\mathbb{N}$, $a+0=0+a$. *Cela est évident au rang* 0. *Si la propriété est vraie au rang* n, *on a* $0+s(n)=s(0+n)=s(n+0)=s(n)=s(n)+0$, *et la propriété est vraie pour* $s(n)$.

- *Montrons ensuite par récurrence sur a que pour tout $a, p \in \mathbb{N}$, $s(p)+a = s(p+a)$. Cela est évident au rang 0. Si la propriété est vraie au rang n, on a $s(p)+s(n) = s(s(p)+n) = s(s(p+n)) = s(p+s(n))$. Ce qui achève la démonstration.*
- *On montre enfin par récurrence sur a, que pour tout $b \in \mathbb{N}$, $a+b = b+a$. On a déjà montré la propriété au rang 0. Si on la suppose vraie au rang n, on a ensuite $s(n)+b = s(n+b) = s(b+n) = b+s(n)$.*

3. *La règle de simplification se montre facilement par récurrence.*

Proposition 10 (Définition de la multiplication) *Il existe une application de $\mathbb{N}\times\mathbb{N} \to \mathbb{N}$, appelée multiplication, qui au couple (n,p) associe l'entier $np := n*p$ et qui est définie en posant pour tout $n \in \mathbb{N}$:*

1. $n*0 = 0$
2. $\forall p \in \mathbb{N}\ n*s(p) = (n*p)+n$

Démonstration: *On vérifie par récurrence que la multiplication est bien définie.*

Proposition 11

1. *La multiplication est associative:*

$$\forall a,b,c \in \mathbb{N} a*(b*c) = (a*b)*c$$

2. *La multiplication est commutative*

$$\forall a,b \in \mathbb{N}\ a*b = b*a$$

3. *La multiplication est distributive par rapport à l'addition:*

$$\forall a,b,c \in \mathbb{N}\ a*(b+c) = a*b+a*c$$

4. *1 est un élément neutre pour la multiplication:*

$$\forall a \in \mathbb{N}\ 1*1 = a*1 = a$$

On a la règle de simplification:

$$\forall a \in \mathbb{N}^* \forall b,c \in \mathbb{N} a*b = a*c \Rightarrow b = c$$

Démonstration: *On montre que la multiplication est distributive par rapport à l'addition. Les autres démonstrations sont laissées en exercice. On montre donc par récurrence sur n que $n*(b+c) = n*b+n*c$ (en supposant démontrées associativité et commutativité).*

- *Au rang* 0, *on a:* $0*(b+c) = (b+c)*0 = 0 = 0+0 = b*0+c*0 = 0*b+0*c$.
- *Supposons que la propriété est vraie au rang n. On a alors:*

$$s(n) * (b + c) = n * (b + c) + (b + c)$$

D'où en utilisant la propriété de récurrence:

$$s(n)*(b+c) = n*b+n*c+(b+c) = n*b+b+n*c+c = s(n)*b+s(n)*c.$$

5.1.2 Propriétés liées à l'ordre

Definition 47 *On définit une relation d'ordre (supérieur ou égal) sur N en posant pour $p, q \in \mathbb{N}$, $p \geq q$ si et seulement si il existe $r \in \mathbb{N}$ tel que $p = q+r$. Cette relation admet une relation symétrique $q \leq p$ (si et seulement si $p \geq q$) et permet également de définir un ordre strict en posant $p > q$ si $p \geq q$ et $p \neq q$.*

Proposition 12 *La relation $\geq$ est une relation d'ordre totale.*

Démonstration: *On fixe $p \in \mathbb{N}$ et on montre par récurrence que $A := \{q \in \mathbb{N} \mid p \geq q \vee q \geq p\} = \mathbb{N}$. Pour $q = 0$, on a $p \geq 0$ car $p = p + 0 = 0 + p$. Si on suppose ensuite la propriété vraie au rang q et qu'on considère $s(q)$. On distingue les cas suivants:*

- *Si $q \geq p$, on a $q = p+r$, d'où $s(q) = s(p+r) = p+s(r)$, ce qui permet de conclure.*
- *Si $p \geq q$ on a $p = q + r$. Si $r = 0$, on se ramène au cas précédent. Sinon $r = s(r')$ et donc $p = q+s(r') = s(q+r') = s(r'+q) = r'+s(q)$, ce qui achève la démonstration.*

Cette relation d'ordre a les propriétés remarquables suivantes.

Théorème 4
1. *Toute partie non-vide de $\mathbb{N}$ a un plus petit élément (on dit que $\mathbb{N}$ est bien ordonné).*
2. *Toute partie finie non-vide de $\mathbb{N}$ a un plus grand élément.*

Démonstration: *1. On suppose que $A \subset \mathbb{N}$ n'a pas de plus petit élément et on montre par récurrence qu'elle ne contient aucun entier i.e qu'elle est vide):*

- *On a clairement $0 \notin A$ sinon 0 serait le plus petit élément de A (c'est le plus petit élément de $\mathbb{N}$ car pour tout $n \in \mathbb{N}$, $n = n + 0$.).*
- *On suppose donc $P(n) : \forall k \leq n \; k \notin A$ est vraie. Si $s(n) \in A$, on aurait alors que $s(n)$ est le plus petit élément de A, ce qui est absurde. La propriété est donc vraie au rang $n + 1$.*

2. On raisonne par récurrence sur le nombre d'éléments.

- *Si B a un unique élément, cet élément est son plus grand élément.*
- *Si on suppose que tout ensemble de n éléments a un plus grand élément et que B a $n + 1$ éléments. On sait que B a un plus petit élément m. En appliquant la propriété de récurrence à $C = B/\{m\}$ qui a n éléments, on obtient l'existence d'un plus grand élément M pour C. M est aussi un plus grand élément pour B. La propriété est donc vraie par récurrence.*

5.1.3 Soustraction et Division

Proposition 6 (Définition de la soustraction) *Si $a, b \in \mathbb{N}$ sont tels que $a \geq b$, il existe un unique $r \in \mathbb{N}$ tel que $a = b + r$, on appelle alors r la différence de a et b et on note $r = a - b$.*

Démonstration: *L'existence découle de la définition de $\geq$. L'unicité de la règle de simplification pour l'addition.*

On peut enfin définir la division euclidienne dans $\mathbb{N}$:

Proposition 13 (Définition de la division euclidienne) *Soient $a, b \in \mathbb{N}$, il existe un unique couple $(q, r) \in N^2$ tels que:*

1. $a = bq + r$

2. $q < r$

q est appelé le quotient et r le reste dans la division euclidienne de a par b

Démonstration: • *Il s'agit de montrer que q et r sont bien définis pour tous $a, b \in \mathbb{N}$. On fait la preuve par récurrence sur a.*

- *Si $a = 0$, on a clairement $a = 0 * b + 0$.*

- *Si la propriété est vraie au rang n, on a $n = bq + r$. Si $s(r) = b$, on a $s(n) = s(bq + r) = bq + s(r) = bq + b = b(q + 1)$ et on pose $q' = q + 1$ et $r' = 0$. Si $s(r) < b$, on a $s(n) = s(bq + r) = bq + s(r)$ et on pose $q' = q$ et $r' = s(r)$.*

- *On montre ensuite l'unicité. Soient deux couples tels que (b, q) et (b', q') tels que $a = bq + r$ et $a = bq' + r'$. Si $q = q'$, il est clair en utilisant les règles de simplification que $r = r'$ et réciproquement. Supposons donc $q > q'$, on a alors $bq + r = bq' + r'$, d'où $b * (q - q') = r' - r$. On en déduit que $r' \geq b$, ce qui est absurde.*

5.1.4 Les entiers relatifs

Les constructions ensemblistes des entiers relatifs sont un peu artificiels. On peut par exemple définir $\mathbb{Z} = \mathbb{N} \times \{0, 1\}/\{(0, 0)\}$ et utiliser la convention de notation $n := (n, 0)$ et $-n := (n, 1)$. On définit ensuite l'addition et la multiplication "naturelles" sur $\mathbb{Z}$.

Remarque 28 *Toute partie majorée de $\mathbb{Z}$ admet un plus grand élément.*

5.1.5 Eléments d'arithmétique

Definition 48 *On dit que $a \in \mathbb{N}$ est un multiple de $b \in \mathbb{N}$ (et b un diviseur de a) si il existe $c \in \mathbb{N}$ tel que $a = bc$.*

Definition 49 *On dit qu 'un entier $p \geq 2$ est premier si ses seuls diviseurs sont 1 et lui-même.*

Théorème 5 *Il existe une infinité de nombres premiers.*

Démonstration: *Voir TD*

Théorème 6 *Soient $a \geq 1$ et $b \geq 1$ deux entiers, il existe un unique entier appelé plus petit commun multiples de a et b, noté $ppcm(a, b)$, tel que c est multiple de a et b si et seulement si c est multiple de $ppcm(a, b)$.*

Démonstration: *Voir TD*

Théorème 7 *Soient $a \geq 1$ et $b \geq 1$ deux entiers, il existe un unique entier appelé plus grand commun diviseur de a et b, noté $pgcd(a, b)$, tel que c divise a et b si et seulement si c divise $pgcd(a, b)$.*

Démonstration: .

- *Existence. On suppose $a > b$ et on applique l'algorithme d'Euclide:*
  - *On effectue la division euclidienne de a par b, il existe $q_1 \in \mathbb{N}$ et $r_1 \in \mathbb{N}$ tels que $a = bq_1 + r_1$ et $r_1 < b$. Si c divise a et b alors c divise r_1. Réciproquement si c divise b et r_1 alors c divise a*
  - *On effectue la division euclidienne de b par r_1, il existe $q_2 \in \mathbb{N}$ et $r_2 \in \mathbb{N}$ tels que $b = r_1q_2 + r_2$ et $r_2 < r_1$. Si c divise a et b, alors b divise aussi r_1 d'après ce qui précède et divise donc également r_2. Réciproquement, si c divise r_2 et r_1 alors c divise b et r_1 et donc a et b.*
  - *Par récurrence, on construit une suite $(r_n)_{n=1,\cdots,N+1}$ d'entiers strictement décroissants avec $r_{N+1} = 0$ tel que c divise a et b si et seulement si c divise r_N et r_{N+1}*
  - *Comme $r_{N+1} = 0$, on a que c divise a et b si et seulement si c divise r_N*
- *unicité: si m, n sont deux pgcd, on a nécesairement m divise n et n divise m. D'où $m = un$ et $n = vm$. Soit $m = uvn$ et donc $uv = 1$ puis $m = n$.*

L'algorithme d'Euclide permet de démontrer également le lemme de Bézout.

Lemme 1 *Soient a et b deux entiers (naturels), il existe $u, v \in \mathbb{Z}$ tels que*

$$pgcd(a, b) = au + bv$$

On en déduit le lemme de Gauss:

Lemme 2 *Soient $a, b, c \in \mathbb{N}$. Si a divise bc et a est premier avec c alors a divise b*

Démonstration: *D'après le lemme de Bezout, il existe $u, v \in \mathbb{Z}$ tels que $au + cv = 1$. On a alors $abu + bcv = b$. Or a divise bc donc $bc = ad$. On a donc $b = abu + adv$ et donc a divise b.*

On en déduit l'existence de la décomposition des entiers en facteurs premiers:

Théorème 8 *Tout entier $n \geq 2$ s'écrit de manière unique sous la forme:*

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

où les p_i sont des nombres premiers et les $\alpha_i \in \mathbb{N}^*$ leur multiplicité.

Démonstration: *On démontre l'existence par récurrence sur n*

- *Pour $n = 2$, la propriété est vraie car 2 est premier.*
- *Si la popriété est vraie jusqu'au rang n alors:*
  - *soit $n+1$ est premier et la propriété est vraie au rang $n+1$.*
  - *soit $n+1$ n'est pas premier et on peu écrire $n+1 = ab$ avec $a, b \leq n$. Il suffit alors d'appliquer la propriété de récurrence à a et b pour conclure.*

L'unicité découle des propriétés de divisibilité des entiers.

La décomposition en facteurs premiers permet de donner rapidement les pgcd et ppcm de deux entiers.

5.2 Nombre rationnels

Definition 50 *Un nombre rationnel est un nombre pouvant s'écrire sous la forme $\frac{p}{q}$ où p est un entier relatif et q un entier naturel non nul.*
On note $\mathbb{Q} = \{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{N}^*\}$, l'ensemble des nombres rationnels.

Remarque 29
1. *En fait les rationnels se définissent comme l'ensemble des couples $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ en identifiant[2] $\frac{p}{q}$ et $\frac{p'}{q'}$, i.e les couples vérifiant $pq' = p'q$.*
2. *Tout nombre rationnel x admet une écriture de la forme $x := \frac{p'}{q'}$ où p' et q' sont premiers entre eux.*

L'ensemble $\mathbb{Q}$ n'est pas complet:

Proposition 7 *$\sqrt{2}$ n'est pas un nombre rationnel.*

Pourtant on peut placer sur une droite un nombre d'abcisse $\sqrt{2}$ en utilisant une règle et un compas...

[2]formellement en quotientant par une relation d'équivalence bien choisie

5.3 Écriture décimale d'un rationnel

Definition 51 *Un nombre décimal est un nombre pouvant s'écrire sous la forme* $\frac{N}{10^n}$ *où* N *et* n *sont des entiers naturels.*
On note $\mathbb{D} = \{\frac{N}{10^n} \mid N \in \mathbb{N}, n \in \mathbb{N}\}$, *l'ensemble des nombres décimaux.*

Remarque 30 *Exemples.* $\mathbb{D} \subset \mathbb{Q}$.

Remarque 31 *Un nombre* d *est décimal si et seulement si il existe* $k \in \mathbb{N}$, $\alpha_0 \in \mathbb{N}$ *et* $\alpha_1, \cdots, \alpha_k \in \{0, \cdots, 9\}$ *tels que* $d = \alpha_0 + 10^{-1}\alpha_1 + \cdots 10^{-n}\alpha_k$.

Definition 52 *Un développement décimal est une suite de nombre décimaux* $d = (d_n)_{n\in\mathbb{N}}$ *de la forme*

$$d_n := \alpha_0 + 10^{-1}\alpha_1 + \cdots 10^{-n}\alpha_n := \alpha_0, \alpha_1\alpha_2 \cdots \alpha_n$$

où $\alpha_0 \in \mathbb{N}$ *et pour tout* $i \in \mathbb{N}$, $\alpha_i \in \{0, \cdots 9\}$

On peut associer à tout nombre rationnel un développement décimal (qu'on appellera son écriture décimale) en utilisant la division euclidienne (on se restreint aux rationnels positifs ; pour les négatifs, il suffit de placer le signe moins devant).

Exemple 33 $\frac{20}{7} = 2,85731428573142\cdots$

Soit $x = p/q$ un nombre rationnel positif ($q > 0$). A priori p et q peuvent être non premiers entre eux. Le quotient de p par q s'obtient en posant la division comme on l'a appris en primaire... Ce qui est, si on y réfléchit bien, relativement complexe. La partie entière de x est obtenue à l'aide de la division euclidienne de p par q.

$$p = \alpha_0 q + \beta_0,$$

où α_0 et β_0 sont des entiers.
Le premier chiffre après la virgule s'obtient à l'aide de la division euclidienne de $10\beta_0$ par q.

$$10\beta_0 = \alpha_1 q + \beta_1,$$

où α_1 et β_1 sont des entiers. On remark que puisque $\beta_0 < q$, l'entier α_1 est compris entre 0 et 9. En combinant les deux, on déduit que

$$10p = (10\alpha_0 + \alpha 1)q + \beta_1$$

soit

$$\frac{p}{q} = \alpha_0 + 10^{-1}\alpha_1 + 10^{-1}\frac{\beta_1}{q}$$

et donc $\frac{p}{q} \approx \alpha_0, \alpha_1$ à 10^{-1} près.
Avec des notations, évidentes on a:

$$10\beta_{k-1} = \alpha_k q + \beta_k,$$

$$10^k p = (10^k\alpha_0 + 10^{k-1}\alpha_1 + \cdots + 10\alpha_{k-1} + \alpha_k)q + \beta_k,$$

$$\frac{p}{q} = \alpha_0 + 10^{-1}\alpha_1 + \cdots + 10^{1-k}\alpha_{k-1} + 10^{-k}\alpha_k + 10^{-k}\frac{\beta_k}{q}$$

et donc $\frac{p}{q} \approx \alpha_0, \alpha_1 \cdots \alpha_k$ à 10^{-k} près.
La suite de nombre décimaux $\alpha_0, \alpha_1 \cdots \alpha_k$ fournit une valeur approchée par défaut de x à 10^{-k} près, qu'on appelle le développement décimal de x.

Remarque 32 *Dans ce qui précède, la valeur de α_{k+1} est entièrement déterminée par celle de β_k.*

Proposition 8 *Le développement décimal d'un nombre décimal est nul à partir d'un certain rang.*

Preuve
Soit $d := \frac{N}{10^n}$ un nombre décimal. Comme $N \in \mathbb{N}$, on peut écrire N sous la forme

$$N := 10^n\alpha_0 + 10^{n-1}\alpha_1 + \cdots + 10\alpha_{n-1} + \alpha_n$$

avec $\alpha_0 \in \mathbb{N}$ et pour $i \geq 1$, $\alpha_i \in \{0, \cdots, 9\}$, on a donc:

$$\frac{N}{10^n} = \alpha_0 + 10^{-1}\alpha_1 + \cdots + 10^{1-n}\alpha_{n-1} + 10^{-n}\alpha_n + 0$$

On a donc $\beta_n = 0$. On obtient alors facilement par récurrence que pour tout $k \geq n$, $\beta_{k+1} = 0$ et donc $\alpha_{k+1} = 0$.

Proposition 9 *Un nombre rationnel a une écriture décimale "périodique" à partir d'un certain rang.*

Preuve.
Dans l'algorithme précédent, la suite $(\beta_k)_{k\in\mathbb{N}}$ prend ses valeurs dans l'ensemble fini $\{0, 1, \ldots, q-1\}$. La suit va donc obligatoirement prendre deux fois la même valeur. Il exister donc un entier n et un entier r tels que $\beta_{r+n} = \beta_r$. Par définition de la division euclidienne, cela entraînera $\alpha_{r+n+1} = \alpha_{r+1}$ et $\beta_{r+n+1} = \beta_{r+1}$. De proche en proche, $\alpha_{r+n+2} = \alpha_{r+2}$ et $\beta_{r+n+2} = \beta_{r+2}$, ce qui permettra de montrer par récurrence que les α_k pour $k \geq r+1$ seront périodiques de période n.

5.4 Nombres réels

5.4.1 Construction (naïve) de $\mathbb{R}$.

Historiquement, l'apparition du premier nombre réel est issu du Théorème de Pythagore. De nombreux problèmes (quadrature du cercle, duplication du cube) posés par les grecs résultent de l'irrationalité de certains nombres apparaissant "naturellement" (équations algébriques). Il faut attendre la fin du XIX-ème siècle pour voir apparaître leur construction rigoureuse (Dedekind, Weierstrass).
Si les nombres rationnels ont un développement décimal périodique, l'ensemble de tous ls développement décimaux doit être "plus grand" que $\mathbb{Q}$. On est donc tenté de définir l'ensemble des nombres réels comme l'ensemble des développements décimaux illimités, mais:
Si on considère le nombre dont le développement décimal est $A = 0,99999999\cdots$, on a $10A = 9,999999\cdots$ et donc $10A = 9 + A$, soit $A = 1$.
En fait, on introduit la notion suivante:

Definition 53 *Un développement décimal $a_0, a_1 \cdots a_n \cdots$ est dit propre si $\forall N \in \mathbb{N}\ \exists i \geq N$ tq $a_i \neq 9$ (i.e les développements décimaux ne se terminant pas par une infinité de 9.)*

Definition 54 *L'ensemble des nombres réels, noté $\mathbb{R}$, est l'ensemble des développements décimaux propres (muni de l'addition, de la multiplication et surtout de l'ordre lexicographique "naturels")*

(voir http://math.univ-lyon1.fr/capes/IMG/pdf/new.decimaux.pdf pour plus de détails).

Remarque 33 *Soient $x = \alpha_0, \alpha_1 \cdots \alpha_n \cdots$ et t $y = \beta_0, \beta_1 \cdots \beta_n \cdots$ deux nombres réels et $I := \{i \in \mathbb{N} \mid \alpha_i \neq \beta_i\}$.*

- *Si $I = \emptyset$, on a $x = y$.*

- *Si $I \neq \emptyset$, soit $k = \min I$. On a*

  1. *$x < y$ si $\alpha_i < \beta_i$*
  2. *$x > y$ si $\alpha_i > \beta_i$*

Propriété 4 *1. $\forall x \in \mathbb{R}$, $\exists! n \in \mathbb{Z}$ tel que $n \leq x < n+1$; n est la partie entière de x, noté $E(x) = [x]$.*

2. $\forall (x, y) \in \mathbb{R}^2$ tels que $x < y$, il existe $z \in \mathbb{Q}$ tel que $x < z < y$. On dit que $\mathbb{Q}$ est dense dans $\mathbb{R}$.

Preuve.

1. Soit $x := \alpha_0, \alpha_1 \cdots \alpha_n \cdots$, on a $E(x) = \alpha_0$.

2. On montre en fait que l'ensemble $\mathbb{D}$ des nombres décimaux est dense dans $\mathbb{R}$ (cela suffit car on a clairement $\mathbb{D} \subset \mathbb{Q}$). Soient $x = \alpha_0, \alpha_1 \cdots \alpha_n \cdots$ et t $y = \beta_0, \beta_1 \cdots \beta_n \cdots$ deux nombres réels tels que $x < y$. D'après la remark précédente, on a $\{i \in \mathbb{N} \mid \alpha_i \neq \beta_i\} \neq \emptyset$ et $k = \min I$ est tel que $\alpha_k < \beta_k$ et pour $i < k, \alpha_i = \beta_i$. D'autre part, on sait qu'il existe $r > k$ tel que $\alpha_r < 9$. On pose alors

$$z = \alpha_0, \alpha_1 \cdots \underbrace{\alpha_k}_{\text{rang } k} 9 \cdots 9 \underbrace{9}_{\text{rang } r}$$

   On a clairement $x < z < y$.

5.4.2 Ordre dans $\mathbb{R}$

Definition 55 *Un sous-ensemble $I \subset \mathbb{R}$ est un intervalle si et seulement si*

$$\forall a, b \in I \ \forall c \in \mathbb{R} \ a < c < b \Rightarrow c \in I.$$

Proposition 10 *Etant donné $a, b \in \mathbb{R}$, les ensembles:*

1. *$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$*
2. *$]a, b[= \{x \in \mathbb{R} \mid a < x < b\}$*
3. *$]a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$*
4. *$[a, b[= \{x \in \mathbb{R} \mid a \leq x < b\}$*

sont des intervalles (dits respectivement fermé, ouvert, ouvert à gauche, ouvert à droite).

Remarque 34 *Soit $A \subset \mathbb{R}$. Si A est fini, il a un plus grand élément* $\max A$ *et un plus petit élément* $\min A$. *Cependant, dès que A n'est plus fini, l'existence de* $\max A$ *et* $\min A$ *n'est plus garantie (penser à $[0,1[$ par exemple).*

Exemple 34 *Déterminer les majorants, minorants, maximums, minimums (s'ils existent) des ensembles : $A = \mathbb{R}$, $B = \left(1 - \frac{1}{n}\right)_{n\in\mathbb{N}^*}$, $C = [0,2[$, $D = \left\{x \in \mathbb{Q}\,,\ x^2 \leq 2\right\}$.*

Théorème 9 (axiome de la borne supérieure) *Toute partie non-vide et majorée de $\mathbb{R}$ admet une borne supérieure*

Preuve. Soit A une partie non-vide de $\mathbb{R}$, majorée par m. Pour tout $x \in A$, on note $\alpha_k(x)$ le kième élément du développement décimal (propre) de x.

- L'ensemble $\{\alpha_0(x) \mid x \in A\}$ est non-vide et majoré par $E[m]$ et a donc un plus grand élément s_0.
- Par récurrence, on suppose qu'on a construit les k premiers termes d'une suite $s_0, \cdots, s_k$ tels que pour tout $j \leq k$, s_j soit le plus grand parmi les jèmes termes des éléments commençant par $s_0, s_1 \cdots s_{j-1}$. C'est à dire:

$$s_j = \max\{\alpha_j(x) \mid x \in A, \alpha_0(x) = s_0, \cdots, \alpha_{j-1}(x) = s_{j-1}\}.$$

- On pose de même

$$s_{k+1} = \max\{\alpha_{j+1}(x) \mid x \in A, \alpha_0(x) = s_0, \cdots, \alpha_j(x) = s_j\}.$$

  N.B : Cet ensemble a bien un plus grand élément car c'est un sous-ensemble non-vide de $\{0, \cdots, 9\}$.

- Le nombre réel défini par $s := s_0, s_1 \cdots s_n \cdots$ est la borne supérieure de A :
  - C'est un majorant de A. Soit $x = x_0, x_1 \cdot x_n \cdots \in A$ avec $x \neq s$ et $k := \inf\{i \in \mathbb{N} \mid x_i \neq s_i\}$. On a par construction $x_i < s_i$ et donc $x < s$.

– C'est le plus petit des majorants de A. Soit en effet $b = \beta_0, \beta_1 \cdots \beta_n \cdots$ un autre majorant ($b \neq s$) et $\ell = \inf\{i \in \mathbb{N} \mid \beta_i \neq s_i\}$. Supposons $\beta_\ell < s_\ell$. Par construction, il existe un élément x de A tel que $x = s_0, s_1 \cdots s_\ell \alpha_{\ell+1}(x) \cdots$. Un tel élément x vérifie alors $x > b$, ce qui contredit le fait que b est un majorant de A. Donc, on a $\beta_\ell > s_\ell$ et ainsi $b > s$. s est donc bien le plus petit majorant de A.

Corollaire 1 *Toute partie non-vide et minorée de $\mathbb{R}$ admet une borne inférieure*

Preuve Si B est une partie non-vide et minorée de $\mathbb{R}$, $-B$ est une partie non-vide et majorée de $\mathbb{R}$, donc elle admet une borne supérieure s. On vérifie que $-s$ est une borne inférieure de B?

Exemple 35 *L'ensemble $\{x \in \mathbb{Q},\ x^2 \leq 2\}$ n'admet pas de borne supérieure en tant que partie de $\mathbb{Q}$ mais il en admet une ($\sqrt{2}$) en tant que partie de $\mathbb{R}$.*

Propriété 5 *Soit A, B et C des sous-ensembles non-vide de $\mathbb{R}$. Alors :*

- *si A est fini, alors* $\sup A = \max A$ *et* $\inf A = \min A$.
- *si* $\max A$ *existe, alors* $\sup A = \max A$.
- $\sup(-A) = -\inf A$ *et* $\inf(-A) = -\sup(A)$.
- $\sup(A \cup B) = \max(\sup A, \sup B)$ *et* $\inf(A \cup B) = \min(\inf A, \inf B)$
- *Si $A \subset C$, alors* $\inf A \leq \inf C$ *et* $\sup A \leq \sup C$ *(avec la convention que pour tout réel u $-\infty \leq u \leq +\infty$.*

Preuve Exercice.

Exemple 36 *Vérifier ces propriétés sur des exemples.*

Definition 56 (Application aux fonctions) *On appelle borne supérieure (respectivement inférieure) de f sur $A \subset \mathcal{D}_f$, le réel* $\sup_A f = \sup(f(A))$ *(respectivement* $\inf_A f = \inf(f(A))$*).*

Propriété 6 (Caractérisation de la borne supérieure) *Soit A une partie majorée non vide de $\mathbb{R}$, $a = \sup A$ si et seulement si .*

1. *a est un majorant de A.*
2. *pour tout $\varepsilon > 0$, il existe un élément x_ε de A tel que $a - \varepsilon < x_\varepsilon \leq a$.*

Preuve

- $\Rightarrow$ On suppose que $a = \sup A$.

  1. Comme A est le plus petit des majorants de A, c'est un majorant de A.
  2. Soit $\epsilon > 0$, si il n'existait pas de $x_\epsilon \in A$ tel que $a - \varepsilon < x_\varepsilon \leq a$, on aurait pour tout $x \in A$, $x \leq a - \varepsilon$. C'est à dire que $a - \varepsilon$ serait un majorant de A, ce qui est absurde puisque a est le plus petit des majorants de A.

- $\Leftarrow$ Réciproquement, soit a un majorant de A tel que pour tout $\varepsilon > 0$, il existe un élément x_ε de A tel que $a - \varepsilon < x_\varepsilon \leq a$. Supposons que a ne soit pas le plus petit des majorants de A. C'est-à-dire qu'il existe $b < a$ tel que $\forall x \in A, x \leq b$. Pour $\varepsilon_0 = a - b > 0$, il n'y a donc pas d'élément x_ϵ de A tel que $b := a - \varepsilon_0 < x_\epsilon < a$, ce qui contredit notre hypothèse. a est donc bien le plus petit des majorant de A, i.e sa borne supérieure

Par symétrie, on obtient:

Propriété 7 *Soit A une partie minorée non vide de $\mathbb{R}$, $c = \inf A$ si et seulement si .*

1. *c est un minorant de A.*
2. *pour tout $\varepsilon > 0$, il existe un élément x_ε de A tel que $c \leq x_\varepsilon < c + \epsilon$.*

5.4.3 Valeur absolue et distance

Definition 57 *On appelle valeur absolue d'un nombre réel x, le réel positif $|x|$ défini par:*

$$|x| = \begin{cases} x & si\ x \geq 0; \\ -x & si\ \ x < 0 \end{cases}$$

.

Proposition 11 *On a*

1. *$|x| = 0$ si et seulement si $x = 0$*
2. *Pour tout $x, y \in \mathbb{R}$: $|xy| = |x||y|$*
3. *Pour tous $x, y \in \mathbb{R}$: $|x + y| < |x| + |y|$*
4. *Pour tous $x, y \in \mathbb{R}$: $||x| - |y|| < |x - y|$*

Definition 58 *La distance (au sens usuel) entre deux réels x et y est définie par $d(x, y) = |x - y|$.*

Proposition 12 *Cette application distance $d : (x, y) \in \mathbb{R}^2 \mapsto d(x, y) \geq 0$ vérifie :*

1. *$\forall x \in \mathbb{R}$, $d(x, x) = 0$;*
2. *$\forall (x, y) \in \mathbb{R}^2$, $d(x, y) = d(y, x)$;*
3. *$\forall (x, y, z) \in \mathbb{R}^3$, $d(x, z) \leq d(x, y) + d(y, z)$ (Inégalité triangulaire);*

Remarque 35 *On a $]x - \epsilon, x + \epsilon[= \{y \in \mathbb{R} \mid d(x, y) < \epsilon\}$*

Remarque 36 *On a $|x| = 0$ si et seulement si $\forall \epsilon > 0, |x| \leq \epsilon$.*

5.5 Nombres complexes

Le corps des nombres complexes, noté $\mathbb{C}$ se construit en munissant $\mathbb{R}^2$ de l'addition naturelle et d'une multiplication. Plus précisément, on note dans cette section $a + ib$ l'élément $(a, b) \in \mathbb{R}^2$. On a alors:

Definition 59 *Le corps des nombres complexes est l'ensemble $\mathbb{R}^2$ muni des opérations suivantes:*

1. *L'addition définie par $(a + ib) + (c + id) = (a + c) + i(b + d)$*
2. *La multiplication définie par $(a + ib) * (c + id) = (ac - bd) + i(ad + bc)$*

Remarque 37 *On identifie $\mathbb{R}$ et le sous ensemble des complexes de la forme $\{a + i0 \mid \ a \in \mathbb{R}\}$. En particulier, on note a pour $a + 0i$. Réciproquement un élément de $\mathbb{C}$ de la forme $0 + ib$ est appelé imaginaire pur et noté ib ou bi. On a en particulier $i * i = i^2 = -1$*

Ces opérations ont les propriétés suivantes:

Proposition 13

1. *L'addition dans $\mathbb{C}$ est associative, commutative et a un élément neutre 0.*
2. *Tout élément a un inverse pour l'addition :*

$$(a + ib) + (-a + i(-b)) = 0$$

3. *La multiplication dans $\mathbb{C}$ est associative commutative, et a un élément neutre 1*

4. Tout élément a un inverse pour la multiplication:

$$(a+ib)*(\frac{a}{a^2+b^2}-i\frac{b}{a^2+b^2})=1$$

Remarque 38 *La notation $a+ib$ est consistante avec les propriétés de l'addition et de la multiplication. C'est à dire qu'on a bien $a+ib=(a+i0)+(0+1i)*(b+0i)$ et on peut appliquer directement les opérations d'addition et de multiplication aux nombres complexes écrits sous cette forme en utilisant les règles naturelles de distributivité.*

Definition 60
- *Le conjugué du nombre complexe $z=a+ib$ est le nombre complexe $\overline{z}=a-ib$.*
- *Le module du nombre complexe $z=(a+ib)$ est $|z|:=\sqrt{z\overline{z}}=\sqrt{a^2+b^2}$*

Proposition 14 *Si z est un nombre complexe de module 1, il existe un unique $\theta\in[0,2\pi]$ tel que $z=\cos(\theta)+i\sin(\theta)$. On note alors $z=e^{i\theta}$*

Démonstration: *Soit $z=a+ib$. on a $|z|=\sqrt{a^2+b^2}=1$, d'où $a^2+b^2=1$. On en déduit que $a\in[-1,1]$. Or $\cos$ est une bijection de $[0,\pi]$ sur $[-1,1]$. Donc il existe $\mu\in[0,\pi]$ tel que $\cos(\mu)=a$. Or, on a $(\cos(\mu))^2+(\sin(\mu))^2=1$. D'où on déduit en utilisant $\cos(\mu)=a$ et $a^2+b^2=1$ que $(\sin(\mu))^2=b^2$. On a donc $\sin(\mu)=b$ auquel cas on pose $\theta=\mu$ ou $\sin(\mu)=-b$ auquel cas on pose $\theta=2\pi-\mu$. On a donc bien $a=\cos(\theta)$ et $b=\sin(\theta)$, soit $z=\cos(\theta)+i\sin(\theta)$.*

Remarque 39 *On a pour tous $\theta,\mu\in[0,2\pi]$ $e^{i\theta}e^{i\mu}=e^{i\theta+\mu}$.*

Proposition 15 *Tout nombre complexe z s'écrit de manière unique sous la forme $z=|z|e^{i\theta}$ avec $\theta\in[0,2\pi]$. On dit alors que z est sous forme trigonométrique.*

Démonstration: *Il suffit de remarquer que $\dfrac{z}{|z|}$ est de module 1.*

6 Polynômes

Dans ce qui suit, $\mathbb{K}=\mathbb{R}$ ou $\mathbb{K}=\mathbb{C}$.

6.1 Définition et opérations

Definition 61 *L'ensemble des polynôme à coefficients dans* $\mathbb{K}$*, noté* $\mathbb{K}[X]$ *est l'ensemble des suites d'éléments de* $\mathbb{K}$ *nulles à partir d'un certain rang. Soit,* $\mathbb{K}[X] := \{(a_n)_{n\in\mathbb{N}} \mid \exists N \in \mathbb{N}\ \forall m \geq N\ a_m = 0\}$*. On note (provisoirement),* $P := (a_0, \cdots, a_N)$ *un tel polynôme. Le terme* a_i *est appelé le coefficient de degré* i *du polynôme et, si le polynôme a au moins un coefficient non nul, le plus grand entier* N *tel que* $a_N \neq 0$ *est appelé le degré du polynôme* P *et noté* $\deg P$

Exemple 37

Le polynôme zéro/nul correspondant à la suite constante nulle, généralement noté 0*.*

Le polynôme $(\lambda, 0, 0, 0 \cdots,)$*, , généralement noté* λ *et appelé polynôme constant* λ

On définit les opérations suivantes sur l'ensemble des polynômes.

Definition 62 (Addition) *La somme de deux polynômes* $P := (a_0, \cdots, a_N)$ *et* $Q := (b_0, \cdots, b_N)$ *est le polynôme noté* $P+Q$ *de degré inférieur à* $\max(\deg P, \deg Q)$ *et dont le coefficient de degré* $i \leq \max(\deg P, \deg Q)$ *est* $a_i + b_i$*.*

Definition 63 (Multiplication) *Le produit de deux polynômes* $P := (a_0, \cdots, a_N)$ *et* $Q := (b_0, \cdots, b_N)$ *est le polynôme noté* PQ *de degré* $\deg P + \deg Q$ *et dont le coefficient de degré* k *est:*

$$c_k := \sum_{i=+j=k} a_i b_j$$

On a en particulier:

$$c_0 = a_0 b_0$$

$$c_1 = a_0 b_1 + a_1 b_0$$

$$c_2 = a_0 b_2 + a_1 b_1 + a_0 b_2$$

Proposition 16

- *L'addition des polynômes est associative, commutative et a pour élément neutre le polynôme*
- *La multiplication des polynômes est commutative, associative, distributive par rapport à l'addition et a pour élément neutre le polynôme constant* 1*.*

Démonstration: *Exercices*

Remarque 40 *Notons X le polynôme $(0,1,0,\cdots)$. On a $X^2 := X * X = (0,0,1,0,\cdots)$ et $X^3 := X * X * X = (0,0,0,1,0,\cdots)$ et par récurrence $X^n := X * X * X * \cdots X = (0,0,0,0,\cdots,0,1,0,\cdots)$. On a alors $a_n X^n = (0,\cdots,0,a_n,0,\cdots)$ et $(a_0,a_1,\cdots,a_n,0,\cdots) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$. Ainsi la définition 61 correspond bien à l'usage. Lorsqu'on note $X = (0,1,0,\cdots)$ et $(a_0,a_1,\cdots,a_n,0,\cdots) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ (ce que nous ferons dans ce qui suit), on parle de polynôme en X, on appelle X l'indéterminée et on note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficient dans $\mathbb{K}$.*

6.2 Division et Factorisation des polynômes

Théorème 10 (Division des polynômes suivant les puissances décroissantes) *Soient A, B dans $\mathbb{K}[X]$ avec $B \neq 0$. Il existe des polynômes Q, R dans $\mathbb{K}[X]$ uniques tels que:*

- $A = BQ + R$
- $\deg(R) < \deg(B)$

Démonstration:

- *Unicité: On suppose que $A = BQ_1 + R_1$ et $A = BQ_2 + R_2$. On en déduit que $BQ_1 + R_1 = BQ_2 + R_2$ puis que $B(Q_1 - Q_2) = R_1 - R_2$. On a donc $Q_1 = Q_2$ et $R_1 = R_2$ ou $Q_1 \neq Q_2$ et $\neq R_2$. Dans le second cas on a $\deg(B) \leq \deg(B(Q_1 - Q_2)) = \deg(R_1 - R_2)$, ce qui est absurde. D'où $Q_1 = Q_2$ et $R_1 = R_2$.*
- *Existence: Soit $A = a_0 + a_1 X + \cdots + a_n X^n$ et $B = b_0 + b_1 X + \cdots b_p X_p$ (avec b_p et a_n non nuls).*
  - *Si $\deg(A) < \deg(B)$, on pose $Q = 0$ et $R = A$.*
  - *Si $\deg(A) \geq \deg(B)$:*
    - *on pose $Q_1 := \frac{a_n}{b_p} X^{n-p}$ et $A_1 = A - Q_1 B$. On a $A = Q_1 B + A_1$ De plus $\deg(A_1) < \deg(A)$. Si $\deg(A_1) < \deg(B)$, on pose $Q = Q_1$ et $R = A_1$,*
    - *Si $\deg(A_1) \geq \deg(B)$, soit $A_1 = d_0 + d_1 X + \cdots + d_q X^q$ (avec $q \geq p$). On pose $Q_2 := \frac{d_q}{b_p} X^{q-p}$ et $A_2 = A_1 - Q_2 B$. On a $A_1 = Q_2 B + A_2$ et $A = Q_1 B + Q_2 B + A_2 = (Q_1 + Q_2)B + A_2$. De plus $\deg(A_2) < \deg(A_1)$. Si $\deg(A_1) < \deg(B)$, on pose $Q = (Q_1 + Q_2)$ et $R = A_2$.*

∗ *Par itération on construit une suite de monômes* $(Q_1, \cdots, Q_k)$ *et* $(A_1, \cdots A_k)$ *tels que* $A = (Q_1 + Q_2 + \cdots + Q_k)B + A_k$ *et* $\deg(A_k) < \deg(A_{k-1})$. *Il est clair qu'on obtient pour un certain* k, $\deg(A_k) < \deg(B)$, *on pose alors* $Q = Q_1 + Q_2 + \cdots + Q_k$ *et* $R = A_k$, *ce qui achève la preuve.*

Exemple 38 $X^4 + 2X^3 - X^2 + 1 = (X^3 + X^2 - 2X + 2)(X + 1) - 1$

Definition 64 *Dans le cadre du théorème* 10, Q *est appelé le quotient et* R *le reste dans la division de* A *par* B. *Si* $R = 0$, *on dit que* B *divise* A *et/ou que* A *est divisible par* B.

Remarque 41

- *Les polynômes constants (i.e de la forme* λ, *où* $\lambda \in \mathbb{R}$) *divisent tout polynôme.*
- *Si* B *divise* A *alors* $\deg(B) \leq \deg(A)$. *Si de plus* $\deg(B) = \deg(A)$, *on a* $B = \lambda A$.

Remarque 42 *Les définitions et résultats suivantes sur l'existence du pgcd, les lemmes de Bezout et de Gauss ainsi que la décomposition en facteurs premiers des polynômes se démontrent de manière quasi-identique au cas des entiers. Ceci découle du fait que l'ensemble des entiers relatifs comme l'ensemble des polynômes (à coefficients réels ou complexes) ont une structure d'anneau euclidien. C'est-à-dire:*

- *Ce sont des groupes abéliens: ils sont munis d'une opération* $+ : E \times E \to E$ *qui est:*
  - *associative: pour tous* $a, b, c \in E$ *on a* $(a + b) + c = a + (b + c)$.
  - *pourvue d'un élément neutre: il existe* $0_E \in E$ *tel que* $a + 0_E = a$.
  - *symétrique: pour tous* $a \in E$, *il existe* $b \in E$ *tel que* $a + b = b + a = 0_E$.
  - *commutative: pour tous* $a, b \in E$, *on a* $a + b = b + a$.
- *Ce sont des anneaux: ils sont munis d'une deuxième opération* $* : E \times E \to E$ *qui est associaitive, possède un élément neutre et est distributive par rapport à l'addition, i.e. pour tous* $a, b, c \in E$ *on a* $a * (b + c) + c = a * b + a * c$ *et* $(a + b) * c = a * c + b * c$.
- *Ce sont des anneaux euclidiens: ils sont munis d'une division euclidienne, i.e d'une application* $v : E \to \mathbb{N}$ *telle que:*

- *Pour tous $a, b \in E$, il ewiste $q, r \in E$ tels que $a = b * q + r$ et $v(r) < v(b)$ ou $r = 0_E$,*
- *Pour tous $a, b \in E/\{0_E\}$, $v(b) \leq v(a * b)$.*

On peut alors vérifier que pour tous les ensembles munis d'une telle structure, on peut définir des notions d'élément premiers, de diviseurs, de multiples... et prouver l'équivalent des lemmes de Bézout et de Gauss et finalement décomposer chaque élément en facteurs premiers;

Proposition 17 (Définition du pgcd) *Soient $A, B \in \mathbb{K}[X]$ non nuls, il existe un unique élément (à un coefficient multiplicatif près) de $\mathbb{K}[X]$ appelé plus grand commun diviseur de A et B et noté $pgcd(A, B)$ tel que tout polynôme qui divise A et B divise D.*

Démonstration: *On a :*

- *$A = BQ_1 + R_1$ avec $\deg(R_1) < \deg(B)$ et il est clair que si D divise A et B alors D divise B.*
- *$B = R_1Q_2 + R_2$ avec $\deg(R_2) < \deg(R_1)$ et il est clair que si D divise B et R_1 alors D divise R_2.*
- *$R_1 = R_2Q_2 + R_3$ avec $\deg(R_3) < \deg(R_2)$ et il est clair que si D divise R_2 et R_1 alors D divise R_3.*
- *Comme les degrés des R_I sont strictement décroissants, on obtient en un nombre fini d'étapes, un premier h tel que $R_{h-1} = QR_h$ et D divise R_h et R_{h-1}.*
- *On remarque alors de proche en proche que R_h divise $R_{h-1}, R_{h-2}, \cdots, B$ et A.*
- *On vient en fait de prouver que $pgcd(A, B) = R_h$.*

Théorème 11 (De Bezout) *Soient $A, B \in \mathbb{K}[X]$. Si $pgcd(A, B) = D$, il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = D$*

Démonstration: *Admis. Voir exercice en TD sur l'algorithme d'Euclide.*

Definition 65 *Deux polynômes A et B sont dits premiers entre eux si $pgcd(A, B) = 1$.*

Théorème 12 *Soient $A, B, C \in \mathbb{K}[X]$, Si A divise BC et A et B sont premiers entre eux, alors A divise C.*

Lemme 3 *Soient $A, B, P \in \mathbb{K}[X]$. Si $D = pgcd(A, B)$, alors $DP = pgcd(AP, BP)$,*

Démonstration: *Il est clair que DP divise AP et BP. Réciproquement, d'après le théorème de Bezout, il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = D$. Donc, si Q divise AP et BP, alors Q divise $AUP + BV = DP$. On en conclut que $DP = pgcd(AP, BP)$,*

Démonstration: *A divise BC et AC et donc divise $pgcd(BC, AC) = C$*

Definition 66 *Un polynôme $P \in \mathbb{K}[X]$ de degré non nul est dit irréductible si ses seuls diviseurs (à la multiplication par une constante près) sont 1 et lui-même.*

Exemple 39

- *Tout polynôme de degré 1 est irréductible.*
- *$X^2 + 1$ est un polynôme irréductible dans $\mathbb{R}[X]$.*
- *$X^2 + 1$ n'est pas un polynôme irréductible dans $\mathbb{C}[X]$.*

Théorème 13 *Soit $P \in \mathbb{K}[X]$ de degré non nul. Alors P s'écrit de manière unique*

$$P = \lambda \prod_{i \in I} P_i^{\alpha_i}$$

où $\lambda \in \mathbb{K}$ est un scalaire, $P_i \in \mathbb{K}[X]$ est un polynôme irréductible et les $\alpha_i \in \mathbb{N}^*$ des entiers.

Démonstration: *On prouve l'existence par récurrence sur le degré de P.*

- *Si $\deg(P) = 0$, la propriété est évidente.*
- *On suppose que la propriété est vraie jusqu'au degré n et on considère P de degré $n + 1$. Si P est irréductible, il n'y a rien à démontrer. Sinon, soit Q un diviseur de P (non constant) de degré minimal. Il est clair que R est irréductible et que $\deg(R) \geq 1$. On a donc $P = QR$ avec R irréductible et on peut appliquer l'hypothèse de récurrence à) Q.*

L'unicité découle des propriétés de divisibilité des polynômes premiers entre eux.

La factorisation d'un polynôme P est en fait étroitement liée à la recherche des solutions de l'équation $P(x) = 0$.

Definition 67 *Un scalaire $\rho \in K$ est une racine du polynôme $P \in \mathbb{K}[X]$ si $P(\rho) = 0$.*

Théorème 14 *Soit $P \in \mathbb{K}[X]$ et $\rho \in \mathbb{K}$. Pour que ρ soit une racine de P il faut et il suffit que $(X - \rho)$ divise P.*

Démonstration:

- *Si $(X - \rho)$ divise P, il existe $Q \in \mathbb{K}[X]$ tel que $P = Q(X - \rho)$. On a clairement $P(\rho) = 0$.*
- *Réciproquement, si ρ est une racine de P, P est de degré non nul et sa division par $(X - \rho)$ s'écrit $P = Q(X - \rho) + \mu$ où $\mu \in \mathbb{K}$. On a de plus $0 = P(\rho) = \mu$, d'où on déduit que$(X - \rho)$ divise P.*

Corollaire 2 *Soit $P \in \mathbb{K}[X]$ et ρ une racine de P, il existe un plus grand entier n tel que P soit divisible par $(X - \rho)^n$. On a alors $P = (X - \rho)^n Q$ où Q n'admet pas ρ comme racine. L'entier n est appelé la multiplicité de la racine ρ.*

Démonstration: *Comme ρ est une racine de P, on sait que $P = (X-\rho)Q_1$. Si Q_1 n'est pas divisible par ρ, on a $n = 1$, sinon on a $n \geq 2$ et $P = (X-\rho)Q_2$ avec $\deg(Q_2) < \deg(Q_1)$. Si Q_2 n'est pas divisible par ρ, on a $n = 2$, sinon on itère l'algorithme et on obtient en un nombre fini d'étapes (car le degré de P est fini) que $P = (X - \rho)^n Q$ avec Q non divisible par ρ.*

Théorème 15 *Soit $P \in \mathbb{K}[X]$ et $\rho_1, \cdots, \rho_k$ des racines distinctes de P de multiplicité $n_1, \cdots, n_k$, alors*

$$P(X) = (X - \rho_1)^{n_1} \cdots (X - \rho_k)^{n_k} Q(X)$$

où Q est un élément de $Q(X)$ n'admettant pas les racines $\rho_1, \cdots, \rho_k$.

Démonstration: *Par récurrence sur lie nombre de racines. Le théorème précédent donne l'initiailisation. L'hérédité utilise les propriétés de divisibilité.*

Corollaire 3 *Un polynôme $P \in \mathbb{K}[X]$ de degré n ne peut avoir plus de n racines.*

Corollaire 4 *Soit un polynôme $P \in \mathbb{K}[X]$ de degré n tel que p admet n racines $\rho_1, \cdots, \rho_n$ (comptées avec leur multiplicité). On a alors*

$$P(X) = \lambda(X - \rho_1) \cdots (X - \rho_n)$$

où λ est le coefficient de degré n de P.

Théorème 16 (théorème fondamental de l'algèbre) *Tout polynôme de* $\mathbb{C}[X]$ *de degré supérieur ou égal à* 1 *admet au moins une racine dans* $\mathbb{C}$

Démonstration: *admis*

Théorème 17 (Décomposition en facteurs irréductibles d'un polynôme dans C) *Soit* $P \in \mathbb{C}[X]$ *de degré* n*, alors* P *admet* n *racines* $\rho_1, \cdots, \rho_n$ *(comptées avec leur multiplicité et donc pas forcément distinctes) et on a*

$$P(X) = \lambda(X - \rho_1) \cdots (X - \rho_n)$$

où λ *est le coefficient de degré* n *de* P*.*

Démonstration: *Par récurrence, en utilisant le théorème fondamental de l'algèbre.*

Definition 68 *Soit* $P \in \mathbb{C}[X]$ *tel que* $P = \sum_{i=0}^{n} a_i X^i$*. On appelle polynôme conjugué de* P *et on note* $\overline{P}$*, le polynôme de* $\mathbb{C}[X]$ *défini par* $\overline{P} = \sum_{i=0}^{n} \overline{a_i} X^i$*.*

Lemme 4 *Soit* $P \in \mathbb{C}[X]$*, on a:*

1. P *divisible par* $Q \Leftrightarrow \overline{P}$ *divisible par* $\overline{Q}$*.*
2. ρ *racine de multiplicité* h *de* $P \Leftrightarrow \overline{\rho}$ *racine de multiplicité* h *de* $\overline{P}$
3. *Si* P *est à coefficients réels,* ρ *racine de multiplicité* h *de* $P \Leftrightarrow \overline{\rho}$ *racine de multiplicité* h *de* P*.*

Démonstration: *exercice*

Proposition 14 *Les polynômes irréductibles de degré* 2 *sont (i) les polynômes du premier degré, (ii) les polynômes du second degré à discriminant négatif.*

Théorème 18 (Décomposition d'un polynôme réel) *Soit* $P \in \mathbb{R}[X]$ *de degré* n*, il existe* $p, q \in \mathbb{N}$ *tel que* $n = p + 2q$ *et* P *admet* p *racines réelles (comptées avec leur multiplicité et donc pas forcément distinctes)* $\rho_1, \cdots, \rho_p$ *et* $2q$ *racines complexes conjuguées (comptées avec leur multiplicité et donc pas forcément distinctes)* $\mu_1, \cdots, \mu_q$ *et* $\overline{\mu_1}, \cdots, \overline{\mu_q}$*. On a alors:*

1. $$P(X) = \lambda(X-\rho_1)\cdots(X-\rho_p)(X-\mu_1)\cdots(X-\mu_q)(X-\overline{\mu}_1)\cdots(X-\overline{\mu}_q)$$
2. $$P(X) = \lambda(X - \rho_1) \cdots (X - \rho_p) Q_1(X) Q_q(X)$$
   où $Q_j(X) = X^2 - (\mu_j + \overline{\mu}_j)X + \mu_j\overline{\mu}_j$ *est un polynôme irréductible de* $\mathbb{R}[X]$ *de degré* 2*.*