Remise à niveau

Logique et ensemble

Suis-je sûr de douter ?

Est-ce vrai ou est-ce faux ? Si je n'en doute pas c'est que je suis certain de douter. Si j'en doute c'est que j'envisage de ne pas douter.

Cette phrase n'est donc ni vrai ni fausse et vrai et fausse en même temps. Une sorte de phrase quantique !

Lorsqu'on va voir un mathématicien, plus précisément un logicien, pour lui demander de rendre des comptes sur ce phénomène, il répond calmement que cette phrase ne rentre pas dans le cadre des phrases étudiables. Lorsque l'on tombe sur ce genre de paradoxe, c'est qu'il y a un problème de cadrage. Alors cadrons un peu tout ça.

Définition

Un **proposition** est un énoncé dont on peut dire sans ambigüité qu'il est vrai ou qu'il est faux.

Ainsi la proposition $p =$"$2+2=4$" est une proposition vrai. De même $q =$"$2+2=5$" est une proposition fausse. Mais $r =$"Suis-je sûr de douter ?" n'est pas une proposition de sorte que la question de la valeur de vérité (vrai ou faux) ne se pose pas. Tout comme $s =$"$x+1>0$". C'est parfois vrai, parfois faux. Cela dépend de x. Il y a donc ambigüité, ce n'est donc pas une proposition.

Maintenant que le cadre est placé nous pouvons enrober de quelques définition et outils.

Définition

- Une **tautologie** est un énoncé toujours vrai. On le note $\top$ (ou 1 ou $\mathcal{V}$).
- Une **contradiction** est un énoncé toujours faux. On le note $\perp$ (ou 0 ou $\mathcal{F}$).

Connecteurs logique et tables de vérité

Pour travailler avec les propositions et définir des outils de calculs, on utilise des *tables de vérité*. Il s'agit de table décrivant toutes les combinaisons de vérité possible d'une expression propositionnelle.

Définition

On définit le connecteur logique **OU** entre deux propositions p et q, noté $p \vee q$ défini par la table de vérité ci-contre.

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

Définition

On définit le connecteur logique **ET** entre deux propositions p et q, noté $p \wedge q$ défini par la table de vérité ci-contre.

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

Définition

On défini le **NON**, la négation logique d'une proposition p, noté $\neg p$, par la table de vérité ci-contre.

p	$\neg p$
0	1
1	0

L'expression $E = p \vee q \wedge r$ n'est pas bien définie. Nous ne savons pas quel connecteur appliquer en premier ni même si cela à une incidence sur le résultat. Cette expression peut soit se comprendre comme $E_1 = p \vee (q \wedge r)$ ou $E_2 = (p \vee q) \wedge r$. Comparons leur table de vérité :

p	q	r	$q \wedge r$	E_1	$p \vee q$	E_2
0	0	0	0	0	0	0
0	0	1	0	0	0	0
0	1	0	0	0	1	0
0	1	1	1	1	1	1
1	0	0	0	1	1	0
1	0	1	0	1	1	1
1	1	0	0	1	1	0
1	1	1	1	1	1	1

Les tables de vérités de E_1 et E_2 sont différentes ce qui laisse à pense que ces expressions le sont aussi. Cela motive la définition suivante.

Définition

Deux propositions p et q sont égales si elles ont les même tables de vérité. Dans ce cas on note $p = q$.

Comme nous l'avons observer dans la table précédente, le parenthésage est important. Dressons la table de vérité de l'expression (bien définie) suivante : $E = [p \vee (r \wedge \neg(q \wedge p))] \wedge (\neg r)$.

			A	B	C	D		$D\wedge\neg r$
p	q	r	$q\wedge p$	$\neg A$	$r\wedge B$	$p\vee C$	$\neg r$	E
0	0	0	0	1	0	0	1	0
0	0	1	0	1	1	1	0	0
0	1	0	0	1	0	0	1	0
0	1	1	0	1	1	1	0	0
1	0	0	0	1	0	1	1	1
1	0	1	0	1	1	1	0	0
1	1	0	1	0	0	1	1	1
1	1	1	1	0	0	1	0	0

CANDIMATICA©

Passer par les tables de vérité peut s'avérer fastidieux. On observe en effet qu'une expression propositionnelle concernant trois propositions fait apparaitre une table de vérité à 8 lignes. On peut montrer qu'une expression impliquant n proposition donnera une table de vérité de 2^n lignes. C'est à dire que si dix propositions sont impliquées alors la table de vérité aura plus de mille lignes ! Vite, un théorème.

Théorème CANDIMATICA

Commutativité. $p\vee q = q\vee p$ et $p\wedge q = q\wedge p$.

Associativité. $p\vee(q\vee r) = (p\vee q)\vee r$ et $p\wedge(q\wedge r) = (p\wedge q)etr$.

Neutralité. $p\wedge\top = p$ et $p\vee\bot = p$.

Distributivité. $p\wedge(q\vee r) = (p\wedge q)\vee(p\wedge r)$ et $p\vee(q\wedge r) = (p\vee q)\wedge(p\vee r)$.

Idempotence. $p\vee p = p$ et $p\wedge p = p$.

Morgan. $\neg(p\vee q) = \neg p\wedge\neg q$ et $\neg(p\wedge q) = \neg p\vee\neg q$.

Absorption 1. $p\vee\top = \top$ et $p\wedge\bot = \bot$.

Tiers exclus. $p\vee\neg p = \top$.

Involution. $\neg(\neg p) = p$.

Contradiction. $p\wedge\neg p = \bot$.

Absoption 2. $p\vee(p\wedge q) = p$ et $p\wedge(p\vee q) = p$.

Le mot Candimatica est purement mnémotechnique. Il m'a été suggéré par Mahmoud.

Démonstration. Il s'agit de comparer les tables de vérité. Nous n'allons pas le faire pour tous. Détaillons une des deux égalités de Morgan[1] et une des deux propriété d'absorption 2.

		A		B	C	
p	q	$p\wedge q$	$\neg A$	$\neg p$	$\neg q$	$B\vee C$
0	0	0	1	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0	1	1
1	1	1	0	0	0	0

On observe ainsi que $\neg(p\wedge q) = \neg p\vee\neg q$.

		A	
p	q	$p\wedge q$	$p\vee A$
0	1	0	0
0	1	0	0
1	0	0	1
1	1	1	1

On observe que $p\vee(p\wedge q) = p$

1. Auguste de Morgan (1806-1871), mathématicien et logicien britannique.

Il en va de même pour les autres propriétés. $\square$

La propriété de l'associativité permet en entre autre de considérer des connections logique entre plus de deux propositions. Tant que le connecteur est le même la priorité des opérations n'est pas problématique. On se permettra alors d'écrire $p \vee q \vee r$ sous entendu qu'il s'agit de $(p \vee q) \vee r$ et qu'il appartient à chacun de déplacer les parenthèses à sa convenance.

Il est souvent plus facile de passer par ces règles que de revenir aux calculs sur les tables de vérité. Comme l'exemple suivant l'illustre.

$$\begin{aligned}
(p \wedge q) \wedge [(\neg p \wedge q) \vee (\neg p \wedge \neg q)] &= (p \wedge q) \wedge [\neg p \wedge (q \vee \neg q)] \qquad \text{factorisation (distributivité)} \\
&= (p \wedge q) \wedge [\neg p \wedge \top] \qquad \text{tiers exclus} \\
&= (p \wedge q) \wedge \neg p \qquad \text{neutralité} \\
&= (p \wedge \neg p) \wedge q \qquad \text{associativité et commutativité} \\
&= \perp \wedge q \qquad \text{contradiction} \\
&= \perp \qquad \text{absorption 1}
\end{aligned}$$

Axiomatique des ensembles

Un ensemble est une boite avec des trucs dedans. Telle est la version simpliste et suffisante d'un ensemble. suffisante pendant un temps, et les mathématiciens faisaient à peu près n'importe quoi avec. Arriva un jour ou cette notion enfantine devint beaucoup trop problématique et on s'aperçut finalement que pour faire bien on ne pouvait pas faire n'importe quoi. Le célèbre *Paradoxe du barbier* de Bertran RUSSELL en est l'exemple emblématique :

> Dans une ville, un barbier rase (uniquement) tous les hommes qui ne se rasent pas eux-même. Qui rase le barbier ?

Pour formaliser la notion d'ensemble (et ainsi esquiver les paradoxes), plusieurs tentatives d'axiomatisation ont été proposées. La plus connue, celle que nous adopteront, est la théorie ZFC pour Zermelo, Frenkel avec l'axiome du Choix.

Définition

Un **ensemble** X est une collection d'**élément**. Un élément x appartenant à X est noté

$$x \in X$$

Les ensembles sont soumis aux axiomes suivants :

Axiome d'extentionnalité. Deux ensembles avec les même éléments sont égaux.

Axiome de l'ensemble vide. Il existe un ensemble sans élément appellé l'**ensemble vide** et généralement noté $\varnothing$.

Axiome de la paire. Si X et Y sont deux ensembles, il existe un ensemble avec ces deux ensembles comme élément. On le note $\{X, Y\}$.

Axiome de la réunion. On vera plus tard.

Axiome de l'ensemble des parties. On vera plus tard.

Axiome de l'infini. Il existe un ensemble X tel que $\varnothing \in X$ et tel que si $x \in X$ alors x et les éléments de x sont des éléments de X.

Schéma d'axiomes de compréhension. On vera plus tard.

Axiome du choix. Étant donné un ensemble X non vide d'ensemble non vide, il existe un ensemble, appelé ensemble de choix, contenant exactement un élément de chaque élément de X.

La majorité de ces axiomes sont très naturels, dans le sens où ils ne sont pas contre nature à la logique classique. L'axiome du choix est beaucoup plus problématique : dans une version simple il stipule qu'étant donné plein d'ensemble, on peut choisir un élément dans chaque ensemble. Ce qui est formellement facile lorsqu'on dispose d'un nombre fini d'ensemble mais est plus compliqué à imaginer avec une infinité. Cela donne naissance à des "paradoxes" qui n'en sont pas. Comme par exemple le paradoxe de Banach-Tarski qui utilise l'axiome du choix : il existe un moyen de découper une boule en 5 morceaux de tel manière qu'un réassemblement de ces morceaux permette d'obtenir deux boules strictement identique à la première. Ce résultat contre nature n'en reste pas moins un théorème c'est à dire un énoncé démontré par un raisonnement logique, donc indiscutablement vrai. Dans le cœur de la preuve il y a l'axiome du choix qui permet de choisir des éléments dans un ensemble sans forcement maitriser ces choix. Ainsi même si l'énoncé du paradoxe semble faire croire que l'axiome du choix est faux, un œil bienveillant sur la démonstration permet de comprendre que c'est "mathématiquement" possible mais irréalisable dans la pratique. Cela suffit à certain pour considérer l'axiome du choix et donc la théorie ZFC. D'autre par contre ne vont pas l'admettre et travailler avec la théorie ZF... Quoiqu'il en soit c'est avec ces axiomes et uniquement eux que l'on construit les ensembles classiques. Partons du commencement avec $\varnothing$, l'ensemble vide (qui ne contient aucun élément). En utilisant l'axiome de la paire, on construit alors l'ensemble $\{\varnothing\}$ qui est donc un ensemble composé d'un élément qui est l'ensemble vide. En utilisant encore l'axiome de la paire on construit l'ensemble $\{\varnothing,\{\varnothing\}\}$. En continuant de la sorte jusqu'à l'infini, ce qui est possible d'après l'axiome de l'infini on construit un ensemble

$$\left\{\underbrace{\varnothing}_{0},\underbrace{\{\varnothing\}}_{1},\underbrace{\{\varnothing,\{\varnothing\}\}}_{2},\underbrace{\{\varnothing,\{\varnothing\},\{\varnothing,\{\varnothing\}\}\}}_{3},\dots\right\}$$

Cet ensemble est communément noté $\mathbb{N}$. Ainsi le nombre 3 manipulé depuis toujours est en fait l'ensemble $\{\varnothing,\{\varnothing\},\{\varnothing,\{\varnothing\}\}\}$. Dans la pratique que nous ferons de la théorie des ensembles nous considérons toujours un **référentielle**, c'est un dire un ensemble de base dont l'existence et la construction sont admises. On le notera dans la pratique $\mathcal{E}$. Toutes les définitions et notations seront relatives à ce référentielle. En particulier tous les ensembles que nous manipulerons seront des sous-ensembles de $\mathcal{E}$.

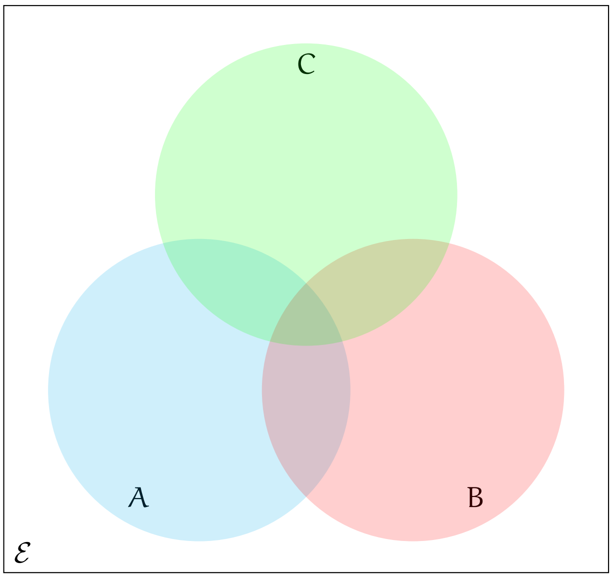
Définition

On dira que A est un **sous-ensemble** de B si tous les éléments de A sont des éléments de B.

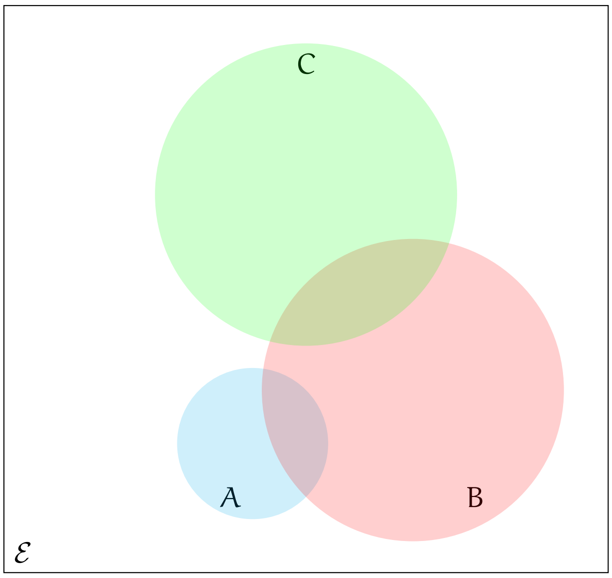
Par exemple $\mathbb{N}$ est un sous-ensemble de $\mathbb{Z}$, lui même un sous-ensemble de $\mathbb{Q}$, lui même un sous-ensemble de $\mathbb{R}$, lui même un sous-ensemble de $\mathbb{C}$, lui même un sous-ensemble de $\mathbb{H}$.

Représentation

L'outil de prédilection en théorie des ensembles est le diagramme de Venn [2]. Il consiste à placer les différents ensemble que l'on souhaite combiner comme des *patates* [3]. Il faut cependant faire attention, il faut, en générale représenter tous les cas de figure possible.



Bon diagramme de Venn



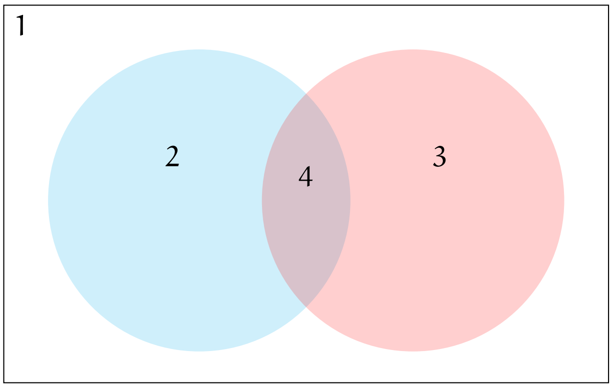
Mauvais diagramme de Venn

2. John Venn (1834-1923) est un mathématicien britannique.
3. On parle d'ailleurs de patatoïdes.

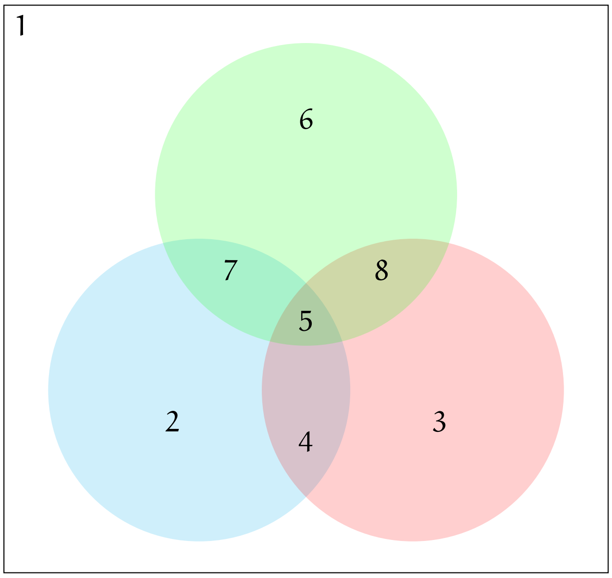
Proposition

Un diagramme de Venn faisant intervenir n ensembles différents, découpe le référentielle en 2^n zone.

Démonstration. Ce résultat se démontre par récurrence sur n ce qui n'est pas le lieu ici. □



Deux ensembles partagent $\mathcal{E}$ en 4 zones



Trois ensembles partagent $\mathcal{E}$ en 8 zones

Peut-être que les curieux pourraient s'intéresser à Newroz...

Le calcul avec les diagramme de Venn, permet assez souvent de représenter des configuration d'ensemble et d'observer des résultats. Il existe deux manières de définir/utiliser les ensembles :

en extension. Dans cette configuration, on décrit l'ensemble par les éléments qui le compose, entre accolade, comme dans l'exemple suivant :

$$A = \{a, 1, \text{"bonjour"}, \pi\}$$

Il y a deux règles a respecter dans ce cas :

1. L'ordre des éléments ne compte pas (c'est en fait l'axiome d'extentionnalité).

$$\{a, 1, \text{"bonjour"}, \pi\} = \{1, a, \text{"bonjour"}, \pi\}$$

2. On ne répète pas le même éléments.

$$\{a, 1, 1, 1, \text{"bonjour"}, \pi\} = \{a, 1, \text{"bonjour"}, \pi\}$$

en compréhension. Cela est une conséquence de l'axiome du schéma d'axiomes en compréhension. On défini un ensemble par la propriété qui le caractérise (qui permet de le *comprendre*).

$$B = \left\{x \in \mathbb{R} \middle| x + 1 < 0\right\}$$

Opérations

Il existe trois opérations élémentaires sur les ensembles. On peut en définir également d'autre mais elles se ramènes souvent à s'interpréter avec ces trois suivantes.

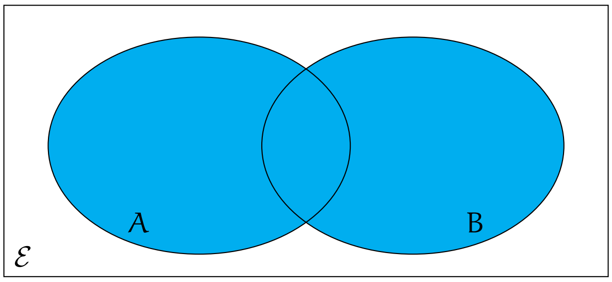
On fixe un référentiel $\mathcal{E}$. C'est entre autre l'axiome de la réunion qui justifie la première définition. Les autres découlent de celle-ci.

Définition

L'**union** de deux ensembles A et B, notée

$$A \cup B$$

est le sous-ensemble de $\mathcal{E}$ formé des éléments qui appartiennent soit à A soit à B.

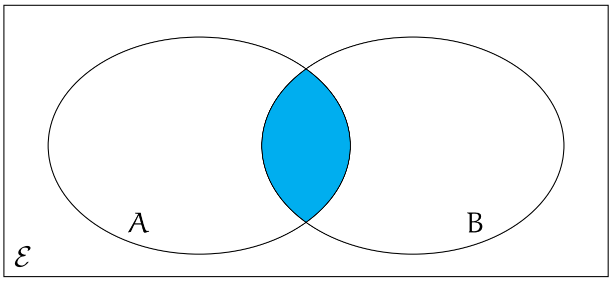


Définition

L'**intersection** de deux ensembles A et B, notée

$$A \cap B$$

est le sous-ensemble de $\mathcal{E}$ formé des éléments qui appartiennent à la fois à A et à B.

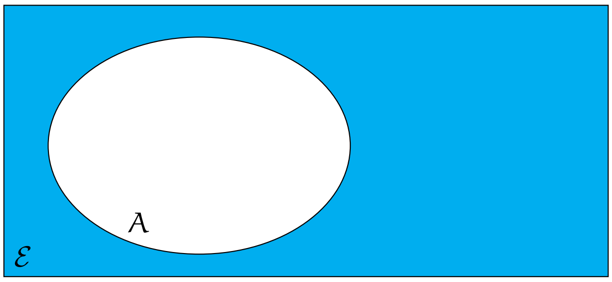


Définition

Le **complémentaire** de A, noté

$$\overline{A}$$

est le sous-ensemble de $\mathcal{E}$ formé des éléments qui ne sont pas dans A.



Le complémentaire est toujours relatif au référentiel. Il est parfois nécessaire de le préciser. On note alors $\complement_{\mathcal{E}} A$ (nous pourrons nous passer de cette notation).

CANDIMATICA©

Il peut être parfois fastidieux de faire des diagramme de Venn. Par exemple le diagramme de Venn à 5 ensembles est d'une part assez difficile à construire et d'autre part, un tel diagramme est assez peu élégant. On peut travailler avec les ensembles en s'appuyant sur des résultats bien connues résumés dans l'acronyme *CANDIMATICA*. On fixe 3 trois ensembles A, B et C d'un même référentiel $\mathcal{E}$.

Théorème CANDIMATICA

Commutativité. $A \cup B = B \cup A$ et $A \cap B = B \cap A$.

Associativité. $(A \cup B) \cup C = A \cup (B \cup C)$ et $(A \cap B) \cap C = A \cap (B \cap C)$.

Neutralité. $A \cup \varnothing = A$ et $A \cap \mathcal{E} = A$.

Distributivité. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ et $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Idempotence. $A \cup A = A$ et $A \cap A = A$.

Morgan. $\overline{A \cup B} = \overline{A} \cap \overline{B}$ et $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Absorption 1. $A \cup \mathcal{E} = \mathcal{E}$ et $A \cap \varnothing = \varnothing$.

Tiers exclus. $A \cup \overline{A} = \mathcal{E}$.

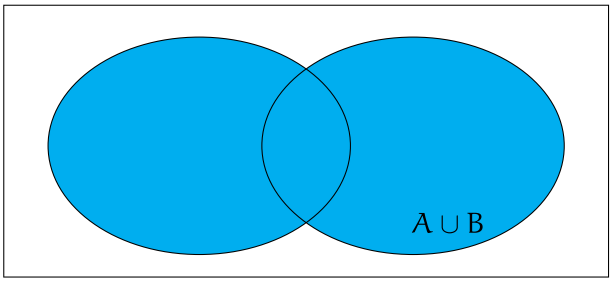
Involution. $\overline{\overline{A}} = A$.

Contradiction. $A \cap \overline{A} = \varnothing$.

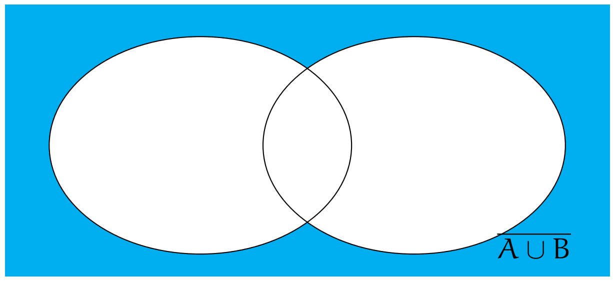
Absoption 2. $A \cup (A \cap B) = A$ et $A \cap (A \cup B) = A$.

Démonstration. On peut par exemple comparer les diagrammes de Venn et vérifier qu'ils couvrent les même zones. Vérifions une des propriétés de Morgan.

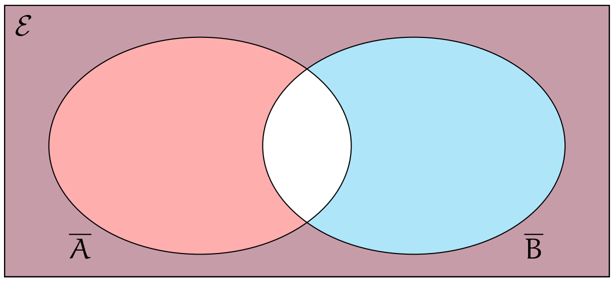
Voici le diagramme de $A \cup B$



Le complémentaire est donc



Colorons $\overline{A}$ (en bleue) et $\overline{B}$ (en rouge).



On observe alors que l'intersection de ces deux ensembles est bien $\overline{A \cup B}$.

$\square$

Cardinalité

Définition

La **cardinalité** d'un ensemble A, noté $\sharp A$ est le nombre d'élément de A.

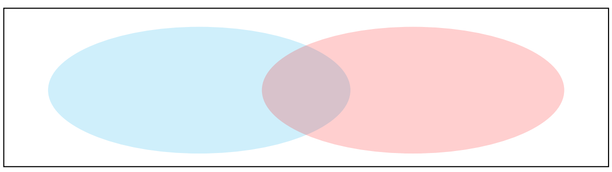
Ainsi, si $A = \{a, b, c\}$ alors $\sharp A = 3$.

Proposition

Soient A et B deux ensembles.

$$\sharp(A \cup B) = \sharp A + \sharp B - \sharp(A \cap B)$$

Démonstration.



Si on compte $\sharp A + \sharp B$ les éléments de $A \cap B$ on été compté deux fois (une fois dans A et une fois dans B) de sorte que $\sharp A + \sharp B - \sharp(A \cap B)$ compte le nombre d'élément de $A \cup B$.

$\square$