République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieure et de la Recherche Scientifique
Université Mustapha Stambouli de Mascara
Faculté des Sciences Exactes

Polycopié de cours :

Algèbre 1

Presenté par ZAGANE Abdelkader

Ce cours est destiné aux étudiants de la première année
LMDSpécialité Mathématiques et Informatique

Table des matières

Avant-propos :
Ce cours est destiné aux étudiants de la première année licence de mathématiques, ainsi qu'aux étudiants des sciences de technologie. Il porte sur les notions de base de la logique, les applications, les relations les structure de groupe, d'anneau.
Le cours est traité en détail avec de nombreux exemples. La plupart des théorèmes et des propositions sont démontrés à quelques exceptions près où nous renvoyons le lecteur aux références correspondantes.
À la fin de chaque chapitre nous proposons une liste d'exercices corrigés dans le dernier chapitre.
Quatre chapitres composent cet cours :
Dans le premier chapitre nous avons donné la définition du proposition mathématique, les quantificateurs,les notions de logique propositionnelle comme la conjonction,la négation l'implication, l'équivalence,et les types de raisonnement.
Dans le deuxième chapitre nous avons traité les définitions et les propriétés de l'ensemble, applications injectives,surjectives et les relation binaires : relation d'équivalence, relation d'ordre et l'espace quotient.
Le troisième chapitre est particulie distiné pour etudier la structure de groupe, sous groupe, homomorphisme de groupe, le noyau et l'image d'un homomorphisme.
Par contre dans la quatrième chapitre on étude l'anneau des polynomes ,le théorème de Bézout, la devision euclidienne dans l'anneau des polynomes.

Finalement dans le dernier chapitre nous avons donné les solutions d' exercices.

1

Quelques notions de logiques

1.1 Propositions mathématiques

1.1.1 Définitions et exemples

Définition 1.1.1.1. *Proposition mathématique est une expression mathématique qui est sans ambiguïté, on peut la donné*
une valeur "vraie" ou fausse.

Exemple 1.1.1.1. *1) 1+3=4 est une proposition vraie*
2) 1=6 est une proposition fausse.

Remarque 1.1.1.1. *On note les propositions par les grandes lettres $P, Q, R, S, ...$*

Table de vérité

On note par 1 pour dire que la proposition est vraie, et par 0 pour dire que la proposition est fausse.
La table pour une seule proposition P est maitre

P
1
0

la table de vérité pour deux propositions P et Q est maitre

P	Q
1	1
1	0
0	1
0	0

La table de vérité pour trois propositions P, Q et R est maitre

P	Q	R
1	1	1
1	1	0
1	0	1
1	0	0
0	1	1
0	1	0
0	0	1
0	0	0

Remarque 1.1.1.2. *Les valeurs dans une table de vérité pour n propositions est constitue n colonnes et 2^n lignes.*

1.2 Connecteurs logiques

1.2.1 Négation

Définition 1.2.1.1. *Soit P une proposition mathématique la négation de P est une proposition mathématique note non P ou $\overline{P}$ qui est vraie si P est fausse, et fausse si P est vraie.*

Table de vérité pour la négation

Soit P une proposition mathématique,

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

Remarque 1.2.1.1. $\overline{\overline{P}}$ *est* P

1.2.2 Conjonction

Définition 1.2.2.1. *Soient P et Q deux propositions mathématiques, on peut construire une nouvelle proposition mathématique note P et Q ou $P \wedge Q$ qui est vraie si P et Q sont vraies en même temps, est fausse si non.*

Table de vérité pour la conjonction

Soient P et Q deux propositions mathématiques,

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

Remarque 1.2.2.1. *La valeur de $P \wedge Q$ peut être obtenu comme produit de les valeurs de P et Q.*

1.2.3 Disjonction

Définition 1.2.3.1. *Soient P et Q deux propositions mathématiques, on peut construire une nouvelle proposition mathématique note P ou Q ou $P \vee Q$ qui est toujours vraie sauf le cas où P et Q sont fausses en même temps.*

Table de vérité pour la disjonction

Soient P et Q deux propositions mathématiques,

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

1.2.4 Implication

Définition 1.2.4.1. *Soient P et Q deux propositions mathématiques,la proposition mathématique P implique Q note $P \Rightarrow Q$ est fausse pour un seul cas qui est P vraie et Q fausse.*

Table de vérité pour l'implication

Soient P et Q deux propositions mathématiques,

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

Remarque 1.2.4.1. *La valeur de la proposition mathématique P implique Q semble comme la valeur de P inférieur ou égale à la valeur de Q.*

1.2.5 Bi-implication ou équivalence

Définition 1.2.5.1. *Soient P et Q deux propositions mathématiques,la proposition mathématique P équivaut Q note $P \Leftrightarrow Q$ est vraie si les P et Q sont vraies en même temps ou fausses en même temps.*

Table de vérité pour l'équivalence

Soient P et Q deux propositions mathématiques,

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

Remarque 1.2.5.1. *La valeur de la proposition mathématique $P \Leftrightarrow Q$ semble comme la valeur de P égale à la valeur de Q.*

Remarque 1.2.5.2. *on a*

$$(P \Rightarrow Q) \Leftrightarrow (\overline{P} \vee Q)$$

en effet la table de vérité

P	$\overline{P}$	Q	$\overline{P} \vee Q$	$P \Rightarrow Q$	$(P \Rightarrow Q) \Leftrightarrow (\overline{P} \vee Q)$
1	*0*	*1*	*1*	*1*	*1*
1	*0*	*0*	*0*	*0*	*1*
0	*1*	*1*	*1*	*1*	*1*
0	*1*	*0*	*1*	*1*	*1*

.

1.2.6 Propriétés de la conjonction

Soient P ,Q et R trois propositions mathématiques :

1. $P \wedge P \Leftrightarrow P$.
2. $P \wedge Q \Leftrightarrow Q \wedge P$.
3. $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$.
4. $P \wedge \overline{P}$ est toujours fausse.

1.2.7 Propriétés de la disjonction

Soient P ,Q et R trois propositions mathématiques :

1. $P \vee P \Leftrightarrow P$.
2. $P \vee Q \Leftrightarrow Q \wedge P$.
3. $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$.
4. $P \vee \overline{P}$ est toujours vraie.

Proposition 1.2.7.1. *Lois de **Morgan***
Soient P, Q et R des propositions mathématiques :

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

Preuve . En utilisant la table de vérité. ∎

Proposition 1.2.7.2. *Soient P, Q et R trois propositions mathématiques :*

1. $(P \vee Q) \wedge R \Leftrightarrow (P \wedge R) \vee (Q \wedge R)$.
2. $(P \wedge Q) \vee R \Leftrightarrow (P \vee R) \wedge (Q \vee R)$.

Preuve . En utilisant la table de vérité. ∎

1.2.8 Propriétés de l'implication

Proposition 1.2.8.1. *Soient P, Q et R trois propositions mathématiques :*

1. $(P \Rightarrow Q) \Leftrightarrow (\overline{Q} \Rightarrow \overline{P})$.
2. $((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Leftrightarrow (P \Rightarrow R)$.

Preuve . En utilisant la table de vérité. ∎

1.2.9 Propriétés de l'équivalence

Proposition 1.2.9.1. *Soient P, Q et R trois propositions mathématiques :*

1. $P \Leftrightarrow P$ *est toujours vraie.*
2. $(P \Leftrightarrow Q) \Leftrightarrow (Q \Leftrightarrow P)$
3. $(P \Leftrightarrow Q) \Leftrightarrow ((P \Rightarrow Q) \wedge (Q \Rightarrow P))$
4. $((P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R)) \Leftrightarrow (P \Leftrightarrow R)$.

Preuve . En utilisant la table de vérité. ∎

1.3 Quantificateurs

1.3.1 Formes propositionnelles

Définition 1.3.1.1. *On se donne un ensemble E et $P(x)$ est une proposition mathématique dont les valeurs de vérité sont depend aux éléments x de E.*

1.3.2 Quantificateur universel

Définition 1.3.2.1. *la proposition : « Pour tous les éléments x de E, la proposition $P(x)$ est vraie » s'écrit en abrégé : « $\forall x \in E / P(x)$ ».*
$\forall$ s'appelle le ***quantificateur universel****.*

Remarque 1.3.2.1. *$\forall x \in E$ signifier : « tous les éléments de E» ,« tout élément x de E » ou « quelque soit x appartient á E.»*

1.3.3 Quantificateur existentiel

Définition 1.3.3.1. *La proposition : « il existe au moins un élément x de E tel que la proposition $P(x)$ est vraie » s'écrit en abrégé : « $\exists x \in E/P(x)$ ».*
*$\exists$ s'appelle le **quantificateur existentiel**.*

Remarque 1.3.3.1. *La proposition :« il existe un et un seul élément x de E tel que la proposition $P(x)$ est vraie » s'écrit en abrégé : « $\exists! x \in E/P(x)$ ».*

Remarque 1.3.3.2. *1.* $\overline{\forall x \in E} \Leftrightarrow \exists x \in E$
2. $\overline{\exists x \in E} \Leftrightarrow \forall x \in E$.

1.4 Types de raisonnement

1.4.1 Raisonnement déductif

Le schéma du raisonnement déductif est le suivant :

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

Remarque 1.4.1.1. *Sachant de plus que l'implication est transitive, une démonstration prend très souvent la forme suivante : P est vraie et $P \Rightarrow Q \Rightarrow R \Rightarrow ... \Rightarrow S \Rightarrow T$ vraie, et on a donc montré que T est vraie.*

Exemple 1.4.1.1. *l'implication (n un nombre entier impair alors n^2 est un impair) est vraie et 3 est nombre entier impair donc $9 = 3^2$ est un nombre impair.*

1.4.2 Raisonnement par l'absurde

On veut montrer qu'une proposition P est vraie. On suppose que c'est sa négation P qui est vraie et on montre que cela entraîne une proposition fausse. On en conclut que P est vraie (puisque Q est fausse, l'implication $P \Rightarrow Q$ ne peut être vraie que si P est fausse ou encore si P est vraie). Le schéma du raisonnement par l'absurde est le suivant :

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

Exemple 1.4.2.1. *Pour montrer que la proposition $\forall n \in \mathbb{N} : n+1 \neq 0$ est vraie, on suppose que l'est fausse c'est à dire $\exists n \in \mathbb{N} : n+1 = 0$ est vraie alors $n = -1 \in \mathbb{N}$ contradiction avec la définition de l'ensemble $\mathbb{N}$.*
Donc la proposition $\forall n \in \mathbb{N} : n+1 \neq 0$ est vraie.

1.4.3 Raisonnement par contra-posée

Le schéma est le suivant :

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

Exemple 1.4.3.1. *Pour montrer que* $\forall n \in \mathbb{N}$ *si* n^2 *un nombre impair implique que* n *est impaire .*
Il suffit montre que $\forall n \in \mathbb{N}$: $n\,nombre\,paire \Rightarrow n^2\,nombre\,pair$.
En effet n *est pair donc s'écrit de forme* $n = 2m$ *avec* $m \in \mathbb{N}$
alors $n^2 = (2m)^2 = 4m^2 = 2(2m^2)$ *c'est un nombre pair.*
D'où la proposition $\forall n \in \mathbb{N} : n^2\,nombre\,impair \Rightarrow n\,nombreimpaire$ *est vraie.*

1.4.4 Raisonnement par contre exemple

On veut montrer qu'une proposition $\forall x \in E\,/P(x)$ est fausse, il suffit de montre qu'il existe un élément $x_0 \in E$ tel que $\overline{P(x)}$ est vraie.

Exemple 1.4.4.1. *Pour montre que* $P(x) : \forall x \in \mathbb{R} : x^2 - 1 \neq 0$ *est fausse il suffit prendre* $x_0 = 1 \in \mathbb{R}$ *tel que* $x_0^2 - 1 = 0$ *alors* $P(x)$ *est fausse.*

1.4.5 Raisonnement par séparation des cas

Le schéma est le suivant :

($P \Rightarrow Q$ et $\overline{P} \Rightarrow Q$) est une proposition vraie on peut affirmer que Q est une proposition vraie.

Exemple 1.4.5.1. *Montrer que* $\forall n \in \mathbb{N}$ *le nombre* $n(n+1)$ *est pair.*
Pour tout nombre naturel On a cas : n *soit pair ou* n *soit impair.*
Si n *est pair alors* n *s'écrit de forme* $n = 2m$ *avec* $m \in \mathbb{N}$ *donc* $n(n+1) = 2m(2m+1)$ *c'est un nombre pair, d'où* $P \Rightarrow Q$ *est une proposition vraie ;*
Si n *est impair c'est a dire* n *s'écrit de forme* $n = 2m + 1$ *avec* $m \in \mathbb{N}$; *Donc* $n(n+1) = (2m+1)(2m+2) = 2(2m+1)(m+1)$ *c'est un nombre pair,*
d'où $\overline{P} \Rightarrow Q$ *est une proposition vraie.*
Alors pour les deux cas déduit que ($\forall n \in \mathbb{N} : n(n+1)$ *un nombre pair) est une proposition vraie.*

1.4.6 Raisonnement par récurrence

Soit $P(n)$ une proposition mathématique depend à n avec $n \in \mathbb{N}$
Pour montrer que la proposition $\forall n \in \mathbb{N}\,(\forall n \geq n_0)\,/P(n)$ est vraie ;
La démonstration se déroule en trois étapes :

1. l'initialisation : on montrer que $P(n_0)$ est vraie.
2. Pour l'étape d'hérédité : on supposer que $P(k)$ pour tout $n_0 \geq k \geq n$, on démontre alors que l'assertion $P(n+1)$ au rang suivant est vraie.
3. Enfin dans la conclusion, on rappelle que par le principe de récurrence $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

Exemple 1.4.6.1. *Montrer que* $\forall n \in \mathbb{N}^*$ *alors* $1+2+...+n = \dfrac{n(n+1)}{2}$.

On pose $P(n)$: $1+2+...+n = \dfrac{n(n+1)}{2}$.

1. Si $n=1$ on a $1 = \dfrac{1(1+1)}{2}$ donc $P(1)$ est vraie.
2. On supposer que $P(2)$,...,$P(n)$ sont vraies.
3. $1+2+...+n+n+1 = \dfrac{n(n+1)}{2} + n + 1 = \dfrac{(n+1)(n+2)}{2}$ alors $P(n+1)$ est vraie.

1.5 Exercices

Exercice 1 : Montrer que $\overline{P \Rightarrow Q} \Leftrightarrow P \wedge \overline{Q}$.

Exercice 2 : Donner la négation

1. $P \wedge Q \Rightarrow L$,
2. $(P \Rightarrow Q) \wedge L$.

Exercice 3 : Soient P et Q deux propositions.
Écrire en forme simple la proposition suivante

$$(\overline{P} \wedge Q) \vee (\overline{P} \wedge \overline{Q}) \vee (P \wedge Q).$$

Exercice 4 : Montrer que la proposition suivante est vraie et donner sa négation

$$\exists x \in \mathbb{R}\ \forall y \in \mathbb{R} : x^2 + y^2 \geq 0.$$

Exercice 5 : Montrer que l'implication suivante est fausse
$(x \leq 3) \Rightarrow (x^2 \leq 9)$.

Exercice 6 : Soit $n \in \mathbb{Z}$.
Montrer que l'implication : $(n^2\, \textit{nombre impaire}) \Rightarrow (n\, \textit{nombre impair})$ est vraie.

Exercice 7 : Soient a et b deux nombres réels positives
Montrer que :si $\dfrac{a}{b+1} = \dfrac{b}{a+1}$ alors $a = b$.

Exercice 8 : Montrer que pour tout $n \in \mathbb{N}$, $2^n \geq n$.

Exercice 9 : Soient $a, b \in \mathbb{R}_+$.
Montrer que si $a \leq b$ alors $a \leq \dfrac{a+b}{2} \leq b$.

Exercice 10 : Soit $n \in \mathbb{N}^*$.
Montrer que $\sqrt{n^2+1}$ n'est pas un entier.

2

Ensembles , applications et relations binaires

2.1 Ensembles

2.1.1 Définitions et exemples

On va définir informellement ce qu'est un ensemble ; Un ensemble est une collection d'éléments par exemple $\{0,1\}$, $\mathbb{N} = \{0,1,2,...\}$.

Notation

- Un ensemble particulier est l'ensemble vide, noté $\varnothing$ qui est l'ensemble ne contenant aucun élément.
- On note $x \in E$ si x est un élément de E, et $x \notin E$ dans le cas contraire.
- Nombre des éléments de E est appelé le cardinal de E noté $cardE$.

2.1.2 Algèbre des ensembles

Définition 2.1.2.1. *Soient E et F deux ensembles,on dit que F est **inclus** dans E si tout élément de F est aussi un élément de E et noté $F \subset E$. On dit alors que F est un sous-ensemble de E ou F une partie de E.*

Exemple 2.1.2.1. *1)* $\{0,1\} \subset \{0,1,2\}$.
2) $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Remarque 2.1.2.1. *On dit que $E = F$ si $E \subset F$ et $F \subset E$.*

Définition 2.1.2.2. *L'ensemble des parties de E, on note $\mathcal{P}(E)$: est l'ensemble de tous les parties de E.*

Remarque 2.1.2.2. *Si E est un ensemble finie c'est à dire $card\, E$ finie alors $card\, \mathcal{P}(E) = 2^{cardE}$.*

Exemple 2.1.2.2. *Soit $E = \{0,1,2\}$ alors $\mathcal{P}(E) = \{\varnothing, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{0,1,2\}\}$.*

Définition 2.1.2.3. *Soient A et B deux parties vides de E;*
L'ensemble des éléments communs qui sont appartient aux A et B, en même temps est appelé ***intersection*** *de A et B est, noté $A \cap B$*
Autrement dit : $A \cap B = \{x \in E\,/(x \in A) \wedge (x \in B)\}$.

Exemple 2.1.2.3. *Soient $E = \mathbb{R}$,$A = \{0,1,2,3,4\}$ et $B\{0,3,6\}$ alors $A \cap B = \{0,3\}$.*

Définition 2.1.2.4. *Soient A et B deux parties vides de E ;*
L'ensemble des éléments qui sont appartient aux A ou B, est appelé ***union*** *de A et B, noté $A \cup B$*
Autrement dit :$A \cup B = \{x \in E\,/(x \in A) \vee (x \in B)\}$.

Exemple 2.1.2.4. *Soient $E = \mathbb{R}$,$A = \{0,1,2,3,4\}$ et $B = \{0,3,6\}$ alors $A \cup B = \{0,1,2,3,4,6\}$.*

Définition 2.1.2.5. *Soit A une partie de E ;*
Complémentaire *de A dans E est l'ensemble des éléments de E qui sont n'appartient pas à A noté C_E^A*
Autrement dit : $\mathrm{C}_E^A = \{x \in E\,/x \notin A\}$.

Remarque 2.1.2.3. *On note aussi le complémentaire de A dans E par A^c, ou $E \setminus A$.*

Exemple 2.1.2.5. *$E = \{0,1,2,3,4\}$ et $A = \{0,3\}$ alors $\mathrm{C}_E^A = \{,1,2,4\}$*

Définition 2.1.2.6. *Soient E un ensemble non vide et A, B deux parties non vides de E.*
La différence symétrique *de A et B notée $A\Delta B$ est définie par $A\Delta B = (A/B) \cup (B/A)$*

Remarque 2.1.2.4. *$(A/B) = \{x \in E/x \in A \wedge x \notin B\}$.*

Remarque 2.1.2.5. *$A\Delta B = (A \cup B)/(A \cap B) = \mathrm{C}_{A\cup B}^{A\cap B}$.*

Exemple 2.1.2.6. *Soient $E = \{0,1,2,3,4,5,6\}$, $A = \{0,3,5,6\}$ et $B = \{0,2,3,4\}$ alors $A \triangle B = \{2,4,5,6\}$.*

Définition 2.1.2.7. *Soient E un ensemble non vide et $\mathcal{A} \subseteq \mathcal{P}(E)$. On dit que $\mathcal{A}$ est une partition de E si et seulement si*

1. *Chaque élément de $\mathcal{A}$ est non vide.*
2. *Les éléments de $\mathcal{A}$ sont disjoints deux à deux.*
3. *Union des éléments de $\mathcal{A}$ égale à E.*

Exemple 2.1.2.7. *Soit $E = \{0,1,2,3,4,5,6\}$ alors $\mathcal{A} = \{\{0,1\},\{2\},\{3,4,5,6\}\}$ est une partition de E.*

2.1.3 Règles de calculs

Soient A, B,et C trois parties non vides d'un ensemble E.

1. $A \cap B = B \cap A$.
2. $A \cap (B \cap C) = (A \cap B) \cap C$.
3. $A \cap \varnothing = \varnothing$, $\quad A \cap A = A$, $\quad A \subset B \Rightarrow A \cap B = A$.

4. $A \cup B = B \cup A$.
5. $A \cup (B \cup C) = (A \cup B) \cup C$.
6. $A \cup \varnothing = A, \qquad A \cup A = A, \qquad A \subset B \Rightarrow A \cup B = B$.
7. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
8. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
9. $(A^c)^c = A \qquad A \subset B \Leftrightarrow B^c \subset A^c$.
10. $(A \cap B)^c = A^c \cup B^c)$.
11. $(A \cup B)^c = A^c \cap B^c$.
12. $A \cap A^c = \varnothing \qquad et\ A \cup A^c = E$.
13. $E^c = \varnothing \qquad et\ \varnothing^c = E$.

2.1.4 Produit cartésien

Définition 2.1.4.1. *Soient E et F deux ensembles non vides.*
***Le produit cartésien**, noté $E \times F$ est l'ensemble des couples (x, y) où $x \in E$ et $y \in F$.*

Exemple 2.1.4.1. *Soient $E = \{0, 1, 2\}$ et $F = \{3, 4\}$ $E \times F = \{(0, 3), (0, 4), (1, 3), (1, 4), (2, 3), (2, 4)\}$.*

2.2 Applications

2.2.1 Définitions et exemples

Définition 2.2.1.1. *Soient E et F deux ensembles non vides*
***Une application** f de E dans F c'est la donnée pour chaque élément $x \in E$ d'un unique élément $f(x)$ de F on noté $f : E \to F$.*

Exemple 2.2.1.1. *Soient $E = \{1, 2, 3\}$, $F = \{-1, -2, -3\}$;*
On peut définir l'application $f : E \to F$ par
$f(1) = -1 \quad f(2) = -2 \quad f(3) = -3$.

Exemple 2.2.1.2. *Soient E un ensemble non vide,l'application $f : E \to E$ définie par $\forall x \in E \quad f(x) = x$ s'appelle d'identité notée id_E.*

Remarque 2.2.1.1. *Nous représenterons l'application par une flèche par exemple $x \mapsto f(x)$.*

Exemple 2.2.1.3. $E = F = \mathbb{R}$

1. $x \mapsto x + 2$.
2. $x \mapsto x^2$.
3. $x \mapsto sin(x)$.

Définition 2.2.1.2. *$f, g : E \to F$ deux applications sont dites égales si et seulement si pour tout $x \in E$ on a $f(x) = g(x)$. On écrit $f = g$.*

Exemple 2.2.1.4. *Soient $E = F = \mathbb{R}_+$ et $f(x) = x$ et $g(x) = |x|$ sont égales.*

Définition 2.2.1.3. *Soient E,F deux ensembles non vides et f une application de E dans F, Le graphe de f est l'ensemble des couples $(x, f(x))$ avec $x \in E$ on note Γ_f c'est à dire $\Gamma_f = \{(x, f(x)) \in E \times F\}$.*

Définition 2.2.1.4. *Soient $f : E \to F$ et $g : F \to G$ deux applications,on note $g \circ f$ de l' application de E dans G définie par $(g \circ f)(x) = f(g(x))$ on la appelée* ***application composée*** *de f et g*

Exemple 2.2.1.5. *Soient $E = G = \mathbb{R}$ $F = \mathbb{R}_+$*
$f(x) = x^2$ et $g(x) = \sqrt{x}$ alors $(f \circ g)(x) = f(g(x)) = (\sqrt{x})^2 = x$.

2.2.2 Image directe

Définition 2.2.2.1. *Soient E, F deux ensembles non vides, et $f : E \to F$, une application de E dans F,* ***l'image directe*** *d'un sous ensemble A de E par f est l'ensemble*

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

Exemple 2.2.2.1. *Soient $E = F = \mathbb{R}$,$A = [0, 2]$ et $f(x) = x^2$ alors $f(A) = [0, 4]$*

2.2.3 Image réciproque

Définition 2.2.3.1. *Soient E ,F deux ensembles non vides, $f : E \to F$, une application de E dans F, et $A \subset F$* ***l'image réciproque*** *de A par f est l'ensemble*

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

Exemple 2.2.3.1. *Soient $E = F = \mathbb{R}$,$A = [0, 4[$ et $f(x) = x^2$ alors $f^{-1}(A) =]-2, 2[$.*

2.2.4 Injection, surjection, bijection

Soient E, F deux ensembles non vides et $f : E \to F$ une application de E dans F

Définition 2.2.4.1. *f est dite* ***injective*** *si et seulement si pour tout $x, x' \in E$ on a*

$$\boxed{f(x) = f(x') \Rightarrow x = x'.}$$

Définition 2.2.4.2. *f est dite* ***surjective*** *si et seulement si pour tout $y \in F$ il existe un élément $x \in E$ tel que $y = f(x)$ c'est à dire*

$$\boxed{\forall y \in F \quad \exists x \in E \quad / \, y = f(x).}$$

Définition 2.2.4.3. *f est* ***bijective*** *si elle est injective et surjective*

$$\boxed{\forall y \in F \quad \exists! x \in E \quad / \, y = f(x).}$$

Exemple 2.2.4.1. *Soient E, F deux parties de $\mathbb{R}$ et $f : E \to F$ avec $f(x) = x^2$*

1. *Si $E = \mathbb{R}_+$ et $F = \mathbb{R}$ alors est injective non surjective.*
2. *Si $E = \mathbb{R}$ et $F = \mathbb{R}_+$ alors est surjective non injective.*
3. *Si $E = F = \mathbb{R}_+$ alors est injective et surjective donc elle est bijective.*

Proposition 2.2.4.1. *Soient E, F deux ensembles et $f : E \to F$ une application de E dans F.*

1. *L'application f est bijective si et seulement s'il existe une application $g : F \to E$ telle que $f \circ g = id_F$ et $g \circ f = id_E$.*
2. *Si f est bijective alors l'application g est unique et elle estaussi est bijective.*
   L'application g s'appelle la bijection réciproque de f et elle est notée f^{-1}.
   De plus on a $(f^{-1})^{-1} = f$.

2.3 Relations binaires

2.3.1 Définitions et exemples

Soit E un ensemble non vide.

Définition 2.3.1.1. *Une* ***relation*** *$\mathcal{R}$ sur E, c'est la donnée pour tout couple $(x, y) \in E \times E$ de « Vrai » on note $x\mathcal{R}y$ (s'ils sont en relation), ou de « Faux » sinon.*

Exemple 2.3.1.1. *On définit sur $\mathbb{R}$ la relation $\mathcal{R}$ par*
$\forall (x, y) \in \mathbb{R}^2 : \; x\mathcal{R}y \Leftrightarrow x \leqslant y$
donc $1\mathcal{R}2$ est vraie.
Mais $2\mathcal{R}1$ est fausse.

Définition 2.3.1.2. *Soit E un ensemble non vide, $\mathcal{R}$ une relation sur E, est dite* ***réflexive*** *si et seulement si :*

$$\boxed{\forall x \in E : \; x\mathcal{R}x.}$$

Exemple 2.3.1.2. *Soit On définit sur $\mathbb{R}$ la relation $\mathcal{R}$ par $\forall (x, y) \in \mathbb{R}^2 : \; x\mathcal{R}y \Leftrightarrow x \leqslant y$.*
$\mathcal{R}$ est réflexive puisque $\forall x \in \mathbb{R}$ on a $x \leqslant x$.

Définition 2.3.1.3. *Soit E un ensemble non vide, $\mathcal{R}$ une relation sur E, est dite* ***symétrique*** *si et seulement si :*

$$\boxed{\forall (x,y) \in E^2 : \ x\mathcal{R}y \Rightarrow y\mathcal{R}x.}$$

Exemple 2.3.1.3. *On définit sur $\mathbb{R}$ la relation $\mathcal{R}$ par $\forall (x,y) \in \mathbb{R}^2 : \ x\mathcal{R}y \Leftrightarrow x = y$ est symétrique.*

Définition 2.3.1.4. *Soit E un ensemble non vide, $\mathcal{R}$ une relation sur E, est dite* ***transitive*** *si et seulement si :*

$$\boxed{\forall (x,y,z) \in E^3 : \ (x\mathcal{R}y) \wedge (y\mathcal{R}z) \Rightarrow x\mathcal{R}z.}$$

Exemple 2.3.1.4. *On définit sur $\mathbb{R}$ la relation $\mathcal{R}$ par $(x,y) \in \mathbb{R}^2 \, x\mathcal{R}y \Leftrightarrow x \leqslant y$ est transitive.*

Définition 2.3.1.5. *Soit E un ensemble non vide, $\mathcal{R}$ une relation sur E, est dite* ***anti-symétrique*** *si :*

$$\boxed{\forall (x,y) \in E^2 : \ (x\mathcal{R}y \wedge y\mathcal{R}x) \Rightarrow x = y.}$$

Exemple 2.3.1.5. *Soit F un ensemble non vide $\mathcal{P}(F) = E$ est l'ensemble des parties de F on définit sur E la relation $\mathcal{R}$ par $\forall (A,B) \in E^2 : \ A\mathcal{R}B \Leftrightarrow A \subseteq B$. $\mathcal{R}$ est anti-symétrique.*

2.3.2 Relation d'équivalence

Définition 2.3.2.1. *$\mathcal{R}$ une relation sur E, est dite* ***relation d'équivalence*** *si elle est :*

1. *réflexive,*
2. *symétrique et*
3. *transitive.*

Exemple 2.3.2.1. *On définit sur $\mathbb{Z}$ la relation $\mathcal{R}$ par $\forall (x,y) \in \mathbb{Z}^2 : \ x\mathcal{R}y \Leftrightarrow (x-y) \in \mathbb{Z}$. alors $\mathcal{R}$ est une relation d'équivalence*

Définition 2.3.2.2. *Soient E un ensemble non vide et $\mathcal{R}$ une relation d'équivalence, Pour tout $a \in E$ on définit* ***la classe d'équivalence de*** *a note $\widehat{a}$ est l'ensemble $\widehat{a} = \{x \in E / x\mathcal{R}a\}$.*

Exemple 2.3.2.2. *On définit sur $\mathbb{Z}$ la relation $\mathcal{R}$ par $\forall (x,y) \in \mathbb{Z}^2 : \quad x\mathcal{R}y \Leftrightarrow (x-y) \in 2\mathbb{Z}$. Est facile démontrer que $\mathcal{R}$ est une relation d'équivalence et on a*

$$\widehat{0} = \{x \in \mathbb{Z} \, / \, x\mathcal{R}0\} = 2\mathbb{Z}.$$

Et

$$\widehat{1} = \{x \in \mathbb{Z} \, / \, x\mathcal{R}1\} = 1 + 2\mathbb{Z}$$

$2\mathbb{Z}$ entiers pairs et $1 + 2\mathbb{Z}$ entiers impairs .

Définition 2.3.2.3. *Soit $\mathcal{R}$ une relation d'équivalence sur E, l'ensemble de tous les classes d'équivalences s'appelle* ***espace quotient*** *note $E/\mathcal{R}$*

Exemple 2.3.2.3. $E = \mathbb{Z}\ \forall (x,y) \in \mathbb{Z}^2 \qquad x\mathcal{R}y \Leftrightarrow (x-y) \in 2\mathbb{Z}$.
Alors $E/\mathcal{R} = \{\widehat{0}, \widehat{1}\} = \{2\mathbb{Z}, 1+2\mathbb{Z}\}$, *aussi on peut écrire* $\mathbb{Z}/2\mathbb{Z} = \{\widehat{0}, \widehat{1}\}$.

2.3.3 Relation d'ordre

Définition 2.3.3.1. *$\mathcal{R}$ une relation sur E, est dite* ***relation d'ordre*** *si elle est :*

1. *réflexive*
2. *anti-symétrique*
3. *transitive.*

Exemple 2.3.3.1. *Soit F un ensemble non vide $\mathcal{P}(F) = E$ est l'ensemble des parties de F on définit sur E la relation $\mathcal{R}$ par $\forall (A,B) \in E^2 :\ A\mathcal{R}B \Leftrightarrow A \subseteq B$. $\mathcal{R}$ est une relation d'ordre.*

Définition 2.3.3.2. *$\mathcal{R}$ une relation d'ordre sur E, est dite* ***relation d'ordre totale*** *si*

$$\boxed{\forall (x,y) \in E^2 \text{ on a } x\mathcal{R}y \text{ ou } y\mathcal{R}x.}$$

Exemple 2.3.3.2. *On définit sur $\mathbb{R}$ la relation $\mathcal{R}$ par $\forall (x,y) \in \mathbb{R}^2 :\ x\mathcal{R}y \Leftrightarrow x \leqslant y$ est une relation d'ordre totale.*

Définition 2.3.3.3. *$\mathcal{R}$ une relation d'ordre sur E, est dite* ***relation d'ordre partielle*** *si elle n'est pas une relation d'ordre totale.*

Remarque 2.3.3.1. *$\mathcal{R}$ une relation d'ordre définie sur un ensemble non vide E, est partielle s'il existe $(x,y) \in E$ tels que $\overline{x\mathcal{R}y} \wedge \overline{y\mathcal{R}x}$*

Exemple 2.3.3.3. *Soit F un ensemble non vide $\mathcal{P}(F) = E$ est l'ensemble des parties de F $\forall (A,B) \in E^2 :\ A\mathcal{R}B \Leftrightarrow A \subseteq B$ est une relation d'ordre partielle .*

Définition 2.3.3.4. *Soient $\mathcal{R}$ une relation d'ordre définie sur un ensemble non vide E, et A une partie non vide de E dite* ***majorée*** *si et seulement si*

$$\boxed{\exists M \in E\,;\, \forall x \in A \text{ on a } x\mathcal{R}M.}$$

Définition 2.3.3.5. *Soient $\mathcal{R}$ une relation d'ordre définie un ensemble non vide E, et A une partie non vide, on dit un élément M de E est* ***majorant de*** *A si et seulement si*

$$\boxed{\forall x \in A \text{ on a } x\mathcal{R}M.}$$

Définition 2.3.3.6. *Soient $\mathcal{R}$ une relation d'ordre définie un ensemble non vide E, A une partie non vide, on dit qu un élément M de E est* ***supérieur de*** *A si et seulement si*

1. *M est un majorant de A*
2. *pour tout x majorant de A alors on a $x\mathcal{R}M$ ou (M, x) non ordonné.*

Remarque 2.3.3.2. *Si $\mathcal{R}$ est une relation d'ordre totale alors la deuxième condition devient : pour tout x majorant de A alors on a $x\mathcal{R}M$.*

Exemple 2.3.3.4. *la relation inférieur ou égale $\leq$ est une relation d'ordre totale sur $\mathbb{R}$ donc l'ensemble $\mathbb{R}_-$ est majorée.*
L'ensemble des majorants de $\mathbb{R}_-$ sont les réels positives $\mathbb{R}_+$
Supérieur de $\mathbb{R}_-$ est 0

Définition 2.3.3.7. *Soient $\mathcal{R}$ une relation d'ordre définie sur un ensemble non vide E, et A une partie non vide de E on dit que A* ***minorée*** *si et seulement si*

$$\boxed{\exists m \in E\,, \forall x \in A \text{ on a } m\mathcal{R}x.}$$

Définition 2.3.3.8. *Soient $\mathcal{R}$ une relation d'ordre définie un ensemble non vide E, A une partie non vide, on dit qu' un élément m de E est* ***minorant de*** *A si et seulement si*

$$\boxed{\forall x \in A \text{ on a } m\mathcal{R}x.}$$

Définition 2.3.3.9. *Soient $\mathcal{R}$ une relation d'ordre définie sur un ensemble non vide E, A une partie non vide, on dit qu' un élément m de E est* ***inférieur de*** *A si seulement si*

1. *m est un minorant de A*
2. *pour tout x minorant de A alors on a $m\mathcal{R}x$ ou (m, x) non ordonnée.*

Remarque 2.3.3.3. *Si $\mathcal{R}$ une relation d'ordre totale alors la deuxième condition devient :pour tout x minorant de A alors on a $m\mathcal{R}x$.*

Exemple 2.3.3.5. *la relation $\leq$ est une relation d'ordre totale sur $\mathbb{Z}$ alors $\mathbb{N}$ l'ensemble des nombres naturels est minorée.*
L'ensemble des minorants de $\mathbb{N}$ sont les entiers négatives $\mathbb{Z}_-$
Donc l'inférieur de $\mathbb{N}$ est 0.

2.4 Exercices

Exercice 1 : Soit $E = \{1, 2, 3, 5\}$.
Déterminer $\mathcal{P}(E)$.

Exercice 2 : Déterminer $\mathbb{R} \cup \mathbb{R}_+$, $\mathbb{R}_- \cup \mathbb{R}_+$, $\mathbb{R} \cup \mathbb{Z}$ et $\mathbb{N} \cup \mathbb{Q}$.

Exercice 3 : Soient $E = \{0, 1, 2, 3, 4, 6, 5, 7, 9\}$, $A = \{1, 2, 3, 4\}$ et $B = \{1, 2, 5, 6\}$.
Déterminer $A \cap B$, $A \cup B$, A^c, $(A \cap B)^c$, $(A \cup B)^c$ et $A \Delta B$.

Exercice 4 : Montrer que $\mathcal{A} = \{[n, n+1[/\ n \in \mathbb{N}\}$ est une partition de $\mathbb{N}$.

Exercice 5 : Soient $f : \mathbb{R}_+ \to \mathbb{R}$ et $g : \mathbb{R} \to \mathbb{R}_+$ telles que $f(x) = 3x + 1$ et $g(x) = x$.
A-t-on $f \circ g = g \circ f$?

Exercice 6 : Soient $f : E \to F$ une application de E dans F et A, B deux parties non vides de E.
Montrer que :

1. $f(A \cap B) \subseteq f(A) \cap f(B)$.
2. $f(A \cup B) = f(A) \cup f(B)$.

Exercice 7 : Soient $f : E \to F$ une application de E dans F et A, B deux parties non vides de F.
Montrer que :

1. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.
2. $f^{-1}(A) \cup f^{-1}(B) \subseteq f^{-1}(A \cup B)$.

Exercice 8 : Soient $f : E \to F$ une application de E dans F ,A une partie non vide de F.
Montrer que : $f^{-1}(\mathrm{C}_F^A) = \mathrm{C}_E^{f^{-1}(A)}$.

Exercice 9 : Soit $f : \mathbb{R} \to \mathbb{R}$ une application définie par $f(x) = \dfrac{x}{x^2 + 1}$

1. f est elle injective ? surjective ?

2. Déterminer $f(\mathbb{R})$.

Exercice 10 : Soit $f : \mathbb{R} \to \mathbb{R}$ une application définie par $f(x) = |x| + 2x$

1. Montrer que$f$ est injective et surjective

2. Déterminer f^{-1}.

Exercice 11 : Montrer que si $\mathcal{R}$ est une relation d'équivalence sur un ensemble non vide E alors $E/\mathcal{R}$ est une partition de E.

Exercice 12 : On définit sur $\mathbb{Z}$ la relation$\mathcal{R}$ par $\forall (x,y) \in \mathbb{Z} : x\mathcal{R}y \Leftrightarrow \exists n \in \mathbb{Z} \,/\, x - y = 5n$.

1. Montrer que $\mathcal{R}$ est relation d'équivalence.

2. Déterminer $\mathbb{Z}/\mathcal{R}$.

Exercice 13 : Soit $\mathcal{R}$ une relation sur E dite relation **circulaire** si

$$\boxed{\forall x, y, z \in E \;\; : \; x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow z\mathcal{R}x}$$

Montrer que si $\mathcal{R}$ est circulaire et réflexive alors elle est une relation d'équivalence.

Exercice 14 : Soit $\mathcal{R}$ une relation d'équivalence sur $\mathbb{R}$ par

$\forall (x,y) \in \mathbb{R} : x\mathcal{R}y \Leftrightarrow \exists n \in \mathbb{Z} \quad x, y \in [n, n+1[$.

1. Déterminer les classes d'équivalences $\mathbb{R}/\mathcal{R}$.

2. Montrer que
$\begin{array}{c} f : \mathbb{Z} \longrightarrow \mathbb{R}/\mathcal{R} \\ x \longmapsto \widehat{x} \end{array}$ est une application bijective.

Exercice 15 : Soit $\mathcal{R}$ une relation définie sur $\mathbb{R} \times \mathbb{R}$ par

$$(x,y)\mathcal{R}(x',y') \Rightarrow (x < x') \vee (x = x') \wedge (y \leq y')$$

Étudier les propriétés de $\mathcal{R}$.

Exercice 16 : Soit $\mathcal{R}$ une relation définie sur $\mathbb{R}$ par

$\forall (x,y) \in \mathbb{R} : x\mathcal{R}y \Rightarrow \exists n \in \mathbb{Z} \quad x, y \in [n, n+1[\;\; et \, x \leq y$.

1. Vérifier que $\mathcal{R}$ est une relation d'ordre.
2. Montrer que [0,1[est majorée ? minorée ?
3. $\begin{array}{c} f : \mathbb{R} \longrightarrow \mathbb{Z} \times [0,1[\\ x \longmapsto ([x], x - [x]) \end{array}$ est une application bijective.

3

Structures algèbriques

3.1 Groupes

3.1.1 Loi de composition

Soit G un ensemble non vide.

Définition 3.1.1.1. *Loi de composition interne dans G noté $\star$ est une application définie par*

$$\begin{array}{c} \star : G \times G \to G \\ (x, y) \mapsto x \star y \end{array}$$

Exemple 3.1.1.1. *On note $\times$ multiplication usuelle des nombres réels*
$\begin{array}{c} \times : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \\ (x, y) \mapsto x \times y \end{array}$ *est une loi de composition interne dans $\mathbb{R}$.*

Définition 3.1.1.2. *Soit $\star$ une loi de composition interne dans G. $\star$ est dite* ***associative*** *si et seulement si*

$$\boxed{\forall x, y, z \in G : \quad x \star (y \star z) = (x \star y) \star z.}$$

Définition 3.1.1.3. *Soit $\star$ une loi de composition interne dans G. $\star$ est dite* ***abélienne ou commutative*** *si et seulement si*

$$\boxed{\forall x, y \in G : \quad x \star y = y \star x.}$$

Définition 3.1.1.4. *Soit $\star$ une loi de composition interne dans G et soit e un élément de G. e est dit* ***un élément neutre*** *dans G si et seulement si*

$$\boxed{\forall x \in G : \quad x \star e = e \star x = x.}$$

Définition 3.1.1.5. *Soient $\star$ une loi de composition interne dans G, et soit e un élément neutre dans G.*
*Soit x' un élément de G. x' est dit **symétrie d'un élément** x de G si et seulement si*

$$\boxed{x \star x' = x' \star x = e.}$$

3.1.2 Groupe et sous groupe

Définition 3.1.2.1. *Soit Gun ensemble non vide et $\star$ une loi définie sur G. On dit que $(G, \star)$ est un **groupe** si et seulement si vérifiant*

1. *$\star$ loi interne dans G,*
2. *$\star$ est associative,*
3. *il existe un élément neutre dans G*
4. *tout élément de G admit un symétrie dans G.*

Remarque 3.1.2.1. *$(G, \star)$ est dit un **groupe abélien ou commutatif** si $(G, \star)$ est un groupe et $\star$ est commutative.*

Exemple 3.1.2.1. *Soient $+$ et $\times$ l'addition et la multiplication usuelles des nombres alors on a :*

1. *$(\mathbb{Z}, +)$ est un groupe abélien.*
2. *$(\mathbb{Q}, +)$ est un groupe abélien.*
3. *$(\mathbb{R}, +)$ est un groupe abélien.*
4. *$(\mathbb{C}, +)$ est un groupe abélien.*
5. *$(\mathbb{Q}^\star, \times)$ est un groupe abélien.*
6. *$(\mathbb{R}^\star, \times)$ est un groupe abélien.*
7. *$(\mathbb{C}^\star, \times)$ est un groupe abélien.*

Proposition 3.1.2.1. 1. *L'élément neutre dans un groupe est unique.*
2. *Le symétrie d'un élément dans un groupe est unique.*

Preuve . Exercice ∎

Remarque 3.1.2.2. *$(\mathbb{N}, +)$ n'est pas un groupe, puisque l'élément symétrie de 1 est (-1) qui n'appartient pas à $\mathbb{N}$.*

Définition 3.1.2.2. *Soit $(G, \star)$ un groupe, on qu'une partie H de G est un **sous groupe** de G si et seulement si vérifiant*

1. *$H \neq \varnothing$,*
2. *$\forall x, y \in H : x \star y \in H$,*
3. *$\forall x \in H : x' \in H$.*

Proposition 3.1.2.2. *Soit $(G,\star)$ un groupe d'élément neutre e et H une partie de G. H est un sous groupe de G si et seulement si*

1. $e \in H$
2. $\forall x, y \in H : x \star y' \in H$.

Preuve .$\Longrightarrow$
H un sous groupe de G. Soit $x \in H$ donc $x' \in H$ alors $x.x' = e \in H$
Soient $x, y \in H$
alors $y' \in H$ donc $xy' \in H$.
$\Longleftarrow$
Comme $e \in H$ alors $H \neq \varnothing$.
On prend $x = e$ et $y \in H$ alors $x.y' = e.y' = y' \in H$.
Soient $x, y \in H$ donc $y' \in H$
alors $x.(y')' = xy \in H$
donc H est un sous groupe. ∎

Exemple 3.1.2.2. $(2\mathbb{Z},+)$ *est un sous groupe de* $(\mathbb{Z},+)$ *en effet*

1. $0 = 2 \times 0 \in 2\mathbb{Z}$ *donc* $2\mathbb{Z} \neq \varnothing$.
2. *Soient* $x = 2k \in 2\mathbb{Z}$ *et* $y = 2l \in 2\mathbb{Z}$ *avec* $k, l \in \mathbb{Z}$,
   donc $x + y = 2k + 2l = 2(k + l) \in 2\mathbb{Z}$.
3. *Soit* $x = 2k \in 2\mathbb{Z}$ *avec* $k \in \mathbb{Z}$
   alors $x' = -x = 2(-k) \in 2\mathbb{Z}$.

Définition 3.1.2.3. *Soit $(G,\star)$ un groupe et H un sous groupe de G est dite un sous groupe* ***distingue ou normal*** *de G si*

$$\boxed{\forall x \in G \ \ \forall h \in H \ \ : \ x \star h \star x' \in H.}$$

3.1.3 Morphisme de groupe

Définition 3.1.3.1. *Soient $(G,\star)$, $(H,\bullet)$ deux groupes, et soit$f : G \to H$ une application.On dit que f est un* ***morphisme ou homomorphisme de groupe*** *si*

$$\boxed{\forall x, y \in G \qquad f(x \star y) = f(x) \bullet f(y).}$$

Exemple 3.1.3.1. *L'application*
$f : (\mathbb{R},+) \to (\mathbb{R}_+^\star,\times)$
$x \mapsto \exp(x)$
est un homomorphisme de groupe.
En effet pour tout $x, y \in \mathbb{R}$ on a $\exp(x + y) = \exp(x) \times \exp(y)$

Proposition 3.1.3.1. *Soient $(G,\star)$ et $(G',\bullet)$ deux groupes, et $f : G \to G'$ un homomorphisme de groupe alors :*
Si e est l'élément neutre de G et e' l'élément neutre de G' alors $f(e) = e'$.

Preuve . Exercice. ∎

Proposition 3.1.3.2. *Soient $(G,\star)$ et $(G',*)$ deux groupes, $f : G \to G'$ un homomorphisme de groupe et soit x un élément de G alors :*
Si x' l'élément symétrie de x dans G alors $f(x')$ l'élément symétrie de $f(x)$ c'est à dire $f(x') = f(x)'$.

Preuve . Exercice. ∎

Définition 3.1.3.2. *Soient $(G,\star)$ et $(H,\bullet)$ deux groupes,et $f : G \to H$ un homomorphisme de groupe le* ***noyau de*** *f , note* $\ker f$ *est l'ensemble*

$$\boxed{\ker f = \{x \in G \ / f(x) = e'\}}$$

tel que e' est l'élément neutre de H.

Remarque 3.1.3.1. $\ker f = f^{-1}\{e'\} \subseteq G$.

Proposition 3.1.3.3. *Soient $(G,\star)$ et $(H,\bullet)$ deux groupes,et $f : G \to H$ un homomorphisme de groupe alors* $\ker f$ *est un sous groupe de G.*

Preuve . En effet

1. $\ker f \neq \varnothing$ puisque $e \in \ker f$
2. Pour tout $x \in H$ on a $f(e) \bullet f(x) = f(e \star x) = f(x)$
   et $f(x) \bullet f(e) = f(x \star e) = f(x)$
   alors $f(e) = e'$ (d'après l'unicité de l'élément neutre) ;
3. Soient $x, y \in \ker f$ donc $f(x \star y) = f(x) \bullet f(y) = e'$;
   Alors $x \star y \in \ker f$
4. Soit $x \in \ker f$ et x' son symétrie on a $f(x) \bullet f(x') = f(x \star x') = f(e) = e'$ d'une part
   Et d'autre part, puisque $f(x) = e'$ donc $f(x) \bullet f(x') = e' \bullet f(x') = f(x')$
   alors $f(x') = e'$
   d'où $x' \in \ker f$.

∎

Définition 3.1.3.3. *Soient $(G,\star)$ et $(H,\bullet)$ deux groupes, $f : G \to H$ un homomorphisme de groupe* ***l'image de*** *f , note Imf, est l'ensemble*

$$\boxed{Imf = \{f(x) \ / x \in G\}.}$$

Remarque 3.1.3.2. $Imf = f(G) \subseteq H$

Proposition 3.1.3.4. *Soient $(G,\star)$ et $(H,\bullet)$ deux groupes, $f : G \to H$ un homomorphisme de groupe alors Imf est un sous groupe de H.*

Preuve . Exercice

■

Définition 3.1.3.4. *Soient $(G,\star)$ et $(H,\bullet)$ deux groupes, $f : G \to H$ un homomorphisme de groupe alors*
f est un isomorphisme si f bijective.

Exemple 3.1.3.2. *L'homomorphisme de groupe.*
$f : (\mathbb{R},+) \to (\mathbb{R}_+^\star,\times)$
$x \mapsto \exp(x)$
est un isomorphisme.
En effet

1. *D'apres l'exemple (3.1.3.1) f est un morphisme de groupe.*
2. *On va montrer que f est injective, soient $x,x' \in \mathbb{R}$*
   si $f(x) = f(x')$ alors $\exp(x) = \exp(x')$ donc $x = x'$
3. *On va montrer que f est surjective, soit $y \in \mathbb{R}_+^\star$ avec $y = f(x)$ donc $y = \exp(x)$ alors $x = \ln y$.*

Exemple 3.1.3.3. *L'homomorphisme de groupe.*
$f : (\mathbb{R}^\star,\times) \to (\mathbb{R}^\star,\times)$
$x \mapsto x^2$
est un homoomorphisme. Le noyau $\ker f = \{-1,1\}$ et l'image de $Imf = \mathbb{R}_+^\star$.
En effet, soit $x,y \in \mathbb{R}^\star$ alors

$$f(x\times y) = (x\times y)^2 = x^2 \times y^2 = f(x)\times f(y)$$

donc f est un homomorphisme de groupe. Et

$$\begin{aligned}\ker f &= \{x \in \mathbb{R}^\star / f(x) = 1\}\\ &= \{x \in \mathbb{R}^\star / x^2 = 1\}\\ &= \{-1,1\}\end{aligned}$$

donc f n'est pas injective. f n'est pas surjective puisque

$$\begin{aligned}Imf &= \{f(x)/x \in \mathbb{R}^\star\}\\ &= \{x^2/x \in \mathbb{R}^\star\}\\ &= \mathbb{R}_+^\star.\end{aligned}$$

Exemple 3.1.3.4. *L'homomorphisme de groupe.*
$f : (\mathbb{R}_+^\star,\times) \to (\mathbb{R}_+^\star,\times)$
$x \mapsto x^2$
est un isomorphisme.

Proposition 3.1.3.5. *Soient $(G,\star)$ et $(H,\bullet)$ deux groupes, $f : G \to H$ un homomorphisme de groupe alors*

$$\boxed{f \text{ est injective si seulement si } \ker f = \{e\},}$$

où e l'élément neutre de G.

Preuve . Exercice. ∎

Proposition 3.1.3.6. *Soient $(G, \star)$ et $(H, \bullet)$ deux groupes, $f : G \to H$ un homomorphisme de groupe alors*

$$\boxed{f \text{ est surjective si seulement si } Imf = H.}$$

Preuve . Exercice. ∎

3.2 Anneau et corps

3.2.1 Anneau

Définition 3.2.1.1. *Soit $(A, \star, \intercal)$ un ensemble non vide muni deux lois internes, on dit $(A, \star, \intercal)$ un **anneau** si et seulement si*

1. *$(A, \star)$ groupe abélien,*
2. *$\intercal$ est associative,*
3. *$\intercal$ est distributive sur $\star$: pour tout $x, y, z \in A$ on a $x \intercal (y \star z) = (x \intercal y) \star (x \intercal z)$ et $(y \star z) \intercal x = (y \intercal x) \star (z \intercal x)$.*

Remarque 3.2.1.1. *Soit $(A, \star, \intercal)$ un anneau :*
Si $(A, \intercal)$ admet un élément neutre alors on dit que $(A, \star, \intercal)$ est un anneau unitaire
Si $\intercal$ commutative alors on dit que $(A, \star, \intercal)$ est un anneau commutatif.

Exemple 3.2.1.1. *Soient $+$ et $\times$ l'addition et la multiplication usuelles des nombres alors :*

1. *$(\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire.*
2. *$(\mathbb{Q}, +, \times)$ est un anneau commutatif unitaire.*
3. *$(\mathbb{R}, +, \times)$ est un anneau commutatif unitaire.*
4. *$(\mathbb{C}, +, \times)$ est un anneau commutatif unitaire.*

Pour tous les anneaux précédents l'élément neutre pour l'addition est 0 et l'élément neutre pour la multiplication est 1.

Exemple 3.2.1.2. *On définit dans $\mathbb{Z}/3\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}\}$ les deux lois interne suivantes :*
La première loi est définie par le tableau suivant :

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

On déduit que l'élément neutre pour $\dot{+}$ *est* $\dot{0}$ *et le symétrie de* $\dot{1}$ *est* $\dot{2}$. *et la loi est commutative Et la deuxième loi est définie par le tableau suivant :*

$\dot{\times}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{1}$

On déduit que l'élément neutre pour $\dot{\times}$ *est* $\dot{1}$ *et la loi* $\dot{\times}$ *est commutative.*
Donc $(\mathbb{Z}/3\mathbb{Z}, \dot{+}, \dot{\times})$ *est un anneau commutatif et unitaire.*

Notation 3.2.1.1. *Dans la suite on va noter l'élément neutre pour la première loi par* 0, *l'élément neutre pour la deuxième loi par* 1.

Définition 3.2.1.2. *Soit* $(A, \star, \intercal)$ *un anneau commutatif. On dit que* $a, b \in A$ ***sont diviseurs de*** 0 *si*

$$a \neq 0 \text{ et } b \neq 0 \text{ mais } a \intercal b = 0.$$

Définition 3.2.1.3. *L' anneau* $(A, \star, \intercal)$ *est dit* ***intègre*** *si et seulement si*

$$a \intercal b = 0 \Longrightarrow a = 0 \vee b = 0$$

C'est à dire A *n'admet aucun diviseur de* 0.

Exemple 3.2.1.3. $(\mathbb{Z}/3\mathbb{Z}, \dot{+}, \dot{\times})$ *est un anneau intègre.*

Définition 3.2.1.4. *Soit* $(A, \star, \intercal)$ *un anneau, et soit* B *une partie non vide de* A. B *est dite* ***sous anneau*** *de* A *si :*

1. $(B, \star)$ *est un sous groupe de* $(A, \star)$.
2. *Pour tout* $x, y \in B$ *:* $x \intercal y \in B$.

Exemple 3.2.1.4. $(2\mathbb{Z}, +, \times)$ *est un sous anneau de* $(\mathbb{Z}, +, \times)$.

Remarque 3.2.1.2.
1. *Si* $(A, \star, \intercal)$ *est un anneau commutatif et* B *est un sous anneau alors* $(B, \star, \intercal)$ *est commutatif.*
2. *Si* $(A, \star, \intercal)$ *anneau unitaire alors pas forcement que* $(B, \star, \intercal)$ *soit un sous anneau unitaire (voir l'exemple précédent).*

Définition 3.2.1.5. *Soient $(A, \star, \intercal)$ un anneau,et I est une partie non vide de A. AlorsI dite* ***idéal àgauche*** *de A si*

$$\boxed{\forall x \in I \ \forall a \in A : x \intercal a \in I.}$$

Définition 3.2.1.6. *Soient $(A, \star, \intercal)$ un anneau, et I est une partie non vide de A dite* ***idéal à droite*** *de A si*

$$\boxed{\forall x \in I \ \forall a \in A : a \intercal x \in I.}$$

Définition 3.2.1.7. *Soient $(A, \star, \intercal)$ un anneau, et I est une partie non vide de A dite* ***idéal*** *de A s'il est idéal à gauche et à droite en même temps.*

Remarque 3.2.1.3.
1. *Si $(A, \star, \intercal)$ est un anneau commutatif les trois définitions précédentes sont coincides.*
2. *Tout idéal est un sous anneau.*

Exemple 3.2.1.5.
1. *$(2\mathbb{Z}, +, \times)$ est un idéal de $(\mathbb{Z}, +, \times)$.*
2. *$(3\mathbb{Z}, +, \times)$ est un idéal de $(\mathbb{Z}, +, \times)$.*

Définition 3.2.1.8. *Soient $(A, \star, \intercal)$, $(B, *, \perp)$, deux anneaux et $f : A \to B$ l' application de A dans B est dite* ***morphisme d'anneau*** *si*

1. $\forall x, y \in A : f(x \star y) = f(x) * f(y)$
2. $\forall x, y \in A : f(x \intercal y) = f(x) \perp f(y)$.

Exemple 3.2.1.6. *L'application*

$$\begin{aligned} f : (\mathbb{Z}, +, \times) &\to (\mathbb{Z}/3\mathbb{Z}, \dot{+}, \dot{\times}) \\ x &\mapsto \dot{x} \end{aligned}$$

est un morphisme d'anneau.

3.2.2 Corps

Définition 3.2.2.1. *Soit $\mathbb{K}$ un ensemble non vide muni de deux lois de composition internes $\star$ et $\intercal$. On dit que $(\mathbb{K}, \star, \intercal)$ est un* ***corps*** *si*

1. *$(\mathbb{K}, \star, \intercal)$ est un anneau unitaire,et*
2. $\forall x \in \mathbb{K} \ (x \neq 0) \ \exists x^{-1} \in \mathbb{K} \quad x \intercal x^{-1} = x^{-1} \intercal x = 1$

Remarque 3.2.2.1. *Si en plus $\intercal$ commutative on dit que $(\mathbb{K}, \star, \intercal)$ est un corps commutatif.*

Exemple 3.2.2.1. *Soient $+$ et $\times$ l'addition et la multiplication usuelles des nombres alors :*

1. $(\mathbb{Q}, +, \times)$ *est un corps commutatif.*
2. $(\mathbb{R}, +, \times)$ *est un corps commutatif.*
3. $(\mathbb{C}, +, \times)$ *est un anneau commutatif.*

Mais $(\mathbb{Z}, +, \times)$ n'est pas un corps puisque si $x \in \mathbb{Z}$ avec $x \neq 1$ et $x \neq -1$ alors $\frac{1}{x} \notin \mathbb{Z}$.

Proposition 3.2.2.1. $(\mathbb{K}, \star, \intercal)$ *est un corps si seulement si*

1. $(\mathbb{K}, \star)$ *est un groupe abélien.*
2. $(\mathbb{K}^*, \intercal)$ *est un groupe.*
3. *La deuxième loi $\intercal$ est distributive sur $\star$*

où $\mathbb{K}^* = \mathbb{K} - \{0\}$.

Preuve . Exercice ∎

Définition 3.2.2.2. *Soit $(\mathbb{K}, \star, \intercal)$ un corps et soit $\mathbb{L}$ un sous ensembles non vide de $\mathbb{K}$. On dit que $\mathbb{L}$ est un* ***sous corps de*** *$\mathbb{K}$ si et seulement si*

1. $(\mathbb{L}, \star)$ *est un sous groupe de* $(\mathbb{K}, \star)$.
2. $(\mathbb{L}^*, \intercal)$ *est un sous groupe de* $(\mathbb{K}^*, \intercal)$.

Exemple 3.2.2.2. *Soient $+$ et $\times$ l'addition et la multiplication usuelles des nombres alors :*

1. $(\mathbb{Q}, +, \times)$ *est sous un corps de* $(\mathbb{R}, +, \times)$.
2. $(\mathbb{R}_+, +, \times)$ *est sous un corps de* $(\mathbb{R}, +, \times)$

Définition 3.2.2.3. *Soient $(\mathbb{K}, \star, \intercal)$, $(\mathbb{L}, *, \perp)$ deux anneaux et $f : \mathbb{K} \to \mathbb{L}$ une application de $\mathbb{L}$ dans $\mathbb{L}$ est dite* ***morphisme de corps*** *si*

1. $\forall x, y \in \mathbb{K} : f(x \star y) = f(x) * f(y)$
2. $\forall x, y \in \mathbb{K} : f(x \intercal y) = f(x) \perp f(y)$.

Proposition 3.2.2.2. *Soit $f : \mathbb{K} \to \mathbb{L}$ application de le corps $(\mathbb{K}, \star, \intercal)$ vers le corps $(\mathbb{L}, *, \perp)$. Si f morphisme de corps alors Imf est un sous corps de $\mathbb{L}$*

Preuve .A) D'abord on va montrer que $(Imf, *)$ est un sous groupe de $(\mathbb{L}, *)$
En effet :

1) On a $0_{\mathbb{L}} = f(0_{\mathbb{K}})$ donc $Imf \neq \phi$
2) Soit y_1 et y_2 deux éléments de Imf donc il existe x_1, x_2 de $\mathbb{K}$ tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$.
Puisque $y_1 * y_2 = f(x_1) * f(x_2) = f(x_1 \star x_2)$ donc $(y_1 * y_2) \in Imf$

B) En suite on note $Imf^* = Imf - \{0_{\mathbb{L}}\}$ on montre que $(Imf^*, \perp)$ est un sous groupe de $(\mathbb{L}^*, \perp)$.
En effet :

1) On a $1_{\mathbb{L}} = f(1_{\mathbb{K}})$ donc Imf^* non vide
2) Soit y_1 et y_2 deux éléments de Imf^* donc il existe $x_1, x_2 \in \mathbb{K}$ tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$.
Puisque $y_1 \perp y_2 = f(x_1) \perp f(x_2) = f(x_1 \intercal x_2)$ alors $(y_1 * y_2) \in Imf^*$
■

Proposition 3.2.2.3. *Soit $f : \mathbb{K} \to \mathbb{L}$ morphisme de corps de le corps $(\mathbb{K}, \star, \intercal)$ vers le corps $(\mathbb{L}, *, \perp)$ alors*
f est injective si seulement si $\forall x \in \mathbb{K} \quad (f(x) = 0_{\mathbb{L}} \Rightarrow x = 0_{\mathbb{K}})$.

3.3 Exercices

Exercice 1 : Montrer que $(3\mathbb{Z}, +)$ est un groupe.

Exercice 2 : On dit qu'un élément x d'un ensemble muni d'une loi de composition interne $(G, *)$ est **régulier** si

$$\forall y, z \in G \ : \ ((x * y = x * z \Rightarrow y = z) \ et \ (y * x = z * x \Rightarrow y = z)).$$

Montrer que tout élément dans un groupe est régulier.

Exercice 3 : Soit $(G, *)$ un groupe e son élément neutre
tel que $\forall x \in G \ x * x = e$.
Montrer que $(G, *)$ est commutatif.

Exercice 4 : Soient $(G, *)$ un groupe, et soientH_1 et H_2 deux sous groupes de G.

1. Montrer que $H_1 \cap H_2$ est un sous groupe de $(G, *)$.
2. $H_1 \cup H_2$ est il un sous groupe de $(G, *)$.
3. Montrer que l'ensemble $H * H = \{x * y \,/\, x \in H_1 \ , y \in H_2\}$ est un sous groupe de $(G, *)$ si $*$ est commutative.

Exercice 5 : Montrer $(5\mathbb{Z}, +)$ est un sous groupe de $(\mathbb{Z}, +)$.

Exercice 6 : Preuve de la proposition (3.1.2.1).

Exercice 7 : Preuve de la proposition (3.1.3.1).

Exercice 8 : Preuve de la proposition (3.1.3.2).

Exercice 9 : Preuve de la proposition (3.1.3.4).

Exercice 10 : Preuve de la proposition (3.1.3.5).

Exercice 11 : Preuve de la proposition (3.1.3.6).

Exercice 12 : On définit dans $\mathbb{Z}/5\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}\}$ les deux lois interne suivantes :
La première loi $\dot{+}$ est définie par le tableau suivant :

$\dot{+}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{4}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$

La deuxième loi $\dot{\times}$ est définie par le tableau suivant :

$\dot{\times}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{1}$	$\dot{3}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{2}$	$\dot{4}$	$\dot{2}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

On accepte que $(\mathbb{Z}/5\mathbb{Z}, \dot{+}, \dot{\times})$ est un anneau.

1. Déterminer l'élément neutre de $\dot{+}$.
2. Déterminer les symétries de $\dot{1} et\ \dot{2}$ par rapport $\dot{+}$.
3. Montrer que $(\mathbb{Z}/5\mathbb{Z}, \dot{+}, \dot{\times})$ est unitaire et commutatif.
4. Déterminer l'élément neutre de l'anneau par rapport à $\dot{\times}$.
5. Déterminer les symétries de $\dot{2}$ et $\dot{4}$ par rapport à $\dot{\times}$.
6. Montrer que $(\mathbb{Z}/5\mathbb{Z}, \dot{+}, \dot{\times})$ est intègre.

Exercice 13 : Soit l'application

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z}/5\mathbb{Z} \\ x &\mapsto \dot{x} \end{aligned}$$

1. Montrer que f est un morphisme d'anneau de $(\mathbb{Z}, +, \times)$ dans $(\mathbb{Z}/5\mathbb{Z}, \dot{+}, \dot{\times})$.
2. Déterminer le noyau et l'image de f.
3. f est elle injective ? surjective ?

Exercice 14 : Soit $(A, *, \bullet)$ un anneau tel que $\forall x \in A \quad x \bullet x = x$

1. Montrer que $\forall x \in A\ x * x = 0_A$.
2. Montrer que $(A, *, \bullet)$ est un anneau commutatif.

Exercice 15 : Preuve de la proposition (3.2.2.1).

Exercice 16 : Montrer que tout corps est un anneau intègre.
la réciproque est elle vraie ?

Exercice 17 : Si $f : A \to B$ est un morphisme d'anneau de $(A, *, \circ)$ vers $(B, \star, \bullet)$ alors Montrer que
$\ker f$ est un idéal dans A.
Et Imf est un sous anneau de B.

4

Anneau des polynômes

4.1 Anneau des polynômes

4.1.1 Construction

Soit $(E, +, \times)$ un anneau commutatif et unitaire .
Soit $\mathfrak{C}$ l'ensemble des suites $(x_n)_{n\in\mathbb{N}}$ dans E tel que $(\exists n_0 \in \mathbb{N}\ \forall n \geq n_0 \ \ x_n = 0)$,
c'est à dire $\mathfrak{C} = \{(x_n)_n \subseteq E\ /\exists n_0 \in \mathbb{N}\ \forall n \geq n_0 \ \ x_n = 0\}$.
On définit dans $\mathfrak{C}$ deux lois de composition $\oplus$ et $\otimes$ tels que

$$(x_n)_n \oplus (y_n)_n = (z_n)_n$$

et

$$(x_n)_n \otimes (y_n)_n = (w_n)_n$$

où $z_n = x_n + y_n$ et $w_n = \sum_{k=0}^{n} x_k y_{n-k}$.

Alors $(\mathfrak{C}, \oplus, \otimes)$ est un anneau commutatif et unitaire.
On a

1. L'élément neutre de $\mathfrak{C}$ par rapport à $\oplus$ est $(e_n)_n$ (tel que pour tout $n \in \mathbb{N}$ $e_n = 0$).
2. L'élément neutre de $\mathfrak{C}$ par rapport à $\otimes$ est $(f_n)_n$ (tel que $f_0 = 1$ et pour tout $n \geqslant 1$ $f_n = 0$).
3. $(-x_n)_n$ est le symétrie de $(x_n)_n$ par rapport à $\oplus$.

4.1.2 Définitions et notation

On écrit la suite $(x_n)_n = (x_0, x_1, \cdots, x_n, \cdots)$.
On note X d'élément $(0, 1, 0, 0, \cdots, 0, \cdots)$.
Et I l'élément $(1, 0, 0, 0, \cdots, 0, \cdots)$.
Alors on a
$X^2 = X \otimes X = (0, 0, 1, 0, \cdots, 0, \cdots)$
$X^3 = X^2 \otimes X = (0, 0, 1, 0, \cdots, 0, \cdots)$
$\vdots$

$X^n = X^{n-1} \otimes X = (0,0,0,0,\cdots,1,0,\cdots)$ tel que 1 dans $(n+1)$ position.
Et $(0,0,0,\cdots,a,0,\cdots) = (a,0,0,\cdots,0,\cdots) \otimes (0,0,0,\cdots,1,0,\cdots) = aX^n$.
D'après ces notations on écrit tout élément $(a_0, a_1, \cdots a_n, 0, 0\cdots)$ de la forme
$a_0 + a_1X^1 + \cdots + a_nX^n$.
On note de l'ensemble $\mathfrak{C}$ par $E[X]$

Définition 4.1.2.1. *On appelle $(E[X], \oplus, \otimes)$ l'anneau des polynômes à un seul variable.*

Notation 4.1.2.1. *On note un élément de $(E[X], \oplus, \otimes)$ par*
$P(X), Q(X), ...$

Définition 4.1.2.2. *Le variable X est appelé **indéterminé** et les $a_k \in E$ sont appelés **coefficients** de $P(X)$.*

Soient $P(X) = a_0 + a_1X^1 + \cdots + a_nX^n$
et $Q(X) = b_0 + b_1X^1 + \cdots + b_mX^m$ avec $m \leqslant n$.
Alors on a
$P(X) \oplus Q(X) = a_0 + b_0 + (a_1 + b_1)X + \cdots + (a_m + b_m)X^m + a_{m+1}X^{m+1} + \cdots + a_nX^n$.
$P(X) \otimes Q(X) = c_0 + c_1X^1 + \cdots + c_{n+m}X^{n+m}$ où $c_i = \sum_{k=0}^{i} a_k b_{i-k}$.

Définition 4.1.2.3. *Soit $P(X) = a_0 + a_1X^1 + \cdots + a_nX^n$ un polynôme tel que $a_n \neq 0$ alors le nombre naturel n est appelé le **degré** du polynôme $P(X)$ on la note $d^oP = n$.*

Propriétés 4.1.2.1. *Soient P et Q deux polynômes alors*

$$d^o(P \otimes Q) \leq d^oP + d^oQ$$

$$d^o(P \oplus Q) \leq max(d^oP, d^oQ).$$

Remarque 4.1.2.1. *Si E est un anneau unitaire alors*

$$d^o(P \otimes Q) = d^oP + d^oQ$$

Définition 4.1.2.4. • *Les polynômes comportant un seul terme non nul (du type a_nX^n) sont appelés **monômes**.*
• *Soit $P(X) = a_0 + a_1X^1 + \cdots + a_nX^n$ un polynôme avec $a_n \neq 0$. On appelle le **terme dominant***
le monôme a_nX^n.
• *Le coefficient a_n est appelé le coefficient dominant de $P(X)$.*
• *Si le coefficient dominant est 1, on dit que $P(X)$ est **un polynôme unitaire**.*

4.1.3 Division euclidienne et dérivation

Soit $(E, +, \times)$ un corps commutatif.

Définition 4.1.3.1. *Soient $A(X)$ et $B(X)$ deux polynômes de $E[X]$,*
*on dit que $B(X)$ **divise** $A(X)$ s'il existe $Q(X) \in E[X]$ tel que $A(X) = B(X)Q(X)$,*
on note alors $B(X)|A(X)$.
*On dit aussi que $A(X)$ est **multiple** de $B(X)$ ou que $A(X)$ est divisible par $B(X)$.*
Outre les propriétés évidentes comme $A(X)|A(X)$, $1|A(X)$ et $A(X)|0$ nous avons :

Exemple 4.1.3.1. *On prend l'anneau* $(\mathbb{R}, +, \times)$ *donc* $E[X] = \mathbb{R}[X]$.
Soient $P(X) = 1 + X + X^2 + X^3$ *et* $Q(X) = 1 + X^2$;
On a $P(X) = Q(X)(1 + X)$ *donc* $Q(X)$ *devise* $P(X)$.

Propriété 4.1.3.1. *Soient* $P(X), Q(X)$ *et* $R(X)$ *trois polynômes de* $E[X]$.
On a

1. *Si* $Q(X)|P(X)$ *et* $P(X)|Q(X)$ *alors il existe* $\lambda \in E^*$ *tel que* $P(X) = \lambda Q(X)$.
2. *Si* $Q(X)|P(X)$ *et* $R(X)|Q(X)$ *alors* $R(X)|P(X)$
3. *Si* $R(X)|Q(X)$ *et* $R(X)|P(X)$ *alors* $R(X)|(U(X)P(X) + V(X)Q(X))$ *avec* $U(X)$ $V(X) \in E[X]$.

Preuve . Exercice ∎

Théorème 4.1.3.1. ***Division euclidienne des polynômes***
Soient $A(X), B(X) \in E[X]$ *alors il existe un unique polynôme* $Q(X)$ *et il existe un unique polynôme* $R(X)$ *tels que*

$$\boxed{A(X) = B(X)Q(X) + R(X) \text{ et } d^oR(X) < d^0B(X).}$$

Le polynôme $Q(X)$ *est appelé le quotient et* $R(X)$ *le reste et cet écriture est appelé* ***la division euclidienne*** *de* $A(X)$ *par* $B(X)$.
Notez que la condition $d^oR(X) < d^0B(X)$ *signifie* $R(X) = 0$ *ou bien* $0 \leqslant d^oR(X) < d^0B(X)$.
Enfin $R(X) = 0)$ *si et seulement si* $B(X)|A(X)$.

Exemple 4.1.3.2. *Soient* $A(X) = 3 + 2X + X^2 + X^3$ *et* $B(X) = 1 + X^2$; *alors la division euclidienne de* $A(X)$ *par* $B(X)$ *est*

$$A(X) = B(X)(1 + X) + (2 + X).$$

le quotient de la division est $Q(X) = 1 + X$ *et le reste de la division est est* $R(X) = 2 + X$.

Définition 4.1.3.2. *Soit* $P(X) \in E[X]$ *tel que*

$$P(X) = a_0 + a_1X^1 + \cdots + a_nX^n$$

alors le polynôme

$$P'(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1}$$

est appelle ***polynôme dérive*** *de* $P(X)$.

Exemple 4.1.3.3. *Si* $P(X) = 1 + 5X + 3X^2 - 2X^3$ *alors* $P'(X) = 5 + 6X - 6X^2$

Propriétés 4.1.3.1.

$$(P(X) + Q(X))' = P'(X) + Q'(X)$$
$$(P(X) \times Q(X))' = P'(X) \times Q(X) + P(X) \times Q'(X).$$

Définition 4.1.3.3. *On associe à tout polynôme $P(X)$* ***fonction polynomiale***

$$\begin{array}{c} f : E \to E \\ x \mapsto f(x) \end{array}$$

Si $P(X) = a_0 + a_1X^1 + \cdots + a_nX^n$ alors $f(x) = a_0 + a_1x^1 + \cdots + a_nx^n$
on note $P(x)$ au lieu $f(x)$.

Définition 4.1.3.4. *Soit $P(X) \in E[X]$ on dit $x_0 \in E$* ***racine*** *de polynôme $P(X)$ si seulement si la fonction polynomiale $P(x)$ s'annule en x_0 c'est à dire $(P(x_0) = 0_E)$*

Exemple 4.1.3.4. *$x_0 = 1$ est une racine de $P(x) = x^2 - 2x + 1$ car $P(1) = 0$*

Proposition 4.1.3.1. *Soit $P(X) \in E[X]$ et $x_0 \in E$. On a*

$$\boxed{P(x_0) = 0 \Leftrightarrow (X - x_0) \text{ divise } P(X).}$$

Preuve . Exercice ∎

Définition 4.1.3.5. *Soit x_0 une racine de $P(X)$ et $n \in \mathbb{N}$ non nul, tel que $P(X)$ est divisible par $(X - x_0)^n$ et non divisible par $(X - x_0)^{n+1}$*
le nombre n s'appelle ***ordre de la racine*** *x_0; On dit que x_0 est une* ***racine d'ordre*** *n.*

Exemple 4.1.3.5.
1. *$P(X) = X^2 - 1 = (X - 1)(X + 1)$ alors $x_0 = 1$ est une racine simple.*
2. *$P(X) = X^3 - 2X^2 + X = X(X - 1)^2$ alors $x_0 = 1$ est une racine double, et $x_1 = 0$ est une racine simple.*

Notation 4.1.3.1. *Soit $P(X) = a_0 + a_1X^1 + \cdots + a_nX^n$ un polynôme de degré n $(a_n \neq 0)$*
On pose
$P^{(0)}(X) = P(X)$
$P^{(1)}(X) = P'(X)$
$P^{(2)}(X) = [P^{(1)}(X)]'$
$\vdots$
$P^{(n)}(X) = [P^{(n-1)}(X)]'$.

On a : $P^{(n)}(X) = n!a_n$, si $m > n$ alors $P^{(m)}(X) = 0$.

4.2 Anneaux $\mathbb{R}[X]$

4.2.1 Anneaux $\mathbb{R}[X]$

$\mathbb{R}[X]$ anneau des polynômes réels

Théorème 4.2.1.1. *Soit $P(X) \in \mathbb{R}[X]$ et $\alpha \in \mathbb{R}$.*
α est une racine de $P(X)$ d'ordre n si seulement si

1. $\forall k \in \{0, 1, 2, \cdots, n-1\}$, $P^{(k)}(\alpha) = 0$,
2. $P^{(n)}(\alpha) \neq 0$.

Définition 4.2.1.1. *Soit $P(X) \in \mathbb{R}[X]$ un polynôme réel de degré superieur à 1. On dit que $P(X)$ est **irréductible** si pour tout polynôme réel non nul $Q(X)$ divisant $P(X)$, il existe un réel non nulλ tel que $P(X) = \lambda Q(X)$.*

Exemple 4.2.1.1. *Les deux polynômes*

1. *$P(X) = X + a$ avec $a \in \mathbb{R}$*
2. *$R(X) = aX^2 + bX + c$ avec $\Delta = b^2 - 4ac < 0$.*
   sont irreductibles

Remarque 4.2.1.1.

1. *Un polynôme irréductible $P(X)$ est donc un polynôme non constant dont les seuls diviseurs de $P(X)$ sont les constantes ou $P(X)$ lui-même (à une constante multiplicative près).*

2. *La notion de polynôme irréductible pour l'arithmétique de $\mathbb{R}[X]$ correspond à la notion de nombre premier pour l'arithmétique de $\mathbb{Z}$.*

3. *Dans le cas contraire, on dit que $P(X)$ est réductible ; Il existe alors des polynômes $A(X)$, $B(X)$ de $\mathbb{R}[X]$ tels que $P(X) = A(X)B(X)$, avec $d^oA(X) > 1$ et $d^oB(X) > 1$.*

Exemple 4.2.1.2.

1. *Tous les polynômes de degré 1 sont irréductibles. Par conséquent il y a une infinité des polynômes irréductibles.*

2. *$X^2 - 1 = (X - 1)(X + 1)$ dans $\mathbb{R}[X]$ est réductible.*

3. *$X^2 + 1 = (X - i)(X + i)$ est réductible dans $\mathbb{C}[X]$ mais il est irréductible dans $\mathbb{R}[X]$.*

4. *$X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ est réductible dans $\mathbb{R}[X]$ mais il est irréductible dans $\mathbb{Q}[X]$.*

On a lemme d'Euclide dans les polynômes que même dans $\mathbb{Z}$:

Proposition 4.2.1.1. ***(Lemme d'Euclide)***
Soit $P(X) \in \mathbb{R}[X]$ un polynôme irréductible et soient $A(X), B(X) \in \mathbb{R}[X]$, Si $P(X)|A(X)B(X)$ alors $P(X)|A(X)$ ou $P(X)|B(X)$.

Théorème 4.2.1.2. *Tout $P(X) \in \mathbb{R}[X]$ s'écrit sous forme*

$$P(X) = b(X - x_1)^{k_1}(X - x_2)^{k_2} \dots (X - x_i)^{k_i}(X^2 + d_1X + e_1)^{k_1} \dots (X^2 + d_jX + e_j)^{k_j}.$$

Tels que :
$b, x_1 \dots x_i, d_1 \dots d_j, e_1 \dots e_j \in \mathbb{R}$
$k_1 \dots k_i, h_1 \dots h_j \in \mathbb{N}$
$d^oP(X) = k_1 + k_2 + \dots + k_i + 2(h_1 + k_2 + \dots + h_j)$,
les polynômes $X - x_1$ et $X^2 + d_jX + e_j$ sont irréductibles.

Exemple 4.2.1.3. *Soit* $A(X) = X^4 + 2X^3 - 2X - 1$.
On remarque que $x = 1$, $x = -1$ *sont des racines de* $A(X)$ *alors*

$$A(X) = (X-1)(X+1)(aX^2 + bX + d)$$

En utilisant la division on trouve $B(X) = (aX^2 + bX + d) = X^2 + 2X + 1 = (X+1)^2$
alors $A(X) = (X-1)(X+1)(X+1)^2 = (X-1)(X+1)^3$.
On déduit $x = 1$ *est une racine simple et* $x = -1$ *est une racine d'ordre* 3.

Proposition 4.2.1.2. *Soient* $A(X), B(X) \in \mathbb{R}[X]$, *avec* $A(X) \neq 0$ *ou* $B(X) \neq 0$.
Il existe un unique polynôme unitaire de plus grand degré qui divise à la fois $A(X)$ *et* $B(X)$.
Cet unique polynôme est appelé ***le plus grand commun diviseur*** *de* $A(X)$ *et* $B(X)$ *que l'on note* $pgcd(A(X), B(X))$.

Remarque 4.2.1.2. *Soient* $A(X), B(X) \in \mathbb{R}[X]$.

1. $pgcd(A(X), B(X))$ *est un polynôme unitaire.*

2. *Si* A *diviseur de* $|B$ *avec* $A \neq 0$, *alors* $pgcd(A(X), B(X)) = \dfrac{1}{\lambda}A(X)$, *où* λ *est le coefficient dominant de* $A(X)$.

3. *Pour tout* $\lambda \in \mathbb{R}^*$ $pgcd(\lambda A(X), B(X)) = pgcd(A(X), B(X))$.

4. *Comme pour les entiers : si la devision euclidienne* $A = BQ + R$ *alors* $pgcd(A, B) = pgcd(B, R)$. *C'est ce qui justifie l'algorithme d'Euclide.*

Exemple 4.2.1.4. *Calculons le* $pgcd(A(X), B(X))$ *avec* $A(X) = X^4 - 1$ *et* $B(X) = X^3 - 1$.
On applique l'algorithme d'Euclide :

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

$$(X^3 - 1) = (X-1)(X^2 + X + 1) + 0.$$

Alors $pgcd(A(X), B(X)) = X - 1$.

Exemple 4.2.1.5. *Calculons le* $pgcd(A(X), B(X))$ *avec* $A(X) = X^5 + 2X^4 + X^3 + X^2 + X + 2$ *et* $B(X) = X^4 + 2X^3 + X^2 - 4$

$$X^5 + 2X^4 + X^3 + X^2 + X + 2 = (X^4 + 2X^3 + X^2 - 4)(X - 1) + 3X^3 + 2X^2 + 5X - 2$$

$$(X^4 + 2X^3 + X^2 - 4) = (3X^3 + 2X^2 + 5X - 2)\frac{1}{9}(3X + 4) + \frac{14}{9}(X^2 + X + 2)$$

$$(3X^3 + 2X^2 + 5X - 2) = (X^2 + X + 2)(3X - 1) + 0$$

Ainsi $pgcd(A(X), B(X)) = X^2 + X + 2$.

4.2.2 Théorème de Bézout

Théorème 4.2.2.1. ***Théorème de Bézout***
Soient $A(X), B(X) \in \mathbb{R}[X]$ deux polynômes non nuls
On note $D(X) = pgcd(A(X), B(X))$.
Alors il existe deux polynômes $U(X), V(X) \in \mathbb{R}[X]$ tels que $A(X)U(X) + B(X)V(X) = D(X)$.

Exemple 4.2.2.1. *On a calculé $pgcd(X^4 - 1, X^3 - 1) = X - 1$.*
Nous remontons dans l'algorithme d'Euclide, ici il n'y avait qu'une ligne : $X^4 - 1 = (X^3 - 1)X + (X - 1)$, pour en déduire $(X^4 - 1) - (X^3 - 1)X = (X - 1)$. avec $U(X) = 1$ et $V(X) = -X$.

Définition 4.2.2.1. *Soient $A(X), B(X) \in \mathbb{R}[X]$.*
On dit que $A(X)$ et $B(X)$ sont ***premiers entre eux*** *si $pgcd(A(X), B(X)) = 1$.*
Pour $A(X), B(X)$ quelconques on peut se ramener à des polynômes premiers entre eux :
si $pgcd(A(X), B(X)) = D(X)$ alors $A(X)$ et $B(X)$ s'écrivent : $A(X) = D(X)A_0(X)$, $B(X) = D(X)B_0(X)$ avec $pgcd(A_0(X), B_0(X)) = 1$

Exemple 4.2.2.2. *$A(X) = X^2 + X + 1$ et $B(X) = X + 1$. En effet $X^2 + X + 1 = X(X + 1) + 1$ donc $1.A(X) - X.B(X) = 1$.*

Corollaire 4.2.2.1. *Soient $A(X), B(X)$ deux polynômes. $A(X)$ et $B(X)$ sont premiers entre eux si et seulement s'il existe deux polynômes $U(X)$ et $V(X)$ tels que*
$A(X)U(X) + B(X)V(X) = 1$.

Corollaire 4.2.2.2. *Soient $A(X), B(X) \in \mathbb{R}[X]$. avec $A(X) \neq 0$ ou $B(X) \neq 0$.*
Si $C(X)|A(X)$ et $C(X)|B(X)$ alors $C(X)|pgcd(A(X), B(X))$.

Corollaire 4.2.2.3. ***Lemme de Gauss***
Soient $A(X), B(X) \in \mathbb{R}[X]$ et $pgcd(A(X), B(X)) = 1$ donc si $A(X)|B(X)C(X)$ alors $A(X)|C(X)$.

Définition 4.2.2.2. *Soient $A(X), B(X) \in \mathbb{R}[X]$ des polynômes non nuls, alors*
il existe un unique polynôme unitaire $M(X)$ de plus petit degré tel que $A(X)|M(X)$ et $B(X)|M(X)$.
Cet unique polynôme est appelé ***le plus petit commun multiple*** *de $A(X)$ et $B(X)$*
qu'on note $ppcm(A(X), B(X))$.

Exemple 4.2.2.3. *Soient*

$$P(X) = X(X - 2)^2(X^2 + 1)^3$$

et

$$Q(X) = (X + 1)(X - 2)^3(X^2 + 1)^2$$

alors

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

Proposition 4.2.2.1. *Soient $A(X), B(X) \in \mathbb{R}[X]$ deux polynômes non nuls et $M(X) = ppcm(A(X), B(X))$.*
Si $C(X) \in \mathbb{R}[X]$ est un polynôme tel que $A(X)|C(X)$ et $B(X)|C(X)$, alors $M(X)|C(X)$.

Définition 4.2.2.3. ***Une fraction rationnelle*** *à coefficients dans* $\mathbb{R}$ *est une expression de la forme*

$$F(X) = \frac{P(X)}{Q(X)}$$

où $P(X), Q(X) \in \mathbb{R}[X]$ *et* $Q(X) \neq 0$.

Exemple 4.2.2.4. $F(X) = \dfrac{X+1}{X^2+X+1}$

Remarque 4.2.2.1. *Toute fraction rationnelle se décompose comme une somme de fractions rationnelles élémentaires que l'on appelle des « éléments simples ».*

4.2.3 Décomposition en éléments simples

Théorème 4.2.3.1. ***Décomposition en éléments simples sur*** $\mathbb{R}[X]$. *Soient* $P(X), Q(X)$ *deux polynômes non nuls si* $pgcd(P(X), Q(X)) = 1$, *alors la fraction rationnelle* $P(X)/Q(X)$ *s'écrit de manière unique comme somme :*

- *d'une partie polynomiale* $E(X)$,
- *d'éléments simples du type* $\dfrac{a}{(X-\alpha)^i}$,
- *d'éléments simples du type* $\dfrac{aX+b}{(X^2+\alpha X+\beta)^i}$.

Où les polynômes $X-\alpha$ *et* $\dfrac{aX+b}{(X^2+\alpha X+\beta)^i}$. *sont des facteurs irréductibles de* $Q(X)$, *et les exposants* i *sont inférieurs ou égaux à la puissance correspondante dans cette factorisation.*

Théorème 4.2.3.2. *Soit* $P(X)$*un polynômes non nul,* n *un entier positif et* α *réel alors tout fraction* $\dfrac{P(X)}{(X-\alpha)^n}$
s'écrit sous forme

$$\frac{P(X)}{(X-\alpha)^n} = Q(X) + \frac{b_1}{(X-\alpha)} + \frac{b_2}{(X-\alpha)^2} + \cdots + \frac{b_n}{(X-\alpha)^n}$$

tels que $b_1, b_2, ..., b_n \in \mathbb{R}$.

Exemple 4.2.3.1. $\dfrac{X^3}{(X-1)^2} = X + 2 + \dfrac{3}{X-1} + \dfrac{1}{(X-1)^2}$.

4.3 Exercices

Exercice 1 : Soient $P(X)$ et $Q(X)$ deux polynômes de $\mathbb{Z}_6[X]$.

1. Calculer $P(X)+Q(X)$ et $P(X)\times Q(X)$ dans les cas suivants
   (a) $P(X) = 2X + 3X^2 \qquad Q(X) = 1 + 2X^2$.
   (b) $P(X) = 2 + 5X^2 \qquad Q(X) = X + X^2$.
   (c) $P(X) = 3X \qquad Q(X) = 2X^2$.
2. $(\mathbb{Z}_6[X], +, \times)$ est il anneau intègre ?

Exercice 2 : Montrer dans $\mathbb{Z}_9[X]$ que $P(X) = 3X + 1$ est inversible.

Exercice 3 : Soit $P(X) = X^3 - 2X^2 + X - 2$.

1. Montrer que 2 est une racine simple de $P(X)$.

2. Écrire $P(X)$ sous formes produit des éléments irréductibles.

Exercice 4 : Décomposer $P(X) = \dfrac{X+1}{(X-1)^2(X+2)}$ sous formes des éléments simples.

Exercice 5 : Prouver les propriétés 4.1.3.

Exercice 6 : Prouver la proposition 4.1.3.

Exercice 7 : Soit $P(X)$ un polynôme réel
Montrer que si $P(X)$ admet une racine de multiplicité supérieure ou égale à deux alors $P(X)$ et $P'(X)$ ne sont pas premiers entre eux.

Exercice 8 : Soient $P(X) = (X^2 + X - 6)^2(X^4 - 1)^3$ et $Q(X) = 3(X^2 - 1)(X^2 - X + \frac{1}{4})$

1. $P(X) et\ Q(X)$ dans $\mathbb{R}[X]$.

2. En déduire leur pgcd et leur ppcm.

Exercice 9 : Chercher tous les polynômes $P(X)$ tels que $(P(X) + 1)$ soit divisible par $(X - 1)^4$ et $(P(X) - 1)$ soit divisible $(X + 1)^4$.

Exercice 10 : Existe-t-il une fraction rationnelle $F(X)$ telle que
$F^2(X) = (X^2 + 1)^3$.

5

Solution des exercices

5.1 Exercices du chapitre 1

Exercice 1 : On sait que $(P \Rightarrow Q) \Leftrightarrow (\overline{P} \vee Q)$
donc

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

Ou en utilisant la table de vérité

Exercice 2 : D'après l'exercice 1 on a $\overline{(P \Rightarrow Q)} \Leftrightarrow P \wedge \overline{Q}$ alors

1. $\overline{(P \wedge Q) \Rightarrow L} \Leftrightarrow (P \wedge Q) \wedge \overline{L}$
2. $\overline{(P \Rightarrow Q) \wedge L} \Leftrightarrow (P \wedge \overline{Q}) \vee \overline{L}$

Exercice 3 : D'abord

$$\begin{aligned}(\overline{P} \wedge Q) \vee (\overline{Q} \wedge \overline{P}) &\Leftrightarrow \overline{P} \wedge (Q \vee \overline{Q}) \\ &\Leftrightarrow \overline{P}\end{aligned}$$

alors

$$\begin{aligned}(\overline{P} \wedge Q) \vee (\overline{P} \wedge \overline{Q}) \vee (P \wedge Q) &\Leftrightarrow \overline{P} \vee (P \wedge Q) \\ &\Leftrightarrow (\overline{P} \vee P) \wedge (\overline{P} \vee Q) \\ &\Leftrightarrow \overline{P} \vee Q \\ &\Leftrightarrow (P \Rightarrow Q)\end{aligned}$$

Exercice 4 :

$$\exists x \in \mathbb{R}\ \forall y \in \mathbb{R}\ : x^2 + y^2 \geq 0$$

est une proposition vraie.
puisque

$$\exists x = 1 \in \mathbb{R}\ \ \forall y \in \mathbb{R} :\ \ x^2 + y^2 = 1 + y^2 \geqslant 0.$$

La négation de

$$\exists x \in \mathbb{R}\ \ \forall y \in \mathbb{R}\ \ : x^2 + y^2 \geq 0$$

est

$$\forall x \in \mathbb{R}\ \ \exists y \in \mathbb{R}\ \ : x^2 + y^2 < 0$$

Exercice 5 : L'implication $(x \leq 3) \Rightarrow (x^2 \leq 9)$ est fausse puisque $x = -4 \leqslant 3 \wedge x^2 = 16 > 9$

Exercice 6 : Pour montrer (n^2 est un nombre impair implique que n est un nombre impair)
.
En utilisant raisonnement par contra posée
On montre l'implication (n est un nombre pair implique que n^2 est un nombre pair).

En effet n est un nombre pair alors $n = 2k\ k \in \mathbb{Z}$ d'où $n^2 = 4k^2 = 2(2k^2)$ donc n^2 est pair.
Alors $(n^2\, nombre\ impaire) \Rightarrow (n\, nombre\ impair)$

Exercice 7 : On montre que pour tout a et b deux nombres réels positifs si $\dfrac{a}{b+1} = \dfrac{b}{a+1}$ alors $a = b$
En effet,on raisonne par l'absurde en supposant que $\dfrac{a}{b+1} = \dfrac{b}{a+1}$ et $a \neq b$.
Comme $\dfrac{a}{b+1} = \dfrac{b}{a+1}$ alors $a(1+a) = b(1+b)$ donc $a^2 + a = b^2 + b$ d'où $a^2 - b^2 = b - a$
Cela conduit à $(a-b)(a+b) = -(a-b)$.
Comme $a \neq b$ alors $a - b \neq 0$ et donc en divisant par $a - b$ on obtient $a + b = -1$
contraduction car la somme des deux nombres positifs a et b ne peut être négative.
Conclusion :$a, b \in \mathbb{R}^+$: si $\dfrac{a}{b+1} = \dfrac{b}{a+1}$ alors $a = b$.

Exercice 8 : En utilisant raisonnement par récurrence pour montrer que $2^n \geq n\ \forall n \in \mathbb{N}$.

On suppose $P(n) : 2^n \geq n$ avec $n \in \mathbb{N}$.
1) Pour $n = 0$ on a $2^0 = 1 \geq 0$ alors $P(0)$ est vraie.
2) On suppose que $P(k)$ est vraie, on montre que $P(k+1)$ est vraie.
Donc on a $2^k \geq k$ par suite $2^{k+1} = 2 \times 2^k \geq 2k \geq k + 1$.
Alors on conclue pour tout $n \in \mathbb{N}\ 2^n \geq n$.

Exercice 9 : Soient $a, b \in \mathbb{R}_+$ on va montrer que si $a \leq b$ alors $a \leq \dfrac{a+b}{2} \leq b$

En utilisant raisonnement directe
On

$$\begin{aligned} a \leq b &\Rightarrow a + a \leq a + b \\ &\Rightarrow \frac{2a}{2} \leq \frac{a+b}{2} \\ &\Rightarrow a \leq \frac{a+b}{2} \end{aligned}$$

et

$$\begin{aligned} a \leq b &\Rightarrow a + b \leq b + b \\ &\Rightarrow \frac{a+b}{2} \leq \frac{2b}{2} \\ &\Rightarrow \frac{a+b}{2} \leq b \end{aligned}$$

Alors
$\forall a, b \in \mathbb{R}_+$, si $a \leq b$ alors $a \leq \dfrac{a+b}{2} \leq b$

Exercice 10 : Soit $n \in \mathbb{N}^*$. Pour montrer que $\sqrt{n^2+1}$ n'est pas un entier.

En utilisant raisonnement par l'absurde
On suppose que $\sqrt{n^2+1}$ est un entier donc $\exists m \in \mathbb{N}^*$ tel que $\sqrt{n^2+1} = m$
alors

$$\begin{aligned} n^2 + 1 = m^2 \Rightarrow m^2 - n^2 &= 1 \\ \Rightarrow (m-n)(m+n) &= 1 \\ \Rightarrow (m+n) = 1 \wedge (m-n) &= 1 \\ \Rightarrow m = 1 \wedge n &= 0 \end{aligned}$$

mais $n \in \mathbb{N}^*$ alors contradiction.
donc $\sqrt{n^2+1}$ n'est pas un entier.

5.2 Exercices du chapitre 2

Exercice 1 : Soit $E = \{1, 2, 3, 5\}$ donc

$\mathcal{P}(E) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{5\}, \{1,2\}, \{1,3\}, \{1,5\}\{2,3\}, \{2,5\}, \{3,5\}, \{1,2,3\}, \{1,2,5\}, \{1,3,5\}, \{2,3,5\}, E\}$.

Exercice 2 : $\mathbb{R} \cup \mathbb{R}_+ = \mathbb{R}$
$\mathbb{R}_- \cup \mathbb{R}_+ = \mathbb{R}$
$\mathbb{R} \cup \mathbb{Z} = \mathbb{R}$
$\mathbb{N} \cup \mathbb{Q} = \mathbb{Q}$.

Exercice 3 : Soient $E = \{0, 1, 2, 3, 4, 5, 6, 7, 9\}$, $A = \{1, 2, 3, 4\}$ et $B = \{1, 2, 5, 6\}$ alors
$A \cap B = \{1, 2\}$
$A \cup B = \{1, 2, 3, 4, 5, 6\}$
$A^c = \{0, 5, 6, 7, 9\}$
$(A \cap B)^c = \{0, 3, 4, 5, 6, 7, 9\}$
$(A \cup B)^c = \{0, 7, 9\}$
$A \Delta B = \{3, 4, 5, 6\}$.

Exercice 4 : Pour montrer que $\mathcal{A} = \{[n, n+1[/\ n \in \mathbb{N}\}$ est une partition de $\mathbb{N}$
On pose $A_n = [n, n+1[$ alors :
1)Pour tout $m \neq n$ on a $A_n \cap A_m = [n, n+1[\cap[m, m+1[= \varnothing$.
2)On a $\mathbb{N} = \cup_{n\in\mathbb{N}}\{n\} \subset \cup_{n\in\mathbb{N}} A_n$ donc $\mathbb{N} = \cup_{n\in\mathbb{N}} A_n$.
Alors $\mathcal{A} = \{[n, n+1[/\ n \in \mathbb{N}\}$ est une partition de $\mathbb{N}$.

Exercice 5 : On a

$$\begin{aligned} f : \mathbb{R}_+ &\to \mathbb{R} \\ x &\mapsto 3x + 1 \end{aligned}$$

et

$$\begin{aligned} g : \mathbb{R} &\to \mathbb{R}_+ \\ x &\mapsto x \end{aligned}$$

alors $f \circ g(x) = f(g(x)) = f(x) = 3x + 1$
$g \circ f = g(f(x)) = g(3x + 1) = 3x + 1$
$f \circ g \neq g \circ f$ puisque $g \circ f : \mathbb{R}_+ \to \mathbb{R}_+$ mais $f \circ g : \mathbb{R} \to \mathbb{R}$

Exercice 6 : Soient $f : E \to F$ une application de E dans F et A, B deux parties non vides de E :
1) Soit $y \in f(A \cap B) \Rightarrow \exists x \in (A \cap B)$ telque $f(x) = y$
donc

$$\begin{aligned} x \in (A \cap B) &\Rightarrow (x \in A) \wedge (x \in B) \\ &\Rightarrow (f(x) \in f(A)) \wedge (f(x) \in f(B)) \\ &\Rightarrow y = f(x) \in f(A) \cap f(B) \end{aligned}$$

alors $f(A \cap B) \subseteq f(A) \cap f(B)$.

2) Pour montrer que $f(A \cup B) = f(A) \cup f(B)$
d'une part on prouve que $f(A \cup B) \subset f(A) \cup f(B)$.

Soit $y \in f(A \cup B) \Rightarrow \exists x \in (A \cup B)$ telque $f(x) = y$ donc

$$\begin{aligned} x \in (A \cup B) &\Rightarrow x \in A \vee x \in B \\ &\Rightarrow f(x) \in f(A) \vee f(x) \in f(B) \\ &\Rightarrow y = f(x) \in f(A) \cup f(B) \end{aligned}$$

alors $f(A \cup B) \subseteq f(A) \cup f(B)$.
Et d'autre part on montre $f(A) \cup f(B) \subset f(A \cup B)$.
Soit $y \in f(A) \cup f(B)$ d'où $y \in f(A) \vee y \in f(B)$
donc ($\exists x \in A$ telque $f(x) = y$) ou ($\exists x \in B$ telque $f(x) = y$)
alors $\exists x \in A$ ou $\exists x \in B$ telque $y = f(x)$
ainsi que $\exists x \in (A \cup B)$ telque $y = f(x)$
d'où $y \in f(A \cup B)$
on déduire que $f(A) \cup f(B) \subset f(A \cup B)$.
On conclue que $f(A \cup B) = f(A) \cup f(B)$.

Exercice 7 : Soient $f : E \to F$ une application de E dans F et A, B deux parties non vides de E.
1)

$$\begin{aligned} f^{-1}(A \cap B) &= \{x \in E | f(x) \in (A \cap B)\} \\ &= \{x \in E | f(x) \in A \text{ et } f(x) \in B\} \\ &= \{x \in E | f(x) \in A\} \cap \{x \in E | f(x) \in B\} \\ &= f^{-1}(A) \cap f^{-1}(B). \end{aligned}$$

2)

$$\begin{aligned} f^{-1}(A \cup B) &= \{x \in E | f(x) \in (A \cup B)\} \\ &= \{x \in E | f(x) \in A \text{ ou } f(x) \in B\} \\ &= \{x \in E | f(x) \in A\} \cup \{x \in E | f(x) \in B\} \\ &= f^{-1}(A) \cup f^{-1}(B). \end{aligned}$$

Exercice 8 : Soient $f : E \to F$ de E dans F ,A une partie non vide de F.
On sait que $x \in f^{-1}(A) \Leftrightarrow f(x) \in A$.
D'une part
$f^{-1}(\mathrm{C}_F^A) = \{x \in E | f(x) \in \mathrm{C}_F^A\}$
donc $f^{-1}(\mathrm{C}_F^A) = \{x \in E | f(x) \notin A\}$.
D'autre part
$\mathrm{C}_E^{f^{-1}(A)} = \{x \in E | x \notin f^{-1}(A)\}$
alors $\mathrm{C}_E^{f^{-1}(A)} = \{x \in E | f(x) \notin A\}$.
D'où $f^{-1}(\mathrm{C}_F^A) = \mathrm{C}_E^{f^{-1}(A)}$.

Exercice 9 : Soit

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto \frac{x}{x^2+1} \end{aligned}$$

1)f est elle injective ?
Soient $x, x' \in \mathbb{R}$

$$\begin{aligned} f(x) = f(x') &\Rightarrow \frac{x}{x^2+1} = \frac{x'}{x'^2+1} \\ &\Rightarrow x'x^2 + x' = xx'^2 + x \\ &\Rightarrow x'x^2 - xx'^2 = x - x' \\ &\Rightarrow x'x(x-x') = x - x' \\ &\Rightarrow (1 - x'x)(x-x') = 0 \\ &\Rightarrow (1-x'x) = 0 \ ou \ (x-x') = 0 \\ &\Rightarrow (1 = x'x) \ ou \ (x = x') \end{aligned}$$

Alors f n'est pas injective.
2)f est elle surjective ?
Soit $y \in \mathbb{R}$ est-ce que $\exists x \in \mathbb{R}$ tel que $y = f(x)$

$$\begin{aligned} y = f(x) &\Rightarrow \frac{x}{x^2+1} = y \\ &\Rightarrow x = y(x^2+1) \\ &\Rightarrow yx^2 - x + y = 0. \end{aligned}$$

$yx^2 - x + y = 0$ est une équation de degré 2 d'inconnu x alors $\Delta = 1 - 4y^2$
Si $y \in]-\infty, \frac{-1}{2}[\cup]\frac{1}{2}, +\infty[$ on a $\Delta < 0$ donc n'existe pas des solutions d'équation $yx^2 - x + y = 0$.
Alors f n'est pas surjective.
3)Pour $y \in [\frac{-1}{2}, \frac{1}{2}]$ c'est a dire $\Delta \geqslant 0$ alors il existe $x \in \mathbb{R}$ tel que $y = f(x)$ alors $f(\mathbb{R}) \subset [\frac{-1}{2}, \frac{1}{2}]$ et comme $f(-1) = \frac{-1}{2}$ et $f(1) = \frac{1}{2}$

Alors $f(\mathbb{R}) = [\frac{-1}{2}, \frac{1}{2}]$.

Exercice 10 : Soit

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto |x| + 2x \end{aligned}$$

1)f est elle injective ?

Soient $x, x' \in \mathbb{R}$ $f(x) = f(x') \Leftrightarrow |x| + 2x = |x'| + 2x'$ on séparé quatre cas :
a)premièrement si $x \geqslant 0$ et $x' \geqslant 0$ alors$|x| + 2x = |x'| + 2x' \Leftrightarrow 3x = 3x' \Leftrightarrow x = x'$
b) deuxièment si $x \geqslant 0$ et $x' \leqslant 0$ alors$|x| + 2x = |x'| + 2x' \Leftrightarrow 3x = x' \Leftrightarrow x = \frac{x'}{3}$
et comme $x \geqslant 0$ et $x' \leqslant 0$ alors $x = x' = 0$

c)ensuite si $x \leqslant 0$ et $x' \geqslant 0$ alors$|x| + 2x = |x'| + 2x' \Leftrightarrow x = 3x'$ et comme $x \leqslant 0$ et $x' \geqslant 0$ alors $x = x' = 0$
d)la dernière si $x \leqslant 0$ et $x' \leqslant 0$ alors

$$|x| + 2x = |x'| + 2x' \Rightarrow x = x'.$$

Conclusion f est injective.

1)f est elle surjective ?
Soit $y \in \mathbb{R}$ est-ce qu'il existe x de $\mathbb{R}$ tel que $y = f(x)$

$y = f(x) \Leftrightarrow y = |x| + 2x$
Si $x \geqslant 0$ alors $y = 3x \Leftrightarrow x = \frac{y}{3}$

Si $x \leqslant 0$ alors $y = -x + 2x \Leftrightarrow x = y$

Alors f est surjective.
3)

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

$$\Leftrightarrow |x| + 2x = -1$$

Si $x \geqslant 0$ alors $3x = 1 \Leftrightarrow x = \frac{-1}{3}$
$x = \frac{-1}{3}$ rejet,car $x \geqslant 0$

Si $x \leqslant 0$ alors $x = -1$
Alors $f^{-1}\{-1\} = \{-1\}$.

Exercice 11 : Montrer si $\mathcal{R}$ une relation d'équivalence sur un ensemble non vide E alors $E/\mathcal{R}$ est une partition de E.
1)Comme $\mathcal{R}$ est réflexive alors pour tout $x \in E$ on a $x \in \widehat{x}$ donc $E \subseteq \cup_{x \in E} \widehat{x}$.
2)Soient $x, y \in E$ alors $\widehat{x} = \widehat{y}$ ou $\widehat{x} \cap \widehat{y} = \varnothing$.
On suppose $\widehat{x} \neq \widehat{y}$ et $\widehat{x} \cap \widehat{y} \neq \varnothing$ donc $\exists z \in \widehat{x} \cap \widehat{y}$ alors $z \in \widehat{x}$ et $z \in \widehat{y}$
d'où $z\mathcal{R}x$ et $z\mathcal{R}y$ comme $\mathcal{R}$ est une relation d'équivalence
donc $x\mathcal{R}y$ donc $\widehat{x} = \widehat{y}$ contradiction.
On dèduit que $E/\mathcal{R}$ est une partition de E.

Exercice 12 : On définit sur $\mathbb{Z}$la relation suivante $\forall (x, y) \in \mathbb{Z} : x\mathcal{R}y \Leftrightarrow \exists n \in \mathbb{Z}\ x - y = 5n$
I)-Montre que $\mathcal{R}$ est une relation d'équivalence.
1) Réflexive :
Pour tout $x \in \mathbb{Z}$ on a $x - x = 0 = 5 \times 0$ alors $\mathcal{R}$ est réflexive.
2) Symétrique :

Soient $x, y \in \mathbb{Z}$ tel que $x\mathcal{R}y \Leftrightarrow \exists n \in \mathbb{Z}\ x - y = 5n$
alors $y - x = 5(-n)$ comme $n \in \mathbb{Z}$ donc $(-n) \in \mathbb{Z}$ d'où $y\mathcal{R}x$
alors $\mathcal{R}$ est symétrique.
3) Transitive :
Soient $x, y, z \in \mathbb{Z}$ tels que

1. $x\mathcal{R}y \Leftrightarrow \exists n \in \mathbb{Z}\ x - y = 5n$
2. $y\mathcal{R}z \Leftrightarrow \exists n' \in \mathbb{Z} y - z = 5n'$

alors

$$(x - y) + (y - z) = 5n + 5n' \Rightarrow x - z = 5(n + n')$$
$$\Rightarrow x\mathcal{R}z$$

donc $\mathcal{R}$ est transitive.
Par conséquent $\mathcal{R}$ est une relation d'équivalence.
II)-On détermine que $E/\mathbb{Z}$.

$$\begin{aligned}\widehat{0} &= \{x \in \mathbb{Z} \,|\, x\mathcal{R}0\} \\ &= \{x \in \mathbb{Z} \,|\, \exists n \in \mathbb{Z}\ x - 0 = 5n\} \\ &= \{x = 5n \,|\, n \in \mathbb{Z}\} \\ &= 5\mathbb{Z}.\end{aligned}$$

$$\begin{aligned}\widehat{1} &= \{x \in \mathbb{Z} \,|\, x\mathcal{R}1\} \\ &= \{x \in \mathbb{Z} \,|\, \exists n \in \mathbb{Z}\ x - 1 = 5n\} \\ &= \{x = 5n + 1 \,|\, n \in \mathbb{Z}\} \\ &= 1 + 5\mathbb{Z}.\end{aligned}$$

$$\begin{aligned}\widehat{2} &= \{x \in \mathbb{Z} \,|\, x\mathcal{R}2\} \\ &= \{x \in \mathbb{Z} \,|\, \exists n \in \mathbb{Z}\ x - 2 = 5n\} \\ &= \{x = 5n + 2 \,|\, n \in \mathbb{Z}\} \\ &= 2 + 5\mathbb{Z}.\end{aligned}$$

$$\begin{aligned}\widehat{3} &= \{x \in \mathbb{Z} \,|\, x\mathcal{R}3\} \\ &= \{x \in \mathbb{Z} \,|\, \exists n \in \mathbb{Z}\ x - 3 = 5n\} \\ &= \{x = 5n + 3 \,|\, n \in \mathbb{Z}\} \\ &= 3 + 5\mathbb{Z}.\end{aligned}$$

$$\begin{aligned}\widehat{4} &= \{x \in \mathbb{Z} \,|\, x\mathcal{R}4\} \\ &= \{x \in \mathbb{Z} \,|\, \exists n \in \mathbb{Z}\ x - 4 = 5n\} \\ &= \{x = 5n + 4 \,|\, n \in \mathbb{Z}\} \\ &= 4 + 5\mathbb{Z}.\end{aligned}$$

Alors $E/\mathbb{Z} = \{\widehat{0}, \widehat{1}, \widehat{2}, \widehat{3}, \widehat{4}\}$.

Exercice 13 : Pour montrer que $\mathcal{R}$ est une relation d'équivalence il suffit de montrer qu'elle est symétrique et transitive.
1) Symétrique :
Soient $x, y \in E$ tel que $x\mathcal{R}y$ et comme $\mathcal{R}$ réflexive donc $y\mathcal{R}y$ alors $y\mathcal{R}x$ (puisque $\mathcal{R}$ est circulaire)
d'où elle est symétrique.
2) Transitive :
Soient $x, y, z \in E$ tel que $x\mathcal{R}y$ et $y\mathcal{R}z$ alors $z\mathcal{R}x$ (puisque $\mathcal{R}$ est circulaire)
et comme $\mathcal{R}$ est symétrique,donc $x\mathcal{R}z$ d'où elle est transitive.

Exercice 14 : Soient $x, y \in \mathbb{R}$ $x\mathcal{R}y \Leftrightarrow \exists n \in \mathbb{Z} \quad x, y \in [n, n+1[$.
Si $x, y \in [n, n+1[\Leftrightarrow E(x) = E(y) = n$
On sait que $\forall x \in \mathbb{R} : x \in [E(x), E(x)+1[$ tel que $[x] = E(x)$ est la partie entière de x
alors $x\mathcal{R}y \Leftrightarrow y \in [E(x), E(x)+1[$ En effet $\hat{0} = [0, 1[$, $\hat{1} = [1, 2[$ et $\hat{-1} = [-1, 0[$
Alors pour tout $m \in \mathbb{Z}$ on a $\hat{m} = [m, m+1[$.
Et pour tout $\forall x \in \mathbb{R} : \hat{x} = [E(x), E(x)+1[$
Donc $\mathbb{R}/x\mathcal{R} = \mathbb{Z}$
$f : \mathbb{Z} \longrightarrow \mathbb{R}/\mathcal{R}$, $x \longmapsto \widehat{x}$ est une application bijective ?
f est une application ?
Soient $n, m \in \mathbb{Z}$ si $m = n$ alors $\hat{m} = \hat{n}$ donc $f(m) = f(n)$.
f est injective ?
Soient $n, m \in \mathbb{Z}$ si $f(m) = f(n)$. alors $\hat{m} = \hat{n}$ donc $m\mathcal{R}n$ d'où $E(m) = E(n)$
alors $m = n$ (puisque $n, m \in \mathbb{Z}$)
f est surjective par définition.

Exercice 15 : Soit $\mathcal{R}$ une relation définie dans $\mathbb{R} \times \mathbb{R}$ par

$$(x, y)\mathcal{R}(x', y') \Rightarrow (x < x') \vee ((x = x') \wedge (y \leq y'))$$

Étudier les propriétés de $\mathcal{R}$:
1) La réflexivité de $\mathcal{R}$:
Pour tout $(x, y) \in \mathbb{R} \times \mathbb{R}$ on a $(x = x) \wedge (y \leq y)$
alors $(x, y)\mathcal{R}(x, y)$.
2) La symétrisation de $\mathcal{R}$: puisque $(2, 3)\mathcal{R}(3, 2)$ est vraie mais $(3, 2)\overline{\mathcal{R}}(2, 3)$ n'est pas vraie alors $\mathcal{R}$ n'est pas symétrique.

3) La transitivité de $\mathcal{R}$:
Soient $(x,y),(x',y')\, et\, (x'',y'') \in \mathbb{R}\times\mathbb{R}$.
Si $(x,y)\mathcal{R}(x',y')$ et $(x',y')\mathcal{R}(x'',y'')$
alors $x<x' \vee ((x=x')\wedge(y\leq y'))$ et $x'<x''\vee((x'=x'')\wedge(y'\leq y''))$
donc on a quatre possibilités :
a) $x<x'\, et\, x'<x''$ alors $x<x''$ donc $(x,y)\mathcal{R}(x'',y'')$,
b) $x<x'\, et\, (x'=x'')\wedge(y'\leq y")$ donc $x<x"$ alors $(x,y)\mathcal{R}(x'',y'')$,
c) $(x=x')\wedge(y\leq y')$ et $x'<x''$ donc $x<x''$ alors $(x,y)\mathcal{R}(x'',y'')$ ou
d) $(x=x')\wedge(y\leq y')$ et $(x'=x'')\wedge(y'\leq y'')$ donc $x=x''$ et $y\leq y''$ alors $(x,y)\mathcal{R}(x'',y'')$
d'où $\mathcal{R}$ est transitive.
4) L'anti-symétrisation de $\mathcal{R}$
Soient $(x,y)\ et\ (x',y')\in\mathbb{R}\times\mathbb{R}$ Si $(x,y)\mathcal{R}(x',y')$ et $(x',y')\mathcal{R}(x,y)$
alors $x<x'\vee(x=x')\wedge(y\leq y')$ et $x'<x\vee(x'=x)\wedge(y'\leq y)$
alors $(x=x')\wedge(y\leq y')\wedge(y'\leq y)$ donc $x=x'\wedge y=y'$
d'où $(x,y)=(x',y')$ ainsi $\mathcal{R}$ est anti-symétrique.
Conclusion $\mathcal{R}$ est une relation d'ordre.
En plus $\mathcal{R}$ est une relation d'ordre total .
Soient $(x,y)\ et\ (x',y')\in\mathbb{R}\times\mathbb{R}$ on a :
soit $x<x'$, $x'<x$ ou $x=x'$ donc
• Si $x<x'$ alors $(x,y)\mathcal{R}(x',y')$
• Si $x'<x$ alors $(x',y')\mathcal{R}(x,y)$
• Si $x=x'$ alors on a $(y\leqslant y'$ ou $y'\leqslant y)$ donc $((x,y)\mathcal{R}(x',y')$ ou $(x',y')\mathcal{R}(x,y))$.

Exercice 16 : Soit $\mathcal{R}$ une relation définie sur $\mathbb{R}$ par

$\forall x,y\in\mathbb{R} : x\mathcal{R}y \Rightarrow \exists n\in\mathbb{Z}\quad x,y\in[n,n+1[\ et\ x\leq y$
• $\mathcal{R}$ est une relation d'ordre ?
1) $\mathcal{R}$ est elle réflexive ?
Soit $x\in\mathbb{R}$ on a $\exists n=E(x)\in\mathbb{Z}\quad x,x\in[n,n+1[\wedge x\leq x$ donc $x\mathcal{R}x$ alors $\mathcal{R}$ est réflexive.
2) $\mathcal{R}$ est elle anti-symétrique ?
Soient $x,y\in\mathbb{R}$ si $x\mathcal{R}y$ et $y\mathcal{R}x$
alors $(\exists n\in\mathbb{Z}\quad x,y\in[n,n+1[\wedge x\leq y)$ et $(\exists n'\in\mathbb{Z}\quad y,x\in[n',n'+1[\wedge y\leq x)$
donc $x=y$ et $n=n'$ d'où $\mathcal{R}$ est anti-symétrique.
3) $\mathcal{R}$ est elle transitive ?
Soient $x,y,z\in\mathbb{R}$ si $x\mathcal{R}y$ et $y\mathcal{R}z$
alors $(\exists n\in\mathbb{Z}\quad x,y\in[n,n+1[\wedge x\leq y)$ et $(\exists n'\in\mathbb{Z}\quad y,z\in[n',n'+1[\wedge y\leq z)$.
Donc $n=n'\, x,y,z\in[n,n+1[\ et\ x\leq y\leq z$ d'où $x\mathcal{R}z$.
Ainsi $\mathcal{R}$ est transitive.
Conclusion $\mathcal{R}$ est une relation d'ordre.
• $[0,1[$ n'est pas majorée.
$\forall x\in[0,1[$ on a $0,x\in[0,1[\, et\, 0\leq x$ alors $\inf[0,1[=0$

- On note $[x]=E(x)$ est la partie entière de x

$f : \mathbb{R} \longrightarrow \mathbb{Z} \times [0,1[$
$x \longmapsto ([x], x - [x])$
est une application bijective ?
1)f est elle bien définie ?
Si $x = y \Rightarrow ([x] = [y] \, et \, x - [x] = y - [y]) \Rightarrow f(x) = f(y)$ donc f est bien définie.
2)f est elle injective ?
Soient $x, y \in \mathbb{R}$ si $f(x) = f(y) \Rightarrow ([x], x - [x]) = ([y], y - [y])$
$\Rightarrow [x] = [y]$ $x - [x] = y - [y] \Rightarrow x = y$ donc f est injective.
3)$\forall (n, y) \in \mathbb{Z} \times [0,1[$ alors $\exists x = (n + y) \in \mathbb{R}$ où $[x] = n$
on a $f(x) = f(n + y) = (n, y)$, donc f est surjective.

5.3 Exercices du chapitre 3

Exercice 1 : On montre que $(3\mathbb{Z}, +)$ est un groupe.
On sait que $3\mathbb{Z} = \{3n \,|\, n \in \mathbb{Z}\}$
1) $0 = 3 \times 0 \in 3\mathbb{Z}$ alors $3\mathbb{Z} \neq \varnothing$
2) Soient $x = 3k$ et $y = 3k'$ avec $k, k' \in \mathbb{Z}$ alors $x + y = 3k + 3k' = 3(k + k')$ d'où $(x + y) \in 3\mathbb{Z}$ alors $+$ est interne.
3) Soient $x, y, z \in 3\mathbb{Z}$ on a $x + (y + z) = (x + y) + z$ alors $+$ est associative.
4) Élément neutre est 0 puisque $\forall x \in 3\mathbb{Z}$ on a $x + 0 = 0 + x = x$
5) Soit $x = 3k \in 3\mathbb{Z}$ on a $-x = -3k \in 3\mathbb{Z}$ avec $3k + (-3k) = (-3k) + 3k = 0$
alors élément symétrique de $x = 3k$ est $x' = -3k$.

Exercice 2 : Montreons que tout élément dans un groupe est régulier.
Soit $(G, *)$ un groupe et soit $x \in G$ avec x' est le symétrique de x alors
$\forall y, z \in G$ si $x * y = x * z$ donc

$$x' * (x * y) = x' * (x * z) \Rightarrow (x' * x) * y = (x' * x) * z$$
$$\Rightarrow e * y = e * z$$
$$\Rightarrow y = z.$$

si $y * x = z * x$ donc

$$(y * x) * x' = (z * x) * x' \Rightarrow y * (x * x') = z * (x * x')$$
$$\Rightarrow y * e = z * e$$
$$\Rightarrow y = z$$

tel que e est l'élément neutre de G.

Exercice 3 : Soit $(G,*)$ un groupe de l'élément neutre e tel que $\forall x \in G\ x*x=e$, montrer que $(G,*)$ est commutatif.
Soient $x,y \in G$ on a $(x*y) \in G$ donc $(x*y)*(x*y)=e$ alors

$$\begin{aligned}(x*y)*(x*y)*(y*x)=e*(y*x) &\Leftrightarrow (x*y)*x*(y*y)*x=y*x\\ &\Leftrightarrow (x*y)*x*(e)*x=y*x\\ &\Leftrightarrow (x*y)*(x*x)=y*x\\ &\Leftrightarrow (x*y)*(e)=y*x\\ &\Leftrightarrow x*y=y*x\end{aligned}$$

d'où $(G,*)$ est commutatif.

Exercice 4 : Soient $(G,*)$ un groupe, H_1 et H_2 deux sous groupes de $(G,*)$
1) Montrer que $H_1 \cap H_2$ est un sous groupe de $(G,*)$.
• Comme H_1 et H_2 deux sous groupes de $(G,*)$
alors l'élément neutre e de G appartient à H_1 et H_2
alors $e \in H_1 \cap H_2$ donc $H_1 \cap H_2 \neq \varnothing$.
• Soient $x,y \in H_1 \cap H_2$ donc $x,y \in H_1$
alors $x*y \in H_1$. D'autre part $x,y \in H_2$ donc $x*y \in H_2$
d'où $x*y \in H_1 \cap H_2$.
• Soit $x \in H_1 \cap H_2$ alors $x \in H_1$ et $x \in H_2$
donc $x' \in H_1$ et $x' \in H_2$ tel que $x*x'=x'*x=e$
d'où $x' \in H_1 \cap H_2$.

2) $H_1 \cup H_2$ est il sous groupe de $(G,*)$. Généralement la réponse est non :
Par exemple : $H_1=2\mathbb{Z}$ et $H_2=3\mathbb{Z}$ sont des sous groupes de $(\mathbb{Z},+)$
on a $2 \in 2\mathbb{Z} \subset 2\mathbb{Z} \cup 3\mathbb{Z}$ et $3 \in 3\mathbb{Z} \subset 2\mathbb{Z} \cup 3\mathbb{Z}$ mais $2+3=5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$
alors $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous groupe de $(\mathbb{Z},+)$.

3) Montrons que $H_1 * H_2 = \{x*y \,/\, x \in H_1\ , y \in H_2\}$ est un sous groupe de $(G,*)$ si $*$ commutative.
Soient $(x*y) \in H_1*H_2$ et $(x'*y') \in H_1*H_2$.
Pour $(x*y)*(x'*y') \in H_1*H_2$ il faut qu'il égale à $(x*x'*y*y')$ ce qui donne que $y*x'=x'*y$
alors $*$ commutative.

Exercice 5 : Montrer $(5\mathbb{Z},+)$ est un sous groupe de $(\mathbb{Z},+)$
1)On a $0 \in 5\mathbb{Z}$ donc $5\mathbb{Z} \neq \varnothing$
2) Soient $x=5k$ et $y=5l$ avec $k,l \in \mathbb{Z}$.
On a $x+y'=x-y=5k+(-5l)=5(k-l) \in 5\mathbb{Z}$.

Exercice 6 : 1) On suppose qu'il existe deux éléments neutres e et e' dans $(G,*)$ alors $e'=e'*e=e$.
2) Soit $x \in G$, on suppose qu'il existe $x',x'' \in G$ deux symétries de x
donc $x'=x'*e=x'*(x*x'')=(x'*x)*x''=e*x''=x''$.

Exercice 7 : Soient $(G, \star)$ et $(G', \bullet)$ deux groupes, et $f : G \to G'$ un homomorphisme de groupe.
Montreonsque si e l'élément neutre de $(G, \star)$ et e' l'élément neutre de $(G', \bullet)$ alors $f(e) = e'$.
On a $\forall x \in G$ alors $f(x) \bullet e' = e' \bullet f(x) = f(x)$.
D'autre part, on a $\forall x \in G$ alors $f(x) = f(x \star e) = f(x) \bullet f(e)$,
d'après l'unicité d'élément neutre alors $f(e) = e'$.

Exercice 8 : Soient $(G, \star)$ et $(G', *)$ deux groupes, et $f : G \to G'$ un homomorphisme de groupe.
Montrer si x' l'élément symétrie de x dans G alors $f(x')$ l'élément symétrie de $f(x)$
c'est à dire $f(x') = f(x)'$.
On a $f(x) * f(x)' = e'$ tel que e' élément neutre de $(G', *)$;
D'autre part, on a $f(x) * f(x') = f(x \star x') = f(e) = e'$ tel que e élément neutre de $(G, \star)$,
d'après l'unicité d'élément symétrique alors $f(x') = f(x)'$.

Exercice 9 : Soient $(G, \star)$ et $(H, *)$ deux groupes, $f : G \to H$ un homomorphisme de groupe.
Montrons que Imf est un sous groupe de H.
On sait que $Imf = \{f(x) \,|\, x \in G\}$
1) $f(e) = e'$ donc $e' \in H$ d'où $H \neq \varnothing$.
2) Soient $y_1, y_2 \in Imf$ donc $\exists x_1, x_2 \in G$ tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$
alors $y_1 * y_2 = f(x_1) * f(x_2) = f(x_1 \star x_2) \in Imf$.
3) Soit $y \in Imf$ donc $\exists x \in G$ avec $y = f(x)$ alors $y' = f(x)' = f(x')$ le symétrie de y donc $y' \in Imf$.
On conclue Imf est un sous groupe de H.

Exercice 10 : Soient $(G, \star)$ et $(H, *)$ deux groupes, $f : G \to H$ un homomorphisme de groupe où e (resp e') l'élément neutre de G. (resp G')
Montrons que f est injective si seulement si $\ker f = \{e\}$.
1) On suppose que f est injective, et on va montrer que $\ker f = \{e\}$.
Soit $x \in G$ tel que $x \in \ker f$ donc $f(x) = e'$ et on a $f(e) = e'$ d'où $f(x) = f(e)$ ce implique $x = e$ puisque f est injective, alors $\ker f = \{e\}$.
2) On suppose que $\ker f = \{e\}$, et on montre que f est injective.
Soit $x_1, x_2 \in G$ tel que $f(x_1) = f(x_2)$ alors $f(x_1) * f(x_2)' = e'$
ainsi $f(x_1 \star x_2') = e'$ donc $x_1 \star x_2' \in \ker f$
d'où $x_1 \star x_2' = e$ alors $x_1 = x_2$ donc f est injective.

Exercice 11 : Soient $(G, \star)$ et $(H, *)$ deux groupes, $f : G \to H$ un homomorphisme de groupe.
Montrons que f est surjective si seulement si $Imf = H$.
On suppose que f est surjective, et on montre que $Imf = H$;
Comme f est surjective alors $\forall y \in H$, $\exists x \in G$ tel que $y = f(x)$ alors $y \in Imf$ donc $H \subset Imf$
d'où $H = Imf$
On suppose que $Imf = H$, et on montre que f est surjective ;

Soit $y \in H$ donc $y \in Imf$ alors $\exists x \in G$ tel que $y = f(x)$
alors f est surjective.

Exercice 11 : D'après le premier tableau on remarque :
1) L'élément neutre de $(\mathbb{Z}/5\mathbb{Z}, \dot{+})$ est $\dot{0}$.
2) Les symétries de $\dot{1}$ et $\dot{2}$ par rapport $\dot{+}$ sont $\dot{4}$ et $\dot{3}$ (respectivement)
puisque $\dot{1}\dot{+}\dot{4} = \dot{0}$ et $\dot{2}\dot{+}\dot{3} = \dot{0}$
3) D'après le deuxième tableau on a
a)$\forall \dot{x} \in \mathbb{Z}/5\mathbb{Z}$ donc $\dot{x}\dot{\times}\dot{1} = \dot{x}\dot{\times}\dot{1} = \dot{x}$ alors $(\mathbb{Z}/5\mathbb{Z}, \dot{+}, \dot{\times})$ est unitaire.
b) Soient $\dot{x}, \dot{y} \in \mathbb{Z}/5\mathbb{Z}$ donc $\dot{x}\dot{\times}\dot{y} = y \dot{\times} x = x \dot{\times} y = \dot{y}\dot{\times}\dot{x}$ d'où $(\dot{\times})$ est commutative.
4) L'élément neutre de $(\mathbb{Z}/5\mathbb{Z}, \dot{\times})$ est $\dot{1}$.
5) Les symétries de $\dot{2}$, et $\dot{4}$ par rapport $\dot{\times}$ sont $\dot{3}$, $\dot{4}$ (respectivement)
puisque $\dot{2}\dot{\times}\dot{3} = \dot{1}$ et $\dot{4}\dot{\times}\dot{4} = \dot{1}$.
6) Soient $\dot{x}, \dot{y} \in \mathbb{Z}/5\mathbb{Z}$ tel que $\dot{x}\dot{\times}\dot{y} = \dot{0}$ alors $x \dot{\times} y = \dot{0}$
donc $x \times y$ est multiple de 5 c'est à dire $x \times y = 5n$ avec $n \in \mathbb{Z}$ et comme 5 est un nombre premier, donc 5 devise x ou 5 devise x d'où $x \in 5\mathbb{Z}$ ou $x \in 5\mathbb{Z}$ alors $(\dot{x} = \dot{0} \vee \dot{y} = \dot{0})$.
On déduit que $(\mathbb{Z}/5\mathbb{Z}, \dot{+}, \dot{\times})$ est intègre.

Exercice 13 : Soit l'application

$$\begin{array}{c} f : \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \\ x \mapsto \dot{x} \end{array}$$

1)On montre que f est un morphisme d'anneau de $(\mathbb{Z}, +, \times)$ vers $(\mathbb{Z}/5\mathbb{Z}, \dot{+}, \dot{\times})$.
Soient $x, y \in \mathbb{Z}$ alors
A)$f(x + y) = x \dot{+} y = \dot{x}\dot{+}\dot{y} = f(x)\dot{+}f(y)$.
B)$f(x \times y) = x \dot{\times} y = \dot{x}\dot{\times}\dot{y} = f(x)\dot{\times}f(y)$.
2) A) $\ker f = \{x \in \mathbb{Z} \,|\, f(x) = \dot{0}\} = \{x \in \mathbb{Z} \,|\, \dot{x} = \dot{0}\} = 5\mathbb{Z}$.
B) $Imf = \mathbb{Z}/5\mathbb{Z}$ par définition.
3) A) f n'est pas injective $\ker f = 5\mathbb{Z} \neq \{0\}$.
B) f est surjective puisque $Imf = \mathbb{Z}/5\mathbb{Z}$.

Exercice 14 : Soit $(A, *, \bullet)$ un anneau tel que $\forall x \in A \qquad x \bullet x = x$
1) On montrer que $\forall x \in A \quad x * x = 0_A$.
$x * x = (x * x) \bullet (x * x) = (x \bullet x) * (x \bullet x) * (x \bullet x) * (x \bullet x) = x * x * x * x = (x * x) * (x * x)$.
comme tout élément de $(A, *)$ est régulier par rapport $(*)$ alors $x * x = 0_A$.
2) On montrer que $(\bullet)$ est commutative :
$\forall x, y \in A : x * y = (x * y) \bullet (x * y)$
alors $x * y = (x \bullet x) \star (x \bullet y) \star (y \bullet x) \star (y \bullet y)$
$= x * (x \bullet y) \star (y \bullet x) \star y = x * [(x \bullet y) \star (y \bullet x)] \star y$
comme tout élément de $(A, *)$ est régulier par rapport $(*)$ alors $(x \bullet y) \star (y \bullet x) = 0_A$,
ensuite

$$(x \bullet y) \star (y \bullet x) * (y \bullet x) = 0_A * (y \bullet x) \Leftrightarrow (x \bullet y) \star [(y \bullet x) * (y \bullet x)] = y \bullet x$$

$$\Leftrightarrow (x \bullet y) \star 0_A = y \bullet x$$

$$\Leftrightarrow x \bullet y = y \bullet x$$

d'où $(\bullet)$ est commutative.

Exercice 15 : En utilisant les définitions.

Exercice 16 : 1) Montrons que tout corps est anneau intègre.
Soit $(\mathbb{K}, \star, \intercal)$ un corps donc $(\mathbb{K}, \star, \intercal)$ est un anneau.
Il suffit montrer qu'il est intègre,
Soient $x, y \in \mathbb{K}$ tel que $x \intercal y = 0_{\mathbb{K}}$
si $x \neq 0_{\mathbb{K}}$ alors $x^{-1} \intercal x \intercal y = x^{-1} \intercal 0_{\mathbb{K}} \Leftrightarrow y = 0_{\mathbb{K}}$
où x^{-1} est le symétrie de x par rapport $\intercal$
2) La réciproque est fausse par exemple $(\mathbb{Z}, +.\times)$ est un anneau intégré mais n'est pas un corps.

Exercice 17 : Soit $f : A \to B$ est un morphisme d'anneau de $(A, *, \circ)$ vers $(B, \star, \bullet)$:
1) Montrer que $\ker f$ est un idéal dans A
Soient $x \in A$ et $y \in \ker f$ alors $f(x \circ y) = f(x) \bullet f(y) = f(x) \bullet 0_B = 0_B$ donc $(x \circ y) \in \ker f$,d'autre part $f(y \circ x) = f(y) \bullet f(x) = 0_B \bullet f(x) = 0_B$ donc $(x \circ y) \in \ker f$ d'où $\ker f$ est un idéal.
2) Montrer que Imf est un sous anneau de B.
A) On sait que $0_B = f(0_A)$ donc $0_B \in Imf$ alors $Imf \neq \varnothing$.
B) Soient $X, Y \in Imf$ on montrer $X \star Y' \in Imf$ et $X \bullet Y \in Imf$
où Y' est le symétrie de Y par rapport $\star$.
Comme $X, Y \in Imf$ alors $\exists x, y \in A$ tels que $X = f(x)$ et $Y = f(y)$ donc
a) $X \star Y' = f(x) \star f(y)' = f(x * y') \in Imf$,
b) $X \bullet Y = f(x) \bullet f(y) = f(x \circ y') \in Imf$.

5.4 Exercices du chapitre 4

Exercice 1 : Soient $P(X)$ et $Q(X)$ deux polynômes de $\mathbb{Z}_6[X]$.
A) Calculer $P(X) + Q(X)$ et $P(X) \times Q(X)$ dans les cas suivants
1)Si $P(X) = 2X + 3X^2$ et $Q(X) = 1 + 2X^2$ alors $P(X) + Q(X) = 1 + 2X + 5X^2$
et $P(X) \times Q(X) = 2X + 4X^3 + 3X^2 + 6X^4 = 2X + 3X^2 + 4X^3 + 0X^4 = 2X + 3X^2 + 4X^3$
2) Si $P(X) = 2 + 5X^2$ et $Q(X) = X + X^2$ alors $P(X) + Q(X) = 2 + X + 6X^2 = 2 + X$
et $P(X) \times Q(X) = 2X + 2X^2 + 5X^3 + 5X^4$
3) Si $P(X) = 3X$ et $Q(X) = 2X^2$ alors $P(X) + Q(X) = 3X + 2X^2$
et $P(X) \times Q(X) = 6X^3 = 0.X^3 = 0$
B) $(\mathbb{Z}_6[X], +, \times)$ n'est pas intègre puisque $P(X) = 3X \neq 0$ et $Q(X) = 2X^2 \neq 0$ mais $P(X) \times Q(X) = 0$

Exercice 2 : Montrons que dans $\mathbb{Z}_9[X]$ que $P(X) = 3X + 1$ est inversible.
On a $(3X + 1)(1 - 3X) = 1 - 9X^2 = 1$ alors $P(X)$ est inversible.

Exercice 3 : Soit $P(X) = X^3 - 2X^2 + X - 2$
1) Montrer que 2 est une racine simple de $P(X)$.
On a $P(2) = 8 - 2.4 + 2 - 2 = 10 - 10 = 0$ donc 2 est une racine de $P(X)$.
$P'(X) = 3X^2 - 4X + 1$ alors $P'(2) = 3.4 - 4.2 + 1 = 5 \neq 0$ alors 2 est une racine simple de $P(X)$.
2) $P(X) = (X-2)(aX^2+bX+c)$ par division de $P(X)$ sur $(X-2)$ on trouve $aX^2+bX+c = X^2+1$ alors $P(X) = (X-2)(X^2+1)$ puisque X^2+1 est irréductible.

Exercice 4 : Soit $P(X) = \dfrac{X+1}{(X-1)^2(X+2)}$.
$P(X)$ s'écrit sous formes $P(X) = \dfrac{a}{(X-1)} + \dfrac{b}{(X-1)^2} + \dfrac{c}{(X+2)}$.
Par l'identification on trouve $a = \frac{1}{9}$, $b = \frac{2}{9}$ et $c = \frac{-1}{9}$.

Exercice 5 : Soit $(E, +, \times)$ un corps commutatif.
Soient $P(X)$, $Q(X)$ et $R(X)$ trois polynômes de $E[X]$.
1) Montrer que si $Q(X)|P(X)$ et $P(X)|Q(X)$ alors il existe $\lambda \in E^*$ tel que $P(X) = \lambda Q(X)$.
On ;
Si $Q(X)|P(X)$ alors il existe $P_1(X)$ tel que $P(X) = Q(X)P_1(X)$
Si $P(X)|Q(X)$ alors il existe $Q_1(X)$ tel que $Q(X) = P(X)Q_1(X)$
Donc $P(X) = P(X)Q_1(X)P_1(X)$ alors $Q_1(X)P_1(X) = 1$ donc $P_1(X) = \lambda \in E^*$.
2) Montrer que si $Q(X)|P(X)$ et $R(X)|Q(X)$ alors $R(X)|P(X)$.
Si $Q(X)|P(X)$ alors il existe $P_1(X)$ tel que $P(X) = Q(X)P_1(X)$;
Si $R(X)|Q(X)$ alors il existe $Q_1(X)$ tel que $Q(X) = R(X)Q_1(X)$,
donc $P(X) = R(X)Q_1(X)P_1(X)$ alors $R(X)|P(X)$
3) Montrer que Si $R(X)|P(X)$ et $R(X)|Q(X)$ alors $R(X)|(U(X)P(X) + V(X)Q(X))$
avec $U(X)$ $V(X) \in E[X]$.
Si $R(X)|P(X)$ alors il existe $P_1(X)$ tel que $P(X) = R(X)P_1(X)$;
Si $R(X)|Q(X)$ alors il existe $Q_1(X)$ tel que $Q(X) = R(X)Q_1(X)$,
donc $(U(X)P(X) + V(X)Q(X)) = R(X)(U(X)P_1(X) + V(X)Q_1(X))$.

Exercice 6 : Montrons que $P(x_0) = 0 \Leftrightarrow (X - x_0)$ *divise* $P(X)$. Lorsque l'on écrit la division euclidienne de $P(X)$ sur $(X - x_0)$ on obtient $P(X) = (X - x_0Q(X) + R(X)$ où $R(X)$ est un constant puisque $d^oR(X) < d^o(X - x_0) = 1$
d'autre part

$$P(x_0) = 0 \Leftrightarrow R(x_0 = 0 \Leftrightarrow R = 0$$
$$\Leftrightarrow (X - x_0) \textit{ divise } P(X).$$

Exercice 7 : Montrer que pour $P(X) \in \mathbb{R}[X]$:
$P(X)$ admet une racine de multiplicité $\geq 2 \Leftrightarrow P(X)$ et $P'(X)$ ne sont pas premiers entre eux.
1) Soit α une racine multiplicité ≥ 2 alors $P(\alpha) = P'(\alpha) = 0$ donc $P(X) = (X - \alpha)^2Q(x)$ et $P(X) = (X - \alpha)R(x)$ alors le polynôme $(X - \alpha)$ divise $P(X)$ et $P'(X)$.
Donc $P(X)$ et $P'(X)$ ne sont pas premiers entre eux.

Exercice 8 : Factoriser dans $\mathbb{R}[X]$.
1) $P(X) = (X^2 + X - 6)^2(X^4 - 1)^3$.
On a $X^2 + X - 6 = (X - 2)(X + 3)$ et $X^4 - 1 = (X^2 - 1)(X^2 + 1) = (X - 1)(X + 1)(X^2 + 1)$ et $X^2 - X + \frac{1}{4} = (X - \frac{1}{2})^2$
alors $P(X) = (X - 2)^2(X + 3)^2(X - 1)^3(X + 1)^3(X^2 + 1)^3$
2) $Q(X) = 3(X - 1)(X + 1)(X - \frac{1}{2})^2$.
3) $pgcd = (X - 1)(X + 1)$ et $ppcm = (X - 2)^2(X + 3)^2(X - 1)^3(X + 1)^3(X^2 + 1)^3(X - \frac{1}{2})^2$.

Exercice 9 : Cherche tous les polynômes $P_0(X)$ tels que
$(P(X) + 1)$ soit divisible par $(X - 1)^4$ et $(P(X) - 1)$ par $(X + 1)^4$.
On remarque si $P(X)$ est solution alors $P_0(X) + 1 = (X - 1)^4 A(X)$
par ailleurs $P_0(X) - 1 = (X + 1)^4 B(X)$ ce qui donne $1 = \frac{A(X)}{2}(X - 1)^4 + \frac{-B(X)}{2}(X + 1)^4$.
Cherchons des polynômes $A(X)$ et $B(X)$ qui convient pour cela, on écrit la relation de Bézout entre $(X - 1)^4$ et $(X + 1)^4$ qui sont premiers entre eux
et obtient

$$\frac{A(X)}{2} = \frac{5}{32}X^3 + \frac{5}{8}X^2 + \frac{9}{32}X + \frac{1}{2},$$

et

$$\frac{B(X)}{2} = \frac{5}{32}X^3 - \frac{5}{8}X^2 + \frac{9}{32}X - \frac{1}{2},$$

on obtient après les calculs

$$P_0(X) = \frac{5}{16}(X^7 - 3X^5 + 7X^3 - 7X).$$

Supposons que $P(X)$ soit une solution du problème. On note toujours $P_0(X)$ la solution particulière obtenue ci-dessus.
Alors $P(X) + 1$ et $P_0(X) + 1$ sont divisibles par $(X - 1)^4$
et $P(X) - 1$ et $P_0(X) - 1$ sont divisibles par $(X + 1)^4$.
Ainsi $P(X) - P_0(X) = (P(X) + 1) - (P_0(X) + 1) = (P(X) - 1) - (P_0(X) - 1)$ est divisible par $(X - 1)^4$ et $(X + 1)^4$.
Comme $(X - 1)^4$ et $(X + 1)^4$ sont premiers entre eux, nécessairement $P(X) - P_0(X)$ est divisible par $(X - 1)^4(X + 1)^4$.
Réciproquement si $P(X) = P_0(X) + (X - 1)^4(X + 1)^4 A(X)$, alors $P(X) - 1$ est bien divisible par $(X + 1)^4$ et $P(X) + 1$ est divisible par $(X - 1)^4$.
Ainsi les solutions sont exactement les polynômes de la forme $P_0(X) + (X - 1)^4(X + 1)^4 A(X)$, où $P_0(X)$ est la solution particulière trouvée précédemment, et $A(X)$ un polynôme quelconque.

Exercice 10 : Existe-t-il une fraction rationnelle $F(X)$ telle que
$F^2(X) = (X^2 + 1)^3$.
Écrivons $F(X) = \dfrac{P(X)}{Q(X)}$ avec $P(X)$ et $Q(X)$ deux polynômes premiers entre eux, avec $Q(X)$ unitaire. La condition $F^2(X) = (X^2 + 1)^3$ devient $P^2(X) = (X^2 + 1)^3 Q^2(X)$.
Ainsi $F(X) = P(X)$ est un polynôme $P^2(X) = (X^2 + 1)^3$ en particulier que $P^2(X)$ de degré

6 donc $P(X)$ doit etre de degré 3.
Écrivons $P(X) = aX^3 + bX^2 + cX + d$ on développe $P^2(X) = (X^2 + 1)^3$

$$X^6+3X^4+3X^2+1 = a^2X^6+2abX^5+(2ac+b^2)X^4+2(ad+bc)X^3+(2bd+c^2)X^2+2cdX+d^2$$

On identifier les coefficients pour le coefficient de X^6 on a $a = \mp 1$ puis pour le coefficient de X^5 on a $b = 0$;
Pour le coefficient de 1 on a $d \mp 1$ puis pour le coefficient de X on a $c = 0$. Mais alors le coefficient de X^3 doit vérifier $2(ad + bc) = 0$ ce qui est faux.
Ainsi aucun polynôme ne vérifie l'équation $P^2(X) = (X^2 + 1)^3$ et par le raisonnement du début, aucune fraction non plus.

Bibliographie

[1] J.Roque, C.Leboeuf, G.Chassard et J.Guegard. *Cours d'algèbre.* Ellipses.Paris, 1987.

[2] J.Escofier. *Toute algèbre de licence cours et exercices corrigés.* 3^{eme}edition-Dunod. Paris, 2011.

[3] M.Gaultier. *Exercices et problèmes.* Dunod. Paris, 2008.

[4] M.Djaa. *Algèbre générale cours et exercices corrigés.* OPU. Alger,1990.

[5] N.Bourbaki. *Algèbre chapitre 4 à 7. Eléments de mathematique.* Masson.s.a,1980.

[6] N.Basbois, P.Abbrugiati. *Algèbre cours et exercices corrigés.* 2^{eme}edition-deboeck supérieur s.a,2016.