Jean-Marc Garnier

Les mathématiques du CAPES

CAPES

Écrit et oral

3e édition

ellipses

Références sciences

Les mathématiques du CAPES

Écrit et oral

3e édition

Jean-Marc Garnier

ellipses

Collection Références sciences

dirigée par Paul de Laboulaye
paul.delaboulaye@editions-ellipses.fr

Retrouvez tous les livres de la collection et des extraits sur www.editions-ellipses.fr

ISBN 9782340-115545
Dépôt légal : mai 2026

www.editions-ellipses.fr

À Julien et Aurélie

et à mes petits-enfants

INTRODUCTION

Ce livre est issu de mon expérience durant une vingtaine d'années dans la préparation au CAPES-CAFEP de mathématiques à l'université de La Rochelle.

Les ambitions de ce livre sont les suivantes :

1. Traiter tout le programme du CAPES-CAFEP de mathématiques dans son intégralité en partant des connaissances que tout bachelier scientifique doit posséder.
2. Donner au futur enseignant de mathématique une vision sur le programme de mathématique du CAPES-CAFEP qui lui permettra d'avoir un recul suffisant et de dominer l'ensemble du programme qu'il aura à enseigner.

   Cet ouvrage englobe donc la totalité du programme « CAPES de mathématique » et le dépasse parfois, mais rarement, uniquement dans le but d'aider à la réussite du concours et dans l'explication de certaines notions éclairant le contenu de ce programme
3. Faire de cet ouvrage un ouvrage de référence pour tous les étudiants durant leurs études universitaires et qui souhaitent devenir enseignant.
4. Le but poursuivi est aussi que cet ouvrage serve de référence pour les enseignants en exercice lorsqu'ils sentiront le besoin d'approfondir ou de revoir une notion.
5. Être surtout un outil et une aide précieuse pour les candidats au CAPES-CAFEP. Ce livre est particulièrement adapté pour aider le futur enseignant à la préparation à l'écrit et à l'oral 1 de ce concours et surtout à réussir à en être lauréat.
6. Donner aux étudiants les connaissances de mathématique que tout mathématicien se doit de maîtriser à la fin de son cursus de licence universitaire.

Les pré-requis mathématiques sont la connaissance des mathématiques des classes terminales scientifiques et surtout une familiarisation du raisonnement mathématique.

À l'exception de ces pré-requis, cet ouvrage se veut totalement autonome dans les contenus.

Un but de ce cours est donc aussi d'aider à la préparation à l'oral du concours. Une leçon d'oral se doit d'être cohérente, logique, avec de nombreux exemples et doit permettre de dégager l'intérêt des notions rencontrées et surtout, le plus important sûrement, le candidat doit maîtriser les sujets qu'il aborde.

Une règle fondamentale à respecter pour l'oral : NE PARLER QUE DES CONTENUS QUE L'ON MAÎTRISE. Tous les candidats n'auront pas 18 à l'oral. Il faut pour la majorité des candidats avoir comme but une note raisonnable, même moyenne ou très moyenne, mais qui permette d'obtenir le CAPES ou le CAFEP. Il vaut donc mieux se placer à un niveau qui ne permettra pas aux jurys d'entraîner le candidat vers des connaissances non maîtrisées, qui aboutiront à une note catastrophique.

J'espère aussi que cet ouvrage procurera un plaisir intellectuel certain, devant la compréhension d'une petite partie de notre réel, que les mathématiques (outil indispensable de cette compréhension) permettent. Si modestement il pouvait contribuer, à sa façon, à atteindre ce but, il aurait aussi rempli totalement son rôle.

Je tiens à remercier mes étudiants des préparations CAPES-CAFEP, pendant toutes mes années d'enseignement, pour le plaisir que j'ai pris à leur enseigner les mathématiques. Il est gratifiant pour un enseignant de s'apercevoir que de très nombreux étudiants (plus très nombreux maintenant et malheureusement) ont encore du plaisir à découvrir les mathématiques et souhaitent transmettre à leur public d'élèves cet enthousiasme.

Je remercie aussi mes collègues de l'université de La Rochelle pour nos échanges et discussions mathématiques pendant la vingtaine d'années où j'y ai enseigné.

Je tiens à remercier particulièrement tous mes collègues, nombreux, qui ont participé à la préparation CAPES-CAFEP, pendant la vingtaine d'années où j'ai eu la responsabilité de cette préparation CAPES.

Je tiens à remercier particulièrement mon frère Lionel, enseignant chercheur en informatique à l'Université de Bourgogne à Dijon, qui m'a fourni l'environnement Latex clés en mains pour la rédaction de cet ouvrage. Il a été pour moi ma personne ressource pour tous les problèmes que j'ai rencontrés avec Latex. Je le remercie enfin pour sa disponibilité à résoudre des problèmes que j'avais parfois avec l'informatique.

Je remercie sincèrement ma compagne qui a su créer autour de moi la sérénité indispensable à la rédaction de cet ouvrage.

Je remercie aussi les éditions Ellipses, et particulièrement, monsieur Paul de Laboulaye pour m'avoir proposé l'édition de ce livre.

Table des matières

Chapitre 1

BASES MATHÉMATIQUES

INTRODUCTION

Les mathématiques reposent sur un système d'axiomes, un axiome étant un énoncé que l'on pose comme vérité. Ensuite, à l'aide du raisonnement logico-déductif, on établit à partir de ces axiomes des propositions, des théorèmes. Toute la difficulté est de bien choisir le système d'axiomes initial et surtout de vérifier que les axiomes choisis ne sont pas contradictoires entre eux. En effet, car si c'est le cas, toute la théorie construite conduit à toutes les propositions à la fois vraies et fausses. L'évolution historique a conduit les mathématiciens, vers 1900, à construire toutes les mathématiques connues à ce jour à partir d'une théorie, appelée « la théorie des ensembles », dépendant d'un système d'axiomes (on devrait dire à partir d'une théorie des ensembles, car il y en a plusieurs). Le système d'axiomes sur lequel on se base dans cet ouvrage est celui de Zermelo-Frankael. À ce jour, ce système semble non contradictoire. On explicitera sommairement ce système, sans rentrer dans les détails qui dépassent le niveau de ce cours. Il est important que de futurs enseignants aient quelques notions sur la base des mathématiques, car toutes les mathématiques connues à ce jour sont construites sur la théorie des ensembles et donc sur ce système d'axiomes. On verra d'ailleurs que la notion d'ensemble sera complètement présente tout au long de cet ouvrage, y compris en probabilité.

Nous définirons donc, après un rappel des règles élémentaires de logique, une ébauche de la théorie des ensembles, les relations fonctionnelles, d'équivalence et d'ordre et ensuite les notions de structure (groupes, anneaux, corps). Tous les paragraphes de ce chapitre sont indispensables et doivent être maîtrisés par les futurs enseignants.

Dans ce chapitre, nous utiliserons parfois dans les exemples qui éclairent des notions rencontrées, les ensembles et sous-ensembles de $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ ou $\mathbf{C}$, ensembles qui sont connus et qui seront revus en détail au chapitre 2.

1.1 Rappels des règles de logique

Une assertion est un énoncé que l'on peut affirmer vrai ou faux sans ambiguïté, l'une de ces deux possibilités excluant l'autre.

Un énoncé vrai dans certaines situations et faux dans d'autres, mais pour lequel dans une situation donnée, nous pouvons décider si cet énoncé est vrai ou faux, s'appelle une proposition.

Une proposition importante s'appelle un théorème. Une proposition se déduisant immédiatement d'une proposition s'appelle un corollaire.

Par exemple, la somme des angles d'un triangle est de 180 degrés est une proposition vraie en géométrie euclidienne, fausse en géométrie hyperbolique et en géométrie sphérique. Ou encore, une des médianes d'un triangle est aussi une hauteur est vraie pour les triangles isocèles et fausses pour les triangles non isocèles.

La négation d'une proposition P, notée « non P » est vraie lorsque P est fausse et fausse lorsque P est vraie.

La conjonction de deux propositions P et Q notée « $P \ et \ Q$ » est vraie si et seulement si P et Q sont vraies simultanément et fausse dans tous les autres cas.

La disjonction de deux propositions P ou Q notée « P ou Q » est fausse si et seulement si P et Q sont fausses simultanément et vraie dans tous les autres cas.

Si P ou Q est vraie, le terme « ou » a toujours le sens suivant, soit P est vraie, soit Q est vraie, soit P et Q sont vraies simultanément. En mathématique, le terme « ou » a toujours le sens précédent.

La proposition « non P ou Q » s'appelle implication et se note $P \Rightarrow Q$ et s'énonce P implique Q ou P entraîne Q. On dit aussi que P est l'hypothèse et Q est la conclusion.

Les propositions P et Q sont dites équivalentes si $P \Rightarrow Q$ et $Q \Rightarrow P$. On note $P \Leftrightarrow Q$ l'équivalence des propositions P et Q.

P	Q	P ou Q	P et Q	$P \Rightarrow Q$	$P \Leftrightarrow Q$
V	V	V	V	V	V
V	F	V	F	F	F
F	V	V	F	V	F
F	F	F	F	V	V

Considérons $P \Rightarrow Q$ vraie, alors si P est vraie, Q est vraie et si Q est faux, alors P est faux. La vérité de P est une condition suffisante de la vérité de Q et la vérité de Q est une condition nécessaire de la vérité de P.

Si $P \Leftrightarrow Q$, on dit que P vraie est une condition nécessaire et suffisante pour que Q soit vraie.

Soit P une proposition, au lieu d'écrire P est vraie, nous écrirons seulement P. Donc, quand nous écrirons une proposition, nous considérerons que cette proposition est vraie.

Remarque 1. On considère qu'une proposition est toujours vraie ou fausse et qu'elle ne peut être à la fois vraie et fausse en même temps. On doit donc rejeter toutes les théories dans lesquelles les propositions P et non P sont vraies et fausses en même temps. De telles théories sont appelées des théories contradictoires. On démontre que dans une théorie contradictoire toute proposition devient alors vraie et fausse, d'où le souci qu'ont eu les mathématiciens d'avoir des système d'axiomes qui ne soient pas contradictoires. Il est impossible parfois de démontrer que certaines théories ne soient pas contradictoires. C'est le cas de la théorie des ensembles sur laquelle repose toutes les mathématiques connues à ce jour. Mais, pour le moment, dans les connaissances actuelles, la théorie des ensembles est non contradictoire.

Remarque 2. En pratique, en mathématique, quand on utilise $P \Rightarrow Q$, on utilise l'implication avec P vraie et on essaye d'en déduire une proposition Q vraie. On utilise, en mathématique, très, très rarement le cas où du faux, on peut en déduire du vrai.

1.2 Théorie des ensembles

1.2.1 Notion d'ensemble

Un ensemble est une collection, un groupement d'objets et est constitué d'éléments. C'est une notion première relativement intuitive. Par exemple l'ensemble contenant les éléments a, b, c se note $\{a, b, c\}$. De même $\{a, b\}$ est l'ensemble contenant les éléments a et b.

On considère les règles suivantes pour les ensembles :

• Un ensemble E est bien défini quand on possède un critère permettant d'affirmer qu'un élément a appartient à E (noté $a \in E$) ou n'appartient pas à E (noté $a \notin E$).

• L'ensemble formé des éléments a, b, c, d ... s'écrira $\{a, b, c, d, ...\}$.

• Un objet mathématique ne peut être à la fois un ensemble et un élément de cet ensemble.

• Si tout élément d'un ensemble A appartient à un ensemble B, on dit que A est inclus dans B que l'on note $A \subset B$.

On dit aussi que A est un sous-ensemble ou une partie de B.

• Deux ensembles A et B sont dit égaux, noté $A = B$, s'ils sont formés exactement des mêmes éléments. Dans le cas contraire, on note $A \neq B$.

Deux ensembles A et B sont donc égaux si et seulement si $A \subset B$ et $B \subset A$.

• On définit l'ensemble ne contenant aucun élément, appelé l'ensemble vide que l'on note $\emptyset$.

• On considère que l'ensemble des éléments de E qui n'appartiennent pas à A (éventuellement vide) est bien un ensemble appelé complémentaire de A dans E et noté $C_E A$ ou C_A s'il n'y a pas d'ambiguïté sur E ou $\overline{A}$ (en probabilité).

• L'ensemble de tous les ensembles n'existe pas.

Remarques.

1. La théorie des ensembles a été inventée ou découverte par Cantor, un peu avant 1900. Elle a été développée les 30 années qui suivirent mais a vécu une période dite des paradoxes car la théorie des ensembles était alors contradictoire. C'est pour cela que les mathématiciens de cette époque définirent des règles et des axiomes sur cette théorie pour ne plus rencontrer ces désordres. Ce qui explique ces distinctions entre éléments appartenant à un ensemble et ensemble inclus dans un ensemble. De nombreux paradoxes venaient de la considération de l'ensemble de tous les ensembles.

2. Le langage courant conduisait aussi à des paradoxes. Considérons les sens différents que peut avoir le verbe être.

   2 est le nombre d'éléments de l'ensemble $\{a, b\}$ (si on note $\{a, b\}$, cela sous-entend que a est différent de b).

   2 est un nombre pair.

   Les nombres pairs sont des entiers.

   Si P désigne l'ensemble des entiers pairs, ces énoncés traduisent :

   1) une égalité $2 =$ le nombre d'éléments de $\{a, b\}$.

   2) une appartenance $2 \in P$.

   3) une inclusion $P \subset \mathbf{Z}$.

   C'est la confusion entre ces trois notions qui a conduit aussi aux problèmes rencontrés par les mathématiciens au début du vingtième siècle et qui les ont amenés à bien distinguer ces notions différentes.

3. La théorie actuelle des ensembles considère des ensembles et des classes d'ensembles. On peut considérer la classe de tous les ensembles qui n'est pas un ensemble.

4. On peut considérer un ensemble ne contenant qu'un élément a, on écrira alors $a \in \{a\}$.
5. L'ordre d'écriture des éléments d'un ensemble n'a pas d'importance, $\{a, b\} = \{b, a\}$. C'est le même ensemble.

1.2.2 Quantificateurs

Soit A une partie d'un ensemble E. On appelle propriété caractéristique des éléments de A tout critère permettant de décider pour tout élément x de E entre les deux propositions $x \in A$ et $x \notin A$.

Donc, si P est une propriété caractéristique des éléments de A, alors « non P » est une propriété caractéristique des éléments de $C_E A$. On dit que P est une propriété définie sur E.

Donc, à $x \in A$, nous pouvons dire x possède la propriété P que nous noterons $P(x)$. Nous écrirons

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

Maintenant, soit P une propriété définie sur un ensemble E et soit A l'ensemble des éléments de E qui possèdent P comme comme propriété caractéristique, alors :

• Soit A est non vide, donc il existe au moins un élément de E vérifiant P, on note

$$\exists x \in E, P(x)$$

qui se lit : il existe au moins un élément x de E vérifiant la propriété P.

• Soit A est vide, aucun élément x de E ne vérifie la propriété P.

• Soit $A = E$, alors tout élément x de E vérifie la propriété P, on note

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

qui se lit : quel que soit un élément x de E, x vérifie la propriété P.

Les symboles $\exists$ et $\forall$ s'appellent des quantificateurs.

Remarques.

1. Un des intérêts des quantificateurs est le suivant :
   la négation de $\exists x \in E, P(x)$ est $\forall x \in E$, non $P(x)$ et
   la négation de $\forall x \in E, P(x)$ est $\exists x \in E$, non $P(x)$
2. Attention à l'ordre dans lequel on utilise les quantificateurs.
   $\forall$..... $\exists$.... n'a pas du tout la même signification que $\exists$..... $\forall$.....
   Par exemple :
   $\forall x \in \mathbf{R}\ \exists y \in \mathbf{R}$, $x \leq y$ est une proposition vraie.
   $\exists x \in \mathbf{R}\ \forall y \in \mathbf{R}$, $x \leq y$ est une proposition fausse.

1.2.3 Axiomes de la théorie des ensembles

Quels que soient les ensembles A et B :

1. Il existe un ensemble appelé réunion de A et B, noté $A \cup B$ dont les éléments sont tous les éléments appartenant à A ou à B.
2. Il existe un ensemble appelé intersection de A et B, noté $A \cap B$ dont les éléments sont tous les éléments appartenant à A et à B.
3. Il existe un ensemble appelé ensemble produit de A et B, noté $A \times B$ dont les éléments sont tous les couples (a, b) tels que $a \in A$ et $b \in B$.
4. Soit P une propriété définie sur A, il existe un ensemble dont les éléments sont tous les éléments appartenant à A vérifiant la propriété P.
5. Il existe un ensemble noté $\mathcal{P}(\mathcal{A})$ appelé ensemble des parties de A, dont les éléments sont tous les sous-ensembles de A.
6. Il existe un ensemble dont les éléments sont toutes les applications de A dans B. Cet ensemble est noté $\mathcal{F}(A, B)$.
7. Si $\mathcal{R}$ est une relation d'équivalence définie sur A, il existe un ensemble appelé ensemble quotient de A par $\mathcal{R}$, noté $\dfrac{A}{\mathcal{R}}$ ou $A/\mathcal{R}$, dont les éléments sont toutes les classes d'équivalence par cette relation.
8. Il existe un ensemble infini noté $\mathbf{N}$ dont les éléments s'appellent les entiers naturels.

Remarque 1. Pour la définition des applications, voir le paragraphe suivant 1.5 et pour la définition des relations, voir le paragraphe suivant 1.4.

Remarque 2. Pour une partie A quelconque d'un ensemble E, on a :

$$\boxed{A \subset E \Leftrightarrow A \in \mathcal{P}(E)}$$

CONVENTION. Dans la suite, les ensembles considérés dans les énoncés des propositions, des théorèmes, des corollaires, des lemmes seront supposés non vides.

1.3 Raisonnements usuels

Les exemples de ce paragraphe utilisent des ensembles connus que l'on abordera au chapitre 2.

• **Raisonnement par l'absurde**.

Soit deux propositions P et Q, on veut montrer que $P \Rightarrow Q$.

On suppose « P et non Q » et on essaye d'aboutir à une contradiction, c'est-à-dire un énoncé faux.

En effet, non(non P ou Q) est la proposition « P et non Q ». Donc si « P et non Q » est faux, non(P et non Q) est vraie et donc « non P ou Q » est vraie.

Exemple. Soit deux réels a et b. Montrons que si $\forall \varepsilon \in \mathbf{R}_+^*$, $a < b + \varepsilon$, alors $a \leq b$.

Supposons $a < b + \varepsilon$ et $a > b$, alors pour $\varepsilon = a - b > 0$, comme $a < b + \varepsilon$, alors $a < b + a - b$, d'où $a < a$, impossible et donc faux.

Donc, $a > b$ est faux et donc $a \leq b$.

• **Raisonnement par contraposition**.

Soit deux propositions P et Q, on veut montrer que $P \Rightarrow Q$. On montre que non $Q \Rightarrow$ non P. Si non $Q \Rightarrow$ non P est vraie, alors la proposition non(non Q) ou non P est vraie. Mais cette proposition est la proposition non P ou Q, qui est $P \Rightarrow Q$.

Exemple. Montrez que si un entier relatif n vérifie n^2 est pair, alors n est un entier pair.

Si n est impair, alors il existe $p \in \mathbf{Z}$ tel que $n = 2p+1$ et donc alors $n^2 = 4p^2+4p+1$ est un entier impair. Donc, n^2 entier pair $\Rightarrow$ n entier pair.

• **Raisonnement par équivalence**.

Soit deux propositions P et Q, on veut montrer que $P \Leftrightarrow Q$, on peut montrer $P \Rightarrow Q$ et $Q \Rightarrow P$ ou raisonner directement par équivalence.

Exemples.

Soit dans $\mathbf{R^2}$ le système $\left\{ \begin{array}{rcl} 2x + 3y & = & 7 \\ 4x - y & = & 7 \end{array} \right.$ à résoudre. En vérifiant que à chaque étape, l'équivalence est légitime,

$$\left\{ \begin{array}{rcl} 2x + 3y & = & 7 \\ 4x - y & = & 7 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rcl} 2x + 3y & = & 7 \\ 7y & = & 7 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rcl} x & = & 2 \\ y & = & 1 \end{array} \right.$$

Si on raisonne par implication, on trouve que les solutions, si elles existent, sont à chercher parmi le couple $(2, 1)$. Il faut alors vérifier que cette solution convient.

Remarque. NE PAS CONFONDRE, « il faut montrer que » et « il suffit de montrer que ».

Il faut savoir distinguer entre condition nécessaire et condition suffisante.

Exemple. Pour que $x > 2$, il est nécessaire que $x^2 > 4$ (mais pas suffisant).
Pour que $x^2 > 4$, il suffit que $x > 2$ (mais pas nécessaire).

• **Existence et unicité**.
Pour établir un résultat d'existence et d'unicité, très souvent on sépare la preuve de l'existence et celle de l'unicité, sauf si on peut démontrer simultanément l'existence et l'unicité.

• **Disjonction des cas**.
On essaye tous les cas possibles, s'ils ne sont pas trop nombreux.

Exemple. Montrez que, dans $\mathbf{R}$, $|x-2| < 1 \Rightarrow 1 < x < 3$.
Si $x \geq 2$, $|x-2| = x-2$ et donc $x < 3$. D'où, $2 \leq x < 3$.
Si $x \leq 2$, $|x-2| = -x+2$ et donc $x > 1$. D'où, $1 \leq x < 2$.
et finalement, $|x-2| < 1 \Rightarrow 1 < x < 3$.

• **Raisonnement par récurrence**.
On établira la démonstration de ce raisonnement dans le chapitre suivant.
Énoncé. Soit $P(n)$ une proposition dépendant d'un entier naturel n. On suppose

1. $\exists n_0 \in \mathbf{N}$ tel que $P(n_0)$ soit vraie.
2. $\forall n \in \mathbf{N}$, $n \geq n_0$, $P(n) \Rightarrow P(n+1)$ est une proposition vraie.

Alors, pour tout $n \geq n_0$, $P(n)$ est une proposition vraie.

Remarque. Un raisonnement par récurrence se fait en trois étapes.
Étape 1. $\exists n_0 \in \mathbf{N}$ tel que $P(n_0)$ soit vraie.
Étape 2. $\forall n \in \mathbf{N}$, $n \geq n_0$, $P(n) \Rightarrow P(n+1)$.
Étape 3. Conclusion.

Il faut éviter de rédiger en écrivant :
« supposons que $\forall n \in \mathbf{N}$, $n \geq n_0$, $P(n)$ est vraie, montrons que $P(n) \Rightarrow P(n+1)$ »,
car dans ce cas, on suppose la conclusion que l'on veut démontrer établie.

Exemples.
Soit la proposition $P(n) : \forall n \in \mathbf{N}$, 3 divise $4^n - 1$. On a $P(1)$ vraie et pour $n \geq 1$, $P(n) \Rightarrow P(n+1)$, donc pour tout $n \geq 1$, $P(n)$ est vraie.

Soit la proposition $P(n) : \forall n \in \mathbf{N}$, 3 divise $4^n + 1$. On a $P(1)$ faux et pour $n \geq 1$, $P(n) \Rightarrow P(n+1)$, mais pour $n \geq 1$, $P(n)$ est faux.
Pour préciser, si 3 divise $4^n + 1$, alors $\exists k \in \mathbf{N}$ tel que $4^n + 1 = 3k$. Donc,

$4^{n+1}+1 = 4.(3k-1)+1 = 3(4k-1)$. Donc, pour $n \geq 1$, $P(n) \Rightarrow P(n+1)$. Et pourtant, pour $n \geq 1$, $P(n)$ est faux.

Le lecteur peut s'amuser à voir que s'il existe $n_0 \in \mathbf{N}$ tel que $P(n_0)$ soit vraie, alors pour $n \geq n_0$, comme 3 divise 4^n+1 et comme 3 divise 4^n-1, alors, en sommant 3 divise 4^n, ce qui est en contradiction avec le théorème de Gauss, paragraphe 4.4.4 page 171. Donc, $\forall n \in \mathbf{N}$, la propriété $P(n)$: 3 divise 4^n+1 est fausse bien que $\forall n \in \mathbf{N}$, l'implication $P(n) \Rightarrow P(n+1)$ soit vraie.

1.4 Relation

1.4.1 Relations binaires

Définition 1. Soit E et F deux ensembles,

on appelle graphe de E vers F, toute partie de $E \times F$.

On appelle correspondance de E vers F la donnée de (Γ, E, F) où Γ est un graphe. L'ensemble E s'appelle l'ensemble de départ, l'ensemble F s'appelle l'ensemble d'arrivée.

L'ensemble $\{x, x \in E$ tel que , $\exists y \in F,\ (x,y) \in \Gamma\}$ s'appelle ensemble de définition de la correspondance (Γ, E, F).

Si $F = E$, toute correspondance de E vers E s'appelle une relation binaire sur E.

Interprétation.

Soit E un ensemble, On dit que l'on a défini une relation binaire sur E, si on se donne une partie du produit cartésien $E \times E$.

On rappelle que d'après la convention énoncée en 1.2.3 page 28, l'ensemble E est supposé non vide.

Notation. Soit $\mathcal{R}$ une telle relation. Si le couple (x,y) de $E \times E$ est en relation par $\mathcal{R}$, on notera $x\mathcal{R}y$.

Exemples.

1. La relation $x = x$ dans un ensemble E est une relation binaire.
2. Soit E un ensemble non vide et $\mathcal{P}(E)$ l'ensemble des parties de E. L'inclusion est une relation binaire dans $\mathcal{P}(E)$.

Définition 2. Une relation binaire sur E est :

réflexive si $\forall x \in E$, $x\mathcal{R}x$.

symétrique si $\forall x,\ y \in E$, $x\mathcal{R}y \Rightarrow y\mathcal{R}x$.

transitive si $\forall x,\ y,\ z \in E$, $x\mathcal{R}y$ et $y\mathcal{R}z \Rightarrow x\mathcal{R}z$.
antisymétrique si $\forall x,\ y \in E$, $x\mathcal{R}y$ et $y\mathcal{R}x \Rightarrow x = y$.

1.4.2 Relations d'équivalence

Définition 3. Une relation binaire sur un ensemble E réflexive, symétrique et transitive s'appelle une relation d'équivalence.
Dans ce cas, si $x \in E$, on appelle classe d'équivalence de x noté $\dot{x}$ (ou $\overline{x}$), l'ensemble $\{y, y \in E, y\mathcal{R}x\}$
On appelle espace quotient de E par la relation $\mathcal{R}$, noté $E/\mathcal{R}$ ou $\dfrac{E}{\mathcal{R}}$, l'ensemble des classes d'équivalence.

Proposition 1. Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E, alors :

1. Toute classe d'équivalence est non vide.
2. Une classe d'équivalence est donnée par l'un quelconque de ses éléments.
3. Deux classes d'équivalence différentes sont disjointes (c'est-à-dire d'intersection vide).
4. Les classes d'équivalence recouvrent l'ensemble E.

Démonstration.

1. Soit α la classe d'un élément a, alors $a \in \alpha$, donc α n'est pas vide.
2. Soit $a \in E$ et $\dot{a}$ la classe de a, si $b \in \dot{a}$, alors $b\mathcal{R}a$.
   $\forall x \in \dot{b}$, $x\mathcal{R}b$ et donc par transitivité, $x\mathcal{R}a$ donc $x \in \dot{a}$ d'où $\dot{b} \subset \dot{a}$.
   $\forall x \in \dot{a}$, $x\mathcal{R}a$ et donc par transitivité et symétrie $x\mathcal{R}b$ donc $x \in \dot{b}$ d'où $\dot{a} \subset \dot{b}$.
   Donc, $\dot{b} = \dot{a}$.
3. Soit $a \in E$ et $\dot{a}$ la classe de a. Soit $b \in E$ et $\dot{b}$ la classe de b. Si $\exists x \in \dot{a} \cap \dot{b}$, alors $x\mathcal{R}a$ et $x\mathcal{R}b$, donc pas symétrie et transitivité de $\mathcal{R}$, on en déduit $a\mathcal{R}b$ et donc $\dot{a} = \dot{b}$. Or, ce résultat est impossible par hypothèse.
4. L'union des classes d'équivalence est un sous-ensemble de E.
   Soit $x \in E$, alors, $x \in \dot{x}$ et donc x appartient à l'union des classes d'équivalence. Les classes d'équivalence recouvrent donc l'ensemble E.

Interprétation. Lorsque sur un ensemble, on ne veut s'intéresser qu'à une propriété particulière des éléments de cet ensemble, on regroupe ensemble tous les éléments ayant la même particularité liée à cette propriété (la classe d'équivalence). Et de ne travailler que dans l'espace quotient revient à ne s'intéresser qu'aux modalités différentes de cette propriété particulière.

Par exemple, considérons un ensemble de propriétaires de voitures de différentes marques et dans cet ensemble la relation : « ...possède une voiture de la même marque automobile que... ». Cette relation est une relation d'équivalence. Les classes d'équivalence correspondent aux différentes marques automobiles.

Cet exemple nous permet de voir ce que sont et à quoi correspondent des classes d'équivalence. On ne s'intéresse qu'à une propriété particulière en occultant les autres propriétés.

1.4.3 Relations d'ordre

Définition 4. Une relation binaire sur un ensemble E réflexive, antisymétrique et transitive s'appelle une relation d'ordre.

Soit $\mathcal{R}$ une relation d'ordre sur un ensemble E, si $\forall x, y \in E$, on a soit $x\mathcal{R}y$, soit $y\mathcal{R}x$, on dit que $\mathcal{R}$ est une relation d'ordre total.

Soit $\mathcal{R}$ une relation d'ordre sur un ensemble E, si $\exists x, y \in E$ tel que x ne soit pas en relation avec y et que y ne soit pas en relation avec x, on dit que $\mathcal{R}$ est une relation d'ordre partiel.

On appelle ensemble ordonné, un ensemble muni d'une relation d'ordre.

On appelle ensemble totalement ordonné, un ensemble muni d'une relation d'ordre total.

Exemples.

1. Soit un ensemble E non vide, la relation d'inclusion entre deux ensembles est une relation d'ordre partiel dans $\mathcal{P}(E)$.
2. Dans $\mathbf{Z}$ la relation notée $\leq$ définie par $x \leq y$ si $y - x \in \mathbf{N}$ est une relation d'ordre total.

Interprétation. L'intérêt des relations d'ordre est de pouvoir comparer, si possible, les éléments d'un ensemble entre eux.

L'intérêt des relations d'ordre total sur un ensemble E est de pouvoir ordonner tous les éléments de cet ensemble.

Notation. En général une relation d'ordre sur un ensemble E ordonné se note $\leq$ pour les ensembles de nombres.

L'ensemble ordonné E par $\leq$ se note $(E, \leq)$.

Définition 5. Soit $(E, \leq)$ un ensemble ordonné, A une partie non vide de E et a un élément de E. Alors, a est

• un majorant de A si $\forall x \in A$, $x \leq a$.

• un minorant de A si $\forall x \in A$, $a \leq x$.

Question. Que se passe-t-il si un majorant de A appartient à A ?

Supposons que A possède deux majorants a et b, tous les deux éléments de A.

Comme $a \in A$ et b majorant de A, alors $a \leq b$.

Comme $b \in A$ et a majorant de A, alors $b \leq a$.

Par antisymétrie, on en déduit que $a = b$. Si il existe un élément de A majorant de A, alors cet élément est unique.

Même raisonnement pour un minorant de A élément de A. D'où la définition suivante :

Définition 6. Soit $(E, \leq)$ un ensemble ordonné, A une partie non vide de E et a un élément de A. Alors, a est

• le plus grand élément de A (noté max A) si $\forall x \in A$, $x \leq a$.

• le plus petit élément de A (noté min A) si $\forall x \in A$, $a \leq x$.

Exemple. Dans $(\mathcal{P}(E), \subset)$, soit $A = \{X, Y, X \cup Y, X \cap Y\}$ où $X \in \mathcal{P}(E)$ et $Y \in \mathcal{P}(E)$ (donc $X \subset E$ et $Y \subset E$). Alors, $\forall Z \in \mathcal{P}(E)$, A est majoré par $X \cup Y \cup Z$ et minoré par $X \cap Y \cap Z$.

Le plus grand élément de A est $X \cup Y$ et le plus petit élément de A est $X \cap Y$.

Le plus grand élément de $\mathcal{P}(E)$ est E et le plus petit élément de $\mathcal{P}(E)$ est $\emptyset$.

Définition 7. Soit $(E, \leq)$ un ensemble ordonné et A une partie non vide de E. On appelle :

• borne supérieure de A (noté $\sup A$), le plus petit élément, si il existe, de l'ensemble des majorants de A.

• borne inférieure de A (noté $\inf A$), le plus grand élément, si il existe, de l'ensemble des minorants de A.

Remarque 1. Des définitions du plus grand élément et du plus petit élément, on déduit que la borne supérieure ou la borne inférieure d'une partie A de E, si elle existe, est unique.

Remarque 2. On verra dans le chapitre suivant que toute partie non vide majorée de $\mathbf{Q}$ n'admet pas forcément une borne supérieure et que toute partie majorée non vide de $\mathbf{R}$ admet nécessairement une borne supérieure.

1.5 Application

1.5.1 Définition

Définition 8. On appelle fonction d'un ensemble E dans un ensemble F toute correspondance (Γ, E, F) dont le graphe Γ vérifie : pour tout x de E, l'ensemble

$$\{y, y \in F,\ (x, y) \in \Gamma\}$$

est vide ou réduit à un élément.

Interprétation. Une fonction est une correspondance d'un ensemble E dans un ensemble F qui, à chaque élément de E associe, au plus, un élément unique de F (certains éléments de E peuvent n'être associés avec aucun élément de F). D'où,

Définition 9. On appelle fonction d'un ensemble E dans un ensemble F toute relation qui à chaque élément de E associe AU PLUS un élément unique de F (certains éléments de E peuvent n'être associés avec aucun élément de F).

Définition 10. On appelle application d'un ensemble E dans un ensemble F toute fonction de E dans F qui, **à chaque** élément de E, associe un élément unique de F.

Remarque 1. Dans le cas d'une application d'un ensemble E dans un ensemble F, CHAQUE élément de E est associé avec un élément UNIQUE de F, mais certains éléments de E peuvent être associés avec le même élément de F.

Remarque 2. Soit une fonction d'un ensemble E dans un ensemble F, notée f, l'ensemble $E' \subset E$, plus grand des ensembles inclus dans E où la fonction de l'ensemble E' dans un ensemble F est une application de E' dans F s'appelle le domaine de définition de f et se note D_f.

Remarque 3. Pour définir une fonction ou une application d'un ensemble E dans un ensemble F, il est nécessaire et suffisant d'avoir trois objets :

• un ensemble de départ E non vide.

• un ensemble d'arrivée F non vide.

• un mécanisme qui permet d'associer à chaque élément de E un élément unique de F dans le cas d'une application et un mécanisme qui permet d'associer à chaque élément de E, soit aucun élément de F, soit un élément unique de F dans le cas d'une fonction.

Notation. Soit f une application d'un ensemble E dans un ensemble F.
Pour $x \in E$, l'élément associé à x par f se note $f(x)$.

$$\begin{array}{rccc} f: & E & \longrightarrow & F \\ & x & \longmapsto & f(x) \end{array}$$

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

Remarque. NE PAS CONFONDRE f et $f(x)$. En effet, $f \in \mathcal{F}(E,F)$ et $f(x) \in F$. Il ne faut pas dire « l'application $f(x)$ », car $f(x)$ est un élément de F, et l'application est f.
Même type de remarque, en remplaçant application par fonction.

Exemple. Soit F une partie non vide d'un ensemble E.

$$\begin{array}{rccc} Id_E: & E & \longrightarrow & E \\ & x & \longmapsto & x \end{array} \qquad \begin{array}{rccc} j: & F & \longrightarrow & E \\ & x & \longmapsto & x \end{array}$$

Id_E s'appelle l'application identité de E et j s'appelle l'injection canonique de F dans E.

1.5.2 Égalité et restriction

Soit E, F, G et H quatre ensembles et soit $f \in \mathcal{F}(E,F)$ et $g \in \mathcal{F}(G,H)$. Alors,

$$f = g \Leftrightarrow \left\{ \begin{array}{rccc} & E & = & G \\ & F & = & H \\ \forall x \in E & f(x) & = & g(x) \end{array} \right.$$

Donc, pour démontrer que deux applications sont égales, trois critères sont à vérifier.
Soit $f \in \mathcal{F}(E,F)$ et soit A une partie non vide de E. Soit $g \in \mathcal{F}(A,F)$ définie par $\forall x \in A$, $g(x) = f(x)$. L'application g s'appelle la restriction de f à A et se note $f_{|A}$.

1.5.3 Image et image réciproque

Définition 11. Soit f une application de E dans F. Soit A une partie de E et B une partie de F. On appelle
• image de A par f l'ensemble noté $f(A)$ défini par $f(A) = \{f(x), x \in A\}$,
• image réciproque de B par f l'ensemble noté $f^{-1}(B)$ défini par
$f^{-1}(B) = \{x, x \in E$ tel que , $f(x) \in B\}$,
• image de f l'ensemble noté Im f défini par
Im $f = f(E) = \{f(x), x \in E\}$.

$f(A)$	=	$\{f(x), x \in A\}$
$f^{-1}(B)$	=	$\{x, x \in E$ tel que , $f(x) \in B\}$
Im f	=	$f(E) = \{f(x), x \in E\}$

1.5.4 Composition d'applications

Définition 12. Soit E, F et G trois ensembles et soit $f \in \mathcal{F}(E, F)$ et $g \in \mathcal{F}(F, G)$, alors, on appelle composée de f et de g l'application de E dans G, notée $g \circ f$ (dans cet ordre) définie par $\forall x \in E$, $g \circ f(x) = g[f(x)]$.

Proposition 2. Soit E, F, G et H quatre ensembles et soit $f \in \mathcal{F}(E, F)$, $g \in \mathcal{F}(F, G)$ et $h \in \mathcal{F}(G, H)$, alors

$$(h \circ g) \circ f = h \circ (g \circ f).$$

Démonstration.
$\forall x \in E$, $(h \circ g) \circ f(x) = (h \circ g)(f(x)) = h(g(f(x))$ et
$h \circ (g \circ f)(x) = h((g \circ f)(x)) = h(g(f(x))$.

Conséquence.
On notera $h \circ g \circ f = (h \circ g) \circ f = h \circ (g \circ f)$.

$$\begin{array}{ccccccc} E & \stackrel{f}{\to} & F & \stackrel{g}{\to} & G & \stackrel{h}{\to} & H \\ x & \mapsto & f(x) & \mapsto & g(f(x)) & \mapsto & h(g(f(x))) = h \circ g \circ f(x) \end{array}$$

1.5.5 Injection, surjection, bijection

Définition 13. Soit f une application de E dans F.

1. On dit que f est injective ou est une injection si
$$\forall x \in E, \forall y \in E, x \neq y \Rightarrow f(x) \neq f(y).$$
2. On dit que f est surjective ou est une surjection si
$$\forall y \in F, \exists x \in E, \text{ tel que } y = f(x).$$
3. On dit que f est bijective ou est une bijection si f est injective et surjective.

Proposition 3. Soit f une application de E dans F. Alors,

1. f est injective si
$$\forall x \in E, \forall y \in E, f(x) = f(y) \Rightarrow x = y.$$

2. f est bijective si
$$\forall y \in F, \exists x \in E, x \textbf{ unique} \text{ tel que } y = f(x).$$

Démonstration.

1. Le premier point s'obtient en effectuant un raisonnement par contraposition de la définition d'une injection.
2. f est bijective donc f est surjective et injective.
   Supposons f injective et surjective. Comme f est surjective, $\forall y \in F, \exists x \in E$, tel que $y = f(x)$.
   Comme f est injective, $y = f(x) = f(x') \Rightarrow x = x'$, donc x est unique. Donc, $\forall y \in F, \exists x \in E, x$ **unique** tel que $y = f(x)$.

   Réciproque. Si $\forall y \in F, \exists x \in E, x$ **unique** tel que $y = f(x)$, alors f est surjective. De plus, l'unicité de l'antécédent x entraîne f injective, donc, f est bijective.

Proposition 4. Soit f une application de E dans F et soit g une application de F dans G.

1. Si f et g sont injectives, alors $g \circ f$ est injective.
2. Si f et g sont surjectives, alors $g \circ f$ est surjective.
3. Si $g \circ f$ est injective, alors f est injective.
4. Si $g \circ f$ est surjective, alors g est surjective.

Démonstration.

1. $\forall x, y \in E, g \circ f(x) = g \circ f(y) \Rightarrow f(x) = f(y)$ car g est injective, et donc $x = y$ car f est injective.
2. $\forall z \in G, \exists y \in F$ tel que $z = g(y)$, car g est surjective. Et comme f est surjective, $\exists x \in E$ tel que $y = f(x)$. Donc, $\forall z \in G, \exists x \in E$ tel que
   $z = g \circ f(x)$.
3. $\forall x, y \in E, f(x) = f(y) \Rightarrow g \circ f(x) = g \circ f(y)$ et comme $g \circ f$ est injective, alors, $x = y$, donc f est injective.
4. Comme $g \circ f$ est surjective, alors, $\forall z \in H, \exists x \in E$ tel que
   $z = g \circ f(x) = g(f(x))$, donc, g est surjective.

Corollaire. Soit f et g deux bijections de E dans E alors $g \circ f$ et $f \circ g$ sont des bijections de E dans E.

Démonstration. Ce corollaire est une conséquence immédiate de la proposition 4.

Remarques. ATTENTION, en général $g \circ f \neq f \circ g$.
Ce corollaire a beaucoup de conséquences mathématiques.
Une bijection de E dans E s'appellera une bijection de E.

1.5.6 Application réciproque d'une bijection

Soit f une bijection de E dans F. Alors, $\forall y \in F$, $\exists x \in E$, x **unique** tel que $y = f(x)$.
La relation qui à chaque y de F associe x de E vérifiant $y = f(x)$ définit une application.

Définition 14. Soit f une bijection de E dans F, alors, l'application, notée f^{-1} de F dans E définie par $f^{-1}(y) = x$ si et seulement si $y = f(x)$, s'appelle application réciproque de f.

$$\begin{array}{|llll|llll|}\hline f: & E & \longrightarrow & F & f^{-1}: & F & \longrightarrow & E \\ & x & \longmapsto & y = f(x) & & y & \longmapsto & x = f^{-1}(y) \\ \hline\end{array}$$

Théorème 1.

1. Si f est une bijection de E dans F, alors f^{-1} est une bijection de F dans E.
2. f est une bijection de E dans F si et seulement si il existe une application g de F dans E vérifiant $g \circ f = Id_E$ et $f \circ g = Id_F$.

Démonstration.

1. Comme f est une bijection, f est donc une application donc, f^{-1} est surjective. Si $x = f^{-1}(y) = f^{-1}(y')$, alors, $y = f(x) = y'$ donc, f est injective.
2. Si f est une bijection de E dans F et si $y = f(x)$, alors, $x = f^{-1}(y)$ et donc $g = f^{-1}$ convient.

   Réciproque. Soit g une application de F dans E vérifiant $g \circ f = Id_E$ et $f \circ g = Id_F$.
   En utilisant la proposition 4, comme $g \circ f = Id_E$ est injective, alors, f est injective, et comme $f \circ g = Id_F$ est surjective, alors, f est surjective. Donc, f est une bijection.

Exemple. Soit E un ensemble et $\mathcal{P}(E)$ l'ensemble des parties de E. Soit f l'application de $\mathcal{P}(E)$ qui à $A \in \mathcal{P}(E)$ associe le complémentaire de $C_E A$ de A dans E. Alors, f est une bijection et $f^{-1} = f$.

Remarque. Soit f une application de E dans F et soit B une partie de F. On a défini l'image réciproque de B par f, que l'on note $f^{-1}(B)$.

ATTENTION, c'est une notation légitime même quand f n'est pas bijective et donc que f^{-1} n'existe pas.

1.5.7 Ensembles équipotents

Définition 15. Deux ensembles E et F sont dits équipotents s'il existe une bijection entre E et F.

Remarque. Si on veut étudier la relation d'équipotence, le problème que l'on rencontre est de savoir dans quel ensemble on peut se placer car l'ensemble des ensembles n'existe pas. Pour pallier à cette difficulté, les mathématiciens ont trouvé une solution : étendre la notion de relation d'équivalence et de classes d'équivalence aux classes d'ensembles. Avec cette extension, on en déduit :

Proposition 5. La relation d'équipotence est une relation d'équivalence.

Démonstration. Démonstration immédiate car l'identité entre deux ensembles est une bijection, donc, l'équipotence est une relation réflexive.
S'il existe une bijection f de l'ensemble E dans l'ensemble F, alors f^{-1} est une bijection de F dans E. Donc, l'équipotence est une relation symétrique.
La composée de deux bijections étant une bijection, l'équipotence est une relation transitive.

1.6 Lois de composition interne

1.6.1 Définition

Définition 16. Soit E un ensemble non vide, on dit que E est muni d'une loi de composition interne si il existe une application T de $E \times E$ dans E.
Si c est l'image d'un élément (a, b) de $E \times E$, on note $c = aTb$, plutôt que
$c = T((a, b))$.
On dit que T est commutative si $\forall (a, b) \in E \times E,\ aTb = bTa$.
On dit que T est associative si $\forall (a, b, c) \in E^3,\ (aTb)Tc = aT(bTc)$.
On dit que T possède un élément neutre si il existe $e \in E$ tel que
$\forall a \in E, aTe = eTa = a$. L'élément e s'appelle élément neutre de la loi T dans E.
On dit qu'un élément a de E possède un symétrique pour T si il existe $a' \in E$ tel que $aTa' = a'Ta = e$. L'élément a' s'appelle élément symétrique de l'élément a pour la loi T dans E.

Si E est muni de deux lois de composition interne, notées T et $*$, on dit que $*$ est distributive à gauche par rapport à T si $\forall a$, b, c éléments de E,
$a*(bTc) = (a*b)T(a*c)$ et que $*$ est distributive à droite par rapport à T si $\forall a$, b, c éléments de E, $(bTc)*a = (b*a)T(c*a)$. Si $*$ est distributive à gauche et à droite par rapport à T, on dit simplement que $*$ est distributive par rapport à T.

Remarque. Si $*$ est une loi commutative, alors la distributivité à droite implique la distributivité à gauche et réciproquement.
Soit a un élément de E munie d'une loi de composition interne commutative T, on dit que a est régulier pour T si $aTx = aTy \Rightarrow x = y$.

Notation. On note (E, T) l'ensemble E muni de la loi de composition interne T.
Si $a \in E$ admet un symétrique pour T, on notera, pour une loi T quelconque a^{-1} ce symétrique.

Exemples.

1. L'addition et la multiplication sont des lois commutatives, associatives et possédant un élément neutre dans les ensembles $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ et $\mathbf{C}$ (voir les paragraphes du chapitre 2).

   De plus, dans ces ensembles, la multiplication est distributive par rapport à l'addition.

2. Soit $\mathcal{P}(E)$ l'ensemble des parties d'un ensemble non vide E, alors, on vérifie facilement que l'union de deux ensembles est une loi interne commutative, associative et possédant $\emptyset$ comme élément neutre.

   L'intersection de deux ensembles est une loi interne commutative, associative et possédant E comme élément neutre.

   De plus, l'union est distributive par rapport à l'intersection et l'intersection est distributive par rapport à l'union.

3. Soit $\mathcal{S}(E)$ l'ensemble des bijections d'un ensemble E, alors la loi de composition des applications est une loi interne, associative (proposition 2), possédant Id_E comme élément neutre, et tout élément f de $\mathcal{S}(E)$ admet pour symétrique f^{-1}, et est en général non commutative.

4. Soit $\mathcal{P}(E)$ l'ensemble des parties d'un ensemble E non vide muni de la loi $\cup$. Il existe, en général, A et B de $\mathcal{P}(E)$ tels que $A \neq B$ et $E \cup A = E \cup B = E$. Donc, E n'est pas régulier.

   Par contre $\emptyset$ est un élément régulier car $\emptyset \cup A = \emptyset \cup B \Rightarrow A = B$.

1.6.2 Propriétés

Proposition 6. Soit un ensemble E muni d'une loi de composition interne T.

1. Si T possède un élément neutre, alors, cet élément est unique.
2. Si un élément a de E possède un symétrique pour une loi de composition interne associative, admettant un élément neutre, alors, cet élément symétrique est unique.

Démonstration.

1. Supposons que T possède deux éléments neutres e et e'. Alors, $eTe' = e'Te = e = e'$. Donc l'élément neutre de T est unique.
2. Si un élément a de E possède deux symétriques a' et a'' pour la loi de composition interne T, alors, $aTa' = e$, d'où $a''T(aTa') = a''Te = a''$. Et comme T est associative, $a''T(aTa') = (a''Ta)Ta' = eTa' = a'$, d'où $a' = a''$. Donc, l'élément symétrique de a est unique.

Proposition 7. Soit, sur un ensemble E, une loi de composition interne T associative, admettant un élément neutre et soit a et b deux éléments de E admettant chacun un symétrique. Alors, aTb admet un symétrique et

$$\boxed{(aTb)^{-1} = b^{-1}Ta^{-1}}$$

Démonstration. Soit e l'élément neutre de T. Et comme T est associative
$(aTb)Tb^{-1}Ta^{-1} = aT(bTb^{-1})Ta^{-1} = aTeTa^{-1} = aTa^{-1} = e$.
Même raisonnement avec, $b^{-1}Ta^{-1}T(aTb) = e$.

Remarque. Si a est un élément inversible d'un ensemble E muni d'une loi de composition interne notée T, alors $(a^{-1})^{-1} = a$.
Si on note la loi additivement, $T = +$, le symétrique de a se note $-a$ et donc $-(-a) = a$.

Définition 17. Soit A une partie non vide d'un ensemble E muni d'une loi de composition interne notée T, on dit que A est une partie stable pour T si

$$\forall x,\ y \in A,\ xTy \in A.$$

1.6.3 Morphismes

Définition 18. Soit (E, T) et (E', T') deux ensembles munis d'une loi de composition interne, on appelle morphisme de E dans E', toute application de E dans E' vérifiant

$$\forall a, b \in E \qquad f(aTb) = f(a)T'f(b).$$

Exemples.

1. Soit f l'application de $\mathcal{P}(E)$ qui à $A \in \mathcal{P}(E)$ associe le complémentaire de $C_E A$ de A dans E.
   On montre facilement que $\forall A,\ B \in \mathcal{P}(E)$, $C_E(A \cap B) = C_E A \cup C_E B$ et $C_E(A \cup B) = C_E A \cap C_E B$.
   Alors, f est un morphisme de $(\mathcal{P}(E), \cup)$ dans $(\mathcal{P}(E), \cap)$ et aussi un morphisme de $(\mathcal{P}(E), \cap)$ dans $(\mathcal{P}(E), \cup)$.
2. Soit f l'application de $(\mathbf{R}, +)$ dans $(\mathbf{R}, \times)$ définie par $f(x) = e^x$. Comme, pour tout x, x' de $\mathbf{R}$, $f(x + x') = e^{x+x'} = e^x \times e^{x'} = f(x) \times f(x')$, on en déduit que f est un morphisme de $(\mathbf{R}, +)$ dans $(\mathbf{R}, \times)$.

1.6.4 Propriétés

Proposition 8. Soit f un morphisme de (E, T) dans (E', T'). Alors, $f(E)$ est stable pour la loi T'.

Démonstration : Soit deux éléments quelconques $f(a)$ et $f(b)$ de $f(E)$.
$fa)T'f(b) = f(aTb) \in f(E)$.

Proposition 9. Soit f un morphisme de (E, T) dans (E', T').

1. Si T est associative (respectivement commutative), alors, T' est associative (respectivement commutative) dans $f(E)$.
2. Si T possède un élément neutre dans E, alors, T' possède $f(e)$ comme élément neutre dans $f(E)$.
3. Soit $a \in E$ admettant pour symétrique a^{-1}, alors, $f(a)$ admet $f(a^{-1})$ pour symétrique dans $f(E)$.

Démonstration.

1. $f(aTb) = f(a)T'f(b)$ et $f(bTa) = f(b)T'f(a)$. Si $aTb = bTa$, alors $f(a)T'f(b) = f(b)T'f(a)$. Même raisonnement pour l'associativité.
2. Soit $f(a) \in f(E)$. $f(a)T'f(e) = f(aTe) = f(a)$, et de même $f(e)T'f(a) = f(a)$.

3. Pour tout élément $f(a)$ de $f(E)$, $f(e) = f(aTa^{-1}) = f(a)T'f(a^{-1})$ et $f(e) = f(a^{-1}Ta) = f(a^{-1})T'f(a)$, donc $f(a^{-1}) = (f(a))^{-1}$.

Exemple. Soit f le morphisme de $(\mathcal{P}(E), \cup)$ dans $(\mathcal{P}(E), \cap)$ définie par $f(A) = C_E A$. On rappelle que l'élément neutre de l'union est $\emptyset$ et que l'élément neutre de l'intersection est E. On vérifie bien que $f(\emptyset) = E$.

1.6.5 Isomorphisme

Définition 19. Soit (E, T) et (E', T') deux ensembles munis chacun d'une loi interne et soit f un morphisme de (E, T) dans (E', T').

• Si $E = E'$ et $T = T'$ le morphisme f s'appelle alors un endomorphisme.

• Si f est une bijection, ce morphisme f s'appelle isomorphisme.

• Si f est un isomorphisme de de (E, T) dans (E', T') et si, $E = E'$ et $T = T'$ l'isomorphisme f s'appelle alors un automorphisme.

Exemple. L'application f de $\mathbf{C}$ qui à z associe $\overline{z}$ est un automorphisme de $(\mathbf{C}, +)$ dans $(\mathbf{C}, +)$ et aussi un automorphisme de $(\mathbf{C}, \times)$ dans $(\mathbf{C}, \times)$.

1.7 Groupes

1.7.1 Définition

Définition 20. Soit G un ensemble muni d'une loi de composition interne T, on dit que (G, T) est un groupe si T est associative, possède un élément neutre et si tout élément de G possède un élément symétrique. Si de plus T est commutative, on dit que (G, T) est un groupe commutatif ou abélien.

Notation. On note (G, T, e) ou (G, T) ou G le groupe G muni de la loi T et d'élément neutre e. Soit x, y deux éléments de G on notera très souvent xy le composé xTy de deux éléments de G.

Conséquences.

• Dans un groupe, l'élément neutre est unique et tout élément de ce groupe admet un symétrique unique. On notera, en général, alors a^{-1} le symétrique d'un élément a de ce groupe.

• On notera simplement G plutôt que (G, T), si il n'y a pas d'ambiguïté sur la loi T.

• Soit a et b deux éléments d'un groupe G, alors aTb admet comme inverse $b^{-1}Ta^{-1}$ (il suffit de composer $b^{-1}Ta^{-1}$ et aTb pour obtenir ce résultat).

• Si le groupe G possède un nombre fini d'éléments, on dit que G est un groupe fini.

Exemples.

1. $(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$, $(\mathbf{C}, +)$, $(\mathbf{Q}^*, \times)$, $(\mathbf{R}^*, \times)$, $(\mathbf{C}^*, \times)$ sont des groupes commutatifs. De même $(\mathbf{Z}/\mathbf{nZ}, +)$ (voir chapitre 4).

2. Soit l'ensemble $G = \{1, -1, i, -i\}$ formé par les racines quatrièmes de l'unité dans $\mathbf{C}$ muni de la loi $\times$ de $\mathbf{C}$. On obtient la table suivante :

$\times$	**1**	**-1**	**i**	**-i**
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

   On vérifie facilement que G est un groupe à 4 éléments, commutatif d'élément neutre 1.

3. Soit l'ensemble $G = \{e, a, b, c\}$ muni de la loi T définie par la table suivante :

T	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

   On vérifie facilement que G est un groupe à 4 éléments, commutatif d'élément neutre e. Ce groupe s'appelle le groupe de Klein. On remarque avec les exemples 2 et 3 que l'on obtient deux groupes distincts de quatre éléments.

   Le groupe de Klein apparaîtra, par exemple, dans la recherche des isométries laissant invariant un rectangle.

4. Soit l'ensemble $G = \{1, -1, i, -i, j, -j, k, -k\}$ muni de la loi $\times$ définie par la table suivante :

$\times$	**1**	**-1**	**i**	**-i**	**j**	**-j**	**k**	**-k**
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1

On vérifie facilement que G est un groupe à 8 éléments, non commutatif et d'élément neutre 1. Ce groupe s'appelle le groupe quaternionique. Donc, il existe des groupes à 8 éléments non commutatifs. On verra (chapitre 12.7.3, proposition 42, page 609) que le groupe du carré a aussi 8 éléments, n'est pas commutatif et est différent du groupe quaternionique.

5. Soit $M_n(\mathbf{R})$ l'ensemble des matrices carrées d'ordre n, alors $(M_n(\mathbf{R})), +)$ est un groupe commutatif (voir chapitre 10).

Remarques.

1. Soit G un groupe fini et soit $a \in G$. Les propriétés de définition d'un groupe impliquent que les applications de $G : x \longmapsto ax$ et $x \longmapsto xa$ sont des bijections de G. Donc, lorsque l'on écrit la table d'un groupe fini, chaque élément de ce groupe apparaît une fois et une seule dans chaque colonne et dans chaque ligne.
2. Si (G, T) et (G', T') sont deux groupes, on vérifie facilement que $G \times G'$ muni de la loi produit (notée .) définie par,
   $\forall (x, x') \in G \times G',\ \forall (y, y') \in G \times G',\ (x, x').(y, y') = (xTy, x'T'y')$.
   est un groupe. Ce produit s'appelle produit direct de G et G'.

   Si on prend $T = +$, $T' = +$, et $G = G' = \mathbf{Z}$ ou $\mathbf{Q}$ ou $\mathbf{R}$ ou $\mathbf{C}$, et si on répète cette opération produit un nombre fini de fois, on obtient, pour $n \in \mathbf{N}^*$, $(\mathbf{Z}^n, +)$, $(\mathbf{Q}^n, +)$, $(\mathbf{R}^n, +)$ sont des groupes commutatifs.

Proposition 10. Soit un groupe (G, T) et a et b deux éléments de G, alors l'équation $aTx = b$ admet une solution unique dans G.

Démonstration.
$aTx = b \Rightarrow a^{-1}T(aTx) = a^{-1}Tb \Rightarrow (a^{-1}Ta)Tx = a^{-1}Tb \Rightarrow eTx = a^{-1}Tb$
$\Rightarrow x = a^{-1}Tb$ et $aT(a^{-1}Tb) = b$.

Remarque. Les axiomes de définition d'un groupe sont exactement ceux qui permettent d'obtenir une solution unique à l'équation $aTx = b$ (associativité, existence d'un élément neutre et existence d'un symétrique pour tout élément d'un groupe).

Convention. En général,
• Si T est commutative, donc, G est un groupe commutatif, on note
additivement la loi T (T est notée $+$), e est noté 0 et on note $-a$ le symétrique d'un élément a de G.
Pour $a \in G$ et $n \in \mathbf{N}^*$, $na = a + ... + a$ (n termes), $0a = 0$ et
$(-n)a = (-a) + ... + (-a)$ (n termes).

• Si T est non commutative, alors G est un groupe non commutatif, on note multiplicativement la loi T (T est notée $\times$ ou .), e est noté 1 et on note a^{-1} le symétrique d'un élément a de G.
Pour $a \in G$ et $n \in \mathbf{N}^*$, $a^n = a \times ..... \times a$ (n termes), $a^0 = 1$ et
$a^{-n} = (a^{-1}) \times ..... \times (a^{-1})$ (n termes).

• Soit a, b deux éléments d'un groupe commutatif $(G, +)$, on pose

$$\mathbf{a - b = a + (-b)}.$$

L'application de G^2 dans G qui au couple (a, b) associe $a - b$ définit une nouvelle loi de composition interne appelée soustraction. Cette loi n'est pas commutative, pas associative et ne possède pas d'élément neutre.

• En notation additive dans un groupe commutatif G,
$-(-a) = a$, $-(a + b) = -a - b$ et $-(a - b) = -a + b$.
La démonstration est immédiate car le symétrique de $-a$ est a et le symétrique de $a + b$ est $-a - b$.

1.7.2 Morphisme de groupes

1.7.2.1 Définition

Définition 21. Soit (G, T) et (G', T') deux groupes, on appelle morphisme de groupe de G dans G', toute application de G dans G' vérifiant

$$\forall a, b \in G \qquad f(aTb) = f(a)T'f(b).$$

Exemples.

1. Soit f l'application de $(\mathbf{Z}, +)$ dans $(\mathbf{R}, +)$ définie par $f(x) = x$, alors f est un morphisme du groupe $(\mathbf{Z}, +)$ dans le groupe $(\mathbf{R}, +)$.
2. Soit f l'application de $(\mathbf{R}, +)$ dans $(\mathbf{R}^*, \times)$ définie par $f(x) = e^x$. Comme, pour tout x, x' de $\mathbf{R}$, $f(x + x') = e^{x+x'} = e^x \times e^{x'} = f(x) \times f(x')$, on en déduit que f est un morphisme de groupes, du groupe $(\mathbf{R}, +)$ dans le groupe $(\mathbf{R}^*, \times)$.
3. Soit $(G, .)$ un groupe et a un élément de G. Soit f l'application de $(\mathbf{Z}, +)$ dans $(G, .)$ définie par $f(n) = a^n$. Alors, pour tout n, n' dans $\mathbf{Z}$,
$f(n + n') = a^{n+n'} = a^n.a^{n'} = f(n).f(n')$. On en déduit que f est un morphisme de groupes, du groupe $(\mathbf{Z}, +)$ dans le groupe $(G, .)$.
4. Soit $(G, .)$ un groupe et a un élément de G. Soit f l'application de $(G, .)$ dans $(G, .)$ définie par $f(x) = axa^{-1}$. Alors, pour tout x, x' dans G,
$f(x.x') = axx'a^{-1} = axa^{-1}ax'a^{-1} = f(x).f(x')$.

On en déduit que f est un morphisme de groupes, du groupe $(G, .)$ dans le groupe $(G, .)$.

5. Soit $M_n(\mathbf{R})$ l'ensemble des matrices carrées d'ordre n, et $A = (a_{i,j})$ une matrice de $M_n(\mathbf{R})$. On rappelle que $(M_n(\mathbf{R})), +)$ est un groupe commutatif. On appelle trace de A (notée tr (A)) le réel défini par
tr $(A) = \sum_{i=1}^{n} a_{i,i}$. Alors, pour toutes matrices A, B de $M_n(\mathbf{R})$,
$f(A + B) =$ tr $(A + B) =$ tr $A +$ tr $B = f(A) + f(B)$. Donc, f est un morphisme du groupe $(M_n(\mathbf{R}), +)$ dans $(\mathbf{R}, +)$.

1.7.2.2 Propriétés

Proposition 11. Soit f un morphisme du groupe (G, T) dans le groupe (G', T'), alors,

1. Si e est l'élément neutre de G et e' l'élément neutre de G', $f(e) = e'$.
2. Pour tout élément a de G, $f(a^{-1}) = (f(a))^{-1}$.

Démonstration.

1. $f(e) = f(eTe) = f(e)T'f(e)$, or $f(e) = f(e)T'e'$, donc,
$f(e)T'f(e) = f(e)T'e'$, d'où $f(e) = e'$ car G' est un groupe donc $f(e)$ admet un symétrique (il suffit de composer à gauche par le symétrique de $f(e)$ dans l'égalité $f(e)T'f(e) = f(e)T'e'$).
2. Pour tout élément a de G, $f(e) = f(aTa^{-1}) = f(a)T'f(a^{-1})$, or,
$e' = f(e) = f(a)T'(f(a))^{-1}$, donc $f(a^{-1}) = (f(a))^{-1}$.

Exemple. Soit f l'application de $(\mathbf{R}, +)$ dans $(\mathbf{R}^*, \times)$ définie par $f(x) = e^x$. On vérifie bien que $f(0) = 1$ et que pour tout x de $\mathbf{R}$,

$$f(-x) = e^{-x} = \frac{1}{e^x} = (e^x)^{-1}.$$

1.7.2.3 Isomorphisme de groupes

Définition 22. Soit (G, T) et (G', T') deux groupes et f un morphisme du groupe G dans le groupe G'. Si f est une bijection, on dit que f est un isomorphisme du groupe G dans le groupe G' et que les groupes (G, T) et (G', T') sont isomorphes.
Si de plus $G = G'$ et $T = T'$ l'isomorphisme f s'appelle alors un automorphisme de groupes.

Exemples.

1. Soit f l'application de $\mathbf{C}$ dans $\mathbf{C}$ définie par $f(z) = \overline{z}$, alors f est un automorphisme du groupe $(\mathbf{C}, +)$ et un automorphisme du groupe $(\mathbf{C}^*, \times)$.
2. Soit f l'application de $(\mathbf{R}, +)$ dans $(\mathbf{R}_+^*, \times)$ définie par $f(x) = e^x$. Alors, f est un isomorphisme du groupe $(\mathbf{R}, +)$ dans le groupe $(\mathbf{R}_+^*, \times)$. Donc, les deux groupes $(\mathbf{R}, +)$ et $(\mathbf{R}_+^*, \times)$ sont isomorphes.
3. Soit $\mathbf{U} = \{z \in \mathbf{C}, \quad |z| = 1\}$ et f l'application de $\mathbf{R}$ dans $\mathbf{U}$ définie par $f(x) = e^{ix}$, alors f est un morphisme du groupe $(\mathbf{R}, +)$ dans le groupe $(\mathbf{U}, \times)$ (on vérifie facilement que $(\mathbf{U}, \times)$ est un groupe commutatif et que f est un morphisme de groupes).
   Pour tout $x \in \mathbf{R}$, $f(x + 2\pi) = e^{i(x+2\pi)} = e^{ix}e^{i2\pi} = e^{ix} = f(x)$. Donc, f est un morphisme de groupes non injectif, d'où, f n'est pas un isomorphisme de groupes. Donc, les groupes $(\mathbf{R}, +)$ et $(\mathbf{U}, \times)$ ne sont pas isomorphes.

Proposition 12. Si f un isomorphisme du groupe (G, T) dans le groupe (G', T'), alors, l'application f^{-1} est un isomorphisme du groupe (G', T') dans le groupe (G, T).

Démonstration. L'isomorphisme est une bijection, donc f^{-1} existe et est une bijection de G' dans G.

Soit u et v deux éléments de G'. Il existe, puisque f est une bijection, deux éléments a et b de G tels que $u = f(a)$ et $v = f(b)$.

$f^{-1}(uT'v) = f^{-1}(f(a)T'f(b)) = f^{-1}(f(aTb)) = aTb = f^{-1}(u)Tf^{-1}(v)$. Donc, $f^{-1}(uT'v) = f^{-1}(u)Tf^{-1}(v)$, d'où, f^{-1} est bien un isomorphisme du groupe (G', T') dans le groupe (G, T).

Exemple. Soit f l'application de $(\mathbf{R}, +)$ dans $(\mathbf{R}_+^*, \times)$ définie par $f(x) = e^x$. Alors, f est un isomorphisme du groupe $(\mathbf{R}, +)$ dans le groupe $(\mathbf{R}_+^*, \times)$.

Alors, $f^{-1} = \ln$ est bien un isomorphisme du groupe $(\mathbf{R}_+^*, \times)$ dans le groupe $(\mathbf{R}, +)$. On retrouve bien la relation :

$$\text{Pour tout } x, x' \text{ de } (\mathbf{R}_+^*), \ln(xx') = \ln x + \ln x'.$$

1.7.3 Sous-groupes

1.7.3.1 Définitions

Rappel. Soit H un sous-ensemble non vide d'un ensemble E muni d'une loi de composition interne T. On dit que H est stable pour T si pour tout élément x et y de H, $xTy \in H$.