Ministère de l'enseignement supérieur et de la recherche scientifique

Centre Universitaire d'Ain Temouchent Belhadj Bouchaib
Institut des sciences
Département de Mathématiques et Informatique

Algèbre I

Recueil d'Exercices Corrigés

Pour Etudiants de Première Année

HELLAL Meryem

Année universitaire 2019-2020

Département de Mathématiques et Informatique
meriem_tlm@yahoo.fr
Institut des sciences
C.U.A.T.B.B

Preface

Ce polycopié est issu du cours d'Algèbre I principalement destiné aux étudiants de première année Mathématiques et Informatiques, Centre universitaire Ain Temouchent Belhadj Bouchaib. Il peut aussi être utilisé par les étudiants d'autres paliers aussi bien en sciences et technologie que ceux de Biologie.

Ce recueil d'exercices s'articule autour de cinq chapitres. Dans chaque chapitre, nous donnons un bref rappel des notions, des définitions de cours d'Algèbre I qu'on pourra retrouver en détail dans [7] , [8]. A la fin de chaque chapitre, on trouve une série de différents exercices avec des corrigés détaillés. La plupart de ces exercices étaient proposés lors des séances de travaux dirigés. Le lecteur intéressé y trouvera aussi des exercices supplémentaires sans corrigé.

Le premier chapitre est consacré aux définitions de bases de la branche des mathématiques appelée la logique des propositions. On s'attardera également sur quelques définitions et des techniques fondamentales de preuves mathématiques. Dans le deuxième chapitre, on donne des définitions de théorie des ensembles et les applications avec quelques exemples illustratifs. Le troisième chapitre porte sur les relations binaires : réflexivité, symétrie, antisymétrie, transitivité, relation d'ordre, relation d'équivalence : classe d'équivalence, ce chapitre est aussi illustré par des exemples. Le quatrième chapitre traite les stréctures algébriques : groupe, sous-groupe, anneau, sous anneau et structure de corps. Le dernier chapitre a pour objectif les notions suivantes : Polynômes, opérations sur les polynômes, arithmétiques des polynômes, racines d'un polynôme, polynômes irréductibles.

A la fin de ce manuscrit, nous avons donné quelques références de base.

Toute remarque ou suggestion est la bienvenue pour m'aider à améliorer le contenu de ce travail.

Table des Matières

Chapitre 1

Notions de Logique

Sommaire

1.1 Rappels de cours

1.1.1 Les connecteurs logiques

Définition 1.1 ***Proposition (ou assertion ou affirmation)*** *Une proposition est un énoncé pouvant être vrai ou faux.*

Exemple 1.1.1 *« tout nombre premier est impair » et « tout carré de réel est un réel positif » sont deux propositions. Il est facile de démontrer que la première est fausse et la deuxième est vraie.*

* Quand la proposition est vraie, on lui affecte le chiffre 1 et dans le cas contraire on lui affecte le chiffre 0.

* On général, on met ces valeurs dans un tableau qu'on appelle **Table de vérité**.
  - Si on a une seul proposition P, il y'a deux possiblités:

P	1	0

- Si on a une deux propositions P et Q, il y'a 4 possibilités:

P	1	1	0	0
Q	1	0	1	0

- Pour n propositions il y'a 2^n possibilités.

1.1.2 Opération logiques:

La négation:

Définition 1.2 *Soit p une proposition donnée, on note $\overline{p}$ sa négation (ou son contraire), ainsi $\overline{p}$ sera fausse si p est vraie, et inversement $\overline{p}$ sera vraie si p est fausse.*

Exemple 1.1.2 *Soit P une proposition:*

P	$\overline{P}$
$x > 2$	$x \leq 2$
$x \in \mathbb{R}$	$x \notin \mathbb{R}$
A, B,C alignés	*ABC triangle*

Proposition 1.1.1 *La négation de la négation d'une proposition P est équivalente à P c'est-à-dire $\overline{\overline{P}}$ est P.*

La conjonction : le connecteur logique ET, "$\wedge$"

Définition 1.3 *Connecteur "et" noté "$\wedge$" : La proposition (P et Q) notée ($P \wedge Q$), ne sera vraie que si P est vraie et Q est vraie. $P \wedge Q$: Conjonction de P et Q.*

Sa table de vérité est donnée par:

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

Propriété: La proposition $P \wedge \overline{P}$ est fausse car

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

La disjonction : le connecteur logique OU, "$\vee$"

Définition 1.4 *Le connecteur logique OU porte sur deux propositions. La proposition (P ou Q) notée $P \vee Q$ est fausse si les deux propositions sont simultanément fausses, la proposition $P \vee Q$ est vraie dans tous les autres cas. $P \vee Q$: Disjonction de P et Q.*

Sa table de vérité est donnée par:

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

Propriété: La proposition $P \vee \bar{P}$ est toujours vraie car

P	$\bar{P}$	$P \vee \bar{P}$
1	0	1
0	1	1

L'implication : le connecteur logique Implcation, "$\Rightarrow$"

Définition 1.5 *Le connecteur logique Implication, porte sur deux propositions. La proposition (Si P alors Q) notée $P \Rightarrow Q$ est fausse lorsque l'on a simultanément la proposition P vraie et la proposition Q fausse, la proposition $P \Rightarrow Q$ est vraie dans tous les autres cas.*

Sa table de vérité est donnée par:

P	Q	$P \Rightarrow Q$
1	1	1
1	0	0
0	1	1
0	0	1

Théoréme Soient P et Q deux propositions alors on a $(P \Rightarrow Q) \Leftrightarrow (\bar{P} \vee Q)$.

Preuve. $P \Rightarrow Q$ est fausse dans l'unique cas où P est vraie et Q est fausse ou encore quand P et Q sont toutes deux fausses. $P \Rightarrow Q$ a donc les mêmes valeurs de vérité que $\bar{P} \vee Q$. ■

Théoréme Soient P, Q, R trois propositions. $\wedge$ est transitive c'est-à-dire

$$((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$$

Preuve. Vous démontrerez ce théorème à l'aide d'une table de vérité à 8 lignes. ■

***Equivalence logique:* le connecteur logique Equivalence, " $\Leftrightarrow$"**

Définition 1.6 *Le connecteur logique Equivalencei porte sur deux propositions. La proposition (P si et seulement si Q) notée $P \Leftrightarrow Q$ est vrai lorque l'on a simultanément P et Q vraies ou fausses. La proposition est fausse dans les autres cas.*

Sa table de vérité est donnée par:

P	Q	$P \Leftrightarrow Q$
1	1	1
1	0	0
0	1	0
0	0	1

Théoréme Soient P et Q deux propositions. Alors, $(P \Leftrightarrow Q) \Leftrightarrow ((P \Rightarrow Q) \wedge (Q \Rightarrow P))$.

Preuve. Il s'agit de vérifier que les deux propositions ont les mêmes valeurs de vérité.

P	Q	$P \Leftrightarrow Q$	$P \Rightarrow Q$	$Q \Rightarrow P$	$((P \Rightarrow Q) \wedge (Q \Rightarrow P))$
1	1	1	1	1	1
1	0	0	0	1	0
0	1	0	1	0	0
0	0	1	1	1	1

On a bien les mêmes valeurs de vérité dans les troisième et sixième colonnes, ce qui démontre le théorème. ■

Le mathématicien Morgan a enoncé les lois qui indiquent comment prendre la négation d'une conjection ou une disconjection.

Théoréme [Lois de de Morgan] Soient P et Q deux propositions
1- $\overline{P \wedge Q} \Leftrightarrow \bar{P} \vee \bar{Q}$
2- $\overline{P \vee Q} \Leftrightarrow \bar{P} \wedge \bar{Q}$

Preuve. On démontre ces équivalences à l'aide de tables de vérité.

P	Q	$p \wedge Q$	$\overline{P \wedge Q}$	$\bar{P}$	$\bar{Q}$	$\bar{P} \vee \bar{Q}$
1	1	1	0	0	0	0
1	0	0	1	0	1	1
0	1	0	1	1	0	1
0	0	0	1	1	1	1

P	Q	$p \vee Q$	$\overline{P \vee Q}$	$\bar{P}$	$\bar{Q}$	$\bar{P} \wedge \bar{Q}$
1	1	1	0	0	0	0
1	0	1	0	0	1	0
0	1	1	0	1	0	0
0	0	0	1	1	1	1

■

Théoréme Soient P, Q, R trois propositions logiques, alors nous avons:

1- $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$ et $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$. $\wedge$, $\vee$ Associatives.

2- $(P \wedge Q) \vee R \Leftrightarrow (P \vee R) \wedge (Q \vee R)$ et $(P \vee Q) \wedge R \Leftrightarrow (P \wedge R) \vee (Q \vee R)$. $\wedge$, $\vee$ Distributives.

3- $P \wedge Q \Leftrightarrow Q \wedge P$ et $P \vee Q \Leftrightarrow Q \vee P$. $\wedge$, $\vee$ Commutatives.

Preuve. Démontrons par exemple la première équivalence de "2" à l'aide d'une table de vérité (vous démontrerez le reste de manière analogue à titre d'exercice).

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

On lit effectivement les mêmes valeurs de vérité dans les cinquième et huitième colonnes.

■

1.1.3 Les quantificateurs

Le quantificateur universel, "$\forall$"

Définition 1.7 *Le symbole $\forall$ qui signifie « quel que soit » ou « pour tout » représente le quantificateur universel. Il doit toujours être suivi du signe d'appartenance $\in$.*

Exemple 1.1.3 $\forall x \in \mathbb{R}^+$, $x \geq 0$
« quelque soit x appartenant à $\mathbb{R}^+$, x est positif ou nul »

Le quantificateur existentiel, "$\exists$"

Définition 1.8 *Le symbole $\exists$ qui signifie « il existe au moins un . . . tel que » représente le quantificateur existentiel. On peut éventuellement rajouter un point d'exclamation pour montrer l'unicité. On a alors : $\exists!$ qui signifie « il existe un unique . . . tel que ».*

Exemple 1.1.4 *« Il existe un unique x appartenant à l'intervalle $[0,1]$ tel que: $x^2+4x+1=0$ » s'écrit:*

$$\exists! x \in [0;1],\ x^2+4x+1=0$$

Remarque 1.1.1 *L'ordre dans lequel on écrit les quantificateurs est trés important car il change la signification, par exemple*

$$\forall x \in \mathbb{R},\ \exists y \in \mathbb{R}, y > x \text{ vraie.}$$

Quel que soit le réel x, il existe au moins un réel x tel que y soit supérieur à x ». On peut toujours trouver un nombre supérieur à un nombre réel donné car l'ensemble $\mathbb{R}$ n'est pas borné. La proposition est vraie.
Inversons maintenant les quantificateurs

$$\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, y > x$$

« Il existe au moins un réel x tel que pour tout réel y, y soit supérieur à x ». Cette proposition cette fois est fausse car on ne peut pas trouver un réel inférieur à tous les autres. En effet l'ensemble $\mathbb{R}$ n'a pas de borne inférieur.

Exemple 1.1.5 *En utilisant les quantificateurs réécrire les propositions suivantes:*
1- P_1: L'équation $\sin x = x$ a une et une seule solution dans $\mathbb{R}$.
$P_1 \Leftrightarrow \exists!\ x \in \mathbb{R},\ \sin x = x.$
2- P_2: Le graphe de f coupe la droite d'équation $y = x$.
$P_2 \Leftrightarrow \exists x \in \mathbb{R},\ f(x) = x.$
3- P_3: Tout entier naturel est pair ou impair.
$P_3 \Leftrightarrow \forall n \in N,\ (\exists k \in \mathbb{N}, n = 2k \vee m = 2k+1).$

1.1.4 Types de raisonnements.

1/. Le raisonnement par l'absurde

On veut montrer qu'une proposition P est vraie. On suppose que c'est sa négation $\overline{P}$ qui est vraie et on montre que cela entraîne une proposition fausse.

Le schéma est le suivant:

Quand $\overline{P} \Rightarrow Q$ est une proposition vraie, et Q est une proposition fausse, on peut affirmer que P est une proposition vraie.

Exemple 1.1.6 *Montrons que si n est un entier strictement positif, alors n^2+1 n'est pas le carré d'un entier naturel.*

Supposons que n est un entier strictement positif et que n^2+1 est le carré d'un entier naturel m. On a donc

$$n^2+1=m^2,$$

alors $m^2-n^2=1$ ce qui donne que

$$(m-n)(m+n)=1,$$

Puisque le produit de ces deux nombres est égal à 1, alors $m+n\neq 0$, or $m+n$ est un entier relatif et puisque nous avons supposé que $m\geq 0$, on a $m+n\geq m>0$ et donc $m+n$ est un entier positif. Il s'ensuit que $m-n$ est entier positif. On sait que le produit entre des entiers positifs n'est égal à 1 que si chacun d' entre eux est égal à 1, on en deduit que

$$m-n=1,$$

ou encore

$$m=1+n,$$

alors

$$m^2=1+n^2+2n$$

puis,on a $n^2+1=m^2$ d'où par soustraction on trouve que $2n=0$.
Puisque n est strictement positif cela est une contraduction.

2/. Le raisonnement par contraposition:

Le schéma est le suivant:

Pour montrer que $P\Rightarrow Q$ est une proposition vraie, il suffit de montrer que $\overline{Q}\Rightarrow\overline{P}$ est une proposition vraie.

Exemple 1.1.7 *Soit $a,b\in\mathbb{R}$, montrons que*

$$a\neq 2 \text{ et } b\neq 2\Rightarrow ab-2a-2b+4\neq 0.$$

Par contraposée, nous allons montrer que

$$(ab-2a-2b+4)=0\Rightarrow a=2 \text{ ou } b=2).$$

On suppose que $(ab-2a-2b+4)=0$, or

$$\begin{aligned} ab-2a-2b+4 &= 0\Rightarrow a(b-2)-2(b-2)=0\\ &\Rightarrow (a-2)(b-2)=0\\ &\Rightarrow (a=2 \text{ ou } b=2)\end{aligned}$$

3/. Le raisonnement par un contre-exemple

Le schéma est le suivant:

Pour montrer qu'une proposition de la forme

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

est fausse, il suffit de trouver un x dans E tel que $P(x)$ est fausse.

Exemple 1.1.8 $\forall n \in \mathbb{N}$: *n est pair. Cette proposition est fausse, un contre exemple* $n = 7$, $7 \in \mathbb{N}$, 7 *impair.*

4/. Le raisonnement par Récurrence:

Le schéma est le suivant:

Montrer qu'une assertion, $P(n)$ dépendant de n est vrai pour tout $n \in \mathbb{N}$
1- On montre que $P(0)$ est vraie.
2- On suppose que $P(n)$ est vraie pour $n \geq 1$ et on démontre que $P(n+1)$ est vraie.
3- Enfin on conclut que $P(n)$ est vraie pour tout $n \in \mathbb{N}$

Exemple 1.1.9 *Montrons par récurrence que pour tout entier naturel* $n > 0$ *on a*

$$P(n) = \sum_{k=1}^{k=n} \frac{k}{2^k} = 2 - \frac{n+2}{2^n}$$

1- Pour $n = 1$, *on a* $\sum_{k=1}^{k=1} \frac{1}{2^1} = 2 - \frac{1+2}{2^1}$ *donc* $P(1)$ *vraie.*
2- Supposons que pour n *un entier strictement positif tel que* $P(n)$ *soit vraie et montrons* $P(n+1)$, *on a*

$$\begin{aligned} \sum_{k=1}^{k=n+1} \frac{k}{2^k} &= \left(\sum_{k=1}^{k=n} \frac{k}{2^k}\right) + \frac{n+1}{2^{n+1}} \\ &= 2 - \frac{n+2}{2^n} + \frac{n+1}{2^{n+1}} \\ &= 2 - \frac{n+3}{2^{n+1}} \\ &= P(n+1) \end{aligned}$$

3- on conclut que

$$\forall n > 0, \sum_{k=1}^{k=n} \frac{k}{2^k} = 2 - \frac{n+2}{2^n}.$$

1.2 Exercices

Exercice **1.1.** Soient P, Q deux propositions données:

1. Simplifier l'expression:
$$K = \left(\bar{P} \wedge Q\right) \vee \left(\bar{P} \wedge \bar{Q}\right) \vee (P \wedge Q)$$
2. Construire la table de vérité des propositions suivantes:
$$R = \overline{(P \vee Q)} \vee (\bar{P} \vee \bar{Q}) \text{ et } S = [P \Rightarrow (Q \Rightarrow R)] \Rightarrow R.$$

Exercice **1.2.** Former la négation des propositions suivantes:

1. $$[(P \Rightarrow Q) \vee R] \vee (P \wedge Q)$$
2. $$[(P \wedge Q) \wedge R] \Rightarrow (P \vee R).$$

Exercice **1.3.** Ecrire sous forme de propositions composées les énoncés suivants et donner leur négation:

1. Ce nombre est pair et premier.
2. Le soleil ne brille pas et la terre est ronde.
3. Si Mohammed joue à la flutte, alors il joue à la guitarre.

Exercice **1.4.** Ecrire à l'aide des quantificateurs logiques les assertions suivantes, puis donner leur négation.

1. Pour tout entier x, pour tout entier z, la relation $z < x$ implique la relation $z < x + 1$.
2. Pour chaque réel, je peux trouver un entier relatif tel que leur produit soit strictement plus grand que 1.
3. Pour chaque réel x, il existe un réel tel que leur somme soit strictement positif.
4. Soient f, g deux fonctions de $\mathbb{R}$ dans $\mathbb{R}$: f est inférieure à g.

Exercice **1.5.** Par l'absurde: Montrer que

1. Le nombre 0 n'a pas d'inverse.

2. $\dfrac{\ln(2)}{\ln(3)}$ est irrationnel.

3. $\forall x, y \geq 0 : \frac{x}{1+y} = \frac{y}{1+x} \Rightarrow x = y$.

Exercice **1.6.** Soit $n \in \mathbb{N}$, montrer par contraposée que: $2^n - 1$ premier implique que n premier.

Exercice **1.7.** Montrer par récurrence ce qui suit:

$$\begin{aligned} \sum_{k=1}^{n} (2k-1) &= n^2, \ n \in \mathbb{N}^*. \\ \sum_{k=1}^{n} k &= \frac{n(n+1)}{2}, \ n \in \mathbb{N}^*. \\ \sum_{k=1}^{n} k^2 &= \frac{n(n+1)(2n+1)}{6}, \ n \in \mathbb{N}^*. \end{aligned}$$

Exercice **1.8.** On définit pour tout entier $n \in \mathbb{N}$, $A_n = 3^{2n+2} - 2^{n+1}$. Montrer par récurrence que $\forall n \in \mathbb{N}$, A_n est divisible par 7.

1.3 Solutions

Exercice **1.1.** Soient P et Q deux propositions données.

1. Simplification de l'expression:

$$K = \left(\bar{P} \wedge Q\right) \vee \left(\bar{P} \wedge \bar{Q}\right) \vee (P \wedge Q)$$

En utilisant la table de vérités, on a

P	Q	$\bar{P} \wedge Q$	$\bar{P} \wedge \bar{Q}$	$\left(\bar{P} \wedge Q\right) \vee \left(\bar{P} \wedge \bar{Q}\right)$	$(P \wedge Q)$	K
1	1	0	0	0	1	1
1	0	0	0	0	0	0
0	1	1	0	1	0	1
0	0	0	1	1	0	1

on remarque que K a les même valeurs de vérité que $P \Rightarrow Q$, alors on deduit que $K \Leftrightarrow (P \Rightarrow Q)$.

2. La table de vérité des propriétés:

$$R = \overline{(P \vee Q)} \vee (\bar{P} \vee \bar{Q})$$

P	Q	$\bar{P}$	$\bar{Q}$	$(P \vee Q)$	$\overline{(P \vee Q)}$	$\bar{P} \vee \bar{Q}$	R
1	1	0	0	1	0	0	0
1	0	0	1	1	0	1	1
0	1	1	0	1	0	1	1
0	0	1	1	0	1	1	1

et

$$S = [P \Rightarrow (Q \Rightarrow R)] \Rightarrow R.$$

P	Q	R	$Q \Rightarrow R$	$[P \Rightarrow (Q \Rightarrow R)]$	S
1	1	0	0	0	1
1	0	1	1	1	1
0	1	1	1	1	1
0	0	1	1	1	1

Exercice **1.2.** La négation des propositions:

1.

$$\begin{aligned}\overline{[(P \Rightarrow Q) \vee R] \vee (P \wedge Q)} &= \overline{[(P \Rightarrow Q) \vee R]} \wedge \overline{(P \wedge Q)} \\ &= [\overline{(P \Rightarrow Q)} \wedge \overline{R}] \wedge \overline{(P \wedge Q)} \\ &= [P \wedge \overline{Q}) \wedge \overline{R}] \wedge \left(\overline{P} \vee \overline{Q}\right)\end{aligned}$$

2.

$$\begin{aligned}\overline{[(P \wedge Q) \wedge R] \Rightarrow (P \vee R)} &= [(P \wedge Q) \wedge R] \wedge \overline{(P \vee R)} \\ &= [(P \wedge Q) \wedge R] \wedge (\overline{P} \wedge \overline{R})\end{aligned}$$

Exercice **1.3.**

1. P: "x est pair", Q: "x est premier"
   $1 \Leftrightarrow P \wedge Q$
   Négation: $\overline{1} \Leftrightarrow \overline{P} \vee \overline{Q}$ c'est-à-dire "x est impair ou x n'est pas premier".

2. P : "Le soleil brille", Q: "la terre est ronde".
   $2 \Leftrightarrow \overline{P} \wedge Q$
   Négation: $\overline{2} \Leftrightarrow P \vee \overline{Q}$ c'est-à-dire " Le soleil brille **ou** la terre n'est pas ronde".

3. P : "Mohammed joue à la flutte, Q: "Mohammed joue à la guitarre"
   $3 \Leftrightarrow P \Rightarrow Q$
   Négation: $\overline{3} \Leftrightarrow P \wedge \overline{Q}$ c'est-à-dire " Mohammed joue à la flutte **et** il ne joue pas à la guitarre".

Exercice **1.4.** Les quantificateurs logiques:

1. $P_1 : \forall x \in \mathbb{N}, \forall z \in \mathbb{N}\ (z < x)) \Rightarrow (z < x + 1)$. Négation: $\overline{P_1} : \exists x \in \mathbb{N}, \exists z \in \mathbb{N}\ (z < x)) \wedge (z \geq x + 1)$.

2. $P_2 : \forall x \in \mathbb{R}, \exists z \in \mathbb{Z}\ /\ x.z > 1$.
   Négation: $\overline{P_2} : \exists x \in \mathbb{R}, \forall z \in \mathbb{Z}\ /\ x.z \leq 1$.

3. $P_3 : \forall x \in \mathbb{R}, \exists y \in \mathbb{R}\ /\ x + z > 0$.
   Négation: $\overline{P_3} : \exists x \in \mathbb{R}, \forall y \in \mathbb{R}\ /\ x + z \leq 0$.

4. $P_4 : \forall x \in \mathbb{R}\ f(x) \leq g(x)$.
   Négation: $\overline{P_4} : \exists x \in \mathbb{R}\ f(x) > g(x)$.

Exercice **1.5.** Raisonnement par l'absurde

1. Supposons que 0 ademet un inverse cela veut dire qu'on peut écrire $0 = \frac{1}{a}$.
   Alors $\exists a \in E$, tel que $a \times 0 = 1$,
   et $a \times 0 = a \times (0+0) = (a \times 0) + (a \times 0)$
   ce qui implique que $1 = 1 + 1 = 2$, contraduction, donc 0 n'a pas d'inverse.

2. $\dfrac{\ln(2)}{\ln(3)}$ est irrationnel
   Supposons que $\frac{ln(2)}{ln(3)}$ est rationnel alors $\frac{ln(2)}{ln(3)} = \frac{p}{q}$, avec $p \in \mathbb{Z}; q \in \mathbb{Z}^*$, p et q premiers entre eux.
   Alors $\frac{ln(2)}{ln(3)}$ est rationnel, donc $\frac{\ln(2)}{\ln(3)} = \frac{p}{q} \Rightarrow q\ln(2) = p\ln(3) \Rightarrow 2^q = 3^p$. Si $q \geq 1$ alors 2 divise 3^p et par suite 2 divise 3, absurde.
   On en déduit que $\frac{ln(2)}{ln(3)}$ est irrationnel.

3. Soient x, $y \geq 0$, Supposons que $\frac{x}{1+y} = \frac{y}{1+x}$ et $x \neq y$. On a

$$\frac{x}{1+y} = \frac{y}{1+x} \Rightarrow x\,(1+x) = y\,(1+y)$$

   ce qui implique que

$$x^2 - y^2 = y - x$$

   ce qui donne

$$(x-y)\,(x+y) = y - x.$$

   Puisque $y \neq x$ on peut divisé par $y - x \neq 0$. Alors on trouve

$$x + y = -1,$$

   contradition avec le faite que x, $y \geq 0$.

Exercice **1.6.** Soit $n \in \mathbb{N}$, montrer que $2^n - 1$ premier $\Rightarrow n$ premier.
Contraposée: n n'est pas premier $\Rightarrow 2^n - 1$ n'est pas premier
n n'est pas premier $\Rightarrow n = pq$ avec $p \neq 1$ et $p \neq n$, alors

$$\begin{aligned} 2^n - 1 &= 2^{pq} - 1 \\ &= (2^p)^q - 1. \end{aligned}$$

On pose $G(X) = X^q - 1$, on remarque que $G(1) = 0$ ce qui implique que

$$G(X) = (X-1)\,F(X),$$

alors

$$G(2^p) = (2^p)^q - 1 = (2^p - 1)\, F\,(2^p)$$

ce qui donne que $(2^p - 1)$ divise $(2^n - 1)$ et puisque on a $p \neq 1$ et $p \neq n$ donc $2^p - 1 \neq 1$ et $2^p - 1 \neq 2^n - 1$.
Conclusion: $(2^n - 1)$ n'est pas premier.

Exercice **1.7.** Raisonnement par récurrence :

$$\begin{aligned}
\sum_{k=1}^{n} (2k-1) &= n^2,\ n \in N^*, \\
\sum_{k=1}^{n} k &= \frac{n(n+1)}{2},\ n \in N^*, \\
\sum_{k=1}^{n} k^2 &= \frac{n(n+1)\,(2n+1)}{6},\ n \in N^*.
\end{aligned}$$

Rédigeons la troixième égalité, $\forall n \in N^* \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.
On pose

$$P(n) = \sum_{k=1}^{n} k^2 = \frac{n(n+1)\,(2n+1)}{6},$$

on décompose la démonstration en trois étapes:

1. **Vérification:** pour $n = 1$, on a bien que $1^2 = \frac{1\times 2\times 3}{6} = 1$ donc $P\,(1)$ est vraie.
2. **Hypothèse de récurrence:** supposons que $P\,(n)$ est vraie et montrons $P\,(n+1)$.
3. Il faut montrer que $\sum_{k=1}^{n+1} k^2 = \frac{(n+1)(n+2)(2(n+1)+1)}{6}$.

$$\begin{aligned}
\sum_{k=1}^{n+1} k^2 &= 1^2 + 2^2 + 3^2 + ... + n^2 + (n+1)^2 \\
&= \frac{n(n+1)\,(2n+1)}{6} + (n+1)^2,
\end{aligned}$$

par l'hypothèse de récurrence on trouve

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

Ainsi $P(n+1)$ est vraie.

Ce qui nous permet de conclure que pour tout entier naturel on a: $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

Exercice **1.8.** Montrons par récurrence que $\forall n \in \mathbb{N}$ A_n est divisible par 7.

1. **Vérification:** pour $n = 0$, on a bien que $A_0 = 7$.
2. **Hypothèse de récurrence:** suposons que A_n est divisible par 7 donc $\exists k \in \mathbb{N}$, $A_n = 7k$.
3. Il faut montrer que A_{n+1} est divisible par 7.
   On remarque que $A_{n+1} - 2A_n = 7\left(3^{2n+2}\right)$ ce qui implique que

$$A_{n+1} = 2A_n + 7\left(3^{2n+2}\right)$$

en utilisant l'hypothèse de récurrence, on obtient que

$$\begin{aligned} A_{n+1} &= 2(7k) + 7\left(3^{2n+2}\right) \\ &= 7\left(2k + 3^{2n+2}\right) \\ &= 7k', \quad k' \in \mathbb{N}. \end{aligned}$$

Ainsi $\forall n \in \mathbb{N}$, A_n est divisible par 7.

1.4 Exercices supplémentaires

Exercice **1.9.** Soient les quatre assertions suivantes:

$$\text{a) } \exists x \in \mathbb{R}\ \forall y \in \mathbb{R}\ y^2 > x,\ \text{c) } \forall x \in \mathbb{R}\ \forall y \in \mathbb{R}\ x + y > 0$$
$$\text{b) } \forall x \in \mathbb{R}\ \exists y \in \mathbb{R}\ x + y > 0, \text{d) } \exists x \in \mathbb{R}\ \forall y \in \mathbb{R}\ x + y > 0$$

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

Exercice **1.10.** Soient A, B, C, D des propositions.
- Montrer que:

$$(\mathrm{A}\ \vee\ \mathrm{B}) \wedge (\mathrm{C}\ \vee\ \mathrm{D}) \Leftrightarrow (\mathrm{A}\ \wedge\ \mathrm{C}) \vee (\mathrm{A}\ \wedge\ \mathrm{D}) \vee (\mathrm{B}\ \wedge\ \mathrm{C}) \vee (\mathrm{B}\ \wedge\ \mathrm{D}).$$

Application: Trouver les couples de réels (a, b) tels que:

$$\begin{cases} (a-2)(b-3) = 0 \\ (a-5)(b-7) = 0 \end{cases}.$$

Exercice **1.11.** Montrer que

$$\forall n \in \mathbb{N},\ n \geq 4 \Rightarrow n^2 \leq 2^n.$$

Exercice **1.12.** Montrer par récurrence que:

$$\forall n \in \mathbb{N},\ (1 + 2 + ... + n)^2 = 1^3 + 2^3 + ... + n^3.$$

Exercice **1.13.** Raisonnement par contraposition :

1. Soit n un entier naturel. Montrer que si n^2 est divisible par 3, alors n est divisible par 3.
2. Soit f une application de $\mathbb{R}$ dans $\mathbb{R}$, telle que $f(x) = 3x + 2$. Montrer que

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2).$$

Chapitre 2

Ensembles et applications.

Sommaire

2.1 Rappels de cours

2.1.1 Ensembles

Définition 2.1 *Un ensemble est une collection d'éléments que l'on peut énumérer ou définir par une propriété. On dit que cet ensemble est défini par* ***extension****, lorsqu'on définit un ensemble par une propriété, on dit que cet ensemble est défini par* ***compréhension****. Si a est un élément de E, on écrit $a \in E$ et on lit a appartient à E. Un ensemble qui ne contient aucun élément s'appelle : l'ensemble vide noté "ϕ"*

Complémentaire d'un ensemble

Définition 2.2 *Soit E un ensemble donné et soit $A \subset E$, le complémentaire de A dans E est l'ensemble noté $C_E A$ composé des éléments de E qui ne sont pas élément de A. On a alors*

$$a \in C_E A \Leftrightarrow a \in E \text{ et } a \notin A$$

Exemple 2.1.1 *Soit Soit E l'ensemble des entiers naturels inférieurs ou égaux à 10 et soit A l'ensemble des entiers naturels pairs inférieurs ou égaux à 10. On a donc*

$$A = \{0,\ 2,\ 4,\ 6,\ 8,\ 10\}$$

L'ensemble $C_E A$ sera donc l'ensemble des entiers naturels inférieurs ou égaux à 10 qui ne sont pas pairs. On a donc:

$$C_E A = \{1,\ 3,\ 5,\ 7,\ 9\}$$

Intersection de deux ensembles

Définition 2.3 *On appelle intersection de deux sous-ensembles A et B dans un ensemble E, l'ensemble noté : $A \cap B$ (A inter B) constitué des éléments communs à A et B. On a donc:*

$$x \in A \cap B \Leftrightarrow x \in x \in A \text{ et } x \in B.$$

Exemple 2.1.2 *Soit Soit A l'ensemble des entiers naturels inférieurs ou égaux à 10 et soit B l'ensemble des entiers naturels premiers inférieurs ou égaux à 10. On a donc*

$$A = \{0,\ 1,\ 2,3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10\}$$

$$B = \{2,\ 3,\ 5,\ 7\}$$

on a donc

$$A \cap B = \{2,\ 3,\ 5,\ 7\}$$

Union de deux ensembles

Définition 2.4 *On appelle union de deux sous-ensembles A et B dans un ensemble E, l'ensemble noté: $A \cup B$ (A union B) constitué des éléments qui appartiennent à A ou à B. On peut alors écrire :*

$$x \in A \cup B \Leftrightarrow x \in A \text{ ou } x \in B$$

Exemple 2.1.3 *Soit A l'ensemble des entiers naturels inférieurs ou égaux à 10 et soit B l'ensemble des entiers naturels premiers inférieurs ou égaux à 10. On a donc*

$$A = \{0,\ 1,\ 2,3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10\},$$

$$B = \{2,\ 3,\ 5,\ 7\},$$

alors

$$A \cup B = \{0,\ 1,\ 2,3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10\}$$

Inclusion et égalité

Définition 2.5 *Soient A et B deux ensembles donnés, on dira que A est inclus dans B, ou que A est une partie de B ou encore que A est un sous ensemble de B, si et seulement si tout élément de A est aussi un élément de B. On note dans ce cas $A \subset B$.*
On dira que A est égal à B, si on a la double inclusion $A \subset B$ et $B \subset A$

$$(A = B) \Leftrightarrow (A \subset B \text{ et } B \subset A)$$

Remarques 2.1.1 *1- Lorsque l'ensemble A est inclus dans l'ensemble B, on a alors :*

$$A \subset B \Rightarrow A \cap B = A$$

2- Lorsque les ensembles A et B sont disjoints, ils ne possèdent aucun élément commun, leur intersection est donc vide, on a donc:

$$A \cap B = \phi \Leftrightarrow A \text{ et } B \text{ sont disjoints}$$

C'est le cas avec l'ensemble A et sont complémentaire $C_E A$, on a donc:

$$A \cap C_E A = \phi.$$

3- Lorsque l'ensemble A est inclus dans l'ensemble B, on a alors:

$$A \subset B \Rightarrow A \cup B = B.$$

4- L'union de l'ensemble A et de son complémentaire donne l'ensemble E, c'est-à-dire: $A \cup C_E A = E$.

Ensemble des parties d'un ensemble

Définition 2.6 *Soit E un ensemble donné, on note $\mathcal{P}(E)$, l'ensemble des parties de E*

$$\mathcal{P}(E) = \{A,\ A \subset E\}$$

Définition 2.7 *On appelle cardinal d'un ensemble, le nombre de ses éléments et on le note card.*

Par exemple, si $E = \{a.b, c\}$ alors $card\ (E) = 3$.

Différence et différence symétrique

Définition 2.8 *Soient A, B deux sous ensembles d'un ensemble E, on note $A \setminus B$ la différence de A et B, comme étant l'ensemble des éléments de A n'appartenant pas à B*

$$\begin{aligned} A \setminus B &= \{x \in E;\ x \in A \text{ et } x \notin B\} \\ &= A \cap C_E B \end{aligned}$$

La différence symétrique de A et B est l'ensemble noté $A \triangle B$ défini par

$$\begin{aligned} A \triangle B &= (A \setminus B) \cup (B \setminus A) \\ &= (A \cup B) \setminus (A \cap B) \end{aligned}$$

Lois De Morgan

Règle 1: Soit A et B deux sous-ensembles de l'ensemble E. On a alors:

$$\begin{aligned} C_E(A \cap B) &= C_E A \cup C_E B \\ C_E(A \cup B) &= C_E A \cap C_E B \end{aligned}$$

Règle 2: Soit trois sous-ensembles A, B et C d'un ensemble E. On a alors les égalités suivantes :

$$\begin{aligned} \cap \text{ est distributive par rapport à } \cup &: A \cap (B \cup C) = (A \cap B) \cup (A \cap C). \\ \cup \text{ est distributive par rapport à } \cap &: A \cup (B \cap C) = (A \cup B) \cap (A \cup C). \end{aligned}$$

2.1.2 Notion d'Applications

Définition 2.9 *Soient E et F deux ensembles. Une application f de E dans F est un "procédé" qui permet d'associer à chaque élément x de E un unique élément y de F ; cet élément y est alors noté $y = f(x)$, on l'appelle l'image de x et on dit que x est un antécédent de y par . On dit que E est l'ensemble de départ de f et que F est l'ensemble d'arrivée de f. On note*

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

Exemple 2.1.4 *1- On définit une application f en prenant : $E = \{a, b, c\}$, $F = \{1, 2, 3, 4\}$, $f(a) = f(b) = 1$, $f(c) = 4$. Alors, l'image de c est 4 et 1 a deux antécédents: a et b.*
2- L'application "identité"

$$\begin{aligned} f : \quad E &\longrightarrow E \\ x &\longmapsto x \end{aligned}$$

Bijection - Injection - Surjection

Définition 2.10 *Soit $f : E \to F$ une application.*
*1 – On dit que f est **surjective** si chaque élément y de F est l'image d'au moins d'un élément de E, c'est-à-dire si pour chaque élément y de F, l'équation $y = f(x)$ a au moins une solution dans E, ce qui s'écrit :*

$$\forall y \in F,\ \exists x \in E;\ y = f(x)$$

*2 – On dit que f est **injective** si chaque élément y de F est l'image d'un élément de E au plus, ou encore, si pour chaque élément y de F, l'équation $y = f(x)$ a au plus une solution dans E, ce qui s'écrit:*

$$\forall x_1, x_2 \in E; \quad f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

*3 – On dit que f est **bijective** si et seulement si elle est injective et surjective à la fois.*

Exemple 2.1.5 *L'application* $\begin{array}{rccc} f: & \mathbb{R}_+ & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & x^2 \end{array}$ *est bijective, car pour chaque réel y, il existe un et un seul réel x tel que $y = x^2$.*

Composition des applications

Soient $f : E \to F$ et $g : F \to G$ deux applications. On définit une application de E dans G notée $g \circ f$ en posant

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

On l'appelle application composée de g et f.

Remarque 2.1.1 *Soient f et g deux éléments de $\mathcal{F}(E, E)$; les deux applications $f \circ g$ et $g \circ f$ sont définies, mais en général elles ne sont pas égales.*

Exemple 2.1.6 *Par exemple, si on a*

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & x^2 \end{array} \quad et \quad \begin{array}{rccc} g: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & 4x \end{array},$$

alors

$$\begin{array}{rccc} f \circ g: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & 16x^2 \end{array} \quad et \quad \begin{array}{rccc} g \circ f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & 4x^2 \end{array},$$

on remarque que ces deux applications sont différentes.

Application réciproque (inverse)

Définition 2.11 *Soit $f : E \longrightarrow F$ Soit B un sous-ensemble de F. On appelle image réciproque de B par f l'ensemble des éléments x de E dont l'image $f(x)$ par f est dans B. C'est un sous-ensemble de E ; on le note $f^{-1}(B)$. On a*

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

Image directe

Définition 2.12 *Soit A un sous-ensemble de E. On appelle image directe de A par f l'ensemble des images $f(x)$ des éléments x de A. C'est un sous ensemble de F; on le note $f(A)$. On a donc pour tout élément y de F:*

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

L'ensemble $f(E)$ est aussi appelé l'image de f.

Egalité

Définition 2.13 *Soient $f : E \to F$ et $f_1 : E' \to F'$ deux applications. On dit qu'elles sont **égales** et on note $f = f_1$ si les trois conditions suivantes sont vérifiées:*

1. $E = E'$,
2. $F = F'$
3. $\forall x \in E, f(x) = f_1(x)$.

Restriction-Prolongement

Définition 2.14 *Soient E et F deux ensembles, E_1 un sous-ensemble de E, $f : E \to F$ et $f_1 : E_1 \to F$. On suppose que pour tout élément x de E_1, on a $f(x) = f_1(x)$. Alors, on dit que f_1 est la restriction de f à E_1 et que f est un prolongement de f_1 à E. On note $f_1 = f\mid_{E_1}$.*

2.2 Exercices

Exercice **2.1.** Soient A, B et C trois ensembles donnés, montrer que $A \cap C = A \cup B$ si et seulement si $B \subset A \subset C$.

Exercice **2.2.** Soient A, B, C trois parties d'un ensemble E. Donner une écriture simplifiée des sous-ensembles suivants:

1. $[A \cup (A \cap B)] \cap B$.
2. $(A \cap B) \cup (A \cap C_E(B))$.
3. $C_E(A \cup B) \cap (C \cup C_E(A))$.
4. $[(A \cup B) \cap (B \cap C)] \cup (A \cup C)$.
5. $(A \cup B) \cap [(B \cap C) \cup (A \cup C)]$.

Exercice **2.3.** Soient A et B deux sous-ensembles d'un ensemble E.

1. La différence symétrique de deux ensembles est-elle commutative?.
2. Expliciter les ensembles suivants: $A \triangle \emptyset$, $A \triangle A$ et $A \triangle B$ si $A \subset B$.
3. Expliciter l'ensemble $(A \triangle B) \cup (A \triangle C_E(B))$.

Exercice **2.4.** Les fonctions suivantes sont elles des applications?

$$\begin{cases} f_1 & \mathbb{R} \longrightarrow \mathbb{R} \\ & x \longmapsto x^2 + 1 \end{cases}, \quad \begin{cases} f_2 & \mathbb{R} \longrightarrow \mathbb{R} \\ & x \longmapsto e^{(x+2)} \end{cases}, \quad \begin{cases} f_3 & \mathbb{R} \longrightarrow \mathbb{R} \\ & x \longmapsto \sqrt{1-x^2} \end{cases}.$$

1. Sont-elles injectives, surjectives?.

Exercice **2.5.** Soit l'application f définie comme suit: $f : \mathbb{R} \to \mathbb{R}$ telle que $f(x) = |x+1|$. f ainsi définie est-elle injective ? surjective ?bijective ?.

Exercice **2.6.** On considère quatre ensembles A, B, C, D et des applications

$$f : A \to B, \quad g : B \to C, \quad h : C \to D.$$

Montrer que:

1. $(g \circ f)$ injective$\Rightarrow$ f injective.
2. $(g \circ f)$ surjective$\Rightarrow$ g surjective.
3. $((g \circ f)$ et $(h \circ g)$ bijectives$)\Rightarrow(f, g$ et h sont bijectives$)$.

2.3 Solutions

Exercice **2.1.** Soit A, B et C trois ensembles donnés, Il faut montrer que $A \cap C = A \cup B$ si et seulement si $B \subset A \subset C$.
"$\Leftarrow$" Hypothèse $B \subset A \subset C$,
$B \subset A \Rightarrow A \cup B = A$ et $A \subset C \Rightarrow A \cap C = A$ donc $B \subset A \subset C \Rightarrow A \cap C = A \cup B$
"$\Rightarrow$" Hypothèse $A \cap C = A \cup B$,
on sait que $B \subset A \cup B$ or $A \cap C = A \cup B$ donc $B \subset A \cap C$ et par suite $B \subset A$.
D'un autre côté on sait que $A \subset A \cup B$ or $A \cap C = A \cup B$ donc $A \subset A \cap C$ et par suite $A \subset C$. En conclusion $B \subset A \subset C$.

Exercice **2.2.**

1. De $A \cap B \subset A$ il vient: $A \cup (A \cap B) = A$. D'où: $(A \cup (A \cap B)) \cap B = A \cap B$.

2. En factorisant par A, on a:

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

   Or, $B \cup C_E(B) = E$ et $A \cap E = A$. Ainsi, $(A \cap B) \cup (A \cap C_E(B)) = A$.

3. En distribuant, on a :

$$C_E(A \cup B) \cap (C \cup C_E(A)) = [C_E(A \cup B) \cap C] \cup [C_E(A \cup B) \cap C_E(A)].$$

   De $A \subset A \cup B$ il vient: $C_E(A \cup B) \subset C_E(A)$. D'où:

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

   On a donc:

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

   Remarquons que $C_E(A \cup B) \cap C$ est un sous-ensemble de $C_E(A \cup B)$. On peut donc écrire :

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

   Finalement,

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

4. On remarque que $B \cap C \subset B \subset A \cup B$. D'où $(A \cup B) \cap (B \cap C) = B \cap C$.
   On a donc:
   $$[(A \cup B) \cap (B \cap C)] \cup (A \cup C) = (B \cap C) \cup (A \cup C).$$

   De même, on remarque que $B \cap C \subset C \subset A \cup C$. D'où $(B \cap C) \cup (A \cup C) = A \cup C$.
   Finalement,
   $$[(A \cup B) \cap (B \cap C)] \cup (A \cup C) = A \cup C.$$

5. On remarque que $B \cap C \subset C \subset A \cup C$. D'où $(B \cap C) \cup (A \cup C) = A \cup C$.
   Ainsi,
   $$(A \cup B) \cap [(B \cap C) \cup (A \cup C)] = (A \cup B) \cap (A \cup C).$$

   Finalement, en factorisant par A, on obtient:
   $$(A \cup B) \cap [(B \cap C) \cup (A \cup C)] = A \cup (B \cap C).$$

Exercice **2.3.**

1. Elle est commutative car " $\cup$ " l'est.

2. Soient A, B deux parties de E. Utilisant que $A \backslash B = A \cap C_E(B)$, on a :
   $A \triangle B = (A \cap C_E(B)) \cup (B \cap C_E(A))$. Ainsi, pour toute partie A de E,
   $$\begin{aligned} A \triangle \emptyset &= (A \cap C_E(\emptyset)) \cup (\emptyset \cap C_E(A)) = (A \cap E) \cup \emptyset = A \cup \emptyset = A, \\ A \triangle A &= (A \cap C_E(A)) \cup (A \cap C_E(A)) = \emptyset \cup \emptyset = \emptyset. \end{aligned}$$

   Supposons à présent $A \subset B$. On a alors: $A \cap C_E(B) = \emptyset$. D'où:
   $$A \triangle B = (A \cap C_E(B)) \cup (B \cap C_E(A)) = \emptyset \cup (B \cap C_E(A)) = B \backslash A.$$

   Remarquons que l'on a aussi : $A \triangle B = (A \cup B) \backslash (A \cap B)$.

3. Soient A, B deux parties d'un ensemble E. Afin d'alléger les écritures,
   posons $M = (A \triangle B) \cup (A \triangle C_E(B))$. On a:
   $$M = [(A \cap C_E(B)) \cup (B \cap C_E(A))] \cup [(A \cap B) \cup (C_E(B) \cap C_E(A))].$$

   L'union étant associative et commutative, on peut réarranger l'ordre des termes:
   $$M = \underbrace{[(A \cap C_E(B)) \cup (A \cap B)]}_{= A \cap (C_E(B) \cup B)} \cup \underbrace{[(B \cap C_E(A)) \cup (C_E(B) \cap C_E(A))]}_{= (B \cup C_E(B)) \cap C_E(A)}.$$

Or, $C_E(B) \cup B = E$. Ainsi,

$$M = [A \cap E] \cup [E \cap C_E(A)] = A \cup C_E(A) = E.$$

Finalement, $(A \triangle B) \cup (A \triangle C_E(B)) = E$.

Exercice **2.4.** $\forall x \in \mathbb{R}$, $f_1(x) \in \mathbb{R}$ ce qui implique que f_1 est une application.
$\forall x \in \mathbb{R}$, $f_2(x) \in \mathbb{R}$ ce qui implique que f_2 est une application.
f_3 n'est pas une application car Pour $x = -2$; $f_3(-2) = \sqrt{-3}$ n'est pas d´efinie.
Injectivités des fonctions:
f_1 n'est pas injective: $f_1(1) = f_1(-1) = 2$ ce qui implique que f_1 n'est pas injective.
f_2 est injective: Soient x_1, $x_2 \in \mathbb{R}/\ f_2(x_1) = f_2(x_2) \Rightarrow e^{(x_1+2)} = e^{(x_2+2)} \Rightarrow x_1 = x_2$.
f_3 n'est pas injective: $f_3(1) = f_3(-1) = 0$ ce qui implique que f_3 n'est pas injective.
Surjectivités des fonctions:
$\forall x \in \mathbb{R}$, $f_1(x) \geq 1 \Rightarrow f_1^{-1}(-3)$ n'existe pas ce qui implique que f_1 n'est pas surjective.
$\forall x \in \mathbb{R}$, $f_2(x) > 0 \Rightarrow f_2^{-1}(-2)$ n'existe pas ce qui implique que f_2 n'est pas surjective.
$\forall x \in \mathbb{R}$, $f_3(x) > 0 \Rightarrow f_3^{-1}(-1)$ n'existe pas ce qui implique que f_3 n'est pas surjective.

Exercice **2.5.** Soit l'application$f$ définie par: $f : \mathbb{R} \to \mathbb{R}$ telle que $f(x) = |x + 1|$.
Commençons par écrire l'expression de f sans la valeur absolue:

$$f(x) = \begin{cases} x + 1 & \text{si } x \geq -1 \\ -x - 1 & \text{si } x \leq -1 \end{cases}$$

Injectivité:
- Soient $x_1, x_2 \in]-\infty, -1]$, $f(x_1) = f(x_2) \Rightarrow -x_1 - 1 = -x_2 - 1 \Rightarrow x_1 = x_2$.
- Soient $x_1, x_2 \in [-1, +\infty[$, $f(x_1) = f(x_2) \Rightarrow x_1 + 1 = x_2 + 1 \Rightarrow x_1 = x_2$.
- Soit $x_1 \in]-\infty, -1]$, $x_2 \in [-1, +\infty[$, $f(x_1) = f(x_2) \Rightarrow -x_1 - 1 = x_2 + 1 \Rightarrow x_2 = -x_1 - 2$.

Il est clair que f n'est pas injective, pour le confirmer nous devons fournir un contre exemple, en effet considérons $x_2 = 0 \in [-1, +\infty[, -x_2 - 2 = x_1$ alors $x_1 = -2 - 0 = -2 \in]-\infty, -1]$ et $f(x_1) = f(-2) = 1$, $f(x_2) = f(0) = 1$, donc $f(0) = f(-2) = 1$ mais $x_1 = -2 \neq x_2 = 0$. Donc f n'est pas injective.

Surjectivité: Soit $y \in \mathbb{R}, \exists x \in \mathbb{R}$ tel que $y = f(x)$
Comme contre exemple $y = -1$, alors l'équation $y = -1 = f(x) = |x + 1|$ n'a pas de solution car $|x + 1| \geq 0$.
Alors f n'est pas surjective.
f n'est ni **injective** ni **surjective** et par suite f **n**'est pas **bijective**.

Exercice **2.6.** On considère les ensembles A, B, C, D et des applications $f : A \to B$, $g : B \to C$, $h : C \to D$:

1. $(g \circ f)$ injective $\Rightarrow$ f injective.
   Supposons que $(g \circ f)$ injective, soient x_1, $x_2 \in A$, tel que $f(x_1) = f(x_2)$ donc

   $$(g \circ f)(x_1) = (g \circ f)(x_2)$$

   (car g est une application) or on a déjà supposé que $(g \circ f)$ injective donc $x_1 = x_2$, alors

   $$f(x_1) = f(x_2) \Rightarrow x_1 = x_2,$$

   d'où f est injective.

2. $(g \circ f)$ surjective $\Rightarrow$ g surjective.
   Soit $z \in C$, comme $(g \circ f)$ est supposée surjective alors

   $$\exists x \in A, z = (g \circ f)(x),$$

   ainsi $z = g(f(x))$, soit encore

   $$\exists y = f(x) \in B, z = g(y),$$

   alors on a exactement la définition de la surjectivité de g.

3. ($(g \circ f)$ et ($h \circ g$) bijectives) $\Rightarrow$ (f, g et h sont bijectives)
   Comme $(g \circ f)$ est bijective, alors en particulier $(g \circ f)$ est surjective et donc g est surjective.
   D'un autre côté puisque $(h \circ g)$ est bijective, elle est en particulier injective, donc par la première question on en déduit que g est injective. Ainsi g est injective et surjective et par suite g est bijective (et dans ce cas g^{-1} existe).
   De plus, on peut écrire $f = g^{-1} \circ (g \circ f)$ qui est bijective, car on a composée d'applications bijectives. On procède de la même manière pour h, en écrivant $h = (h \circ g) \circ g^{-1}$, donc h est bijective.

2.4 Exercices supplémentaires

Exercice **2.7.** Montrer par contraposition les assertions suivantes, E étant un ensemble:

1. $\forall A, B \in P(E)$, $(A \cap B = A \cup B) \Rightarrow A = B$.
2. $\forall A, B, C \in P(E)$, $(A \cap B = A \cap C$ et $A \cup B = A \cup C) \Rightarrow B = C$.

Exercice **2.8.** Soient E, F, G trois ensembles, f une application de E vers F et g une application de F vers G.

1. Montrer que si $g \circ f$ est injective et f est surjective alors g est injective.
2. Montrer que si $g \circ f$ est surjective et g est injective alors f est surjective.

Exercice **2.9.** Soient x et y deux nombres rationnels. Montrons l'équivalence:

$$x + \sqrt{2}y = 1 \Leftrightarrow (x = 1 \text{ et } y = 0).$$

Exercice **2.10.** Soit X un ensemble. Pour $f \in F(X, X)$, on définit $f^0 = id$ et par récurrence pour $n \in \mathbb{N}$ $f^{n+1} = f^n \circ f$.

1. Montrer que $\forall n \in \mathbb{N}$ $f^{n+1} = f \circ f^n$.
2. Montrer que si f est bijective alors $\forall n \in \mathbb{N}$ $(f^{-1})^n = (f^n)^{-1}$.

Chapitre 3

Relations binaires sur un ensemble

Sommaire

3.1 Rappels de cours

3.1.1 Relation Binaires

Définition 3.1 *Une relation binaire $\Re$ sur un ensemble E est une propriété portant sur les couples d'éléments de E. On notera $a\Re b$ le fait que la propriété est vraie pour le couple $(a, b) \in E \times E$.*

Définition 3.2 *Soit $\Re$ une relation sur E. Pour tous x, y, $z \in E$, on dit que $\Re$ est:*

1. *Reflexive si: $\forall\ x \in E$, $x\Re x$.*
2. *Symétrique si: $\forall\ x,y \in E$, $x\Re y \Longrightarrow y\Re x$.*
3. *Transitive si: $\forall\ x, y, z \in E$, $[x\Re y$ et $y\Re z] \Longrightarrow x\Re z$.*
4. *Anti-symétrique si: $\forall\ x,y \in E$, $[x\Re y$ et $y\Re x] \Longrightarrow x = y$.*

3.1.2 Relation d'équivalence

Définition 3.3 *Une relation binaire $\Re$ sur un ensemble E est une relation d'équivalence si et seulement si elle est réflexive, symétrique et transitive.*

Exemple 3.1.1 *Soit $E = \mathbb{Z}$, Soit $\Re$ définie par*

$$\forall n, m \in \mathbb{Z} n \Re m \Leftrightarrow \exists k \in \mathbb{Z},\ n - m = 2$$

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

$$n \Re m \Leftrightarrow n - m = 2.k, k \in \mathbb{Z}$$

i) $\Re$ est réflexive: $n \Re n$ alors $\forall n \in \mathbb{N}$, $n - n = 2.0$ donc $\Re$ est réflexive.
ii) si $n \Re m$ alors on a $n - m = 2.k$ ce qui implique que $m - n = -2.k = 2k'$, $k, k' \in \mathbb{Z}$ alors $m \Re n$ la relation $\Re$ est symétrique.
iii) $\Re$ est transitive: on a

$$\begin{cases} \text{si } n \Re m \text{ alors on a } n - m = 2.k \\ \text{si } m \Re l \text{ alors on a } m - l = 2.k' \end{cases}, \quad k, k' \in \mathbb{Z}\,,$$

alors on trouve $n - l = 2.k''$, $k'' = (k + k') \in \mathbb{Z}$ donc on a $n \Re l$, la relation $\Re$ est transitive. Finalement , on a i), ii) iii) donc $\Re$ est une relation d'équivalence.

3.1.3 Classe d'équivalence.

Définition 3.4 *Soit $\Re$ une relation d'équivalence sur E, on appelle classe d'équivalence d'un élément a de E, l'ensenmble des éléments de E en relation avec a par $\Re$, noté*

$$C(a) \text{ ou bien } \dot{a} = \{x \in E :\ x \Re a\}$$

La classe d'équivalence $\dot{a}$ est non vide car $\Re$ est réflexive et contient de ce fait au moins a. On notera par

$$E/\Re = \left\{\dot{a},\ a \in E\right\}$$

l'ensemble des classes d'équivalence (appelé l'ensemble quotient) de E par la relation $\Re$.

Exemple 3.1.2 *Dans l'exemlpe précédant calculons $\dot{3} = \{x \in \mathbb{Z} \ / \ x \Re 3\}$, on a $x \Re 3 \Leftrightarrow x - 3 = 2k$ alors $x = 2k+3$, $k \in \mathbb{Z}$, $x = 2k+3$ sont en relation avec 3, $\dot{3} = \{2k + 3 \ / \ k \in \mathbb{Z}\}$.*

Propriété: Si $\Re$ est une relation d'équivalence sur E et si a, $b \in E$ vérifient $a \Re b$, alors a et b ont la même classe d'équivalence

Théoréme Soit $\Re$ une relation d'équivalence sur E. Les classes d'équivalence $(C(x))_{x \in E}$ constituent une partition de E.

3.1.4 Relation d'ordre

Définition 3.5 *Une relation binaire $\Re$ sur E est une relation d'ordre si et seulement si elle est réfexive, antisymétrique et transitive.*

Exemple 3.1.3 *Soit $\Re$ la relation définie sur $\mathbb{N}^*$ par la relation "x divise y", vérifions qu'elle est antisymétrique*

$$\begin{aligned} x\Re y &\iff \exists k \in \mathbb{N}^* : y = kx, \\ y\Re x &\iff \exists k' \in \mathbb{N}^* : x = k'y, \end{aligned}$$

alors $kk^{'} = 1$, comme k et $k^{'} \in \mathbb{N}^*$, on trouve $k = k' = 1$ c'est-à-dire $x = y$.

Définition 3.6 *Une relation d'ordre sur E est dite totale si deux éléments quelconques de E sont toujours comparables : pour tout $x, y \in E$, on a $x\Re y$ ou $y\Re x$. Dans le cas contraire, on dit que l'ordre est partiel.*

Exemple 3.1.4 *Dans $\mathbb{Z}^*$ on définit la relation $\Re$ par : $a \preccurlyeq b$ si a divise b.*

$$\forall a, b \in \mathbb{Z}^*, a \preccurlyeq b \Longleftrightarrow \exists k \in \mathbb{Z}; b = k.a$$

1. Montrons que $\Re$ est une relation d'ordre.
i). $\Re$ est une relation reflexive:

$$\forall a \in \mathbb{Z}^*, \exists k = 1 \in \mathbb{Z}; a = k.a$$

donc

$$\forall a \in \mathbb{Z}, a \preccurlyeq a$$

ce qui montre que est $\Re$ une relation reflexive.
ii). $\Re$ est une relation antisymétrique: $\forall a, b \in \mathbb{Z}^*$,

$$(a \preccurlyeq b) \wedge (b \preccurlyeq a) \Leftrightarrow (\exists k_1 \in \mathbb{Z}; b = k_1.a) \wedge (\exists k_2 \in \mathbb{Z};\ a = k_2.b)$$

alors

$$(\exists k_1 \in \mathbb{Z}; b = k_1.a) \wedge (\exists k_2 \in \mathbb{Z};\ a = k_2.b) \wedge b = k_1k_2.b$$

ce qui implique que

$$(\exists k_1 \in \mathbb{Z}; b = k_1.a) \wedge (\exists k_2 \in \mathbb{Z};\ a = k_2.b) \wedge k_1k_2 = 1,\ \ car\ b \neq 0$$

alors

$$b = a, car\ \forall k_1, k_2 \in \mathbb{Z}, k_1 k_2 = 1 \Rightarrow k_1 = k_2 = 1$$

donc

$$\forall a, b \in \mathbb{Z}^*, a \preccurlyeq b \wedge b \preccurlyeq a \Rightarrow b = a$$

ce qui montre que $\Re$ *est antisymétrique.*
iii). $\Re$ *est une relation transitive:* $\forall a, b, c \in \mathbb{Z}^*$,

$$a \preccurlyeq b \wedge b \preccurlyeq c \Leftrightarrow \exists k_1 \in \mathbb{Z}; b = k_1.a \wedge \exists k_2 \in \mathbb{Z}; c = k_2.b$$

ce qui implique

$$\exists k = k_1 k_2 \in \mathbb{Z};\ c = k.a$$

alors

$$a \preccurlyeq c$$

ce qui montre que $\Re$ *est transitive.*
De i) ii) et iii), on déduit que $\Re$ *est une relation d'ordre.*
2. L'ordre est-il total ?
L'ordre est partiel, car si on considére $a = 2$ *et* $b = 3$, *alors* a *et* b *ne sont pas comparables.*

Définition 3.7 *Une relation binaire est un ordre strict si elle est transitive et vérifie*

$$x \Re y \Rightarrow x \neq y.$$

Exemple 3.1.5 *L'inégalité stricte* $<$ *définit un ordre strict sur* $\mathbb{N}$, $\mathbb{Z}$ *et* $\mathbb{R}$.

3.1.5 Plus petit, Plus grand élément

Définition 3.8 *Si X est une partie non vide de E muni de la relation d'ordre $\leq$.*

1) L'élément $\alpha \in X$ est le plus grand élément de X si est seulement si

$$\forall x \in X, x \leq \alpha.$$

2) L'élément $\alpha \in X$ est un majorant de X si est seulement si

$$\forall x \in X, x \leq \alpha.$$

3) L'élément $\alpha \in X$ est l'élément maximal de X si est seulement si

$$\forall x \in X, [\alpha \leq x \Rightarrow x = \alpha] .$$

3.2 Exercices

Exercice **3.1.** Soit $\Re$ la relation définie sur par:

$$x\Re y \Leftrightarrow x^2 - y^2 = x - y$$

1. Montrer $\Re$ que est une relation d'équivalence.
2. Déterminer la classe d'équivalence de pour tout réel x.

Exercice **3.2.** Les relations $\Re$ définies ci-dessous sont-elles des relations d'ordre sur $\mathbb{R}$.

1. $\forall x, y \in \mathbb{R}$, $x\Re y \Leftrightarrow x \leq y$,
2. $\forall x, y \in \mathbb{R}$, $x\Re y \Leftrightarrow e^x \leq e^y$,
3. $\forall x, y \in \mathbb{R}$, $x\Re y \Leftrightarrow x - y \in \mathbb{N}$.

Exercice **3.3.** Déterminer sur $\mathbb{R}$ les classes d'équivalence et la décomposition des fonctions correspondantes des relations suivantes:

$$\begin{aligned} x\Re_1 y &\Leftrightarrow x + x^{-1} = y + y^{-1}, \quad 0\Re_1 0 \\ x\Re_2 y &\Leftrightarrow x^4 - x^2 = y^4 + y^2, \quad 0\Re_2 0. \end{aligned}$$

Exercice **3.4.** Soit $\Re_1$ la relation définie sur $]1, +\infty[$ par:

$$x\Re_1 y \Longleftrightarrow \frac{x}{1+x^2} \geq \frac{y}{1+y^2}$$

Montrer que $\Re_1$ est une relation d'ordre total.

Exercice **3.5.** On définit dans $\mathbb{N}^*$ la relation $\Re$ par:

$$x\Re y \Longleftrightarrow x \text{ divise } y.$$

1. Vérifier que $\Re$ est une relation d'ordre et dite si l'ordre est total.

Exercice **3.6.** On définit dans $\mathbb{Z}$ la relation $\Re$ par:

$$x\Re y \Leftrightarrow \frac{5}{(x-y)}.$$

1. Vérifier que $\Re$ est une relation d'équivalence.
2. Déterminer l'ensemble quotient $\mathbb{Z}/\Re$.

3.3 Solutions

Exercice **3.1.**

1. i) $\Re$ est réflexive: $x\Re x$ alors $x^2 - x^2 = x - x$ donc $\Re$ est réflexive.

ii) $\Re$ est symétrique: si $x\Re y$ alors on a $x^2 - y^2 = x - y$ donc $-\left(y^2 - x^2\right) = -(y - x)$ ce qui donne $\left(y^2 - x^2\right) = (y - x)$ alors $y\Re x$, donc $\Re$ est symétrique.

iii) $\Re$ est transitive: on a

$$\begin{cases} \text{si } x\Re y \text{ alors on a } x^2 - y^2 = x - y \\ \text{si } y\Re z \text{ alors on a } y^2 - z^2 = y - z \end{cases},$$

en additionnant ces deux égalités on trouve $x^2 - z^2 = x - z$, donc on a $x\Re z$, $\Re$ est transitive.

Finalement , on a i), ii) iii) donc $\Re$ est une relation d'équivalence.

2. Soit $x \in \dot{a}$ si $x\Re a$ c'est-à-dire si

$$x^2 - a^2 = x - a \text{ ce qui donne } x^2 - x - a^2 + a = 0,$$

autrement dit si x est solution de l'équation du second degré, $X^2 - X - a^2 + a = 0$ évidemment a est solution, le produit des solutions est $(-a^2 + a) = a(1 - a)$ donc l'autre solution est $(1 - a)$. Donc $\dot{a} = \{a, 1 - a\}$ sauf si $a = \frac{1}{2}$ alors $\dot{a} = \{\frac{1}{2}\}$.

Exercice **3.2.**

1. i) $\Re$ est réflexive: $x\Re x$ alors $x \leq x$ donc $\Re$ est réflexive.

ii) si $x\Re y$ alors on a $x \leq y$ et si $y\Re x$ alors on a $y \leq x$ donc $x = y$ alors la relation $\Re$ est antisymétrique.

iii) $\Re$ est transitive: on a

$$\begin{cases} \text{si } x\Re y \text{ alors on a } x \leq y \\ \text{si } y\Re z \text{ alors on a } y \leq z \end{cases},$$

alors on trouve $x \leq z$, donc on a $x\Re z$, la relation $\Re$ est transitive.

Finalement , on a i), ii) iii) donc $\Re$ est une relation d'ordre.

2. i) $\Re$ est réflexive: $x\Re x$ alors $e^x \leq e^x$ donc $\Re$ est réflexive.

ii) si $x\Re y$ alors on a $e^x \leq e^y$ et si $y\Re x$ alors on a $e^y \leq e^x$ donc $e^x = e^y$ alors on trouve $x = y$ donc la relation $\Re$ est antisymétrique.

iii) $\Re$ est transitive: on a

$$\begin{cases} \text{si } x\Re y \text{ alors on a } e^x \leq e^y \\ \text{si } y\Re z \text{ alors on a } e^y \leq e^z \end{cases},$$

alors on trouve $e^x \leq e^z$, donc on a $x\Re z$, la relation $\Re$ est transitive.

Finalement , on a i), ii) iii) donc $\Re$ est une relation d'ordre.

3. i) $\Re$ est réflexive: $x\Re x$ alors $x - x = 0 \in \mathbb{N}$ donc $\Re$ est réflexive.

ii) si $x\Re y$ alors on a $x - y \in \mathbb{N}$ et si $y\Re x$ alors on a $y - x \in \mathbb{N}$ ce qui implique que

$$\begin{cases} \exists k \in \mathbb{N},\ x - y = k \\ \exists k' \in \mathbb{N},\ y - x = k' \end{cases}, k, k' \in \mathbb{N}$$

ce qui donne

$$(x-y)+(y-x)=k+k^{'}=k''=0, k''\in\mathbb{N}.$$

Si la somme de deux entiers positifs est nul, c'est que ces deux entiers sont nuls, par conséquent $k''=0$, donc $x-y=0\Rightarrow x=y$ alors la relation $\Re$ est antisymétrique.
iii) $\Re$ est transitive: on a

$$\begin{cases} \text{si } x\Re y \text{ alors on a } x-y\in\mathbb{N} \\ \text{si } y\Re z \text{ alors on a } y-z\in\mathbb{N} \end{cases},$$

alors on trouve $x-z\in\mathbb{N}$, donc on a $x\Re z$, la relation $\Re$ est transitive.
Finalement , on a i), ii) iii) donc $\Re$ est une relation d'ordre.

Exercice **3.3.**

Puisque $\Re_1$ et $\Re_2$ sont des relatin d'équivalence est facile à prouver. La classe d'équivalence de $x\neq 0$ pour $\Re_1$ est

$$\overline{x}=\{y\in\mathbb{R}/\ y+y^{-1}=x+x^{-1}\}.$$

or,

$$(y-x)\left(1-\frac{1}{xy}\right)=0\Leftrightarrow y=x \text{ ou } y=x^{-1}.$$

Le graphe de $\Re_1$ dans $\Re_2$ est la réunion de la première bissectrice et de l'hyperbole d'équation $y=\frac{1}{x}$. On vérifie de la même façon que le graphe de $\Re_2$ est la réunion des droites $y=x$, $y=-x$ et le cercle unité $x^2+y^2=1$.

Exercice **3.4.**

i) $\Re_1$ est réflexive: $x\Re_1 x$ alors $\frac{x}{1+x^2}\geq\frac{x}{1+x^2}$ donc $\Re_1$ est réflexive.
ii) si $x\Re_1 y$ et $y\Re_1 x$ alors on a

$$\frac{x}{1+x^2}\geq\frac{y}{1+y^2}$$

et

$$\frac{y}{1+y^2}\geq\frac{x}{1+x^2}$$

donc

$$\begin{aligned} \frac{x}{1+x^2} &= \frac{y}{1+y^2} \\ \text{alors } x(1+y^2) &= y(1+x^2) \\ \text{ce qui implique que } (x-y)(1-xy) &= 0 \end{aligned}$$

on trouve $x-y=0$ ce qui donne $x=y$ car $x>1$, $y>1$ entraine $(1-xy)<0$ en

particulier $(1-xy)\neq 0$. Donc $\Re_1$ est antisymétrique.
iii) $\Re_1$ est transitive: on a

$$\begin{cases} \text{si } x\Re_1 y \text{ alors on a } \frac{x}{1+x^2}\geq\frac{y}{1+y^2} \\ \text{si } y\Re_1 z \text{ alors on a } \frac{y}{1+y^2}\geq\frac{z}{1+z^2} \end{cases},$$

alors on trouve $\frac{x}{1+x^2}\geq\frac{z}{1+z^2}$, donc on a $x\Re_1 z$, $\Re_1$ est transitive.
Finalement, on a i), ii) iii) donc $\Re_1$ est une relation d'ordre.
- Soit $h:]1,+\infty[\to\mathbb{R}$ définie par

$$h(k)=\frac{k}{1+k^2},$$

et

$$h'(k)=\frac{1-k^2}{(1+k^2)^2}<0$$

donc h est décroissante sur $]1,+\infty[$.
Donc $x\Re_1 y \Leftrightarrow h(x)\geq h(y)\Leftrightarrow x\leq y$, $\leq$ est une relation d'ordre total donc $\Re_1$ est une relation d'ordre total.

Exercice **3.5.**

1. i) $\Re$ est réflexive: $x\Re x$ alors x divise x (car pour $x\in\mathbb{N}^*$ $x=1.x$) donc $\Re$ est réflexive.
ii) si $x\Re y$ et $y\Re x$ alors on a x divise y et y divise x donc

$$\begin{cases} y=kx \\ x=k'x \end{cases},\ k,k'\in\mathbb{N}^*,$$

alors $y=kk'y$ ce qui. Donc $\Re$ est antisymétrique.
iii) $\Re$ est transitive: on a

$$\begin{cases} \text{si } x\Re y \text{ alors on a } y \text{ divise } x \\ \text{si } y\Re z \text{ alors on a } y \text{ divise } z \end{cases},$$

alors on trouve

$$\begin{cases} y=kx \\ z=k'y \end{cases},\ k,k'\in\mathbb{N}^*,$$

donc x divise z alors on a $x\Re z$, $\Re$ est transitive.
Finalement, on a i) ii) et iii) donc $\Re$ est une relation d'ordre.
2. Cette relation est une relation d'ordre partielle car 2 ne divise pas 3 et 3 ne divise pas 2.

Exercice **3.6.**

1. i) $\Re$ est réflexive.

ii) si $x\Re y$ et $y\Re x$ alors on a

$$\begin{cases} x-y=5k \\ y-x=5k^{'} \end{cases}, \; k,k^{'} \in \mathbb{Z}\,,$$

alors pour $k=-k^{'}$ on trouve $y\Re x$. Donc $\Re$ est symétrique.

iii) $\Re$ est transitive: on a

$$\begin{cases} \text{si } x\Re y \text{ alors on a } \frac{5}{x-y} \\ \text{si } y\Re z \text{ alors on a } \frac{5}{y-z} \end{cases},$$

alors on trouve $\frac{5}{x-z}$, donc $x\Re z$, $\Re$ est transitive. Finalement, on a i), ii) iii) donc $\Re$ est une relation d'équivalence.

2. L'ensemble quotient est

$$\dot{a}=\{x\in\mathbb{Z}\ /\ x\Re a\} \Leftrightarrow \dot{a}=\left\{x\in\mathbb{Z}\ /\ \frac{5}{x-a}\right\}$$

et

$$\begin{aligned}
0\Re(5k) \text{ avec } k \in \mathbb{Z} &\Rightarrow \dot{0}=(5k),\ \forall k\in\mathbb{Z} \\
1\Re(5k+1) \text{ avec } k \in \mathbb{Z} &\Rightarrow \dot{1}=(5k+1),\ \forall k\in\mathbb{Z} \\
2\Re(5k+2) \text{ avec } k \in \mathbb{Z} &\Rightarrow \dot{2}=(5k+2),\ \forall k\in\mathbb{Z} \\
3\Re(5k+3) \text{ avec } k \in \mathbb{Z} &\Rightarrow \dot{3}=(5k+3),\ \forall k\in\mathbb{Z} \\
4\Re(5k+4) \text{ avec } k \in \mathbb{Z} &\Rightarrow \dot{4}=(5k+4),\ \forall k\in\mathbb{Z}
\end{aligned}$$

alors $\mathbb{Z}/\Re=\left\{\dot{0},\dot{1},\dot{2},\dot{3},\dot{4}\right\}$

3.4 Exercices supplémentaires

Exercice **3.7.** Sur $\mathbb{R}^2$, on considère la relation $\Re$ définie par

$$(x, y)\,\Re\,(x_1, y_1) \Longleftrightarrow x^2 + y^2 = x_1^2 + y_1^2.$$

1. Montrer que $\Re$ est une relation d'équivalence.
2. Décrire la classe d'équivalence (x, y) du couple (x, y).

Exercice **3.8.** Soit f une application de E dans F et $\Re_1$ une relation d'equivalence sur F. On définit la relation $\Re$ sur E par

$$x\Re x^{'} \Leftrightarrow f\,(x)\,\Re_1 f\left(x^{'}\right)$$

Montrer que $\Re$ est une relation d'équivalence et déterminer ses classes d'équivalence.

Exercice **3.9.** Soit $\Re_1$et $\Re_2$ deux relations d'équivalence définies sur un ensemble E. On considère la relation $\Re$ définie par

$$x\Re y \Leftrightarrow x\Re_1 y \text{ et } x\Re_2 y \quad x, y \in E.$$

Montrer que $\Re$ est une relation d'équivalence. Caratériser ses classes d'équivalence.

Exercice **3.10.** On définit dans $\mathbb{R}^*$ la relation $\Re$ par:

$$xy > 0.$$

1. Est-elle une relation d'éuivalence ?
2. On définit dans $\mathbb{R}$ la relation δ par:

$$x\delta y \Leftrightarrow xy \geq 0.$$

Est-elle une relation d'équivalence?.

Chapitre 4

Structure algèbrique

Sommaire

4.1 Rappels de cours

4.1.1 Généralités sur les groupes

4.1.2 Notion de loi

Définition 4.1 *Une loi de composition interne dans un ensemble E est une application $N : E \times E \to E$. Si cette loi est notée $*$, on a $N(a, b) = a * b$.*

- La loi $+$ est une loi interne de composition sur $\mathbb{R}$.

- Les lois $\cup$ et $\cap$ sont des lois internes de composition sur $P(E)$.

Associativité

Si on a:

$$a * (b * c) = (a * b) * c$$

quels que soient a, b, c dans E.

Comniutativité

Si on a:

$$a * b = b * a$$

quels que soient a, b dans E.

Élément neutre

Définition 4.2 *Soit $e \in E$, e est un élément neutre a gauche (repectivement à droite) de la loi $*$ si $e * x = x$ (respectivement $x * e = x$) pour tout $x \in E$, et c'est un élément neutre si $x * e = e * x = x$ pour tout $x \in E$.*

Élément symétrique

Définition 4.3 *Soit $*$ une loi interne sur un ensemble E, possèdant un élément neutre e et soit a un élément de E. On dit que à admet un symétrique b pour la loi $*$, si $a * b = b * a = e$.*

Distributivité

Soit E un ensemble muni de deux lois de composition internes, notées $+$ et $*$. On dit que $*$ est distributive par rapport à $+$ si $\forall a, b, c \in E$, $a * (b + c) = (a * b) + (a * c)$ et $(a + b) * c = (a * c) + (b * c)$.

4.1.3 Groupes

On appelle groupe tout ensemble G muni d'une loi interne $*$ vérifiant les conditions suivantes :

i) La loi $*$ est associative.

ii) Il existe un élément neutre noté "e".

iii) Si tout élément de G admet un symétrique.

Si de plus la loi $*$ est commutative, G est un **groupe commutatif** ou **abélien** (du nom du mathématicien Abel).

Si le groupe G est réduit à son élément neutre, c'est-à-dire si $G = \{e\}$, on dit que le groupe est trivial.

Exemple 4.1.1 *Soit $*$ une loi de composition interne sur $\mathbb{R}^2$ définie par*

$$\forall (a,b),(c,d) \in \mathbb{R}^2,\ (a,b) * (c,d) = (a-2c, b+3d).$$

$\left(\mathbb{R}^2, *\right)$ *n'est pas un groupe car:*
- $(0,0)$ *est un élément neutre de* $*$. *Ainsi* $(\frac{a}{2}, \frac{-b}{3})$ *est l'inverse de* (a,b). *Mais,* $*$ *n'est pas associative.*

4.1.4 Sous Groupe

Définition 4.4 *Soit $(G,*)$ un groupe, on appelle sous groupe de $(G,*)$ tout sous ensemble non vide G_1 de G tel que la restriction de $*$ à G_1 en fait un groupe.*

Comme $*$ est associative dans G alors sa restriction à G_1 est aussi associative, par suite $G_1 \neq \emptyset$ est un sous groupe de $(G,*)$ s'il est stable par rapport à $*$ et à l'opération inversion, c'est-à-dire

i) $G_1 \neq \emptyset$.

ii) $\forall a,\ b \in G_1,\ a * b \in G_1$.

iii) $\forall a \in G_1,\ a^{-1} \in G_1$.

4.1.5 Morphisme de Groupes

Soient$(G,*)$ et (G',Δ) deux groupes. Une application $f : G \to G'$ est un morphisme de groupes si :

$$\text{pour tout } x,\ x' \in G \qquad f\left(x * x'\right) = f(x)\ \Delta\ f\left(x'\right)$$

- Si $G = G'$, on dit que f est **endomorphisme**

- Si f est bijective, on dit que f est un **Isomorphisme**.

- Si f est bijective avec $G = G'$, on dit que f est un **automorphisme.**

Exemple 4.1.2 *Soient les deux groupe $(\mathbb{R},+)$ et $\left(\mathbb{R}_+^*, \times\right)$, soit la fonction f telle que*

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & f(x) = e^x \end{array}$$

f est morphisme de ces groupes, car

$$\begin{aligned} f(x+y) &= e^{x+y} = e^x\ e^y \\ &= f(x)\ f(y) \end{aligned}$$

4.1.6 Structure d'Anneaux

Définition 4.5 *On appelle anneau, tout ensemble A muni de deux lois de composition internes $+$ et Δ telles que :*
i) $(A, +)$ est un groupe abélien (on notera 0 ou 0_A l'élément neutre de $+$),
ii) Δ est associative et distributive par rapport à $+$.

* Si la lois Δ admet un élément neutre, on dit que l'anneau est unitaire.
* Si la lois Δ est commutative, on dit que l'anneau est commutatif.

Régles de Calcul dans un Anneau

Soit $(A, +, \Delta)$ un anneau, alors on a les règles de calculs suivantes:

Proposition 4.1.1 *Pour tous x, y et $z \in A$,*

1/ $0_A \ \Delta \ x = x \ \Delta \ 0_A = 0_A$.

2/ $x \ \Delta \ (-y) = (-x) \ \Delta \ y = -(x \ \Delta \ y)$.

3/ $x \ \Delta \ (y - z) = (x \ \Delta \ y) - (x \ \Delta \ z)$.

4/ $(y - z) \ \Delta \ x = (y \ \Delta \ x) - (z \ \Delta \ x)$.

Homomorphismes d'Anneaux

Soient $(A, +, \Delta)$ et $(B\ , \oplus\ , \otimes)$ deux anneaux et $f : A \to B$.

Définition 4.6 *On dit que f est un homomorphisme d'anneaux si :*

$$\forall x,\ y \in A,\ f(x + y) = f(x) \oplus f(y) \text{ et } f(x \Delta y) = f(x) \otimes f(y)$$

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

2) Si f est bijective, on dit que f est un isomorphisme d'anneaux.

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

Anneau intègre: On dit qu'un un anneau $(A, +, \Delta)$ est intègre, si pour tous x, $y \in A$, on a: $x \Delta y = 0_A$ implique $x = 0_A$ ou $y = 0_A$.

4.1.7 Corps

Définition 4.7 *On dit qu'un anneau unitaire$(K, +, \Delta)$ est un corps si tout élément non nul de K est inversible. Si de plus Δ est commutative, on dit que K est un corps commutatif.*

Proposition 4.1.2 *Tout corps est un anneau intègre.*

Exemple 4.1.3 $(\mathbb{R}, +, \times)$ *et* $((\mathbb{C}, +, \times)$ *sont des corps.*

Définition 4.8 *On appelle sous corps, d'un corps $(K, +, \Delta)$, tout sous ensemble K' de K tel que, muni des restrictions des lois $+$ et Δ est un corps.*

Proposition 4.1.3 *$K' \subset K$ est **un sous corps** de $(K, +, \Delta)$ si et seulement si*
i) $K' \neq \emptyset$,
ii) $\forall a, b \in K'$, $a - b$ et $a \Delta b^{-1} \in K$.

Exemple 4.1.4 *L'ensemble $\mathbb{R}$ des nombres réels est sous-corps du corps $\mathbb{C}$.*

4.2 Exercices

Exercice **4.1.** Soit $*$ la loi définie sur $\mathbb{R}$ par

$$\forall a,\ b \in \mathbb{R}^+,\ a * b = (a+b)^{\frac{1}{2}}$$

1. Montrer que $*$ est commutative, associative et que 0 est élément neutre.
2. Montrer que aucun élément de $\mathbb{R}^{+*}$ n'a de symétrique pour $*$.

Exercice **4.2.** Soit $*$ la loi définie sur $\mathbb{R}$ par

$$\forall\,(a,b) \in \mathbb{R}^2 \quad a * b = a \times b + \left(a^2-1\right)\left(b^2-1\right)$$

avec $+$ et $\times$ les opérations usuelles sur $\mathbb{R}$.

1. La loi $*$ est-elle associative sur $\mathbb{R}$?. Commutative sur $\mathbb{R}$?. Vérifier que $\mathbb{R}$. Possède un élément neutre pour la loi $*$. Cette loi confère-t-elle à $\mathbb{R}$ une structure de groupe?
2. Calculer le(s) symétrique(s) du réel 2 pour la loi $*$.
3. Résoudre les équations suivantes: $2 * a = 2$, $2 * a = 5$.

Exercice **4.3.**

1. Soient x et y deux éléments d'ordres finis, premiers entre eux, d'un groupe commutatif G. Montrer que l'ordre de xy est égal au produit des ordres de x et y.
2. Soit y un élément d'un groupe G d'ordre $p^\alpha m$ où m est un entier et p est premier. Montrer que y^m est d'ordre p^α.
3. Soit G un groupe commutatif fini. Montrer que si x, $y \in G$ sont d'ordre respectif a, b, alors il existe un élément dans G dont l'ordre est $PPCM\ (a,b)$.

Exercice **4.4.** On appelle centre d'un groupe $(G,*)$ non commutatif, la partie C de G définie par

$$C = \{c \in G, \forall b \in G,\ c * b = b * c\}$$

1. Montrer que C est un sous-groupe de $(G,*)$.
2. Que devient C si $(G,*)$ est commutatif?.

Exercice **4.5.** Soit X un anneau tel que $\forall a \in X$ on ait la relation

$$a^2 = a.$$

1. Montrer que pour tout a dans X on a $a + a = 0$.

2. Montrer que X est commutatif.

Exercice **4.6.** On définit l'opération T par:

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

- Montrer $(]-1, 1[, T)$ est un groupe abélien.

Exercice **4.7.** On considère la loi de composition interne $*$ sur $\mathbb{N}$ définie par

$$a * b = a^2 + b^2$$

1. La loi $*$ est-elle associative sur $\mathbb{N}$?. Commutative sur $\mathbb{N}$?. Possède un élément neutre?.

4.3 Solutions

Exercice **4.1.**

1. On a $a*b = \left(a^2+b^2\right)^{\frac{1}{2}} = \sqrt{a^2+b^2} = \sqrt{b^2+a^2} = b*a$, alors la loi $*$ est commutative.

$$\begin{aligned}(a*b)*c &= \sqrt{a^2+b^2}*c \\ &= \sqrt{\left(\sqrt{a^2+b^2}\right)^2+c^2} = \sqrt{a^2+b^2+c^2}\end{aligned}$$

En reprenant le calcul ci-dessus en changeant (a,b,c) en (b,c,a) :

$$(b*c)*a = \sqrt{b^2+c^2+a^2}$$

et puisque $*$ est commutative:

$$(b*c)*a = x*(b*c),$$

donc

$$(a*b)*c = x*(b*c)$$

alors, la loi $*$ est associative.

$$0*a = \sqrt{0^2+a^2} = |a| = a, \text{ car } a \in \mathbb{R}^{+*}.$$

Comme $*$ est commutative

$$0*a = a*0.$$

Conclusion

$$0*a = a*0 = a.$$

Alors 0 est l'élément neutre.

2. Supposons que a admette un symétrique

$$\begin{aligned}a*b &= 0 \Leftrightarrow \sqrt{a^2+b^2} = 0 \\ &\Leftrightarrow a^2+b^2 = 0 \\ &\Leftrightarrow a^2 = -b^2\end{aligned}$$

or, $a > 0$ et $b > 0$ donc $a * b = 0$ est impossible, pour tout $a > 0$, a n'admet pas de symétrique

Exercice **4.2.**

1. Remarquons tout d'abord que $*$ définit bien une loi de composition interne sur $\mathbb{R}$ car les deux opérations usuelles $+$ et $\times$ sont elles-mêmes des lois de composition interne sur $\mathbb{R}$. La loi $*$ est n'est pas associative sur $\mathbb{R}$ car

$$2 * (3 * 4) = 52533 \neq (2 * 3) * 4 = 13605.$$

Elle est en revanche commutative sur $\mathbb{R}$. Vérifions-le. Soient x et y deux réels. La multiplication étant commutative sur $\mathbb{R}$, on a:

$$a * b = a \times b + (a^2 - 1) \times (b^2 - 1) = b \times a + (b^2 - 1) \times (a^2 - 1) = b * a.$$

La propriété de commutativité de la loi $*$ se déduit de celle des deux lois usuelles $+$ et $\times$. On remarque que $1 * a = a = a * 1$ pour tout réel a. L'élément neutre est donc le réel 1. La loi $*$ n'est pas associative sur $\mathbb{R}$, ainsi $\mathbb{R}$ ne possède pas une structure de groupe.

2. Si s est un symétrique de l'élément 2 pour la loi $*$ dans $\mathbb{R}$, il vérifie alors: $s * 2 = 1 = 2 * s$. Calculer le réel s revient à chercher les solutions de l'équation: $3s^2 + 2s - 4 = 0$. Le réel 2 possède deux symétriques pour la loi $*$. Ce sont les deux réels:

$$s_1 = (-1 + \sqrt{13})/3$$

et

$$s_2 = (-1 - \sqrt{13})/3.$$

3. L'équation $2 * a = 2$ (d'inconnue a) admet pour solutions 1 et $-5/3$, l'équation $2 * a = 5$ (d'inconnue a) admet comme solutions $4/3$ et -2.

Exercice **4.3.**

1. Notons a l'ordre de x, b l'ordre de y, c l'ordre de xy. On veut montrer $c = ab$. D'une part on a

$$(xy)^{ab} = x^{ab}y^{ab} = (xa)^b(yb)^a = 1,$$

donc ab est un multiple de c.
D'autre part

$$1 = (xy)^c = x^c y^c,$$

donc x^cet y^c sont de même ordre et par lagrange cet ordre divise respectivement a et b qui sont premier entre eux.
Donc x^c et y^c sont d'ordre 1, c'est-à-dire sont égaux au neutre $1 \in G$, donc c est un multiple à la fois de a et de b, comme ils sont premiers entre eux, du produit ab. Donc: $c = ab$.

2. On a $(y^m)^{p^\alpha} = y^{p^\alpha m} = 1$ et d'autre part si $q < p^\alpha$ on a $(y^m)^q = y^{mq} \neq 1$ par définition de l'ordre de y. Ainsi p^α est bien le plus petit entier supérieure ou égale à 1 tel que $(y^m)^{p^\alpha} = 1$.

3. Montrons que si x, $y \in G$ sont d'ordre respectif a, b, il existe un élément dans G d'ordre $PPCM\ (a, b)$.
On note d le $PGCD$ de a, b et $a = da^{'}$, $b = db^{'}$, donc

$$PPCM(a, b) = da^{'}b^{'}.$$

Par la question 2, on a ordre $(x^d) = a'$ et par la question 1, ordre $(x^d y) = a^{'}b = PPCM\ (a, b)$.

Exercice **4.4.**

1. $\forall b \in G\ e * b = b * e$ donc $e \in C$
Pour tout $c_1 \in C$ et pour tout $c_2 \in C$,

$$\left(c_1 * c_2^{-1}\right) * b = c_1 * \left(b^{-1} * c_2\right)^{-1}$$

or, $b^{-1} \in G$ alors $b^{-1} * c_2 = c_2 * b^{-1}$

$$\begin{aligned}
\left(c_1 * c_2^{-1}\right) * b &= c_1 * \left(b^{-1} * c_2\right)^{-1} \\
&= c_1 * \left(c_2 * b^{-1}\right)^{-1} \\
&= c_1 * \left(b * c_2^{-1}\right) \\
&= (c_1 * b) * c_2^{-1} \\
&= (b * c_1) * c_2^{-1} = b * \left(c_1 * c_2^{-1}\right)
\end{aligned}$$

ce qui montre que $c_1 * c_2^{-1} \in C$, Donc $(C, *)$ est un sous-groupe de $(G, *)$.

2. Si G est commutatif alors pour tout $c \in G$ et pour $b \in G$, $c * b = b * c$ donc $C = G$.

Exercice **4.5.**

1. On a

$$\begin{aligned}(a+a) &= (a+a)^2 = a^2+a^2+a^2+a^2\\ &= a+a+a+a\end{aligned}$$

d'où on tire $a+a=0$, soit $a=-a$.

2. Soit $a,\, b \in X$,

$$\begin{aligned}(a+b) &= (a+b)^2 = a^2+b^2+ab+ba\\ &= a+b+ab+ba,\end{aligned}$$

cet égalité est réduit à

$$ab+ba=0,$$

et puisque $a=-a$

$$ab=ba.$$

Alors X est commutatif.

Exercice **4.6.**

1. T est une loi de composition interne dans $]-1,1[$.
Soient $a,\, b \in]-1,1[$, alors

$$-1<a<1 \text{ et } -1<b<1,$$

ce qui est équivalent à

$$|a|<1 \wedge |b|<1$$

donc

$$|ab| = |a|\,|b| < 1,$$

par suite

$$1+ab > 1-|ab| > 0.$$

Ainsi $\forall a,b \in]-1,1[$

$$\begin{aligned}\left|\frac{a+b}{1+ab}\right| &< 1 \Leftrightarrow |a+b|<|1+ab|\\ &\Leftrightarrow |a+b|<1+ab \text{ car } 1+ab>0\\ &\Leftrightarrow -(1+ab)<a+b<1+ab\end{aligned}$$

alors on trouve

$$\begin{cases} a+b-ab-1<0 \\ a+b+ab+1>0 \end{cases},$$

donc

$$\begin{cases} a\,(1-b)+b-1<0 \\ a\,(1+b)+b+1>0 \end{cases},$$

par suite

$$\begin{cases} (1-b)+b-1<0 \\ (1+b)+b+1>0 \end{cases},$$

puisque $-1<a,\,b<1$,

$$\begin{array}{rcl} 1-b & > & 0 \wedge a-1<0 \\ & & \text{et} \\ 1+b & > & 0 \wedge a+1>0 \end{array}$$

donc

$$\begin{array}{rcl} (1-b)(a-1) & < & 0 \\ & & \text{et} \\ (1+b)(a+1) & > & 0 \end{array}$$

d'où on déduit que T est vraie pour tous $a,b\in]-1,1[$, par suite

$$\forall a,b\in]-1,1[,\ |aTb|=\left|\frac{a+b}{1+ab}\right|<1,$$

ce qui montre que T est une loi de composition interne dans $]-1,1[$.

2. **Associative**: Soient a, b, $c\in]-1,1[$, alors

$$\begin{array}{rcl} aT\,(bTc) & = & \dfrac{a+(bTc)}{1+a\,(bTc)}=\dfrac{a+\left(\frac{b+c}{1+bc}\right)}{1+a\left(\frac{b+c}{1+bc}\right)} \\ & = & \dfrac{a+b+c+abc}{1+ab+ac+bc}, \end{array}$$

et on a

$$\begin{aligned}(aTb)\,Tc &= \frac{(aTb)+c}{1+(aTb)\,c} = \frac{\left(\frac{a+b}{1+ab}\right)+c}{1+\left(\frac{a+b}{1+ab}\right)c} \\ &= \frac{a+b+c+abc}{1+ab+ac+bc},\end{aligned}$$

en comparant les deux expressions on obtient,

$$\forall a,b,c \in]-1,1[\ aT\,(bTc) = (aTb)\,Tc,$$

d'où on déduit que T est associative.

3. **Commutative**: D'après la commutativité de l'addition et de la multiplication dans $\mathbb{R}$ on a : $\forall a,b \in]-1,1[$

$$\begin{aligned}aTb &= \frac{a+b}{1+ab} \\ &= \frac{b+a}{1+ba}, \\ &= bTa,\end{aligned}$$

ce qui montre que T est commutative.

4. **L' élément neutre**: Soit $e \in \mathbb{R}$, alors

$$\forall a \in]-1,1[,\ eTa = aTe = a,$$

comme T est commutative et

$$aTe = a \Leftrightarrow \frac{a+e}{1+ae} = a,$$

ce qui est équivalent à

$$e(1-a^2) = 0,$$

ce qui donne

$$e = 0 \vee a = \mp 1,$$

on déduit que $e = 0 \in]-1,1[$ est l'élément neutre de T.

5. **Tout élément de** $]-1,1[$ **a un symétrique**: Soient $a \in]-1,1[$ et $a^{'} \in \mathbb{R}$, alors

$$aTa^{'} = e \Leftrightarrow \frac{a+a^{'}}{1+aa^{'}} = e$$

ce qui est équivalent à

$$\frac{a+a^{'}}{1+aa^{'}} = 0,$$

ce qui donne

$$a + a^{'} = 0,$$

alors

$$a = -a^{'},$$

comme T est commutative on déduit que tout élément $a \in]-1,1[$ est symétrisable et son symétrique est $a^{'} = -a \in]-1,1[$.

De 1), 2), 3), 4) et 5) on déduit que $(]-1,1[, T)$ est un groupe abélien.

Exercice **4.7.**

- **Associative**: Soient a, b, $c \in \mathbb{N}$, alors

$$a * (b * c) = \left(a^2 + b^2\right)^2 + c^2,$$

et on a

$$(a * b) * c = a^2 + \left(b^2 + c^2\right)^2.$$

C'est deux ne sont généralement pas égales, par exemple, pour $a = 2$, $b = 0$ et $c = 0$. d'où on déduit que $*$ n'est pas associative.

- **Commutative**: D'après la commutativité de l'addition dans $\mathbb{N}$ on a : $\forall a, b \in \mathbb{N}$

$$\begin{aligned} a * b &= a^2 + b^2 \\ &= b^2 + a^2, \\ &= b * a \end{aligned}$$

ce qui montre que $*$ est commutative.

- **L' élément neutre**: Soit $e \in \mathbb{N}$, alors

$$\forall a \in \mathbb{N},\ e * a = a * e = a$$

comme $*$ est commutative et puisque

$$a * e = a \Leftrightarrow a^2 + e^2 = a$$

ce qui est équivalent à

$$a^2 + e^2 - a = 0 \tag{1}$$

l'égalité (1) n'est pas possible, par exemple si $a = 2$ on trouve $e = \sqrt{2} \notin \mathbb{N}$, d'où on déduit que $*$ n'admet pas un élément neutre.

4.4 Exercices supplémentaires

Exercice **4.8.** Sur $\mathbb{R} - \{1\}$ on définit la loi $*$ comme suit:

$$a * b = a + b + ab.$$

1. Vérifier que $*$ est une loi de composition interne.
2. Montrer que $(\mathbb{R} - \{1\}, *)$ est un groupe commutatif.
3. Résoudre l'équation: $2 * 3 * a * 5 = 5 * 3$.

Exercice **4.9.** Soit $G = \mathbb{R}^* \times \mathbb{R}$ et $*$ la loi dans G définie par

$$(a, b) * \left(a', b'\right) = \left(aa', ab' + b\right)$$

1. Montrer que $(G, *)$ est un groupe non commutatif
2. Montrer que $(G_1, *)$ est un sous-groupe de $(G, *)$, avec $G_1 =]0, +\infty[\times \mathbb{R}$.

Exercice **4.10.** Soit $\Gamma = \mathbb{R} \times \mathbb{R}$ munit de deux lois définies par:

$$\begin{aligned} (a, b) + \left(a', b'\right) &= (a + a', b + b') \\ &\text{et} \\ (a, b) * \left(a', b'\right) &= (aa', ab' + a'b) \end{aligned}$$

1. Montrer que $(\Gamma, +)$ est un groupe commutatif.
2. Montrer que la loi $*$ est commutative, associative et déterminer l'élément neutre.
3. Montrer que $(\Gamma, +, *)$ est un anneau commutatif.

Exercice **4.11.**

Soit $(G, *)$ un groupe, H et M deux sous-groupes de G.

- Montrer que $H \cap M$ est aussi un sous-groupe de G.

Chapitre 5

Anneaux des polynômes

Sommaire

5.1 Rappels de cours

5.1.1 Généralités

Dans tout ce chapitre $\mathbb{k}$ désignera:
- Soit le corps $\mathbb{Q}$ des nombres rationnels.
- Soit le corps $\mathbb{R}$ des nombres réels.
- Soit le corps $\mathbb{C}$ des nombres complexes.

Définition 5.1 *On appelle polynôme à coefficients dans $\mathbb{k}$ (ou polynôme formel à coefficients dans $\mathbb{k}$), un objet mathématique qui s'écrit de manière unique sous la forme :*

$$P(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + ... + a_nX^n$$

où $n \in \mathbb{N}$, $a_0, a_2, ..., a_{n-1}, a_n$ sont des éléments de $\mathbb{k}$, appelés coefficients du polynôme.

Exemple 5.1.1 *$P(X) = 2 + 5X^2 - X^3$ est un polynôme à coefficients réels.*

Remarques 5.1.1
- *Soit m un élément quelconque de $\mathbb{N}$. Alors X^m est un polynôme.*
- *Si n est un entier **égal à zéro**, on dit que l'on a un polynôme **constant**.*
- *Deux polynômes constants particuliers vont intervenir: le polynôme zéro appelé le polynôme **nul** (tout les coefficients a_n sont nuls) et le polynôme 1.*
- *L'enensemble de tous les polynômes à coefficients dans $\mathbb{k}$ est noté: $\mathbb{k}[X]$*

5.1.2 Degré d'un polynôme

La notion de degré joue un rôle essentiel dans la théorie des polynômes.

Définition 5.2 *Soit $P(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + ... + a_nX^n$ un polynôme non nul. Le degré de P est le plus grand entier n tel que a_n soit différent de 0 et on note **deg** P.*

Exemple 5.1.2 *Soit le polynôme à coefficients dans $\mathbb{R}$, $-1 + X^2 + 6X^3 + X^6$. Il est de degré 6.*

Remarques 5.1.2 *- L'écriture $P(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + ... + a_nX^n$ ne signifie pas que P est de degré n tant que l'on n'a pas rajouté la condition $a_n \neq 0$.*
- Si P est de degré n alors a_n est appelé coefficient dominant du polynôme.
*- Un polynôme est dit **unitaire** si son coefficient dominant est égal à 1.*

5.1.3 Opérations sur les polynômes

Soit P et H deux polynômes à coefficients dans $\mathbb{k}$, il existe un entier n tel que:

$P(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + ... + a_nX^n$,
$H(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + ... + b_nX^n$,

Égalité de deux polynômes

Définition 5.3 *Deux polynômes P, H de $\mathbb{k}[X]$ sont égaux si et seulement si tous leurs coefficients sont égaux. c'est à dire $\forall i$, $1 \leq i \leq n$, $a_i = b_i$*

Somme de deux polynômes

Définition 5.4 *La somme des deux polynômes $P+H$ sur $\mathbb{k}[X]$ définie par*

$$P + H = c_0 + c_1X + c_2X^2 + c_3X^3 + ... + c_nX^n$$

avec $\forall k,\ 0 \leq k \leq n,\ c_k = a_k + b_k$ *et* $deg(P + H) \leq \max(\deg\ P,\ deg\ H)$.

Propriété : de l'addition des polynômes

1. **Associativité**: pour tout polynôme P , H et Q on a :

$$(P + H) + Q = P + (H + Q)$$

2. **Commutativité**: pour tout polynôme P et H on a :

$$P + H = H + P$$

3. **L' élément neutre**: il existe un polynôme P_0 tel que pour tout polynôme P, on a:

$$P + P_0 = P_0 + P = P$$

C'est le polynôme nul, noté 0.

4. **Tout élément a un symétrique**: pour tout polynôme P il existe un polynôme P' tel que:

$$P + P' = P' + P = 0$$

le symétrique de P est noté $-P$

Ces propriétés permettent de dire que l'ensemble des polynômes muni de la loi + est un groupe commutatif.

Produit d'un polynôme par un scalaire

Définition 5.5 *Soit* $P(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + ... + a_nX^n$ *un polynôme à coefficients dans* $\mathbb{k}$. *Soit* β *un élément quelconque de* $\mathbb{k}$. *Alors* βP *est le polynôme*

$$\beta P = c_0 + c_1X + c_2X^2 + c_3X^3 + ... + c_nX^n$$

avec $\forall k,\ 0 \leq k \leq n,\ c_k = \beta a_k$.

Propriété: du produit d'un polynôme par un scalaire

1. pour tout polynôme , P, H et tout scalaire β, on a : $\beta(P+H)=\beta P+\beta H$.
2. pour tout polynôme P et tous scalaires β et μ, on a : $(\beta+\mu)P=\beta P+\mu P$.
3. pour tout polynôme P et tous scalaires β et μ, on a : $(\beta\mu)P=\beta(\mu P)$.
4. pour tout polynôme : $1.P=P$ où 1 est l'unité de $\mathbb{k}$.

Produit de deux polynômes

Définition 5.6 *Soit* $\deg(P)=n$, $\deg(H)=s$, *le produit des deux polynômes* P *et* (H) *est défini par:*

$$PH=c_0+c_1X+c_2X^2+c_3X^3+...+c_{n+s}X^{n+s}$$

avec $\forall k,\ 0\leq k\leq n+s,\ c_k=\sum_{j=0}^{j=k}a_jb_{k-j}$ *et* $\deg P(H)=n+s$.

Propriété: du produit des polynômes

1. **Associativité**: pour tout polynôme P , H et Q on a :
$$(P.H).Q=P.(H.Q)$$
2. **Commutativité**: pour tout polynôme P et H on a :
$$P.H=H.P$$
3. **L'élément neutre**: il existe un polynôme P_0 tel que pour tout polynôme P, on a:
$$P.P_0=P_0.P=P$$
C'est le polynôme constant égal à 1, $P.1=1.P=P$
4. **Distributivité du produit par rapport à l'addition**: pour tout polynôme P, H et Q on a :
$$P.(H+Q)=P.H+P.Q$$

Exemple 5.1.3 *Soient les polynôme* P *et* H*:*

$$\begin{aligned}P(X) &= 1+2X-6X^2+7X^3\\ &\quad et\\ H(X) &= -1-2X+6X^2\end{aligned}$$

calculons, $P+H$, $P-H$, $3H$ *et* PH*:*

$$\begin{aligned} P+H &= 0, \\ P-H &= 2+4X-12X^2+7X^3, \\ 3H &= -3-6X+12X^2, \\ PH &= 42X^5-50X^4+17X^3+8X^2-4X-1. \end{aligned}$$

5.1.4 Arithmétique des Polynômes

Divisibilité

Définition 5.7 *Soient P, H deux polynômes dans $\Bbbk[X]$. On dit que H divise P ou que H est un diviseur de P ou que P est un multiple de H s'il existe un polynôme $Q \in \Bbbk[X]$ tel que $P = HQ$. Lorsque H divise P on écrit: $H \mid P$.*

Exemple 5.1.4 - *Tout polynôme divise le polynôme nul.*
- *Le polynôme $X-1$ divise X^2-1 car $X^2-1=(X-1)(X+1)$.*

Division Euclidienne

Théoréme Soient P, H deux polynômes dans $\Bbbk[X]$ avec H non nul. Alors il existe deux polynômes Q, $R \in \Bbbk[X]$ uniques tels que

$$P = QH + R$$

Avec le deg $R <$ deg H. On dit Q est le quotient et R est le reste de la division euclidienne de P par H.

Propriétés

- Si $P \mid H$ et $H \mid P$, alors il existe $\alpha \in \Bbbk^*$ tel que $P = \alpha H$.
- Si $P \mid H$ et $H \mid C$ alors $P \mid H$.
- Si $C \mid P$ et $C \mid H$ alors $C \mid (PL + HM)$, pour tout L, $M \in \Bbbk[X]$.

Exemple 5.1.5 - *Soit un polynôme non nul. Alors, quel que soit le scalaire α non nul, le polynôme constant α et le polynôme αP sont des diviseurs de P.*
- *Si $P = X^3+X^2-2X+1$ et $H = X+3$. Alors on trouve $Q = X^2-2X+4$ et $R = -11$. On n'oublie pas de vérifier que $P = HQ + R$.*

5.1.5 PGCD (plus grand diviseur commun)

Définition 5.8 *Soient P, H deux polynômes dans $\mathbb{k}[X]$ avec P, H non nuls tous les deux. Il existe un unique polynôme unitaire de plus grand degré qui divise à la fois P et H appelé le* ***PGCD*** *(plus grand diviseur commun) de P et H noté* $\mathbf{PGCD(P;H)}$.

Propriétés

- Si $P \mid H$ et P est non nul , $PGCD\ (A,B) = \frac{1}{\delta}A$, où δ est le coefficient dominant de P.
- $\forall \alpha \in \mathbb{k}^*$, $PGCD\ (\alpha P, H) = PGCD(P,H)$.
- si $P = HQ + R$ alors $PGCD\ (P,H) = PGCD\ (B,R)$. C'est ce qui justifie l'algorithme d'Euclide.

5.1.6 Algorithme d'Euclide.

Soient P et H des polynômes, H est non nul. On calcule les divisions euclidiennes successives, $P = HQ_1 + R_1$ avec $\deg R_1 < \deg H$.

$$\begin{aligned}
P &= HQ_1 + R_1 \quad \deg\ R_1 < \deg H \\
H &= R_1Q_2 + R_2 \quad \deg\ R_2 < \deg R_1 \\
R_1 &= R_2Q_3 + R_3 \quad \deg\ R_3 < \deg R_2 \\
&\ \ \vdots \\
R_{k-2} &= R_{k-1}Q_k + R_k \quad \deg\ R_k < \deg R_{k-1} \\
R_{k-1} &= R_kQ_{k+1}
\end{aligned}$$

On arrête l'algorithme lorsque le reste est nul. Le $PGCD$ est le dernier reste non nul R_k.

Exemple 5.1.6 *Calculons le $PGCD$ de $P = X^5 - 2X^4 + X^2 - 2$ et $H = X^3 - X^2 + X - 2$, On applique l'algorithme d'Euclide, on trouve:*

$$\begin{aligned} P &= H\underbrace{(X^2-X)}_{Q_1}+\underbrace{2X^2-X-2}_{R_1} \\ H &= R_1\underbrace{\left(\frac{1}{2}X+\frac{1}{4}\right)}_{Q_2}+\underbrace{\frac{3}{4}X-\frac{3}{2}}_{R_2} \\ R_1 &= R_2\underbrace{\left(\frac{8}{3}X+\frac{4}{3}\right)}_{Q_2} \end{aligned}$$

le PGCD est le dernier reste non nul, donc PGCD $(P,H) = X-2$.

Définition 5.9 *Soient P, H deux polynômes dans $\mathbb{k}[X]$. On dit que P et H sont premiers entre eux si $PGCD(P,H) = 1$*

5.1.7 Théorème de Bézout et théorème de Gauss

Théoréme Soient P, H deux polynômes dans $\mathbb{k}[X]$. Si $p\gcd(P,H) = S$ alors il existe L, M deux polynômes dans $\mathbb{k}[X]$ tels que $S = PL + HM$.

Exemple 5.1.7 *La relation de Bézout dans l'exemple précédent est donnée par la formule suivante:*

$$LP + HM = S$$

avec

$$L = -\frac{2}{3}X - \frac{1}{3} \text{ et } M = \frac{2}{3}X^3 - \frac{1}{3}X^2 - \frac{1}{3}X + \frac{4}{3}$$

Théoréme Soient P, H deux polynômes dans $\mathbb{k}[X]$. Si $P \mid HC$ et $pgcd\ (P,H) = 1$ alors $P \mid C$.

5.1.8 $PPCM$ (plus petit multiple commun)

Définition 5.10 ***Déffinition*** *Soient P, H deux polynômes dans $\mathbb{k}[X]$ non nuls, alors il existe un unique polynôme unitaire M de plus petit degré tel que $P \mid M$ et $H \mid M$ est appelé le* ***PPCM*** *(plus petit multiple commun) de P et H, noté $PPCM(P,H)$.*

Exemple 5.1.8 *Soit*

$$\begin{aligned} P &= (X-3)^2(X^2+2)^5 \quad et \\ H &= (X-1)(X-3)^3(X^2+2)^4. \end{aligned}$$

Alors $PPCM\ (P,H) = (X-1)(X-3)^3(X^2+2)^5$.

De plus le $PPCM$ est aussi le plus petit au sens de la divisibilité.

Proposition 5.1.1 *Soient P, H deux polynômes dans $\mathbb{k}[X]$ non nuls et $M = PPCM\,(P, H)$. Si $C \in \mathbb{k}[X]$ est un polynôme tel que $P \mid C$ et $H \mid C$, alors $M \mid C$.*

5.1.9 Racine d'un polynôme, factorisation

Racine d'un polynôme

Définition 5.11 *Soit P un polynôme dans $\mathbb{k}[X]$ et $a \in \mathbb{k}$. On dit que a est une racine de P si $P(a) = 0$.*

Exemple 5.1.9 - *X^2-1 admet deux racines réelles 1 et -1, car $X^2-1 = \left(X^2-1\right)(X+1)$*

Proposition 5.1.2 *Soit P un polynôme dans $\mathbb{k}[X]$ et $a \in \mathbb{k}$. On dit que a est une racine de P si est seuement si le polynôme $X - a$ divise P.*

Théorème D'Alembert-Gauss

Théoréme Tout polynôme P dans $\mathbb{C}[X]$ admet au moins une rcine dans $\mathbb{C}$.

Exemple 5.1.10 *Soit $P(X) = X^2 + X + 1$, le discriminant $\Delta = -3 < 0$, alors $P(X)$ admet deux racines complexes distinctes*

$$\begin{aligned} X_1 &= \frac{-1 - i\sqrt{3}}{2}, \\ X_2 &= \frac{-1 + i\sqrt{3}}{2}. \end{aligned}$$

5.1.10 Polynôme irréductibles

On peut écrire $P = \left(\frac{1}{a}\right) aP$ pour tout polynôme P dans $\mathbb{k}[X]$ et toute constante non nulle $a \in \mathbb{k}$. Donc, toute constante non nulle est un diviseur de P et toute constante non nulle $a \in \mathbb{k}$, aP est diviseur de P. Il existe des polynômes P dont les seuls diviseurs sont les polynômes constants et les polynômes de la forme aP, on les appelle: polynômes **irréductibles** de $\mathbb{k}[X]$.

D'autre part, il existe des polynômes dans $\mathbb{k}[X]$ qui admettent d'autres diviseurs, à part les constantes et eux mêmes. Ces polynômes on les appelle réductibles de $\mathbb{k}[X]$.

Exemple 5.1.11 - *Tous les polynômes de degré 1 sont irréductibles.*
- *$X^2 - 1 = (X-1)(X+1) \in \mathbb{R}[X]$ est réductible.*
- *Le polynôme X^2+1 est irréductible de $\mathbb{R}[X]$, mais il est réductible de $\mathbb{C}[X]$, car $X^2+1 = (X-i)(X+i)$.*

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

Théoréme Soit P un polynôme dans $\Bbbk[X]$ non constant, alors il existe$k \in \mathbb{N}^*$ et des polynômes $P_1, P_2,..., P_k$ irréductibles de $\Bbbk[X]$, tels que

$$P = \beta P_1^{\alpha_1} P_2^{\alpha_2} ... P_k^{\alpha_k},$$

où, $\beta \in \Bbbk^*$ et $\alpha_1, \alpha_2, \ . \ . \ . \ , \alpha_p \in \mathbb{N}^*$. Les polynômes P_1, P_2,..., P_k sont uniques à permutation près.

Exemple 5.1.12 *Factorisons le polynôme* $X^4 - 1$ *sur* $\mathbb{R}$ *et sur* $\mathbb{C}$.

Sur $\mathbb{R}$

$$\begin{aligned} X^4 - 1 &= \left(X^2 - 1\right)\left(X^2 + 1\right) \\ &= (X - 1)(X + 1)\left(X^2 + 1\right). \end{aligned}$$

Sur $\mathbb{C}$

$$\begin{aligned} X^4 - 1 &= \left(X^2 - 1\right)\left(X^2 + 1\right) \\ &= (X - 1)(X + 1)\left(X^2 + 1\right) \\ &= (X - 1)(X + 1)(X + i)(X - i) \end{aligned}$$

5.2 Exercices

Exercice **5.1.** Factoriser le polynôme:

$$P(x) = -8 - 6X + 7X^2 + 6X^3 + X^4$$

sachant que $P(-2) = P(1) = 0$.

Exercice **5.2.** Dans $\mathbb{k}[X]$, on considère les polynômes suivants

$$\begin{aligned} f(X) &= X^2 + 2X + 3, \\ g(X) &= 2X^2 + 3X + 1, \\ h(X) &= 3X^2 + X + 2. \end{aligned}$$

1. Pour $\mathbb{k} = \mathbb{Z}$, calculer $P = f^3 + g^3 + h^3 - 3fgh$.

Exercice **5.3.** Effectuer la division euclidienne de P par H :

1. $P = X^4 - 3X^3 + 2X^2 - X + 2$ et $H = X - 3$.
2. $P = X^4 + 2X^3 - X + 6$ et $H = X^3 - 6X^2 + X + 4$.
3. $P = -27X^8 + 36X^6 - 9X^5 + 18X^4$ et $H = -9X^2$.

Exercice **5.4.** Déterminer L et M deux polynômes à coefficients réels vérifiant $LP + HM = 1$ dans les deux cas suivants:

$$\begin{cases} P = X^7 - X - 1 \\ H = X^5 + 1 \end{cases}, \qquad \begin{cases} P = X^5 - X^4 + 2X^3 + 1 \\ H = X^5 + X^4 + 2X^2 - 1 \end{cases}$$

Exercice **5.5.** Décomposer en produit de facteurs irréductibles les polynômes suivant:

1. $X^3 + 1$ dans $\mathbb{C}[X]$.
3. $X^8 - X^4 + 1$ dans $\mathbb{C}[X]$.

Exercice **5.6.** On considère les deux polynômes:

$$\begin{aligned} P &= X^4 + 5X^3 + 5X^2 - 5X - 6 \\ H &= X^4 + 2X^3 - X^2 - 2X \end{aligned}$$

a. Décomposer ces polynômes en produit de facteurs irréductibles.
b. En déduire le $PGCD\ (P, H)$ et $PPCM\ (P, H)$.
c. Déterminer le $PGCD\ (P, H)$ par l'algorithme d'Euclide.

5.3 Solutions

Exercice **5.1.** On a

$$P(-2) = P(1) = 0$$

ce qui implique que

$$P\,(X) \text{ divisible par } (X+2)(X-1)$$

et on remarque que

$$(X+2)(X-1) = X^2 + X - 2,$$

la division euclidinne donne

$$\begin{aligned} P(X) &= X^4 + 6X^3 + 7X^2 - 6X - 8 \\ &= \left(X^2 + 5X + 4\right)\left(X^2 + X - 2\right) \end{aligned}$$

avec

$$X^2 + 5X + 4 = (X+4)(X+1),$$

ainsi

$$P(X) = (X+1)(X+4)(X+2)(X-1).$$

Exercice **5.2.** On a l'expression suivante:

$$p^3 + g^3 + h^3 = (f+g+h)^3 - 3(f+g+h)(fg+gh+hf) + 3fgh.$$

Alors le polynôme P à calculer est de la forme suivante

$$P = (f+g+h)^3 - 3(f - Kg + h)(fg+gh+hf).$$

Soit encore

$$P = (f+g+h)\left[(f+g+h)^2 - 3\,(fg+gh+hf)\right].$$

Pour $\Bbbk = \mathbb{Z}$, on trouve

$$\begin{aligned} f(X) + g(X) + h(X) &= 6(X^2 + X + 1). \\ f(X).g(X) &= 2X^4 + 7X^3 + 13X^2 + 11X + 3. \\ g(X).h(X) &= 6X^4 + 11X^3 + 10X^2 + 7X + 2. \\ h(X).f(X) &= 3X^4 + 7X^3 + 13X^2 + 7X + 6. \end{aligned}$$

Alors

$$(fg + gh + hf)(X) = 11X^4 + 25X^3 + 36X^2 + 25X + 11.$$

Ainsi

$$(f + g + h)^2(X) = 36[X^4 + 2X^3 + X^2 + 2X + 1],$$

par conséquent

$$\begin{aligned} P(X) &= 6[X^2 + X + 1][36[X^4 + 2X^3 + 3X^2 + 2X + 1] \\ &\quad -33X^4 - 75X^3 - 108X^2 - 75X - 33], \end{aligned}$$

Ce qui donne

$$\begin{aligned} P\,(X) &= 6[X^2 + X + 1][3X^4 - 3X^3 - 3X + 3] \\ &= 18[X^6 - 2X^3 + 1] \\ &= 18[X^3 + 1]^2. \end{aligned}$$

Exercice **5.3.** Division Euclidienne:

1. $Q = X^3 + 2X + 5$ et $R = 17$.
2. $Q = 8 + X$ et $R = 47X^2 - 13X - 26$.
3. $Q = 3X^6 - 4X^4 + X^3 - 2X^2$ et $R = 0$.

Exercice **5.4.**

1. Soit

$$\begin{cases} P = X^7 - X - 1 \\ H = X^5 + 1 \end{cases}$$

on a

$$\begin{aligned} P &= X^2H - \left(X^2 + X + 1\right) \\ H &= (X^2 + X + 1)(X^3 - X^2 + 1) - X, \end{aligned}$$

et

$$X^2 + X + 1 = (-X)(-X - 1) + 1.$$

P et H sont premier entre eux avec

$$\begin{aligned} M &= X^4 - X^2 + X, \\ L &= -X^6 + X^4 - X^3 + X + 1. \end{aligned}$$

2. Soit

$$\begin{cases} P = X^5 - X^4 + 2X^3 + 1 \\ H = X^5 + X^4 + 2X^2 - 1 \end{cases},$$

on a

$$\begin{aligned} P &= H - 2X^4 + 2X^3 - 2X^2 + 2 \\ H &= \left(-2X^4 + 2X^3 - 2X^2 + 2\right)\left(\frac{1}{2}X - 1\right) + 1 + X + X^3, \end{aligned}$$

et

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

Alors P et H ne sont pas premiers entre eux.
Le $PGCD\,(P, H) = 1 + X + X^3$. Donc il n'existe pas de couple (L, M).

Exercice **5.5.**

1. La factorisation de $X^3 + 1$ dans $\mathbb{C}\,[X]$ en facteur irréductibles est donné par :

$$X^3 + 1 = (X + 1)\,(X + X_1)\,(X + X_2)\,,$$

où

$$\begin{aligned} X_1 &= \frac{1 + i\sqrt{3}}{2} \\ X_2 &= \frac{1 - i\sqrt{3}}{2} \end{aligned}$$

2. En posant $Y = X^4$, on se ramène à une équation du second degré en Y,

$$Y^2 + Y + 1 = 0$$

alors

$$\begin{aligned} Y_1 &= \frac{-1 + i\sqrt{3}}{2} = e^{i\frac{4\pi}{3}} \\ Y_2 &= \frac{-1 - i\sqrt{3}}{2} = e^{i\frac{2\pi}{3}} \end{aligned}$$

ce qui donne

$$\begin{aligned} Y_1 &= X^4 = e^{4\alpha} = e^{i\frac{4\pi}{3}}, \text{ donc } \alpha = \frac{\pi}{3} + \frac{k\pi}{2}, \\ Y_2 &= X^4 = e^{4\alpha} = e^{i\frac{2\pi}{3}}, \text{ donc } \alpha = \frac{\pi}{6} + \frac{k\pi}{2}. \end{aligned}$$

Ainsi

$$\begin{aligned} X^8 + X^4 + 1 &= \left(X - e^{i\frac{\pi}{3}}\right)\left(X - e^{i\frac{5\pi}{6}}\right)\left(X - e^{i\frac{11\pi}{6}}\right) \\ &\quad \times \left(X - e^{i\frac{\pi}{6}}\right)\left(X - e^{i\frac{2\pi}{3}}\right)\left(X - e^{i\frac{5\pi}{3}}\right)\left(X - e^{i\frac{7\pi}{6}}\right). \end{aligned}$$

Exercice **5.6.**

a. La factorisation de P et H

$$\begin{aligned} P &= (X-1)(X+3)(X+2)(X+1) \\ H &= X(X-1)(X+2)(X+1) \end{aligned}$$

b. $PGCD\ (P,H)$, $PPCM\ (P,H)$

$$\begin{cases} PGCD\ (P,H) = (X-1)(X+3)(X+2), \\ PPCM\ (P,H) = X(X-1)(X+2)(X+1)(X+3). \end{cases}$$

c. La division Euclidinne donne
$P = X^4+5X^3+5X^2-5X-6 = 1\times(X^4+2X^3-X^2-2X)+(3X^3+6X^2-3X-6)$, ensuite

$$\begin{aligned} H &= X^4 + 2X^3 - X^2 - 2X \\ &= \frac{X}{3} \times \left(3X^3 + 6X^2 - 3X - 6\right) + 0 \end{aligned}$$

alors le $PGCD\ (P,H)$ est le dernier reste non nul, on retrouve

$$PGCD\,(P,H) = (X-1)(X+3)(X+2).$$

5.4 Exercices supplémentaires

Exercice **5.7.** Pour quelles valeurs de $n \in \mathbb{N}$ le polynôme:

$$(X+1)^n - X^{n-1} \text{ est divisible par } X^2 + X + 1?.$$

Exercice **5.8.** Factoriser dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$ le polynôme:

$$P = -X^8 + 2X^4 - 1.$$

Exercice **5.9.** Déterminer le $PGCD$ de

$$P = X^5 + X^3 + X^2 + 1 \text{ et } H = 2X^3 + 3X^2 + 2X + 3.$$

- Trouver les coefficients de Bézout L, M.

Exercice **5.10.** Soit n un entier strictement positif

1. Déterminer le $PGCD$ des polynômes $X^n - 1$ et $(X-1)^n$.
2. Démontrer qu'il existe un couple de polynômes (L, M) pour $n = 3$ avec

$$(X^3 - 1)L + (X-1)^3 M = X - 1.$$

Exercice **5.11**

1. Montrer que pour tout $n \in \mathbb{N}$, $X^{4n} - 1$ est divisible par $X^4 - 1$.
2. En déduire que le polynôme

$$P = X^{4a+3} + X^{4b+2} + X^{4c+1} + X^{4d}$$

avec a, b, c et d des entiers naturels est divisible par $Q = X^3 + X^2 + X + 1$.

Bibliographie

[1] Hitta, Amara, Cours d'algèbre et exercices corrigés. O.P.U., 1994.

[2] A. Bodin, B. Boutin, P. Romon. Algèbre : Cours de Mathématiques première année Ex07.

[3] Damien Etienne, Exercices corrigés d'algèbre linéaire. De Boeck Supérieur, 12 avr. 2006 - 280 pages.

[4] Elie Azouly, Jean Avignant, Mathématique 4.Algèbre, enseignement superieur technique, cours et exercice, 1984

[5] M. Mechab, Cours d'algèbre, Maths1 LMD Sciences et Techniques.

[6] S. Miri, Algèbre et Analyse, université Tlemcen, Algérie, 2013.

[7] M. Mignotte et J. Nervi, Algèbre : licences sciences 1ère année, Ellipses, Paris, 2004.

[8] Jean-Pierre Escofier, Toutes l'algèbre de la licence. Cours et exercices corrigés, DUNOD.

[9] Patrice Tauvel , Cours d'Algèbre, Dunod, Sciences sup. 1999.