Théorie des ensembles

Roland Christophe

4 avril 2014

Table des matières

1 Une branche fondamentale

1.1 Introduction - paradoxe de Galilée

À la fin du XIXe siècle, un mathématicien, Georg Cantor, posa les bases de la théorie des ensembles. L'étude des ensembles en mathématique est donc relativement récente. Le développement de cette théorie a permis d'apporter certaines réponses à des questions mathématiques délicates sur l'infini.

Le problème se pose avec un énoncé qui semble très intuitif (considéré même comme un axiome) qui est le suivant : «le tout est plus grand que la partie». Cet axiome a été énoncé au départ par Euclide et semblait tellement évident que certains mathématiciens comme Leibniz ne pouvaient même pas imaginer qu'il soit mis en défaut. Pourtant, cet axiome mène à un paradoxe : *le paradoxe de Galilée.*

Ce paradoxe est simple à énoncer : «un segment de 2 cm ne contient pas plus de points qu'un segment de 1 cm». Cette fois ci on a vraiment quelque chose de contre-intuitif ! ! Mais si on arrive à démontrer cette assertion, on aura une contradiction avec l'axiome vu précédemment ce qui l'invaliderai. Voyons si c'est possible.

Intuitivement, on se dit que le segment de 2 cm contient deux fois plus de points que le segment de 1 cm (donc il y a plus de point). Mais le nombre de points est infini et il faut se méfier de l'intuition. Dans ce cas, comment comparer le nombre de points ? On va essayer de préciser ce que l'on entend par «même nombre de points» et surtout, comment on fait pour le savoir.

C'est très simple, même intuitif. Si on a deux groupes de personnes par exemple (un groupe «A» et un groupe «B»), et que l'on veut savoir si il y a autant de personnes dans chaque groupe, un moyen possible est de ranger ces personnes par groupes de deux. Dans chacun de ces groupes de deux, on a une personne du groupe «A» et une personne du groupe «B». Si cela est possible sans qu'il reste de personne en dehors de ce groupement, alors il y a autant de personnes dans le groupe «A» que dans le groupe «B».

Appliquons cela pour les points des segments. Pour y voir plus clair, on va placer les deux segments de telle sorte qu'ils aient une extrémité en commun (que nous appeler O) et que les segment soient superposées. Si on choisit un point quelconque sur le petit segment, il est a une certaine distance de O (distance comprise entre zéro et un centimètre). À ce point on va faire correspondre un point deux fois plus éloigné de O, on aura que cet autre point est sur le grand segment. On peut faire correspondre à chaque point sur le petit segment un point sur le grand segment et inversement. On a donc réussi à faire ce groupement par deux et la conclusion est là : il y a autant de points sur le grand que sur le petit segment !

De ce genre de considérations va naître la théorie des ensembles. Parler d'ensemble infini mène parfois à des paradoxes si on n'y prend pas garde. Cela ne veut pas dire que ces ensembles n'existent pas (dans le sens qu'ils seraient impossibles à définir mathématiquement) mais qu'il faudra faire bien attention.

1.2 La crise des fondements

Au départ, la théorie des ensembles (qualifiée aujourd'hui souvent de «naïve») a été développée principalement par Cantor. Cette théorie a vite montré ses lacunes car on a découvert des paradoxes dans la théorie ce qui a provoqué une sorte de crise des mathématiques : la crise des fondements.

Donnons en exemple un paradoxe nommé "Paradoxe de Russell".

Ce paradoxe peut s'énoncer assez simplement. On considère l'ensemble des ensembles n'appartenant pas à eux-mêmes. Cet ensemble est-il élément de lui même ou pas ?

1. Si on répond que oui, alors par définition, il n'est pas élément de lui même...
2. Si on répond que non, alors par définition, il est cette fois ci élément de lui même.

On a là une contradiction apparemment incontournable, ce qui a intrigué beaucoup de mathématiciens.

Il existe une formulation plus simple de ce paradoxe, une illustration attribué à Russell en personne. Il s'agit du paradoxe du barbier :

C'est un barbier à qui l'on demande de raser tous les hommes du village qui ne se rasent pas eux-mêmes, *et seulement ceux-là*. Le problème est le suivant : se rase-t-il lui-même ou pas ?

1. Si il se rase lui-même, il ne doit pas se raser...
2. Si il ne se rase pas lui-même, alors il doit se raser !

Cette illustration simple du paradoxe de Russell a l'avantage d'être facile à résoudre : on voit que la règle imposée au barbier est absurde, et qu'un barbier capable de respecter cette règle n'existe pas. Tout comme il est absurde de définir un ensemble comme étant l'ensemble des ensembles n'appartenant pas à eux-mêmes.

Pour éviter ce genre de paradoxe, il faut donc axiomatiser la théorie des ensembles. En effet, nous avons vu que toute théorie doit être basée sur une axiomatique, et que cette théorie doit être consistante. Si on tombe sur des paradoxes, la théorie n'est pas consistante, et il faut changer un ou plusieurs axiomes.

C'est le travail qui a été fait par les mathématiciens sur la théorie des ensembles. On obtient alors *l'axiomatisation de Zermelo-Fraenkel*, et on obtient une théorie consistante. On ajoute à cette axiomatique un axiome supplémentaire : l'axiome du choix, et on parle donc souvent de l'axiomatique ZFC.

1.3 Quelques remarques sur les axiomes ZFC

On a donc des objets mathématiques appelés *ensembles* qui sont simplement définis comme étant des groupements d'objets. Attention, il s'agit d'une définition «naïve», la notion d'ensemble est défini correctement par les axiomes ZFC.

Les axiomes de la théorie des ensembles sont en fait assez simples à comprendre et la seule difficulté c'est peut être de comprendre l'axiome écrit de manière formelle. Il faut préciser en effet que les notions vues dans le cours de logique sont supposées connues, car les axiomes sont écrit dans le langage de la logique des prédicats égalitaire, avec juste le symbole $\in$ en plus (plus d'autre que l'on peut définir, c'est à dire des symboles non primitifs, comme $\subset$ par exemple). On peut donner un sens intuitif à «$\in$» : si on écrit $A \in B$ par exemple, on dit que A est un élément de B.

On peut encore préciser qu'en théorie des ensembles, on ne considère *que* des ensembles, par exemple, tout les éléments d'un ensemble sont des ensembles (et on verra même que l'on peut considérer les nombres $0, 1, 2, 3, \ldots$ comme des ensembles !).

Une dernière remarque : vous verrez peut être des cours de théorie des ensembles où il y a plus d'axiomes, mais dans ce cas certains axiomes peuvent se déduire des autres. Ici, j'ai choisi de ne mettre que des axiomes indépendants.

2 Axiome d'extensionnalité

2.1 Idée générale de l'axiome

Cet axiome définit l'égalité de deux ensemble : si ils ont les mêmes éléments alors ils sont égaux. On peut déjà tirer comme conclusion qu'il n'y a pas d'ordre dans les éléments d'un ensemble, on peut lister les éléments d'un ensemble dans l'ordre que l'on veut : on a toujours le même ensemble. Puisqu'un ensemble n'est définit que par ses éléments, on dit qu'un ensemble ne dépend que de son *extension*.

2.2 Énoncé de l'axiome

Axiome : *Si deux ensembles ont les mêmes éléments, alors ils sont égaux.*

2.3 Écriture formelle

On peut écrire cet axiome de manière formelle en utilisant ce qui a été vu au cours de logique. Considérons deux ensembles quelconques, A et B. On regarde tous les ensembles possibles X, on a, si $A = B$:

1. si X appartient à A, alors X appartient à B,
2. si X appartient à B, alors X appartient à A.

Ceci peut s'écrire en utilisant le langage de la logique (voir section précédente) :

$$(X \in A \Rightarrow X \in B) \wedge (X \in B \Rightarrow X \in A)$$

qui n'est jamais que la traduction en langage mathématique de ce que nous avons écrit en français.

Or nous avons vu dans le cours de logique ce que nous avions appelé une tautologie remarquable :

$$(A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B) \wedge (B \Rightarrow A))$$

qui dit que si A implique B et B implique A, alors A est équivalent à B. On peut appliquer cela à l'expression que nous venons d'écrire et on obtient :

$$X \in A \Leftrightarrow X \in B$$

Si cette condition est remplie quel que soit l'ensemble X (c'est à dire dans le langage de la logique : $\forall X, X \in A \Leftrightarrow X \in B$) alors on a que $A = B$ et on peut écrire l'axiome en langage formel :

$$\boxed{\forall A, \forall B, ((\forall X, X \in A \Leftrightarrow X \in B) \Rightarrow A = B)}$$

3 Axiome de la réunion

3.1 Idée générale de l'axiome

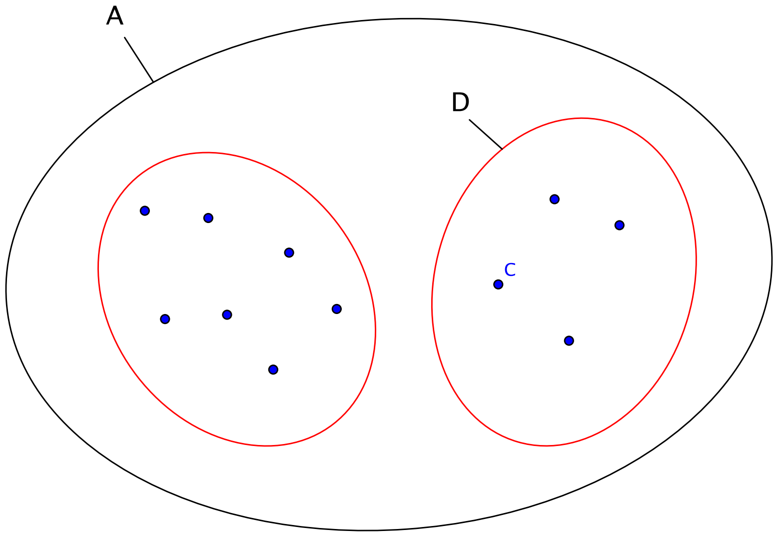
Cet axiome est utile pour définir la notion de l'union de deux ensembles (concept que l'on verra plus tard). Il exprime que pour un ensemble donné, il existe un ensemble qui est l'ensemble des éléments des éléments de cet ensemble.

3.2 Énoncé de l'axiome

Axiome : *Quel que soit l'ensemble A, il existe un ensemble B tel que les élément de B soient les éléments de tout les éléments de A.*

3.3 Écriture formelle

Considérons l'illustration ci-dessous :



Sur ce dessin, on a représenté un ensemble A quelconque ainsi que deux de ses éléments. Ici il faut faire attention car le dessin est trompeur : on pourrait croire que les deux «patates» en rouges sont des sous-ensembles alors que ce sont des *éléments* de A.

L'un des éléments de A est un ensemble noté D dont l'un des éléments est C. L'axiome nous dit qu'il existe un ensemble B qui est l'ensemble des éléments des éléments de A. Cet ensemble B est représenté sur ce dessin en pointillés bleu, on a en particulier $C \in B$.

À partir de ce dessin, on peut essayer de trouver la formulation formelle de l'axiome. Soit donc un ensemble A quelconque. On doit exprimer qu'il existe un ensemble B qui soit l'ensemble des éléments des éléments de A. Pour cela, considérons un ensemble quelconque C. On a, si C appartient à B, que C appartient à un élément de A. Appelons D cet élément. On a :

$$D \in A \wedge C \in D$$

Cet ensemble D n'existe que si il existe un ensemble C appartenant à B. On peut intégrer tout cela en une expression logique qui est donc :

$$C \in B \Rightarrow \exists D, D \in A \wedge C \in D$$

Cela marche aussi dans l'autre sens, c'est à dire que si D est un ensemble appartenant à A alors il existe un ensemble B tel que C appartient à B et à D (voir encore schéma). On peut donc écrire :

$$\exists D, D \in A \wedge C \in D \Rightarrow C \in B$$

Comme pour l'axiome précédent, on peut invoquer la tautologie :

$$(A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B) \wedge (B \Rightarrow A))$$

qui permet comme nous l'avons vu de remplacer deux implications par une équivalence.

On peut écrire l'axiome de manière formelle :

$$\boxed{\forall A, \exists B, \forall C, (C \in B \Leftrightarrow \exists D(D \in A \wedge C \in D))}$$

On verra un peu plus tard comment on définit l'union de deux ensembles (et surtout montrer que l'union de deux ensembles est un ensemble) et on se servira de cet axiome.

4 Axiome de l'ensemble des parties

4.1 Idée générale de l'axiome

Cet axiome introduit l'idée de «sous-ensemble». Il affirme que pour un ensemble donné, il existe un ensemble qui est l'ensemble des sous-ensemble de cet ensemble. On va donc préciser cette notion de sous-ensemble avant d'énoncer l'axiome.

4.2 Notion de sous-ensemble

La notion de sous-ensemble est simple à comprendre. Considérons deux ensembles quelconques A et B. On dit que B est un sous-ensemble de A si tout les éléments de B sont aussi éléments de A. Dans ce cas note :

$$A \subset B$$

On introduit donc un nouveau symbole : «$\subset$». Il est possible de le définir avec les notations vues en logique. En regardant la définition de la notion de sous-ensemble, on peut se rendre compte que la formule :

$$\forall X, X \in A \Rightarrow X \in B$$

et équivalent à écrire $A \subset B$ ce qui définit donc le symbole «$\subset$».

Remarque : on dit aussi lorsque $A \subset B$ que A est *inclus* dans B.

4.3 Énoncé de l'axiome

Axiome : *Quel que soit l'ensemble A, il existe un ensemble noté $P(A)$ qui est l'ensemble des sous-ensembles de A.*

4.4 Écriture formelle

En langage formel, l'axiome s'écrit :

$$\boxed{\forall A, \exists P, \forall X (X \in P \Leftrightarrow X \subset A)}$$

5 Schéma d'axiomes de remplacement

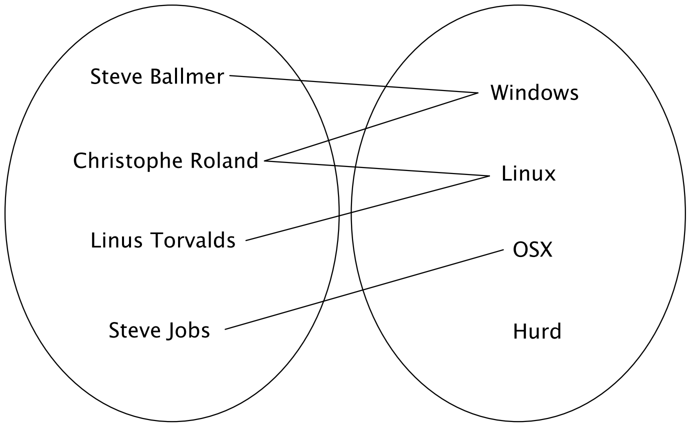
5.1 Idée générale de l'axiome

Cet axiome introduit l'idée de «relation fonctionnelle». Attention, il ne faut pas confondre avec la notion de fonction (au sens de la théorie des ensembles une fonction est un ensemble - à ne pas confondre avec les fonctions en logique). L'axiome dit simplement que l'image d'un ensemble par une relation fonctionnelle est un ensemble. Mais il est important d'introduire cette notion de relation fonctionnelle.

5.2 Les relations fonctionnelles

La notion de *relation* peut être comprise de manière «naïve» ce qui va nous aider pour écrire cet axiome. Il est important de souligner le fait que l'on va développer cette notion de manière naïve car la notion exacte de relation sera vue plus tard. Ce sera cependant suffisant pour écrire l'axiome correctement.

Considérons deux ensembles A et B. On peut définir une relation entre ces deux ensembles. Disons pour donner un exemple ludique que la relation est «utilise le système d'exploitation» et que A est l'ensemble contenant les éléments suivants : Steve Ballmer, Linus Torvalds, Steve Jobs, Christophe Roland (moi) et que B contient les éléments : Windows, Linux, OSX, Hurd. On peut représentez la relation par un diagramme :



On dit par exemple que l'élément «Christophe Roland» est envoyé sur les élément «Windows» et «Linux» par cette relation. On dit que les éléments «Windows» et «Linux» sont les *images* de «Christophe Roland», et que «Christophe Roland» est un *antécédent* de «Windows» et «Linux» Pour donner d'autres exemples, «OSX» est l'image de «Steve Jobs» et «Hurd» n'a pas antécédents.

Une relation fonctionnelle est un type particuliers de relation : une relation fonctionnelle est une relation où chaque élément a au plus une image (on dit bien «au plus» car on peut avoir des éléments qui n'ont pas d'image). On voit bien que l'exemple donné n'est pas une relation fonctionnelle car «Christophe Roland» a deux images.

5.3 Énoncé de l'axiome

Axiome : *l'image d'un ensemble par une relation fonctionnelle est un ensemble.*

5.4 Écriture formelle

On peut maintenant écrire l'axiome proprement. Pour cela considérons un prédicat à deux arguments X et Y plus d'autres paramètres éventuels que nous allons noter $A_1, A_2, A_3, ..., A_n$, on a donc : $P(X, Y, A_1, ..., A_n)$. En fait, pourquoi fait-on cela ? On veut avoir une relation qui envoie X sur Y c'est à dire que Y est une image de X. On va dire que $P(X, Y, A_1, ..., A_n)$ est équivalent à dire que Y est une image de X par cette relation. Pour que cette relation soit fonctionnelle, on doit écrire que si Y est une image de X, et si Y' est aussi une image de X, alors $Y = Y'$ car une relation fonctionnelle a au plus une image. On écrit alors :

$$\forall A_1, ..., A_n, \forall X, \forall Y, \forall Y', ((P(X, Y, A_1, ..., A_n) \wedge P(X, Y', A_1, ..., A_n)) \Rightarrow Y = Y')$$

Une fois ceci établi, il reste à dire que l'image d'un ensemble A par une fonction est un ensemble (on va le noter B), c'est à dire que quel que soit X appartenant à A, son image par la relation fonctionnelle appartient à B et que tout élément de B a un antécédent dans A. Pour cela, considérons un élément $Y \in B$. Il a un antécédent X c'est à dire :

$$Y \in B \Leftrightarrow \exists X(X \in A \wedge P(X, Y, A_1, ..., A_n))$$

On remet tout cela ensemble pour écrire l'axiome :

$$\boxed{\begin{gathered}\forall A_1, ..., A_n, (\forall X, \forall Y, \forall Y', (P(X, Y, A_1, ..., A_n) \wedge P(X, Y', A_1, ..., A_n) \Rightarrow Y = Y')) \\ \Rightarrow \forall A, \exists B, \forall Y, (Y \in B \Leftrightarrow \exists X(X \in A \wedge P(X, Y, A_1, ..., A_n)))\end{gathered}}$$

Pourquoi dit-on que nous avons un schéma d'axiomes ? C'est simple : il y a autant d'axiomes que de prédicats P, on a en réalité un nombre infini d'axiomes.

5.5 Conséquences

Parlons maintenant des conséquences de cet axiome.

5.5.1 Schéma de compréhension

On peut tout d'abord trouver un cas particuliers de cet axiome : le cas où $X = Y = Y'$. On a que le début de l'axiome :

$$P(X, Y, A_1, ..., A_n) \wedge P(X, Y', A_1, ..., A_n) \Rightarrow Y = Y'$$

devient toujours vrai car $A \Rightarrow B$ est toujours vrai quand B est vrai. On peut donc tout simplement supprimer cette partie. De même, la lettre Y peut être remplacée par X (pour la simplicité) et $P(X, Y, A_1, ..., A_n)$ devient : $P(X, X, A_1, ..., A_n)$. On peut ensuite remplacer ce prédicat par un autre prédicat P' ayant un argument en moins en posant :

$$P(X, X, A_1, ..., A_n) \Leftrightarrow P'(X, A_1, ..., A_n)$$

On a donc (le prédicat P' est renommé P car il n'y a plus de confusion possible) :

$$\boxed{\forall A_1, ..., A_n, \forall A, \exists B, \forall X, (X \in B \Leftrightarrow (X \in A \wedge P(X, A_1, ..., A_n)))}$$

Ce résultat est souvent appelé «schéma d'axiome de compréhension» mais comme on peut le démontrer, il est préférable de ne pas le considérer comme un axiome. On l'appellera tout simplement schéma de compréhension (et on le considère comme un théorème).

On va maintenant parler des conséquences du schéma de compréhension.

5.5.2 Définition en compréhension

Si vous le relisez bien, vous pouvez remarquer que l'on peut l'énoncer ainsi : soit un ensemble A et une propriété P, il existe un ensemble B d'éléments de A vérifiant la propriété P. C'est à dire qu'on peut définir un ensemble B comme ceci :

Il est possible à partir de cet axiome de démontrer ce que l'on appelle parfois le «schéma d'axiome de compréhension». Il peut s'énoncer ainsi : soit un ensemble A et une propriété P, il existe un ensemble B d'éléments de A vérifiant la propriété P. C'est à dire qu'on peut définir un ensemble B comme ceci :

1. on donne un ensemble A dont B sera un sous-ensemble,
2. on donne une propriété P pour définir quels seront les éléments de B parmi les éléments de A.

Imaginons par exemple que l'on ait un ensemble A qui contienne les éléments suivants : 1, 2, 3, 4, 5. Si on a une propriété P qui veut dire : «strictement plus grand que 3», on peut alors définir l'ensemble B en utilisant le schéma de compréhension qui contiendra les éléments 4 et 5.

5.5.3 Ensemble vide

On peut à partir de cela trouver un autre résultat. Si on a un ensemble A quelconque, on peut définir un ensemble (que l'on va noter $\emptyset$) avec la propriété P : «$X \neq X$» avec le schéma de compréhension. Comme il n'existe aucun élément qui puisse satisfaire à P, l'ensemble B est vide, il n'a aucun éléments. L'ensemble vide est donc bien un ensemble au sens des axiomes ZFC.

Remarque : il faut pour cela que A existe dans le modèle de la théorie des ensembles, mais cela est assuré car en logique des prédicats on ne considère que des modèles non vide : il existe donc au moins un ensemble à partir duquel on peut définir l'ensemble vide.

5.5.4 Théorème de la paire

À partir du schéma d'axiomes de remplacement, on peut faire une autre déduction : ce que l'on nomme souvent «l'axiome de la paire» mais que nous n'allons pas considérer comme un axiome car on va le démontrer, et nous allons appeler ce résultat «théorème de la paire». Attention, vous ne rencontrerez cette expression pratiquement que sur ce site internet, car c'est historiquement un axiome.

Le théorème de la paire peut s'énoncer ainsi : soit deux ensembles A et B, il existe un ensemble C qui admet A et B comme élément - et seulement ceux ci. Démonstration : on sait que l'ensemble vide existe. Si nous appliquons l'axiome de l'ensemble des parties sur cet ensemble, on a que l'ensemble qui contient comme seul élément l'ensemble vide existe. En effet, le seul sous-ensemble de l'ensemble vide est l'ensemble vide.

On a donc un ensemble qui a $\emptyset$ comme seul élément, et on va noter cet ensemble E. On applique une deuxième fois l'axiome de l'ensemble des parties sur E cette fois. On a donc comme résultat qu'il existe un ensemble qui contient deux éléments : l'ensemble vide et l'ensemble E et on va noter cet ensemble E'.

C'est là qu'on doit appliquer le schéma d'axiome de remplacement. Soit deux ensemble A et B. On utilise une relation fonctionnelle $P(X,Y)$ définit comme ceci :

$$P(X,Y) \Leftrightarrow ((X=\emptyset \wedge Y=A) \vee (X=E \wedge Y=B))$$

On peut facilement voir que cette relation est bien fonctionnelle. Pour ceux qui ont du mal avec cette expression logique, il faut juste se dire que A est l'image de $\emptyset$ et que B est l'image de E. On applique donc cette relation sur l'ensemble E' :

1. comme $\emptyset \in E'$, par la relation P son image est A,
2. comme $E \in E'$, par la relation P son image est B.

Et on obtient l'ensemble qui contient A et B comme seuls éléments et c'est bien un ensemble à cause du schéma d'axiome de remplacement.

6 Axiome de l'infini

6.1 Idée générale de l'axiome

Cet axiome est intéressant car il introduit un nouvel ensemble qui peut être vu comme un ensemble de nombres. Mais avant commencer nous avons besoin de définir la notion d'union de deux ensembles.

6.2 Union de deux ensembles

Soit deux ensembles A et B. On peut construire l'ensemble «A union B» qui contient tout les éléments de A et de B. On va essayer de construire l'ensemble «A union B» qui contient tout les éléments de A et de B. À partir des ensembles A et B on applique le théorème de la paire et on sait qu'il existe un ensemble C ayant A et B comme seuls éléments. On applique maintenant l'axiome de la réunion sur l'ensemble C, on sait donc qu'il existe un ensemble qui contient tout les éléments des éléments de C, c'est à dire tout les éléments de A et de B. On va noter cet ensemble $A \cup B$.

6.3 Ensemble ayant un élément quelconque

On doit utiliser un ensemble ayant un seul élément X, et il faut montrer qu'il est possible de construire cet ensemble à partir d'un ensemble quelconque X. Tout d'abord, si on applique le théorème de la paire sur deux fois le même ensemble X, on peut construire l'ensemble C qui contient deux fois l'élément X. En appliquant l'axiome d'extensionnalité sur l'ensemble C, on voit que C est égal à l'ensemble qui ne contient qu'un élément X (on peut supprimer les répétitions) et on a donc prouvé que l'on pouvait construire cet ensemble que nous allons noter $\{X\}$.

6.4 Énoncé de l'axiome

Axiome : *Il existe un ensemble ω dont l'ensemble vide est élément, tel que quel que soit X appartenant à ω, $X \cup \{X\} \in \omega$.*

6.5 Écriture formelle

En langage formel, l'axiome s'écrit :

$$\boxed{\exists \omega (\emptyset \in \omega \wedge \forall X (X \in \omega \Rightarrow X \cup \{X\} \in \omega))}$$

6.6 Conséquences

Il reste à discuter des conséquences de cet axiome.

Nous savons que l'ensemble vide appartient à ω. L'axiome nous dit encore que puisque $\emptyset \in \omega$, $\emptyset \cup \{\emptyset\} \in \omega$ mais on a (par définition de l'union et de l'ensemble vide) $\emptyset \cup \{\emptyset\} = \{\emptyset\}$ et donc $\{\emptyset\} \in \omega$ (rappelons que l'on note $\{X\}$ l'ensemble qui contient X comme unique élément).

Pour pousser le raisonnement plus loin on doit avoir des notations plus simples. On va donc noter $0 = \emptyset$. On a aussi l'ensemble $0 \cup \{0\}$ dans ω, ensemble que nous allons noter 1. On va dire que le *successeur* de 0 est 1, et on peut définir le successeur de 1 qui est $1 \cup \{1\}$ et qu'on note 2 et ainsi de suite. On a donc :

— $0 = \emptyset$,
— $1 = 0 \cup \{0\} = \{0\}$,
— $2 = 1 \cup \{1\} = \{0\} \cup \{1\}$,
— $3 = 2 \cup \{2\} = \{0\} \cup \{1\} \cup \{2\}$,
— $4 = 3 \cup \{3\} = \{0\} \cup \{1\} \cup \{2\} \cup \{3\}$,
— ... ainsi de suite.

On peut donc considérer les nombres entiers comme des ensembles : chaque nombre est l'ensemble de tous les nombres entiers qui le précèdent. Par exemple l'ensemble $3 = \{0\} \cup \{1\} \cup \{2\}$ contient comme éléments les nombres 0, 1 et 2 (définition de l'union).

On sait donc qu'il existe un ensemble ω qui contient les éléments 0, 1, 2, 3, ... mais il est hâtif de dire qu'il ne contient que des nombres. Rien dans l'axiome ne permet d'affirmer cela. Pourtant, le fait qu'un tel ensemble existe ne fait pas de doute car cet ensemble est un sous-ensemble de ω. Cette remarque ne suffit cependant pas à définir cet ensemble de manière formelle. On verra cependant dans la partie «Nombres naturels» que l'on peut définir cet ensemble en compréhension.

7 Axiome de fondation

7.1 Idée générale de l'axiome

Ce axiome a comme conséquence qu'il n'existe pas d'ensemble X tel que $X \in X$. Pour pouvoir l'énoncer, il faut introduire la notion d'intersetion entre deux ensembles.

7.2 Intersection

On considère deux ensembles A et B. L'intersection de A et B est l'ensemble qui contient tout les éléments qui appartiennent à la fois à A et à B et on le note $A \cap B$. Pour définir cet ensemble de manière rigoureuse, on utilise le schéma de compréhension. On a vu que pour définir un ensemble en compréhension, il faut un ensemble et une propriété. Dans le cas de l'intersection, il suffit d'utiliser l'ensemble $A \cup B$ et la propriété $P(X) \Leftrightarrow (X \in A \wedge X \in B)$ pour que X appartienne à la fois à A et à B.

7.3 Énoncé de l'axiome

Axiome : *Soit un ensemble $A \neq \emptyset$, il existe un ensemble B appartenant à A tel que A et B n'ont aucun éléments en commun.*

7.4 Écriture formelle

Il n'est pas difficile d'écrire cet axiome de manière formelle :

$$\boxed{\forall A, A \neq \emptyset \Rightarrow \exists B (B \in A \wedge A \cap B = \emptyset)}$$

8 Éléments, sous-ensembles

8.1 Élément d'un ensemble

Rappelons tout d'abord une notion fondamentale : si on a deux ensembles A et B et que A est un élément de B, on note :

$$A \in B$$

Dans le cas contraire, on peut écrire :

$$A \notin B$$

8.2 Inclusion

Rappelons que si tout les éléments de A sont aussi élément de B, on dit que A est inclus dans B et qu'il est un sous-ensemble de B et on note :

$$A \subset B$$

On peut écrire aussi :

$$B \supset A$$

On dit aussi que B est un sur-ensemble de A. On rappelle aussi que l'on peut formaliser cette notion :

$$A \subset B \Leftrightarrow (\forall X, X \in A \Rightarrow X \in B)$$

8.3 Propriétés

Deux propriétés faciles à démontrer : *Première propriété :*

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

Démonstration :

On utilise la définition de l'inclusion, on peut réécrire :

$$\forall X, ((X \in A \Rightarrow X \in B) \wedge (X \in B \Rightarrow X \in C)) \Rightarrow (X \in A \Rightarrow X \in C)$$

On peut rappeler le modus barbara vu en logique :

$$(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$$

Et en comparant les deux expressions on voit qu'elle sont équivalentes ce qui achève la démonstration. *Deuxième propriété :*

$$(A \in B \wedge B \subset C) \Rightarrow A \in C$$

On utilise encore la définition de l'inclusion :

$$\forall X, (A \in B \wedge (X \in B \Rightarrow X \in C)) \Rightarrow A \in C$$

Si l'expression $A \in B \wedge (X \in B \Rightarrow X \in C)$ est vraie on a que $A \in B$ est vrai ; et comme elle vraie pour tout X, elle est donc vraie en particuliers pour $X = A$, on a donc :

$$\forall X, (A \in B \wedge (X \in B \Rightarrow X \in C)) \Rightarrow (A \in B \wedge (A \in B \Rightarrow A \in C))$$

On a donc que $A \in B \wedge (A \in B \Rightarrow A \in C)$ est vrai, alors on sait que $A \in B \Rightarrow A \in C$ est vrai. Comme on sait que $A \in B$ est vraie, alors $A \in C$ est vrai aussi et on a donc prouvé l'implication.

9 Définir un ensemble

9.1 Définition en extension

Soit E un ensemble. Si $a_1, a_2, ..., a_n$ sont les éléments de E, on note :

$$E = \{a_1, a_2, ..., a_n\}$$

On peut donc définir un ensemble en listant tout ses éléments entre des accolades (on dit alors que l'on défini l'ensemble en extension).

Il faut maintenant prouver que l'on a vraiment le droit de faire cela c'est à dire que c'est compatible avec les axiomes vus précédemment.

Tout d'abord, nous avons montré que l'on pouvais avoir un ensemble du type $\{a_1\}$. Nous avons montré aussi que nous pouvions avoir des ensembles ayant deux éléments :

$\{a_1, a_2\}$ grâce au théorème de la paire. Cependant, il faut que cette définition soit valide pour un nombre quelconque d'éléments.

Pour cela, il suffit simplement de faire appel à l'union de deux ensembles. Et il suffit d'écrire, pour définir formellement cette notation :

$$\{a_1, a_2, ..., a_n\} = \{a_1\} \cup \{a_2\} \cup ... \cup \{a_n\}$$

Gràce à l'axiome d'extensionnalité, on sait qu'un ensemble ne dépend que de ses éléments ce qui montre qu'on définit bien un ensemble unique et ce qui valide la définition en extension.

9.2 Définition en compréhension

Nous savons déjà comment définir un ensemble en compréhension en donnant un sur-ensemble et une propriété.

Par exemple, si on veut définir l'ensemble E, sous-ensemble de A avec la propriété P, on note :

$$E = \{x \in A | P(x)\}$$

On verra plus tard des exemples d'utilisation de cette méthode de définition.

10 Union et intersection

10.1 Union

10.1.1 Propriétés

Il est possible à partir de la définition de l'union de deux ensembles de prouver certaines propriétés :

Idempotence

$$A \cup A = A$$

Commutativité

$$A \cup B = B \cup A$$

Associativité

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

10.1.2 Définition

On a déjà définit l'union de deux ensembles, rappelons que si on a deux ensembles A et B, on forme l'ensemble $\{A, B\}$ gràce à l'axiome de la paire, et on applique à cet ensemble l'axiome de la réunion : on obtient l'ensemble $A \cup B$ noté par la lettre D dans l'axiome de la réunion.

10.1.3 Propriétés

On peut déjà lister quelques propriétés de l'union. On peut toutes les prouver avec les axiomes vues précédemment.

Idempotence

$$A \cup A = A$$

Commutativité

$$A \cup B = B \cup A$$

Associativité

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

10.2 Intersection

10.2.1 Définition

Si on a deux ensembles A et B, on forme l'ensemble $A \cap B$ qui est l'ensemble des éléments qui appartiennent à la fois à A et à B. On le définit en compréhension :

$$A \cap B = \{X \in A \cup B | X \in A \wedge X \in B\}$$

10.2.2 Propriétés

Elles sont similaires à celle de l'union.

Idempotence

$$A \cap A = A$$

Commutativité

$$A \cap B = B \cap A$$

Associativité

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

10.3 Distributivité

On peut énoncer encore deux propriétés de l'union et de l'intersection :

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

Et :

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

11 Relations binaires

On peut maintenant voir de manière formelle la notion de relation déjà abordée de manière naïve.

11.1 Notion de couple

On doit tout d'abord définir la notion de *couple*. L'idée est qu'à partir de deux éléments a et b, on construit un couple que l'on va noter (a, b). Un couple est une paire ordonnée c'est à dire que l'ordre a une importance, on a $(a, b) \neq (b, a)$.

On doit définir cette notion à partir de la théorie des ensembles c'est à dire comme d'habitude qu'on doit n'avoir que des ensembles donc un couple sera un ensemble. Malheureusement, on ne peut pas définir simplement le couple en écrivant $(a, b) = \{a, b\}$ car nous avons vu (axiome d'extensionnalité) que $\{a, b\} = \{b, a\}$ ce qui contredit $(a, b) \neq (b, a)$.

Pour pouvoir résoudre cette difficulté, on définit le couple comme ceci :

$$(a, b) = \{\{a\}, \{a, b\}\}$$

Avec cette définition on a bien $(a, b) \neq (b, a)$ car $\{\{a\}, \{a, b\}\} \neq \{\{b\}, \{b, a\}\}$.

11.2 Produit cartésien

En utilisant la notion de couple, on définit la notion de *produit cartésien*. Si on a deux ensembles A et B, leur produit cartésien est l'ensemble noté $A \times B$, et dont les éléments sont des couples avec le premier élément dans A et le deuxième dans B.

Par exemple, si $A = \{1, 2\}$ et $B = \{0, 2, 4\}$, alors :

$$A \times B = \{(1, 0), (1, 2), (1, 4), (2, 0), (2, 2), (2, 4)\}$$

On peut maintenant définir cette notion de manière formelle. On a deux ensembles A et B. On va essayer de définir cet ensemble en compréhension. La propriété qu'on va utiliser pour que $(a, b) \in A \times B$ est tout simplement $a \in A \wedge b \in B$. Reste à définir le sur-ensemble de $A \times B$ et c'est plus compliqué.

Soit $a \in A$ et $b \in B$. On a bien $(a, b) \in A \times B$. On a aussi que $\{a, b\} \subset A \cup B$ donc que $\{a, b\} \in P(A \cup B)$. De même on a que $\{a\} \subset A \cup B$ donc que $\{a\} \in P(A \cup B)$ (rappel : $P(X)$ est l'ensemble des parties de X).

On sait donc que $\{a, b\} \in P(A \cup B)$ et que $\{a\} \in P(A \cup B)$. On conclut alors que $\{\{a\}, \{a, b\}\} \in P(P(A \cup B))$. On peut alors écrire :

$$A \times B = \{(a, b) \in P(P(A \cup B)) | a \in A \wedge b \in B\}$$

De plus on écrit souvent A^2 au lieu de $A \times A$ ou A^3au lieu de $A \times A \times A$,...

11.3 Relations binaires

11.3.1 Définition

On a déjà vu cette notion de manière naïve, il est temps d'en donner une définition formelle dans le cadre de la théorie des ensembles. On va dire (sans surprise encore une fois) qu'une *relation binaire* est un ensemble.

On sait déjà qu'une relation binaire met en relation deux ensembles. On va donc considérer une relation comme un ensemble de couples. Par exemple si la relation est notée R, et si a et b sont en relation, alors on a $(a, b) \in R$.

Supposons donc qu'on ait deux ensembles A et B. On a une relation R entre ces deux ensembles. Il s'agit d'un ensemble de couple (a, b) avec $a \in A$ et $b \in B$, donc un sous-ensemble de $A \times B$.

On peut alors considérer que tout sous-ensemble de $A \times B$ est une relation binaire. L'ensemble des relations binaires entre A et B sera noté $A \rightleftharpoons B$. On a évidemment :

$$A \rightleftharpoons B = P(A \times B)$$

11.3.2 Domaine et ensemble image

On définit aussi le *domaine* d'une relation binaire. Une relation binaire entre A et B associe à des éléments de A des éléments de B, mais certains éléments de A ne sont associés à aucun élément de B. On va donc définir un ensemble (le domaine) qui est l'ensemble des éléments de A qui sont en relation avec au moins un élément de B. Si la relation est R, on note le domaine : $Dom(R)$.

On peut facilement définir le domaine en compréhension :

$$Dom(R) = \{x \in A | \exists y, (x, y) \in R\}$$

De même, il existe des éléments de B qui ne sont associés à aucun élément de A. On définit alors l'*ensemble image* qui est l'ensemble des éléments de B qui sont en relation avec au moins un élément de A, ensemble que l'on note $Im(R)$.

$$Im(R) = \{y \in B | \exists x, (x, y) \in R\}$$

11.3.3 Inverse

On a une relation R entre A et B. On peut définir l'*inverse* de R, que l'on note R^{-1}, qui est la même relation en échangeant les ensembles A et B, c'est à dire que si le couple (a, b) appartient à R alors (b, a) appartient à R^{-1}. On a donc :

$$R^{-1} = \{(y, x) \in A \times B | (x, y) \in R\}$$

11.3.4 Composée

Si on a une relation R de A vers B et une relation R' de B vers C, alors on peut définir la *composée* de R et R' que l'on note $R \circ R'$ qui est une relation de A vers C. Si par exemple on a un élément $a \in A$ en relation par R avec un élément $b \in B$ et que cet élément est en relation par R' avec un élément $c \in C$, alors a et c sont en relation par $R \circ R'$.

On définit cet ensemble en compréhension :

$$R \circ R' = \{(x, z) \in A \times C | \exists y, ((x, y) \in R \wedge (y, z) \in R')\}$$

12 Différents types de relations

12.1 Fonction

Une *fonction* est une relation où chaque élément a au plus une image. C'est à dire que si on a une fonction f, alors un élément $a \in Dom(f)$ a un seule image, donc il existe un seul élément $b \in Im(f)$ tel que $(a, b) \in f$.

Puisque chaque élément $x \in Dom(f)$ a une seule image, on note cette image $f(x)$ ce qu'on ne pourrai pas faire avec une relation qui ne soit pas une fonction, car si x avait deux images, on ne saurait pas laquelle des deux désigne l'expression $f(x)$.

On a donc si f est une fonction :

$$x \in Dom(f) \Rightarrow \exists! y, (x, y) \in f$$

12.2 Application

Une *application* est un type particuliers de fonction : il s'agit d'une fonction où tous les éléments de l'ensemble de départ on une image. Si A est l'ensemble de départ, on a :

$$Dom(f) = A$$

12.3 Injection

Une *injection* est un type particuliers d'application : tous les éléments de l'ensemble d'arrivée on au plus un antécédent. C'est à dire que :

$$y \in Im(f) \Rightarrow \exists! x, (x, y) \in f$$

12.4 Surjection

Une *surjection* est un type particuliers d'application : tous les éléments de l'ensemble d'arrivée on au moins un antécédent. C'est à dire que si B est l'ensemble d'arrivée :

$$Im(f) = B$$

12.5 Bijection

Une *bijection* est une application à la fois injective et surjective. Dans le cas d'une bijection, chaque élément de l'ensemble de départ a une et une seule image et chaque élément de l'ensemble d'arrivée a un et un seul antécédent. On peut donc conclure que si il existe une bijection entre A et B, alors ils ont le même nombre d'éléments.

12.6 Loi de composition interne

Définition 1. *Soit E un ensemble, une* loi de composition interne sur E *est une application de $E \times E$ dans E dans E.*

Une loi de composition interne est souvent noté avec un simple symbole comme $\circ$. On note, si l'image de $(a, b) \in E$ est $c \in E$:

$$a \circ b = c$$

Définition 2. *Soit E un ensemble, $\circ$ une loi de composition interne sur cet ensemble, on dit que cette loi est* commutative *si :*

$$\forall a, b \in E, a \circ b = b \circ a$$

Définition 3. *Soit E un ensemble, $\circ$ une loi de composition interne sur cet ensemble, on dit que cette loi est* associative *si :*

$$\forall a, b, c \in E, a \circ (b \circ c) = (a \circ b) \circ c$$

Définition 4. *Soit E un ensemble, $\circ$ une loi de composition interne sur cet ensemble, on dit qu'il existe un* élément neutre *pour $\circ$ si :*

$$\exists n \in E : \forall a \in E, a \circ n = a$$

Définition 5. *Soit E un ensemble, $\circ$ une loi de composition interne sur cet ensemble, on dit qu'il existe un* élément neutre *pour $\circ$ si :*

$$\exists n \in E : \forall a \in E, a \circ n = a$$

Définition 6. *Soit E un ensemble, $\circ$ une loi de composition interne sur cet ensemble qui admet un élément neutre n, on dit qu'il existe un* élément symétrique *pour chaque élément de E si :*

$$\forall a \in E, \exists a^* \in E : a \circ a^* = n$$

Définition 7. *Soit E un ensemble, $\circ$ et $\bullet$ deux lois de composition interne sur cet ensemble, on dit qu'on a distributivité de $\circ$ par rapport à $\bullet$ si :*

$$\forall a, b, c \in E, a \circ (b \bullet c) = (a \circ b) \bullet (a \circ c)$$