Préparation à l'agrégation externe de Mathématiques 2026-2027
Université Paris Cité-Grands Moulins

Ensembles, Relations, Construction de $\mathbb{N}$, Notion de cardinalité

Muriel Livernet

Table des matières

Fichier mis à jour le 1er septembre, corrections de quelques typos

1. Ensembles

Définition 1.1. Soit E un ensemble.

- L'ensemble *des parties de* E est noté $\mathcal{P}(E) = \{A \mid A \subset E\}$. Traduction : $A \in \mathcal{P}(E) \iff A \subset E$.
- *Inclusion, égalité* : soient $A, B \in \mathcal{P}(E)$. $A \subset B$ signifie que tout élément de A est aussi un élément de B. Traduction : $A \subset E \Leftrightarrow \forall x \in E,\ x \in A \Rightarrow x \in B$. Conséquence : $A = B \iff (A \subset B)$ et $(B \subset A)$.
- *Complémentaire* de A dans E : ${}^cA = \{x \in E \mid x \notin A\}$.
- *Union, intersection de parties de* E : soit $(A_i)_{i\in I}$ une famille quelconque d'éléments de $\mathcal{P}(E)$. On définit l'union comme étant l'ensemble $\cup_{i\in I} A_i = \{x \in E \mid \exists i, x \in A_i\}$ et l'intersection comme étant l'ensemble $\cap_{i\in I} A_i = \{x \in E \mid \forall i, x \in A_i\}$.
- *Partition de* E : une famille $(A_i)_{i\in I}$ d'éléments de $\mathcal{P}(E)$ est une partition de E si les A_i sont disjoints deux à deux et si leur union est E. Traduction : $E = \cup_{i\in I} A_i$ et pour tout $i \neq j$ on a $A_i \cap A_j = \emptyset$. On note aussi $E = \sqcup_{i\in I} A_i$.
- *Produit cartésien de deux ensembles* : Soient E et F des ensembles. On définit le produit cartésien $E \times F = \{(x, y) \mid x \in E \text{ et } y \in F\}$.

Proposition 1.2. *L'intersection, la réunion et le produit cartésien sont des opérations associatives.*

L'intersection et la réunion sont des opérations commutatives.

L'intersection est distributive par rapport à la réunion et la réunion est distributive par rapport à l'intersection.

L'opéraction complémentaire : $\mathcal{P}(E) \to \mathcal{P}(E)$ *est involutive et envoie union sur intersection et intersection sur union.*

Exercice 1.3. En considérant les ensembles $A = \{x \in \mathbb{R} \mid x \geq 1 \text{ et } x < 4\}$ et $B = \{x \in \mathbb{R} \mid x < -1 \text{ ou } x \geq 2\}$, montrer que $A \times B \neq B \times A$.

Cet exercice permet de prendre conscience que bien que ces deux ensembles ne soient pas égaux, ils sont comparables. Pour les comparer, on a besoin de la notion d'applications et parmi celles-ci les applications bijectives jouent un grand rôle. On verra dans la section 7 que cela permet de définir la notion de cardinal.

Beaucoup de structures sur les ensembles ont été introduites : groupes, anneaux, corps, espaces vectoriels, espaces topologiques et à chaque notion correspond une notion de comparaison : morphisme de groupes, d'anneaux, corps, applications linéaires, applications continues. Pour chaque notion de morphisme, il y a une notion d'isomorphisme. Dans le cadre algébrique ce sont les morphismes bijectifs. Mais dans le cadre topologique un isomorphisme est un homéomorphisme, notion plus forte que celle d'application continue bijective.

2. Lien entre ensembles et logique

Si P **est une propriété portant sur les éléments d'un ensemble** E**, on peut définir le sous-ensemble des éléments de** E **qui vérifient la propriété** P**. Si l'on note** A **ce sous-ensemble, on écrit**

$$A = \{x \in E \mid \mathrm{P}(x) \textbf{ est vraie}\} = \{x \in E \mid \mathrm{P}(x)\}.$$

Cette écriture formelle se lit donc "A **est l'ensemble des éléments** x **de** E **pour lesquels la propriété** $\mathrm{P}(x)$ **est vraie". Soient** P **et** Q **deux propriétés portant sur des éléments d'un ensemble** E**. On définit les sous-ensembles** A **et** B **comme suit :**

$$A = \{x \in E \mid \mathrm{P}(x)\} \qquad \textbf{et} \qquad B = \{x \in E \mid \mathrm{Q}(x)\}.$$

L'union des sous-ensembles A **et** B **est l'ensemble** $\{x \in E \mid \mathrm{P}(x) \vee \mathrm{Q}(x)\}$**.**
L'intersection des sous-ensembles A **et** B **est l'ensemble** $\{x \in E \mid P(x) \wedge \mathrm{Q}(x)\}$**.**
Le complémentaire du sous-ensemble A **est l'ensemble** $\{x \in E \mid \neg \mathrm{P}(x)\}$**.**
De plus, l'inclusion $A \subseteq B$ **est équivalente à la proposition** P **implique** Q**.**
L'égalité $A = B$ **est équivalente à la proposition** P **équivaut à** Q**.**

On rappelle également la table de vérité des opérateurs logiques les plus courants.

P	Q	$\neg\mathrm{P}$	$\mathrm{P} \wedge \mathrm{Q}$	$\mathrm{P} \vee \mathrm{Q}$	$\mathrm{P} \Rightarrow \mathrm{Q}$	$\mathrm{P} \Leftrightarrow \mathrm{Q}$
V	**V**	**F**	**V**	**V**	**V**	**V**
V	**F**	**F**	**F**	**V**	**F**	**F**
F	**V**	**V**	**F**	**V**	**V**	**F**
F	**F**	**V**	**F**	**F**	**V**	**V**

En étudiant les tables de vérité on montre :

$$\Big(\mathrm{P} \Rightarrow \mathrm{Q}\Big) \Longleftrightarrow \Big(\neg\mathrm{P} \vee \mathrm{Q}\Big).$$

$$\Big(\mathrm{P} \Rightarrow \mathrm{Q}\Big) \Longleftrightarrow \Big(\neg\mathrm{Q} \Rightarrow \neg\mathrm{P}\Big).$$

$$\neg(\mathrm{P} \Rightarrow \mathrm{Q}) \iff \Big(\mathrm{P} \wedge \neg\mathrm{Q}\Big).$$

On rappelle également que prouver $\neg\mathrm{Q} \Rightarrow \neg\mathrm{P}$ pour prouver $\mathrm{P} \Longrightarrow \mathrm{Q}$ s'appelle le *raisonnement par contraposée*, et que prouver $\mathrm{P} \wedge \neg\mathrm{Q}$ pour montrer $\neg(\mathrm{P} \Rightarrow \mathrm{Q})$ s'appelle le *raisonnement par contre-exemple*.

3. Applications

Définition 3.1. Soient E et F des ensembles, f est une *application* de E dans F si et seulement si f associe à tout élément x de E un et un seul élément de F appelé *image* de x et noté $f(x)$. E est appelé *ensemble de départ* de f et F *ensemble d'arrivée*. Soit $y \in F$, tout élément x de E dont l'image est y (i.e. $f(x) = y$) est appelé *antécédent* de y (par f).

Définition 3.2. Soient $f : E \to F$ une application. Pour tout $A \in \mathcal{P}(E)$ on définit *l'image directe de A* (ou *image de A par f*) comme $f(A) = \{f(x) \mid x \in A\} \subset F$. Autrement dit $\forall y \in F,\ y \in f(A) \iff \exists x \in A,\ y = f(x)$.

Pour tout $B \in \mathcal{P}(F)$, *l'image réciproque* de B par f est l'ensemble $\{x \in E \mid f(x) \in B\} \subset E$. Il est malheureusement noté $f^{-1}(B)$, mais ATTENTION, ce n'est qu'une notation, et cela ne veut pas dire que f admet une application réciproque. On a

$$x \in f^{-1}(B) \iff f(x) \in B$$

Définition 3.3. Soit $f : E \to F$ une application. On dit que

- f est *surjective* ou *est une surjection* si tout élément de F admet **au moins** un antécédent par f. En écriture mathématique cela donne, f est surjective si et seulement si

$$\begin{aligned} &\forall y \in F, f^{-1}(\{y\}) \neq \emptyset \\ \iff &\forall y \in F,\ \exists x \in E,\ y = f(x) \\ \iff &f(E) = F. \end{aligned}$$

- f est *injective* ou *est une injection* si tout élément de F admet **au plus** un antécédent par f. En écriture mathématique cela donne, f est injective si et seulement si

$$\begin{aligned} &\forall x, y \in E,\ f(x) = f(y) \Rightarrow x = y \\ \iff &\forall x, y \in E,\ x \neq y \Rightarrow f(x) \neq f(y). \end{aligned}$$

- f est *bijective* ou *est une bijection* si tout élément de F admet **un unique** antécédent par f, c'est-à-dire que f est à la fois surjective et injective.

Remarque 3.4. Si $f : E \to F$ est une bijection, on peut construire une application $g : F \to E$ qui à $y \in F$ associe l'unique antécédent de y par f. Cela définit bien une application.

Définition 3.5. Soient $f : E \to F$ et $g : F \to G$ deux applications. La composée de f et g est l'application $g \circ f : E \to G$ définie par $(g \circ f)(x) = g(f(x))$.

Exercice 3.6. Soient $f : E \to F$ et $g : F \to G$ deux applications. Soit $A \in \mathcal{P}(E), C \in \mathcal{P}(G)$. On a $(g \circ f)(A) = g(f(A))$ et $(g \circ f)^{-1}(C) = f^{-1}(g^{-1}(C))$.

Proposition 3.7. *Soient $f : E \to F$ et $g : F \to G$ deux applications.*

(1) *Si f est surjective alors g est surjective si et seulement si $g \circ f$ est surjective.*

(2) *Si g est injective alors f est injective si et seulement si $g \circ f$ est injective.*

(3) *Si 2 parmi les 3 applications f, g et $g \circ f$ sont bijectives alors la troisième l'est aussi.*

Exercice 3.8. Sous les hypothèses de la proposition ci-dessus, montrer que si g est injective et $g \circ f$ est surjective alors f est surjective ; montrer que si f est surjective et $g \circ f$ est injective alors g est injective.

Proposition 3.9. *Soit $f : E \to F$ une application. f est bijective si et seulement si il existe $g : F \to E$ telle que $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$. De plus g est unique et est l'application décrite en remarque 3.4. Elle est notée f^{-1}.*

4. Relation d'équivalence

Définition 4.1. Soit E un ensemble. On appelle *relation binaire* $\mathcal{R}$ dans E un sous-ensemble G de $E \times E$ appelé *graphe de la relation.*

Notation : pour $x, y \in E$ on a $x\mathcal{R}y$ si et seulement si $(x, y) \in G$.

La relation est dite

— *réflexive* si $\forall x \in E,\ x\mathcal{R}x$ $((x, x) \in G)$

— *symétrique* si $\forall x, y \in E,\ x\mathcal{R}y \Rightarrow y\mathcal{R}x$ $((x, y) \in G \Rightarrow (y, x) \in G)$.

— *antisymétrique* si $\forall x, y \in E,\ x\mathcal{R}y$ et $y\mathcal{R}x \Rightarrow x = y$ $((x, y) \in G$ et $(y, x) \in G \Rightarrow x = y)$.

— *transitive* si $\forall x, y, z \in E,\ x\mathcal{R}y$ et $y\mathcal{R}z \Rightarrow x\mathcal{R}z$ $((x, y) \in G$ et $(y, z) \in G \Rightarrow (x, z) \in G)$.

— *totale* si $\forall x, y \in E,\ x\mathcal{R}y$ ou $y\mathcal{R}x$ ou *partielle* si elle n'est pas totale.

Exemples 4.2. La relation "$x = y$" est partielle ainsi que la relation "a divise b" dans $\mathbb{N}$. La relation "a divise b" est antisymétrique dans $\mathbb{N}$, mais elle ne l'est pas dans $\mathbb{Z}$: en effet, si a divise b et b divise a dans $\mathbb{Z}$ alors $a = \pm b$.

Définition 4.3. Soit E un ensemble. On appelle *relation d'équivalence* toute relation binaire $\mathcal{R}$ sur E qui est réflexive, symétrique et transitive. Soit $x \in E$. On appelle *classe d'équivalence de x modulo $\mathcal{R}$* le sous-ensemble de E défini par

$$[x]_{\mathcal{R}} = \bar{x} = \mathrm{cl}_{\mathcal{R}}(x) := \{y \in E \mid y\mathcal{R}x\}.$$

On appelle *ensemble quotient de E par la relation $\mathcal{R}$* que l'on note $E/\mathcal{R}$ l'ensemble des classes d'équivalence pour la relation $\mathcal{R}$. Autrement dit

$$E/\mathcal{R} = \{\mathrm{cl}_{\mathcal{R}}(x) \mid x \in E\}$$

On note $q_{\mathcal{R}} : E \to E/\mathcal{R}$ l'application quotient, qui est surjective. Un *système complet de représentants de E pour $\mathcal{R}$* est un sous-ensemble de E en bijection avec l'ensemble quotient $E/\mathcal{R}$. De manière équivalente c'est un sous-ensemble X de E tel que l'application quotient $q_{\mathcal{R}}$ restreinte à X soit une bijection.

Remarque 4.4. L'existence d'un système complet de représentants (pour n'importe quel relation d'équivalence) nécessite l'axiome du choix, car cela équivaut à se donner une fonction de choix $s : E/\mathcal{R} \to E$ qui à $A \in E/\mathcal{R}$ associe $s(A) \in A$. Dans tous les exemples que nous allons rencontrer on n'aura pas besoin de l'axiome du choix car on saura décrire un système complet de représentants.

Théorème 4.5. *Soit $\mathcal{R}$ une relation d'équivalence sur E. Les classes d'équivalence modulo $\mathcal{R}$ forment une partition de E. Réciproquement, si $P = \{A_i\}_{i\in I}$ est une partition de E alors il existe une relation d'équivalence $\mathcal{R}$ sur E et une bijection entre $E/\mathcal{R}$ et P.*

Démonstration. Il est clair que $E = \cup_{x\in E}\mathrm{cl}_{\mathcal{R}}(x)$. Montrons que soit $\mathrm{cl}_{\mathcal{R}}(x) = \mathrm{cl}_{\mathcal{R}}(y)$ soit $\mathrm{cl}_{\mathcal{R}}(x) \cap \mathrm{cl}_{\mathcal{R}}(y) = \emptyset$. Si $\mathrm{cl}_{\mathcal{R}}(x) \cap \mathrm{cl}_{\mathcal{R}}(y) \neq \emptyset$ alors il existe z dans l'intersection. On a $z\mathcal{R}x$ et $z\mathcal{R}y$ et en utilisant la symétrie et la transitivité on obtient $y\mathcal{R}x$ donc $y \in \mathrm{cl}_{\mathcal{R}}(x)$. Si $z \in \mathrm{cl}_{\mathcal{R}}(y)$, comme $z\mathcal{R}y$ et $y\mathcal{R}x$, alors on a $z\mathcal{R}x$ donc $z \in \mathrm{cl}_{\mathcal{R}}(x)$. On a montré que $\mathrm{cl}_{\mathcal{R}}(y) \subset \mathrm{cl}_{\mathcal{R}}(x)$. Par symétrie on obtient $\mathrm{cl}_{\mathcal{R}}(x) \subset \mathrm{cl}_{\mathcal{R}}(y)$ d'où l'égalité des deux ensembles. Réciproquement, on définit la relation sur E par $x\mathcal{R}y \Leftrightarrow \exists i \in I,\ x \in A_i \wedge y \in A_i$. C'est une relation d'équivalence et pour tout $x \in E$ il existe un unique $i \in I$ tel que $\mathrm{cl}_{\mathcal{R}}(x) = A_i$ ce qui donne la bijection voulue. □

Exemples 4.6. Soit $\mathbb{K}$ un corps, E et F des $\mathbb{K}$-espaces vectoriels de dimension n et m respectivement. En fixant une base de E et de F on a un isomorphisme de $\mathbb{K}$-espaces vectoriels entre le $\mathbb{K}$-espace vectoriel des applications linéaires de E vers F et le $\mathbb{K}$-espace vectoriel des matrices de taille $m \times n$ à coefficients dans $\mathbb{K}$, noté $M_{m,n}(\mathbb{K})$. La relation "matrices équivalentes" ($B = PAQ^{-1}$, P, Q inversibles) est une relation d'équivalence. Comme deux matrices sont équivalentes si et seulement si elles ont même rang, les classes d'équivalence pour cette relation sont en bijection avec l'ensemble des entiers $\{0, 1, \ldots, p\}$ où $p = \min\{m, n\}$.

Si $m = n$, la relation "matrices semblables" ($B = PAP^{-1}$, P inversible) est une relation d'équivalence. Un *invariant de similitude* est une application $f : M_n(\mathbb{K}) \to F$ pour F un certain ensemble qui est constante sur les classes d'équivalence modulo la relation de similitude. Par exemple : la trace, le déterminant, le polynôme caractéristique, le polynôme minimal sont des invariants de similitude.

Exemple 4.7 (L'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$.). Dans $\mathbb{Z}$, on dit que x *est congru à* y *modulo* n si n divise $x - y$. La relation "être congru à" est une relation d'équivalence et l'ensemble quotient est noté $\mathbb{Z}/n\mathbb{Z}$. Un système de représentants est $\{0, 1, \ldots, n-1\}$. Si n est impair, un autre système de représentants est $\{-\frac{n-1}{2}, -\frac{n-1}{2}+1, \ldots, 0, 1, \ldots, \frac{n-1}{2}-1, \frac{n-1}{2}\}$. Les éléments de $\mathbb{Z}/n\mathbb{Z}$ sont les ensembles $\overline{0} = \{kn,\ k \in \mathbb{Z}\}$, $\overline{1} = \{1 + kn,\ k \in \mathbb{Z}\}, \ldots,$ $\overline{n-1} = \{n - 1 + kn,\ k \in \mathbb{Z}\}$.

Soient E et F des ensembles, $\mathcal{R}$ une relation d'équivalence sur E et $f : E \to F$ une application. Notons $\pi : E \to E/\mathcal{R}$ l'application quotient. On suppose que f est *constante sur les classes d'équivalence*, c'est-à-dire que $x\,\mathcal{R}\,y \Rightarrow f(x) = f(y)$. Alors, pour $A = \mathrm{cl}_{\mathcal{R}}(x) \in E/\mathcal{R}$ on peut poser $\overline{f}(A) = f(x)$. On obtient ainsi une application $\overline{f} : E/\mathcal{R} \to F$ et l'on a $f = \overline{f} \circ \pi$. L'application $\overline{f}$ ainsi construite s'appelle *l'application déduite de f par passage au quotient.*

On note $\mathcal{R}_f$ la relation d'équivalence sur E donnée par $x\mathcal{R}_f y \Leftrightarrow f(x) = f(y)$. La proposition suivante compare $\mathcal{R}$ et $\mathcal{R}_f$.

Proposition 4.8. *Soit $f : E \to F$ une application et $\mathcal{R}$ une relation d'équivalence sur E.*

(1) f est constante sur les classes d'équivalence modulo $\mathcal{R}$ si et seulement si

$$\forall x, y \in E,\ x\mathcal{R}y \Longrightarrow x\mathcal{R}_f y.$$

(2) L'application $\tilde{f} : E/\mathcal{R}_f \to F$ est bien définie et injective.

(3) Réciproquement, si f est constante sur les classes d'équivalence modulo $\mathcal{R}$, alors l'application $\overline{f} : E/\mathcal{R} \to F$ est injective si et seulement si

$$\forall x, y \in E,\ x\mathcal{R}y \iff x\mathcal{R}_f y.$$

Démonstration.

(1) Par définition, f est constante sur les classes d'équivalence modulo $\mathcal{R}$ si

$$\forall x, y \in E,\ x\mathcal{R}y \implies f(x) = f(y)$$

puis on remarque que $f(x) = f(y)$ si et seulement si $x\mathcal{R}_f y$.

(2) L'application $\tilde{f} : E/\mathcal{R}_f \to F$ est bien définie car f est constante sur les classes d'équivalence modulo $\mathcal{R}_f$. Montrons que $\tilde{f}$ et injective. Soient $A = \mathrm{cl}_{\mathcal{R}_f}(x)$ et $B = \mathrm{cl}_{\mathcal{R}_f}(y)$ deux éléments de $E/\mathcal{R}_f$ tels que $\tilde{f}(A) = \tilde{f}(B)$. Comme $\tilde{f}(A) = f(x)$ et $\tilde{f}(B) = f(y)$ on en déduit $f(x) = f(y)$. Donc $x\mathcal{R}_f y$ et $A = B$.

(3) Comme par hypothèse, f est constante sur les classes d'équivalence modulo $\mathcal{R}$, par le point (1) on a $\forall x, y \in E,\ x\mathcal{R}y \Rightarrow x\mathcal{R}_f y$. Supposons $\overline{f}$ injective et montrons

$$\forall x, y \in E,\ x\mathcal{R}_f y \Rightarrow x\mathcal{R}y$$

Si $x\mathcal{R}_f y$ alors $f(x) = f(y)$ donc $\overline{f}(\mathrm{cl}_{\mathcal{R}}(x)) = \overline{f}(\mathrm{cl}_{\mathcal{R}}(y))$. Par injectivité de $\overline{f}$, on déduit $\mathrm{cl}_{\mathcal{R}}(x) = \mathrm{cl}_{\mathcal{R}}(y)$, donc $x\mathcal{R}y$. Réciproquement, supposons, $\forall x, y \in E,\ x\mathcal{R}_f y \Rightarrow x\mathcal{R}y$ et supposons $\overline{f}(A) = \overline{f}(B)$ avec $A = \mathrm{cl}_{\mathcal{R}}(x)$ et $B = \mathrm{cl}_{\mathcal{R}}(y)$. Par définition de l'application $\overline{f}$ on obtient $f(x) = f(y)$ donc $x\mathcal{R}_f y$ et par hypothèse $x\mathcal{R}y$. Ce qui donne $A = B$ et permet de conclure que $\overline{f}$ est injective. □

Définition 4.9. Soit $f : E \to F$ une application. Alors $f = \overline{f} \circ \pi$ avec $\overline{f} : E/\mathcal{R}_f \to F$ injective et $\pi : E \to E/\mathcal{R}_f$ surjective. On dit que cette décomposition est **canonique** car elle ne dépend que de f.

Proposition 4.10 (Décomposition canonique 2)**.** *Soit $f : E \to F$ une application. f se décompose de façon* **canonique** *en $f = j \circ \check{f} \circ \pi$ avec $\pi : E \to E/\mathcal{R}_f$ la projection canonique (surjective), $\check{f} : E/\mathcal{R}_f \to f(E)$ définie par $\check{f}(\mathrm{cl}_{\mathcal{R}_f}(x)) = f(x)$ bijective et $j : f(E) \to F$ l'inclusion canonique d'ensembles.*

Démonstration. On a déjà décomposé $f = \overline{f} \circ \pi$ de manière canonique avec $\overline{f} : E/\mathcal{R}_f \to F$ injective. Remarquons que $\overline{f}(E/\mathcal{R}_f) = f(E)$ donc on peut restreindre l'espace d'arrivée et factoriser $\overline{f} = j \circ \check{f}$ avec $\check{f} : E/\mathcal{R}_f \to f(E)$ définie par $\check{f}(A) = \overline{f}(A)$. Il est clair que $\check{f}$ est injective car $\overline{f}$ l'est et qu'elle est surjective puisque $\check{f}(E/\mathcal{R}_f) = \overline{f}(E/\mathcal{R}_f) = f(E)$. □

Remarque 4.11. Dans la pratique on se donne $f : E \to F$ et on dit que f induit une bijection $\check{f} : E/\mathcal{R}_f \to f(E)$ donnée par $\check{f}(\mathrm{cl}_{\mathcal{R}_f}(x)) = f(x)$.

Exemple 4.12. Soit $f : \mathbb{R} \to \mathbb{C}$ l'application $t \mapsto e^{2it\pi}$. Pour $s, t \in \mathbb{R}$, on a

$$f(s) = f(t) \iff e^{2i(s-t)\pi} = 1 \iff s - t \in \mathbb{Z}.$$

La relation $\mathcal{R}_f$ est donc la relation $\equiv_{\mathbb{Z}}$ définie par $s \equiv_{\mathbb{Z}} t \Leftrightarrow s - t \in \mathbb{Z}$. Par ailleurs, $f(\mathbb{R})$ est l'ensemble $\mathbb{U}$ des nombres complexes de module 1. On obtient une bijection $\check{f} : \mathbb{R}/\equiv_{\mathbb{Z}} \to \mathbb{U}$.

5. Relation d'ordre

Définition 5.1. Soit E un ensemble. On appelle *relation d'ordre* toute relation binaire $\mathcal{R}$ sur E qui est réflexive, antisymétrique et transitive. Souvent on note "$\leq$" cette relation et $(E, \leq)$ est appelé *ensemble ordonné*. L'ordre est *total* si la relation est totale, *partiel* dans le cas contraire.

Exemples 5.2. $(\mathcal{P}(E), \subset)$ est un ensemble ordonné, l'ordre est partiel. De même pour l'ensemble $(\mathbb{N}, ''\, divise'')$.

Définition 5.3. Soit $(E, \leq)$ un ensemble ordonné. Soit $A \subset E$.

majorant, minorant, borne supérieure, borne inférieure : on dit que $M \in E$ est UN majorant de A si pour tout $a \in A$ on a $a \leq M$. On dit que $m \in E$ est UN minorant de A si pour tout $a \in A$ on a $m \leq a$. S'il existe, le plus petit des majorants de A est unique et s'appelle *borne supérieure* de A. S'il existe, le plus grand des minorants de A est unique et s'appelle *borne inférieure* de A.

plus grand élément, plus petit élément : s'il existe un majorant M de A qui appartient à A, alors il est unique et on l'appelle LE plus grand élément de A. S'il existe un minorant m de A qui appartient à A, alors il est unique et on l'appelle LE plus petit élément de A.

élément maximal, élément minimal : on dit que $P \in A$ est UN élément maximal de A si $\forall a \in A, P \leq a \Rightarrow a = P$. On dit que $p \in A$ est UN élément minimal de A si $\forall a \in A, a \leq p \Rightarrow a = p$.

6. L'ensemble $\mathbb{N}$, esquisse de construction

L'ensemble $\mathbb{N}$ des entiers naturels est à la base de la construction des autres ensembles de nombres $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. Son existence est axiomatique (c'est-à-dire admise et non pas démontrée). Il existe deux axiomatiques équivalentes : *l'axiomatique ordinale* qui permet de démontrer le principe de récurrence et l'autre présentée avec les *axiomes de Peano* dont le principe de récurrence en est un axiome. On présente l'axiomatique ordinale.

6.1. **Axiomatique ordinale. On admet l'existence d'un ensemble ordonné $\mathbb{N}$, non vide vérifiant les axiomes suivants :**

(A1) Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
(A2) Toute partie non vide majorée de $\mathbb{N}$ admet un plus grand élément.
(A3) L'ensemble $\mathbb{N}$ est non majoré.

6.1.1. *Conséquences immédiates.*

- **L'ensemble $\mathbb{N}$ est totalement ordonné. En effet, si $p, q \in \mathbb{N}$ alors le sous-ensemble $\{p, q\}$ admet un plus petit élément : si c'est p alors $p \leq q$ et si c'est q alors $q \leq p$.**
- **On note 0 le plus petit élément de $\mathbb{N}$ (existe d'après (A1)). Fixons $n \in \mathbb{N}$. Alors $\{k \in \mathbb{N}, k > n\}$ n'est pas vide d'après (A3) donc admet un plus petit élément d'après (A1). On le note $s(n)$, s pour *successeur*.**
- **De même si $n > 0$ l'ensemble $\{k \in \mathbb{N}, k < n\}$ est non vide et majoré donc il admet un plus grand élément d'après (A2). On le note $p(n)$, p pour *prédécesseur*.**

On note $\mathbb{N}^* = \mathbb{N}\backslash\{0\}$. Remarquez que $\mathbb{N}^*$ vérifie les axiomes $(A1), (A2), (A3)$. Les applications $s : \mathbb{N} \to \mathbb{N}^*$ et $p : \mathbb{N}^* \to \mathbb{N}$ sont inverses l'une de l'autre.

6.1.2. *Corollaire : le principe de récurrence. Soit $E \subset \mathbb{N}$. Si $0 \in E$ et si l'implication*

$$n \in E \Rightarrow s(n) \in E$$

est vraie alors $E = \mathbb{N}$.

Démonstration. Soit F le complémentaire de E dans $\mathbb{N}$. On raisonne par l'absurde en supposant que F est non vide. Donc il admet un plus petit élément $n_0 \neq 0$ car $0 \in E$. Comme $p(n_0) < n_0$ on a $p(n_0) \in E$ et donc $s(p(n_0)) = n_0 \in E$ ce qui est absurde car $n_0 \in F$. Donc F est vide. □

6.1.3. *Unicité de $\mathbb{N}$ à isomorphisme ordonné près.* **Grâce au principe de récurrence, on peut montrer que l'ensemble $\mathbb{N}$ est unique à isomorphisme d'ensembles ordonnés près. Si Δ est un ensemble qui vérifie les axiomes $(A1), (A2)$ et $(A3)$ alors on peut définir δ son plus petit élément et σ, π ses applications successeur et prédecesseur puis construire par récurrence une bijection croissante : $\phi : \mathbb{N} \to \Delta$ qui à 0 associe δ et à $s(n)$ associe $\sigma(\phi(n))$. On choisit alors un tel ensemble $\mathbb{N}$ et on l'appelle** *ensemble des entiers naturels*.

6.2. **Construction des opérations dans $\mathbb{N}$.**

6.2.1. *L'addition.* **On définit une loi $+$ interne par récurrence en posant**

$$\forall n \in \mathbb{N},\ n + 0 = n \quad \forall n, m \in \mathbb{N},\ n + s(m) = s(n + m).$$

On peut alors montrer que la loi $+$ est associative, commutative, et compatible avec la relation d'ordre. Si l'on pose $1 = s(0)$ alors $s(n) = n + 1$. On peut construire également la soustraction $a - b$ si $a \geq b$ en posant $a - 1 = p(a)$.

Le principe de récurrence est équivalent à l'énoncé suivant. On note $\mathcal{P}(n)$ une propriété qui dépend de l'élément n dans $\mathbb{N}$.

6.2.2. *Principe de récurrence. Si $\mathcal{P}(0)$ est vrai et si l'implication $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ est vraie alors $\mathcal{P}(n)$ est vrai pour tout n.*

6.2.3. *Corollaire :* Récurrence forte. Soient n_0 un élément de $\mathbb{N}$ et P une propriété portant sur les éléments du sous-ensemble $\{n \in \mathbb{N} \mid n \geqslant n_0\}$ de $\mathbb{N}$. On suppose que :
1. $\mathrm{P}(n_0)$ est vraie ;
2. si n est un élément de $\{n \in \mathbb{N} \mid n \geqslant n_0\}$ tel que $\mathrm{P}(k)$ soit vraie pour tout élément $k \in \mathbb{N}$ tel que $n_0 \leqslant k \leqslant n$, alors $\mathrm{P}(n+1)$ est vraie.
Alors, $\mathrm{P}(n)$ est vraie pour tout élément $n \geqslant n_0$ de $\mathbb{N}$.

On peut montrer par la récurrence forte que tout entier $n \geq 2$ est produit de nombres premiers.

6.2.4. *Corollaire :* Récurrence à deux pas. Soient n_0 dans $\mathbb{N}$ et P une propriété portant sur les éléments du sous-ensemble $\{n \in \mathbb{N} \mid n \geqslant n_0\}$ de $\mathbb{N}$. On suppose que :
1. $\mathrm{P}(n_0)$ est vraie et $\mathrm{P}(n_0 + 1)$ est vraie ;
2. si n est un élément de $\{n \in \mathbb{N} \mid n \geqslant n_0\}$ tel que $\mathrm{P}(n)$ et $\mathrm{P}(n+1)$ soient vraies, alors $\mathrm{P}(n+2)$ est vraie.
Alors, $\mathrm{P}(n)$ est vraie pour tout élément de $\{n \in \mathbb{N} \mid n \geqslant n_0\}$.

6.2.5. *La multiplication.* On définit une loi $\times$ interne par récurrence en posant

$$\forall n \in \mathbb{N},\ n \times 0 = 0, \quad \forall n, m \in \mathbb{N},\ n \times (m+1) = (n \times m) + n$$

On peut alors montrer que la loi $\times$ est associative, commutative, distributive par rapport à la loi $+$ et compatible avec la relation d'ordre. En particulier $\mathbb{N}$ est *archimédien*, c'est-à-dire

$$\forall a \in \mathbb{N}, b \in \mathbb{N}^*, \exists n \in \mathbb{N},\ a \leq n \times b.$$

En effet comme $1 \leq b$, par compatibilité on obtient $a \times 1 = a \leq a \times b$. Donc a convient. On peut montrer également que si $a \times b = a' \times b$ et $b \neq 0$, alors $a = a'$.

6.2.6. *Corollaire : Division euclidienne dans* $\mathbb{N}$. *Soit* $a \in \mathbb{N}$ *et* $b \in \mathbb{N}^*$. *Il existe un unique couple* (q, r) *avec* $0 \leq r < b$ *tel que* $a = b \times q + r$.

Démonstration. Existence du couple : posons $A = \{q \in \mathbb{N} \mid b \times q > a\}$. A est une partie non vide de $\mathbb{N}$ car $\mathbb{N}$ est archimédien, donc A possède un plus petit élément s_0. On a alors $b \times s_0 > a$ et $b \times (s_0 - 1) \leq a$. Posons $q = s_0 - 1$ et $r = a - b \times q$. Comme $b \times (s_0 - 1) \leq a < b \times s_0$ on a $0 \leq r < b \times s_0 - b \times (s_0 - 1) = b$, donc le couple (q, r) répond à la question.

Unicité du couple : supposons qu'il y en ait deux : $a = b \times q + r = b \times q' + r'$. Supposons $r \leq r'$, alors $q' \leq q$ et $b \times (q - q') = r' - r$. Puisque $0 \leq r' - r \leq r' < b$ on en déduit $q - q' < 1$ donc $q = q'$ et $r = r'$. Il en va de même si l'on suppose $r \geq r'$. □

7. Notion de cardinal

Définition 7.1. Deux ensembles A et B sont dits *équipotents* s'il existe une application bijective de A vers B. On dit aussi que A et B ont *même cardinal*.

Remarque 7.2. La relation "être équipotent" est une relation d'équivalence. La notion de cardinal correspond donc aux classes d'équivalence des ensembles modulo la relation d'équipotence. Le cardinal nous donne une mesure de la taille des ensembles. Le cas des ensembles finis ne pose pas de problème car cela correspond à "compter" les éléments de l'ensemble. Le cas des ensembles infinis est plus délicat.

Pour tout entier $n \geq 1$, on note $\mathbb{N}_n = \{1, 2, 3, \ldots, n\}$.

Définition 7.3. Soit E un ensemble. Il est dit fini si E est l'ensemble vide ou E est équipotent à $\mathbb{N}_n$ pour un certain entier $n \geq 1$.

Théorème 7.4. *Soit* E *un ensemble fini non vide. Il existe un unique entier* $n \in \mathbb{N}^*$ *tel que* E *est équipotent à* $\mathbb{N}_n$.

Ce théorème découle facilement du lemme suivant :

Lemme 7.5. *Si* n *et* m *sont deux entiers distincts, alors* $\mathbb{N}_n$ *et* $\mathbb{N}_m$ *ne sont pas équipotents.*

Démonstration. Pour prouver ce lemme, on montre par récurrence sur $n \in \mathbb{N}^*$ la propriété $H(n)$ suivante : $\forall m > n$, il n'existe pas de bijection entre $\mathbb{N}_n$ et $\mathbb{N}_m$.

$n = 1$: une application $\{1, 2, \ldots, m\} \to \{1\}$ ne peut pas être injective si $m > 1$.

Pour montrer que $H(n) \Rightarrow H(n+1)$, on raisonne par contraposée. Supposons donc qu'il existe une application bijective $f : \mathbb{N}_{n+1} \to \mathbb{N}_m$ pour un certain entier $m > n + 1$. En composant f avec l'application bijective $\mathbb{N}_m \to \mathbb{N}_m$ qui échange m et $f(n+1)$ et qui ne change pas les autres éléments, on obtient une application bijective $g : \mathbb{N}_{n+1} \to \mathbb{N}_m$ qui vérifie $g(n+1) = m$. La restriction de g à $\mathbb{N}_n$ est alors une application bijective de $\mathbb{N}_n$ dans $\mathbb{N}_{m-1}$, avec $m - 1 > n$, et ceci prouve l'implication requise.

En vertu du principe de récurrence, on en déduit que $\mathbb{N}_n$ et $\mathbb{N}_m$ ne sont pas équipotents pour tout $m > n$. □

On est maintenant en mesure de définir le cardinal d'un ensemble fini :

Définition 7.6. Soit E un ensemble fini. Si $E = \emptyset$, on pose par convention $\mathrm{Card}(E) = 0$. Sinon, on appelle cardinal de E et on note $\mathrm{Card}(E)$ l'unique entier n tel que E est équipotent à $\mathbb{N}_n$.

Remarque 7.7. Si $f : \mathbb{N}_n \to E$ est bijective, elle permet de numéroter de 1 à n les éléments de E. Le cardinal d'un ensemble fini correspond donc bien à son nombre d'éléments au sens intuitif.

On peut montrer, à partir de cette définition, que le cardinal des ensembles finis a les propriétés bien connues suivantes :

Proposition 7.8. *(i) Si E est fini et si F est équipotent à E, alors F est fini et de même cardinal que E.*

(ii) Si E est fini et si F est un sous-ensemble de E, alors F est fini et $\mathrm{Card}(F) \leq \mathrm{Card}(E)$. *Si de plus $E \neq F$, alors* $\mathrm{Card}(F) < \mathrm{Card}(E)$.

(iii) Si E est fini et si F est un sous-ensemble de E, alors $E \setminus F$ est fini et de cardinal $\mathrm{Card}(E) - \mathrm{Card}(F)$.

(iv) Si F est fini et s'il existe une application injective de E dans F, alors E est fini et de cardinal au plus $\mathrm{Card}(F)$.

(v) Si E et F sont finis et s'il existe une application injective de E dans F et une application injective de F dans E, alors E et F sont de même cardinal (et donc équipotents).

(vi) Si E et F sont deux ensembles finis, alors $E \cup F$ est fini et de cardinal $\mathrm{Card}(E \cup F) = \mathrm{Card}(E) + \mathrm{Card}(F) - \mathrm{Card}(E \cap F)$.

(vii) Soient E et F deux ensembles finis de même cardinal et f une application de E dans F. Alors les trois propriétés suivantes sont équivalentes :

(a) f est injective ; (b) f est surjective ; (c) f est bijective.

(viii) Si E et F sont finis alors $E \times F$ est fini de cardinal $\mathrm{Card}(E) \times \mathrm{Card}(F)$.

Définition 7.9. Un ensemble est dit *infini* s'il n'est pas fini. Par exemple $\mathbb{N}$ est infini.

Parmi les ensembles infinis, ceux qui sont équipotents à $\mathbb{N}$ jouent un rôle particulier, puisque l'on peut tout de même numéroter leurs éléments (jusqu'à l'infini). D'où la définition suivante :

Définition 7.10. Un ensemble E est dit *dénombrable* s'il est équipotent à $\mathbb{N}$.

En utilisant l'unicité de $\mathbb{N}$ (voir 6.1.3) on démontre

Proposition 7.11. *Tout sous-ensemble infini de $\mathbb{N}$ est dénombrable.*

Les ensembles infinis n'ont pas tous le même cardinal. En particulier :

Théorème 7.12 (Cantor)**.** *Quel que soit l'ensemble E, il n'est jamais équipotent à l'ensemble $\mathcal{P}(E)$ de ses parties.*

Démonstration. Supposons par l'absurde que E et $\mathcal{P}(E)$ sont équipotents, et considérons une application bijective $\Phi : E \to \mathcal{P}(E)$. Posons $A = \{x \in E,\ x \notin \Phi(x)\}$. Comme A est une partie de E et que Φ est bijective, il existe $a \in E$ tel que $A = \Phi(a)$. Si $a \in A$, alors $a \notin \Phi(a) = A$ (par définition de A), absurde. Si $a \notin A$, alors $a \in \Phi(a) = A$ (par définition de A), absurde. □

Remarque 7.13. Comme il existe une injection $E \to \mathcal{P}(E)$ $(x \mapsto \{x\})$, le théorème précédent signifie que le cardinal de $\mathcal{P}(E)$ est "strictement plus grand" que celui de E. Ceci permet, à partir de $\mathbb{N}$, de construire des ensembles ayant une infinité d'éléments "de plus en plus grande" : $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))$.

On peut montrer que le cardinal de $\mathbb{R}$ est égal au cardinal de $\mathcal{P}(\mathbb{N})$. Ce cardinal s'appelle la puissance du continu.

8. Dénombrement

Proposition 8.1. *Soit E un ensemble de cardinal p et F de cardinal n.*

(1) L'ensemble des parties de E est fini et de cardinal 2^p.

(2) Le nombre d'applications de E dans F est n^p.

(3) Le nombre d'injection de E dans F est noté A_n^p et appelé arrangement de p objets pris parmi n. *Si $p \leqslant n$, alors $A_n^p = \dfrac{n!}{(n-p)!} = n(n-1)\dots(n-p+1)$.*
Si $p > n$, alors $A_n^p = 0$.

Démonstration. (1) Pour chaque élément de E, il y a deux possibilités : être ou ne pas être dans un sous-ensemble A.

(2) Une application est exactement déterminée par le choix des p images, et chaque image a n possibilités.

(3) On peut supposer que E est l'ensemble $\{1, \dots, p\}$. Choisir une injection de E dans F revient à choisir un premier élément dans F, puis un second (différent du premier), puis un troisième (différents des deux premiers), etc, jusqu'à un p-ième, en retenant dans quel ordre les éléments ont été choisis. Pour $p > n$, il est impossible de trouver une telle injection, car au moins un élément de F aurait deux antécédents. Pour $p \leqslant n$, on a n choix pour l'image de 1, puis $n-1$ choix pour l'image de 2, etc, et $n-p+1$ choix pour l'image de p. Il y a donc $n(n-1)(n-2)\dots(n-p+1)$ injections de E dans F. □

Définition 8.2. On appelle une permutation d'un ensemble E une bijection de E dans E.

Proposition 8.3. *Si E est un ensemble fini à n éléments, il y a $n!$ permutations de E.*

Démonstration. Comme E est un ensemble fini, une application de E dans E est bijective si et seulement si elle est injective. Il y a donc autant de bijections de E dans E que d'injections de E dans E. Ce nombre est $A_n^n = n!$. □

Remarque 8.4. Compter les surjections est beaucoup plus compliqué, il n'y a pas de formule simple.

Définition 8.5. – Une combinaison de p objets pris parmi n est un sous-ensemble à p éléments d'un ensemble à n éléments. On note $\binom{n}{p}$ (ou C_n^p) le nombre de combinaisons de p objets pris parmi n. On appelle ces nombres les *coefficients binômiaux*.

Formules à connaitre

$$\binom{n}{p} = \begin{cases} \frac{n!}{p!(n-p)!} & p \leq n \\ 0 & p > n. \end{cases}$$

(Symétrie) $$\binom{n}{p} = \binom{n}{n-p},\ 0 \leq p \leq n.$$

(Formule de Pascal) $\quad \binom{n+1}{p+1} = \binom{n}{p+1} + \binom{n}{p},\ 0 \leq p < n.$

(Formule du Binôme de Newton) $\quad \forall (a,b) \in \mathbb{C}^2, \forall n \in \mathbb{N}^*,\ (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$

La dernière formule est encore valable si l'on remplace $\mathbb{C}$ par un anneau commutatif unitaire quelconque A. Il faut cependant interpréter $\binom{n}{k}$ comme étant l'image de l'entier $\binom{n}{k}$ par le morphisme caractéristique $\mathbb{Z} \to A$, c'est-à-dire l'unique morphisme de groupes qui envoie $1 \in \mathbb{Z}$ sur $1_A \in A$.

9. Exercices–Ensembles et applications

Exercice 9.1. Calculer l'union et l'intersection des familles $\{A_i\}_{i\in I}$ de sous-ensembles de E dans les cas suivants.

(1) $E=\mathbb{R}$, $I=\mathbb{N}^*$ et pour $i\in I$, $A_i=[-\frac{1}{i},\frac{1}{i}]$.

(2) $E=\mathbb{R}^2$, $I=\mathbb{R}$ et pour $i\in I$, $A_i=\{(x,y)\in\mathbb{R}^2 \mid x^2+y^2\leq i^2\}$.

(3) $E=\mathbb{R}$, $I=\mathbb{N}^*$ et pour $i\in I$, $A_i=[-\frac{1}{i};i]$.

Exercice 9.2. Soit E un ensemble et A un sous-ensemble de E. On appelle *fonction caractéristique* de A, l'application $f_A : E\to\{0,1\}$ définie par $f_A(x)=1$ si $x\in A$ et $f_A(x)=0$ si $x\notin A$. Montrer les assertions suivantes

(1) $A=B\Rightarrow f_A=f_B$

(2) $f_{A\cap B}=f_Af_B$

(3) $f_{A\cup B}=f_A+f_B-f_Af_B$

(4) $f_{^cA}=1-f_A$

Exercice 9.3. Soit $f:E\to F$ une application. Montrer les affirmations suivantes et dans les item (3) à (5) donner des exemples où il n'y a pas égalité.

(1) $\forall U,V\in\mathcal{P}(F), f^{-1}(U\cup V)=f^{-1}(U)\cup f^{-1}(V)$ et $f^{-1}(U\cap V)=f^{-1}(U)\cap f^{-1}(V)$.

(2) $\forall A,B\in\mathcal{P}(E),\ f(A\cup B)=f(A)\cup f(B)$.

(3) $\forall A,B\in\mathcal{P}(E), f(A\cap B)\subset f(A)\cap f(B)$ et

$$(\forall A,B\in\mathcal{P}(E), f(A)\cap f(B)\subset f(A\cap B))\iff f \text{ est } \textit{injective}.$$

(4) $\forall B\in\mathcal{P}(F),\ f(f^{-1}(B))=B\cap f(E)$. En particulier $f(f^{-1}(B))\subset B$ et si f est surjective on a égalité.

(5) $\forall A\in\mathcal{P}(E),\ A\subset f^{-1}(f(A))$. Si f est injective, il y a égalité.

Exercice 9.4. Dans le plan euclidien $\mathcal{P}$ muni d'un repère orthonormé, on considère l'hyperbole $\mathcal{H}$ d'équation $x^2-5y^2=1$. Montrer que l'application

$$\begin{array}{rl} g: & \mathcal{P}\to\mathcal{P} \\ & (x,y)\mapsto(9x+20y,4x+9y)\end{array}$$

induit une bijection de $\mathcal{H}$ sur elle-même.

10. Exercices–Relations d'équivalence, quotients

Exercice 10.1. Soit E un ensemble. Soit $\mathcal{R}$ une relation binaire sur E. Dans chacun des cas suivants, déterminer si $\mathcal{R}$ est une relation d'équivalence. Le cas échéant, décrire les classes d'équivalence et donner un système complet de représentants

(1) $E=\mathbb{N}$ et : $\forall x,y\in E, x\mathcal{R}y\Leftrightarrow x=-y$.

(2) $E=\mathbb{R}$ et : $\forall x,y\in E, x\mathcal{R}y\Leftrightarrow\cos^2x+\sin^2y=1$.

(3) $E=\mathcal{P}(F)$, $A\subset F$, et : $\forall X,Y\in\mathcal{P}(F), X\mathcal{R}Y\Leftrightarrow X\cap A=Y\cap A$.

Exercice 10.2 (Construction de $\mathbb{Z}$ et $\mathbb{Q}$). On considère sur $\mathbb{N}\times\mathbb{N}$ la relation définie par : $\forall(a,b)\in\mathbb{N}\times\mathbb{N},\ \forall(a',b')\in\mathbb{N}\times\mathbb{N},\ (a,b)\ \mathcal{R}\ (a',b')\Leftrightarrow a+b'=a'+b$.

(1) Démontrer que $\mathcal{R}$ est une relation d'équivalence.

(2) Décrire les classes d'équivalence.

(3) Démontrer qu'il existe une application de $(\mathbb{N}\times\mathbb{N})/\mathcal{R}$ dans $\mathbb{Z}$ telle que, pour tout $(m,n)\in\mathbb{N}\times\mathbb{N}$, l'image de la classe d'équivalence de (m,n) par cette application soit $m-n$.

(4) Démontrer que l'application obtenue à la question précédente est bijective.

Soit $\sim$ la relation binaire sur l'ensemble $E=\mathbb{Z}\times\mathbb{Z}\backslash\{0\}$ définie par :

$$\forall (x,y),(x',y')\in E,\ (x,y)\sim(x',y')\Leftrightarrow xy'=x'y.$$

Montrer que $\sim$ est une relation d'équivalence et démontrer que $E/\sim$ est en bijection avec $\mathbb{Q}$.

Exercice 10.3 (Construction de $\mathbb{C}$). Soit $B\in\mathbb{R}[X], B\neq 0$. On note $\mathcal{R}$ la relation binaire sur $\mathbb{R}[X]$ définie par : $\forall A,A'\in\mathbb{R}[X],\ A\mathcal{R}A'\Leftrightarrow B|(A-A')$.

(1) Démontrer que $\mathcal{R}$ est une relation d'équivalence.

(2) Soit $A\in\mathbb{R}[X]$. Décrire la classe d'équivalence de A.

(3) Démontrer qu'il existe une application de $\mathbb{R}[X]/\mathcal{R}$ dans $\mathbb{R}_{\deg(B)-1}[X]$ telle que, pour tout $A\in\mathbb{R}[X]$, l'image de la classe d'équivalence de A par cette application soit le reste de la division euclidienne de A par B.

(4) Démontrer que l'application obtenue à la question précédente est bijective.

(5) Montrer que pour $B=X^2+1$ on obtient une bijection avec $\mathbb{C}$.

Exercice 10.4. Soit $f:E\to F$ une application. On considère la relation d'équivalence donnée par $f: x\mathcal{R}y\Leftrightarrow f(x)=f(y)$.

(1) Soie $e\in E$. Démontrer que la classe d'équivalence de e est égale à $f^{-1}(f(e))$.

(2) Pour les 3 fonctions

(a) $f:\mathbb{C}\to\mathbb{R}_+$ définie par $f(z)=|z|$.

(b) $f:\mathbb{R}\to\mathbb{R}$ définie par $f(x)=x^4-x^2$.

(c) $f:\mathbb{R}\to\mathbb{R}$ définie par $f(x)=2x^3+3x^2$.

On répondra aux questions suivantes
— Décrire (dessiner) les classes d'équivalence.
— Donner un système complet de représentants des classes d'équivalence.
— Donner la factorisation canonique de f.

11. Exercices-Raisonnement, Cardinal, dénombrement

Exercice 11.1. Soit $f:E\to F$ une application surjective. Montrer qu'il existe une relation d'équivalence $\mathcal{R}$ sur E telle que $E/\mathcal{R}$ et F soient equipotents. En déduire que F est équipotent à un sous-ensemble de E.

Montrer que si $f:E\to\mathbb{N}$ est injective alors E est fini ou dénombrable. Montrer que si $f:\mathbb{N}\to E$ est surjective alors E est fini ou dénombrable. Montrer que $\mathbb{Z}$ est dénombrable. Montrer que l'application $\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ qui à (p,q) associe $\frac{(p+q)(p+q+1)}{2}+q$ est une bijection. En déduire que le produit de deux ensembles dénombrables est dénombrable et que $\mathbb{Q}$ est dénombrable.

Exercice 11.2. Soit E une ensemble. Montrer que $\mathcal{P}(E)$ et $\{0,1\}^E$ sont équipotents. Montrer que $\{(A,B)\in\mathcal{P}(E)\times\mathcal{P}(E), A\subseteq B\}$ est équipotent à $\{0,1,2\}^E$.

Exercice 11.3. Soit E un ensemble fini non vide à n éléments et A un sous-ensemble de E à p éléments.

(1) Combien y a-t-il d'applications f de E dans E tel que l'image directe de A par f soit incluse dans A ?

(2) Combien y a-t-il d'applications f de E dans E tel que tout élément de A soit dans l'image de A par f ?

Exercice 11.4. Dénombrer les surjections d'un ensemble à $n+1$ éléments dans un ensemble à n éléments.

Exercice 11.5. La démonstration ci-dessous est-elle correcte ?

Pour tout $n \geqslant 2$ on considère la propriété $P(n)$: n points distincts du plan sont alignés.

Initialisation : $P(2)$ est vraie car deux points distincts sont toujours alignés.

Hérédité : On suppose que $P(n)$ est vraie et on va démontrer $P(n+1)$.
Soit donc $A_1, \ldots, A_{n+1}$ des points distincts. Les points $A_1, \ldots, A_n$ sont alignés sur une droite (D) d'après l'hypothèse $P(n)$. Les points $A_2, \ldots, A_{n+1}$ sont aussi alignés sur une droite (D'). Les deux droites (d) et (d') ont $n-1$ points en communs $A_2, \ldots, A_n$. Donc $A_1, \ldots, A_{n+1}$ sont alignés, ce qui montre l'hérédité de la propriété.

Conclusion : $P(n)$ est vraie pour tout $n \geq 2$.

Exercice 11.6. Soit A une partie de $\mathbb{N}^*$ contenant 1 et telle que :

$$(\forall n \in A\ ,\ 2n \in A) \quad \text{et} \quad (\forall n \in \mathbb{N}^*\ ,\ n+1 \in A \Rightarrow n \in A).$$

Montrer que : $\forall m \in \mathbb{N}\ ,\ 2^m \in A$. puis montrer $A = \mathbb{N}^*$.

Exercice 11.7. Montrer que $\sqrt{3} \notin \mathbb{Q}$. En déduire que pour tout $n \in \mathbb{N}$, il existe un unique couple $(p_n, q_n) \in \mathbb{Z}^2$ tel que : $(2+\sqrt{3})^n = p_n + q_n\sqrt{3}$.