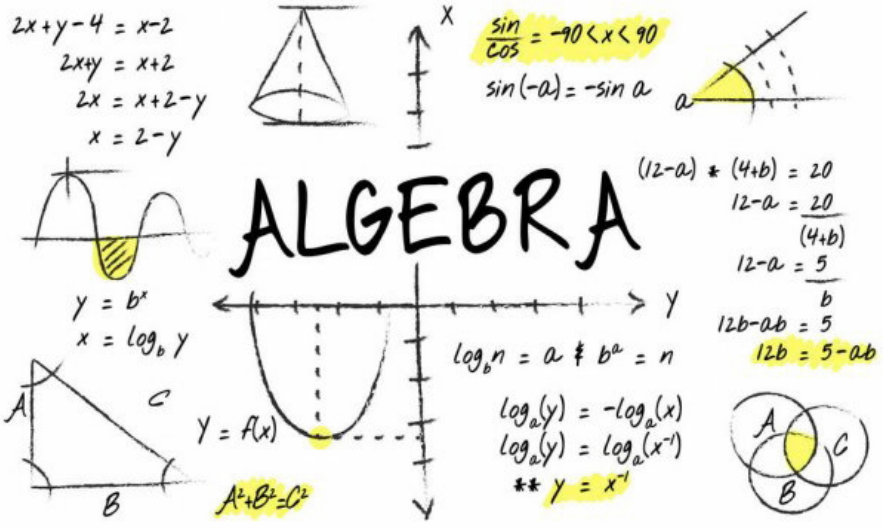
RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abdelhamid Ibn Badis de Mostaganem
Faculté des Sciences Exactes et de l'Informatique

Algèbre I
Cours et exercices

Réalisé par

Louiza TABHARIT



Année universitaire

2020/2021

Table des matières

Remerciements **i**

Notations **ii**

Introduction **iii**

1 Notions de Logique **2**

1.1 Assertions et Prédicats 2

1.2 Combinaisons Logiques 3

1.2.1 L'opérateur Logique "et" (conjonction) 3

1.2.2 L'opérateur Logique "ou" (disjonction) 4

1.2.3 La Négation 4

1.2.4 L'implication 5

1.2.5 Équivalence logique 6

1.2.6 Tautologie 7

1.2.7 Assertions Incompatibles 8

1.3 Quantificateurs Mathématiques 8

1.3.1 Quantificateur Universel 8

1.3.2 Quantificateur Existentiel 9

1.4 Types de Raisonnements 10

1.4.1 Raisonnement Direct 10

1.4.2 Raisonnement par disjonction des Cas 11
1.4.3 Raisonnement par Contraposée 12
1.4.4 Raisonnement par l'Absurde 12
1.4.5 Raisonnement par un Contre-exemple 13
1.4.6 Raisonnement par Récurrence 13
1.5 Exercices corrigés 16
1.6 Exercices supplémentaires 19

2 Ensembles et Applications 22
2.1 Ensembles 22
2.1.1 Notion d'Ensemble 22
2.1.2 Inclusion d'ensembles 24
2.1.3 Égalité d'ensembles 25
2.1.4 Opérations sur les ensembles 25
2.2 Relations, Fonctions, Applications 31
2.2.1 Relations 31
2.2.2 Fonctions 32
2.2.3 Applications 34
2.3 Exerices corrigés 42
2.4 Exercices supplémentaires 47

3 Relations Binaires 49
3.1 Définitions et Propriétés 49
3.2 Relation d'équivalence 50
3.3 Relations d'ordre 51
3.3.1 Parties majorées, minorées, bornées 51
3.4 Exercices corrigés 54
3.5 Exercices supplémentaires 61

4 Structures Algébriques 62
4.1 Lois de composition internes 62

4.1.1 Commutativité, Associativité, Distributivité 63
4.1.2 Élément neutre, élément symétrique, stabilité 63
4.2 Morphisme, Endomorphisme, Isomorphisme, Automorphisme 65
4.3 Groupes, Anneaux, Corps 66
4.3.1 Structure de groupe 66
4.3.2 Congruence dans $\mathbb{Z}$ 70
4.3.3 Structure d'anneaux 71
4.3.4 Structure de Corps 76
4.4 Exercices corrigés 77
4.5 Exercice supplémentaire 83

5 Anneaux de Polynômes 86
5.1 Introduction 86
5.2 Polynômes 86
5.3 Opérations sur les polynômes 87
5.3.1 Somme et produit de deux polynômes 87
5.3.2 Division dans $(A[X], +, \cdot)$ 88
5.4 Division euclidienne 89
5.4.1 Le pgcd et le ppcm de deux ou plusieurs polyômes 89
5.4.2 Algorithme d'Euclide 91
5.4.3 Polynômes premiers entre eux 92
5.5 Polynômes irréductibles 92
5.5.1 Factorisation des polynômes 93
5.6 Exercices corrigés 94
5.7 Exercices supplémentaires 96

Bibliographie 96

Remerciements

Je tiens à remercier, très chaleureusement, le professeur Ahmed Medeghri pour l'expertise méticuleuse de ce document.

Je souhaiterais exprimer ma gratitude au professeur Berrabah Bendoukha pour ses multiples conseils, pour toute le temps qu'il a consacré à lire et relire ce manuscrit et pour l'aide qu'il m'a apporté.

Je remercie, également, mes amies et collègues N. Lahmar-Ablaoui, M. Hamou mamar, L. Bouzid, H. Ali Merina pour leurs encouragements.

Merci à mon époux Mohammed el Mustapha Miroud pour sa patience, ce travail n'aurait pu être mené à bien sans son aide, sa disponibilité et son soutien quotidien.

J'adresse aussi mes remerciements à mes parents, mes soeurs et mon frère.

Notations

- ✓ $\mathbb{N}$: L'ensemble des nombres entiers naturels.
- ✓ $\mathbb{Z}$: L'ensemble des nombres entiers relatifs.
- ✓ $\mathbb{Q}$: L'ensemble des nombres rationnels.
- ✓ $\mathbb{R}$: L'ensemble des nombres reéls.
- ✓ $\sum$: Sigma : somme
- ✓ Π : Pi : produit
- ✓ Ω : Omega
- ✓ $\digamma$: Digamma
- ✓ Γ : Gamma
- ✓ Φ : Phi
- ✓ Ψ : Psi

INTRODUCTION

L'algèbre est une branche de mathématique intervenant dans tout autre fondement et théorie mathématique et aussi dans les sciences techniques et naturelles. Le Bagage algèbrique est indispensable pour tout scientifique, il permet de formuler des données , simplifier des problèmes réels et les résoudre en utilisant des symboles et des caractères alphabétiques (pour les variables inconnues).

Ce document est un support de cours d'algèbre I. Il est principalement destiné aux étudiants de 1 ère année en licence mathématiques et informatique, aux étudiants de certaines écoles supérieures ainsi qu'aux étudiants de certaines classes préparatoires. Il a été réalisé pendant la période dans laquelle j'ai exercé ma charge pédagogique au sein du département de Mathématiques et informatique. J'ai eu l'immence honneur et un grand plaisir de travailler avec le **Prof. Ahmed Medeghri** et ce polycopié est essentiellement inspiré de son cours.

Ce manuel est composé de cinq chapitres subdivisés en deux sections : des notions de cours suivis par une série d'exercices corrigés. Le but de ce cours est de familiariser l'étudiant avec de nouveaux outils algèbriques tout en lui rappellant les prérequis des années ultérieures, la bonne compréhension des notions de base de la théorie des ensembles et des structures algèbriques. Le lecteur désirant explorer plus en détails certaines notions du cours, pourra consulter la bibliographie fournie à la fin du document.

- ✓ La première partie de cet ouvrage est consacrée à la présentation des notions de logiques, la définition du calcul propositionnel, la formulation et le raisonnement mathématique.
- ✓ Le deuxième chapitre est dédié à l'algèbre ensembliste, portant sur la caractérisation et les opérations sur les ensembles, l'image directe et réciproque d'un ensemble par une application.
- ✓ Dans le troisième chapitre, on définit deux types de relations binaires, à savoir une relation d'équivalence et une relation d'ordre. Appuyés par des exemples illustratifs, les notions de classes d'équivalences, majorants, minorants, borne inférieure et suppérieure d'un ensemble sont également abordées.

- ✓ Le chapitre quatre traite une partie très importante et essentielle pour tout apprenant : les Structures algèbriques. En effet, cette section met en évidence les définitions et propriétés liées aux structures de : groupe, anneaux et corps.
- ✓ L'objectif du dernier chapitre est d'enrichir les connaissances antérieures de l'étudiant sur les polynômes, par de nouveaux concepts tels que la divisibilité dans un anneau, le pgcd et le ppcm de deux polynômes et l'irréductibilité.

Chapitre 1

Notions de Logique

La fin du XIX^e siècle fut marquée par la naissance de " la logique symbolique " appelée aujourd'hui " logique mathématique " et qui avait pour objectif initial : la formatlisation des mathématiques et l'étude des raisonnements. Afin de simplifier et abréger l'écriture mathématique, Leibniz a introduit un grand nombre de notations symboliques (quantificateurs, intégral,...etc). Aussi, le calcul de vérité fondé par G. Boole donne un sens symbolique aux combinaisons logiques (conjonction, disjonction, ...etc). Cette branche de mathématique a subi une révolution spéctaculaire au fil du temps avec l'arrivée des travaux d'autres logiciens qui ont contribué dans le fondement de ses rudiments.

1.1 Assertions et Prédicats

Définition 1.1.1 *Une assertion (proposition) est un énnoncé (une phrase) qui peut être soit vrai, soit faux.*

Notation : Généralement, on note les assertions par des lettres majuscules : P, Q, R, A, $B, \cdots$

Exemple 1.1.1

1. A : *"Le nombre* -5 *est un entier naturel".*
2. B : *"Pour tout* $x \in \mathbb{R}$, *on a :* $x^2 \geq 0$".
3. P : *"Jupiter est une planète".*
4. Q : *"Je suis née au mois de septembre".*

Définition 1.1.2 *Soit Ω un ensemble. Un prédicat sur Ω est un enoncé contenant une variable.En remplaçant la variable par des éléments de Ω, on obtient une assertion.*

Exemple 1.1.2

1. *Soit $a \in \mathbb{N}$, l'expression : "a est un multiple de 3 " est un prédicat noté $P(a)$.*

   $P(5)$: " 5 est un multiple de 3 " est une assertion fausse.

   $P(9)$: " 9 est un multiple de 3 " est une assertion Vraie.

2. *Soit $\Omega = \{1, 2, 5, 7, 9\}$. Le prédicat sur Ω : $Q(x)$: " x divise 45 " est vrai si on remplace x par $1, 5, 9$; et $Q(x)$ est faux si x est égal à 2 ou 7.*

3. *Soit $m \in \mathbb{N}$, $R(m)$: " m est pair " est un prédicat sur l'ensemble $\mathbb{N}$. Pour $m = 6$, $R(m)$ est vrai. $R(7), R(11)$ sont des propositions fausses.*

Notation : Si une assertion est vraie (resp. fausse), alors sa valeur logique est notée V (resp. F).

1.2 Combinaisons Logiques

A partir de deux assertions (ou plus) simples, on peut construire de nouvelles assertions dites assertions composées. Ces dernières sont connectées (liées) à l'aide de Connecteurs (ou Opérateurs) logiques. La valeur logique d'une proposition composée dépend de celles des phrases qui la composent et de la nature des connecteurs logiques utilisés. Les résultats peuvent être résumés dans un tableau appelé **Table de vérité**.

1.2.1 L'opérateur Logique "et" (conjonction)

Définition 1.2.1 *Soient P, Q deux assertions. L'assertion "P et Q" notée "$P \wedge Q$" est vraie si P est vraie et Q est vraie.*

Table de vérité

P	Q	$P \wedge Q$
V	V	**V**
V	F	F
F	V	F
F	F	F

Exemple 1.2.1 *P : "2 divise 5", Q :"Le chat est un animal", R :" Mostaganem est en Algérie"*

On a : P est fausse , Q est vraie, R est vraie. Ainsi, $(P \wedge Q)$ est fausse et $(Q \wedge R)$ est vraie.

1.2.2 L'opérateur Logique "ou" (disjonction)

Définition 1.2.2 *Soient P, Q deux assertions. L'assertion "P ou Q" notée "$P \vee Q$" est fausse si P est fausse et Q est fausse.*

Table de vérité :

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	**F**

Exemple 1.2.2 *P : " un entier naturel est strictement négatif ", Q :" Mozart est chinois ", R :" $12 \times 3 = 36$ ".*

Alors : P est fausse ; Q est fausse ; R est vraie. Donc, $(P \vee Q)$ est fausse et $(P \vee R)$ est Vraie.

1.2.3 La Négation

Définition 1.2.3 *La négation d'une assertion P est l'assertion non$P$ qui est vraie si P est fausse et est fausse sinon. non$P$ est notée $\neg P$ ou bien $\overline{P}$.*

Table de vérité :

P	$\neg P$
V	F
F	V

Exemple 1.2.3

1. *P :" Une heure est égale à 60 minutes".$(Vraie)$*

   $\neg P$:" Une heure n'est pas égale à 60 minutes".$(Fausse)$

2. *Q :" Le ciseau est un moyen de transport". $(Fausse)$*

   $\neg Q$:" Le ciseau n'est pas un moyen de transport". $(Vraie)$

1.2.4 L'implication

Définition 1.2.4 *Soient P, Q deux assertions. On appelle l'implication de Q par P l'assertion " $\neg P \vee Q$ ". La phrase " P implique Q " et notée " $P \Rightarrow Q$ " est fausse dans le cas où P est vraie et Q est fausse.*

Table de vérité :

P	Q	$P \Rightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

Exemple 1.2.4 *1. P : "$5 \times 11 - 10 = 45$", Q : " Napoléon est belge".*

P est vraie , Q est fausse, $P \Rightarrow Q$ est fausse mais $Q \Rightarrow P$ est vraie.

2. " $2 < 3 \implies 2^2 = 4$ " est vraie.

3. " Si j'aurai la moyenne, alors je passerai en $2^{ème}$ année" est vraie.

Remarque 1.2.1 *Lorsque la proposition $P \Rightarrow Q$ est vraie, on dit que Q est une condition nécessaire de P, c'est à dire que pour que P soit vraie il faut que Q soit vraie.*
On dit aussi que P est une condition suffisante de Q. Autrement dit, pour que Q soit vraie il suffit que P soit vraie.

Implication Réciproque

Définition : *Soient P, Q deux assertions. L'implication réciproque de $P \Rightarrow Q$ est $Q \Rightarrow P$.*

Remarque 1.2.2 *$P \Rightarrow Q$ et $Q \Rightarrow P$ n'ont pas toujours la même valeur logique.*

Exemple 1.2.5 *-L'implication " $3^3 = 27 \implies 5 < 4$" est fausse. Mais, la réciproque " $5 < 4 \implies 3^3 = 27$" est vraie.*

Contraposée d'une implication

Définition 1.2.5 *Soient P, Q deux assertions. La contraposée de $P \Rightarrow Q$ est la proposition $\overline{Q} \Rightarrow \overline{P}$.*

Remarque 1.2.3 *$P \Rightarrow Q$ et $\overline{Q} \Rightarrow \overline{P}$ ont toujours la même valeur logique.*
On dit qu'une implication et sa contraposée sont équivalentes.

1.2.5 Équivalence logique

Définition 1.2.6 *Deux propositions P et Q deux sont dites équivalentes si les deux implications $(P \Rightarrow Q)$ et $(Q \Rightarrow P)$ sont simultanément vraies. Dans ce cas, on écrit " $P \Leftrightarrow Q$ " .*

La phrase " $P \Leftrightarrow Q$ " se lit : " P équivaut Q " ou encore "P si et seulement si Q".

Remarque 1.2.4 *L'équivalence est vraie si les deux assertions P et Q ont la même valeur de logique.*

Définition 1.2.7 ***Table de vérité***

P	Q	$P \Leftrightarrow Q$
V	V	$\boldsymbol{V}$
V	F	F
F	V	F
F	F	$\boldsymbol{V}$

Exemple 1.2.6
1. $(4 \times 5 = 20) \Leftrightarrow (7 \leq 23)$ *est Vraie.*
2. $(4 \times 5 = 20) \Leftrightarrow (7 \geq 23)$ *est Fausse.*
3. $(4^2 = 10) \Leftrightarrow (6 + 3 = 13)$ *est Vraie.*

Proposition 1.2.1 *Soient P, Q et R des assertions :*

1. $\neg(\neg P) \Leftrightarrow P$
2. $P \wedge P \Leftrightarrow P$
3. $P \vee P \Leftrightarrow P$
4. $P \wedge Q \Leftrightarrow Q \wedge P$
5. $P \vee Q \Leftrightarrow Q \vee P$
6. $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$
7. $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$
8. $\neg\,(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$
9. $\neg\,(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$
10. $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$

11. $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$

12. $[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$

13. $[(P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R)] \Rightarrow (P \Leftrightarrow R)$

14. $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$

Preuve. Pour démontrer ces propositions , on peut établir les tables de vérité :

Propriété (8) : $\neg (P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q)$

P	Q	$\neg (P \wedge Q)$	$\neg P \vee \neg Q$	$\neg (P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$
V	V	F	F	V
V	F	V	V	V
F	V	V	V	V
F	F	V	V	V

Propriété (14) : $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$

P	Q	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$	$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$
V	V	V	V	V
V	F	F	F	V
F	V	V	V	V
F	F	V	V	V

;

Ou bien, en transformant l'expression

$$\begin{aligned}(\neg Q \Rightarrow \neg P) &\Leftrightarrow (\neg (\neg Q) \vee \neg P)\\ &\Leftrightarrow Q \vee \neg P\\ &\Leftrightarrow \neg P \vee Q\\ &\Leftrightarrow P \Rightarrow Q.\end{aligned}$$

□

1.2.6 Tautologie

Définition 1.2.8 *Une proposition (simple ou composée) qui est toujours vraie est appelée* ***tautologie****.*

Exemple 1.2.7 *1. L'assertion "$P \vee \neg P$" est une tautologie. En effet,*

P	V	$P \vee \neg P$
V	F	V
F	V	V

2. L'assertion "$T : [(P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R)] \Rightarrow (P \Leftrightarrow R)$" est une tautologie, car :

P	Q	R	$P \Leftrightarrow Q$	$Q \Leftrightarrow R$	$P \Leftrightarrow R$	$(P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R)$	T
V	V	V	V	V	V	V	V
V	V	F	V	F	F	F	V
V	F	V	F	F	V	V	V
V	F	F	F	V	F	F	V
F	V	V	F	V	F	F	V
F	V	F	F	F	V	V	V
F	F	V	V	F	F	F	V
F	F	F	V	V	V	V	V

1.2.7 Assertions Incompatibles

Définition 1.2.9 *Deux assertions sont dites incompatibles si leurs conjonction est fausse quelque soient leurs valeurs de vérité.*

Exemple 1.2.8 *1. les assertions P , $\neg P$ sont incompatibles. En effet,*

P	$\neg P$	$P \wedge (\neg P)$
V	F	F
F	V	F

2. Les prédicats " $n \leq 3$ " et " $n \geq 7$ " sont incompatibles.

1.3 Quantificateurs Mathématiques

Le mot "Quantificateur" provient du mot "Quantité" et on l'utilise pour décrire une certaine quantité par rapport à un ensemble (tout) . En mathématique, décrire une quantité se fait en utilisant le quantificateur **universel** ou le quantificateur **existentiel** . Le prédicat muni d'un quantificateur est appelé **assertion quantifiée** .

1.3.1 Quantificateur Universel

Définition 1.3.1 *L'expression "Quelque soit" (se lit aussi "Pour tout") est le quantificateur noté " $\forall$ " permttant de définir l'assertion quantifiée : " $\forall x \in \Omega,\ P(x)$ ".*

Exemple 1.3.1 *1.* $\forall n \in \mathbb{N}^*,\ n^2 \geq 1.$ *(vraie)*

2. $\forall x \in \mathbb{R}, \forall y \in \mathbb{R},\ x^2 + y^2 \geq 0.$ (*vraie*)

3. $\forall a \in \mathbb{Z},\ a - 2 \leq 0.$ (*fausse*)

4. $\forall x \in [0, 1[\ ,\ x + 1 \leq 0.$ (*fausse*)

Remarque 1.3.1 *L'assertion " $\forall x \in \Omega,\ P(x)$ " est vraie, si tout les élements de l'ensemble Ω vérifient le prédicat $P(x)$. Elle est fausse si on peut trouver au moins un élément de Ω qui ne vérifie pas $P(x)$.*

1.3.2 Quantificateur Existentiel

Définition 1.3.2 *Le quantificateur "Il existe" noté " $\exists$ " permet de définir l'assertion quantifiée : " $\exists x \in \Omega,\ P(x)$ ".*

Exemple 1.3.2 1. $\exists n \in \mathbb{N},\ n^2 - 3 \geq 1.$ (*vraie*)

2. $\exists x \in \mathbb{R}, \exists y \in \mathbb{R},\ x + y = -5.$ (*vraie*)

3. $\exists x \in \mathbb{R},\ x^2 \leq 0.$ (*fausse*)

4. $\exists x \in \mathbb{C},\ x^2 \leq 0.$ (*vraie*)

Remarque 1.3.2 *L'assertion " $\exists x \in \Omega,\ P(x)$ " est vraie, si on trouve au moins un élément de l'ensemble Ω vérifiant le prédicat $P(x)$. Elle est fausse si tout les éléments de Ω ne vérifient pas $P(x)$.*

Négation des assertions quantifiées

Assertion	Négation
$\forall x \in \Omega,\ P(x)$	$\exists x \in \Omega,\ \neg P(x)$
$\exists x \in \Omega,\ P(x)$	$\forall x \in \Omega,\ \neg P(x)$

.

Exemple 1.3.3

Assertion	*Négation*
$\forall n \in \mathbb{N}, n + 4 > 0$	$\exists n \in \mathbb{N}, n + 4 \leq 0$
$\exists x \in \mathbb{N} : 2x = 3$	$\forall x \in \mathbb{N} : 2x \neq 3$
$\exists n \in \mathbb{Z} : n + 5 \geq 0$	$\forall n \in \mathbb{Z} : n + 5 < 0$
$\forall x \in \mathbb{R}, x^2 + 1 \leq 0$	$\exists x \in \mathbb{R}, x^2 + 1 > 0$
$\exists y \in \mathbb{N} : \forall x \in \mathbb{R}, x < y$	$\forall y \in \mathbb{N} : \exists x \in \mathbb{R}, x \geq y$

.

Remarque 1.3.3 *On peut permuter deux quantificateurs identiques.*
L'ordre des quantificateurs est ***important****. On a*

$$\exists a \in \Omega, \forall b \in \Omega'; P(a,b) \implies \forall b \in \Omega', \exists a \in \Omega; P(a,b) \quad (1)$$

mais,

$$\forall a \in \Omega, \exists b \in \Omega'; P(a,b) \not\Rightarrow \exists b \in \Omega', \forall a \in \Omega; P(a,b) \quad (2)$$

(Preuve de l'implication (1) en exercice).

Exemple 1.3.4 *1- L'ennoncé :" $P(a,b) : \exists n \in \mathbb{N}, \forall k \in \mathbb{N} : k \leq n$ " signifie qu'il existe un entier n plus grand que tous les autres. Ce qui est évidemment faux. Par contre, dire que pour tout entier k on peut trouver un n plus grand que k (" $\forall k \in \mathbb{N}, \exists n \in \mathbb{N} : k \leq n$ ") est vrai.*
2- L'ennoncé :" $P(a,b) : \forall a \in \mathbb{R}, \exists b \in \mathbb{R} : b = a + 1$ " est vrai, car pour tout réel a on peut trouver un réel b tel que $a = b - 1$. Mais, l'assertion " $Q(a,b) : \exists b \in \mathbb{R}, \forall a \in \mathbb{R} : b = a + 1$ " sigifie qu'il existe un b qui s'écrit en fonction de tout les réels a comme étant $b = a + 1$, ce qui est faux.

1.4 Types de Raisonnements

Un raisonnement mathématiques est une suite d'opérations ou un enchaînement logique d'un nombre fini d'étapes permettant la confirmation d'un résultat.
Dans cette section, on présente les différents types et structures de la démonstration mathématique.

1.4.1 Raisonnement Direct

Soient P et Q deux assertions.
Méthode : Pour montrer que $P \Rightarrow Q$, on considère que P est vraie et on montre que Q l'est aussi.

Exemple 1.4.1 *Soient a et b deux réels. Montrer que si $|a| < 1$ et $|b| < 1$, alors $ab + 1 \neq 0$.*

Démonstration : *On a*

$$\begin{array}{rcl} \left\{ \begin{array}{l} |a|<1 \\ |b|<1 \end{array} \right. & \Rightarrow & \left\{ \begin{array}{l} -1<a<1 \\ -1<b<1 \end{array} \right. \\ & \Rightarrow & -1<ab<1 \\ & \Rightarrow & 0<ab+1<2 \\ & \Rightarrow & ab+1\neq 0 \end{array}$$

Donc, $|a|<1$ et $|b|<1$, alors $ab+1\neq 0$ est vraie.

1.4.2 Raisonnement par disjonction des Cas

Méthode : Pour montrer qu'un prédicat $P(x)$ est vrai pour tout $x\in\Omega$, on peut montrer que : $\left\{ \begin{array}{l} 1^{er}\text{cas} : \forall x\in A\subset\Omega, P(x) \text{ est vrai} \\ \qquad\qquad et \\ 2^{eme}\text{cas} : \forall x\notin A, P(x) \text{ est vrai.} \end{array} \right.$.

Exemple 1.4.2 *Soit $n\in\mathbb{N}^*$. Montrer que $n(n+1)(n+2)$ est un multiple de 3.*

Démonstration :

1^{er} ***cas*** *: pour n multiple de $3, ie$ $(n=3k \ \ /k\in\mathbb{N}^*)$, on a :*

$$\begin{array}{rcl} n(n+1)(n+2) & = & 3k(3k+1)(3k+2) \\ & = & 3\left[k(3k+1)(3k+2)\right] \\ & = & 3k'. \end{array}$$

Ainsi, $n(n+1)(n+2)$ est un multiple de 3.

2^{eme} ***cas*** *: si n n'est pas un multiple de $3, ie$. $(n=3k+1 \ \ /k\in\mathbb{N}^*)$ ou $(n=3k+2 \ /k\in\mathbb{N}^*)$.*

Alors, si $n=3k+1 \ \ /k\in\mathbb{N}^*$, on a :

$$\begin{array}{rcl} n(n+1)(n+2) & = & (3k+1)(3k+2)\,(3k+3) \\ & = & 3\left[(3k+1)(3k+2)\,(k+1)\right] \\ & = & 3k''. \end{array}$$

Et si $n=3k+2 \ /k\in\mathbb{N}^*$, on a :

$$\begin{array}{rcl} n(n+1)(n+2) & = & (3k+2)(3k+3)\,(3k+4) \\ & = & 3\left[(3k+2)(k+1)\,(3k+4)\right] \\ & = & 3k'''. \end{array}$$

Donc, $(n$ *n'est pas un multiple de* $3) \Rightarrow (n(n+1)(n+2)$ *est un multiple de* $3)$.

Par conséquent, $\forall n \in \mathbb{N}^* : n(n+1)(n+2)$ *est un multiple de* 3.

1.4.3 Raisonnement par Contraposée

Soient P et Q deux assertions.

Méthode : pour montrer que $P \Rightarrow Q$, il suffit de montrer que $\overline{Q} \Rightarrow \overline{P}$.

Exemple 1.4.3 *Soit* $n \in \mathbb{N}^*$, *montrer que si* n *est le carré d'un entier, alors* $2n$ *n'est pas le carré d'un entier.*

Démonstration :

Supposons que $2n$ *est le carré d'un entier, alors* $\exists k \in \mathbb{N}$ *tel que :*

$$\begin{aligned} 2n &= k^2 \Rightarrow n = \frac{k^2}{2} \\ &\Rightarrow n = \left(\frac{k}{\sqrt{2}}\right)^2. \end{aligned}$$

On sait que $\frac{k}{\sqrt{2}} \notin \mathbb{N}$. *Ainsi,* n *n'est pas le carré d'un entier.*

Donc , par contraposée : si n *est le carré d'un entier, alors* $2n$ *n'est pas le carré d'un entier.*

1.4.4 Raisonnement par l'Absurde

Soient P et Q deux assertions.

Méthode : pour montrer que P est vraie , on suppose que $\overline{P}$ est vraie et on montre que ça entraine une contradiction.

Exemple 1.4.4 *Soit* $n, m \in \mathbb{N}^*$, *monter que* $nm = 1 \Rightarrow n = 1 \wedge m = 1$.

Démonstration :

Rappelons que $\overline{P \Rightarrow Q} \Leftrightarrow P \wedge \overline{Q}$. *C'est à dire qu'on suppose que* P *est vraie et* Q *est fausse.*

Suppospons que $nm = 1$ *et* $(n \neq 1$ *ou* $m \neq 1)$. *Ainsi, on distingue 2 situations :*

si $n \neq 1$, *alors :* $nm = 1 \Rightarrow m = \dfrac{1}{n}$ *ce qui est absurde car* $m \in \mathbb{N}^*$ *mais* $\dfrac{1}{n} \notin \mathbb{N}^*$.

et si $m \neq 1$, *alors :* $nm = 1 \Rightarrow n = \dfrac{1}{m}$ *(contradiction car* $n \in \mathbb{N}^*$ *mais* $\dfrac{1}{m} \notin \mathbb{N}^*$*).*

D'où, l'implication est vraie.

1.4.5 Raisonnement par un Contre-exemple

Soit le prédicat $P(x)$ défini sur un ensemble Ω.

Méthode : Pour montrer que $P(x)$ est faux, il suffit de trouver un élément x de Ω vérifiant $\overline{P(x)}$.

Exemple 1.4.5

1. *Montrer que* $\forall x \in \mathbb{R}, x < 4 \Rightarrow x^2 < 16$ *est fausse.*

   Le contre exemple est $x = -5$. *En effet,* $-5 < 4$ *mais* $(-5)^2 > 16$.

2. *Montrer que la proposition suivante est fausse :*

   $\forall n \in \mathbb{N}$, "*Si* (n *est pair et multiple de* 4), *alors* (n *un est multiple de* 8)".

   Prenons $n = 12 : 12$ *est pair et un multiple de 4, mais ce n'est pas un multiple de* 8.

1.4.6 Raisonnement par Récurrence

Soit P un prédicat, n_0 un entier naturel, tel que $n \geq n_0$.

Récurrence simple

Méthode :

Pour montrer que $P(n)$ est vraie pour tout $n \geq n_0$, Il suffit de :

- Vérifier que $P(n_0)$ est vraie.
- Supposer que $P(n)$ est vraie pour l'entier naturel $n \geq n_0$.
- Montrer que $P(n+1)$ est vraie.

Exemple 1.4.6 *Montrer que* $\forall n \in \mathbb{N} : 2^n > n$.

Notons $P(n) : 2^n > n$. *On a* $n_0 = 0$.

-$P(0)$ *est vraie, car :* $2^0 > 0$.

-Supposons que $(P(n) : 2^n > n)$ *est vraie.*

-Montrons que $\forall n \in \mathbb{N} : P(n+1) : 2^{n+1} > n + 1$.

On sait que $\forall n \in \mathbb{N} : 2^n \geq 1$. *Alors,*

$$\begin{cases} 2^n \geq 1 \\ 2^n > n \end{cases} \Rightarrow 2^n + 2^n > n + 1 \Rightarrow 2^{n+1} > n + 1.$$

D'où, $P(n)$ *est vraie pour tout* $n \in \mathbb{N}$.

Exemple 1.4.7 *Soit $a > 0$. Montrer que pour tout entier $n > 1, (1+a)^n > 1 + na$.*

Notons $P(n) : (1+a)^n > 1 + na$. On a $n_0 = 2$.

- $P(2)$ est vraie, car : $(1+a)^2 = 1 + 2a + a^2 > 1 + 2a$.

-Supposons que $(P(n) : (1+a)^n > 1 + na)$ est vraie.

-Montrons que $\forall n \in \mathbb{N} : P(n+1) : (1+a)^{n+1} > 1 + (n+1)\,a$. On a

$$\begin{aligned}(1+a)^{n+1} &= (1+a)(1+a)^n \\ &= (1+a)^n + a(1+a)^n \\ &> 1 + na + a\,(1+na) \\ &> 1 + a + na + na^2 \\ &> 1 + a + na.\end{aligned}$$

Par conséquent, $\forall n \in \mathbb{N} : (1+a)^{n+1} > 1 + (n+1)\,a$. D'où, $P(n)$ est vraie.

Récurrence forte (cumulative)

Méthode : Cette méthode repose sur les mêmes piliers :

1) **Initialisation :** montrer que $P(n_0)$ est vraie.

2) **Héridité :** montrer que $(\forall k \in \{n_0, \cdots, n\} : P(k)) \implies P\,(n+1)\,.$

Exemple 1.4.8 *Soit la suite (u_n) des réels positifs telle que : $u_1 = 1$ et $\forall n \geq 2 : u_n^2 = u_1 + u_2 + \cdots + u_{n-1}$.*

On veut démontrer par récurrence forte que $\forall n \geq 1 : u_n \geq \frac{n}{4}$.

***Initialisation : pour** $n = 1$, on a $u_1 = 1 \geq \frac{1}{4}$.*

***Héridité :** on suppose que $\forall k \in \{1, \cdots, n\} : u_k \geq \frac{k}{4}$. Ainsi, on a*

$$\left\{\begin{array}{l} u_1 \geq \frac{1}{4} \\ u_2 \geq \frac{2}{4} \\ \quad\vdots \\ u_n \geq \frac{n}{4} \end{array}\right. \underset{somme}{\Longrightarrow} u_1 + u_2 + \cdots + u_n \geq \frac{1}{4}\,(1 + 2 + \cdots + n)$$

$$\implies u_{n+1}^2 \geq \frac{1}{4}\left(\frac{n\,(n+1)}{2}\right)$$

$$\implies u_{n+1} \geq \sqrt{n\frac{(n+1)}{8}} \qquad .$$

Pour montre que $u_{n+1} \geq \frac{n+1}{4}$, *il suffit de remarquer que* $\frac{n+1}{4} = \sqrt{\frac{(n+1)^2}{16}} = \sqrt{\frac{(n+1)}{2} \times \frac{(n+1)}{8}}$. *De plus, on a* $\forall n \geq 1 : n + n \geq n + 1$ *. D'où,* $n \geq \frac{n+1}{2}$. *Donc,*

$$u_{n+1} \geq \sqrt{n\frac{(n+1)}{8}} \implies u_{n+1} \geq \sqrt{\frac{(n+1)}{2} \times \frac{(n+1)}{8}} \implies u_{n+1} \geq \frac{n+1}{4}.$$

Par conséquent, $\forall n \geq 1 : u_n \geq \frac{n}{4}$.

1.5 Exercices corrigés

Exercice 1.5.1 *Dire si les propositions suivantes sont vraies ou fausses en justifiant la réponse, puis donner leurs négations.*

1. $\exists x \in \mathbb{N} : 7x - 3 = 0$.
2. $\forall x \in \mathbb{R}, 5x^2 - 26 > 0$.
3. $\exists x \in \mathbb{R}, \exists y \in \mathbb{R} : x^2 + y^2 = 2$.
4. $\forall x \in \mathbb{R}, \exists y \in \mathbb{R} : x = \dfrac{y+1}{y-1}$.

Solution : Valeurs logiques :

1. " $\exists x \in \mathbb{R} : 7x - 3 = 0$ " est vraie car $x = \frac{3}{7}$ vérifie l'équation.
2. " $\forall x \in \mathbb{R}, 5x^2 - 26 > 0$ " est fausse car il existe au moins un élement $x \in \mathbb{R}$ pour lequel $5x^2 - 26 \leq 0$, par exemple $x = 0$.
3. " $\exists x \in \mathbb{R}, \exists y \in \mathbb{R} : x^2 + y^2 = 4$ " est vraie en prenant $x = y = \sqrt{2}$ ou bien $x = 0, y = -2$.
4. " $\forall x \in \mathbb{R}, \exists y \in \mathbb{R} : x = \dfrac{y+1}{y-1}$ " est fausse car pour $x = 1$, on a : $y + 1 = y - 1$ ce qui n'est pas possible.

Négations :

1 $\forall x \in \mathbb{N} : 7x - 3 \neq 0$.

2 $\exists x \in \mathbb{R}, 5x^2 - 26 \leq 0$.

3 $\forall x \in \mathbb{R}, \forall y \in \mathbb{R} : x^2 + y^2 \neq 2$.

4 $\exists x \in \mathbb{R}, \forall y \in \mathbb{R} : x \neq \dfrac{y+1}{y-1}$.

Exercice 1.5.2 *Démontrer les équivalences suivantes :*

1. $[P \wedge (P \vee Q)] \Leftrightarrow P$.
2. $[P \Leftrightarrow Q] \Leftrightarrow [Q \Leftrightarrow P]$.
3. $\left[\overline{P} \Rightarrow Q\right] \wedge \left[\overline{P} \Rightarrow \overline{Q}\right] \Leftrightarrow P$.

Solution

1) $[P \wedge (P \vee Q)] \overset{??}{\iff} P$

P	Q	$P \vee Q$	$P \wedge (P \vee Q)$	$P \wedge (P \vee Q) \iff P$
V	V	V	V	V
V	F	V	V	V
F	V	V	F	V
F	F	F	F	V

2) $(P \iff Q) \overset{??}{\iff} (Q \iff P)$

P	Q	$P \iff Q$	$Q \iff P$	$(P \iff Q) \iff (Q \iff P)$
V	V	V	V	V
V	F	F	F	V
F	V	F	F	V
F	F	V	V	V

3) Montrons que $\left(\overline{P} \Rightarrow Q \wedge \overline{Q} \Rightarrow P\right) \iff P$

P	Q	$\overline{P} \Rightarrow Q$	$\overline{Q} \Rightarrow P$	$\overline{P} \Rightarrow Q \wedge \overline{Q} \Rightarrow P$	$\left(\overline{P} \Rightarrow Q \wedge \overline{Q} \Rightarrow P\right) \iff P$
V	V	V	V	V	V
V	F	V	V	V	V
F	V	V	F	F	V
F	F	F	V	F	V

Exercice 1.5.3 *Soit $x \in \mathbb{R}$. Montrer que si $x^3 + x^2 - x - 1 > 0$, alors $x > 1$.*

Solution (raisonnement direct)

On remarque que $A(x)$=$x^3 + x^2 - x - 1$ s'annule si $x = 1$. Alors, $A(x) = (x-1)\,B(x)$ tel que $B(x) = ax^2 + bx + c$. Ainsi,

$$\begin{aligned} A(x) &= (x-1)\left(ax^2 + bx + c\right) \\ &= ax^3 + (b-a)\,x^2 + (c-b)\,x - c. \end{aligned}$$

Par identification, on trouve $a = 1, b = 2, c = 1$ ie

$$\begin{aligned} A(x) &= (x-1)\left(x^2 + 2x + 1\right) \\ &= (x-1)\,(x+1)^{\,2}. \end{aligned}$$

D'autre part,

$$\begin{aligned} A(x) \quad &> \quad 0 \implies (x-1)(x+1)^2 > 0 \\ &\implies \quad (x-1) > 0 \text{ et } x \neq -1 \\ &\implies \quad x > 1 \ . \end{aligned}$$

D'où, le résultat.

Exercice 1.5.4 *Démontrer par contraposée la proposition suivante : Si n^2 est impair, alors n est impair.*

Solution

Montrons que : si n est pair, alors n^2 est pair

Si n est pair, alors $n = 2k \ / \ k \in \mathbb{N}$. Ainsi, $n^2 = (2k)^2 = 2(2k^2)$.

Donc, n^2 est pair. Par contraposée : n^2 impair $\implies$ n impair.

Exercice 1.5.5 (intervertion des quantificateurs) *Soient Ω, Ω' deux ensembles et P une proposition. Montrer que*

$$\exists a \in \Omega, \forall b \in \Omega'; P(a,b) \implies \forall b \in \Omega', \exists a \in \Omega; P(a,b)$$

Solution *(raisonnement par l'absurde)*

Supposons que $\exists a \in \Omega, \forall b \in \Omega'; P(a,b)$ est vraie et $\forall b \in \Omega', \exists a \in \Omega; P(a,b)$ est fausse. i.e $\left((\exists a \in \Omega, \forall b \in \Omega'; P(a,b)) \wedge \left(\exists b \in \Omega', \forall a \in \Omega; \overline{P(a,b)}\right)\right)$.

C'est à dire qu'il existse un élément a de Ω qui est compatible avec tout élément b de Ω'. D'autre part, il existe au moins un élément b de Ω' qui n'est compatible avec aucun élément de Ω. Ce qui est absurde. D'où, le résultat.

Exercice 1.5.6 *Démontrer que pour tout entier naturel $n > 0$, $7^n - 1$ est divisible par 6.*

Solution

i) Pour $n = 1$, on a $(7^1 - 1)$ est un multiple de 6.

ii) Supposons que $7^n - 1$ est divisible par 6. i.e $7^n - 1 = 6k \ / \ k \in \mathbb{N}$.

iii) Montrons que $7^{n+1}-1$ est divisible par 6 :

$$\begin{aligned} 7^{n+1}-1 &= (7\times 7^n)-1 \\ &= (7\times 7^n)-7+6 \\ &= 7\,(7^n-1)+6 \\ &= (7^n-1)+6\,(7^n-1)+6 \\ &= 6k+6\,(6k)+6 \\ &= 6\,(7k+1)\,; \end{aligned}$$

ce qui achève la démonstration.

1.6 Exercices supplémentaires

Exercice 1.6.1 *Écrire la négation simplifiée des propositions suivantes :*

a. $(\neg P \wedge Q) \Rightarrow R$.

b. $\neg(P \vee \neg Q) \wedge (S \Rightarrow P)$.

c. $\neg(P \wedge Q) \wedge (P \vee Q)$.

d. $P \Rightarrow (\neg Q \vee R)$.

e. $\forall x \in \mathbb{R},\ f(x) > 0 \Rightarrow x \leq 0$.

f. $\forall \varepsilon > 0,\ \exists \eta > 0,\ \forall (x,y) \in \mathbb{R},\ (|x-y| \leq \eta \Rightarrow |f(x)-f(y)| \leq \varepsilon)$.

i. $\forall M > 0,\ \exists A > 0,\ \forall x \geq A,\ f(x) > M$.

j. $\exists\ n \in \mathbb{N}; (n < 7) \Rightarrow (n^2 < 49)$.

Exercice 1.6.2 *Montrer que les assertions suivantes sont des tautologies :*

A : $[(P \Rightarrow R) \wedge (P \Rightarrow Q)] \Rightarrow [P \Rightarrow (R \wedge Q)]$

B : $[P \Rightarrow (Q \Rightarrow R)] \Leftrightarrow [(P \wedge Q) \Rightarrow R]$

Exercice 1.6.3 *Soient les assertions suivantes :*

P : *" Si je suis un étudiant universitaire, alors j'ai un Baccalauréat".*

Q : " Si $AB^2 + AC^2 = BC^2$, alors ABC est un triangle rectangle en B ".

-Donner les valeurs logique de :

a) *P et $(nonQ)$;*

b) *Q ou $(P \Rightarrow Q)$;*

c) *P si et seulement si Q.*

Exercice 1.6.4 *Écrire la négation mathématique de chacune des phrases suivantes :*

1. *Ni Marie ni Martin ne sont malades.*
2. *Certains membres de la chorale n'assisteront pas au spectacle.*
3. *Il existe des rectangles qui ne sont pas des parallélogrammes.*
4. *Si $ABCD$ est un rectangle, alors il pleut.*
5. *Un pommier est un animal, si et seulement si, le ciel est rouge.*
6. *Tout réel positif est un entier.*
7. *Soit je passe mes vacances à Londres, soit en Tunisie.*
8. *Sur $\mathbb{R}$, l'équation $x^3 - 1 = 0$ admet un nombre de solutions strictement inferieur à 3.*

Exercice 1.6.5 *Donner les contraposées des phrases suivantes :*

1. *S'il pleut, alors je joue aux dominos ou je vais au cinéma.*
2. *Si AB=AC, alors ABC est un triangle isocèle.*

Exercice 1.6.6 *Écrire en utilisant les quantificateurs :*

1. *Il existe des réels x dont le carré est strictement supérieur à 100.*
2. *Pour tout rationnel q, il existe un entier n strictement supérieur à q.*
3. *Certains entiers naturels n vérifient que $n^2 + 3n$ soit pair.*

   Soit la fonction f définie sur $\mathbb{R}$.

4. *f s'annule deux fois sur $\mathbb{R}$:*
5. *f est constante sur l'intervalle $I \subset \mathbb{R}$.*

Exercice 1.6.7 *Montrer que : Pour tout entier naturel n, $n^2 + 3n$ est pair.*

Exercice 1.6.8 *Soient $(x, y) \in \mathbb{R}$. Démontrer que $xy \leq \frac{x^2+y^2}{2}$.*

Exercice 1.6.9 *Montrer que : si x et y sont des réels distincts et différents de 1, alors $\dfrac{1}{x-1} \neq \dfrac{1}{y-1}$.*

Exercice 1.6.10 *En utilisant le raisonnement par l'absurde, montrer que : $\sqrt{2} \notin \mathbb{Q}$.*

Exercice 1.6.11 *En utilisant le raisonnement par contraposée montrer que : Si l'entier $(n^2 - 1)$ n'est pas divisible par 8, alors l'entier n est pair.*

Exercice 1.6.12 *Démontrer que pour tout entier $n \geq 1$, on a :*

$$1^2 + 2^2 + 3^2 + ... + n^2 = \frac{n\,(n+1)\,(2n+1)}{6}.$$

Chapitre 2

Ensembles et Applications

L'objectif de ce chapitre est de :

1) Donner un sens mathématique bien précis aux pré-requis (de l'étudiant) liés aux ensembles, l'intersection et l'union...

2) Maîtriser de nouvelles notions telles que la différence de deux ensembles et le complémentaire d'une collection d'objets.

3) Établir la différence entre une relation mathématique, une fonction et une application.

4) Définir une application injective / surjective / bijective.

2.1 Ensembles

2.1.1 Notion d'Ensemble

Définition 2.1.1 ***Un ensemble*** *est une collection (ou multitude) d'objets appelés* ***éléments.***

Notations

- On note les ensembles par des lettres majuscules : $\Omega, F, \Gamma, A, B, E, F, ...$
- les éléments d'un ensemble sont notés par des lettres minuscules : $\alpha, \beta, a, b, x, y, z, ...$
- Si x est un élément de Ω, on écrit $x \in \Omega$ et on lit : x appartient à Ω.
- Si x n'est pas dans Ω, on écrit $x \notin \Omega$ et on lit : x n'appartient pas à Ω.

Exemple 2.1.1 *1.* $\Omega = \{0, a, \blacksquare, 5, d, \clubsuit\}$ *est un ensemble et* $\clubsuit \in \Omega, 3 \notin \Omega$.

2. Lyon $\in \{$*villes de France*$\}$.

3. $11 \notin \{$ *les entiers pairs*$\}$

4. $\mathbb{N}$ *est l'ensemble des entiers naturels.*

5. $\mathbb{Z}$ *est l'ensemble des entiers relatifs.*

6. $\mathbb{Q}$ *est l'ensemble des nombres rationels.*

7. $\mathbb{R}$ *est l'ensemble des nombres réels.*

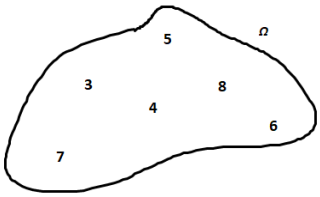
8. $\mathbb{C}$ *est l'ensemble des nombres complexes.*

Remarque 2.1.1 *On peut définir un ensemble de trois façons :*

1 – *Extension énumerer tous les éléments (l'ordre et la répitition sont sans influence),par exemple* $\Omega = \{0, a, \blacksquare, 5, d, \clubsuit\} = \{\clubsuit, a, d, \blacksquare, 5, 0\} = \{0, a, a, \blacksquare, \blacksquare, \blacksquare, 5, 5, d, \clubsuit, \clubsuit, \clubsuit, \clubsuit\}$.

2 – *Compréhension énoncer une propriété caractérisant les éléments de l'ensemble, par exemple :* $A = \{n \in \mathbb{N} : \ 3 \leq n \leq 8\}$, *l'ensemble des entiers pairs* $B = \{2n, \ n \in \mathbb{Z}\}$.

3 – *Diagramme de Venn par une représentation graphique d'un ensemble i.e le diagramme de Venn*



Définition 2.1.2 -***Un ensemble fini*** *est un ensemble dont le nombre d'éléments est fini. Le nombre d'éléments d'un ensemble* Ω *est appelé cardinal de* Ω.

-*Un ensemble qui n'est pas fini est dit* ***infini.***

-*Un ensemble qui ne contient aucun élément est* ***un ensemble vide.***

-*Un ensemble contenant un seul élément est appelé* ***Singleton.***

Notation : On note le cardinal de Ω par $Card\,(\Omega)$ et l'ensemble vide par $\emptyset$.

Exemple 2.1.2 *1.* $\Omega = \{0, a, \blacksquare, 5, d, \clubsuit\}$, $Card(\Omega) = 6$.

2. $A = \{n \in \mathbb{N} :\ 3 \leq n \leq 15\}$, $Card(A) = 13$.
3. $B = \{n \in \mathbb{N} : n \leq -1\}$, $Card(B) = 0$, *car* $B = \emptyset$.
4. $C = \left\{\frac{1}{2}\right\}$, $Card(C) = 1$.

2.1.2 Inclusion d'ensembles

Définition 2.1.3 *Soient les ensembles A et B. On dit que A est inclus dans B si et seulement si tout élément de A appartient à B.*

Notation : L'inclusion de A dans B est notée : $A \subset B$.

Remarque 2.1.2

1. *Si A est inclus dans B, on peut dire que A est une partie de B (ou A est un sous ensemble de B ou A est contenu dans B ou bien B contient A) et on écrit :*
$$(A \subset B) \Leftrightarrow (\forall a \in \Omega;\ a \in A \Rightarrow a \in B).$$
2. *On dit que A n'est pas inclus dans B s'il existe au moins un élément de A qui n'appartient pas à B et on écrit :*
$$(A \not\subseteq B) \Leftrightarrow (\exists a \in \Omega;\ a \in A \wedge a \notin B).$$
3. *Tout ensemble est inclu dans ui même* $(\Omega \subset \Omega)$.
4. *Si $A \subset B$ (finis), alors $Card(A) \leq Card(B)$.*
5. *Si $\Omega, \digamma$ et $\beth$ sont trois ensembles , alors on a :* $\begin{cases} \Omega \subset \digamma \\ \digamma \subset \beth \end{cases} \Rightarrow \Omega \subset \beth$.
6. *L'ensemble vide est inclus dans tout ensemble.*

Exemple 2.1.3 **a)** $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

b) *Dans tout les cas suivant on a $A \subset B$:*

1. $A = \{-2, 0, 3, 5\}$ *et* $B = \{-5, -2, -1, 0, 1, 3, 4, 5, 7, 10\}$.
2. $A =]2, 5[$ *et* $B = [2, 5]$.
3. $A =]-3, 1]$ *et* $B =]-4, 2[$.
4. $A = \{2n + 1, n \in \mathbb{N}\}$ *et* $B = \mathbb{Z}$.

Définition 2.1.4 *Soit Ω un ensemble. Les parties de Ω forment un ensemble dit l'**Ensemble des parties de** Ω, noté : $P(\Omega)$.*

Exemple 2.1.4 *L'ensemble des parties de $\Omega = \{1, 2, 3\}$ est*

$$P(\Omega) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

Remarque 2.1.3 *1. Si $Card(\Omega) = n$, alors $Card(P(\Omega)) = 2^n$.*

2. $A \in P(B) \Leftrightarrow A \subset B$.

2.1.3 Égalité d'ensembles

Définition 2.1.5 *Soient A et B deux ensembles. On dit que A et B sont égaux et on écrit $A = B$, s'ils contiennent les mêmes éléments. i.e*

$$(A = B) \Leftrightarrow ((A \subset B) \wedge (B \subset A)).$$

Exemple 2.1.5 *Dans les cas suivants, $A = B$:*

1. $A = \left\{x \in \mathbb{R}; \dfrac{x-1}{x+2} > 0\right\}$, $B = \{x \in \mathbb{R}; (x-1)(x+2) > 0\}$.

2. $A = \{x \in \mathbb{R}; x^2 + 4x + 3 = 0\}$, $B = \{-1, -3\}$.

Remarque 2.1.4 a) *L'´ecriture $A \subseteq B$ signifie que : $(A \subset B) \vee (A = B)$.*

b) *Si $A \neq B$, on dit que A et B sont distincts (ou différents) .*

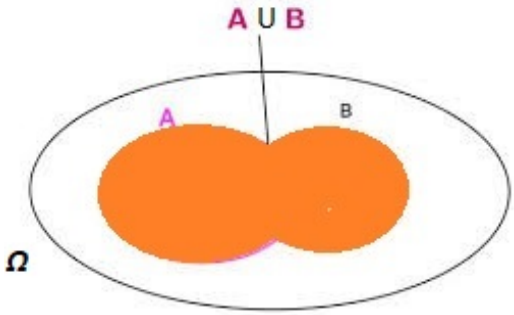
c) *Si $A \subset B$ et $A \neq B$, on dit que A est strictement inclus dans B et on note $A \subsetneq B$.*

2.1.4 Opérations sur les ensembles

Union d'ensembles

Définition 2.1.6 *Soient A et B deux parties de Ω. L'ensemble contenant les éléments appartenants à A ou à B est appelé l'**union** de A et B notée $A \cup B$.*

$$A \cup B = \{x \in \Omega;\ (x \in A) \vee (x \in B)\}.$$



Exemple 2.1.6 *1. Soit* $A = \{0, 2, 5, 8\}$, $B = \{1, 3, 6\}$, *alors* $A \cup B = \{0, 1, 2, 3, 5, 6, 8\}$.

2. Soit $A =]-3, 1]$, $B = [0, 4[$, *alors* $A \cup B =]-3, 4[$.

Proposition 2.1.1 *Soient* A, B *et* C *trois parties de* Ω. *On a :*

* $A \cup A = A$.

* $A \cup \varnothing = A$.

* $A \cup B = B \cup A$.

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

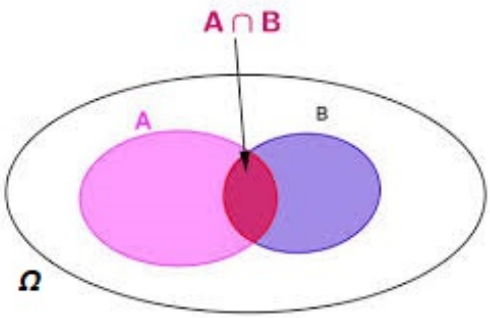
* $A \subset (A \cup B)$ *et* $B \subset (A \cup B)$.

* $(A \cup B = B) \Leftrightarrow (A \subset B)$.

Intersection d'ensembles

Définition 2.1.7 *Soient* A *et* B *deux parties de* Ω. *L'intersection de* A *et* B *notée* $(A \cap B)$ *est l'ensemble qui contient les éléments appartenant à* A *et à* B. *i.e*

$$A \cap B = \{x \in \Omega;\ \ (x \in A) \wedge (x \in B)\}.$$



Exemple 2.1.7 *1. Soit* $A = \{0, 2, 5\}$, $B = \{0, 1, 5, 6\}$, *alors* $A \cap B = \{0, 5\}$.

2. Soit $A =]-3, 1]$, $B = [0, 4[$, *alors* $A \cap B = [0, 1]$.

3. Soit $A = \{x \in \mathbb{R}, x^2 - 1 \geq 0\}$ *et* $B = \{x \in \mathbb{R}, x + 2 \geq 0\}$. *Alors* $A \cap B = [-2, -1] \cup [1, +\infty[$.

Proposition 2.1.2 *Soient* A, B *et* C *trois parties de* Ω. *On a :*

a) $A \cap A = A$.

b) $A \cap \varnothing = \varnothing$.

c) $A \cap B = B \cap A$.

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

e) $(A \cap B) \subset A$ *et* $(A \cap B) \subset B$.

f) $(A \subset B) \Leftrightarrow ((A \cap B) = A)$

Ensembles disjoints

Définition 2.1.8 *Deux ensembles* A *et* B *sont disjoints si leurs intersection est vide. i.e* $A \cap B = \emptyset$.

Exemple 2.1.8 *1.*

2. $\mathbb{Z}_+$ *et* $\mathbb{Z}_-^*$ *sont disjoints.*

3. $A = \{a, 1, d, 5\}$ *et* $B = \{0, p, 3\}$ *sont disjoints.*

4. $A =]-5, 3]$ *et* $B =]3, \frac{9}{2}[$ *sont disjoints.*

Proposition 2.1.3 *Soient* A, B *et* C *trois parties de* Ω. *On a :*

1. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
2. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
3. $Card(A \cup B) = Card(A) + Card(B) - Card(A \cap B)$.

Preuve.

□

Montrons que $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

a) $A \cup (B \cap C) \overset{??}{\subset} (A \cup B) \cap (A \cup C)$:

Pour tout élément x *de l'ensemble* $A \cup (B \cap C)$, *on a*:

1) Si $x \in A$, *alors* $x \in (A \cup B) \cap (A \cup C)$.

2) Si $x \notin A$, *alors* $x \in (B \cap C)$.*Donc,* $x \in (A \cup B) \cap (A \cup C)$.

b) $(A \cup B) \cap (A \cup C) \overset{??}{\subset} A \cup (B \cap C)$:

Soit $x \in (A \cup B) \cap (A \cup C)$. *On a :*

1) Si $x \in A$, *alors* $x \in A \cup (B \cap C)$.

2) Si $x \notin A$, *alors* $x \in B$ *et* $x \in C$. *Donc,* $x \in A \cup (B \cap C)$.

Produit cartésien

Définition 2.1.9 *Soient* A, B *deux ensembles. L'ensemble des couples* (x, y) *pris dans cet ordre avec* $x \in A$ *et* $y \in B$ *est appelé ensemble produit cartésien de* A *et* B*; et on note*

$$A \times B = \{(x, y) \setminus x \in A,\ y \in B\}.$$

Le nombre d'éléments de $A \times B$ *est* $Card(A \times B) = Card(A) \times Card(B)$.

Exemple 2.1.9 *Soit* $A = \{a, b, c\}$ *et* $B = \{1, 2\}$; $card(A \times B) = 6$;

$$A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}.$$

Remarque 2.1.5 *Le produit cartésien n'est pas commutatif, i.e* $A \times B \neq B \times A$. *En effet, dans l'exemple précédent*

$$B \times A = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\} \neq A \times B.$$

Définition 2.1.10 *Soit* $n \in \mathbb{N}^*, (A_1, A_2, ..., A_n)$ *des ensembles non vides. On appelle produit cartésien des ensembles* $A_1, A_2, ..., A_n$ *les* $n-$*uplets* $(a_1, a_2, ..., a_n)$ *avec* $\left(a_i \in A_i \backslash i = \overline{1, n}\right)$ *et on note :*

$$A_1 \times A_2 \times ... \times A_n = \left\{(a_1, a_2, ..., a_n) \setminus a_i \in A_i \backslash i = \overline{1, n}\right\}.$$

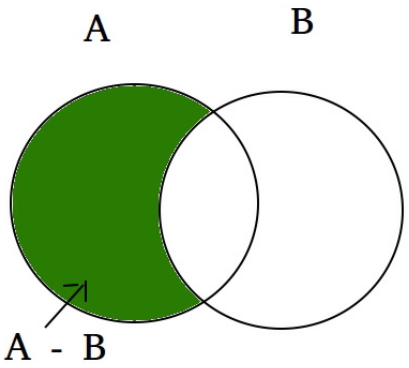
Exemple 2.1.10 *Le triplet* $\left(1, \sqrt{5}, -3\right) \in \mathbb{N} \times \mathbb{R} \times \mathbb{Z}$.

Remarque 2.1.6 *Pour tout ensemble* A, $A \times \emptyset = \emptyset \times A = \emptyset$.

Différence d'ensembles

Définition 2.1.11 *Soient* A *et* B *deux sous ensembles de* Ω *. On appelle différence de* A *et* B *l'ensemble, noté* $A \backslash B$ *(A moins B), constitué des élément de* A *qui n'appartiennent pas à* B.

$$A \backslash B = \{x \in \Omega;\ \ (x \in A) \wedge \ \ (x \notin B)\}.$$



1. Soit $A = \{x \in \mathbb{R}, x - 2 \geq 0\}$ et $B = \{x \in \mathbb{R}, x < 5\}$. Alors, $A \backslash B = [5, +\infty[$.
2. Soit $A = \{a, b, c, d, e\}$ et $B = \{b, e, o, g\}$. Alors, $A \backslash B = \{a, c, d\}$

Proposition 2.1.4 *Soient* A, B *et* C *trois parties de* Ω. *On a les proriétés suivantes :*

a) $A \backslash \emptyset = A$.

b) $(A \backslash B = \emptyset) \Leftrightarrow (A \subset B)$.

c) $A \backslash (B \cap C) = (A \backslash B) \cup (A \backslash C)$.

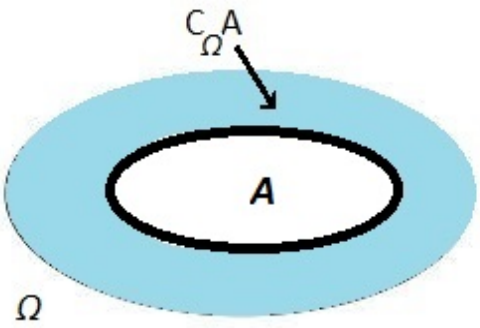
d) $A \backslash (B \cup C) = (A \backslash B) \cap (A \backslash C)$.

Preuve. En exercice. □

Complémentaire d'un ensemble

Définition 2.1.12 *Soit A un sous ensemble de Ω. Le complémentaire de A dans Ω est un sous ensemble de Ω, noté $C_\Omega A$, formé des éléments de Ω qui n'appartiennent pas à A et on écrit*

$$C_\Omega A = \{x \in \Omega, x \notin A\} = \Omega \backslash A.$$



Exemple 2.1.11

1. *Soit* $\Omega = \{a, b, c, d, e, f, g\}$ *et* $A = \{b, e, g\}$. *Alors,* $C_\Omega A = \{a, c, d, f\}$.
2. *Soit* $\Omega = \mathbb{R}$ *et* $A =]-3, 5]$. *Alors,* $C_\Omega A =]-\infty, -3] \cup [5, +\infty[$.
3. *Soit* $\Omega = \mathbb{N}$ *et* $A = \{2n, n \in \mathbb{N}\}$. *Alors,* $C_\Omega A = \{2n + 1, n \in \mathbb{N}\}$.

Proposition 2.1.5 *Soient A et B deux parties de Ω. On a :*

a) $C_\Omega \emptyset = \Omega$ *et* $C_\Omega \Omega = \emptyset$.

b) $C_\Omega (C_\Omega A) = A$.

c) $A \cap C_\Omega A = \emptyset$ *et* $A \cup C_\Omega A = \Omega$.

d) *Si* $A \subset B$, *alors* $C_\Omega B \subset C_\Omega A$.

e) $A \backslash B = A \cap C_\Omega B$.

f) $C_\Omega (A \cap B) = (C_\Omega A) \cup (C_\Omega B)$ *.(Loi de Morgan)*

g) $C_\Omega (A \cup B) = (C_\Omega A) \cap (C_\Omega B)$. *(Loi de Morgan)*

Preuve. ***g)*** $C_E (A \cup B) = (C_E A) \cap (C_E B)$.

1) Montrons : $C_E(A \cup B) \subset (C_E A) \cap (C_E B)$ *: soit* $x \in C_E(A \cup B)$,

$$\begin{aligned} x \in C_E(A \cup B) &\Longrightarrow x \notin (A \cup B) \\ &\Longrightarrow x \notin A \wedge x \notin B \\ &\Longrightarrow x \in (C_E A) \wedge x \in (C_E B) \\ &\Longrightarrow x \in (C_E A) \cap (C_E B) . \end{aligned}$$

2)Montrons : $(C_E A) \cap (C_E B) \subset C_E(A \cup B)$ *: soit* $x \in (C_E A) \cap (C_E B)$ *, on a*

$$\begin{aligned} x \quad \in \quad & (C_E A) \cap (C_E B) \Rightarrow x \in (C_E A) \wedge x \in (C_E B) \\ \Rightarrow \quad & x \notin A \wedge x \notin B \\ \Rightarrow \quad & x \notin (A \cup B) \\ \Rightarrow \quad & x \in C_E(A \cup B) . \end{aligned}$$

De 1) et 2), on déduit que $C_E(A \cup B) = (C_E A) \cap (C_E B)$. □

2.2 Relations, Fonctions, Applications

2.2.1 Relations

Définition 2.2.1 *Soient* Ω *et* $\digamma$ *deux ensembles non vides, tout triplet* $(\Omega, \digamma, \Gamma)$ *est appelé* ***relation*** $\Re$ *de* Ω *vers* $\digamma$ *tel que :*

Ω *est l'ensemble de* ***départ*** *de* $\Re$.

$\digamma$ *est appelé ensemble d'****arrivée*** *de* $\Re$.

$\Gamma \subset \Omega \times \digamma$ *est le* ***graphe*** *de* $\Re$, *où* $\Gamma = \{(x, y) \in \Omega \times \digamma \setminus x \Re y\}$.

x *est appelé l'antécédent de* y *et* y *est l'image de* x *par* $\Re$.

Exemple 2.2.1 *Soient* $\Omega = \{1, 2, 3, 4, 5\}$, $\digamma = \{a, b, c, d\}$ *, on définit la relation* $\Re$ *de* Ω *vers* $\digamma$ *par le graphe*

$$\Gamma = \{(1, a), (1, c), (2, c), (3, a), (4, b)\} .$$

$\Re$ *peut être, aussi, représentée par un diagramme sagittal ou cartésien, comme suit :*

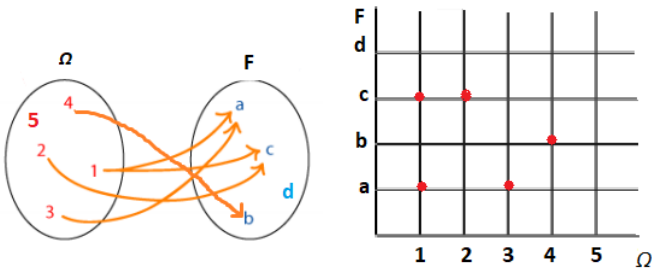


Diagramme sagittal *Diagramme Cartésien*

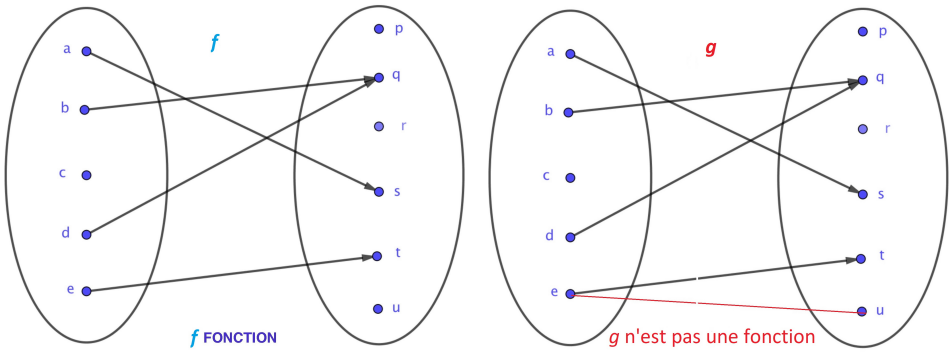
2.2.2 Fonctions

Définition 2.2.2 *Soient Ω et F deux ensembles non vides. On appelle* ***fonction*** *de Ω dans F toute relation de Ω vers F qui associe à chaque x de Ω au plus un élément y de F.*

Notation : Écriture mathématique : $\begin{array}{l} f : \Omega \to F \\ x \mapsto y \end{array}$ ou bien $\Omega \xrightarrow{f} F$.

Les fonctions sont notées généralement par : $f, g, h, \cdots$

Exemple 2.2.2 *1.* $\Omega = \{a, b, c, d, e\}, F = \{p, q, r, s, t, u\}$, *$f$ et g deux relations de Ω vers F.*



f est une fonction telle que : $f(a) = s$, $f(b) = f(d) = q$, $f(e) = t$.

g n'est pas une fonction car : e a deux images différentes ($g(e) = t$ et $g(e) = u$).

2. $\begin{array}{l} f : \mathbb{R} \longrightarrow \mathbb{R} \\ x \mapsto \frac{3}{x+1} \end{array}$, *$x = -1$ n'a pas d'image, $y = 0$ n'admet aucun antécédent par f.*

3. $\begin{array}{l} g : \mathbb{R}^* \longrightarrow \mathbb{R} \\ x \mapsto \sqrt{x} \end{array}$, *$x = -2$ n'a pas d'image, $y = 0$ n'admet aucun antécédent par g.*

Définition 2.2.3 *Soient Ω et $\digamma$ deux ensembles non vides. Le* ***domaine de définition*** *d'une fonction f noté D_f est l'ensemble des éléments de Ω admettant une image dans $\digamma$.*

$$D_f = \{x \in \Omega \ / \ \exists y \in \digamma : y = f(x)\} \subset \Omega.$$

Exercice 2.2.1 *Déterminer le domaine de définition des fonctions $f, g : \mathbb{R} \to \mathbb{R}$ avec $f(x) = \sqrt{x^2-1}$, $g(x) = \frac{-2}{x+3}$*

a) Pour $f(x) = \sqrt{x^2-1}$, on peut écrire :

$$D_f = \left\{x \in \mathbb{R} : x^2 - 1 \geq 0\right\}.$$

Ainsi,

$$\begin{aligned} x^2 - 1 \quad &\geq \quad 0 \iff (x-1)(x+1) \geq 0 \\ &\iff \quad x \in]-\infty, -1] \cup [1, +\infty[\end{aligned}$$

Donc,

$$D_f =]-\infty, -1] \cup [1, +\infty[.$$

b) Pour la fonction $g(x) = \frac{-2}{x+3}$, on a :

$$\begin{aligned} D_g &= \{x \in \mathbb{R} : x + 3 \neq 0\}. \\ &= \{x \in \mathbb{R} : x \neq -3\} \\ &= \mathbb{R} \setminus \{-3\}. \end{aligned}$$

Egalité de deux fonctions

Définition 2.2.4 *Soient f et g deux fonctions. On dit que f et g sont égales et on écrit $f = g$ si :*

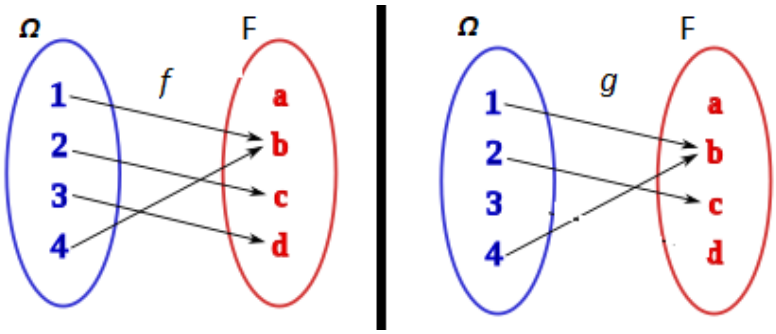
i. f et g ont le même ensemble de départ, d'arrivée et $D_f = D_g = D$.

ii. $\forall x \in D$, $f(x) = g(x)$.

2.2.3 Applications

Définition 2.2.5 *Soient Ω et F deux ensembles non vides. On appelle* ***application*** *de Ω vers F toute fonction f qui fait correspondre à chaque élément $x \in \Omega$ un élément unique $y \in F$. C'est à dire $D_f = \Omega$.*

Exemple 2.2.3 *f et g deux relations définies de Ω vers F, telles que :*



f est une application car $D_f = \Omega$, mais g n'est pas une application car $x = 3$ n'admet aucune image.

Application identique

Définition 2.2.6 *Soit Ω un ensemble non vide. On appelle application identique dans Ω, notée Id_Ω, l'application qui associe à tout $x \in \Omega$, x lui même. i.e*

$$\begin{aligned} Id_\Omega \quad : \quad & \Omega \to \Omega \\ & x \mapsto Id_\Omega(x) = x \ . \end{aligned}$$

Composition d'applications

Définition 2.2.7 *Soient $\Omega, F, \Im$ trois ensembles non vides, $f : \Omega \to F, g : F \to \Im$ applications. La composée de f et g est l'application notée $g \circ f$ définie par :*

$$\begin{aligned} g \circ f \quad : \quad & \Omega \to \Im \\ & x \mapsto g \circ f(x) = g(f(x)) \end{aligned}$$

Exemple 2.2.4 *On considère f et g deux applications définies sur $\mathbb{R}$, par : $f(x)=\sqrt{x-1}, g(x)=\frac{2x}{x^2+1}$. on a :*

$$\begin{aligned} g\circ f(x) &= g(f(x))=\frac{2f(x)}{[f(x)]^2+1}=\frac{2\sqrt{x-1}}{x}. \\ f\circ g(x) &= f(g(x))=\sqrt{g(x)-1}=\sqrt{\frac{2x}{x^2+1}-1}. \end{aligned}$$

Proposition 2.2.1 *Soient $f:\Omega\to F, g:F\to \eth, h:\eth\to H$ trois applications, on a*

1. $f\circ Id_\Omega = f$.
2. $Id_F\circ f = f$.
3. $h\circ(g\circ f)=(h\circ g)\circ f$.

Image dircete, Image réciproque

Définition 2.2.8 *Soient Ω, F deux ensembles non vides, $f:\Omega\to F$ une application et $A\subset\Omega$, $B\subset F$:*

1. *On appelle **image directe** de A par f l'ensemble noté $f(A)$ tel que*

$$f(A)=\{f(x)/x\in A\}\subset F.$$

2. *On appelle **image réciproque de** B par f l'ensemble*

$$f^{-1}(B)=\{x\in\Omega/f(x)\in B\}\subset\Omega.$$

Exemple 2.2.5 *On considère l'application $f(x)=x^3$, $A=[0,2]$, $B=[-1,1]$; on a*

1. *L'image directe de A par f est $f(A)=\{y=f(x)/0\le x\le 2\}$. Comme $0\le x\le 2$, alors $0\le x^3\le 8$. D'où, $f([0,2])=[0,8]$.*
2. *Aussi, l'image réciproque de B est*

$$\begin{aligned} f^{-1}([-1,1]) &= \{x\in\mathbb{R}/f(x)\in[-1,1]\} \\ &= \left\{x\in\mathbb{R}/-1\le x^3\le 1\right\} \\ &= \left\{x\in\mathbb{R}/\sqrt[3]{-1}\le\sqrt[3]{x^3}\le\sqrt[3]{1}\right\} \\ &= \{x\in\mathbb{R}/-1\le x\le 1\} \\ &= [-1,1]. \end{aligned}$$

Proposition 2.2.2 *Soient Ω, F deux ensembles non vides, $f : \Omega \to F$ une application, $A_1, A_2 \subset \Omega$ et $B_1, B_2 \subset F$. On a :*

1. $A_1 \subset A_2 \implies f(A_1) \subset f(A_2)$.
2. $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$.
3. $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.
4. $B_1 \subset B_2 \implies f^{-1}(B_1) \subset f^{-1}(B_2)$
5. $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.
6. $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.
7. $A \subset f^{-1}(f(A)) \ / \ A \subset \Omega$.
8. $f(f^{-1}(B)) \subset B \ / \ B \subset F$.

Preuve. 1) Soit $y \in f(A_1)$, alors $\exists x \in A_1 / y = f(x)$. Or, $A_1 \subset A_2 \implies x \in A_2$. Ainsi, $y = f(x) \in f(A_2)$. Donc, $f(A_1) \subset f(A_2)$.
3) Soit $y \in f(A_1 \cup A_2)$, on a :

$$\begin{aligned} y \in f(A_1 \cup A_2) &\iff \exists x \in A_1 \cup A_2 / y = f(x) \\ &\iff (\exists x \in A_1 / y = f(x)) \vee (\exists x \in A_2 / y = f(x)) \\ &\iff (y \in f(A_1)) \vee (y \in f(A_2)) \\ &\iff y \in f(A_1) \cup f(A_2). \end{aligned}$$

D'où, $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.
4) On a $B_1 \subset B_2$. Soit $x \in E$, alors

$$\begin{aligned} x \in f^{-1}(B_1) &\iff f(x) \in B_1 \\ &\iff f(x) \in B_2 \\ &\iff x \in f^{-1}(B_2). \end{aligned}$$

Donc, si $B_1 \subset B_2$, alors $f^{-1}(B_1) \subset f^{-1}(B_2)$.
7) Si $x \in A$, alors $f(x) \in f(A)$. Ainsi, $x \in f^{-1}(f(A))$. □

Injectivité, Surjectivité, Bijectivité

Soient Ω, F deux ensembles non vides et $f : \Omega \to F$ une application.

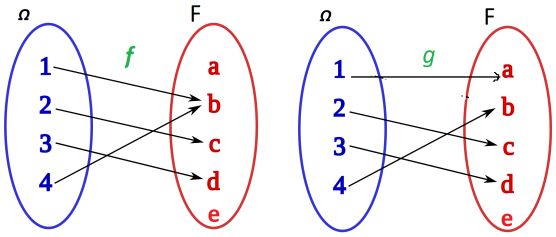
Définition 2.2.9 *f est dite injective si et seulement si toute image de F admet un unique antécédent de Ω.i.e*

$$\forall x, x' \in \Omega : f(x) = f(x') \implies x = x'.$$

f est non injective si il existe une image de F qui admet plus d'un antécédent de Ω.i.e

$$\exists x, x' \in \Omega : f(x) = f(x') \wedge x \neq x'.$$

Exemple 2.2.6 *1.*



f n'est pas injective car : $f(1) = f(4) \wedge 1 \neq 4$.

g est injective car toute image de F a au plus un antécédent dans Ω.

2. On a

$$\begin{aligned} h \quad : \quad & \mathbb{R} \to \mathbb{R} \\ & x \mapsto h(x) = |x| \end{aligned}$$

Cette application n'est pas injective car $|-2| = |2|$ avec $-2 \neq 2$.

3. Soit g une application définie par

$$\begin{aligned} g \quad : \quad & \mathbb{R}_+ \to \mathbb{R}_+ \\ & x \mapsto g(x) = \frac{1}{x+1} \end{aligned}$$

Soient $x, x' \in \mathbb{R}_+$, on a :

$$\begin{aligned} g(x) = g(x') \quad & \implies \frac{1}{x+1} = \frac{1}{x'+1} \\ & \implies x + 1 = x' + 1 \\ & \implies x = x'. \end{aligned}$$

Donc, g est injective.

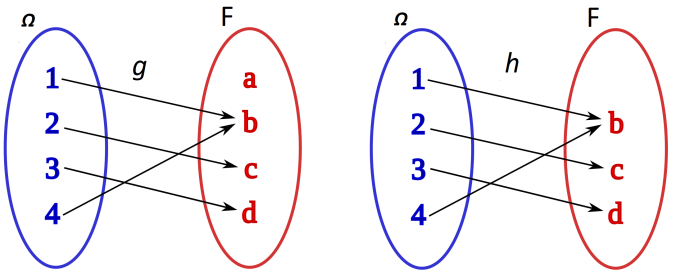
Définition 2.2.10 *Une application f est dite surjective si et seulement si tout élément de F admet au moins un antécédent dans Ω. i.e*

$$\forall y \in F, \exists x \in \Omega : y = f(x).$$

f n'est pas injective s'il existe un élément de F qui n'admet aucun antécédent. i.e

$$\exists y \in F, \forall x \in \Omega : f(x) \neq y.$$

Exemple 2.2.7 *1. Soient g, h deux appliactions telles que*



h est surjective, mais g n'est pas surjective car $a \neq g(x)$ pour tout $x \in \Omega$.

2. L'application

$$\begin{aligned} f \quad : \quad & \mathbb{R}_+ \to \mathbb{R} \\ & x \mapsto f(x) = \sqrt{x} \end{aligned}$$

n'est pas surjective car $y = -1$ n'admet aucun antécédent dans $\mathbb{R}_+$ par f.

3. On a

$$\begin{aligned} g \quad : \quad & \mathbb{R} \to \mathbb{R} \\ & x \mapsto g(x) = x^3 \ . \end{aligned}$$

Cette application est surjective car $\forall y \in \mathbb{R}, \exists x \in \Omega : y = g(x)$, toute image y admet un antécédent de la forme $\sqrt[3]{y}$.

Définition 2.2.11 *Soit $f : \Omega \to F$ une application.*

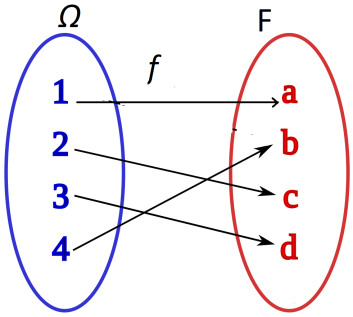
a) *f est dite bijective si elle est injective et surjective. Autrement dit, f est bijective si toute image de F admet un antécédent unique dans Ω.i.e :*

$$\forall y \in F, \exists! x \in \Omega; y = f(x).$$

b) *L'application qui fait correspondre à chaque $y \in F$, un unique $x \in \Omega$ est notée f^{-1} et est appelée la bijection réciproque de f. i.e*

$$f(x) = y \iff f^{-1}(y) = x.$$

Exemple 2.2.8 *Soit $\Omega = \{1, 2, 3, 4\}, F = \{a, b, c, d\}$. On considère l'application $f : \Omega \to F$ définie par*



f est bjective, car elle fait correspondre à chaque $x \in \Omega$ un unique $y \in F$.

Remarque 2.2.1 *Soient Ω, F deux ensembles de cardinaux finis et $f : \Omega \to F$ une application.*

1. f n'est pas bijective, si elle est non injective ou non surjective.

2. Si f est bijective, alors $Card(\Omega) = Card(F)$.

3. Si f est injective, alors $Card(\Omega) \leq Card(F)$.

4. Si f est surjective, alors $Card(\Omega) \geq Card(F)$.

Proposition 2.2.3 *(les ensembles $\Omega, F, \supset, H$ sont de cardinaux finis)*

a) *Soient $f : \Omega \to F$, $g : \Omega \to F$ deux applications :*

a.1. *Si $g \circ f$ est injective, alors f est injective.*

a.2. *Si $g \circ f$ est surjective, alors g est surjective.*

a.3. *Si f et g sont injectives, alors $g \circ f$ est injective.*

a.4. *Si f et g sont surjectives, alors $g \circ f$ est surjective.*

a.5. *Si f et g sont bijectives, alors $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

b) *Soit $h : \Im \to H$ une bijection. L'application réciproque h^{-1} vérifie :*

b.1. $(h^{-1})^{-1} = h$.

b.2. $h^{-1} \circ h = id_\Omega$, $h \circ h^{-1} = id_F$

Preuve.

a.1. Soient $x_1, x_2 \in E$ tels que $f(x_1) = f(x_2)$. Alors, $g(f(x_1)) = g(f(x_2)) \implies (g \circ f)(x_1) = (g \circ f)(x_2) \implies x_1 = x_2$ (car $g \circ f$ est injective). Ainsi, f est injective.

a.2. Si $g \circ f$ est surjective, alors

$$\forall z \in G, \exists x \in E \backslash z = (g \circ f)(x) = g(f(x)).$$

Si on pose $f(x) = y \in F$, alors on peut écrire :

$$\forall z \in G, \exists y \in F \backslash z = g(y).$$

D'où la surjectivité de g.

a.5. Montrons que si f et g sont bijectives, alors $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

On a : f et g bijectives $\implies$ $g \circ f$ est bijective. Ainsi,

$$\begin{aligned}
\left(f^{-1} \circ g^{-1}\right) \circ (g \circ f) &= f^{-1} \circ \left(g^{-1} \circ g\right) \circ f \\
&= f^{-1} \circ id_F \circ f \\
&= \left(f^{-1} \circ id_F\right) \circ f \\
&= f^{-1} \circ f \\
&= id_E.
\end{aligned}$$

D'où, $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

b.1. Soient $x \in G$ et $h(x) = y \in H$, on a $(h^{-1} \circ h)(x) = h^{-1}(h(x)) = h^{-1}(y) = x$.

Donc, $h^{-1} \circ h = id_G$.

b.2. Soient $x \in G$ et $h(x) = y \in H$, on a $(h \circ h^{-1})(y) = h(h^{-1}(y)) = h(x) = y$.

Donc, $h \circ h^{-1} = id_H$.

□

Théorème 2.2.1 *Soient deux applications* $f : \Omega \to F$, $g : F \to \Omega$ *telles que* $g \circ f = id_\Omega$ *et* $f \circ g = id_F$. *Alors :*

i. f *et* g *sont bijectives .*

ii. $f^{-1} = g$ *et* $g^{-1} = f$.

Restriction et Prolongement d'une application

Définition 2.2.12 *Soient* Ω, F *deux ensembles,* $f : \Omega \to F$ *une application et* A *un sous ensemble de* Ω. *Si pour tout élément* $x \in A$, *on a* $f(x) = f_A(x)$, *alors on dit que l'application* f_A *est la restriction de* f *à l'ensemble* A *et on écrit*

$$\begin{aligned} f_A \ : \ & A \to F \\ & x \mapsto f_A(x) = f(x) \ . \end{aligned}$$

Définition 2.2.13 *Soient* Ω, F *deux ensembles,* $f, g : \Omega \to F$ *deux applications . On dit que* g *est un prolongement de* f *si :*

$$D_f \subset D_G \ et \ \forall x \in D_f : g(x) = f(x).$$

Exemple 2.2.9 *Soient les applications suivantes :*

$$\begin{array}{ll} f : \mathbb{R} \to \mathbb{R} & f_A : \mathbb{R}_+ \to \mathbb{R} \\ \quad x \mapsto f(x) = x^2 & \quad x \mapsto f_A(x) = x^2 \end{array}$$

$$g : \mathbb{R} \to \mathbb{R}$$

$$x \mapsto g(x) = \begin{cases} x^2 & / \, x \in \mathbb{R}_+ \\ 0 & / \, x \in \mathbb{R}_-^* \end{cases} .$$

- On remarque que f_A *est la restriction de* f *à l'ensemble* $\mathbb{R}_+$. *On peut dire aussi que* f *est le prolongement de* f_A *à l'ensemble* $\mathbb{R}$.

- Par un simple dessin on peut vérifier que l'application g *représente un autre prologement de* f_A.

2.3 Exerices corrigés

Exercice 2.3.1 *Donner $A \cap B, A \cup B, A\backslash B, \complement_{\mathbb{R}} B$ dans les cas suivants*

1. $A = [-3, 2]$, $B =]0, 6]$

2. $A = [1, 4[$, $B = [4, 7]$

3. $A =]-2, 0[$, $B = [-1, +\infty[$

Solution

A	B	$A \cap B$	$A \cup B$	$A\backslash B$	$\complement_{\mathbb{R}} B$
$[-3, 2]$	$]0, 6]$	$]0, 2]$	$[-3, 6]$	$[-3, 0]$	$]-\infty, 0] \cup]6, +\infty[$
$[1, 4[$	$[4, 7]$	$\emptyset$	$[1, 7]$	A	$]-\infty, 4[\cup]7, +\infty[$
$]-2, 0[$	$[-1, +\infty[$	$[-1, 0[$	$]-2, +\infty[$	$]-2, -1[$	$]-\infty, -1[$

Exercice 2.3.2 *Soient A, B et C deux parties non vides de Ω. Montrer que :*

1. $A \cup B = B \iff A \subseteq B$.

2. $A\backslash B = A \cap C_\Omega B$.

3. $A \subset B \implies \complement_\Omega B \subset \complement_\Omega A$.

Solution : *1) Montrons que $A \cup B = B \iff A \subseteq B$.*

i. Supposons que $A \subseteq B$ et soit $x \in A \cup B$. Alors, $x \in A \cup B \implies (x \in A \vee x \in B)$. *Comme $A \subseteq B$, on a $x \in A \cup B \implies (x \in B \vee x \in B) \implies x \in B \implies A \cup B \subset B$.*

Si $x \in B$ et $A \subseteq B$, alors $x \in A$ ou $x \in B$.D'où; $B \subset A \cup B$. Donc, $A \subseteq B \implies A \cup B = B$.

ii. Supposons que $A \cup B = B$. Alors, soit $x \in A$

$x \in A \implies x \in A \cup B \implies x \in B$. Ainsi, $A \subseteq B$. Donc, $A \cup B = B \implies A \subseteq B$.

2. Montrons que $A\backslash B = A \cap \complement_\Omega B$. Soit $x \in E$.

$$\begin{aligned} x \quad \in \quad & A\backslash B \implies x \in A \text{ et } x \notin B \\ \implies \quad & x \in A \text{ et } x \in \complement_\Omega B \\ \implies \quad & x \in A \cap \complement_\Omega B. \end{aligned}$$

Ainsi, $A\backslash B \subset A \cap \complement_\Omega B$. De la même manière, on montre $A \cap \complement_\Omega B \subset A\backslash B$. On a

$$\begin{aligned} x \quad \in \quad & A \cap \complement_\Omega B \implies x \in A \text{ et } x \in \complement_\Omega B \\ \implies \quad & x \in A \text{ et } (x \in E \text{ et } x \notin B) \\ \implies \quad & x \in A\backslash B. \end{aligned}$$

D'où le résultat.

3. Supposons que $A \subset B$. Soit $x \in E$ tel que $x \in \complement_\Omega B$, alors $x \in E, x \notin B$. Comme $A \subset B$, alors $x \notin A$. Donc, $x \in \complement_\Omega A$.

Exercice 2.3.3 *E , F et G étant trois parties de Ω, on définit l'opérateur de la différence symétrique " Δ " par*

$$E\Delta F = (E\backslash F) \cup (F\backslash E)\,.$$

Montrer les égalités suivantes :

a. $(E \cap F) \cap \complement_\Omega (E \cap G) = E \cap F \cap \complement_\Omega G$

b. $(E \cap G) \cap \complement_\Omega (E \cap F) = E \cap G \cap \complement_\Omega F$

En déduire que $(E \cap F)\,\Delta\,(E \cap G) = E \cap (F\Delta G)\,.$

Solution a. $(E \cap F) \cap \complement_\Omega (E \cap G) = E \cap F \cap \complement_\Omega G$. En effet, en utilisant la loi de Morgan on a

$$\begin{aligned}(E \cap F) \cap \complement_\Omega (E \cap G) &= (E \cap F) \cap \left(\complement_\Omega E \cup \complement_\Omega G\right)\\ &= \left[E \cap F \cap \complement_\Omega E\right] \cup \left[E \cap F \cap \complement_\Omega G\right]\\ &= \emptyset \cup \left[E \cap F \cap \complement_\Omega G\right]\\ &= E \cap F \cap \complement_\Omega G\end{aligned}$$

De manière similaire on aura $(E \cap G) \cap \complement_\Omega (E \cap F) = E \cap G \cap \complement_\Omega F$.

Maintenant, on a

$$(E \cap F)\,\Delta\,(E \cap G) = ((E \cap F) \setminus (E \cap G)) \cup ((E \cap G) \setminus (E \cap F))\,.$$

De plus,

$$\begin{aligned}(E \cap F) \setminus (E \cap G) &= (E \cap F) \cap \complement_\Omega (E \cap G)\\ \text{et } (E \cap G) \setminus (E \cap F) &= (E \cap G) \cap \complement_\Omega (E \cap F)\,.\end{aligned}$$

En utilisant les résultats de la question précédente et la loi de Morgan, on obtient

$$\begin{aligned}(E \cap F)\,\Delta\,(E \cap G) &= \left(E \cap F \cap \complement_\Omega G\right) \cup \left(E \cap G \cap \complement_\Omega F\right)\\ &= E \cap \left[\left(F \cap \complement_\Omega G\right) \cup \left(G \cap \complement_\Omega F\right)\right]\\ &= E \cap [(F\backslash G) \cup (G\backslash F)]\\ &= E \cap (F\Delta G)\,.\end{aligned}$$

Exercice 2.3.4 *Soit* $f : \mathbb{N}^2 \to \mathbb{N}$ *et* $g : \mathbb{N} \to \mathbb{N}^2$ *deux applications définies par* $f(n,m) = nm$ *et* $g(n) = \left(n, (n+1)^2\right)$. *Que peut-on dire sur l'injectivité et la surjectivité de* f *et* g.

Solution

1) - L'application f *n'est pas injective car les deux antécédents* $(1,4)$ *et* $(2,2)$ *sont différents mais ont la même image. i.e* $f(1,4) = f(2,2) = 4$.

- Elle est surjective car pour toute image $y \in \mathbb{N}, \exists (n,m) \in \mathbb{N}^2$ *tel que* $f(n,m) = y$. *Par exemple, on peut prendre* $(n,m) = (1,y)$.

2) L'application g *est injective.En effet, en appliqunt la définition de l'injectivité pour tout* $n, n' \in \mathbb{N}$, *peut écrire :*

$$\begin{aligned} g(n) &= g(n') \implies \left(n,(n+1)^2\right) = \left(n',(n'+1)^2\right) \\ &\implies n = n' \wedge (n+1)^2 = (n'+1)^2 \\ &\implies n = n'. \end{aligned}$$

-L'image $(0,2)$ *n'admet aucun antécédent dans* $\mathbb{N}$ *car*

$$\begin{aligned} g(n) &= (0,2) \implies \left(n,(n+1)^2\right) = (0,2) \\ &\implies n = 0 \wedge (n+1)^2 = 2 \\ &\implies n = 0 \wedge 1^2 = 2 \end{aligned}$$

ce qui est absurde. Donc, g *n'est pas surjective.*

Exercice 2.3.5 *On considère l'application* $f : \mathbb{R} \to \mathbb{R}$ *définie par* $f(x) = 5x + 17$.

- Déterminer $f^{-1}(\{2\})$, $f^{-1}(\{-5\})$, $f^{-1}(\{y\})$.

- Montrer que f *est bijective.*

- Déterminer l'application f^{-1}.

- Vérifier que $f^{-1} \circ f = id_{\mathbb{R}}$ *et* $f \circ f^{-1} = id_{\mathbb{R}}$.

Solution

1)On a

$$\begin{aligned} f^{-1}(\{2\}) &= \{x \in \mathbb{R} : \ f(x) = 2\} \\ &= \{x \in \mathbb{R} : \ 5x + 17 = 2\} \\ &= \{-3\}, \end{aligned}$$

et

$$\begin{aligned} f^{-1}(\{-5\}) &= \{x \in \mathbb{R} :\ f(x) = -5\} \\ &= \{x \in \mathbb{R} :\ 5x + 17 = -5\} \\ &= \left\{-\frac{22}{5}\right\}. \end{aligned}$$

Puis,

$$\begin{aligned} f^{-1}(\{y\}) &= \{x \in \mathbb{R} :\ f(x) = y\} \\ &= \{x \in \mathbb{R} :\ 5x + 17 = y\} \\ &= \left\{\frac{y-17}{5}\right\}. \end{aligned}$$

2) f est surjective, toute image y admet un antécédent par f de la forme $\frac{y-17}{5}$. De plus, elle est injective car pour tout $x, x' \in \mathbb{R}$, on a

$$f(x) = f(x') \implies 5x + 17 = 5x' + 17 \implies x = x'.$$

Donc, f est bijective.

3) De ce qui précède, on a $f^{-1}(x) = \dfrac{x-17}{5}$, et

$$\begin{aligned} \left(f^{-1} \circ f\right)(x) &= f^{-1}\left(f(x)\right) = \frac{f(x) - 17}{5} = x; \\ \left(f \circ f^{-1}\right)(x) &= f\left(f^{-1}(x)\right) = 5\left(\frac{x-17}{5}\right) + 17 = x. \end{aligned}$$

D'où, $f^{-1} \circ f = id_{\mathbb{R}}$ et $f \circ f^{-1} = id_{\mathbb{R}}$.

Exercice 2.3.6 *Soient $\Omega = [-3, 2], \Gamma = [0, 4]$ et l'application $h : \mathbb{R} \to \mathbb{R}$, telle que $h(x) = x^2 + 1$.*

- A-t-on $h(\Omega \cap \Gamma) \subset h(\Omega) \cap h(\Gamma)$?

- Sous quelle condition peut on avoir $h(\Omega \cap \Gamma) = h(\Gamma) \cap h(\Omega)$.

Solution 1. *On a $\Omega \cap \Gamma = [0, 2]$, ainsi*

$$\begin{aligned} h(\Omega \cap \Gamma) &= \{h(x) : x \in \Omega \cap \Gamma\} \\ &= \left\{x^2 + 1 : 0 \leq x \leq 2\right\} \\ &= [1, 5]. \end{aligned}$$

De plus ,

$$\begin{aligned} h(\Omega) &= \{h(x) : x \in \Omega\} \\ &= \left\{x^2 + 1 : -3 \leq x \leq 2\right\} \\ &= \left\{x^2 + 1 : -3 \leq x \leq 0 \vee 0 \leq x \leq 2\right\} \\ &= [1, 10] \cup [1, 5] \\ &= [1, 10] \end{aligned}$$

et

$$\begin{aligned} h(\Gamma) &= \{h(x) : x \in \Gamma\} \\ &= \left\{x^2 + 1 : 0 \leq x \leq 4\right\} \\ &= [1, 17]. \end{aligned}$$

D'où, $h(\Omega) \cap h(\Gamma) = [1, 10]$.

Il est clair que $h(\Omega \cap \Gamma) \subset h(\Omega) \cap h(\Gamma)$, mais $h(\Omega) \cap h(\Gamma) \subsetneq h(\Omega \cap \Gamma)$.

2. Cherchons une condition pour avoir l'égalité $h(\Omega \cap \Gamma) = h(\Omega) \cap h(\Gamma)$.

Soit $b \in h(\Omega) \cap h(\Gamma)$, alors $b \in h(\Omega)$ et $b \in h(\Gamma)$. Ainsi, $\exists\, (a, a') \in \Omega \times \Gamma$ tels que $h(a) = b$ et $h(a')$.

Si h est injective, alors $a = a'$. Donc, on peut dire que pour tout $b \in h(\Omega) \cap h(\Gamma), \exists a \in \Omega \cap \Gamma$: $b = h\,(a)$. D'où, $b \in h(\Omega \cap \Gamma)$.

Par conséquent, $(h\ injective) \implies h(\Omega \cap \Gamma) = h(\Omega) \cap h(\Gamma)$.

2.4 Exercices supplémentaires

Exercice 2.4.1 *Écrire mathématiquement les ensembles suivants :*

A : *l'ensemble des entiers relatifs impairs.*

B : *l'ensemble des entiers naturels de 4 à 13.*

C : *l'ensemble des nombres réels strictement positifs.*

Exercice 2.4.2 *Soit* $E = \{0, 1, 2, 3, 4, 5, 6\}$, $A = \{1, 3\}$, $B = \{2, 3, 4, 6\}$.
Déterminer $A \cup B$, $A \cap B$, $E \backslash A$, $A \times B$, $\complement_\Omega A$, $\complement_\Omega B$.

Exercice 2.4.3 *Écrire en extension (c'est-à-dire en donnant tous leurs éléments) les ensembles suivants :*

$$\begin{aligned} A &= \left\{ \text{ nombres entiers compris entre } \sqrt{2} \text{ et } 2\pi \right\}. \\ B &= \left\{ x \in \mathbb{Q}; \exists\, (n,p) \in \mathbb{N} \times \mathbb{N},\ x = \frac{p}{n} \text{ et } 1 \leq p \leq 2n \leq 7 \right\}. \end{aligned}$$

Exercice 2.4.4 *Soit* $A = \{(x, y) \in \mathbb{R}^2,\ x^2 + y^2 \leq 1\}$. *Démontrer que* A *ne peut pas s'écrire comme le produit cartésien de deux parties de* $\mathbb{R}$.

Exercice 2.4.5 *Soient* A *et* B *deux ensembles non vides. Montrer que :*

1. $A \cap B = B \iff B \subseteq A$.

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

3. $A \cup B = A \cap B \iff A = B$.

4. $A \backslash B = A \iff B \backslash A = B$.

Exercice 2.4.6 E , F *et* G *étant trois parties de* Ω, *on définit l'opération* Δ *par*

$$E \Delta F = (E \backslash F) \cup (F \backslash E).$$

Montrer les égalités suivantes :

a. $(E \cup F) \cap \complement_\Omega (E \cup G) = \complement_\Omega E \cap F \cap \complement_\Omega G$

b. $(E \cup G) \cap \complement_\Omega (E \cup F) = \complement_\Omega E \cap G \cap \complement_\Omega F$

En déduire que $(E \cup F) \Delta (E \cup G) = \complement_\Omega E \cap (F \Delta G)$.

Exercice 2.4.7 *Soient* $f : \mathbb{N} \to \mathbb{N}$ *et* $g : \mathbb{N} \to \mathbb{N}$ *deux applications définies par* $f(n) = n+1$ *et* $g(n) = \begin{cases} 0 & si\ n = 0 \\ n-1 & si\ n \neq 0 \end{cases}$.

-Etudier l'injectivité, la surjectivité et la bijectivité de f *et* g.

-Préciser et comparer $f \circ g$ *et* $g \circ f$.

Exercice 2.4.8 *Soient* $g : E \to F, h : E \to F$ *et* $f : F \to G$ *trois applications. Démontrer que si* f *est injective et* $f \circ g = f \circ h$, *alors* $g = h$.

Exercice 2.4.9 *On considère l'application* $f : \mathbb{R}\setminus\{-1\} \to \mathbb{R}\setminus\{1\}$ *définie par* $f(x) = \dfrac{x+2}{x+1}$.

-Démontrer que f *est une bijection et déterminer sa réciproque.*

-Répondre aux mêmes questions pour

$$\begin{array}{c} g : \mathbb{R} \to]-1, 1[\\ x \mapsto \dfrac{x}{1+|x|} \end{array}.$$

Exercice 2.4.10 *Soient* I *et* J *deux intervalles de* $\mathbb{R}$. *Soit* $f \in \mathcal{F}(I, J)$.

-Montrer que si f *est strictement monotone sur* I, *alors elle est injective.*

-Si on suppose que f *est uniquement monotone sur* I, f *est-elle nécessairement injective ?*

Soient A *et* B *deux sous-ensembles d'un ensemble* Ω. *Pour tout* $x \in \Omega$, *on définit les propositions* $P_A(x)$ *et* $P_B(x)$ *comme suit*

$$P_A(x) : x \in A \quad \text{et } P_B(x) : x \in B.$$

1. Ecrire en fonction de $P_A(x)$ *et* $P_B(x)$ *les relations ensemblistes :*

$$A \subset B, \quad A = B, \quad A \cap B, \quad A \cup B, \quad A\setminus B.$$

2. En déduire utilisant les tables de vérité que :

$$(A\setminus B) \cup (B\setminus A) = (A \cup B) \setminus (A \cap B).$$

Soient $f : E \to F$ *une fonction donnée. Montrer que*

1. f *est injective si et seulement s'il existe une fonction* $g : F \to E$ *telle que* $g \circ f = Id_E$.

2. f *est surjective si et seulement s'il existe une fonction* $h : F \to E$ *telle que* $f \circ h = Id_F$.

Chapitre 3

Relations Binaires

Cette partie du cours est consacrée aux relations binaires. En se basant sur les définitions vues dans le chapitre précédent, on présentera deux types de relations binaires " les relations d'équivalence" et "les relations d'ordre". Et pour une bonne compréhension de ces nouvelles notions, on proposera quelque exercices corrigés à la fin du chapitre.

3.1 Définitions et Propriétés

Définition 3.1.1 *Une relation $\Re$ est dite binaire si elle est définie de Ω vers Ω.*

Définition 3.1.2 *Une relation binaire $\Re$ dans Ω est dite :*

Réflexive $\iff \forall x \in \Omega;\ x\Re x$.

Symétrique $\iff \forall (x,y) \in \Omega^2;\ x\Re y \implies y\Re x$.

Antisymétrique $\iff \forall (x,y) \in \Omega^2;\ x\Re y$ *et* $y\Re x \implies x = y$.

Transitive $\iff \forall (x,y,z) \in \Omega^3;\ x\Re y$ *et* $y\Re z \implies x\Re z$.

Exemple 3.1.1

1. *Sur $\mathbb{R}$, l'égalité est une relation refléxive, symétrique et transitive.*
2. *La relation perpendiculaire notée $\perp$ sur l'ensemble des droites du plan euclidien est symétrique.*
3. *L'inclusion des ensembles "$\subset$" est une relation réflexive, antisymétrique et transitive.*

3.2 Relation d'équivalence

Définition 3.2.1 *Soit $\Re$ une relation binaire sur Ω.*

$\Re$ est dite relation d'équivalence si et seulement si : $\Re$ est réflexive, symétrique et transitive.

Exemple 3.2.1 *Soit $\Re$ une relation binaire de $\mathbb{R}^2$ définie par*

$$(x,y)\,\Re\,(x',y') \iff x+y=x'+y'$$

$\Re$ est réflexive car : $\forall (x,y)\in\mathbb{R}^2$, on a

$$x+y=x+y \iff (x,y)\,\Re\,(x,y)\,.$$

$\Re$ est symétrique car pour tout $(x,y),(x',y')\in\mathbb{R}^2$, on a

$$\begin{aligned}(x,y)\,\Re\,(x',y') &\iff x+y=x'+y'\\ &\iff x'+y'=x+y\\ &\iff (x',y')\,\Re\,(x,y)\,.\end{aligned}$$

$\Re$ est transitive parce que : $\forall (x,y),(x',y'),(x'',y'')\in\mathbb{R}^2$, on a

$$\begin{aligned}\begin{cases}(x,y)\,\Re\,(x',y')\\ (x',y')\,\Re\,(x'',y'')\end{cases} &\iff \begin{cases}x+y=x'+y'\\ x'+y'=x''+y''\end{cases}\\ &\iff x+y=x''+y''\\ &\iff (x,y)\,\Re\,(x'',y'')\,.\end{aligned}$$

Par conséquent, $\Re$ est une relation d'équivalence.

Définition 3.2.2 *Soit l'ensemble Ω muni d'une relation d'équivalence $\Re$.*

-On appelle la classe d'équivalence de $x\in\Omega$, et on note $\dot{x}$ l'ensemble des éléments de Ω équivalents à x; et on écrit

$$\dot{x}=\{\alpha\in\Omega : x\Re\alpha\}\,.$$

-Les classes d'équivalence forment une partition de Ω . L'ensemble des classes d'équivalence noté $\Omega/_{\Re}$ appelé ensemble quotient de Ω par $\Re$.

$$\Omega/_{\Re}=\left\{\dot{x}\ /\ x\in\Omega\right\}.$$

Exemple 3.2.2 *En utilisant l'exemple précédent ,*

$$\begin{aligned}\dot{\widehat{(0,0)}} &= \left\{(x,y)\in\mathbb{R}^2 : (0,0)\,\Re\,(x,y)\right\}\\ &= \left\{(x,y)\in\mathbb{R}^2 : 0+0=x+y\right\}\\ &= \left\{(x,y)\in\mathbb{R}^2 : -x=y\right\}\\ &= \{(x,-x)\,/x\in\mathbb{R}\}\,.\end{aligned}$$

3.3 Relations d'ordre

Définition 3.3.1 *Soit Ω un ensemble non vide. On dit qu'une relation binaire $\Re$ dans Ω est une relation d'**ordre** si elle est réflexive, antisymétrique et transitive.*

Remarque 3.3.1

1. *Muni d'une relation d'ordre, Ω est dit **ordonné**.*
2. *La relation d'ordre est notée, généralement, par $\preceq$.*
3. *La relation $x \preceq y$ se lit x inférieur ou égal à y.*
4. *On dit que x et y sont **comparables** si $x \preceq y$ ou $y \preceq x$.*
5. *On dit que l'ordre est **total** dans $(\Omega, \preceq)$ si tout les éléments de Ω sont comparables, et que Ω est totalement ordonné.*
6. *Si l'ordre dans $(\Omega, \preceq)$ n'est pas total, alors on dit qu'il est **partiel,** et Ω est partiellement ordonné.*

Exemple 3.3.1

1. *Dans l'ensemble $P(\Omega)$ des parties d'un ensemble Ω, la relation d'inclusion est une relation d'ordre partiel.*
2. *La relation $\leq$ est d'ordre total dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ et $\mathbb{R}$.*
3. *La relation $<$ n'est pas une relation d'ordre car elle n'est pas réflexive.*

3.3.1 Parties majorées, minorées, bornées

Définition 3.3.2 *Soient Ω un ensemble muni de la relation d'ordre $\preceq$, P une partie non vide de Ω.*

1. *-On dit que $x \in \Omega$ est un* ***majorant*** *de P (x majore P ou P est majorée par x) si :* $\forall p \in P : p \leq x$.

   -L'ensemble des majorants de P dans Ω, se note $Maj_{\Omega}(P)$.i.e

$$Maj_{\Omega}(P) = \{x \in \Omega,\ \forall p \in P : p \leq x\}.$$

2. *-On dit que $y \in \Omega$ est un* ***minorant*** *de P (y minore P ou P est minorée par y) si :* $\forall p \in P : y \leq p$.

   -L'ensemble des minorants de P dans Ω, se note $Min_{\Omega}(P)$.i.e

$$Maj_{\Omega}(P) = \{y \in \Omega,\ \forall p \in P : y \leq p\}.$$

3. *La partie P est dite* ***bornée*** *si elle est majorée et minorée.*

4. ***Le plus grand élément*** *de P qu'on note "α" est l'unique majorant de P appartenant à P. i.e*

$$\text{" } \alpha \in P,\ \forall p \in P : p \leq \alpha \text{ "}$$

5. ***Le plus petit élément*** *de P est l'unique minorant de P appartenant à P. i.e*

$$\text{" } \beta \in P,\ \forall p \in P : \beta \leq p \text{ "}$$

6. ***La borne supérieure*** *de P est le plus petit des majorant (s'il existe) et se note* $\sup\limits_{p \in P}(p)$.
7. ***La borne inférieure*** *de P est le plus grand des minorant (s'il existe) et se note* $\inf\limits_{p \in P}(p)$.

Exemple 3.3.2 *Soit $\Omega = \{1, a, 2, 4, b\}$, $(\digamma, \subset)$ ordonné tel que $\digamma = P(\Omega)$ et une partie $A = \{\{a, 2\}, \{2, 4, b\}, \{1, 2, b\}, \{a, 2, 4\}\}$, on a :*

- *Le seul majorant de A est $\Omega = \{1, a, 2, 4, b\}$.*
- $\sup(A) = \Omega$.
- *Le plus grand élément n'existe pas.*
- *Les minorants de A sont $\emptyset$ et $\{2\}$.*
- $\inf(A) = \{2\}$.
- *Le plus petit élément n'existe pas.*

Remarque 3.3.2 *1. Si les bornes supérieure et inférieure d'une partie P existent, alors elles sont uniques.*

2. Si un ensemble Ω est totalement ordonné, alors toute partie $P \subset \Omega$ admet un plus grand et un plus petit élément.

3. Le plus petit élément de P (résp. le plus grand élément) est un minorant (résp. majrant) de P. Mais, la réciproque n'est pas toujours vraie.

3.4 Exercices corrigés

Exercice 3.4.1 *Soit la relation binaire définie dans* $\mathbb{R}^*$ *par :*

$$\forall x, y \in \mathbb{R}^*, x\Re y \iff xy > 0.$$

- *Montrer que* $\Re$ *est une relation d'équivalence.*
- *Déterminer la classe d'équivalence de* $x \in \mathbb{R}^*$.
- *Déterminer l'ensemble quotient* $\mathbb{R}^*/\Re$.

Solution

a) Montrons que $\Re$ est une relation d'équivalence

1. $\Re$ est réflexive car pour tout $x \in \mathbb{R}^*$; on a $x^2 > 0$. D'où, $x\Re x$.
2. $\Re$ est symétrique. En effet, pour $x, y \in \mathbb{R}^*$, on a

$$x\Re y \iff xy > 0 \iff yx > 0 \iff y\Re x.$$

3. $\Re$ est transitive. Pour tout $x, y, z \in \mathbb{R}^*$, $x\Re y$ et $y\Re z$

$$\begin{aligned} x\Re y \text{ et } y\Re z &\iff xy > 0 \text{ et } yz > 0 \\ &\iff xy^2z > 0 \\ &\iff xz > 0 \\ &\iff x\Re z. \end{aligned}$$

Par conséquent, $\Re$ est une relation d'équivalence.

b) La classe d'équivalence de $x \in \mathbb{R}^*$ est

$$\begin{aligned} \dot{x} &= \{\alpha \in \mathbb{R}^* : x\Re\alpha\} \\ &= \{\alpha \in \mathbb{R}^* : x\alpha > 0\}. \end{aligned}$$

Si $x < 0$ alors $\dot{x} = \{\alpha \in \mathbb{R}^* : \alpha < 0\} = \mathbb{R}^*_-$.

Si $x > 0$ alors $\dot{x} = \{\alpha \in \mathbb{R}^* : \alpha > 0\} = \mathbb{R}^*_+$.

c) L'ensemble quotient $\mathbb{R}^*/\Re = \left\{\dot{x}/x \in \mathbb{R}^*\right\} = \left\{\mathbb{R}^*_-, \mathbb{R}^*_+\right\}$.

Exercice 3.4.2 *Soit* $E = \{a, b, c\}$.

- *Déterminer l'ensemble* $P(E)$ *des parties de* E.

- *Soit* $\Re$ *la relation définie sur* $P(E)$ *par*

$$A\Re B \iff Card(A) = Card(B).$$

i) *Montrer que* $\Re$ *est une relation d'équivalence.*

ii) *Déterminer toutes les classes d'équivalence* $\dot{A}$ *pour* $A \in P(E)$.

iii) *Déterminer l'ensemble quotient* $E/\Re$.

Solution

1. L'ensemble des parties de $E = \{a, b, c\}$ est

$$P(E) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

2.i Pour tout $A, B \in P(E)$; on a

$$A\Re B \iff Card(A) = Card(B).$$

a. $\Re$ est réflexive car $\forall A \in P(E)$;

$$Card(A) = Card(A) \iff A\Re A.$$

b. On a aussi,

$$\begin{aligned} A\Re B &\iff Card(A) = Card(B) \\ &\iff Card(B) = Card(A) \\ &\iff B\Re A. \end{aligned}$$

Ainsi, $\Re$ est symétrique.

c. Soient $A, B, C \in P(E)$,

$$\begin{aligned} \begin{cases} A\Re B \\ B\Re C \end{cases} &\iff \begin{cases} Card(A) = Card(B) \\ Card(B) = Card(C) \end{cases} \\ &\iff Card(A) = Card(C) \\ &\iff A\Re C. \end{aligned}$$

D'où, la transitivité.

De **a, b** et **c** , on déduit que $\Re$ est une relation d'équivalence.

2.ii Les classes d'équivalence de tout élément de $P(E)$ sont :

$$\dot{\emptyset} = \{\emptyset\}, \qquad \dot{E} = \{E\},$$

$$\dot{\{a\}} = \dot{\{b\}} = \dot{\{c\}} = \{\{a\}, \{b\}, \{c\}\},$$

$$\dot{\{a, b\}} = \dot{\{a, c\}} = \dot{\{b, c\}} = \{\{a, b\}, \{a, c\}, \{b, c\}\}.$$

2.iii Pour construire l'ensemble quotient de $P(E)$ par $\Re$, on prend un seul représentant par classe. On obtient alors :

$$P(E)/\Re = \left\{\dot{\emptyset}, \dot{\{a\}}, \dot{\{a, b\}}, \dot{E}\right\}.$$

Exercice 3.4.3 *Soit la relation S définie sur $\mathbb{R}^2$ par*

$$\forall (a, b), (c, d) \in \mathbb{R}^2; (a, b) S (c, d) \iff a^2 + b^2 = c^2 + d^2.$$

- *Montrer que S est une relation d'équivalence.*
- *Déterminer la classe d'équivalence $\overline{(a, b)}$ de $(a, b) \in \mathbb{R}^2$, que représente-t-elle géométriquement.*

Solution

1. -S est une relation d'équivalence. En effet, pour tout $(a, b) \in \mathbb{R}^2$, $a^2 + b^2 = a^2 + b^2 \iff (a, b) S (a, b)$. (réflexivité)

   -Il est claire qu'elle est symétrique $\forall (a, b), (c, d) \in \mathbb{R}^2$;

   $$(c, d) S (a, b) \iff c^2 + d^2 = a^2 + b^2.$$

   -(transitivité) $\forall (a, b), (c, d), (e, f) \in \mathbb{R}^2$; on a $(a, b) S (a, b)$ et $(a, b) S (a, b)$ entraine $a^2 + b^2 = c^2 + d^2 = e^2 + f^2$.

   Donc, S est d'équivalence.

2. La classe d'équivalence de (a,b)

$$\begin{aligned}\overline{(a,b)} &= \left\{(c,d)\in\mathbb{R}^2;(a,b)\,S\,(c,d)\right\}\\ &= \left\{(c,d)\in\mathbb{R}^2;a^2+b^2=c^2+d^2\right\}.\end{aligned}$$

$\overline{(a,b)}$ représente le cercle de centre $(0,0)$ et de rayon $\sqrt{a^2+b^2}$.

Exercice 3.4.4 *Dans* $\mathbb{N}^*$, *on définit une relation* $\Re$ *par*

$$\forall\,(a,b)\in\mathbb{N}^*\times\mathbb{N}^*,\quad a\Re b \iff \exists n\in\mathbb{N}^*/b=a^n.$$

- *Démontrer que* $\Re$ *est une relation d'ordre partiel.*
- *Soient* $A=\{2,4,16\}$ *et* $B=\{3,9,27,729\}$; *déterminer le plus grand élément et le plus petit élément de* A *et* B.

Solution

1. -Soit $a\in\mathbb{N}^*$. Pour $n=1$, on a $a=a^1$. Ainsi, $\Re$ est réflexive.

   - *Soient* a,b deux entiers non nuls et différents. Alors , $a\Re b$ et $b\Re a$ signifie qu'il existe $n,m\in\mathbb{N}^*$ tel que $b=a^n$ et $a=b^m$, ainsi $b=(b^m)^n=b^{mn}$. Ce qui mène à $b^{mn-1}=1$, d'où $nm=1$. Donc, $n=m=1$ et $a=b$. On conclut que la relation est antisymétrique.

   -Soient $a,b,c\in\mathbb{N}^*$et $m,n\in\mathbb{N}^*$ tels que $b=a^n$ et $c=b^m$. Alors, $\exists l\in\mathbb{N}^*:c=a^l$ tel que $l=mn$. D'où, $a\Re b$ et $b\Re c \iff a\Re c$.

   De tout ce qui précède, on déduit que $\Re$ est une relation d'ordre. De plus, 3 n'est pas en relation avec 4 car $\forall n\in\mathbb{N}^*, 4\neq 3^n$. Donc, l'ordre est partiel.

2. i) On a $A=\{2,4,16\}$.

   -Le plus grand élément de A est 16 car on a $2\Re 16, 4\Re 16, 16\Re 16$.

   -Le plus petit élément de A est 2 car on a $2\Re 2, 2\Re 4, 2\Re 16$.

   ii) Pour $B=\{3,9,27,729\}$, on a

   -Le plus grand élément est 729.

   -Le plus petit élément est 3.

Exercice 3.4.5 *Soit $\Re$ la relation définie sur $\mathbb{N}^*$ par*

$$n\Re m \iff \exists a \in \mathbb{N}^* : n = am$$

1. Montrer que $\Re$ est une relation d'ordre.

2. L'ordre est-il total ? Justifier la réponse.

Solution

1. **Montrons que $\Re$ est d'ordre**

Pour tout $n \in \mathbb{N}^*$, on a $n = 1 \cdot n$. D'où, $n\Re n$. Donc, $\Re$ est réflexive.

$\Re$ est antisymétrique car $\forall n, m \in \mathbb{N}^*$:

$$\begin{aligned} n\Re m \text{ et } m\Re n &\iff \exists a, b \in \mathbb{N}^* : n = am \text{ et } m = bn \\ &\iff \exists a, b \in \mathbb{N}^* : \ n = a\,(bn) \\ &\iff \ ab = 1 \quad / \quad a, b \in \mathbb{N}^* \\ &\iff a = b = 1. \end{aligned}$$

Ainsi, $n = m$.

La relation $\Re$ est transitive. En effet, pour $n, m, l \in \mathbb{N}^*$ on a

$$\begin{aligned} n\Re m \text{ et } m\Re l &\iff \exists a, b \in \mathbb{N}^* : n = am \text{ et } m = bl \\ &\iff \exists a, b \in \mathbb{N}^* : n = a\,(bl) \\ &\iff \exists c \in \mathbb{N}^* : n = cl \qquad \text{où } c = ab. \\ &\iff n\Re l. \end{aligned}$$

De ce qui précède, on conclut que $\Re$ est une relation d'ordre.

2. L'ordre n'est pas total dans $\mathbb{N}^*$, par exemple 2 et 5 ne sont pas comparables (5 n'est pas multiple de 2).

Exercice 3.4.6 *Sur $\mathbb{R}^2$, on définit la relation T par*

$$\forall\,(x, y)\,, (x', y') \in \mathbb{R}^2 : (x, y)\,T\,(x', y') \iff |x - x'| \leq y' - y.$$

- *Vérifier que T est une relation d'ordre. Cet ordre est-il total ?*

- *Soit* $(a,b) \in \mathbb{R}^2$, *représenter l'ensemble* $\{(x,y) \in \mathbb{R}^2 / \, (x,y)\, T\, (a,b)\}$.

Solution

La relation T est une relation d'ordre. En effet, elle est réflexive car pour tout $(x,y) \in \mathbb{R}^2$, l'equivalence : $|x-x| \leq y-y \iff (x,y)\, T\, (x,y)$ est vérifiée.

On a, aussi, $\forall\, (x,y), (x',y') \in \mathbb{R}^2$:

$$\begin{array}{rcl} \left\{ \begin{array}{l} (x,y)\, T\, (x',y') \\ (x',y')\, T\, (x,y) \end{array} \right. & \iff & \left\{ \begin{array}{l} |x-x'| \leq y'-y \\ |x'-x| \leq y-y' \end{array} \right. \\ & \iff & 2\,|x-x'| \leq 0 \\ & \iff & |x-x'| = 0 \\ & \iff & x = x' \end{array}$$

et on a

$$\begin{array}{rcl} x = x' & \iff & y-y' \geq 0 \text{ et } y'-y \geq 0 \\ & \iff & y-y' \geq 0 \text{ et } y-y' \geq 0 \\ & \iff & y-y' = 0 \\ & \iff & y = y'. \end{array}$$

D'où, $(x,y) = (x',y')$.

Pour montrer que T est transitive on prend $(x,y), (x',y'), (x'',y'')$ quelconques dans $\mathbb{R}^2$, tels que $(x,y)\, T\, (x',y') \wedge (x',y')\, T\, (x'',y'')$. Alors,

$$\begin{array}{rcl} (x,y)\, T\, (x',y') \wedge (x',y')\, T\, (x'',y'') & \iff & \left\{ \begin{array}{l} |x-x'| \leq y'-y \\ |x'-x''| \leq y''-y' \end{array} \right. \\ & \iff & \left\{ \begin{array}{l} y-y' \leq x-x' \leq y'-y \\ y'-y'' \leq x'-x'' \leq y''-y' \end{array} \right. \\ & \iff & y-y'' \leq x-x'' \leq y''-y \\ & \iff & |x-x'| \leq y''-y \\ & \iff & (x,y)\, T\, (x'',y''). \end{array}$$

Ainsi, T est transitive.

Par conséquent, T est une relation d'ordre.

L'ordre n'est pas total car $(2,1)$ et $(3,0)$ ne sont pas comparables. i.e

$$(2,1)\,T\,(3,0) \iff 1 \leq -1 \text{ (ce qui est absurde).}$$

-Pour $(a,b) \in \mathbb{R}^2$; on a

$$\begin{aligned}
\overset{\cdot}{\overline{(a,b)}} &= \left\{(x,y) \in \mathbb{R}^2 / \,(x,y)\,T\,(a,b)\right\} \\
&= \left\{(x,y) \in \mathbb{R}^2 / \,|x-a| \leq b-y\right\} \\
&= \left\{(x,y) \in \mathbb{R}^2 / \,(x-a)^2 - (b-y)^2 \leq 0\right\},
\end{aligned}$$

alors

$$\begin{array}{rcl}
(x-a)^2 - (b-y)^2 \leq 0 & \iff & (x-y-a+b)\,(x+y-a-b) \leq 0 \\
& \iff & \begin{array}{l}(x-y-a+b) > 0 \wedge (x+y-a-b) \leq 0 \\ \vee\, (x-y-a+b) \leq 0 \wedge (x+y-a-b) > 0\end{array}
\end{array}.$$

Notons :

-D_1 le demi-plan ouvert d'équation $(x-y-a+b) > 0$.

-D_2 le demi-plan fermé d'équation $(x+y-a-b) \leq 0$.

-D_3 le demi-plan fermé d'équation $(x-y-a+b) \leq 0$.

-D_4 le demi-plan ouvert d'équation $(x+y-a-b) > 0$.

Ainsi, $\overset{\cdot}{\overline{(a,b)}} = \{(x,y) \in \mathbb{R}^2 / \,(x,y)\,T\,(a,b)\} = (D_1 \cap D_2) \cup (D_3 \cap D_4)$.

3.5 Exercices supplémentaires

Exercice 3.5.1 *On définit la relation $\triangle$ sur $\mathbb{Z}$ par $x \triangle y \iff x^2 \equiv y^2[5]$.*
-Montrer que $\triangle$ est une relation d'équivalence et déterminer l'ensemble quotient $\mathbb{Z}/\triangle$.

Utiliser la définition suivante :

$$\forall a, b \in \mathbb{Z}; n \in \mathbb{N} - \{0, 1\} : a \equiv b\,[n] \iff \exists k \in \mathbb{Z} : a = kn + b.$$

Exercice 3.5.2 *On definit dans $\mathbb{N}^2$ une relation binaire S par $(x, y)S(x', y')$ si $x+y' = x'+y$. Montrer que S est une relation d'équivalence. Trouver une bijection de l'ensemble-quotient $\mathbb{N}^2/S$ sur $\mathbb{Z}$.*

Exercice 3.5.3 *On définit sur $\mathbb{N}$ la relation division notée "/", par $\forall p \in \mathbb{N}^*, q \in \mathbb{N}$: $q/p \iff (\exists k \in \mathbb{N}, q = kp)$.*
-Montrer que / est une relation d'ordre sur $\mathbb{N}$. Est-ce un ordre total ?
-Est-ce que $(\mathbb{N}, /)$ admet un plus petit et un grand élément. Comparer ces résultats à ce que l'on a dans $(\mathbb{N}, \leq)$.

Exercice 3.5.4 *Soit E une partie non vide de $\mathbb{R}$. On note $\mathbb{R}^E$ l'ensemble des fontions définies sur E à valeurs dans $\mathbb{R}$. Pour tout $f, g \in \mathbb{R}^E$ on pose*

$$f \leq g \iff f(x) \leq g(x),\ \forall x \in E.$$

-Montrer que $\leq$ est une relation d'ordre sur $\mathbb{R}^E$. Est-ce un ordre total ?
-On note $A = \{f, g\} \subset \mathbb{R}^E$. Montrer que $|f|+|g|$ est un majorant de A. Proposer un minorant de A.

Chapitre 4

Structures Algébriques

Les structures algébriques sont essentiellement utilisées dans l'étude des équations algébriques, la géométrie, la théorie des nombres et interviennent aussi en chimie, physique théorique...etc.
Dans ce cours, on présentera des définitions et propriétés liées aux structures algébriques de base : groupes, anneaux et corps.

4.1 Lois de composition internes

Définition 4.1.1 *Soit Ω un ensemble non vide. On appelle loi de composition interne toute application de $\Omega \times \Omega$ à valeurs dans Ω. i.e*

$$\begin{aligned} * : \Omega \times \Omega &\to \Omega \\ (a, b) &\mapsto a * b \end{aligned}$$

Notaion : On note souvent les lois internes par : $*, \circ, \triangle, \top, \perp$...

Exemple 4.1.1 *1.*

2. *L'addition " + " est une loi interne dans $\mathbb{N}$ $(\forall n, m \in \mathbb{N} : n + m \in \mathbb{N})$.*
3. *La division n'est pas interne dans $\mathbb{Z}$ (on a : $-3, 4 \in \mathbb{Z}$, mais $-3 \div 4 \notin \mathbb{Z}$).*
4. *Dans $\mathbb{R}^*$, les lois suivantes sont internes : $+, -, \times, \div$.*
5. *La loi $\circ$ est interne sur $\mathcal{F}(\Omega, \Omega)$ l'ensemble des applications d'un ensemble Ω vers lui même.*
6. *Dans l'ensemble des parties de Ω $(P(\Omega))$, l'union et l'intersection sont internes.*

4.1.1 Commutativité, Associativité, Distributivité

Définition 4.1.2 *Soit Ω un ensemble non vide et $*, \triangle$ deux lois internes.*

1. *$*$ est dite **commutative** si et seulement si :*

$$\forall x, y \in \Omega; x * y = y * x.$$

2. *$*$ est dite **associative** si et seulement si :*

$$\forall x, y, z \in \Omega; (x * y) * z = x * (y * z).$$

3. *$*$ est dite **distributive** sur (ou par rapport à) $\triangle$ si et seulement si :*

$$\forall x, y, z \in \Omega; \begin{cases} x * (y \triangle z) = (x * y) \triangle (x * z) & \text{(distributivité à gauche)} \\ \text{et} \\ (x \triangle y) * z = (x * z) \triangle (y * z) & \text{(distribitivité à droite)} \end{cases}.$$

Exemple 4.1.2

1. *L'addition est commutative dans $\mathbb{R}$.*
2. *La multiplication est associative dans $\mathbb{Q}$.*
3. *Pour $A, B, C \subset \Omega$. L'intersection est distributive par rapport à l'union (loi de Morgan : $A \cap (B \cup C) = (B \cup C) \cap A = (A \cap B) \cup (A \cap C)$).*
4. *La soustraction n'est pas commutative dans $\mathbb{C}$.*

4.1.2 Élément neutre, élément symétrique, stabilité

Définition 4.1.3 *Soit l'ensemble Ω muni d'une loi de composition interne $*$ et $e \in \Omega$.*

*On dit que e est un **neutre à gauche** pour $*$ si $\forall x \in \Omega : e * x = x$.*

*On dit que e est un **neutre à droite** pour $*$ si $\forall x \in \Omega : x * e = x$.*

*On dit que e est un **neutre** pour $*$ si c'est un neutre à gauche et à droite, i.e*

$$\forall x \in \Omega : e * x = x * e = x.$$

Exemple 4.1.3

1. *Dans $\mathbb{R}$, l'élément neutre de l'addition est 0 et celui de la multiplication est 1.*
2. *Dans $P(\Omega)$, l'ensemble vide $\emptyset$ est un neutre pour la loi $\cup$ et pour $\cap$ l'élément neutre est l'ensemble Ω .*

Proposition 4.1.1 *Soit Ω muni d'une loi de composition interne $*$. Si $e \in \Omega$ est un élément neutre pour $*$, alors il est unique.*

Preuve. *Supposons que e et $e\prime$ sont les neutres de $*$ dans Ω. Alors, e et $e\prime$ vérifient : $e\prime = e*e\prime$ (car e' est un neutre) et $e * e\prime = e$ (car e' est un neutre). D'où, $e\prime = e$.* □

Définition 4.1.4 *Soit $(\Omega, *)$ et e le neutre de Ω pour $*$.*

*On appelle un **symétrique gauche** (ou inverse à gauche) de $x \in \Omega$, l'élément $\alpha \in \Omega$ tel que : $\alpha * x = e$.*

*On appelle un **symétrique droit** (ou inverse à droite) de $x \in \Omega$, l'élément $\alpha \in \Omega$ tel que : $x * \alpha = e$.*

On dit que $\alpha \in \Omega$ est le symétrique (ou l'inverse) de $x \in \Omega$ si et seulement si

$$\alpha * x = x * \alpha = e.$$

Exemple 4.1.4

1. *Dans $(\mathbb{R}^*, \cdot)$, l'inverse de x est $\frac{1}{x}$ noté x^{-1}.*
2. *Dans $(\mathbb{Z}, +)$, l'inverse de y est $-y$ (opposé de y).*
3. *Les élément de l'ensemble $\mathbb{N}$ n'admettent pas des symétriques pour l'addition.*

Remarque 4.1.1 *Un élément qui admet un inverse est dit inversible ou symétrisable.*

Si α est le symétrique de x, alors on dit aussi que x est le symétrique de α.

Proposition 4.1.2 *Soit Ω muni de la loi interne $*$ associative et $e \in \Omega$ l'élément neutre. Si l'inverse de $x \in \Omega$ existe, alors il est unique.*

Preuve. *Supposons que $\alpha, \alpha' \in \Omega$ sont les inverse de x pour la loi $*$. Alors, on a :*

$$\begin{aligned} \alpha' &= \alpha' * e \\ &= \alpha' * (x * \alpha) \\ &= (\alpha' * x) * \alpha \\ &= e * \alpha \\ &= \alpha. \end{aligned}$$

□

Proposition 4.1.3 *Soient Ω un ensemble muni de la loi interne $*$ associative et admettant un neutre e et $x, y \in \Omega$. Si x et y sont symétrisables (inversibles) pour $*$ alors $(x * y)$ l'est aussi et $(x * y)^{-1} = y^{-1} * x^{-1}$.*

Preuve. *On a $x^{-1} * x = e$ et $y^{-1} * y = e$, alors*

$$\begin{aligned}\left(y^{-1} * x^{-1}\right) * (x * y) &= y^{-1} * \left(x^{-1} * x\right) * y \\ &= y^{-1} * e * y \\ &= y^{-1} * y \\ &= e.\end{aligned}$$

De la même manière, on montre que $(x * y) * (y^{-1} * x^{-1}) = e$.

Ainsi, $(y^{-1} * x^{-1})$ est le symétrique de $(x * y)$. □

Définition 4.1.5 *Soit $(\Omega, *)$ et A un sous ensemble de Ω. A est **stable** pour $*$ si et seulement si $\forall (x, y) \in A^2 : x * y \in A$. De plus, $*$ est dite loi induite sur A.*

4.2 Morphisme, Endomorphisme, Isomorphisme, Automorphisme

Définition 4.2.1 *Soient $(\Omega, *), (F, \triangle)$ deux ensembles munis de lois internes et une application $f : \Omega \to F$. On dit que :*

*f est un **morphisme** de Ω dans F, si $\forall (x, y) \in \Omega^2 : f(x * y) = f(x) \triangle f(y)$.*

*f est un **endomorphisme** de Ω, si f est un morphisme de Ω dans Ω.*

*f est un **isomorphisme** de Ω dans F, si f est un morphisme bijectif.*

*f est un **automorphisme** de Ω, si f est un endomorphisme bijectif.*

Exemple 4.2.1

1. *L'application $f : (\mathbb{R}, +) \to (\mathbb{R}^*, \times)$ telle que $f(x) = e^x$ est un morphisme, on a*

$$\forall x, y \in \mathbb{R} : f(x + y) = e^{x+y} = e^x \times e^y = f(x) \times f(y).$$

2. *L'application $g : \left(\mathbb{R}_+^*, \times\right) \to (\mathbb{R}, +)$ telle que $g(x) = \ln x$ est un isomorphisme, car on a*

$$\forall x, y \in \mathbb{R} : g(x + y) = \ln(xy) = \ln x + \ln y = g(x) + g(y).$$

De plus, g est bijective.

3. *L'application* $id : (\Omega, *) \to (\Omega, *)$ *est un automorphisme.*

Proposition 4.2.1 a) *Si* $f : (\Omega, *) \to (F, \triangle)$ *et* $g : (F, \triangle) \to (\ni, \nabla)$ *sont des morphismes, alors* $g \circ f : (\Omega, *) \to (\ni, \nabla)$ *est un morphisme.*

b) *Si* $f : (\Omega, *) \to (F, \triangle)$ *est un isomorphisme, alors* $f^{-1} : (F, \triangle) \to (\Omega, *)$ *est un isomorphime.*

4.3 Groupes, Anneaux, Corps

4.3.1 Structure de groupe

Définition 4.3.1 *Soit* G *un ensemble muni d'une loi interne* $*$*. On dit que* $(G, *)$ *est un groupe si et seulement si :*

i. La loi $*$ *est associative,*

ii. G *admet un élément neutre pour* $*$*,*

iii. $\forall x \in G, \exists x^{-1} \in G$ *pour* $*$*.*

Remarque 4.3.1 *1.*

2. *Si* G *est un groupe et* $*$ *est commutative, alors* $(G, *)$ *est dit groupe commutatif ou Abélien.*

3. *Si* G *est un groupe, alors* $G \neq \emptyset$ *(car* $e \in G$*).*

4. $(\{e\}, *)$ *est un groupe .*

Exemple 4.3.1 *1.* $(\mathbb{Q}, +)$ *est un groupe commutatif.*

2. $(\mathbb{Z}, \times)$ *n'est pas un groupe (le symétrique de -5 est* $\frac{-1}{5} \notin \mathbb{Z}$*).*

Sous-groupe

Définition 4.3.2 *On dit que* $(S, *)$ *est un* ***sous-groupe*** *du groupe* $(G, *)$ *tout sous ensemble* S *de* G *tel que :*

- $\forall x, y \in S; x * y \in S;$ *(stabilité)*

- *Le neutre* $e \in S$*;*

- $\forall x \in S, \exists x^{-1} \in S$*.*

Exemple 4.3.2 *1.* $(\{0\},+)$ *est un sous-groupe de* $(\mathbb{Q},+)$,

2. $(\{1\},\times)$ *sous-groupe de* $(\mathbb{R},\times)$.

3. $(3\mathbb{Z},+)$ *est un sous-groupe de* $(\mathbb{Z},+)$.

Proposition 4.3.1 $(S,*)$ *est un sous-groupe de* $(G,*)$ *si et seulement si* $S \neq \emptyset$ *et* $\forall x,y \in S; x * y^{-1} \in S$.

Preuve.

a) *Si* S *est un sous-groupe alors,* $e \in S$. *D'où,* $S \neq \emptyset$. *On a aussi,* $x,y \in S$ *implique que* y^{-1} *et* $x * y^{-1} \in S$ *par stabilité.*

b) *Réciproquement :*

-Si $S \neq \emptyset$ *, alors* $\exists \alpha \in S$ *tel que* $\alpha * \alpha^{-1} \in S$. *D'où,* $e \in S$.

- Pour tout $x \in S$, *on a* $e * x^{-1} = x^{-1} \in S$.

- S *est stable pour* $*$ *car* $\forall x,y \in S$, *on a* $x * (y^{-1})^{-1} = x * y \in S$.

Donc, S *est un sous-groupe.*

□

Théorème 4.3.1 *Soient* $(G,*)$, $J \subset \mathbb{N}$. *Si* $(S_i)_{i\in J}$ *est une famille de sous-groupes de* G, *alors* $\bigcap_{i\in J} S_i$ *est un sous-groupe de* G.

Preuve. *1) Comme* $(S_i)_{i\in J}$ *sont des sous-groupes alors* $\forall i \in J : e \in S_i$ *ce qui implique que* $\bigcap_{i\in J} S_i \neq \emptyset$.

2) Soient $x,y \in \bigcap_{i\in J} S_i$, *ainsi*

$$\forall i \in J : x,y \in S_i \implies \forall i \in J : x * y \in S_i \text{ (par stabilité)}$$
$$\implies x * y \in \bigcap_{i\in J} S_i \quad .$$

3) Soit $x \in \bigcap_{i\in J} S_i$. *Alors, on a* $\forall i \in J : x \in S_i$, *d'où* $\forall i \in J : x^{-1} \in S_i$ *(car* S_i *sous-groupe).*

Par conséquent, $x^{-1} \in \bigcap_{i\in J} S_i$. □

Remarque 4.3.2 *Le théorème précédent ne s'applique pas pour l'union des sous-groupes. En effet, supposons que $G = S \cup S'$ avec S et S' des sous-groupes de G. Ainsi, puisque $S \subset G$, alors $\exists a \in G, a \notin S$ (i.e $a \in S'$) . De plus, $S' \subset G$, alors $\exists b \in G, b \notin S'$ (i.e $b \in S$). Comme*

$$\begin{aligned} a, b \quad &\in \quad G \Longrightarrow a * b \in G \\ &\Longrightarrow \quad a * b \in S \cup S' \\ &\Longrightarrow \quad a * b \in S \text{ ou } a * b \in S'. \end{aligned}$$

Proposition 4.3.2 ***Remarque 4.3.3*** *Si $a * b \in S$, alors $\exists b^{-1} \in S$ et par stabilité on peut écrire $(a * b) * b^{-1} \in S$. Comme $*$ est associative, on obtient $a * (b * b^{-1}) = a \in S$ (contradiction avec $a \notin S$).*
De la même façons, on a $b \in S'$ ce qui est absurde car $b \notin S'$.
Donc, l'hypothèse est fausse.

Exemple 4.3.3 *L'union des sous-groupes $(3\mathbb{Z}, +), (4\mathbb{Z}, +)$ n'est pas un sous-groupe de $\mathbb{Z}$. En effet, en prenant les éléments $6 \in 3\mathbb{Z}$ et $8 \in 4\mathbb{Z}$, la somme $(6 + 8 = 14)$ n'est ni un multiple de 3 ni de 4 (c.à.d $14 \notin (3\mathbb{Z} \cup 4\mathbb{Z})$).*

Morphismes de groupes

Définition 4.3.3 *Soient deux groupes $(G, *)$ et $(G', \triangle)$.*
*- On appelle **homomorphisme** (ou morphisme de groupe) toute application $\phi : G \to G'$.*
*- Si $G = G', \phi$ est dit **endomorphisme de groupe.***
*- Si $\phi : G \to G'$ est bijective, alors on dit que ϕ est un **Isomorphisme de groupe**.*
*- Si $G = G'$ et ϕ est bijective, alors ϕ est appellé **automorphisme de groupe.***

Proposition 4.3.3 *Tout morphisme de groupes $\phi : (G, *) \to (G', \triangle)$ vérifie les propriétés suivantes :*

1. *$\phi(e) = e'$. (e, e' les neutres de G, G' resp.)*
2. *$\forall x \in G : \phi(x^{-1}) = (\phi(x))^{-1}$.*

Preuve. 1) On a $\phi(e) = \phi(e * e) = \phi(e) \triangle \phi(e)$. D'autre part, on a $\phi(e) \triangle e' = \phi(e)$. D'où, le résultat.

2) En utilisant la propriété (1), on peut écrire :

$$\begin{aligned} e' &= \phi(e) \Longrightarrow e' = \phi\left(x * x^{-1}\right) \\ &\Longrightarrow e' = \phi(x) \triangle \phi\left(x^{-1}\right); \end{aligned}$$

Et

$$\begin{aligned} e' &= \phi(e) \Longrightarrow e' = \phi\left(x^{-1} * x\right) \\ &\Longrightarrow e' = \phi\left(x^{-1}\right) \triangle \phi(x). \end{aligned}$$

Ainsi, $\phi(x^{-1}) \triangle \phi(x) = \phi(x) \triangle \phi(x^{-1}) = e'$.

Donc, $\phi(x^{-1})$ est le symétrique de $\phi(x)$. □

Noyeau et image d'un morphisme de groupe

Définition 4.3.4 *Soit $\phi : G \to G'$ un homomorphisme, e et e' les neutres de G et G'.*

*- Le **noyau** de ϕ est la partie de G des antécédents de e', noté* $\ker \phi$ *et donné par :*

$$\ker \phi = \{x \in G, \phi(x) = e'\} = \phi^{-1}(\{e'\}).$$

*- L'**image** de ϕ est le sous ensemble de G', noté par* $\operatorname{Im} \phi$ *tel que*

$$\operatorname{Im} \phi = \{y \in G', \exists x \in G; \phi(x) = y\} = \phi(G).$$

Remarque 4.3.4 ker *est l'abréviation de kernel (noyau en anglais).*

Proposition 4.3.4 *Soit ϕ un homomorphisme du groupe G dans le groupe G'*

1) $\ker \phi$ *est un sous-groupe de G.*

2) $\operatorname{Im} \phi$ *est un sous-groupe de G'.*

3) ϕ injectif $\Longleftrightarrow \ker \phi = \{e\}$.

4) ϕ surjectif $\Longleftrightarrow \operatorname{Im} \phi = G'$.

Preuve. "En exercice". □

4.3.2 Congruence dans $\mathbb{Z}$

Définition 4.3.5 *Soient $n \in \mathbb{N}^* \setminus \{1\}$ et $a, b \in \mathbb{Z}$. On dit que a est congru à b modulo n et on écrit $a \equiv b\,[n]$ si $a - b \in n\mathbb{Z}$.*

Remarque 4.3.5 *L'expression $a - b \in n\mathbb{Z}$ équivaut à dire que $a - b$ est un multiple de n, ou encore b est le reste de la division de a sur n $(\exists k \in \mathbb{Z} : a = kn + b)$.*

Exemple 4.3.4 $26 \equiv 2\,[3]$ *car* $26 = 8 \cdot 3 + 2$ *ou* $26 - 2 = 24 \in 3\mathbb{Z}$.

Proposition 4.3.5 *La congruence est une relation d'équivalence.*

Preuve. *Il est facile de vérifier la réflexivité, la symétrie et la transitivité.* □

Proposition 4.3.6 *Soient $n \in \mathbb{N}^* \setminus \{1\}$ et $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b\,[n], c \equiv d\,[n]$. On a*

1. $a + c \equiv b + d\,[n]$.
2. $-a \equiv -b\,[n]$.
3. $ac \equiv bd\,[n]$.
4. $\forall r \in \mathbb{N}, a^r \equiv b^r\,[n]$.

Définition 4.3.6 *L'ensemble des classes d'équivalence pour la relation de congruence modulo n noté $\mathbb{Z}/_{n\mathbb{Z}}$ (appelé aussi ensemble des classes de congruence modulo n) et donné par*

$$\mathbb{Z}/_{n\mathbb{Z}} = \left\{\dot{0}, \dot{1}, \dot{2}, ..., \dot{n-1}\right\}$$

- On définit les lois internes suivantes sur $\mathbb{Z}/_{n\mathbb{Z}}$:

La somme notée $\dot{+}$

$$\forall \dot{a}, \dot{b} \in \mathbb{Z}/_{n\mathbb{Z}} : \ \dot{a} \dot{+} \dot{b} = \widehat{a + b}$$

et la multiplication notée $\dot{\cdot}$

$$\forall \dot{a}, \dot{b} \in \mathbb{Z}/_{n\mathbb{Z}} : \ \dot{a} \dot{\cdot} \dot{b} = \widehat{a \cdot b}.$$

Exemple 4.3.5 *Pour* $n = 5$, $\mathbb{Z}/_{5\mathbb{Z}} = \left\{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}\right\}$.

$\dot{+}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{4}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$

Table d'addition

$\dot{\cdot}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{1}$	$\dot{3}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{1}$	$\dot{4}$	$\dot{2}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

Table de multiplication

Proposition 4.3.7 *Dans* $\mathbb{Z}/_{n\mathbb{Z}}$:

1. *Les lois* $\dot{+}$ *et* $\dot{\cdot}$ *sont commutatives et associatives.*
2. *La loi* $\dot{+}$ *(resp.* $\dot{\cdot}$ *) admet l'élément neutre* $\dot{0}$ *(resp.* $\dot{1}$*).*
3. *L'addition* $\dot{+}$ *est distributive par rapport à la multiplication* $\dot{\cdot}$.

Remarque 4.3.6 *L'ensemble* $\mathbb{Z}/_{n\mathbb{Z}}$ *muni de l'addition est un groupe abélien.*
Pour tout $a \in \mathbb{Z}$, *le symétrique de* $\dot{a}$ *pour* $\dot{+}$ *est noté* $\dot{-a}$ *et pour* $\dot{\cdot}$ *on note* $\left(\dot{a}\right)^{-1}$.

4.3.3 Structure d'anneaux

Dans ce qui suit, on utilise les lois de composition internes $+$ et $\cdot$ (appelée resp. addition et multiplication), dont les éléments neutres sont notés resp. 0 et 1 et les symétriques d'un élément x sont : pour l'addition $-x$ et pour la multiplication x^{-1}.

Définition 4.3.7 *1)Un ensemble* A *muni de* $+$ *et* $\cdot$ *est appelé* ***anneau*** *si et seulement si*

i) $(A, +)$ *est un groupe abélien,*

ii) $\cdot$ *est associative,*

iii) $\cdot$ *est distributive par rapport à* $+$,

iv) $\cdot$ *admet un neutre (noté1).*

2) Si de plus $\cdot$ *est commutative alors* $(A, +, \cdot)$ *est dit anneau commutatif.*

Exemple 4.3.6 *1. Les ensembles* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *munis des opérations usuelles forment des anneaux.*

2. L'ensemble $\left(\mathbb{Z}/_{4\mathbb{Z}}, \dot{+}, \dot{\cdot}\right)$ *des classes modulo* 4 *est un anneau commutatif.*

Remarque 4.3.7 *1. Pour tout* $a \in A : a \cdot 0 = 0 \cdot a$ *et* $a \cdot (-1) = (-1) \cdot a = -a$.

2. Pour tout $a, b \in A$, *on a* $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$ *et* $(-a) \cdot (-b) = a \cdot b$.

Sous-anneau

Définition 4.3.8 *Soient l'anneau* $(A, +, \cdot)$, X *une partie de* A.
$(X, +, \cdot)$ *est un sous-anneau de* A *si et seulement si*

$$\begin{aligned} &a)\ (X, +)\ \textit{est un sous-groupe de}\ (A, +)\ , \\ &b)\ \forall (x, y) \in X^2 : \quad x \cdot y \in X \quad \textit{(stabilité de } \cdot\textit{)}, \\ &c)\ \ 1_A \in X. \end{aligned}$$

Exemple 4.3.7 *1.* $(\mathbb{Z}, +, \cdot)$ *est un sous-anneau de* $(\mathbb{C}, +, \cdot)$.

2. $(3\mathbb{Q}, +, \cdot)$ *n'est pas un sous-anneau de* $(\mathbb{Q}, +, \cdot)$ $(1_{\mathbb{Q}} \notin 3\mathbb{Q})$.

Proposition 4.3.8 *Une partie* X *d'un anneau* $(A, +, \cdot)$ *est dite sous-anneau si et seulement si*

$$\begin{aligned} &i)\ \forall (x, y) \in X^2 : \quad x - y \in X \quad , \\ &ii)\ \forall (x, y) \in X^2 : \quad x \cdot y \in X \quad \textit{(stabilité de } \cdot\textit{)}, \\ &iii)\ 1_A \in X. \end{aligned}$$

Preuve. *1) Les propriétés ii) et iii) sont vérifiées. De plus, si* X *est un sous anneau de* A *alors* $(X, +)$ *est un sous-groupe de*$(A, +)$. *D'où, la stabilité de l'addition.*
2) Supposons que i),ii) et iii) sont vérifiées et Montrons que : $(X, +)$ *est un sous-groupe de* $(A, +)$.
On a $1_A \in X$ *. En appliquant i), on obtient* $1_A - 1_A \in X$. *D'où,* $0_A \in X$.
Puis, pour tout $x \in X$ *on a* $0_A - x \in X$; *ce qui implique que* $-x \in X$. *Ainsi, tout élément de* X *est symétrisable.*
Soient $x, y \in X$. *De ce qui précède, on a* $-y \in X$. *Alors, grâce à i) on peut écrire :* $x - (-y) = x + y \in X$. *Donc,* $+$ *est stable.*
Par conséquent, $(X, +)$ *est un sous-groupe de*$(A, +)$.

Proposition 4.3.9 *Soit $(X_i)_{i\in J}$ une famille de sous-anneaux d'un anneau A, $\bigcap_{i\in J} X_i$ est un sous-anneau de A.*

□

L'anneau $\mathbb{Z}/_{n\mathbb{Z}}$

Proposition 4.3.10 *1) Soit l'entier $n > 1$. L'ensemble $\left(\mathbb{Z}/_{n\mathbb{Z}}, \dot{+}, \dot{\cdot}\right)$ est un anneau commutatif.*
2) L'élément $\dot{a}$ de l'anneau $\left(\mathbb{Z}/_{n\mathbb{Z}}, \dot{+}, \dot{\cdot}\right)$ est inversible si et seulement si a et n sont premiers entre eux ($i.e: \ a \wedge n = 1$) .

Pour démontrer la propriété (2), on utilise le théorème suivant dit de Bezout.

Théorème 4.3.2 *Soit $p \in \mathbb{N}^*$, les entiers relatifs non nuls $a_1, a_2, ..., a_p$ sont premiers entre eux si et seulement s'il existe $(\lambda_1, \lambda_2, ..., \lambda_p) \in \mathbb{Z}^p$ tels que $\sum_{s=1}^{p} a_s\lambda_s = 1$.*

Preuve. Soit $\dot{a} \in \mathbb{Z}/_{n\mathbb{Z}}$ inversible, i.e

$$\begin{aligned} \exists \dot{b} \quad \in \quad & \mathbb{Z}/_{n\mathbb{Z}} : \ \dot{a}\dot{b} = \dot{1} \iff \exists b \in \mathbb{Z} : a \cdot b \equiv 1\,[n] \\ \iff \quad & \exists\,(b,k) \in \mathbb{Z}^2 : a \cdot b = k \cdot n + 1 \\ \iff \quad & \exists\,(b,k) \in \mathbb{Z}^2 : a \cdot b - k \cdot n = 1 \end{aligned}$$

D'apèrs le théorème de Bezout, $a \wedge n = 1$. □

Morphisme d'anneaux

Dans la définition suivante $(A, +, \cdot)$ et $(A', *, \triangle)$ représentent des anneaux.

Définition 4.3.9 *1. On appelle **morphisme d'anneaux** toute application $\psi : A \to A'$ vérifiant*

$$\begin{aligned} i.\forall\,(x,y) \quad & \in \quad A^2 : \psi(x+y) = \psi(x) * \psi(x); \\ ii.\forall\,(x,y) \quad & \in \quad A^2 : \psi(x \cdot y) = \psi(x) \triangle \psi(x); \\ iii. \ \psi(1_A) \quad & = \quad 1_{A'}. \end{aligned}$$

2. *On appelle* ***endomorphisme d'anneaux*** *tout morphisme* $\psi : A \to A$.
3. *On appelle* ***isomorphisme d'anneaux*** *tout morphisme bijectif* $\psi : A \to A'$.
4. *On appelle* ***automorphisme d'anneaux*** *tout morphisme bijectif* ψ *de l'anneau* A.

Exemple 4.3.8 *L'application* $\psi : \mathbb{Z} \to \mathbb{Z}/_{p\mathbb{Z}}$ *avec* $(p \in \mathbb{N})$ *qui associe à un entier relatif* x *sa classe d'équivalence, i.e* $\psi(x) = \dot{x}$, *est un homomorphisme.*

Remarque 4.3.8
1. *La composée de deux morphismes d'anneaux est un morphisme d'anneaux.*
2. *La réciproque d'un isomorphisme d'anneaux est un isomorphisme d'anneaux.*
3. *L'application identité* $(id_A : A \to A)$ *est un automorphisme d'anneaux.*

Diviseurs de Zéro

Définition 4.3.10 *Soit l'anneau* $(A, +, \cdot)$ *et* d *un élément de* A.

1. $d \neq 0$ *est un diviseur de zéro à gauche (resp. à droite) dans l'anneau* A *s'il existe* $u \in A^*$ *tel que* $d \cdot u = 0$ *(resp.* $u \cdot d = 0$ *).*
2. $d \neq 0$ *est un diviseur de zéro à dans l'anneau* A *si et seulement si* d *est un diviseur à gauche et à droite dans* A.

Autrement dit, un élément non nul est dit diviseur de zéro si son produit avec un autre élément non nul est égal à zéro.

Exemple 4.3.9
1. *L'anneau* $(\mathbb{Q}, +, \cdot)$ *n'admet aucun diviseur de zéro.*
2. *Dans* $(\mathbb{Z}/_{8\mathbb{Z}}, +, \cdot)$, *on a* $\dot{4} \cdot \dot{6} = \dot{0}$, *mais* $(\mathbb{Z}/_{7\mathbb{Z}}, +, \cdot)$ *ne possède aucun diviseur de zéro.*

Remarque 4.3.9 *Si* $(A, +, \cdot)$ *est un anneau commutatif, alors tout diviseur à droite est un diviseur à gauche.*

Anneau intègre

Définition 4.3.11 *Un anneau commutatif et non nul* $(A, +, \cdot)$ *est dit intègre s'il n'admet aucun diviseur de zéro.*

Remarque 4.3.10 *Dans un anneau intègre, si on a* $d \cdot u = 0$, *alors* $d = 0$ *ou* $u = 0$.

Exemple 4.3.10 *1.* $(\mathbb{Z}/_{8\mathbb{Z}}, +, \cdot)$ *n'est pas intègre* $\left(car\ \dot{4} \dot{\cdot} \dot{6} = \dot{0}\right)$.

2. $(\mathbb{R}, +, \cdot)$ *est intègre.*

Définition 4.3.12 *Soit* α *un élément de l'anneau* $(A, +, \cdot)$. *S'il existe* $n \in \mathbb{N}^*$ *tel que* $\alpha^n = 0$, *alors* α *est dit* ***nilpotent.***
Le plus petit $n \in \mathbb{N}^*$ *tel que* $\alpha^n = 0$ *est appelé* ***indice*** *(ou ordre)* ***de nilpotence.***

Exemple 4.3.11 *Dans l'exemple précédent* $(\mathbb{Z}/_{8\mathbb{Z}}, +, \cdot)$, *on a* $\left(\dot{2}\right)^3 = 0$. *Donc,* $\dot{2}$ *est nilpotent d'ordre* 3.

Idéaux

Définition 4.3.13 *Un idéal bilatère* I *dans* $(A, +, \cdot)$ *est un groupe additif de* $(A, +)$ *vérifiant :* $\forall\, (i, a) \in I \times A : a \cdot i \in I$ *et* $i \cdot a \in I$.

Exemple 4.3.12 *- Pour* $n \in \mathbb{N}^*, n\mathbb{Z}$ *est un idéal de* $\mathbb{Z}$.

Remarque 4.3.11 *1. Si on a* $\forall\, (i, a) \in I \times A : a \cdot i \in I$, *alors* I *est un idéal à gauche (Si on a* $\forall\, (i, a) \in I \times A : i \cdot a \in I$, *alors* I *est un idéal à droite).*

2. L'idéal contenant 1_A *est* A.

3. Le noyau d'un morphisme d'anneau $\psi : A \to A'$, $\ker \psi = \{x \in A : \psi(x) = 0\}$ *est un idéal de* A.

Proposition 4.3.11 *-L'intersection de deux idéaux* I *et* I' *de* A *est un idéal de* A.
-La somme de deux idéaux donnée par : $I + I' = \{(i + i') \in A : i \in I, i' \in I'\}$ *est un idéal de* A.
-Le produit $II' = \left\{ \sum_{finie} i_r i'_r \in A : i_r \in I, i'_r \in I' \right\}$ *est un idéal de* A.

4.3.4 Structure de Corps

Définition 4.3.14 *Soit $(K,+,\cdot)$ un anneau. Si tout élément non nul de K est symétrisable pour $\cdot$ et $1_K \neq 0_K$, alors $(K,+,\cdot)$ est appelé corps.*
$(K,+,\cdot)$ est un corps commutatif si $\cdot$ est commutative.

Exemple 4.3.13 *$(\mathbb{R},+,\cdot),(\mathbb{C},+,\cdot)$ sont des corps commutatifs.*
L'anneau commutatif $(\mathbb{Z},+,\cdot)$ n'est pas un corps.

Proposition 4.3.12 *Soit $n \in \mathbb{N}^*$, les propriétés suivantes sont équivalentes :*
i) n premier ;
ii) $\mathbb{Z}/_{n\mathbb{Z}}$ est un corps commutatif ;
iii) $\mathbb{Z}/_{n\mathbb{Z}}$ est un annneau intègre.

Sous-corps

Définition 4.3.15 *On appelle sous-coprs de $(K,+,\cdot)$ toute partie non vide de K' telle que $(K',+,\cdot)$ soit un sous-anneau et tout élément non nul de K' est inversible.*

Exemple 4.3.14 *1. $K' = \{\alpha + i\beta; \alpha,\beta \in \mathbb{Q}\}$ est un sous corps de $\mathbb{C}$.*

Proposition 4.3.13 *Soit K' une partie non vide de K. On dit que $(K',+,\cdot)$ est un sous-corps de K si et seulement si*

$$\begin{array}{ll} i. & \forall x,y \in K' : x-y \in K'; \\ ii. & \forall x,y \in K' : x \cdot y \in K'; \\ iii. & 1_K \in K'; \\ iv. & \forall x \in (K')^*, \exists x^{-1} \in K'. \end{array}$$

4.4 Exercices corrigés

Exercice 4.4.1 *Soit la loi de composition interne $*$ définie sur $A =]-1,1[$ par*

$$x * y = \frac{x+y}{1+xy}$$

1) Montrer que $(A,*)$ est un groupe abélien.

2) Soit $B =]0,1[$, $(B,*)$ est-il un sous-groupe de A?

Solution

1) Montrons que $(A,*)$ est un groupe abélien :

Pour tout $x,y,z \in A$ la loi $*$ est commutative :

$$y * x = \frac{y+x}{1+yx} = \frac{x+y}{1+xy} = x * y.$$

Associative car $(x*y)*z = x*(y*z)$, en effet :

$$\begin{aligned}(x*y)*z &= \frac{x+y}{1+xy} * z \\ &= \frac{\dfrac{x+y}{1+xy}+z}{1+\left(\dfrac{x+y}{1+xy}\right)z} \\ &= \frac{x+y+z+xyz}{1+xy+xz+yz}\end{aligned}$$

et

$$\begin{aligned}x*(y*z) &= x * \frac{y+z}{1+yz} \\ &= \frac{x+\dfrac{y+z}{1+yz}}{1+x\left(\dfrac{y+z}{1+yz}\right)} \\ &= \frac{x+y+z+xyz}{1+xy+xz+yz}\end{aligned}$$

Supposons que $*$ admet un neutre e, alors $\forall x \in A$

$$\begin{aligned} x * e &= x \Longrightarrow \frac{x+e}{1+xe} = x \\ &\Longrightarrow x + e = x\left(1 + xe\right) \\ &\Longrightarrow x^2 e - e = 0 \\ &\Longrightarrow \left(x^2 - 1\right) e = 0 \\ &\Longrightarrow e = 0. \end{aligned}$$

Supposons que x' est le symétrique de x, alors

$$\begin{aligned} x * x' &= e \Longrightarrow \frac{x+x'}{1+xx'} = 0 \\ &\Longrightarrow x' = -x. \end{aligned}$$

Donc, $(A, *)$ est un groupe abélien.

2) B n'est pas un sous groupe de A car $0 \notin B$.

Exercice 4.4.2 *Soit ϕ un homomorphisme du groupe $(G, *)$ dans le groupe $(G', \triangle)$. Montrer que :*

1) $\ker \phi$ *et* $\operatorname{Im} \phi$ *sont deux sous-groupes de G et G' respectivement.*

2) ϕ injectif $\Longleftrightarrow \ker \phi = \{e\}$.

Solution

1) Soient e, e' les neutres de G et $G\prime$.Vérifions les critères d'un sous groupe. Pour $\ker \phi$ sous-groupe de G, on a :

i) On sait que $\phi(e) = e'$ alors $e \in \ker \phi$. D'où, $\ker \phi \neq \emptyset$.

ii)Pour tout $a, b \in \ker \phi$, on a

$$\begin{aligned} \phi(a * b^{-1}) &= \phi(a) \triangle \phi(b^{-1}) \Longrightarrow \phi(a * b^{-1}) = \phi(a) \triangle \left[\phi(b)\right]^{-1} \\ &\Longrightarrow \phi(a * b^{-1}) = e' \triangle \left(e'\right)^{-1} \\ &\Longrightarrow \phi(a * b^{-1}) = e' \\ &\Longrightarrow (a * b^{-1}) \in \ker \phi. \end{aligned}$$

Similairement, pour $\operatorname{Im} \phi$ sous-groupe de G' on remarque que :

i) $\phi(e) = e'$ alors $e' \in \operatorname{Im}\phi$. Donc, $\operatorname{Im}\phi \neq \emptyset$.

ii) Pour tout $y, y' \in G'$ admettant $x, x' \in G$ comme antécédents , on peut écrire

$$\begin{aligned} y\triangle (y')^{-1} &= \phi(x)\triangle [\phi(y)]^{-1} \implies y\triangle (y')^{-1} = \phi(x)\triangle \left[\phi(y^{-1})\right] \\ &\implies y\triangle (y')^{-1} = \phi(x * (y^{-1})) \\ &\implies y\triangle (y')^{-1} \in \operatorname{Im}\phi. \end{aligned}$$

D'où le résultat.

3)Montrons que ϕ injectif $\iff \ker\phi = \{e\}$

i) Supposons que ϕ injectif, alors $\forall a \in \ker\phi$

$$\phi(a) = \phi(e) \implies a = e \implies \ker\phi = \{e\}.$$

ii) Si $\ker\phi = \{e\}$, alors soient $a, b \in G$ tels que:

$$\begin{aligned} \phi(a) &= \phi(b) \implies \phi(a)\triangle (\phi(b))^{-1} = e' \\ &\implies \phi(a)\triangle\phi(b^{-1}) = e' \\ &\implies \phi(a * b^{-1}) = e' \\ &\implies a * b^{-1} \in \ker\phi \\ &\implies a * b^{-1} = e \quad (\text{car } \ker\phi = \{e\}) \\ &\implies b = a. \end{aligned}$$

Donc, ϕ est surjective.

En combinant i) et ii), on obtient l'equivalence.

Exercice 4.4.3 *Soit la loi interne $\triangle$ définie sur $E = \mathbb{R}\setminus\{-3\}$ par*

$$a\triangle b = ab + 3(a + b) + 6.$$

1) Montrer que $(E, \triangle)$ est un groupe abélien.

2) Montrer que $F =]-3, +\infty[$ est un sous-groupe de E.

3) Soit l'application $f : (E, \triangle) \to (\mathbb{R}^*, \cdot)$, définie par

$$f(a) = \lambda a + 3.$$

i) Déterminer λ pour que f soit un morphisme de groupes.

ii) Déterminer $\ker f$.

iii) Es ce que f est un isomorphisme ? Si oui, déterminer f^{-1}.

Solution

1) Montrons que $(E, \triangle)$ est un groupe abélien.

-Pour tout $a, b \in \mathbb{R}\setminus\{-3\}$, on a

$$\begin{aligned} a\triangle b &= ab + 3(a+b) + 6 \\ &= ba + 3(b+a) + 6 \\ &= b\triangle a. \end{aligned}$$

D'où, $\triangle$ est commutative.

-Pour tout $a, b, c \in \mathbb{R}\setminus\{-3\}$, on a

$$\begin{aligned} (a\triangle b)\triangle c &= [ab + 3(a+b) + 6]\triangle c \\ &= [abc + 3(a+b)c + 6c] + 3([ab + 3(a+b) + 6] + c) + 6 \\ &= abc + 3(a+b)c + 6c + 3ab + 9(a+b) + 18 + 3c + 6 \\ &= abc + 3(a+b)(c+3) + 3ab + 9c + 24 \qquad (1) \end{aligned}$$

et

$$\begin{aligned} a\triangle (b\triangle c) &= a\triangle [bc + 3(b+c) + 6] \\ &= (a[bc + 3(b+c) + 6]) + 3(a + [bc + 3(b+c) + 6]) + 6 \\ &= abc + 3ab + 3ac + 6a + 3a + 3bc + 9(b+c) + 18 + 6 \\ &= abc + 3(a+b)(c+3) + 3ab + 9c + 24. \qquad (2) \end{aligned}$$

De (1) et (2), $\triangle$ est associative.

-Cherchons un neutre e pour $\triangle$. Soit $a \in E$, on a

$$\begin{aligned} a\triangle e = a &\Longrightarrow ae + 3(a+e) + 6 = a \\ &\Longrightarrow ae + 2a + 3e + 6 = 0 \\ &\Longrightarrow e(a+3) + 2(a+3) = 0 \\ &\Longrightarrow (a+3)(e+2) = 0. \\ &\Longrightarrow e = -2 \quad (\text{car } a \neq -3). \end{aligned}$$

-Tout $a \in E$ est symétrisable. En effet,

$$\begin{aligned} a\triangle a' = e &\Longrightarrow aa' + 3(a+a') + 6 = -2 \\ &\Longrightarrow aa' + 3a + 3a' = -8 \\ &\Longrightarrow (a+3)a' = -3a - 8 \\ &\Longrightarrow a' = \frac{-3a-8}{a+3} \end{aligned}$$

Par conséquent, $(E, \triangle)$ est un groupe commutatif.

2) On a $F \subset E$. Pour tout $a, b \in]-3, +\infty[$; on a

$$\begin{aligned} a\triangle b &= ab + 3(a+b) + 6 \\ &= (a+3)(b+3) - 3 > -3. \end{aligned}$$

D'où, $a\triangle b \in F$. Aussi, $e = -2 \in F$. De plus, $a^{-1} = \frac{-3a-8}{a+3} \in F$ car $a+3 > 0$ et $\frac{-3a-8}{a+3} > \frac{-3a-9}{a+3} > -3$.

De ce qui précède, on déduit que F est un sous-groupe de E.

3) Pour que f soit un homomorphisme de groupe il faut et il suffit que $f(a\triangle b) = f(a) \cdot f(b)$.

On a

$$\begin{aligned} f(a\triangle b) &= f(ab + 3(a+b) + 6) \\ &= \lambda ab + 3\lambda(a+b) + \lambda 6 + 3. \end{aligned}$$

De plus,

$$\begin{aligned} f(a) \cdot f(b) &= (\lambda a + 3)(\lambda b + 3) \\ &= \lambda^2 ab + 3(a+b) + 9. \end{aligned}$$

Par identification, on obtient

$$\begin{cases} \lambda^2 = \lambda \\ 3\lambda = 3 \\ \lambda 6 + 3 = 9 \end{cases} \Longrightarrow \lambda = 1 \vee \lambda = 0,$$

si $\lambda = 0$, $f(a) = 3$ n'est pas un homomorphisme de groupe (car $f(-2) \neq 1$). Alors, $\lambda = 1$.

ii) Déterminons $\ker f$ tel que $f(a) = a + 3$. On a

$$\begin{aligned} \ker f &= \{a \in E, f(a) = 1\} \\ &= \{a \in E, a + 3 = 1\} \\ &= \{-2\}. \end{aligned}$$

iii) Comme $\ker f = \{-2\}$ (-2 étant le neutre de E) alors f est injective. Toute image $\alpha \in F$ admet un antécédent de la forme $(\alpha - 3)$, d'où f est surjective. Donc, f est un homomorphisme de groupes bijectif i.e isomorphisme de groupes. L'isomorphisme inverse est $f^{-1} : F \to E, f^{-1}(a) = a - 3$ (car $f^{-1} \circ f = id_E$, $f \circ f^{-1} = id_F$).

Exercice 4.4.4 *Soit D l'ensemble des nombres décimaux et donné par*

$$D = \left\{ \frac{p}{10^n}, (p, n) \in \mathbb{Z} \times \mathbb{N} \right\}.$$

1) Montrer que D est un sous-anneau de l'anneau $(\mathbb{Q}, +, \cdot)$.

2) L'ensemble D est-il un sous corps de $(\mathbb{Q}, +, \cdot)$.

3) Soit $\psi : (\mathbb{Q}, +, \cdot) \to (\mathbb{Q}, +, \cdot)$ définie par

$$\psi(x) = \frac{x}{10^n}, n \in \mathbb{N}.$$

L'application ψ est elle un homomorphisme d'anneaux.

Solution

1) Montrons que D est un sous-anneau de $(\mathbb{Q}, +, \cdot)$.

On sait que $D \subset \mathbb{Q}$. Soit $d, d' \in D$ tels que $d = \frac{p}{10^n}, d' = \frac{q}{10^m}$ où $p, p' \in \mathbb{Z}$ et $n, n' \in \mathbb{N}$. On a,

$$d - d' = \frac{p}{10^n} - \frac{q}{10^m} = \frac{10^m p - 10^n q}{10^{n+m}} \in D. \ (10^m p - 10^n q \in \mathbb{Z}, n + m \in \mathbb{N})$$

De plus,

$$d \cdot d' = \frac{pq}{10^{n+m}} \in D. \ (pq \in \mathbb{Z}, n+m \in \mathbb{N})$$

L'élément neutre de $\mathbb{Q}$ pour $\cdot$ est $1 = \frac{1}{10^0} \in D$.

Donc, $(D, +, \cdot)$ est un sous-anneau de $(\mathbb{Q}, +, \cdot)$.

2) $(D, +, \cdot)$ n'est pas un sous corps car $\frac{7}{10}$ n'est pas inversible pour $\cdot$ dans D.

3) On a $\psi(1) = \frac{1}{10^n}$.

Si $n = 0$, alors $\psi(1) = 1$. D'où, ψ est un homomorphisme.

Si $n \neq 0$, alors $\psi(1) \neq 1$. Donc, ψ ne peut pas être un homomorphisme.

4.5 Exercice supplémentaire

Exercice 4.5.1 *On définit sur $\mathbb{R}$ une loi de composition interne $\bigstar$ par*

$$\forall x, y \in \mathbb{R}, x \bigstar y = x + y + \frac{1}{6}.$$

1) Montrer que $(\mathbb{R}, \bigstar)$ est un groupe abélien.

2) Soit $f : (\mathbb{R}, \bigstar) \to (\mathbb{R}, +)$ telle que $f(x) = 3x + \frac{1}{2}$.

Montrer que f est un isomorphisme de groupes et donner l'expression de f^{-1}.

3) Soit $S = \left\{ \frac{2n-1}{6}, n \in \mathbb{Z} \right\}$. Montrer que $(S, \bigstar)$ est un sous-groupe de $(\mathbb{R}, \bigstar)$.

4)Soit $g : (\mathbb{Z}, +) \to (S, \bigstar)$ telle que $g(n) = \frac{2n-1}{6}$. Montrer que g est un isomorphisme de groupes.

Exercice 4.5.2 *Montrer que la composée de deux homomorphismes de groupes est un homomorphisme de groupes.*

Exercice 4.5.3 *Soit $(\Omega, +, \cdot)$ un anneau tel que $\forall \omega \in \Omega, \omega^2 = \omega$.*

1) Montrer que $\forall \omega \in \Omega, \omega + \omega = 0$.

2) Montrer que $(\Omega, +, \cdot)$ est un anneau commutatif.

Exercice 4.5.4 *Soit $\left(\mathbb{Z}/_{5\mathbb{Z}}, \dot{+}, \dot{\cdot}\right)$, tel que*

$$\forall \dot{a}, \dot{b} \in \mathbb{Z}/_{n\mathbb{Z}} : \ \dot{a} \dot{+} \dot{b} = \widehat{a+b} \ et \dot{a} \dot{\cdot} \dot{b} = et \cdot \widehat{a \cdot b}.$$

1) Montrer que $\left(\mathbb{Z}/_{5\mathbb{Z}}, \dot{+}, \dot{\cdot}\right)$ est un anneau. Est-il commutatif ?

2) $\left(\mathbb{Z}/_{5\mathbb{Z}}, \dot{+}, \dot{\cdot}\right)$ admet-il des diviseurs de zéro. Es ce que $\left(\mathbb{Z}/_{5\mathbb{Z}}, \dot{+}, \dot{\cdot}\right)$ est intègre ?

Exercice 4.5.5 *Soit l'ensemble* $G = \{(\alpha, \beta) \in \mathbb{R}^2 / x \geq 0, y > 0\}$. *Pour tout* $(a,b), (c,d) \in G$, *on pose*

$$(a,b) \top (c,d) = \left(a + c, bde^{2ac}\right).$$

1) Montrer que G *muni de* $\top$ *est un groupe abélien.*

2)Soit l'application $\phi : \mathbb{Z} \to G$ *définie par*

$$\phi(n) = \left(2n, 3^n e^{4n(n-1)}\right).$$

i) Vérifier que ϕ *est un homomorphisme de* $(\mathbb{Z}, +)$ *dans* $(G, \top)$.

ii) Déterminer $\ker \phi$.

iii) ϕ *est-il un isomorphisme de groupes ? justifier la réponse.*

3) Soit $H = \left\{\left(x, e^{(x^2)}\right), x \geq 0\right\}$, *vérifier que c'est un sous groupes de* $(G, \top)$.

Exercice 4.5.6 *Soit* $\xi : (E, *) \to (F, \perp)$ *un morphisme de groupes et la relation* $\Re$ *définie pour tout* $\alpha, \beta \in E$, *par* $x \Re y \iff x * y^{-1} \in \ker \xi$.

1) Vérifier que $\Re$ *est une relation d'équivalence.*

2) Montrer que l'ensemble quotient $\left(E/_{\ker \xi}, \dot{*}\right)$ *est un groupe où* $\dot{\alpha} \dot{*} \dot{\beta} = \widehat{\alpha * \beta}$.

3) Soit $\aleph : \left(E/_{\ker \xi}, \dot{*}\right) \to (\operatorname{Im} \xi, \perp)$ *défini par* $\aleph\left(\dot{\alpha}\right) = \xi(\alpha)$. *Montrer que* $\aleph$ *est un isomorphisme de groupes.*

Soit G *un ensemble muni d'une relation d'équivalence* $\Re$.

1. Montrer que pour tout couple $(a,b) \in G^2$, *on a l'une des deux possibilité suivantes :*

$$\dot{a} = \dot{b} \quad \text{ou} \quad \dot{a} \cap \dot{b} = \emptyset.$$

2. En déduire que les classes d'équivalence forment une partition de G.

3. On suppose, maintenant, que G *est muni d'une loi de groupe commutatif* $*$. *Soit* H *un sous-groupe de* G *et on définit dans* G *la relation binaire comme suit :*

$$\forall (a,b) \in G^2 : a \Re b \iff a * b^{-1} \in H.$$

a. Montrer que $\Re$ *est une relation d'équivalence.*

b. Décrire $\dot{a}$ *pour tout* $a \in G$.

c. Montrer en utilisant la question 2 que si G *est fini, alors* $Card(H) = Card(G)$.

4. **Application** *: Déterminer tous les sous-groupes des groupes* $(\mathbb{Z}/_{3\mathbb{Z}}, +)$ *et* $(\mathbb{Z}/_{4\mathbb{Z}}, +)$ *.*
Soient $(G, *)$ *un groupe commutatif et* H *un sous-groupe de* G*. On note* $\Re$ *la relation d'équivalence définie dans* G *comme dans l'exercice précédent. On définit dans l'ensemble quotient* $G/_{\Re}$ *la loi de composition* $\circledast$ *comme suit :*

$$\forall\,(a,b) \in G^2 :\ \dot{a} \circledast \dot{b} = \dot{\overline{a * b}}.$$

1. Montrer que cette loi est indépendante du choix des représentants, c'est à dire :

$$\forall x \in \dot{a},\ \forall y \in \dot{b}\ :\ \dot{a} \circledast \dot{b} = \dot{\overline{x * y}}.$$

2. Montrer que $(G/_{\Re}, \circledast)$ *est un groupe commutatif.*
Soient $(B, +)$ *un groupe et* A *un ensemble non vide quelconque. On suppose qu'il existe une bijection* $f : A \to B$ *et on définit dans* A *l'opération* $\oplus$ *comme suit :*

$$\forall\,(a,b) \in A^2 : a \oplus b = f^{-1}\left(f\left(a\right) + f\left(b\right)\right).$$

1. Montrer que $(A, \oplus)$ *est un groupe. A quelle condition est-il commutatif ?*
2. Montrer que f *est un morphisme de groupes.*
Soit $\Bbbk$ un ensemble non vide muni de deux lois internes $+$ et $\cdot$ ($\cdot$ distributive par rapport à $+$).
Montrer que $(\Bbbk, +, \cdot)$ est un corps si et seulement si $(\Bbbk, +)$ est un groupe commutatif et $(\Bbbk^*, \cdot)$ est aussi un groupe, $\Bbbk^*$ désigne l'ensemble $\Bbbk$ privé de l'élément neutre de la loi $+$.

Chapitre 5

Anneaux de Polynômes

5.1 Introduction

Par son ouvrage *" Abrégé du calcul par la restauration et la comparaison" ,* al-Khawarizmi donne naissance aux polynômes. Ces derniers interviennent dans la résolution des équations avec une ou plusieurs inconnues. Dans la même époque (IX^e siècle), Ibn al-Banna introduit les plynômes de degré n. Depuis, les polynômes sont devenus un outil important dans l'algèbre générale et linéaire.
Ce chapitre vise à compléter les connaissances acquises (opérations sur les polynômes, division euclidienne, racine d'un polynôme) de l'étudiant en matière de techniques algèbriques avec de nouvelles notions.

5.2 Polynômes

Définition 5.2.1 *Étant donné un anneau commutatif* $(A, +, \cdot)$ *, on dit que* P *est un polynôme si*

$$P = \alpha_0 + \alpha_1 X + \alpha_2 X^2 + \cdots + \alpha_n X^n + \cdots$$

où les ***coéfficients*** $(\alpha_i)_{i\in\mathbb{N}}$ *de* P *appartiennent à* A *et sont nuls sauf un nombre fini.*
On appelle $\alpha_i X^i$ *un* ***terme*** *de* P *et* X *l'****indéterminée****.*
On appelle ***degré*** *de* P *, le plus grand indice* n *pour lequel* $\alpha_n \neq 0$ *et on note* $\deg(P) = n$*.*
Dans ce cas, $\alpha_n X^n$ *est dit* ***terme dominant.***

Remarque 5.2.1 *1. Si* $\alpha_n = 1$*, alors on dit que* P *est unitaire.*

2. *Si* $\forall i \in \mathbb{N} : \alpha_i = 0$, P *est le polynôme nul et* $\deg(0) = -\infty$.

3. *Si* $P = \alpha$ $(\alpha \in A)$, *alors* P *est constant.*

4. *Si tout les coefficients sont nuls sauf un, on dit que* P *est un monôme.*

5. *On note par* $A[X]$ *l'ensembles des polynômes à une indéterminée à coefficients dans* A.

6. *Soit* $Q \in A[X]$, *tels que*

$$Q = \beta_0 + \beta_1 X + \beta_2 X^2 + \cdots + \beta_n X^n + \cdots$$

$P = Q$ si et seulement si $\forall i \in \mathbb{N} : \alpha_i = \beta_i$.

Exemple 5.2.1 1. $P = X^8 + 2X^5 - 3$, $P \in \mathbb{Z}[X]$ *car les coéfficients* $(-3, 0, 0, 0, 0, 2, 0, 0, 1, 0, \cdots)$ *sont des entier relatifs. C'est un polynôme unitaire de degré* 8 *et* X^8 *est le terme dominant.*

2. $Q = -\sqrt{7}X^3$, *le monôme* $Q \in \mathbb{R}[X]$ *car le seul coéfficient non nul* $\left(0, 0, 0, -\sqrt{7}, 0, \cdots\right)$ *est réel. C'est un polynôme non unitaire de degré* 3.

3. $R = (3 - i) X^2 + i - 2$ *est un polynôme à coéfficients complexes (i.e* $R \in \mathbb{C}[X]$*) où* $\alpha_2 = (3 - i)$, $\alpha_0 = i - 2$, $\deg(R) = 2$.

4. $S = 2i - 3$ *et* $T = 3 + \sqrt{5}$ *sont constants.*

5.3 Opérations sur les polynômes

5.3.1 Somme et produit de deux polynômes

Définition 5.3.1 *Soient deux polynômes de* $A[X]$

$$P = \alpha_0 + \alpha_1 X + \alpha_2 X^2 + \cdots + \alpha_n X^n + \cdots$$

et

$$Q = \beta_0 + \beta_1 X + \beta_2 X^2 + \cdots + \beta_n X^n + \cdots$$

La somme $P + Q$ *est un polynôme de* $A[X]$ *tel que*

$$P + Q = (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1) X + \cdots + (\alpha_n + \beta_n) X^n + \cdots$$

Le produit $P \cdot Q$ est un polynôme de $A[X]$ tel que

$$P \cdot Q = \left(\sum_{i+j=0} \alpha_i \beta_j \right) + \left(\sum_{i+j=1} \alpha_i \beta_j \right) X + \cdots + \left(\sum_{i+j=n} \alpha_i \beta_j \right) X^n + \cdots$$

Proposition 5.3.1 *Soient R, S deux polynômes de $A[X]$, on a*

1. $\deg(R+S) \leq \max(\deg(R); \deg(S))$.
2. $\deg(R \cdot S) \leq \deg(R) + \deg(S)$.
3. *A intègre* $\Longrightarrow \deg(R \cdot S) = \deg(R) + \deg(S)$.

Exemple 5.3.1

1. $P = X^8 + 2X^5 - 3, Q = -X^8 - 3X^5 + 5$

$$\begin{aligned} P + Q &= -X^5 - 2, \\ P \cdot Q &= -X^{16} - 5X^{13} - 6X^{10} + 8X^8 + 19X^5 - 15 \end{aligned}$$

$\deg(P+Q) = 5$ *et* $\deg(PQ) = 16 \leq \deg(P) + \deg(Q)$.

2. *Dans l'anneau* $(\mathbb{Z}/_{4\mathbb{Z}}, +, \cdot)$, *on a* $R = \dot{2}X^3 + \dot{3}X - \dot{1}$ *et* $S = \dot{3}X - \dot{2}$ *et*

$$\begin{aligned} R + S &= \dot{2}X^3 + \dot{3}X - \dot{1} \\ RS &= \dot{2}X^4 - \dot{0}X^3 + \dot{1}X^2 - \dot{1}X + \dot{2} \\ &= \dot{2}X^4 + X^2 - X + \dot{2} \end{aligned}$$

5.3.2 Division dans $(A[X], +, \cdot)$

Dans ce paragraphe, $(A, +, \cdot)$ est un anneau commutatif et intègre.

Définition 5.3.2 *Soient P, D des polynômes de l'anneau $(A[X], +, \cdot)$. S'il existe $Q \in A[X]$ vérifiant $P = Q \cdot D$, alors on dit que D divise P (ou encore P est un multiple de D).*

Exemple 5.3.2

1. *On a $0 = 0 \cdot P$, alors le polynôme nul est divisible par tout $P \in A[X]$.*
2. *Aussi, $P = X^2 + 5X + 6 = (X+2)(X+3)$. Alors, $(X+2)$ et $(X+3)$ divisent P.*

1. Tout élément inversible de $A[X]$ est un diviseur du polynôme constant 1.
2. Si $\exists Q \in A[X] : P = 0 \cdot Q$, alors $P = 0$.

Proposition 5.3.2

1. *$P \neq 0$, s'il existe $Q \in A[X] : P = S \cdot Q$, alors* $\deg(Q) \leq \deg(P)$.
2. *Si P divise Q et Q divise S, alors P divise S.*
3. *(P divise Q) $\wedge$ (Q divise P)* $\Longrightarrow \exists \lambda \in A : P = \lambda Q$.

5.4 Division euclidienne

Théorème 5.4.1 *Soient P, D deux polynômes de $A[X]$ où $D \neq 0$. Alors, il existe $Q, R \in A[X]$ tels que $P = Q \cdot D + R$ où $\deg(R) < \deg(D)$.*

Remarque 5.4.1 *On appele Q le quotient et R le reste.*

Exemple 5.4.1 *Soit $P = X^3 + 9X^2 + 26X + 24$, $D = X + 3$.*

$$\begin{array}{rl} X^3 + 9X^2 + 26X + 24 & X + 3 \\ -X^3 - 3X^2 & X^2 + 6X + 8 \\ \quad 6X^2 + 26X + 24 & \\ \quad -6X^2 - 18X & \\ \quad\quad 8X + 24 & \\ \quad\quad -8X - 24 & \\ \quad\quad 0 & \end{array}$$

Ainsi, $P = D \cdot Q$ avec $Q = X^2 + 6X + 8$ et $R = 0$. Donc, D divise P.

2) Pour $P = X^5 - 6X^3 + 17X + 4, D = X^3 - 2$, on a

$$\begin{array}{rl} X^5 - 6X^3 + 0X^2 + 17X + 4 & X^3 - 2 \\ -X^5 \quad\quad -2X^2 & X^2 - 6 \\ \quad -6X^3 - 2X^2 + 17X + 4 & \\ \quad +6X^3 - 12X^2 & \\ \quad\quad -14X^2 + 17X + 4 & \end{array}$$

P n'est pas divisible pas D car le reste de la division n'est pas nul $R = -14X^2 + 17X + 4$.

5.4.1 Le pgcd et le ppcm de deux ou plusieurs polyômes

Soient $(K, +, \cdot)$ un corps commutatif , $P_1, \cdots, P_r$ une famille finie de polynômes avec $I = \{1, \cdots, r\} \subset \mathbb{N}$.

Définition 5.4.1 *Le **plus grand diviseur commun** des polynômes $(P_i)_{i \in I}$ noté pgcd$(P_1, \cdots, P_r)$ est le polynôme unitaire ou nul Δ vérifiant les conditions :*

1. Δ divise tous les P_i, $(i \in I)$;

2. Tout autre polynôme Q qui divise tous les P_i, divise aussi Δ.

On a la caractérisation suivante :

Théorème 5.4.2 $\Delta = pgcd(P_1, \cdots, P_r)$ *si et seulement s'il existe une famille* $Q_1, \cdots, Q_r$ *de polynômes tels que*

$$P_1Q_1 + \cdots + P_rQ_r = \Delta.$$

Définition 5.4.2 *Le* ***plus petit multiple commun*** *des polynômes* $(P_i)_{i\in I}$ *noté* $ppcm\,(P_1, \cdots, P_r)$ *est le polynôme unitaire* Π *vérifiant les conditions :*

1. Π *est un multiple de tous les* P_i, $(i \in I)$;

1. Tout autre polynôme S *qui est multiple de tous les* P_i, *aussi un multiple de* Π.

Remarque 5.4.2 *1. Si* Δ *existe, alors il est unique et est aussi noté* $P_1 \wedge P_2 \wedge \cdots \wedge P_r$.

2. Si Π *existe, alors il est unique et est encore noté* $P_1 \vee P_2 \vee \cdots \vee P_r$.

3. Δ *et* Π *sont commutatifs :*

$$\begin{aligned} pgcd\,(P_1, P_2) &= pgcd\,(P_2, P_1)\,, \\ ppcm\,(P_1, P_2) &= ppcm\,(P_2, P_1) \end{aligned}$$

et associatifs

$$\begin{aligned} p\gcd\,(P_1, P_2, P_3, P_4) &= pgcd\,(pgcd\,(P_2, P_1)\,; pgcd\,(P_3, P_4))\,, \\ ppcm\,(P_1, P_2, P_3, P_4) &= ppcm\,(ppcm\,(P_2, P_1)\,; ppcm\,(P_3, P_4))\,. \end{aligned}$$

4. $pgcd\,(\alpha_1 P_1, \alpha_2 P_2) = pgcd\,(P_2, P_1)$ / $\alpha_1, \alpha_2 \in K$.

5. $pgcd\,(\alpha_1 U P_1, \alpha_2 U P_2) = U \cdot pgcd\,(P_2, P_1)$ / $U \in K\,[X]$.

Exemple 5.4.2 *1. On a* $P_1 = X^2 + 8X + 15 = (X+5)\,(X+3)$ *et* $P_2 = X^3 + 9X^2 + 26X + 24 = (X+3)\,(X^2 + 6X + 8)$. *Alors, on peut dire que* $\Delta = pgcd\,(P_1, P_2) = X + 3$.

2. Pour $P_1 = 2X^2 - 14 = 2\left(X + \sqrt{7}\right)\left(X - \sqrt{7}\right)$ *et* $P_2 = \left(X + \sqrt{7}\right)$, *on a* $\Pi = ppcm\,(P_1, P_2) = X^2 - 7$.

3. $pgcd(X^2 + 5, 3X - 6) = 1$.

4. $\forall P \in K\,[X] : p\gcd\,(P, 1) = 1$.

Théorème 5.4.3 (théorème de Bezout) *Soient* P,$Q \in K\,[X]$, $\Delta \in K\,[X]$ *unitaire non nul. Si* Δ *est le pgcd de* P *et* Q, *alors il esxiste* $(U, V) \in K\,[X]^{\,2}$ *tel que* $PU + QV = \Delta$.

Pour déterminer le *pgcd* de deux polynômes on utilise l'algorthime d'Euclide, c'est une méthode qui se base sur la division euclidienne.

5.4.2 Algorithme d'Euclide

Soit P et D deux polynômes non nuls avec $\deg P \geq \deg D$. Il existe alors Q et R tels que

$$P = D \cdot Q + R$$

Le procédé itératif d'euclide est $pgcd\ (P, D) = pgcd\ (D, R)$, i.e

Étape 1 : On divise P par D.

Étape2 : Si $R = 0$ alors $pgcd\ (P, D) = D$, Sinon on va à l'étape 3.

Étape3 : on divise D par R et on revient a l'étape (2).

Ainsi de suite, jusqu'à avoir un reste nul.

Exemple 5.4.3 *Calculer du pgcd* (P, D) *tel que*

$$P = X^5 - 2X^4 + X^2 - X - 2, \quad D = X^3 - X^2 - X - 2.$$

Étape 1 : On divise P par D

$$\begin{array}{cc} X^5 - 2X^4 + X^2 - X - 2 & X^3 - X^2 - X - 2 \\ 2X^2 - 3X - 2 & X^2 - X \end{array}, \ \textit{ainsi } P = D \cdot \underbrace{\left(X^2 - X\right)}_{Q_1} + \underbrace{\left(2X^2 - 3X - 2\right)}_{R}$$

Puisque $R \neq 0$ *, alors on passe à (3) et on divise D par R*

$$\begin{array}{cc} X^3 - X^2 - X - 2 & 2X^2 - 3X - 2 \\ \frac{3}{4}X - \frac{3}{2} & \frac{1}{2}X - \frac{1}{4} \end{array}, \ d'où\ D = R \cdot \underbrace{\left(\frac{1}{2}X - \frac{1}{4}\right)}_{Q_2} + \underbrace{\left(\frac{3}{4}X - \frac{3}{2}\right)}_{R_1}.$$

Comme $R_1 \neq 0$, *alors on continue les divisions*

$$\begin{array}{cc} 2X^2 - 3X - 2 & \frac{3}{4}X - \frac{3}{2} \\ 0 & \frac{8}{3}X - \frac{4}{3} \end{array}, \ d'où\ R = R_1 \cdot \underbrace{\left(\frac{8}{3}X - \frac{4}{3}\right)}_{Q_2} + \underbrace{(0)}_{R_2}.$$

On a $R_2 = 0$, *alors* $pgcd\,(P, D) = \frac{4}{3}\ R_1 = X - 2$.

Remarque 5.4.3 *Le* $pgcd\,(P, D)$ *est le dernier reste non nul de la division euclidienne.*

5.4.3 Polynômes premiers entre eux

Définition 5.4.3 *Soient P et Q deux polynômes de $K[X]$. On dit que P et Q sont premiers entre eux si $pgcd(P,Q)=1$.*

En appliquant le théorème de Bezout, on obtient

Théorème 5.4.4 *Les polynômes P,$Q \in K[X]$ sont premiers entre eux si et seulement s'il existe $U,V \in K[X]$ tel que $PU+QV=1$.*

Remarque 5.4.4 *Plus généralement, les $(P_i)_{i\in I}$ sont premiers entre eux si on a $pgcd(P_i)=1$ / $i \in I$ ou s'il existe $(U_i) \in K[X]$ avec $i \in I$, vérifiants $\sum_{i\in I} P_i \cdot U_i = 1$.*

1. Si $pgcd(P,Q)=1$ et $pgcd(P',Q)=1$, alors $pgcd(P\cdot P',Q)=1$.
2. Si $pgcd(P,Q)=1$, alors $pgcd(P^n,Q^m)=1$ / $n,m \in \mathbb{N}$.
3. $\exists \gamma \in K : pgcd(P,Q)\cdot ppcm(P,Q)=1$.
4. Si $\forall i \in I, \exists Q_i \in K[X] : P_i = D_i \cdot Q$, alors $\prod_{\forall i\in I} P_i$ divise Q.

5.5 Polynômes irréductibles

Définition 5.5.1 *On dit qu'un polynôme $A \in K[X]$ $(\deg A \geq 1)$ est irréductible (ou premier) s'il n'est divisible que par γ et (γA) où $\gamma \in K^*$.*

Exemple 5.5.1

1. *Tout polynôme de la forme $\alpha X+\beta$ est irréductible.*
2. *Dans $\mathbb{R}[X]$, $A=X^2+2$ est irréductible. Mais, dans $\mathbb{C}[X]$ A n'est pas premier car on a : $A=X^2+2=\left(X-i\sqrt{2}\right)\left(X+i\sqrt{2}\right)$.*

Proposition 5.5.1 *Soit un polynôme irréductible A et $P,(P_i)_{i\in I}$ dans $K[X]$.*

1. *Si A ne divise pas P, alors $pgcd(A,P)=1$.*
2. *A divise $\prod_{i\in I} P_i \iff A$ divise au moins un P_i.*

5.5.1 Factorisation des polynômes

Similairement à la décomposition des entiers naturels en facteurs premiers on a la factorisation des polynômes, appelée aussi "Décomposition en facteurs irréductible".

Théorème 5.5.1 *Soit $P \in K[X]$ de degré $n \geq 1$. Il existe des polynômes irréductibles A_i dans $K[X]$ / $i \in I$ tels que*

$$P = \Lambda \prod_{i \in I} A_i^{\lambda_i};$$

où $\Lambda \in K^*$ et $\lambda_i \in \mathbb{N}^*$ pour tout $i \in I$. Les A_i sont uniques à permutation près.

Exemple 5.5.2 *Soit $P = X^6 - 1$. Pour décomposer P on pose $Y = X^3$, on obtient alors : $P = Y^2 - 1$. Or, $Y^2 - 1 = (Y-1)(Y+1)$. Ainsi, $P = X^6 - 1 = (X^3-1)(X^3+1)$. En utilisant la division euclidienne, la factorisation de P dans $\mathbb{R}[X]$ est*

$$P = \underbrace{(X-1)}_{A_1} \cdot \underbrace{(X+1)}_{A_2} \cdot \underbrace{\left(X^2+X+1\right)}_{A_3} \cdot \underbrace{\left(X^2-X+1\right)}_{A_4}.$$

Mais, dans $\mathbb{C}[X]$ on a

$$P = (X-1)(X+1)\left(X + \frac{1+i\sqrt{3}}{2}\right)\left(X - \frac{1+i\sqrt{3}}{2}\right)\left(X - \frac{1-i\sqrt{3}}{2}\right)\left(X + \frac{1-i\sqrt{3}}{2}\right).$$

5.6 Exercices corrigés

Exercice 5.6.1 *Soit* $Q \in \mathbb{R}[X]$ *défini par* $Q = X^4 + 2\alpha X^3 + \beta X^2 + 2X + 1$.
Trouver $(\alpha, \beta) \in \mathbb{R}$ *pour que* Q *soit le carré d'un polynôme de* $\mathbb{R}[X]$.

Solution

Si Q est le carré d'un polynôme de $\mathbb{R}[X]$, alors $\exists P \in \mathbb{R}[X] : Q = (\pm P)^2$. Ainsi, $\deg P = 2$ et $P = X^2 + aX + b$. Alors,

$$P^2 = X^4 + 2aX^3 + \left(2b + a^2\right) X^2 + 2abX + b^2.$$

En comparant les deux formules, on a

$$\left\{ \begin{array}{c} 2ab = 2 \\ b^2 = 1 \end{array} \right. \Longrightarrow \left\{ \begin{array}{c} ab = 1 \\ b = 1 \vee b = -1 \end{array} \right. ,$$

si $b = 1$, alors $a = 1$ *et* si $b = -1$, alors $a = -1$. D'où,

$$P = X^2 + X + 1 \text{ ou } P = X^2 - X - 1$$

Donc, $Q = (X^2 + X + 1)^2$ ou $Q = (-X^2 - X - 1)^2$ ou $Q = (X^2 - X - 1)^2$ ou $Q = (-X^2 + X + 1)^2$.

Exercice 5.6.2 *Soit* $A \in \mathbb{R}[X], \alpha, \beta$ *deux réels différents. Trouver le reste de la division euclidienne de* A *par* $(X - \alpha)(X - \beta)$ *si le reste de la division de* A *par* $(X - \alpha)$ *vaut* 1 *et par* $(X - \beta)$ *est égal à* -1.

Solution

Si le reste de la division de A par $(X - \alpha)$ vaut 1 et par $(X - \beta)$ est égal à -1, alors $\exists P, Q \in \mathbb{R}[X]$:

$$A = (X - \alpha) \cdot P + 1 \text{ et } A = (X - \beta) \cdot Q - 1$$

On remarque ,aussi, que $A(\alpha) = 1$ et $A(\beta) = -1$. De plus, le division de A par $(X - \alpha)(X - \beta)$ est de la forme

$$A = (X - \alpha)(X - \beta) \cdot P + aX + b$$

Après simplification, on trouve

$$a\alpha + b = 1 \text{ et } a\beta + b = -1 \iff a = \frac{2}{\alpha - \beta} \text{ et } b = \frac{-\alpha - \beta}{\alpha - \beta}.$$

Il en résulte que $R = \dfrac{2}{\alpha - \beta} X + \dfrac{-\alpha - \beta}{\alpha - \beta}$.

Exercice 5.6.3 *Effectuer la division euclidienne de P par D :*

1. *Dans* $\mathbb{C}[X]$: $P = iX^3 - X^2 - i + 1$; $D = (i+1)X^2 - iX + 3$.
2. *Dans* $\mathbb{R}[X]$: $P = X^3 + X^2 + X + 1$; $D = X^2 + 1$.

Solution

On a $P = Q \cdot D + R$ *i.e* Q est le quotient et R est le rest de la division :

1. $Q = \frac{i+1}{2}X + \frac{2i-1}{2}$; $R = \frac{5-4i}{2}X + \frac{5-8i}{2}$.
2. $Q = X + 1; R = 0$.

Exercice 5.6.4 *Déterminer le $pgcd(P, Q)$ dans les cas suivants (effectuer la division euclidienne) :*

1. $P = X^4 - 3X^3 + X^2 + 4$, $Q = X^3 - 3X^2 + 3X - 2$;
2. $P = X^5 - 3X^3 + X^2 + 4$, $Q = X^3 - 3X^2 + 3X - 2$;
3. $P = X^4 + 4X^3 + X^2 - 16$, $Q = X^3 + 3X^2 - 3X + 4$

Solution

1. $pgcd(P, Q) = X - 2$.
2. $pgcd(P, Q) = X^2 - X + 1$.
3. $pgcd(P, Q) = X + 4$

Exercice 5.6.5 *Montrer que $P = X^3 - X^2 + X - 1$ est divisible par $X - 1$.*
Factoriser P dans $\mathbb{R}[X]$, puis dans $\mathbb{C}[X]$.

Solution

On remarque que $a = 1$ est une racine de P, donc $X - a$ divise P.
En effectuant la division euclidienne on obtient $P = (X-1)(X^2+1)$. Dans $\mathbb{R}[X]$, les deux polynômes $(X-1)$ et (X^2+1) sont premiers. D'où, la factorisation .
Dans $\mathbb{C}[X]$, $b = i$ est une racine de (X^2+1). Ainsi, on peut écrire $X^2+1 = (X-i)(X+i)$.
Alors, la décomposition de P est $P = (X-1)(X-i)(X+i)$.

5.7 Exercices supplémentaires

Exercice 5.7.1 *Factoriser les polynômes suivants dans* $\mathbb{R}[Y]$:

1) $Y^3 - 3Y^2 + 9Y + 13$.

2) $Y^4 - 16$.

3) $Y^5 + 2Y^4 - 16Y - 32$.

Exercice 5.7.2 *Soient* $P = Y^7 - Y - 1$ *et* $Q = X^5 - 1$.

Trouver $U, V \in \mathbb{R}[Y]$ *tels que* $PU + QV = 1$.

En déduire $pgcd(P, Q)$.

Exercice 5.7.3 *Soient* P *et* Q *deux polynômes. Montrer l'équivalence suivante :*

$$P \wedge Q = 1 \iff (P + Q) \wedge (P \cdot Q) = 1.$$

Exercice 5.7.4 *Soit* $A \in \mathbb{R}[Y]$ *donné par* $A = Y^4 + \frac{1}{3}Y^3 + Y^2 + 10$.

1) Montrer que A *n'admet aucune racine réelle.*

2) Dire si A *est irréductible dans* $\mathbb{R}[Y]$ *et pourquoi ?*

Bibliographie

[1] E. Azoulay, J. Avignant, Mathématiques 4. algèbre, McGrow-Hill-Paris. (1984)

[2] A. Bodin, B. Boutin, P. Romon : Algèbre : cours de mathématiques première année Ex07.

[3] F. Liret, D. Martinais : Algèbre première année : cours et exercices avec solution. DUNOD (2003) .

[4] J. Marie Monier, Les méthodes et exercices de mathématiques PCSI-PTSI, Dunod, Paris. (2008)