Université Paul Sabatier - UFR MIG - Département de mathématiques.
Année scolaire 2007/2008.

Cours polycopié pour le module UE8 (Mathématiques II)

Conventions.
Dans ce qui suit, les *mots en italiques* sont ceux que l'on est en train de définir. On emploie le symbole := lorsqu'une égalité sert à définir le membre gauche à partir du membre droit. Par exemple :
On appelle *carré* du réel x le réel $x^2 := x.x$.
On peut aussi introduire un terme sans définition complète et sans que sa connaissance soit exigible : on le mettra plutôt entre guillemets. Par exemple :
On résume les propriétés de l'addition dans $\mathbf{R}$ en disant que $(\mathbf{R}, +)$ est un "groupe commutatif".

À propos du module UE8. Tous les étudiants qui suivent le module UE8 suivent par ailleurs le module UE2, qui vise essentiellement à consolider les acquis du secondaire afin de servir aux sciences exactes, comme à la suite de l'enseignement mathématique. *A contrario*, on adopte ici un style propre aux mathématiciens : mise en avant des fondements (axiomes et définitions), des concepts abstraits, des démonstrations.

D'où l'idée de commencer par la théorie des ensembles, qui fournit un cadre idéal pour la pratique du raisonnement "pur". Tout le début du cours repose donc très peu sur les connaissances acquises au lycée. Pour la suite (arithmétique, analyse), on se rapprochera des notions déjà connues, mais on sera préparé à les aborder de manière théorique.

Ce polycopié s'appuie lourdement sur le manuel suivant, qui a en partie été écrit par des enseignants de l'Université Paul Sabatier :
"Mathématiques. Tout-en-un pour la Licence. Niveau L1" sous la direction de Jean-Pierre Ramis et André Warusfel, Éditions Dunod.
Ce livre coûte 49 euros pour près de 900 pages, *mais il n'est absolument pas nécessaire de l'acheter*. Il est consultable à la Bibliothèque Universitaire, et les étudiants pourront y trouver de nombreux compléments, éclaircissements et exercices supplémentaires.
Il est parfois cité comme référence des différents chapitres du polycopié sous le nom de "L1, module ..." (dans cette collection, les chapitres sont appelés modules).
Signalons qu'il existe un autre ouvrage de qualité pour le L1, écrit dans un style un peu différent :
"Mathématiques, L1", sous la direction de Jean-Pierre Marco, Éditions Pearson.

Chapitre 1

Ensembles, relations binaires

Référence pour ce chapitre : le module I.1 du L1, sections 1, 2, 5, plus une partie des sections 4 et 6 [1].

Dans la "vie courante" de l'usager des mathématiques, le langage des ensembles apparait très tôt comme moyen de parler collectivement d'objets de même nature : l'ensemble des entiers, l'ensemble des solutions d'une équation, d'une inéquation ou d'un système d'équations, divers ensembles de points du plan et de l'espace comme droites, cercles, etc. En fait, depuis le vingtième siècle, ce langage est devenu le langage commun de *toutes les mathématiques* et, par contrecoup, un langage nécessaire pour la plupart des sciences. Pour notre usage en L1 (et L2 et L3), nous n'avons besoin que d'une compréhension intuitive et de la maitrise de quelques règles de calcul et de raisonnement sur les ensembles (comme $\mathbf{N}$, $\mathbf{R}$, et d'autres, que le lecteur a déjà rencontrés), sur les applications (comme la fonction exponentielle, la fonction logarithme, et d'autres, que le lecteur a déjà rencontrées) sur les relations d'ordre (comme la relation $\leq$ entre les nombres réels, ou la relation de divisibilité entre entiers naturels) et sur les relations d'équivalence (comme la congruence modulo un entier, par exemple la relation "avoir même parité").

Cependant, il n'est pas inutile de commencer par montrer que la théorie des ensembles elle-même peut être fondée mathématiquement. Cela signifie qu'au lieu de se baser l'intuition, on part de définitions ou d'axiomes et l'on essaie d'enchainer des raisonnements complets. C'est une excellente occasion de s'exercer au raisonnement "pur" et à formuler et rédiger des démonstrations. En effet, si cela n'est pas toujours indispensable dans la pratique scientifique courante, il est assez fréquent que l'on ne puisse étudier un nouveau domaine qu'en se fiant au raisonnement rigoureux tant que l'on

[1] À titre *purement culturel* (mais la culture, c'est important pour un scientifique !), on peut également lire le volume "Théorie des ensembles" de Bourbaki, qui donne une bonne vision des fondements formels des mathématiques *vus par les mathématiciens* (et non par les logiciens).

n'est pas encore assez familier.

Autrefois, on apprenait la géométrie axiomatique d'Euclide dans le secondaire (en quatrième, en fait !) ; mais le style actuel d'enseignement des mathématiques au lycée a largement délaissé la *pratique de la démonstration*, et c'est en entrant à l'Université que l'on doit s'y mettre énergiquement. La section 1.1, par laquelle nous commençons ce chapitre, a donc un parfum assez inhabituel. Le lecteur peut y prendre plaisir en la considérant comme un jeu logique (comme les échecs ou le sudoku) et un échauffement pour la suite (comme on se remue les muscles et les ligaments sur place avant d'entreprendre une randonnée, un concert ou un ballet). Signalons à ce sujet que ***la lecture de ce texte doit se faire avec papier et crayon, pour vérifier ou compléter les raisonnements et les calculs, résoudre les exercices, etc.***

À partir de la section 1.2, les "choses sérieuses" commencent et l'on aborde des notions et des résultats dont la connaissance est *indispensable* pour toute la suite.

1.1 Ensembles et applications

1.1.1 Ensembles et éléments

Dans le monde mathématique de tous les jours, il y a des objets (nombres, fonctions, points ...) et il y a des ensembles ($\mathbf{N}$, le plan, et bien d'autres). Dans la présentation formalisée des mathématiques, il n'y a pas de telle distinction, tous les objets sont mis sur le même plan. Il y a une relation fondamentale, la *relation d'appartenance* notée $x \in E$ (lire : "x appartient à E", ou "x est élément de E"). Sa négation est notée : $x \notin E$.

Exemple.
On a bien entendu, $2 \in \mathbf{N}$, $2 \in \mathbf{Z}$, $2 \in \mathbf{Q}$ et $2 \in \mathbf{R}$. On a également : $\sqrt{2} \notin \mathbf{Z}$ (très facile puisque $\sqrt{2} \approx 1,414$) et $\sqrt{2} \notin \mathbf{Q}$ (plus difficile, mais nous le prouverons en arithmétique).

Définition.
La *relation d'inclusion* entre ensembles est définie par :

$$E \subset F \Longleftrightarrow (\forall x\ ,\ x \in E \Rightarrow x \in F),$$

autrement dit, E est inclus dans F si tout élément de E est élément de F. On dit que "E est inclus dans F", que "E est (une) partie de F" ou encore que "E est (un) sous-ensemble de F". La négation de cette relation est notée $E \not\subset F$.

On dit parfois également "est contenu" (ou "contient") mais ce terme est ambigu, car il ne distingue pas nettement entre appartenance et inclusion.

Exemple.
On a les inclusions : $\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$. Mais, bien entendu : $\mathbf{C} \not\subset \mathbf{Q}$ (par exemple).

Exercice.
Est-ce que $2 \subset \mathbf{N}$? Est-ce que $\mathbf{N} \in \mathbf{Q}$?

La relation d'inclusion est évidemment *réflexive*, c'est-à-dire que tout ensemble E est partie de lui-même :

$$E \subset E.$$

(Argument : tout élément de E est élément de E.)
Cette relation est également *transitive*, c'est-'a-dire qu'une partie d'une partie de E est-elle même une partie de E :

$$(G \subset F \text{ et } F \subset E) \Longrightarrow G \subset E.$$

(Argument : si tout élément de G est élément de F et si tout élément de F est élément de E, alors tout élément de G est élément de E.)

Il est évident *a priori* que deux ensembles égaux ont mêmes éléments. (C'est justifié dans l'alinéa en petits caractères ci-dessous, dont la lecture est facultative.) La question de savoir si deux ensembles qui ont les mêmes éléments sont égaux est traitée au paragraphe sur l'extensionalité.

Un peu de logique. De manière générale, l'égalité, en mathématiques, fonctionne de la manière suivante : deux objets égaux ont les mêmes propriétés. Pour le formaliser, disons que l'on note $P(x)$ une propriété d'un élément x inconnu. Pour certaines valeurs de x, la propriété $P(x)$ est *vraie*, pour d'autres valeurs, elle est *fausse*. Une telle propriété dépendant d'un élément inconnu x (donc d'une *variable*) est appelée "prédicat". On dit parfois aussi "relation", même si elle ne concerne qu'une variable. Ce que nous avons dit de l'égalité mathématique s'écrit ainsi : $\forall x, y\ ,\ (x = y) \Longrightarrow \big(P(x) \Leftrightarrow P(y)\big)$. On peut l'appliquer en prenant pour x, y deux ensembles égaux $E = F$ et pour prédicat $P(x) := (a \in x)$, où a est un élément arbitraire. On en déduit : $P(E) \Leftrightarrow P(F)$, *i.e.* $(a \in E) \Leftrightarrow (a \in F)$. Comme c'est vrai pour a arbitraire, on voit bien que E et F ont mêmes éléments.

La propriété d'extensionalité

C'est la propriété la plus typique de la théorie des ensembles. Elle dit (informellement) qu'un ensemble est totalement défini par ses éléments. C'est un *axiome*.

Axiome *(d'extensionalité).*
Deux ensembles qui ont les mêmes éléments sont égaux :

$$(\forall x\ ,\ x \in E \Leftrightarrow x \in F) \Longrightarrow (E = F).$$

La condition $(\forall x\ ,\ x \in E \Leftrightarrow x \in F)$ est la *conjonction logique* (le "et") des deux conditions : $(\forall x\ ,\ x \in E \Rightarrow x \in F)$, et $(\forall x\ ,\ x \in F \Rightarrow x \in E)$, autrement dit, des deux conditions $E \subset F$ et $F \subset E$. Une traduction de l'axiome d'extensionalité est donc celle-ci :

$$(E \subset F \text{ et } F \subset E) \Longrightarrow (E = F).$$

On dit que la relation d'inclusion est *antisymétrique*. Nous verrons à la section 1.2.3 qu'une relation réflexive, transitive et antisymétrique est une *relation d'ordre* : la relation d'inclusion est donc une relation d'ordre.

On a déjà vu que, si deux ensembles sont égaux, alors ils ont mêmes éléments. On a donc deux implications réciproques l'une de l'autre, c'est-à-dire une équivalence logique : pour que deux ensembles soient égaux, il faut, et il suffit, qu'ils aient les mêmes éléments. Formellement :

$$(\forall x\ ,\ x \in E \Leftrightarrow x \in F) \Longleftrightarrow (E = F).$$

Un peu de sémantique. La propriété d'extensionalité contredit l'usage courant des noms collectifs. Si, par exemple, on constate que "les étudiants du portail IA" sont exactement les mêmes que "les habitants du tripode B de la résidence universitaire", on n'en déduira pas que les deux notions sont identiques. Simplement, de façon contingente, elles se trouvent s'appliquer aux mêmes individus. Voici un exemple classique dans le même esprit : on sait que "le vainqueur d'Austerlitz" = {Napoléon} et que "le vaincu de Waterloo" = {Napoléon}. Mais dire que Joséphine a épousé le vainqueur d'Austerlitz n'a pas la même signification que de dire qu'elle a épousé le vaincu de Waterloo.

Nos premiers (petits) ensembles

Jusque là, nous parlons d'ensembles mais nous n'en avons pas fabriqué un seul. Bien entendu, nous avons des exemples en tête, tirés de notre expérience antérieure. Mais il faut bien que la théorie (que nous effleurons) donne elle-même des moyens d'en définir, ou d'en construire. C'est le rôle d'une série d'*axiomes* que nous allons énoncer. On commence par les plus petits ensembles, et même, par le plus petit de tous !

Axiome *(de l'ensemble vide).*
Il y a un ensemble sans élément, appelé *ensemble vide* et noté $\emptyset$:

$$\forall x\ ,\ x \notin \emptyset.$$

D'après l'axiome d'extensionalité, cet ensemble est unique : tout ensemble sans élément lui est égal. En effet, si E est un (peut-être autre) ensemble n'ayant aucun élément, les propriétés $(x \in E)$ et $(x \in \emptyset)$ sont *fausses* quel que soit x, elles sont donc équivalentes. L'axiome d'extensionalité garantit alors que $E = \emptyset$.

Axiome *(du singleton).*
Pour tout objet a, il existe un ensemble ayant a pour seul élément, appelé *singleton* et noté $\{a\}$ (lire "singleton a") :

$$\forall x\ ,\ x \in \{a\} \iff (x = a).$$

D'après l'axiome d'extensionalité, cet ensemble est unique : tout ensemble ayant ce seul élément lui est égal. En effet, si E est un ensemble ayant pour seul élément a, les propriétés $(x \in E)$ et $(x \in \{a\})$ sont toutes deux équivalentes à $(x = a)$, elles sont donc équivalentes entre elles. L'axiome d'extensionalité dit alors que $E = \{a\}$.

Exemples.
Un singleton n'est jamais vide, puisqu'il a un élément : $\forall a\ ,\ \{a\} \neq \emptyset$.
L'ensemble $\{\sqrt{2}\}$ est un singleton ; c'est un sous-ensemble de $\mathbf{R}$.
L'ensemble dont le seul élément est $\emptyset$ est le singleton $\{\emptyset\}$. On a $\{\emptyset\} \neq \emptyset$, car le membre droit est vide, alors que le membre gauche ne l'est pas.

Axiome *(de la paire).*
Soient a, b deux éléments (non nécessairement distincts). Il existe un ensemble dont les seuls éléments sont a et b. On le note $\{a, b\}$.

$$\forall x\ ,\ x \in \{a, b\} \iff (x = a \text{ ou } x = b).$$

D'après l'axiome d'extensionalité, cet ensemble est unique : tout ensemble ayant ces seuls éléments lui est égal. (Le lecteur est chaudement encouragé à *démontrer* cette affirmation.) Si $a \neq b$, on l'appelle *paire formée de a et b*. Et si $a = b$, on voit que $\{a, b\} = \{a\}$. L'axiome du singleton est donc conséquence logique de l'axiome de la paire, et on aurait pu économiser le premier ! (Mais l'économie n'est pas un but en soi.)

Exemples.
L'ensemble $\{1, 2\}$ est une paire ; c'est un sous-ensemble de $\mathbf{N}$.
L'ensemble $\{\emptyset, \{\emptyset\}\}$ est aussi une paire. En effet, on a vu que $\emptyset \neq \{\emptyset\}$.
L'ensemble $\{1, 1\}$ est le singleton $\{1\}$, mais cette dernière notation est préférable !

Définition en extension

On ne va pas continuer en donnant un axiome des ensembles à trois éléments (ou brelans ?), des ensembles à quatre éléments (ou carrés ?), etc. Nous prendrons donc un raccourci par rapport à la vraie théorie formelle et admettrons le principe suivant (qui n'est pas un véritable axiome, car trop vague) : chaque fois que l'on se donne des objets $a_1, \ldots, a_n$, il existe un ensemble dont les seuls éléments sont $a_1, \ldots, a_n$. D'après l'axiome d'extensionalité, cet ensemble est unique. On le note $\{a_1, \ldots, a_n\}$. On dit que l'on a défini cet ensemble *en extension*, c'est-à-dire en énumérant ses éléments.

Exemple.
L'ensemble $\{1, 2, 3\}$, l'ensemble $\{1, 3, 2\}$ et l'ensemble $\{1, 2, 3, 1\}$ sont des sous-ensembles de $\mathbf{N}$. Ces trois ensembles ont d'ailleurs les mêmes éléments, ils sont donc égaux.

Généralisation de la définition en extension. Il s'agit d'un principe encore plus vague que le précédent : chaque fois que l'on se donne des objets $a_1, \ldots, a_n, \ldots$ en nombre indéfini mais avec une "règle de construction" connue, il existe un ensemble dont les seuls éléments sont $a_1, \ldots, a_n, \ldots$. D'après l'axiome d'extensionalité, cet ensemble est unique. On le note $\{a_1, \ldots, a_n, \ldots\}$. En fait, une fois admise l'existence de l'ensemble $\mathbf{N}$ des entiers naturels, on utilise plutôt la notation $\{a_n \mid n \in \mathbf{N}^*\}$. Naturellement, on peut aussi utiliser $\{a_0, \ldots, a_n, \ldots\} = \{a_n \mid n \in \mathbf{N}\}$. On dit encore que l'on a défini cet ensemble en extension, c'est-à-dire en énumérant ses éléments.

Exemples.
L'ensemble $\{0, 1, 2, 3, \ldots\}$ est bien entendu $\mathbf{N}$.
En revanche, il n'est pas aussi évident de reconnaitre l'ensemble $\{2, 3, 5, 7, 11, \ldots\}$. (C'est sans doute l'ensemble des nombres premiers.)
Il est possible (bien que pas très simple) d'énumérer les éléments de $\mathbf{Q}$, mais il est impossible d'énumérer les éléments de $\mathbf{R}$ (ce sera prouvé à la section 1.2.4).

Exercice.
Montrer que les ensembles $\emptyset$, $\{\emptyset\}$, $\{\{\emptyset\}\}$ sont deux à deux distincts.

Exercice.
Que dire de la relation $E \subset F$ lorsque E ou F est l'ensemble vide ? un singleton ?

1.1.2 Définition en compréhension

On a vu (ou admis) qu'il peut être difficile, voir impossible, de décrire un ensemble en extension. Même quand c'est "simple", cela peut être fastidieux : par exemple, l'ensemble des nombres premiers inférieurs à $2^{32582657}$ (Selon Wikipedia, référence : URL `\http://fr.wikipedia.org/wiki/Nombre_premier_de_Mersenne`, le plus grand nombre premier connu en septembre 2006 était $2^{32582657} - 1$.) Nous allons apprendre à définir un ensemble par une propriété caractéristique de ses éléments.

Prédicats collectivisants

Soit $P(x)$ un "prédicat", c'est-à-dire une propriété d'un argument variable x. Nous ne serons pas très précis sur le "domaine de définition" de $P(x)$, c'est-à-dire sur le "type" de valeurs de x pour lequel il est défini. (On pourraitt détailler ce point, mais cela conduirait à des énoncés extrêmement lourds.)

Définition.
On dit que le prédicat $P(x)$ est *collectivisant* si les éléments x tels que $P(x)$ est vérifié forment un ensemble, autrement dit, s'il existe E tel que :

$$\forall x\ ,\ (x \in E) \iff P(x). \tag{1.1}$$

Il découle de l'axiome d'extensionalité que l'ensemble E est alors unique. Soit en effet E' un ensemble ayant la même propriété. Alors les propriétés $(x \in E)$ et $(x \in E')$ sont toutes deux équivalentes à $P(x)$, elles sont donc équivalentes entre elles, et l'axiome d'extensionalité implique $E = F$. L'ensemble ci-dessus est noté :

$$E := \{x \mid P(x)\},$$

ce que l'on lit (lonlère) "ensemble des x tels que $P(x)$".

Exemples.
Le prédicat informel "x est un entier naturel" est collectivisant, il définit l'ensemble $\mathbf{N}$.
Le prédicat $P(x) := (x = a)$ est collectivisant, il définit l'ensemble $\{a\}$. Le prédicat $P(x) := (x = a \text{ ou } x = b)$ est collectivisant, il définit l'ensemble $\{a, b\}$.
Le $P(x) := (x \neq x)$ est collectivisant, il définit l'ensemble vide $\emptyset$. En effet, cette propriété est fausse quel que soit x.

Un peu d'épistémologie. Au début de la théorie des ensembles, on croyait que tout prédicat était collectivisant, autrement dit que l'on pouvait former un ensemble à partir de n'importe quelle propriété arbitrairement formulée. Puis, à la fin du dix-neuvième siècle et au début du vingtième sont apparues les "antinomies" (c.-à-d. les paradoxes) de la théorie des ensembles, qui ont ébranlé les fondements des mathématiques. La plupart tournaient autour d'une version mathématique de paradoxes anciens, tels : "Épiménide dit que tous les Crétois sont des menteurs" (bien entendu, Épiménide est un Crétois).
"Dans cette ville, le barbier rase ceux qui ne se rasent pas eux-mêmes et ne rase pas ceux qui se rasent eux-mêmes" (à laquelle des deux catégories appartient le barbier ?), etc.
L'axiomatique actuelle de la théorie des ensembles a fait disparaitre les antinomies (on croise les doigts), mais un résidu est resté, qui a la forme de divers théorèmes d'impossibilité, dans la démonstration desquels on reconnait les anciens raisonnements paradoxaux. Outre le théorème qui suit, le théorème de Cantor de la section 1.1.4 en est un exemple.

Théorème.
Le prédicat $P(x) := (x \notin x)$ n'est pas collectivisant.
Démonstration. On le prouve par l'absurde (après tout, c'est la version décantée d'une ancienne absurdité). On suppose donc que $P(x)$ est collectivisant, autrement dit, qu'il existe un ensemble :

$$E := \{x \mid x \notin x\}.$$

Par définition, on a l'équivalence logique :

$$\forall x\ ,\ (x \in E) \iff (x \notin x).$$

On n'a fait qu'appliquer la relation (1.1) de la page 8 avec le prédicat $P(x) := (x \notin x)$. Puisque cette équivalence est vraie pour tout x, on peut l'appliquer en particulier à $x := E$. On trouve :

$$(E \in E) \Longleftrightarrow (E \notin E).$$

On se retrouve alors avec une *proposition logique* parfaitement définie : $E \in E$, qui est équivalente à sa propre négation, ce qui est contradictoire. L'hypothèse d'existence d'un tel ensemble E est donc absurde, de même que l'hypothèse que ce prédicat est collectivisant. □

Il est un cas où l'on peut, en toute sécurité, définir un ensemble par une propriété : c'est celui où on l'*extrait* d'un ensemble déjà connu. C'est l'axiome suivant qui nous le garantit :

Axiome *(de séparation).*
On suppose que le prédicat $P(x)$ est défini pour tout élément x de l'ensemble E. Alors le prédicat $P_E(x) := (P(x)$ et $x \in E)$ est collectivisant. On note :

$$\{x \in E \mid P(x)\} := \{x \mid P(x) \text{ et } x \in E\}.$$

En règle générale, pour définir un ensemble, il vaudra mieux employer la construction "sécurisée" $\{x \in E \mid P(x)\}$ (qui a un sens à coup sûr, en vertu de l'axiome de séparation) que la construction "risquée" $\{x \mid P(x)\}$ (qui peut aboutir à un non-sens)[2].

Définition.
On appelle *intersection* de E et de F l'ensemble :

$$E \cap F := \{x \in E \mid x \in F\}.$$

Les ensembles E et F sont dits *disjoints* si $E \cap F = \emptyset$.

On a donc, par définition :

$$(x \in E \cap F) \Longleftrightarrow (x \in E \text{ et } x \in F),$$

d'où il découle que $E \cap F = F \cap E$. On prouve de même que $E \cap E = E$, que $E \cap (F \cap G) = (E \cap F) \cap G$, que l'on note donc $E \cap F \cap G$, etc. (Voir 1.1.3).

Définition.
On appelle *différence* de E et de F l'ensemble :

$$E \setminus F := \{x \in E \mid x \notin F\}.$$

Si $F \subset E$, l'ensemble $E \setminus F$ est appelé *complémentaire de F dans E* et noté $\complement_E F$

[2]De même, les *quantificateurs* restreints à un domaine E (on les appelle "quantificateurs typiques") $\forall x \in E$, $\cdots$ et $\exists x \in E$: $\cdots$ sont préférables aux quantificateurs $\forall x$, $\cdots$ et $\exists x$: $\cdots$ écrits sans mention d'un domaine.

Nos premiers constructeurs de gros ensembles

Nous allons proposer des constructeurs qui créent (enfin) du nouveau. Les deux premiers sont bien connus et le lecteur en trouvera des exemples dans ses souvenirs du lycée.

Axiome *(de la réunion).*
Soient E et F des ensembles. Alors le prédicat $P(x) := (x \in E \text{ ou } x \in F)$ est collectivisant et définit la *réunion* (ou l'*union*) de E et de F :

$$E \cup F := \{x \mid x \in E \text{ ou } x \in F\}.$$

Pour l'axiome suivant, on admet qu'à deux éléments quelconques a, b on sait associer le *couple* (a, b), qui obéit à la règle suivante :

$$\forall a\ ,\ \forall b\ ,\ \forall a'\ ,\ \forall b'\ ,\ (a, b) = (a', b') \Longleftrightarrow a = a' \text{ et } a' = b'.$$

Le couple (a, b) n'est donc pas la paire $\{a, b\}$.

Axiome *(du produit).*
Soient E et F des ensembles. Alors le prédicat $P(x) := \big(\exists a \in E\ :\ \exists b \in F\ :\ x = (a, b)\big)$ est collectivisant ; autrement dit, il existe un ensemble formé des couples (a, b) tels que $a \in E$ et $b \in F$. On définit ainsi l'ensemble *produit*, ou *produit cartésien* de E et F :

$$E \times F := \{x \mid \exists a \in E\ :\ \exists b \in F\ :\ x = (a, b)\} = \{(a, b) \mid a \in E, b \in F\}.$$

(Remarquer la deuxième notation "allégée".) Il est d'usage d'identifier les ensembles $E \times (F \times G)$ et $(E \times F) \times G$ et de noter :

$$E \times F \times G := \{(a, b, c) \mid a \in E, b \in F, c \in G\}.$$

Les (a, b, c) sont appelés triplets. Il peut y avoir des difficultés dues au fait que la "première composante" de $(a, (b, c)) \in E \times (F \times G)$, de $((a, b), c) \in (E \times F) \times G$ et de $(a, b, c) \in E \times F \times G$ sont respectivement a, (a, b) et a (problème analogue pour la deuxième composante). On affrontera ces difficultés à l'aide du bon sens. Pour distinguer les triplets, quadruplets, quintuplets des triplés, quadruplés et quintuplés, remarquer que les premiers font moins de bruit mais que les derniers sont plus mignons.

Axiome *(de l'ensemble des parties).*
Soit E un ensemble. Alors le prédicat $x \subset E$ est collectivisant ; autrement dit, les parties de E forment un ensemble. On définit ainsi l'*ensemble des parties de* E :

$$\mathcal{P}(E) := \{x \mid x \subset E\}.$$

Exemples.
L'unique sous-ensemble de $\emptyset$ est lui-même : $\mathcal{P}(\emptyset) = \{\emptyset\}$.
Les seuls sous-ensembles de $\{a\}$ sont $\emptyset$ et lui-même : $\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$.

Exercice.
Calculer l'ensemble des parties de $\{a, b\}$.

Exercice.
Parmi les affirmations suivantes, lesquelles sont équivalentes : $x \in E$, $x \in \mathcal{P}(E)$, $x \subset E$, $x \subset \mathcal{P}(E)$? Peut-on écrire la dernière sous la forme $x \in y$?

1.1.3 Calcul booléen

Il s'agit des règles algébriques du calcul sur les ensembles. On commence par des règles qui sont valables pour des ensembles quelconques :

$$\begin{aligned}
E \cup (F \cup G) &= (E \cup F) \cup G \text{ (associativité de la réunion)} \\
E \cup F &= F \cup E \text{ (commutativité de la réunion)} \\
\emptyset \cup E = E \cup \emptyset &= E \text{ (l'ensemble vide est neutre pour la réunion)} \\
E \cup E &= E \text{ (tout ensemble est idempotent pour la réunion)} \\
E \cap (F \cap G) &= (E \cap F) \cap G \text{ (associativité de l'intersection)} \\
E \cap F &= F \cap E \text{ (commutativité de l'intersection)} \\
\emptyset \cap E = E \cap \emptyset &= \emptyset \text{ (l'ensemble vide est absorbant pour l'intersection)} \\
E \cap E &= E \text{ (tout ensemble est idempotent pour l'intersection)} \\
E \cap (F \cup G) &= (E \cap F) \cup (E \cap G) \text{ (distributivité de l'intersection par rapport à la réunion)} \\
E \cup (F \cap G) &= (E \cup F) \cap (E \cup G) \text{ (distributivité de la réunion par rapport à l'intersection),} \\
E \subset F &\iff E \cap F = E, \\
E \subset F &\iff E \cup F = F.
\end{aligned}$$

Si l'on se restreint aux sous-ensembles d'un ensemble de référence fixé Ω, on peut dire que l'on a muni $\mathcal{P}(\Omega)$ des deux "lois de composition interne" $\cap$ et $\cup$ et de la relation d'ordre $\subset$, et qu'il s'agit des propriétés de cette "structure algébrique".

La série suivante de règles est valable à l'intérieur de $\mathcal{P}(E)$:

$$\begin{aligned}
E \cap F = F \cap E &= F \text{ (l'ensemble } E \text{ est neutre pour l'intersection)} \\
E \cup F = F \cup E &= E \text{ (l'ensemble } E \text{ est absorbant pour la réunion)} \\
\complement_E(\complement_E F) &= F \text{ (involutivité du passage au complémentaire)} \\
\complement_E(F \cup G) &= (\complement_E F) \cap (\complement_E G) \text{ (le passage au complémentaire est un morphisme } \cup \to \cap) \\
\complement_E(F \cap G) &= (\complement_E F) \cup (\complement_E G) \text{ (le passage au complémentaire est un morphisme } \cap \to \cup)
\end{aligned}$$

Exercice.
On pose $F \star G := \complement_E(F \cap G)$. Montrer que toutes les opérations définies dans $\mathcal{P}(E)$ (y compris la complémentation) peuvent se définir à partir de celle-là.

1.1.4 Applications d'un ensemble dans un autre

On ne cherche pas à définir "ce qu'est" une application. Il faut garder en tête le modèle des fonctions numériques. Par exemple, la fonction exponentielle $x \mapsto e^x$ définit une application de $\mathbf{R}$ dans $\mathbf{R}$. Mais elle définit également une application de $\mathbf{R}$ dans $\mathbf{R}_+^*$, et même, par restriction, une application de $\mathbf{R}_+$ dans $[1, +\infty[$, etc. Nous devrons donc ici être un petit peu plus précis.

Vocabulaire

Une application $f : E \to F$ (on dit : "de l'ensemble E dans l'ensemble F") a une *source*, ou *ensemble de départ* E et un *but*, ou *ensemble d'arrivée* F (qui sont donc des ensembles). À tout $x \in E$ elle associe son *image* $f(x) \in F$.

Il y a un équivalent de l'axiome d'extensionalité qui dit que deux applications *supposées de mêmes but et source* $f : E \to F$ et $g : E \to F$ sont égales si, et seulement si, elles ont même effet sur les éléments de E :

$$\forall x \in E \ , \ f(x) = g(x).$$

Avec cette convention, l'application sin de $\mathbf{R}$ dans $\mathbf{R}$ et l'application sin de $\mathbf{R}$ dans $[-1, 1]$ ne sont pas les mêmes, malgré l'ambiguïté de la notation, car elles n'ont pas le même ensemble d'arrivée : d'ailleurs, l'une est surjective et pas l'autre. Il est donc préférable de parler de la "fonction sinus" par opposition à l'application $x \mapsto \sin x$ de $\mathbf{R}$ dans $\mathbf{R}$. On est conduit à la définition suivante.

Définition.
Soit $f : E \to F$ une application. Si $E' \subset E$, l'application $x \mapsto f(x)$ de E' dans F est appellée *restriction de* f *à* E' et notée $f_{|E'}$.

Un peu de tetracapillectomie. De manière analogue, si $F' \subset F$ et si $\mathrm{Im} f \subset F'$, ce qui (comme on le verra) signifie $\forall x \in E \ , \ f(x) \in F'$, alors on peut définir la *corestriction* de f à F' comme l'application $x \mapsto f(x)$ de E dans F'. Il n'y a pas de notation, et d'ailleurs cette construction est peu usitée. Par convention, si $E := \emptyset$, il y a une et une seule application de E dans F, que l'on appelle "application vide" et que l'on note $\emptyset$.

Exemples.
Toutes les fonctions usuelles donnent lieu à diverses applications selon l'ensemble de départ et l'ensemble d'arrivée choisis.
L'*application identité (ou application identique)* sur un ensemble E est l'application $x \mapsto x$ de E dans lui-même. On la note Id_E.
Pour tout $b \in F$, l'*application constante* $x \mapsto a$ de E dans F est notée (par abus) a.
Si $E \neq \emptyset$ et si $F = \emptyset$, il n'y a aucune application de E dans F.

Définition.
Le *graphe* de l'application $f : E \to F$ est l'ensemble :

$$G_f := \{(x, y) \in E \times F \mid y = f(x)\} \subset E \times F.$$

L'application f est totalement déterminée par son graphe : si $G_f = G_g$, alors $f = g$.

Exemples.
Le graphe de Id_E est la *diagonale* $\{(x, y) \in E \times E \mid x = y\}$, que l'on note également $\{(x, x) \mid x \in E\}$. Le graphe de l'application constante a de E dans F est $E \times \{a\}$.

Images, images réciproques, injectivité, surjectivité, bijectivité

Définition.
Soit $f : E \to F$ une application. Lorsque $x \in E$ a pour image $y := f(x) \in F$, on dit que x est un *antécédent* de y. L'*ensemble image* de f est l'ensemble des éléments de F qui admettent un antécédent :

$$\mathrm{Im} f := \{y \in F \mid \exists x \in E \ : \ f(x) = y\} = \{f(x) \mid x \in E\} \text{ (notation “allégée”).}$$

Plus généralement, si $E' \subset E$, on définit l'*image de E' par f* comme l'ensemble des images des éléments de E' :

$$f(E') := \{y \in F \mid \exists x \in E' \ : \ f(x) = y\} = \{f(x) \mid x \in E'\} \text{ (notation “allégée”).}$$

Si $F' \subset F$, on définit l'*image réciproque de F' par f* comme l'ensemble des antécédents des éléments de F' :

$$f^{-1}(F') := \{x \in E \mid f(x) \in F'\}.$$

Dans les règles de calcul qui suivent, A et B désignent des parties de E :

$$\begin{aligned} f(\emptyset) &= \emptyset, \\ f(A \cup B) &= f(A) \cup f(B), \\ f(A \cap B) &\subset f(A) \cap f(B), \\ f(B) \setminus f(A) &\subset f(B \setminus A), \\ A \subset B &\implies f(A) \subset f(B). \end{aligned}$$

Dans les règles de calcul qui suivent, C et D désignent des parties de F :

$$\begin{aligned} f^{-1}(\emptyset) &= \emptyset, \\ f^{-1}(F) &= E, \\ f^{-1}(C \cup D) &= f^{-1}(C) \cup f^{-1}(D), \\ f^{-1}(C \cap D) &= f^{-1}(C) \cap f^{-1}(D), \\ f^{-1}(D) \setminus f^{-1}(C) &= f^{-1}(D \setminus C), \\ C \subset D &\implies f^{-1}(C) \subset f^{-1}(D). \end{aligned}$$

La règle sur l'intersection montre que l'image réciproque "se comporte mieux" que l'image directe (pour un complément, voir les exercices).

Définition.
On dit que l'application $f : E \to F$ est *surjective* si tout élément de l'ensemble d'arrivée F admet au moins un antécédent :

$$\forall y \in F \ , \ \exists x \in E \ : \ f(x) = y.$$

Définition.
On dit que l'application $f : E \to F$ est *injective* si tout élément de F admet au plus un antécédent, ce qui s'écrit :

$$\forall x, x' \in E \ , \ f(x) = f(x') \Longrightarrow x = x'.$$

Définition.
On dit que l'application $f : E \to F$ est *bijective* si elle est injective et surjective, autrement dit, si tout élément de F admet un unique antécédent :

$$\forall y \in F \ , \ \exists\, ! x \in E \ : \ f(x) = y.$$

Définition.
Lorsque f est bijective, l'application de F dans E qui, à tout élément y de F, associe son unique antécédent x, est appelée *application réciproque de* f et notée f^{-1} :

$$\forall x \in E \ , \ \forall y \in F \ , \ x = f^{-1}(y) \Longleftrightarrow y = f(x).$$

Définition.
Soient $f : E \to F$ et $g : F \to G$ deux applications. La *composée de* f *et* g *(ou de* g *par* f*)* est l'application $x \mapsto g\big(f(x)\big)$ de E dans G. On la note $g \circ f$. La composée de g par f n'est donc définie que si l'ensemble d'arrivée de f est égal à l'ensemble de départ de g : on dit alors que f et g sont *composables*.

Ces notions donnent lieu à des propriétés algébriques : $f \circ \mathrm{Id}_E = \mathrm{Id}_F \circ f = f$, et (si les applications sont composables) $h \circ (g \circ f) = (h \circ g) \circ f$.

On voit alors que l'application réciproque d'une bijection f est l'unique application qui vérifie :

$$f^{-1} \circ f = \mathrm{Id}_E \text{ et } f \circ f^{-1} = \mathrm{Id}_F.$$

Réciproquement, si f et g vérifient $g \circ f = \mathrm{Id}_E$ et $f \circ g = \mathrm{Id}_F$, alors elles sont bijectives et réciproques l'une de l'autre.

De *nombreuses* propriétés relient injectivité, surjectivité et composition. À titre d'exemple, voir les exercices. Pour plus de détails, voir L1, module I.1, section 2.

Théorème *(Cantor).*
Quelque soit l'ensemble E, il n'existe pas d'application surjective de E sur $\mathcal{P}(E)$.
Démonstration. Considérons une application $f : E \to \mathcal{P}(E)$. On va montrer que l'ensemble $y := \{x \in E \mid x \notin f(x)\}$, qui est une partie de E, donc un élément de $\mathcal{P}(E)$. n'est pas dans l'image $\mathrm{Im} f$ de f. Pour cela, on raisonne par l'absurde.
Soit $x \in E$ un antécédent de y : donc $f(x) = y$. Puisque x est un élément de E et que y est une partie de E, on peut se demander si $x \in y$:
- Si $x \in y$, alors, par définition de y, on a $x \notin f(x)$, c'est-à-dire $x \notin y$;
- Si $x \notin y$, c'est-à-dire si $x \notin f(x)$, alors, par définition de y, on a $x \in y$.

On trouve donc une contradiction, et l'hypothèse $f(x) = y$ est intenable. □

L'ensemble $\mathcal{F}(E, F)$ des applications de E dans F

Axiome.
Les applications de E dans F forment un ensemble noté $\mathcal{F}(E, F)$ ou F^E.

Pour expliquer la deuxième notation, nous allons faire le lien entre applications et *suites*. Pour cela, nous supposons déjà connu l'ensemble $\mathbf{N}$ des entiers naturels.

Soit $n \in \mathbf{N}^*$ un entier naturel non nul. Notons $[\![1, n]\!]$ l'intervalle $\{1, \ldots, n\}$. Il revient au même de se donner une application $f : [\![1, n]\!] \to E$ ou le n-uplet $\big(f(1), \ldots, f(n)\big) \in E^n$. Il est d'usage de noter une telle application (ou un tel n-uplet) avec des "indices" : $(u_1, \ldots, u_n) \in F^n$ (c'est une *suite finie*). On peut donc *identifier* $\mathcal{F}([\![1, n]\!], F) = F^{[\![1,n]\!]}$ à F^n, ce qui explique en partie la notation F^E. On verra d'ailleurs, dans l'étude des dénombrements (chapitre 2), que, si F est un ensemble fini :

$$\mathrm{card}\ \mathcal{F}(E, F) = (\mathrm{card}\ F)^{\mathrm{card}\ E}.$$

En fait, cela découle directement de l'identification ci-dessus.

De la même manière, il revient au même de se donner une application $f : \mathbf{N} \to E$ ou la *suite* $\big(f(0), f(1), \ldots\big)$ de ses valeurs. On emploie alors plutôt la "notation indicielle" $(u_0, u_1, \ldots) \in F^{\mathbf{N}}$, ce que l'on abrège souvent en $(u_n)_{n \in \mathbf{N}}$.

Un peu de généralisation. Considérons un "ensemble d'indices" I. La "notation indicielle" d'une application $f : I \to E$ est la convention d'écriture $f_i := f(i)$. L'application f est alors notée $(f_i)_{i \in I}$ et appelée "famille d'éléments de E indexée par I". On a alors : $(f_i)_{i \in I} \in F^I$. Cette notion généralise la notion de suite. Nous ne détaillerons pas le formalisme associé.

Fonctions caractéristiques. Il y a un lien étroit entre les sous-ensembles d'un ensemble fixé E et les applications de E dans $\{0,1\}$, et ce lien a d'ailleurs des applications en informatique. Pour l'expliquer, nous admettrons que l'on dispose de symboles 0 et 1 : on peut les interpréter comme de purs symboles, comme des entiers naturels, ou comme des booléens au sens de la logique ou d'un langage de programmation (Pascal ou CAML par exemple), ou encore comme des bits.

On fixe maintenant un ensemble E. À tout sous-ensemble $F \subset E$, on associe sa *fonction caractéristique* χ_F : c'est l'application de E dans $\{0,1\}$ définie par :

$$\forall x \in E\ ,\ \chi_F(x) := \begin{cases} 1 \text{ si } x \in F, \\ 0 \text{ si } x \notin F. \end{cases}$$

Théorème.
L'application $F \mapsto \chi_F$ est une bijection de $\mathcal{P}(E)$ sur $\mathcal{F}(E,\{0,1\})$.
Démonstration. Soit $\phi : E \to \{0,1\}$ une application quelconque. On définit son *support* $\mathrm{Supp}(\phi) := \phi^{-1}(1) = \{x \in E \mid x = 1\}$, qui est une partie de E. On a l'équivalence :

$$\phi = \chi_F \iff F = \mathrm{Supp}(\phi).$$

Les applications $F \mapsto \chi_F$ et $\phi \mapsto \mathrm{Supp}(\phi)$ sont donc réciproques l'une de l'autre. □

Dans le cas où $E := [\![1,n]\!]$, on a identifié $\mathcal{F}(E,\{0,1\})$ à $[\![1,n]\!]^n$ et les applications $\phi : [\![1,n]\!] \to \{0,1\}$ à des suites finies $(\epsilon_1,\dots,\epsilon_n)$ de 0 et de 1 : donc des *vecteurs de bits*. Le théorème ci-dessus revient donc à dire que l'on peut *coder* les sous-ensembles de E par des vecteurs de bits. (Ce codage est utilisé en Pascal.) Le vecteur $(\epsilon_1,\dots,\epsilon_n)$ code l'ensemble des $i \in [\![1,n]\!]$ tels que $\epsilon_i = 1$. Ce procédé permet de remplacer les opérations ensemblistes par du calcul sur les bits. Par exemple, si $(\epsilon_1,\dots,\epsilon_n)$ code $F \subset E$ et si $(\epsilon'_1,\dots,\epsilon'_n)$ code $F' \subset E$, alors $F \cap F'$ est codé par $(\epsilon_1\epsilon'_1,\dots,\epsilon_n\epsilon'_n)$ ("produit bit à bit"). En effet, pour tout $i \in [\![1,n]\!]$:

$$(\epsilon_i\epsilon'_i = 1) \iff (\epsilon_i = 1 \text{ et } \epsilon'_i = 1) \iff (i \in F \text{ et } i \in F') \iff (i \in F \cap F').$$

De même, si l'on note $\overline{1} := 0$ et $\overline{0} := 1$ ("bit complémentaire"), on voit que le complémentaire $\complement_E F$ est codé par $(\overline{\epsilon_1},\dots,\overline{\epsilon_n})$. On trouvera en exercice d'autres exemples d'opérations ensemblistes réalisées par du calcul sur les bits.

L'usage des fonctions caractéristiques permet une interprétation de la démonstration du théorème de Cantor connue sous le nom de "procédé diagonal". Nous la décrirons dans le cas où $E := [\![1,n]\!]$. Une application f de E dans $\mathcal{P}(E)$ prend la forme d'une suite finie $(F_1,\dots,F_n)$ de parties de E, elles-mêmes codées par des vecteurs de bits $V_1,\dots,V_n \in \{0,1\}^n$. Écrivons les sous la forme $V_i = (\epsilon_{i,1},\dots,\epsilon_{i,n})$ et formons un

tableau : $\begin{vmatrix} V_1 = & \epsilon_{1,1} & \dots & \epsilon_{1,i} & \dots & \epsilon_{1,n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ V_n = & \epsilon_{n,1} & \dots & \epsilon_{n,i} & \dots & \epsilon_{n,n} \end{vmatrix}$. On peut alors *voir* que le vecteur $V := (\overline{\epsilon_{1,1}}, \dots, \overline{\epsilon_{n,n}})$, formé des des bits complémentaires des coefficients diagonaux, ne figure pas comme ligne de ce tableau, donc qu'il n'est égal à aucun des V_i. En fait, il code la partie $\{x \in E \mid x \notin f(x)\}$, qui n'admet pas d'antécédent par f.

Exercice.
Est-ce que l'ensemble d'arrivée et l'ensemble image de f sont égaux ?

Exercice.
Montrer que, si f est injective, alors $f(A \cap B) = f(A) \cap f(B)$; et sinon ?

Exercice.
Si f et g sont injectives (resp. surjectives), il en est de même de $g \circ f$. Réciproque ?

Exercice.
Soient E et F des ensembles, F étant non vide. Pour qu'il existe une application surjective de E sur F, il faut, et il suffit, qu'il existe une application injective de F dans E.

Exercice.
Interpréter en termes de calcul sur les vecteurs de bits la réunion $F \cup F'$ et la différence symétrique $F \oplus F'$. Comment tester l'inclusion $F \subset F'$?

1.1.5 Synthèse

Le principe qui nous guidera dorénavant est le suivant : des axiomes, on a tiré un certain nombre de méthodes raisonnables pour définir ou construire des ensembles. Autant que possible, nous n'utiliserons que ces méthodes. Les méthodes de base sont les suivantes :

1. Pour les petits ensembles, la définition en extension convient.
2. À partir d'un ensemble E déjà construit, on peut extraire des sous-ensembles par la construction $\{x \in E \mid P(x)\}$.
3. À partir d'ensembles déjà connus, on peut en fabriquer de plus gros grâce aux "constructeurs" réunion $E \cup F$, produit $E \times F$, ensemble des parties $\mathcal{P}(E)$, ensemble des applications $\mathcal{F}(E, F) = F^E$.
4. Le cas où $E := \mathbf{N}$ nous fournit l'ensemble $\mathcal{F}(\mathbf{N}, F) = F^{\mathbf{N}}$ des suites d'éléments de F.

Enfin, nous verrons à la section 1.2.4 apparaitre notre premier ensemble infini, $\mathbf{N}$. Au deuxième semestre, on verra que la connaissance de $\mathbf{N}$ et la notion de suite suffisent à construire le corps $\mathbf{R}$ des réels. En fait, *toutes les mathématiques* sont accessibles à

partir de là. (En exceptant certaines branches exotiques de la théorie des ensembles et de la logique mathématique.)

1.2 Relations binaires

1.2.1 Vocabulaire

Une relation est un "prédicat" portant sur un ou plusieurs arguments : $P(x)$ (prédicat simple, ceux que l'on a abordés jusqu'ici), $R(x, y)$ (relation binaire), $S(x, y, z)$ (relation ternaire), etc. Exemple : "x, y, z sont premiers entre eux dans leur ensemble" est une relation ternaire.

Une relation binaire $R(x, y)$ qui n'est définie que pour $x \in E$, $y \in F$, s'appelle *correspondance* entre E et F. Il lui est associé un *graphe* $G_R := \{(x, y) \in E \times F \mid R(x, y)\}$. Par exemple, on peut poser $R(x, y) := (y = f(x))$, où $f : E \to F$ est une application. De même, $x \in y$ définit une correspondance entre E et $\mathcal{P}(E)$.

Une relation binaire $R(x, y)$ qui n'est définie que pour $x, y \in E$ s'appelle *relation binaire sur* E. On rencontre principalement (mais pas uniquement) de telles relations. Exemples : $x \leq y$ est une relation binaire sur $\mathbf{R}$; $x \mid y$ (divisibilité) est une relation binaire sur $\mathbf{N}$; $x \equiv y \pmod{a}$ (congruence) est une relation binaire sur $\mathbf{Z}$; $x \subset y$ est une relation binaire sur $\mathcal{P}(E)$.

Propriétés classiques : réflexivité, symétrie, transitivité, antisymétrie.

Clôture transitive, clôture transitive réflexive.

Facultatif : On peut envisager la notion de graphe décrivant une relation (au sens de la théorie des graphes), la matrice d'adjacence, l'interprétation et le calcul de la clôture transitive réflexive (parties accessibles).

Exercice.
Soit $E = \{a, b, c, d\}$. Soit R une relation dont le graphe est $G = \{(a, b), (b, c)\}$. Déterminer sa clôture transitive réflexive.

1.2.2 Relations d'équivalence

Une *relation d'équivalence* est une relation réflexive, symétrique, transitive. Par exemple, l'égalité est une relation d'équivalence (pas sur un ensemble !), la congruence modulo a est une relation d'équivalence sur $\mathbf{Z}$.

Soit $x \sim y$ une relation d'équivalence sur l'ensemble E. On appelle *classe d'équivalence de* $x \in E$ et l'on note $\mathrm{Cl}(x)$ l'ensemble des éléments de E équivalents à x :

$$\mathrm{Cl}(x) := \{y \in E \mid y \sim x\}.$$

Tout élément d'une telle classe est appelé *un représentant* de la classe. On appelle *ensemble de représentants* une partie qui contient exactement un représentant de chaque classe, *i.e.* $F \subset E$ telle que $\forall x$, $\mathrm{Cl}(x) \cap F$ est un singleton. Exemples : pour la congruence modulo a sur $\mathbf{Z}$, l'ensemble $0, \dots a-1$; pour la congruence modulo 2π sur $\mathbf{R}$, chacun des intervalles $]-\pi, \pi]$ et $[0, 2\pi[$, mais pas les intervalles $[0, 2\pi]$ et $]0, 2\pi[$.

Les classes d'équivalence forment une *partition* de E : elles sont non vides, deux à deux disjointes et leur réunion est E. Réciproquement, toute partition $(E_i)_{i\in I}$ de E provient d'une relation d'équivalence définie par : $x \sim y$ si, et seulement si, x et y sont dans le même E_i. Remarquer l'usage "intuitif" de la notation $(E_i)_{i\in I}$ pour une famille de parties : on ne fondera pas la notion de famille, il faudra guider l'usage.

On veut savoir dans quelle mesure on peut travailler avec des objets "connus à équivalence près" : par exemple, peut-on calculer avec l'argument d'un complexe qui n'est qu'un réel "connu à 2π près", ce qui signifie "connu à congruence modulo 2π près". Peut-on calculer le double d'un argument, sa moitié, etc ? On constate que le double d'un argument est bien défini (il ne dépend pas du représentant choisi pour le calculer), mais pas sa moitié. En tout cas, celle-ci n'est ni un réel ni un argument ... Notant $\mathbf{R}/2\pi\mathbf{Z}$ l'ensemble des arguments (notation qui sera expliquée une autre année), on en tire l'existence d'une application $\overline{\theta} \mapsto \overline{2\theta}$ de $\mathbf{R}/2\pi\mathbf{Z}$ dans lui même (on abrège $\overline{\theta} := \theta \pmod{2\pi}$) ; ou encore la possibilité d'additionner les arguments ; mais pas celle de les diviser par 2, ni de les multiplier entre eux.

Dans ce qui suit, on fixe E muni de la relation d'équivalence $x \sim y$. La classe de $x \in E$ est notée $\overline{x}$. On dira que x (ou tout $y \sim x$) est un représentant de la classe $\overline{x}$, etc. On notera $\overline{E}$ ou$E/\sim$ l'ensemble des classes, que l'on appellera *ensemble quotient de* E *par la relation d'équivalence* $\sim$:

$$\overline{E} := E/\sim := \{\overline{x} \mid x \in E\}.$$

Il est certain que cet ensemble existe et que c'est une partie de $\mathcal{P}(E)$ (*i.e.* un ensemble de parties de E). On note $p : E \to \overline{E}$ l'application qui, à tout élément, associe sa classe (elle est évidemment surjective).

Il n'est pas judicieux dans ce type de raisonnement de se polariser sur le fait que $\overline{x}$ *est un ensemble et que* $x, y, \dots$ *en sont des éléments.* Il vaut mieux penser à $\overline{x}$ comme à x "incomplètement connu", avec la seule règle : $\overline{x} = \overline{y} \Leftrightarrow x \sim y$ et la seule méthode : pour tout calcul sur une classe, on commence par en choisir un représentant, puis on

vérifie à la fin que le calcul ne dépend pas du choix arbitraire du représentant.

On commence par le cas de $f : E \to F$. On veut savoir s'il est possible de définir $\overline{f} : \overline{E} \to F$ par la formule :

$$\overline{f}(\overline{x}) := f(x).$$

Pour que ce soit possible, il faut, et il suffit, que le membre de droite de l'égalité ne dépende pas du choix du représentant x de $\overline{x}$, autrement dit, que :

$$\forall x, y \in E \ , \ \overline{x} = \overline{y} \Longrightarrow f(x) = f(y).$$

De manière équivalente :

$$\forall x, y \in E \ , \ x \sim y \Longrightarrow f(x) = f(y).$$

On dit alors que *la relation $\sim$ et l'application f sont compatibles*. Dans ce cas, $\overline{f}$ existe (et est uniquement déterminé) et l'on dit que f *passe au quotient en* $\overline{f} : \overline{E} \to F$. Noter que cela signifie que $f = \overline{f} \circ p$ (on peut faire le "diagramme commutatif" correspondant).

Corollaire.
On suppose que E est muni de la relation d'équivalence $\sim$ et F de la relation d'équivalence $\equiv$, et que $f : E \to F$ est telle que : $\forall x, y \in E \ , \ x \sim y \Longrightarrow f(x) \equiv f(y)$. Alors f passe au quotient en $\overline{f} : \overline{E} \to \overline{F}$.
Démonstration. supozon □

De la même manière, on est conduit à se demander si une loi de composition $\star$ sur E passe au quotient en une loi $*$ sur $\overline{E}$, définie par la formule :

$$\overline{x} * \overline{x'} := \overline{x \star x'}.$$

La condition nécessaire et suffisante est que *la relation $\sim$ et la loi de composition $\star$ soient compatibles*, autrement dit :

$$\forall x, x', y, y' \in E \ , \ x \sim y \text{ et } x' \sim y' \Longrightarrow x \star x' \sim y \star y'.$$

Dans ce cas, la loi de composition $*$ existe (et est uniquement déterminée) et l'on dit que *la loi de composition $\star$ passe au quotient en la loi de composition $*$*.

Exercice.
Appliquer le corollaire à la division par deux d'un argument.
D'où vient l'unicité de $\overline{f}$ et de $*$?

Exercice.
Pour une loi de composition, il suffit de vérifier la compatibilité à gauche et la compatibilité à droite.

1.2.3 Relations d'ordre

Une *relation d'órdre* est une relation réflexive, antisymétrique, transitive. Par exemple, l'inclusion est une relation d'ordre (pas sur un ensemble !), la relation $x \leq y$ est une relation d'ordre sur $\mathbf{R}$, la relation $x|y$ est une relation d'ordre sur $\mathbf{N}$ (mais pas sur $\mathbf{Z}$).

Si $x \preceq y$ est une relation d'ordre, on définit *l'ordre strict asocié* par :

$$x \prec y \Longleftrightarrow x \preceq y \text{ et } x \neq y.$$

C'est une relation transitive et antiréflexive (*i.e.* on n'a jamais $x \prec x$). Réciproquement, de toute relation d'ordre strict (transitive et antiréflexive) on déduit une relation d'ordre en posant :

$$x \preceq y \Longleftrightarrow x \prec y \text{ ou } x = y.$$

Définition : ordre total ; exemples, contre-exemples.

Ordre produit, ordre lexicographique (sur un produit de deux ou d'un nombre fini d'ensembles seulement). Cas où l'on part d'ensembles totalement ordonnés.

Majorant, minorant d'un ensemble ; maximum, minimum ; élément maximal, élément minimal ; borne inférieure, borne supérieure ; successeur, prédécesseur (sous-entendu : immédiats). Liens logiques entre ces notions, existences et unicités éventuelles.

Application croissante, décroissante, monotone, strictement croissante, strictement décroissante, strictement monotone. Suite croissante, décroissante, monotone, strictement croissante, strictement décroissante, strictement monotone. (On remarque qu'une suite est, sauf pour la notation, une application de $\mathbf{N}$ dans E.)

Propriétés algébriques. La question de la compatibilité avec une loi de composition ne se traite pas de la même manière dans le cas, par exemple, de l'addition et de la multiplication de $\mathbf{R}$. Dans le cas d'un "groupe commutatif", on imposera la règle suivante :

$$\forall a, b, c \in E \ , \ a \leq b \Longrightarrow a + c \leq b + c.$$

On a alors les règles de calcul connues dans $(\mathbf{R}, +)$. Il revient au même de se donnner l'ensemble $E_+ := \{x \in E \mid 0 \leq x\}$ des éléments positifs ou nuls, qui est caractérisé par les propriétés suivantes :

$$\begin{aligned} E_+ + E_+ &\subset E_+, \\ E_+ \cap (-E_+) &= \{0\}. \end{aligned}$$

L'ordre défini par un tel E_+ est total si, et seulement si, $E_+ \cup (-E_+) = E$.

Dans le cas d'un "corps (ou anneau) commutatif" $(E, +, .)$, tel que $(E, +)$ est déjà un groupe ordonné, on imposera la règle suivante :

$$\forall a, b \in E\ ,\ 0 \leq a \text{ et } 0 \leq b \Longrightarrow 0 \leq a.b.$$

Si la relation d'ordre a été définie à l'aide de E_+, cela équivaut à la condition :

$$E_+.E_+ \subset E_+. \tag{1.2}$$

On a alors les règles usuelles de calcul de $(\mathbf{R}, +, .)$.

On est évidemment intéressé par les corps (ou anneaux) *totalement* ordonnés (on leur réserve d'ailleurs l'appellation de *corps ordonnés*). Dans ce cas, on prouve alors les faits suivants : tout carré est positif (on a $x \leq 0$ ou $0 \leq x$ et, dans les deux cas, $0 \leq x^2$) ; -1 n'est pas un carré (en effet, on ne peut avoir $0 \leq -1$ car $0 < 1$). *Il est donc impossible de mettre un ordre sur* $\mathbf{C}$ *qui en fasse un corps ordonné.*

Induction. Un ensemble *noetherien* est un ensemble dans lequel toute suite croissante est stationnaire ; ou bien, de manière équivalente (et on le prouve) : toute partie non vide admet un élément maximal.

Un ensemble *artinien* est un ensemble dans lequel toute suite décroissante est stationnaire ; ou bien, de manière équivalente (et on le prouve) : toute partie non vide admet un élément minimal.

Un ensemble *bien ordonné* est un ensemble totalement ordonné et artinien ; ou bien, de manière équivalente (et on le prouve) : toute partie non vide admet un minimum. Par exemple, $\mathbf{N}$ est bien ordonné, l'ensemble des parties finies de E quelconque est artinien.

Théorème *(Principe d'induction).*
Soit $(E, \preceq)$ un ensemble artinien et soit $P(x)$ un prédicat sur E qui satisfait la propriété d'*hérédité* :

$$\forall x \in E\ \big(\forall y \prec x\ ,\ P(y)\big) \Longrightarrow P(x).$$

Alors :

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

Démonstration. supozon Preuve par l'absurde : si $\{x \in E \mid \neg P(x)\}$ est non vide, il admet un minimal, etc. L'exemple de $\mathbf{N}$: pourquoi n'a-t-on pas besoin d'initialiser la récurrence (forte) ?
□

L'ordre produit sur un produit fini d'ensembles artiniens ; l'ordre lexicographique sur un produit fini d'ensembles bien ordonnés.

Exercice.
Dans quel cas un ordre produit est-il total ?

1.2.4 Cardinaux

On dit que deux ensembles E et F sont *équipotents* s'il existe une bijection de E sur F. L'équipotence est une relation d'équivalence, qui signifie "avoir le même nombre d'éléments", à cela près quel'on n'a pas encore défini le "nombre d'éléments".

À tout ensemble E on associe un objet appelé *cardinal de* E et noté card E, qui vérifie la propriété suivante :

$$(\text{card } E = \text{card } F) \iff (E \textit{ est équipotent à } F).$$

(Il ne va pas de soi qu'il existe de tels objets : c'est un axiome.) Exemples :
Le seul ensemble équipotent à $\emptyset$ est lui-même ; son cardinal est noté 0.
Les singletons sont équipotents entre eux. Leur cardinal est noté 1.
Les paires sont équipotentes entre elles. Leur cardinal est noté 2.
(Ces trois cardinaux sont deux à deux distincts.)

On définit la relation suivante entre cardinaux : card $E \leq$ card F s'il existe une application injective de E dans F. Pour que cette définition ait un sens, il faut vérifier qu'en changeant respectivement E et F par des ensembles équipotents E' et F', la propriété est conservée. (On a $i : E \to F$ injective, $u : E \to E'$ bijective et $v : F \to F'$ bijective ; alors $i' : E' \to F'$ est injective, où $i' := v \circ i \circ u^{-1}$.) La relation ainsi définie est évidemment réflexive et transitive.

Théorème *(Cantor, Schröder, Bernstein).*
La relation $\leq$ entre cardinaux est une relation d'ordre.
Pratiquement, il s'agit de démontrer que, s'il existe une injection de E dans F et une injection de F dans E, alors il existe une bijection entre eux. C'est élémentaire mais compliqué et nous l'admettrons.
Démonstration. supozon □

On note $<$ la relation d'ordre stricte associée. On voit facilement que $1 < 2$, que pour tout ensemble non vide E, $1 \leq$ card E, que l'on n'a jamais card $E < 0$. On voit aussi que, pour tout ensemble non vide E, on a $0 <$ card E : soit en admettant la notion d'application vide (pourquoi pas ?) soit en le posant comme convention.

Enfin, on remarque la possibilité d'un autre critère : si E et F sont non vides, card $E \leq$ card F équivaut à l'existence d'une surjection de F sur E. Comme $x \mapsto \{x\}$ est une injection de E dans $\mathcal{P}(E)$ et qu'il n'existe pas de surjection, on en déduit que

card $\mathcal{P}(E) >$ card E.

Théorème (Cantor) : C'est un ordre total.
On prouve (mais ce n'est pas élémentaire) qu'il existe toujours une injection de E dans F ou une injection de F dans E. Nous l'admettrons.

Opérations sur les cardinaux. Pour additionner des cardinaux, il faut évidemment réunir des ensembles *disjoints*. Or, si E et F sont quelconques, $E \times \{0\}$ et $F \times \{1\}$ leur sont respectivement équipotents (bijections $x \mapsto (x, 0)$ et $y \mapsto (y, 1)$) et sont disjoints (on ne peut avoir $(x, 0) = (y, 1)$). On posera donc card $E +$ card $F :=$ card $(E \times \{0\} \cup F \times \{1\})$. Il faut évidemment vérifier que, si l'on remplace E et F par des ensembles équipotents E' et F', on obtient le même résultat, autrement dit, que $E \times \{0\} \cup F \times \{1\}$ et $E' \times \{0\} \cup F' \times \{1\}$ sont équipotents (ce qui est facile).
On vérifie sans peine que l'addition des cardinaux est commutative et associative et que 0 est élément neutre. On calcule de plus :

$$1 + 1 = 2.$$

On peut ensuite définir les "cardinaux finis" usuels : $3 := 2 + 1$, $4 := 3 + 1$, etc. Nous y reviendrons plus loin.

Pour multiplier les cardinaux, c'est plus simple : on pose card Ecard $F :=$ card $E \times F$. Il faut évidemment vérifier que, si l'on remplace E et F par des ensembles équipotents E' et F', on obtient le même résultat, autrement dit, que $E \times F$ et $E' \times F'$ sont équipotents (ce qui est facile).
On vérifie sans peine que la multiplication des cardinaux est commutative et associative et que 1 est élément neutre et 0 est élément absorbant ($E \times \emptyset$ est vide). La multiplication est distributive par rapport à l'addition. On calcule de plus :

$$2 \times 2 = 4.$$

Il reste l'exponentiation. On pose : $(\text{card } F)^{\text{card } E} :=$ card $\big(\mathcal{F}(E, F)\big)$. Cette définition paraitra plus naturelle après lecture du chapitre 2.

Théorème : On a l'égalité :

$$\text{card } \mathcal{P}(E) = 2^{\text{card } E}.$$

Cela découle de la bijection entre $\mathcal{P}(E)$ et $\mathcal{F}(E, \{0, 1\})$.

Cardinaux finis et infinis. On dit qu'un ensemble est *infini* s'il est en bijection avec une partie stricte de lui-même : par exemple, $\mathbf{N}$ avec $\mathbf{N}^*$ ou avec $2\mathbf{N}$, $\mathbf{Z}$ avec $\mathbf{N}$, $\mathbf{R}$ avec $\mathbf{R}_+^*$ ou avec $]-1, 1[$, etc. (Ce sont des exemples faciles ; de moins faciles suivront.)

On dit qu'un ensemble est *fini* dans le cas contraire. Ces propriétés sont conservées par bijection, on peut donc parler de *cardinaux finis* et de *cardinaux infinis*.

À partir des axiomes que nous avons énoncé, on démontre que les cardinaux $0, 1, \ldots$ sont finis et que ce sont les seuls. Nous les appellerons *entiers naturels* (ce sont eux qui ont servi depuis toujours à compter les troupeaux, les étoiles et les jours avant les vacances).

En revanche, on ne peut en déduire qu'il existe des cardinaux infinis. Il faut pour cela un nouvel axiome, l'axiome de l'infini. Nous le remplacerons par un axiome qui lui est équivalent mais qui est plus commode : les entiers naturels forment un ensemble, noté $\mathbf{N} := \{0, 1, 2, 3, \ldots\}$. Il est clair que c'est un ensemble totalement ordonné, et la notation suivante a un sens :

$$[\![0, p]\!] := \{0, 1, \ldots, p\}.$$

En fait, on prouve sans trop de difficulté que c'est un ensemble bien ordonné, chaque élément n a un successeur qui est $n+1$ et chaque élément non nul n a un prédécesseur, qui est noté $n-1$. De même, on peut retrouver à partir de là toute l'arithmétique élémentaire. *Nous l'admettrons.*

Pour en revenir aux cardinaux finis et infinis, on démontre alors :
L'ensemble $\mathbf{N}$ est infini. Son cardinal est noté $\aleph_0$ (ce qui se lit aleph zéro).
Tout ensemble fini est équipotent à un unique $[\![0, n-1]\!]$, et n est son cardinal.
Tout ensemble infini a un cardinal $\geq \aleph_0$, autrement dit, $\aleph_0$ est le plus petit cardinal infini.

Ensembles dénombrables. Un ensemble est dit *dénombrable* s'il est de cardinal $\aleph_0$, c'est-à-dire s'il peut être mis en bijection avec $\mathbf{N}$. Une bijection de $\mathbf{N}$ sur E est appelée une *énumération* de E. Par exemple, on énumère $\mathbf{Z}$ par $n \mapsto n/2$ si n pair, $n \mapsto -(n+1)/2$ si n impair. Donc $\operatorname{card} \mathbf{Z} = \aleph_0$. On énumère $\mathbf{Z} \setminus \mathbf{N}$ par $n \mapsto -(n+1)$. Comme l'ensemble dénombrable $\mathbf{Z}$ est l'union disjointe des ensembles dénombrables $\mathbf{N}$ et $\mathbf{Z} \setminus \mathbf{N}$, on a prouvé :

$$\aleph_0 + \aleph_0 = \aleph_0.$$

On aurait aussi pu utiliser l'union disjointe $\mathbf{N}$ de $2\mathbf{N}$ et de $2\mathbf{N}+1$.

On peut énumérer $\mathbf{N} \times \mathbf{N}$ en parcourant successivement les ensembles suivants : $\{(0,0)\}$, puis $\{(1,0),(0,1)\}$, puis $\{(2,0),(1,0),(2,2)\}$, etc. On vérifie que l'image de n s'obtient comme suit : on encadre n par $\dfrac{k(k+1)}{2} \leq n < \dfrac{(k+1)(k+2)}{2}$, ce qui revient à écrire $n = \dfrac{k(k+1)}{2} + l$, avec $0 \leq l \leq k$. Cette écriture est unique. On associe alors à

n le couple $(k-l,l) \in \mathbf{N}\times\mathbf{N}$. De cette énumération, on déduit que card $\left(\mathbf{N}\times\mathbf{N}\right) = \aleph_0$. On a prouvé :

$$\aleph_0\aleph_0 = \aleph_0.$$

Il en découle que, si $(E_n)_{n\in\mathbf{N}}$ est une suite d'ensembles au plus dénombrables, alors $\bigcup_{n\in\mathbf{N}} E_n$ est au plus dénombrable : en effet, son cardinal est majoré par $\aleph_0\aleph_0 = \aleph_0$. C'est donc soit un ensemble fini soit un ensemble dénombrable (en général, il est facile de trancher).

Cet énoncé est très important en analyse, car, comme on va le voir, $\mathbf{R}$ est infini non dénombrable. Une première conséquence est que tout intervalle ouvert non vide de $\mathbf{R}$ est infini non dénombrable (il est en bijection avec $\mathbf{R}$ via la composée de tan et d'une fonction affine), donc aussi tout intervalle non vide et non réduit à un point. À l'inverse, les parties dénombrables de $\mathbf{R}$ sont très petites et très rares (dispersées) : cela sera précisé en topologie et en analyse.

Reste à prouver que $\mathbf{R}$ est infini (c'est évident, il contient $\mathbf{N}$) et non dénombrable. On sait que card $\mathcal{P}(\mathbf{N}) = 2^{\aleph_0} > \aleph_0$. On obtient une application injective de $\mathcal{P}(\mathbf{N})$ dans $\mathbf{R}$ comme suit : à toute partie $A \subset \mathbf{N}$ on associe $\sum_{a\in A} 10^{-a}$ (réel dont le développement décimal a des 1 aux endroits codés par A, des 0 ailleurs). On en déduit que card $\mathbf{R} \geq$ card $\mathcal{P}(\mathbf{N}) = 2^{\aleph_0} > \aleph_0$. En fait, on peut montrer que card $\mathbf{R} = 2^{\aleph_0}$, mais c'est un petit peu plus fatigant.

Exercice.
Existe-t-il un cardinal plus grand que tous les autres ?

Exercice.
Démontrer la distributivité de la multiplication par rapport à l'addition.

Exercice.
Montrer que $\mathbf{Q}$ est dénombrable.

Chapitre 2

Dénombrements

Référence pour ce chapitre : le module II.1 du L1, section 2.2.

On admet : $\mathbf{N}$, sa relation d'ordre, le principe de récurrence (trois formes au moins : simple, forte, à deux pas), sa structure algébrique.

Tout ensemble fini E est équipotent à un unique intervalle $[\![0, n-1]\!]$, et card $E = n$.

On sait : card $(A \coprod B) =$ card $A +$ card B et card $(A \times B) = (\text{card } A)(\text{card } B)$.

On redémontre : card $\mathcal{F}(E, F) = (\text{card } F)^{\text{card } E}$ et card $\mathcal{P}(E) = 2^{\text{card } E}$, en remplaçant E par $[\![0, n-1]\!]$ et par bijection explicite avec F^n, avec $\{0,1\}^n$.

Soit $f : E \to F$, où card $E =$ card F. Alors f injective sssi bijective sssi surjective.

Principe de Dirichlet (ou des tiroirs), exemples amusants.

Principe des bergers, exemples utiles.

Cardinal d'une réunion, formule d'inclusion-exclusion (preuve énumérative et preuve algérbrique).

Nombre d'arrangements, de permutations, de combinaisons.

Étude des coefficients binomiaux : formule et triangle de Pascal ; formule du binôme ; diverses identités classiques, avec preuve algébrique et preuve combinatoire.

Exos :
Nombre de surjections.

Nombre de dérangements.

Chapitre 3

Arithmétique élémentaire

Chapitre 4

Suites numériques