RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
Ministère de l'enseignement supérieur et de la recherche scientifique

Université L'arbi Ben M'hidi Oum El Bouaghi

Faculté des Sciences exactes et de sciences de la nature et de la vie
Département de Mathématiques et Informatiques

Cours du module : Algèbre1

Première année

Guerarra Sihem

2016 / 2017

Table des Matières

1 Notions de Logique **2**
1.1 Notions de Logique . . . 2
1.1.1 Opérations logiques . . . 2
1.1.2 **Règles de Demorgan:** . . . 4
1.2 Les quantificateurs . . . 5
1.2.1 Le quantificateur ∀, ou "pour tout" . . . 5
1.2.2 Le quantificateur ∃, ou "il existe" . . . 6
1.2.3 La négation des quatificateurs . . . 6
1.3 Types de raisonnements . . . 7
1.3.1 Raisonnement direct: . . . 7
1.3.2 Cas par cas . . . 7
1.3.3 Contraposé . . . 7
1.3.4 Absurde . . . 8
1.3.5 Contre exemple . . . 8
1.3.6 Récurrence . . . 8
1.4 Exercices . . . 9

2 Ensembles et applications **12**
2.1 Ensemles . . . 12
2.1.1 Opérations sue les ensembles . . . 12
2.2 Les applications . . . 14
2.2.1 Image directe , Image réciproque . . . 15
2.2.2 Injection, surjection, bijection . . . 16
2.2.3 L'application réciproque . . . 18
2.2.4 Prolongement et restriction . . . 19
2.3 Exercices . . . 20

3 Relations binaire sur un ensemble **23**
3.1 Relation d'équivalence . . . 23
3.2 Relation d'ordre . . . 25
3.2.1 Ordre total ou partiel . . . 25
3.3 Exercices . . . 28

4 Structures algébriques **32**
4.1 Loi de composition interne . . . 32
4.2 Les groupes . . . 33
4.2.1 Sous-groupes . . . 34

4.2.2 Homomorphisme de groupes . . . 34
4.3 Structure d'Anneau . . . 36
4.3.1 Sous anneau . . . 37
4.3.2 Homomorphismes d'Anneaux . . . 37
4.3.3 Diviseurs de zéro, les éléments inversibles . . . 37
4.3.4 Idéaux . . . 38
4.4 Corps . . . 39
4.4.1 Sous corps . . . 39
4.5 Exercices . . . 40

5 Anneaux des polynômes **46**
5.1 Construction de l'anneau des polynomes . . . 46
5.2 Arithmétique des polynômes . . . 47
5.2.1 Division euclidienne . . . 47
5.2.2 Racine d'un polynôme . . . 49
5.2.3 factorisation (Décomposition en facteurs irréductibles) . . . 50
5.3 Exercices . . . 51

Bibliographie **55**

Introduction

L'algèbre (de l'arabe al-jabr) est une branche des mathématiques qui permet d'exprimer les propriétés des opérations et le traitement des équations et aboutit à l'étude des structures algébriques. Selon l'époque et le niveau d'études considérés, elle peut être décrite comme :

· Une arithmétique généralisée, étendant à différents objets ou grandeurs les opérations usuelles sur les nombres,

· La théorie des équations et des polynômes,

· Depuis le début du $XX^{ème}$ siècle, l'étude des structures algébriques (algèbre générale ou abstraite).

Historiquement, les structures algébriques sont apparues dans différents domaines des mathématiques, et n'y ont pas été étudiées séparément. C'est pourquoi l'algèbre générale pos-sède beaucoup de connexions avec toutes les branches des mathématiques, un grand nombre de types de structures algébriques vérifient différents axiomes (groupes, anneaux, corps, espaces vectoriels,...etc.). Pour ces différents types de structures, on définit une notion d'homomorphisme et des constructions de structures qui sont analogues ou qui ont des propriétés analogues (sous-structures, quotients, produits,...etc.). Ces homomorphismes et ces constructions ont un grand nombre de propriétés qui sont semblables (l'intersection de sous-groupes, de sous-anneaux,...etc., en est un, l'image d'un sous-groupe, d'un sous-anneau,...etc., par un homomorphisme en est un aussi). On a alors définit de manière générale et abstraite les structures algébriques pour pouvoir traiter de manière uniforme ces constructions et leurs propriétés, et on a pu, par la suite, se concentrer sur les propriétés propres à chacune de ces structures.

Vue à l'interet de ce domain vaste de mathématique, on s'interesse dans ce cours de mathématiques de première année essentielement, par les notions d'algèbre générale, et se divise en cinq chapitres, le premier débute par la logique et les ensembles, qui sont des fondamentaux en mathématiques, ensuite on présente les relations binaires définies sur un ensemble. Enfin il se termine par l'étude, des structures algébriques ainsi que l'anneau de polynômes, et pour motiver ces notions d'algèbre, le cours se comporte à la fin de chaque partie, des exercices avec des solutions.

Chapitre 1

Notions de Logique

1.1 Notions de Logique

Définition 1.1 *On appelle "proposition logique" toute relation P qui est soit vraie soit fausse.*

- *Quand la proposition est vraie, on lui affecte la valeur* 1
- *Quand la proposition est fausse, on lui affecte la valeur* 0.

Ces valeurs sont appelées “Valeurs de vérité de la proposition”.

Exemple 1.1 •*« Il pleut. » est une proposition*

- *« Je suis plus grand que toi. », est une proposition*
- *« $2+2=4$ » est une proposition*
- *« $2\times 3=7$ » est une proposition*
- *« Pour tout $x\in\mathbb{R}$, on a $x^2\geq 0$» est une proposition*
- *« Comment allez vous aujourd'hui ? » n'est pas une proposition.*

Ainsi, pour définir une proposition logique, il suffit de donner ses valeurs de vérités. En général, on met ces valeurs dans un tableu qu'on nommera “Table de vérités” ou “Tableau de vérités”

1.1.1 Opérations logiques

La négation: $\overline{P}$

Etant donnée une proposition logique P, on appelle négation de P la proposition logique $\overline{P}$, qui est fausse quand P est vraie et qui est vraie quand P est fausse, donc on peut la représenter comme suit:

P	$\overline{P}$
1	0
0	1

La conjonction "$\wedge$"

Soient P, Q deux propositions logiques, on appelle "conjonction" de P et Q la proposition "$P \wedge Q$", qui est vraie quand P et Q sont vraies à la fois et fausse dans les autres cas.

Sa table de vérité:

P	Q	$P \wedge Q$
1	1	1
0	0	0
1	0	0
0	1	0

La disjonction "$\vee$"

Soient P, Q deux propositions logiques, on appelle "disjonction" de P et Q la proposition "$P \vee Q$", qui est vraie si l'une des propositions logiques P ou Q est vraie. Sa table de vérité:

P	Q	$P \vee Q$
1	1	1
0	0	0
1	0	1
0	1	1

L'implication "$\Longrightarrow$"

Considérons deux propositions logiques P et Q, on note "$P \Longrightarrow Q$" la proposition logique qui est fausse si P est vraie et Q est fausse.
La proposition $P \Longrightarrow Q$ se lit "P implique Q".

P	Q	$P \Longrightarrow Q$
1	1	1
0	0	1
1	0	0
0	1	1

Etant données deux propositions logiques P et Q, alors la table de vérités de $\overline{P} \vee Q$ est la suivante :

P	Q	$\overline{P}$	$\overline{P} \vee Q$
1	1	0	1
0	0	1	1
1	0	0	0
0	1	1	1

On voit que cette table est identique à celle de $P \Longrightarrow Q$, donc on dit que la proposition $P \Longrightarrow Q$ est equivalent à la proposition $\overline{P} \vee Q$.

L'équivalence "$\Longleftrightarrow$"

On dit que les deux propositions logiques P et Q sont logiquement équivalentes, si elles sont vraies simultanément ou fausse simultanément, et on note "$P \Longleftrightarrow Q$", sa table de vérité est

P	Q	$P \Longleftrightarrow Q$
1	1	1
0	0	1
1	0	0
0	1	0

1.1.2 Règles de Demorgan:

Soient P et Q deux propositions logiques, alors :

1. $\overline{P \wedge Q} \Longleftrightarrow \overline{P} \vee \overline{Q}$.
2. $\overline{P \vee Q} \Longleftrightarrow \overline{P} \wedge \overline{Q}$.

Preuve. On établit la preuve de ces règles en donnant les valeurs de vérités des propositions logiques correspondantes

P	Q	$\overline{P}$	$\overline{Q}$	$P \vee Q$	$\overline{P} \vee \overline{Q}$	$\overline{P \wedge Q}$	$\overline{P \vee Q}$	$\overline{P} \vee \overline{Q}$	$\overline{P} \wedge \overline{Q}.$
1	1	0	0	1	1	0	0	0	0
0	0	1	1	0	0	1	1	1	1
1	0	0	1	1	0	1	0	1	0
0	1	1	0	1	0	1	0	1	0

■

On voit que les propositions logiques $\overline{P \vee Q}$ et $\overline{P} \wedge \overline{Q}.$ ont les mêmes valeurs de vérité, donc elles sont équivalentes. De même pour $\overline{P \wedge Q}$ et $\overline{P} \vee \overline{Q}$.

Proposition 1.1 *Soient P, Q, R trois propositions logiques alors,*

1. $P \Longleftrightarrow \overline{\overline{P}}$,
2. $P \vee Q \Longleftrightarrow Q \vee P$, *($\vee$ est commutatif)*
3. $P \wedge Q \Longleftrightarrow Q \wedge P$ *($\wedge$ est commutatif)*
4. $(P \vee Q) \vee R \Longleftrightarrow P \vee (Q \vee R)$ *($\vee$ est associatif)*
5. $(P \wedge Q) \wedge R \Longleftrightarrow P \wedge (Q \wedge R)$ *($\wedge$ est associatif)*
6. $(P \wedge Q) \vee R \Longleftrightarrow (P \vee R) \wedge (Q \vee R)$ *($\vee$ est distributive sur $\wedge$)*
7. $(P \vee Q) \wedge R \Longleftrightarrow (P \wedge R) \vee (Q \wedge R)$ *($\wedge$ est distributive sur $\vee$)*
8. $[(P \Longrightarrow Q) \wedge (Q \Longrightarrow R)] \Longrightarrow (P \Longrightarrow R)$.
9. $[(P \Longrightarrow Q) \wedge (Q \Longrightarrow P)] \Longleftrightarrow (P \Longleftrightarrow Q)$

Preuve. On se limitera à la preuve des trois dernières propriétés

7.

P	Q	R	$P \vee Q$	$(P \vee Q) \wedge R$	$P \wedge R$	$Q \wedge R$	$(P \wedge R) \vee (Q \wedge R)$
1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0
1	1	0	1	0	0	0	0
1	0	1	1	1	1	0	1
0	1	1	1	1	0	1	1
1	0	0	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	0	0	0	0	0

9.

P	Q	$P \Longrightarrow Q$	$Q \Longrightarrow P$	$(P \Longrightarrow Q) \wedge (Q \Longrightarrow P)$	$P \Longleftrightarrow Q$
1	1	1	1	1	1
0	0	1	1	1	1
1	0	0	1	0	0
0	1	1	0	0	0

8.

P	Q	R	$P \Longrightarrow Q$	$Q \Longrightarrow R$	$(P \Longrightarrow Q \wedge Q \Longrightarrow R)$	$P \Longrightarrow R$	$(P \Longrightarrow Q \wedge Q \Longrightarrow R) \Longrightarrow (P \Longrightarrow R)$
1	1	1	1	1	1	1	1
0	0	0	1	1	1	1	1
1	1	0	1	0	0	0	1
1	0	1	0	1	0	1	1
0	1	1	1	1	1	1	1
1	0	0	0	1	0	0	1
0	1	0	1	0	0	1	1
0	0	1	1	1	1	1	1

Ce qui montre que la proposition $[(P \Longrightarrow Q) \wedge (Q \Longrightarrow R)] \Longrightarrow (P \Longrightarrow R)$ est toujours vraie. ■

1.2 Les quantificateurs

1.2.1 Le quantificateur $\forall$, ou "pour tout"

Une proposition P peut dépendre d'un paramètre x, par exemple « $x^2 \geq 1$ », l'assertion $P(x)$ est vraie ou fausse selon la valeur de x.

La proposition

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

est une proposition vraie lorsque les propositions $P(x)$ sont vraies pour tous les éléments x de l'ensemble E. On lit « Pour tout x appartenant à E, $P(x)$ »

Exemple 1.2 • *«*$\forall x \in [1, +\infty[\,;\, x^2 \geq 1$*» est une proposition vraie.*
• *«*$\forall x \in \mathbb{R};\, x^2 \geq 1$ *» est une proposition fausse.*
• *«* $\forall n \in \mathbb{N},\, n(n+1)$ *est divisible par 2 » est vraie.*

1.2.2 Le quantificateur ∃, ou "il existe"

La proposition

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

est une proposition vraie lorsque l'on peut trouver au moins un x de E pour lequel $P(x)$ est vraie. On lit « il existe x appartenant à E tel que $P(x)$ soit vraie ».

Exemple 1.3 • *«*$\exists x \in \mathbb{R},\, x(x-1) \prec 0$*» est vraie*
• *«*$\exists n \in \mathbb{N},\, n^2 - n \succ n$*» est vraie*
• *«* $\exists x \in \mathbb{R},\, x^2 = -4$*) » est fausse*

1.2.3 La négation des quatificateurs

• La négation de « $\forall x \in E, P(x)$ » est « $\exists x \in E, \overline{P(x)}$ » .
par exemple la négation de « $\forall x \in \mathbb{R};\, x^2 \geq 1$ » est l'assertion « $\exists x \in \mathbb{R};\, x^2 \prec 1$».
• La négation de « $\exists x \in E, P(x)$ » est « $\forall x \in E, \overline{P(x)}$ »
par exemple la négation de «$\exists n \in \mathbb{N},\, n^2 - n \succ n$» est «$\forall n \in \mathbb{N},\, n^2 - n \leq n$»
• la négation de phrases complexes: soit par exemple la proposition «$\forall x \in E,\, \exists y \in E,\, P(x,y)$»
sa négation est «$\exists x \in E,\, \forall y \in E,\, \overline{P(x,y)}$»

Exemple 1.4 *pour la proposition «*$\forall x \in \mathbb{R},\, \exists y \in \mathbb{R},\, x+y \succ 0$*», sa négation est «*$\exists x \in \mathbb{R},\, \forall y \in \mathbb{R},\, x+y \leq 0$*»*

Remarque 1.1 *L'ordre des quantificateurs est très important. Par exemple les deux phrases logiques*

$$\text{«}\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x+y \succ 0\text{»} \quad \textit{et} \quad \text{«}\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, x+y \succ 0\text{»}$$

sont différentes. La première est vraie, la seconde est fausse. En effet la première phrase affirme que « Pour tout réel x, il existe un réel y (qui peut donc dépendre de x) tel que $x+y>0$.» (par exemple pour un x donné on peut prendre $y=-x+1$). C'est donc une phrase vraie. Par contre la deuxième se lit : « Il existe un réel y, tel que pour tout réel x, $x+y>0$. » Cette phrase est fausse, cela ne peut pas être le même y qui convient pour tous les x.

1.3 Types de raisonnements

1.3.1 Raisonnement direct:

On veut montrer que la proposition "$P \Longrightarrow Q$" est vraie,

On suppose que P est vraie et on montre qu'alors Q est vraie

Exemple 1.5 *Montrer que* "$\forall x,\, y \in \mathbb{R}^+,\, x \leq y \Longrightarrow x \leq \dfrac{x+y}{2} \leq y$

Preuve. $x \leq y \Longrightarrow x + x \leq x + y$

$\Longrightarrow 2x \leq x + y$

$\Longrightarrow x \leq \dfrac{x+y}{2}$.....(1)

$y \geq x \Longrightarrow x + y \leq y + y$

$\Longrightarrow \dfrac{x+y}{2} \leq y$.....(2)

de (1) et (2) on a: $x \leq \dfrac{x+y}{2} \leq y$

Alors $\forall x,\, y \in \mathbb{R}^+,\, x \leq y \Longrightarrow x \leq \dfrac{x+y}{2} \leq y$ est vraie ■

1.3.2 Cas par cas

Si on veut vérifier une proposition $P(x)$ pour tout les x dans un ensemble E, on montre la proposition $P(x)$ pour les $x \in A \subset E$, puis pour les $x \notin A$.

Exemple 1.6 *Montrer que :*$\forall x \in \mathbb{R},\, |x-1| \leq x^2 - x + 1$.

Preuve. • Si $x \geq 1 : |x-1| = x - 1$, alors $x^2 - x + 1 - |x-1| = x^2 - x + 1 - x + 1 = x^2 - 2x + 2 = (x-1)^2 + 1 \geq 0$.

Ainsi $x^2 - x + 1 \geq |x-1|$.

• si $x \prec 1 : |x-1| = -x + 1$, alors $x^2 - x + 1 - |x-1| = x^2 - x + 1 + x - 1 = x^2 \geq 0$.

Ainsi $x^2 - x + 1 \geq |x-1|$.

Conclusion: dans tous les cas $|x-1| \leq x^2 - x + 1$. ■

1.3.3 Contraposé

Le raisonnement par "contraposition" est basé sur l'équivalence suivante:

$$(P \Longrightarrow Q) \Longleftrightarrow \left(\overline{Q} \Longrightarrow \overline{P}\right)$$

Donc si l'on souhaite montrer l'assertion "$P \Longrightarrow Q$" on montre en fait que si $\overline{Q}$ est vraie alors $\overline{P}$ est vraie.

Exemple 1.7 *Montrer que :* $\forall n \in \mathbb{N}$, n^2 *est pair alors* n *est pair.*

Preuve. on veut montrer que *si* n^2 est impair$\Longrightarrow n$ est impair.
n est impair, alors il existe $k \in \mathbb{N}$ tel que $n = 2k+1$, alors $n^2 = 4k^2+4k+1 = 2\left(2k^2+2k\right)+1 = 2\alpha+1$, alors n^2 est impair. ■

1.3.4 Absurde

Le raisonnement par "l'absurde" pour montrer que "$P \Longrightarrow Q$" est basé sur le principe suivant

"on suppose à la fois que P est vraie et que Q est fausse, et on cherche une contradiction. Ainsi si P est vraie alors Q doit être vraie et donc "$P \Longrightarrow Q$" est vraie.

Exemple 1.8 *Montrer que:* $\forall x, y \in \mathbb{R}^+$,*si* $\dfrac{x}{1+y} = \dfrac{y}{1+x}$ *alors* $x = y$.

Preuve. on suppose que $\dfrac{x}{1+y} = \dfrac{y}{1+x}$ et $x \neq y$.
Comme $\dfrac{x}{1+y} = \dfrac{y}{1+x}$ alors $x(1+x) = y(1+y)$ donc $x + x^2 = y + y^2$ d'où $x^2 - y^2 = -x + y$ donc $(x-y)(x+y) = -(x-y)$.
Comme $x \neq y$ alors $x-y \neq 0$ et donc en divisant par $x-y$ on obtient $x+y = -1$ c'est une contradiction (la somme de deux nombres positifs est positive)
Conclusion: $\forall x, y \in \mathbb{R}^+$, si $\dfrac{x}{1+y} = \dfrac{y}{1+x}$ alors $x = y$. ■

1.3.5 Contre exemple

Par contre exemple pour montrer que "$\forall x \in E$, $P(x)$" est fausse, il suffit de trouver $x \in E$ tel que $P(x)$ soit fausse.

Exemple 1.9 *Montrer que "tout entier positif est somme de trois carrés"*

Preuve. Considérons l'entier $n = 7$, les carrés inferieurs à 7 sont 0, 1, 4 mais $0+1+4 \neq 7$.
■

1.3.6 Récurrence

Le principe de "récurrence" permet de montrer qu'une proposition $P(n)$ dépend de n, est vraie pour tout $n \in \mathbb{N}$.

La démonstration par récurrence se déroule en trois étapes :

1) "L'initialisation": on verifie que $P(0)$ est vraie,

2) "L'hérédité": on suppose $n > 0$ donné avec $P(n)$ vraie, et on démontre alors que la proposition $P(n+1)$ au rang suivant est vraie.

3) La conclusion: on rappelle que par le principe de récurrence $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

Exemple 1.10 *Montrer que* $\forall n \in \mathbb{N}, \sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

Preuve. 1- l'initialisation : pour $n = 0$, on $0^2 = 0$, alors $P(0)$ est vraie

2- l'hérédité :pour $n > 0$, on suppose que $\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$ est vraie, et on montre que $\sum_{k=0}^{n+1} k^2 = \frac{(n+1)(n+2)(2n+3)}{6}$ est vraie.

$P(n)$ est vraie alors $\sum_{k=0}^{n} k^2 = 0^2 + 1^2 + 2^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}$,

On a $\sum_{k=0}^{n+1} k^2 = 0^2 + 1^2 + 2^2 + ... + n^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2$

$= \frac{n(n+1)(2n+1) + 6(n+1)(n+1)}{6}$

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

D'où $P(n+1)$ est vraie

3- Conclusion: $\forall n \in \mathbb{N}, \sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$. ■

1.4 Exercices

Exercice 1.1 *Soient les quatre assertions suivantes :*

a) $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y \succ 0$,

b) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y \succ 0$.

c) $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y \succ 0$,

d) $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, y^2 \succ x$.

1) Les assertions a, b, c, d, sont-elles vraies ou fausses ? Donner leur négation.

2) Soient P, Q, et R trois assertions, vérifier en dressant la table de vérité :

a) $P \wedge (Q \vee R) \Longleftrightarrow (P \wedge Q) \vee (P \wedge R)$, *b)* $\overline{(P \Longrightarrow Q)} \Longleftrightarrow P \wedge \overline{Q}$.

Solution 1.1 *a) est fausse puisque sa négation est* $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y \leq 0$, *est vraie. Etant donné* $x \in \mathbb{R}$, *il existe toujours* $y \in \mathbb{R}$, *tel que* $x + y \leq 0$, *par exemple on peut prendre* $y = -(x+1)$ *et alors* $x + y = x - x - 1 = -1 \leq 0$.

b) est vraie, pour un x donné on peut prendre par exemple $y = -x + 1$, *et alors* $x + y = 1 \succ 0$. *La négation de b) est* $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y \leq 0$.

c) est fausse par exemple $x = -1$, $y = 0$. *La négation est* $\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y \leq 0$.

d) est vraie, on peut prendre $x = -1$, *la négation est* $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y^2 \leq x$.

Exercice 1.2 *Soient f et g deux fonctions de* $\mathbb{R}$ *dans* $\mathbb{R}$. *Traduire en termes de quantificateurs les expressions suivantes*

1) f est majorée ; 2) f est bornée ; 3) f est paire ; 4) f ne s'annule jamais ; 5) f est périodique

;

6) f est croissante ; 7) f n'est pas la fonction nulle ; 8) f atteint toutes les valeurs de $\mathbb{N}$.

Solution 1.2 *1)* $\exists M \in \mathbb{R}, \forall x \in \mathbb{R}, f(x) \leq M$.

2) $\exists M \in \mathbb{R}, \exists m \in \mathbb{R}, \forall x \in \mathbb{R}, m \leq f(x) \leq M$.

3) $\forall x \in \mathbb{R}, f(x) = f(-x)$.

4) $\forall x \in \mathbb{R}, f(x) \neq 0$.

5) $\exists a \in \mathbb{R}^*, \forall x \in \mathbb{R}, f(x+a) = f(x)$.

6) $\forall (x,y) \in \mathbb{R}^2, x \leq y \Longrightarrow f(x) \leq f(y)$.

7) $\exists x \in \mathbb{R}, f(x) \neq 0$.

8) $\forall n \in \mathbb{N}, \exists x \in \mathbb{R},\ f(x) = n$.

Exercice 1.3 *Soit $f : \mathbb{R} \to \mathbb{R}$ Quelle différence de sens ont les deux assertions proposées :*

a) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R},\ y = f(x)$ *et* $\exists y \in \mathbb{R}, \forall x \in \mathbb{R},\ y = f(x)$.

b) $\forall y \in \mathbb{R}, \exists x \in \mathbb{R},\ y = f(x)$ *et* $\exists x \in \mathbb{R}, \forall y \in \mathbb{R},\ y = f(x)$.

c) $\forall x \in \mathbb{R}, \exists M \in \mathbb{R},\ f(x) \leq M$ *et* $\exists M \in \mathbb{R}, \forall x \in \mathbb{R},\ f(x) \leq M$.

Solution 1.3 *a) La première assertion est verifiée par toute application, la seconde signifie que f est constante.*

b) La première assertion signifie que f prend toute valeur dans $\mathbb{R}$, la seconde est absurde.

c) La première assertion est toujours verifiée, la seconde signifie que f est majorée.

Exercice 1.4 *Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction continue.*

On considère les assertions suivantes:

P : "$\forall x \in \mathbb{R}, f(x) = 0$"

Q : "$\exists x \in \mathbb{R}, f(x) = 0$"

R : "$(\forall x \in \mathbb{R}, f(x) \succ 0)$ *ou* $(\forall x \in \mathbb{R}, f(x) \prec 0)$"

Parmi les implications suivantes les quelles sont vraies?

a) $P \Longrightarrow Q$, *b)* $Q \Longrightarrow P$, *c)* $Q \Longrightarrow R$

d) $\overline{R} \Longrightarrow Q$, *e)* $\overline{Q} \Longrightarrow \overline{P}$, *f)* $\overline{P} \Longrightarrow \overline{R}$.

Solution 1.4 *seulement les assertions: a) d) e) sont vraies.car :*

a) $(\forall x \in \mathbb{R}, f(x) = 0) \Longrightarrow (\exists x \in \mathbb{R}, f(x) = 0)$.

d) $[(\exists x \in \mathbb{R}, f(x) \leq 0)$ *et* $(\exists x \in \mathbb{R}, f(x) \geq 0)] \Longrightarrow [\exists x \in \mathbb{R}, f(x) = 0]$.

e) $(\forall x \in \mathbb{R}, f(x) \neq 0) \Longrightarrow (\exists x \in \mathbb{R}, f(x) \neq 0)$. *(la contraposé de a))*

Exercice 1.5 *Ecrire les contraposées des implications suivantes et les démontrer.*

$\forall n \in \mathbb{N}$, $\forall x, y \in \mathbb{R}$

1). n premier $\Longrightarrow n = 2$ *ou n est impair,*

2) $x \neq y \Longrightarrow (x+1)(y-1) \neq (x-1)(y+1)$.

Solution 1.5 *1) n paire,* $n \neq 2 \Longrightarrow n$ *non premier*
si n est paire, $n \neq 2$ *alors* 2 *divise n et n n'est pas premier.*
2) $(x+1)(y-1) = (x-1)(y+1) \Longrightarrow x = y$.
si $(x+1)(y-1) = (x-1)(y+1)$ *alors en dévellopant:* $-x + y = x - y$, *d'où* $2y = 2x$, *ainsi* $x = y$.

Exercice 1.6 *1) Soit* $n \geq 2$ *un entier. Montrer par l'absurde que, si n n'est pas premier, il admet un diviseur premier p qui est inférieur ou égal à* $\sqrt{n}$.
2). A l'aide de ce critère, déterminer si les nombres 89, 167 *sont premiers.*

Solution 1.6 *1) Soit n non premier, supposons que n n'a pas de diviseur premier* $p \leq \sqrt{n}$.
n *non premier*$\Longrightarrow \exists a, b \geq 2$, $n = ab$, *tout nombre* $x \geq 2$ *a un diviseur premier* $\leq x$.
Si $a \leq \sqrt{n}$ *ou* $b \leq \sqrt{n}$, *cela donne une contradiction, donc* $a \succ \sqrt{n}$ *et* $b \succ \sqrt{n}$, *ce qui implique* $n \succ n$. (*absurde*)
2) $\bullet\sqrt{89} \simeq 9.4$, *le nombre* 89 *n'est pas divisible par* $2, 3, 5$ *ou* 7, *donc* 89 *est premier.*
$\bullet$ $\sqrt{167} \simeq 12.9$, *le nombre* 167 *n'est pas divisible par* $2, 3, 5, 7$ *ou* 11 *donc* 167 *est premier.*

Exercice 1.7 *1) Soit* $n \in \mathbb{N}$, *Montrer que soit* 4 *divise* n^2, *soit* 4 *divise* $n^2 - 1$.
2) Montrer que pour tout $n \in \mathbb{N}$, $n^3 - n$ *est divisible par* 6.
3) Montrer par récurrence que $\forall n \in \mathbb{N} - \{0, 1, 2, 3\}$, $n^2 \leq 2^n$.

Solution 1.7 *1) (raisonnement cas par cas)*
Si $n = 2k$ *(paire) alors,* 4 *divise* $n^2 = 4k^2$.
Si $n = 2k + 1$ *(impaire) alors,* 4 *divise* $n^2 - 1 = 4\left(k^2 + k\right)$
2) (raisonnement cas par cas)
On a $n^3 - n = n\left(n^2 - 1\right)$.
n *paire* $\Longrightarrow n^3 - n$ *multiple de* 2.
n *impaire* $\Longrightarrow n^2 - 1$ *paire et* $n^3 - n$ *multiple de* 2.
n *multiple de* $3 \Longrightarrow n^3 - n$ *multiple de* 3
$n = 3k + 1 \Longrightarrow n^2 - 1 = 3\left(3k^2 + 2k\right)$ *multiple de* $3 \Longrightarrow n^3 - n$ *multiple de* 3
$n = 3k + 2 \Longrightarrow n^2 - 1 = 3\left(3k^2 + 4k + 1\right)$ *multiple de* $3 \Longrightarrow n^3 - n$ *multiple de* 3
Dans les 3 cas, $n^3 - n$ *est multiple de* 3.
$n^3 - n$ *est divisible par* 2 *et* 3 *qui sont premiers entre eux donc* $n^3 - n$ *est divisible par* 6.
3) (Par réccurence) :
$\bullet$ *pour* $n = 4$, $4^2 = 16 = 2^4$. *(la propriété est vraie)*
$\bullet$ *on suppose que* $n^2 \leq 2^n$ *avec* $n \geq 4$,
($n \succ 2$ *on a* $2n \prec n^2 - 1$*), d'où:*
$(n+1)^2 = n^2 + 2n + 1 \leq n^2 + n^2 \leq 2 \times 2^n = 2^{n+1}$.
la propriété est vraie au rang $n + 1$

Chapitre 2

Ensembles et applications

2.1 Ensemles

Définition 2.1 *Un ensemble est un collection d'éléments, exemple* $\{0,\ 1\}$, $\mathbb{N}$,.....

- *l'ensemble vide est un ensemble ne contenant aucun élément, noté* $\emptyset$
- *On nôte* $x \in E$, *si* x *est un élément de* E, *et* $x \notin E$ *dans le cas contraire*

2.1.1 Opérations sue les ensembles

- **Inclusion:**

  $E \subset F$, si tout élément de E est un élément de F

  Autremendit: $\forall x \in E$, $x \in F$. Et on dit alors que E est un sous ensemble de F, (E est une partie de F)

- **L'égalité**

  $E = F \Longleftrightarrow E \subset F$ et $F \subset E$

- **Ensemble des parties de** E :

  On nôte $P(E)$ l'ensemble des parties de E

  Par exemple si $E = \{1, 2, 3\}$, alors $P(E) = \{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, E, \emptyset\}$

  Si $card(E) = n$ alors, $card(P(E)) = 2^n$.

- **Différence et différence symetrique**

  Soient A et B deux sous-ensembles d'un ensemble E. On note

  1 – la différence de A et B est l'ensemble : $A \backslash B = \{x \in A \mid x \notin B\}$.

  2 – la différence symétrique de A et B est l'ensemble $A \triangle B = (A \cup B) \backslash (A \cap B)$.

• **Complémentaire d'un ensemble**

si $A \subset E$, alors le complementaire de A dans E est noté par $\complement_E A$, définie par

$$\complement_E A = \{x \in E \ / \ x \notin A\}$$

On le note aussi $E \backslash A$ ou A^c, ou $\overline{A}$.

• **Intersection et Union**

1− On appelle intersection de A et B, l'ensemble, noté $A \cap B$, des éléments de A appartenant aussi à B.

2- On appelle réunion de A et B, l'ensemble, noté $A \cup B$, des éléments de A et de ceux de B.

Formellement, on a :

$$\begin{aligned} A \cap B &= \{x/(x \in A) \wedge (x \in B)\}. \\ A \cup B &= \{x/(x \in A) \vee (x \in B)\}. \end{aligned}$$

• **Produit cartésien**

Le produit cartésien des ensembles E et F est l'ensemble des couples (x, y) où $x \in E$ et $y \in F$,

$$E \times F = \{(x, y) \mid \ x \in E \text{ et } y \in F\}$$

Si $card\,(E) = n$, $card\,(F) = m$ alors, $card\,(E \times F) = nm$.

Proposition 2.1 *Soient A, B, C des parties de E alors,*

1. $A \cap B = B \cap A$, $A \cup B = B \cup A$,

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

3. $A \cap \emptyset = \emptyset$, $A \cap A = A$, $A \cup \emptyset = A$, $A \cup A = A$,

4. $A \cap B = A \Longleftrightarrow A \subset B$,

5. $A \cup B = B \Longleftrightarrow A \subset B$,

6. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,

7. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,

8. $\complement_E \left(\complement_E A\right) = A$,

9. $\complement_E (A \cap B) = \complement_E A \cup \complement_E B$,

10. $\complement_E (A \cup B) = \complement_E A \cap \complement_E B$,

11. $A \subset B \Longleftrightarrow \complement_E B \subset \complement_E A$.

Preuve. 8. Soit $x \in E$, alors $x \in \complement_E A \left(\complement_E A\right) \Longleftrightarrow x \notin \complement_E A$
$\Longleftrightarrow \overline{x \in \complement_E A}$

$\Longleftrightarrow \overline{x \notin A}$

$\Longleftrightarrow x \in A$

Donc $\complement_E A\left(\complement_E A\right) = \complement_E A$

9. Soit $x \in E$, alors $x \in \complement E(A \cap B) \Longleftrightarrow x \notin (A \cap B)$

$\Longleftrightarrow (x \notin A) \vee (x \notin B)$

$\Longleftrightarrow (x \in \complement_E A) \vee (x \in \complement_E B)$

$\Longleftrightarrow x \in (\complement_E A \cup \complement_E B)$

Donc $\complement_E(A \cap B) = \complement_E A \cup \complement_E B$

De même on montre la propriété 10.

11. $A \subset B \Longleftrightarrow \forall x \in E\ ((x \in A) \Longrightarrow (x \in B))$

$\Longleftrightarrow \forall x \in E\ ((x \notin B) \Longrightarrow (x \notin A))$ Contrapposée de l'implication

$\Longleftrightarrow \forall x \in E\ \left((x \in \complement_E B) \Longrightarrow (x \in \complement_E A)\right)$

$\Longleftrightarrow \complement_E B \subset \complement_E A$, donc $A \subset B \Longleftrightarrow \complement_E B \subset \complement_E A$ ■

Remarquez que l'on repasse aux éléménts pour les preuves.

2.2 Les applications

Définition 2.2 *Une application ou une fonction $f : E \longrightarrow F$, est une relation qui associe à chaque élément $x \in E$, un unique élément de F noté $f(x)$.*

• *f, g deux applications, $f = g \Longleftrightarrow \forall x \in E,\ f(x) = g(x)$.*

• *Le graphe de l'application $f : E \longrightarrow F$ est l'ensemble noté G_f définie par*

$$G_f = \{(x, f(x)) \in E \times F \ /\ x \in E\}$$

• *La Composition de deux applications f et g telles que $f : E \longrightarrow F$ et $g : F \longrightarrow G$ est lapplication $g \circ f : E \longrightarrow G$ définie par*

$$g \circ f(x) = g(f(x))$$

Exemple 2.1 *Soient $f :]0, +\infty[\longrightarrow]0, +\infty[$ et $g :]0, +\infty[\longrightarrow \mathbb{R}$ tels que $f(x) = \dfrac{1}{x}$, $g(x) = \dfrac{x-1}{x+1}$.*

Alors

$$\begin{array}{rccc} g \circ f :]0, +\infty[& & \longrightarrow & \mathbb{R} \\ x & & \mapsto & g(f(x)) \end{array}$$

$$g(f(x)) = g\left(\frac{1}{x}\right) = \frac{\frac{1}{x} - 1}{\frac{1}{x} + 1} = \frac{1-x}{1+x} = -g(x).$$

Remarque 2.1 *Le composé de deux applications n'est pas toujours définies, par exemple $g \circ f$ est défini si l'ensemble d'arrivée de f est l'ensemble de départ de g.*

2.2.1 Image directe , Image réciproque

Définition 2.3 • *Soit $A \subset E$, et $f : E \longrightarrow F$ une application, l'image directe de A par f est l'ensemble*

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

c-à-d:

$$y \in f(A) \Longleftrightarrow \exists x \in A, y = f(x)$$

• *Soit $B \subset F$, et $f : E \longrightarrow F$ une application, l'image réciproque de B par f est l'ensemble*

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

c-à-d:

$$x \in f^{-1}(B) \Longleftrightarrow f(x) \in B$$

Exemple 2.2 *Soit* $\begin{array}{ccc} f : \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \mapsto & x^2 \end{array}$

alors:

$f(\{2\}) = \{4\}, \quad f([-1,3]) = \{f(x) \ / \ x \in [-1,3]\} = [0,9]$

$f([-1,0] \cup [1,3]) = [0,9]$

$f^{-1}(\{2\}) = \{x \in \mathbb{R} \ / \ f(x) \in \{2\}\} = \left\{-\sqrt{2}, \ \sqrt{2}\right\}$

$f^{-1}([0,3]) = \left\{x \in \mathbb{R} \ / \ x^2 \in [0,3]\right\} = \left[-\sqrt{3}, \sqrt{3}\right]$

$f^{-1}([-1,3]) = \left[-\sqrt{3}, \sqrt{3}\right]$

$f^{-1}([-1,0] \cup [1,3]) = \{0\} \cup \left[-\sqrt{3}, \ -1\right] \cup \left[1, \sqrt{3}\right]$

$f^{-1}(\mathbb{R}^+) = \mathbb{R}, \qquad f^{-1}\left(\mathbb{R}^*_-\right) = \emptyset$

Remarque 2.2 • *$f(A)$ est un sous ensemble de F, $f^{-1}(B)$ est un sous ensemble de E*

• *La notation $f^{-1}(B)$ est un tout rien ne dit que f est bijective, l'image réciproque existe quelque soit la fonction.*

• *L'image directe d'un singleton $f(\{x\}) = \{f(x)\}$ est un singleton, par contre l'image réciproque d'un singleton $f^{-1}(\{y\})$ dépond de f, elle peut être un singleton, un ensemble à plusieurs éléments, peut être E si f est une fonction constante.*

Proposition 2.2 *Soit $f : E \longrightarrow F$ une application, A, $A^{'}$ des parties de E, B, $B^{'}$ des partie de F*

1. $A \subset A^{'} \Longrightarrow f(A) \subset f\left(A^{'}\right)$,
2. $B \subset B^{'} \Longrightarrow f^{-1}(B) \subset f^{-1}\left(B^{'}\right)$,
3. $f\left(A \cap A^{'}\right) \subset f(A) \cap f\left(A^{'}\right)$,
4. $f\left(A \cup A^{'}\right) = f(A) \cup f\left(A^{'}\right)$,
5. $f^{-1}\left(B \cap B^{'}\right) = f^{-1}(B) \cap f^{-1}\left(B^{'}\right)$,

6. $f^{-1}\left(B \cup B^{'}\right) = f^{-1}(B) \cup f^{-1}\left(B^{'}\right)$,
7. $A \subset f^{-1}(f(A))$,
8. $f\left(f^{-1}(B)\right) \subset B$.

Preuve. 1. Soit $y \in f(A)$, alors $\exists x \in A$, $y = f(x)$, comme $A \subset A^{'}$ alors, $x \in A^{'}$, alors $y \in f\left(A^{'}\right)$, donc $f(A) \subset f\left(A^{'}\right)$.
2. Soit $x \in f^{-1}(B)$, alors $f(x) \in B$, comme $B \subset B^{'}$, alors $f(x) \in B^{'}$, alors $x \in f^{-1}\left(B^{'}\right)$, d'où $f^{-1}(B) \subset f^{-1}\left(B^{'}\right)$.
3. Soit $y \in f\left(A \cap A^{'}\right)$, il existe $x \in A \cap A^{'}$ tel que $y = f(x)$, or $x \in A$ donc $y = f(x) \in f(A)$ et de même $x \in A^{'}$ donc $y \in f\left(A^{'}\right)$. D'où $y \in f(A) \cap f\left(A^{'}\right)$ donc $f\left(A \cap A^{'}\right) \subset f(A) \cap f\left(A^{'}\right)$.
4. Soit $y \in f\left(A \cup A^{'}\right)$, $\exists x \in A \cup A^{'}$ tel que $y = f(x)$, si $x \in A$ alors $y \in f(A)$, sinon $x \in A^{'}$ et $y \in f\left(A^{'}\right)$, dans les deux cas $y \in f(A) \cup f\left(A^{'}\right)$
inversement: soit $y \in f(A) \cup f\left(A^{'}\right)$, si $y \in f(A)$ alors $\exists x \in A$ tel que $y = f(x)$. or $x \in A \subset \left(A \cup A^{'}\right)$ donc $y \in f\left(A \cup A^{'}\right)$. de même si $y \in f\left(A^{'}\right)$ par double inclusion on a l'égalité.
5. Soit $x \in f^{-1}\left(B \cap B^{'}\right)$, alors $f(x) \in \left(B \cap B^{'}\right)$, donc $f(x) \in B$ et $f(x) \in B^{'}$, donc $x \in f^{-1}(B)$ et $x \in f^{-1}\left(B^{'}\right)$, donc $x \in f^{-1}(B) \cap f^{-1}\left(B^{'}\right)$, alors $f^{-1}\left(B \cap B^{'}\right) = f^{-1}(B) \cap f^{-1}\left(B^{'}\right)$
6. démontré comme -5-.
7. Soit $x \in A$, Posons $B = f(A)$, on a $f(x) \in B$ donc $x \in f^{-1}(B) = f^{-1}(f(A))$, d'où $f(A) \subset f^{-1}(f(A))$.
8. Soit $y \in f\left(f^{-1}(B)\right)$, posons $A = f^{-1}(B)$, on a $y \in f(A)$ donc $\exists x \in A$, $y = f(x)$, comme $x \in A = f^{-1}(B)$, on a $f(x) \in B$, donc $y \in B$, alors $f\left(f^{-1}(B)\right) \subset B$. ■

Définition 2.4 ***Antécédent***
Fixons $y \in F$, tout élément $x \in E$ tel que $f(x) = y$ est un antécédent de y
• *En terme d'image réciproque, l'ensemble des antécédents de y est $f^{-1}(\{y\})$.*

2.2.2 Injection, surjection, bijection

Définition 2.5 *Soit $f : E \longrightarrow F$ une application,*
• *f est injective, si tout élément de l'ensemble d'arrivée a au plus un antécédent par f.*
• *f est surjective, si tout élément de l'ensemble d'arrivée a au moins un antécédent par f.*
• *f est bijective, si tout élément de l'ensemble d'arrivée a un unique antécédent par f.*

Cette définition peut se reformuler comme:

Définition 2.6 • *f est injective, si pour tout $y \in F$, l'équation $f(x) = y$ a au plus une solution dans E.*

- *f est surjective, si pour tout $y \in F$, l'équation $f(x) = y$ a au moins une solution dans E.*
- *f est bijective, si pour tout $y \in F$, l'équation $f(x) = y$ a une unique solution dans E.*

Autremendit f est bijective, si elle est injective et surjective.

Proposition 2.3 *Soit $f : E \longrightarrow F$ une application, les assertions suivantes sont équivalentes:*

- *1.f est injective* $\Longleftrightarrow \forall x_1, x_2 \in E;\ f(x_1) = f(x_2) \Longrightarrow x_1 = x_2$,
- *2. f est injective* $\Longleftrightarrow \forall x_1, x_2 \in E;\ x_1 \neq x_2 \Longrightarrow f(x_1) \neq f(x_2)$.
- *1.f est surjective* $\Longleftrightarrow \forall y \in F, \exists x \in E;\ y = f(x)$
- *2.f est surjective* $\Longleftrightarrow f(E) = F$
- *f est bijective* $\Longleftrightarrow \forall y \in F, \exists! x \in E;\ y = f(x)$.

Le symbole ! exprime l'unicité, c-à-d: il existe une solution unique pour l'équation $f(x) = y$.

Exemple 2.3 *Soient les applications $f_1 : \mathbb{N} \longrightarrow \mathbb{R}$, $f_2 : \mathbb{R}^+ \longrightarrow \mathbb{R}$, $f_3 : \mathbb{R} \longrightarrow \mathbb{R}^+$, telles que $f_1(x) = \dfrac{1}{1+x}$, $f_2(x) = x^2$, $f_3(x) = x^2$.*
Les applications f_1, f_2, f_3 sont elles injectives, surjectives, bijectives?

Preuve. 1. $f_1 : \mathbb{N} \longrightarrow \mathbb{R}$, $f_1(x) = \dfrac{1}{1+x}$

- $\forall x_1, x_2 \in \mathbb{N};\ f_1(x_1) = f_1(x_2) \Longrightarrow \dfrac{1}{1+x_1} = \dfrac{1}{1+x_2}$,

$\Longrightarrow x_1 = x_2$,

Donc f_1 est injective.

- $\forall y \in \mathbb{R}$, $\dfrac{1}{1+x} = y \Longrightarrow x = \dfrac{1-y}{y}$, par exemple pour $y = 5$, on obtient $x = \dfrac{-4}{5} \notin \mathbb{N}$, alors f_1 n'est pas surjective.

par conséquence f_1 n'est pas bijective.

2. $f_2 : \mathbb{R}^+ \longrightarrow \mathbb{R}$, $f_2(x) = x^2$

- $\forall x_1, x_2 \in \mathbb{R}^+;\ f_2(x_1) = f_2(x_2) \Longrightarrow x_1^2 = x_2^2$

$\Longrightarrow x_1 = \pm x_2$

$\Longrightarrow x_1 = x_2$, ($x_1, x_2$ ont même signe)

Alors f_2 est injective.

- $\forall y \in \mathbb{R};\ x^2 = y \Longrightarrow x = \pm\sqrt{y}$, si $y \geq 0$, alors pour $y \in \mathbb{R}^-$, $x \nexists$, d'où f_2 n'est pas surjective.

par conséquence f_2 n'est pas bijective.

3. $f_3 : \mathbb{R} \longrightarrow \mathbb{R}^+$, $f_3(x) = x^2$

- $\forall x_1, x_2 \in \mathbb{R}^+;\ f_2(x_1) = f_2(x_2) \Longrightarrow x_1^2 = x_2^2$

$\Longrightarrow x_1 = \pm x_2$,

alors, $\exists 2, -2 \in \mathbb{R}$, $2 \neq -2$ mais $(2)^2 = (-2)^2$, donc f_3 n'est pas injective.

- $\forall y \in \mathbb{R}^+$, $x^2 = y \Longrightarrow x = \pm\sqrt{y}$, si $y \geq 0$,

alors $\forall y \in \mathbb{R}^+, \exists x \in \mathbb{R};\ y = f_3(x)$. donc f_3 est surjective

par conséquence f_3 n'est pas bijective. ■

Proposition 2.4 *Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$, alors*

1. f injective et g injective$\Longrightarrow g \circ f$ injective,

2. f surjective et g surjective$\Longrightarrow g \circ f$ surjective,

3. $g \circ f$ injective$\Longrightarrow f$ injective,

4. $g \circ f$ surjective$\Longrightarrow g$ surjective.

Preuve. 1. Soient $x_1, x_2 \in E$, alors :$x_1 \neq x_2 \Longrightarrow f(x_1) \neq f(x_2)$ car f injective
$\Longrightarrow g(f(x_1)) \neq g(f(x_2))$ car g injective
$\Longrightarrow g \circ f(x_1) \neq g \circ f(x_2)$ ce qui montre que $g \circ f$ est injective.
2. Soit $z \in G$, g étant surjective, il existe $y \in F$ tel que $z = g(y)$, comme $y \in F$ et f est surjective alors il existe $x \in E$ tel que $y = f(x)$, donc $z = g(f(x))$ et on déduit que : $\forall z \in G, \exists x \in E; z = g \circ f(x)$, ce qui montre que $g \circ f$ est surjective.
3. $\forall x_1, x_2 \in E;\ f(x_1) = f(x_2) \Longrightarrow g(f(x_1)) = g(f(x_2))$ (car g : une application)
$\Longrightarrow (g \circ f)(x_1) = (g \circ f)(x_2)$
$\Longrightarrow x_1 = x_2$ (car $g \circ f$ est injective), d'où f est injective.
4. Soit $z \in G$, alors $g \circ f$ surjective $\Longrightarrow \exists x \in E;\ g \circ f(x) = z$
$\Longrightarrow \exists x \in E;\ g(f(x)) = z$
$\Longrightarrow \exists y = f(x) \in F;\ g(y) = z$,
donc $\forall z \in G, \exists y \in F;\ g(y) = z$, ce qui montre que g est surjective. ■

2.2.3 L'application réciproque

Proposition 2.5 *Une application $f : E \longrightarrow F$ est bijective si et seulement s'il existe une unique application $g : F \longrightarrow E$ telle que*

$$f \circ g = Id_F \text{ et } g \circ f = Id_E.$$

On dit que f est inversible et g, notée f^{-1}, est appelée "l'application réciproque" ou "l'application inverse" de f.

Preuve. I.) Supposons qu'il existe une application $g : F \longrightarrow E$ telle que $f \circ g = Id_F$ et $g \circ f = Id_E$.
Montrons que f est bijective.
1. Soit $y \in F$, comme $f \circ g = Id_F$ alors $f \circ g(y) = y$, par suite il existe $x = g(y) \in E$ tel que $f(x) = y$, ce qui montre que f est surjective.
2. Soient $x_1, x_2 \in E$, comme $g \circ f = Id_E$ alors $g \circ f(x_1) = x_1$ et $g \circ f(x_2) = x_2$, par suite:
$f(x_1) = f(x_2) \Longrightarrow g(f(x_1)) = g(f(x_2))$ (car g application)
$\Longrightarrow g \circ f(x_1) = g \circ f(x_2)$
$\Longrightarrow x_1 = x_2$, ce qui montre que f est injective.

De 1. et 2. on déduit que f est bijective.

II.) Supposons que f est bijective. Construisons l'unique application $g : F \longrightarrow E$,
telle que $f \circ g = Id_F$ et $g \circ f = Id_E$.
f étant bijective, alors : $\forall y \in F$, $\exists! x \in E$; $y = f(x)$.
Ainsi, à tout élément $y \in F$, on fait associer un unique élément $x \in E$, qu'on notera $g(x)$, tel que $f(x) = y$. On définit ainsi une application

$$g : F \longrightarrow E$$
$$y \mapsto g(y) = x$$

Montrons que $f \circ g = Id_F$ et $g \circ f = Id_E$..
1. Soit $y \in F$, alors $g(y) = x$, avec $f(x) = y$, donc $f \circ g(y) = f(g(y)) = f(x) = y$, ce qui montre que : $f \circ g = Id_F$.
2. Soit $x \in E$, alors pour $y = f(x)$ on a $g(y) = x$, par suite $g \circ f(x) = g(f(x)) = g(y) = x$, ce qui montre que : $g \circ f = Id_E$.
3. Montrons l'unicité de g. Soit $g_1 : F \longrightarrow E$ vérifiant les deux propriétés précédentes,
alors pour tout $y \in F$, il existe $x \in E$ tel que $y = f(x)$, donc $g_1(y) = g_1(f(x)) = g_1 \circ f(x) = Id_E(x) = g \circ f(x) = g(f(x)) = g(y)$
ce qui montre que $g_1 = g$. ■

Exemple 2.4 *$f : \mathbb{R} \longrightarrow]0, +\infty[$ définie par $f(x) = exp(x)$ est bijective, sa bijection réciproque est $g :]0, +\infty[\longrightarrow \mathbb{R}$ définie par $g(y) = ln(y)$. Nous avons bien $exp\,(ln(y)) = y$, pour tout $y \in]0, +\infty[$ et $ln\,(exp(x)) = x$ pour tout $x \in \mathbb{R}$.*

Proposition 2.6 *Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$ des applications bijectives. L'application $g \circ f$ est bijective et sa bijection réciproque est*

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

Preuve. D'après la proposition 2.5, il existe $u : F \longrightarrow E$ tel que $u \circ f = id_E$ et$f \circ u = id_F$.
Il existe aussi $v : G \longrightarrow F$ tel que $v \circ g = id_F$ et $g \circ v = id_G$.
On a alors $(g \circ f) \circ (u \circ v) = g \circ (f \circ u) \circ v = g \circ id_F \circ v = g \circ v = id_E$.
Et $(u \circ v) \circ (g \circ f) = u \circ (v \circ g) \circ f = u \circ id_F \circ f = u \circ f = id_E$.
Donc $g \circ f$ est bijective et son inverse est $u \circ v$.
Comme u est la bijection réciproque de f et v celle de g alors : $u \circ v = f^{-1} \circ g^{-1}$. ■

2.2.4 Prolongement et restriction

Définition 2.7 *Soit $f : E \longrightarrow F$ une application, soit $A \subset E$, $B \subset F$, tel que $f\,(A) \subset B$.*
On appelle restriction de f à A comme ensemble de départ et B comme ensemble d'arrivée et on nôte

$f_{|A\longrightarrow B}$ *l'application de* A *dans* B *qui à tout* x *dans* A *associe* $f(x)$.

• *Cette application a la même règle de calcul que* f*, seuls changent les ensemble de départ et d'arrivée*

Remarque 2.3 *Quand on restreint uniquement l'ensemble de départ* ($B = F$) *on utilise la notation* $f_{|A}$.

Définition 2.8 *Soient* f, g *des applications, on dit que* f *est un prolongement de* g *si* g *est un restriction de* f.

Exemple 2.5 *1. Soient* $\begin{array}{ccc} f:\mathbb{R} & \longrightarrow \mathbb{R} \\ x & \mapsto x^2 \end{array}$, $\begin{array}{ccc} g:\mathbb{R}^+ & \longrightarrow \mathbb{R}^+ \\ x & \mapsto x^2 \end{array}$

c-à-d g *est la restriction de* f *sur* $\mathbb{R}^+$, ($g = f_{|\mathbb{R}^+\longrightarrow\mathbb{R}^+}$), *on remarque que* g *est croissante et bijective, mais* f *ne l'est pas.*

2. Soient $\begin{array}{ccc} g:\mathbb{R}^* & \longrightarrow \mathbb{R} \\ x & \mapsto \dfrac{\sin x}{x} \end{array}$, $\begin{array}{ccc} f:\mathbb{R} & & \\ x & \mapsto \begin{cases} \dfrac{\sin x}{x}\ , & si\ x \neq 0 \\ 1\ , & si\ x = 0 \end{cases} \end{array}$

L'application f *est prolongement de* g. ($g = f_{|\mathbb{R}^*}$)

De plus on peut montrer que f *est continue sur* $\mathbb{R}$, *et on dit que* f *est le prolongement par continuité de* g.

2.3 Exercices

Exercice 2.1 *Soient* $A, B, C \in P(E)$, *établir:*

1) $A\backslash(B \cap C) = (A\backslash B) \cup (A\backslash C)$,

2) $A \subset B \Longleftrightarrow A \cup B = B$,

3) $A \cup B = A \cap C \Longleftrightarrow B \subset A \subset C$,

Solution 2.1 *1)* $A\backslash(B \cap C) = A \cap \complement_E(B \cap C) = \left(A \cap \complement_E B\right) \cup \left(A \cap \complement_E C\right) = (A\backslash B) \cup (A\backslash C)$

2) • ($\Longrightarrow$) *supposons* $A \subset B$, *on a toujours* $B \subset (A \cup B)$, *pour* $x \in A \cup B$ *que* $x \in A$ *ou* $x \in B$ *on a* $x \in B$, *donc* $(A \cup B) \subset B$. *ainsi* $A \cup B = B$.

• ($\Longleftarrow$) *supposons que* $A \cup B = B$. *puisque* $A \subset (A \cup B)$, *on a* $A \subset B$.

3) • ($\Longrightarrow$) *supposons que* $A \cup B = A \cap C$, *on a* $B \subset (A \cup B) = (A \cap C) \subset A \subset (A \cup B) = (A \cap C) \subset C$.

• ($\Longleftarrow$) *supposons que* $B \subset A \subset C$, $A \cup B = A = A \cap C$.

Exercice 2.2 *Soient* E, F *deux ensembles,* $f : E \to F$ *une application, démontrer que:*

1)$\forall A, B \in P(E)$, $f(A \cap B) \subset f(A) \cap f(B)$,

2) $\forall A, B \in P(E)$, $f(A \cup B) = f(A) \cup f(B)$,

3) $\forall A \in P(F)$, $f^{-1}(F\backslash A) = E\backslash f^{-1}(A)$.

Solution 2.2 *1) soit* $y \in f(A \cap B)$, *il existe* $x \in A \cap B$ *tel que* $y = f(x)$, *or* $x \in A$ *donc* $y = f(x) \in f(A)$ *et de même* $x \in B$ *donc* $y \in f(B)$. *D'où* $y \in f(A) \cap f(B)$ *donc* $f(A \cap B) \subset f(A) \cap f(B)$
2) Soit $y \in f(A \cup B)$, $\exists x \in A \cup B$ *tel que* $y = f(x)$, *si* $x \in A$ *alors* $y \in f(A)$, *sinon* $x \in B$ *et* $y \in f(B)$, *dans les deux cas* $y \in f(A) \cup f(B)$
inversement: soit $y \in f(A) \cup f(B)$, *si* $y \in f(A)$ *alors* $\exists x \in A$ *tel que* $y = f(x)$. *or* $x \in A \subset (A \cup B)$ *donc* $y \in f(A \cup B)$. *de même si* $y \in f(B)$ *par double inclusion on a l'égalité.*
3) $x \in f^{-1}(F \backslash A) \Longleftrightarrow f(x) \in F \backslash A$.
$\Longleftrightarrow f(x) \notin A$
$\Longleftrightarrow x \notin f^{-1}(A)$
$\Longleftrightarrow x \in E \backslash f^{-1}(A)$.

Exercice 2.3 *Décrire l'image directe de* $\mathbb{R}$ *par la fonction exponentielle.*
Déterminer $f([0,\ 1[)$, $f(\mathbb{R})$, $f(]-1,\ 2[)$, $f^{-1}(\{3\})$, *par la fonction* $f : x \mapsto x^2$, *définie sur* $\mathbb{R}$.

Solution 2.3 $\exp(\mathbb{R}) = \mathbb{R}^{*+}$, $\quad f([0,\ 1[) = [0,\ 1[\ ,\ \ f(\mathbb{R}) = \mathbb{R}^{+}\ \ ,\ f\,]-1,\ 2[= [0,\ 4[\ \ ,\ \ \ f^{-1}(\{3\}) = \left\{\sqrt{3},\ -\sqrt{3}\right\}$

Exercice 2.4 *Soit* $f : [1,\ +\infty[\to [0,\ +\infty[$ *une application telle que* $f(x) = x^2 - 1$, f *est elle bijective ?*

Solution 2.4 • f *est injective car : soit* $x, y \in [1,\ +\infty[$,
$f(x) = f(y) \Longrightarrow x^2 - 1 = y^2 - 1 \Longrightarrow x = \pm y$, *or* $x, y \in [1,\ +\infty[$ *donc* x, y *sont de même signe donc* $x = y$
• f *est surjective car : soit* $y \in [0,\ +\infty[$, *on cherche un élément* $x \in [1,\ +\infty[$ *tel que* $y = f(x) = x^2 - 1$, *le réel* $x = \sqrt{y+1}$ *convient*
par conclusion f *est bijective*

Exercice 2.5 *Soient* E, F, G *trois ensembles,* $f : E \to F, g : F \to G$ *et* $h : G \to E$
Etablir que si $h \circ g \circ f$ *est injective et que* $g \circ f \circ h$ *et* $f \circ h \circ g$ *sont surjectives alors,* f, g *et* h *sont bijectives.*

Solution 2.5 *on a les imlications suivantes*
1) $g \circ f$ *injective*$\Longrightarrow f$ *injective*
2) $g \circ f$ *surjective*$\Longrightarrow g$ *surjective*
Supposons que $h \circ g \circ f$ *est injective et* $g \circ f \circ h$ *ainsi que* $f \circ h \circ g$ *sont surjectives*
Puisque $(h \circ g) \circ f$ *est injective, on a* f *injective et puisque* $f \circ (h \circ g)$ *surjective, on a* f *surjective par suite* f *est bijectiveet on peut introduire* f^{-1}.
par composition $h \circ g = (h \circ g \circ f) \circ f^{-1}$ *est injective et par suite* g *est injective*
D'autre part $g \circ f \circ h$ *est surjective et donc* g *aussi, finalement* g *est bijective*
par composition $h = (h \circ g) \circ g^{-1}$ *est injective et* $h = f^{-1} \circ (f \circ h \circ g) \circ g^{-1}$ *est surjective donc* h *est bijective*

Exercice 2.6 *Soit $f:\mathbb{R}\to\mathbb{C}$, telle que $f(x)=e^{ix}$, Changer les ensembles de départ et d'arrivée afin que la restriction de f devienne bijective.*

Solution 2.6 *Considérons la restriction suivante de f :* $\begin{array}{ccc} f_1:[0,\ 2\pi[& \longrightarrow & U \\ t & \mapsto & e^{it} \end{array}$

on montre que f_1 est bijective, (ici U est le cercle d'unité de $\mathbb{C}$)

• *f_1 est surjective car tout nombre complexe de U s'écrit sous la forme exponentielle $e^{i\theta}$,et l'on peut choisir $\theta\in[0,\ 2\pi[$*

• *f_1 est injective car: $f_1(t)=f_1\left(t^{'}\right)\Longrightarrow e^{it}=e^{it^{'}}\Longrightarrow t=t^{'}+2k\pi$ avec $k\in\mathbb{Z}$*

$\Longrightarrow t=t^{'}$ car $t,t^{'}\in[0,\ 2\pi[$ et donc $k=0$.

En conclus f_1 est bijective.

Exercice 2.7 *Soient E,F,G trois ensembles,*

1) Soient $f_1,\ f_2:E\to F$ et $g:F\to G$, on suppose $g\circ f_1=g\circ f_2$ et g injective. Montrer que $f_1=f_2$.

2) Soient $f:E\to F$ et $g_1,\ g_2:F\to G$, on suppose $g_1\circ f=g_2\circ f$ et f surjective. Montrer que $g_1=g_2$.

Solution 2.7 *1) $\forall x\in E$, on a $(g\circ f_1)(x)=(g\circ f_2)(x)$, i,e: $g(f_1(x))=g(f_2(x))$ donc $f_1(x)=f_2(x)$ (car g injective) ainsi $f_1=f_2$*

2) $\forall y\in F,\exists x\in E$ tel que $y=f(x)$ et alors $g_1(y)=(g_1\circ f)(x)=(g_2\circ f)(x)=g_2(y)$ donc $g_1=g_2$.

Chapitre 3

Relations binaire sur un ensemble

Définition 3.1 *On appelle relation binaire, tout proposition entre deux objets, pouvant être vérifiée ou non. On note $x\Re y$ et on lit "x est en relation avec y".*

Exemple 3.1 • *L'inégalité $\leq$ est une relation binaire sur $\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{R}$,*
• *Le parallélisme " $\parallel$ " et l'orthogonalité " $\perp$ " sont des relations binaires sur l'ensemble des droites du plan ou de l'espace,*
• *L'inclusion $\subset$ est une relation binaire sur $P(E)$ où sur E,*
• *La relation " plus grand que" sur l'ensemble des étudiants, est une relation binaire.*

Définition 3.2 *Etant donnée une relation binaire $\Re$ entre les éléments d'un ensemble non vide E, on dit que :*
1. $\Re$ est Reflexive $\Longleftrightarrow \forall x \in E$, $x\Re x$,
2. $\Re$ est Transitive $\Longleftrightarrow \forall x, y, z \in E$, $(x\Re y) \wedge (y\Re z) \Longrightarrow (x\Re z)$
3. $\Re$ est Symétrique $\Longleftrightarrow \forall x, y \in E$, $(x\Re y) \Longrightarrow (y\Re x)$
4. $\Re$ est Anti-Symétrique $\Longleftrightarrow \forall x, y \in E$, $(x\Re y) \wedge (y\Re x) \Longrightarrow x = y$.

3.1 Relation d'équivalence

Définition 3.3 *On dit qu'une relation binaire $\Re$ sur un ensemble E est une relation d'équivalence, si elle est Réflexive, Symétrique et Transitive.*

Soit $\Re$ une relation d'équivalence sur un ensemble E.

Définition 3.4 *1. On dit que deux éléments x et $y \in E$ sont équivalents si $x\Re y$.*
2. On appelle classe d'équivalence d'un élément $x \in E$, l'ensemble : $\dot{x} = \{y \in E;\ x\Re y\}$.
3. x est dit un représentant de la calsse d'équivalence $\dot{x}$.
4. On appelle ensemble quotient de E par la relation d'équivalence $\Re$, l'ensemble des classes d'équivalence

de tous les éléments de E. Cet ensemble est noté $E_{/\Re}$.
5. $\dot{x} = \dot{y} \Longleftrightarrow x\Re y$

Exemple 3.2 ***:*** *Dans* $\mathbb{R}$ *on définit la relation* $\Re$ *par :*
$\forall x, y \in \mathbb{R},\ x\Re y \Longleftrightarrow x^2 - 1 = y^2 - 1.$
Montrer que $\Re$ *est une relation d'équivalence et donner l'ensemble quotient* $\mathbb{R}_{/\Re}$.
1. $\Re$ *est une relation d'équivalence.*
i) $\Re$ *est une relation Reflexive, car :* $\forall x \in \mathbb{R},\ x^2 - 1 = x^2 - 1 \Longrightarrow x\Re x$
ii) $\Re$ *est une relation Symétrique, car :* $\forall x, y \in R,\ x\Re y \Longrightarrow x^2 - 1 = y^2 - 1$
$\Longrightarrow y^2 - 1 = x^2 - 1$ *car l'égalité est symétrique*
$\Longrightarrow y\Re x$
iii) $\Re$ *est une relation Transitive, car :* $\forall x, y, z \in \mathbb{R}, (x\Re y) \wedge (y\Re z) \Longrightarrow (x^2 - 1 = y^2 - 1) \wedge (y^2 - 1 = z^2 - 1)$
$\Longrightarrow (x^2 - 1 = z^2 - 1)$ *car l'égalité est Transitive.*
$\Longrightarrow x\Re z$
De i) , ii) et iii) , on déduit que $\Re$ *est une relation déquivalence.*
2. Déterminer l'ensemble quotient $\mathbb{R}_{/\Re}$.
Soit $x \in \mathbb{R}$, *alors :* $\forall y \in \mathbb{R},\ x\Re y \Longleftrightarrow x^2 - 1 = y^2 - 1$
$\Longleftrightarrow x^2 - y^2 = 0$
$\Longleftrightarrow (x - y)(x + y) = 0$
$\Longleftrightarrow (y = x) \vee (y = -x)$
donc : $\dot{x} = \{x,\ -x\}$, *par suite* $\mathbb{R}_{/\Re} = \{\{x, -x\},\ x \in \mathbb{R}\}$

Exemple 3.3 *Soient* $n \in \mathbb{N}^*$ *; et* $p,\ q \in \mathbb{Z}$. *On dit que* p *est congru à* q *modulo* n, *et on note* $p \equiv q[n]$, *si* n *divise* $p - q$, *c'est-à-dire si :* $\exists k \in \mathbb{Z};\ p - q = kn$.
Par exemple, 22 *est congru à* 1 *modulo* 7, *ce que l'on note* $22 \equiv 1[7]$, *car* $22 - 1 = 21$ *est divisible par* 7.
L'entier -6 *est aussi congru à* 1 *modulo* 7*ce que l'on note* $-6 \equiv 1[7]$ *car* $-6 - 1 = -7$ *est divisible par* 7.
On vérifie facilement que "la relation de congruence modulo n*" est une relation d'équivalence sur* $\mathbb{Z}$.
On note $\dot{p}$ *la classe d'équivalence de* $p \in \mathbb{Z}$,
Par exemple, on considère "la relation de congruence modulo 7*" alors,*
$\dot{1} = \{p \in \mathbb{Z}, p \equiv 1\,[7]\}\,,$
$= \{p \in \mathbb{Z}, p - 1$ *est divisible par* $7\}\,,$
$= \{1 + k7,\ k \in \mathbb{Z}\}\,,$
$= \{..., -20, -13, -6, 1, 8, 15, 22...\}$
En générale la classe d'équivalence de p *modulo* n *est l'ensemble:*
$\dot{p} = \{p + k7,\ k \in \mathbb{Z}\}$.

D'où l'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n, noté $\mathbb{Z}/n\mathbb{Z}$,est donné par

$$\mathbb{Z}/n\mathbb{Z} = \left\{\dot{0},\ \dot{1},\ \dot{2}, ...,\ \dot{n-1}\right\}$$

C'est un sous-ensemble fini, il contient n éléments.

Proposition 3.1 *Soit $\Re$ une relation d'équivalence sur un ensemble E.*
Alors, les classes d'équivalences forment une partition de E, c'est-à-dire que
- *toute classe d'équivalence est non vide ,*
- *la réunion des classes d'équivalence est égale à E ,*
- *deux classes d'équivalence sont soient disjointes soient confondues,*

$$\forall x, y \in E,\ \dot{x} \cap \dot{y} = \emptyset \text{ ou } \dot{x} = \dot{y}$$

3.2 Relation d'ordre

Définition 3.5 *On appelle relation d'ordre sur un ensemble E toute relation binaire réflexive, anti-symétrique et transitive.*

On dit alors que $(E,\ \Re)$ est un ensemble ordonné (par $\Re$), Une relation d'ordre est souvent notée $\leq$.

Exemple 3.4 *La relations "$\subset$" est une relation d'ordre sur $P(E)$.*
1. "$\subset$" est Réflexive, car $\forall A \in P(E)$, on a $A \subset A$.
2. "$\subset$" est Transitive, car $\forall A, B, C \in P(E)$, $(A \subset B) \wedge (B \subset C) \Longrightarrow A \subset C$
3. "$\subset$" est Anti-symétrique, car $\forall A, B \in P(E)$, $(A \subset B) \wedge (B \subset A) \Longrightarrow A = B$
De 1), 2) et 3) on déduit que "$\subset$" est une relation d'ordre sur E.

Exemple 3.5 *1. Les relations "$\leq$", "$\geq$" sont des relations d'ordre sur $\mathbb{R}$.*
2. La relation "$\diagdown$" (divise) est une relation d'ordre sur $\mathbb{N}$.

3.2.1 Ordre total ou partiel

Définition 3.6 *Soit E un ensemble muni d'une relation d'ordre $\Re$.*
- *On dit que $\Re$ est une relation d'ordre total si*

$$\forall x,\ y \in E;\ x\Re y \text{ ou } y\Re x.$$

- *Dans le cas contraire, on dit que l'ordre est partiel, c'est à dire $\exists x,\ y \in E$; x n'est pas en relation avec y, et y n'est pas en relation avec x.*

Exemple 3.6 *1. Les relations "$\leq$", "$\geq$" sont des relations d'ordre total sur* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.
2. La relation "$\nmid$" (divise) est une relation d'ordre partiel sur $\mathbb{N}$.
3. La relations "$\subset$" est une relation d'ordre partiel sur $P(E)$.
▶ *par exemple soit* $E = \{1, 2, 3\}$, *alors* $P(E) = \{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, E, \emptyset\}$
alors $\exists A = \{2\} \in P(E)$, *et* $B = \{1, 3\} \in P(E)$; *mais* $A \nsubseteq B$ *et* $B \nsubseteq A$.

Plus petit élément, plus grand élément

Définition 3.7 *Soit* $(E, \leq)$ *un ensemble ordonné et* A *une partie de* E,
1. On dit que $m \in A$ *est le plus petit élément de* A *(ou un minimum)si*

$$\forall x \in A,\ m \leq x$$

2. On dit que $M \in A$ *est le plus grand élément de* A *(ou un maximum) si*

$$\forall x \in A, x \leq M$$

Proposition 3.2 ***Unicité du minimum et du maximum***
Soit $(E, \leq)$ *un ensemble ordonné et* A *une partie de* E
1. Si A *admet un minimum, il est unique : on le note* $\min A$.
2. Si A *admet un maximum, il est unique : on le note* $\max A$.

Exemple 3.7 *On définie sur* $\mathbb{Z}^*$, *la relation d'ordre* $\Re$ *suivante:*

$$\forall n, m \in \mathbb{Z}^*, n \Re m \Longleftrightarrow \exists k \in \mathbb{N},\ m = kn$$

• *le plus petit élement de* $\mathbb{Z}^*$ *par* $\Re$ *est* 1
• $\mathbb{Z}^*$ *n'admet pas un plus grand élément.*
Soit A, B *des parties de* $\mathbb{Z}^*$ *tels que,* $A = \{2, -6, -10, -14, -18, -20\}$, $B = \{7, 6, 2, 3, -42\}$
Déterminer le plus petit élément ($\min$*), le plus grand élément (*$\max$*) de* A, B *par la relation* $\Re$ *s'ils existent.*
• $\min A = 2$
• $\max A = \nexists$
• $\min B = \nexists$
• $\max B = -42$

Majorant, minorant

Définition 3.8 *Soit* $(E, \leq)$ *un ensemble ordonné et* A *une partie de* E
1. On dit que $m \in E$ *est un minorant de* A *si*

$$\forall x \in A,\ m \leq x.$$

On dit alors que A est minorée.

2. On dit que $M \in E$ est un majorant de A si

$$\forall x \in A,\ x \leq M.$$

On dit alors que A est majorée.

3 On dit que A est bornée si elle est minorée et majorée.

Borne inférieure et borne supérieure

Définition 3.9 *Soit $(E,\ \leq)$ un ensemble ordonné et A une partie de E*

1 Si l'ensemble des minorants de A admet un plus grand élément, on l'appelle borne inférieure de A et on le note $\inf A$.

2 Si l'ensemble des majorants de A admet un plus petit élément, on l'appelle borne supérieure de A et on le note $\sup A$.

Proposition 3.3

Soit $(E,\ \leq)$ un ensemble ordonné et A une partie de E

1 Si A admet un minimum, alors il admet une borne inférieure et $\min A = \inf A$.

2 Si A admet un maximum, alors il admet une borne supérieure et $\max A = \sup A$.

Remarque 3.1 • *Le plus petit élément de A ($\min A$), s'il existe est un minorant de A, par contre un minorant de A peut ne pas être le plus petit élément de A car il n'est pas nécéssairement dans A.*

• *Même pour le plus grand élément ($\max A$) et le majorant.*

Cette remarque exprime que l'implication réciproque dans la **Proposition** (3.2.2) n'est pas toujours vraie.

Exemple 3.8 *Soient $E = \{1, a, 2, 5, \gamma\}$, considérons $(P(E), \subset)$ est ordonné, et soit A une partie de $P(E)$,*

$$A = \{\{a, 2\},\ \{2, 5, \gamma\},\ \{1, 2, \gamma\},\ \{a, 2, 5\}\}$$

alors,

• *Les minorants de A sont : $\emptyset$ et $\{2\}$.*

• $\inf A = \{2\}$

3. A n'a pas de plus petit élément, car $\inf A \notin A$.

4. Le seul majorant de A est : $E = \{1, a, 2, 5, \gamma\}$

5. $\sup A = E$.

6. A n'a pas de plus grand élément, car $\sup A \notin A$.

3.3 Exercices

Exercice 3.1 *Soit P^* l'ensemble des nombres premiers strictement supérieurs à 2. On considère la relation $\Re$ entre deux éléments de P^* définie par :*

$$p\Re q \Longleftrightarrow \frac{p+q}{2} \in P^*$$

- La relation $\Re$ est-elle réflexive, symétrique et transitive ?

Solution 3.1 *1) $\forall p \in P^*$, $\frac{p+p}{2} = p \in P^* \Longrightarrow p\Re p$, donc $\Re$ est reflexive.*
2) $\forall p, q \in P^*$, $p\Re q \Longrightarrow \frac{p+q}{2} \in P^* \Longrightarrow \frac{q+p}{2} \in P^* \Longrightarrow q\Re p \Longrightarrow \Re$ symetrique.
3) $\forall p, q, r \in P^*, \begin{cases} p\Re q \\ et\ q\Re r \end{cases} \Longrightarrow \begin{cases} \frac{p+q}{2} \in P^* \\ et\ \frac{q+r}{2} \in P^* \end{cases}$
il faudrait pouvoir en déduire que $\frac{q+r}{2} \in P^*$, mais ça n'est pas toujours verifié, voici un contre exemple sous forme d'un tableau,
(dans ce tableau: la premiere ligne: les valeurs de q, la premiere colonne: les valeurs de p, et les valeurs internes sont les nombres: $\frac{p+q}{2}$)

$$\begin{bmatrix} p \diagdown q & 3 & 5 & 7 & 11 & 13 & 17 \\ 3 & 3 & 4 & 5 & 7 & 8 & 10 \\ 5 & 4 & 5 & 6 & 8 & 9 & 11 \\ 7 & 5 & 6 & 7 & 9 & 10 & 12 \\ 11 & 7 & 8 & 9 & 11 & 12 & 14 \\ 13 & 8 & 9 & 10 & 12 & 13 & 15 \\ 17 & 10 & 11 & 12 & 14 & 15 & 17 \end{bmatrix}$$

dans ce tableau on a par exemple: $11\Re 3$ *et* $3\Re 7$ *mais* 11 *n'est pas en relation avec* 7.
sur ce tableau l'exemple cité est le seul contre-exemple, pour en trouver d'autre il faudrait faire un tableau plus grand.
donc $\Re$ n'est pas transitive.

Exercice 3.2 *Soit $\Re$ une relation binaire réflexive et transitive. On définit une relation S par :*

$$xSy \Longleftrightarrow x\Re y \ et\ y\Re x.$$

- Montrer que S est une relation d'équivalence et que $\Re$ permet de définir une relation d'ordre sur les classes d'équivalences de S.

Solution 3.2 *1)- on a $x\Re x$ et $x\Re x \Longrightarrow xSx$, donc S reflexive*
si $xSy \Longrightarrow x\Re y$ et $y\Re x$.

$\Longrightarrow y\Re x$ *et* $x\Re y$

$\Longrightarrow ySx$, *donc* S *symetrique*

xSy *et* $ySz \Longrightarrow (x\Re y$ *et* $y\Re x)$ *et* $(y\Re z$ *et* $z\Re y)$

$\Longrightarrow (x\Re y$ *et* $y\Re z)$ *et* $(z\Re y$ *et* $y\Re x)$

$\Longrightarrow (x\Re z)$ *et* $(z\Re x)$ *(car* $\Re$ *est transitive)*

$\Longrightarrow xSz$, *donc* S *est transitive, alors* S *est une relation d'équivalence.*

2) On définit sur l'ensemble des classes d'équivalence de S *la relation* $\triangle$ *par:*

$$\dot{x}\triangle\dot{y} \Longleftrightarrow x\Re y.$$

La relation $\triangle$ *est bien définie reflexive et transitive*

$\cdot$ *si* $\dot{x}\triangle\dot{y}$ *et* $\dot{y}\triangle\dot{x}$ *alors* $x\Re y$ *et* $y\Re x$ *alors* xSy *donc* $\dot{x} = \dot{y}$

(d'aprés la propriétés: R *relation d'équivalence alors,* $xRy \Longleftrightarrow \dot{x} = \dot{y}$*)*

donc $\triangle$ *est antisymetrique*

alors $\triangle$ *est bien définie une relation d'ordre sur l'ensemble des classes d'équivalence de* S.

Exercice 3.3 *Soit* $\Re$ *une relation définie sur* $\mathbb{Z}\times\mathbb{N}^*$ *par :*

$$(a,b)\,\Re\left(a^{'},b^{'}\right) \Longleftrightarrow ab^{'} = a^{'}b$$

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

2) soit $(p,q)\in\mathbb{Z}\times\mathbb{N}^*$ *, avec* $p\wedge q = 1$*, décrire la classe d'équivalence de* (p,q) *.*

Solution 3.3 *1)*$\forall\,(a,b)\in\mathbb{Z}\times\mathbb{N}^*, ab = ab \Longrightarrow (a,b)\,\Re\,(a,b)$ *donc* $\Re$ *reflexive*

$\forall\,(a,b),\left(a^{'},b^{'}\right)\in\mathbb{Z}\times\mathbb{N}^*, (a,b)\,\Re\left(a^{'},b^{'}\right) \Longrightarrow ab^{'} = a^{'}b \Longrightarrow a^{'}b = ab^{'} \Longrightarrow \left(a^{'},b^{'}\right)\Re\,(a,b)$ *,donc* $\Re$ *symetrique*

$\forall\,(a,b),\left(a^{'},b^{'}\right),\left(a^{"},b^{"}\right)\in\mathbb{Z}\times\mathbb{N}^*,$

$(a,b)\,\Re\left(a^{'},b^{'}\right)$ *et* $\left(a^{'},b^{'}\right)\Re\left(a^{"},b^{"}\right)\Rightarrow$

$$\begin{cases} ab^{'} = a^{'}b \\ a^{'}b^{"} = a^{"}b^{'} \end{cases} \Rightarrow \begin{cases} a^{'} = \frac{ab^{'}}{b}, \quad car\ b\neq 0 \\ a^{'}b^{"} = a^{"}b^{'} \end{cases}$$

donc $\frac{ab^{'}}{b}b^{"} = a^{"}b^{'}$*, d'où* $ab^{"} = a^{"}b$ *i.e:* $(a,b)\,\Re\left(a^{"},b^{"}\right)$*, donc* $\Re$ *transitive, et par consequence* $\Re$ *est une relation d'équivalence*

2) si $(a,b)\in\dot{\widehat{(p,q)}} \Longleftrightarrow aq = pb$ *donc* q *divise* pb *et* $p\wedge q = 1$ *alors d'aprés le théorème de Gauss* q *divise* b*. D'où* $\exists d\in\mathbb{Z}, b = dq$*, d'où* $aq = pdq$*,* $q\neq 0$*, donc* $a = dp$

Alors $\dot{\widehat{(p,q)}} = \{(dp,dq)\,,\ d\in\mathbb{Z}\}$ *.*

Exercice 3.4 *Soit* E *l'ensemble des couples* (I,f) *formé d'un intervalle* I *et d'une fonction réelle* f *définie sur* I*. On définit une relation* $\top$ *sur* E *par :*

$$(I,f)\top(J,g) \Longleftrightarrow I\subset J \text{ et } g|_I = f.$$

- Montrer que $\top$ *est une relation d'ordre sur* E.

Solution 3.4 *la fonction* $f : I \longrightarrow \mathbb{R}$,
- $\forall (I,f) \in E,\ I \subset I, f_{|I} = f \Longrightarrow (I,f)\top(I,f)$, *donc* $\top$ *est reflexive,*
- $\forall (I,f),(J,g) \in E,\ (I,f)\top(J,g)$ *et* $(J,g)\top(I,f) \Longrightarrow (I \subset J$ *et* $g|_I = f)$ *et* $\big(J \subset I$ *et* $f_{|J} = g\big) \Longrightarrow I = J,\ f = g$. *donc* $\top$ *est antisymetrique*
- $\forall (I,f),(J,g),(K,h) \in E,\ (I,f)\top(J,g)$ *et* $(J,g)\top(K,h) \Longrightarrow (I \subset J$ *et* $g|_I = f)$ *et* $\big(J \subset K, h_{|J} = g\big)$
$\Longrightarrow I \subset J,\ h_{|I} = \big(h_{|J}\big)_{|I} = g|_I = f$. *donc* $\top$ *est transitive*

par consequence $\top$ *est une relation d'ordre sur* E.

Exercice 3.5 *On définit une relation binaire* S *sur* $\mathbb{R}_+^*$ *par :*

$$xSy \Longleftrightarrow \exists n \in \mathbb{N}, y = x^n.$$

1) Montrer que S *est une relation d'ordre. Cet ordre est-il total ?*
On considère dans la suite de l'exercice que l'ensemble est ordonné par la relation .
2) Soit $A = \{2,4,16\}$. *Déterminer le plus grand élément et le plus petit élément de* A.

Solution 3.5 *1)- soit* $x \in \mathbb{R}_+^*$, *on a* $x = x^n$ *pour* $n = 1 \in \mathbb{N}$ *donc* xSx, *alors* S *reflexive*
- *soient* $x, y \in \mathbb{R}_+^*$, *si* xSy *et* ySx, *alors* $\exists n, m \in \mathbb{N}$, *tel que* $y = x^n \wedge x = y^m$.
On a alors: $x = x^{nm}$ *donc* $\ln x = nm \ln x$ *d'où* $\ln x\,(1 - nm) = 0$.
· *si* $x = 1$ *alors* $y = x^n = 1 = x$.
· *si* $x \neq 1$, *alors* $\ln x \neq 0$, *d'où* $nm = 1$, *or* $n, m \in \mathbb{N}$, *donc* $n = m = 1$ *donc* $x = y$, *alors* S *est antisymetrique*
- *Soient* $x, y, z \in \mathbb{R}_+^*$, *si* xSy *et* ySz *alors* $\exists n, m \in \mathbb{N}$; $y = x^n$ *et* $z = y^m$.
On a $z = x^{nm}$ *avec* $n, m \in \mathbb{N}$, *donc* xSz, *donc* S *est transitive*
et par conséquence S *est une relation d'ordre.*
2) Cet ordre n'est pas total car :
$\exists\ 2, 3 \in \mathbb{R}_+^*$, 2 *n'est pas en relation avec* 3 *et* 3 *n'est pas en relation avec* 2.
Càd: $\nexists n \in \mathbb{N}, 2 = 3^n$ *et* $3 = 2^n$.
2) On considère dans la suite de l'exercice que l'ensemble est ordonné par la relation S.
Soit $A = \{2,4,16\}$ *le plus petit élément de* A *est* 2 *car :*
$4 = 2^2$ *càd* $\exists n = 2$ *tel que* $4 = 2^n \Longrightarrow 2S4$,
et $16 = 2^4$ *càd:* $\exists n = 4$ *tel que* $16 = 2^n \Longrightarrow 2S16$
et le plus grand élément de A *est* 16 *car :*
$16 = 2^4 \Longrightarrow 2S16$
et $16 = 4^2 \Longrightarrow 4S16$.

Exercice 3.6 *Soient* A *et* B *deux parties non vides et bornées de* $\mathbb{R}$ *telles que* $A \subset B$.
Comparer $\inf A$, $\sup A$, $\inf B$ *et* $\sup B$.

Solution 3.6 *A et B sont des parties non vides et bornées de $\mathbb{R}$, donc les bornes* $\sup$ *et* $\inf$ *considéeées existent*

· *pour tout $a \in A$, on a $a \in B$, donc $a \leq \sup B$,* $\sup B$ *majore A donc* $\sup A \leq \sup B$.

· *pour tout $a \in A$, on a $a \in B$, donc* $\inf B \leq a$, $\inf B$ *minore A donc* $\inf B \leq \inf A$

Enfin puisque $A \neq \varnothing$, $\inf A \leq \sup A$.

Exercice 3.7 *Soit A une partie non vide et minorée de $\mathbb{R}$. On pose*
$m = \inf A$ *et* $B = A \cap]-\infty\ ,\ m+1]$
Déterminer la borne inférieure de B.

Solution 3.7 *Puisque $m+1$ ne minore pas A, la partie B est non vide.*
De plus $B \subset A$ donc la borne inférieure de B existe et

$$\inf A \leq \inf B$$

Soit $x \in A$, si $x \leq m+1$ alors $x \in B$ et donc $x \geq \inf B$.

Si $x > m+1$ alors à nouveau $x \geq \inf B$.
Ainsi $\inf B$ *minore A et donc*

$$\inf A \geq \inf B$$

Finalement

$$\inf A = \inf B$$

Chapitre 4

Structures algébriques

4.1 Loi de composition interne

Définition 4.1 *On appelle loi de composition interne (LCI) sur un ensemble E tout application $* : E \times E \longrightarrow E$.*
Un sous ensemble F de E est dite "stable" par rapport à la loi $*$ si

$$\forall x, y \in F; x * y \in F.$$

Exemple 4.1 *1. $\cap$ et $\cup$ sont des lois de compositions internes sur $P(E)$.*
2. La somme "$+$" et le produit "$\times$" sont des LCI sur $\mathbb{N}$, $\mathbb{N}^*$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, mais pas sur $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$,
3. La difference "$-$" sur $\mathbb{R}, \mathbb{C}$.
4. La composition "$\circ$" des applications sur F^F (applications définies de F dans F).

Exemple 4.2 *Soit $E = \{1,2,3\}$, et $F = \{\{1,2\}, \{2,3\}, \{1,3\}\} \subset P(E)$*
F n'est pas stable par rapport à l'intersection $\cap$ et la réunion $\cup$ car :
$\exists \{1,2\}, \{2,3\} \in F; \{1,2\} \cap \{2,3\} = \{2\} \notin F,$
$\exists \{1,2\}, \{2,3\} \in F; \{1,2\} \cup \{2,3\} = \{1,2,3\} \notin F.$

Définition 4.2 *Soient $*$ et $\bigtriangledown$ deux lois de composition internes (LCI) sur un ensemble E, on dit que:*
1. $*$ est commutative si: $\forall x, y \in E; x * y = y * x$,
2. $*$ est associative si: $\forall x, y, z \in E; (x * y) * z = x * (y * z)$,
3. $e \in E$ est un élément neutre à gauche (respectivement à droite) de la loi $*$ si

$$\forall x \in E; \ e * x = x \text{ (respectivement } x * e = x)$$

- Si e est un élément neutre à droite et à gauche de $*$ on dit que e est un élément neutre de $*$.
4. Soit $e \in E$ est un élément neutre, on dit qu'un élément $x \in E$ est inversible, ou symetrisable, à droite (respectivement à gauche) de $*$ si

$$\exists x' \in E, \ x * x' = e \text{ (respectivement } x' * x = e)$$

x est inversible (ou symetrisable) s'il est inversible à droite et à gauche de $*$. et $x^{'}$ est dit un inverse (ou un symétrique) à droite (respectivement à gauche) de x.

5. $*$ est distributive par rapport à $\bigtriangledown$ si : $\forall x, y, z \in E$,

$$x * (y \bigtriangledown z) = (x * y) \bigtriangledown (x * z) \text{ et } (y \bigtriangledown z) * x = (y * x) \bigtriangledown (z * x).$$

6. On dit qu'un élément $r \in E$ est régulier à droite (respectivement à gauche) de Soit $*$ si

$$\forall x, y \in E;\ x \star r = y \star r \Longrightarrow x = y$$

$$(\text{respectivement } \forall x, y \in E;\ r \star x = r \star y \Longrightarrow x = y)$$

Exemple 4.3 *1. La somme et le produit sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ est associative et commutative, et admettent pour neutres respectifs 0 et 1.*

2. La différence n'est ni associative ni commutative sur $\mathbb{R}$..

3. La loi $"\circ"$ est associative, mais n'est pas commutative sur F^F, elle admet un neutre, qui est l'application Id_F.

4. Les lois $\cap$, $\cup$, $\triangle$ sur $P(E)$ sont associatives et commutatives. Elles admettent pour neutres respectifs E, $\emptyset$, $\emptyset$

Remarque 4.1 *1. Si $*$ est une loi de composition interne associative sur E qui admet un élément neutre, alors ce neutre est unique*

2. L'élément neutre e est inversible (ou symétrisable) et son unique inverse (ou symétrique) est e.

3. Si l'élément symetrique $x^{'}$ de x existe, il est unique. On le note généralement x^{-1}.

4.2 Les groupes

Définition 4.3 *Un groupe est un ensemble non vide G muni d'une loi de composition interne $*$, noté $(G, *)$ tels que :*

1. $*$est associative ;

2. $*$ admet un élément neutre e;

3. tout élément de G est symétrisable (admet un symétrique) pour $*$.

Si $*$ est commutative, on dit que $(G, *)$ est commutatif, ou encore abélien.

Exemple 4.4 *1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munis de la somme sont des groupes abéliens,*

2. $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$, Un munis du produit sont des groupes abéliens,

3. $P(E)$ muni de $\triangle$ est un groupe abélien.

Exemple 4.5 *(à démontrer)Les couples suivants ne sont pas des groupes :*

1. $(N, +)$, $(\mathbb{R}, \times)$, $(\mathbb{Z}, \times)$,

2. $(P(E), \cap)$, $(P(E), \cup)$.

4.2.1 Sous-groupes

Définition 4.4 *Un sous-groupe d'un groupe $(G,*)$ est une partie non vide H de G telle que :*
1. $*$ induit sur H une loi de composition interne.
2. H muni cette loi est un groupe.

En pratique, pour montrer qu'une partie non vide H de G en constitue un sous-groupe, il suffit de vérifier l'une des propositions suivantes:

Proposition 4.1 *Soient $(G,*)$ un groupe et $H \subset G$ alors,*

$$H \text{ est un sous groupe de } G \Longleftrightarrow \begin{cases} i.\ H \neq \emptyset \\ ii.\ \forall x,y \in H,\ x*y \in H.\ (H \text{ est stable par rapport à } *) \\ iii.\ \forall x \in H,\ x^{-1} \in H\ (\ x^{-1} \text{ le symytrique de } x\ ) \end{cases}$$

Proposition 4.2 *Soient $(G,*)$ un groupe et $H \subset G$ alors,*

$$H \text{ est un sous groupe de } G \Longleftrightarrow \begin{cases} i.\ H \neq \emptyset \\ ii.\ \forall x,y \in H,\ x*y^{-1} \in H. \end{cases}$$

Remarque 4.2 *Si e est l'élément neutre d'un groupe $(G,*)$, alors tout sous groupe de G contient e et on déduit la propriété suivante:*

Proposition 4.3 *Soient $(G,*)$ un groupe, e l'élément neutre de $*$ et H un sous ensemble de G alors,*

$$H \text{ est un sous groupe de } G \Longleftrightarrow \begin{cases} i.\ e \in H \\ ii.\ \forall x,y \in H,\ x*y^{-1} \in H. \end{cases}$$

Exemple 4.6 *1. Considérons le groupe $(\mathbb{C}^*,\times)$, et soit $U = \{z \in \mathbb{C},\ |z| = 1\}$,*
- Montrer que U est un sous groupe de $\mathbb{C}^*$.
▶ *i) $|1| = 1$ donc $1 \in U$, d'où $U \neq \emptyset$.*
ii) soient $z_1, z_2 \in \mathbb{C}$, $\left|z_1 \times (z_2)^{-1}\right| = \left|\dfrac{z_1}{z_2}\right| = \dfrac{1}{1} = 1$, d'où $z_1 \times (z_2)^{-1} \in U$.
Alors $(U,\times)$ est un sous groupe de $\mathbb{C}^*$.
2. Soit $n \in \mathbb{N}$, $n\mathbb{Z} = \{np,\ p \in \mathbb{Z}\}$ est un sous groupe de $(\mathbb{Z},+)$.
▶ *i) $0 \in n\mathbb{Z}$ car $\exists p = 0$, $n0 = 0 \in n\mathbb{Z}$ donc $n\mathbb{Z} \neq \emptyset$,*
ii) $\forall x,y \in n\mathbb{Z}$, $\exists p_1, p_2 \in \mathbb{Z}$, $x = np_1$, $y = np_2$ alors,
$x - y = np_1 - np_2 = n(p_1 - p_2) = nh$ $(h = p_1 - p_2 \in \mathbb{Z})$, D'où $x - y \in n\mathbb{Z}$
Alors $(n\mathbb{Z},+)$ est un sous groupe de $\mathbb{Z}$.

4.2.2 Homomorphisme de groupes

Définition 4.5 *Soient $(G,*)$ et (G',T) deux groupes. Une application f de G dans G' est un "homomorphisme de groupes" lorsque :*

$$\forall x,y \in G;\ f(x*y) = f(x)Tf(y).$$

- *Si $G = G'$ et $* = T$, on parle d'endomorphisme.*
- *Si f est bijective, on parle d'isomorphisme.*
- *Si f est un endomorphisme bijectif, on parle d'automorphisme.*

Exemple 4.7 *1. $x \mapsto 2^x$ est un un isomorphisme de $(\mathbb{R}, +)$ dans $\left(\mathbb{R}_+^*, \times\right)$,*
2. $x \mapsto 2x$ est un automorphisme de $(\mathbb{R}, +)$,
3. $x \mapsto 3\ln x$ est un isomorphisme de $\left(\mathbb{R}_+^*, \times\right)$ dans $(\mathbb{R}, +)$,
4. $z \mapsto |z|$ est un homomorphisme de $(\mathbb{C}^*, \times)$.dans $\left(\mathbb{R}_+^*, \times\right)$.

Exemple 4.8 *Montrer que la composition de deux homomorphismes de groupes est un homomorphisme de groupes.*

Proposition 4.4 *Soient e, e' les éléments neutres de G, G' respectivement et soit $f : G \longrightarrow G'$ un homomorphisme de groupes, alors*
1. $f(e) = e'$,
2. $\forall x \in G, (f(x^{-1})) = (f(x))^{-1}$. ($x^{-1}$ est le symtrique de x).

Proposition 4.5 *Soit $f : (G, *) \longrightarrow (G', T)$ un homomorphisme de groupes, alors*
1. L'image d'un sous groupe de G parf est un sous groupe de G'.
2. L'image réciproque d'un sous groupe de G' par f est un sous groupe de G.

Preuve. 1. Soit H un sous groupe de G et montrons que $f(H)$ vérifie les deux conditions de la caractérisation des sous groupes.
i) Comme H est un sous groupe de G, alors $e \in H$ donc $f(e) \in f(H)$, par suite $f(H) \neq \emptyset$.
ii) Soient $x', y' \in f(H)$, alors il existe $x, y \in H$ tels que $x' = f(x)$ et $y' = f(y)$, donc d'après la deuxième propriété on aura
$x'T\left(y'\right)^{-1} = f(x)T\left(f(y)\right)^{-1} = f(x)Tf(y^{-1}) = f(x * y^{-1})$
et comme H est un sous groupe de G alors $(x * y^{-1}) \in H$, par suite $x'T\left(y'\right)^{-1} = f(x * y^{-1}) \in f(H)$
de i) et ii) on déduit que $f(H)$ est un sous groupe de G'.
2. Soit H' un sous groupe de G', alors
i) D'après la première propriété $f(e) = e'$ et comme H' est un sous groupe de G' alors $e' \in H'$ donc $e \in f^{-1}(H')$.
ii) Soient $x, y \in f^{-1}(H')$, alors $f(x)$, $f(y) \in H'$ et comme H' est un sous groupe de G' alors $f(x)T\left(f(y)\right)^{-1} \in H'$ et de la deuxième propriété on déduit que
$f(x * y^{-1}) = f(x)Tf(y^{-1}) = f(x)T\left(f(y)\right)^{-1} \in H'$, ce qui montre que $(x * y^{-1}) \in f^{-1}(H')$.
De i) et ii) on déduit que $f^{-1}(H')$ est un sous groupe de G. ■

Le noyau et l'image d'un homomorphisme

Définition 4.6 *Soit f un homomorphisme de G dans G', e, e' les éléments neutres de G, G' respectivement*

• *Le noyau de f, noté* $\ker f$ *est l'ensemble définie par:*

$$\ker f = \left\{ x \in G;\ f(x) = e^{'} \right\} = f^{-1}\left(e^{'}\right).$$

• *L'image de f, noté* $\operatorname{Im} f$ *est l'ensemble définie par:*

$$\operatorname{Im} f = \{ f(x),\ x \in G \} = f(G)$$

Corollaire 4.1 *Comme cas particuliers de la proposition (4.2.5) on a:*
1. $\operatorname{Im} f$ *est un sous groupe de* $(G^{'}, T)$,
2. $\ker f$ *est un sous groupe de* $(G, *)$.

Le résultat suivant est bien plus intéressant, puisqu'il réduit énormément le travail, pour montrer qu'un homomorphisme est bijectif.

Proposition 4.6 *Soit* $f : (G, *) \longrightarrow (G^{'}, T)$ *un homomorphisme de groupe, alors*
1. f est injective si et seulement si $\ker f = \{e\}$, *(où e est l'élément neutre de G)*
2. f est surjective si et seulement si $\operatorname{Im} f = G^{'}$.

4.3 Structure d'Anneau

Définition 4.7 *On appelle anneau, tout ensemble A muni de deux lois de composition internes $+$ et $\times$ telles que :*
1. $(A, +)$ *est un groupe abélien (on notera* 0 *ou* 0_A *l'élément neutre de $+$),*
2. $\times$ est associative et distributive par rapport à $+$.
• *Si de plus $\times$ est commutative, on dit que* $(A, +, \times)$ *est un anneau commutatif.*
• *Si de plus Si $\times$ possède un élément neutre, on le note* 1 *ou* 1_A *et on dit que l'anneau* $(A, +, \times)$ *est unitaire.*

Exemple 4.9 $(\mathbb{Z}, +, \times)$, $(Q, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ *sont des anneaux commutatifs unitairs.*

Exemple 4.10 *Considérons l'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n; (définie dans l'exemple 3.3)*

$$\mathbb{Z}/n\mathbb{Z} = \left\{ \dot{0},\ \dot{1},\ \dot{2}, ...,\ \dot{n-1} \right\}$$

On définit sur cet ensemble les deux lois de compositions internes " $\dot{+}$ *" et "*$\dot{\times}$ *" comme:*

$$\forall \dot{p},\ \dot{q} \in \mathbb{Z}/n\mathbb{Z},\ \dot{p} \dot{+} \dot{q} = \widehat{p + q} \quad et \quad \dot{p} \dot{\times} \dot{q} = \widehat{p \times q}$$

où $+$ et $\times$ sont l'addition et la multiplication définies sur $\mathbb{Z}$ respectivement.
On peut verifier facilementque pour tout $n \in \mathbb{N}$; l'ensmble quotient $\mathbb{Z}/n\mathbb{Z}$ muni des deux lois "$\dot{+}$*" et "*$\dot{\times}$ *" possède une structure d'anneau commutatif unitair, où* $\dot{0}$ *et* $\dot{1}$ *sont les éléments neutres de "*$\dot{+}$*" et "*$\dot{\times}$ *" respectivement.*

4.3.1 Sous anneau

Définition 4.8 *Soit $(A,+,\times)$ un anneau. Une partie non vide $A^{'}$ de A est un sous-anneau de A lorsque :*

• $1_A \in A$;

• *les lois $+$ et $\times$ induisent des lois de composition internes sur $A^{'}$, et muni de ces lois, $(A^{'},+,\times)$ est un anneau.*

Pratiquement pour montrer qu'une partie non vide $A^{'}$ de A est un sous anneau, il suffit de vérifier la proposition suivante:

Proposition 4.7 *Soit $(A,+,\times)$ un anneau. et $A^{'} \subset A$ alors,*

$$A^{'} \text{ est un sous anneau de } A \Longleftrightarrow \begin{cases} i.\ A^{'} \neq \emptyset, \\ ii.\ \forall x,y \in A^{'},\ x-y \in A^{'} \\ iii.\ \forall x,y \in A^{'},\ x \times y \in A^{'}. \end{cases}$$

4.3.2 Homomorphismes d'Anneaux

Soient $(A,+,\times)$ et $(B,\oplus,\otimes)$ deux anneaux et $f : A \longrightarrow B$,

Définition 4.9 *On dit que f est un homomorphisme d'anneaux si :*

$$\forall x,y \in A, f(x+y) = f(x) \oplus f(y)$$

et

$$f(x \times y) = f(x) \otimes f(y)$$

– *Si $A = B$ on dit que f est un endomorphisme d'anneau de A.*

– *Si f est bijective, on dit que f est un isomorphisme d'anneaux*

– *Si f est bijective et $A = B$, on dit que f est un automorphisme d'anneaux.*

Exemple 4.11 *1. $z \mapsto \overline{z}$ est un automorphisme d'anneaux de $\mathbb{C}$.*

Exemple 4.12 *Montrer que la composition de deux homomorphismes d'anneaux est un homomorphisme d'anneaux.*

4.3.3 Diviseurs de zéro, les éléments inversibles

Définition 4.10 *Soit $(A,+,\times)$ un anneau commutatif. S'ils existent dans l'anneau A deux éléments a, b tels que:*

$$(a \times b = 0) \wedge (a \neq 0 \wedge b \neq 0)$$

alors, on dit que a et b sont des diviseurs de 0.

Définition 4.11 *On appelle anneau intègre ou complète, tout anneau ne contient pas un diviseur de zéro autre que* 0 *lui-même, c'est à dire*

$$ab = 0 \Longleftrightarrow a = 0 \text{ ou } b = 0.$$

Exemple 4.13 *1.* $(\mathbb{Z}, +, \times)$, $(\mathbb{R}, +, \times)$ $(\mathbb{Q}, +, \times)$, $(\mathbb{C}, +, \times)$ *sont des anneaux intègres,*
2. l'anneau des matrices $M_n(\mathbb{k})$ *muni les deux lois* $+$ *(somme des matrices) et* $\times$ *(produit des matrices) n'est pas intègre, car*

$$\exists A = \begin{pmatrix} 0 & -1 \\ 0 & 5 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R}),\ \exists B = \begin{pmatrix} 2 & -3 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R}),$$

$$\text{mais} \quad AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Définition 4.12 *Soit* $(A, +, \times)$ *un anneau commutatif.*
• *On dit que* $x \in A$ *est inversible s'il admet un symétrique pour la loi "*$\times$*".*

Exemple 4.14 *1. Dans* $\mathbb{Z}$ *l'éléments inversibles sont* 1 *et* -1,
2. dans les anneaux $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ *tous les éléments non nuls sont inversibles.*

Proposition 4.8 *Dans un anneau commutatif* $(A, +, \times)$ *:*
• 0_A *n'est jamais inversible.*
• *Si* x *est inversible, alors ce n'est pas un diviseur de* 0.
• *Si* $x_1, x_2, y \in A$ *intègre, avec* $y \neq 0$ *et* $x_1 y = x_2 y$, *alors* $x_1 = x_2$.
On dit qu'" on peut simplifier" (ce qui ne veut pas dire diviser) par $y \neq 0$
▶ $x_1 y = x_2 y \Longrightarrow (x_1 - x_2)\, y = 0$
$\Longrightarrow x_1 - x_2 = 0$ *ou* $y = 0$ *car* A *est intègre,*
$\Longrightarrow x_1 = x_2$, *car* $y \neq 0$.

4.3.4 Idéaux

Soit $(A, +, \times)$ un anneau.

Définition 4.13 *On appelle "idéal" à droite (respectivement à gauche) de l'anneau* A, *tout ensemble* $I \subset A$ *tel que*
1. .I *est un sous groupe de* $(A, +)$,
2. $\forall x \in A$, $\forall y \in I$, $x \times y \in I$ (*respectivement* $y \times x \in I$).

- Si I est idéal à droite et à gauche de A, on dit que I est un "idéal bilatère" de A.

- Si l'anneau A est commutatif, tout idéal de A est bilatère, et dans ce cas on parle seulement d'idéal sans préciser s'il l'est à droite, à gauche ou bilatère.

Exemple 4.15 *1. Soit $(A,+,\times)$ un anneau, alors $I=\{0_A\}$ est un idéal bilatère de A.*
2. Dans l'anneau commutatif $(\mathbb{Z},+,\times)$, $n\mathbb{Z}$ est un idéal.

Définition 4.14 *On appelle idéal principal d'un anneau commutatif $(A,+,\times)$, tout idéal I de A tel que*

$$\exists x\in A;\ I=xA$$

L'anneau A est dit principal si tous ses idéaux sont principaux.

4.4 Corps

Définition 4.15 *On dit qu'un anneau unitaire $(\Bbbk,+,\times)$ est un corps si tout élément non nul de $\Bbbk$ est inversible.*
Si de plus $\times$ est commutative, on dit que $\Bbbk$ est un corps commutatif.

Il est à remarquer que dans la pratique, tous les corps utilisés sont commutatifs.

Exemple 4.16 $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$, *sont des corps.*

Proposition 4.9 *Tout corps est un anneau intègre.*

Preuve. Fixons $a\in A$ et considérons l'homomorphisme d'anneaux $A\to A$, $x\mapsto ax$. Alors cet homomorphisme d'anneaux est injectif, car son noyau est réduit à $\{0_A\}$ puisque A est intègre. Puisque A est fini, cet homomorphisme est nécessairement bijectif, et donc il existe $x\in A$ tel que $ax=1_A$. Par commutativité de A, on a aussi $xa=1_A$ et donc a admet un inverse, et par concequense A est un corps. ■

4.4.1 Sous corps

Définition 4.16 *On appelle sous corps, d'un corps $(\Bbbk,+,\times)$, tout sous ensemble $\Bbbk'$ de $\Bbbk$ tel que, muni des restrictions des lois $+$ et $\times$ est un corps.*

Proposition 4.10 $\Bbbk'\subset\Bbbk$ *est un sous corps de $(\Bbbk,+,\times)$ si et seulement si*
1. $\Bbbk'\neq 0$
2. $\forall x,y\in\Bbbk', a-b\in\Bbbk'$ *et* $ab^{-1}\in\Bbbk'$.

On a aussi la caractérisation suivante des corps.

Proposition 4.11 *Soit $(\Bbbk,+,\times)$ un anneau commutatif unitaire, alors $\Bbbk$ est un corps si et seulement si les seuls idéaux de $\Bbbk$ sont $\{0_\Bbbk\}$ et $\Bbbk$ lui même.*

Exemple 4.17 $(\mathbb{Z},+,\times)$ *n'est pas un corps car les idéaux dans $\mathbb{Z}$ sont $\{0_\mathbb{Z}\}$, $n\mathbb{Z}$, et $\mathbb{Z}$.*

Exemple 4.18 *Considérons l'anneau quotient* $\left(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times}\right)$ *définie dans l'exemple 4.10, dans cet anneau on va traiter les trois cas:* $n = 2,\ 3,\ 4$

On écrit par exemple les tables de la multiplication dans les trois ensembles quotients $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$,

1. *Dans* $\mathbb{Z}/2\mathbb{Z} = \left\{\dot{0},\ \dot{1}\right\}$ *le tableau est:*

$$\begin{array}{ccc} \dot{\times} & \dot{0} & \dot{1} \\ \dot{0} & \dot{0} & \dot{0} \\ \dot{1} & \dot{0} & \dot{1} \end{array}$$

2. *Dans* $\mathbb{Z}/3\mathbb{Z} = \left\{\dot{0},\ \dot{1},\ \dot{2}\right\}$ *le tableau est:*

$$\begin{array}{cccc} \dot{\times} & \dot{0} & \dot{1} & \dot{2} \\ \dot{0} & \dot{0} & \dot{0} & \dot{0} \\ \dot{1} & \dot{0} & \dot{1} & \dot{2} \\ \dot{2} & \dot{0} & \dot{2} & \dot{1} \end{array}$$

3. *Dans* $\mathbb{Z}/4\mathbb{Z} = \left\{\dot{0}, \dot{1},\ \dot{2},\ \dot{3}\right\}$ *le tableau est:*

$$\begin{array}{ccccc} \dot{\times} & \dot{0} & \dot{1} & \dot{2} & \dot{3} \\ \dot{0} & \dot{0} & \dot{0} & \dot{0} & \dot{0} \\ \dot{1} & \dot{0} & \dot{1} & \dot{2} & \dot{3} \\ \dot{2} & \dot{0} & \dot{2} & \dot{0} & \dot{2} \\ \dot{3} & \dot{0} & \dot{3} & \dot{2} & \dot{1} \end{array}$$

D'aprés ces tableaux, on remaque que, tous les éléments non nuls dans $\mathbb{Z}/2\mathbb{Z}$ *et* $\mathbb{Z}/3\mathbb{Z}$ *sont inversibles d'où* $\left(\mathbb{Z}/2\mathbb{Z}, \dot{+}, \dot{\times}\right)$ *et* $\left(\mathbb{Z}/3\mathbb{Z}, \dot{+}, \dot{\times}\right)$ *sont des corps commutatifs. Mais dans* $\mathbb{Z}/4\mathbb{Z}$ *seulement les éléments* 1 *et* 3 *sont inversible, et l'élément* 2 *n'est pas, d'où* $\left(\mathbb{Z}/4\mathbb{Z}, \dot{+}, \dot{\times}\right)$ *n'est pas un corps.*

Plus généralement, on peut montrer qu'une condition nécessaire et suffisante pour que l'anneau $\left(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times}\right)$ *soit un corps est que l'entier naturel* n *soit un nombre premier.*

4.5 Exercices

Exercice 4.1 *On munit* $\mathbb{R}$ *de la loi de composition interne définie par :*

$$\forall x, y \in \mathbb{R}^+, x * y = \sqrt{x^2 + y^2}.$$

1) Montrer que $*$ *est commutative, associative, et admet un élément neutre.*

2) Déterminer les éléments symetrisables..

Solution 4.1 *1) il est claire que $*$ est commutative et associative, et accepte un élément neutre $e = 0$, $(x * 0 = \sqrt{x^2 + 0^2} = |x| = x,\ car\ x \succ 0)$*

2) comme $*$ admet un élément neutre alors on cherche les éléments symetrisables s'ils existent.

on suppose que y est le symetrique de x donc,

$\forall x \in \mathbb{R}^+, x * y = 0 \Longrightarrow \sqrt{x^2 + y^2} = 0 \Longrightarrow x^2 = -y^2$ ce qui est impossilble, càd $\nexists y \in \mathbb{R}^+$ tel que $x * y = 0$, et par conséquence tout les élément de $\mathbb{R}^{+*}$ n'acceptent pas un élément symetrique, le seul élément symetrisable par rapport à $*$ est l'élément neutre $e = 0$ (l'élément neutre est un élément symétrique de lui même).

Exercice 4.2 *Montrer que $(G, *)$ est un groupe, et préciser s'il est abélien (commutatif) :*

$$x * y = \frac{x + y}{1 + xy},\ sur\ G =]-1, 1[$$

Solution 4.2 *1) $x * y = \dfrac{x + y}{1 + xy}$ sur $G =]-1, 1[$;*

1) D'aprés la question il est pas annoncer que $*$ est une loi de composition interne sur G

alors on verifier d'abord que $*$ est bien définie une loi de composition interne sur G c à d,

si $x, y \in G$, alors $x * y \in G$.

Etudions la fonction définie sur $]-1, 1[$ par $f(t) = \dfrac{t + y}{1 + ty}$.

Elle est dérivable sur $[-1, 1]$, et sa dérivée vérifie

$f'(t) = \dfrac{1 - y^2}{(1 + ty)^2} > 0$ sur $]-1, 1[$., f est donc strictement croissante sur $[-1, 1]$,

Comme $f(-1) = (-1 + y)/(1 - y) = -1$, et $f(1) = (1 + y)/(1 + y) = 1$, alors $f(-1) < x * y = f(x) < f(1)$, donc on obtient que $x * y \in G$.

2) la loi est associative :

pour tout $x, y, z \in G$, $x * (y * z) = \dfrac{x + (y * z)}{1 + x(y * z)} = \dfrac{x + \dfrac{y + z}{1 + yz}}{1 + x\dfrac{y + z}{1 + yz}} = \dfrac{x + y + z + xyz}{1 + xy + xz + yz}$, et un calcul similaire donne le même résultat pour $(x * y) * z$.

3) e est un élément neutre pour la loi $*$, alors

$\forall x \in G,\ x * e = x \Longrightarrow x + e = x + x^2 e \Longrightarrow e\left(1 - x^2\right) = 0 \Longrightarrow e = 0$

donc $*$ admet un élément neutre $e = 0$.

4) Tout élément $x \in G$ est symetrisable, et l'élément symetrique est $-x$. En effet, on a

$x * (-x) = (-x) * x = 0$.

- De plus, la loi $*$ est clairement abélienne.car, pour tout $x, y \in G$, $x * y = \dfrac{x + y}{1 + xy} = y * x$

D'où $(G, *)$ est un groupe abelien.

Exercice 4.3 *Soit $(G, \times)$ un groupe. Démontrer que les parties suivantes sont des sous-groupes de G :*

1) $C(G) = \{x \in G; \forall y \in G, xy = yx\}$, $C(G)$ s'appelle le centre de G;

2) $aHa^{-1} = \{aha^{-1}; h \in H\}$ où $a \in G$ et H est un sous-groupe de G.

Solution 4.3 *I)*

1) Soit e l'élément neutre de G, On a : $\forall y \in G$, $ey = ye = y$ *donc* $e \in C(G)$, *alors* $C(G) \neq \emptyset$.

2) Soient $x_1, x_2 \in C(G)$. *Alors,*

$\forall y \in G$; $(x_1x_2)\, y = x_1(x_2y) = x_1(yx_2) = (x_1y)\, x_2 = (yx_1)\, x_2 = y\,(x_1x_2)$.

Donc $x_1x_2 \in C(G)$.

3) Soit $x \in C(G)$, *alors* $\forall y \in G$; $xy = yx$, *on multiplie par* x^{-1} *à droite on obtient:*

$xyx^{-1} = yxx^{-1} \Longrightarrow xyx^{-1} = y$, *aussi on multiplie par* x^{-1} *à gauche on obtient:*

$x^{-1}xyx^{-1} = x^{-1}y$ *d'où* $yx^{-1} = x^{-1}y$ *ce qui implique que* $x^{-1} \in C(G)$,

On conclut que $C(G)$ *est un sous groupe de G.*

II)

1) Puisque H est un sous-groupe de G, $e \in H$ *et donc* $aea^{-1} \in G$. *Mais* $aea^{-1} = e$ *et donc* $e \in aHa^{-1}$.

2) Soient $x = aha^{-1}$ *et* $y = ah'a^{-1}$ *deux éléments de* aHa^{-1} *avec* $h, h' \in H$. *On a*

$xy = aha^{-1}ah'a^{-1} = ahh'a^{-1} \in aHa^{-1}$, *puisque* $hh' \in H$ *(H est un sous-groupe de G). Enfin, on a* $x^{-1} = (aha^{-1})^{-1} = ah^{-1}a^{-1} \in aHa^{-1}$.

puisque $h^{-1} \in H$. aHa^{-1} *est donc bien un sous-groupe de G.*

Exercice 4.4 *Montrer que* $H = \{x + y\sqrt{3};\ x \in \mathbb{N},\ y \in \mathbb{Z},\ x^2 - 3y^2 = 1\}$ *est un sous-groupe de* $(\mathbb{R}^{+*}, \times)$.

Solution 4.4 *On montre d'abord que* $H \subset \mathbb{R}^{+*}$ *(càd: H est stable par rapport à* $\times$*.)*

Pour $x+y\sqrt{3} \in H$, *on a* $x^2-3y^2 \succ 0$ *alors,* $x > \sqrt{3}|y|$, *càd* $\begin{cases} x > \sqrt{3}y & si\ y \succ 0 \\ x > -\sqrt{3}y & si\ y \prec 0 \end{cases}$

mais comme $x \in N$ *dans les deux cas, on a* $x > -\sqrt{3}y$ *alors* $x + y\sqrt{3} > 0$

· *On remarque ensuite que* $1 = 1 + 0\sqrt{3} \in H$ *, alors* $H \neq \emptyset$

· *Soient* $a = x + y\sqrt{3}$ *et* $b = u + v\sqrt{3}$ *deux éléments de H. Alors :*

$ab = \left(x + y\sqrt{3}\right)\left(u + v\sqrt{3}\right) = (xu + 3yv) + \sqrt{3}(xv + yu)$.

On remarque ensuite que

$(xu + 3yv)^2 - 3(xv + yu)^2 = x^2u^2 + 9y^2v^2 - 3x^2v^2 - 3y^2u^2$

$= x^2\left(u^2 - 3v^2\right) + 3y^2\left(3v^2 - u^2\right)$

$= x^2 - 3y^2 = 1$

il est clair que $xu + 3yv \in \mathbb{Z}$ *et* $xv + yu \in \mathbb{Z}$. *Il reste de montrer que* $xu + 3yv \in \mathbb{N}$

on a $x \succ \sqrt{3}|y|$ *et* $u \succ \sqrt{3}|v|$, *alors* $xu \succ 3\,|yv|$, *d'apres ci-dessus on a* $xu \succ -3yv$ *(comme* $xu \in \mathbb{N}$*)*

alors $xu + 3yv \succ 0$

Ainsi, $ab \in H$

· *On a* $\dfrac{1}{a} = \dfrac{1}{x + y\sqrt{3}} = \dfrac{x - y\sqrt{3}}{x^2 - 3y^2} = x - y\sqrt{3} \in H$.

Ainsi, H est bien un sous-groupe de $(\mathbb{R}^{+*}, \times)$.

Exercice 4.5 *Les applications suivantes sont elles des homomorphismes de groupes? si oui, calculer le noyau et l'image, et déduire s'elles des isomorphismes de groupes, des Automorphismes de groupes.*

a) $\varphi : (\mathbb{R}^*, \times) \to (\mathbb{R}^*, \times), \quad \varphi : x \mapsto x^n$. $n \in \mathbb{N}^*$.
b) $\varphi : (\mathbb{R}, +) \to (\mathbb{C}^*, \times), \quad \varphi : t \mapsto e^{2\pi i t}$.
c) $\varphi : (\mathbb{C}^*, \times) \to \left(\mathbb{R}_+^*, \times\right), \quad \varphi : z \mapsto |z|$.
d) $\varphi : (\mathbb{R}, +) \to (\mathbb{R}, +), \quad \varphi : x \mapsto 2x - 3$.

Solution 4.5 *a)* $\forall x, y \in \mathbb{R}^*$, $\varphi(x \times y) = (xy)^n = x^n y^n = \varphi(x) \times \varphi(y)$ *donc c'est un homomorphisme*

$$\begin{aligned} \ker \varphi &= \{x \in \mathbb{R}^*, x^n = 1\} \\ \operatorname{Im} \varphi &= \{x^n, x \in \mathbb{R}^*\} \end{aligned}$$

On caractérise deux cas:
- Si n est paire: $\ker \varphi = \{1, -1\}$, $\operatorname{Im} \varphi = \mathbb{R}^{+*}$
- Si n est impaire: $\ker \varphi = \{1\}$, $\operatorname{Im} \varphi = \mathbb{R}^*$.
Alors φ *est un isomorphisme de groupes si n est impaire (dans ce cas* φ *est bijective),*
aussi comme $\varphi : \mathbb{R}^* \to \mathbb{R}^*$ *alors* φ *est un endomorphisme bijective et alors est un Automorphisme de groupes si n est impaire.*
(Si n est paire: φ *n'est pas injective et n'est pas surjective)*
b) $\forall t, t' \in \mathbb{R}$, $\varphi\left(t + t'\right) = e^{2\pi i\left(t+t'\right)} = e^{2\pi i t} e^{2\pi i t'} = \varphi(t) \times \varphi\left(t'\right)$ *donc c'est un homomorphisme.*
Puisque $e^{2\pi i t} = 1$ *si et seulement si* $t \in \mathbb{Z}$, *alors* $\ker \varphi = \mathbb{Z}$, *donc* φ *n'est pas injective,*
$\operatorname{Im} \varphi = \left\{e^{2\pi i t},\ t \in \mathbb{R}\right\} = \{z \in \mathbb{C},\ |z| = 1\}$, *donc* φ *n'est pas surjective,*
D'où φ *n'est pas un isomorphisme.*

Exercice 4.6 *Soit* $(G, +)$ *un groupe commutatif. On note* $End(G)$ *l'ensemble des endomorphismes de* G *sur lequel on définit la loi* $+$ *par* $f + g : G \to G$, $x \mapsto f(x) + g(x)$,
Démontrer que $(End(G), +, \circ)$ *est un anneau.*

Solution 4.6 *On remarque d'abord que* $+$ *et* $\circ$ *sont bien des lois de composition interne sur* $End(G)$.
1. $(End(G), +)$ *est un groupe commutatif.*
En effet, la loi $+$ *est associative, l'application* $0_G : G \to G, g \mapsto 0$ *est un élément neutre pour la loi* $+$,
et tout élément $f \in End(G)$ *admet un inverse* $-f : G \to G, x \mapsto -f(x)$,
2. *La loi* $\circ$ *est associative.*
3. *La loi* $\circ$ *est distributive par rapport à la loi* $+$ *: pour tous* $f, g, h \in End(G)$ *et tout* $x \in G$,
$((f + g) \circ h)(x) = (f + g)(h(x)) = f(h(x)) + g(h(x)) = (f \circ h + g \circ h)(x)$.
Ainsi, $(End(G), +, \circ)$ *est un anneau.*

Exercice 4.7 *On note l'ensemble de réels suivant :* $A = \left\{m + n\sqrt{6},\ m, n \in \mathbb{Z}\right\}$.
1) Montrer que $(A, +, \times)$ *(ensemble muni de l'addition et de la multiplication des réels), est un sous-anneau de* $(\mathbb{R}, +, \times)$.
2) On considère l'application φ, *de* A *dans lui-même, définie par* $\varphi\left(m + n\sqrt{6}\right) = m - n\sqrt{6}$.

- Montrer que φ est un automorphisme de l'anneau $(A,+,\times)$ (c'est-à-dire une bijection, et un homomorphisme pour chacune des deux lois).

3) Pour tout $x \in A$, on pose $N(x) = x\varphi(x)$. Montrer que N est une application de A dans $\mathbb{Z}$, qui est un homomorphisme pour la multiplication.

4) montrer que x est un élément inversible de A si et seulement si $N(x) = \pm 1$.

5) Vérifier que $5+2\sqrt{6}$ est inversible dans A et calculer son inverse.

Solution 4.7 *1) On $0+0\sqrt{6} = 0 \in A$ alors $A \neq \emptyset$.*

Soient $m,n,m',n' \in \mathbb{Z}$, $(m+n\sqrt{6}) - \left(m'+n'\sqrt{6}\right) = \left(m-m'\right) + \left(n-n'\right)\sqrt{6}$ donc $(m+n\sqrt{6}) - \left(m'+n'\sqrt{6}\right) \in A$.

$(m+n\sqrt{6})\left(m'+n'\sqrt{6}\right) = \left(mm'+6nn'\right) + \left(mn'+m'n\right)\sqrt{6}$ donc $(m+n\sqrt{6})\left(m'+n'\sqrt{6}\right) \in A$.

2) On a $\forall a \in A, \varphi(\varphi(a)) = a$ donc φ est une bijection, puisque tout élément a de A a pour antécédent $\varphi(a)$

· On montre maintenant que φ est homomorphisme pour l'addition et la multiplication:

· $\varphi\left((m+n\sqrt{6}) + \left(m'+n'\sqrt{6}\right)\right) = \varphi\left(\left(m+m'\right) + \left(n+n'\right)\sqrt{6}\right) = \left(m+m'\right) - \left(n+n'\right)\sqrt{6} = (m-n\sqrt{6}) + \left(m'-n'\sqrt{6}\right) = \varphi(m+n\sqrt{6}) + \varphi\left(m'+n'\sqrt{6}\right)$

·$\varphi\left((m+n\sqrt{6})\left(m'+n'\sqrt{6}\right)\right) = \varphi\left(\left(mm'+6nn'\right) + \left(mn'+m'n\right)\sqrt{6}\right) = \left(mm'+6nn'\right) - \left(\left(mn'+m'n\right)\sqrt{6}\right) =$ $(m-n\sqrt{6})\left(m'-n'\sqrt{6}\right) = \varphi(m+n\sqrt{6})\,\varphi\left(m'+n'\sqrt{6}\right)$.

3) Soit $a = m+n\sqrt{6} \in A$,

$N(a) = a\varphi(a) = (m+n\sqrt{6})(m-n\sqrt{6}) = m^2-6n^2$. donc N est bien une application de A dans $\mathbb{Z}$.

soient $a,a' \in A$, $N\left(aa'\right) = aa'\varphi\left(aa'\right) = aa'\varphi(a)\,\varphi\left(a'\right) = a\varphi(a)\,a'\varphi\left(a'\right) = N(a)\,N\left(a'\right)$, donc N est un homomorphisme.

4) ($\Longleftarrow$)Si $N(x) = x\varphi(x) = 1$, alors $\varphi(x)$ est un inverse de x, et si $N(x) = x\varphi(x) = -1$, alors $-\varphi(x)$ est un inverse de x.

($\Longrightarrow$) soit x unélément inversible de $A : \exists y,\ xy = 1$. et comme N est homomorphisme pour la multiplication, alors $N(x)\,N(y) = 1$, or $N(x)$ et $N(y)$ sont des entiers, les seuls éléments de $\mathbb{Z}$ inversibles pour la multiplication sont -1, $+1$.

5) $N\left(5+2\sqrt{6}\right) = 25-24 = 1$, l'inverse de $5+2\sqrt{6}$ est $5-2\sqrt{6}$

Exercice 4.8 *Soit p un nombre premier. On note $\mathbb{Z}_p = \{x = \frac{m}{n}; (m,n) \in \mathbb{Z}\times\mathbb{N}^*, p\wedge n = 1\}$.*

1) Vérifier que $\mathbb{Z}_p$ est un sous-anneau de $(\mathbb{Q},+,\times)$.

2) Soit $k \geq 0$. On note $J_{p^k} = \{\frac{m}{n}; (m,n) \in \mathbb{Z}\times\mathbb{N}^*, p\wedge n = 1, p^k | m\}$.

Montrer que J_{p^k} est un idéal de $\mathbb{Z}_p$.

Solution 4.8 *1) Claire,*

2) D'abord, on peut remarquer que $0 \in J_{p^k}$ et donc $J_{p^k} \neq \emptyset$.

Soient $x = \frac{m}{n}$, $y = \frac{m'}{n'} \in J_{p^k}$ alors,$x-y = \frac{mn'-m'n}{nn'}$ avec $p\wedge nn' = 1$, (car p est premier avec n et

premier avec n' alors il est premier avec nn')
et $p^k|m$, $p^k|m'$ et donc $p^k|mn' - m'n$, ensuite si $z = \frac{a}{b} \in \mathbb{Z}_p$ alors $xz = \dfrac{am}{bn}$ et tel que $p^k|am$ et $p \wedge bn = 1$ donc $xz \in J_{p^k}$
Alors J_{p^k} est bien un ideal de $\mathbb{Z}_p$.

Chapitre 5

Anneaux des polynômes

Dans ce chapitre, on introduit la notion de polynôme sur un corps ou un anneau. Tout au long du chapitre, $\mathbb{k}$ désigne un corps et A un anneau commutatif unitaire.

5.1 Construction de l'anneau des polynomes

Définition 5.1 *On appelle polynôme à une indéterminée à coefficients dans A toute suite $P = (a_n)_{n\in\mathbb{N}}$ d'éléments de A tous nul à partir d'un certain rang.*
Les polynômes sont munis des opérations usuelles d'addition et de produit de polynômes.
Soient $P = (a_n)_{n\in\mathbb{N}}$, $Q = (b_n)_{n\in\mathbb{N}}$ deux polynômes à une indéterminée à coefficients dans A. On a alors :

$$\begin{aligned} P+Q &= (a_n+b_n)_{n\in\mathbb{N}}, \\ PQ &= (c_n)_{n\in\mathbb{N}},\ avec\ c_n = \sum_{0\leq k\leq n} a_k b_{n-k}. \end{aligned}$$

On vérifie que le produit de deux polynômes est bien un polynôme.
On pose $X = (0,1,0,0,...,0)$, $X^0 = (1,0,0,...,0)$,, on montre alors que $X^i = (0,0,...,0,1,0,...)$ où le 1 est situé à la $i^{ème}$ place et que

$$X^i X^j = X^{i+j}$$

Ainsi tout polynôme $P = (a_n)_{n\in\mathbb{N}}$ à une indéterminée à coefficients dans A s'écrit sous la forme $P = \sum_{i\in\mathbb{N}} a_i X^i = (a_0, a_1, ..., a_n, 0, ...)$.
Les polynômes constants sont ceux de la forme $P = (a, 0, 0, ...)$, dans ce cas, on note simplement $P = a$.
Le degré de P, noté $\deg(P)$, est le plus grand entier n tel que $a_n \neq 0$.
Par convention $\deg(0) = -\infty$.

Définition 5.2 *L'ensemble des polynômes à une indéterminée à coefficients dans A muni de l'addition et de la multiplication définies ci-dessus est un anneau. On le note $A[X]$, appellé l'anneau des polynômes.*

Définition 5.3 *Un polynôme P est dit unitaire si son coefficient dominant, c'est-à-dire le coefficient du terme de plus haut degré, est égale à 1.*

Proposition 5.1 *Si A est intègre alors pour tout P, $Q \in A[X]$, on a*

$$\deg(PQ) = \deg(P) + \deg(Q).$$

Preuve. Soit $n = \deg(P)$ et $m = \deg(Q)$. On pose $P = \sum a_i X^i$et $Q = \sum b_i X_i$ où $a_i, b_i \in A$. Alors le coefficient du terme dominant de PQ est $a_n b_m$. Or $a_n \neq 0$ et $b_m \neq 0$ et donc, puisque A est intègre, $a_n b_m \neq 0$. Ce qui implique $\deg(PQ) = n + m$. ■

5.2 Arithmétique des polynômes

Pour simplifier les énoncés, nous travailleront dorénavant sur un corps $\Bbbk$, où $\Bbbk$ désignera l'un des corps $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

5.2.1 Division euclidienne

Définition 5.4 *Soient $A, B \in \Bbbk[X]$, on dit que B divise A s'il existe $Q \in \Bbbk[X]$ tel que $A = BQ$. On note alors $B \diagup A$.*

On dit aussi que A est multiple de B ou que A est divisible par B.

Théorème 5.1 ***Division euclidienne des polynômes***
Soient $A, B \in \Bbbk[X]$, avec $B \neq 0$, alors il existe un unique polynôme Q et il existe un unique polynôme R tels que :

$$A = BQ + R \qquad \text{et} \qquad \deg R \prec \deg B$$

Q est appelé le quotient et R le reste et cette écriture est "la division euclidienne" de A par B.
Notez que la condition $\deg R \prec \deg B$ signifie $R = 0$ ou bien $0 \leq \deg R \prec \deg B$.
Enfin $R = 0$ si et seulement si $B \diagup A$.

Exemple 5.1 *Effectyer la division euclidienne de A par B tels que:*

$$A = x^3 + 2x^2 - 3 \quad \text{et} \quad B = x^2 - 4,$$

▶ *On fait la division de polynômes comme la division euclidienne de deux entiers*

$$\begin{array}{rl} x^3+2x^2-3 & \mid \underline{x^2-4} \\ \underline{-\quad 2x^2+4x-3} & \\ -2x^2+8 & \mid x+2 \\ 4x+5 & \end{array}.$$

alors le quotient $Q=x+2$, *et le reste* $R=4x+5$.
Donc: $x^3+2x^2-3=\left(x^2-4\right)(x+2)+(4x+5)=BQ+R$.

Le plus grand commun diviseur "pgcd"

Proposition 5.2 *Soient* $A,B\in\Bbbk[X]$, *avec* $A\neq 0$ *ou* $B\neq 0$. *Il existe un unique polynôme unitaire de plus grand degré qui divise à la fois* A *et* B. *Cet unique polynôme est appelé le pgcd (plus grand commun diviseur) de* A *et* B *que l'on note* $pgcd(A,B)$.

Algorithme d'Euclide. Soient A et B des polynômes, $B\neq 0$.
On calcule les divisions euclidiennes successives,

$$\begin{array}{rcll} A & = & BQ_1+R_1 & \deg R1\prec\deg B \\ B & = & R_1Q_2+R_2 & \deg R_2\prec\deg R_1 \\ R_1 & = & R_2Q_3+R_3 & \deg R_3\prec\deg R_2 \\ & & \vdots & \\ R_{k-2} & = & R_{k-1}Q_k+R_k & \deg R_k\prec\deg R_{k-1} \\ R_{k-1} & = & R_kQ_{k+1} & \end{array}$$

Le degré du reste diminue à chaque division. On arrête l'algorithme lorsque le reste est nul.
Le pgcd est le dernier reste non nul R_k

Exemple 5.2 *Déterminer le* $pgcd\,(A,B)$, *où*

$$A=x^5{+}3x^4{+}x^3{+}x^2{+}3x+1,\quad B=x^4{+}2x^3{+}x+2,$$

▶ $x^5{+}3x^4{+}x^3{+}x^2{+}3x+1=\left(x^4{+}2x^3{+}x+2\right)(x+1)+x^4{+}x^3{+}x+1$
puis $x^4{+}2x^3{+}x+2=\left(-x^3{-}1\right)(-x-2)$
Alors le $pgcd\,(A,B)=x^3+1$.

Définition 5.5 *Soient* $A,B\in\Bbbk[X]$.
On dit que A *et* B *sont premiers entre eux si* $pgcd(A,B)=1$.

Le plus petit commun multiple "ppcm"

Proposition 5.3 *Soient $A, B \in \Bbbk[X]$ des polynômes non nuls, alors il existe un unique polynôme unitaire M de plus petit degré tel que $A \diagup M$ et $B \diagup M$.*
Cet unique polynôme est appelé le ppcm (plus petit commun multiple) de A et B qu'on note $ppcm(A, B)$.

Exemple 5.3 *Le* $ppcm(x^2(x+1)\left(x^2+2\right), x^4(x-2)(x+1)^2) = x^4(x+1)^2(x-2)\left(x^2+2\right)$.

5.2.2 Racine d'un polynôme

Définition 5.6 *Soit $P \in \Bbbk[X]$ et $a \in \Bbbk$,. On dit que a est une racine (ou un zéro) de P si $P(a) = 0$.*

Proposition 5.4 *$P(a) = 0 \Longleftrightarrow (x-a)$ divise P.*

Preuve. Il existe deux polynômes $Q, R \in \Bbbk[X]$ tels que

$$P = Q.(X-a) + R \quad \text{avec} \quad degR < 1$$

Ainsi R est une constante. En évaluant l'expression ci-dessus en a, on trouve $P(a) = R(a)$
et on a :
a est une racine de $P \Leftrightarrows P(a) = 0 \Longleftrightarrow R = 0 \Leftrightarrows (X-a)$ divise P.
■

Définition 5.7 *Soit $k \in \mathbb{N}^*$,. On dit que a est une racine de multiplicité k de P si $(x-a)^k$ divise P alors que $(x-a)^{k+1}$ ne divise pas P.*
Lorsque $k = 1$ on parle d'une "racine simple",
Lorsque $k = 2$ on parle d'une "racine double" etc...

Proposition 5.5 *Les assertions suivantes sont équivalentes:*
i) a est une racine de multiplicité k de P.
ii) Il existe $Q \in \Bbbk[X]$ tel que $P = (x-a)^k Q$, avec $Q(a) \neq 0$.

Théorème d'Alembert-Gauss

Théorème 5.2 ***Théorème d'Alembert-Gauss***
Tout polynôme à coefficients complexes de degré $n \geq 1$ a au moins une racine dans $\mathbb{C}$. Il admet exactement n racines si on compte chaque racine avec multiplicité.

Exemple 5.4 *Soit $P = ax^2 + bx + c$ un polynôme de degré 2 à coefficients réels : $a, b, c \in \mathbb{R}$ et $a \neq 0$.*
– Si $\triangle = b^2 - 4ac \succ 0$ alors P admet 2 racines réelles distinctes $x_1 = \frac{-b-\sqrt{\triangle}}{2a}$,.$x_2 = \frac{-b+\sqrt{\triangle}}{2a}$,
– Si $\triangle \prec 0$, alors P admet 2 racines complexes distinctes $x_1 = \frac{-b-i\sqrt{\triangle}}{2a}$,.$x_2 = \frac{-b+i\sqrt{\triangle}}{2a}$,
– Si $\triangle = 0$ alors P admet une racine réelle double $x = \frac{-b}{2a}$..
En tenant compte des multiplicités on a donc toujours exactement 2 racines.

Définition 5.8 *Un polynôme irréductible P est un polynôme non constant dont les seuls diviseurs de P sont les constantes ou P lui-même.*
Dans le cas contraire, on dit que P est réductible ; il existe alors des polynômes $A, B \in \Bbbk[X]$ tels que $P = AB$, avec $\deg A \geq 1$ et $\deg B \geq 1$.

Exemple 5.5 *1. Tous les polynômes de degré 1 sont irréductibles. Par conséquent il y a une infinité de polynômes irréductibles.*
2. $x^2 - 4 = (x-2)(x+2)$ est réductible.
3. $x^2 + 2 = \left(x - i\sqrt{2}\right)\left(x + i\sqrt{2}\right)$ est réductible dans $\mathbb{C}[X]$ mais est irréductible dans $\mathbb{R}[X]$.
4. $x^2 - 6 = \left(x - \sqrt{6}\right)\left(x + \sqrt{6}\right)$ est réductible dans $\mathbb{R}[X]$ mais est irréductible dans $\mathbb{Q}[X]$.

5.2.3 factorisation (Décomposition en facteurs irréductibles)

Théorème 5.3 *Tout polynôme non constant $A \in \Bbbk[X]$ s'écrit comme un produit de polynômes irréductibles unitaires :*

$$A = \lambda P_1^{k_1} P_2^{k_2} ... P_r^{k_r}.$$

où ¸ $\lambda \in \Bbbk^*$, $r \in \mathbb{N}^*$, $k_i \in \mathbb{N}^*$, et les Pi sont des polynômes irréductibles distincts.
De plus cette décomposition est unique à l'ordre près des facteurs.

Preuve. On peut supposer sans perdre de généralité que P est unitaire. On cherche alors à décomposer P sous la forme $P = P_1^{k_1} P_2^{k_2} ... P_r^{k_r}$.
1. **Existence de la décomposition.**
On raisonne par récurrence sur $d = deg(P)$.
Si $d = 1$, P est un polynôme de degré 1 donc irréductible. Le résultat est clair.
On suppose le résultat vrai pour tout polynôme de degré $\leq d$. Soit P un polynôme de degré $d+1$. Soit P est irréductible auquel cas le résultat est clair soit P est réductible et il existe deux polynômes unitaires Q et R non constants tels que $P = QR$.
Comme Q et R sont de degrés ≥ 1, on a $1 \leq deg(Q), deg(R) \leq d$. L'hypothèse de récurrence s'applique donc à Q et à R. Il existe alors des polynômes unitaires irréductibles $P_1, ..., P_r$ et $P_{r+1}, ..., P_r$ tels que $Q = P_1 ... P_r$ et $R = P_{r+1} ... P_r$. On a alors $P = P_1 ... P_r$ et on obtient le résultat en regroupant les P_i qui sont égaux.

2. **Unicité de la décomposition.**
On suppose que $P = P_1^{k_1} P_2^{k_2} ... P_r^{k_r} = Q_1^{\beta_1} Q_2^{\beta_2} ... Q_s^{\beta_s}$ où les Pi (respectivement les Q_i) sont des polynômes distincts, unitaires et irréductibles dans $\Bbbk[X]$.Soit $i \in \{1, ..., r\}$.
Puisque $P_i | Q_1^{\beta_1} Q_2^{\beta_2} ... Q_s^{\beta_s}$ et P_i est irréductible, on voit d'après le lemme d'Euclideque $P_i | Q_j$ pour un certain $j \in \{1, ..., s\}$. Comme P_i et Q_j sont irréductibles et unitaires, on a alors $P_i = Q_j$ Ceci permet

de définir une application de $\{1,...,r\}$ dans $\{1,...,s\}$ tel que $P_i = Q_j$.
De plus comme les Q_i sont distincts, cette application est injective. Par symétrie, on peut construire une applicationinjective de $\{1,...,s\}$ dans $\{1,...,r\}$, ce qui montre que $s = r$ et
$\{P_1,...,P_r\} = \{Q_1,...,Q_r\}$.
Quitte à réordonner les facteurs on supposera que $P = P_1^{k_1}P_2^{k_2}...P_r^{k_r} = P_1^{\beta_1}P_2^{\beta_2}...P_r^{\beta_r}$. Pour tout $i \neq j$ on a $pgcd(P_i^{k_i}, Q_i^{\beta_i}) = 1$, ainsi $P_i^{k_i}|Q_i^{\beta_i}$ et $k_i \leq \beta_i$.
De manière symétrique, on montre que $Q_i^{\beta_i}|P_i^{k_i}$ et $\beta_i \leq k_i$. Ainsi $k_i = \beta_i$ pour tout i. ■

Factorisation dans $\mathbb{C}$[X] et $\mathbb{R}$[X]

Théorème 5.4 *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*
Donc pour $P \in \mathbb{C}[X]$ de degré $n \geq 1$ la factorisation s'écrit $P = \lambda (x-a_1)^{k_1} (x-a_2)^{k_2} ... (x-a_r)^{k_r}$,
Où $a_1, a_2, ..., a_r$ sont les racines distinctes de P et $k_1, ..., k_r$ sont leurs multiplicités.

Théorème 5.5 *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 ainsi que les polynômes de degré 2 ayant un discriminant $\triangle \prec 0$.*
Soit $P \in \mathbb{R}[X]$ de degré $n \geq 1$. Alors la factorisation s'écrit $P = \lambda (x-a_1)^{k_1} (x-a_2)^{k_2} ... (x-a_r)^{k_r} Q_1^{l_1}...Q_s^{l_s}$,
Où les a_i sont exactement les racines réelles distinctes de multiplicité k_i et les Q_i sont des polynômes irréductibles de degré 2.

Exemple 5.6 *1. Décomposer en produits d'irréductibles dans $\mathbb{R}[X]$ les polynômes: $x^8 - 1$, $x^4 + 1$*
► *On commence par chercher les racines complexes pour factoriser dans $\mathbb{C}[X]$, puis on regroupe les racines complexes conjuguées afin d'obtenir la décomposition sur $\mathbb{R}[X]$*
1) $x^4 + 1 = \left(x^2 - i\right)\left(x^2 + i\right)$
$= \left(x - \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)\right)\left(x + \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)\right)\left(x - \left(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)\right)\left(x + \left(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)\right)$, *(C'est la décomposition sur $\mathbb{C}$,)*
$= \left[\left(x - \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)\right)\left(x - \left(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)\right)\right]\left[\left(x + \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)\right)\left(x + \left(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)\right)\right]$
$= \left(x^2 + \sqrt{2}x + 1\right)\left(x^2 - \sqrt{2}x + 1\right)$, *(C'est la décomposition sur $\mathbb{R}$,)*
2) $x^8 - 1 = \left(x^4 - 1\right)\left(x^4 + 1\right)$
$= \left(x^2 - 1\right)\left(x^2 + 1\right)\left(x^2 + \sqrt{2}x + 1\right)\left(x^2 - \sqrt{2}x + 1\right)$
$= (x-1)(x+1)\left(x^2 + 1\right)\left(x^2 + \sqrt{2}x + 1\right)\left(x^2 - \sqrt{2}x + 1\right)$.

5.3 Exercices

Exercice 5.1 *Effectuer la division euclidienne de A par B :*
1) $A = x^5 - 7x^4 - x^2 - 9x + 9$, $B = x^2 - 5x + 4$.
2) $A = x^3 + x^2 - 2x + 1$, $B = x^2 + 2x + 1$.

Solution 5.1 *1)* $x^5 - 7x^4 - x^2 - 9x + 9 = \left(x^2 - 5x + 4\right)\left(x^3 - 2x^2 - 14x - 63\right) - 268x + 261$.
2) $x^3 + x^2 - 2x + 1 = \left(x^2 + 2x + 1\right)(x-1) - x + 2$.

Exercice 5.2 *Déterminer le pgcd et le ppcm des polynômes suivants:*
1) $P(x) = x^4 - 3x^3 + x^2 + 4$ *et* $Q(x) = x^3 - 3x^2 + 3x - 2$;
2) $P(x) = x^5 - x^4 + 2x^3 - 2x^2 + 2x - 1$ *et* $Q(x) = x^5 - x^4 + 2x^2 - 2x + 1$;
3) $P(x) = x^n - 1$ *et* $Q(x) = (x-1)^n, n \geq 1$.

Solution 5.2 *1) On applique l'algorithme d'Euclide. Le dernier reste non-nul donne un pgcd des deux polynômes. On a successivement :*
$x^4 - 3x^3 + x^2 + 4 = \left(x^3 - 3x^2 + 3x - 2\right) x + \left(-2x^2 + 2x + 4\right),$
$x^3 - 3x^2 + 3x - 2 = \left(-2x^2 + 2x + 4\right)\left(\frac{-1}{2}x + 1\right) + (3x - 6),$
$-2x^2 + 2x + 4 = (3x - 6)\left(\frac{2}{3}x - \frac{2}{3}\right).$
Donc le $pgcd\,(P, Q) = x - 2$,
2) On répète le même procédé :
$x^5 - x^4 + 2x^3 - 2x^2 + 2x - 1 = \left(x^5 - x^4 + 2x^2 - 2x + 1\right) 1 + \left(2x^3 - 4x^2 + 4x - 2\right),$
$x^5 - x^4 + 2x^2 - 2x + 1 = \left(2x^3 - 4x^2 + 4x - 2\right)\left(\frac{1}{2}x^2 + \frac{1}{2}x\right) + x^2 - x + 1,$
$2x^3 - 4x^2 + 4x - 2 = \left(x^2 - x + 1\right)(2x - 2) + 0$
Donc le $pgcd\,(P, Q) = x^2 - x + 1$
3) Les diviseurs non-constants de Q *sont les polynômes du type* $c(x-1)^p$, *avec* $1 \leq p \leq n$. *Parmi ces diviseurs, seuls ceux de la forme* $c(x-1)$ *divisent aussi* P *(par exemple, car* 1 *est racine simple et non double de* P, *ou bien parce qu'on sait comment décomposer* P *en produits d'irréductibles...). Ainsi, le* $pgcd\,(P, Q) = x - 1$.

Exercice 5.3 *1) Décomposer en produits d'irréductibles dans* $\mathbb{R}[X]$ *le polynôme* $(x^2 - x + 1)^2 + 1$
2) Décomposer en produits d'irréductibles de $\mathbb{C}[X$ *le polynôme* $P\,(x) = x^9 + x^6 + x^3 + 1$..

Solution 5.3 *1) On commence par factoriser le polynôme dans* $\mathbb{C}[X]$ *en remarquant qu'il s'agit alors d'une différence de deux carrés :*
$(x^2 - x + 1)^2 + 1 = (x^2 - x + 1)^2 - i^2 = (x^2 - x + 1 - i)\left(x^2 - x + 1 + i\right),$
$= (x + i)(x - 1 - i)(x - i)(x - 1 + i)$
$= \left(x^2 + 1\right)\left(x^2 - 2x + 2\right).$
On factorise alors chacun des polynômes de degré 2 *dans* $\mathbb{C}$, *par exemple en calculant leur discriminant ou en remarquant que* i *(resp.* $-i$*) sont des racines évidentes. On trouve :*

$$(x^2 - x + 1)^2 + 1 = (x + i)(x - 1 - i)(x - i)(x - 1 + i)$$

En regroupant les termes conjugués, on trouve finalement :

$$(x^2 - x + 1)^2 + 1 = \left(x^2 + 1\right)\left(x^2 - 2x + 2\right)$$

C'est la décomposition dans $\mathbb{R}\,[X]$.
2) On va commencer par décomposer $Q\,(x) = x^3 + x^2 + x + 1$, *dont* -1 *est racine évidente. On en*

déduit

$$Q(X) = (x^2+1)(x+1) = (x+1)(x-i)(x+i).$$

On a $P(x) = Q(x^3)$ *et il s'agit maintenant de trouver les racines* $3^{ièmes}$ *de* 1, i *et* $-i$. *On en déduit que*

$$P(x) = (x+1)\left(x-e^{i\pi/3}\right)\left(x-e^{-i\pi/3}\right)\left(x-e^{i\pi/2}\right)\left(x-e^{-i5\pi/6}\right)\left(x-e^{-i\pi/6}\right)\left(x-e^{-i\pi/2}\right)\left(x-e^{i5\pi/6}\right)\left(x-e^{i}\right.$$

Exercice 5.4 *Soit le polynôme* $P(x) = x^4 - 6x^3 + 9x^2 + 9$.
1) Décomposer $x^4 - 6x^3 + 9x^2$ *en produit de facteurs irréductibles dans* $\mathbb{R}[X]$.
2) En déduire une décomposition de P *en produit de facteurs irréductibles dans* $\mathbb{C}[X]$, *puis dans* $\mathbb{R}[X]$

Solution 5.4 *1) On écrit simplement*
$x^4 - 6x^3 + 9x^2 = x^2\left(x^2 - 6x + 9\right) = x^2(x-3)^2$,
2) $x^4 - 6x^3 + 9x^2 + 9 = (x(x-3))^2 - (3i)^2$
$= (x(x-3) - 3i)(x(x-3) + 3i)$
$= \left(x^2 - 3x - 3i\right)\left(x^2 - 3x + 3i\right)$
- On factorise $x^2 - 3x - 3i$
$\triangle = 9 + 12i = \left(\sqrt{3}(2+i)\right)^2$
d'où les racines sont: $x_1 = \frac{3}{2} - \sqrt{3} - \frac{\sqrt{3}}{2}i$, *et* $x_2 = \frac{3}{2} + \sqrt{3} + \frac{\sqrt{3}}{2}i$ *donc,*

$$x^2 - 3x - 3i = \left(x - \left(\frac{3}{2} - \sqrt{3} - \frac{\sqrt{3}}{2}i\right)\right)\left(x - \left(\frac{3}{2} + \sqrt{3} + \frac{\sqrt{3}}{2}i\right)\right)$$

- On factorise $x^2 - 3x + 3i$
$\triangle = 9 - 12i = \left(\sqrt{3}(2-i)\right)^2$
d'où les racines sont: $x_1 = \frac{3}{2} + \sqrt{3} - \frac{\sqrt{3}}{2}i$, *et* $x_2 = \frac{3}{2} - \sqrt{3} + \frac{\sqrt{3}}{2}i$ *donc,*

$$x^2 - 3x + 3i = \left(x - \left(\frac{3}{2} + \sqrt{3} - \frac{\sqrt{3}}{2}i\right)\right)\left(x - \left(\frac{3}{2} - \sqrt{3} + \frac{\sqrt{3}}{2}i\right)\right)$$

Alors la décomposition de P *en produit d'irréductibles de* $\mathbb{C}[X]$ *est donc,*
$P(x) = \left[x - \left(\frac{3}{2} - \sqrt{3} - \frac{\sqrt{3}}{2}i\right)\right]\left[x - \left(\frac{3}{2} + \sqrt{3} + \frac{\sqrt{3}}{2}i\right)\right]\left[x - \left(\frac{3}{2} + \sqrt{3} - \frac{\sqrt{3}}{2}i\right)\right]\left[x - \left(\frac{3}{2} - \sqrt{3} + \frac{\sqrt{3}}{2}i\right)\right]$,
Pour obtenir la décomposition en produit d'irréductibles de $\mathbb{R}[X]$, *on regroupe les racines complexes conjuguées,.on trouve*

$$P(x) = \left[x^2 - \left(2\sqrt{3}+3\right)x + 3\sqrt{3} + 6\right]\left[x^2 + \left(2\sqrt{3}-3\right)x - 3\sqrt{3} + 6\right].$$

Exercice 5.5 *On considère les deux polynômes suivants :*
$P(x) = x^3 - 9x^2 + 26x - 24, \quad Q(x) = x^3 - 7x^2 + 7x + 15.$
Décomposer ces deux polynômes en produits d'irréductibles de $\mathbb{R}[X]$ *sachant qu'ils ont une racine commune.*

Solution 5.5 *Si a est une racine commune de P et Q, alors $x-a$ divise le pgcd (P,Q). On commence donc par chercher ce pgcd, par exemple en appliquant l'algorithme d'Euclide. Ici, on a*

$x^3-9x^2+26x-24 = x^3-7x^2+7x+15+\left(-2x^2+19x-39\right)$

$x^3-7x^2+7x+15 = \left(-2x^2+19x-39\right)\left(\frac{-1}{2}x-\frac{5}{4}\right)+\left(\frac{45}{4}x-\frac{135}{4}\right)$

$\left(-2x^2+19x-39\right) = \left(\frac{45}{4}x-\frac{135}{4}\right)\left(\frac{-8}{45}x+\frac{52}{45}\right)$

Le pgcd (P,Q) est donc $\left(\frac{45}{4}x-\frac{135}{4}\right)$, ou encore $x-3$. On divise alors P et Q par $x-3$, et on trouve :

$P(x) = (x-3)\left(x^2-6x+8\right)$ *et* $Q(x) = (x-3)\left(x^2-4x-5\right)$.

On factorise encore chacun des polynômes de degré 2 pour trouver finalement :

$P(x) = (x-3)(x-2)(x-4)$ *et* $Q(x) = (x+1)(x-3)(x-5)$.

N.B: On aurait aussi pu factoriser ces polynômes en cherchant des racines évidentes.

Bibliographie

[1] Algèbre: Cours de Mathématiques première année, Arnaud, Bodin.

[2] Mathématiques 4. Algèbre-cours et exercices- Elie Azoulay, Jean Avignant, 1984.

[3] Algèbre et Analyse, Stéphane. Balac, Frédéric. Sturm, 2 eme édition 2008.