N° d'ordre :
N° de série :

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Superieur et de la Recherche Scientifique

---

UNIVERSITÉ ECHAHID HAMMA LAKHDAR EL OUED

FACULTÉ DES SCIENCES ET DE TECHNOLOGIE

Mémoire de fin d'étude

LICENCE ACADEMIQUE

Domaine: Mathématiques et Informatique
Filière: Mathématiques
Spécialité: Modélisation mathématiques & simulation numérique

Thème

Théorie des anneaux

Présenté par:
DJANI Hiam
LABADI Fatiha
TOUAHRIA Sarah

Sous la supervision de :

Mr FERHAT Mohammed Saïd

Année universitaire 2014 – 2015


بسم الله الرحمن الرحيم

Remerciements

Nous tenons à remercier avant et après tout Allah le Tout Puissant qui nous a donné la fois et la force pour réaliser notre rêve.

Ensuite, nous adressons nos vifs remerciements à ceux qui nous ont guidé, nous ont enseigné, nous ont aidé à arriver, surtout notre directeur de recherche, notre enseignant : "FERHAT MOHAMMED SAID" pour l'aide la plus précieuse qu'il nous a fourni durant ce parcours, pour que cette recherche aboutisse à sa fin, pour son soutient tout au long de la recherche et pour le grand intérêt qu'il a porté à ce travail de recherche. Un grand merci à tous ceux qui nous ont donné le savoir et les connaissances, nous ont conseillé et guidé, à ce tour et édifice, notre université "EL CHAHID HAMMA LKHDAR D'ELOUED", surtout la faculté des sciences et de technologie, à Mr LE RECTEUR, et à tous ceux qui travaillent pour notre université.

Nous remercions chaleureusement tous les enseignants de mathématiques, et de la faculté des sciences et de technologie.

Nous présentons nos véridiques remerciements à tout personne du proche ou du loin, qui a prié pour nous, qui nous a donné un coup de main, afin de terminer ce travail de recherche.

En fin nous remercions vivement nos familles pour l'aide matérielle et morale durant la péride de préparation.

Qu'Allah vous bénisse.

MERCI

Table des matières

Introduction générale

L'algèbre est la branche des mathématiques qui étudie les structures algébriques. Elle joue un rôle essentiel dans l'évolution de la Mathématique, ainsi qui elle participe, d'une façon efficace, dans la résolution des difficultés et des problèmes, dans les différents domaines ainsi : l'économie, la physique, la médcine, la programation, les satellites artificiels,etc.

De ce fait, les mathématiciens ont distingué deux grandes parties de l'algébre : l'algébre générale et l'algébre linéaire. D'abord l'algébre linéaire s'interesse aux espaces vectoriels et les applications linéaires. Quant à l'algébre générale se base sur les structures algébriques, surtout la structure du groupe, la structure d'anneau, la structure du corps.

Parlant alors, dans notre travail d'une théorie qui fait partie de l'algébre générale c'est la théorie des anneaux.

L'étude des anneaux trouve son origine dans l'école allemande du XIX^e siècle. Elle est développée par les mathématiciens Dedekind, Hilbert, Fraenkel et Noether.

Elle naît de l'étude des équations algebriques, des nombres algébriques et de la recherche d'une démonstration du grand théorème de Fermat. Elle conduira à un développement important de l'algèbre générale et de la géomètrie algébrique.

Dans notre travail, nous allons donné une petite idée sur les éléments de la théorie des anneaux, ce mémoire comporte deux chapitres:

Le premier pour les notions et théorèmes sur les ensembles, relations, et applications.

Le second est pour les groupes, les anneaux et ideaux et quelques types d'anneaux (anneaux de pôlynomes, anneaux de matrices).

Notations et conventions

$\in$ appartient à.

$\notin$ n'appartient pas à.

$\emptyset$ ensemble vide.

$=$ égal.

$\neq$ est différent de.

$\{x\}$ ensemble à un élément x.

$\subset$ est une partie de.

$P(E)$ ensemble des parties de E.

$\complement_E P$ complémentaire de P dans E.

$\cap$ intersection.

$\cup$ réunion.

$-$ différence.

$\triangle$ différence symétrique.

$E \times F$ produit cartésien de E et F.

$\Re$ relation équivalence.

$x \Re y$ couple $(x,\ y)$ vérifiant la relation $\Re$.

$x \equiv y \,(\mathrm{mod}\, n)$ x congru à y modulo n.

$E/\Re$ ensemble quotient de E par $\Re$.

$\mathbb{Z}/n\mathbb{Z}$ anneau des classes résiduelles modulo n.

$f : E \longrightarrow F$ application de E dans F.

$f\ (x)$ image d'un élément.

$g \circ f$ application composée.

$f^{-1}(x)$ image réciproque d'un élément.

$\sup\limits_{x \in p}(x)$ borne supérieure de p.

$\inf\limits_{x \in p}(x)$ borne inférieure de p.

$\mathrm{Im}\,(u)$ image d'une application linéaire.

$\ker(u)$ noyau d'une application linéaire.

$\mathcal{F}(A,\ F)$ espace vectoriel des applications d'un ensemble A dans un espace vectoriel F.

$\mathcal{L}(E,\ F)$ espace vectoriel des applications linéaires d'un espace vectoriel E dans un espace vectoriel F.

$\dim E$ dimension d'un espace vectoriel.

$M_n(A)$ matrice associée à un endomorphisme A dans une base a.

$x \cdot y$ produit scalaire.

$(G,\ *)$ un groupe.

$G \times \acute{G}$ le produit direct de deux groupes.

e_G élément neutre de groupe G.

$(A,\ +,\ \cdot)$ un anneau.

$\sum$ la somme .

Chapitre 1

Eléments de la théorie des ensembles et relations

1.1 Les ensembles

Définition 1.1.1 *On appelle ensemble E toute collection d'objets, appelés éléments de l'ensemble E.*

Si le nombre de ces objets est fini, on l'appelle cardinal de E et on le note $Card\,(E)$.

Si E posséde une infinité d'élémentes, on dit qu'il est de cardinal infini et on note $Card\,(E) = \infty$.

Définition 1.1.2 *Si un objet x est un élément de E, on dit que x appartient à E et note $x \in E$. Si x n'est pas un élément de E, on note $x \notin E$.*

Définition 1.1.3 *L'ensemble qui ne contient aucun élément est appellé l'ensemble vide, noté $\emptyset$ ou par fois $\{\}$. On remarquera bien que $E = \{\emptyset\}$ n'est pas l'ensemble vide puisqu'il contient un élément.*

Exemple 1.1.1 $\mathbb{N}$ =*l'ensemble des nombres entiers positifs* : $\{1, 2, 3.....\}$

$\mathbb{Z}$ = *l'ensemble des nombres entiers relatifs* : $\{..... - 2, -1, 0, 1, 2.....\}$

$\mathbb{Q}$ =*l'ensemble des nombres rationnels*

$\mathbb{R}$ =*l'ensemble des nombres réels*

$\mathbb{C}$ =*l'ensemble des nombres complexes*

1.1.1 Les quantificateurs

On utilise les symboles suivants :

1. $\exists$ le quantificateur existentiel, on écrit $\exists x$ pour lire il existe au moins x .
2. $\forall$ le quantificateur universel , on écrit $\forall x$ pour lire pour tout x.
3. on écrit $\exists! x$ pour lire il existe un unique x.

En utilisant ces quantificateurs pour un ensemble A, on a :
* $A = \emptyset \Longleftrightarrow \forall x \left(x \notin A\right).$
* A est un singleton $\Longleftrightarrow \exists! x \left(x \in A\right).$

1.1.2 Parties d'un ensemble

Définition 1.1.4 *On dit qu'un ensemble A est inclus dans un ensemble B, si tout élément de A est un élément de B, noté $A \subset B$ et on a formellement :*

$A \subset B \Longleftrightarrow \forall x \left(x \in A \Longrightarrow x \in B\right).$

Quand A n'est pas une partie de B, on note $A \nsubseteq B$ et on a formellement :

$A \subsetneq B \Longleftrightarrow \exists x \left(\left(x \in A\right) \wedge \left(x \notin B\right)\right).$

Définition 1.1.5 *L'ensemble de toutes les parties d'un ensemble A est noté $P\left(A\right)$.*

Exemple 1.1.2 *Soit $A = \{a,\, b,\, c\}$ alors $P\left(A\right) = \{\emptyset,\ \{a\},\ \{b\},\ \{c\},\ \{a,\, b\},\ \{a,\, c\},\ \{b,\, c\},\ A\}$.*

Proposition 1.1.1 *Soit A un ensemle alors $\emptyset \in P\left(A\right)$ et $A \in P\left(A\right)$.*

Définition 1.1.6 *A est strictement inclus dans B, on note $A \subsetneq B$, si et seulement si :*

A est inclus dans B sans lui être égal.

Théorème 1.1.1 *Soient A, B, C des ensembles quelconques alors :*

1. $A \subset A$.
2. Si $\left(A \subset B\right) \wedge \left(B \subset A\right)$ alors $A = B$.
3. Si $\left(A \subset B\right) \wedge \left(B \subset C\right)$ alors $A \subset C$.

1.1.3 Opérations sur les ensembles

Définition 1.1.7 *Soient A et B deux ensembles :*

- La réunion de A et de B est l'ensemble, qui contient tous les éléments de A ainsi que tous les éléments de B, noté $A \cup B$.

Formellement on a : $A \cup B = \{x;\ (x \in A) \vee (x \in B)\}$.

-L'intersection de A et de B est l'ensemble, qui contient les éléments communs à A et B, noté $A \cap B$.

Formellement on a : $A \cap B = \{x;\ (x \in A) \wedge (x \in B)\}$.

Exemple 1.1.3 *Soient $A = \{a,\ b,\ c,\ 1,\ 2,\ 3\}$ et $B = \{a,\ d,\ e,\ 1,\ 4,\ 5\}$ alors :*

$A \cap B = \{a,\ 1\}$.

$A \cup B = \{a,\ b,\ c,\ d,\ e,\ 1,\ 2,\ 3,\ 4,\ 5\}$.

Proposition 1.1.2 *[15]. Soient A et B deux ensembles alors :*

- $(A \cap B \subset A) \wedge (A \cap B \subset B)$
- $(A \subset A \cup B) \wedge (B \subset A \cup B)$

Proposition 1.1.3 *[15]. Soient A, B, C trois ensembles on a :*

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

Définition 1.1.8 *- La différence de A et de B est l'ensemble qu'on note $A \backslash B$, qui contient tous les éléments de A qui ne sont pas dans B.*

- La différence symétrique de A et de B est ensemble qu'on note $A \triangle B$, formé de la différence de $A \cup B$ et de $A \cap B$.

Définition 1.1.9 *Soit E un ensemble et A un sous ensemble de E.*

On appelle complémentaire de A dans E l'ensemble, noté $\complement_E A$, constitué des éléments de E qui n'appartiennent pas à A.

Formellement on a : $\complement_E A = \{x \in E;\ x \notin A\}$.

Exemple 1.1.4 *Soient $E = \{1,\ a,\ \alpha,\ 3,\ \gamma,\ x,\ b,\ l\}$ et $A = \{1,\ a,\ \alpha,\ b\}$ alors :*

$\complement_E A = \{3,\ \gamma,\ x,\ l\}$.

Remarque 1.1.1 *Si $A \cap B = \emptyset$, on dit que A et B sont deux ensembles disjoints, et si de plus $E = A \cup B$ on dit que A est le complémentaire de B dans E ou que A et B sont deux ensembles complémentaires dans E, et on note :*

$A = \complement_E B$ *ou* $B = \complement_E A$ *noté aussi* $A = E \backslash B$.

Proposition 1.1.4 *Soit E un ensemble et A, B des sous ensembles de E, on a :*

1. $\complement_E \left(\complement_E A\right) = A$.
2. Si $A \subset B$ alors $\complement_E B \subset \complement_E A$.
3. $\complement_E (A \cup B) = \complement_E A \cap \complement_E B$.
4. $\complement_E (A \cap B) = \complement_E A \cup \complement_E B$.

Définition 1.1.10 *Soient A et B deux ensembles non vide, on note $A \times B$ l'ensemble des couples ordonnés $(x,\, y)$ tels que $x \in A$ et $y \in B$. Il est appellé produit cartésien des ensembles A et B on convient que :*

$\forall\, (x,\, y),\, (x_1,\, y_1) \in A \times B$: $(x,\, y) = (x_1,\, y_1) \Longleftrightarrow ((x = x_1) \wedge (y = y_1))$.

Exemple 1.1.5 *Soient $A = \{1,\, 5,\, a\}$ et $B = \{b,\, c,\, d\}$ alors :*

$A \times B = \{(1,\, b)\,,\ (1,\, c)\,,\ (1,\, d)\,,\ (5,\, b)\,,\ (5,\, c)\,,\ (5,\, d)\,,\ (a,\, b)\,,\ (a,\, c)\,,\ (a,\, d)\}$

$B \times A = \{(b,\, 1)\,,\ (c,\, 1)\,,\ (d,\, 1)\,,\ (b,\, 5)\,,\ (c,\, 5)\,,\ (d,\, 5)\,,\ (b,\, a)\,,\ (c,\, a)\,,\ (d,\, a)\}\,.$

Remarque 1.1.2 *$A \times B = B \times A$ si et seulement si $A = B$.*

Définition 1.1.11 *Soit E un ensemble, $A_1 ... A_n$ des parties de E, on dit que la famille $A_1 ... A_n$ est une partition de E si :*

1. $\forall i \in \{1, ..., n\},\ i \neq j \Longrightarrow A_i \cap A_j = \emptyset$ les parties A_i sont 2 à 2 disjointes.
2. $A_1 \cup A_2 \cup ... \cup A_n = E$.

Exemple 1.1.6 $A_1 =]-\infty,\, 2]$, $A_2 =]2,\, 3]$, $A_3 =]3,\ +\infty[$ *forment une partition de* $\mathbb{R}$.

1.2 Applications et fonctions

Définition 1.2.1 *On appelle application d'un ensemble E dans un ensemble F, toute correspondance f entre les éléments de E et ceux de F qui à tout élément $x \in E$ fait correspondre un unique élément $y \in F$ on note $f(x)$.*

$y = f(x)$ est appellé image de x et x est un antécédant de y.

On représente l'application f de E dans F par $f : E \longrightarrow F$.

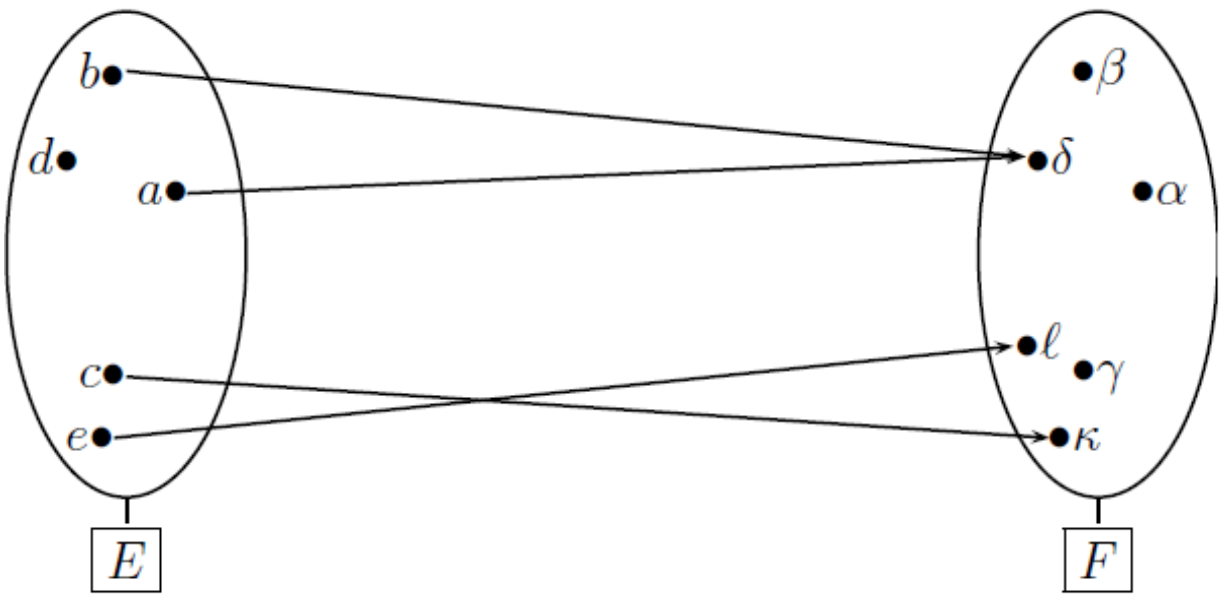
E est appellé ensemble de départ et F l'ensemble d'arrivée de l'application f.

Une correspondance entre E et F est représenteé par : $f : E \rightsquigarrow F$.

Une application f entre E et F est aussi représenteé par : $f : \underset{x \longmapsto f(x)}{E \longrightarrow F}$

Définition 1.2.2 *Formellement une correspondance f entre deux ensembles non vides est une application si et seulement si : $\forall x,\, x_1 \in E\,((x = x_1) \Longrightarrow (f(x) = f(x_1)))$.*

Exemple 1.2.1



Cette correspondance n'est pas une application car il existe un élément $d \in E$ qui n'a pas d'image dans F.

Définition 1.2.3 *On appelle fonction de E dans F toute application f d'un sous ensemble $D_f \subset E$ dans F, D_f est appellé (ensemble de définition de f).*

Remarque 1.2.1 *Toutes les notions données pour les applications peuvent être adaptées pour les fonctions.*

Exemple 1.2.2 *L'application* $Id_E : E \longrightarrow E$ *telleque* $\forall x \in E$: $Id_E(x) = x$
est appellée application identité sur E.

Définition 1.2.4 *On dit que deux applications* f *et* g *sont égales si :*

1. Elles ont le même ensemble de départ E.
2. Elles ont le même ensemble d'arrivée F.
3. $\forall x \in E : f(x) = g(x)$.

Exemple 1.2.3 *On concidère les applications suivantes :* $f : \underset{x \longmapsto x^2}{\mathbb{R} \longrightarrow \mathbb{R}}$; $g : \underset{x \longmapsto x^2}{\mathbb{R} \longrightarrow \mathbb{R}_+}$
$h : \underset{x \longmapsto x^2}{\mathbb{R}_+ \longrightarrow \mathbb{R}}$; $k : \underset{x \longmapsto x^2}{\mathbb{R}_+ \longrightarrow \mathbb{R}_+}$ *alors :*

$f \neq g$ car elles n'ont pas le même ensemble d'arrivée.

$f \neq h$ car elles n'ont pas le même ensemble de départ.

$f \neq k$ car elles n'ont pas ni le même ensemble de départ ni le même ensemble d'arrivée

1.2.1 Compositions des applications

Définition 1.2.5 *Soient* $f : E \longrightarrow F$ *et* $g : F \longrightarrow G$, *on note* $g \circ f$ *l'application de* E *dans* G *définie par :* $\forall x \in E \quad g \circ f(x) = g(f(x))$ *cette application est appellée composé de* f *et* g.

Exemple 1.2.4 *Etant données les applications* f *et* g *:* $f : \underset{x \longmapsto x^2}{\mathbb{R} \longrightarrow \mathbb{R}_+}$ *et* $g : \underset{x \longmapsto x^3}{\mathbb{R}_+ \to \mathbb{R}_+}$ *alors* $g \circ f : \underset{x \longmapsto (x^2)^3 = x^6}{\mathbb{R} \to \mathbb{R}_+}$ *et* $f \circ g : \underset{x \longmapsto (x^3)^2 = x^6}{\mathbb{R}_+ \longrightarrow \mathbb{R}_+}$ *il est claire que* $\boxed{f \circ g \neq g \circ f}$.

1.2.2 Restriction et prolongement d'une application

Définition 1.2.6 *Etant donnée une application $f : E \to F$*

1. *On appelle restriction de f à un sous ensemble non vide X de E*

   l'application $g : X \longrightarrow F$ telleque : $\forall x \in X \; g(x) = f(x)$ on note $g = f_{X}$.

2. Etant donné un ensemble G telque $E \subset G$.

   On appelle prolongement de l'application f à l'ensemble G, toute application h de G dans F tellque f est la restriction de h à E.

Exemple 1.2.5 *Etant donnée l'application $f : \underset{x \longmapsto \log(x)}{\mathbb{R}_+ \longrightarrow \mathbb{R}}$ alors :*

$g : \underset{x \longmapsto \log|x|}{\mathbb{R} \longrightarrow \mathbb{R}}$ et $h : \underset{x \longmapsto \log(2|x|-x)}{\mathbb{R} \longrightarrow \mathbb{R}}$
sont deux prolongements différents de f à $\mathbb{R}$.

1.2.3 Image directe et image réciproque

Définition 1.2.7 *Soit $f : E \to F$ une application pour toute partie $A \subset E$, on appelle image directe de A par f l'ensemble $f(A) = \{y \in F / \exists x \in A \; f(x) = y\}$ et pour toute partie B de F, on appelle image réciproque de B par f l'ensemble $f^{-1}(B) = \{x \in E / f(x) \in B\}$.*

Exemple 1.2.6 *Soit $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = x^2$ soit $B = [1, 2]$*
on a alors $f^{-1}(B) = \left[-\sqrt{2}, -1\right] \cup \left[1, \sqrt{2}\right]$.
Soit maintenant $A = \left[1, \sqrt{2}\right]$ on a $f(A) = [1, 2] = B$ on remarque alors :
$f^{-1}(f(A)) \neq A$.

Proposition 1.2.1 *[12] Soient $f : E \to F$, A, $B \subset E$ et M, $N \subset F$ alors :*

1. *$f(A \cup B) = f(A) \cup f(B)$.*
2. *$f(A \cap B) \subset f(A) \cap f(B)$.*
3. *$f^{-1}(M \cup N) = f^{-1}(M) \cup f^{-1}(N)$.*

4. $f^{-1}(M \cap N) = f^{-1}(M) \cap f^{-1}(N)$.

5. $f^{-1}\left(\complement_F M\right) = \complement_E f^{-1}(M)$.

Preuve. 1. Soit $y \in F$ alors $y \in f(A \cup B) \Longleftrightarrow \exists x \in A \cup B;\ y = f(x)$
$\Longleftrightarrow \exists x\,[((x \in A) \vee (x \in B)) \wedge (y \in f(A))]$
$\Longleftrightarrow \exists x\,[((x \in A) \wedge (y \in f(A))) \vee ((x \in B) \wedge (y \in f(A)))]$
$\Longleftrightarrow (y \in f(A) \vee (y \in f(B))) \Leftrightarrow y \in f(A) \cup f(B)$.
3. Soit $x \in E$ alors : $x \in f^{-1}(M \cup N) \Longleftrightarrow f(x) \in M \cup N \Longleftrightarrow (f(x) \in M) \vee (f(x) \in N)$
$\Longleftrightarrow (x \in f^{-1}(M)) \vee (x \in f^{-1}(N)) \Longleftrightarrow x \in f^{-1}(M) \cup f^{-1}(N)$
5. Soit $x \in E$ alors : $x \in f^{-1}\left(\complement_F M\right) \Longleftrightarrow f(x) \in \complement_F M \Longleftrightarrow (f(x) \in F) \wedge (f(x) \notin M)$
$\Longleftrightarrow (x \in E) \wedge (x \notin f^{-1}(M)) \Longleftrightarrow x \in \complement_E f^{-1}(M)$. ■

1.2.4 Applications injectives, surjectives, bijectives

Définition 1.2.8 *Soit $f : E \to F$ une application, on dit que f est :*

i) injective si $\forall x, y \in E,\ f(x) = f(y) \Longrightarrow x = y$.
ii) surjective si $\forall y \in F,\ \exists x \in E,\ f(x) = y$.
iii) bijective si f est injective et surjective.

Lemme 1.2.1 *Soit $f : E \to F$ une application alors les propositions suivantes sont équivalentes :*

1. f est bijective.

2. f est injective et surjective.

Proposition 1.2.2 *Soient $f : E \to F$ et $g : F \to G$ alors :*

i) (f injective) $\wedge$ (g injective) $\Longrightarrow$ ($g \circ f$ injective).
ii) (f surjective) $\wedge$ (g surjective) $\Longrightarrow$ ($g \circ f$ surjective).
iii) (f bijective) $\wedge$ (g bijective) $\Longrightarrow \left(g \circ f \text{ bijective et } (g \circ f)^{-1} = f^{-1} \circ g^{-1}\right)$.

Preuve. On a $g \circ f : E \to G$:
i) Supposons f et g injectives et montrons que $g \circ f$ est injective soient

x, $x_1 \in E$ alors : $x \neq x_1 \Longrightarrow f(x) \neq f(x_1)$ car f injective $\Longrightarrow g(f(x)) \neq g(f(x_1))$ car g injective $\Longrightarrow g \circ f(x) \neq g \circ f(x_1)$.

Ce qui montre que $g \circ f$ est injective

ii) Supposons f et g surjectives et montrons que $g \circ f$ est surjective soit $z \in G$

g étant surjective, il existe $y \in F$ tel que $z = g(y)$, comme $y \in F$

et f est surjective alors il existe $x \in E$ tel que $y = f(x)$.

Donc $z = g(f(x))$ et on déduit que :

$\forall z \in G\ \exists x \in E;\ z = g \circ f(x)$ ce qui montre que $g \circ f$ est surjective.

iii) De i) et ii) on déduit que si f et g sont bijectives alors $g \circ f$ est bijective

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

d'aprés ii) pour $z \in G$, $z = g(y)$, $y = f(x)$ et $z = g \circ f(x)$, comme f, g et $g \circ f$ sont bijectives alors $y = g^{-1}(z), x = f^{-1}(y)$ et $x = (g \circ f)^{-1}(z)$ par suite : $\forall z \in G$

$(g \circ f)^{-1}(z) = x = f^{-1}(y) = f^{-1}(g^{-1}(z)) = f^{-1} \circ g^{-1}(z)$ donc $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. ■

Proposition 1.2.3 *Etant données deux applications $f : E \to F$ et $g : \acute{F} \to G$ telles que $F \subset \acute{F}$ alors :*

1. $(g \circ f$ injective $) \Longrightarrow f$ injective.

2. $(g \circ f$ surjective$) \Longrightarrow g$ surjective.

3. Si $f(E) = \grave{F}$ alors $(g \circ f$ injective $) \Longrightarrow g$ injective.

Preuve. Comme $F \subset \acute{F}$ alors $g \circ f : E \to G$ est bien définie

1. Supposons que $g \circ f$ est injective et montrons que f est injective soint x, $\acute{x} \in E$

alors :

$f(x) = f(\acute{x}) \Longrightarrow g(f(x)) = g(f(\acute{x}))$ car g est une application

$\Longrightarrow g \circ f(x) = g \circ f(\acute{x}) \Longrightarrow x = \acute{x}$ car $g \circ f$ est injective.

Donc : $\forall x, \acute{x} \in E\ (f(x) = f(\acute{x})) \Longrightarrow (x = \acute{x})$ ce qui montre que f est injective.

2. Supposons que $g \circ f$ est surjective et montrons que g est surjective soit $z \in G$ alors

$g \circ f$ surjective $\Longrightarrow \exists x \in E : g \circ f(x) = z \Longrightarrow \exists x \in E : g(f(x)) = z$

$\Longrightarrow \exists y = f(x) \in F;\ g(y) = z$.

Donc : $\forall z \in G\ \exists y \in F;\ g(y) = z$ ce qui montre que g est surjective.

3. Soient $f\colon E \to F$ et $g\colon \acute{F} \to \grave{G}$ avec $\acute{F} = f(E)$ supposons que $g \circ f$ est tels que $y = f(x)$ et $\acute{y} = f(\acute{x})$ donc :

$g(y) = g(\acute{y}) \Longrightarrow g(f(x)) = g(f(\acute{x})) \Longrightarrow g \circ f\ (x) = g \circ f\ (\acute{x})$

$\Longrightarrow x = \acute{x}$ car $g \circ f$ est injective $\Longrightarrow f(x) = f(\acute{x})$ car f application $\Longrightarrow y = \acute{y}$. ■

1.2.5 Caractérisation de l'injectivité et de la surjectivité

Proposition 1.2.4 *Soit $f : E \to F$ une application alors les propositions suivantes sont équivalentes :*

i) f est injective.

ii) $\forall A, B \subset E : f(A \cap B) = f(A) \cap f(B)$.

iii) $\forall A \subset E :\ f^{-1}(f(A)) = A$.

Proposition 1.2.5 *Soit $f\colon E \to F$ une application alors les propositions suivantes sont équivalentes :*

i) f est surjective.

ii) $\forall B \subset F : f\ (f^{-1}(B)) = B$.

1.3 Relations binaires

Définition 1.3.1 *Etant donnée une relation binaire $\Re$ entre les éléments d'un ensemble non vide E, on dit que :*

1. *$\Re$ est reflexive $\Longleftrightarrow \forall x \in E\ (x \Re x)$.*

2. *$\Re$ est transitive $\Longleftrightarrow \forall x, y, z \in E\ ((x \Re y) \wedge (y \Re z) \Longrightarrow (x \Re z))$.*

3. *$\Re$ est symétrique $\Longleftrightarrow \forall x, y \in E\ ((x \Re y) \Longrightarrow (y \Re x))$.*

4. *$\Re$ est Anti-symétrique $\Longleftrightarrow \forall x, y \in E\,(((x \Re y) \wedge (y \Re x)) \Longrightarrow x = y)$.*

1.3.1 Relation d'équivalence

Définition 1.3.2 *Soit E un ensemble et $\Re$ un relation binaire sur E, on dit que $\Re$ est une relation d'équivalence si $\Re$ est reflexive, symétrique et transitive.*

Exemple 1.3.1 *Soient $\mathbb{Z}$ l'ensemble des entiers relatifs, et n un nombre entier strictement supérieur à 1.*

La relation définie par les couples $(x,\ y)$ tels que n divise $x-y$ est une relation d'équivalence dans $\mathbb{Z}$, appelée congruence modulo n, et notée $x \equiv y \,(\mathrm{mod}\, n)$.

Définition 1.3.3 *Si $\Re$ est relation d'équivalence sur un ensemble E.*

Pour tout $x \in E$ on note : $\bar{x} = \{y \in E / x \Re y\}$.

Cet ensemble s'appelle la classe d'équivalence de $x \bmod \Re$.

Proposition 1.3.1 *[12] Soit E un ensemble et $\Re$ une relation d'équivalence sur E*

i) Si $x, y \in E$ tels que $\bar{x} \neq \bar{y}$ alors $\bar{x} \cap \bar{y} = \emptyset$.

ii) $(x \Re y) \Longleftrightarrow (\bar{x} = \bar{y})$.

Définition 1.3.4 *Soit E un ensemble et $\Re$ une relation d'équivalence sur E.*

On appelle ensemble quotient de E par $\Re$ l'ensemble des classes d'équivalences des éléments de $E \bmod \Re$, on note cet ensemble $E/\Re$ (c'est un sous-ensemble de $P(E)$).

Exemple 1.3.2 *Soit $\Re_5$ la relation définie dans $\mathbb{Z}$ ensemble des entiers relatifs par :*

$x \equiv y \,(\mathrm{mod}\, 5)$ qui se lit (x est congru à $y \ \mathrm{mod}\, 5$) ce qui veut dire ($x - y$ est divisible par 5)

alors $\Re_5$ est une relation d'équivalence dans $\mathbb{Z}$, il y a exactement cinq classes d'équivalence distinctes dans $\mathbb{Z} l \Re_5$

$A_0 = \{....., -10, -5, 0, 5, 10, ...\}$

$A_1 = \{....., -9, -4, 1, 6, 11, ...\}$

$A_2 = \{....., -8, -3, 2, 7, 12, ...\}$

$A_3 = \{....., -7, -2, 3, 8, 13, ...\}$

$A_4 = \{....., -6, -1, 4, 9, 14, ...\}$

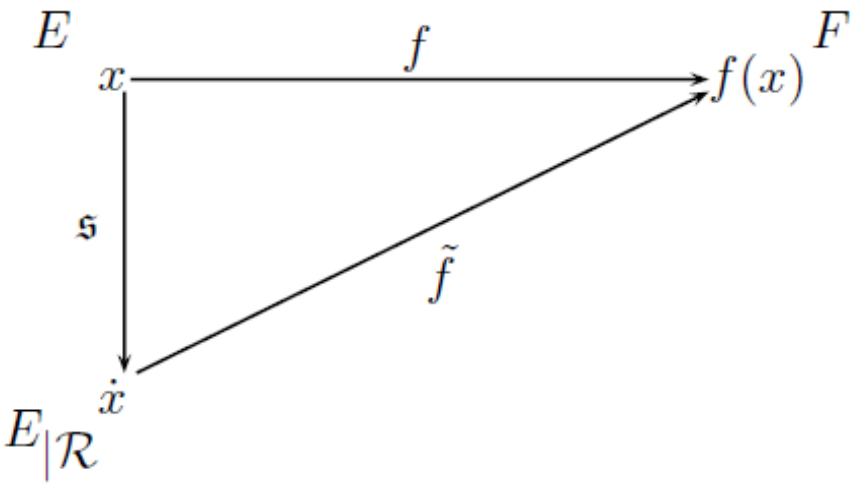
Chaque entier x peut s'écrire de manière unique sous la forme $x = 5q + r$ avec

$0 \leqslant r \leqslant 4 < 5$, remarquons que $x \in E_r$ ou r est le reste de la devision de x par 5.

Décomposition d'une application

Etant donnée une application $f\colon E \to F$, on note $E/\Re$ le quotient de E par la relation $\Re$ et pour toute classe $\bar{x}$ on pose $\tilde{f}\ (\bar{x}) = f\,(x)$, alors :

$\tilde{f}$ est une application de $E/\Re$ dans f injective et le diagramme suivant est commutatif. $f = s \circ \tilde{f} \quad S(x) = \bar{x} = x$.



Décomposition de l'application f.

Partition et relation d'équivalence

Définition 1.3.5 *Soit E un ensemble, on appelle partition de E toute partie $\{E_i\}_{i\in I}$ de $P\,(E)$ telle que :*

1. $\forall i \in I,\ E_i \neq \emptyset$.
2. $\forall i \neq j,\ E_i \cap E_j = \emptyset$.
3. $\underset{i\geqslant 1}{\cup} E_i = E$.

Théorème 1.3.1 *[12] Soit $\Re$ une relation d'équivalence dans A, l'ensemble quotient $A/\Re$ est une partition de A, c'est à dire chaque $a \in A$ appartient à un élément de $A/\Re$ et les éléments de $A/\Re$ sont deux à deux disjoints.*

Exemple 1.3.3 *D'après l'exemple 1.3.2 nous remarquons les classes d'équivalence sont disjointes deux à deux et que* $\mathbb{Z} = A_0 \cup A_1 \cup A_2 \cup A_3 \cup A_4$

1.3.2 Relation d'ordre

Définition 1.3.6 *On dit qu'une relation binaire* $\Re$ *sur* E *est une relation d'ordre si elle est Réflexive, Transitive, Anti-Symétrique.*

Dans la littérature, les relations d'ordre sont souvent notées $\preceq$.

Si $x \preceq y$, *on dit que* x *est inférieur ou égal à* y *ou que* y *est supérieur ou égal à* x.

On dit aussi que x *est plus petit (ou égal) que* y *et* y *est plus grand (ou égal) que* x.

Exemple 1.3.4 .

1. Soit E un ensemble. La relation $A \subset B$ est une relation d'ordre sur $P(E)$.
2. La relation n divise m est une relation d'ordre sur $\mathbb{N}^*$.
3. Soit E l'ensemble des fonctions d'un ensemble A vers $\mathbb{R}$: la relation $g \geq f$ signifiant $\forall x \in A$, $g(x) \geq f(x)$ est une relation d'ordre.

Définition 1.3.7 *Soit* $\preceq$ *une relation d'ordre sur un ensemble* E.

1. *On dit que deux éléments* x *et* y *de* E *sont comparables si :* $x \preceq y$ *ou* $y \preceq x$.
2. *On dit que* $\preceq$ *est une relation d'ordre total , ou que* E *est totalement ordonné par* $\preceq$, *si tous les éléments de* E *sont deux à deux comparables. Si non, on dit que la relation* $\preceq$ *est une relation d'ordre partiel ou que* E *est partiellement ordonné par* $\preceq$.

Plus petit, plus grand élément

Définition 1.3.8 *Soit* $(E, \preceq)$ *un ensemble ordonné et* $A \in P(E)$.

1. On dit que $m \in A$ est le plus petit élément de A si $\forall y \in A\,(m \preceq y)$.
2. On dit que $M \in A$ est le plus grand élément de A si $\forall y \in A\,(y \preceq M)$.

Proposition 1.3.2 *[15] Soit $(E,\ \preceq)$ un ensemble ordonné et $A \in P(E)$ alors si A possède un plus petit ou un plus grand élément, il est unique.*

Preuve. .

$$\begin{cases} (m \text{ plus petit élément de } A) \\ \wedge \\ (\grave{m} \text{ plus petit élément de } A) \end{cases} \Longrightarrow \begin{cases} m \preceq \grave{m} \\ \wedge \\ \grave{m} \preceq m \end{cases} \quad \text{(Anti-symetrie)} \Longrightarrow m = \grave{m}$$

d'ou l'unicité du plus petit élément de A, s'il existe.

Le même type de raisonnement nous montre l'unicité du plus grand élément de A, s'il existe. ■

Eléments minimaux et éléments maximaux

Définition 1.3.9 *Soit $(E, \preceq)$ un ensemble ordonné et $A \in P(E)$.*

1. On dit qu'un élément $m \in A$ est un élément minimal dans A s'il n'ya pas dans A

   un élément plus petit que m.
   Ceci est formellement équivalent à : $\forall y \in A\,(y \preceq m \Longrightarrow y = m)$.

2. On dit qu'un élément $M \in A$ est un élément maximal dans A s'il n'ya pas dans A

   un élément plus grand que M.
   Ceci est formellement équivalent à : $\forall y \in A\,(M \preceq y \Longrightarrow y = M)$.

Exemple 1.3.5 *Soit $A = \{\{1,\ 2,\ 3\},\ \{0,\ 4\},\ \{1,\ 3,\ 5\},\ \{1,\ 5\},\ \{1,\ 3\},\ \{5,\ 3\},\ \{0,\ 5,\ 6,\ 7\}\}$, alors :*

1. Les éléments minimaux de A sont : $\{0,\ 4\}$, $\{1,\ 5\}$, $\{1,\ 3\}$, $\{5,\ 3\}$ et $\{0,\ 5,\ 6,\ 7\}$.
2. Les éléments maximaux de A sont : $\{0,\ 4\}$, $\{1,\ 2,\ 3\}$, $\{1,\ 3,\ 5\}$ et $\{0,\ 5,\ 6,\ 7\}$.
3. A n'a pas de plus petit élément.
4. A n'a pas de plus grand élément.

Proposition 1.3.3 *[15] Soit $(E,\ \preceq)$ un ensemble ordonné et m, $M \in E$, alors :*

1. m plus petit élément de $A \Longrightarrow m$ est le seul élément minimal dans A.

2. M plus grand élément de $A \Longrightarrow M$ est le seul élément maximal dans A.

Borne inférieure, borne supérieure

Définition 1.3.10 *Soit $(E, \preceq)$ un ensemble ordonné, A une partie de E.*

- On appelle minorant de l'ensemble A, tout élément $m \in E$ tel que $\forall x \in A$, $m \preceq x$.
- On appelle majorant de l'ensemble A, tout élément $M \in E$ tel que $\forall x \in A$, $x \preceq M$.

Définition 1.3.11 *Soit A une partie d'un ensemble ordonné E.*

1. Soit S l'ensemble des majorants de A. Si S admet un plus petit élément α alors α est appelé borne supérieure de A. On note $\sup A = \alpha \leq M$.

2. Soit I l'ensemble des minorants de A. Si I admet un plus grand élément β alors β est appelé borne inférieure de A. On note $\inf A = m \leq \beta$.

Définition 1.3.12 *La borne supérieure est le plus petit des majorans et la borne inférieure est le plus grand des minorans.*

D'une manière plus formalisée (ce qui est utile dans certaines démonstrations), on a :

$$\alpha = \sup A \Longleftrightarrow \begin{cases} \forall a \in A,\ a \leq \alpha \\ \forall M \in E,\ \text{majorants de } A,\ \alpha \leq M. \end{cases}$$

$$\beta = \inf A \Longleftrightarrow \begin{cases} \forall a \in A,\ \beta \leq a \\ \forall m \in E,\ \text{minirant de } A,\ m \leq \beta. \end{cases}$$

Proposition 1.3.4 *[15] Soit A une partie d'un ensemble ordonné E :*

1. $\sup A \in A$ si et seulement si A possède un maximum.

Dans ce cas, $\sup A$ est le maximum.

2. $\inf A \in A$ si et seulement si A possède un minimum.

Dans ce cas, inf A est le minimum.

Théorème 1.3.2 *[12].*

1. Toute partie non vide et majorée admet une borne supérieure.
2. Toute partie non vide et minorée admet une borne inférieure.

Diagramme de Hasse

- Le diagramme de Hasse d'un ensemble ordonné s'obtient en procédant de proche en proche à partir des éléments maximaux et de leurs prédécesseurs immédiats.
- Le diagramme d'un ensemble totalement ordonné s'appelle une chaîne.
- Une partie A d'un ensemble ordonné est une chaîne maximale si :

1. C'est une chaîne de E.
2. Il n'existe pas de chaîne B telle que AB.

Dessiner un diagramme de Hasse

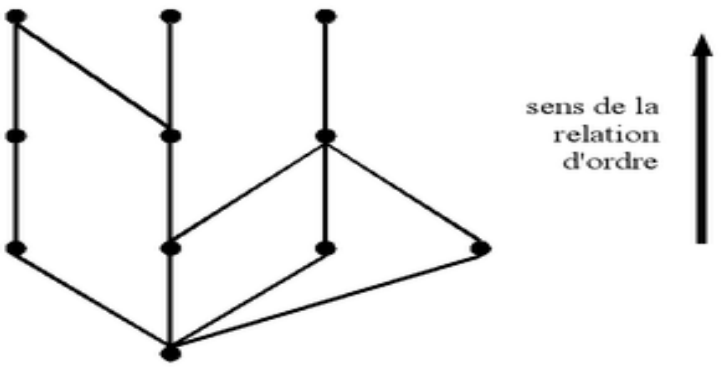
- On représente les éléments de l'ordre par des points.
- Si un élément x est plus grand qu'un autre élément y selon " $\leq$ ".

On place la représentation de x plus haute que celle de y.

- Le fait que deux éléments sont en relation est représenté par un segment entre ces deux points . Du fait de la disposition des points, on n'a pas besion d'orienter ces segments avec une flèche (on sait qu'on va du bas vers le haut) .
- Pour ne pas charger le schéma, on ne représente pas toute la relation d'ordre, mais seulement sa réduction réflixive et transitive : d'une part si $x \leq y$, mais qu'il existe z différent de x et de y tel que $(x \leq z) \wedge (z \leq y)$, alors on ne trace pas le segment entre x et y; d'autre part on ne représente pas les boucles d'un élément vers lui-même.

- On veille autant que possible à ne pas croiser les segments. En cas d'ordre infini, on peut néanmoins aussi utiliser le diagramme de Hasse pour représenter une restriction finie de l'ordre.

Exemple 1.3.6 *Le diagramme de Hasse :*



Ici, on a représenté un ensemble ordonné de 11 éléments avec trois éléments maximaux, et un minimun(qui est donc aussi un minorant de l'ensemble et sa borne inférieure) .

Chapitre 2

Lois de composition interne, groupes et anneaux

Les anneaux sont des structures mathématiques munies de deux lois internes. La théorie des groupes nous aidera à dégager certaines informations sur la nature réelle des anneaux et leurs propriétés.

2.1 Lois de composition interne

Définition 2.1.1 *On appelle loi de composition interne (l.c.i.) sur un emsemble E toute application de $E \times E$ dans E.*

Notation 2.1.1 *On utilise les symboles $\times$, $+$, $*$, $\cdot$, $\circ$, $\perp$, $\top$ pour désigner une l.c.i.*

Exemple 2.1.1 *La somme dans $\mathbb{C}$ est une loi de composition interne.*

La différence dans $\mathbb{N}$ ne l'est pas.

Définition 2.1.2 *Soit $*$ une l.c.i. sur un ensemble E. On dit que :*

1) $*$ est associative ssi : $\forall\,(x,\ y,\ z) \in E^3,\ (x * y) * z = x * (y * z)$

2) $*$ est commutative ssi : $\forall\,(x,\ y) \in E^2,\ x * y = y * x$

Définition 2.1.3 *Lorsqu'un ensemble E est muni d'une l.c.i. $*$*

On appelle magma le couple $(E,\ *)$.

Notation 2.1.2 *[18] Soit $(E,\ *)$ un magma associatif $(ou\ (E,\ \times)\ ou\ (E,\ +))$.*

Pour $n \in \mathbb{N}^*$ et $x_1, ..., x_n$, n élément de E, on abrège l'écriture :

$x_1 \times x_2 \times ... \times x_n$ en $\prod_{i=1}^{n} x_i$

$x_1 + x_2 + ... + x_n$ en $\sum_{i=1}^{n} x_i$

Proposition 2.1.1 *[18] Soit $(E,\ +)$ un magma associatif et commutatif. On a :*

1. $\forall n \in \mathbb{N}^*, \begin{cases} \forall\,(x_1, ...x_n) \in E^n \\ \forall\,(y_1, ...y_n) \in E^n \end{cases}, \sum_{i=1}^{n}(x_i + y_i) = \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i$

2. $\forall n,\ p \in \mathbb{N}^*, \forall\,(x_{ij})_{\substack{1\leq i\leq n \\ 1\leq j\leq p}} \in E^{n.p},\ \sum_{i=1}^{n}\left(\sum_{j=1}^{p} x_{ij}\right) = \sum_{j=1}^{p}\left(\sum_{i=1}^{n} x_{ij}\right)$

Définition 2.1.4 *Soit α un élément d'un magma $(E,\ *)$. On dit que :*

1. α est régulier à gauche pour $*$ (ou simplifiable à gauche) ssi :

$\forall x,\ y \in E,\ \alpha * x = \alpha * y \Longrightarrow x = y$

2. α est régulier à droite pour $*$ (ou simplifiable à droite) ssi :

$\forall x,\ y \in E,\ x * \alpha = y * \alpha \Longrightarrow x = y$

3. α est régulier pour $*$ ssi il l'est à gauche et à droite.

Définition 2.1.5 *Soient $(E,\ *)$ un magma et $e \in E$. On dit que :*

1. e est un élément neutre à gauche pour $*$ ssi : $\forall x \in E,\ e * x = x$.

2. e est un élément neutre à droite pour $*$ ssi : $\forall x \in E,\ x * e = x$.

3. e est un élément neutre ssi il l'est à gauche et à droite.

2.1.1 Unicité de l'inverse (du symétrique)

Proposition 2.1.2 *[15] Soit $*$ une loi de composition interne dans un ensemble E, associative et admettant un élément neutre e, alors si a et b sont deux éléments inversibles (symétrisables) il en sera de même de $(a*b)$ et on a :*

$$\boxed{(a*b)^{-1} = b^{-1}*a^{-1}}$$

Preuve. Soient a, $b \in E$ deux éléments inversibles, alors : comme $(a*b)(a*b)^{-1} = e$ on à :

$$\begin{aligned}(a*b)*(b^{-1}*a^{-1}) = \ & (a*(b*b^{-1}))*a^{-1} \ \ (\text{car } * \text{ est associative})\\ = \ & (a*e)*a^{-1}\\ = \ & a*a^{-1}\\ = \ & e\end{aligned}$$

De la même manière on montre que $(b^{-1}*a^{-1})*(a*b) = e$

d'où on déduit que $(a*b)$ est inversible et que $(a*b)^{-1} = b^{-1}*a^{-1}$. ■

Proposition 2.1.3 *[15] Soit $*$ une loi de composition interne associative admettant un élément neutre e dans E, alors tout élément symétrisable dans $(E,\ *)$ est régulier.*

Preuve. Soit $x \in E$ un élément symétrisable dans E, alors x^{-1} existe et pour tous a et b dans E, on a :

$$\begin{aligned}a*x = b*x \ &\Longrightarrow (a*x)*x^{-1} = (b*x)*x^{-1}\\ &\Longrightarrow a*(x*x^{-1}) = b*(x*x^{-1}) \text{ car } * \text{ est associative}\\ &\Longrightarrow a*e = b*e\\ &\Longrightarrow a = b.\end{aligned}$$

Ce qui montre que x est régulier à droite de $*$.

De la même manière on montre que x est régulier à gauche de $*$. ■

Remarque 2.1.1 *Si x est symétrisable à droite, respectivement à gauche, alors x est régulier à droite, respectivement à gauche de $*$.*

2.1.2 Morphisme des magmas

Définition 2.1.6 *Soient* $(E,\ *)$ *et* $(F,\ \top)$ *deux magmas.*

1. Un morphisme du magma $(E,\ *)$ dans $(F,\ \top)$ est une application $f : E \to F$

   telle que : $\forall x,\ y \in E,\ f(x * y) = f(x) \top f(y)$.

2. Un isomorphisme du magma $(E,\ *)$ vers $(F,\ \top)$ est un morphisme de magmas

   qui est bijectif.

3. Un endomorphisme du magma $(E,\ *)$ est un morphisme de magma$(E,\ *)$

   vers lui-même.

4. Un automorphisme du magma $(E,\ *)$ est un endomorphisme bijectif de magma $(E,\ *)$.

Exemple 2.1.2 .

1. $\varphi : (\mathcal{F}(\mathbb{R},\ \mathbb{R}),\ +) \to (\mathbb{R},\ +)\ ;\ f \longmapsto f(0)$ est un morphisme de magma.

2. L'application $(\mathbb{C},\ +) \to (\mathbb{C},\ +)\ ;\ z \longmapsto \bar{z}$ est un automorphisme de magma.

2.2 Structure de Groupe

Définition 2.2.1 *On appelle groupe, tout ensemble non vide G muni d'une loi de composition interne $*$ telle que :*

1) $*$ est associative .

2) $*$ posséde un élément neutre e.

3) Tout élément de E est symetrisable.

Si de plus $*$ est commutative, on dit que $(G,\ *)$ est un groupe commutatif, ou groupe Abélien.

Définition 2.2.2 *Si $(G,\ *)$ est un groupe fini, on appelle ordre de G le cardinal de G, on note : $|G| = CardG$.*

Proposition 2.2.1 *[18] Dans un groupe, tous les éléments sont réguliers.*

Preuve. Soient $x,\ y,\ z$ de $(G,\ *)$. Supposons $x * y = x * z$.
Comme x admet un inverse x^{-1} alors $x^{-1} * (x * y) = x^{-1} * (x * z)$
et ainsi $(x^{-1} * x) * y = (x^{-1} * x) * z$ (car la loi $*$ est associative).
Il vient $e * y = e * z$ ce qui donne $y = z$. ■

Exemple 2.2.1 *On définit l'opération $*$ par :*

$\forall x,\ y \in\ ]-1,\ 1[\ ,\ x * y = \dfrac{x+y}{1+xy}$.
Montrer que $(]-1,\ 1[\ ,\ *)$ est un groupe abélien.

1. $*$ est une loi de composition interne dans$]-1,\ 1[$.

Soient $x,\ y \in\ ]-1,\ 1[$, alors : $(|x| < 1) \wedge (|y| < 1)$
donc $(|xy| = |x|\,|y| < 1)$ par suite $1 + xy > 1 - |xy| > 0$.
Ainsi $\forall x,\ y \in\ ]-1,\ 1[$:

- $-1 < x$ et $-1 < y \implies (x+1) > 0$ et $(y+1) > 0$

$(x+1)(y+1) > 0 \Longrightarrow xy + y + x + 1 > 0$
$-1 - xy < x + y \implies -(1+xy) < x + y$ ...(1).

- $x < 1$ et $y < 1 \Longrightarrow (x-1) < 0$ et $(y-1) < 0$

$(x-1)(y-1) > 0 \Longrightarrow xy - x - y + 1 > 0$
$x + y < xy + 1$...(2).
$-(1+xy) < x + y < (1+xy)$ comme $xy + 1 \neq 0$
$-1 < \frac{x+y}{xy+1} < 1\ \forall x,\ y \in\ ]-1,\ 1[\Longrightarrow x * y \in\ ]-1,\ 1[$.

2. $*$ est commutative.

D'après la commutativé de l'addition et de la multiplication dans $\mathbb{R}$ on a :
$\forall x,\, y \in]-1,\ 1[\,,\ x * y = \dfrac{x+y}{1+xy} = \frac{y+x}{1+yx} = y * x$
Ce qui montre que $*$ est commutative.

3. $*$ est associative.

Soient $x,\, y,\, z \in]-1,\ 1[\,$, alors

$$(x*y)*z = \frac{(x*y)+z}{1+(x*y)\,z} = \frac{\frac{x+y}{1+xy}+z}{1+x\frac{x+y}{1+xy}z}$$
$$= \frac{\frac{(x+y)+z\,(1+xy)}{1+xy}}{\frac{(1+xy)+(x+y)\,z}{1+xy}} = \frac{(x+y)+z\,(1+xy)}{(1+xy)+(x+y)\,z} = \frac{x+y+z+xyz}{1+xy+xz+yz}\ ;\ 1+xy \neq 0$$

et on a : $x*(y*z) = \dfrac{x+(y*z)}{1+x\,(y*z)} = \dfrac{x+\frac{y+z}{1+yz}}{1+x\frac{y+z}{1+yz}}$

$$= \frac{\frac{x\,(1+yz)+(y+z)}{1+yz}}{\frac{(1+yz)+x\,(y+z)}{1+yz}} = \frac{x\,(1+yz)+(y+z)}{(1+yz)+x\,(y+z)};\ 1+yz \neq 0.$$
$$= \frac{(x+xyz)+(y+z)}{(1+yz)+(xy+xz)} = \frac{x+y+z+xyz}{1+xy+xz+yz}$$

en comparant les deux expressions on obtient :

$\forall x,\, y,\, z \in]-1,\ 1[\,,\ (x*y)*z = x*(y*z)$

d'où on déduit que $*$ est associative.

4. $*$ admet un élément neutre.

Soit $e \in \mathbb{R}$, alors : (e élément neutre de $*$) $\Longleftrightarrow$ ($\forall x \in]-1,\ 1[\,,\ e*x = x*e = x$)

comme $*$ est commutative et $x*e = x$

$$\Longleftrightarrow \frac{x+e}{1+xe} = x$$
$$\Longleftrightarrow x+e = x+x^2e$$
$$\Longleftrightarrow e = x^2e$$
$$\Longleftrightarrow e\,(1-x^2) = 0$$
$$\Longleftrightarrow (e=0) \vee (x=\pm 1) \text{ mais } x \neq \pm 1.$$

on déduit que $e = 0$ est l'élément neutre de $*$.

5. Tout élément de $]-1,\ 1[$ est symétrisable.

Soient $x \in]-1,\ 1[$ et $\acute{x} \in \mathbb{R}$, alors :
$x * \acute{x} = e \Longleftrightarrow \dfrac{x+\acute{x}}{1+x\acute{x}} = 0 \Longleftrightarrow x + \acute{x} = 0 \Longleftrightarrow \acute{x} = x.$
Comme $*$ est commutative on déduit que tout élément $x \in]-1,\ 1[$ est symétrisable et son symétrique est $\acute{x} = -x \in]-1,\ 1[$.

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

2.2.1 Groupes à deux éléments

Soit $G = \{a,\ b\}$ un ensemble à deux éléments,définit toutes les lois de composition interne dans G qui lui confèrent une structure de groupe.

Soit $*$ une loi de composition sur G, alors pour que $(G,\ *)$ soit un groupe; il faut que $*$ soit interne dans G et admette un élément neutre qui peut être a ou b, donc $*$ doit être définie de la sorte :

1. Si a est l'élément neutre de $*$, alors :

a. $a * a = a$

b. $a * b = b$

c. $b * a = b$

reste à définir $b * b$, or pour que $(G,\ *)$ soit un groupe il faut que tout élément soit inversible, en particulier il faut trouver b^{-1}. Si on pose $b * b = b$, alors on remarque que
$\forall x \in G,\ b * x \neq a$, donc b ne sera pas inversible, ce qui nous amène à poser :

d. $b * b = a$.

Ainsi, on a défini une l.c.i. dans G avec un élément neutre a, reste à voir si la loi ainsi définie est associative. On a :

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

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

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

En remarquant que la loi est commutative on déduit que

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

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

ce qui montre que : $\forall x,\ y,\ z \in G,\ x * (y * z) = (x * y) * z$

donc $*$ est associative dans G, et par suite $(G,\ *)$ est un groupe.

2. Si b est l'élément neutre de $*$, alors de la même manière on construit la loi $*$

comme suit :

a. $b * b = b$

b. $b * a = a$

c. $a * b = a$

d. $a * a = b$

D'après ce qui précède : il existe deux groupes à deux éléments et formellement on les définit ainsi :

$*$	a	b		$*$	a	b
a	a	b	et	a	b	a
b	b	a		b	a	b

2.2.2 Sous groupes

Définition 2.2.3 *Soit $(G,\ *)$ un groupe, on appelle sous groupe de $(G,\ *)$ tout sous ensemble non vide $\acute{G}$ de G tel que la restriction de $*$ à $\acute{G}$ en fait un groupe.*

Comme $*$ est associative dans G alors sa restriction à $\acute{G}$ est aussi associative,

par suite $\acute{G} \neq \emptyset$ est un sous groupe de $(G,\ *)$ s'il est stable par rapport à $*$ et à l'opération d'inversion, c'est à dire :

$$\begin{cases} \forall a,\ b \in \acute{G},\ a * b \in \acute{G} \\ \forall a \in \acute{G},\ a^{-1} \in \acute{G} \end{cases}$$

Il est claire que si $(G,\ *)$ est un groupe, alors G est un sous groupe de G.

Proposition 2.2.2 *[15] Soient* $(G,\ *)$ *un groupe et* $\acute{G} \subset G$*, alors :*

$\acute{G}$ est un sous groupe de $\acute{G} \iff \forall a,\ b \in \acute{G},\ a * b^{-1} \in \acute{G}$

Remarque 2.2.1 *Si* e *est l'élément neutre d'un groupe* $(G,\ *)$*, alors tout sous groupe de* G *contient* e *et on déduit la propriété suivante.*

Proposition 2.2.3 *[15] Soient* $(G,\ *)$ *un groupe,* e *l'élément neutre de* $*$ *et* $\acute{G}$ *un sous ensemble de* G*, alors* $\acute{G}$ *est un sous groupe de* $\acute{G}$ *et seulement si :*

$$\begin{cases} e \in \acute{G} \\ \forall x,\ y \in \acute{G},\ x * y^{-1} \in \acute{G}. \end{cases}$$

Définition 2.2.4 *Soit* $(G,\ *)$ *un groupe.*

On dit que $\acute{G}$ *est un sous groupe propre de* G *si* $\acute{G} \neq \{e\}$ *et* $\acute{G} \neq G$ *.*

Exemple 2.2.2 *Soit* $n \notin \mathbb{N}$*, alors* $n\mathbb{Z} = \{n.p;\ p \in \mathbb{Z}\}$ *est un sous groupe de* $\mathbb{Z}$*.*

En effet :

1. $0 \in n\mathbb{Z}$, car : $\exists p = 0 \in \mathbb{Z};\ 0 = n.p$
2. Soient $x,\ y \in n\mathbb{Z}$, alors il existe $p_1,\ p_2 \in \mathbb{Z}$ tels que $x = n.p_1$ et $y = n.p_2$, donc $x - y = n.p_1 - n.p_2 = n.\,(p_1 - p_2) = n.p \in n\mathbb{Z}$.

Par suite $\forall x,\ y \in n\mathbb{Z},\ x - y \in n\mathbb{Z}$.

De 1. et 2. on déduit que $n\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$.

Remarque 2.2.2 *Pour* $n \in \mathbb{N}/\left\{0,\ 1\right\}$*,* $n\mathbb{Z}$ *est un sous groupe propre de* $\mathbb{Z}$*.*

Proposition 2.2.4 *[6] Soit* G *un groupe et* $\{H_i\}_{i\in I}$ *une famille de sous-groupes de* G*;*

alors $\underset{i\in I}{\cap} H_i$ *est un sous-groupe de* G*.*

Preuve. Soient $x,\ y \in \underset{i\in I}{\cap} H_i$, pour tout $i \in I$ on a $x,\ y \in H_i$ comme H_i est un sous-groupe alors $xy^{-1} \in H_i$ pour tout i. Donc $xy^{-1} \in \underset{i\in I}{\cap} H_i$. ■

Remarque 2.2.3 *En général* $\underset{i\in I}{\cup} H_i$ *n'est pas un sous-groupe de* G*. Soient les sous-groupes de* $G = (Z,\ +)$ *:* $H_1 = 3\mathbb{Z}$ *et* $H_2 = 8\mathbb{Z}$*. Comme* $3 + 8 = 11 \notin H_1 \cup H_2$ *alors :*

$H_1 \cup H_2$ n'est pas un sous-groupe de $\mathbb{Z}$.

Proposition 2.2.5 *[6] Soient G un groupe et $\mathcal{F} = \{H_i\}_{i\in I}$ une famille de sous-groupes de G ordonnée par inclusion alors $\underset{i\in I}{\cup} H_i$ est un sous-groupe de G.*

Preuve. Soient $x,\ y \in \underset{i\in I}{\cup} H_i$, il existe $j,\ k \in I$ tels que $x \in H_j$ et $y \in H_k$,
supposons que $H_k \subset H_j$ alors $xy^{-1} \in H_j$ donc $xy^{-1} \in \underset{i\in I}{\cup} H_i$ ■

2.2.3 Groupes Quotients

Soient $(G,\ *)$ un groupe et $\acute{G}$ un sous groupe de G. On définit une relation binaire $\Re$ sur G par : $\forall a,\ b \in G,\ a * b^{-1} \in \grave{G}$

Proposition 2.2.6 *[15] $\Re$ est une relation d'équivalence sur G.*

Proposition 2.2.7 *[15] Si $*$ est commutative, alors $\oplus$ est une loi de composition interne dans $G/\grave{G}$.*

Proposition 2.2.8 *[15] Si $(G,\ *)$ est un groupe abélien, alors $\left(G/\grave{G},\ \oplus\right)$ est un groupe abélien, appelé groupe quotient de G par $\grave{G}$.*

Exemple 2.2.3 *On sait que dans le groupe commutatif $(\mathbb{Z},\ +)$; pour tout $n \in \mathbb{N}$, $n\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$, donc on peut parler du groupe quotient $n\mathbb{Z} = \mathbb{Z}_{/n\mathbb{Z}}$.*

2.2.4 Morphisme des groupes

Définition 2.2.5 *Une application φ d'un groupe multiplicatif G dans un groupe multiplicatif $\grave{G}$ est un morphisme de groupe si :*

$\varphi(xy) = \varphi(x)\,\varphi(y),\ \ \forall x,\ y \in G.$ $\qquad (**)$

Posons $y = x^{-1}$ dans l'expression $(**)$, il vient que

$\varphi(1_G) = 1_{\grave{G}}$ et $\varphi(x^{-1}) = \varphi(x)^{-1}$

De plus les sous ensembles suivants appelés respectivement *noyou* et *image* de φ sont des sous groupes respectifs de G et $\grave{G}$

$\ker(\varphi) = \{x \in G\ :\ \varphi(x) = 1_{\grave{G}}\}$

$\mathrm{Im}(\varphi) = \{y \in G\ :\ \exists x \in G \text{ et } \varphi(x) = y\}.$

Définition 2.2.6 *Soient G et $\grave{G}$ deux groupes.*

- Un épimorphisme est un morphisme surjerctif.
- Un isomorphisme entre G et $\grave{G}$ est un morphisme bijectif entre les deux groupes.
- Un endomorphisme de G est un morphisme de G dans lui même. On notera par $End(G)$ le groupe des endomorphismes de G muni de la loi $(f.g)(x) = f(x)\, g(x)$.
- Un automorphisme de G est un endomorphisme bijectif de G.

L'ensemble des automorphismes de G muni de la loi $\circ$ est un groupe noté $(Aut(G),\ \circ)$.

2.2.5 Homomorphisme des groupes

Dans ce paragraphe, on considère $(G,\ \cdot)$ et $(H,\ *)$ deux groupes, avec e et h leurs éléments neutres respectifs.

Définition 2.2.7 *Une application $f : G \longrightarrow H$ est appelée homomorphisme de G dans H si : $\forall a,\ b \in G,\ f(a \cdot b) = f(a) * f(b)$.*

Définition 2.2.8 *Soit $f : G \longrightarrow H$ un homomorphisme de groupe.*

On appelle noyau de f l'ensemble $\ker f = f^{-1}(\{h\}) = \{a \in G;\ f(a) = h\}$

et l'image de f l'ensemble $\operatorname{Im} f = f(G) = \{f(a),\ a \in G\}$.

Remarque 2.2.4 $\operatorname{Im} f$ *est un sous groupe de* $(H,\ *)$ *et* $\ker f$ *est un sous groupe de* $(G,\ \cdot)$.

Proposition 2.2.9 *[15] Soit $f : G \longrightarrow H$ un homomorphisme de groupe, alors :*

1. f est injective si et seulement si $\ker f = \{e\}$.
2. f est surjective si et seulement si $\operatorname{Im} f = H$.
3. f est un isomorphisme si et seulement si f^{-1} existe et est un homomorphisme de groupe de H dans G.

2.3 Structure d'anneaux

Définition 2.3.1 *Un anneau est un ensemble A non vide muni de deux lois de composition interne $\star$ et $\circ$ telles que :*

1. $(A,\ \star)$ soit un groupe abélien (on note 0 son élément neutre)
2. La loi $\circ$ soit associative et admette un élément neutre (on le note 1) , élément dit l'unité de A.
3. La loi $\circ$ soit distributive par rapport à la loi $\star$, i.e.

$\forall x,\ y,\ z \in A,\ x \circ (y \star z) = (x \circ y) \star (x \circ z)$.
Si de plus :

4. La loi $\circ$ est commutative, on dit que l'anneau $(A,\ \star,\ \circ)$ est commutatif.

Exemple 2.3.1 .

1. Les anneaux suivants $(\mathbb{Z},\ +,\ \times)$, $(\mathbb{Q},\ +,\ \times)$, $(\mathbb{R},\ +,\ \times)$, $(\mathbb{C},\ +,\ \times)$

   sont tous commutatifs.

2. Soit n un entier naturel strictement positif. On a l'anneau commutatif $(\mathbb{Z}/n\mathbb{Z},\ +,\ \times)$.

Définition 2.3.2 *Soit A un anneau et $a \in A$.*

On dit que a est inversible si et seulement s'il existe $b \in A$ tel que $ab = 1$.
On dit que a est diviseur de 0 si et seulement si $a \neq 0$ et il existe $b \neq 0$ tel que $ab = 0$.
On dit que a est nilpotent si et seulement s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$.

Définition 2.3.3 *Soit A un anneau.*

On dit que A est intègre si $A \neq \{0\}$ et ne possède pas de diviseurs de 0.
On dit que A est réduit si A ne possède pas d'autres éléments nipotents que 0.

2.3.1 Régles de calcul dans un anneau

Soit $(A,\ +,\ \cdot)$ un anneau, alors on a les régles de calcul suivantes :

Proposition 2.3.1 *[15] Pour tous x, y et $z \in A$:*

1) $0_A \cdot x = x \cdot 0_A = 0_A$

2) $x \cdot (-y) = (-x) \cdot y = -(x \cdot y)$

3) $x \cdot (y - z) = (x \cdot y) - (x \cdot z)$

4) $(y - z) \cdot x = (y \cdot x) - (z \cdot x)$

Définition 2.3.4 *Soit $(A,\ +,\ \cdot)$ un anneau commutatif. On dit que $y \in A^*$ divise $x \in A$, ou que y est un diviseur de x ou que x est divisible par y, si $\exists z \in A^*$, $x = y \cdot z$*

Remarque 2.3.1 *Soit $(A,\ \star,\ \circ)$ un anneau :*

1. Pour la première loi $\star$: on note $x \star y = x + y$ et ainsi,

   pour tout entier $n \in \mathbb{N}$, on pose $nx = \underbrace{x + ... + x}_{n \text{ fois}}$.

2. Pour la deuxième loi $\circ$: on note $x \circ y = xy$ et ainsi,

   pour tout entier $n \in \mathbb{N}$, on pose $x^n = \underbrace{x \times ... \times x}_{n \text{ fois}}$

Théorème 2.3.1 *[6] Dans un anneau commutatif $(A,\ +,\ \cdot)$, on a la formule du binôme de Newton :*

$$(x + y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k},\ \forall n \in \mathbb{N},\ \ x,\ y \in A.$$

2.3.2 Sous-anneaux

Définition 2.3.5 *Soit A un anneau. On dit qu'une partie B de A est un sous-anneau de A si les conditions suivantes sont satisfaites :*

1) $\forall x,\, y \in B,\, x - y \in B$

2) $\forall x,\, y \in B,\, x \cdot y \in B$

3) $1 \in B$

Remarque 2.3.2 .

Un sous-anneau de l'anneau A est donc en particulier un sous-groupe de $(A,\ +)$.

2.3.3 Morphisme des anneaux

Définition 2.3.6 *Soient A, B deux anneaux unitaires munis chacuns de deux lois notées $+$ et $\times$ et φ une application de A sur B.*

On dit que φ est un morphisme d'anneaux si pour tout $(x,\, y) \in A^2$ on a :

$\varphi(x+y) = \varphi(x) + \varphi(y),\ \varphi(xy) = \varphi(x)\,\varphi(y)$.

Le noyau $\ker\varphi$ et l'image $\operatorname{Im}\varphi$ du morphisme φ, sont définis par :

$\ker\varphi = \{x \in A :\ \varphi(x) = 1_B\}$ $\quad$ $\operatorname{Im}\varphi = \{y \in B :\ \exists x \in A \text{ et } y = \varphi(x)\}$.

Proposition 2.3.2 *[6] Le noyau du morphisme d'anneaux $\varphi : A \longrightarrow B$ est un sous-anneau de A. De même, l'image de φ est un sous-anneau de B.*

Preuve. Puisque $\ker\varphi$ est un sous-groupe de A, il suffit de montrer que $\ker\varphi$ est stable pour la multiplication. Soient $a,\, b \in \ker\varphi$, alors $\varphi(a) = \varphi(b) = 1_B$.

Donc : $\varphi(ab) = \varphi(a)\,\varphi(b) = 1_B \Longrightarrow ab \in \ker\varphi$. ■

2.3.4 Homomorphisme d'anneaux

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

Définition 2.3.7 *On dit que f est un homomorphisme d'anneaux si :*

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

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

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

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

Définition 2.3.8 *Soient A et B deux anneaux unitaires, on dit qu'un homomorphisme d'anneaux f de A dans B est unitaire si $f(1_A) = 1_B$.*

Proposition 2.3.3 *[15] Soit $f : A \to B$ un homomorphisme d'anneaux, alors f est injectif si et seulement si* $\ker f = \{0_A\}$

Si A et B sont deux anneaux unitaires et f un homomorphisme d'anneaux surjectif, alors f est unitaire .

2.3.5 Idéaux d'un anneau

Définition 2.3.9 *Soient A un anneau et $I \subseteq A$. On dit que I est un idéal à gauche (resp. à droite)de A si et seulement si* :

1. $(I,\ +)$ est un sous-groupe de $(A,\ +)$.
2. $\forall \alpha \in A,\, \forall x \in I,\, \alpha x \in I$.

Définition 2.3.10 *Si I est un idéal à gauche et un idéal à droite de A, on dit que I est un idéal bilatère de A ou plus simplement un idéal de A.*

Remarque 2.3.3 $\{0\}$ *et A sont des idéaux de A.*

Si I est un idéal diffirent de A, on dira que c'est un idéal propre.

Exemple 2.3.2 *Les idéaux de $\mathbb{Z}$ sont les ensembles $n\mathbb{Z}\ / n \in \mathbb{Z}^+$.*

Proposition 2.3.4 *[19] Soit A un anneau et $I \subset A$*

$$I \text{ est un idéal si et seulement si } \begin{cases} \forall \alpha,\ \beta \in I,\ \alpha + \beta \in I \\ \forall \alpha \in I,\ \forall x \in A,\, \alpha x \in I \end{cases}.$$

Proposition 2.3.5 *[5] Soient A et B deux anneaux et $f : A \longrightarrow B$ un morphisme d'anneaux. On a :*

1. $f(A)$ est un anneau.
2. Si I est un idéal de B, $f^{-1}(I)$ est un idéal de A.
3. En particulier $\ker(f)$ est un idéal de A.
4. Si I est un idéal de A alors $f(I)$ est un idéal de $f(A)$, donc de B si f est surjective.

Opérations sur les idéaux

Considérons deux idéaux I, J. On définit les opérations suivantes :

Définition 2.3.11 *La somme de I et J est l'ensemble $I + J = \{a + b \mid a \in I \text{ et } b \in J\}$, c'est un idéal (à gauche, à droite, bilatère) de A applé somme des idéaux I et J .*

L'ensemble $IJ = \{\text{somme finie de } ab \mid a \in I \text{ et } b \in J\}$ est un idéal de A appelé produit de deux idéaux bilatères I et J.

Remarque 2.3.4 .

1. L'intersection $I \cap J$ est un idéal de A, appelé intersection des deux idéaux.
2. On montre facilement que $IJ \subseteq I \cap J$. On pourrait aussi définir le produit d'un idéal à gauche par un idéal à droite, dans cet ordre.

Générateurs d'un idéal

Définition 2.3.12 *Si S est une partie de A, l'intersection des idéaux à gauche (resp à droite, bilatère) contenant S, est un idéal, et on dit que S engendre cet idéal, ou encore que les éléments de S sont les générateurs de cet idéal.*

Exemple 2.3.3 *Si $S = \{a_1, ..., a_n\}$, on notera $(a_1, ..., a_n)$ l'idéal engendré par S.*

2.3.6 Anneaux quotients

Soient A un anneau commutatif non nul et I un idéal de A. Alors la relation définie par : $x\Re y \iff x - y \in I$ est une relation d'équivalence sur A.

L'ensemble quotient, noté $A\,/I$, muni des deux lois quotients est un anneau commutatif appelé anneau quotient de A par I.

Il est clair que :

- $A\,/I = \{x + I \;/\; x \in A\}$
- L'élément neutre de l'addition est : $\bar{0} = I$.
- L'élément neutre de la multiplication est : $\bar{1} = 1 + I$.

Définition 2.3.13 *Soient A un anneau et I un idéal bilatère de A.*

Le groupe qoutient A / I peut être muni d'une structure d'anneau au moyen de la multiplication définie par :

$(x + I) \times (y + I) = (x \cdot y) + I$

C'est par définition l'anneau quotient de A par I.

Exemple 2.3.4 *Si $A = \mathbb{Z}$ (l'anneau des entiers) et $I = n\mathbb{Z}$ pour un certain entier n, l'anneau quotient A / I est l'anneau $\mathbb{Z}/n\mathbb{Z}$.*

2.3.7 Idéaux premiers. Idéaux maximaux

On supposera dans ce paragraphe que les anneaux sont tous commutatifs.

Définition 2.3.14 *Un idéal p de A est dit premier si $p \neq A$ et si*

$(\forall x,\ y \in A)$, $(xy \in p \Longrightarrow x \in p$ *ou* $y \in p)$.

Un idéal m de A est dit maximal si $m \neq A$ et si $(I \supseteq m \Longrightarrow I = m)$.

Proposition 2.3.6 *Soit A un anneau commutatif .*

Soit P un idéal de A. On dit que P est premier si l'anneau quotient $A\,/P$ est intègre.

Proposition 2.3.7 *[19]*

Tout idéal I de A différent de A est contenu dans un idéal maximal.

Corollaire 2.3.1 *Tout élément non inversible de A est contenu dans un idéal maximal.*

Définition 2.3.15 *Si un anneau A ne posséde qu'un seul idéal maximal, on dira qu'il est local (on écrira souvent $(A,\ m)$ pour préciser le nom de l'idéal maximal).*

Si A possède un nombre fini, au moins 2 idéaux maximaux, on dira qu'il est semi-local.

Remarque 2.3.5 *Un idéal maximal est un idéal premier, la réciproque est fausse en général.*

2.3.8 Anneau principal

Définition 2.3.16 *L'idéal I de l'anneau A est dit principal s'il existe $x \in A$ tel que*

$I = xA = Ax = (x)$.

L'anneau A est dit anneau principal si tout idéal de A est principal.

En supposant que l'anneau A est commutatif et unitaire, l'idéal engendré par le singleton $\{a\}$ est l'idéal principal $(a) = aA$ constitué par des multiples de a.

Soient a et $b \in A$, l'idéal $(a,\ b)$ engendré par a et b est l'ensemble des éléments $x \in A$ qui s'écrivent $x = au + bv$, $u,\ v \in A$.

Si d divise à la fois a et b, on a : $(a,\ b) \subset (d)$.

On appelle $p\,\text{gcd}$ des éléments $x_1, x_2, ..., x_n$ de A, l'élément $d \in A$ tel que :

$(d) = (x_1, ..., x_n) \Longleftrightarrow \exists u_1, ..., u_n \in A$ tels que $d = u_1x_1 + ... + u_nx_n$.

L'idéal $(a) \cap (b)$ est constitué des multiples communs à a et b, et contient l'idéal engendré $(a,\ b) \subset (a) \cap (b)$.

On appelle *ppcm* des éléments $x_1, x_2, ..., x_n$ de A, l'élément $m \in A$, tel que :

$(m) = \bigcap_{i=1}^{n} (x_i) \Longleftrightarrow (x_i \mid h \in A,\ \forall i = 1, ..., n \Longrightarrow m \mid h)$.

Exemple 2.3.5 *L'ensemble $n\mathbb{Z}$ est un idéal principal de l'anneau $\mathbb{Z}$ engendré par l'entier n.*

Soient p et q deux entiers et m leur multiple commun, alors :

$p\mathbb{Z} \cap q\mathbb{Z} = m\mathbb{Z}$ par exemple : $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$.

Si d est le diviseur commun de p et q, il existe alors u_1 et $u_2 \in \mathbb{Z}$ tels que l'on ait l'identitué de Bezout : $u_1 p + u_2 q = d \Longleftrightarrow (p,\ q) = (d)$.

2.3.9 Anneau factoriel

Définition 2.3.17 *Soit A un anneau integre. Un élément a de A est dit irréductible s'il verifie les propriétés suivantes :*

1. a n'est pas invirsible .
2. Si b et c sont des éléments de A tels que $a = bc$, l'un des deux, b ou c, est invirsible.

Exemple 2.3.6 *Un entier relatif est irréductible si et seulement s'il est un nombre premier ou l'opposé d'un nombre premier .*

Proposition 2.3.8 *[2] Soit k corps.*

1. Dans l'anneau $k[X]$, un polynôme ayant une racine dans k est irréductible s'il et seulement si est de degré 1.
2. Un polynôme de degré 2 ou 3 dans $k[X]$ est irréductible s'il et seulement si il n'a pas de racine dans k.
3. Dans l'anneau $C[X]$, les polynômes irréductibles sont les polynômes de degré 1. Dans l'anneau $R[X]$, les polynômes irréductibles sont les polynômes de degré 1 et les polynômes du second degré sans racine réelle.

Théorème 2.3.2 *[2] (les anneaux principeaux sont factoriels)*

La démonstration est en deux parties. D'abord on démontre l'existence
d'une décomposition en facteurs et irréductibles, ensuite, on établit l'unicitué.

2.3.10 Anneau de matrices

Soit A un anneau commutatif, alors l'ensemble des matrices carrés d'ordre n à coefficients dans A, muni des formules d'addition et de multiplication habituelles, forme un anneau noté $M_n(A)$; l'application qui à un élément de a associe la matrice scalaire correspondante définit une structure d'algebre. Si A est un anneau de B, alors $M_n(A)$ est un sous-anneau de $M_n(B)$.

2.3.11 Anneau de polynômes

Soit A un anneau commutatif et X une indéterminée (un symbole).

On note $A[X]$ l'ensemble des suites d'éléments de A avec un nombre fini de ternes non mul, notées comme combinaisons linéares des X^n, $n \geqslant 0$:

les éléments de $A[X]$ s'ecrivent sous la forme :

$P = \sum_n a_n X^n = \sum_{n=0}^{N} a_n X^n$

$A[X]$ est muni des opérations :

$$\left(\sum_n a_n X^n\right) + \left(\sum_n b_n X^n\right) = \sum_n (a_n + b_n) X^n$$

$$\left(\sum_n a_n X^n\right) \times \left(\sum_m b_m X^m\right) = \sum_p c_p X^p,\ c_p = \sum_k a_k b_{p-k}\ .$$

Proposition 2.3.9 *[19] $A[X]$ est une algébre sur A.*

Remarque 2.3.6 *L'application qui définit la structure d'algébre est injective, d'image les polynômes constants; A est identifié au sous anneau de $A[X]$ formé par les polynômes constants.*

Définition 2.3.18 *Soient B_1 et B_2 deux algébres sur l'anneau commutatif A,*

avec morphisme de structure $\eta_1 : A \longrightarrow B_1$.

Un morphisme d'algébre de B_1 vers B_2 est un morphisme d'anneau

$f : B_1 \longrightarrow B_2$ tel que : $\eta_2 = f \circ \beta_1$.

Proposition 2.3.10 *[19] (propriété universelle) .*

Soit B une algébre sur l'anneau commutatif A, et b un élément de B, alors il existe un unique morphisme d'algébre $E_b : A[X] \longrightarrow B$ tel que $E_b(X) = b$.

Remarque 2.3.7 *E_b est appelé morphisme d'évalution et $E_b(P)$ est noté $P(E_b)$.*

Définition 2.3.19 *Le degré d'un polynôme non mul $p = \sum_n a_n X^n$ est le plus grand n pour lequel $a_n \neq 0$ (convention : $\deg(0) = -\infty$).*

Proposition 2.3.11 *[19] Si A est un anneau commutatif integre, alors :*

1. $\deg(PQ) = \deg(P) + \deg(Q)$.
2. Les inversibles de $A[X]$ sont les inversibles de A, et $A[X]$ est un anneau integre.

Conclusion

Dans cette étude, nous avons abordé les lois de composition interne, les idéaux et la théorie des anneaux et des groupes.

Finalement, toutes les remarques et commentaires nous permettront certainement d'améliorer le contenu ainsi que la présentation de la version finale.Ils sont les bienvenus de la part des étudiants ainsi que de la part d'enseignants ou spécialistes en mathématiques ou utilisateurs de mathématiques.

Bibliographie

[1] *A.LEORY, Théorie des anneaux sujet de mémoire.*

[2] *ANTOINE.CHAMBERT-LOI, algébre commutative, centre de mathématique, ecole polytechnique, 91128 palaiseau cedex.*

[3] *BRUNO.DESCHAMP, cours de license d'informatique saint-Etienne, 2002/2003.*

[4] *C.DESCHAMPS, E.RAMIS, J.ODOUX, cours de mathématiques spéciales, imprimé en Frence, Paris 1974..*

[5] *C.QUITTE, H.LOMBARDI, L.DUCOS, M.SALOU, théorie algorithmique des anneaux de DEDEKIND, avril 2003.*

[6] *DR.HITTA.AMARA, Algébre, Analuse1, université 8 mais 1945 Guelma, Faculté des sciences et de l'ingénieur.*(cours).

[7] *E.VIEILLARD-BARON, G.PHILIPPE, S.ROUZES, anneau et corps, janvier 2001.*

[8] *F.PECATAINGS, J.SEVIN, chemins vers l'algébre tome1, imprimé en france, N° imprimeur 1513, avril 1980.*

[9] *JEROME.GENSEL, mathématiques pour l'informatique relations binaires, master ICA, Année 2007/2008.*

[10] *L.CHAMBADAL, P.ROSENSTIEHL, mathématiques1 éléments d'algébre, Paris 1969.*

[11] *LORENXO.RAMERO, GRIMOIRE d'algébre commutative, derière mise-à-jour 16 Novembere 2014.*

[12] *MC.GRAW-HILLINC, SEYMOUR.LIPSCHUTZ, Algébre lineare, cours et problemes, New york 1973.*

[13] *Mémoire l'anneaux des entiers d'un corps de nombre , université d'El-Oued Faculté des sciences et de technologie, juin 2014.*

[14] *Mémoire Introduction de théorie des groupes, université d'El-Oued Faculté des sciences et de technologie, juin 2013.*

[15] *M.MECHAB, Les cours d'algébre, Math1, LMD sciences et techniques.*

[16] *M.TEISSIER, Application de la théorie des anneaux à l'étude de demi-groupes, séminaire Dubreil algébe et théorie des nombres, tome4(1950-1951), exp.n°5, p.1-11.*

[17] *PIERRE.GUILLOT, cours concis de mathématiques.*

[18] *P.SAADE, Structures algebriques fondamentables(1) : Groupes, Anneaux, Corps, Année2005-2006.*

[19] *WWW.Les-Mathématiques.net*

Resumé

La théorie des anneaux est une partie très importante de la théorie des nombres, que les mathématiciens, se sont donnés à font, elle étudie plusieurs propriétés des ensembles, et leur groupes, les morphismes et les homomorphismes

Les mots clés

Ensemble, Opération interne, Relation, Image, Groupe, Morphisme, Homomorphisme, Anneau.

Abstract

The rings theory is a very important part of the numbers theory; mathematicians have studied many proprieties of the sets, and its groups, the morphismes and the homomorphismes

Keywords

Set, Operation, Relation, Image, Group, Morphisme, Homomorphisme, Ring.

ملخص

نظرية الحلقات هي جزء مهم في نظرية الأعداد. ندرس منها خصائص المجموعات، والزمر الناتجة عنها ، التشاكل و التماثل .

كلمات مفتاحية

المجموعة، العملية الداخلية، العلاقة، الصورة، الزمرة، التشاكل، التماثل، الحلقة.