MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÉ ABDELHAMID BEN BADIS DE MOSTAGANEM
FACULTÉ DES SCIENCES EXACTES ET DE L'INFORMATIQUE
DÉPARTEMENT DE MATHÉMATIQUES ET INFORMATIQUE
FILIÈRE : MATHÉMATIQUES

Polycopié de cours

Algèbre

Cours et Exercices corrigés

Réalisé par :

Dr. Mansouria SAIDANI

Première année licence MI LMD

Année universitaire : 2019 / 2020

Table des matières

Introduction

Le cours que nous présentons ici s'adresse aux étudiants de la première année licence mathématiques et informatique LMD, aux étudiants de certains écoles supérieures ainsi qu'aux étudiants des classes préparatoires en sciences et Technologie. Il regroupe les notions de base du programme de l'Algèbre.

Ce polycopié est inspiré du cours que j'ai réalisé durant les années 2005-2011 au sein du département de tronc commun SETI et du cours qui a été réalisé par M. Medeghri Ahmed au sein du département de Mathématiques et Informatique à l'université Abdelhamid Ibn Badis.

L'objectif de ce polycopié est présenter les points essentiels permettant à l'étudiant de comprendre certaines parties du cours magistral pour aborder efficacement les exercices proposés dans les séances de travaux dirigés. Il a aussi pour but de l'aider, par la pratique de l'Algèbre à mieux aborder les notions nouvelles lors leurs première année de premier cycle.

Le polycopié s'articule autour de cinq chapitres. À la fin de chaque chapitre, on pourra trouver une série d'exercices corrigés et d'autres proposés.

Le premier chapitre est consacré aux notions de bases de la logique : proposition logique, connecteurs logiques, quantificateurs. Nous donnons par la suite quelques méthodes de démonstration avec quelques exemples illustratifs.

Le deuxième chapitre traite les notions suivantes : les ensembles, opérations sur un ensemble, les applications, image directe et image réciproque d'un ensemble par une application.

Dans le troisième chapitre, nous définissons les deux types des relations binaires : relation d'équivalence et relation d'ordre, classes d'équivalences, ensemble quotient. Ce chapitre est aussi illustré par des exemples.

Nous définissons dans le chapitre quatre les structures algébriques que l'on rencontre dans presque toutes les branches des mathématiques. En particulier, nous définissons la structure de corps qui est la base dans la définition d'un espace vectoriel. Nous commencerons par donner la définition d'un groupe qui est utilisée dans plusieurs autres structures algébriques.

Nous étudions dans le dernier chapitre l'ensemble des polynômes sur un corps $\mathbb{K}$ et nous montrons qu'ils ont plusieurs propriétés qui sont analogues aux propriétés des entiers relatifs.

À la fin de ce manuscrit, nous présentons quelques références de bases classiques et récentes et que le lecteur ou l'étudiant pourra aisément consulter.

Chapitre 1

Logique et raisonnement

1 Introduction

Ce chapitre est consacré aux notions de base concernent la logique mathématique : proposition logique, les connecteurs logiques, méthodes de raisonnement,... etc. Ces notions nous permettent de motiver les méthodes de démonstration employées dans les preuves mathématiques. Ce chapitre est basé sur les références ([2],[4], [5], [8], [9], [12]).

2 Proposition logique

Définition 1.1 *[4], [5], [9] Une proposition logique est une phrase qui a une seule valeur de vérité : vraie ou fausse (pas les deux en même temps).*

Exemple 1.1
- *Le soleil brillera chaque matin.*
- *12 :4=3.*
- *Pour tout* $x \in \mathbb{R}, x^2 \geqslant 0$.

Notation 1.1 *[4], [5], [9] Une proposition logique est notée généralement par une lettre majuscule :* P, Q, R...

3 Connecteurs logiques

On peut obtenir des nouvelles propositions à partir de propositions P, Q, ...

3.1 Négation

Définition 1.2 *[4], [5], [9] Étant donné une proposition logique* P. *la proposition logique non*P *(ou bien* $\neg$P*) est appelée la négation de* P *qui est vraie si la proposition* P *est fausse, et fausse si* P *est vraie. On résume ceci dans la table de vérité :*

P	$\neg$P
V	F
F	V

TABLEAU 1.1 – Table de vérité de "non P"

Exemple 1.2 *P : "3 est un diviseur de 12" est une proposition vraie.* $\neg$P *: "3 n'est pas un diviseur de 12" est une proposition fausse.*

3.2 Conjonction

Définition 1.3 *[4], [5], [9] Étant données deux propositions logiques* P_1 *et* P_2*. La proposition "*P_1 *et* P_2*" (ou bien* $P_1 \wedge P_2$*) est appelée conjonction de* P_1 *et* P_2*, qui est vraie si* P_1 *est vraie et* P_2 *est vraie. La proposition "*P_1 *et* P_2*" est fausse sinon .*

P_1	P_2	$P_1 \wedge P_2$
V	V	V
V	F	F
F	V	F
F	F	F

TABLEAU 1.2 – Table de vérité de "$P_1 \wedge P_2$"

Exemple 1.3 P_1 *: "2 est un diviseur de 20" est une proposition logique vraie.*
P_2 *: "*$3 \leqslant 11$*" est une proposition logique vraie.*
La proposition logique $P_1 \wedge P_2$ *est vraie.*

Exemple 1.4 *Soient les deux propositions logiques suivantes.*
P_1 *: "*$x \leqslant 5$*"*
P_2 *: "*$x \geqslant 11$*" avec x est un réel.*
La proposition logique $P_1 \wedge P_2$ *est fausse pour tout nombre réel x.*

3.3 Disjonction

Définition 1.4 *[4], [5], [9] Étant données deux propositions logiques* P_1 *et* P_2*. La proposition "*P_1 *ou* P_2*" (ou bien* $P_1 \vee P_2$*) est appelée disjonction de* P_1 *et* P_2*, qui est vraie si l'une des propositions logiques* P_1 *ou* P_2 *est vraie. La proposition "*$P_1 \vee P_2$*" est fausse si les deux propositions logiques* P_1 *et* P_2 *sont fausses.*

P_1	P_2	$P_1 \vee P_2$
V	V	V
V	F	V
F	V	V
F	F	F

TABLEAU 1.3 – Table de vérité de "$P_1 \vee P_2$"

Exemple 1.5 P_1 *: "2 est un diviseur de 20" est une proposition logique vraie.*
P_2 *: "*$3 \leqslant 11$*" est une proposition logique vraie.*
La proposition logique $P_1 \vee P_2$ *est vraie.*

Exemple 1.6 *Soient les deux propositions logiques suivantes.* P_1 *: "*$x \leqslant 5$*."*
P_2 *: "*$x \geqslant 11$*" x est un réel.*
La proposition logique $P_1 \vee P_2$ *est vraie pour tout* $x \in]-\infty, 5] \cup [11, +\infty[$ *et fausse pour* $x \in]5, 11[$ *.*

3.4 Implication

Définition 1.5 *[4], [5], [9] Étant données deux propositions logiques* P_1 *et* P_2*. La proposition "non*P_1 *ou* P_2*" est notée "*$P_1 \Rightarrow P_2$*" qui est fausse si la proposition logique* P_1 *est vraie et la proposition logique* P_2 *est fausse. Dans les autres cas, la proposition "*$P_1 \Rightarrow P_2$*" est vraie.*

On dit que "la proposition P_1 *implique la proposition* P_2*" ou bien "si* P_1 *est vraie, alors* P_2 *est vraie "*

De cette définition, on obtient la table de vérité suivante :

P_1	P_2	$P_1 \Rightarrow P_2$
V	V	V
V	F	F
F	V	V
F	F	V

TABLEAU 1.4 – Table de vérité de "$P_1 \Rightarrow P_2$"

Exemple 1.7 P_1 *: " 24 est divisible par 8" est une proposition logique vraie.*
P_2 *: "24 est divisible par 2 " est une proposition logique vraie. La proposition logique* $P_1 \Rightarrow P_2$ *est vraie.*

Exemple 1.8 *Soient les deux propositions logiques suivantes.*
P_1 *: "Je suis un citoyen français"*
P_2 *: "Je maîtrise la langue française " .*
La proposition logique $P_1 \Rightarrow P_2$ *est vraie, mais la proposition logique* $P_2 \Rightarrow P_1$ *est fausse.*

Exemple 1.9 *La proposition logique" Si* $\cos\alpha = 1$*, alors* $\alpha = 2\pi$ *" est fausse.*

3.5 Équivalence

Définition 1.6 *[4], [5], [9] Étant données deux propositions logiques* P_1 *et* P_2*. On dit que la proposition* P_1 *et la proposition* P_2 *sont logiquement équivalentes si elles ont les mêmes valeurs de vérité. On note* $P_1 \Leftrightarrow P_2$ *et on lit "*P_1 *est équivalent à* P_2*" ou "*P_1 *si et seulement si* P_2*". Sa table de vérité est donnée comme suit :*

P_1	P_2	$P_1 \Leftrightarrow P_2$
V	V	V
V	F	F
F	V	F
F	F	V

TABLEAU 1.5 – Table de vérité de "$P_1 \Leftrightarrow P_2$"

Exemple 1.10 P_1 *: " 25 est divisible par 2" est une proposition logique fausse.*
P_2 *: "Pour tout nombre réel x,* x^2 *est positif" est une proposition logique vraie.*
La proposition logique $P_1 \Leftrightarrow P_2$ *est fausse.*

Exemple 1.11 *Soient les deux propositions logiques suivantes.*
P_1 *: "Alger est la capitale de l'Algérie"*
P_2 *: "*$\frac{5}{7}$ *est un nombre rationnel " . La proposition logique* $P_1 \Leftrightarrow P_2$ *est toujours vraie.*

3.6 Propriétés

[4], [5], [9] Étant données les trois propriétés suivantes P_1, P_2 et P_3. Alors,

1. $\neg(P_1 \wedge P_2) \Leftrightarrow (\neg P_1 \vee \neg P_2)$, Règle de Morgan.
2. $\neg(P_1 \vee P_2) \Leftrightarrow (\neg P_1 \wedge \neg P_2)$, Règle de Morgan.
3. $P_1 \Leftrightarrow \neg(\neg P_1)$.
4. $((P_1 \wedge P_2) \wedge P_3) \Leftrightarrow (P_1 \wedge (P_2 \wedge P_3))$, associativité de $\wedge$.
5. $((P_1 \vee P_2) \vee P_3) \Leftrightarrow (P_1 \vee (P_2 \vee P_3))$, associativité de $\vee$.
6. $((P_1 \vee P_2) \wedge P_3) \Leftrightarrow ((P_1 \wedge P_3) \vee (P_2 \wedge P_3))$, distributivité de $\wedge$ par rapport à $\vee$.
7. $((P_1 \wedge P_2) \vee P_3) \Leftrightarrow ((P_1 \vee P_3) \wedge (P_2 \vee P_3))$, distributivité de $\vee$ par rapport à $\wedge$.
8. $(P_1 \Rightarrow P_2) \Leftrightarrow (\neg P_2 \Rightarrow \neg P_1)$, la contraposée.

Preuve. 1. et 2.

P_1	P_2	$\neg P_1$	$\neg P_2$	$\neg P_1 \vee \neg P_2$	$\neg P_1 \wedge \neg P_2$	$P_1 \vee P_2$	$\neg(P_1 \vee P_2)$	$(P_1 \wedge P_2)$	$\neg(P_1 \wedge P_2)$
F	F	V	V	V	V	F	V	F	V
F	V	V	F	V	F	V	F	F	V
V	F	F	V	V	F	V	F	F	V
V	V	F	F	F	F	V	F	V	F

On remarque que les propositions logiques $\neg(P_1 \wedge P_2)$ et $(\neg P_1 \vee \neg P_2)$ ont les mêmes valeurs de vérité, donc elles sont équivalentes.

De même pour $\neg(P_1 \vee P_2)$ et $(\neg P_1 \wedge \neg P_2)$.

3.

P_1	$\neg P_1$	$\neg(\neg P_1)$
V	F	V
F	V	F

Donc, la négation de la négation d'une proposition logique P_1 est équivalente à P_1, donc $\neg(\neg P_1) \Leftrightarrow P_1$.

4.

P_1	P_2	P_3	$P_2 \wedge P_3$	$P_1 \wedge (P_2 \wedge P_3)$	$P_1 \wedge P_2$	$(P_1 \wedge P_2) \wedge P_3$
V	V	V	V	V	V	V
V	F	V	F	F	F	F
F	V	V	V	F	F	F
F	F	V	F	F	F	F
V	V	F	F	F	V	F
V	F	F	F	F	F	F
F	V	F	F	F	F	F
F	F	F	F	F	F	F

Donc, $((P_1 \wedge P_2) \wedge P_3) \Leftrightarrow P_1 \wedge (P_2 \wedge P_3)$, de même pour $((P_1 \vee P_2) \vee P_3) \Leftrightarrow P_1 \vee (P_2 \vee P_3)$.

6. En utilisant le tableau suivant, on déduit que les propositions $((P_1 \vee P_2) \wedge P_3)$ et $((P_1 \wedge P_3) \vee (P_2 \wedge P_3))$ ont les mêmes valeurs de vérité.

P_1	P_2	P_3	$(P_1 \wedge P_3)$	$(P_2 \wedge P_3)$	$((P_1 \wedge P_3) \vee (P_2 \wedge P_3))$	$(P_1 \vee P_2)$	$((P_1 \vee P_2) \wedge P_3)$
F	F	F	F	F	F	F	F
F	F	V	F	F	F	F	F
F	V	F	F	F	F	V	F
F	V	V	F	V	V	V	V
V	F	F	F	F	F	V	F
V	F	V	V	F	V	V	V
V	V	F	F	F	F	V	F
V	V	V	V	V	V	V	V

Donc $((P_1 \vee P_2) \wedge P_3) \Leftrightarrow ((P_1 \wedge P_3) \vee (P_2 \wedge P_3))$.
De même pour $((P_1 \wedge P_2) \vee P_3) \Leftrightarrow ((P_1 \vee P_3) \wedge (P_2 \vee P_3))$.

8. En utilisant la définition de l'implication, on obtient

$$\begin{aligned}(P_1 \Rightarrow P_2) &\Leftrightarrow (\neg P_1 \vee P_2)\\ &\Leftrightarrow (\neg P_1 \vee \neg(\neg P_2))\\ &\Leftrightarrow (\neg(\neg P_2) \vee \neg P_1), \text{ en utilisant la symétrie de la disjonction.}\\ &\Leftrightarrow (\neg P_2 \Rightarrow \neg P_1)\end{aligned}$$

■

4 Quantificateurs

Définition 1.7 *Quantificateur universel [4], [5], [9]*

L'expression "quel que soit" notée "$\forall$" est appelée quantificateur universel, ce dernier permet de réécrire l'assertion "pour tout x dans E, x vérifie A" sous la forme "$\forall x \in E, A(x)$".

Définition 1.8 *Quantificateur existentiel [4], [5], [9]*

L'expression "il existe au moins " notée "$\exists$" est appelée quantificateur existentiel, ce dernier permet de réécrire l'assertion "il existe au moins un x dans E, x vérifie A" sous la forme "$\exists x \in E, A(x)$".

Exemple 1.12 *La proposition logique "$\forall a \in \mathbb{R}, a^2 < 0$" est fausse.*

Exemple 1.13 *La proposition logique"$\exists a \in \mathbb{C}, a^2 < 0$" est vraie.*

4.1 Ordre

[4], [5], [9] Dans le cas de l'utilisation d'un quantificateur deux fois dans une proposition logique, l'ordre n'a pas d'importance, autrement dit on peut permuter les quantificateurs dans des écritures de type

$$\forall a \in E, \forall b \in E \quad A(a,b),$$

$$\exists a \in E, \exists b \in E \quad A(a,b).$$

Mais, dans le cas où les quantificateurs sont différents, alors leur ordre est important.

Dans l'écriture $\forall a \in E, \exists b \in E \quad A(a,b)$, b dépend de a.

Dans l'écriture $\exists b \in E, \forall a \in E \quad A(a,b)$, b ne dépend pas de a.

4.2 Négation des quantificateurs

[4], [5], [9] La négation de "$\forall a \in$ E, a vérifie A" est "$\exists$ a $\in$ E, "a" ne vérifie pas A", et la négation de "$\exists$ a $\in$ E, a vérifie A" est "$\forall a \in$ E , "a" ne vérifie pas A"

Exemple 1.14 *La négation de la proposition logique "$\exists a \in \mathbb{C}, a^2 < 0$" est la proposition logique "$\forall a \in \mathbb{C}, a^2 \geqslant 0$".*

Exemple 1.15 *La négation de la proposition logique "$\forall a \in \mathbb{Z}_+, \sqrt{a} = 4$" est la proposition logique "$\exists a \in \mathbb{Z}_+, \sqrt{a} \neq 4$".*

5 Quelques méthodes de démonstration

5.1 Déduction ou Raisonnement direct

[4], [5], [9] Étant donnés deux assertions P_1 et P_2. On veut montrer que l'assertion "$P_1 \Rightarrow P_2$" est vraie. Si P_1 est fausse, l'assertion "$P_1 \Rightarrow P_2$" est vraie, quelle que soit la valeur de vérité de P_2. Il suffit donc d'accepter que P_1 est vraie et vérifier que P_2 est vraie.

Exemple 1.16 *Montrons que* $\forall a \in \mathbb{N}^*, \quad 16\frac{a(a+1)}{4} + 1$ *est un carré.*

Preuve. *Soit* $a \in \mathbb{N}^*$*, nous avons*

$$\begin{aligned} 16\frac{a(a+1)}{4} + 1 &= 4a^2 + 4a + 1 \\ &= (2a+1)^2 \end{aligned}$$

■

5.2 Absurde

[4], [5], [9] Pour montrer que "$P_1 \Rightarrow P_2$" est vraie, on suppose que P_1 est vraie et que P_2 est fausse pour aboutir à une contradiction, autrement dit on suppose qu'une proposition est vraie et on montre que cela conduit à une absurdité.

Exemple 1.17 *Montrons que* $\forall a \in \mathbb{N}, \quad a + 3 \neq a + 4$.

Preuve. *En écrivant la négation de la proposition, on obtient*
$\exists a \in \mathbb{N}$*, tel que* $a + 3 = a + 4$*, alors on obtient* $3 = 4$*. D'où* $\forall a \in \mathbb{N}, \quad a + 3 \neq a + 4$. ■

Exemple 1.18 *Montrer que*

$$\text{"}2a\text{" est le carré d'un entier} \Rightarrow \text{"}a\text{" n'est pas le carré d'un entier.}$$

Preuve. *Supposons que "2a" est le carré d'un entier, et que "a" est lui aussi le carré d'un entier. Dans ce cas, "2a" s'écrit sous la forme*

$$2a = a_1^2 \quad et \quad a = a_2^2.$$

Alors,

$$2 = \frac{a_1^2}{a_2^2}$$

d'où $\sqrt{2} = \pm\frac{a_1}{a_2}$*. Or* $\sqrt{2}$ *est nombre irrationnel, c'est une contradiction. On en déduit que* "$2a$" *est le carré d'un entier* $\Rightarrow$ "a" *n'est pas le carré d'un entier.* ■

5.3 Raisonnement par contraposée

[4], [5], [9] Étant données P_1 et P_2 deux propositions logiques. Les deux propositions logiques $(P_1 \Rightarrow P_2)$ et $(\neg P_2 \Rightarrow \neg P_1)$, ont la même valeur de vérité. L'utilisation du raisonnement par contraposée est utile si le passage de (non P_2) à (non P_1) est plus simple que le passage de P_1 à P_2.

Exemple 1.19 *Soient $l \in \mathbb{N}, p \in \mathbb{N}$". Montrer que si "$l^2+7=2^p$" , alors "$l$" est impair.*

Preuve. *Soit $l \in \mathbb{N}$. Supposons que l est pair, alors l^2 est pair d'où l^2+7 est impair ; or 2^p est pair. Alors, $l^2+7 \neq 2^p$. On en déduit que si l est pair, alors $l^2+7 \neq 2^p$. Par contraposée, c'est équivalent à si $l^2+7=2^p$, alors l est impair,* ■

5.4 Raisonnement par "cas par cas"

[4], [5], [9] Pour montrer que une assertion $P(x)$ est vraie pour tout les éléments x de E, il suffit de montrer qu'elle est vérifiée pour les éléments x appartenant à une partie $A \subset E$ puis pour les éléments x n'appartenant pas à A.

Exemple 1.20 *Prouver en utilisant le raisonnement par "cas par cas" que, pour tout réel a, $|a-2| \leq a^2-a+2$.*

Preuve.

On peut préciser deux cas :

1) Cas 1 : Si $a<2$, on a $|a-2|=-(a-2)$ et

$$a^2-a+2-|a-2|=a^2-a+2+a-2=a^2 \geq 0.$$

D'où $a^2-a+2 \geq |a-2|$.

1) Cas 2 : Si $a \geq 2$, on a $|a-2|=a-2$ et

$$a^2-a+2-|a-2|=a^2-2a+4=(a-1)^2+3.$$

Comme les deux termes de cette somme sont strictement positifs, alors $a^2-a+2-|a-2| \geq 0$. Ce qui donne $|a-2| \leq a^2-a+2$. ■

5.5 Raisonnement par production d'un contre exemple

[4], [5], [9] La démonstration qu'une assertion de la forme "$\forall a \in E, P(a)$" est fausse, nécessite la démonstration que sa négation "$\exists a \in E, non P(a)$" est vraie. Si on peut trouver un élément a de E qui vérifie (non P(a)) : on dit qu'on a trouvé un contre-exemple.

Exemple 1.21 *La propriété suivante est-elle vraie : "Tout nombre entier pair est un produit de deux nombres pairs ?"*

Preuve. *Les deux nombres 2 et 3 constituent un contre-exemple. Car le nombre 3 est impair et le produit $2.3=6$ est un nombre pair.* ■

5.6 Raisonnement par récurrence

[4], [5], [9] Pour démontrer une proposition logique dont l'énoncé dépend d'un entier naturel n, on utilise le raisonnement par récurrence.

Ce raisonnement peut dérouler en trois étapes suivantes :

1. On vérifie que la propriété est vraie en n_0,
2. On suppose que la propriété est vraie pour $k \geqslant n_0$, et on démontre qu'elle reste vraie pour $k+1$,
3. On conclue que la propriété est vraie pour tout entier $k \geqslant n_0$.

Exemple 1.22 *Prouver que pour tout entier* $m \geqslant 8, \quad 2^m \geqslant 7m+8$.

Preuve. *Si* $m = 8, \quad 2^8 = 256$ *et* $7m+8 = 64$. *Puisque* $64 < 256$, *l'inégalité est vraie quand* $m = 8$. *Soit* $m > 8$. *Supposons que* $\quad 2^m \geqslant 7m+8$ *et prouvons que* $\quad 2^{m+1} \geqslant 7(m+1)+8$.

$$\begin{aligned} 2^{m+1} &= 2(2^m) \\ &\geqslant 2(7m+8) \quad \textit{(par hypothèse de récurrence)} \\ &= 14m+16 \\ &= 7(m+1)+8+7m+1 \\ &\geqslant 7(m+1)+8 \end{aligned}$$

Donc, pour tout entier $m \geqslant 8, \quad 2^m \geqslant 7m+8$ ■

6 Exercices corrigés

6.1 Connecteurs logiques

Exercice 1.1 *Étudier la valeur de vérité des assertions suivantes puis donner leurs négation.*

1. $(1+2=4) \wedge (0+3=3)$.
2. $(1+2=4) \vee (0+3=3)$.
3. $(1+2=4) \Rightarrow (0+3=3)$.
4. $(0+3=3) \Rightarrow (1+2=4)$.
5. $\forall a \in \mathbb{R}, a^2 = 4$.
6. $\exists a \in \mathbb{R}, a^2 = 4$.
7. $\forall a \in \mathbb{R}, \exists b \in \mathbb{R}, a^2 = b$.
8. $\forall a \in \mathbb{R}, \exists b \in \mathbb{R}, b^2 = a$.
9. $\exists b \in \mathbb{R}, \forall a \in \mathbb{R}, a^2 = b$.

Solution.

1. $(1+2=4) \wedge (0+3=3)$ est fausse, sa négation est $(1+2 \neq 4) \vee (0+3 \neq 3)$.
2. $(1+2=4) \vee (0+3=3)$ est vraie, sa négation est $(1+2 \neq 4) \wedge (0+3 \neq 3)$.
3. $(1+2=4) \Rightarrow (0+3=3)$ est vraie, sa négation est $(1+2=4) \wedge (0+3 \neq 3)$.
4. $(0+3=3) \Rightarrow (1+2=4)$ est fausse, sa négation est $(0+3=3) \wedge (1+2 \neq 4)$.
5. $\forall a \in \mathbb{R}, a^2 = 4$ est fausse, sa négation est $\exists a \in \mathbb{R}, a^2 \neq 4$.

6. $\exists a \in \mathbb{R}, a^2 = 4$ est vraie, sa négation est $\forall a \in \mathbb{R}, a^2 \neq 4$.
7. $\forall a \in \mathbb{R}, \exists b \in \mathbb{R}, b = a^2$ est vraie, sa négation est $\exists a \in \mathbb{R}, \forall b \in \mathbb{R}, b \neq a^2$.
8. $\forall a \in \mathbb{R}, \exists b \in \mathbb{R}, a = b^2$ est fausse , sa négation est $\exists a \in \mathbb{R}, \forall b \in \mathbb{R}, a \neq b^2$.
9. $\exists b \in \mathbb{R}, \forall a \in \mathbb{R}, a^2 = b$ est vraie, sa négation est $\forall b \in \mathbb{R}, \exists a \in \mathbb{R}, a^2 \neq b$.

Exercice 1.2 *Mettre le connecteur logique qui convient :* $\Rightarrow, \Leftrightarrow$.

1. $n \in \mathbb{N}$, *n pair*.....n^2 *pair*.
2. $z \in \mathbb{C}, z' \in \mathbb{C}, (\mathrm{R}e\ z = \mathrm{R}e\ z' \quad et \quad \mathrm{I}mz = \mathrm{I}mz')$.....$z = z'$.
3. $x \in \mathbb{R}, x = \frac{\pi}{2}$..... $\cos x = 0$.

Solution.

1. $n \in \mathbb{N}$, n pair $\Rightarrow$ n^2pair.
2. $z \in \mathbb{C}, z' \in \mathbb{C}, (\mathrm{R}e\ z = \mathrm{R}e\ z' \quad \text{et} \quad \mathrm{I}mz = \mathrm{I}mz') \Leftrightarrow z = z'$.
3. $x \in \mathbb{R}, x = \frac{\pi}{2} \Rightarrow \cos x = 0$.

Exercice 1.3 *Étudier la valeur de vérité des assertions suivantes en justifiant la réponse.*

1. *Si la Turquie était en Afrique alors 6 :2=4.*
2. *Soit Newton ne connait pas les règles de la gravité de la terre, soit 4 divise 12.*
3. *Les chats ne sont ni des êtres humains, ni des animaux.*
4. *L'homme est un être humain si et seulement si les étoiles brillent durant toute la nuit.*

Solution.

1. Il s'agit ici d'une implication. "la Turquie était en Afrique" est faux et "6 :2=4" est faux, or la seule possibilité pour qu'une implication soit fausse est qu'une assertion vraie implique une assertion fausse, donc l'assertion 1. est vraie.
2. "Newton ne connait pas les règles de la gravité de la terre" est faux et " 4 divise 12" est vrai et comme en français, une phrase de genre "soit...., soit...." se traduit mathématiquement par "...ou...", donc l'assertion 2 est vraie.
3. L'assertion "Les chats ne sont ni des êtres humains, ni des animaux" se traduit "Les chats ne sont pas des êtres humains et les chats ne sont pas des animaux". "Les chats ne sont pas des êtres humains" est vrai, " les chats ne sont pas des animaux" est faux, donc l'assertion 3 est fausse.
4. "L'homme est un être humain" est vrai, "les étoiles brillent durant toute la nuit"est vrai, une équivalence entre deux assertions vraies est vraie.

Exercice 1.4 *Nier les phrases suivantes.*

1. *Si un nombre naturel est premier, alors il est un multiple de 5.*
2. *Tous les nombres réels sont positifs.*
3. *Si tu travailles régulièrement alors tu auras ton BEM.*
4. *Certains nombres entiers naturels sont divisibles par 3.*
5. *S'il fait chaud alors Amine prend sa casquette.*

Solution.

1. Un nombre naturel est premier et il n'est pas un multiple de 5.
2. Certains nombres réels sont positifs.
3. Tu travailles régulièrement et tu n'auras pas ton BEM.
4. Tous les nombres entiers naturels sont divisibles par 3.
5. Il il fait chaud et Amine ne prend pas sa casquette.

6.2 Quantificateurs

Exercice 1.5 *Donner la contraposée des phrases suivantes.*

1. *Pour tout entier naturel n, si n est inférieur strictement à onze, alors n est supérieur ou égale neuf.*
2. *Pour tout entier naturel n, si le carré de n égale* 4*, alors n égale* 2*.*
3. $\forall F_1 \subset F, \forall F_2 \subset F, (F_1 \cap F_2 = F_1 \cup F_2) \Rightarrow (F_1 = F_2)$.
4. $\forall \epsilon > 0, \exists l \in \mathbb{N}, \forall m' \in \mathbb{N}, (m \geqslant l \text{ et } m' \geqslant 0) \Rightarrow |u_{m+m'} - u_m| < \epsilon$.

Solution.

1. Pour tout entier naturel n, si n est inférieur strictement à neuf, alors n est supérieur ou égale onze.
2. Pour tout entier naturel n, si n n'égale pas 2, alors le carré de n est différent de 4.
3. $\forall F_1 \subset F, \forall F_2 \subset F, (F_1 \neq F_2) \Rightarrow (F_1 \cap F_2 \neq F_1 \cup F_2)$.
4. $\forall \epsilon > 0, \exists l \in \mathbb{N}, \forall m' \in \mathbb{N}, |u_{m+m'} - u_m| \geqslant \epsilon \Rightarrow (m < l \text{ ou } m' < 0)$.

Exercice 1.6 *Étant donnée la fonction* $g : E_1 \to E_2$*. Écrire avec des quantificateurs les propositions suivantes.*

1. *La fonction g est strictement croissante.*
2. *Le graphe de g coupe la droite d'équation* $y = x$*.*
3. *g n'est pas nulle (où* $E_1 = E_2 = \mathbb{R}$*).*
4. *g n'est pas l'identité de* $\mathbb{R}$ *(où* $E_1 = E_2 = \mathbb{R}$*).*

Solution.

1. $\forall a \in E_1, \forall b \in E_1, \text{si} \quad a < b, \text{alors} \quad g(a) < g(b)$.
2. $\exists a \in \mathbb{R}, g(a) = a$.
3. $\exists a \in \mathbb{R}, g(a) \neq 0$.
4. $\forall a \in \mathbb{R}, g(a) \neq a$.

Exercice 1.7 *Compléter avec* $\forall$ *ou* $\exists$ *pour que les énoncés suivants soient vrais.*

1. $....a \in \mathbb{N}, a^2 > 8$.
2. $....a \in \mathbb{R}, a^2 - 2a + 1 = (a-1)^2$.
3. $....a \in \mathbb{N} \quad pair, ...b \in \mathbb{N}; a = 2b$.

Solution.

1. $\exists a \in \mathbb{N}, a^2 > 8$.
2. $\forall a \in \mathbb{R}, a^2 - 2a + 1 = (a-1)^2$.
3. $\forall a \in \mathbb{N} \quad \text{pair}, \exists b \in \mathbb{N}; a = 2b$.

6.3 Quelques méthodes de démonstration

Exercice 1.8 *Étant donnés p et p' deux entiers naturels non nuls. Montrer l'implication suivante*

$$pp' = 1 \Rightarrow p = p' = 1$$

Solution. Étant donnés p et p' deux entiers naturels non nuls. En utilisant la contraposée, on suppose que $p \neq 1$ ou $p' \neq 1$. On obtient, $p \geqslant 2$ et $p' \geqslant 1$ ou bien $p \geqslant 1$ et $p' \geqslant 2$. Dans ce cas, on a $pp' \geqslant 2$, et en particulier $pp' > 1$. On en déduit que

$$pp' = 1 \Rightarrow p = p' = 1$$

Exercice 1.9 *Prouver par l'absurde que si $a \in \mathbb{Q}$ et $b \notin \mathbb{Q}$ alors $(a+b) \notin \mathbb{Q}$.*

Solution. Par un raisonnement par l'absurde. Supposons que $a+b \in \mathbb{Q}$. Dans ce cas, $(a+b)-a = b \in \mathbb{Q}$, or $b \notin \mathbb{Q}$. On obtient ainsi une contradiction, d'où $(a+b) \notin \mathbb{Q}$.

Exercice 1.10 *Prouver par récurrence que la proposition logique P(l) : $\forall l \in \mathbb{N}^*, \quad 2^l > l$ est vraie.*

Solution. On a $2^1 = 2 > 1$, donc P(1) est vraie, donc la proposition est vraie pour $l = 1$. On suppose que P(l) est vraie et on montre que P($l+1$) est vraie. On a

$$\begin{aligned} 2^{l+1} &= 2^l \times 2 \\ &> l \times 2 \\ &> l+1 \end{aligned}$$

ce qui donne P($l+1$) est vraie. Alors, on déduit que $\forall l \in \mathbb{N}^*, \quad 2^l > l$ est vraie.

Exercice 1.11 *Soit a un entier premier. Montrer que soit $a = 2$, soit a est impair.*

Solution. Il s'agit d'une implication qu'on peut la démontrer par la contraposée. Montrons que si "a" est différent de 2 et "a" est pair alors "a" n'est pas premier. Si a est pair, alors $a = 2p, p \in \mathbb{Z}$ et $a \neq 2$, alors 2 divise a, par suite a n'est pas premier.

Exercice 1.12 *Étant données deux nombres réels q et r . Montrer que si $(q+1)(r-1) = (q-1)(r+1)$ alors $q = r$.*

Solution. Par un raisonnement direct.

$$\begin{aligned} (q+1)(r-1) = (q-1)(r+1) &\Rightarrow qr - q + r - 1 = qr + q - r - 1 \\ &\Rightarrow 2r = 2q \\ &\Rightarrow q = r. \end{aligned}$$

Exercice 1.13 *Soit $l \in \mathbb{Z}$. Prouver que $\frac{l(l+1)}{2}$ est un entier."*

Solution. En utilisant un raisonnement cas par cas. Soit $l \in \mathbb{Z}$. On peut distinguer deux cas : l est pair ou l est impair.

1. Cas 1 : l est pair. Alors, $\exists m \in \mathbb{Z}$ tel que $l = 2m$,

$$\frac{l(l+1)}{2} = m(2m+1),$$

d'où $\frac{l(l+1)}{2}$ est un entier.

2. Cas 2 : l est impair. Alors, $\exists m \in \mathbb{Z}$ tel que $l = 2m+1$;

$$\frac{l(l+1)}{2} = \frac{(2m+1)(2m+2)}{2} = (2m+1)(m+1),$$

donc $\frac{l(l+1)}{2}$ est un entier.

Exercice 1.14 *Étudier la valeur de vérité de la proposition suivante "pour tout a dans* $\mathbb{R}$*,* $2a^3 - 9a^2 + 4a = (a-3)(a+2)(a+6)$"

Solution. Par un contre exemple. Mettons $M = 2a^3 - 9a^2 + 4a$ et $N = (a-3)(a+2)(a+6)$. On a pour $a = 1$, $M = -3$ et $N = (1-3)(1+2)(1+6) = -42$. On a $M \neq N$. Donc, la proposition logique "pour tout a dans $\mathbb{R}, 2a^3 - 9a^2 + 4a = (a-3)(a+2)(a+6)$" est fausse.

7 Exercices proposés

Exercice 1.15 *Évaluer les propositions logiques suivantes en justifiant la réponse puis donner leurs négations.*

1. $\exists a \in \mathbb{R}, \forall b \in \mathbb{R}, b^2 + 3 > a$.
2. 137 *est un multiple de 17 et 2 divise 167.*
3. *Le carré d'un nombre réel est positif ou tous les nombres réels sont divisibles par 3.*
4. $\exists a \in \mathbb{R}, \forall b \in \mathbb{R}, a^2 + b > 0$.
5. *Pour tout entier naturel n, si n est supérieur ou égale 4 alors n est égale 6.*

Exercice 1.16 *Écrire la négation des propositions logiques suivantes :*

1. *Dans chaque zoo, il existe un tigre dont la couleur est jaune clair.*
2. *Il existe une écolière dans le collège qui a les yeux verts.*
3. $\forall a \in \mathbb{Q}, \exists b \in \mathbb{Z}, b - 1 < a < a + 1$.
4. *Dans chaque école, il existe des élèves qui ne maitrisent pas les mathématiques.*

Exercice 1.17 *Étudier les relations logiques existant entre les phrases suivantes :*

1. *A : Tous les nombres entiers sont positifs.*
2. *B : Aucun nombre entier n'est positif.*
3. *C : Il existe des nombres entiers négatifs.*
4. *D : Tous les nombres entiers sont négatifs.*
5. *E : Aucun nombre entier n'est négatif.*
6. *F : Il existe des nombres entiers positifs.*

Exercice 1.18 *Utiliser les quantificateurs convenables pour réécrire les propositions logiques suivantes.*

1. *Tout entier relatif est positif ou négatif.*
2. *L'application* $h : \mathrm{A} \to \mathrm{B}$ *est l'identité de A.*
3. *La valeur absolue de tout entier est positif.*
4. *L'application* $h : \mathrm{A} \to \mathrm{B}$ *est constante.*

Exercice 1.19 *Peut-on renverser l'ordre des quantificateurs* $\forall a \in \mathbb{Z}$ *et* $\exists b \in \mathbb{Z}$ *dans les propositions suivantes ?*

1. $\forall a \in \mathbb{Z}, \exists b \in \mathbb{Z}, a^2 < b$.
2. $\forall a \in \mathbb{Z}, \exists b \in \mathbb{Z}, a^2 > b$.
3. $\forall a \in \mathbb{Z}, \exists b \in \mathbb{Z}, a^2 \geqslant b$.

Exercice 1.20 *Démonter les proposions logiques suivantes.*

1. $\sum_{l=1}^{l=m} l^2 = \frac{m(m+1)(2m+1)}{6}$.
2. *Si* $a \in \mathbb{Q}^*$ *et* $b \notin \mathbb{Q}^*$, *alors le produit* $(a.b) \notin \mathbb{Q}^*$.
3. *Soit* $l \in \mathbb{N}$. *Soit* l^2 *est pair, soit* $(l^2 - 1)$ *est pair.*

Chapitre 2

Ensembles et applications

1 Introduction

L'objectif de ce chapitre est de rappeler les définitions et les notations que nous faisons dans l'utilisation pratique de la théorie des ensembles et la théorie des applications. Ce chapitre est basé sur les références([1], [2],[3],[4], [5], [7],[8], [9], [12]).

2 Ensembles

Définition 2.1 *[1], [3], [4], [5] Tout regroupement d'objets qui présentent mêmes propriétés est appelée ensemble.*

2.1 Notations

On note les ensembles par les lettres A, B , C ,..., les familles d'ensembles par les lettres $\mathscr{A}$, $\mathscr{B}$, $\mathfrak{C}$,... et les éléments d'un ensemble sont notés par les lettres minuscules $a, b, c, \alpha, \beta, ...$

L'ensemble des entiers naturels est noté par $\mathbb{N}$.

L'ensemble des entiers relatifs est noté par $\mathbb{Z}$.

L'ensemble des nombres rationnels est noté par $\mathbb{Q}$.

L'ensemble des nombres réels est noté par $\mathbb{R}$.

L'ensemble des nombres complexes est noté par $\mathbb{C}$.

On convient de noter $\mathbb{N}^*, \mathbb{Z}^*, \mathbb{Q}^*$, $\mathbb{R}^*$ et $\mathbb{C}^*$ les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ privés de l'élément 0.

2.2 Appartenance

Définition 2.2 *[1], [3], [4], [5] Étant donné un ensemble E non vide. On dit que x appartient à* E *et on note* $x \in$ E *si x est l'un des éléments de l'ensemble* E*, et si x n'est pas un élément de* E *on écrit* $x \notin$ E *et on dit que l'élément x n'appartient pas à l'ensemble* E.

2.3 Ensemble vide

Définition 2.3 *L'ensemble qui ne contient aucun élément est appelé l'ensemble vide. On le note* $\emptyset$.

2.4 Cardinal d'un ensemble

Définition 2.4 *[1], [3] Le nombre d'éléments d'un ensemble H, noté card(H), est appelé cardinal de H, .*

Si card(H) est fini, on dit que H est un ensemble fini, et dans le cas contraire, on dit que H est un ensemble infini.

Exemple 2.1 *Soit* $A = \{x \in \mathbb{N} : 6 \leq x \leq 10\}$ *et* $B = \{x \in \mathbb{R} : 6 \leq x \leq 10\}$ *alors,* $card(A) = 5$ *et* $card(B) = \infty$.

2.5 Inclusion

Définition 2.5 *([1], [3] Soient* A_1 *et* A_2 *deux ensembles. Si chaque élément de* A_1 *est élément de* A_2*, on dit que* A_1 *est une partie de* A_2 *(ou bien l'ensemble* A_1 *est inclus dans l'ensemble* A_2 *ou* A_1 *est un sous ensemble de* A_2 *) et on note* $A_1 \subset A_2$ *et on a*

$$A_1 \subset A_2 \Leftrightarrow \forall x (x \in A_1 \Rightarrow x \in A_2).$$

Exemple 2.2 *On reprend l'exemple précédent, on a* $A = \{x \in \mathbb{N} : 6 \leq x \leq 10\}$ *est un sous ensemble de* $B = \{x \in \mathbb{R} : 6 \leq x \leq 10\}$.

Définition 2.6 *([1], [3] Soient* A_1 *et* A_2 *deux ensembles. On dit que* A_1 *et* A_2 *sont égaux s'ils ont les mêmes éléments et on note* $A_1 = A_2$ *et on a*

$$A_1 = A_2 \Leftrightarrow \forall x (x \in A_1 \Leftrightarrow x \in A_2) \Leftrightarrow ((A_1 \subset A_2) \wedge (A_2 \subset A_1)).$$

Exemple 2.3 *Soient* $A_1 = \{a, b, 1, 8, \square\}$ *et* $A_2 = \{8, b, \square, 1, a, \}$ *alors l'ensemble* A_1 *est égal à l'ensemble* A_2.

2.6 Ensemble des parties d'un ensemble

Définition 2.7 *[1], [3] Soit H un ensemble. L'ensemble de sous ensembles de H est noté* $\mathscr{P}(H)$.

Exemple 2.4 *Soit* $H = \{a_1, a_2, a_3\}$*, alors l'ensemble des parties de H est*

$$\mathscr{P}(H) = \{\emptyset, \{a_1, a_2, a_3\}, \{a_1\}, \{a_2\}, \{a_3\}, \{a_1, a_2\}, \{a_2, a_3\}, \{a_1, a_3\}\}.$$

Et

$$card(\mathscr{P}(H)) = 2^3 = 8.$$

2.7 Propriétés sur les ensembles

Soient A_1 et A_2 deux parties de l'ensemble A.

Réunion

Définition 2.8 *[1], [3] L'ensemble noté* $A_1 \cup A_2$ *est appelé la réunion des deux ensembles* A_1 *et* A_2*, c'est l'ensemble qui contient des éléments qui appartiennent à* A_1 *ou à* A_2*. L'équivalence suivante résume la définition*

$$(x \in A_1 \cup A_2) \Leftrightarrow ((x \in A_1) \vee (x \in A_2)).$$

Intersection

Définition 2.9 *[1], [3] L'ensemble noté* $A_1 \cap A_2$ *est appelé l'intersection des deux ensembles* A_1 *et* A_2*, c'est l'ensemble qui contient des éléments qui appartiennent à* A_1 *et à* A_2*. L'équivalence suivante traduit la définition*

$$(x \in A_1 \cap A_2) \Leftrightarrow ((x \in A_1) \wedge (x \in A_2)).$$

Exemple 2.5 *Soient* $A_1 = \{1,2,5,6\}$ *et* $A_2 = \{2,4\}$ *alors l'ensemble* $A_1 \cap A_2 = \{2\}$ *et* $A_1 \cup A_2 = \{1,2,4,5,6\}$.

Propriétés

[1], [3] Soient A_1, A_2 et A_3 des parties de l'ensemble A. Alors, on a

1. $A_1 \cap A_2 = A_2 \cap A_1$.
2. $A_1 \cap \emptyset = \emptyset$.
3. $(A_1 \cap A_2) \cap A_3 = A_1 \cap (A_2 \cap A_3)$.
4. $A_1 \subset A_2 \Leftrightarrow A_1 = A_1 \cap A_2$.
5. $A_1 \cap A = A_1$.
6. $A_1 \cup A_2 = A_2 \cup A_1$.
7. $A_1 \cup \emptyset = A_1$.
8. $(A_1 \cup A_2) \cup A_3 = A_1 \cup (A_2 \cup A_3)$.
9. $A_1 \subset A_2 \Leftrightarrow A_1 \cup A_2 = A_2$.
10. $A_1 \cup A = A$.
11. $(A_1 \cap A_2) \subset A_1$ et $(A_1 \cap A_2) \subset A_2$.
12. $A_1 \subset (A_1 \cup A_2)$ et $A_2 \subset (A_1 \cup A_2)$.
13. $A_1 \cap (A_2 \cup A_3) = (A_1 \cap A_2) \cup (A_1 \cap A_3)$.
14. $A_1 \cup (A_2 \cap A_3) = (A_1 \cup A_2) \cap (A_1 \cup A_3)$.

Preuve.

- Pour 1,2,3, 6, 7 et 8 il suffit d'utiliser les propriétés de la conjonction et la disjonction.
- Pour 4 : Supposons que $A_1 \subset A_2$. Soit "a" un élément de A_1, alors "a" appartient à A_2, donc "a" appartient à $A_1 \cap A_2$. D'où $A_1 \subset A_1 \cap A_2$ et réciproquement si "a" appartient à $A_1 \cap A_2$, donc "a" appartient à A_1 . D'où $A_1 = A_1 \cap A_2$. Inversement, $A_1 = A_1 \cap A_2$ implique que tout "a" appartenant à A_1 appartient à A_2, d'où $A_1 \subset A_2$.
- En prenant $A_2 = A$ dans 4, on obtient 5.
- Pour 9 : Supposons que $A_1 \subset A_2$ et montrons que $A_1 \cup A_2 = A_2$. Soit "a" appartenant à A_2, alors "a" appartient à A_1 ou à A_2, donc "a" appartient à $A_1 \cup A_2$ et réciproquement si "a" appartient à $A_1 \cup A_2$, donc "a" appartient à A_1 ou à A_2 . D'où $A_2 = A_1 \cup A_2$. Inversement, supposons que $A_2 = A_1 \cup A_2$ et montrons que $A_1 \subset A_2$. Si "a" appartient à A_1, alors "a" appartient à $A_1 \cup A_2$ et donc à A_2, d'où $A_1 \subset A_2$.

- 10 découle de 9 avec $A_2 = A$.
- Montrons 13. Soit $a \in A_1 \cap (A_2 \cup A_3)$

$$\begin{aligned} a \in A_1 \cap (A_2 \cup A_3) &\Rightarrow (a \in A_1) \wedge a \in (A_2 \cup A_3) \\ &\Rightarrow (a \in A_1) \wedge (a \in A_2 \vee a \in A_3) \\ &\Rightarrow (a \in A_1 \wedge a \in A_2) \vee (a \in A_1 \wedge a \in A_3) \\ &\Rightarrow a \in ((A_1 \cap A_2) \cup (A_1 \cap A_3)). \end{aligned}$$

Donc

$$A_1 \cap (A_2 \cup A_3) \subset ((A_1 \cap A_2) \cup (A_1 \cap A_3)).$$

Inversement, soit $a \in ((A_1 \cap A_2) \cup (A_1 \cap A_3))$.

$$\begin{aligned} a \in ((A_1 \cap A_2) \cup (A_1 \cap A_3)) &\Rightarrow (a \in A_1 \cap A_2) \vee (a \in A_1 \cap A_3) \\ &\Rightarrow (a \in A_1 \wedge a \in A_2) \vee (a \in A_1 \wedge a \in A_3) \\ &\Rightarrow (a \in A_1 \vee a \in A_1) \wedge (a \in A_1 \vee a \in A_3) \\ &\wedge \quad (a \in A_2 \vee a \in A_1) \wedge (a \in A_2 \vee a \in A_3) \\ &\Rightarrow (a \in A_1) \wedge (a \in A_1 \cup A_3) \wedge (a \in A_2 \cup A_1) \wedge (a \in A_2 \cup A_3) \\ &\Rightarrow (a \in A_1) \wedge (a \in A_2 \cup A_3) \\ &\Rightarrow a \in (A_1 \cap (A_2 \cup A_3)). \end{aligned}$$

Donc

$$((A_1 \cap A_2) \cup (A_1 \cap A_3)) \subset A_1 \cap (A_2 \cup A_3).$$

D'où l'égalité

$$((A_1 \cap A_2) \cup (A_1 \cap A_3)) = A_1 \cap (A_2 \cup A_3).$$

- Montrons 14. Soit $a \in A_1 \cup (A_2 \cap A_3)$

$$\begin{aligned} a \in A_1 \cup (A_2 \cap A_3) &\Rightarrow (a \in A_1) \vee a \in (A_2 \cap A_3) \\ &\Rightarrow (a \in A_1) \vee (a \in A_2 \wedge a \in A_3) \end{aligned}$$

Si $a \in A_1$, alors $(a \in A_1 \cup A_2)$ et $(a \in A_1 \cup A_3)$. Donc, $a \in ((A_1 \cup A_2) \cap (A_1 \cup A_3))$.
Si $(a \in A_2 \wedge a \in A_3)$ alors, $(a \in A_1 \cup A_2)$ et $(a \in A_1 \cup A_3)$. Donc

$$A_1 \cup (A_2 \cap A_3) \subset ((A_1 \cup A_2) \cap (A_1 \cup A_3)).$$

Inversement, soit $a \in ((A_1 \cup A_2) \cap (A_1 \cup A_3))$.

$$\begin{aligned} a \in ((A_1 \cup A_2) \cap (A_1 \cup A_3)) &\Rightarrow (a \in (A_1 \cup A_2) \wedge a \in (A_1 \cup A_3) \\ &\Rightarrow (a \in A_1 \vee a \in A_2) \wedge (a \in A_1 \vee a \in A_3) \\ &\Rightarrow (a \in A_1 \wedge a \in A_1) \vee (a \in A_1 \wedge a \in A_3) \vee (a \in A_2 \wedge a \in A_1) \\ &\vee \quad (a \in A_2 \wedge a \in A_3) \\ &\Rightarrow (a \in A_1) \vee (a \in A_1 \cap A_3) \vee (a \in A_2 \cap A_1) \vee (a \in A_2 \cap A_3) \\ &\Rightarrow (a \in A_1) \vee (a \in A_2 \cap A_3) \\ &\Rightarrow a \in (A_1 \cup (A_2 \cap A_3)). \end{aligned}$$

Donc

$$((A_1 \cup A_2) \cap (A_1 \cup A_3) \subset (A_1 \cup (A_2 \cap A_3)).$$

Finalement ; $((A_1 \cup A_2) \cap (A_1 \cup A_3)) = (A_1 \cup (A_2 \cap A_3))$.

■

Complémentaire

Définition 2.10 *[7], [9] Soit* A_1 *une partie d'un ensemble A. L'ensemble des éléments de A qui n'appartiennent pas à* A_1 *est appelé complémentaire de* A_1 *dans A noté par* $C_A^{A_1}$ *ou* ${A_1}^c$. *On a*

$$C_A^{A_1} = \{x \in A, x \notin A_1\}.$$

Exemple 2.6 *Soient* $A = \{1,2,4,5,6\}$ *et* $A_1 = \{2,4\}$ *alors* $C_A^{A_1} = \{1,5,6\}$.

Propriétés

[7], [9] Étant donnés A_1 et A_2 des parties de l'ensemble A. Alors, on a

1. $C_A^{C_A^{A_1}} = A_1$.
2. $C_A^{A_1 \cap A_2} = C_A^{A_1} \cup C_A^{A_2}$.
3. $C_A^{A_1 \cup A_2} = C_A^{A_1} \cap C_A^{A_2}$.
4. $A_1 \subset A_2 \Leftrightarrow C_A^{A_2} \subset C_A^{A_1}$.

Preuve.

- Soit $a \in A$, alors

$$\begin{aligned} a \in C_A^{C_A^{A_1}} &\Leftrightarrow \overline{a \notin C_A^{A_1}} \\ &\Leftrightarrow \overline{\overline{a \in C_A^{A_1}}} \\ &\Leftrightarrow \overline{\overline{a \notin A_1}} \\ &\Leftrightarrow a \in A_1. \end{aligned}$$

- Soit $a \in A$, alors

$$\begin{aligned} a \in C_A^{(A_1 \cap A_2)} &\Leftrightarrow a \notin (A_1 \cap A_2) \\ &\Leftrightarrow (a \notin A_1) \vee (a \notin A_2) \\ &\Leftrightarrow (a \in C_A^{A_1}) \vee (a \in C_A^{A_2})) \\ &\Leftrightarrow a \in (C_A^{A_1} \cup C_A^{A_2}). \end{aligned}$$

- Soit $a \in A$, alors

$$\begin{aligned} x \in C_A^{A_1 \cup A_2} &\Leftrightarrow x \notin (A_1 \cup A_2) \\ &\Leftrightarrow (a \notin A_1) \wedge (a \notin A_2) \\ &\Leftrightarrow (a \in C_A^{A_1} \wedge (a \in C_A^{A_2})) \\ &\Leftrightarrow a \in (C_A^{A_1} \cap C_A^{A_2}). \end{aligned}$$

- Soit $a \in A$, alors

$$\begin{aligned} A_1 \subset A_2 &\Leftrightarrow \forall a \in A (a \in A_1) \Rightarrow (a \in A_2) \\ &\Leftrightarrow \forall a \in A (a \notin A_2) \Rightarrow (a \notin A_1) \quad \text{Contraposée de l'implication} \\ &\Leftrightarrow (a \in C_A^{A_2})) \Rightarrow (a \in C_A^{A_1})) \\ &\Leftrightarrow (C_A^{A_2}) \subset C_A^{A_1})). \end{aligned}$$

■

Définition 2.11 *[5], [7], [9] Soient* A_1 *et* A_2 *deux parties d'un ensemble A. On dit que* A_1 *et* A_2 *sont complémentaires si leur réunion est l'ensemble A et leur intersection est l'ensemble vide, autrement dit*

$$A_1 \cap A_2 = \emptyset \text{ et } A_1 \cup A_2 = A.$$

Dans ce cas, on note $A_2 = C_A^{A_1}$ *ou bien* $A_2 = A_1^c$ *ou encore* $A_2 = \overline{A_1}$.

Différence des ensembles

Définition 2.12 *[1], [7] Soient* A_1 *et* A_2 *deux parties d'un ensemble A. On appelle la différence des ensembles* A_1 *et* A_2 *l'ensemble des éléments de* A_1 *qui n'appartiennent pas à* A_2 *noté par* $A_1 \setminus A_2$. *On a*

$$A_1 \setminus A_2 = \{a \in A, a \in A_1 \text{ et } a \notin A_2\}.$$

Exemple 2.7 *Soient* $A = \{1,2,4,5,6\}$ *et* $A_1 = \{1,2,4\}, A_2 = \{2,4,5\}$ *alors* $C_A^{A_2} = \{1,6\}$. *Donc,*

$$A_1 \setminus A_2 = \{1\}.$$

Produit Cartésien

Définition 2.13 *[4], [5], [7], [9] Étant donnés* A_1 *et* A_2 *deux parties d'un ensemble A. On appelle produit cartésien des ensembles* A_1 *et* A_2, *l'ensemble noté* $A_1 \times A_2$, *des couples* (a_1, a_2) *avec* $a_1 \in A_1$ *et* $a_2 \in A_2$.
Et le produit cartésien de n ensembles A_i *est*

$$A_1 \times A_2 \times ... \times A_n = \{(a_1, a_2, ..., a_n); a_1 \in A_1, ..., a_n \in A_n\}.$$

Si $A_1 = A_2 = ... = A_n$, *on le note* A^n.

Remarque 2.1 *Le couple* (a_2, a_1) *est différent du couple* (a_1, a_2), *sauf si* $a_1 = a_2$.

Exemple 2.8 *Soient* $A_1 = \{a_1, a_2, a_3\}$ *et* $A_2 = \{2,4,6\}$, *alors*

$$A_1 \times A_2 = \{(a_1,2),(a_1,4),(a_1,6),(a_2,2),(a_2,4),(a_2,6),(a_3,2),(a_3,4),(a_3,6)\}.$$

Et

$$card(A_1 \times A_2) = 3 \times 3 = 9.$$

Proposition 2.1 *[1] Étant donnés* A_1 *et* A_2 *deux ensembles finis non vides. On a*

$$card(A_1 \times A_2) = card(A_1) \times card(A_2).$$

Preuve. Soient $card(A_1) = n$ et $card(A_2) = m$. On obtient le nombre des couples (a_1, a_2) avec $a_1 \in A_1$ et $a_2 \in A_2$ en correspondant à tout élément $a_1 \in A_1$ tout les éléments de A_2, c'est à dire m éléments, en répétant cette technique autant de fois qu'il y a d'éléments dans A_1 c'est à dire n fois. Le nombre des éléments de $A_1 \times A_2$ est $card(A_1) \times card(A_2)$. ■

Notion de Partition et de Recouvrement

Définition 2.14 *[1], [5] Soit A un ensemble. On appelle recouvrement de A, toute famille* $(A_i)_{i\in I}$ *de parties de A, indexés par l'ensemble I, vérifiant* $\cup_{i\in I}A_i = A$ *c'est à dire*

$$\forall a \in A, \exists A_i \quad tel\ que \quad a \in A_i.$$

Si de plus,

$$\begin{cases} \forall i \in I & A_i \neq \emptyset \\ A_i \cap A_j = \emptyset & i \neq j \end{cases}$$

on dit que la famille $(A_i)_{i\in I}$ *forme une partition de A.*

Remarque 2.2 *Soit A en ensemble, alors pour toute partie* A_1 *de A,* $F = \{A_1, C_A^{A_1}\}$ *est une partition de A.*

Exemple 2.9 *Soit* $A = \{1, a, l, 3, b, c, d, \alpha, \beta, \gamma\}$ *alors*

$$H = \{\{a, \gamma\}, \{d, \alpha, \beta\}, \{c, 1\}, \{l, 3\}, \{b\}\}$$

est une partition de l'ensemble A.

3 Applications

3.1 Relations, Fonction, Application

Soient A_1 et A_2 deux ensembles non vides et $\Gamma \subset A_1 \times A_2$.

Définition 2.15 *[1], [5], [7] Tout triplet* (A_1, Γ, A_2) *est appelé une relation de* A_1 *vers* A_2*, notée* $\mathcal{R}$ *. L'ensemble de départ de* $\mathcal{R}$ *est* A_1*, l'ensemble d'arrivée de* $\mathcal{R}$ *est* A_2 *et* Γ *est le graphe de* $\mathcal{R}$*.*
On dit que a_1 *est en relation avec* a_2 *par la relation* $\mathcal{R}$ *et on note* $a_1 \mathcal{R} a_2$ *si* $(a_1, a_2) \in \Gamma$*, dans ce cas* a_1 *est appelé l'antécédent de* a_2 *et* a_2 *est l'image de* a_1 *par* $\mathcal{R}$*.*

Exemple 2.10 *Soit* $A_1 = \{\alpha, \beta, \gamma, \delta\}$, $A_2 = \{a_1, a_2, a_3, a_4\}$ *et* $\Gamma = \{(\alpha, a_1), (\alpha, a_2), (\beta, a_3), (\gamma, a_2), (\gamma, a_3), (\gamma, a_4)\}$.
On a (A_1, Γ, A_2) *est une relation de* A_1 *vers* A_2 *tel que* $\alpha \mathcal{R} a_1, \alpha \mathcal{R} a_2, \beta \mathcal{R} a_3, \gamma \mathcal{R} a_2, \gamma \mathcal{R} a_3, \gamma \mathcal{R} a_4$ *et* δ *n'est en relation avec aucun élément de* A_2*.*

Définition 2.16 *[1], [5] On appelle une fonction de* A_1 *vers* A_2 *toute relation f entre les éléments de* A_1 *et ceux de* A_2 *de graphe* Γ *qui à tout élément de* A_1 *fait correspondre au plus un élément de* A_2*.*
On représente la fonction f par

$$\begin{array}{rccc} f: & A_1 & \longrightarrow & A_2 \\ & x & \longmapsto & y = f(x) \end{array}$$

Exemple 2.11 *On reprend l'exemple précédent avec* $A_1 = \{\alpha, \beta, \gamma, \delta\}$, $A_2 = \{a_1, a_2, a_3, a_4\}$ *et* $\Gamma = \{(\alpha, a_1), (\alpha, a_2), (\beta, a_3), (\gamma, a_2), (\gamma, a_3), (\gamma, a_4)\}$*. On a* $f(\alpha) = a_1$, $f(\alpha) = a_2$, $f(\beta) = a_3$, $f(\gamma) = a_2$, $f(\gamma) = a_3$, $f(\gamma) = a_4$*. On remarque que f n'est pas une fonction de* A_1 *vers* A_2*.*

Exemple 2.12 *Soit* $f=(\mathbb{R},\Gamma,\mathbb{R})$ *avec* $\Gamma=\{(a,b)\in\mathbb{R}^2/\,b=\ln a\}$, *alors* f *est une fonction notée*

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & a & \longmapsto & b=\ln a. \end{array}$$

Les réels négatifs n'ont pas d'images.

Définition 2.17 *[1], [4], [5] Soient* A_1 *et* A_2 *deux ensembles non vides et* f *une fonction de* A_1 *dans* A_2. *L'ensemble noté* D_f *est appelé domaine de définition de* f *; c'est l'ensemble des éléments de* A_1 *ayant une image par* f *et on écrit*

$$D_f=\{a\in A_1/\exists b\in A_2: b=f(a)\}$$

Exemple 2.13 *Le domaine de définition de la fonction*

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & b=\ln a. \end{array}$$

est $D_f=]0,+\infty[$.

Définition 2.18 *[1], [4], [5] Soient* A_1 *et* A_2 *deux ensembles non vides. On appelle une application* $f: A_1\longrightarrow A_2$ *toute relation* f *qui à tout élément* $a\in A_1$ *fait correspondre un élément unique* $b\in A_2$.

L'ensemble $\{b=f(a), a\in A_1\}$ *s'appelle l'image de* f *qu'on note* $\quad Imf$.

L'ensemble des applications d'un ensemble A_1 *dans un ensemble* A_2 *se note* $\mathscr{F}(A_1,A_2)$ *ou encore* ${A_2}^{A_1}$.

Exemple 2.14

$$\begin{array}{rccc} f: & \mathbb{R}_+^* & \longrightarrow & \mathbb{R} \\ & a & \longmapsto & b=\ln a. \end{array}$$

est une application.

Exemple 2.15 *Soient* $A_1=\{\alpha,\beta,\gamma,\delta\}$, $A_2=\{a_1,a_2,a_3,a_4\}$ *et* $\Gamma=\{(\alpha,a_1),(\alpha,a_2),(\beta,a_3),(\gamma,a_2),(\gamma,a_3),(\gamma,a_4)\}$. *On a* $f(\alpha)=a_1$, $f(\alpha)=a_2$, $f(\beta)=a_3$, $f(\gamma)=a_2$, $f(\gamma)=a_3$, $f(\gamma)=a_4$. *On remarque que* f *n'est pas une application de* A_1 *dans* A_2 *car* α *a deux images dans* A_2 *et* γ *a trois images dans* A_2.

Exemple 2.16 *Soient* $A_1=\{\alpha,\beta,\gamma,\delta\}$, $A_2=\{a_1,a_2,a_3,a_4,a_5,a_6\}$ *et* $\Gamma=\{(\alpha,a_1),(\beta,a_1),(\gamma,a_2),(\delta,a_3)\}$. *Cette correspondance est une application malgré qu'il existe des éléments de* A_2 *qui n'ont pas d'antécédent dans* A_1 *et plusieurs éléments de* A_1 *qui ont une même image dans* A_2.

Égalité des Applications

Définition 2.19 *[9] Étant données deux applications* $f: E_1\longrightarrow F_1$ *et* $g: E_2\longrightarrow F_2$ *sont égales si*

1. $E_1=E_2=E$ *et* $F_1=F_2$,
2. $\forall a\in E, f(a)=g(a)$.

Exemple 2.17 *On considère les applications suivantes*

$$\begin{array}{rcl} f_1 : \mathbb{R} & \longrightarrow & \mathbb{R} \\ a & \longmapsto & a^2. \end{array}$$

$$\begin{array}{rcl} f_2 : \mathbb{R} & \longrightarrow & \mathbb{R}_+ \\ a & \longmapsto & a^2. \end{array}$$

$$\begin{array}{rcl} f_3 : \mathbb{R}_+ & \longrightarrow & \mathbb{R} \\ a & \longmapsto & a^2. \end{array}$$

$$\begin{array}{rcl} f_4 : \mathbb{R}_+ & \longrightarrow & \mathbb{R}_+ \\ a & \longmapsto & a^2. \end{array}$$

Alors,
$f_1 \neq f_2$, *car les ensembles d'arrivées sont différents*
$f_1 \neq f_3$, *car les ensembles de départ sont différents.*
$f_1 \neq f_4$, *car les ensembles d'arrivées sont différents et les ensembles de départ sont différents.*

Application Identité

Définition 2.20 *[4], [5], [9] Soit* A *un ensemble non vide. L'application Identité dans* A, *notée* Id_A *est l'application de A dans A qui à* $a \in \mathrm{A}$ *associe a.*

Applications Composées

Définition 2.21 *[4], [5], [9] Soient* $\mathrm{A}_1, \mathrm{A}_2$ *et* A_3 *des ensembles non vides. Soient* $f_1 \in \mathscr{F}(\mathrm{A}_1, \mathrm{A}_2)$ *et* $f_2 \in \mathscr{F}(\mathrm{A}_2, \mathrm{A}_3)$. *On appelle composée des applications* f_1 *et* f_2, *notée* $f_2 o f_1$, *l'application définie sur* A_1 *et à valeur dans* A_3 *et qui fait correspondre à tout a de E l'élément* $b = f_2(f_1(a))$.

Exemple 2.18 *On considère les applications suivantes*

$$\begin{array}{rcl} f_1 : \mathbb{R} & \longrightarrow & \mathbb{R}_+ \\ a & \longmapsto & a^2. \end{array}$$

$$\begin{array}{rcl} f_2 : \mathbb{R}_+ & \longrightarrow & \mathbb{R}_+ \\ a & \longmapsto & a^3 + 1. \end{array}$$

Alors,

$$\begin{array}{rcl} f_2 o f_1 : \mathbb{R} & \longrightarrow & \mathbb{R}_+ \\ a & \longmapsto & (a^2)^3 + 1 = a^6 + 1. \end{array}$$

$$\begin{array}{rcl} f_1 o f_2 : \mathbb{R}_+ & \longrightarrow & \mathbb{R}_+ \\ a & \longmapsto & (a^3 + 1)^2 = a^6 + 2a^3 + 1. \end{array}$$

Il est clair que $f_2 o f_1 \neq f_1 o f_2$.

Proposition 2.2 *[9] Soient* $\mathrm{A}_1, \mathrm{A}_2, \mathrm{A}_3$ *et* A_4 *des ensembles non vides. Soient* $f_1 \in \mathscr{F}(\mathrm{A}_1, \mathrm{A}_2)$, $f_2 \in \mathscr{F}(\mathrm{A}_2, \mathrm{A}_3)$ *et* $f_3 \in \mathscr{F}(\mathrm{A}_3, \mathrm{A}_4)$. *On a*

$$f_1 o (f_2 o f_3) = (f_1 o f_2) o f_3.$$

Preuve. L'ensemble de départ et l'ensemble d'arrivé des applications $f_1 o(f_2 o f_3)$ et $(f_1 o f_2) o f_3$ sont les mêmes et pour tout $a \in A_1$, on a

$$f_1 o(f_2 o f_3)(a) = f_1((f_2 o f_3)(a)) = f_1(f_2(f_3(a)))$$

et

$$(f_1 o(f_2 o f_3))(a) = (f_1 o f_2)(f_3(a)) = f_1(f_2(f_3(a)))$$

ce qui prouve le résultat. ■

Image directe et Image réciproque

Définition 2.22 *[4], [5], [9] Soient* A *et* B *deux ensembles non vides et* $A_1 \subset A$ *et* $B_1 \subset B$. *Soit* $f \in \mathscr{F}(A, B)$.

1) L'ensemble des images des éléments de A_1 *noté*

$$f(A_1) = \{f(a), a \in A_1\} \subset B$$

est appelé image directe de A_1 *par* f.
2) L'ensemble des antécédents des éléments de B noté

$$f^{-1}(B_1) = \{a \in A, f(a) \in B_1\} \subset A$$

est appelé image réciproque de B_1 *par* f.

Exemple 2.19 *On considère l'application suivante.*

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & a & \longmapsto & a^2 + a. \end{array}$$

Cherchons $f(\{1\}), f(]0,2[), f^{-1}(\{0\}), f^{-1}(]0,+\infty[)$.

$$\begin{array}{rcl} f(\{1\}) = & = & \{a^2 + a, a \in \{1\}\} \\ & = & \{2\}. \end{array}$$

Alors,

$$\begin{array}{rcl} f(]0,2[) = & = & \{a^2 + a, a \in]0,2[\} \\ & = &]0,6[. \end{array}$$

$$\begin{array}{rcl} f^{-1}(\{0\}) & = & \{a \in \mathbb{R}, f(a) \in \{0\}\} \\ & = & \{a \in \mathbb{R}, a^2 + a = 0\} \\ & = & \{-1, 0\}. \end{array}$$

$$\begin{array}{rcl} f^{-1}(]0,+\infty[) & = & \{a \in \mathbb{R}, f(a) \in]0,+\infty[\} \\ & = & \{a \in \mathbb{R}, a^2 + a > 0\} \\ & = &]-\infty,-1[\cup]0,+\infty[. \end{array}$$

Proposition 2.3 *[4], [5], [9] Étant donnés* A *et* B *des ensembles non vides,* A_1, A_2 *deux parties de* A *et* B_1, B_2 *deux parties de* B. *Soient* $f \in \mathscr{F}(A, B)$. *On a*

1. $A_1 \subset A_2 \Rightarrow f(A_1) \subset f(A_2)$.
2. $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

3. $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$.
4. $f^{-1}(B) = A$.
5. $B_1 \subset B_2 \Rightarrow f^{-1}(B_1) \subset f^{-1}(B_2)$.
6. $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.
7. $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

Preuve.

1. Soit $A_1 \subset A_2$ et soit $b \in f(A_1)$.

$$\begin{aligned} b \in f(A_1) &\Rightarrow \exists a \in A_1 \subset A_2 : b = f(a) \\ &\Rightarrow \exists a \in A_2 : b = f(a) \\ &\Rightarrow b \in f(A_2). \end{aligned}$$

   D'où $f(A_1) \subset f(A_2)$.

2. Soit $b \in f(A_1 \cup A_2)$.

$$\begin{aligned} b \in f(A_1 \cup A_2) &\Leftrightarrow \exists a \in A_1 \cup A_2 : b = f(a) \\ &\Leftrightarrow \exists a[((a \in A_1) \vee (a \in A_2)) \wedge (b = f(a))] \\ &\Leftrightarrow \exists a[((a \in A_1) \wedge (b = f(a))] \vee [((a \in A_2) \wedge (b = f(a))] \\ &\Leftrightarrow (b \in f(A_1)) \vee (b \in f(A_2)) \\ &\Leftrightarrow b \in (f(A_1) \cup f(A_2)) \end{aligned}$$

   D'où $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

3. Soit $b \in f(A_1 \cap A_2)$.

$$\begin{aligned} b \in f(A_1 \cap A_2) &\Leftrightarrow \exists a \in A_1 \cap A_2 : b = f(a) \\ &\Leftrightarrow \exists a[(a \in A_1) \wedge (a \in A_2) \wedge (b = f(a))] \\ &\Leftrightarrow \exists a[((a \in A_1) \wedge (b = f(a))] \wedge [((a \in A_2) \wedge (b = f(a))] \\ &\Rightarrow (\exists a \in A_1 \wedge b = f(a)) \wedge (\exists a \in A_2 \wedge b = f(a)) \\ &\Rightarrow (b \in f(A_1)) \wedge (b \in f(A_2)) \\ &\Rightarrow b \in (f(A_1) \cap f(A_2)) \end{aligned}$$

   D'où $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$.

4. $f^{-1}(B) = \{a \in A, f(a) \in B\} = A$

5. Soit $B_1 \subset B_2$ et soit $a \in f^{-1}(B_1)$.

$$\begin{aligned} a \in f^{-1}(B_1) &\Rightarrow a \in A, f(a) \in B_1 \subset B_2 \\ &\Rightarrow a \in A, f(a) \in B_2 \\ &\Rightarrow a \in f^{-1}(B_2). \end{aligned}$$

   D'où $f^{-1}(B_1) \subset f^{-1}(B_2)$.

6. Soit $a \in f^{-1}(B_1 \cup B_2)$.

$$\begin{aligned} a \in f^{-1}(B_1 \cup B_2) &\Leftrightarrow f(a) \in B_1 \cup B_2 \\ &\Leftrightarrow (f(a) \in B_1) \vee (f(a) \in B_2) \\ &\Leftrightarrow [a \in f^{-1}(B_1)] \vee [a \in f^{-1}(B_2)] \\ &\Leftrightarrow a \in (f^{-1}(B_1) \cup f^{-1}(B_2)) \end{aligned}$$

D'où $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.

7. Soit $a \in f^{-1}(B_1 \cap B_2)$.

$$\begin{aligned} a \in f^{-1}(B_1 \cap B_2) &\Leftrightarrow f(a) \in B_1 \cap B_2 \\ &\Leftrightarrow (f(a) \in B_1) \wedge (f(a) \in B_2) \\ &\Leftrightarrow [a \in f^{-1}(B_1)] \wedge [a \in f^{-1}(B_2)] \\ &\Leftrightarrow a \in (f^{-1}(B_1) \cap f^{-1}(B_2)) \end{aligned}$$

ce qui montre que $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

■

Applications injectives, surjectives, bijectives

Étant donnés A et B deux ensembles non vides et f une application de A dans B.

Définition 2.23 *[4], [5], [9] f est dite injective (ou une injection) si tout élément de B admet au plus un antécédent dans A, ce qui est équivalent à dire qu'un élément de B ne peut pas être une image de deux antécédents différents de A. Ce qui revient à écrire*

$$f \text{ est injective} \Leftrightarrow \forall a \in A, a' \in A \quad ((f(a) = f(a') \Rightarrow a = a')$$

ou bien

$$f \text{ est injective} \Leftrightarrow \forall a \in A,\ a' \in A \quad (a \neq a' \Rightarrow f(a) \neq f(a')).$$

Par négation,

$$f \text{ n'est pas injective} \Leftrightarrow \exists a \in A,\ a' \in A \quad (a \neq a' \wedge f(a) = f(a')).$$

Définition 2.24 *[4], [5], [9] f est dite surjective (ou une surjection) si tout élément de B admet au moins un antécédent dans A. Ce qui revient à écrire*

$$f \text{ est surjective} \Leftrightarrow \forall b \in B, \exists a \in A \quad b = f(a).$$

Par négation,

$$f \text{ n'est pas surjective} \Leftrightarrow \exists b \in B,\ \forall a \in A \quad b \neq f(a).$$

Définition 2.25 *[4], [5], [9] f est dite bijective (ou une bijection) si elle est injective et surjective, autrement dit si tout élément de B admet un seul et un seul antécédent. Ce qui revient à écrire*

$$f \text{ est bijective} \Leftrightarrow \forall b \in B, \exists! a \in A \quad b = f(a).$$

Exemple 2.20 *1. L'application*

$$\begin{array}{rccc} g_1 : & \mathbb{R}_+ & \longrightarrow & \mathbb{R} \\ & a & \longmapsto & a^2. \end{array}$$

est injective mais pas surjective car les images négatives n'admettent pas des antécédents par g_1.

2. *L'application*

$$\begin{array}{rccc} g_2 : & \mathbb{R} & \longrightarrow & \mathbb{R}_+ \\ & a & \longmapsto & a^2. \end{array}$$

est surjective car tout élément de $\mathbb{R}_+$ *a au moins un antécédent mais pas injective car* -1 *et* 1 *ont même image.*

3. *L'application*

$$\begin{array}{rccc} g_3 : & \mathbb{R}_+ & \longrightarrow & \mathbb{R}_+ \\ & a & \longmapsto & a^2. \end{array}$$

est bijective car tout élément de $\mathbb{R}_+$ *a un unique antécédent qui est sa racine carrée.*

Proposition 2.4 *[5], [9] Étant* A_1, A_2 *et* A_3 *des ensembles non vides. Soit* $f_1 \in \mathscr{F}(A_1, A_2)$ *et* $f_2 \in \mathscr{F}(A_2, A_3)$.

1. *Si* f_1 *et* f_2 *sont injectives, alors* $f_2 o f_1$ *est injective.*
2. *Si* f_1 *et* f_2 *sont surjectives, alors* $f_2 o f_1$ *est surjective.*
3. *Si* f_1 *et* f_2 *sont bijectives, alors* $f_2 o f_1$ *est bijective.*
4. *Si* $f_2 o f_1$ *est injective alors* f_1 *est injective.*
5. *Si* $f_2 o f_1$ *est surjective alors* f_2 *est surjective.*

Preuve.

1. Supposons f_1 et f_2 sont injectives. Étant donnés a et a' deux éléments de A_1 tels que $(f_2 o f_1)(a) = (f_2 o f_1)(a')$. En utilisant l'injectivité de f_2, on obtient $f_1(a) = f_1(a')$, l'injectivité de f_1 donne $a = a'$. Par suite, $f_2 o f_1$ est injective.
2. Supposons que f_1 et f_2 sont surjectives. Soit $a"$ un élément de A_3. En utilisant la surjectivité de f_2, on peut trouver $a' \in A_2$ tel que $a" = f_2(a')$. Comme f_1 est surjective, on peut déduire l'existence de $a \in A_1$ tel que $a' = f_1(a)$. D'où, $a" = f_2(f_1(a)) = (f_2 o f_1)(a)$. L'application $f_2 o f_1$ est donc surjective.
3. Conséquences immédiate des précédents.
4. Supposons que $f_2 o f_1$ est injective. Soient $(a_1, a_2) \in A_1^2$:

$$\begin{array}{rcl} f_1(a_1) = f_1(a_2) & \Rightarrow & f_2(f_1(a_1)) = f_2(f_1(a_2)) \\ & \Rightarrow & (f_2 o f_1)(a_1) = (f_2 o f_1)(a_2) \\ & \Rightarrow & a_1 = a_2, \quad \text{car } f_2 o f_1 \text{est injective.} \end{array}$$

   Donc, f_1 est injective.
5. Soit $a" \in A_3$: Comme $f_2 o f_1$ est surjective, il existe $a \in A_1$ tel que $a" = (f_2 o f_1)(a)$. En notant $a' = f_1(a)$, on a $a' \in A_2$ et $a" = (f_2 o f_1)(a) = f_2(a')$. Ceci montre que f_2 est surjective.

■

Applications Réciproque

Proposition 2.5 *[5], [9] Étant donnés* A_1, A_2 *deux ensembles non vides et f une application de* A_1 *dans* A_2*. Alors,* f_1 *est bijective si et seulement si il existe une unique application* f_2 *de* A_2 *dans* A_1 *telle que*

$$f_1 o f_2 = Id_{A_2} \quad et \quad f_2 o f_1 = Id_{A_1}.$$

Dans ce cas, f_1 *est dite inversible et* f_2 *est appelée l'application inverse (application réciproque) de* f_1 *et on la note* $f_2 = {f_1}^{-1}$

Preuve. I- On suppose que f_1 est bijective, donc à tout élément $b \in A_2$, en associant un seul élément $a \in A_1$, qu'on notera $f_1(a)$ tel que $f_1(a) = b$. Étant donné l'application

$$\begin{array}{rccc} f_2 : & A_2 & \longrightarrow & A_1 \\ & b & \longmapsto & f_2(b) = a. \end{array}$$

On montre que

$$f_1 o f_2 = Id_{A_2} \quad \text{et} \quad f_2 o f_1 = Id_{A_1}.$$

1. Supposons que $b \in A_2$, alors pour $f_2(b) = a$ avec $f_1(a) = b$, donc

$$f_1 o f_2(b) = f_1(f_2(b)) = f(a) = b,$$

donc, $f_1 o f_2 = Id_{A_2}$.

2. Étant donné $a \in A_1$, alors pour $b = f_1(a)$ on a $f_2(b) = a$, donc

$$(f_2 o f_1)(a) = f_2(f_1(a)) = f_2(b) = a,$$

d'où $f_2 o f_1 = Id_{A_1}$.

3. Prouvons l'unicité de f_2. Étant donné $g_1 : A_2 \to A_1$ satisfaisant les deux propriétés précédentes, alors pour tout $b \in A_2$, il existe $a \in A_1$ tel que $b = f_1(a)$. Donc,

$$g_1(b) = g_1(f_1(a)) = g_1 o f_1(a) = Id_{A_1}(a) = f_2 o f_1(a) = f_2(f_1(a)) = f_2(b).$$

Par suite, $g_1 = f_2$

II- On suppose l'existence d'une application $f_2 : A_2 \to A_1$ telle que

$$f_1 o f_2 = Id_{A_2} \quad \text{et} \quad f_2 o f_1 = Id_{A_1}.$$

Prouvons que f est bijective.

1. Étant donnés $a_1 \in A_1, a_2 \in A_1$. Comme $f_2 o f_1 = Id_{A_1}$, on obtient $(f_2 o f_1)(a_1) = a_1$ et $(f_2 o f_1)(a_2) = a_2$. Alors,

$$\begin{array}{lll} f_1(a_1) = f_1(a_2) & \Rightarrow & f_2(f_1(a_1)) = f_2(f_1(a_2)) \quad \text{puisque } f_2 \text{ est une application} \\ & \Rightarrow & (f_2 o f_1)(a_1) = (f_2 o f_1)(a_2) \\ & \Rightarrow & a_1 = a_2. \end{array}$$

2. Supposons que $b \in A_2$. Du fait que $f_1 o f_2 = Id_{A_2}$, on obtient $f_1 o f_2(b) = Id_{A_2}(b)$, par suite il existe $a = f_2(b) \in A_1$ tel que $f_1(a) = b$, donc f_1 est surjective.
De 1. et 2., on obtient f_1 est bijective.

■

Exemple 2.21 *Étant donnée l'application suivante*

$$\begin{array}{rcl} f:\mathbb{R}\backslash\{3\} & \longrightarrow & \mathrm{B} \\ a & \longmapsto & \frac{a+4}{a-3} \end{array}$$

Trouver B pour que l'application f soit bijective et donner l'application réciproque de f.
Montrons que f est bijective équivaut à chercher l'existence de $b\in\mathrm{B}$ *tel que* $b=f(a)$.
Soit $b\in\mathrm{B}$, *alors*

$$\begin{array}{rcl} b=f(a) & \Leftrightarrow & b=\frac{a+4}{a-3} \\ & \Leftrightarrow & b(a-3)=a+4 \\ & \Leftrightarrow & a=\frac{3b+4}{b-1} \quad si \quad b\neq 1 \end{array}$$

d'où

$$\forall b\in\mathbb{R}\backslash\{1\},\exists! a=\frac{3b+4}{b-1}; b=f(a)$$

pour montrer que f est bijective, il faut vérifier si $a=\frac{3b+4}{b-1}\in\mathbb{R}\backslash\{3\}$?
On a

$$\frac{3b+4}{b-1}=3 \quad \Leftrightarrow \quad 4=-3 \quad ce\ qui\ est\ impossible$$

ce qui prouve que $\frac{3b+4}{b-1}\in\mathbb{R}\backslash\{3\}$, *par suite, f est bijective si* $\mathrm{B}=\mathbb{R}\backslash\{1\}$ *et l'inverse de f est*

$$\begin{array}{rcl} f^{-1}:\mathbb{R}\backslash\{1\} & \longrightarrow & \mathbb{R}\backslash\{3\} \\ b & \longmapsto & \frac{3b+4}{b-1}. \end{array}$$

Prolongement et restriction d'une application

Définition 2.26 *[5], [9] Étant donnés A, B deux ensembles non vides et f une application de A dans B.*
Soit $\mathrm{A}_1\subset\mathrm{A}$, *l'application de* A_1 *vers B définie par*

$$\forall a\in\mathrm{A}_1, f_{/\mathrm{A}_1}(a)=f(a)$$

est appelée restriction de f à A_1 *qu'on note* $f_{/\mathrm{A}_1}$,
Soit A' *tel que* $\mathrm{A}\subset\mathrm{A}'$, *toute application* f_1 *de* A' *vers B définie par*

$$\forall a\in\mathrm{A}, f_1(a)=f(a)$$

est appelée prolongement de f à A'.
On dit que f_1 *est un prolongement de f si f est une restriction de* f_1.

Exemple 2.22 *On considère l'application*

$$\begin{array}{rcl} f_1:\mathbb{R}_+ & \longrightarrow & \mathbb{R}_+ \\ a & \longmapsto & a. \end{array}$$

Alors

$$\begin{array}{rcl} f_2:\mathbb{R} & \longrightarrow & \mathbb{R}_+ \\ a & \longmapsto & |a| \end{array}$$

et

$$\begin{array}{rcl} f_3:\mathbb{R} & \longrightarrow & \mathbb{R}_+ \\ a & \longmapsto & \begin{cases} a & si \quad a\geq 0 \\ 0 & si \quad a<0 \end{cases} \end{array}$$

sont des prolongements de f_1 *à* $\mathbb{R}$.

Remarque 2.3 *Le prolongement d'une application n'est pas unique.*

4 Exercices corrigés

4.1 Exercices sur les ensembles

Exercice 2.1 *Étant donnés* $F=\{a_1,a_2,a_3,a_4\}$, $G=\{a_1,a_2,a_4\}$, $H=[0,5]$, $I=[2,6]$. *Déterminer* $F\cap G$, $F\cup G$, $F\times G$, $H\cap I$, $H\cup I$, $H^H_{\mathbb{R}}$, $\mathbb{R}\setminus(H\cap I)$, $\mathbb{R}\setminus(H)$, $\mathbb{R}\setminus(I)$, $(\mathbb{R}\setminus(H))\cup(\mathbb{R}\setminus(I))$.

Solution.

1. $F\cap G=\{a_1,a_2,a_4\}=G$,
2. $F\cup G=\{a_1,a_2,a_3,a_4\}=F$,
3. $F\times G=\{(a_1,a_1),(a_1,a_2),(a_1,a_4),(a_2,a_1),(a_2,a_2),(a_2,a_4),(a_3,a_1),(a_3,a_2),(a_3,a_4),(a_4,a_1),(a_4,a_2),(a_4$
4. $H\cap I=[2,5]$, $H\cup I=[0,6]$.
5. $H^H_{\mathbb{R}}=]-\infty,0[\cup]5,+\infty[$,
6. $\mathbb{R}\setminus(H\cap I)=]-\infty,2[\cup]5,+\infty[$,
7. $\mathbb{R}\setminus(H)=H^H_{\mathbb{R}}=]-\infty,0[\cup]5,+\infty[$,
8. $\mathbb{R}\setminus(I)=H^I_{\mathbb{R}}=]-\infty,2[\cup]6,+\infty[$.
9. $(\mathbb{R}\setminus(H))\cup(\mathbb{R}\setminus(I))=]-\infty,0[\cup]5,+\infty[\cup]-\infty,2[\cup]6,+\infty[=]-\infty,2[\cup]5,+\infty[$.

On remarque que $(\mathbb{R}\setminus(H))\cup(\mathbb{R}\setminus(I))=\mathbb{R}\setminus(H\cap I)$.

Exercice 2.2 *Étant donné A un ensemble. Déterminer les ensembles* A_1,A_2,A_3 *de A telles que*

$$A_1\cup A_2\cap A_3)=(A_1\cup A_2)\cap A_3. \tag{2.1}$$

Solution. cherchons une condition nécessaire et suffisante sur (A_1,A_2,A_3) de $(\mathscr{P}(A))^3$ pour que (2.1) soit vérifier.
On suppose la propriété (2.1). On a $A_1\subset A_1\cup(A_2\cap A_3)$. En utilisant (2.1), on obtient $A_1\subset(A_1\cup A_2)\cap A_3\subset A_3$. Par conséquent, $A_1\subset A_3$ est une condition nécessaire pour que l'on ait (2.1).
D'autre part, on suppose que $A_1\subset A_3$. On obtient :

$$(A_1\cup A_2)\cap A_3=(A_1\cap A_3)\cup(A_2\cap A_3)=A_1\cup(A_2\cap A_3),$$

d'où la propriété (2.1).
Une condition nécessaire et suffisante pour que l'on ait (2.1) est donc $A_1\subset A_3$.

Exercice 2.3 *Étant donné A un ensemble et* A_1,A_2 *et* A_3 *des parties de A telles que*

$$(A_1\cup A_3)\subset(A_1\cup A_2)\quad et\quad (A_1\cap A_3)\subset(A_1\cap A_2).$$

Prouver que A_3 *est une partie de* A_2.

Solution. Supposons $a\in A_3$; alors $a\in(A_1\cup A_3)$ et comme $(A_1\cup A_3)\subset(A_1\cup A_2)$, alors $a\in(A_1\cup A_2)$, ce qui donne $a\in A_1$ ou $a\in A_2$.
Si $a\in A_1$, $a\in A_1\cap A_3$. De la propriété $(A_1\cap A_3)\subset(A_1\cap A_2)$, on conclue que $a\in A_1\cap A_2$. Donc, $a\in A_2$.
D'où, A_3 est une partie de A_2.

Exercice 2.4 *Étant donnés les ensembles* A_1,A_2 *et* A_3. *Prouver que*

1. $(A_1\times A_2)\cup(A_1\times A_3)=A_1\times(A_2\cup A_3)$.

2. $(A_1 \times A_2) \cup (A_3 \times A_2) = (A_1 \cup A_3) \times A_2$.

Solution.

1. Étant donnés $(a_1, a_2) \in (A_1 \times A_2) \cup (A_1 \times A_3)$.

$$\begin{aligned}
(a_1, a_2) \in ((A_1 \times A_2) \cup (A_1 \times A_3)) &\Leftrightarrow ((a_1, a_2) \in (A_1 \times A_2)) \vee ((a_1, a_2) \in (A_1 \times A_3)) \\
&\Leftrightarrow ((a_1 \in A_1) \wedge (a_2 \in A_2)) \vee ((a_1 \in A_1) \wedge (a_2 \in A_3)) \\
&\Leftrightarrow (a_1 \in A_1) \wedge ((a_2 \in A_2) \vee (a_2 \in A_3) \\
&\Leftrightarrow (a_1 \in A_1) \wedge ((a_2 \in (A_2 \cup A_3)) \\
&\Leftrightarrow (a_1, a_2) \in A_1 \times (A_2 \cup A_3).
\end{aligned}$$

2. Étant donnés $(a_1, a_2) \in (A_1 \times A_2) \cup (A_3 \times A_2)$.

$$\begin{aligned}
(a_1, a_2) \in (A_1 \times A_2) \cup (A_3 \times A_2) &\Leftrightarrow ((a_1, a_2) \in (A_1 \times A_2)) \vee ((a_1, a_2) \in (A_3 \times A_2)) \\
&\Leftrightarrow ((a_1 \in A_1) \wedge (a_2 \in A_2)) \vee ((a_1 \in A_3) \wedge (a_2 \in A_2)) \\
&\Leftrightarrow ((a_1 \in A_1) \vee (a_1 \in A_3) \wedge (a_2 \in A_2) \\
&\Leftrightarrow ((a_1 \in (A_1 \cup A_3)) \wedge (a_2 \in A_2) \\
&\Leftrightarrow (a_1, a_2) \in (A_1 \cup A_3) \times A_2.
\end{aligned}$$

Exercice 2.5 *Déterminer toutes les partitions de l'ensemble* $A = \{1, 4, 6\}$.

Solution. Les partitions de l'ensemble A sont :

1. $A_1 = \{\{1, 4, 6\}\}$.
2. $A_2 = \{\{1\}, \{4\}, \{6\}\}$.
3. $A_3 = \{\{1\}, \{4, 6\}\}$.
4. $A_4 = \{\{4\}, \{1, 6\}\}$.
5. $A_5 = \{\{6\}, \{1, 4\}\}$.

Exercice 2.6 *Étant donnés A un ensemble et* A_1, A_2, A_3 *des sous ensembles de A. On note*

$$E = (A_1 \cap A_2) \cup (A_2 \cap A_3) \cup (A_3 \cap A_1)$$

et

$$F = (A_1 \cup A_2) \cap (A_2 \cup A_3) \cap (A_3 \cup A_1).$$

Prouver que $E = F$.

Solution. On a :

$$\begin{aligned}
E &= (A_1 \cap A_2) \cup (A_2 \cap A_3) \cup (A_3 \cap A_1) \\
&= ((A_1 \cap A_2) \cup (A_2 \cap A_3)) \cup (A_3 \cap A_1) \quad \text{associativité de} \cup \\
&= ((A_1 \cup A_3) \cap A_2) \cup (A_3 \cap A_1) \quad \text{en mettant } A_2 \text{ en facteur} \\
&= ((A_1 \cup A_3) \cup (A_3 \cap A_1)) \cap (A_2 \cup (A_3 \cap A_1)) \quad \text{la distributivité de} \cup \text{sur} \cap \\
&= (A_1 \cup A_3) \cap ((A_2 \cup A_3) \cap (A_2 \cup A_1)) \quad \text{la distributivité de} \cup \text{sur} \cap \\
&= (A_1 \cup A_2) \cap (A_2 \cup A_3) \cap (A_3 \cup A_1) \\
&= F.
\end{aligned}$$

5 Exercices proposés

Exercice 2.7 *Étant donnés les ensembles* $A_1, A_2, A_3 et A_4$. *Montrer l'égalité suivante*

$$(A_1 \times A_2) \cap (A_3 \times A_4) = (A_1 \cap A_3) \times (A_2 \cap A_4)$$

.

Exercice 2.8 *Étant donnés A, B des ensembles,* $(E_i)_{i\in I}$ *une famille de sous ensembles de A,* $(F_i)_{i\in I}$ *une famille de de sous ensembles B, indexés par le même ensemble I, G une partie de A, H une partie de B. Prouver que*

1. $\cup_{i\in I}(E_i \times H) = (\cup_{i\in I} E_i) \times H$.
2. $\cup_{i\in I}(G \times F_i) = G \times (\cup_{i\in I} F_i)$.

Exercice 2.9 *Soient G un ensemble et* H_1 *et* H_2 *deux parties de G vérifiant les propriétés suivantes*

1. $H_1 \cap H_2 \neq \emptyset$;
2. $H_1 \cup H_2 \neq G$;
3. $H_1 \not\subseteq H_2$;
4. $H_2 \not\subseteq H_1$.

On note

1. $G_1 = H_1 \cap H_2$,
2. $G_2 = H_1 \cap C_G^{H_2}$,
3. $G_3 = H_2 \cap C_G^{H_1}$,
4. $G_4 = C_G^{H_1 \cup H_2}$.

Prouver que $\{G_1, G_2, G_3, G_4\}$ *est une partition de G.*

5.1 Exercices sur les applications

Exercice 2.10 *Considérons les applications suivantes :*

$$\begin{array}{rccc} f_1 : & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & a & \longmapsto & a^2. \end{array}$$

et

$$\begin{array}{rccc} f_2 : & \mathbb{R} & \longrightarrow & [-1,1] \\ & a & \longmapsto & \cos(\pi a). \end{array}$$

Déterminer $f_1^{-1}(\{1\})$, $f_1^{-1}([1,2])$, $f_1^{-1}(]-\infty,0[)$, $f_1(\{0\})$, $f_1([0,+\infty[)$, $f_2(\mathbb{N})$, $f_2^{-1}(\{\pm 1\})$.

Solution.

$$\begin{array}{rcl} f_1^{-1}(\{1\}) & = & \{a \in \mathbb{R}, f_1(a) \in \{1\}\} \\ & = & \{a \in \mathbb{R}, a^2 = 1\} \\ & = & \{-1, 1\}. \end{array}$$

$$\begin{array}{rcl} f_1^{-1}([1,2]) & = & \{a \in \mathbb{R}, f_1(a) \in [1,2]\} \\ & = & [-\sqrt{2}, -1] \cup [1, \sqrt{2}]. \end{array}$$

$$\begin{aligned} f_1^{-1}(]-\infty,0[) &= \{a\in\mathbb{R}, f_1(a)\in]-\infty,0[\} \\ &= \emptyset. \end{aligned}$$

$$\begin{aligned} f_1(\{0\}) = &= \{a^2, a\in\{0\}\} \\ &= \{0\}. \end{aligned}$$

$$\begin{aligned} f_1([0,+\infty[) = &= \{a^2, x\in[0,+\infty[\} \\ &= [0,+\infty[. \end{aligned}$$

$$\begin{aligned} f_2(\mathbb{N}) = &= \{\cos(\pi a), a\in\mathbb{N}\} \\ &= \{-1,1\}. \end{aligned}$$

$$\begin{aligned} f_2^{-1}(\{\pm 1\}) &= \{a\in\mathbb{R}, f_2(a)\in\{-1,1\}\} \\ &= \mathbb{N}. \end{aligned}$$

Exercice 2.11 *Étant donnés* $\mathrm{A}_1, \mathrm{A}_2$ *et* A_3 *des ensembles non vides. Étant donnés* $f_1 \in \mathscr{F}(\mathrm{A}_1, \mathrm{A}_2)$ *et* $f_2 \in \mathscr{F}(\mathrm{A}_2, \mathrm{A}_3)$. *Prouver que si on a la bijection de* f_1 *et* f_2, *alors on peut déduire la bijection de* $f_2 o f_1$ *et* $(f_2 o f_1)^{-1} = f_1^{-1} o f_2^{-1}$.

Solution. Supposons que f_1 et f_2 sont bijectives, alors $f_2 o f_1$ est bijective, et f_1^{-1} , f_2^{-1} et $(f_2 o f_1)^{-1}$ existent satisfaisant

$$f_2^{-1} o f_2 = \mathrm{I}d_{\mathrm{A}_2} \quad \text{et} \quad f_1^{-1} o f_1 = \mathrm{I}d_{\mathrm{A}_1}.$$

Alors, $(f_1^{-1} o f_2^{-1}) o (f_2 o f_1) = f_1^{-1} o (f_2^{-1} o f_2) o f_1 = f_1^{-1} o \mathrm{I}d_{\mathrm{A}_2} o f_1 = f_1^{-1} o f_1 = \mathrm{I}d_{\mathrm{A}_1}$.

Exercice 2.12 *Étant donnés A , A' des ensembles non vides,* $\mathrm{A}_1, \mathrm{A}_2$ *deux sous ensembles de E. Notons* $h \in \mathscr{F}(\mathrm{A}, \mathrm{A}')$.
1) Prouver que l'égalité suivante n'est pas satisfaite $h(\mathrm{A}_1 \cap \mathrm{A}_2) = h(\mathrm{A}_1) \cap h(\mathrm{A}_2)$ *en donnant un contre exemple.*
2) Prouver que les propositions suivantes sont équivalentes :

a) $h(\mathrm{A}_1 \cap \mathrm{A}_2) = h(\mathrm{A}_1) \cap f(\mathrm{A}_2)$.

b) h est injective.

Solution. *1) On définit l'application*

$$\begin{aligned} h: \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto 2x^2. \end{aligned}$$

et les ensembles $\mathrm{A}_1 =]-1,0], \mathrm{A}_2 = [0,2[$.
Alors
$\mathrm{A}_1 \cap \mathrm{A}_2 = \{0\}, h(\mathrm{A}_1) = [0,2[, h(\mathrm{A}_2) = [0,8[, h(\mathrm{A}_1 \cap \mathrm{A}_2) = \{0\}, et h(\mathrm{A}_1) \cap h(\mathrm{A}_2) = [0,2[$. *On remarque bien que*

$$h(\mathrm{A}_1 \cap \mathrm{A}_2) = \{0\} \subsetneqq [0,2[= h(\mathrm{A}_1) \cap h(\mathrm{A}_2).$$

2) On suppose que la propriété a) est vérifiée. Soient a et a' deux éléments différents de A. En utilisant a) aux deux sous ensembles suivants : $\mathrm{A}_1 = \{a\}$ *et* $\mathrm{A}_1 = \{a'\}$; *on obtient*

$$h(\mathrm{A}_1) = \{h(a)\}, \quad h(\mathrm{A}_2) = \{h(a')\}$$

et

$$\emptyset = h(\mathrm{A}_1 \cap \mathrm{A}_2) = \{h(a)\} \cap \{h(a')\}.$$

D'où $\{h(a)\} \neq \{h(a')\}$ *. Ce qui implique que h est injective et que* $a) \Rightarrow b)$.
D'après le cours (chapitre 2), pour toutes $\mathrm{A}_1, \mathrm{A}_2$ *de* A, *nous avons*

$$h(\mathrm{A}_1 \cap \mathrm{A}_2) \subset h(\mathrm{A}_1) \cap h(\mathrm{A}_2).$$

On suppose l'existence deux sous ensembles A_1 *et* A_2 *de A telles que* $h(\mathrm{A}_1 \cap \mathrm{A}_2) \neq h(\mathrm{A}_1) \cap h(\mathrm{A}_2)$ *alors, il existe b de* $h(\mathrm{A}_1) \cap h(\mathrm{A}_2)$ *qui n'est pas un élément de* $h(\mathrm{A}_1 \cap \mathrm{A}_2)$, *mais,* $b \in h(\mathrm{A}_1) \cap h(\mathrm{A}_2)$ *est équivaut à* $b \in h(\mathrm{A}_1)$ *et* $b \in h(\mathrm{A}_2)$, *et*

$$(b \in h(\mathrm{A}_1)) \Leftrightarrow (\exists a_1 \in \mathrm{A}_1, b = h(a_1)) \quad et \quad (\exists a_2 \in \mathrm{A}_2, b = h(a_2)).$$

Ce qui nécessite $a_1 \neq a_2$ *puisque si* $a_1 = a_2$ *alors* $a_1 \in \mathrm{A}_1 \cap \mathrm{A}_2$ *et*

$$b \in h(\mathrm{A}_1 \cap \mathrm{A}_2)$$

ce qui contredit l'hypothèse. L'application h n'est pas donc injective, donc $non\ a) \Rightarrow non\ b)$ *soit encore* $b) \Rightarrow a)$, *d'où* $a) \Leftrightarrow b)$.

Exercice 2.13 *Notons G et H des ensembles non vides. Soient* $h \in \mathscr{F}(\mathrm{G}, \mathrm{H})$. *Montrer l'équivalence entre les propositions suivantes.*

a) Quel que soit G_1 *inclus dans G,* $h^{-1}(h(\mathrm{G}_1)) = \mathrm{G}_1$

b) h est injective.

De même pour les propositions

1. *Quel que soit* H_1 *inclus dans H,* $h(h^{-1}(\mathrm{H}_1)) = \mathrm{H}_1$
2. *h est surjective.*

Solution. On a pour toute partie G_1 de G et toute partie H_1 de H

$$\mathrm{G}_1 \subset h^{-1}(h(\mathrm{G}_1)) \quad h(h^{-1}(\mathrm{H}_1)) \subset \mathrm{H}_1.$$

Soit $a \in \mathrm{G}_1$.

$$\begin{aligned} a \in \mathrm{G}_1 &\Rightarrow h(a) \in h(\mathrm{G}_1) \\ &\Rightarrow a \in h^{-1}(h(\mathrm{G}_1)). \end{aligned}$$

Étant donné $b \in h(h^{-1}(\mathrm{H}_1))$.

$$\begin{aligned} b \in h(h^{-1}(\mathrm{H}_1)) &\Rightarrow \exists a \in h^{-1}(\mathrm{H}_1), b = h(a) \\ &\Rightarrow \exists a \in \mathrm{G}, b \in \mathrm{H}_1, b = h(a) \\ &\Rightarrow b \in \mathrm{H}_1. \end{aligned}$$

On va montrer maintenant l'équivalence des propriétés a) et b) en prouvant que $non\ a) \Leftrightarrow non\ b)$.

On suppose l'existence d'un sous ensemble G_1 de G telle que $h^{-1}(h(G_1)) \neq G_1$ alors il existe b de $h^{-1}(h(G_1))$ qui n'est pas un élément de G_1 ; or

$$b \in h^{-1}(h(G_1)) \Leftrightarrow h(b) \in h(G_1),$$

donc, il existe un élément a de G_1 tel que $h(a) = h(b)$ et comme $b \notin G_1$, $a \neq b$, par suite h n'est pas injective et $non\ a) \Rightarrow non\ b)$.
D'autre part, si h est non injective, alors il existe deux éléments a et b de G tels que $a \neq b$ et $h(a) = h(b)$. Supposons que G_1 est un sous ensemble de G qui possède un seul élément a, alors $h(G_1) = \{h(a)\}$ et $\{(a,b)\} \subset h^{-1}(h(G_1))$ donc

$$A \neq h^{-1}(h(G_1)),$$

ce qui montre que $nonb) \Rightarrow nona)$ donc $nona) \Leftrightarrow nonb)$.
On montre maintenant que 1) $\Leftrightarrow$ 2). On suppose que 1) vraie et utilisons cette propriété à H de H ; il découle $h(h^{-1}(H)) = H$ or $h^{-1}(H) = G$, donc $h(G) = H$. Ce dernier résultat signifie que h est surjective, donc 1) $\Rightarrow$ 2). Supposons 2) vraie, alors si b est un élément de H_1, il existe un élément a de G tel que $b = h(a)$ et $a \in h^{-1}(H_1)$ car $h(a) \in H_1$; donc $b \in h(h^{-1}(H_1))$ et comme cette propriété est vraie pour tout $b \in H_1$, alors

$$H_1 \subset h(h^{-1}(H_1)),$$

or $h(h^{-1}(H_1)) \subset H_1$, par suite $h(h^{-1}(H_1)) = H_1$ et 2) $\Rightarrow$ 1) d'où 1) $\Leftrightarrow$ 2).

Exercice 2.14 *Considérons l'application $f_1 : A \to B$. Prouver que*

$$f_1 \quad \textit{est injective} \Leftrightarrow \exists f_2 : B \to A \quad \textit{une application telle que} \quad f_2 o f_1 = Id_A$$

puis donner un exemple.

Solution. I. On suppose l'injectivité de f_1 et

$$\begin{array}{rccl} h: & f_1(A) & \longrightarrow & A \\ & b & \longmapsto & h(b) = a. \end{array}$$

Nous avons h est une application. Étant donné f_2 le prolongement de h à B. Alors,

$$\begin{array}{rccl} f_2 o f_1: & A & \longrightarrow & A \\ & a & \longmapsto & (f_2 o f_1)(a) = f_2(f_1(a)) = f_{2/f_1(A)}(f_1(a)) = h(f_1(a)) = a. \end{array}$$

D'où, $f_2 o f_1 = Id_A$
II. On suppose maintenant qu'il existe une application $\exists f_2 : B \to A$ telle que $f_2 o f_1 = Id_A$ et a, a' appartenant à A tels que $f_1(a) = f_1(a')$

$$\begin{array}{rcl} f_1(a) = f_1(a') & \Rightarrow & f_2(f_1(a)) = f_2(f_1(a')) \\ & \Rightarrow & f_2 o f_1(a) = f_2 o f_1(a') \\ & \Rightarrow & Id_A(a) = Id_A(a') \\ & \Rightarrow & a = a'. \end{array}$$

D'où l'injectivité de f_1.

Exemple 2.23 *Soient* $A = \{8,10,12,14\}$ *et* $B = \{8,9,10,11,12,13,14\}$ *et* $f_1 : A \to B$ *avec* $f_1(8) = 9, f_1(10) = 12, f_1(12) = 11, f_1(14) = 13$. f_1 *est une application injective. Considérons l'application* $f_2 : B \to A$ *satisfaisant* $f_2 o f_1 = Id_A$. *On pose* $f_1(A) = \{9,11,12,13\} \subset B$ *et* $h : f_1(A) \longrightarrow A$ *tel que* $h(9) = 8, h(11) = 12, h(12) = 10, h(13) = 14$. *On peut vérifier facilement que* h *est une application possède le prolongement suivant* $f_2 : B \longrightarrow A$ *tel que* $f_2(9) = 8, f_2(11) = 12, f_2(12) = 10, f_2(13) = 14$ *et* $f_2(8) = f_2(10) = 10$. f_2 *est une application satisfait* $f_2 o f_1(8) = f_2(f_1(8)) = f_2(9) = 8, f_2 o f_1(10) = f_2(f_1(10)) = f_2(12) = 10, f_2 o f_1(12) = f_2(f_1(12)) = f_2(11) = 12$ *et* $f_2 o f_1(14) = f_2(f_1(14)) = f_2(13) = 14$. *D'où,* $f_2 o f_1 = Id_A$

Exercice 2.15 *Étant donnés* A_1 *et* A_2 *deux ensembles finis tels que* $card A_1 = p, card A_2 = q$. *On rappel que* A_1 *et* A_2 *sont équipotents s'il existe une bijection entre* A_1 *et* A_2.
Prouver que les deux propriétés suivantes sont équivalentes :

a) A_1 *et* A_2 *sont équipotents.*

b) $p = q$.

Solution.*I. On suppose que* A_1 *et* A_2 *sont équipotents, on peut trouver donc* $h : A_1 \to A_2$ *une application bijective. Alors,*

$$\begin{aligned} h \text{ est bijective} &\Rightarrow h \text{ est injective et } h \text{ est surjective} \\ &\Rightarrow p \leq q \quad et \quad q \leq p \\ &\Rightarrow p = q. \end{aligned}$$

II. On suppose que $p = q$, *donc* $A_1 = \{a_1, a_2, ..., a_p\}$ *et* $A_2 = \{b_1, b_2, ..., b_q\}$. *Soit*

$$\begin{array}{rccl} h : & A_1 & \longrightarrow & A_2 \\ & a_k & \longmapsto & h(a_k) = b_k. \end{array}$$

avec $k = 1, 2..., p$. *Il est simple à prouver que* h *est bijective, donc* A_1 *et* A_2 *sont équipotents.*

5.2 Exercices proposés

Exercice 2.16 *Considérons les applications suivantes :*

$$\begin{array}{rccl} h_1 : & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & a & \longmapsto & a+1. \end{array}$$

et

$$\begin{array}{rccl} h_2 : & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & b & \longmapsto & \begin{cases} 0 & si \quad b = 0 \\ b-1 & si \quad b \geq 1. \end{cases} \end{array}$$

a) Les applications h_1 *et* h_2 *est elles injectives, surjectives, bijectives ?*
b) Trouver $h_1 o h_2$ *et* $h_2 o h_1$.

Exercice 2.17 *Étant donné* $h_1 : A \to B$ *une application. Prouver que*

$$h \quad \text{est surjective} \Leftrightarrow \exists h_2 : B \to A \quad \text{une application telle que} \quad h_1 o h_2 = Id_B$$

puis donner un exemple.

Exercice 2.18 *Étant donnés* A_1, A_2, A_3 *des ensembles,* $h_1 : A_1 \to A_2$, $h_2 : A_2 \to A_3$ *et* $h_3 : A_3 \to A_1$ *des applications. Prouver les implications suivantes*
a) $(h_3 o h_2 o h_1 et h_2 o h_1 o h_3 sont\ surjectives\ et h_1 o h_3 o h_2\ injective) \Rightarrow (h_1, h_2, h_3 sont\ bijectives)$.
b) $(h_3 o h_2 o h_1 et h_2 o h_1 o h_3 sont\ injectives\ et h_1 o h_3 o h_2 surjective) \Rightarrow (h_1, h_2, h_3 sont\ bijectives)$.

Exercice 2.19 *Soient* $A_1 = \{a_1\}$ *et* $A_2 = \{a_2, a_3\}$. *Existe-t-il des applications surjectives (resp. des injections , des bijections) de* A_1 *dans* A_2 *?*

Exercice 2.20 *Étant donnés* A_1, A_2, A_3 *et* A_4 *des ensembles non vides et* $h_1 \in \mathscr{F}(A_1, A_2)$. *Prouver l'équivalence des propriétés suivantes.*

a) Pour toutes applications $h_2 \in \mathscr{F}(A_3, A_1)$, $h_3 \in \mathscr{F}(A_3, A_1)$, *on a* $[h_1 o h_2 = h_1 o h_3 \Rightarrow h_2 = h_3]$

b) h_1 *est injective.*

De même

1. Pour toutes applications $h'_2 \in \mathscr{F}(A_2, A_4)$, $h'_3 \in \mathscr{F}(A_2, A_4)$, *on a* $[h'_2 o h_1 = h'_3 o h_1 \Rightarrow h'_2 = h'_3]$.

2. h_1 *est surjective.*

Chapitre 3

Relations binaires sur un ensemble

1 Introduction

L'objectif de ce chapitre est de rappeler les définitions et les conventions que nous faisons dans l'utilisation pratique de la notion de relations d'équivalences et d'ordres. Ce chapitre est basé sur les références ([1], [2], [3], [4], [7],[8], [9], [12]).

2 Relations Binaires

Définition 3.1 *[1], [3], [4] On appelle une relation binaire toute relation $\mathscr{R}$ d'un ensemble E vers lui même.*

Exemple 3.1 *Dans l'ensemble de parties d'un ensemble E, l'inclusion est une relation binaire.*
Dans l'ensemble des entiers naturels, la division et l'égalité sont aussi des relations binaires.

3 Propriétés des relations binaires dans un ensemble

Définition 3.2 *[1], [3], [4]*
Considérons $\mathscr{S}$ une relation binaire sur un ensemble A.

- *$\mathscr{S}$ est réflexive si seulement si*
$$\forall a \in \mathrm{A}, a \mathscr{S} a.$$
- *$\mathscr{S}$ est symétrique si seulement si*
$$\forall a \in \mathrm{A}, \forall b \in \mathrm{A}, a \mathscr{S} b \Rightarrow b \mathscr{S} a.$$
- *$\mathscr{S}$ est antisymétrique si seulement si*
$$\forall a \in \mathrm{A}, \forall b \in \mathrm{A}, (a \mathscr{S} b et b \mathscr{S} a) \Rightarrow a = b.$$
- *$\mathscr{S}$ est transitive si seulement si*
$$\forall a \in \mathrm{A}, \forall b \in \mathrm{A}, \forall c \in \mathrm{A}, (a \mathscr{S} b et b \mathscr{S} c) \Rightarrow a \mathscr{S} c.$$

Exemple 3.2
- *La relation " $\perp$ " définie sur l'ensemble des droites est une relation binaire symétrique mais n'est ni réflexive, ni transitive.*

- *La relation "=" est une relation binaire dans l'ensemble des entiers naturels, appelée la relation binaire d'égalité.*
  Cette relation est réflexive, symétrique et transitive.
  En effet, quelque soit a, b et c des entiers naturels on a "=" est réflexive car $a = a$, "=" est transitive car
  $$(a = b \quad et \quad b = c) \Rightarrow a = c$$
  et "=" est symétrique car
  $$a = b \Rightarrow b = a.$$
- *La relation $\mathscr{S}$:"la divisibilité dans l $\mathbb{N}$". On a tout entier est divisible par lui même, autrement dit $\mathscr{S}$ est réflexible, de plus elle est transitive puisque a divise b et b divise c, alors : "a divise c". Mais, si "a" divise "b", "a" n'est pas divisible par "b", donc $\mathscr{S}$ n'est pas symétrique.*

4 Relation d'équivalence

Définition 3.3 *[1], [3] , [9] Étant donnée $\mathscr{S}$ une relation binaire sur un ensemble A. $\mathscr{S}$ est une relation d'équivalence si elle est réflexive, symétrique et transitive.*
On note
$$a \sim b(\mathscr{S})$$
et on lit a est équivalent à b modulo $\mathscr{S}$ si a est correspond à b par une relation d'équivalence $\mathscr{S}$.

Exemple 3.3
- *La relation "=" est une relation d'équivalence sur tout ensemble.*
- *Étant donnés A et B deux ensembles non vides et $h : \mathrm{A} \to \mathrm{B}$ une application. La relation $\mathscr{S}$ définie par*
  $$\forall (a_1, a_2) \in \mathrm{A}^2, a_1 \mathscr{S} a_2 \Leftrightarrow h(a_1) = h(a_2)$$
  définit une relation d'équivalence.

5 Classe d'équivalence

Définition 3.4 *[1], [3]*
Étant donnée $\mathscr{R}$ une relation d'équivalence sur un ensemble A et soit $a \in \mathrm{A}$.
- *L'ensemble $\{b \in \mathrm{A}, b\mathscr{R}a\} \subset \mathrm{A}$ noté $\dot{a}$ ou bien $\overline{a}$, est appelé classe d'équivalence de a .*
- *L'ensemble de toutes les classes d'équivalence modulo $\mathscr{R}$ se nomme l'ensemble quotient de A par $\mathscr{R}$ et se note $\mathrm{A}/\mathscr{R}$. On a donc*
  $$\mathrm{A}/\mathscr{R} = \{\dot{a}, a \in \mathrm{A}\}.$$
- *Les éléments de l'ensemble $\dot{a}$ sont appelés les représentants de $\dot{a}$.*
- *A partir d'une relation d'équivalence, on peut définir la surjection canonique S, c'est l'application qui à tout élément $a \in \mathrm{A}$ fait correspondre sa classe d'équivalence $\dot{a}$.*

Exemple 3.4
- *Étant donnés A et B deux ensembles non vides et $h : \mathrm{A} \to \mathrm{B}$ une application. La relation $\mathscr{R}$ donnée par*
  $$\forall (a, b) \in \mathrm{A}^2, a\mathscr{R}b \Leftrightarrow h(a) = h(b)$$

est une relation d'équivalence. On a

$$\begin{aligned}\dot{a} &= \{b \in \mathrm{A}, a\mathscr{R}b\} \\ &= \{b \in \mathrm{A}, h(a) = h(b)\} \\ &= \left\{b \in \mathrm{A}, b \in h^{-1}(\{h(a)\})\right\}\end{aligned}$$

- *L'ensemble de toutes les classes d'équivalence est* $\mathrm{A}/\mathscr{R} = \left\{h^{-1}(\{h(a)\}), a \in \mathrm{E}\right\}$.

Proposition 3.1 *[1], [3] Étant donnée $\mathscr{R}$ une relation d'équivalence sur un ensemble A. Alors*

- $\forall a \in \mathrm{A}, \dot{a} \neq \emptyset$
- $\forall a_1 \in \mathrm{A}, \forall a_2 \in \mathrm{A}, (\dot{a}_1 \cap \dot{a}_2 = \emptyset) \vee (\dot{a}_1 = \dot{a}_2)$
- *Les classes d'équivalences sont non vides, elles sont deux à deux disjointes et leur réunion est A c'est à dire qu'elles forment une partition de A.*

Preuve.

- Si $a \in \mathrm{A}$, en utilisant la réflexivité de $\mathscr{R}$ on obtient $a \in \dot{a}$.
- Étant donnés $a_1 \in \mathrm{A}, a_2 \in \mathrm{A}$, si $\dot{a}_1 \cap \dot{a}_2 \neq \emptyset$. Alors il existe $a_3 \in \dot{a}_1 \cap \dot{a}_2$, donc $a_3\mathscr{R}a_2$ et $a_3\mathscr{R}a_1$. Prouvons que $\dot{a}_1 = \dot{a}_2$. Si $a_4 \in \dot{a}_1$, alors

  $$((a_4\mathscr{R}a_1) \wedge (a_3\mathscr{R}a_1) \wedge (z\mathscr{R}y))$$

  en utilisant la symétrie et la transitivité de la relation $\mathscr{R}$, on obtient

  $$(a_4\mathscr{R}a_3) \wedge (a_3\mathscr{R}a_2)$$

  et comme $\mathscr{R}$ est transitive on déduit que $a_4\mathscr{R}a_2$, d'où $a_4 \in \dot{a}_2$, ce qui prouve que $\dot{a}_1 \subset \dot{a}_2$. De la même manière, on montre que $\dot{a}_2 \subset \dot{a}_1$, ce qui termine la preuve de la propriété.
- D'après ce qui précède, on déduit que $\mathrm{A}/\mathscr{R}$ est une partition de A.

■

5.1 Factorisation d'une application

Définition 3.5 *[9], [10] Étant donné une application $h : \mathrm{A} \to \mathrm{B}$, on note $\mathrm{A}/\mathscr{S}$ le quotient de A par la relation d'équivalence $\mathscr{S}$ telle que $a\mathscr{S}b \Leftrightarrow f(a) = f(b)$. Soit $\mathrm{B}' = f(\mathrm{A})$. Si $\dot{a} \in \mathrm{A}/\mathscr{S}$, alors $f(a) = f(b), \forall (a,b) \in \dot{a}^2$.*
Soit R *la surjection canonique de A dans* $\mathrm{A}/\mathscr{S}$ *et i l'injection canonique de B' dans B. Alors,*

$$\begin{array}{rccl}\tilde{h}: & \mathrm{A}/\mathscr{S} & \longrightarrow & \mathrm{B}' \\ & \dot{a} & \longmapsto & \tilde{h}(\dot{a}) = h(a) \quad si\ a \in \dot{x}\end{array}$$

est une application bijective et l'écriture $h = i\,o\,\tilde{h}\,o\mathrm{R}$ s'appelle la factorisation de h.

Preuve.

- Pour montrer que $\tilde{h}$ est une application il faut prouver que $\tilde{h}(\dot{a})$ ne dépend pas du représentant de la classe $\dot{a}$. Étant donnés $a, b \in \mathrm{A}$ tels que $\dot{a} = \dot{b}$. Alors $h(a) = h(b)$, d'où

  $$\tilde{h}(\dot{a}) = h(a) = h(b) = \tilde{h}(\dot{b}),$$

  donc

  $$\forall (\dot{a}, \dot{b}) \in (\mathrm{A}/\mathscr{S})^2, (\dot{a} = \dot{b}) \Leftrightarrow (\tilde{h}(\dot{a}) = \tilde{h}(\dot{b})),$$

  ce qui prouve que $\tilde{h}$ est une application de $\mathrm{A}\backslash\mathscr{S}$ dans B'.

- Prouvons que $\tilde{h}$ est bijective. Étant donnés $(\dot{a},\dot{b}) \in (A/\mathcal{S})^2$,donc

$$\begin{aligned} \tilde{h}(\dot{a}) = \tilde{h}(\dot{b}) &\Leftrightarrow h(a) = h(b) \\ &\Leftrightarrow a \mathcal{S} ! b \\ &\Leftrightarrow \dot{a} = \dot{b} \end{aligned}$$

  ce qui montre que $\tilde{h}$ est injective. De plus $\tilde{h}$ est surjective par construction.

■

6 Relation d'ordre

Définition 3.6 *[9] Étant donné $\mathcal{S}$ une relation binaire sur un ensemble A. On dit que $\mathcal{S}$ est une relation d'ordre si elle est réflexive, antisymétrique et transitive.*
On appelle ensemble ordonné un couple $(A,\mathcal{S})$ où $\mathcal{S}$ est une relation d'ordre sur A.
Une relation d'ordre $\mathcal{S}$ sur A est dite relation d'ordre total si deux éléments quelconques a_1 et a_2 sont toujours comparables, c'est à dire si l'on a $a_1 \mathcal{S} a_2$ ou $a_2 \mathcal{S} a_1$. Dans le cas contraire, l'ordre est partiel.

Exemple 3.5

- *Les relations d'ordre usuelles sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{R}$ notées $\leq$ ou $\geq$ sont d'ordre total.*
- *La relation $<$ utilisée habituellement sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{R}$ n'est pas une relation d'ordre car elle est antisymétrique et transitive mais pas réflexive.*
- *La relation $\subset$ est un ordre partiel sur $\mathcal{P}(E)$ lorsque E contient au moins deux éléments.*
- *La relation de divisibilité sur l'ensemble $\mathbb{N}$ est une relation d'ordre partiel car 7 et 8, par exemple, ne sont pas comparables (aucun des deux ne divise l'autre).*
- *Comme la relation de divisibilité définie sur l'ensemble $\mathbb{Z}$ n'est pas antisymétrique : les éléments x et -x se divisent mutuellement, alors la relation n'est pas une relation d'ordre.*

Remarque 3.1 *On note souvent une relation d'ordre par le symbole $\leq$, qui se lit " inférieur ou égal", ce qui ne signifie pas forcément que l'on travaille sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{R}$ munis de leur relation d'ordre usuelle.*

Définition 3.7 *[1], [3], [9] Étant donnés $(A,\leq)$ un ensemble ordonné, A_1 une partie de A.*

- *On dit qu'un élément $M \in A$ est un majorant de A_1 (ou qu'il majore A_1) s'il majore tous les éléments de A_1, autrement dit :*

$$\forall a \in A_1, a \leq M.$$

  L'ensemble A_1 est dit ensemble majoré.
- *On dit qu'un élément $m \in A$ est un minorant de A_1 (ou qu'il minore A_1) s'il minore tous les éléments de A_1, autrement dit :*

$$\forall a \in A_1, m \leq a.$$

  L'ensemble A_1 est dit ensemble minoré.
- *L'ensemble A_1 est dit borné s'il est majoré et minoré.*
- *Lorsque l'ensemble des majorants de A_1 possède un plus petit élément, cet élément est appelé borne supérieure de A et noté $\sup A_1$.*
- *Lorsque l'ensemble des minorants de A_1 possède un plus grand élément, cet élément est appelé borne inférieure de A_1 et noté $\inf A_1$.*

- *On dit qu'un élément* $\alpha \in A$ *est le plus grand élément de* A_1 *(ou maximum de* A_1*, noté* $\max A_1$*) si et seulement si*
$$\alpha \in A_1, \forall a \in A_1, a \leq \alpha.$$
- *On dit qu'un élément* $\beta \in A$ *est le plus petit élément de* A_1 *(ou minimum de* A_1*, noté* $\min A_1$*) si et seulement si*
$$\beta \in A_1, \forall a \in A_1, \beta \leq a.$$

Exemple 3.6
- *Dans* $(\mathbb{R}, \leq)$*, l'intervalle* $[3,8]$ *a pour majorant tout élément de* $[8, +\infty[$.
- *Dans* $(\mathscr{P}(A), \subset)$*, la partie* $\{A_1, A_2\}$ *est majorée par tout ensemble contenant* $A_1 \cup A_2$.
- *Dans* $\mathbb{N}$ *munit de la relation de la divisibilité, les majorants de* $\{8, 12, 18\}$ *sont les multiples de 72.*
- *Les ensembles* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ *ou* $\mathbb{R}$ *munis de leur relation d'ordre usuelle n'admettent pas de plus grand élément.*
- $\mathscr{P}(A)$ *possède, pour l'inclusion, un plus grand élément A et un plus petit élément* $\emptyset$.

7 Exercices corrigés

7.1 Exercices sur les relations d'équivalences

Exercice 3.1 *Étant donnés* $H = \{a, b, c, d\}$ *et* L *le graphe d'une relation* $\mathscr{R}$ *définie par*

$$L = \{(a,c), (c,d), (a,d), (b,a), (a,b), (b,b)\}.$$

Étudier la réflexibilité , la symétrie et la transitivité de $\mathscr{R}$.

Solution. Comme les couples $(a,a), (c,c), (d,d)$ n'appartiennent pas à L, alors $\mathscr{R}$ n'est pas réflexive.
Nous avons à titre d'exemple $(c,d) \in L$ donc $c\mathscr{R}d$ mais non $d\mathscr{R}c$, dans ce cas $\mathscr{R}$ n'est pas symétrique.
Comme
$$((a\mathscr{R}c) \quad \text{et} \quad (c\mathscr{R}d)) \Rightarrow a\mathscr{R}d,$$
et
$$((b\mathscr{R}a) \quad \text{et} \quad (a\mathscr{R}b)) \Rightarrow (b\mathscr{R}b),$$
alors $\mathscr{R}$ est transitive.

Exercice 3.2 *On définit dans* $]0, +\infty[$ *la relation* $\mathscr{S}$ *comme suit*

$$a_1 \mathscr{S} a_2 \Leftrightarrow a_1 \ln a_2 = a_2 \ln a_1.$$

Prouver que $\mathscr{S}$ *est une relation d'équivalence.*

Solution. Nous avons dans $]0, +\infty[$,

$$a_1 \mathscr{S} a_2 \Leftrightarrow \frac{\ln a_1}{a_1} = \frac{\ln a_2}{a_2} \Leftrightarrow h(a_1) = h(a_2),$$

avec h est la fonction de $]0, +\infty[$ dans $\mathbb{R}$ définie par $h(a) = \frac{\ln a}{a}$ et de classe $\mathscr{C}^\infty$ sur son intervalle de définition.
Par suite, la relation d'équivalence associée à h est $\mathscr{S}$.

Exercice 3.3 *Étant donnée la relation $\mathscr{R}$ définie sur $\mathbb{R}^2$ par*

$$(a_1, a_2)\mathscr{R}(a_1', a_2') \Leftrightarrow a_1 + a_2 = a_1' + a_2'$$

1) Vérifier que $\mathscr{R}$ est une relation d'équivalence.
2) Déterminer la classe d'équivalence du (0,0).
3) On définit l'application

$$\begin{array}{rcl} h: \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ (a,b) & \longmapsto & a+b. \end{array}$$

Prouver que les éléments qui ont des images non identiques par h , ne sont pas équivalents modulo $\mathscr{R}$ et les éléments qui ont des images identiques par h, sont équivalents modulo $\mathscr{R}$
4) Préciser la bijection h' qui existe entre l'ensemble quotient $\mathbb{R}^2/\mathscr{R}$ et $\mathbb{R}$.

Solution. 1) Étant donnés $(a,b),(a',b'),(a'',b'')$ des éléments de $\mathbb{R}^2$, on a $a+b=a+b$ autrement dit $(a,b)\mathscr{R}(a,b)$ par suite $\mathscr{R}$ est réflexive. D'autre part, $a+b=a'+b' \Rightarrow a'+b'=a+b$, donc $\mathscr{R}$ est symétrique.
$((a+b=a'+b') \quad \text{et} \quad (a'+b'=a''+b'')) \Rightarrow a+b=a''+b''$, par suite, $\mathscr{R}$ est une relation d'équivalence.
2) L'ensemble

$$\overline{(0,0)} = \{(a,b) \in \mathbb{R}^2 : a+b=0\}$$

est la classe d'équivalence du couple (0,0) n'est autre que l'ensemble des points éxistant sur la deuxième bissectrice du plan xOy.
3) Etant donnés a, b dans $\mathbb{R}^2$. Alors,

$$a\mathscr{R}b \Leftrightarrow h(a) = h(b).$$

4.On note par h' l'application qui pour toute classe fait correspondre la somme des composants d'un représentant quelconque de cette classe. On déduit l'injectivité de cette application de la troisième question.
D'autre part, en admettant que $(\frac{\lambda}{2}, \frac{\lambda}{2}) \in \mathbb{R}^2$ est l'antécédent de λ, avec $\lambda \in \mathbb{R}$, on obtient la surjectivité de h'. Par suite h' est bijective.

Exercice 3.4 *Étant donné $\mathscr{R}$ une relation pré-ordre définie sur un ensemble A , autrement dit qu'elle est réflexive et transitive et on définit la relation binaire $\mathscr{R}'$ sur A par*

$$\forall (a_1, a_2) \in \mathrm{A} \times \mathrm{A}) \quad [a_1 \mathscr{R}' a_2 \Leftrightarrow a_1 \mathscr{R} a_2 \quad et \quad a_2 \mathscr{R} a_1].$$

Prouver que $\mathscr{R}'$ est une relation d'équivalence.

Solution. Réflexivité : de la réflexivité de $\mathscr{R}$, nous avons pour tout élément $a_1 \in \mathrm{A}$, $a_1 \mathscr{R} a_1$, d'où $a_1 \mathscr{R}' a_1$ et donc $\mathscr{R}'$ est réflexive.
Symétrie : Soient $(a_1, a_2) \in \mathrm{A} \times \mathrm{A}$, tels que $a_1 \mathscr{R}' a_2$ ce qui est équivaut à

$$a_1 \mathscr{R} a_2 \quad et \quad a_2 \mathscr{R} a_1$$

qu'on peut réécrire en utilisant les propriétés de la conjonction

$$a_2 \mathscr{R} a_1 \quad et \quad a_1 \mathscr{R} a_2$$

ce qui signifie $a_2 \mathscr{R}' a_1$.
Transitivité : Soient $(a_1, a_2, a_3) \in \mathrm{A} \times \mathrm{A} \times \mathrm{A}$ tels que

$$a_1 \mathscr{R}' a_2 \quad et \quad a_2 \mathscr{R}' a_3,$$

ce qui équivaut à

$$a_1 \mathscr{R} a_2 \quad et \quad a_2 \mathscr{R} a_1$$

et

$$a_2 \mathscr{R} a_3 \quad et \quad a_3 \mathscr{R} a_2.$$

Comme $\mathscr{R}$ est transitive, on obtient

$$a_1 \mathscr{R} a_3 \quad et \quad a_3 \mathscr{R} a_1$$

ce qui montre que $\mathscr{R}'$ est transitive. On en déduit que $\mathscr{R}'$ est une relation d'équivalence.

7.2 Exercices sur les relations d'ordre

Exercice 3.5 *On définit dans* $\mathbb{N} \times \mathbb{N}$ *la relation* $<$ *par*

$$\forall (x,y) \in \mathbb{N}^2, \quad \forall (x',y') \in \mathbb{N}^2 \quad (x,y) < (x',y') \Leftrightarrow x \leq x' et y \leq y'.$$

1. Vérifier que cette relation est une relation d'ordre. Étudier si l'ordre est total ?
2. Etant donné $X = \{(6,7),(7,8),(8,6),(8,7),(8,9),(9,8),(9,9),(10,10)\}$. *Préciser des minorants de X, des majorants de X.*
Existe il un plus grand élément ? Un plus petit élément ? Une borne supérieure ? Une borne inférieure ? dans l'ensemble X.

Solution. 1. Soient $(x,y) \in \mathbb{N}^2$, on a $x \leq x$ et $y \leq y$, et donc $(x,y) < (x,y)$, d'où la relation $<$ est réflexive.
Soient $(x,y) \in \mathbb{N}^2$, $(x',y') \in \mathbb{N}^2$, on a $(x,y) < (x',y')$ et $(x',y') < (x,y)$, donc $(x,y) = (x',y')$. Par suite, La relation $<$ est antisymétrique.
Soient $(x,y) \in \mathbb{N}^2$, $(x',y') \in \mathbb{N}^2$, $(x'',y'') \in \mathbb{N}^2$, si $(x,y) < (x',y')$ et $(x',y') < (x'',y'')$, de plus, $a \leq x' et x' \leq x''$, on obtient $x \leq x''$, puis d'une manière similaire $y \leq y''$. On trouve $(x,y) < (x'',y'')$. Par conséquent, $<$ est une relation d'ordre.
Cet ordre n'est pas total, car par exemple $(6,7)$ et $(7,6)$ ne sont pas comparables pour $<$.
2. On a tout élément (x,y) de X satisfait $(x,y) < (10,10)$ et $(10,10)$ est un élément de X. Donc, le plus grand élément de X est $(10,10)$, il est aussi la borne supérieure de X. Supposons que (x,y) est un minorant de X, de $(x,y) < (6,7)$, alors $x \leq 6$; de $(x,y) < (8,6)$, on obtient $y \leq 6$; d'où $(x,y) < (6,6)$.
Inversement, tout élément (x,y) tel que $(x,y) < (6,6)$ est un minorant de X. Donc, l'ensemble

$$Y = \{(x,y) \in \mathbb{N}^2; x \leq 6, y \leq 6\}$$

représente l'ensemble des minorants de X. X n'admet pas de plus petit élément car aucun élément de X n'appartient à ensemble Y.
La borne inférieure de X est $(6,6)$ car ce dernier majore Y.

Exercice 3.6 *On définit dans* $\mathbb{N}^*$ *la relation* $\leq$ *par*

$$\forall a_1, a_2 \in \mathbb{N}^* \quad a_1 \leq a_2 \Leftrightarrow (\exists l \in \mathbb{N}^*), a_2 = l.a_1.$$

1. Vérifier que $\leq$ *est une relation d'ordre. L'ordre est -il total ?*
2. $\mathbb{N}^*$ *admet -il un plus grand élément ou un plus petit élément ?*

Solution. 1.i. Réflexivité : pour tout $a_1 \in \mathbb{N}^*, \exists l \in \mathbb{N}^*, l = 1$ tel que $a_1 = l.a_1$. D'ou

$$\forall a_1 \in \mathbb{N}^*, a_1 \leq a_1.$$

Par suite la relation est réflexive.
ii. Antisymétrie : Soient $a_1 \in \mathbb{N}^*, a_2 \in \mathbb{N}^*$ tels que $a_1 \leq a_2$ et $a_2 \leq a_1$.

$$\begin{aligned} a_1 \leq a_2 \wedge a_2 \leq a_1 &\Leftrightarrow (\exists l \in \mathbb{N}^*, a_2 = l.a_1) \wedge (\exists l' \in \mathbb{N}^*, a_1 = l'.a_2) \\ &\Rightarrow (\exists l \in \mathbb{N}^*, a_2 = l.a_1) \wedge (\exists l' \in \mathbb{N}^*, a_1 = l'.a_2) \wedge (a_2 = l.l'.a_2) \\ &\Rightarrow (\exists l \in \mathbb{N}^*, a_2 = l.a_1) \wedge (\exists l' \in \mathbb{N}^*, a_1 = l'.a_2) \wedge (l.l' = 1, \quad \text{car} \quad a_2 \neq 0) \\ &\Rightarrow a_2 = a_1 \quad \text{car} \quad \forall l, l' \in \mathbb{N}^*, (l.l' = 1 \Rightarrow l = l' = 1) \end{aligned}$$

donc

$$\forall a_1, a_2 \in \mathbb{N}^* \quad (a_1 \leq a_2 \wedge a_2 \leq a_1) \Rightarrow a_2 = a_1$$

par suite, la relation est antisymétrique.
iii. Transitivité. Soient $a_1 \in \mathbb{N}^*, a_2 \in \mathbb{N}^*, a_3 \in \mathbb{N}^*$ tels que $a_1 \leq a_2$ et $a_2 \leq a_3$.

$$\begin{aligned} a_1 \leq a_2 \wedge a_2 \leq a_3 &\Leftrightarrow (\exists l \in \mathbb{N}^*, a_2 = l.a_1) \wedge (\exists l' \in \mathbb{N}^*, a_3 = l'.a_2) \\ &\Rightarrow (\exists l_1 \in \mathbb{N}^*, l_1 = l'l, a_3 = l_1.a_1) \\ &\Rightarrow a_1 \leq a_3. \end{aligned}$$

D'où la relation est transitive. On en déduit que la relation est une relation d'ordre.
En considérant $a_1 = 7$ et $a_2 = 8$, on remarque que ces deux chiffres ne sont pas comparables (aucun des deux ne divise l'autre), par suite l'ordre n'est pas total.
2. I. On remarque que

$$\forall a \in \mathbb{N}^*, \exists l = a \in \mathbb{N}^*, \quad a = l.1$$

donc

$$\forall a \in \mathbb{N}^*, \quad 1 \leq a.$$

Dans ce ca, on peut dire que 1 est le plus petit élément de $\mathbb{N}^*$.
II. Comme

$$\forall a \in \mathbb{N}^*, \exists b = 2a \in \mathbb{N}^*, \quad a \leq b.$$

Donc, $\mathbb{N}^*$ n'a pas de plus grand élément.

Exercice 3.7 *On définit la relation $\mathcal{S}$ dans $\mathbb{R}^2$ par*

$$(a_1, b_1)\mathcal{S}(a_2, b_2) \Leftrightarrow a_1 \geq a_2 \wedge b_1 \geq b_2.$$

1. Vérifier que $\mathcal{S}$ est une relation d'ordre.
2. Étudier la totalité de la relation $\mathcal{S}$ sur $\mathbb{R}^2$?

Solution. 1. Soit $(a_1, b_1) \in \mathbb{R}^2$. On a

$$a_1 \geq a_1 \wedge b_1 \geq b_1$$

donc $(a_1, b_1)\mathcal{S}(a_1, b_1)$. Par suite, $\mathcal{S}$ est réflexive.
Étant donnés les deux éléments $(a_1, b_1) \in \mathbb{R}^2, (a_2, b_2) \in \mathbb{R}^2$. On a

$$\begin{aligned} (a_1, b_1)\mathcal{S}(a_2, b_2) \wedge (a_2, b_2)\mathcal{S}(a_1, b_1) &\Leftrightarrow [a_1 \geq a_2 \wedge b_1 \geq b_2] \wedge [a_2 \geq a_1 \wedge b_2 \geq b_1] \\ &\Rightarrow a_1 = a_2 \wedge b_1 = b_2 \\ &\Rightarrow (a_1, b_1) = (a_2, b_2). \end{aligned}$$

d'où la relation est antisymétrique.
Étant donnés $(a_1,b_1)\in\mathbb{R}^2,(a_2,b_2)\in\mathbb{R}^2,(a_3,b_3)\in\mathbb{R}^2$, car

$$\begin{aligned}(a_1,b_1)\mathscr{S}(a_2,b_2)\wedge(a_2,b_2)\mathscr{S}(a_3,b_3) &\Leftrightarrow [a_1\geq a_2\wedge b_1\geq b_2]\wedge[a_2\geq a_3\wedge b_2\geq b_3]\\ &\Rightarrow a_1\geq a_3\wedge b_1\geq b_3\\ &\Rightarrow (a_1,b_1)\mathscr{S}(a_3,b_3).\end{aligned}$$

D'où, la relation $\mathscr{S}$ est d'ordre.
2. $\mathscr{S}$ n'est pas totale sur $\mathbb{R}^2$ car à titre d'exemple $(2,6)$ et $(8,5)$ ne sont pas comparables.

Exercice 3.8 *Étant donné $\mathscr{B}$ l'ensemble des relations binaires entre éléments d'un ensemble A et S et S' deux relations de $\mathscr{B}$. S est dite contenue dans S' et on note* $S\subset S'$ *si*

$$(\forall(a,b)\in A\times A)\quad [aSb\Rightarrow aS'b].$$

Prouver que la relation $(\subset)$ *est une relation d'ordre dans $\mathscr{B}$.*

Solution.i. Soient $(a,b)\in A\times A$, $S\in\mathscr{B}$, on a $[aSb\Rightarrow aSb]$ donc $S\subset S$. D'où, la relation est réflexive.
ii. Soient $(a,b)\in A\times A$. Supposons $S\in\mathscr{B}$, $S'\in\mathscr{B}$ telles que $S\subset S'$ et $S'\subset S$. On a

$$([aSb\Rightarrow aS'b]et[aS'b\Rightarrow aSb]).$$

Donc,

$$(\forall(a,b)\in A\times A)\quad [aSb\Leftrightarrow aS'b]$$

donc $S=S'$. Par suite la relation est antisymétrique.
iii. Soient $(a,b)\in A\times A$,$S\in\mathscr{B}$, $S'\in\mathscr{B}$ et $S''\in\mathscr{B}$ telle que $S\subset S'$ et $S'\subset S''$, alors :

$$(\forall(a,b)\in A\times A)\quad ([aSb\Rightarrow aS'b]et[aS'b\Rightarrow aS''b]).$$

En utilisant la transitivité de l'implication, on obtient

$$(\forall(a,b)\in A\times A)\quad ([aSb\Rightarrow aS''b]),$$

autrement dit $S\subset S''$. On conclue que la relation d'inclusion $(\subset)$ est une relation d'ordre dans $\mathscr{B}$.

Exercice 3.9 *Étant donnés* $(A,\leq)$ *un ensemble totalement ordonné et* A_1 *et* A_2 *deux parties qui possèdent des bornes inférieures et supérieures. Prouver que*
1. $\sup(A_1\cup A_2)=\max\{\sup A_1,\sup A_2\}$,
2. $\inf(A_1\cup A_2)=\min\{\inf A_1,\inf A_2\}$.

Solution.1. Admettons $L=max\{\sup A,\sup B\}$ et $l=\min\{\inf A,\inf B\}$. Donc,

$$\begin{aligned}\forall a(a\in(A_1\cup A_2) &\Rightarrow [(a\in A_1)\vee(a\in A_2)]\\ &\Rightarrow (a\leq\sup A_1)\vee(a\leq\sup A_2)\\ &\Rightarrow (a\leq L)\vee(a\leq L)\\ &\Rightarrow (a\leq L).\end{aligned}$$

D'où L est un majorant de $A_1\cup A_2$.
Il reste à montrer que L est le plus petit des majorants de $A_1\cup A_2$. Supposons L' un majorant de $A_1\cup A_2$, alors L' est un majorant de A_1 et de A_2, donc

$$(\sup A_1\leq L')\wedge(\sup A_2\leq L').$$

D'où

$$L=\max\{\sup A_1,\sup A_2\}\leq L'$$

Par suite $L=\sup(A_1\cup A_2)$.
La démonstration de la deuxième question est similaire.

8 Exercices proposés

Exercice 3.10 *Étudier la réflexibilité, la symétrie et la transitivité des relations suivantes :*
1) La relation "$\perp$" définie sur l'ensemble des droites d'un plan.
2) La relation $x^3 + 2x = y^3 + 2y$ dans l'ensemble $\mathbb{Z}$.

Exercice 3.11 *Étant donnée la relation $\mathcal{S}$ définie sur $\mathbb{R}_+^*$ par*

$$a_1 \mathcal{S} a_2 \Leftrightarrow a_1.a_2 > 0.$$

1. Vérifier que $\mathcal{S}$ est une relation d'équivalence.
2. Donner la classe d'équivalence de 10.

Exercice 3.12 *Étant donnée $\mathcal{S}$ une relation d'équivalence définie sur un ensemble non vide A. Prouver que l'ensemble quotient $\mathrm{A}/\mathcal{S}$ est une partition de A.*

Exercice 3.13 *Considérons $(\mathrm{H}, \leq)$ un ensemble totalement ordonné et H_1 et H_2 deux parties de H. Supposons que les bornes inférieures et supérieures de H_1 et H_2 existent. Montrer 1.* $\sup(\mathrm{H}_1 \cap \mathrm{H}_2) = \min\{\sup \mathrm{H}_1, \sup \mathrm{H}_2\}$, *2.* $\max\{\inf \mathrm{H}_1, \inf \mathrm{H}_2\} = \inf(\mathrm{H}_1 \cap \mathrm{H}_2)$.

Exercice 3.14 *Étant donnés $\mathrm{H} = \{h_1, h_2, h_3, h_4, h_5\}$, $\mathcal{S}$ une relation d'ordre définie sur H telle que*

$$h_1 \mathcal{S} h_2,\ h_1 \mathcal{S} h_3,\ h_1 \mathcal{S} h_4, h_2 \mathcal{S} h_5,\ h_3 \mathcal{S} h_5$$

et $\mathrm{H}_1 = \{h_2, h_3\}, \mathrm{H}_2 = \{h_2, h_4\}, \mathrm{H}_3 = \{h_1, h_2, h_5\}$.

Trouver l'ensemble des majorants dans H, la borne supérieure et le plus grand élément de chacune des parties $\mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_3$ s'ils existent.

Chapitre 4

Structures algébriques

1 Introduction

Le but de ce chapitre est de définir les structures algébriques usuelles (groupes, anneaux, corps). Ces structures sont une formulation des propriétés classiques des ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{R}^n$ munis de leurs opérations usuelles + et −, propriétés que nous supposerons connues.
Ce chapitre est basé sur les références ([1],[2],[3], [4], [6], [10],[8], [9], [10], [11], [12]).

2 Lois de composition interne

2.1 Généralités

Définition 4.1 *[1], [3], [6],[9], [11] Étant donné A un ensemble non vide. Toute application de* $\mathrm{A}\times\mathrm{A}$ *dans A*

$$\begin{array}{rcl} \star : \mathrm{A}\times\mathrm{A} & \longrightarrow & \mathrm{A} \\ (a_1, a_2) & \longmapsto & a_1 \star a_2. \end{array}$$

est appelée loi de composition interne dans A.
Si A_1 *est un sous ensemble de A satisfaisant*

$$\forall a, b, \in \mathrm{A}_1,\ a\star b \in \mathrm{A}_1,$$

alors on dit que A_1 *est stable par rapport à la loi* $\star$.

Exemple 4.1 *1. L'addition et la multiplication dans* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
2. La soustraction dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
3. La division dans $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{R}_+^*$, $\mathbb{C}^*$.
4. Si A est un ensemble, alors l'intersection $\cap$ *et la réunion* $\cup$ *sont deux lois de composition internes dans* $\mathscr{P}(\mathrm{A})$.
5. La composition des applications notée "o" est une loi de composition interne dans l'ensemble des applications d'un ensemble dans lui même.
6.Dans l'ensemble des entiers naturels impaires, l'addition n'est pas interne en effet : si $a_1 = 2p_1 + 1$ *et* $a_2 = 2p_2 + 1$ *avec* $(p_1, p_2) \in \mathbb{N}^2$ *alors,* $a_1 + a_2 = 2(p_1 + p_2 + 1)$ *n'est pas impair.*
7. Considérons la loi $\star$ *qui est définie sur* $\mathbb{N}^*$ *par*

$$a_1 \star a_2 = a_1 + a_2 - 4.$$

Cette loi n'est pas interne dans $\mathbb{N}^*$ *car pour* $a_1 = a_2 = 2$, *on obtient* $a\star a_2 = a_1 + a_2 - 4 = 0 \notin \mathbb{N}^*$.

Exemple 4.2 *Considérons* $A = \{\{a_1, a_2\}, \{a_1, a_3\}, \{a_2, a_3\}\} \subset \mathscr{P}(\{a_1, a_2, a_3\})$. *On remarque que*

$$\exists A_1 = \{a_1, a_2\}, A_2 = \{a_1, a_3\};\ A_1 \cap A_2 = \{a_1\} \notin A \text{ et } A_1 \cup A_2 = \{a_1, a_2, a_3\} \notin A$$

donc A n'est pas stable par rapport à l'intersection et la réunion.

Notation

Les lois de composition sont généralement notées par $\perp, \star, \blacktriangle, \top, +, ., o$, ...

Définition 4.2 *[1], [3], [6],[9], [11] Soient* $\star$, $\blacktriangle$ *deux lois de composition internes dans un ensemble A.*
1. $\star$ *est dite commutative si et seulement si*

$$\forall (a_1, a_2) \in A^2, a_1 \star a_2 = a_2 \star a_1.$$

2. $\star$ *est dite associative si et seulement si*

$$\forall (a_1, a_2, a_3) \in A^3, (a_1 \star a_2) \star a_3 = a_1 \star (a_2 \star a_3).$$

3. $\star$ *est dite distributive par rapport à* $\blacktriangle$ *si est seulement si*

$$\forall (a_1, a_2, a_3) \in A^3, a_1 \star (a_2 \blacktriangle a_3) = (a_1 \star a_2) \blacktriangle (a_1 \star a_3).$$

et

$$(a_2 \blacktriangle a_3) \star a_1 = (a_2 \star a_1) \blacktriangle (a_3 \star a_1).$$

4. $e_A \in A$ *est dit un élément neutre à gauche de la loi* $\star$ *si*

$$\forall a_1 \in A,\ e_A \star a_1 = a_1,$$

$e_A \in A$ *est dit un élément neutre à droite de la loi* $\star$ *si*

$$\forall a_1 \in A,\ a_1 \star e_A = a_1.$$

Si e_A *est un élément neutre à droite et à gauche de la loi* $\star$ *, on dit que* e_A *est un élément neutre de* $\star$.

Exemple 4.3 *1. Dans* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, *l'addition est une loi commutative, associative , elle admet un élément neutre 0.*
2. Si A est un ensemble, alors l'intersection $\cap$ *et la réunion* $\cup$ *sont deux lois de composition internes associatives, commutatives dans* $\mathscr{P}(A)$.
$\emptyset$ *est l'élément neutre de* $\cup$.
A est l'élément neutre de $\cap$.
$\cap$ *est distributive par rapport à* $\cup$ *et* $\cup$ *est distributive par rapport à* $\cap$.
3. La soustraction dans $\mathbb{C}$ *n'est pas commutative.*

Proposition 4.1 *[3] Étant donnés A un ensemble non vide muni d'une loi interne* $\star$, e_1 *un élément neutre à droite de* $\star$ *et* e_2 *un élément neutre à gauche , alors* $e_1 = e_2$. *Dans ce cas, on dit que* $e_1 = e_2$ *est l'élément neutre de* $\star$.

Preuve. Supposons que e_1 est un élément neutre à droite de $\star$ et que e_2 un élément neutre à gauche de $\star$. Comme e_2 est un élément neutre à gauche de $\star$, on a

$$e_1 = e_2 \star e_1$$

et comme e_1 est un élément neutre à droite de $\star$, on a

$$e_2 = e_2 \star e_1.$$

Alors, $e_1 = e_2$. ■

Remarque 4.1 *On déduit de la proposition précédente que la loi $\star$ admet un élément neutre unique.*

Définition 4.3 *[1], [3], [6],[9], [11] Soit A un ensemble non vide muni d'une loi interne $\star$ admettant un élément neutre e_A. Un élément $a_1 \in A$ est dit un élément symétrisable (ou admet un symétrique) s'il existe un élément a_2 dans A vérifiant*

$$a_1 \star a_2 = a_2 \star a_1 = e_A.$$

a_2 est appelé le symétrique de a_1 par rapport à $\star$, noté $-a_1$.

Exemple 4.4 *1. Dans $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, chaque élément a_1 admet un symétrique $(-a_1)$ pour l'addition.*
2. Dans $\mathscr{P}(E)$, toute partie différente de E n'a pas de symétrique pour la loi "intersection" car

$$\forall A \in \mathscr{P}(E), \nexists B \in \mathscr{P}(E), A \cap B = E$$

Remarque 4.2 *Le symétrique d'un élément n'est pas toujours unique.*

Exemple 4.5 *On définit dans l'ensemble $A = \{\alpha, \beta, \gamma\}$ la loi de composition interne par*

▲	α	β	γ
α	α	β	γ
β	β	γ	α
γ	γ	α	α

On a : 1. α est l'élément neutre de ▲,
2. α est le symétrique de α,
3. γ est le symétrique de β,
4. β et γ sont des symétriques de γ.

Proposition 4.2 *[3] Considérons A un ensemble non vide muni d'une loi interne $\star$ admettant un élément neutre e_A telle que cette loi est associative. Supposons que a est un élément de A symétrisable par $\star$, alors son symétrique est unique.*

Preuve. Soient $a \in A$ et a_1 et a_2 sont des symétriques de a. On a

$$\begin{aligned} a_1 &= a_1 \star e_A \\ &= a_1 \star (a \star a_2) \\ &= (a_1 \star a) \star a_2 \\ &= e_A \star a_2 = a_2. \end{aligned}$$

■

Exemple 4.6 *Dans l'exemple 4.5, l'élément* γ *admet deux symétriques et la loi n'est pas associative car*

$$(\beta \blacktriangle \beta) \blacktriangle \gamma = \gamma \blacktriangle \gamma = \alpha$$

et

$$\beta \blacktriangle (\beta \blacktriangle \gamma) = \beta \blacktriangle \alpha = \beta.$$

On déduit donc que l'associativité de la loi assure l'unicité du symétrique.

3 Groupes

Définition 4.4 *[1], [3], [6],[9], [11] Étant donné A un ensemble non vide muni d'une loi interne* $\star$. $(A, \star)$ *est dit un groupe si la loi* $\star$ *est associative, admet un élément neutre et tout élément de A admet un symétrique.*
Le groupe $(A, \star)$ *est dit groupe commutatif ou abélien si la loi* $\star$ *est commutative.*

Exemple 4.7 *1. Dans* $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$ *sont des groupes abéliens.*
2. $(\mathbb{N}, +)$ *n'a pas une construction d'un groupe.*

Définition 4.5 *Soit* $(A, \blacktriangle)$ *est un groupe fini. Alors le cardinal de A est appelé ordre de A.*

3.1 Sous groupe

Définition 4.6 *[1], [3], [6],[9], [11] Étant donnés* $(A, \blacktriangle)$ *un groupe et* A_1 *une partie non vide de A.* $(A_1, \blacktriangle)$ *est appelé un sous groupe de* $(A, \blacktriangle)$ *si et seulement si la restriction de la loi de A à* A_1 *a une structure de groupe dans* A_1 *, autrement dit*
1. L'élément neutre de A est un élément de A_1 *;*
2. Pour tout $(a_1, a_2) \in {A_1}^2$, $(a_1 \blacktriangle a_2) \in A_1$ *;*
3. Le symétrique de chaque élément de A_1 *est un élément de* A_1.

Exemple 4.8 *1.* $(\mathbb{Z}, +)$ *est un sous groupe de* $(\mathbb{R}, +)$.
2. Supposons que $(A, \blacktriangle)$ *est un groupe, alors* $(A, \blacktriangle)$ *est le plus grand sous groupe de* $(A, \blacktriangle)$ *et* $(\{e_A\}, \blacktriangle)$ *est le plus petit sous groupe de* $(A, \blacktriangle)$.

Proposition 4.3 *[6] Tout sous groupe est un groupe.*

Preuve. Étant donné $(A_1, \blacktriangle)$ un sous groupe de $(A, \blacktriangle)$. En utilisant la définition d'un sous groupe, il suffit de montrer l'associativité de la loi $\blacktriangle$ dans H. Étant donnés a_1, a_2 et a_3 des éléments de A_1, et comme ce dernier est une partie de A, alors ses éléments sont aussi des éléments de A, on a dans ce cas

$$(a_1 \blacktriangle a_2) \blacktriangle a_3 = a_1 \blacktriangle (a_2 \blacktriangle a_3).$$

■

Théorème 4.1 *[6] Étant donnés* $(A, \blacktriangle)$ *un groupe et* A_1 *une partie non vide de A. Alors,* $(A_1, \blacktriangle)$ *est un sous groupe de* $(A, \blacktriangle)$ *si et seulement si* $\forall (a_1, a_2) \in {A_1}^2, (a_1 \blacktriangle (-a_2)) \in A_1$.

Preuve. 1. On suppose que $(A_1, \blacktriangle)$ est un sous groupe de $(A, \blacktriangle)$. Prenons $(a_1, a_2) \in {A_1}^2$, sachant que A_1 est un sous groupe alors, $(-y) \in A_1$ et en utilisant la stabilité de A_1 par la

loi, on obtient $(a_1 \blacktriangle (-a_2)) \in A_1$.
D'autre part, si pour tout $a_1, a_2 \in A_1$, on a

$$(a_1 \blacktriangle (-a_2)) \in A_1. \tag{4.1}$$

Il suffit de montrer que
i. $e \in A_1$.
ii. $-a_2 \in A_1$.
iii. $(a_1 \blacktriangle a_2) \in A_1$.
i. En remplaçant dans (4.1), a_1 par a_2 on trouve $e \in A_1$.
ii. En remplaçant dans (4.1), a_1 par e, on obtient $-a_2 \in A_1$.
iii. Pour a_1 et $-a_2$, on a

$$(a_1 \blacktriangle (-(-a_2))) = (a_1 \blacktriangle a_2) \in A_1.$$

■

Théorème 4.2 *(**Théorème de Lagrange**) [6],[11] Étant donnés* $(A, \star)$ *un groupe du cardinal fini. Si* $(A_1, \star)$ *est un sous groupe de* $(A, \star)$*, alors le cardinal de A est divisible par le cardinal de* A_1.

Proposition 4.4 *[6] Étant donnés* $(A, \blacktriangle)$ *un groupe et* A_1 *et* A_2 *deux sous groupes de* $(A, \blacktriangle)$. *Alors, l'intersection de* A_1 *et* A_2 *muni de la loi* $\blacktriangle$ *est un sous groupe de* $(A, \blacktriangle)$.

Preuve. Montrons que

$$\forall (a_1, a_2) \in (A_1 \cap A_2)^2, (a_1 \blacktriangle - a_2) \in (A_1 \cap A_2).$$

Soient $a_1 \in (A_1 \cap A_2)$ et $a_2 \in (A_1 \cap A_2)$.

$$a_1 \in (A_1 \cap A_2) \text{et} a_2 \in (A_1 \cap A_2) \quad \Rightarrow \quad \begin{cases} a_1 \in A_1 & \text{et} \quad a_1 \in A_2 \\ a_2 \in A_1 & \text{et} \quad a_2 \cap A_2. \end{cases}$$

Le fait que A_1 et A_2 sont des sous groupes, alors

$$(a_1 \blacktriangle (-a_2)) \in A_1 \quad \text{et} \quad (a_1 \blacktriangle (-a_2)) \in A_2.$$

D'où, $(A_1 \cap A_2, \blacktriangle)$ est un sous groupe de $(A, \blacktriangle)$. ■

Remarque 4.3 $(A_1 \cup A_2, \blacktriangle)$ *n'est pas nécessairement un sous groupe de* $(A, \blacktriangle)$.

Exemple 4.9 *Considérons* $A_1 = \{4k, k \in \mathbb{Z}\} = 4\mathbb{Z}$ *est un sous groupe de* $(\mathbb{Z}, +)$ *et* $A_2 = \{5k, k \in \mathbb{Z}\} = 5\mathbb{Z}$ *est un sous groupe de* $(\mathbb{Z}, +)$ *donc, d'après la proposition précédente* $(A_1 \cap A_2, +)$ *est un sous groupe de* $(\mathbb{Z}, +)$.
On a $4 \in A_1$ *et* $5 \in A_2$*, 4 et 5 sont deux éléments de* $(A_1 \cup A_2)$*, mais* $4 + 5 = 9 \notin (A_1 \cup A_2)$.

3.2 Groupe quotient

Proposition 4.5 *[6] Étant donnés* $(A, \star)$ *un groupe et* $(A_1, \star)$ *un sous groupe de* $(A, \star)$. *En définissant dans A la relation* $\mathscr{S}$ *comme suit*

$$\forall (a_1, a_2) \in A^2, (a_1 \mathscr{S} a_2) \Leftrightarrow (a_1 \star (-a_2)) \in A_1,$$

alors relation est une relation d'équivalence.

Preuve. 1. La réflexivité de $\mathscr{S}$.
Si $a_1 \in \mathrm{A}$, on a $a_1 \star (-a_1) = e \in \mathrm{A}_1$, donc $\mathscr{S}$ est réflexive
2 . La symétrie de $\mathscr{S}$.
Si $(a_1, a_2) \in \mathrm{A}^2$,

$$\begin{aligned} a_1 \mathscr{S} a_2 &\Leftrightarrow (a_1 \star (-a_2)) \in \mathrm{A}_1 \\ &\Rightarrow -(a_1 \star (-a_2) \in \mathrm{A}_1 \\ &\Rightarrow (a_2 \star -a_1) \in \mathrm{A}_1 \\ &\Rightarrow a_2 \mathscr{S} a_1 \end{aligned}$$

3. La transitivité de $\mathscr{S}$.
Si $(a_1, a_2, a_3) \in \mathrm{A}^3$,

$$\begin{aligned} a_1 \mathscr{S} a_2 \quad \text{et} \quad a_2 \mathscr{S} a_3 &\Rightarrow (a_1 \star (-a_2)) \in \mathrm{A}_1 \quad \text{et} \quad (a_2 \star (-a_3)) \in \mathrm{A}_1 \\ &\Rightarrow ((a_1 \star (-a_2)) \star (a_2 \star (-a_3))) \in \mathrm{A}_1 \\ &\Rightarrow (a_1 \star (-a_3)) \in \mathrm{A}_1 \\ &\Rightarrow a_1 \mathscr{S} a_3. \end{aligned}$$

■

Remarque 4.4 *Pour tout $a \in \mathrm{A}$, on a*

$$\begin{aligned} \overline{a} &= \{a_1 \in \mathrm{A}, a_1 \mathscr{S} a\} \\ &= \{a_1 \in \mathrm{A}, a_1 \star (-a) \in \mathrm{A}_1\} \\ &= \{a_1 \in \mathrm{A}, \exists h \in \mathrm{A}_1, h = a_1 \star (-a)\} \\ &= \{a_1 \in \mathrm{A}, \exists h \in \mathrm{A}_1, a_1 = h \star a\} \\ &= \{h \star a, h \in \mathrm{A}\} = \mathrm{A}_1 \star a \end{aligned}$$

On peut définir dans l'ensemble quotient $\mathrm{A}/\mathscr{S} = \mathrm{A}/\mathrm{A}_1$ la loi interne $\overline{\star}$ comme suit

$$\overline{a} \quad \overline{\star} \quad \overline{b} = \overline{a \star b}$$

satisfaisant les propriétés suivantes : commutativité, associativité, admet un élément neutre $\overline{e}$ et l'inverse de chaque élément $\overline{a}$ est $\overline{-a}$. Par suite $(\mathrm{A}/\mathrm{A}_1, \overline{\star})$ est un groupe commutatif appelé groupe quotient.

Exemple 4.10 *Étant donné $m \in \mathbb{N}^*$; alors*

$$m\mathbb{Z} = \{mz, z \in \mathbb{Z}\}$$

est un sous groupe de $\mathbb{Z}$, et la relation "...est congru à...modulo...m" définie par

$$(\forall (a_1, a_2) \in \mathbb{Z}^2, a_1 \equiv a_2 [m]) \Leftrightarrow m \diagup (a_1 - a_2)$$

est une relation d'équivalence. La classe d'équivalence d'un élément $a_1 \in \mathbb{Z}$ est donnée par

$$\overline{a} = \{a_1 + km, k \in \mathbb{Z}\}.$$

L'ensemble des classes d'équivalence est donnée par

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$$

On a $(\mathbb{Z}/m\mathbb{Z}, \overline{+})$ *est un groupe commutatif. En effet*
1. $\overline{+}$ *est interne dans* $(\mathbb{Z}/m\mathbb{Z})$.
2. $\forall (a_1, a_2, a_3) \in \mathbb{Z}^3$,

$$\begin{aligned}(\overline{a_1}\,\overline{+}\,\overline{a_2})\,\overline{+}\,\overline{a_3} &= \overline{a_1 + a_2}\,\overline{+}\,\overline{a_3} \\ &= \overline{(a_1 + a_2) + a_3} \\ &= \overline{a_1 + (a_2 + a_3)} \\ &= \overline{a_1}\,\overline{+}\,\overline{a_2 + a_3} \\ &= \overline{a_1}\,\overline{+}\,(\overline{a_2}\,\overline{+}\,\overline{a_3})\end{aligned}$$

Donc $\overline{+}$ *est associative.*
3. $\forall (a_1, a_2) \in \mathbb{Z}^2$,

$$\begin{aligned}(\overline{a_1}\,\overline{+}\,\overline{a_2}) &= \overline{a_1 + a_2} \\ &= \overline{a_2 + a_1} \\ &= \overline{a_2}\,\overline{+}\,\overline{a_1}\end{aligned}$$

Donc $\overline{+}$ *est commutative.*
4. $\forall a_1 \in \mathbb{Z}$,

$$\begin{aligned}(\overline{a_1}\,\overline{+}\,\overline{0}) &= \overline{a_1 + 0} \\ &= \overline{a_1}\end{aligned}$$

donc $\overline{0}$ *est un élément neutre pour* $\overline{+}$.
5. $\forall a_1 \in \mathbb{Z}$,

$$\begin{aligned}(\overline{a_1}\,\overline{+}\,\overline{-a}) &= \overline{a_1 + (-a)} \\ &= \overline{0}\end{aligned}$$

donc tout élément de $(\mathbb{Z}/m\mathbb{Z})$ *admet un élément symétrique* $\overline{-a}$ *e pour* $\overline{+}$. *On en déduit que* $(\mathbb{Z}/m\mathbb{Z}, \overline{+})$ *est un groupe commutatif.*

Exercice 4.1 *Déterminer tous les sous groupes de* $(\mathbb{Z}/3\mathbb{Z}, \overline{+})$.
On a $\mathbb{Z}/3 = \{\overline{0}, \overline{1}, \overline{2}\}$ *avec*
$\overline{0} = \{3k, k \in \mathbb{Z}\}$,
$\overline{1} = \{3k+1, k \in \mathbb{Z}\}$,
$\overline{2} = \{3k+2, k \in \mathbb{Z}\}$. *On peut vérifier que* $(\mathbb{Z}/3\mathbb{Z}, \overline{+})$ *est un groupe commutatif en utilisant le tableau de Pythagore*

$\overline{+}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Supposons que A_1 est un sous groupe de $(\mathbb{Z}/3\mathbb{Z}, \overline{+})$, d'après le théorème de Pythagore, le cardinal de A_1 divise le cardinal de $\mathbb{Z}/3\mathbb{Z}$, c'est à dire que $card A_1 = 1$ ou $card A_1 = 3$. Alors $A_1 = \{\overline{0}\}$ ou bien $A_1 = \{\overline{0}, \overline{1}, \overline{2}\} = \mathbb{Z}/3\mathbb{Z}$.

3.3 Morphismes de Groupes

Définition 4.7 *[6], [11] Étant donnés* $(A,\star)$ *et* $(A',\bullet)$ *deux groupes. Une application* $h : A \to A'$ *est appelée morphisme (ou encore homomorphisme) de groupes si et seulement si*

$$\forall a_1, a_2 \in A,\ h(a_1 \star a_2) = h(a_1) \bullet h(a_2).$$

Si h *est bijective,* h *est dite un isomorphisme de groupes. Alors, que* A *est dit isomorphe à* A'*, ou que* A *et* A' *sont isomorphes.*
Si $A = A'$*, on dit que* h *est un endomorphisme de* A*, et si de pus* h *est bijective, on dit que* H *est un automorphisme de groupes de* E*.*

Exemple 4.11 *Considérons les deux applications suivantes*

$$\begin{array}{rccc} h_1 : & (\mathbb{R}_+^*, .) & \longrightarrow & (\mathbb{R}, +) \\ & a & \longmapsto & b = \ln a. \end{array}$$

$$\begin{array}{rccc} h_2 : & (\mathbb{R}, +) & \longrightarrow & (\mathbb{R}_+^*, .) \\ & a & \longmapsto & b = \exp a. \end{array}$$

Nous avons

$$\ln(a_1.a_2) = \ln a_1 + \ln a_2$$

et

$$\exp(a_1 + a_2) = \exp a_1 . \exp a_2$$

Alors, h_1 *et* h_2 *sont des morphismes.*

Proposition 4.6 *[3], [6] Étant donnés* $h : (A,\star) \to (A',\bullet)$ *un morphisme et* $e_A \in A$ *et* $e'_A \in A'$ *des éléments neutres. Alors,*
1. $h(e_A) = e'_A$.
2. $\forall a \in A,\ h(-a) = -h(a)$.
3. $Imh = h(A)$ *est un sous groupe de A'.*
4. $\ker h$ *est un sous groupe de A.*

Preuve. 1. Considérons a le symétrique de $h(e_A)$ dans A', alors

$$\begin{array}{rcl} e'_A = & a \bullet h(e_A) & \\ = & a \bullet h(e_A \star e_A) & \\ = & a \bullet h(e_A) \bullet h(e_A) & \\ = & e'_A \bullet h(e_A) & \\ = & h(e_A) & \text{car } e'_A \text{ est l'élément neutre dans A'.} \end{array}$$

2. Soit $a \in A$, on a

$$\begin{array}{rcl} e'_A = & h(e_A) & \\ = & h(a \star (-a)) & \\ = & h(a) \bullet h((-a)) & \end{array}$$

donc, $h(-a) = -h(a)$.
3. En utilisant la définition de $Imh = h(A)$, on a $h(A) \neq \emptyset$ car $\exists e_A \in A, h(e_A) \in h(A)$. Soient maintenant $(b_1, b_2) \in (h(A))^2$. On a

$$(b_1 \in h(A)) \Rightarrow (\exists a_1 \in A : b_1 = h(a_1)$$

et

$$(b_2 \in h(A)) \Rightarrow (\exists a_2 \in A : b_2 = h(a_2).$$

Alors

$$\begin{aligned} b_1 \bullet (-b_2) = & \quad h(a_1) \bullet (-h(a_2)) \\ = & \quad h(a_1 \star (-a_2))) \in h(A). \end{aligned}$$

D'où $Imh = h(A)$ est un sous groupe de A'.
4. $\ker h = \{a \in A, h(a) = e'_A\}$ est un ensemble non vide car $h(e_A) = e'_A$ et donc $e_A \in \ker h$. Considérons a et a' deux éléments de $\ker h$, montrons que $a \star (-a') \in \ker h$, il suffit donc de montrer que $h(a \star (-a')) = e'_A$. On a

$$\begin{aligned} h(a \star (-a')) = & \quad h(a) \bullet h(-a') \\ = & \quad h(a) \bullet (-h(a')) \\ = & \quad e'_A \bullet (-e'_A) = e'_A. \end{aligned}$$

Par suite, $\ker h$ est un sous groupe de A. ■

Exemple 4.12 *Considérons l' application suivante*

$$\begin{array}{rccc} h : & (\mathbb{R}^2, +) & \longrightarrow & (\mathbb{R}, +) \\ & (a, b) & \longmapsto & h(a, b) = a. \end{array}$$

Alors,

$$\begin{aligned} \ker h &= \{(a, b) \in \mathbb{R}^2, h(a, b) = 0\} \\ &= \{(a, b) \in \mathbb{R}^2, a = 0\} \\ &= \{(0, b), b \in \mathbb{R}\} \\ &= \{0\} \times \mathbb{R}. \end{aligned}$$

et

$$\begin{aligned} Imh &= \{h(a, b), (a, b) \in \mathbb{R}^2\} \\ &= \{a, (a, b) \in \mathbb{R}^2\} \\ &= \{a, a \in \mathbb{R}\} \\ &= \mathbb{R}. \end{aligned}$$

D'où, $\ker h$ *et* Imh *sont deux sous groupes de* $(\mathbb{R}^2, +)$ *et* $(\mathbb{R}, +)$ *respectivement.*

4 Anneaux

Définition 4.8 *[6] On appelle anneau, tout ensemble H non vide muni de deux lois de composition internes + et • telles que*
1. $(H, +)$ *construit un groupe abélien (on notera 0 ou* 0_H *l'élément neutre de +),*

2.• est associative et distributive par rapport à +.

3. La loi • possède un élément neutre dans H.

Si de plus, la loi • est commutative, alors $(H,+,\bullet)$ *est dit anneau commutatif.*

Exemple 4.13 *1.* $(\mathbb{R},+,.)$, $(\mathbb{C},+,.)$ *représentent des anneaux abéliens.*
2. $(\mathbb{N},+,.)$ *n'est pas un anneau car il n'est pas un groupe.*

Notation

1. L'élément neutre de la loi • dans l'anneau $(H,+,\bullet)$ est noté souvent 1 ou 1_H.
2.Dans un anneau, un élément est inversible par rapport à la deuxième loi •, on dit qu'il est inversible. L'inverse d'un élément $a \in H$ est noté a^{-1}.
3. On note $H^* = H\backslash\{0_H\}$.
4. Notons pour tout $l \in H^*$

$$nl = l + l + ... + l \quad (n \text{ termes}) \text{ si } n \in \mathbb{N}^*,$$

$$nl = 0 \quad \text{si } n = 0,$$

$$nl = -((-n) \bullet l) \quad \text{si } n \in \mathbb{Z}^*,$$

et

$$l^n = l \bullet l \bullet ... \bullet l \quad (n \text{ termes}).$$

Calcul dans un anneau

Proposition 4.7 *[3], [6] Soit* $(H,+,\bullet)$ *un anneau, alors pour tous* a,b *et* c *dans H,* $n \in \mathbb{Z}$ *et* $n' \in \mathbb{Z}$*, on a*
1. $0_H \bullet a = a \bullet 0_H = 0_H$*, on dit que* 0_H *est un élément absorbant pour la loi • dans H.*
2. $a \bullet (-b) = (-a) \bullet b = -(a \bullet b)$.
3.$1_H \bullet (-b) = (-1_H) \bullet b = -b$.
4.$a \bullet (b-c) = (a \bullet b) - (a \bullet c)$.
5. $(b-c) \bullet a = (b \bullet a) - (c \bullet a)$.
6. $(n+n')a = na + n'a$.
7. $n(-a) = (-n)a = -(na)$.
8. $n(a+b) = na + nb$ *et* $n(a-b) = na - nb$.
9.$n(ab) = (na) \bullet b = a \bullet (nb)$.

Preuve. 1. En utilisant la distributivité de la loi • par rapport à +, on obtient

$$0_H \bullet a = (0_H + 0_H) \bullet a = (0_H \bullet a + 0_H \bullet a)$$

et comme $(0_H \bullet a)$ est un élément symétrisable dans H, on déduit que $0_H \bullet a = 0_H$. De la même technique, on peut montrer que $a \bullet 0_H = 0_H$.
2. Il suffit de montrer que $a \bullet (-b)$ est le symétrique de $(a \bullet b)$. D'après la propriété 1. et la distributivité de la loi • par rapport à +, on a

$$a \bullet (-b) + (a \bullet b) = a \bullet (-b + b) = a \bullet 0_H = 0_H$$

d'où $a \bullet (-b) = -(a \bullet b)$. D'une manière similaire, on prouve que $(-a) \bullet b = -(a \bullet b)$.
3. Il suffit de remplacer dans la propriété 2. a par1_H.

Pour 4. et 5. En utilisant la distributivité de la loi $\bullet$ par rapport à $+$ et la propriété 2. on peut écrire

$$a \bullet (b-c) = (a \bullet b) + a \bullet (-c) = (a \bullet b) - (a \bullet c)$$

et

$$(b-c) \bullet a = (b \bullet a) + (-c \bullet a) = (b \bullet a) - (c \bullet a).$$

6. On a $(n+n')a = \underbrace{a+a+...+a}_{n+n' \text{ terme}} = \underbrace{(a+a+...+a)}_{n \text{ terme}} + \underbrace{(a+a+...+a)}_{n' \text{ terme}} = na + n'a.$

7. On a

$$n(-a)+(na) = \underbrace{(-a+(-a)+...+(-a))}_{n \text{ terme}} + \underbrace{(a+a+...+a)}_{n \text{ terme}} = \underbrace{((-a+a)+(-a+a)+...+(-a+a))}_{n \text{ terme}} = 0_A$$

D'où $n(-a) = -(na)$. De même pour $(-n)a = -(na)$.

8. En utilisant la commutativité de la loi $+$, on obtient

$$n(a+b) = \underbrace{(a+b)+(a+b)+...+(a+b)}_{n \text{ terme}} = \underbrace{(a+a+...+a)}_{n \text{ terme}} + \underbrace{(b+b+...+b)}_{n \text{ terme}} = na + nb$$

et

$$n(a-b) = \underbrace{(a-b)+(a-b)+...+(a-b)}_{n \text{ terme}} = \underbrace{(a+a+...+a)}_{n \text{ terme}} + \underbrace{(-b+(-b)+...+(-b))}_{n \text{ terme}} = na+n(-b)$$

et d'après la propriété 7, on obtient

$$n(a-b) = na - nb.$$

9. L'égalité $n(ab) = (na) \bullet b$ est vraie si $n = 0$, vu 1, elle est vraie si $n > 0$ par distributivité. Si $n < 0$, soit $k = -n$. Alors $na = -(ka)$, donc $(na)b = (-(ka))b = -((ka)b)$, puis $(na)b = -(k(ab)) = (-k)(ab) = n(ab)$. De même pour $a(nb) = n(ab)$. ■

4.1 Diviseur de zéro

Définition 4.9 *[3], [6] Soient* $(H,+,\bullet)$ *un anneau et* $a_1 \in H$.
1. a_1 *est un diviseur de zéro à gauche si et seulement si* $a_1 \neq 0_H$ *et* $\exists a_2 \in H$ *tel que* $a_2 \neq 0_H$ *et* $a_1 \bullet a_2 = 0_H$.
2. a_1 *est un diviseur de zéro à droite si et seulement si* $a_1 \neq 0_H$ *et* $\exists a_3 \in H$ *tel que* $a_3 \neq 0_H$ *et* $a_3 \bullet a_1 = 0_H$.
3.a_1 *est un diviseur de zéro si et seulement si* $a_1 \neq 0_H$ *et* a_1 *est un diviseur de zéro à gauche et à droite dans H.*

Remarque 4.5 *Dans un anneau commutatif, tout diviseur de zéro à gauche est un diviseur de zéro à droite.*

Définition 4.10 *[3], [6] Un anneau* $(H,+,\bullet)$ *est dit intègre s'il est un anneau commutatif distinct de* $\{0_H\}$ *et n'admet aucun diviseur de zéro.*

Exemple 4.14 *1.* $(\mathbb{Z},+,.)$, $(\mathbb{Q},+,.)$, $(\mathbb{R},+,.)$ *et* $(\mathbb{C},+,.)$ *sont des anneaux intègres.*
2. $(\mathbb{R}^2,+,\bullet)$ *où* $+$ *est l'addition habituelle et* $\bullet$ *est la multiplication produit définie par* $(a,b) \bullet (a',b') = (aa',bb')$ *n'est pas intègre, comme* $(0,1) \bullet (1,0) = (0,0)$.

4.2 Sous anneau

Définition 4.11 *[1], [3] Soient* $(H,+,\bullet)$ *un anneau, et* H_1 *une partie non vide de H. On dit que* $(H_1,+,\bullet)$ *est un sous anneau de* $(H,+,\bullet)$ *si et seulement si*
1. $(H_1,+)$ *est un sous groupe de* $(H,+)$
2. Pour tout $(a_1,a_2)\in {H_1}^2, (a_1\bullet a_2)\in H_1$ *;*
3. 1_H *est un élément de* H_1.

Exemple 4.15 *1.* $(\mathbb{Z},+,.)$ *est un sous anneau de* $(\mathbb{R},+,.)$.
2. $(n\mathbb{Z},+,.)$ *est un sous anneau de* $(\mathbb{Z},+,.)$.

Proposition 4.8 *[1], [3] Soient* $(H,+,\bullet)$ *un anneau, et* H_1 *une partie non vide de H.* $(H_1,+,\bullet)$ *est un sous anneau de* $(H,+,\bullet)$ *si et seulement si*
1. $\forall (a_1,a_2)\in {H_1}^2, (a_1-a_2)\in H_1$,
2. $\forall (a_1,a_2)\in {H_1}^2, (a_1\bullet a_2)\in H_1$,
3. $1_H\in H_1$.

Preuve. $\Rightarrow$) En utilisant la définition d'un sous anneau , on obtient 1., 2., 3.
$\Leftarrow$) Supposons que les propriétés 1., 2., 3 sont vérifiées. Alors,

$$0_H=(1_H-1_H)\in H$$

$$\forall a\in H_1, -a=(0_H-a)\in H_1$$

et

$$\forall (a,b)\in {H_1}^2, a+b=a+(-b)\in H_1.$$

On en déduit que $(H_1,+,\bullet)$ est un sous anneau de $(H,+,\bullet)$. ■

4.3 Morphismes d'anneaux

Définition 4.12 *[1], [3] Soient* $(H,+,\bullet)$ *et* $(H',\bigstar,\blacktriangle)$ *deux anneaux. Une application* $h:H\to H'$ *est appelée morphisme (ou encore homomorphisme) d'anneaux si et seulement si*
1. $\forall a_1,a_2\in H,\ f(a_1+a_2)=f(a_1)\bigstar f(a_2)$,
2. $\forall a_1,a_2\in H,\ f(a_1\bullet a_2)=f(a_1)\blacktriangle f(a_2)$,
3. $f(1_H)=1'_H$.

Les morphismes d'anneaux de $(H,+,\bullet)$ dans $(H',+,\bullet)$ sont en particulier des morphismes de groupes de $(H,+)$ dans $(H',+)$. Ils en ont toutes les propriétés et on utilise la même terminologie : isomorphisme, endomorphisme et automorphisme.

Exemple 4.16 *L'application*

$$\begin{array}{rccc} h_1: & (\mathbb{R},+,.) & \longrightarrow & (\mathbb{R},+,.) \\ & a & \longmapsto & h(a)=0. \end{array}$$

on remarque qu'on a pas l'égalité $h(1)=1$. *Donc* h_1 *n'est pas un morphisme d'anneaux. Et l'application*

$$\begin{array}{rccc} h_2: & (\mathbb{Z},+,.) & \longrightarrow & (\mathbb{Z},+,.) \\ & a & \longmapsto & h_2(a)=a. \end{array}$$

est l'unique endomorphisme de $\mathbb{Z}$, *car* h_2 *est un endomorphisme, on a* $h_2(1)=1$ *ce qui entraine par récurrence :*

$$\forall m\in\mathbb{Z}_+, h_2(m)=m$$

puis

$$\forall m\in\mathbb{Z}_-, h_2(m)=-h_2(-m)=-(-m)=m$$

4.4 Anneau quotient $\mathbb{Z}/n\mathbb{Z}$

Proposition 4.9 *[1], [3]* $(\mathbb{Z}/n\mathbb{Z}, \overline{+}, \overline{\cdot})$ *est un anneau commutatif où*

$$\overline{a}\overline{+}\overline{b} = \overline{a+b}$$

et

$$\overline{a}\,\overline{\cdot}\,\overline{b} = \overline{a.b}$$

Preuve. D'après ce qui précède, on sait que $(\mathbb{Z}/n\mathbb{Z}, \overline{+})$ est un groupe commutatif.
1. $\overline{\cdot}$ est interne dans $(\mathbb{Z}/n\mathbb{Z})$.
2. $\forall (a_1, a_2, a_3) \in \mathbb{Z}^3$,

$$\begin{aligned}
(\overline{a_1}\overline{\cdot}\overline{a_2})\overline{\cdot}\overline{a_3} &= \overline{a_1.a_2}\,\overline{\cdot}\,\overline{a_3} \\
&= \overline{(a_1.a_2).a_3} \\
&= \overline{a_1.(a_2.a_3)} \\
&= \overline{a_1}\,\overline{\cdot}\,\overline{a_2.a_3} \\
&= \overline{a_1}\overline{\cdot}(\overline{a_2}\overline{\cdot}\overline{a_3})
\end{aligned}$$

Donc $\overline{\cdot}$ est associative.
3. $\forall (a_1, a_2) \in \mathbb{Z}^2$,

$$\begin{aligned}
(\overline{a_1}\overline{\cdot}\overline{a_2}) &= \overline{a_1.a_2} \\
&= \overline{a_2.a_1} \\
&= \overline{a_2}\overline{\cdot}\overline{a_1}
\end{aligned}$$

Donc $\overline{\cdot}$ est commutative.
4. $\forall a_1 \in \mathbb{Z}$,

$$\begin{aligned}
(\overline{a_1}\overline{\cdot}\overline{1}) &= \overline{a_1.1} \\
&= \overline{a_1}
\end{aligned}$$

donc $\overline{1}$ est un élément neutre pour $\overline{\cdot}$.
5. $\forall (a_1, a_2, a_3) \in \mathbb{Z}^3$,

$$\begin{aligned}
\overline{a_1}\overline{\cdot}(\overline{a_2}\,\overline{+}\,\overline{a_3}) &= \overline{a_1}\,\overline{\cdot}\,\overline{(a_2+a_3)} \\
&= \overline{a_1.(a_2+a_3)} \\
&= \overline{(a_1.a_2)+(a_1.a_3)} \\
&= \overline{(a_1.a_2)}\,\overline{+}\,\overline{a_1.a_3} \\
&= \overline{a_1}\overline{\cdot}\overline{a_2}\overline{+}\overline{a_1}\overline{\cdot}\overline{a_3})
\end{aligned}$$

Donc $\overline{\cdot}$ est distributive sur $\overline{+}$. On en déduit que$(\mathbb{Z}/n\mathbb{Z}, \overline{+}, \overline{\cdot})$ est un anneau commutatif. ■

5 Corps

Définition 4.13 *[1], [3], [6] On appelle corps, tout ensemble M muni de deux lois de composition internes + et • telles que*
1. $(\mathrm{M}, +, \bullet)$ *est un anneau non réduit à* $\{0_\mathrm{M}\}$ *tel que tous ses éléments non nuls sont inversibles, autrement dit*

1. $(M,+,\bullet)$ *est un anneau ,*
2. $0_M \neq 1_M$,
3. Tout élément de $M-\{0_M\}$ *a un inverse pour* $\bullet$ *dans M.*

Dans le cas où la loi $\bullet$ *est abélienne, alors* $(M,+,\bullet)$ *est appelé corps abélien.*

Exemple 4.17 *1.* $(\mathbb{R},+,.)$, $(\mathbb{C},+,.)$ *sont des corps abéliens.*
2. $(\mathbb{Z},+,.)$ *n'est pas un corps car seuls 1 et -1 sont inversibles.*

Proposition 4.10 *[1], [3], [6] Chaque corps commutatif est un anneau intègre.*

Preuve. Étant donnés $(M,+,\bullet)$ un corps abélien et $a_1 \in M$, $a_2 \in M$ tels que $a_1 \neq 0$. Montrons que

$$(a_1 \bullet a_2) = 0 \Rightarrow a_2 = 0.$$

En effet

$$\begin{aligned}(a_1 \bullet a_2) = 0 &\Rightarrow {a_1}^{-1} \bullet (a_1 \bullet a_2) = a_1^{-1} \bullet 0\\ &\Rightarrow ({a_1}^{-1} \bullet a_1) \bullet a_2 = 0\\ &\Rightarrow 1_M \bullet a_2 = 0\\ &\Rightarrow a_2 = 0.\end{aligned}$$

D'où, M est intègre. ■

Remarque 4.6 *La réciproque de cette proposition n'est vraie en général.*

Exemple 4.18 $(\mathbb{Z},+,.)$ *est intègre mais n'est pas un corps.*

6 Sous corps

Définition 4.14 *[1], [3], [6] Étant donnés* $(M,+,\bullet)$ *un corps, et M' une partie non vide de M. On dit que* $(M',+,\bullet)$ *est un sous corps de* $(M,+,\bullet)$ *si et seulement si*
1. $(M',+,\bullet))$ *est un sous anneau de* $(M,+,\bullet)$.
2. Pour tout $x \in M'-\{0'_M\}$, $x^{-1} \in M'$.

On a aussi la caractérisation suivante des corps.

Définition 4.15 *Étant donnés* $(M,+,\bullet)$ *un corps et M' une partie non vide de K. On dit que* $(M',+,\bullet)$ *est un sous corps de* $(M,+,\bullet)$ *si et seulement si*
1. $\forall (a,b) \in M'^2, (a-b) \in M'$,
2. $\forall (a,b) \in M'^2, (a \bullet b) \in M'$,
3. $1_M \in M'$.
4. Pour tout $x \in M'-\{0'_M\}$, $x^{-1} \in M'$.

Proposition 4.11 *[1], [3], [6] Soit* $m \in \mathbb{Z}$. *Les trois propriétés suivantes sont équivalentes :*
1. m est premier.
2.$(\mathbb{Z}/m\mathbb{Z},\overline{+},\cdot)$ *est un corps commutatif.*
3. $(\mathbb{Z}/m\mathbb{Z},\overline{+},\cdot)$ *est un anneau intègre.*

Preuve. Considérons m premier et $a_2 \in \mathbb{Z}/m\mathbb{Z} - \{\overline{0}\}$, $\exists a_1 \in \mathbb{Z}$ tel que $a_2 = \overline{a_1}$ et $\overline{a_1} \neq \overline{0}$ donc m n'est pas un diviseur de a_1 et puisque m est premier donc $m \wedge a_1 = 1$. Donc, $\overline{a_1}$ est inversible dans $\mathbb{Z}/m\mathbb{Z}$. Par suite, $\mathbb{Z}/m\mathbb{Z}$ est un corps. Donc, 1. $\Rightarrow$ 2.
Supposons que M est un corps commutatif et $(a_1, a_2) \in \mathrm{M}^2$, $a_1 a_2 = 0$ et $a_1 \neq 0$ alors, $a_2 = {a_1}^{-1}(a_1 a_2) = 0$. D'où, tout corps commutatif est un anneau intègre.
Pour montrer que 3. $\Rightarrow$ 1. en utilisant la contraposée, montrons que si m n'est pas premier alors $\mathbb{Z}/m\mathbb{Z}$ n'est pas intègre . Si m n'est pas premier alors il existe $(a_1, a_2) \in \mathbb{N}^2$ tels que a_1 et a_2 sont non nuls et $m = a_1 a_2$, $1 < a_1 < m$ et $1 < a_2 < m$ d'où $\overline{a_1 a_2} = \overline{0}$ avec $\overline{a_1} \neq \overline{0}$ et $\overline{a_2} \neq \overline{0}$.
■

7 Exercices corrigés

7.1 Groupes

Exercice 4.2 *Considérons la loi* $\bullet$ *définie sur* $]-1,1[$ *comme suit*

$$\forall a, b \in]-1,1[,\ a \bullet b = \frac{a+b}{1+ab}.$$

Prouver que $(]-1,1[, \bullet)$ *est un groupe abélien.*

Solution. 1. $\bullet$ est-elle une loi de composition interne dans $]-1,1[$?
Soient $a, b \in]-1,1[$, alors

$$(|a| < 1) \wedge (|b| < 1)$$

d'où

$$|ab| = |a||b| < 1$$

donc

$$1 + ab > 1 - |ab| > 0.$$

Par suite

$$\begin{aligned} \frac{|a+b|}{|1+ab|} < 1 &\Leftrightarrow |a+b| < |1+ab| \\ &\Leftrightarrow |a+b| < 1+ab \ \text{car} 1+ab > 0 \\ &\Leftrightarrow -(1+ab) < a+b < 1+ab \\ &\Leftrightarrow (a+b-1-ab < 0) \text{ et } (a+b+1+ab > 0) \\ &\Leftrightarrow ((1-b)(a-1) < 0) \text{ et } ((1+b)(a+1) > 0) \end{aligned}$$

puisque $-1 < a, b < 1$, alors

$$((1-b > 0) \wedge (a-1 < 0)) \text{ et } ((1+b > 0) \wedge (a+1 > 0))$$

donc

$$((1-b)(a-1) < 0) \text{ et } ((1+b)(a+1) > 0),$$

d'où $\bullet$ est une loi de composition interne dans $]-1,1[$.
2. $\bullet$ est -elle commutative ?
En utilisant la commutativité de l'addition et de la multiplication dans $\mathbb{R}$, on a

$$\forall a, b \in]-1,1[, a \bullet b = \frac{a+b}{1+ab} = \frac{b+a}{1+ba} = b \bullet a.$$

Ce ci prouve que $\bullet$ est commutative.
3. $\bullet$ est -elle associative ?
Soient $a, b, c \in]-1,1[$, alors

$$(a \bullet b) \bullet c = \frac{(a \bullet b) + c}{1 + (a \bullet b)c}$$

$$= \frac{(\frac{a+b}{1+ab})+c}{1+(\frac{a+b}{1+ab})c}$$
$$= \frac{\frac{a+b+c(1+ab)}{1+ab}}{\frac{1+ab+ac+bc}{1+ab}}$$

et on a

$$a \bullet (b \star c) = \frac{a+(b \bullet c)}{1+a(b \bullet c)}$$
$$= \frac{a+(\frac{b+c}{1+bc})}{1+a(\frac{b+c}{1+bc})}$$
$$= \frac{\frac{a(1+ab)+b+c}{1+bc}}{\frac{1+bc+ac+bc}{1+bc}}$$
$$= \frac{a+b+c(1+ab)}{1+ab+ac+bc}$$

En comparant les deux résultats, on trouve

$$\forall a,b,c \in]-1,1[, (a \bullet b) \bullet c = a \bullet (b \bullet c).$$

Par suite $\bullet$ est associative.
4. $\bullet$ admet elle un élément neutre ?
Soit $e \in \mathbb{R}$, alors

$$(\text{ e élément neutre de } \bullet) \Leftrightarrow (\forall a \in]-1,1[, a \bullet e = e \bullet a = a)$$

la commutativité $\bullet$ et

$$\begin{array}{rcl} a \bullet e = a & \Leftrightarrow & \frac{a+e}{1+ae} = a \\ & \Leftrightarrow & a+e = a+a^2 e \\ & \Leftrightarrow & e = a^2 e \\ & \Leftrightarrow & e(1-a^2) = 0 \\ . & \Leftrightarrow & (e=0) \vee (a = \pm 1) \end{array}$$

on obtient $e = 0 \in]-1,1[$ est l'élément neutre de $\bullet$.
5. Tout élément de $]-1,1[$ est - il symétrisable ?
Soient $a \in]-1,1[$ et $a \in \mathbb{R}$ alors

$$\begin{array}{rcl} a \bullet a' = e & \Leftrightarrow & \frac{a+a'}{1+aa'} = 0 \\ & \Leftrightarrow & a+a' = 0 \\ & \Leftrightarrow & a' = -a. \end{array}$$

En utilisant la commutativité de $\bullet$, on obtient tout élément $a \in]-1,1[$ est symétrisable et son symétrique est $a' = -a \in]-1,1[$.
On déduit que $(]-1,1[, \bullet)$ est un groupe commutatif.

Exercice 4.3 *Définissons la loi de composition interne $\bullet$ dans un ensemble A dont l'élément neutre noté e_A. Démontrer les propriétés suivantes*
1. e_A admet un seul symétrique e_A.
2. Étant donné a_1 un élément symétrisable dans A par la loi $\bullet$. Si a_1 admet un symétrique a_2, alors ce dernier est aussi symétrisable et son symétrique est a_1.

Solution. Supposons que $a_1 \in \mathrm{A}$, alors

$$\begin{array}{rcl}(a_1 \text{est un symétrique de } e_\mathrm{A}) & \Leftrightarrow & (e_\mathrm{A} \bullet a_1 = a_1 \bullet e_\mathrm{A} = e_\mathrm{A}) \\ & \Leftrightarrow & a_1 = e_\mathrm{A}.\end{array}$$

D'où le symétrique de e_A est lui même et est unique.
2. Supposons que $a_1 \in \mathrm{A}$ est un élément symétrisable par rapport à la loi $\bullet$ et son symétrique est $a_2 \in \mathrm{A}$. Donc,

$$a_1 \bullet a_2 = a_2 \bullet a_1 = e_\mathrm{A}$$

par suite a_2 est symétrisable par rapport à la loi $\bullet$ et que a_1 est un symétrique de a_2.

Exercice 4.4 *Étant donnée $\star$ une loi de composition interne associative dans un ensemble A dont l'élément neutre est e_A. Considérons a_1 et a_2 deux éléments de A symétrisables. Démontrer que la composition de a_1 et a_2 par la loi $\star$ l'est aussi et*

$$-(a_1 \star a_2) = -a_2 \star (-a_1).$$

Solution. Étant donnés $(a_1, a_2) \in \mathrm{A}^2$ deux éléments symétrisables. En utilisant l'associativité de $\star$, on a

$$\begin{array}{rcl}(a_1 \star a_2) \star (-a_2 \star (-a_1)) & = & (a_1 \star (a_2 \star (-a_2))) \star (-a_1) \\ & = & (a_1 \star e_\mathrm{A}) \star (-a_1) \\ & = & a_1 \star (-a_1) \\ & = & e_\mathrm{A}.\end{array}$$

D'une manière similaire, on montre que

$$((-a_2) \star (-a_1)) \star (a_1 \star a_2) = e_\mathrm{A}.$$

D'où on déduit que

$$-(a_1 \star a_2) = (-a_2) \star (-a_1).$$

Exercice 4.5 *Étant donnés* $(\mathrm{A}, \blacktriangle)$ *un groupe et* A_1 *et* A_2 *deux sous groupes de* $(\mathrm{A}, \blacktriangle)$. *Prouver que* $(\mathrm{A}_1 \cup \mathrm{A}_2, \blacktriangle)$ *est un sous groupe de* $(\mathrm{A}, \blacktriangle)$ *si et seulement si* $\mathrm{A}_1 \subset \mathrm{A}_2$ *ou* $\mathrm{A}_2 \subset \mathrm{A}_1$.

Solution. 1. $\Leftarrow$) Supposons que $\mathrm{A}_1 \blacktriangle \mathrm{A}_2$ alors, $\mathrm{A}_1 \cup \mathrm{A}_2 = \mathrm{A}_1$. Supposons maintenant que $\mathrm{A}_2 \blacktriangle \mathrm{A}_1$ alors $\mathrm{A}_1 \cup \mathrm{A}_2 = \mathrm{A}_2$, et donc dans les deux cas, on obtient $(\mathrm{A}_1 \cup \mathrm{A}_2, \blacktriangle)$ est un sous groupe de $(\mathrm{A}, \blacktriangle)$.
2. $\Rightarrow$) Supposons que $(\mathrm{A}_1 \cup \mathrm{A}_2, \blacktriangle)$ est un sous groupe de $(\mathrm{A}, \blacktriangle)$ et que $\mathrm{A}_1 \nsubseteq \mathrm{A}_2$ et montrons que $\mathrm{A}_2 \subset \mathrm{A}_1$. On a

$$(\mathrm{A}_1 \nsubseteq \mathrm{A}_2) \Rightarrow (\exists a_1 \in \mathrm{A}_1) et (a_1 \notin \mathrm{A}_2).$$

Soit $a_2 \in \mathrm{A}_2$, alors $a_2 = a_2 \blacktriangle e = (a_2 \blacktriangle a_1) \blacktriangle (-a_1)$. Comme $(\mathrm{A}_1 \cup \mathrm{A}_2, \blacktriangle)$ est un sous groupe , on déduit que

$$(a_2 \blacktriangle a_1) \in (\mathrm{A}_1 \cup \mathrm{A}_2).$$

Puisque $(a_2 \blacktriangle a_1)$ ne peut pas être dans A_2 car $(a_1 \notin \mathrm{A}_2)$, donc $(a_2 \blacktriangle a_1) \in \mathrm{A}_1$, par suite $a_2 \in \mathrm{A}_1$, d'où $\mathrm{A}_2 \subset \mathrm{A}_1$.

Exercice 4.6 *Considérons* $(A,\star)$ *et* $(A',\bullet)$ *deux groupes et* $h : A \to A'$ *un morphisme de groupes avec* $e_A \in A$ *et* $e'_A \in A'$ *les éléments neutres. Prouver que les deux propriétés suivantes sont équivalentes*
1. h *est injective.*
2. $\ker h = \{e_A\}$.
De même pour les deux propriétés suivantes
1. h *est surjective.*
2. $Imh = A'$.

Solution.1. Supposons que h est injectif et montrons que $\ker h = \{e_A\}$. Comme $\ker h$ est un sous groupe, alors il est clair que $\{e_A\} \subset \ker h$. Soit $a \in \ker h$.

$$\begin{aligned} a \in \ker h &\Rightarrow h(a) = e'_A \\ &\Rightarrow h(a) = h(e_A) \\ &\Rightarrow a = e_A \quad \text{car h est injective.} \end{aligned}$$

D'où $\ker h \subset e_A$, donc $\ker h = \{e_A\}$.
D'autre part, si $\ker h = \{e_A\}$. Soient $(a,b) \in A^2$ tels que $h(a) = h(b)$.

$$\begin{aligned} h(a) = h(b) &\Rightarrow h(a) \bullet (-h(b)) = e'_A \\ &\Rightarrow h(a) \bullet (h(-b)) = e'_A \\ &\Rightarrow h(a \star (-b)) = e'_A \\ &\Rightarrow a \star (-b) \in \ker h \\ &\Rightarrow a \star (-b) = e_A \\ &\Rightarrow a = b. \end{aligned}$$

D'où h est injective.
2. Supposons que h est surjective et montrons que $Imh = A'$. On a $Imh \subset A'$. Il suffit de montrer que $A' \subset Imh$. Soit $a_2 \in A'$.

$$\begin{aligned} a_2 \in A' &\Rightarrow \exists a_1 \in A, a_2 = h(a_1) \quad \text{car } h \text{ est surjective} \\ &\Rightarrow a_2 = h(a_1) \in Imh. \end{aligned}$$

Par suite, $Imh = A'$.
D'autre part, supposons que $Imh = A'$ et montrons que h est surjective. Soit $a_2 \in A' = Imh$.
D'après la définition de Imh, on a

$$a_2 \in A' = Imh \Rightarrow \exists a_1 \in A, a_2 = h(a_1)$$

d'où la surjectivité de h.

Exercice 4.7 *Étant donné* $(E,\star)$ *un groupe, pour tout* $a \in E$, *on note* $f_a : E \to E$ *l'application définie par :*

$$f_a(x) = a \star x \star (-a).$$

a. Prouver que f_a *est un automorphisme de E.*
b. Prouver que $\forall (a,b) \in E^2, f_a \circ f_b = f_{a\star b}$.

Solution. Soient $(x,y) \in E^2$,

$$f_a(x \star y) = a \star (x \star y) \star (-a) = (a \star x \star (-a)) \star (a \star y \star (-a)) = f_a(x) \star f_a(y)$$

d'où f_a est un endomorphisme de E.
Soit $x \in$ E,on a

$$(f_a o f_{-a})(x) = f_a((-a) \star x \star a) = a \star ((-a) \star x \star a) \star (-a) = x$$

et

$$(f_{-a} o f_a)(x) = f_{-a}(a \star x \star (-a)) = (-a) \star (a \star x \star (-a)) \star a = x,$$

donc

$$f_a o f_{-a} = f_{-a} o f_a = \mathrm{I}d_{\mathrm{E}},$$

donc f_a est bijectif de réciproque f_{-a}. Ainsi, f_a est un automorphisme de groupe E.
b. Soient $(a,b) \in \mathrm{E}^2$, on a pour $x \in$ E,

$$\begin{aligned}(f_a o f_b)(x) &= f_a(b \star x \star (-b)) \\ &= a \star (b \star x \star (-b) \star (-a) \\ &= (a \star b) \star x \star (-b \star (-a)) \\ &= (a \star b) \star x \star (-(a \star b)) \\ &= f_{(a \star b)}(x).\end{aligned}$$

d'où : $f_a o f_b = f_{(a \star b)}$. On en déduit que l'application $a \mapsto f_a$ est un morphisme du groupe E dans le groupe des automorphismes de E(muni de la loi o).

Exercice 4.8 *1. Montrer par un exemple qu'il existe un groupe A qui contient un ensemble* A_1 *de cardinal infini, stable pour la loi de A mais* A_1 *n'est un sous groupe de A.*
2. Soit A un groupe. Prouver que si A_1 *est un sous ensemble non vide de cardinal fini et stable pour la loi de groupe A, alors* A_1 *est un sous-groupe de A.*

Solution.1. Considérons $\mathrm{A} = \mathbb{Z}$ et $\mathrm{A}_1 = \mathbb{N}$ pour la loi d'addition.
2. si A_1 est un sous ensemble non vide de cardinal fini et stable pour la loi de groupe A, alors si a_1 est un élément de A_1, ${a_1}^n$ est un élément de A_1, pour $n \geq 1$. Par suite $\{{a_1}^n, n \in \mathbb{N}^*\}$ est un 'ensemble inclus dans A et donc est de cardinal fini. Il existe donc $n \geq 1$ tel que ${a_1}^n = e_{\mathrm{A}}$. D'autre par, comme A_1 est un sous groupe, il contient e_{A} et l'inverse de a_1 . Par suite, A_1 est un sous groupe de A.

7.2 Anneaux

Exercice 4.9 *Étant donnés* $(\mathrm{H}, +, \bullet)$ *un anneau vérifiant pour tout élément a dans H est idempotent c'est-à-dire*

$$a^2 = a \bullet a = a$$

1.Prouver que pour tout a dans H, on a $a + a = 0_{\mathrm{H}}$ *et que H est abélien.*
2. Prouver que $(a_1 \bullet a_2) \bullet (a_1 + a_2) = 0_{\mathrm{A}}$ *sachant que* a_1 *et* a_2 *sont deux éléments de H. Que peut-on conclure dans le cas où A est intègre ?*

Solution.1. Considérons $a_1 \in$ A, on a

$$\begin{aligned}a_1 + a_1 &= (a_1 + a_1)^2 \\ &= a_1 + a_1) \bullet (a_1 + a_1) \\ &= {a_1}^2 + {a_1}^2 + {a_1}^2 + {a_1}^2 \quad \text{par la distributivité de la loi } \bullet \text{ sur } + \\ &= a_1 + a_1 + a_1 + a_1.\end{aligned}$$

D'où $a_1 + a_1 = 0_A$ et $a_1 = -a_1$.
Soient $a_1 \in A, a_2 \in A$,

$$\begin{aligned} a_1 + a_2 &= (a_1 + a_2)^2 \\ &= (a_1 + a_2) \bullet (a_1 + a_2) \\ &= {a_1}^2 + a_1 \bullet a_2 + a_2 \bullet a_1 + {a_2}^2 \quad \text{par la distributivité de la loi } \bullet \text{ sur } + \\ &= a_1 + a_1 \bullet a_2 + a_2 \bullet a_1 + a_2. \end{aligned}$$

ce qui donne

$$a_1 \bullet y + y \bullet a_1 = 0_A$$

et comme $a_1 = -a_1$, on obtient

$$a_1 \bullet a_2 = a_2 \bullet a_1.$$

A est bien commutatif.
2. Soient a_1 et a_2 deux éléments de A. On a

$$(a_1 \bullet a_2) \bullet (a_1 + a_2) = (a_1 \bullet a_2) \bullet a_1 + (a_1 \bullet a_2) \bullet a_2 = (a_1 \bullet a_2) \bullet a_1 + a_1 \bullet {a_2}^2 = {a_1}^2 \bullet a_2 + a_1 \bullet {a_2}^2 = a_1 \bullet a_2 + a_1 \bullet a_2 = 0_A \quad \text{c}$$

Supposons que A contient deux éléments a_1, a_2 différents de 0_A. Puisque $a_1 \neq a_2$, on trouve $a_1 \neq -a_2$ donc $a_1 + a_2 \neq 0_A$. Si A est intègre, alors A possède au plus deux éléments, donc $(a_1 \bullet a_2) \bullet (a_1 + a_2) \neq 0$, c'est une contradiction . D'où si A est intègre, alors A admet au plus deux éléments.

Exercice 4.10 *Étant donné* $(H, +, \bullet)$ *un anneau. On appelle le centre de H l'ensemble C des éléments c de H tels que pour tout élément h de H, on ait c.h = h.c c'est à dire*

$$C = \{c \in H, \forall h \in H : c.h = h.c\}.$$

Justifier que C est un sous anneau de H.

Solution. Puisque pour tout élément h de H, on a $0_H \bullet h = h \bullet 0_H = 0_A$, on a donc, l'élément neutre 0_H de la loi + est un élément de C et C est non vide. Il reste à montrer que si h et h' sont deux élément de C, il en est de même de $h - h'$ et de $h \bullet h'$. Considérons h et h' deux éléments de C et $h"$ un élément de H. On a $h" \bullet (h - h') = h" \bullet h - h" \bullet h'$ et comme h et h' appartiennent à C donc $h" \bullet h = h \bullet h"$ et $h" \bullet h' = h' \bullet h"$, d'où

$$h" \bullet (h - h') = h \bullet h" - h' \bullet h" = (h - h') \bullet h"$$

ce qui prouve que $(h - h') \in C$. On calcul $h" \bullet (h \bullet h')$. Considérons $h"$ un élément quelconque de H ; en utilisant l'associativité de la loi $\bullet$, on peut écrire $h" \bullet (h \bullet h') = (h" \bullet h) \bullet h'$, or $h" \bullet h = h \bullet h"$ car $h \in C$; donc $(h" \bullet h) \bullet h' = (h \bullet h") \bullet h'$ mais $(h \bullet h") \bullet h' = h \bullet (h" \bullet h')$ et $h" \bullet h' = h' \bullet h"$ car $h' \in C$, donc $(a \bullet h") \bullet h' = (h \bullet h') \bullet h"$ d'où $h" \bullet (h \bullet h') = (h \bullet h') \bullet h"$, par suite $(h \bullet h') \in C$ et C est un sous-anneau de H.

Exercice 4.11 *Considérons* $(H, +, \bullet)$ *un anneau intègre. Prouver que tout élément inversible à droite dans H est inversible à gauche.*

Solution. Soit h un élément de H admettant un inverse à droite, il existe alors $h' \in H$ tel que $h \bullet h' = 1_H$. On a

$$(h' \bullet h - 1_H) \bullet h' = (h' \bullet h) \bullet h' - h' = h' - h' = 0_H.$$

Comme $h \bullet h' = 1_H$, on a $h' \neq 0_H$ car sinon on aurait $0_H = 1_H$ et l'anneau H est réduit à $\{0_H\}$. Du fait que $(h' \bullet h - 1_H) \bullet h' = 0_H$ et $h' \neq 0_H$ dans un anneau intègre, on obtient $h' \bullet h - 1_H = 0_A$, soit $h'h = 1_H$.
h admet donc aussi un symétrique à gauche.

Exercice 4.12 *Étant donnés* $(\mathrm{H},+,\bullet)$ *un anneau et* h_1 *et* h_2 *deux éléments de H. Supposons que* 1_H *est le neutre de la deuxième loi de H et que* $h_1, h_2, h_1 \bullet h_2 - 1_\mathrm{H}$ *sont inversibles dans H.*
a) Notons $h = h_1 \bullet h_2 - 1_\mathrm{H}$. *Montrer que* $h_1 - {h_2}^{-1}$ *est inversible dans H et que* $(h_1 - {h_2}^{-1})^{-1} = h_2 \bullet h^{-1}$.
b) On note $h'' = h_1^{-1} - (h_1 - {h_2}^{-1})^{-1}$. *Vérifier que h" est inversible dans H et que* $h"^{-1} = -h \bullet h_1$.

Solution. a) On a

$$h_1 - {h_2}^{-1} = (h_1 \bullet h_2 - 1) \bullet {h_2}^{-1} = h \bullet {h_2}^{-1}.$$

Puisque h et ${h_2}^{-1}$ sont inversibles dans H, donc $h \bullet {h_2}^{-1}$ l'est aussi dans H, d'où $h_1 - {h_2}^{-1}$ est inversible dans H et

$$(h_1 - {h_2}^{-1})^{-1} = (h \bullet {h_2}^{-1})^{-1} = ({h_2}^{-1})^{-1} \bullet h^{-1} = h_2 \bullet h^{-1}.$$

b) On a

$$h" = h_1^{-1} - (h_1 - {h_2}^{-1})^{-1} = {h_1}^{-1} - h_2 \bullet h^{-1} = ({h_1}^{-1} \bullet h - h_2) \bullet h^{-1}$$

d'où

$$h" = {h_1}^{-1} \bullet (h - h_1 \bullet h_2) \bullet h^{-1} = {h_1}^{-1} \bullet ((h_1 \bullet h_2 - 1) - h_1 \bullet h_2) \bullet h^{-1}$$

ce qui donne

$$h" = {h_1}^{-1}(-1)h^{-1} = -{h_1}^{-1} \bullet h^{-1}.$$

Puisque ${h_1}^{-1}$ et h^{-1} sont inversibles dans H, alors, ${h_1}^{-1} \bullet h^{-1}$ l'est aussi dans H, donc $h"$ est inversible dans A et : On a

$$h"^{-1} = (-{h_1}^{-1} \bullet h^{-1})^{-1} = -({h_1}^{-1} \bullet h^{-1})^{-1}$$

donc

$$h"^{-1} = -(h^{-1})^{-1} \bullet ({h_1}^{-1})^{-1} = -h \bullet h_1$$

7.3 Corps

Exercice 4.13 *Montrer que le corps des rationnels* $\mathbb{Q}$ *contient un seul sous-corps qui est lui-même.*

Solution. Supposons que M est un sous-corps.
Il est est clair que M contient les éléments neutres $0_\mathbb{Q}$ et $1_\mathbb{Q}$ de l'addition et de la multiplication.
Par la stabilité de l'addition, on peut dire que $\mathbb{N} \subset \mathrm{K}$ car tout entier naturel non nul $m = 1 + ... + 1$ appartient aussi à M. Donc
Sachant que (M ,+) est un groupe, alors pour tout entier naturel m, son symétrique $-m \in$ M. D'où $\mathbb{Z} \subset$ M.
Étant donné $h = \frac{h_1}{h_2}$ un rationnel avec $h_2 \neq 0$. Comme h_1 et h_2 appartiennent au corps M, alors $r = h_1 \times {h_2}^{-1} \in$ M. Donc $\mathbb{Q} \subset$ M. Comme M $\subset \mathbb{Q}$, on obtient donc que M $= \mathbb{Q}$.

Exercice 4.14 *Étant donné* $(\mathrm{H},+,\bullet)$ *un anneau intègre fini quelconque. Prouver qu'il définit un corps.*

Solution. Considérons $(H,+,\bullet)$ un anneau intègre fini, $h \in H - \{0_H\}$. Du fait que H est intègre, les applications

$$\begin{array}{rccl} h_a : & H & \longrightarrow & H \\ & a_1 & \longmapsto & h_a(a_1) = a \bullet a_1. \end{array}$$

et

$$\begin{array}{rccl} h'_a : & HA & \longrightarrow & H \\ & a_1 & \longmapsto & h'_a(a_1) = a_1 \bullet a. \end{array}$$

sont injectives, en effet $\forall (a_1, a_2) \in H^2$,

$$\begin{array}{rcl} h_a(a_1) = h_a(a_2) & \Leftrightarrow & a \bullet a_1 = a \bullet a_2 \\ & \Leftrightarrow & a \bullet (a_1 - a_2) = 0 \\ & \Leftrightarrow & a_1 - a_2 = 0 \\ & \Rightarrow & a_1 = a_2. \end{array}$$

d'une manière similaire pour h'_a. Sachant que H est fini, alors h_a et h'_a sont bijectives. De plus, il existe $(a_3, a_4) \in H^2$ tel que $h_a(a_3) = 1_H$ et $h'_a(a_4) = 1_H$, c'est à dire tel que $a \bullet a_3 = 1_H$ et $a_4 \bullet a = 1_H$. On a

$$a_4 = a_4 \bullet (a \bullet a_3) = a_4 \bullet a \bullet a_3 = a_3.$$

Par suite

$$\forall a \in H - \{0_H\}, \exists a_3 \in H, a \bullet a_3 = a_3 \bullet a = 1_H.$$

Tout élément de $H - \{0_H\}$ admet un inverse, on déduit que H est un corps.

Exercice 4.15 *Étant donné $\mathbb{M}$ l'ensemble des complexes de type $z = n + i.m$ ou $n \in \mathbb{Q}$ et $m \in \mathbb{Q}$.*
1. Prouver que $(\mathbb{M}, +)$ est un groupe commutatif.
2. Prouver que $(\mathbb{M}^*, .)$ est un groupe commutatif.
3. En déduire que $(\mathbb{M}, +, .)$ est un corps commutatif.

Solution.1. Puisque 0 est un élément neutre de $\mathbb{Q}$ alors $0 = (0 + i.0) \in \mathbb{M}$.
Étant donné $(z_1, z_2) \in \mathbb{M}^2$, montrons que $(z_1 - z_2) \in \mathbb{M}$. On a $z_1 = n_1 + i.m_1$ et $z_2 = n_2 + i.m_2$ avec n_1, n_2, m_1 et m_2 sont des éléments de $\mathbb{Q}$ et

$$z_1 - z_2 = (n_1 + i.m_1) - (n_2 + i.m_2) = ((n_1 - n_2) + i.(m_1 - m_2)) \in \mathbb{M}$$

car $(n_1 - n_2) \in \mathbb{Q}$ et $(m_1 - m_2) \in \mathbb{Q}$. Par suite, $(\mathbb{M}, +)$ est un sous groupe commutatif de $(\mathbb{C}, +)$ et donc est un groupe commutatif .
2. On a $1 = (1 + i.0) \in \mathbb{M}$ car $1 \in \mathbb{Q}$ et $0 \in \mathbb{Q}$.
Soient z_1, z_2 deux éléments de $\mathbb{M}^*$, montrons que $(z_1.z_2^{-1}) \in \mathbb{M}^*$. On a $z_1 = n_1 + i.m_1$ et $z_2 = n_2 + i.m_2$ avec n_1, n_2, m_1 et m_2 sont des éléments de $\mathbb{Q}^*$, et

$$\begin{aligned} z_1.z_2^{-1} &= \frac{n_1 + i.m_1}{n_2 + i.m_2} \\ &= \frac{(n_1 + i.m_1)(n_2 - i.m_2)}{n_2^2 + m_2^2} \\ &= \frac{n_1.n_2 + m_1.m_2}{n_2^2 + m_2^2} + i.\frac{n_2.m_1 - n_1.m_2}{n_2^2 + m_2^2} \end{aligned}$$

Utilisant le fait que

$$\left(\frac{n_1.n_2 + m_1.m_2}{n_2^2 + m_2^2}\right) \in \mathbb{Q}$$

et

$$\left(\frac{n_2.m_1 - n_1.m_2}{n_2^2 + m_2^2}\right) \in \mathbb{Q},$$

on obtient $(z_1.z_2^{-1}) \in \mathbb{M}^*$ et comme la multiplication est commutative dans $\mathbb{C}$ donc $(\mathbb{M}^*, .)$ est un sous groupe commutatif de $(\mathbb{C}, +)$ et donc est un groupe commutatif .
3. Sachant que la multiplication est distributive par rapport à l'addition dans $\mathbb{C}$,on en déduit que $(\mathbb{M}, +, .)$ est un corps commutatif.

8 Exercices proposés

Exercice 4.16 *Considérons* $\mathrm{A} = \mathbb{C} \times \mathbb{R}$ *muni de la loi interne* $\blacktriangle$ *définie comme suit : pour tout* $(r, t), (r', t')$ *dans A par*

$$(r, t) \blacktriangle (r', t') = (r + r', t + t' + \mathrm{I}m(r\, r')).$$

Prouver que $(\mathrm{A}, \blacktriangle)$ *est un groupe. Est-il commutatif ?*

Exercice 4.17 *Étant donné* $(\mathrm{H}, \bullet)$ *un groupe. Soit* $\mathrm{H}_1 \subset \mathrm{H}$*, on note* $\mathrm{H}' = \{x \in \mathrm{H}, \forall a \in \mathrm{H}_1, a \bullet x = x \bullet a\}$*, prouver que* $(\mathrm{H}', \bullet)$ *représente un sous groupe de* $(\mathrm{H}, \bullet)$.

Exercice 4.18 *Justifier qu'il n'existe pas un isomorphisme entre les deux groupes* $(\mathbb{Z}, +)$ *et* $(\mathbb{Z}^2, +)$.

Exercice 4.19 *Étant donné* $(\mathrm{L}, +, \bullet)$ *un anneau commutatif. On dit qu'un élément* $l \in \mathrm{L}$ *est nilpotent s'il existe* $n \in \mathbb{N}$ *tel que* $l^n = 0$.
1. Vérifier que, si $l \in \mathrm{L}$ *est nilpotent, alors* $1_{\mathrm{L}} - l$ *est inversible.*
2. Vérifier que si $l \in \mathrm{L}$ *et* $l' \in \mathrm{L}$ *sont nilpotents, alors* ll' *et* $l + l'$ *le sont aussi.*

Exercice 4.20 *Considérons* $\mathrm{H} = \{h_1 + h_2\sqrt{6}, \quad h_1, h_2 \in \mathbb{Z}\}$.
1. Vérifier que $(\mathrm{H}, +, \times)$ *est un sous anneau de* $(\mathbb{R}, +, \times)$.
2. Étant donnée l'application $h : \mathrm{H} \to \mathrm{H}$ *telle que* $h(m + n\sqrt{6}) = h_1 - h_2\sqrt{6}$*. Prouver que h est un automorphisme de l'anneau* $(\mathrm{H}, +, \times)$.
3. Pour tout $h' \in \mathrm{A}$*, on pose* $\mathrm{H}'(h') = h'.h(h')$*. Montrer que* H' *est une application de H dans* $\mathbb{Z}$ *qui est un morphisme pour la multiplication.*
4. Vérifier que h' *est un élément inversible de H si et seulement si* $\mathrm{H}'(h') = \pm 1$.
5. Justifier que $5 + 2\sqrt{6}$ *admet un inverse dans H et préciser son inverse.*

Chapitre 5

Anneaux de polynômes

1 Introduction

L'objectif de ce chapitre est de rappeler la construction de l'anneau des polynômes. Ce chapitre est basé sur les références ([2],[4], [6], [7],[8], [9], [10], [11], [12]).

2 Polynôme

Définition 5.1 *[6], [10], [11] Étant donner* $(\mathbb{P},+,.)$ *un anneau commutatif et* $(b_i)_{i\in\mathbb{N}}$ *une suite d'éléments de* $\mathbb{P}$ *nuls sauf un nombre fini* $b_0, b_1, b_2, b_3, ..., b_{n-1}, b_n$. *Toute écriture de la forme* $P = b_0 + b_1X + b_2X^2 + b_3X^3 + ... + b_{n-1}X^{n-1} + b_nX^n$ *est appelée un polynôme à une indéterminée, à coefficients dans* $\mathbb{P}$.

Notations

[6], [10], [11]

1. Les scalaire $(b_i)_{i\in\mathbb{N}}$ de $\mathbb{P}$ sont appelés les coefficients du polynôme P.

2. Le plus grand indice n tel que $b_n \neq 0$ est appelé degré de P, noté $\deg P$ et le terme b_nX^n est appelé terme dominant de P et b_n est appelé coefficient dominant de P.

2. On convient de noter $\deg P = -\infty$ pour le polynôme nul (dont les coefficients sont tous nuls).

3. L'anneau commutatif $(\mathbb{P}[X],+,.)$ représente l'ensemble des polynômes à une indéterminée X, à coefficients dans $\mathbb{P}$.

4. L'ensemble des polynômes à une indéterminée X de degré inférieur ou égal à n est noté $\mathbb{P}_n[X]$.

5. La fonction polynôme (ou bien polynomiale) d'une variable X associé au polynôme $P = b_0 + b_1X + b_2X^2 + b_3X^3 + ... + b_{n-1}X^{n-1} + b_nX^n$ dans $\mathbb{P}_n[X]$ est la fonction $\tilde{P} : \mathbb{P} \to \mathbb{P}$ définie par $:X \mapsto \tilde{P}(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + ... + b_{n-1}X^{n-1} + b_nX^n$.

2.1 Opérations dans $(\mathbb{P}[X],+,.)$

[6], [10] Étant donnés deux polynômes $P_1 = b_0+b_1X+b_2X^2+b_3X^3+...+b_{n-1}X^{n-1}+b_nX^n$ et $P_2 = b'_0+b'_1X+b'_2X^2+b'_3X^3+...+b'_{n-1}X^{n-1}+b'_nX^n$ de $\mathbb{P}[X]$. Alors
1. **Égalité**

$P_1 = P_2$ si et seulement si $b_i = b'_i$ pour tout $i \in \mathbb{N}$.
2. **Somme de deux polynômes**

$$P_1+P_2 = (b_0+b'_0)+(b_1+b'_1)X+(b_2+b'_2)X^2+(b_3+b'_3)X^3+...+(ab_{n-1}+b'_{n-1})X^{n-1}+(b_n+b'_n)X^n$$

3.**Produit de deux polynômes**

$$P_1.P_2 = (\sum_{i+j=0} b_ib'_j)+(\sum_{i+j=1} b_ib'_j)X+(\sum_{i+j=2} b_ib'_j)X^2+...+(\sum_{i+j=n} b_ib'_j)X^n$$

4. **Multiplication d'un polynômes par un scalaire** Si λ est un scalaire et $P = b_0+b_1X+b_2X^2+b_3X^3+...+b_{n-1}X^{n-1}+b_nX^n$ est un polynôme, alors λP est un polynôme tel que le i-ème coefficient est λb_i.
5. P_1 et P_2 dans $\mathbb{P}[X]$ sont dits associés s'il existe $\lambda \in \mathbb{P}$ inversible tel que $P_1 = \lambda P_2$.

Exemple 5.1 *1.* $P_1 = X^4-7X+\sqrt{2}$ *est un polynôme unitaire de degré 4 dans* $\mathbb{R}[X]$.
2. $P_2 = 4$ *est un polynôme constant de degré 0.*
3. $P_3 = (8+i)X+9$ *est un polynôme dans* $\mathbb{C}[X]$.
4. $P_4 = 3X^4-X^3+2$ *est un polynôme de degré 4 dont le terme dominant est* $3X^4$ *et le coefficient dominant est* 3 *dans* $\mathbb{R}[X]$. *Alors*

$$6P_1 = 6X^4-42X+6\sqrt{2}$$

et

$$P_1+P_4 = 4X^4-X^3-7X+2+\sqrt{2}.$$

Proposition 5.1 *[6], [10] Étant donnés* P_1 *et* P_2 *deux polynômes non nuls de* $\mathbb{P}[X]$. *Alors*

$$\deg(P_1+P_2) \leq \max(\deg P_1, \deg P_2)$$

et

$$\deg(P_1.P_2) \leq \deg P_1+\deg P_2.$$

Dans le cas où $\mathbb{P}$ *est intègre, alors*

$$\deg(P_1.P_2) = \deg P_1+\deg P_2$$

Preuve. Supposons que $n_1 = \deg P_1$ et $n_2 = \deg P_2$, alors

$$P_1 = b_0+b_1X+b_2X^2+b_3X^3+...+b_{n_1-1}X^{n_1-1}+b_{n_1}X^{n_1},$$

et

$$P_2 = b'_0+b'_1X+b'_2X^2+b'_3X^3+...+b'_{n_2-1}X^{n_2-1}+b'_{n_2}X^{n_2}.$$

1. On a

$$P_1+P_2 = (b_0+b'_0)+(b_1+b'_1)X+...+(b_{\min(n_1,n_2)}+b'_{\min(n_1,n_2)})X^{\min(n_1,n_2)}+$$

$$\ldots+(b_{\max(n_1,n_2)}+b'_{\max(n_1,n_2)})\mathrm{X}^{\max(n_1,n_2)}+(b_{\max(n_1,n_2)+1}+b'_{\max(n_1,n_2)+1}\mathrm{X}^{\max(n_1,n_2)+1}+\ldots$$

avec $b_i+b'_i=0, \quad \forall i>\max(n_1,n_2) \quad$ car $\quad b_i=0, b'_i=0$. Par conséquent,

$$\mathrm{P}_1+\mathrm{P}_2=\sum_{i=0}^{\max(n_1,n_2)}(b_i+b'_i)\mathrm{X}^i$$

D'où, $\deg(\mathrm{P}_1+\mathrm{P}_2)\leq\max(\deg\mathrm{P}_1,\deg\mathrm{P}_2)$.
2. On a

$$\mathrm{P}_1.\mathrm{P}_2=(\sum_{i+j=0}b_ib'_j)+(\sum_{i+j=1}b_ib'_j)\mathrm{X}+(\sum_{i+j=2}b_ib'_j)\mathrm{X}^2+\ldots+(\sum_{i+j=n_1+n_2-1}b_ib'_j)\mathrm{X}^{n_1+n_2-1}+b_{n_1}b'_{n_2}\mathrm{X}^{n_1+n_2}.$$

Par suite, $\mathrm{P}_1.\mathrm{P}_2$ est un polynôme de degré inférieur ou égale à n_1+n_2. On a donc bien $\deg(\mathrm{P}_1.\mathrm{P}_2)\leq\deg\mathrm{P}_1+\deg\mathrm{P}_2$.
Si l'anneau est intègre, alors $b_{n_1}b'_{n_1}\neq 0$ et dans ce cas, on obtient $\deg(\mathrm{P}_1.\mathrm{P}_2)=n_1+n_2=\deg\mathrm{P}_1+\deg\mathrm{P}_2$. ■

Remarque 5.1 *Par convention, on a pour tout* $n\in\mathbb{N}, n+(-\infty)=(-\infty)+n=(-\infty)$ *donc pour le cas particulier* $\mathrm{P}_1=0$ *on a* $\mathrm{P}_1.\mathrm{P}_2=0$ *alors* $(-\infty)=(-\infty)+\deg\mathrm{P}_2$*, ce qui démontre la proposition.*

Proposition 5.2 *[6], [10]* $\mathbb{P}[\mathrm{X}]$ *est un anneau intègre si* $(\mathbb{P},+,.)$ *est un anneau intègre.*

Preuve. Supposons que $\mathrm{P}_1.\mathrm{P}_2=0$. Donc $\deg(\mathrm{P}_1.\mathrm{P}_2)=\deg(0)=-\infty$. Par suite

$$\deg\mathrm{P}_1+\deg\mathrm{P}_2=-\infty.$$

Alors $\deg\mathrm{P}_1=-\infty$ ou $\deg\mathrm{P}_2=-\infty$, d'où $\mathrm{P}_1=0$ ou $\mathrm{P}_2=0$. ■

3 Divisibilité dans l'anneau de polynômes

Dans tous ce qui suit , désigne un anneau commutatif intègre.

Définition 5.2 *[7], [11] Soient* P_1 *et* P_2 *deux polynômes de* $\mathbb{P}[\mathrm{X}]$*. On dit que* P_1 *est divisible par* P_2 *s'il existe* $\mathrm{P}_3\in\mathbb{P}[\mathrm{X}]$ *tel que* $\mathrm{P}_1=\mathrm{P}_3.\mathrm{P}_2$

Remarque 5.2 *1. On dit aussi que* P_1 *est multiple de* P_2 *, ou que* P_2 *est un diviseur de* P_1 *ou encore* P_2 *divise* P_1*.*
2. Si P_2 *divise* P_1*, alors* $\deg\mathrm{P}_2\leq\deg\mathrm{P}_1$*.*

Exemple 5.2 *1. Chaque polynôme non nul vérifie* P_1 *divise* P_1*,* 1 *divise* P_1 *et* P_1 *divise* 0*.*

2. Le polynôme $\mathrm{X}^4+5\mathrm{X}^3+12\mathrm{X}^2+19\mathrm{X}-7$ *est divisible par le polynôme* $\mathrm{X}^2+3\mathrm{X}-1$ *, en effet*

$$\mathrm{X}^4+5\mathrm{X}^3+12\mathrm{X}^2+19\mathrm{X}-7=(\mathrm{X}^2+2\mathrm{X}+7)(\mathrm{X}^2+3\mathrm{X}-1).$$

3.1 Division euclidienne dans l'anneau de polynômes

Théorème 5.1 *[7], [11] Étant donnés* P_1 *et* P_2 *deux polynômes de* $\mathbb{P}[X]$. *Si le coefficient du terme dominant de* P_2 *est inversible dans* $\mathbb{P}$, *alors il existe deux polynômes* $(P_3, P_4) \in \mathbb{P}[X]^2$ *tel que*

$$P_1 = P_2.P_3 + P_4 \quad et \quad \deg P_4 < \deg P_2.$$

Preuve. On décompose la preuve en deux étapes : la preuve de l'existence et la preuve de l'unicité, qui se fait par l'absurde.

1. **Unicité** On démontre l'unicité par l'absurde.

Étant donnés $(P_3, P_4) \in \mathbb{P}[X]^2$ et $(P'_3, P'_4) \in \mathbb{P}[X]^2$ vérifiant les conditions du théorème.

Donc, $P_1 = P_2.P_3 + P_4$ et $P_1 = P_2.P'_3 + P'_4$ avec $\deg P_4 < \deg P_2$et $\deg P'_4 < \deg P_2$. Ce qui donne

$$P_2.(P_3 - P'_3) = P_4 - P'_4.$$

Supposons que $P_3 \neq P'_3$, puisque $\mathbb{P}[X]$ est intègre, $P_2.(P_3 - P'_3)$ et $P_4 - P'_4$ sont différents de zéro.

Cela implique :$\deg(P_4 - P'_4) = \deg(P_2.(P_3 - P'_3)) = \deg(P_2) + \deg(P_3 - P'_3)$.

Par suite : $\deg(P_4 - P'_4) \geq \deg(P_2)$

Or, le polynôme $P_4 - P'_4$ est différent de zéro, l'un au moins des deux polynômes P_4 ou P'_4 est différent de zéro et on a donc en utilisant les propriétés $\deg P_4 < \deg P_2$ et ($\deg P'_4 < \deg P_2$) : $\deg(P_4 - P'_4) < \deg(P_2)$.

D'où la contradiction.

On en déduit que $P_3 = P'_3$ et par conséquent $P_4 = P'_4$.

2. **Existence** La preuve donnée se base essentiellement sur le lemme suivant.

Lemme 5.1 *[7],[11] Étant donnés* P_1 *et* P_2 *deux polynômes non nuls de* $\mathbb{P}[X]$. *Supposons que*

$$P_1 = a_0 + a_1X + a_2X^2 + a_3X^3 + ... + a_{n_1-1}X^{n_1-1} + a_{n_1}X^{n_1},$$

et

$$P_2 = a'_0 + a'_1X + a'_2X^2 + a'_3X^3 + ... + a'_{n_2-1}X^{n_2-1} + a'_{n_2}X^{n_2}$$

avec $n_1 \geq n_2$ *et* a_{n_1} *et* $a'_{n_2} \neq 0$. *Donc, le polynôme* $P_3 = P_1 - \frac{a_{n_1}}{b_{n_2}}X^{n_1-p}P_2$ *est soit de degré strictement inférieur au degré de* P_1, *soit nul,* .

La méthode de démonstration de l'existence est basée sur une démonstration par récurrence.

Étant donnés P_1 et P_2 deux polynômes de $\mathbb{P}[X]$, avec P_2 non nul ; soit n_2 le degré de P_2.

Premier cas : $P_1 = 0$

On a $P_1 = 0P_2 + 0$, avec $P_1 = 0$ et donc il existe des polynômes P_3 et P_4 satisfaisant les conditions de la division euclidienne (le quotient P_3 et le reste P_4 sont tous les deux égaux au polynôme nul). La propriété est donc vraie dans ce cas.

Deuxième cas : On considère que les polynômes P_1 sont différents de zéro.

En faisant une preuve par récurrence sur le degré des polynômes.

Supposons H_{n_1} la propriété : L'identité de la division est satisfaite pour tout polynôme P_1 de degré inférieur ou égal à n_1.

Montrons que pour tout entier n_1 supérieur ou égal à $n_2 - 1$, on a la propriété (Rappel : n_2 est le degré de P_2)

Étape 1 : Preuve de H_{n_2-1}

Supposons que $\deg P_1 \leq n_2 - 1$, alors l'identité de la division euclidienne est satisfaite avec $Q = 0$ et $R = P_1$ car on a $P_1 = 0P_2 + P_1$ et $\deg P_1 \leq \deg P_2$.

Étape 2 : Preuve de $H_{n_1} \Rightarrow H_{n_1+1}$.

Considérons P_1 un polynôme de degré inférieur ou égal à $n_1 + 1$. S'il est de degré inférieur ou égal à n_1 , l'utilisation de la propriété H_{n_1} donne le résultat. Il suffit donc d'étudier le cas où P_1 est de degré exactement égal à $n_1 + 1$.

Considérons P_1 de degré égal à $n_1 + 1$ différent de $\mathbb{P}[X]$. Supposons que

$$P_1 = a_0 + a_1X + a_2X^2 + a_3X^3 + ... + a_{n_1-1}X^{n_1-1} + a_{n_1}X^{n_1} + a_{n_1+1}X^{n_1+1},$$

avec $a_{n_1+1} \neq 0$.

Puisque $\deg P_2 = n_2$, alors $P_2 = a'_0 + a'_1X + a'_2X^2 + a'_3X^3 + ... + a'_{n_2-1}X^{n_2-1} + a'_{n_2}X^{n_2}$ avec $a'_{n_2} \neq 0$.

En utilisant le lemme démontre que le polynôme $P_3 = P_1 - \frac{a_{n_1+1}}{a'_{n_2}}X^{n_1+1-n_2}P_2$ n'admet plus de terme de degré $n_1 + 1$; il est soit un polynôme nul, soit à un polynôme de degré inférieur ou égal à n_1 .

Alors on a, pour les polynômes P_3 et n_1 , l'identité de la division euclidienne.

Il existe donc Q_1 et R_1 tel que :$P_3 = P_2.Q_1 + R_1$, avec $\deg R_1 < \deg P_2$.

D'où :

$$P_1 = [\frac{a_{n_1+1}}{a'_{n_2}}X^{n_1+1-p} + Q_1]P_2 + R_1$$

avec $\deg R_1 < \deg P_2$.

Ceci est l'identité de la division euclidienne pour les polynômes P_1 et P_2 avec :

$$Q = \frac{a_{n_1+1}}{a'_{n_2}}X^{n_1+1-n_2} + Q_1$$

et $R = R_1$

■

Exemple 5.3 *1. En effectuant la division euclidienne de* $P_1 = 2X^3 - X^2 - 2X + 1$ *par le polynôme* $X^2 + X + 1$ *dans* $R[X]$*, on obtient le quotient* $Q = 2X - 3$ *et le reste* $R = -X + 4$.
On écrit dans ce cas $2X^3 - X^2 - 2X + 1 = (X^2 + X + 1)(2X - 3) - X + 4$
2. En effectuant la division euclidienne de $P = iX^3 - X^2 + 1 - i$ *par le polynôme* $(1+i)X^2 - iX + 3$ *dans* $C[X]$*, on obtient le quotient* $Q = \frac{1+i}{2}X + \frac{-1+2i}{2}$ *et le reste* $R = \frac{-5-4i}{2}X + \frac{5-8i}{2}$.

Dans la partie qui suit, on considère $(\mathbb{P}, +, .)$ un corps commutatif.

Définition 5.3 *[6], [7] Étant donnés* $P_1, P_2, ..., P_n$ *n polynômes de* $\mathbb{P}[X]$.
*1.**Le plus grand diviseur commun pgcd***
Il existe un unique polynôme unitaire ou nul A *de plus grand degré divisant tous les polynômes* P_i*, autrement dit*

$$\sum_{i=1}^{n} P_i\mathbb{P}[X] = A.\mathbb{P}[X].$$

Ce polynôme est appelé le plus grand diviseur commun de la famille $P_1, P_2, ..., P_n$ *et noté* $pgcd(P_1, P_2, ..., P_n)$ *ou bien* $P_1 \wedge P_2 \wedge ... \wedge P_n$.
*2.**Le plus petit commun multiple ppcm***
Étant donnés $P_1, P_2, ..., P_n$ *n polynômes de* $\mathbb{P}[X]$*. Il existe un unique polynôme unitaire ou nul* B *tel que :*
le polynôme B *est un multiple des polynômes* $P_1, P_2, ..., P_n$,
chaque polynôme multiple de $P_1, P_2, ..., P_n$ *est un multiple de* B*, autrement dit*

$$\cap_{i=1}^{n} P_i.\mathbb{P}[X] = B.\mathbb{P}[X].$$

On le note $ppcm(P_1, P_2, ..., P_n)$ *ou bien* $P_1 \vee P_2 \vee ... \vee P_n$, *c'est le plus petit commun multiple des polynômes* $(P_1, P_2, ..., P_n)$.

Caractérisation du pgcd et du ppcm

Théorème 5.2 *[6], [7] Étant donnés* $P_1, P_2, ..., P_n$ *n polynômes de* $\mathbb{P}[X]$.
1. $A = pgcd(P_1, P_2, ..., P_n)$ *si et seulement si A est unitaire ou nul et*
i. $\forall i \in \{1, ..., n\}$, A *divise* p_i,
ii. $\forall i \in \{1, ..., n\}$, $(A' \quad divise \quad p_i) \Rightarrow$ (*A' divise A*).
2.$B = ppcm(P_1, P_2, ..., P_n)$ *si et seulement si B est unitaire ou nul et*
i. $\forall i \in \{1, ..., n\}$, $p_i \quad divise \quad B$,
ii. $\forall i \in \{1, ..., n\}$, $(p_i \quad divise \quad B') \Rightarrow (B \quad divise \quad B')$.

Remarque 5.3 *[7] Étant donnés* $Q_1, Q_2, ..., Q_n$ *n polynômes de* $\mathbb{P}[X]$. *Alors, on a les propriétés suivantes :*
1. Pour tout $\alpha_1, \alpha_2, ..., \alpha_n$

$$ppcm(\alpha_1 Q_1, \alpha_2 Q_2, ..., \alpha_n Q_n) = ppcm(Q_1, Q_2, ..., Q_n)$$

et

$$pgcd(\alpha_1 Q_1, \alpha_2 Q_2, ..., \alpha_n Q_n) = pgcd(Q_1, Q_2, ..., Q_n).$$

2. $\forall l \in \{1, ..., n\}$, *on a*

$$ppcm(Q_1, Q_2, ..., Q_n) = ppcm(ppcm(Q_1, Q_2, ..., Q_l), ppcm(Q_{l+1}, Q_{l+2}, ..., Q_n))$$

et

$$pgcd(Q_1, Q_2, ..., Q_n) = pgcd(pgcd(Q_1, Q_2, ..., Q_l), pgcd(Q_{l+1}, Q_{l+2}, ..., Q_n)).$$

3.2 Algorithme d'Euclide

[7], [10] Pour chercher le pgcd de deux polynômes il suffit d'utiliser l'algorithme d'Euclide qui est une succession de divisions euclidiennes.

Étant donnés P_1 et P_2 deux polynômes de $\mathbb{P}[X]$. Pour chercher le pgcd(P_1, P_2), il suffit d'effectuer la division euclidienne de P_1 par P_2 pour obtenir un reste R_1 tel que

$$P_1 = P_2 Q_1 + R_1 \quad \text{avec} \quad \deg R_1 < \deg P_2.$$

Si le reste R_1 n'est pas nul, on divise P_2 par R_1 et on obtient

$$P_2 = R_1 Q_2 + R_2 \quad \text{avec} \quad \deg R_2 < \deg R_1.$$

Si le reste R_1 n'est pas nul, on recommence la division à chaque étape et on continue ainsi jusqu'à ce que l'on obtienne un reste nul.

Le pgcd de P_1 et P_2 est le dernier reste non nul. On obtient les résultats suivant

$$P_1 = P_2 Q_1 + R_1 \quad \text{avec} \quad \deg R_1 < \deg P_2,$$

$$P_2 = R_1 Q_2 + R_2 \quad \text{avec} \quad \deg R_2 < \deg R_1,$$

$$R_1 = R_2 Q_3 + R_3 \quad \text{avec} \quad \deg R_3 < \deg R_2,$$

$$\vdots$$

$$R_{k-2} = R_{k-1}Q_k + R_k \quad \text{avec} \quad \deg R_k < \deg R_{k-1},$$

$$R_{k-1} = R_k Q_{k+1}$$

et

$$pgcd(P_1, P_2) = pgcd(P_2, R_1) = pgcd(R_1, R_2) = ... = pgcd(R_k, 0) = R_k.$$

Exemple 5.4 *Trouvons pgcd(A,B) avec*

$$A = X^5 - 4X^4 + 6X^3 - 6X^2 + 5X - 2$$

et

$$B = X^4 + X^3 + 2x^2 + X + 1.$$

En utilisant l'algorithme d'Euclide, on divise A par B, on obtient

$$A = B(X-5) + (9X^3 + 2X^2 + 9X + 3).$$

On divise ensuite B par le reste obtenu $R_1 = 9X^3 + 2X^2 + 9X + 3$. *On écrit donc*

$$B = R_1(\frac{1}{9}X) + (\frac{2}{3}X^3 + X^2 + \frac{2}{3}X + 1)$$

et

$$R_1 = (\frac{2}{3}X^3 + X^2 + \frac{2}{3}X + 1)(2X^3 + 3X^2 + 2X + 3) + X^2 + 1.$$

Donc

$$pgcd(A, B) = X^2 + 1.$$

3.3 Polynômes premiers entre eux

Définition 5.4 *[6], [7], [11] Étant donnés* $R_1, R_2, ..., R_n$ *n polynômes de* $\mathbb{P}[X]$. *Alors*
1. Si

$$pgcd(R_1, R_2, ..., R_n) = 1$$

alors, on dit que $R_1, R_2, ..., R_n$ *sont premiers entre eux.*
2. Si

$$pgcd(R_i, R_j) = 1 \quad i \neq j \quad i, j \in \{1, 2, ..., n\},$$

on dit que $R_1, R_2, ..., R_n$ *sont deux à deux premiers entre eux.*

Théorème 5.3 ***Théorème de Bézout*** *[6],*
Étant donnés $R_1, R_2, ..., R_n$ *n polynômes de* $\mathbb{P}[X]$. *Les polynômes* $R_1, R_2, ..., R_n$ *sont premiers entre eux si et seulement s'il existent des polynômes* $V_1, V_2, ..., V_n$ *tels que*

$$\sum_{i=1}^{n} R_i V_i = 1.$$

Preuve. $\Rightarrow$) Supposons que $R_1, R_2, ..., R_n$ sont premiers entre eux , alors $pgcd(R_1, R_2, ..., R_n) = 1$ et $\sum_{i=1}^{n} R_i \mathbb{P}[X] = 1.\mathbb{P}[X]$. Ceci nécessite l'existence des polynômes $V_1, V_2, ..., V_n$ tels que

$$\sum_{i=1}^{n} R_i V_i = 1.$$

$\Leftarrow$) Si $\sum_{i=1}^{n} R_i V_i = 1$. Donc, chaque diviseur commun des polynômes R_i divise 1, par suite $pgcd(R_1, R_2, ..., R_n)$ divise 1, ce qui implique que $pgcd(R_1, R_2, ..., R_n) = 1$. ■

Exemple 5.5 *Montrons que les polynômes* $P_1 = X^4 + 1$ *et* $P_2 = X^3 - 1$ *sont premiers entre eux. En utilisant l'algorithme d'Euclide, on obtient*

$$P_1 = XP_2 + (X+1)$$

$$P_2 = (X+1)(X^2 - X + 1) + (-2)$$

$$X + 1 = (-2)(-\frac{1}{2}X) + 1$$

$$-2 = -2(1) + 0.$$

D'où $pgcd(P_1, P_2) = 1$.

Théorème 5.4 ***Théorème de Gauss*** *[6],[9]*
Étant donnés P_1, P_2, P_3 *trois polynômes de* $\mathbb{P}[X]$. *Si* P_1 *divise* $P_2.P_3$ *et* P_1 *et* P_2 *sont premiers entre eux alors* P_1 *divise* P_3.

Preuve. Les polynômes P_1 et P_2 étant premiers entre eux, il existe donc U_1 et U_2 tels que $U_1.P_1 + U_2.P_2 = 1$. On déduit

$$U_1.P_1.P_3 + U_2.P_2.P_3 = P_3.$$

Par suite le polynôme P_1 divise $U_1.P_1.P_3 + U_2.P_2.P_3$. D'où P_1 divise P_3. ■

Proposition 5.3 *[6] Étant donnés* $P_1, P_2, ..., P_n$, *P,Q,R des éléments de* $\mathbb{P}[X]$, $m_1 et m_2 \in \mathbb{N}$. *Alors*
1. Si $\forall i \in \{1,2,...,n\}, pgcd(P_i, P) = 1$, *alors*

$$pgcd(\prod_{i=1}^{n} P_i, P) = 1.$$

2. Si $\forall i \in \{1,2,...,n\}, pgcd(P_i, P) = 1$, *alors*

$$pgcd(\prod_{i=1}^{n} P_i^{\alpha_i}, P) = 1.$$

quels que soient les entiers $\alpha_i, i \in \{1,2,...,n\}$.
3. Si $pgcd(Q,R) = 1$, *alors* $pgcd(Q^{m_1}, R^{m_2}) = 1$.
4. $pgcd(P,Q).ppcm(P,Q) = \lambda.P.Q$ *pour un certain* $\lambda \in \mathbb{P}$.
5. Si P, Q, R *sont des polynômes tels que P et Q sont premiers entre eux et* P *divise* R *et* Q *divise* R *alors* P.Q *divise* R.

Preuve. 1. $\forall i \in \{1,2,...,n\}, pgcd(P_i, P) = 1$, alors on peut trouver des polynômes $U, U_i, i \in \{1,2,...,n\}$ tels que

$$U.P + U_i.P_i = 1, \forall i \in \{1,2,...,n\}.$$

Alors

$$\prod_{i=1}^{n} (U.P + U_i.P_i) = 1$$

d'où P et $\prod_{i=1}^{n} P_i$ sont premiers entre eux.
2. En utilisant la récurrence dans la première propriété, on obtient le résultat.
3. C'est un résultat qui découle de la propriété précédente.
4. Soit $D = pgcd(P,Q)$ et $M = ppcm(P,Q)$. Par le théorème de Bézout, il existe $(u,v) \in \mathbb{P}[X]^2$ tel que $U.P + V.Q = D$. En multipliant cette égalité par M, on obtient $M.U.P + M.V.Q = D$. Puisque M est un multiple de Q alors P.M est aussi un multiple de P.Q. D'autre part,

puisque M est un multiple de P alors Q.M est un multiple de P.Q. Alors D.M est un multiple de P.Q.
D'après les propriétés des multiples des polynômes, on peut trouver un scalaire λ non nul tel que $D.M = \lambda.P.Q$.
5. P et Q sont premiers entre eux, alors par le théorème de Bézout, il existe deux polynômes U_1 et U_2 dans $\mathbb{P}[X]$ tels que $P.U_1 + Q.U_2 = 1$. D'où,

$$R = P.U_1.R + Q.U_2.R.$$

Or il existe deux polynômes U_1' et U_2' dans $\mathbb{P}[X]$ tels que $R = U_1'.P$ et $R = U_2'.Q$. Donc, on a

$$R = P.U_1.U_2'.Q + Q.U_2.U_1'.P = P.U_1.U_2'.Q + Q.U_2.U_1'.P = P.Q(U_1.U_2' + U_2.U_1')$$

d'où le résultat. ■

Définition 5.5 ***Polynôme irréductible*** *[6], [7], [9]*
Un polynôme P de $\mathbb{P}[X]$ *est dit polynôme irréductible (ou premier) dans* $\mathbb{P}[X]$ *si* $\deg P \geq 1$ *et s'il n'est divisible que par les polynômes associés à P et à 1, c'est à dire que P soit une constante et que pour tout* $(P_1, P_2) \in \mathbb{P}[X]^2$*, on ait*

$$P = P_1.P_2 \Rightarrow (\deg P_1 = 0 \quad ou \quad \deg P_2 = 0)$$

Exemple 5.6 *1. Chaque polynôme de degré 1 est irréductible, car le produit de deux polynômes non constants est au moins de degré 2.*
2. Le polynôme $P = X^2 + 2X - 3$ *est un polynôme réductible car il est divisible par deux polynômes irréductibles* $X - 1$ *et* $X + 3$ *dans* $\mathbb{R}[X]$ *et dans ce cas ,* $P = (X-1)(X+3)$.
3. $Q = X^2 + 1$ *est irréductible dans* $\mathbb{R}[X]$ *car on ne peut pas l'écrire comme produit de deux polynômes de degré 1 à coefficients dans* $\mathbb{R}$.

Proposition 5.4 *[9] Tous les polynômes de degré 1 dans* $\mathbb{C}[X]$ *sont irréductibles.*

Preuve. Il est clair que tout polynôme de degré 1 est irréductible. De plus, en utilisant le théorème de d'Alembert qui nous informe qu'un polynôme non constant est scindé sur $\mathbb{C}[X]$, autrement dit produit de polynômes de degré 1. Par suite, tout polynôme de degré inférieur ou égale 2 est réductible. ■

Remarque 5.4 *1. Chaque polynôme de degré 1 est irréductible de* $\mathbb{R}[X]$*, de même pour les polynômes de degré 2 dont le discriminant est strictement négatif.*
Si p est un polynôme irréductible dans $\mathbb{P}[X]$ *ne l'est pas forcément dans* $\mathbb{P}'[X]$ *où* $\mathbb{P}[X]$ *est un sous corps de* $\mathbb{P}'[X]$ *. Par exemple,* $P = X^2 + 9$ *est irréductible dans* $\mathbb{R}[X]$*, mais pas dans* $\mathbb{C}[X]$ *puisque* $P = (X - 3i)(X + 3i)$.

Proposition 5.5 *[9]*
1. Tout polynôme R irréductible est premier avec tous les polynômes qu'il ne divise pas.
2. Un polynôme irréductible R divise un produit $\prod_{i=1}^{n} R_i$ *si et seulement si R divise l'un des facteurs* R_i.

Preuve. Étant donnés R et $R_1, R_2, ..., R_n$ des polynômes de $\mathbb{P}[X]$.
1. On sait que les diviseurs communs à R et à un polynôme R' sont des diviseurs de R, donc sont, soit constants, soit associés à R. Par suite, si R ne divise pas R', les seuls diviseurs commun à R et R' sont les constantes.
2. Supposons que R ne divise aucun des facteurs R_i, dans ce cas R est premier avec chacun d'entre eux et alors avec le produit $\prod_{i=1}^{n} R_i$, d'où R n'est pas un diviseur de ce produit. La réciproque est évidente. ■

3.4 Décomposition d'un polynôme en facteurs irréductibles

Proposition 5.6 *[9] Tout polynôme non constant de* $\mathbb{P}[X]$ *se décompose d'une façon unique comme produit d'un scalaire par un produit de polynômes irréductibles unitaires de* $\mathbb{P}[X]$.

Preuve. Existence En utilisant une démonstration par récurrence, on prouve pour $n \geq 1$ la propriété A_n :" chaque polynôme non constant de $\mathbb{P}[X]$ de degré inférieur ou égal à n peut se décomposer sous forme d'un produit de polynômes irréductibles."
-A_1 est vérifiée puisque chaque polynôme de degré 1, étant irréductible, est un produit d'un seul polynôme irréductible.
- On suppose que A_n est vraie. Étant donné R un polynôme de degré $n+1$.
  - Si R est irréductible, alors c'est un produit d'un seul polynôme irréductible.
  - Dans le cas inverse, il existe deux polynômes non constants R' et R" tels que $R = R'.R''$ et donc il est évident que R' et R" ont des degrés strictement inférieurs à celui de R et l'on peut leur appliquer l'hypothèse de récurrence, ce qui donne une décomposition de R en un produit de polynômes irréductibles.

Pour obtenir la décomposition annoncée, il suffit de mettre en facteur les coefficients dominants de chaque polynôme irréductible.
Unicité Étant donné $R = \alpha.R_1.R_2....R_k$ une telle décomposition d'un polynôme R. Donc, le scalaire α représente le coefficient dominant de R. D'autre part, tout polynôme irréductible unitaire R_i est un diviseur R et inversement si un polynôme irréductible unitaire Q est un diviseur de R, alors c'est un diviseur de l'un des R_i alors, ils sont égaux puisqu'il s'agit de deux irréductibles unitaires. Les facteurs de cette décomposition sont donc tous les diviseurs irréductibles unitaires de R. Supposons donc deux décompositions de R que l'on peut donc écrire

$$R = \alpha.R_1^{\lambda_1}.R_2^{\lambda_2}...R_r^{\lambda_r},$$

avec les R_i sont irréductibles unitaires et deux à deux différents.
Si, pour un entier i, on a $\alpha_i \neq \beta_i$, par exemple $\lambda_i < \beta_i$, alors on a

$$\prod_{j\neq i} R_j^{\lambda_j} = R_i^{\beta_i-\lambda_j} \prod_{j\neq i} R_j^{\beta_i}$$

et donc R_i divise $\prod_{j\neq i} R_j^{\lambda_j}$, ce qui est une contradiction car R_i est premier avec R_j si $j \neq i$.
Par suite, $\forall i, \lambda_i = \beta_i$, d'où l'unicité de la décomposition. ■

Exemple 5.7 *Le polynôme* X^4-1 *se décompose en facteurs irréductibles dans* $\mathbb{R}[X]$ *comme suit*

$$X^4-1 = (X^2-1)(X^2+1) = (X-1)(X+1)(X^2+1)$$

et dans $\mathbb{C}[X]$ *comme suit*

$$X^4-1 = (X^2-1)(X^2+1) = (X-1)(X+1)(X+i)(X+i).$$

3.5 Fonction polynôme d'une variable

Définition 5.6 *[9] Étant donné* $R = a_0 + a_1X + a_2X^2 + a_3X^3 + ... + a_{n-1}X^{n-1} + a_nX^n$ *un polynôme de* $\mathbb{P}[X]$.
La fonction définie par

$$\begin{array}{rccl} \tilde{R}: & \mathbb{P} & \longrightarrow & \mathbb{P} \\ & X & \longmapsto & \tilde{R}(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + ... + a_{n-1}X^{n-1} + a_nX^n. \end{array}$$

est appelée fonction polynôme d'une variable X *associé à R.*

Remarque 5.5 *1. Un élément* $\lambda \in \mathbb{P}$ *est appelé une racine (ou un zéro) de R si* $\tilde{R}(\lambda) = 0$.
2. Pour que $\lambda \in \mathbb{P}$ *soit une racine de R, il faut et il suffit que* $X - \lambda$ *divise R.*
3. La dérivée de la fonction polynôme du R est la fonction notée $\tilde{R}'(X)$ *définie par*

$$\tilde{R}'(X) = a_1 + 2a_2X + 3a_3X^2 + ... + (n-1)a_{n-1}X^{n-2} + na_nX^{n-1}.$$

Théorème 5.5 *[9] Étant donné* $S \in \mathbb{P}[X]$ *et* $\lambda \in \mathbb{P}$. *Alors*
1. En effectuant la division euclidienne de S par $X-\lambda$, *on obtient un reste qui est exactement* $\tilde{S}(\lambda)$.
2.$X - \lambda$ *divise S si est seulement si* λ *est une racine de S .*

Preuve. 1. En effectuant la division euclidienne, on obtient

$$S = (X - \lambda)Q + R$$

où Q est le quotient et R est le reste de la division. Alors,

$$\tilde{S}(X) = (X - \lambda)\tilde{Q} + \tilde{R}.$$

Donc

$$\tilde{S}(\lambda) = \tilde{R}(\lambda)$$

or $\deg R < 1$. On déduit que R est constant , ce qui implique que $\tilde{R} = R$, $\tilde{R}(\lambda) = R$ et $\tilde{S}(\lambda) = R$.
2. C'est un résultat direct de la première propriété de ce théorème. ■

3.6 Ordre de multiplicité d'une racine

Définition 5.7 *[9] Soit* $S \in \mathbb{P}[X]$ *et* $\lambda \in \mathbb{P}$ *une racine de S. On appelle ordre de multiplicité de la racine* λ *de S, le plus grand* $k \in \mathbb{N}$ *tel que* $(X - \lambda)^k$ *divise S.*

- *Si* $k = 1$, λ *est appelé une racine simple de S,*
- *Si* $k = 2$, λ *est appelé une racine double de S,*
- *Si* $k = 3$, λ *est appelé une racine triple de S etc...*

Exemple 5.8 *Le polynôme* $X^3 - 8X^2 + 5X + 50$ *possède une racine simple* $X = -2$ *et une racine double* $X = -5$ *car*

$$X^3 - 8X^2 + 5X + 50 = (X + 5)^2(X + 2).$$

Théorème 5.6 *[9] Étant donné* $S \in \mathbb{P}[X]$ *et* $\lambda \in \mathbb{P}$. λ *est une racine simple de S si et seulement si* $\tilde{S}(\lambda) = 0$ *et* $\tilde{S}'(\lambda) \neq 0$.

Preuve. En utilisant la définition d'une racine simple, on a λ est une racine simple si et seulement s'il existe un polynôme Q dans $\mathbb{P}[X]$ tel que

$$S = (X - \lambda).Q$$

et $Q(\lambda) \neq 0$ or

$$\tilde{S}' = \tilde{Q} + (X - \lambda)\tilde{Q}'$$

donc

$$\tilde{S}'(\lambda) = \tilde{Q}(\lambda)$$

d'où le résultat. ■

Remarque 5.6 *Pour montrer que* λ *est une racine d'ordre* m *d'un polynôme* S *il suffit de montrer que*

$$\tilde{S}(\lambda)=0,\tilde{S}'(\lambda)=0,...,\tilde{S}^{(m-1)}(\lambda)=0,\tilde{S}^{(m)}(\lambda)\neq 0.$$

Exemple 5.9 *Le polynôme* $P=(X^2-2X-3)^2$ *possède deux racines doubles* $X=-1$ *et* $X=3$ *car*

$$P=(X+1)^2(X-3)^2.$$

Proposition 5.7 *[9] Étant donné* $P\in\mathbb{P}[X]$ *et* $\lambda_1,\lambda_2,...\lambda_r\in\mathbb{P}$ *sont des racines deux à deux différentes de* S*, d'ordre de multiplicité respectif* $m_1,m_2,...,m_r$*. Alors* $\prod_{i=1}^{r}(X-\lambda_i)^{m_i}$ *divise* S*.*

Preuve. Pour tout $i\in\{1,...,r\}$, on a $(X-\lambda_i)$ sont des polynômes premiers entre eux car $\lambda_1,\lambda_2,...,\lambda_r\in\mathbb{P}$ sont des racines deux à deux distincts de S. Alors, $(X-\lambda_i)^{m_i}$ sont premiers entre eux. En utilisant la Proposition 5.3, on obtient $\prod_{i=1}^{r}(X-\lambda_i)^{m_i}$ divise S puisque $(X-\lambda_i)^{m_i}$ divise S. ■

4 Exercices corrigés

Exercice 5.1 *Effectuer la division euclidienne de* X^m *par* X^2-X-2 *dans* $\mathbb{R}[X]$ *en précisant le reste de cette division pour tout* $m\in\mathbb{N}$ *fixé.*

Solution. En effectuant la division euclidienne, on peut trouver deux polynômes $(P_1,P_2)\in(\mathbb{R}[X])^2$ unique tel que :

$$X^m=(X^2-X-2)P_1+P_2$$

et $\deg(P_2)<2$. Donc, il existe $(i,j)\in(\mathbb{R})^2$ unique tel que $P_2=iX+j$. Puisque

$$X^2-X-2=(X+1)(X-2),$$

on obtient , en remplaçant X par -1 et par 2

$$\begin{cases}(-1)^m &= -i+j\\ 2^m &= 2i+j\end{cases}$$

En résolvant ce système linéaire de deux équations à deux inconnues, par exemple en utilisant les coefficients indiqués, et on trouve

$$3i=2^m-(-1)^m,\quad 3j=2^m+2(-1)^m.$$

Par suite, le reste de la division euclidienne de X^m par X^2-X-2 est

$$P_2=\frac{1}{3}(2^m-(-1)^m)X+\frac{1}{3}(2^m+2(-1)^m).$$

Exercice 5.2 *Préciser l'ensemble des* $m\in\mathbb{N}^*$ *tels que* $(X^4+1)^m-X^m$ *soit divisible par* X^2+X+1 *dans* $\mathbb{R}[X]$.

Solution. On note $K = X^2 + X + 1$ et $S_m = (X^4+1)^m - X^m$. Puisque $K = (X-l)(X-l^2)$ dans $\mathbb{C}[X]$, K est un polynôme scindé simple sur $\mathbb{C}$, par suite :

$$K \quad \text{divise} \quad S_m \Leftrightarrow S_m(l) = 0 \quad \text{et} \quad S_m(l^2) = 0).$$

D'autre part, sachant que $S_m \in \mathbb{R}[X]$, on a

$$S_m(l^2) = S_m(l) = \overline{S_m(l)},$$

donc

$$A \quad \text{divise} \quad S_m \Leftrightarrow S_m(l) = 0.$$

Et :

$$\begin{aligned} S_m(l) = 0 &\Leftrightarrow (l^4+1)^m - l^m = 0 \\ &\Leftrightarrow (l+1)^m = l^m \\ &\Leftrightarrow (-l^2)^m = l^m \\ &\Leftrightarrow (e^{\frac{l\pi}{3}})^m = (e^{\frac{2l\pi}{3}})^m \\ &\Leftrightarrow m\tfrac{\pi}{3} \equiv \tfrac{2m\pi}{3}[2\pi] \\ &\Leftrightarrow m\tfrac{\pi}{3} \equiv 0[2\pi] \\ &\Leftrightarrow m \equiv 0[6]. \end{aligned}$$

On déduit que l'ensemble des m demandé est l'ensemble contient tous les multiples de 6 dans $\mathbb{N}^*$.

Exercice 5.3 *Écrire la factorisation en produit de polynômes irréductibles dans* $\mathbb{R}[X]$*, des polynômes suivants :*
1. $Y^6 + 9Y^3 + 8$,
2. $Y^4 - 2Y^2 + 9$,
3. $Y^4 + Y^2 - 6$.

Solution. 1. On peut réécrire le premier polynôme sous forme d'un trinôme en Y^3 :

$$\begin{aligned} Y^6 + 9Y^3 + 8 &= (Y^3+1)(Y^3+8) \\ &= (Y+1)(Y^2-Y+1)(Y+2)(Y^2-2Y+4). \end{aligned}$$

Les deux termes du second degré sont irréductibles dans $\mathbb{R}[X]$, puisque le discriminant est strictement négatif.
2.

$$\begin{aligned} Y^4 - 2Y^2 + 9 &= (Y^2+3)^2 - 8Y^2 \\ &= (Y^2+3-2\sqrt{2}Y)(Y^2+3+2\sqrt{2}Y) \\ &= (Y^2-2\sqrt{2}Y+3)(Y^2+2\sqrt{2}Y+3). \end{aligned}$$

De même que précédemment, les deux termes du second degré sont irréductibles dans $\mathbb{R}[X]$, puisque le discriminant est strictement négatif.

3. En écrivant le polynôme sous forme d'un trinôme bicarré :

$$\begin{aligned} Y^4 + Y^2 - 6 &= (Y^2-2)(Y^2+3) \\ &= (Y-\sqrt{2})(Y+\sqrt{2})(Y^2+3). \end{aligned}$$

Exercice 5.4 *Chercher le pgcd dans* $\mathbb{K}[X]$ *(*$\mathbb{K}$ *étant* $\mathbb{R}$ *ou* $\mathbb{C}$*) des polynômes* P_1 *et* P_2 *suivants*

$$P_1 = Y^5 - 2Y^4 + Y^3 - Y^2 + 2Y - 1$$

et

$$P_2 = Y^3 - Y^2 + 2Y - 2.$$

Soit D ce pgcd. Trouver P_1' *et* P_2' *tels que*

$$P_1 = DP_1'$$

et

$$P_2 = DP_2'.$$

Déterminer le ppcm de P_1 *et* P_2.

Solution. En utilisant l'algorithme d'Euclide, on peut déterminer le pgcd des polynômes. On obtient

$$P_1 = P_2(Y^2 - Y - 2) + Y^2 + 4Y - 5.$$

Alors, le pgcd de P_1 et P_2 est égal au pgcd des polynômes P_2 et $Y^2 + 4Y - 5$. En effectuant la division euclidienne de P_2 par $Y^2 + 4Y - 5$, on trouve

$$P_2 = (Y^2 + 4Y - 5)(Y - 5) + 27Y - 27.$$

Puisque

$$27Y - 27 = 27(Y - 1),$$

ensuite la division euclidienne de $Y^2 + 4Y - 5$ par $Y - 1$, puisque

$$pgcd(P_1, P_2) = pgcd(P_1, \alpha P_2)$$

si α est un scalaire non nul.
Le pgcd des polynômes P_2 et $Y^2 + 4Y - 5$ est égal au pgcd des polynômes

$$Y^2 + 4Y - 5$$

et

$$Y - 1.$$

Par la division euclidienne de $Y^2 + 4Y - 5$ par $Y - 1$, on déduit le quotient $Y + 5$ et le reste 0. Par suite $Y^2 + 4Y - 5$ est un multiple du polynôme $Y - 1$. Alors le polynôme $Y - 1$ est le pgcd de $Y^2 + 4Y - 5$ et $Y - 1$. Donc celui de P_2 et $Y^2 + 4Y - 5$ et donc le pgcd de P_1 et P_2.

2. Étant donné $D = Y - 1$. Pour chercher P_1' et P_2' tels que $P_1 = DP_1'$ et $P_2 = DP_2'$, on divise P_1 et P_2 par D. On trouve

$$P_1 = (Y - 1)(Y^4 - Y^3 - Y + 1)$$

et

$$P_2 = (Y - 1)(Y^2 + 2).$$

Pour trouver le ppcm de P_1 et P_2, on fait appelle à la formule (polynômes P_1 et P_2 étant unitaires) :

$$P_1P_2 = pgcd(P_1, P_2) \times ppcm(P_1, P_2).$$

En calculant le produit P_1P_2, puis en divisant le résultat par le pgcd de P_1 et P_2, mais il vaut mieux d'utiliser la question 2.

$$P_1 = DP_1'$$

et

$$P_2 = DP_2'$$

où $P_1' = Y^4 - Y^3 - YX + 1$ et $P_2' = Y^2 + 2$.
Comme

$$P_1P_2 = DP_1'DP_2' = D.ppcm(P_1, P_2)$$

on en déduit que $ppcm(P_1, P_2) = DP_1'P_2'$, autrement dit

$$ppcm(P_1, P_2) = (Y-1)(Y^4 - Y^3 - Y + 1)(Y^2 + 2)$$

$$= Y^7 - 2Y^6 - 5Y^4 + 4Y^3 - Y^2 + 4Y + 1).$$

On peut remarquer que

$$ppcm(P_1, P_2) = P_1P_2' = P_1'P_2$$

comme $P_1 = DP_1'$ et $P_2 = DP_2'$ et l'on pouvait alors calculer un de ces deux produits.

Exercice 5.5 *1. Prouver que si y_0 est racine commune à $P(y)$ et $Q(y)$, elle l'est également de leur PGCD et inversement.*
2. Déduire les racines multiples de $P = y^5 + y^3 - 4y^2 - 3y - 2$.

Solution. 1. Supposons que A est le PGCD de P et Q, on a

$$P = AA_1$$

et

$$Q = AA_2.$$

Si $A(y_0) = 0$ alors $P(y_0) = A(y_0)A_1(y_0)$ et de même $Q(y_0) = A(y_0)A_2(y_0)$.
Inversement, supposons que y_0 est une racine de $P(y)$ et $Q(y)$,en utilisant le théorème de Bézout, on peut trouver deux polynômes U et V tels que

$$A = PU + QV$$

et

$$A(y_0) = P(y_0)U(y_0) + Q(y_0)V(y_0) = 0.$$

2. Supposons que y_0 est une racine multiple de $P = y^5 + y^3 - 4y^2 - 3y - 2$ alors elle est racine de $P' = 5y^4 + 3y^2 - 8y - 3$.
Trouvons le PGCD de P et P' par l'algorithme d'Euclide :

$$P = P'.\frac{y}{5} - \frac{2}{5}(y^3 + 6y^2 + 6y + 5)$$

$$P' = (y^3 + 6y^2 + 6y + 5)(5y - 30) + 147(y^2 + y + 1)$$

$$y^3 + 6y^2 + 6y + 5 = (y^2 + y + 1)(y + 5)$$

le reste étant nul le PGCD est $y^2 + y + 1$. Le polynôme P possède comme racines multiples celles de $y^2 + y + 1$ autrement dit

$$k = \frac{-1 + i\sqrt{3}}{2} \quad \text{et} \quad k^2 = \frac{-1 - i\sqrt{3}}{2}.$$

Ces racines sont de multiplicité au moins égal à 2 donc P est divisible par $y^2 + y + 1$ qui est de degré 4, P étant de degré 5 il ne peut y en avoir d'autres.

Exercice 5.6 *Montrer que les polynômes A et B sont premiers entre eux si et seulement si* $A+B$ *et* AB *sont premiers entre eux.*

Solution. Si A et B sont premiers entre eux, alors

$$(A+B)\wedge A=1$$

et

$$(A+B)\wedge B=1.$$

On a donc :

$$(A+B)\wedge AB=1$$

Inversement, supposons que $A+B$ et AB sont premiers entre eux. Alors, dans le cas où D divise A et B, alors D divise $A+B$ et AB . Par suite, D est de degré 0.

5 Exercices proposés

Exercice 5.7 *Étant donné* $m\in\mathbb{N}$, *prouver que le polynôme* Y^2-Y+1 *divise*

$$(Y-1)^{m+2}+Y^{2m+1}\in\mathbb{C}[X].$$

Exercice 5.8 *Préciser tous les polynômes A tels que :*

$$A(2)=6, A'(2)=1 \quad et \quad A''(2)=4$$

et

$$\forall k\geq 3, A^{(k)}(2)=0.$$

Exercice 5.9 *Donner la factorisation en produit de polynômes irréductibles dans* $\mathbb{R}[X]$, *des polynômes suivants :*
1. $(Y^2-4Y+1)^2+(3Y-5)^2$,
2. Y^5+1,
3. Y^6-1.

Exercice 5.10 *Étant donnés* α_1,α_2, α_3,α_4 *des entiers naturels. Considérons les deux polynômes*

$$A=Y^{4\alpha_1+3}+Y^{4\alpha_2+2}+Y^{4\alpha_4+1}+Y^{4\alpha_4}$$

et

$$B=Y^3+Y^2+Y+1.$$

Montrer que B divise A.

Exercice 5.11 *Déterminer le PGCD des deux polynômes* $X^6-5X^4+4X^3-+10X^2+3X-2$ *et* $X^3+2X^2+4X+11$.

Bibliographie

[1] **E. Azoulay, J. Avignant**, (1984) *Mathématiques 4. algèbre,* McGrow-Hill-Paris. 16, 17, 18, 21, 22, 23, 39, 40, 41, 42, 49, 50, 51, 52, 60, 61, 62

[2] **A. Calvo, F. Boschiet**, (1996) *exercices d'algèbre,* 1 er cycle scientifique, 1ere année préparation aux grandes écoles, Armand Colin-collection U, Paris 5. 3, 16, 39, 49, 72

[3] **C. Deschamps et A. Warusfel**, (2003) *Mathématiques, Tout en un, 1re année , cours et exercices corrigés,* 2édition, nouveau tirage, DUNOD, Paris . 16, 17, 18, 39, 40, 41, 42, 49, 50, 51, 52, 56, 58, 59, 60, 61, 62

[4] **Exo7**, *Cours et exercices de maths, Licence Créative Commons-BY-NC-SA-3.0 FR,* exo7.emath.fr . 3, 4, 5, 6, 7, 8, 9, 10, 16, 21, 23, 24, 25, 27, 39, 49, 72

[5] **D. Fredon, M.Maumy-Bertran**, (2009) *Mathématiques, algèbre et géométrie en 30 fiches,* Dunod, Paris. 3, 4, 5, 6, 7, 8, 9, 10, 16, 21, 22, 23, 24, 25, 27, 28, 29, 30

[6] **X. Gourdon**, (1996) *Les mathématiques en tête Algèbre,* INRIA-Rocquencourt, ellipses. 49, 50, 51, 52, 53, 56, 57, 58, 59, 61, 62, 72, 73, 74, 76, 77, 78, 79, 80

[7] **S. Lipschutz**, (1973) *Algèbre linéaire, cours et problèmes,* McGraw-Hill Inc, New York. 16, 20, 21, 22, 39, 72, 74, 75, 76, 77, 78, 80

[8] **J. Marie Monier**, (2008) *Les méthodes et exercices de mathématiques PCSI-PTSI,* Dunod, Paris. 3, 16, 39, 49, 72

[9] **J. Ramis et A. Warusfel**, (2006) *Mathématiques Tout en un pour la licence, niveau L1, cours complet avec 270 exercices corrigés,* Série Ramis, DUNOD. 3, 4, 5, 6, 7, 8, 9, 10, 16, 20, 21, 23, 24, 25, 27, 28, 29, 30, 39, 40, 41, 42, 49, 50, 51, 52, 72, 79, 80, 81, 82, 83

[10] **J. Ramis et A. Warusfel**, (2007) *Mathématiques Tout en un pour la licence, niveau L2, cours complet avec applications et 760 exercices corrigés,* Série Ramis, DUNOD. 41, 49, 72, 73, 74, 77

[11] **L. Schwarts**, (2003) *Algèbre 3 eme année, Cours et exercices avec solutions,* Série Ramis, DUNOD, Paris . 49, 50, 51, 52, 53, 56, 72, 74, 75, 78

[12] **A. Szpirglas**, (2001) *exercices d'algèbre,* Cassini, Paris . 3, 16, 39, 49, 72