

Also sprach Marc Schaul

Mathe für alle und keinen

Thomas AROCENA
Constance SARRAZIN
Marc SCHAUL (apocryphe)

« Une exposition très claire, presque éblouissante. Je n'ai jamais lu quoi que ce soit d'aussi brillant depuis mon arrivée en sup 4. »

— Marc Schaul (probablement)

« Vous savez, ce n'est pas parce que vous ajoutez des « probablement » que vous pouvez me faire dire tout et n'importe quoi ! »

— Marc Schaul (probablement)

Table des matières

Le niveau d'une section est indiqué par sa couleur : verte quand sa quasi-entiereté est au programme (officiel ou officieux) des classes préparatoires (MPSI/MP) ; bleue quand son contenu est directement accessible à un spé sans être au programme, autrement dit, quand tous ses préliminaires sont verts ; rouge pour les divagations au delà.

Les items grisés signalent une section en cours de rédaction. L'ensemble est en amélioration constante et comporte selon toute probabilité des erreurs graves. Pour toute réclamation, merci de frapper Thomas (mais pas trop fort histoire qu'il puisse quand même passer les concours)

On a veillé à ce que l'ensemble ne soit pas circulaire, mais cela ne veut pas dire que nous avons évité les références en avant, au contraire. Nous nous sommes affranchis de l'ordre linéaire sans scrupule lorsque cela était nécessaire. En particulier, les sections rouges piochent librement dans le contenu des sections vertes sans forcément renvoyer aux pages correspondantes.

Cette version est celle du 6 décembre 2022. Pour accéder à l'historique, faites un tour sur le repo GitHub.

I	Fourre-tout	1
1	Théorie des ensembles	2
1.1	Une théorie sur des bases frêles	2
	► Une introduction à la terminologie ensembliste sur le mode dit naïf : unions, intersections, produit cartésien. Algèbre de Boole des parties d'un ensemble. Relations binaires, relations d'ordre, d'équivalence, partition. Applications, injections, surjections, bijections. Argument diagonal de Cantor. Théorème de Schröder-Bernstein. ◀	
1.2	Axiomatisation de Zermelo-Frankel (ZFC)	8
	► Paradoxes de Berry, de Russel : axiomes de compréhension, de compréhension restreinte. Classes, correspondances fonctionnelles. Axiome de séparation. Axiomes de l'union, de la paire, de l'ensemble des parties. Bons ordres, ordinaux, cardinaux, leur arithmétique. Axiome du choix, lemme de Zorn, théorème de Zermelo et cardinal de tout ensemble. ◀	

1.3	Objets mathématiques usuels et ensembles purs	8
	► Retour sur l'axiome de fondation. Rang, hiérarchie cumulative de Von Neumann, ensemble pur. Construction de copies de \mathbb{N} , \mathbb{Z} , \mathbb{Q} dans ZFC. Une première construction de \mathbb{R} . Application des ordinaux : les suites de Goodstein. ◀	
II	Algèbre	9
2.1	Groupes, premières définitions et exemples	10
	► Loi de composition, monoïde, groupe. Morphismes. Sous-groupe, théorème de Lagrange. Ordre d'un élément. Groupe produit, sous-groupe normal et groupe quotient. Exemples : \mathbb{Z} , $(\mathbb{Z}/n\mathbb{Z}, +)$, \mathfrak{S}_n . Groupe symétrique, signature et théorème de Cayley. ◀	
2.2	Anneaux et corps, premières définitions et exemples	10
	► Idéal, anneau quotient. Arithmétique dans un anneau intègre : divisibilité, anneaux euclidiens. \mathbb{Z} et $\mathbb{R}[X]$ sont principaux. Relation de Bézout. Éléments irréductibles, premiers, factorisation. Anneau de polynômes. Corps, caractéristique. Corps de fractions. Clôture algébrique et théorème fondamental de l'algèbre. Indicatrice d'Euler et \mathbb{F}_p . ◀	
III	Topologie	11
IV	Analyse	12
V	Théorie des nombres	13
VI	Histoire et philosophie	14

Première partie

Fourre-tout

Chapitre 1

Théorie des ensembles

1.1 Une théorie sur des bases frêles

Premières opérations ensemblistes

On considère ici qu'un ensemble est un concept intuitif, qui correspond à une collection d'objets mathématiques. Ces objets sont définis par une propriété ou par une liste exhaustive, de la façon suivante :

- $\mathbb{R}_+ = \{x \in \mathbb{R} | x \geq 0\}$
- $P = \{1, 4, 9, 16\} = \{n \in \mathbb{N} | n \text{ est un carré parfait et } n < 20\}$

Cette première expression se lit par exemple « \mathbb{R}_+ est l'ensemble des x dans \mathbb{R} tels que $x \geq 0$ ».

On verra dans le chapitre suivant que pour éviter d'aboutir à certaines contradictions techniques, il est nécessaire de restreindre quelque peu ce qu'on s'autorise à considérer comme un ensemble. Mais pour le moment, on suppose acquise cette fondation et on introduit un peu de vocabulaire, en commençant par les opérations ensemblistes de base.

Définition 1 (UNION ET INTERSECTION)

Soient A et B deux ensembles.

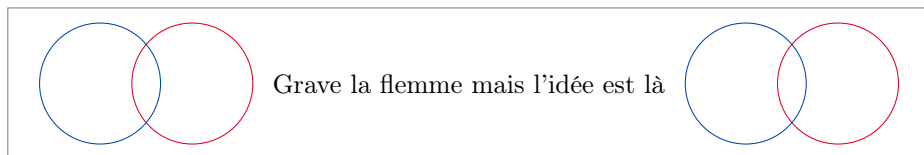
On note $A \cup B$ l'union de A et B , c'est à dire l'ensemble

$$\{x | x \in A \text{ ou } x \in B\}$$

On note $A \cap B$ l'intersection de A et B , c'est à dire l'ensemble

$$\{x | x \in A \text{ et } x \in B\}$$

Cette situation est bien résumée par un diagramme de Venn :



Ces opérations sont la transcription directe du « et » et du « ou » logique¹. On peut donc écrire nos premières propriétés :

Propriété 1

Pour tous ensembles A , B et C :

- | | |
|--|--|
| — $A \cup A = A$ | — $A \cap A = A$ |
| — $A \cup B = B \cup A$ | — $A \cap B = B \cap A$ |
| — $(A \cup B) \cup C = A \cup (B \cup C)$ | — $(A \cap B) \cap C = A \cap (B \cap C)$ |
| — $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ | — $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ |

Ces propriétés s'appellent respectivement l'idempotence, la commutativité, l'associativité et la distributivité.

► Démonstration : Ces propriétés proviennent directement des propriétés des opérateurs logiques et et ou. Par exemple, étant donné une proposition P , P ou P équivaut à P . ◀

On peut encore faire quelques diagrammes de Venn pour illustrer la situation.

Toujours pas

On peut encore transcrire l'implication logique par la notion de partie.

Définition 2 (PARTIES)

Soit A et B deux ensembles. On dit que A est inclus, contenu dans B , ou encore que c'est une partie ou un sous-ensemble de B , quand $x \in A \implies x \in B$, c'est à dire $\forall x \in A, x \in B$. On le note $A \subset B$. On notera $\mathfrak{P}(B)$ l'ensemble de toutes les parties de B .

Par exemple, comme $x \in A$ et $x \in B \implies x \in A$, il est facile de se convaincre que $A \cap B$ est une partie de A .

1. Notons que le ou logique, contrairement à certains usages en français, est un ou inclusif : autrement dit, P ou Q signifie que soit P est vrai, soit Q est vrai, soit P et Q sont tous deux vrais. On verra dans quelques pages l'opération ensembliste traduisant le ou exclusif (P ou Q mais pas les deux.)

De même, comme $x \in A \implies x \in A$, on a toujours $A \subset A$.²

Un ensemble remarquable est l'ensemble vide, ne comportant aucun élément, qu'on note \emptyset : $x \in \emptyset$ étant toujours faux, l'implication $x \in \emptyset \implies x \in A$ est, elle, toujours vraie, et pour tout ensemble A , $\emptyset \subset A$.

De plus, dans le cas particulier où A est un ensemble avec un nombre fini d'éléments, on peut lister toutes ses parties. Par exemple, l'ensemble $\{1, 2\}$ a pour parties :

$$\emptyset \quad \{1\} \quad \{2\} \quad \{1, 2\}$$

$\mathfrak{P}(\{1, 2\})$ comporte donc 4 éléments.

Propriété 2

Soit E un ensemble à n éléments. Alors $\mathfrak{P}(E)$ comporte 2^n éléments.

► Démonstration : Dénombrons toutes les parties de E . On peut faire la liste de tous les éléments de E , de telle sorte qu'il a un sens de parler du premier élément, du deuxième, etc. On a deux choix pour le premier élément : soit on l'inclut, soit on ne l'inclut pas. De même, on a ensuite deux choix pour le deuxième élément, ce qui nous amène à un total de quatre choix, et ainsi de suite : on aura huit choix au troisième élément et de proche en proche 2^n à l'énième. ◀

Enfin, la négation logique correspond à la notion de complémentaire, et à la notion liée d'ensemble privé d'un autre.

Définition 3 (COMPLÉMENTAIRE ET « PRIVÉ DE »)

Soit A une partie de B . On note A_C l'ensemble $\{x \in B \mid x \notin A\}$. C'est le complémentaire de A dans B .

Soient maintenant A et B quelconques. On note $B \setminus A$ et on lit « B privé de A » le complémentaire de $A \cap B$ (qu'on sait être une partie de B) dans B .

Quand A est une partie de B , comme $A \cap B = A$, ces deux notions sont confondues.

Remarquons que la notation A_C peut être ambiguë si il y a un doute sur l'ensemble de référence : en clair, dans une situation où on manipule trois ensembles A , B et C avec $A \subset B \subset C$, A_C peut être le complémentaire de A dans B ou dans C . Dans une telle situation, on préférera les notations $B \setminus A$ et $C \setminus A$ qui dissiperont ce doute.

2. Les anglo-saxons écrivent souvent \subseteq pour l'inclusion telle que nous venons de la définir et réservent \subset à l'inclusion stricte : pour eux, $A \subset B \iff A \subseteq B \text{ and } A \neq B$. On écrira $A \subsetneq$ dans ce cas.

Comme précédemment pour les unions et les intersections, on dispose de propriétés permettant de simplifier certaines expressions.

Propriété 3

Soient A et B deux parties d'un même ensemble.

- $(A_C)_C = A$
- $(A \cup B)_C = A_C \cap B_C$
- $(A \cap B)_C = A_C \cup B_C$

Ces deux dernières propriétés s'appellent les lois de De Morgan, et s'illustrent bien par des diagrammes de Venn.

♪ *Never gonna give you up, never gonna let you down* ♪

On peut maintenant définir une opération qui rend compte du « ou exclusif » :

Définition 4

Soit A et B deux ensembles. On note $A \Delta B$ la différence symétrique de A et B c'est à dire l'ensemble $A \cup B \setminus A \cap B$.

Hahahahaha

Enfin, une dernière opération est importante pour la suite : le produit cartésien.

Définition 5

Soient deux ensembles A et B . Le produit cartésien $A \times B$ (« A croix B ») est l'ensemble des couples (a, b) où a appartient à A et b appartient à B .

On suppose ici que la notion de couple est intuitive¹ : il s'agit d'une paire ordonnée, contrairement à un ensemble à deux éléments qui ne l'est pas. Autrement dit $(a, b) = (a', b') \implies a = a' \text{ et } b = b'$, tandis que $\{a, b\} = \{a', b'\} \implies (a = a' \text{ et } b = b') \text{ ou } (a = b' \text{ et } b = a')$.

En l'état, $(A \times B) \times C$ et $A \times (B \times C)$ ne sont pas égaux, mais une fois qu'on disposera d'une définition du produit cartésien d'une famille d'ensembles, on pourra identifier ces deux ensembles à $A \times B \times C$.

1. Cela dit, on peut aussi définir un couple d'une façon purement ensembliste, par exemple en posant $(a, b) = \{a, \{a, b\}\}$. Une telle définition permet d'identifier le premier élément, mais elle peut sembler artificielle à ce stade.

Pour le moment ceci n'est pas très important, et on peut provisoirement se restreindre à des situations mettant en jeu le produit simple de deux éléments. En particulier, ceci suffit pour définir les relations binaires.

Relations binaires et d'ordre

D'un point de vue logique, une relation binaire entre deux objets est comparable à une fonction – au sens informatique du terme – prenant deux arguments et renvoyant une valeur logique, vrai ou faux. Ceci correspond en général à l'introduction d'un nouveau symbole. Par exemple, l'égalité, l'appartenance d'ensembles, l'inclusion d'ensembles sont des relations binaires.

D'un point de vue ensembliste, ceci correspond à la donnée d'un sous-ensemble :

Définition 6

Une relation binaire \mathcal{R} entre éléments de X et de Y peut être vue comme un sous-ensemble \mathcal{R} de produit cartésien $X \times Y$. On notera $x\mathcal{R}y$ pour $(x, y) \in \mathcal{R}$.

On parlera de relation binaire sur X pour une relation entre éléments de X . Un type particulier de relations binaires sont les relations d'ordre, habituellement notées \leq .

Définition 7

Une relation binaire sur un ensemble X est une relation d'ordre \leq sur X quand :

- réflexive : $\forall x \in X, x \leq x$
- antisymétrique : $\forall x, y \in X, x \leq y \text{ et } y \leq x \implies x = y$
- transitive : $\forall x, y, z \in X, x \leq y \text{ et } y \leq z \implies x \leq z$

On peut d'ores et déjà donner un exemple.

Propriété 4

Soit E un ensemble. L'inclusion \subset est une relation d'ordre sur $\mathfrak{P}(E)$.

► Démonstration :

- Il s'agit bien d'une relation binaire, qui correspond à l'ensemble $\{(A, B) \in \mathfrak{P}(E)^2 \mid \forall x \in E, x \in A \implies x \in B\}$.
- Pour tout ensemble A , $A \subset A$.
- Si $X \subset Y$ et $Y \subset X$, par double implication, $x \in X \iff x \in Y$. Autrement dit, X et Y ont exactement les mêmes éléments, soit $X = Y$.

- Si $x \in X \implies x \in Y$ et $x \in Y \implies x \in Z$, $x \in X \implies x \in Z$.
Autrement dit, si $X \subset Y$ et $Y \subset Z$, alors $X \subset Z$.

D'où \subset relation d'ordre. ◀

Remarquons que selon cette définition, la relation $<$ (par exemple sur les entiers) n'est pas une relation d'ordre. Cependant, on peut définir les relations d'ordre stricte :

Définition 8

Une relation binaire sur un ensemble X est une relation d'ordre strict $<$ sur X quand :

- Elle est irréflexive : $\forall x$, non $x < x$
- Elle est transitive.

À partir d'une relation d'ordre \leq , on définit l'ordre strict correspondant $x < y \iff x \leq y$ et $x \neq y$. Réciproquement, à partir d'un ordre strict $<$, on peut poser $x \leq y \iff x < y$ ou $x = y$.
[majorant, minorant, yada yada]

Applications, bijections et familles

On va en fait définir une application comme une certaine relation binaire.

Définition 9

Relations d'équivalences et partitions

Un autre type de relations binaires remarquables sont les relations d'équivalence.

Définition 10

Une relation d'équivalence sur un ensemble X est une relation binaire \sim sur X :

- réflexive,
- symétrique : $\forall x \forall y, x \sim y \implies y \sim x$,
- transitive.

Un premier exemple de relation d'équivalence est bien sûr l'égalité. Un autre exemple est donné par les congruences en arithmétique : en particulier si on pose $p \sim q \iff p$ et q ont la même parité, il s'agit d'une relation d'équivalence.

Toute l'utilité de la notion réside en la possibilité de classer tous les éléments en « paquets », qui sont les classes d'équivalences :

Définition 11

Soit $x \in X$. On note \bar{x} ou $[x]$ la classe d'équivalence de x , qui est l'ensemble $\{y \in X \mid x \sim y\}$

Formellement, on dit que les classes d'équivalences forment une partition de X :

Définition 12

Soit X un ensemble. On dit que la famille d'ensembles (X_i) forme une partition de X quand :

- $\forall i \in I, X_i \neq \emptyset$
- $\bigcup X_i = X$
- $\forall i \neq j, X_i \cap X_j = \emptyset$

Oui oui baguette

1.2 Axiomatisation de Zermelo-Frankel (ZFC)

1.3 Objets mathématiques usuels et ensembles purs

Deuxième partie

Algèbre

- 2.1 Groupes, premières définitions et exemples**
- 2.2 Anneaux et corps, premières définitions et exemples**

Troisième partie

Topologie

Quatrième partie

Analyse

Cinquième partie

Théorie des nombres

Sixième partie

Histoire et philosophie