# STRUCTURES ALGEBRIQUES GROUPES, ANNEAUX, CORPS & ARITHMETIQUE DANS $\mathbb{Z}$ et $\mathbb{R}[X]$

Adolphe CODJIA

25 Septembre 2018

# Table des matières

# Introduction

L'algèbre est la discipline mathématique qui sert à formuler des structures de données pour parler comme en science informatique. Une structure de données est constituée d'une déclaration d'ensembles, de description fonctionnelle liant ensembles et éléments, description axiomatique entre autre ; permettant de construire les théories et des **modèles abstraits** de la question qu'on veut étudier. Car de nos jours on peut dire que l'étude d'une question concrète est très avancée si on a réussi à poser cette question dans un langage formalisé en en construisant un modèle abstrait.Un modèle abstrait d'un phénomène ou d'une situation est une abstraction construite pour décrire, comprendre, expliquer, prévoir, voire gérer ou piloter ce phénomène ou cette situation.Un modèle est l'expression d'un problème sous la forme d'un ensemble de grandeurs numériques et / ou logiques ainsi que de relations qui permettent de calculer certaines de ces grandeurs les (resultats) à partir d'autres les (données). Ainsi l'abstraction que constitue un modèle est simplement une structure de données dite **STRUCTURE ALGEBRIQUE**. Il y a plusieurs types de structures algébriques comme exemples, on peut citer : les monoïdes, les groupes, les anneaux, les modules, les espaces vectoriels, les algèbres, les groupoïdes entre autres.

**L'ARITHMETIQUE** est la plus ancienne dicipline mathématique qui est partie du fait de savoir compter et a débouché sur l'étude des relations d'équivalence qui dans son approfondissement à donner une géométrie qui pourrait être qualifiée de géométrie arthmétique. Je parle ici de géométrie car qui parle d'algèbre lorgne la berge de la géométrie.

# Chapitre 1

# GROUPES

**Définiton**

Soit $G$ un ensemble quelconque non vide, on appelle une loi de **composition interne** "$*$" dans $G$ une application : $G \times G$ dans $G$ qui à $(a, b)$ associe $a * b$. On dit que $(G, *)$ est un **magma** i.e que $G$ est muni de la loi de composition interne "$*$".

**En pratique**

Généralement on prend "$*$" comme une somme "$+$" ou une multiplication "." ou "$\times$" et on note $a \times b = a.b = ab$ aussi.

**Définition**

$(G,.)$ est un **groupe** ssi

(i) $\forall a, b, c \in G,\ a.(b.c) = (a.b).c$ (associativité)

(ii) $\exists! e \in G;\ \forall a \in G,\ a.e = e.a = a$

($e$ est l'élément neutre de $G$)

(iii) $\forall a \in G,\ \exists! b \in G;\ a.b = b.a = e$

($b$ est le symétrique de $a$).

Si de plus : $\forall a, b \in G,\ ab = ba$, alors $(G,.)$ est un groupe **commutatif** ou **abélien**.

**Définiton**

On appelle **ordre** d'un groupe, le nombre de ses éléments.

Un groupe peut être d'ordre fini ou infini.

**Remarque**

1.$(G,.)$ est un semi-groupe ssi on a (i), donc un semi-groupe est un magma associatif.

2. $(G,.)$ est un monoïde ssi on a (i) et (ii),c'est donc un magma associatif et unitaire.

3. Tous les éléments d'un groupe $G$ sont réguliers cela signifie que(i.e) : $\forall a, b, c \in G,\ ab = ac \Rightarrow b = c$ aussi $bc = ac \Rightarrow b = a$.

**Exemples**

**1**. $(\mathbb{R}, +)$ est un groupe commutatif d'ordre infini

**2**. $(\mathbb{R}, \times)$ n'est pas un groupe car 0 n'a pas de symétrique.
Par contre $(\mathbb{R}^*, \times)$ est un groupe commutatif d'ordre infini

**3**. L'ensemble $G = \{e, a\}$ est un groupe d'ordre fini pour la table suivante dite table de **Cayley** ou de **Pythagore.**

| $\vec{\Gamma} *$ | $e$ | $a$ |
|---|---|---|
| $e$ | $e$ | $a$ |
| $a$ | $a$ | $e$ |

.

$(G, *)$ est un groupe d'ordre 2,
on note $cardG = |G| = o(G) = 2$.

**4**.$\forall n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \left\{\bar{0}, \bar{1}, \bar{2}, ..., \overline{(n-1)}\right\}$.
$(\mathbb{Z}_n, +)$ est un groupe abélien d'ordre $n$.

**5**. $\forall n \in \mathbb{N}^*$, $D_{2n} = (\mathbb{Z}_n, +) \times (\mathbb{Z}_2, +)$ est munit de la loi suivante :
$(a, b) * (a', b') = \left(a + (-1)^b a', b + b'\right)$ avec la convention que
$(-1)^b = 1$ si $b = \bar{0}$ sinon $(-1)^b = -1$. Montrer que $(D_{2n}, *)$ est un groupe.

Aussi les éléments de la forme $(a, \bar{1})$ sont d'ordre 2, ainsi que les couples $(a, \bar{0})$ pour $a$ vérifiant $2a = \bar{0}$, cela fait donc un élément supplémentaire lorsque $n$ est pair. Ces groupes s'appellent groupes diédraux (pluriel de diédral) et noté $D_{2n}$(car il contient $2n$ éléments).
Il a une présentation de la forme suivante :
$D_{2n} =< x, y \mid x^n = y^2 = e, yxy = x^{-1} >$, ou $e$ est élément neutre.
Le groupe des isométries qui conservent un polygône régulier à $n$ côtés est un groupe **isomorphe***(voir plus bas,définition)* au groupe diédral $D_{2n}$.
En effet, observons que le modèle des sommets d'un polygône convexe régulier à $n$ côtés est l'ensemble des racines $n^{ièmes}$ de l'unité, sur le cercle trigonométrque.
Un rotation $r$ conservera ce polygône si son centre $O$ est le centre du polynône, son angle est un multiple de $\dfrac{2\pi}{n}$. Le groupe des rotations est donc cyclique d'ordre $n$*(voir plus bas,définition)*, en composant avec la réflection $s$ d'axe fixe passant par le centre $O$, on obtient le groupe $D'_{2n} = \{e, r, r^2, ..., r^{n-1}, \sigma, r\sigma, r^2\sigma, ..., r^{n-1}\sigma\}$ qui es isomorphe au groupe diédral $D_{2n}$.

**6**. Soit $G_K =< x, y \mid x^2 = y^2 = xyx^{-1}y^{-1} = e >$ muni de la tabulation suivante :

| $\vec{\Gamma}$ . | $e$ | $x$ | $y$ | $xy$ |
|---|---|---|---|---|
| $e$ | $e$ | $x$ | $y$ | $xy$ |
| $x$ | $x$ | $e$ | $xy$ | $y$ |
| $y$ | $y$ | $xy$ | $e$ | $x$ |
| $xy$ | $xy$ | $y$ | $x$ | $e$ |

.

$(G_K\ ,.)$ est un groupe dit groupe de **Klein**.

**7**. $H_8\ =< a, b \mid a^4 = e,\ b^2 = a^2,\ ba = a^3b >$ est un groupe dit groupe **quaternionique.**

*Sa tabulation est la suivante :*

| $\vec{\Gamma}$ . | $e$ | $a$ | $a^2$ | $a^3$ | $b$ | $ab$ | $a^2b$ | $ba$ |
|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $a^2$ | $a^3$ | $b$ | $ab$ | $a^2b$ | $ba$ |
| $a$ | $a$ | $a^2$ | $a^3$ | $e$ | $ab$ | $a^2b$ | $ba$ | $b$ |
| $a^2$ | $a^2$ | $a^3$ | $e$ | $a$ | $a^2b$ | $ba$ | $b$ | $ab$ |
| $a^3$ | $a^3$ | $e$ | $a$ | $a^2$ | $ba$ | $b$ | $ab$ | $a^2b$ |
| $b$ | $b$ | $ba$ | $a^2b$ | $ab$ | $a^2$ | $a$ | $e$ | $a^3$ |
| $ab$ | $ab$ | $b$ | $ba$ | $a^2b$ | $a^3$ | $a^2$ | $a$ | $e$ |
| $a^2b$ | $a^2b$ | $ab$ | $b$ | $ba$ | $e$ | $a^3$ | $a^2$ | $a$ |
| $ba$ | $ba$ | $a^2b$ | $ab$ | $b$ | $a$ | $e$ | $a^3$ | $a^2$ |

**Définition**

On appelle **ordre** d'un élément $x$ d'un groupe $G$ le plus petit entier $n$ tel que $x^n = 1_G$ élément neutre de $G$. Si $n$ n'existe pas, on dit que $x$ est d'ordre infini.

Dans $H_8$ , il y a un élément d'ordre 1 : $e$ ; un élément d'ordre 2 : $a^2$ ; 6 éléments d'ordre 4 : $a$, $a^3$, $b$, $ab$, $a^2b$, $ba$.
Vu que $ab \neq ba$ $H_8$ n'est pas un groupe commutatif.

## 1.1 Sous-groupes d'un groupe

**Définition**

Une partie non vide $H$ d'un groupe $G$ est un sous-groupe de $(G, .)$ ssi $HH^{-1} \subset H$ c'est-à-dire :$\forall x,\ y \in H,\ xy^{-1} \in H$. On note $H < G$.

**Propriétés des sous-groupes**

a) Soit $(G, .)$ un groupe d'élément neutre $e$, tout sous-groupe de $(G, .)$ contient $e$.

b) Un sous-groupe $H$ de $(G, .)$ est un groupe pour l'opération induite sur $H$.

c) Pour toute famille $(H_i)_{i\in I}$ de sous-groupes de $(G, .)$, $\bigcap_{i\in I} H_i$ est un sous-groupe de $(G, .)$.

d) Le sous-groupe engendré par $A \subset G$, avec $A \neq \varnothing$ est l'intersection des sous-groupes de $(G,.)$ contenant $A$.

e) $(G,.)$ étant un groupe d'élément neutre $e$, $(G,.)$ et $\{e\}$ sont des sous-groupes triviaux(pluriel de trivial) de $(G,.)$

f) Un sous-groupe de $(\mathbb{Z},+)$ est toujours de la forme $(n\mathbb{Z},+)$, avec $n \in \mathbb{N}$(montrer cela).

**Définition**

On dit qu'un groupe est **monogène** s'il est engendré par une partie à un seul élément et qu'il est **cyclique** s'il est mongène et fini.

**Exemple**

1) $\forall n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \left\{\bar{0}, \bar{1}, \bar{2}, ..., \overline{(n-1)}\right\}$.

$(\mathbb{Z}_n,+) =< \bar{1} >$ est un groupe abélien cyclique d'ordre $n$.

2)Un groupe engendré par un seul élément $x$, se note $G =< x >$.

Multiplicativement si $G$ est infini, il est de la forme :

$G = \{..., x^{-1}, 1_G, x, x^2, ...\}$ ; sinon il est de la forme

$G = \{1_G, x, x^2, ...x^{n-1}\}$, donc d'ordre $n$.

## 1.2 Morphismes de magmas

**Définition**

Soient $(G,.)$ et $(G',*)$ deux magmas et $f$ une application de $G$ dans $G'$, $f$ est un morphisme de $(G,.)$ dans $(G',*)$ quand :

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

**Définitions-notations**

1) $Hom(G,G')$ est l'ensemble des morphismes de $(G,.)$ dans $(G',*)$.

2) Un isomorphisme est un morphisme bijectif. $G \cong G'$ exprime qu'il existe un isomorphisme de $(G,.)$ sur $(G',*)$.

3) Un endomorphisme est un morphisme d'un magma dans lui-même. $End(G)$ est l'ensemble des endomorphisme de $(G,.)$.

4) Un automorphisme est un endomorphisme bijectif. $Aut(G)$ est l'ensemble des automorphismes de $(G,.)$.

**Exemple**

Soit l'application $f : (\mathbb{R},+) \to (\mathbb{R}_*^+,\times)$, $x \mapsto f(x) = e^x$ est un isomorphisme de magmas.

### 1.2.1 Sous-groupes et morphismes

Soient $(G,.)$ et $(G',*)$ des groupes d'éléments neutres respectifs $e_1$ , $e_2$ et $f \in Hom(G,G')$.

1) $f(e_1) = e_2$ , $\forall x \in G$, $f(x^{-1}) = (f(x))^{-1}$.

2) Si $H$ est un sous-groupe de $(G,.)$, alors
$f(H)$ est un sous-groupe de $(G',*)$.
3) Si $H'$ est un sous-groupe de $(G',*)$,
alors $f^{-1}(H')$ est un sous-groupe de $(G,.)$.

### 1.2.2 Noyau et image

Soient $(G,.)$ et $(G',*)$ des groupes d'éléments neutres
respectifs $e_1$ , $e_2$ et $f \in Hom(G,G')$.
1) Le sous-groupe $f(G)$ de $(G',*)$ est l'**image** du morphisme $f$,
noté $\operatorname{Im} f$.
2) Le sous-groupe $f^{-1}(e_2)$ de $(G,.)$ est le **noyau** du morphisme $f$,
noté $\ker f$.
3) $f$ est injectif ssi $\ker f = \{e_1\}$.
4) $f$ est Surjectif ssi $\operatorname{Im} f = f(G) = G'$.

### 1.2.3 Composition de morphismes

1) $(G_1,.)$, $(G_2,*)$, $(G_3,\otimes)$ des groupes. Si $f \in Hom(G_1,G_2)$
et $g \in Hom(G_2,G_3)$ alors $g \circ f \in Hom(G_1,G_3)$.
2) Si $f \in aut(G_1)$ alors $f^{-1} \in aut(G_1)$.
**Proposition**
Soit $f$ un isomorphisme de magmas en $(G,T)$ et $(G',*)$, si l'un des magma est associatif, unitaire ou un groupe alors l'autre est aussi associatf, unitaire ou un groupe.

## 1.3 Groupe quotient d'un groupe

Soit $(G,.)$ un groupe, $H$ un sous-groupe de $G$. On définit sur $G$,
deux relations d'équivalence $\mathcal{R}_1$ et $\mathcal{R}_2$à l'aide de $H$ de la façon suivante :
Soient $x,y \in G$, $x\mathcal{R}_1 y \Longleftrightarrow x^{-1}y \in H$.
Soient $x,y \in G$, $x\mathcal{R}_2 y \Longleftrightarrow yx^{-1} \in H$.
**Définition**
Les ensembles quotient de ces relations d'équivalence se notent :
$\dfrac{G}{\mathcal{R}_1} = \left(\dfrac{G}{H}\right)_g = \{xH,\ x \in G\}$l'ensemble des classes
suivant $\mathcal{R}_1$, cet ensemble des classes est dit l'ensemble des **classes à gauche** suivant $H$, et **s'appelle** groupe quotient à gauche de $G$ par $H$.
Aussi, $\dfrac{G}{\mathcal{R}_2} = \left(\dfrac{G}{H}\right)_d = \{Hx,\ x \in G\}$l'ensemble des classes

suivant $\mathcal{R}_2$, cet ensemble des classes est dit l'ensemble des **classes à droite** suivant $H$. et **s'appelle** groupe quotient à droite de $G$ par $H$.
Pour tout $x \in G$.

**Attention :**

Groupe quotient à gauche(à droite) est **juste une appélation** cela ne signifie pas que c'est un groupe au sens de la structure.

**Définition**

L'ensemble $xH$ est appelé **Classe à gauche de** $x$ **modulo** $H$ et l'ensemble $Hx$ est appelé **Classe à droite de** $x$ **modulo** $H$.

**Remarque**

Si $G$ est un groupe commutatif, $\forall x \in G,\ xH = Hx$, pour tout sous-groupe $H$ de $G$.

**Définition**

Soit $(G, .)$ un groupe, $H$ un sous-groupe de $G$, on dit que
$H$ est **distingué**
ou **normal** dans $G$, lorsque $\forall x \in G$,
on a $Hx = xH \Longleftrightarrow x^{-1}Hx = H$, on note cela $H \triangle G$.

**Proposition**

$\forall x \in G,\ x^{-1}Hx = H \Longleftrightarrow x^{-1}Hx \subset H$.

Preuve

En effet soit $\forall x \in G,\ x^{-1}Hx \subset H$, alors $xHx^{-1} \subset H$ or
$H = (x^{-1}x)\, H\, (x^{-1}x) = x^{-1}\, (xHx^{-1})\, x \subset x^{-1}Hx$,
d'où $x^{-1}Hx = H$. Dans l'autre sens, c'est évident.

**Remarques**

1) Quand $H$ est distingué dans $G$, on parle simplement de
**classe suivant** $H$, car $\left(\frac{G}{H}\right)_d = \left(\frac{G}{H}\right)_g$.
Inversement $\left(\frac{G}{H}\right)_d = \left(\frac{G}{H}\right)_g \Rightarrow H$ est distingué dans $G$.

2) Un groupe qui possède un sous-groupe distingué n'est pas necessairement commutatif.

**Exemples**

1) Si $G$ est un groupe commutatif, tout sous-groupe est distingué
2) Les commutateurs d'un groupe $(G, .)$ sont les éléments de $(G, .)$ de la forme $xyx^{-1}y^{-1},\ \forall x, y \in G$.
$D(G) = < xyx^{-1}y^{-1} \mid x, y \in G >$ est un sous-groupe normal dans $G$, s'appelant le groupe **dérivé** de $G$, il mésure la commutativité du groupe.

**Proposition-définition**

Quand $H \triangle G$, sur $G/H$, on définit une loi de composition interne :

$\forall x,\, y \in G,\, (xH)\,.\,(yH) = (xy)\,H$
(i) Pour cette loi de composition, $(G/H,\ .)$ est un groupe.
(ii) L'application canonique $\varphi$ de $G$ dans $G/H$ est un homomorphisme.
$G/H$ est appelé **groupe quotient** de $G$ par $H$.

**Proposition**

Soit $f \in Hom\,(G, G')$, $\ker f \triangle G$.

Preuve

En effet, $\forall x \in \ker f$ et $\forall y \in G$, on a

$$f\,(y^{-1}xy) = f\,(y^{-1})\,f\,(x)\,f\,(y) = (f\,(y))^{-1}\,e_2\ f\,(y) = e_2\ ,$$

d'où $y^{-1}xy \in \ker f$.

**Proposition 1** *(de factorisation)*

Soit $f \in Hom\,(G, G')$, on a le diagramme commutatif suivant,
qui est la factorisation canonique de $f$.

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ p\downarrow & & \uparrow j \\ G/\ker f & \xrightarrow{\bar{f}} & f\,(G) \end{array} \quad .$$

$p$ est l'application canonique, $\bar{f}$ la bijection canonique et $j$ l'injection canonique. Alors $p$ et $j$ sont des homomorphismes et $\bar{f}$ est un isomorphisme du groupe quotient $G/\ker f$ sur le sous-groupe $f\,(G)$ et on a $f = j \circ \bar{f} \circ p$

**Définition**

Dire que $f \in Hom\,(G, G')$ est factorié, c'est dire que $f$ peut s'écrire comme composé d'autres applications.

**Définition**

$\forall x \in (G, .)$, l'application $i_x\ :\ \begin{array}{ccc} G & \longrightarrow & G \\ y & \longmapsto & xyx^{-1} \end{array}$ ,
est un automorphisme de $G$, dit automorphisme intérieur de $G$.
L'ensemble des automorphismes intérieurs de $G$ sera noté $Aut_{int}\ (G)$.

**Proposition**

Soit $(G, .)$ un groupe, $H$ un sous-groupe de $G$. Pour que $H$ soit distingué, il faut et il suffit que $H$ soit invariant par tout automorphisme intérieur de $G$.

Preuve

En effet $H$ distingué$\Longleftrightarrow xHx^{-1} = H,\, \forall x \in G \Longleftrightarrow i_x\ (H) = H,\, \forall x \in G$.

**Remarque**

Soit $N = \{x \in (G, .)\ \text{un groupe} \mid \forall y \in G,\ xy = yx\}$ c'est le centre de $(G, .)$ et c'est un sous-groupe distingué.

**Proposition**

On montre que $G/N$ est

isomorphe au groupe $A$ des automorphismes intérieurs de $G$.
Preuve

En effet : soit
$$f : \begin{array}{ccc} G & \longrightarrow & Aut_{int}\ (G) \\ y & \longmapsto & i_y \end{array}, \text{ on a}$$
$\ker f = \{x \in G;\ i_x\ = id_G\ \} = N$, et $f\,(G) = A = Aut_{int}\ (G)$,
d'après le théorème de la factorisation, on a $G/N \cong f\,(G) = A$.

**Proposition 2** *(premier théorème d'isomorphisme)*

$\forall f \in Hom\,(G, G')$, on a $(G/\ker f) \cong \operatorname{Im} f$.
**Corollaire** (deuxième théorème d'isomorphisme)
$H$ et $K$ sont deux sous-groupes de $(G, .)$ un groupe.
On suppose que $K \triangle H$, alors $(H \cap K) \triangle H$ et $(H/(H \cap K)) \cong HK/K$
*Preuve*
Rappelons que le groupe engendré par $H$ et $K$ est alors $HK$ puisque $K$ est distingué dans $H$. De plus $K$ est distingué dans $HK$,
car il est distingué dans le groupe $H$.
Considérons alors la restriction à $H$ de la projection de $HK$ sur $(HK/K)$ :
$$\phi : \begin{array}{ccc} H & \longrightarrow & (HK/K) \\ h & \longmapsto & hK \end{array}, \text{ alors } \phi \text{ est surjectif,}$$
car pour tout $hkK \in (HK/K)$, on a $hkK = hK = \phi\,(h)$.
Son noyau est défini par :
$\ker \phi = \{h \in H \mid hK = K\} = \{h \in H \mid h \in K\} = H \cap K$,
ainsi on a bien $(H \cap K) \triangle H$, et le premier théorème d'isomorphisme
donne alors $(H/(H \cap K)) \cong (HK/K)$.
**Corollaire**(troisième théorème d'isomorphisme)
$H$ et $K$ sont deux sous-groupes distingués dans $(G, .)$.
On suppose que $K \subset H$, alors $(H/K) \triangle (G/K)$ et
$(G/K)/(H/K) \cong (G/H)$.
*Preuve*
Soit $p$ la projection de $G$ sur $(G/H)$. Comme $K < H = \ker p$,
Considerons
$$\bar{p} : \begin{array}{ccc} G/K & \longrightarrow & G/H \\ gK & \longmapsto & gH \end{array}. \ \bar{p} \text{ est surjectif, car } p \text{ est surjectif.}$$
Enfin $\ker(\bar{p}) = \{gK \mid gH = H\} = \{gK \mid g \in H\} = (H/K)$.
de là $(H/K) \triangle (G/K)$ et d'après le premier théorème d'isomorphisme,
on a $(G/K)/(H/K) \cong (G/H)$.
**Exemple d'application**
$(\mathbb{Z}//12\mathbb{Z})/(3\mathbb{Z}/12\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z})$.

## 1.4 Groupes finis

Si $(G,.)$ est un groupe fini dont le cardinal est égal à $n$, on a $[G] = card\,(G)$. Quand on a un groupe quotient $(G/H)$ dans $G$.

**Définiton**

le cardinal de $(G/H)$ s'appelle **indice** de $H$ dans $G$ et se note $[G:H]$.

**Thèorème**(de Lagrange)

Si $(G,.)$ est un groupe fini et $H$ un sous-groupe de $G$, on a $[G] = [G:H] \times [H]$.

*Preuve*

Considérons par exemple l'ensemble $(G/H)_d$ , si $X \in (G/H)_d$ et $x \in X$, l'application $\varphi : h \longmapsto hx$ de $H$ dans $G$, a son image contenue dans $X$ et est injective. De plus, si $x' \in X$, on a $x'x^{-1} \in H$ donc il existe $h \in H$ tel que $x' = hx = \varphi\,(h)$, donc $\varphi$ est une bijection de $H$ sur $X$ (ceci ne depend pas du fait que $G$ soit fini).

Il en résulte que toutes les classes à droites ont le même nombre d'éléments, égal à $[H]$, et comme on sait que $G$ est réunion disjointe de classes à droite en ce qui nous concerne et qu'il y a $[G:H]$ de classes à droite alors, on a bien : $[G] = [G:H] \times [H]$.

**Conséquences immédiates**

1) Si $H$ est un sous-groupe de $(G,.)$ et $K$ un sous-groupe de $H$, on a : $[G:K] = [G:H] \times [H:K]$.

2) Si $(G,.)$ est un groupe fini et si $x \in G$, l'ordre de $x$ divise $[G]$. En particulier si $n = [G]$, on a : $x^n = 1_G$ (élément neutre de $G$).

## 1.5 Groupe $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$

Pour $n \geq 2$, on note $\varphi\,(n)$ le cardinal de l'ensemble des entiers $k$ tel que $0 \leq k \leq n-1$ et $n \wedge k = p\gcd\,(n,k) = 1$. On convient que $\varphi\,(1) = 1$.

**Définition**

La fonction $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ ainsi définie est appelée la **fonction d'Euler**.

**Proposition**

Soient $(G,.)$ un groupe cyclique d'ordre $n$ et $a$ un générateur de $G$. Pour tout $k \in \mathbb{N}^*$, l'ordre de $a^k$ est $o\left(a^k\right) = \dfrac{n}{n \wedge k}$ où $n \wedge k = p\gcd\,(n,k)$.

En particulier, $a^k$ est un générateur de $G$ si et seulement si $n \wedge k = p\gcd\,(n,k) = 1$. Il existe $\varphi\,(n)$ générateurs distincts dans $G$.

*Preuve*

Soit $k \in \mathbb{N}^*$, posons $d = n \wedge k = p\gcd\,(n,k) \in \mathbb{N}^*$, on a $n = dn'$,

$k = dk'$, avec $n' \wedge k' = p\gcd(n', k') = 1$.
$\forall m \in \mathbb{N};\ \left(a^k\right)^m = a^{km} = 1_G \iff n$ divise $km \iff dn'$
divise $dk'm \iff n'$ divise $k'm \iff n'$ divise $m$
car $n' \wedge k' = p\gcd(n', k') = 1$.
Ainsi $n'$ est le plus petit entier non nul tel que $\left(a^k\right)^{n'} = 1_G$ .
On a donc $n' = o\left(a^k\right) = \dfrac{n}{n \wedge k}$.

**Proposition**
Le nombre de générateurs distincts du groupe cyclique $G = (a)$ d'ordre $n$ est exactement $\varphi(n)$, où $\varphi$ est la fonction d'Euler.

**Lemme**
Soient $(G, .)$ un groupe cyclique d'ordre $n$ et $a$ un générateur de $G$.
L'homomorphisme $k \longmapsto a^k$ de $\mathbb{Z}$ dans $G$ se factorise et définit un isomorphisme
$\alpha_a\ : \bar{k} \longmapsto a^k$, où $0 \leq k \leq n-1$ du groupe $(\mathbb{Z}/n\mathbb{Z})$ sur $G$.
*Preuve*
Soit : $\alpha : \mathbb{Z} \longrightarrow G,\ \ k \longmapsto a^k$, c'est un morphisme surjectf de groupes où $\ker\alpha = \left\{k \in \mathbb{Z},\ a^k = 1_G\right\} = n\mathbb{Z}$, d'après le premier théorème d'isomorphisme, on a bien : $(\mathbb{Z}/n\mathbb{Z}) \cong G$.

**Proposition**
Le sous groupe $\left(a^k\right) \subset (a)$ d'ordre $n$, $1 \leq k \leq n$, coincide avec le sous-groupe $\left(a^d\right)$ où $d = p\gcd(k, n)$.
*Preuve*
Posons, $k = k'd$,
on a $a^k = a^{k'd} = \left[a^d\right]^{k'} \in \left(a^d\right) \Rightarrow \left(a^k\right) \subset \left(a^d\right)$.
D'après la relation de Bézout : $d = \alpha n + \beta k$, et on a :
$a^d = a^{\alpha n+\beta k} = a^{\alpha n}.a^{\beta k} = a^{\beta k} \in \left(a^k\right) \Rightarrow \left(a^d\right) \subset \left(a^k\right)$,
d'où, on a bien $\left(a^k\right) = \left(a^d\right)$.

**Proposition**
Soient $(G, .)$ un groupe cyclique d'ordre $n$ et $a$ un générateur de $G$.
(i) Soit $f$ un homomorphisme surjectif de $G$ sur un groupe $(G', .)$.
Alors $G'$ est cyclique, $a' = f(a)$ engendre $G'$ et l'ordre de $G'$ :
$n'$ divise $n$.
En particulier, tout groupe quotient de $G$ est un groupe cyclique.
(ii) Soit $G'$ un groupe cyclique dont l'ordre $n'$ divise $n$. Soit $a' \in G'$,
il existe un unique homomorphisme $f$ de $G$ dans $G'$ tel que $f(a) = a'$.
pour que $f$ soit surjectif, il faut et il suffit que $a'$ soit un générateur de $G'$.
*Preuve*
(i) Puisse que $f$ est surjectif, pour tout $y \in G'$, il existe $x \in G$ tel que $f(x) = y$, puis il existe $k \in \{0, 1, ..., n-1\}$ tel que $x = a^k$.

On a $f\left(a^k\right) = (f(a))^k$. Donc $f(a)$ engendre $G'$. De plus l'ordre de $G'$ :
$n'$ divise $n$ car $(f(a))^n = 1_{G'}$ .
*Comme on sait qu'il y a un morphisme surjectif canonique entre $G$ et tout groupe quotient de $G$, d'après ce qui précède, un groupe quotient de $G$ est forcément cyclique.*
(ii) D'après le théorème de Lagrange, $m = o(a')$ divise $n'$ et $n'$ divise $n$, donc $m$ divise $n$ et on a $n\mathbb{Z} \subset m\mathbb{Z}$.

L'homomorphisme canonique $k \longmapsto a'^k$
de $\mathbb{Z}$ dans $< a' >$ a pour noyau $m\mathbb{Z}$. Il se factorise à travers $n\mathbb{Z}$ et définit un homomorphisme $\beta$ de $(\mathbb{Z}/n\mathbb{Z}) \longrightarrow < a' >$ tel que $\beta\left(\bar{k}\right) = a'^k$
pour tout $\bar{k} \in (\mathbb{Z}/n\mathbb{Z})$.
Soit $\alpha_a$ l'isomomorphisme de $(\mathbb{Z}/n\mathbb{Z})$ sur $G$ donné par le lemme ci-dessus.
Alors $f = \beta \circ \alpha_a^{-1} : G \longrightarrow (\mathbb{Z}/n\mathbb{Z}) \longrightarrow < a' >$ est tel que $f(a) = \beta \circ \alpha_a^{-1}(a) = \beta(\bar{1}) = a'$. Il est unique car la donnée de $f(a) = a' \Rightarrow f\left(a^k\right) = a'^k,\ \forall k \in \mathbb{Z}$. Pour que $f$ soit surjectif il faut et il suffit que $a'$ engendre $G'$ car $\operatorname{Im} f = \operatorname{Im} \beta = < a' >$.

**Proposition**
On a exactement $\varphi(k)$ homomorphismes de $G$ dans $G'$ dont l'image est d'ordre $k$. et $card(Hom(G, G')) = p \gcd(n, n')$,
où $n$ =ordre de $G$ et $n'$ =ordre de $G'$.

## 1.6 Groupes symétriques

Soit $n \geq 1$, $E_n = \{1, 2, ..., n\}$.

**Définition**

On appelle permutation de $E_n$ toute application bijective

$$\sigma : E_n \longrightarrow E_n .$$

On note $\mathcal{S}_n$ l'ensemble des permutations de $E_n$.

**Proposition**

$(\mathcal{S}_n , \circ)$ est un groupe appelé **groupe symétrique**

$\mathcal{S}_n$ est fini et comprend $n!$ éléments.

**Ecrture pratique**

Si $\sigma \in \mathcal{S}_n$, on écrit :

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}.$$

**Exemple**

$n = 3$. $\quad |\mathcal{S}_3| = 3! = 6$.

$$id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}; \ \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \ \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

La table de $(\mathcal{S}_3 , \circ)$ est la suivante :

| $\curvearrowright \circ$ | $id$ | $\tau_1$ | $\tau_2$ | $\tau_3$ | $\sigma_1$ | $\sigma_2$ |
|---|---|---|---|---|---|---|
| $id$ | $id$ | $\tau_1$ | $\tau_2$ | $\tau_3$ | $\sigma_1$ | $\sigma_2$ |
| $\tau_1$ | $\tau_1$ | $id$ | $\sigma_1$ | $\sigma_2$ | $\tau_2$ | $\tau_3$ |
| $\tau_2$ | $\tau_2$ | $\sigma_2$ | $id$ | $\sigma_1$ | $\tau_3$ | $\tau_1$ |
| $\tau_3$ | $\tau_3$ | $\sigma_1$ | $\sigma_2$ | $id$ | $\tau_1$ | $\tau_2$ |
| $\sigma_1$ | $\sigma_1$ | $\tau_3$ | $\tau_1$ | $\tau_2$ | $\sigma_2$ | $id$ |
| $\sigma_2$ | $\sigma_2$ | $\tau_2$ | $\tau_3$ | $\tau_1$ | $id$ | $\sigma_1$ |

ceci est à vérifier.

**Exercice 1. pratique**

On considère les sous-ensembles de $\mathcal{S}_3$ suivants : $K = \{id, \tau_1\}$, $H = \{id, \sigma_1 , \sigma_2\}$.

1. Montrer que $K$ et $H$ sont des sous-groupes de $\mathcal{S}_3$.
2. Déterminer les classes d'équivalence suivant $K$ et $H$ respectivement.
3. Montrer que le sous-groupe $H$ est distingué, et que $K$ n'est pas distingué.
4. Ecrire la table des groupes quotients $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$ et $\dfrac{\mathcal{S}_3}{H}$.

**Exercice 2. pratique**

Soient $A = \{1, 2, 3\}$ et $\mathcal{P}(A)$ l'ensemble des parties de $A$.

1. Montrer que $(\mathcal{P}(A), \triangle)$ est un groupe commutatif où $\triangle$ est la différence symétrique.
2. Quels sont les cardinaux possibles des sous-groupes de $(\mathcal{P}(A), \triangle)$.
3. Montrer que $H = \{\varnothing, A\}$ est un sous-groupe de $(\mathcal{P}(A), \triangle)$.
4. Déterminer le groupe quotient de $\dfrac{\mathcal{P}(A)}{H}$, puis la table de sa loi quotient.

**Décomposition en cycles**

**Définition**

On appelle $r$-cycle, où $r \in \{2, 3, ..., n\}$, une permutation $c$ telle qu'il existe $\begin{pmatrix} i_1 & i_2 & ... & i_r \end{pmatrix}$ entiers distincts pris dans $\{1, 2, 3, ..., n\}$ et tels que $c(i_1) = i_2$, $c(i_2) = i_3$, $c(i_3) = i_4$, ... ,$c(i_r) = i_1$.
Tous les autres éléments étant invariants. Le $r$-cycle est noté $\begin{pmatrix} i_1 & i_2 & ... & i_r \end{pmatrix}$ et s'appelle une permutation circulaire.

**Définition**

Un $r$-cycle $c$ est d'ordre $r$, cela signifie que $c^r = id_{E_n}$ .
On appelle support du $r$-cycle $c$ l'ensemble des entiers $\{i_1, i_2, ..., i_r\}$=supp$(c)$ et l'ordre de $c = Card\,(supp(c))$.

**Proposition**

Deux cycles ayant des supports disjoints commutent.

Preuve

En effet, il suffit de se souvenir que tout cycle laisse invariant un entier qui n'est pas dans son support. La réciproque est fausse(dans $S_3$ , supp$(\sigma_1)$=supp$(\sigma_2)$ et pourtant, $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$ )

**Proposition**

Toute permutation est composée de façon unique de cycles de supports disjoints.

Preuve

On conviendra que l'identité est composée de $0-$cycle.
En effet, soit $\sigma$ une permutation, on cherche l'image de 1 s'il n'est pas fixe, on cherche l'image de cette image jusqu'à retrouver 1, cela donne un premier cycle. Puis on prend le plus petit entier qui n'est pas dans le support du premier cycle et on procède comme pour le 1, cela donne un nouveau cycle de support disjoint du premier et ainsi de suite. L'unicité resulte de ce que les supports des cycles sont entièrementt déterminés par $\sigma$.

**Définition**

On appelle **décomposition canonique** de $\sigma$ une permutation, la décomposition de $\sigma$ en un produit de cycles de supports disjoints.

**Définition**

Soit $\sigma \in S_n$ avec $\sigma = c_1\ c_2\ ...c_k$ décomposition canonique de $\sigma$.
L'**ordre** de $\sigma$ est égal au $PPCM$ des ordres de $c_1$ , $c_2$ , . . ., $c_k$ .

**Exemples**

$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 3 & 1 & 2 & 4 & 7 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 2 & 6 & 4 \end{pmatrix}$,

$\sigma_1$ est un cycle. supp($\sigma_1$)= $\{1, 5, 2, 6, 4\}$.

$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 3 & 8 & 7 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 6 & 4 & 8 \end{pmatrix} \begin{pmatrix} 2 & 5 & 7 \end{pmatrix}$,

$\sigma_2$ n'est pas un cycle, mais décomposée en produit de cycles

L'ordre de $\sigma_1 = 5 = o(\sigma_1)$ et l'ordre de $\sigma_2 = PPCM(4, 3) = 12$.

**Définition**

Soit $\sigma \in S_n$ et $i \in E_n$ . On appelle $\sigma$-orbite de $i \in E_n$ et on note $\Omega_\sigma(i) = \left\{\sigma^k(i),\ k \in \mathbb{N}\right\}$, $\Omega_\sigma(i)$ est un ensemble fini. Si $i$ n'appartient pas au support de $\sigma$, $\Omega_\sigma(i) = \{i\}$ dit ponctuelle.

**Définition**

Soient $n \geq 2$, $E_n = \{1, 2, ..., n\}$.

On appelle transposition toute permutation qui échange 2 éléments $i$ et $j$ et laisse invariante les $(n-2)$ autres.

Si $i$ et $j$ sont les éléments échangés , on note :

$\tau_{ij} = \begin{pmatrix} 1 & ... & i-1 & i & i+1 & ... & j-1 & j & j+1 & ... & n \\ 1 & ... & i-1 & j & i+1 & ... & j-1 & i & j+1 & ... & n \end{pmatrix}$.

**Proposition**

Il y a $\dfrac{n(n-1)}{2}$ transpositions et

$\tau_{ij}^2 = \tau_{ij} \circ \tau_{ij} = id \Longleftrightarrow \tau_{ij}^{-1} = \tau_{ij}$ .

**Définition**

Toute permutation est produit d'un nombre fini de transpositions.

Mais ce produit n'est pas unique.

**Définition**

On dit que $\sigma$ et $\sigma'$ sont **conjuguées** s'il existe une permutation $\varphi$ telle que $\sigma' = \varphi \circ \sigma \circ \varphi^{-1}$.

### 1.6.1 Inversions

**Définition**

Soient $i \neq j$ deux éléments de $E_n = \{1, 2, ..., n\}$ . et soit $\sigma \in \mathcal{S}_n$ .

On dit que $\sigma$ présente une inversion en $\{i, j\}$ si $\dfrac{\sigma(j) - \sigma(i)}{j - i} < 0$.

**Définition**

Notons $\mathcal{V}_\sigma$ le nombre de parties $\{i, j\}$ de $E_n$ où $\sigma$ présente une inversion.

Soit $\varepsilon_\sigma = (-1)^{\mathcal{V}_\sigma}$ , $\varepsilon_\sigma$ est la **signature** de la permutation $\sigma$.

$\sigma$ est dite paire si $\mathcal{V}_\sigma$ est pair c'est-à-dire $\varepsilon_\sigma = 1$.

$\sigma$ est dite impaire si $\mathcal{V}_\sigma$ est impair c'est-à-dire $\varepsilon_\sigma = -1$.

**Exemple**

On vérifie dans $\mathcal{S}_3$ ,

$id$, $\sigma_1$ , $\sigma_2$ sont paires et $\tau_1$ , $\tau_2$ , $\tau_3$ sont impaires.

**Propriétés**

$\forall \sigma, \sigma' \in \mathcal{S}_n$ , on a $\varepsilon_{\sigma\circ\sigma'} = \varepsilon_\sigma \times \varepsilon_{\sigma'}$ .

Soit $\theta : (\mathcal{S}_n , \circ) \longrightarrow (\{-1, 1\} , \times)$

$$\sigma \longmapsto \theta(\sigma) = \varepsilon_\sigma .$$

$\theta$ est un morphisme de groupes i.e.

$$\theta(\sigma \circ \sigma') = \varepsilon_{\sigma\circ\sigma'} = \varepsilon_\sigma \times \varepsilon_{\sigma'} = \theta(\sigma) \times \theta(\sigma').$$

**Remarque**

$\ker\theta = \{\sigma \in \mathcal{S}_n / \ \theta(\sigma) = 1\} = \{\text{permutations paires}\}$.

$= $ Le groupe alterné noté $\mathcal{A}_n$.

$\ker\theta \lhd \mathcal{S}_n$ ($\ker\theta$ est un sous-groupe distingué de $\mathcal{S}_n$ ).

$$\left|\frac{\mathcal{S}_n}{\mathcal{A}_n}\right| = \frac{|\mathcal{S}_n|}{|\mathcal{A}_n|} = \frac{n!}{|\mathcal{A}_n|} = card\{-1, 1\} = 2 \Rightarrow |\mathcal{A}_n| = \frac{n!}{2}$$

**Conséquence**

$\theta : (\mathcal{S}_n , \circ) \longrightarrow (\{-1, 1\} , \times)$

$$\sigma \longmapsto \theta(\sigma) = \varepsilon_\sigma .$$

$\varepsilon_{\sigma^{-1}} = \theta(\sigma^{-1}) = (\theta(\sigma))^{-1} = (\varepsilon_\sigma)^{-1} = \varepsilon_\sigma$ .

**Proposition**

$A_n$ est engendré par les 3-cycles pour $n \geq 3$.

Preuve

Les 3-cycles et leurs composée sont des permutations paires,
car un $r$-cycle est de signature $(-1)^{r-1}$. Réciproquement
on a $(a, b)(b, c) = (a, b, c)$ , $(a, b)(c, d) = (a, c, b)(a, c, d)$.
Ceci prouve que toute composée d'un nombre paire de transposition
est aussi composée de 3-cycles.

## 1.7 Groupes opérant sur un ensemble

**Définition**
Soit $(G,.)$ un groupe, $X$ un ensemble, $S(X)$ le groupe des permutations de $X$. On dit que $(G,.)$ opère dans $X$ lorsqu'il est défini un morphisme de $G$ vers $S(X)$ : $g \mapsto \varphi_g$ . Ainsi, on a les relations suivantes :
a) $\forall x \in X$, $\forall g,\ g' \in (G,.)$, $\varphi_{gg'}(x) = \varphi_g \circ \varphi_{g'}(x)$.
b) $\forall g \in (G,.)$, $\left(\varphi_g\right)^{-1} = \varphi_{g^{-1}}$ .
Lorsque le morphime est injectif, on dit que $G$ opère **fidèlement** dans $X$
**Exemple**
Soit $(G,.)$ un groupe, $H$ un sous-groupe de $(G,.)$, $X = (G/H)_g$ ;
$\forall g, x \in (G,.)$, posons $\varphi_g\ (xH) = gxH$, alors $G$ opère ainsi sur $X$.
**Définition**
On pose $\forall x \in X$, $N(x) = \left\{g \in (G,.) \mid \varphi_g\ (x) = x\right\}$ est appelé **stabilisateur** de $x$, c'est un sous-groupe de $(G,.)$.
**Définition**
$\Omega(x) = \left\{\varphi_g(x),\ g \in (G,.)\right\}$ est l'**orbite** de $x$.
**Proposition**
La relation $\forall x,\ y \in X$, $y \in \Omega(x)$ est une relation d'équivalence.
Ainsi les orbites forment un partition de $X$.
**Remarque**
Lorsque $X$ est formé d'une seule orbite, on dit que $(G,.)$ opère **transitivement** sur $X$.
**Proposition**
Soit $(G,.)$ un groupe opérant sur l'ensemble $X$ ; soit $x \in X$,
alors il y a une bijection entre l'orbite $\Omega(x)$ de $x$ et $(G/N(x))_g$ .
*Preuve*
En effet, pour $g,\ g' \in (G,.)$, $g^{-1}g' \in N(x) \Longleftrightarrow \varphi_{g^{-1}g'}(x) = x$
$\Longleftrightarrow \varphi_{g^{-1}} \circ \varphi_{g'}(x) = x \Longleftrightarrow \left(\varphi_g\right)^{-1} \circ \varphi_{g'}(x) = x$
$\Longleftrightarrow \varphi_{g'}(x) = \varphi_g\ (x)$.
A tout $y \in \Omega(x)$, il existe un $g \in (G,.)$ tel que $y = \varphi_g\ (x)$
on a l'ensemble $A$ des $g'$ de $(G,.)$ tel que
$\varphi_{g'}(x) = y = \varphi_g\ (x) \Longleftrightarrow g^{-1}g' \in N(x) \Longleftrightarrow g' \in gN(x)$.
Il est alors clair que $A = gN(x)$.
Dès lors, on a la bijection bien définie :
$\varphi_g\ (x) \longmapsto gN(x)$ de $\Omega(x)$ de $x$ sur $(G/N(x))_g$ .

# Chapitre 2

# STRUCTURE D'ANNEAU

**Définition**
On appelle **anneau**, un ensemble $E$ non vide muni de deux lois de compositions **internes** $(E, \heartsuit, \clubsuit)$, satisfaisant aux axiomes suivants :
(i) $(E, \heartsuit)$ est un groupe abélien ;
(ii) La deuxième loi $\clubsuit$ étant **associative** et **distributive** par rapport à la première loi $\heartsuit$ i.e.

- $\forall x, y, z \in E,\ (x \clubsuit y) \clubsuit z = x \clubsuit (y \clubsuit z)$ (associativité de $\clubsuit$)
- $\left.\begin{array}{l} x \clubsuit (y \heartsuit z) = (x \clubsuit y) \heartsuit (x \clubsuit z) \text{ ceci est la distributivité à gauche} \\ (y \heartsuit z) \clubsuit x = (y \clubsuit x) \heartsuit (z \clubsuit x) \text{ ceci est la distributivité à droite} \end{array}\right\}$

Ceci est la distributivité de $\clubsuit$ par rapport à $\heartsuit$= la distributivité à gauche et la distributivité à droite.
On dit que l'anneau est **commutatif** si la deuxième loi $\clubsuit$ est commutative.
On dit que l'anneau est **unitaire** si la deuxième loi $\clubsuit$ admet un élément neutre celui-ci est appelé élément **unité** de $E$, et souvent noté 1.

**Exemple**
$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munis de l'addition et de la multiplication ordinaires sont des anneaux commutatifs et unitaires.

### 2.0.1 Règles de calculs dans un anneau

soit $(E, +, \times)$ un anneau. Toutes les règles de calculs valables dans un groupe abélien s'appliquent au groupe additif de $E$, e.i.$(E, +)$.
1. $\forall x \in E$, $x \times 0 = 0 \times x = 0$, 0 est l'élément neutre de la première loi de l'anneau $E$, il est donc l'élément absorbant de la deuxième loi de l'anneau(en claire $\forall x \in E$, $x \times 1_{\heartsuit} = 1_{\heartsuit} \times x = 1_{\heartsuit}$,

$1_\heartsuit$ est l'élément neutre de la première loi $\heartsuit$de l'anneau $(E, \heartsuit, \clubsuit)$,
il est donc l'élément absorbant de la deuxième loi $\clubsuit$de l'anneau $(E, \heartsuit, \clubsuit)$).
**2**. $\forall x, y \in E$, $x \times (-y) = (-x) \times y = -xy$ (en clair,
$x \clubsuit (symét_\heartsuit (y)) = (symét_\heartsuit (x)) \clubsuit y = (symét_\heartsuit (x \clubsuit y))$.
où $(symét_\heartsuit (y))$ est le symétrique de $y$ par rapport à la
première loi $\heartsuit$ qui fait de $(E, \heartsuit)$, un groupe).
**3**. $\forall x, y \in E$,$(-x) \times (-y) = -(-x) y = -(-xy) = xy$ (en clair,
$symét_\heartsuit (x) \clubsuit (symét_\heartsuit (y)) = symét_\heartsuit ((symét_\heartsuit (x)) \clubsuit y)$
$= symét_\heartsuit (symét_\heartsuit (x \clubsuit y)) = x \clubsuit y)$.
**4**. $\forall x \in E \backslash \{0\}$, $x^0 = 1$ ( dans la suite $\cdot = \times$)
$x^n = x^{n-1} x$, $n \geq 1$, $n \in \mathbb{N}$,
$nx = (n-1) x + x = (n.1) x = x (n.1)$
$(m, n) \in \mathbb{N} \times \mathbb{N}$, $x^n x^m = x^{n+m}$ ; $(n+m) x = nx + mx$.
**5**. Formule du binôme de Newton
$\forall a, b \in E$, commutant(permutant) e.i. $a \times b = b \times a$ ;

$$(a+b)^n = \sum_{k=0}^{n} \mathbb{C}_n^k a^{n-k} b^k \text{ ; } n \geq 1,\ n \in \mathbb{N},\ \mathbb{C}_n^k = \frac{n!}{k!\,(n-k)!}.$$

## 2.1 Sous-anneau

**Définition**
Soit $(E, \heartsuit, \clubsuit)$ un anneau et $F$ une partie non vide de $E$.
On dit que $F$ est un **sous-anneau** de $E$ si $F$ est stable pour les deux lois de $E$ et si munie des lois de composition induites par celles de $E$, $(F, \heartsuit, \clubsuit)$ est un anneau.
**En pratique**
Pour que $F$ soit un sous-anneau de $E$ il faut et il
suffit que $F$ soit une partie non vide de $E$ et tout couple $(x, y)$
d'éléments de $F$, on a :
$x \heartsuit (symét_\heartsuit (y))$ et $x \clubsuit y$ sont des éléments de $F$.

## 2.2 Morphisme d'anneaux

**Définition**
Soient $(E, \heartsuit, \clubsuit)$ et $(A, +, \times)$ deux anneaux. Un **morphisme d'anneaux** $f$ de $E$ dans $A$ est une application de $E$ dans $A$ telle que :
$\forall x, y \in E$, $f(x \heartsuit y) = f(x) + f(y)$ et $f(x \clubsuit y) = f(x) \times f(y)$.
**Propriétés**

Si $f$ est un morphisme d'anneaux on a :
(i) $f(e_{\heartsuit}) = e_{+}$
($e_{\heartsuit}$ est l'élément neutre de $\heartsuit$, $e_{+}$ est l'élément neutre de $+$)
(ii) Si $B$ est un sous-anneau de $E$, $f(B)$ est un sous-anneau de $A$.
(iii) Si $B'$ est un sous-anneau de $A$, $f^{-1}(B')$ est un sous-anneau de $E$.

## 2.3 Idéal d'un anneau commutatif

**Définition**
Soit $(E, \heartsuit, \clubsuit)$ un anneau et $I$ une partie non vide de $E$.
On dit que $I$ est un **idéal** de $E$ si $I$ est un sous-groupe de $(E, \heartsuit)$ tel que $\forall x \in E$ ,$\forall y \in I$, $x \clubsuit y \in I$.
**Exemple**
Etant donnée Si $f$ est un morphisme d'anneaux de $(E, \heartsuit, \clubsuit)$ dans $(A, +, \times)$, $\ker f$ est un idéal de $(E, \heartsuit, \clubsuit)$.
Je rappelle que $\ker f = \{x \in E,\ f(x) = 1_{+}\}$.
**Exercice 1**
Montrer que le noyau d'un morphisme d'anneaux est un idéal.
*Proposition de réponse*
*Soit* $f : (E, \heartsuit, \clubsuit) \to (A, +, \times)$ *un morphisme d'anneaux,*
$\ker f = \{x \in E,\ f(x) = 1_{+}\}$, $\forall x \in (E, \heartsuit, \clubsuit)$,
$\forall y \in \ker f$, *évaluons* $f(x \clubsuit y) = f(x) \times f(y) = f(x) \times 1_{+} = 1_{+}$
*donc* $x \clubsuit y \in \ker f$. *CQFD*
**Proposition**
Soit $f : (E, \heartsuit, \clubsuit) \to (A, +, \times)$ un morphisme d'anneaux. Alors
1. $I$ idéal de $E$ implique$f(I)$ idéal de $Im(f)$,
2. $J$ idéal de $A$ implique $f^{-1}(J)$ est un idéal de $E$.

## 2.4 Anneau quotient

**Définition**
Soit un anneau $(A, \heartsuit, \clubsuit)$ muni d'une relation d'équivalence $\rho$ compatibles avec les deux lois de l'anneau(i.e. $a, b, c, d \in A$, avec $a \rho\ b$ et $c \rho\ d$ alors $(a \heartsuit c)\, \rho\, (b \heartsuit d)$ et $(a \clubsuit c)\, \rho\, (b \clubsuit d)$). L'ensemble quotient, muni des deux lois est un anneau noté $\dfrac{A}{\rho}$ qu'on appelle anneau **quotient**.
Si $A$ est unitaire(commutatif), $\dfrac{A}{\rho}$ est unitaire(commutatif).
**Proposition**
Etant donné un anneau commutatif $(E, \heartsuit, \clubsuit)$ et un de ses idéaux $I$.

Il existe une relation d'équivalence $\rho$ sur $E$ compatible avec les lois de composition : "$\heartsuit, \clubsuit$" qui est définie comme suit :
Pour $x$, $y \in E$, $x\rho y \Leftrightarrow y \heartsuit sym\acute{e}t_{\heartsuit}(x) \in I$. De là l'anneau quotient $\left(\frac{E}{\rho}, \heartsuit, \clubsuit\right)$ est noté : $\left(\frac{E}{I}, \heartsuit, \clubsuit\right)$ et c'est un anneau quotient commutatif.

**Exemple**

$(\mathbb{Z}, +, \times)$ est un anneau commutatif et soit $n\mathbb{Z}$ un idéal de $(\mathbb{Z}, +, \times)$ ; la relation d'équivalence $\rho$ sur $\mathbb{Z}$ compatible avec les lois de composition : "$+, \times$" est définie comme suit :
Pour $x, y \in \mathbb{Z}$, $x\rho y \Leftrightarrow y - x \in n\mathbb{Z}$. Et alors l'anneau quotient $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \times\right)$ est appelé l'anneau des classes résiduelles modulo $n$.

### 2.4.1 Idéal principal

Soit $S = \{a_1, a_2, ..., a_n\}$ une partie finie d'un anneau $(A, +, .)$, l'idéal **engendré par** $S$ est l'ensemble des éléments de la forme

$$\sum_{i=1}^{n} \alpha_i a_i \text{ avec } \alpha_i \in A.$$

**Définition**

Un idéal **principal** est un idéal engendré par un seul élément de $(A, +, .)$.

**Remarque**

Un idal principal peut admettre plusieurs générateurs distincts

**Définition**

Soit $I$ un idéal de l'anneau $A$. On dit que $I$ est un idéal **premier** si $I \neq A$ et si, pour tous $x$ et $y$ de $A$, avec $xy \in A$, alors $x \in I$ ou $y \in I$.

**Définition**

Soit $I$ un idéal de l'anneau $A$. On dit que $I$ est un idéal **maximal** si $I \neq A$ et si, pour tout idéal $J$ diffèrent de $I$, $I\ C\ J$ implique $J = A$.

**Définition**

Soit $(A, +, .)$ un anneau non réduit à $\{0\}$, on dit qu'un élément $a \in A$ est un **diviseur de zéro à gauche(à droite)** si $a \neq 0$ et s'il existe $b \neq 0$ de $A$ tel que $ab = 0 (ba = 0)$(en clair si on est dans $(A, \heartsuit, \clubsuit)$ si $a \neq 1_{\heartsuit}$ et s'il existe $b \neq 1_{\heartsuit}$ de $A$ tel que $a \clubsuit b = 1_{\heartsuit}$ $(b \clubsuit a = 1_{\heartsuit}))$.

NB : $1_{\heartsuit}$ est l'élément neutre de la première loi $\heartsuit$de l'anneau $(A, \heartsuit, \clubsuit)$

**Définition**

On dit qu'un anneau $(A, +, .)$ est **intègre** ou est un anneau d'**intégrité** s'il est non vide, et s'il ne possède pas de diviseur de zéro. Autrement dit dans un anneau d'intégrité :

$a, b \in A,\ \ ab = 0 \Rightarrow a = 0$ ou $b = 0$(en clair si on est dans $(A, \heartsuit, \clubsuit)$ on a $a\clubsuit b = 1_\heartsuit \Rightarrow a = 1_\heartsuit$ ou $b = 1_\heartsuit$ pour $a, b \in A$).

**Définition**

Un anneau intègre dont tous les idéaux sont principaux est un anneau **principal.**

**Remarque**

Soit $(A, +, .)$ un anneau unitaire d'unité 1 ; l'application $\varphi : \mathbb{Z} \longrightarrow A$ qui a $n \mapsto n.1 = \underbrace{1 + 1 + ... + 1}_{n \text{ termes}}$ si $n \in \mathbb{N}$

sinon $n.1 = \underbrace{(-1) + (-1) + ... + (-1)}_{(-n) \text{ termes}}$

est un morphisme d'anneaux donc $\varphi(0) = 1_+$ élément neutre de "+" dans $(A, +, .)$. Son noyau $\ker\varphi$ est donc un ideal de $\mathbb{Z}$ donc de la forme $p\mathbb{Z}$ avec $p \in \mathbb{N}$.

En considerant la decomposition canonique de $\varphi$ on obtient un isomorphisme de $\mathbb{Z}/p\mathbb{Z}$ sur $\varphi(\mathbb{Z})$(en clair si on est dans $(A, \heartsuit, \clubsuit)$ unitaire d'unité $1_\clubsuit$, on a :

$\varphi : \mathbb{Z} \longrightarrow A$ qui a $n \mapsto n\clubsuit 1_\clubsuit = \underbrace{1_\clubsuit \heartsuit 1_\clubsuit \heartsuit ... \heartsuit 1_\clubsuit}_{n \text{ termes}}$ si $n \in \mathbb{N}$

sinon $n\clubsuit 1_\clubsuit = \underbrace{symet_\heartsuit(1_\clubsuit) \heartsuit symet_\heartsuit(1_\clubsuit) \heartsuit ... \heartsuit symet_\heartsuit(1_\clubsuit)}_{(-n) \text{ termes}}$

et si $n = 0$, on a $\varphi(0) = 1_\heartsuit$ ).

**Definition**

L'entier naturel $p$ ainsi defini s'appelle caracteristique de l'anneau $A$ et se note $car(A)$.

**Remarque**

Si $p = 0$ , alors $\ker\varphi = \{0\}$ donc $\varphi$ est injective et donc $\mathbb{Z}$ est isomorphe a $\varphi(\mathbb{Z})$ : $A$ contient un sous-anneau isomorphe a $\mathbb{Z}$ et en particulier $A$ est infini ;

Si $p \neq 0$ : alors $\ker\varphi = \mathbb{Z}/p\mathbb{Z}$ isomorphe a $\varphi(\mathbb{Z})$ ; $p$ est le plus petit entier $> 0$ tel que $p.1 = 0$ et $p \in \mathbb{N}$ est caracterisé par : $\forall n \in \mathbb{N} : n.1 = 0 \Longleftrightarrow n$ multiple de $p$.

**Proposition**

Si l'anneau $A$ est integre sa caracteristique est soit 0 soit un nombre premier.

En particulier la caractéristique d'un corps (car un corps est d'abord un anneau unitaire intègre) est donc 0 ou un nombre premier.

Preuve

si la caractéristique de $A$ n'est pas nulle, $\varphi(\mathbb{Z})$ est inclus dans

$A$ intègre, donc $\varphi(\mathbb{Z})$ est lui-même intègre et de plus il est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Donc $\mathbb{Z}/p\mathbb{Z}$ est intègre donc $p$ est premier.
La réciproque est fausse pour la caractéristique 0, car l'anneau des matrices carrées d'ordre 2 est de caractéristique 0, mais n'est pas intègre.

**Exemple**

$car(\mathbb{Z}/n\mathbb{Z}) = n$ ; $car(\mathbb{Q}) = car(\mathbb{R}) = 0$.

**Corollaire**

Soit $(K, +, .)$ un anneau de caractéristique $n$, et $a, b \in K$ commutant, alors
$(a+b)^n = a^n + b^n$

## 2.5 Structure de corps

**Définition**

On appelle **corps** tout anneau $(\mathbb{K}, \heartsuit, \clubsuit)$ non vide dans lequel $(\mathbb{K}\backslash\{1_\heartsuit\}, \clubsuit)$ est un groupe, où $1_\heartsuit$ est l'élément neutre de $\heartsuit$.
On dit qu'un corps est commutatif si le groupe $(\mathbb{K}\backslash\{1_\heartsuit\}, \clubsuit)$ est commutatif.

**Exemple**

Les anneaux $(\mathbb{Q}, +, .)$ et $(\mathbb{R}, +, .)$, $(\mathbb{C}, +, .)$ sont des corps commutatifs.

**Théorème**

Tout corps $(\mathbb{K}, \heartsuit, \clubsuit)$ est intègre.

*Preuve*

*Soient* $a, b \in \mathbb{K}$ *avec* $a \clubsuit b = 1_\heartsuit$ *a-t-on* $a = 1_\heartsuit$ *ou* $b = 1_\heartsuit$ *?*
*Supposons* $a \neq 1_\heartsuit$, *on aura :*
$(symet_\clubsuit(a)) \clubsuit (a \clubsuit b) = (symet_\clubsuit(a)) \clubsuit 1_\heartsuit = 1_\heartsuit \Rightarrow$
$(symet_\clubsuit(a) \clubsuit a) \clubsuit b = 1_\heartsuit \Rightarrow 1_\clubsuit \clubsuit b = b = 1_\heartsuit$.
*Par analogie si* $b \neq 1_\heartsuit \Rightarrow a = 1_\heartsuit$. *CQFD*

**Proposition**

Tout corps $(\mathbb{K}, \heartsuit, \clubsuit)$ fini est commutatif.

*(Admettre)*

**Exercice 2**

Montrer que tout anneau $(A, +, \times)$ fini intègre contenant au moins deux éléments est un corps.

*Proposition de reponse*

*Soit* $a \in A$ ; $a \neq 0$. *L'application* $L_a : A \to A$
*définie par* $L_a(x) = ax$ *est un homomorphisme de groupe additif injectif.*

*En effet* $L_a(x+y) = L_a(x) + L_a(y)$ *et* $L_a(x) = 0$ *implique* $ax = 0$ *;*
*Comme* $A$ *est intègre, alors* $x = 0$ *et* $L_a$ *est injective. Mais*
$A$ *est un ensemble fini ; donc toute application injective de* $A$ *à valeurs dans* $A$ *est surjective donc bijective.*
*Il existe donc un élément* $a_0$ *tel que* $L_a(a_0) = aa_0 = a$.
*On a également* $L_a(a_0x) = a(a_0x) = (aa_0)\,x = ax = L_a(x)$ *et*
*comme* $L_a$ *est injective* $a_0x = x$ *et ceci pour tout* $x \in A$.
*Calculons à présent* $xa_0$. *On a*
$(xa_0 - x)a = (xa_0)a - xa = x\,(a_0a = a) - xa = x\,(a) - xa = 0$
*et donc, comme* $A$ *est intègre,* $xa_0 = x$ *et ceci pour tout* $x \in A$.
*Ainsi* $a_0$ *vérifie* $xa_0 = a_0x = x$ *pour tout* $x \in A$, *et* $a_0$ *est un élément neutre pour la multiplication de* $A$ *et* $A$ *est donc un anneau intègre fini* ***unitaire***. *Comme* $L_a$ *est bijective, il existe* $b \in A$ *tel que* $L_a(b) = ab = a_0$ *et* $b$ *est l'inverse à droite de* $a$. *Mais*
$L_a(ba) = a(ba) = (ab)a = a_0a = aa_0 = a = L_a(a_0)$
*montre que* $ba = a_0$ *car* $L_a$ *est injectif et* $b$ *est l'inverse de* $a$.
*Comme* $a$ *a été choisi quelconque non nul dans* $A$, *on en déduit que tout élément non nul est inversible et* $A$ *est un corps.*

**Définition**

On dit qu'un corps commutatif $\mathbb{K}$ est un corps des fractions de l'anneau intègre $A$ si les deux conditions suivantes sont vérifiées :
a) $A$ est un sous-anneau du corps $\mathbb{K}$.
b) Pour tout $x \in \mathbb{K}$, il existe dans $A$ des éléments $a$ et $b$ tels que $x = ab^{-1}$.

**Théorème**

Tout anneau commutatif intègre $A$ admet un corps des fractions.
Si $\mathbb{K}$ et $\mathbb{L}$ sont des corps des fractions de l'anneau $A$, alors $\mathbb{K}$ et $\mathbb{L}$ sont isomorphes.(Admettre)

**Exemple**

$(\mathbb{Z}, +, .)$ est un anneau commutatif intègre ; son corps des fractions est : $(\mathbb{Q}, +, .)$.

## 2.6 Sous-corps

**Définition**

Si $(\mathbb{K}, \heartsuit, \clubsuit)$ est un corps et si $\varnothing \neq \mathbb{K}' \subset (\mathbb{K}, \heartsuit, \clubsuit)$ est stable pour les lois induites(i.e $\mathbb{K}'\heartsuit\mathbb{K}' \subset \mathbb{K}'$ et $\mathbb{K}'\clubsuit\mathbb{K}' \subset \mathbb{K}'$), on dit que $\mathbb{K}'$ est un **sous-corps** de $\mathbb{K}$ ssi $\mathbb{K}'$ est un corps pour les lois induites. On dit aussi que $\mathbb{K}$ est une **extension** ou un sur-corps de $\mathbb{K}'$.

**Caractérisation pratique d'un sous-corps**

$\varnothing \neq \mathbb{K}' \subset \mathbb{K}$ est un sous-corps de $(\mathbb{K}, \heartsuit, \clubsuit)$ ssi
$\left.\begin{array}{l}(i)\forall a,\, b \in \mathbb{K}',\, a\heartsuit\left(sym\acute{e}t_{\heartsuit}\left(b\right)\right) \in \mathbb{K}' \text{ et } a\clubsuit b \in \mathbb{K}' \\ (ii)\forall a \in \mathbb{K}' \backslash \left\{1_{\heartsuit}\right\}, \text{ on a } sym\acute{e}t_{\clubsuit}\left(a\right) \in \mathbb{K}'.\end{array}\right\} \Longleftrightarrow$
$\left\{\begin{array}{l}\forall a,\, b \in \mathbb{K}',\, a\heartsuit\left(sym\acute{e}t_{\heartsuit}\left(b\right)\right) \in \mathbb{K}' \text{ et} \\ \forall x \in \mathbb{K}' \backslash \left\{1_{\heartsuit}\right\}, \text{ on a } sym\acute{e}t_{\clubsuit}\left(x\right) \clubsuit b \in \mathbb{K}'.\end{array}\right. \Leftrightarrow$
$\forall a \in \mathbb{K}' \backslash \left\{1_{\heartsuit}\right\}, \forall b \in \mathbb{K}',$
on a $sym\acute{e}t_{\clubsuit}\left(a\right) \clubsuit b \in \mathbb{K}'$ et $a\heartsuit\left(sym\acute{e}t_{\heartsuit}\left(b\right)\right) \in \mathbb{K}'$ .
(autrement dit $\mathbb{K}'$ est un sous-anneau unitaire de $\mathbb{K}$ où tout élément différent de $1_{\heartsuit}$ admet un symétrique par rapport à la loi $\clubsuit$).

**Exercice 3**

Montrer que $\mathbb{Z}/p\mathbb{Z}$ est un corps ssi $p$ est premier.

*Proposition de solution*

*Supposons* $0 \neq p = ab$ *avec* $a < p$ *et* $b < p \Rightarrow \overline{ab} = \bar{a}\bar{b} = \overline{0}$ *avec* $\bar{a} \neq \overline{0}$ *et* $\bar{b} \neq \overline{0} \Rightarrow \mathbb{Z}/p\mathbb{Z}$ *n'est pas intègre.*

*Supposons* $p$ *premier, on sait* $\forall \bar{x} \in \mathbb{Z}/p\mathbb{Z}$ *différent de* $\overline{0}$*,* $x$ *est premier avec* $p$*, et alors* $\overline{x}$ *est inversible dans* $\mathbb{Z}/p\mathbb{Z}$ *qui est un anneau unitaire*

**Exercice 4**

Montrer que $S = \left\{a + b\sqrt{3}\,;\, a, b \in \mathbb{Q}\right\}$ est un corps.

*(Il suffit de montrer que* $S$ *est un sous-corps du corps* $(\mathbb{R}, +, \times)$*).*

## 2.7 Les idéaux d'un corps

**Proposition**

Un corps $(\mathbb{K}, \heartsuit, \clubsuit)$ ne possède que deux idéaux : $\{1_{\heartsuit}\}$ et $\mathbb{K}$.

*Preuve*

*Soit* $I$ *un idéal de* $\mathbb{K}$*. Si* $I \neq \{1_{\heartsuit}\}$*, il possède un élément* $x \neq 1_{\heartsuit}$*, et comme cet élément est inversible, tout élément* $y$ *de* $\mathbb{K}$ *s'écrit* $y = y\clubsuit\left(sym\acute{e}t_{\clubsuit}\left(x\right)\clubsuit x\right) \in I$*. Donc* $I = \mathbb{K}$*.*

**Théorème**

Soit $M$ un idéal d'un anneau commutatif $A$. Alors $M$ est maximal si et seulement si l'anneau quotient $A/M$ est un corps.(admettre)

**Théorème**

Soit $\mathbf{K}$ un anneau commutatif non nul. Pour que $\mathbf{K}$ soit un corps il faut et il suffit que les seuls idéaux de $\mathbf{K}$ soient $\{0\}$ et $\mathbf{K}$.(Admettre)

## 2.8 Morphisme de corps

**Définition**

Soient $(E, \heartsuit, \clubsuit)$ et $(A, +, \times)$ deux corps. Un **morphisme de corps** $f$ de $E$ dans $A$ est une application de $E$ dans $A$ telle que, $\forall x,\, y \in E,\, f(x \heartsuit y) = f(x) + f(y)\,;\, f(x \clubsuit y) = f(x) \times f(y)$.

**Proposition**

Pour tout morphisme de corps non nul(i.e.$\neq 1_+$) $f : (E, \heartsuit, \clubsuit) \to (A, +, \times)$ on a : $f(1_\clubsuit) = 1_\times$

($1_\clubsuit$ est l'élément neutre de "$\clubsuit$" et $1_\times$ est l'élément neutre de "$\times$").

*Preuve*

$\forall x, y \in E$, $f(x \clubsuit y) = f(x) \times f(y)$, *avec* $x = y = 1_\clubsuit$, *on a :*

$f(1_\clubsuit) = f(1_\clubsuit \clubsuit 1_\clubsuit) = f(1_\clubsuit) \times f(1_\clubsuit) \Leftrightarrow$

$f(1_\clubsuit) \times 1_\times = f(1_\clubsuit) \times f(1_\clubsuit) \Leftrightarrow$

$(f(1_\clubsuit) \times 1_\times) - (f(1_\clubsuit) \times f(1_\clubsuit)) = f(1_\clubsuit) \times (1_\times - f(1_\clubsuit)) = 0 = 1_+$

*comme* $(A, +, \times)$ *est un anneau intègre, on a :*

$(*) \Leftrightarrow f(1_\clubsuit) \times (1_\times - f(1_\clubsuit)) = 0 \Leftrightarrow f(1_\clubsuit) = 0$ *ou* $1_\times - f(1_\clubsuit) = 0$,

*mais avec* $f(1_\clubsuit) = 0 \Rightarrow 1_\clubsuit \in \ker f$ *qui est un idéal,*

*d'où* $\forall x \in E$, $x = (x \clubsuit 1_\clubsuit) \in \ker f \Rightarrow \ker f = E \Leftrightarrow$

$f$ *est identiquement nul. Ce qui est contraire à l'hypothèse,*

*donc on n'a pas* $f(1_\clubsuit) = 0$, *mais plutôt* $f(1_\clubsuit) \neq 0$, *ainsi*

$(*) \Rightarrow 1_\times - f(1_\clubsuit) = 0 \Leftrightarrow f(1_\clubsuit) = 1_\times$.

**Proposition**

Tout morphisme non nul de corps est injectif.

*Preuve*

*Soit* $f : (E, \heartsuit, \clubsuit) \to (A, +, \times)$ *un morphisme de corps.*

*Alors* $\ker f$ *est un idéal du corps* $E$. *Donc* $\ker f$ *ne peut-être que l'idéal* $\{1_\heartsuit\}$ *ou l'idéal plein(c'est-à-dire* $E$*). Or* $\ker f = E$ *est absurde car* $f(1_\clubsuit) = 1_\times \neq 0 = 1_+$. *Donc* $1_\clubsuit \notin \ker f$. *Donc* $\ker f = \{1_\heartsuit\}$, *c'est-a-dire* $f$ *injectif.*

# Chapitre 3

# LES POLYNÔMES

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Dans ce chapitre, on considère les applications
$P : \mathbb{K} \longrightarrow \mathbb{K}$ avec $P(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_0$ ,
où $a_i \in \mathbb{K}$ sont donnés, ils s'appellent les coefficients de $P$.
**Définiton**
$P$ s'appelle polynôme, on dit aussi le polynôme $P(X)$.
Si $n \in \mathbb{N}$ est tel que $a_n \neq 0$, alors $n$ est le dégré de $P$.
On note $d^o P = n$. $(\mathbb{K}[X], +, .)$ est l'anneau des polynômes à coefficients dans $\mathbb{K}$, qui est commutatif unitaire et intègre.

## 3.1 Division suivant les puissances décroissantes

**Définition**
Diviser un polynôme $A(X)$ par un polynôme $B(X)$ suivant les puissances décroissantes de $X$, c'est trouver deux polynômes
$Q$ et $R$ ,vérifiant :
$A(X) = B(X)Q(X) + R(X)$ avec $d^O R < d^o B$.
Et cette division s'appelle la division **euclidienne** dans $\mathbb{K}[X]$.
**Exemple**
$A(X) = X^4 + 2X^3 + 5X^2 + 4X + 1$, $B(X) = X^2 + 3X - 1$.
On trouve : $Q(X) = X^2 - X + 9$ et $R(X) = -24X + 10$.
**Proposition**
*Pour que le polynôme $A(X)$ soit divisible par $(X - a)$, il faut et il suffit que $A(a) = 0$.*

## 3.2 Division suivant les puissances croissantes

**Théorème**
Soit $A(X)$ et $B(X)$ deux polynômes de $\mathbb{K}[X]$ ($\mathbb{K}$ un corps) tel que $B(0) \neq 0$ et soit $n$ un entier naturel. Il existe, de manière unique, deux polynômes $Q_n(X)$ et $R_n(X)$ tels que :

$$A(X) = Q_n(X) B(X) + X^{n+1} R_n(X) \text{ et } \deg(R_n) \leq n.$$

Le polynôme $Q_n$ s'appelle le quotient et le polynôme $X^{n+1}R_n$ s'appelle le reste à l'ordre $n$ de la division de $A$ par $B$ suivant les puissances croissantes.

**Exemple**
Avec $A(X) = 1 = (1 + X + X^2 + ... + X^n)(1 - X) + X^{n+1}$
on a la division de $A(X) = 1$ par $B(X) = 1 - X$ à l'ordre $n$ suivant les puissances croissantes.

**Exercice pratique**
1.Ecrire les tables de l'addition et de la multiplication de l'anneau quotient $\frac{\mathbb{Z}}{5\mathbb{Z}}$.
2. Dans $\frac{\mathbb{Z}}{5\mathbb{Z}}[X]$ effectuer la division euclidienne de $X^5 + X^4 + \mathring{3}X + \mathring{2}$ par $\mathring{4}X^3 + X + \mathring{3}$
3. Dans $\frac{\mathbb{Z}}{5\mathbb{Z}}[X]$ effectuer la division suivant les puissances croissantes jusqu'à l'ordre 3 de $X^2 + X + \mathring{2}$ par $\mathring{4}X^3 + X + \mathring{2}$

## 3.3 Factorisation

### 3.3.1 Zéros d'un polynôme(ou racine d'un polynôme)

**Définition**
Un nombre $a \in \mathbb{K}$ est un zéro d'un polynôme

$$P(X) \in \mathbb{K}[X] \text{ ssi } P(a) = 0.$$

### 3.3.2 Ordre de multiplicité d'un zéro

**Définition**
On dit que $a \in \mathbb{K}$ est un zéro d'ordre de multiplicité $n \in \mathbb{N}$ d'un polynôme $P(X) \in \mathbb{K}[X]$, si $P(X)$ est divisible par $(X - a)^n$, mais n'est pas divisible par $(X - a)^{n+1}$.

**Théorème de D'Alembert**

*Tout polynôme $P(X) \in \mathbb{C}[X]$ de dégré supérieur à zéro admet au moins une racine $r$ (réelle ou complexe).*

### 3.3.3 Décomposition en produit de facteurs premiers

**Corollaire**

*Tout polynôme $P(X) \in \mathbb{C}[X]$ de dégré $n \geq 1$ peut se mettre d'une manière unique sous la forme :*

$P(X) = a_n \ (X - x_1)^{\alpha_1} \ (X - x_2)^{\alpha_2} \ ....(X - x_k)^{\alpha_k}$ , *où* $a_n \ \in \mathbb{C}^*$,

*les $x_i$ sont deux à deux distincts et* $\alpha_1 \ + \alpha_2 \ + ... + \alpha_k \ = n$.

On dit que le polynôme est décomposé en produit de facteurs premiers

**Corollaire**

1. Tout polynôme $P(X) \in \mathbb{C}[X]$ de dégré $n \geq 1$ possède exactement $n$ racines à condition de compter chaque racine avec son ordre de multiplicité.
2. Si un polynôme à coefficients complexes s'annulle en une infinité de valeurs de $X$, alors ce polynôme est identiquement nul.

## 3.4 P.G.C.D. et P.P.C.M. de deux polynômes

**Définition**

Le *P.G.C.D.* qui est le plus grand commun diviseur de $A(X)$ et $B(X)$ est le produit des facteurs communs aux décompositions en facteurs premiers des polynômes affectés du plus petit des exposants du facteur commun figurants dans les décompositions.

On note : $PGCD(A, B) = A \wedge B$.

**Théorème d'Euclide**

Soit $A$ et $B$ deux polynômes non nuls.

s'il existe des polynômes $Q$ et $R$ tels que $A = BQ + R$ alors

$PGCD(A, B) = A \wedge B = B \wedge R = PGCD(B, R)$.

**Définition**

Le *P.P.C.M.* qui est le plus petit commun multiple de $A(X)$ et $B(X)$ est le produit des différents facteurs qui sont dans les décompositions en produit de facteurs premiers de $A(X)$ et $B(X)$ et chaque facteur du produit est affecté du plus grand exposant.

On note : $PPCM(A, B) = A \vee B$

**Proposition**

Soit $A$ et $B$ deux polynômes non nuls.

$PGCD(A, B) \times PPCM(A, B) = A \times B$.

### 3.4.1 Identité de Bezout

**Définition**
Deux polynômes $A$ et $B$ sont premiers entre eux s'il n'existe aucun polynôme autre que les constantes qui soient diviseurs communs de $A$ et $B$. On dit aussi que $A$ et $B$ sont premiers.

**Théorème de Bezout**
*Soient deux polynômes $A$ et $B$ tel que $PGCD(A,B) = D$ alors il existe deux polynômes $U$ et $V$ tel que $AU + BV = D$.*

**Proposition(Identité de Bezout)**
*Deux polynômes $A$ et $B$ sont premiers entre eux ssi il existe deux polynômes $U$ et $V$ tel que $AU + BV = 1$.*

## 3.5 Equation algébrique

On appelle équation algébrique,
une équation $P(X) = 0$ où $P(X) \in \mathbb{K}[X]$.

### 3.5.1 Relation entre coefficients et racines d'une équation algébrique

Soit $P(X) = a_n X^n + a_{n-1} X^{n-1} + ...a_1 X + a_0 \in \mathbb{C}[X]$,
avec $a_n \neq 0$, et $x_1$ , $x_2$ , $x_3$ , ..., $x_n$ les racines de $P$ comptées avec leur ordre de multiplicité.
On pose $S_0 = 1$, $S_1 = \sum_{1 \leq i \leq n} x_i$ ,
$S_2 = \sum_{1 \leq i \neq j \leq n} x_i x_j$ , $S_k = \sum_{1 \leq i_1 < i_2 < ... < i_k \leq n} x_{i_1} x_{i_2} ... x_{i_k}$ ,
$S_n = \prod_{i=1}^{n} x_i$ . On montre que :
$\forall k \in \mathbb{N}, 1 \leq k \leq n, S_k = \dfrac{(-1)^k a_{n-k}}{a_n}$.

## 3.6 Fractions rationnelles

Soient $P$ et $Q$ deux polynômes de $\mathbb{K}[X]$ tel que $Q \ncong 0$.
La fonction $f(X) = \dfrac{P(X)}{Q(X)}$ est appelée **fraction rationnelle**.
L'ensemble des fractions rationnelles à coefficients dans $\mathbb{K}$ est un anneau intègre unitaire et commutatif se notant $\mathbb{K}(X)$. $\mathbb{K}(X)$ est le corps de fractions de l'anneau commutatif et intègre $\mathbb{K}[X]$.

Dans le même esprit que le corps des rationnelles, dont les éléments quotientent des entiers relatifs où le dénominateur est non nul.

### 3.6.1 Décomposition d'une fraction rationnelle en éléments simples

**Partie entière de $f$**

On appelle partie entière de $f(X) = \dfrac{P(X)}{Q(X)}$ , le quotient de la division euclidienne suivant les puissances décroissantes de $P(X)$ par $Q(X)$.
0n la note $E(X)$.
Pour toute fraction rationnelle $f$, il existe deux polynômes premiers entre eux $U(X)$ et $V(X)$ tel que $f(X) = E(X) + \dfrac{U(X)}{V(X)}$.

**Décomposition en éléments simples dans $\mathbb{C}(X)$**

On commence par la décomposition de $V(X)$ en produit de facteurs premiers dans $\mathbb{C}$.
Soit $V(X) = (X-a_1)(X-a_2)^2 ... (X-a_k)^k$. Alors la décomposition en éléments simples de $f(X)$ est une expression de $f(X)$ dépendante des facteurs premiers de $V(X)$. En ce qui nous concerne, on a :

$$f(X) = E(X) + \frac{A_1}{X-a_1} + \frac{A_{2_1}}{X-a_2} + \frac{A_{2_2}}{(X-a_2)^2} + \frac{A_{k_1}}{X-a_k} + \frac{A_{k_2}}{(X-a_k)^2} + \frac{A_{k_3}}{(X-a_k)^3} + ... + \frac{A_{k_k}}{(X-a_k)^k},$$ où les

$A_1, A_{2_1}, A_{2_2}, A_{k_1}, A_{k_2}, A_{k_3}, ..., A_{k_k}$ des constantes complexes à déterminer.
Les fractions $\dfrac{A_{k_k}}{(X-a_k)^k}$ sont appelées

**éléments simples de première espèce.**

**Décomposition en éléments simples dans $\mathbb{R}(X)$**

On commence par la décomposition de $V(X)$ en produit de facteurs premiers dans $\mathbb{R}$.
Soit $V(X) = (X-a_1)(X-a_2)^2 ... (X-a_k)^k (X^2+b_1X+c_1)$
$\times (X^2+b_2X+c_2)^2 ... (X^2+b_lX+c_l)^l$. Alors la décomposition en éléments simples de $f(X)$ est une expression de $f(X)$ dépendante des facteurs premiers de $V(X)$. En ce qui nous concerne, on a :

$$f(X) = E(X) + \frac{A_1}{X-a_1} + \frac{A_{2_1}}{X-a_2} + \frac{A_{2_2}}{(X-a_2)^2} + \frac{A_{k_1}}{X-a_k}$$

$$+\frac{A_{k_2}}{(X-a_k)^2}+\frac{A_{k_3}}{(X-a_k)^3}+...+\frac{A_{k_k}}{(X-a_k)^k}+\frac{A_{l_1}X+B_{l_1}}{X^2+b_lX+c_l}$$
$$+\frac{A_{l_2}X+B_{l_2}}{(X^2+b_lX+c_l)^2}+\frac{A_{l_3}X+B_{l_3}}{(X^2+b_lX+c_l)^3}+...+\frac{A_{l_l}X+B_{l_l}}{(X^2+b_lX+c_l)^l},$$

où les $A_1$, $A_{2_1}$, $A_{2_2}$, $A_{k_1}$, $A_{k_2}$, $A_{k_3}$, ..., $A_{k_k}$, $A_{l_i}$, $B_{l_i}$ avec $i \in \{1,2,3,...,l\}$ des constantes réelles à déterminer.

Les fractions $\frac{A_{k_k}}{(X-a_k)^k}$ sont appelées

**éléments simples de première espèce.**

Les fractions $\frac{A_{l_l}X+B_{l_l}}{(X^2+b_lX+c_l)^l}$ sont appelées

**éléments simples de deuxième espèce.**

## 3.7 Idéaux de $\mathbb{K}[X]$

**Proposition**

Soit $A$ un élément de $\mathbb{K}[X]$ et soit $(A)$ l'ensemble des multiples de $A$ dans $\mathbb{K}[X]$.

$(A)$ est un idéal de $\mathbb{K}[X]$ appelé **idéal principal engendré par** $A$

**Exercice**

Montrer que $\mathbb{K}[X]$ l'anneau des polynômes à une variable $X$ est un anneau principal.

# Exercices de renforcement

**Exercice 1**

A. On considère une loi de composition "$*$" définie dans $\mathbb{R}$ par :

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

La loi "$*$" est-elle interne dans $\mathbb{R}$ ? Est-elle commutative ? Associative ? Admet-elle d'élément neutre ? tout réel admet-il de symétrique ?

B. On considère une loi de composition "$*$" définie dans $\mathbb{R}$ par :

$$\forall\,(x,y)\in\mathbb{R}^2,\ x*y=\ln\left(e^x+e^y\right).$$

La loi "$*$" est-elle interne dans $\mathbb{R}$ ? Est-elle commutative ? Associative ? Admet-elle d'élément neutre ? Y a-t-il des éléments réguliers ?

**Exercice 2**

Soit $*$ la loi définie sur $\mathbb{R}$ par :

$\forall x,\ y\in\mathbb{R},\ x*y=xy+\left(x^2-1\right)\left(y^2-1\right)$.

1) La loi $*$ est-elle commutative ? Associative ? Admet-elle un élément neutre ?

2) Résoudre les équations suivantes d'inconnue $x\in\mathbb{R}$ :

$$2*x=5\,;\ x*x=1.$$

**Exercice 3**

On suppose un ensemble $E$ muni d'une loi interne "$*$", possédant les propriétés suivantes :

a) Elle est associative.

b) Il existe un neutre à droite $e$, c'est-à-dire :

$$\forall a\in E,\ a*e=a.$$

c) Tout élément $a$ de $E$ admet un symétrique à droite, c'est-à-dire : $\forall a\in E,\ \exists a'\in E\ /\ a*a'=e$.

1. i) Montrer que $\forall a\in E,\ a'*a=e$.
   (On pourra considérer le symétrique à droite $a''$ de $a'$).
   ii) En déduire que $e$ est un élément neutre à gauche. Que peut-on dire de $(E,*)$ ?
2. On suppose maintenant que la loi dans $E$ possède les propriétés suivantes :

a) Elle est associative.

b) $\forall a\in E,\ \forall b\in E,\ \exists x,\ y\in E$ tels que $a*x=b=y*a$.

Montrer que $(E,*)$ est un groupe.

**Exercice 4**

Soit $T$ une loi de composition interne associative sur un ensemble $E$. On suppose qu'il existe $a\in E$ tel que l'application

$$f:E\longrightarrow E \text{ définie par } f(x)=aTxTa$$

soit surjective et on note $b$ un antécédent de $a$ par $f$.

1) Montrer que $e = aTb$ et $e' = bTa$ sont neutres respectivement à gauche et à droite.Puis montrer que $e = e'$.

2) Montrer que $a$ est symétrisable et $f$ bijective.

**Exercice 5**

Soit $E = ]-1, 1[$, on définit sur $E$ la loi $*$ par :

$$\forall\,(x, y) \in E^2,\ x * y = \frac{x + y}{1 + xy}.$$

1) Montrer que la loi $*$ est interne dans $E$.

2) Soit $\varphi$ une fonction définie dans $E$ par : $\varphi\,(x) = \ln \dfrac{1 + x}{1 - x}$.

Montrer que $\varphi$ est un isomorphisme de $(E, *)$ dans $(\mathbb{R}, +)$.

En déduire une structure de $(E, *)$.

**Exercice 6**

On note $G$ l'ensemble des applications de $\mathbb{C}$ dans $\mathbb{C}$, définie par :

$f_{a,b}\,(z) = az + b,\ (a, b) \in \mathbb{C}^* \times \mathbb{C}$.

1) Montrer que $f_{a,b}$ est une bijection de $\mathbb{C}$ sur $\mathbb{C}$.

2) Montrer que $G$ est un groupe pour la composition des applications. Est-il abélien ?

3) Soit $H$ l'ensemble des éléments de $G$ de la forme $f_{a,0}$ et $K$ l'ensemble des éléments de la forme $f_{1,b}$.

(i) Montrer que $H$ est un sous-groupe de $G$ isomorphe à $\mathbb{C}^*$.

(ii) Montrer que $K$ est un sous-groupe de $G$ isomorphe à $\mathbb{C}$.

(iii) Montrer que tout élément de $G$ peut s'écrire comme composé d'un élément de $H$ et d'un élément de $K$.

**Exercice 7**

On considère la loi de composition interne notée $\triangle$ définie sur le corps $\mathbb{R}$ par : $a \triangle b = \dfrac{a^3 + b^3}{a^2 + b^2}$ si $a^2 + b^2 \neq 0$ et $0 \triangle 0 = 0$.

1. Cette loi est-elle commutative ? Associative ? Distributive à droite ou à gauche par rapport à la multiplication sur $\mathbb{R}$ ? La multiplication sur $\mathbb{R}$ est-elle distributive par rapport à l'opération $\triangle$.

2. Existe-t-il un élément neutre pour l'opération $\triangle$ ?

Un nombre réel donné a-t-il un symétrique ? La loi est-elle une loi de groupe.

**Exercice 8**

On considère les lois de composition internes $T$ et $*$ sur $\mathbb{Z}$ définies par :

$$\forall x, y \in \mathbb{Z},\ \begin{cases} xTy = x + y + xy \\ x * y = x + y + 1 \end{cases}.$$

1. Montrer que $(\mathbb{Z}, *, T)$ est un anneau commutatif.

Préciser l'élément neutre de $(\mathbb{Z}, T)$.

2. Les éléments de $\mathbb{Z}$ sont-ils réguliers pour la loi $T$ ?
3. L'anneau $(\mathbb{Z}, *, T)$ est-il unitaire ?
4. Les éléments de $\mathbb{Z}$ sont-ils inversibles pour $T$ ?
5. Préciser ceux qui sont symétrisables pour $T$.

**Exercice 9**

On considère l'anneau commutatif unitaire $(\mathbb{Z}, +, \times)$.
1. Montrer que les idéaux de l'anneau $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}$.
2. Pour tous $m, n \in \mathbb{N}$ on pose

$m\mathbb{Z} + n\mathbb{Z} = \{x \in \mathbb{Z},\ \exists u, v \in \mathbb{Z}\,;\ x = mu + nv\}$.

(i) Montrer que $m\mathbb{Z} + n\mathbb{Z}$ est un idéal de l'anneau $\mathbb{Z}$.
(ii) Montrer que $p\mathbb{Z} = m\mathbb{Z} \cap n\mathbb{Z}$ où $p = ppcm\,(m, n)$.
(iii) Montrer que $d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$ où $d = p\gcd(m, n)$.

En déduire le théorème de Bezout.

**Exercice 10**

$M_2(\mathbb{Q})$ est l'ensemble des matrices carrées d'ordre 2 à coefficients rationnels muni de l'addition et de la multiplication est un anneau unitaire.
1. Cet anneau est-il commutatif ? Intègre ? Justifier vos réponses.
2. On désigne par $\mathcal{M}$ l'ensemble des éléments $A$ de $M_2(\mathbb{Q})$ qui sont de la forme $A(x, y) = \begin{bmatrix} x+y & 4y \\ -y & x-y \end{bmatrix}$ $x, y \in \mathbb{Q}$.

Montrer que $\mathcal{M}$, muni de l'addition et de la multiplication matricielle est un corps commutatif.

**Exercice 11**

$K$ est un corps, non nécessairement commutatif.
Les deux opérations sont notées + et . et 0 et 1 les éléments neutres respectifs de + et .
On désigne par $C = \{c \in K,\ \forall x \in K, cx = xc\}$ le *centre* de $K$.
$a$ étant fixé dans $K$, on désigne par $C_a = \{\ x \in K\,;\ ax = xa\}$ le commutateur de $a$ dans $K$.
1. a)Montrer que $C_a$ est un sous-corps de $K$
b) $C$ un sous-corps commutatif de $C_a$.
2. Soit $K^*$(resp.$C_a^*$) le groupe multiplicatif constitué par les éléments non nuls de $K$(resp. de $C_a$).

$a \in K^*$, $\forall x \in K$, on pose $\varphi_a(x) = axa^{-1}$.

a) Montrer que $\varphi_a$ est un automorphisme de $K$.
b) Montrer que $\forall \alpha, \beta \in K^*$, $\varphi_\alpha \circ \varphi_\beta = \varphi_{\alpha\beta}$ et $(\varphi_\alpha)^{-1} = \varphi_{\alpha^{-1}}$.

3) $a \in K^*$, montrer que la relation $x^{-1}y \in C_a^*$ est une relation d'équivalence $\rho_a$ sur $K^*$.

Exercices complémentaires. Série A

**Exercice 1**

Soit $E$ un ensemble muni d'une loi interne $*$.

On appelle translation à droite (resp. à gauche) par $a \in E$, l'application $d_a$ (resp. $g_a$) de $E$ dans $E$ définie par $d_a(x) = a * x$ (resp. $g_a(x) = x * a$).

1. Montrer que dans un groupe les translations à droite et à gauche sont des bijections.

2. Réciproquement, si la loi $*$ de $E$ est associative, et que les translations à droite et à gauche sont des bijections, on va montrer que $(\mathrm{E};*)$ est un groupe.

(a) Montrer que pour tout $x \in E$, il existe un unique élément $e_x \in E$ (resp. $f_x \in E$) tel que $e_x * x = x$ (resp. $x * f_x = x$).

(b) Si $x\ ;\ y \in E$, montrer que $e_x = e_y$ (noté $e$ dorénavant) et $f_x = f_y$ (noté $f$ dorénavant).

(c) Montrer que $e = f$(noté $e$ dorénavant).

(d) Montrer que pour tout $x \in E$, il existe un unique élément $\bar{x} \in E$ (resp. $\mathring{x} \in E$) tel que $\bar{x} * x = e$ (resp.$x * \mathring{x} = e$).

(e) Montrer que $\mathring{x} = \bar{x}$.

(f) Conclure.

**Exercice 2**

On munit l'ensemble $G = \{a; b; c; d\}$ d'une loi de composition interne dont la table de Pythagore est

| $\overset{\curvearrowright}{*}$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $c$ | $a$ | $c$ | $a$ |
| $b$ | $a$ | $d$ | $c$ | $b$ |
| $c$ | $c$ | $c$ | $c$ | $c$ |
| $d$ | $a$ | $b$ | $c$ | $d$ |

1. Cette loi possède-t-elle un élément neutre ?

2. Cette loi est-elle commutative ?

3. Cette loi est-elle associative ?

4. Est-ce une loi de groupe ?

**Exercice 3**

Soient les quatre fonctions de $\mathbb{R}^*$ dans $\mathbb{R}^*$

$f_1(x) = x\,;\quad f_2(x) = \dfrac{1}{x}\ :\ f_3(x) = -x\,;\ f_4(x) = -\dfrac{1}{x}.$

Montre que$G = \{f_1;\ f_2;\ f_3;\ f_4\}$ est un groupe pour la loi $\circ$ de la composition des applications.

Exercices complémentaires, série B

**Exercice 1**. On appelle **ordre** d'un élément $x$ d'un groupe $G$ le plus petit entier $n \geq 1$ tel que $x^n = 1_G$ élément neutre de $G$. Si $n$ n'existe pas, on dit que $x$ est d'ordre infini. L'ordre de $x$ est souvent noté $|x|$ comme le cardinal d'un ensemble.

1) Montrer que l'ordre de $x$ est l'ordre (i. e. le cardinal) du sous-groupe engendré par $x$.

2) Montrer que si l'ordre de $x$ est $n$, alors $x^p = 1_G \Longleftrightarrow p \in n\mathbb{Z}$.

3) Si l'ordre de $x$ est $n$, quel est l'ordre de $x^k$ ?

4) Si $a$ et $b$ commutent, que peut-on dire de l'ordre de $ab$ en fonction des ordres de $a$ et de $b$ ?
On examinera le cas où les ordres de $a$ et de $b$ sont premiers entre eux.

5) Comparer les ordres de $ab$ et de $ba$.

6) Dans un groupe fini, l'ordre de tout élément est fini. Réciproque ?

**Exercice 2**. Déterminer les sous-groupes d'un groupe cyclique.
Traiter le cas infini, puis le cas d'un groupe cyclique d'ordre $n$; il y a alors un sous-groupe de cardinal $d$ pour chaque entier $d$ divisant $n$.
Que peut-on dire si $n$ est premier ?

**Exercice 3**. Soit $G$ un groupe cyclique d'ordre $n$ engendré par $x$.
On dit qu'un élément $y$ de $G$ est un **générateur** si $G = \langle\ y\ \rangle$.
Montrer que les générateurs de $G$ sont les éléments de la forme $x^k$ où $k$ est premier avec $n$. Détailler le cas où $n = 12$ puis où $n$ est premier.
On note $\phi(n)$ le nombre des générateurs d'un groupe cyclique d'ordre $n$ ; il s'appelle **indicateur d'Euler**.

**Exercice 4**. Trouver les sous-groupes engendrés par les matrices suivantes (la loi est le produit des matrices) :

1) $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

2) $B = \begin{pmatrix} j & 0 \\ 0 & j^2 \end{pmatrix}$ avec $j = e^{\dfrac{2i\pi}{3}}$.

3) Etudier le groupe engendré par $A$ et $B$. On vérifiera qu'il y a douze éléments, et l'on en cherchera les sous-groupes.

**Exercice 5**. Soit $G$ un groupe et $H \leq G$, $K \leq G$ deux sous-groupes.
On s'intéresse à l'ensemble des éléments de la forme $hk$ où $h \in H$, $k \in K$, ensemble que l'on note $HK$.

1) Démontrer que $HK$ est un sous-groupe si et seulement si $HK = KH$.

2) Quel est le cardinal de $HK$ quand les deux groupes $H$ et $K$ sont finis ?

3) Montrer que si $H \cap K = \{1_G\}$, alors tout élément de $HK$ s'écrit de façon unique comme produit $hk$.

4) Soit $G = \mathbb{Z}/6\mathbb{Z}$ et $H = \langle\ \bar{2}\ \rangle$, $K = \langle\ \bar{3}\ \rangle$. Vérifier que $G = HK$ et qu'il y a unicité de l'écriture comme dans la question précédente.

**Exercice 6**. Soit $H \lhd G$. Montrer que l'application $K \longmapsto K/H$ est une bijection de l'ensemble des sous-groupes $K$ tels que $H \leq K \leq G$ sur l'ensemble des sous-groupes de $G/H$.
Montrer que c'est aussi une bijection de l'ensemble de tels sous-groupes $K$ normaux dans $G$ dans l'ensemble des sous-groupes normaux dans $G/H$. Retrouver ainsi les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

**Exercice 7**. $H$ et $K$ sont deux sous-groupes de $G$.
On suppose que $K \lhd G$.
Montrer que : $H \cap K \lhd H$ et $H/H \cap K \tilde{=} HK/K$.

**Exercice 8**. $H$ et $K$ sont tous les deux normaux dans $G$.
On suppose que $K \subset H$.
Montrer que $(H/K) \lhd (G/K)$ et $(G/K)/(H/K) \tilde{=} G/H$.

**Exercice 9**. $H$ et $K$ sont deux sous-groupes de $G$. Si $g \in G$, une double classe est l'ensemble $HgK = \{hgk \ / \ h \in H,\ k \in K\}$.
1) Montrer qu'une double classe est la réunion de classes à gauche et aussi une réunion de classes à droite. Montrer que les doubles classes partitionnent $G$.
2) Lorsque $G$ est fini, calculer le cardinal d'une double classe.
On pourra introduire $xKx^{-1}$, $x \in G$.
3) Que dire si l'un des sous-groupes est normal dans $G$.

**Exercice 10**. **Sous-groupes caractéristiques, centre**.
Rappelons qu'une caractérisation possible d'un sous-groupe normal (ou distingué) dans $G$ est qu'il est stable par tout automorphisme intérieur. On dit qu'un sous-groupe $H$ est caractéristique dans $G$ s'il est stable par tout automorphisme de $G$.
On note $H \sqsubset G$ pour dire que $H$ est caractéristique dans $G$, et, bien sûr, un sous-groupe caractéristique dans $G$ est aussi normal dans $G$.
1) Démontrer que : $H \sqsubset K \sqsubset G \Longrightarrow H \sqsubset G$.Cette propriété, n'est pas vraie pour la relation de $<$ normalité $>$.
2) Démontrer que : $H \sqsubset K \lhd G \Longrightarrow H \lhd G$.
3) Si $G$ est un groupe, on appelle **centre** de $G$ l'ensemble des éléments de $G$ qui commutent avec tous les éléments de $G$.
On le note $Z(G)$ et l'on peut écrire :
$Z(G) = \{\ z \in G \ / \ \forall x \in G,\ xz = zx\}$.
Bien sûr le centre contient toujours $1_G$ et est égal à $G$ ssi $G$ est commutatif. D'une certaine façon, la taille du centre mesure le degré de commutativité de $G$.
Démontrer que le centre d'un groupe est toujours un sous-groupe caractéristique. Est-ce encore le cas des sous-groupes du centre ?
4) On note $G'$ ou $D(G)$ le sous-groupe engendré par les **commutateurs**, c'est-à-dire les éléments de la forme $xyx^{-1}y^{-1}$. Démontrer que c'est un

sous-groupe caractéristique de $G$. Ce sous-groupe,
appelé **groupe dérivé**.Il mesure également le degré
de commutativité de $G$, et est reduit au neutre quand $G$ est commutatif.
5) On note $G^n(*)$ le sous-groupe de $G$ engendré par les éléments
de la forme $x^n$ où $x \in G^1$ $n \in \mathbb{N}^*$.
Démontrer que pour tout $n$ ce sous-groupe est caractéristique.
6) Une notion encore plus forte est celle de
**sous-groupe pleinement invariant** de $G$.
Ceux sont les sous-groupes de $G$ qui sont invariants par tous les
morphismes de $G$ dans $G$ (appelés parfois endomorphismes).
Démontrer que les groupes $G'$et $G^n$ sont pleinement
invariants. On peut montrer que le centre d'un groupe n'est pas
toujours pleinement invariant.
7) Quellle relation y a t-il entre le centre de $G$ et le centre d'un de ses
sous-groupes ?
8) Montrer que le centre de $\mathbf{GL}(n, \mathbb{K})$, groupe des matrices inversibles
à coefficients dans le corps $\mathbb{K}$, est le groupe des matrices scalaires,
c'est-à-dire de la forme $\lambda I$ où $\lambda$ est un scalaire non nul et $I$ est
la matrice identité . On pourra utiliser les matrices
de la forme $T_{ij} = I + E_{ij}$ où $I$ est la matrice identité et
$E_{ij}$ est la matrice dont tous les coefficients sont nuls, sauf le
coefficient d'indices $i, j$ qui est égal à 1.
Chercher le centre de $\mathbf{T}(2, \mathbb{K})$, groupe des matrices triangulaires
supérieures et de $\mathbf{TU}(2, \mathbb{K})$, groupe des matrices triangulaires
unipotentes. C'est-à-dire les matrices triangulaires supérieures
n'ayant que des 1 sur la diagonale.
9) Soit $\phi$ l'application qui à $x \in G$ associe $i_x$ automorphisme intérieur.
Montrer que c'est un morphisme de groupes.
Déterminer son noyau. En déduire : $G/Z(G) \tilde{=} Int(G)$.
$(*)$ Cette notation est ambiguë. Dans un autre contexte, *
elle représente le produit cartésien de $n$ exemplaires de $G$.
**Exercice 11.** A)Montrer que $A$, $B \in \mathbb{C}[X]$ sont premiers entre eux dans
chacun des cas suivants :
1) $A(X) = X^4 - 1$ et $B(X) = X^{4n} + X^2 + 2$ où $n \in \mathbb{N}$ ;
2) $A(X) = X^2 + X + 1$ et $B(X) = (X+1)^{2n+1} - X^{n+2}$ où $n \in \mathbb{N}$ ;
3) $A(X) = (X-1)^{3p} + (X-1)^{3p+1} + (X-1)^{3p+2} - 2j$ et
$B(X) = X^4 - X^3 + X - 1$ où $j = \frac{1}{2}\left(-1 + i\sqrt{3}\right)$ et $p \in \mathbb{N}$.
B) Déterminer, suivant les valeurs de l'entier naturel $n$, le $PGCD$ des
deux polynômes $A(X) = X^{n+1} + X^n + 1$ et
$B(X) = X^4 + X^3 + 2X^2 + X + 1$ de $\mathbb{R}[X]$.

C) Calculer le $PGCD$ des polynômes $A$ et $B$ de $\mathbb{R}[X]$ dans chacun des cas suivants :

1) $A(X) = X^{n+2} - X^n + X^2 - 1$ et
$B(X) = X^{n+3} - X^{n+1} + X^2 - 1$ où $n \in \mathbb{N}$ ;

2) $A(X) = X^6 - 1$ et $B(X) = X^6 - 7X^3 - 8$ ;

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

D) Montrer que le polynôme $A(X) = X^{n+1} - X^n + 1$ de $\mathbb{C}[X]$ $(n \in \mathbb{N})$ n'a que des racines simples.

**Exercice 12**

Factoriser le polynôme $P(X) = 8X^3 - 12X^2 - 2X + 3$ sachant que ses racines sont en progression arithmétique.

**Exercice 13**

Trouver les racines du polynôme $P(X) = X^3 - 37X + 84$ sachant que la différence de deux d'entre elles vaut 1.

**Exercice 14**

A quelle condition le polynôme $A(X) = X^4 + aX^2 + bX + c$ est-il divisible par $B(X) = X^2 + X + 1$ ?

**Exercice 15.** On considère dans $\mathbb{R}[X]$,
$A(X) = 1 + X + 2X^2 + X^3 + 2X^4 + X^5 + X^6$
et $B(X) = 1 + X^2$. Effectuer la division de $A$ par $B$ suivant les puissances croissantes jusqu'à l'ordre 3 et en déduire la décomposition de $A$ en facteurs irréductibles dans $\mathbb{R}[X]$
et $\mathbb{C}[X]$.

**Exercice 16.** Soient $n \in \mathbb{N}$, $A(X) = X^n - 1$ et $B(X) = X - 1$. Effectuer la division de $A$ par $B$ suivant les puissances croissantes jusqu'à l'ordre $n$.

**Exercice 17.**

1) Décomposer $\dfrac{1}{X^2 - a}$ en éléments simples dans $\mathbb{R}$ et dans $\mathbb{C}$ ($a$ paramètre réel).

2) Décomposer dans $\mathbb{R}$ et dans $\mathbb{C}$ les fractions rationnelles suivantes :

$$F_1(X) = \frac{1}{X^3 - 1} \qquad F_2(X) = \frac{1}{X(X^4 - 1)}$$

$$F_3(X) = \frac{X^5 + X + 1}{X^4 - 1}.$$

**Exerciec 18**

Soit $n \in \mathbb{N}^*$. Décomposer en éléments simples dans $\mathbb{R}$ la fraction rationnelle suivante :

$$F(X) = \frac{n!}{X(X-1)\cdots(X-n)}.$$

**Exerciec 19**

1.Ecrire les tables de l'addition et de la multiplication de l'anneau

quotient $\frac{\mathbb{Z}}{5\mathbb{Z}}$.

2. Dans $\frac{\mathbb{Z}}{5\mathbb{Z}}[X]$ effectuer la division euclidienne de $X^5 + X^4 + \mathring{3}X + \mathring{2}$ par $\mathring{4}X^3 + X + \mathring{3}$

3. Dans $\frac{\mathbb{Z}}{5\mathbb{Z}}[X]$ effectuer la division suivant les puissances croissantes jusqu'à l'ordre 3 de $X^2 + X + \mathring{2}$ par $\mathring{4}X^3 + X + \mathring{2}$

**Exerciec 20**

Considère l'anneau $\mathbb{F} = \frac{\mathbb{Z}}{7\mathbb{Z}}$

a) L'anneau $\mathbb{F}$ est-il un corps ?

b) Ecrire les tables de l'addition et de la multiplication de l'anneau $\mathbb{F}$.

c) Quels sont les entiers $X$ tels que $X^2 + 4X - 2$ soit multiple de 7.

d) Quels sont les entiers naturels $n$ tels que 7 divise $4^n + 3^n$ ?

**Exerciec 21**

On dit qu'un corps est **premier** s'il n'admet pas d'autre sous-corps que lui-même.

1) Montrer que tout corps admet un unique sous-corps qui est premier, appelé **sous-corps premier**.

2) Soit $(\mathbb{K}, +, .)$ un corps. Montrer que le centre $C = \{a \in \mathbb{K}; \forall x \in \mathbb{K} ax = xa\}$ est un sous-corps de $(\mathbb{K}, +, .)$.

3) Montrer que tout corps premier est commutatif et que le seul morphisme d'un corps premier dans lui-même est l'identité.

4) Montrer que $\mathbb{Q}$ et $\frac{\mathbb{Z}}{p\mathbb{Z}}$ où $p$ est un nombre premier sont des corps premiers.

5) Montrer que tout corps premier de caractéristique nulle est isomorphisme à $\mathbb{Q}$ et que tout corps premier de caractéristique $p$ est isomorphe à $\frac{\mathbb{Z}}{p\mathbb{Z}}$.

6) Soit $(\mathbb{K}, +, .)$ un corps. Montrer que tout sous-corps et tous sur-corps de $(\mathbb{K}, +, .)$ ont la même caractéristique que $(\mathbb{K}, +, .)$.

7) Montrer qu'un corps est de caractéristique $p$ non nul si, et seulement si, son sous-corps premier est isomorphe à $\frac{\mathbb{Z}}{p\mathbb{Z}}$.

8) Montrer qu'un corps est de caractéristique nulle si,seulement si, son sous-corps premier est isomorphe à $\mathbb{Q}$.

9) Montrer que le cardinal de tout corps fini est une puissance de sa caractéristique.

**T.D.**
**Eventuellement**

**EXERCICE 1**
Démontrer qu'un groupe d'ordre $p$ premier est cyclique.
**EXERCICE 2**
Montrer qu'un groupe $G$ est commutatif si et seulement si
$x \longmapsto x^{-1}$ est un automorphisme de $G$.
**EXERCICE 3**
Soit $\varphi$ un morphisme du groupe $G$ dans le groupe $H$. Si $x \in G$ est d'ordre $n$, que dire de l'ordre de $\varphi(x)$ ? Et si $\varphi$ est injectif ?
**EXERCICE 4**
Soit $\mathbb{D}_8$ le groupe engendré par les matrices
$a = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ et $b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
Montrer qu'il a huit éléments. Déterminer ses sous-groupes.
On l'appelle groupe diédral d'ordre huit.
**EXERCICE 5**
On note $\mathbb{H}_8$ le groupe engendré par les matrices
$a = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ et $b = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.
Montrer qu'il a huit éléments et déterminer ses sous-groupes.
Vérifier qu'il n'est pas isomorphe au groupe diédral $\mathbb{D}_8$.
On l'appelle groupe quaternionique.
**EXERCICE 6**
Décrire l'ensemble des morphismes de $C_n$
(un groupe cyclique d'ordre $n$) dans lui-même ; lesquels
sont des isomorphismes ?
**EXERCICE 7**
Soit $A$ un anneau et $a \in A$. Montrer que $a$ est régulier à gauche si et seulement si l'application $x \longmapsto ax$ est injective. En déduire que, dans les anneaux finis, la notion d'élément régulier coïncide avec
la notion d'élément inversible.
**EXERCICE 8**
1) Calculer $37 + 55 \bmod 63$, $37 \times 55 \mod 63$.
2) Calculer $p\gcd(433014481, 18000)$ en décomposant 18000 en produit de facteurs premiers.
3) a) Calculer le $p\gcd$ de $a = 42098$ et de $b = 36146$ avec des divisions euclidiennes.
b) Retrouver ce résultat en décomposant $a$ et $b$ en produit de facteurs premiers.

c) Déterminer des entiers $u$ et $v$ tels que $p \gcd(a,b) = au + bv$.

d) En déduire tous les couples $(s,t)$ d'entiers tels que
$$p \gcd(a,b) = as + bt.$$

e) 583 est-elle inversible dans $\dfrac{\mathbb{Z}}{679\mathbb{Z}}$, si oui quel son inverse ?

**EXERCICE 9**

Soit $n$ un entier et $S(n)$ la somme des chiffres $a_0$, $a_1$,...,$a_N$ de l'écriture décimale de
$n = a_N a_{N-1} ... a_0 = \sum_{0 \leq k \leq N} a_k 10^k$.

a) Comparer $n \mod 3$ et $S(n) \mod 3$ ; en déduire un critère de divisibilité par 3.

b) Comparer $n \mod 9$ et $S(n) \mod 9$ ; en déduire un critère de divisibilité par 9.

c) Donner un critère de divisibilité par 11 en étudiant les puissances de 10 modulo 11.

**EXERCICE 10**

Dans les questions suivantes, on pourra raisonner modulo un entier convenable.

1) Pour quelles valeurs de l'entier $n$ a-t-on $4n^4 + 17n - 31$ divisible par 5 ?

2) Montrer que, pour tout $n \geq 3$, l'un des nombres $2^n - 1$ et $2^n + 1$ est divisible par 3.

3) Montrer qu'il n'existe qu'un seul nombre premier $n$ tel que $8n^2 + 1$ soit premier.

4) a) Montrer que, si $x^2 + y^2 = 0 \mod 3$, on a $x, y = 0 \mod 3$.

b) Montrer que $x^2 + y^2 = 7500000$ n'a pas de solution dans $\mathbb{Z}$.

5) Montrer que $7x^2 - 3y^2 = 5$ n'a pas de solutions entières.

6) a) Montrer qu'un nombre de la forme $8n + 7$ n'est pas la somme de trois carrés d'entiers.

b) Montrer que l'ensemble des entiers qui sont somme de trois carrés d'entiers n'est pas stable par multiplication.

**EXERCICE 11**

*Petit théorème de Fermat*

1) Soient $p$ un nombre premier et $k$ un entier tel que $1 \leq k \leq p$.
Montrer que $C_p^k = \dfrac{p!}{k!\,(p-k)!}$ est divisible par $p$.

2) Montrer que $a^p = a \mod p$ pour tout entier $a$ par récurrence sur $a$.

**EXERCICE 12**

Soit $A$ un anneau non nul tel que $x^2 = x$ pour tout $x$ de $A$. On dit que $A$ est un anneau de Boole.

(1) Montrer que pour tout $x$ de $A$, on a : $x + x = 0$
($A$ est de caractéristique 2), puis que $A$ est commutatif.
(2) Montrer que $A$ ne peut avoir exactement 3 éléments.
Quel peut-être le nombre d'éléments d'un anneau de Boole fini ?
(3) Trouver des exemples d'anneaux de Boole.

**EXERCICE 13**

$A$ est un anneau commutatif intègre, $S$ est un sous-ensemble stable pour le produit et ne contenant pas 0 mais contenant 1.
On dit alors que $S$ est multiplicatif,
et on définit une relation dans $A \times S$ par :
$(a, s)R(a', s') \iff as' - a's = 0 \Leftrightarrow \dfrac{a}{s} = \dfrac{a'}{s'}$.
(1) Montrer que c'est une relation d'équivalence.
(2) On note $S^{-1}A$ l'ensemble quotient et $\dfrac{a}{s}$ la classe de $(a, s)$.
Montrer que $S^{-1}A$ est
un anneau pour les lois + et × définies par :
$\dfrac{a}{s} + \dfrac{b}{t} = \dfrac{at + bs}{st}$ et $\dfrac{a}{s} \times \dfrac{b}{t} = \dfrac{ab}{st}$
(ne pas oublier de vérifier que ces opérations sont bien définies).
3) Vérifier que $S = A\backslash\{0\}$ est une partie multiplicative, et qu'alors $S^{-1}A$ est un corps contenant un sous-anneau isomorphe canoniquement à $A$. Reconnaître le cas
$A = \mathbb{Z}$ et $A = \mathbb{K}[X]$. On dit alors que $S^{-1}A$ est le corps des fractions de $A$.
(4) Montrer que si $I$ est un idéal premier de $A$, $S = A\backslash I$ est une partie multiplicative.
Décrire le cas où $A = \mathbb{Z}$ et où $I = (2) = 2\mathbb{Z}$.

**EXERCICE 14**

Soit $P \in A[X]$, $P(X) = \sum_{i=0}^{n} a_i X^i$. On définit $P'$ par : $P'(X) = \sum_{i=1}^{n} i a_i X^{i-1}$
et on a les propriétés habituelles de la dérivation.
Montrer que $a$ est racine simple de $P$ si et seulement si $P(a) = 0$ et $P'(a) \neq 0$. Généraliser à des racines multiples.

**EXERCICE 15**

a) Factoriser le polynôme $P(X) = 8X^3 - 12X^2 - 2X + 3$ sachant que ses racines sont en progression arithmétique.
b) Trouver les racines du polynôme $P(X) = X^3 - 37X + 84$ sachant que la différence de deux d'entre elles vaut 1.
c) A quelle condition le polynôme $A(X) = X^4 + aX^2 + bX + c$ est-il divisible par $B(X) = X^2 + X + 1$ dans $\mathbb{R}[X]$ ?
d) Calculer le reste de la division euclidienne de

$(\cos a + X \sin a)^n$ par $X^2 + 1$ dans $\mathbb{R}[X]$.

**EXERCICE 16**

1) On considère les polynômes $A(X) = X^4 + X^3 + X + 1$ et $B(X) = X^3 + X^2 + X + 1$ de $\mathbb{R}[X]$.

a) Calculer $D(X) = p\gcd(A(X), B(X))$.

b) Trouver des polynômes $U(X)$ et $V(X)$ de $\mathbb{R}[X]$tels que $U(X)A(X) + V(X)B(X) = D(X)$.

c) Décomposer $A(X)$ et $B(X)$ en produits de facteurs irréductibles dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$.

2) Trouver le ou les polynômes $P$ de degré $\leq 5$ tels que $(X-1)^3$ divise $P(X)+1$, $(X+1)^3$ divise $P(X)-1$, en utilisant le polynôme dérivé $P'$.

**EXERCICE 17**

Soient $\mathbb{K}$ un corps, et $P$ et $Q$ deux polynômes de $\mathbb{K}[X]$. On suppose que $a$ est une racine commune de $P$ et $Q$ dans $\mathbb{K}$ de multiplicité $r$ dans $P$ et $s$ dans $Q$. Que peut-on dire de la multiplicité de $a$ comme racine de :

a) $P + Q$ ;

b) $P^2 + Q^2$ ;

c) $P^3Q^3$ ?

**EXERCICE 18**

Soit $P(X) = a_0 + a_1X + ....a_nX^n$ un polynôme à coefficients entiers.

1)Montrer que si $P(X)$ admet une racine rationnelle $\dfrac{p}{q}$ avec $p$ et $q$ entiers et $p\gcd(p,q) = 1$, alors $p$ divise $a_0$ et $q$ divise $a_n$.

2) Factoriser en produit de facteurs irréductibles dans $\mathbb{Q}[X]$ les polynômes suivants :

a) $P_1(X) = 4X^4 - 28X^3 + 45X^2 - 6X - 18$, b) $P_2(X) = 5X^3 - 4X^2 + 6$.

## COMPLEMENT

**Exercice 1(Théorème de Gauss)**

Soient trois entiers non nuls $x, y, z \in \mathbb{Z}^*$.

On suppose que $x$ divise $yz$ ; $x$ et $y$ sont premiers entre eux.

Montrer que $x$ divise $z$.

**Exercice 2**

Résoudre dans $\mathbb{Z}$ : $1665x + 1035y = 45$.

**Exercice 3**

$(A, +, .)$ désigne un anneau tel que $\forall x \in A$, $x^2 = x$.

On dit que $A$ est un anneau idempotent.

1. Montrer que $\forall x \in A,\ x + x\ = 0$.
2. Montrer que $\forall x, y \in A,\ xy = yx$.
3. En remarquant que $\forall x, y \in A,\ xy\,(x + y) = 0$, montrer que si $A$ est intègre, ou bien $A$ ne contient qu'un élément (0), ou bien $A$ ne contient que deux éléments.

**Exercice 4**

On considère les lois de composition internes $T$ et $*$ sur $\mathbb{Z}$ définies par :

$$\forall x, y \in \mathbb{Z},\ \begin{cases} xTy = x + y + xy \\ x * y = x + y + 1 \end{cases}.$$

1. Montrer que $(\mathbb{Z}, *, T)$ est un anneau commutatif.
   Préciser l'élément neutre de $(\mathbb{Z}, *)$.
2. Les éléments de $\mathbb{Z}$ sont-ils réguliers pour la loi $T$ ?
3. L'anneau $(\mathbb{Z}, *, T)$ est-il unitaire ?
4. Les éléments de $\mathbb{Z}$ sont-ils inversibles pour $T$ ?

**Exercice 5**

$M_2(\mathbb{Q})$ est l'ensemble des matrices carrées d'ordre 2 à coefficients rationnels muni de l'addition et de la multiplication est un anneau unitaire.

1. Cet anneau est-il commutatif ? Intègre ? Justifier vos réponses.
2. On désigne par $\mathcal{M}$ l'ensemble des éléments $A$ de $M_2(\mathbb{Q})$ qui sont de la forme $A(x, y) = \begin{bmatrix} x + y & 4y \\ -y & x - y \end{bmatrix}\ x, y \in \mathbb{Q}$.

Montrer que $\mathcal{M}$, muni de l'addition et de la multiplication matricielle est un corps commutatif.

**Exercice 6**

On considère l'anneau commutatif unitaire $(\mathbb{Z}, +, \times)$.

1. Montrer que les idéaux de l'anneau $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}$.
2. Pour tous $m, n \in \mathbb{N}$ on pose
   $m\mathbb{Z} + n\mathbb{Z} = \{x \in \mathbb{Z},\ \exists u, v \in \mathbb{Z}\,;\ x = mu + nv\}$.

(i) Montrer que $m\mathbb{Z} + n\mathbb{Z}$ est un idéal de l'anneau $\mathbb{Z}$.
(ii) Montrer que $p\mathbb{Z} = m\mathbb{Z} \cap n\mathbb{Z}$ où $p = ppcm\,(m, n)$.
(iii) Montrer que $d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$ où $d = p\gcd(m, n)$.
En déduire le théorème de Bezout.

**Exercice 7**

Soit $A$ un anneau commutatif. A toute partie $B$ de $A$, on associe la partie $\phi(B)$ de $A$
définie par : $\phi(B) = \{x \in A\,;\ \exists n \in \mathbb{N}^*\,;\ x^n \in B\}$.
Soient $I$ et $J$ deux idéaux de $A$.
Montrer que

1. $I + J$ et $I \cap J$ sont des idéaux de $A$, où
$I + J = \{x, \exists a \in I, b \in J\,;\, x = a + b\}$.
2. $I \subset \phi(I)$.
3. $\phi(I)$ est un idéal de $A$.
4. $I \subset J \Longrightarrow \phi(I) \subset \phi(J)$.
5. $\phi(\phi(J)) = \phi(J)$.
6. $\phi(I \cap J) = \phi(I) \cap \phi(J)$.
7. $\phi(\phi(I) + \phi(J)) = \phi(I + J)$.

**Exercice 8**

Soit $A$ l'anneau des applications de $\mathbb{R}$ dans $\mathbb{R}$.
1. Déterminer l'ensemble des éléments inversibles de $A$.
L'anneau $A$ est-il intègre ? Justifier votre réponse.
2. Montrer que l'application $\varphi : A \longrightarrow \mathbb{R}$ définie par :
$\varphi(f) = f(1)$ est un homomorphisme d'anneaux qui est surjectif.
3. Déterminer le noyau $\ker\varphi$ de $\varphi$ et prouver que l'anneau quotient $\dfrac{A}{\ker\varphi}$ est un corps qui est isomorphe à $\mathbb{R}$.

# Bibliographie

[1] Algèbre-Géométrie 1 H Prépa Maths Collection Hachette Supérieur

[2] Algèbre de J. Lelong-Ferrand et J.M.Arnaudiès Dunod

[3] Toute l'algèbre de la licence de Jean-Pierre Escofier Dunod