N° d'ordre :
N° de série :

**République Algérienne Démocratique et Populaire**

**Ministère de l'Enseignement Superieur et de la Recherche Scientifique**

---

**UNIVERSITÉ ECHAHID HAMMA LAKHDAR EL OUED**

**FACULTÉ DES SCIENCES ET DE TECHNOLOGIE**

**Mémoire de fin d'étude**

# LICENCE ACADEMIQUE

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

Présenté par: **GHANABZIA Tayeb**
**HAFOUDA Oussama**
**KAROUI El hadi**

**Thème**

# Corps finis

Devant le jury composé de :

| | |
|---|---|
| **Mr.FERHAT Mohamed Said** | **MA(A) Univ.El Oued Président** |
| **Mr.CHAIA Ahmed** | **MC (B) Univ.El Oued examinateur** |
| **Mr. DJEDIDI Mohamed yacine** | **MA(A) Univ.El Oued Rapporteur** |

Année universitaire 2014 – 2015

# *Remerciements*

Nous remercions Dieu le tout puissant qui nous a guidé dans l'accomplissement de ce travail.
Ce travail à été réalisé sous l'encadrement " **DJEDIDI Mohamed Yacine"**, à l'université Echahid Hamma Lahkdar - d'El Oued, a qu'elle nous voudrons exprimer nos profondes gratitudes pour sa disponibilité, son aides et ses pour réaliser ce travail.
Ainssi qu'à tous les professeurs de l'université Echahid Hamma Lahkdar - d'El Oued.
Nous remercions vivement nos familles surtouts nos parents pour l'aide et le soutient moral.

*Notations générales*

$\mathbb{N}$ : ensemble des nombres entiers naturels.

$\mathbb{Z}$ : l'anneau des nombres rationnels.

$\mathbb{Q}$ : corps des nombres rationnels

$\mathbb{R}$ : corps des nombre réels.

$\mathbb{C}$ : corps des nombres complexes.

$\mathbb{N}^*$ : ensemble des nombres entiers naturels non nuls.

$K^*$ : est l'ensemble inversible de élément $K$ pour la lois $\cdot$ dans l'anneau$(K, +, \cdot)$.

$car\,(k)$ : le caractéristique de l'ensemble de $k$.

$card\,(k)$ : le cardinal de l'ensemble de $k$.

$P\,(X)$ : un polynôme.

$E/K$ : $E$ est une extension de $K$.

$[E : K]$ : degré de l'extension $E$ sur $K$.

$F_p$ : l'anneau $\mathbb{Z}/p\mathbb{Z}$ et $p$ un nombre premier.

$F_p\,[X]$ : L'anneau des polynôme à coefficients dans $F_p$.

$\dim K$ : dimension de l'ensemble $K$.

$\ker f$ : noyou du morphisme $\varphi$.

$imf$ : l'image du morphisme $\varphi$.

$1_A$ : l'élément neutre de l'ensemble $A$.

$F$ : l'endomorphisme de Frobenius.

# Table des matières

# Introduction générale

En mathématiques et plus précisément en algèbre nous sommes toujours besoin de connaitre et étudier les corps finis puisque ils sont utilisés dans plusieurs branches comme la théorie algébrique et l'informatique et le cryptographie et la théorie des codes.

Pour le premier chapitre le sujet d'étude est l'algèbre des anneaux, les corps, les groupes et leurs propriétés.

Deuxième chapitre est consacré a l'étude de l'extension de corps, extension algébrique et extension transcendente.

Enfin le troisième chapitre sera consacré à étudier l'introduction de corps finis et les constructions des corps finis.

# Chapitre 1

# Structure Algebrique

## 1.1 Groupes

**Définition 1.1.1** *Un ensemble $G$ muni d'une la loi $(\cdot)$ interne noteé multiplicativement est un groupe si :*

*1)* $\forall\,(x,y,z)\in G^3$, *on a :* $x\,(yz)=(xy)\,z$.

*2)* $\exists!e\in G$ *tel que :* $\forall x\in G$, *on a :* $ex=xe=x$.

*3)* $\forall x\in E$, $\exists x^{-1}\in E$, *tel que :* $x\;x^{-1}=x^{-1}x=e$.

**Définition 1.1.2** *Si $(G,\cdot)$ est un groupe tel que la loi $(\cdot)$ satisfait la propriété :*

$$\forall\,(x,y)\in G,\ \ on\ a : x\cdot y=y\cdot x$$

*alors le groupe $(G,\cdot)$ est dit* ***commutatif*** *ou* ***abélien****.*

**Exemple 1.1.1** *1)* $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ *sont des groupes; mais,* $(\mathbb{N},+)$ *n'est pas un groupe, puisque l'opposé d'un entier strictement positif pour l'addition n'existe pas dans* $\mathbb{N}$.

*2)* $\{-1,1\}$ *c'est un groupe avec la multiplication.*

### 1.1.1 Sous-groupe

**Définition 1.1.3** *Soit* $(G, \cdot)$ *un groupe. On appelle sous-groupe de* $G$*, un sous-ensemble* $H \subset G$ *tel que* :
*1)* $H$ *est stable par la multiplication*
*ie* $\forall\,(x, y) \in H^2$*; on a* $xy \in H$*.*
*2) l'élément neutre de* $G$ *est dans* $H$*.*
*3)* $H$ *est stable par inversion c'est-à-dire pour tout* $x$ *de* $H$*, l'inverse de* $x$ *pour la loi* $(\cdot)$ *de* $G$ *est dans* $H$*.*

**Remarque 1.1.1** *l) L'ensemble* $H$ *étant muni de la loi de groupe induite par la loi* $(\cdot)$ *de* $G$*. Le sous-ensemble* $\{e\}$ *et* $G$ *d'un groupe* $G$ *définissent des sous-groupes de* $G$*.*
*2)* $H \subset G$ *est un sous groupe de* $(G, \cdot)$ *ssi* $\forall\,(x, y) \in H^2$*; on a* $xy^{-1} \in H$*.*

## 1.2 Anneau

**Définition 1.2.1** *On appelle anneau un ensemble* $A$ *muni de deux lois de composition internes: l'addition (notée en général "*$+$*") et la multiplication (notée en général "*$\cdot$*") satisfaisant les axiomes suivants* :
*1)* $(A, +)$ *est un groupe abélien.*
*2) La multiplication est associative et distributive à droite et à gauche par rapport à l'addition, c'est-à-dire satisfait* :
*i)* $\forall (a, b, c) \in A^3 :\ (ab)c = a(bc)$
*ii)* $\forall (a, b, c) \in A^3 :\ (a + b)c = ac + bc$ *et* $a(b + c) = ab + ac$*.*
*On note l'anneau* $A$ *par* $(A,+,\cdot)$*.*
*La multiplication admet un élément neutre (notée en général* $1_A$*, ou* $1$ *si aucune confusion n'en résulte, et appelé élément unité de* $A$ *).*

### 1.2.1 Anneau commutatif

**Définition 1.2.2** *Un anneau* $(A, +, \cdot)$ *est dit* ***commutatif*** *si la loi* $(\cdot)$ *de multiplication est commutative.*

### 1.2.2 Quelques types d'anneaux

#### Anneaux intégres

**Définition 1.2.3** *Soit $(A,+,\cdot)$ un anneau commutatif. On dit que $a \in A$ est un diviseur de zéro si $a \neq 0$ et s'il existe un élément $b$ de $A$ non nul tel que $ab = 0$.*

**Définition 1.2.4** *L'anneau $(A,+,\cdot)$ est dit **intégre** s'il est différent de $\{0\}$, et sans diviseur de $0$ c'est-à-dire,*
*$\forall\,(a,b) \in A^2$, on a $\qquad ab = 0 \Longrightarrow a = 0$ ou $b = 0$.*

**Exemple 1.2.1** *1) $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$et $(\mathbb{C},+,\cdot)$,sont des anneaux intègres.*
*2) $\mathbb{Z}/6\mathbb{Z}$ n'est pas un anneau intègre puisque $\overline{2} \times \overline{3} = \overline{6} = \overline{0}$.*

#### Anneau factoriel

**Définition 1.2.5** *Un élément $a$ d'un anneau $(A,+,\cdot)$ est dit irréductible si*
*$(\forall\,(b,c) \in A^2;\ a = bc) \Longrightarrow (b$ ou $c$ est inversible mais pas les deux$)$.*

**Définition 1.2.6** *Un anneau commutatif $A$ est dit factoriel s'il satisfait les trois propriétés suivantes*:
*1) $A$ est intégre.*
*2)Tout élément non nul $a$ de $A$ s'écrit comme produit*

$$a = up_1 \times .... \times p_r$$

*avec $u \in A^*$ et les $p_i$ irréductibles $i = 1.....r$ ($A^*$ est les éléments inversibles de $A$).*
*3) Il y a unicité de cette décomposition au sens suivant : si $a = vq_1 \times .... \times q_s$ est une autre, alors $r = s$ et il existe une permutation $\delta$de $\{1,....,r\}$ tel que pour tout $i$ de $\{1,....,r\}$, les élements $p_i$ et $q_{\delta(i)}$ soient associés .*

#### Anneau produit

**Définition 1.2.7** *Soient $A_1$ et $A_2$ deux anneaux. On appelle **anneau produit** des anneaux $A_1$et $A_2$, et on note $A_1 \times A_2$ l'ensemble $A_1 \times A_2$ muni des lois définies par :*
*$(a_1,b_1)+(a_2,b_2) = (a_1+a_2, b_1+b_2)$*
*$(a_1,b_1)\cdot(a_2,b_2) = (a_1a_2, b_1b_2)$, avec $a_1,a_2 \in A_1$ et $b_1,b_2 \in A_2$.*

### 1.2.3 Sous-anneau

**Définition 1.2.8** *soient $A$ un anneau et $B$ une partie de $A$. on dit que $B$ est un sous anneau de $A$ si* $\forall (a\ , b) \in B \times B$
*i)* $a - b \in B$.
*ii)* $ab \in B$.

### 1.2.4 Idéal dans un anneau

**Définition 1.2.9** *Soit* $(A, +, \cdot)$ *un anneau.* ***Un ideal à gauche*** $I \subseteq A$ $(resp.$**à droite**$)$ *est un sous-groupe additif* $(I, +) \subseteq (A, +)$, *stable par la multiplication à gauche (à droite) :* $AI \subseteq I$ $(resp. IA \subseteq I)$.
$I$ *est* ***bilatére*** *s'il est idéal à gauche et à droite, donc* $x \in I$ , $a, b \in A$ *implique* $axb \in I$

**Définition 1.2.10** *On dit qu'un idéal $I$ de $A$ est* ***premier*** *si :* $\forall x; y \in A$;

$$(x \cdot y \in I \Longrightarrow x \in I \text{ ou } y \in I).$$

**Définition 1.2.11** *On dit qu'un idéal $I$ de $A$ est maximal dans $A$ si il n'y a pas d'ideal $J \subseteq A$ tel que $I \subsetneq J \subsetneq A$.*

### 1.2.5 Morphisme d'anneaux

**Définition 1.2.12** *soient* $(A, +, \cdot), (B, +, \cdot)$ *deux anneaux unitaires et $\varphi$ une application de $A \longrightarrow B$.*
*On dit que $\varphi$ est un morphisme d'anneaux si,*
$\forall x, y \in A \times A$ *on a :*
*1)* $\varphi(x + y) = \varphi(x) + \varphi(y)$.
*2)* $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$.
*3)* $\varphi(1_A) = 1_B$.
*Le noyau et l'image du morphisme $\varphi$, sont définis par*

$$\ker \varphi = \{x \in A\ : \varphi(x) = 1_B\}$$

$$\operatorname{Im} \varphi = \{y \in B\ : \exists\ x \in A \text{ et } y = \varphi(x)\}$$

## 1.3 Corps

**Définition 1.3.1** *Un ensemble $k \neq \{0\}$ muni de deux lois $+, \cdot$ est appelé* ***corps*** *si et seulement si :*
*i) $(k, +, \cdot)$ est anneau.*
*ii) Tout élément de $k - \{0\}$ admet un inverse pour $(\cdot)$ dans $k$.*
*Si, de plus, $(\cdot)$ est commutative dans $k$, on dit $(k, +, \cdot)$ est un* ***corps commutatif***

**Exemple 1.3.1** *L'ensemble $\mathbb{Q}$ des nombres rationnels, muni de l'addition et de la multiplication ordinaires, est un corps commutatif. De même, l'ensemble $\mathbb{R}$ des nombres réels et l'ensemble $\mathbb{C}$ des nombres complexes .*

**Théorème 1.3.1** *Si $(k, +, \cdot)$ est un corps, alors $(k^*, \cdot)$ est un groupe multiplicatif.*
*telque $k^* = k/\{0\}$*

**Preuve.** Si $a \in k^*$, on a aussi $a^{-1} \in k^*$, car les relations :

$$aa^{-1} = a^{-1}a = 1_k$$

prouvent que $a^{-1} \neq 0_k$.
Si $a \in k^*$et $b \in k^*$, on a :

$$(ab) \cdot \left(b^{-1} \cdot a^{-1}\right) = a \ \left(b \cdot b^{-1}\right) a^{-1} = a \cdot 1_k \cdot a^{-1} = 1_k$$

et de même, on montre que $(b^{-1} \cdot a^{-1}) \cdot (ab) = 1_k$, ce qui prouve que $ab$ est inversible, et que $(ab)^{-1} = b^{-1} \cdot a^{-1}$. En particulier, $ab \in k^*$. Donc $k^*$est stable pour la multiplication .
On a : $1_k \in k^*$car, par hypothèse, $1_k \neq 0_k$. Donc la multiplication définit sur $k^*$ une loi associative, d'élément neutre $1_k$; et si $a \in k^*$, l'élément $a^{-1}$, qui appartient à $k^*$, est inverse de $a$ pour cette loi. Ceci achève de prouver que $k^*$, muni de la multiplication, est un groupe. Ce groupe (que l'on note encore $k^*$)est appelé **groupe multiplicatif du corps** $k$. ■

**Remarque 1.3.1** *Pour que le corps $k$ soit* ***commutatif,*** *il faut et il suffit que le groupe multiplicatif $k^*$ soit* ***abélien*** *.*

### 1.3.1 Sous-corps

**Définition 1.3.2** *Une partie $L$ d'un corps $k$ est appelée un sous-corps de $k$ si, et seulement si :*

*i) $L$ est stable pour l'addition et la multiplication de $k$ .*

*ii) $L$ Muni des deux lois internes $(x\ , y) \mapsto x+y$ et $(x\ , y) \mapsto x \cdot y$ l'ensemble $L$ est un corps.*

*Autrement dit, $L$ est un sous corps de $k$ si et seulement si :*

*1) $\forall\,(a,b) \in L^2 : a-b \in L$.*

*2) $\forall\,(a,b) \in L \times L - \{0\}\,, ab^{-1} \in L$.*

### 1.3.2 Corps premier

**Définition 1.3.3** *On dit que le corps $\mathbb{Q}$, ainsi que les corps $\mathbb{Z}\ /P\mathbb{Z}$ sont des **corps premiers**.*

*Plus génaralement, on apellera **corps premier**, tout corps isomorphe soit à $\mathbb{Q}$, soit à un corps du type $\mathbb{Z}\ /P\mathbb{Z}$.*

#### Sous-corps premier d'un corps

**Définition 1.3.4** *$k$ étant un corps, soit $\{k_i\}_{i\ \in I}$ la famille des sous-corps de $k$.Cette famille est non vide.*

*Posons $\triangle :\ = \cap_{i\ \in I} k_i$; $\triangle$ est alors le plus petit sous-corps de $K$ .*

*Donc, $\triangle$ est appelé le **sous-corps premier** de $k$.*

#### Propriétés des sous-corps

Si $L$ est un sous-corps du corps $k$, alors :

1) $L$ est **un sous-groupe additif de** $k$. Il en résulte que l'élément nul du corps $L$ **n'est autre que** $0_K$ on a $(0_K = 0_L)$.

2) $L^*$**est un sous-groupe du groupe multiplicatif de** $k^*$. Il en résulte que **l'élément** unité de $L$ est $1_k$ $(1_L = 1_k)$, ceci puisque l'élément neutre du groupe $k^*$ est aussi l'élément neutre de chacun de ses sous-groupes.

### 1.3.3 Caractéristique d'un corps

**Définition 1.3.5** *Soient $k$ un corps et $\varphi : \mathbb{Z} \longrightarrow k$ est une application définit par $\varphi(n) = n.1 = 1 + ... + 1$.Est un homomorphisme d'anneaux .*
*on a $\ker\varphi$ est un idéal de $\mathbb{Z}$:*
*1) Si $\varphi$ injectif : $\ker\varphi = \{0\}$, on dit que le corps $k$ est de caractéristique $0$ (ou par fois infinie ).*
*2) Si $\varphi$ non injectif : $\ker\varphi = p\mathbb{Z}$, où $p$ est un nombre premier, on dit que $k$ est de caractéristique $p$ ou d'exposant caractéristique $p$. Les corps de caractéristiques premier sont dits de caractéristiques positives .*

**Exemple 1.3.2** *Les corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont de caractéristique $0$.*
*Pour $p$ nombre premier, le corps $\mathbb{Z}/p\mathbb{Z}$ est de caractéristique $p$.*

# Chapitre 2

# Extension de corps

## 2.1 Extension de corps

**Définition 2.1.1** *Soit $K$ un corps , on appelle une extension de $K$, tout corps $L$ contenant un sous corps isomorphe à $K$.*
*Si $L$ est un corps tel que $K \subset L$, on dit que $L$ est une extension de $K$.*

**Définition 2.1.2 (K-morphisme)** *Si $L$ et $L^{'}$ sont deux extensions d'un même corps $K$, un $K$-morphisme $\varphi : L \to L^{'}$ est un morphisme de corps $\varphi$ tel que $\varphi_{|K}$ est l'identité.*
*i.e* $\forall \alpha \in K, \varphi(\alpha x) = \alpha \varphi(x)$.

**Exemple 2.1.1** *1) $\mathbb{C}$ et $\mathbb{R}$ sont des extensions de $\mathbb{Q}$. Plus généralement, tout corps est une extension de son sous-corps premier.*
*2)* $E = \mathbb{Q}\left(\sqrt{2}\right) = \left\{p + q\sqrt{2}; (p,q) \in \mathbb{Q}^2\right\}$, *alors $E$ est une extension de $\mathbb{Q}$.*

**Exemple 2.1.2** *1) Tout corps de caractéristique* 0 *est une extension du corps $\mathbb{Q}$.*
*2) Tout corps $K$ est un sous-corps du corps $K(x)$ des fractions rationnelles à coefficients dans $K$, donc $K(x)$ est une extension de $K$.*

### 2.1.1 Extension intermédiaire

**Définition 2.1.3** *On dira qu'un corps $L$ est un corps intermédiaire pour une extension $E/K$, si $K \subseteq L \subseteq E$, on dit alors que $L/K$ et $E/L$ sont des sous-extensions de $E/K$.*

**Proposition 2.1.1** *E extension d'un corps K alors E est un K−espace vectoriel.*

Soit $\alpha, \beta \in \mathbb{C}$ tel que $\alpha = a + ib, \beta = c + id$ avec $a, b, c$ et $d \in \mathbb{R}$,

1) la lois interne $(+)$ défini comme suit :

$+ : \mathbb{C}^2 \longrightarrow \mathbb{C}\ (\alpha, \beta) \longrightarrow\ \alpha + \beta = (a + b) + i\ (c + d)$.

2) la lois externe $(\cdot)$ défini comme suit :

$\cdot : \mathbb{R} \times \mathbb{C} \to \mathbb{C}\ (\lambda, a + ib) \longrightarrow (\lambda \times a) + i\ (\lambda \times b)$.

La famille $\{1, i\}$ est une base de l'espace $\mathbb{C}$ sur $\mathbb{R}$.

### 2.1.2 Extension par adjonction

**Définition 2.1.4** *Soient L /K une extension et M partie de L. Le plus petit sous-corps de L contenant K et M s'appelle le sous-corps de L engendré sur K par M, ou encore la sous-extension de L /K engendrée par M. Ce corps se noté K (M), ou K (α1, ..., αn) si M est fini, M = {α1, ..., αn}.*

**Exemple 2.1.3** $\mathbb{C} = \mathbb{R}(i)$. *Si* $M = \emptyset$, *alors* $K(M) = M$.

**Proposition 2.1.2** *Pour n > 1, le corps K (α1, α2, ..., αn) peut être considéré comme l'extension de K obtenue par les adjonctions successives de α1, α2, ..., αn.*

*C'est -à-dire que :*

$K(\alpha_1, \alpha_2) = K(\alpha_1)(\alpha_2), K(\alpha_1, \alpha_2, \alpha_3) = K(\alpha_1, \alpha_2)(\alpha_3), ..., K(\alpha_1, \alpha_2, ..., \alpha_n) = K(\alpha_1, \alpha_2, ..., \alpha_{n-1})(\alpha_n)$

**Preuve.** On démontre ce résultat par récurrence sur $n$.

Supposons $n = 2$; les éléments $\alpha_1$ et $\alpha_2$ étant, par hypothése, dans le corps $L$, $K(\alpha_1, \alpha_2)$ est le plus petit sous-corps de $L$ contenant $K$, $\alpha_1$ et $\alpha_2$. Or on a $K(\alpha_1) \subseteq K(\alpha_1, \alpha_2)$ et $\alpha_2 \in K(\alpha_1, \alpha_2)$,d'ou

$$K(\alpha_1)(\alpha_2) \subseteq K(\alpha_1, \alpha_2) \subseteq L.$$

Le corps $K(\alpha_1)(\alpha_2)$ étant un sous corps de $L$, contenant $K$ , $\alpha_1$ et $\alpha_2$, on en déduit que

$$K(\alpha_1, \alpha_2) = K(\alpha_1)(\alpha_2).$$

Supposons $n > 2$; si $K(\alpha_1, \alpha_2, ..., \alpha_{n-1})$ est l'extension de $K$ obtenue par les adjonctions successives de $\alpha_1, \alpha_2, ..., \alpha_{n-1}$, alors le raisonnement fait pour $n = 2$, permet de prouver que

$$K(\alpha_1, \alpha_2, ..., \alpha_n) = K(\alpha_1, \alpha_2, ..., \alpha_{n-1})(\alpha_n),$$

d'ou le résultat énoncé. ■

**Remarque 2.1.1** *l'extension $K(\alpha_1, \alpha_2, ..., \alpha_n)$ de $K$ est indépandante de l'ordre dans lequel sont faites les adjonctions des $\alpha_i$, $1 \leq i \leq n$.*
*On a, en particulier*

$$K(\alpha_1, \alpha_2) = K(\alpha_1)(\alpha_2) = K(\alpha_2)(\alpha_1).$$

**Cas particuliers** :

1) Pour $T = \{\alpha\}$, où $\alpha \in L$, $K(T)$ s'écrit $K(\alpha)$ est dite **extension simple** de $K$, obtenue par l'adjonction de $\alpha$ à $K$.
On note que si $\alpha \in K$ alors $K(\alpha) = K$
2) Plus généralement, pour $T = \{\alpha_1, \alpha_2, ..., \alpha_n\}$, où $n \in \mathbb{N}^*$et les $\alpha_i$, $1 \leq i \leq n$, sont des éléments de $L$, $K(T)$ est noté $K(\alpha_1, \alpha_2, ..., \alpha_n)$ et appelé extension de $K$ obtenue par l'adjonction de $\alpha_1, \alpha_2, ..., \alpha_n$ à $K$.

**Définition 2.1.5** *On dit que $E$ une extension de $K$ simple si et seulement si, il existe $\alpha \in E$ où $E = K(\alpha), K(\alpha)$ appellé extension simple sortie en ajoutant élément primitif.*

**Exemple 2.1.4** *1)* $\mathbb{C} = \{\alpha + \beta i; (\alpha, \beta) \in \mathbb{R}^2, i^2 = -1\} = \mathbb{R}(i)$.
*2)* $\{p + qi\ ; (p, q) \in \mathbb{Q}^2, i^2 = -1\} = \mathbb{Q}(i)$.
*3)* $\left\{p + q\sqrt{2}; (p, q) \in \mathbb{Q}^2\right\} = \mathbb{Q}\left(\sqrt{2}\right)$.

**Exemple 2.1.5** *On démontre que* $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$. *On a d'une part*
$\sqrt{2} + \sqrt{3} \in \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) \Longrightarrow \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right) \subseteq \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$.
*D'autre part, vérifions que* $\sqrt{2}$ *et* $\sqrt{3}$ *appartient à* $\mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$.

$\left(\sqrt{2}+\sqrt{3}\right)^2 = 5+2\sqrt{6} \Rightarrow \sqrt{6} \in \mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$
$\sqrt{6}\left(\sqrt{2}+\sqrt{3}\right) = 2\sqrt{3}+3\sqrt{2} = 2\left(\sqrt{2}+\sqrt{3}\right)+\sqrt{3}$ *d'où* $\sqrt{3} \in \mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$ ;
*on déduit que* $\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$ *et par suite* $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$ *donc*
$\sqrt{2}+\sqrt{3}$ *est un élément primitif pour l'extension* $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}$.

### 2.1.3 Degré d'une extension de corps

**Définition 2.1.6** *Soit $E$ une extension d'un corps $K$. La dimension de $E$ comme $K$ espace vectoriel est appelée degré de l'extension $E$ sur $K$ et notée $[L : K]$.*
*L'extension $E$ est dite de degré fini de $K$ si $[L : K]$ est fini. Une extension de degré 2 est appelée extension quadratique.*

**Exemple 2.1.6** *1)* $[C : R] = 2$.
*2)* $\mathbb{R}$ *est une extension infinie de* $\mathbb{Q}$, *puisque* $\mathbb{Q}$ *est dénombrable.*

**Définition 2.1.7** *Compte tenu des hypothéses ci-dessus,* $[L\colon K]$ *est appelé* ***degré*** *de l'extension $L/K$ ( ou* ***degré*** *de $L$ sur $K$ ).*
*i) Si $L$ est de dimension finie sur $K$, on dit que $L$ est une extension de* ***degré fini*** *sur $K$ et* $[L\colon K] = \dim_k L$.
*ii) Si $L$ est de dimension infinie sur $K$, on dit que $L$ est une extension de* ***degré infini*** *sur $K$.*

**Remarque 2.1.2** $L = K \iff [L\colon K] = 1$.

**Exemple 2.1.7** *1) Si $E/K$ est une extension telle que $[E : K] = 1$, alors $E = K$.*
*2)* $[\mathbb{C} : \mathbb{R}] = 2$.
*3)* $\mathbb{R}$ *est une extension infinie de* $\mathbb{Q}$, *puisque* $\mathbb{Q}$ *est dénombrable.*

**Théorème 2.1.1** *Quelles que soient les extensions des corps $L/K$ et $M/L$, on a*

$$[M : K] = [M : L] \times [L : K]. \tag{1}$$

**Preuve.** On suppose $K \subseteq L \subseteq M$.
Soit $\{x_i\}_{i\in I}$ une base de $L$ sur $K$ et $\{y_j\}_{j\in J}$ une base de $M$ sur $L$, où $I$ et $J$ sont des

ensembles non vides.

Montrons que $\{x_i y_j\}_{(i\ ,j)\in I\times J}$ est une base de $M$ sur $K$.

Soit $z \in M$ ; $z = \sum_{j\in J} \alpha_j y_j$, où les $\alpha_j$ sont des éléments de $L$, nuls, sauf un nombre fini d'entre eux ( ce que l'on exprime aussi, en disant que les $\alpha_j$ sont presque tous nuls dans $L$).

Pour tout $j \in J$, $\alpha_j = \sum_{i\in I} \beta_{ij} x_i$,les éléments $\beta_{ij}$ étant presque tous nuls dans $K$; alors $z = \sum_{i\ \in I, j\ \in J} \beta_{ij} x_l y_j$,les $\beta_{ij}$ étant presque tous nuls dans $K$.

On en déduit que la famille $\{x_i y_j\}_{(i,j)\in I\times J}$ est une partie génératrice de l'espace vectoriel $M$ sur $K$; montrons que c'est aussi une partie libre sur $K$.

Supposons $\sum_{i\ \in I, j\ \in J} c_{ij} x_i y_j = 0$,les $c_{ij}$ étant presque tous nuls dans $K$.

On peut alors écrire

$$\sum_{j\in J} \left( \sum_{i\in I} c_{ij} x_i \right) y_j = 0.$$

Or $\{y_j\}_{j\in J}$ est une base de $M$ sur $L$ et pour tout $j \in J, \sum c_{ij} x_i \in L$ par suite

$$\sum_{i\in I} c_{ij} x_i = 0, \forall j \in J \Longrightarrow c_{ij} = 0, \forall\, (i,j) \in I \times J$$

puisque $\{x_i\}_{i\in I}$ est une base de $L$ sur $K$.

Ainssi la famille $\{x_i y_j\}_{(i,j)\in I\times J}$ est une partie libre et génératrice du $K$ espace vectoriel $M$, c'est donc une base de $M$ sur $K$.

D'autre part, on a

$$card\,(I \times J) = card\,(I) \times card\,(J)\,;$$

on en déduit la relation (1). ■

**Remarque 2.1.3** *a) On écrira souvent* $[L : K] < \infty$ *pour exprimer que l'éxtension* $L\ /K$ *est de degré fini .*

*b) Dans la relation (1),*

$$[M\ : K] < \infty \Longrightarrow [M\ : L] < \infty\ et\ \ [L\ : K] < \infty.$$

*D'une façon générale, si deux des degrés qui figurent dans la relation (1) sont finis, le troisiéme est fini et dans ce cas , les entiers* $[M\ : L]et\ [L\ : K]$ *divisent l'entier* $[M\ : K]$ *.*

**Conclusion 2.1.1** *Soit $L\ /K$ une extension de corps, de degré fini ; si $\{K_i\}_{1\leq\ i\leq r}$ ,*
*$r \geq 1$, est une famille finie, totalement ordonnée, de corps intermédiaires, alors :*

$$K \subseteq K_1 \subseteq K_2 \subseteq ... \subseteq K_r \subseteq L$$

*implique*

$$[L\colon K] = [L\colon K_r]\,[K_r\colon K_{r-1}]\,...\,[K_1\colon K]\,.$$

**Remarque 2.1.4** *Soit $L\ /K$ une extension d'un corps et $B = \{x_i\}_{i\in I}$ une base de $L$ sur $K$; alors $L$ peut toujours être considéré comme obtenu par l'adjonction de $B$ à $K$.*
*En effet, $B \subseteq L$ et $K \subseteq L$, donc l'extension $K(B)$, obtenue par l'adjonction de $B$ à $K$, est un sous-corps de $L$. D'autre part, tout $x \in L$ s'écrit, de façon unique,*
*$x = \sum_{i\in I}\alpha_i x_i$, les $\alpha_i$ étant presque tous nuls dans $K$.*
*Par suite, tout élément de $L$ est dans $K(B)$, on en conclut que $L = K(B)$.*
*En particulier, si $[L\ :\ K] = n \in \mathbb{N}^*$ et si $\{x_i\}_{1\leq\ i\ \leq\ n}$ est une base de $L$ sur $K$, alors*

$$L = K(x_1, x_2, ..., x_n)\,.$$

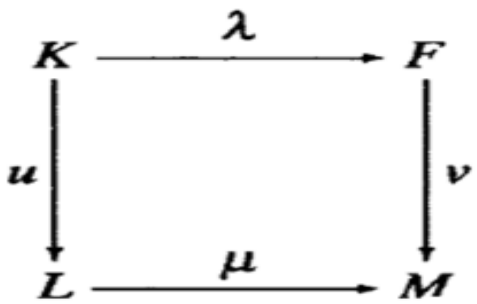
### 2.1.4 Isomorphismes d'extensions de corps

**Rappel**

1) Deux corps $K$ et $F$ sont dits isomorphes s'il existe un isomorphisme d'anneaux unitaires de $K$ sur $F$.

2) Etant donné un corps $K$, une extension $L\ /K$ est définie par la donné d'un couple $(L\ , u)$, où $u$ est un plongement
de $K$ dans $L$.

**Définition 2.1.8** *Soit $K$ et $F$ deux corps isomorphes. On dira que les **extensions** $L\ /K$ et $M\ /F$, respectivement définies par les couples $(L\ , u)$ et $(M\ , \upsilon)$, sont **isomorphes**, s'il existe un couple d'isomorphismes $(\lambda\ , \mu)$, respectivement, de $K$ sur $F$ et $L$ sur $M$, tel que le diagramme suivant commute :*



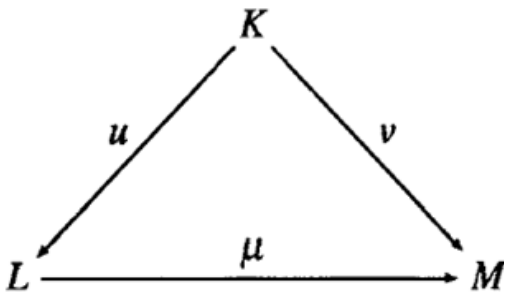

*c'est-à-dire* $\mu \circ u = \nu \circ \lambda$.
*On dit alors, que le couple* $(\lambda\ , \mu)$ *est un* ***isomorphisme d'extensions de corps*** *de* $L\ /K$ *sur* $M\ /F$.

**cas particuliers**

1) Si $K \subseteq L$ et $F \subseteq M$, $u$ et $\nu$ étant alors, respectivement, les injections canoniques de $K$ dans $L$ et $F$ dans $M$, on a

$$\mu \circ u = \nu \circ \lambda \Longleftrightarrow \mu_{|K} = \lambda$$

2) Si $K = F$ et $\lambda = id_K$, le diagramme commutatif devient:



d'où $\mu \circ u = \nu$.

Si de plus, $u$ et $\nu$ sont les injections canoniques, alors

$$\mu \circ u = \nu \iff \mu_{|K} = id_K$$

et dans ce cas, on dit que $\mu$ est un **K isomorphisme** de $L$ sur $M$.

Les corps $L$ et $M$ sont alors $K$ **isomorphes** (dans certins ouvrages, on dit que les corps $L$ et $M$ sont conjugués sur $K$ ).

## 2.2 Extensions Algébriques et extensions Transcendentes

### 2.2.1 Extensions Algébriques

**Nombre et extension algébrique**

**Définition 2.2.1** *Soit $E$ /$K$ une extension. Un élément $\alpha$ de $E$ est **algébrique** sur $K$ s'il existe*

$$P(X) \in K\ [X]\ \text{tel que } P(\alpha) = 0.$$

**Définition 2.2.2** *Une extension $E$ /$K$ est **algébrique** si tout élément de $E$ est algébrique sur $K$.*

**Proposition 2.2.1** *Soient $E$ /$K$ une extension et $\alpha$ un élément de $E$.*
*Les propositions suivants sont équivalentes.*
*i) $\alpha$ est algébrique sur $K$.*
*ii) Le corps $K(\alpha)$ est isomorphe à $K\ [\alpha]$.*
*iii) $K\ [\alpha]$est un $K$ espace vectoriel de dimension finie.*

**Démonstration.** cf [5] . ■

**Proposition 2.2.2** *Une extension de degré finie est algébrique.*

**Démonstration.** Soient $E$ /$K$ une extension finie et $\beta \in E$; puisque $\dim_K (K(\beta)) \leq \dim_K (E)$ ; il existe un entier $n$ tel que $1, \beta, ..., \beta^n$ soient linéairement indépendants. Il existe

donc des éléments $\alpha_0, ..., \alpha_n$ de $K$ tels que $\alpha_0 + ... + \alpha_n\beta^n = 0$. Autrement dit, il existe un polynôme $P(X\ ) \in K[X]$ telque $P(\beta) = 0$. ■

**Proposition 2.2.3** *Pour qu'une extension $E\ /K$ soit algébrique, il faut et il suffit que tout anneau $A$, tel que $K \subset A \subset E$, soit un corps.*

**Démonstration.** Soient $E\ /K$ une extension algébrique et $A$ un anneau tel que $K \subset A \subset E$. Tout élément non nul $\alpha \in A$ étant algébrique, le sous-anneau de $A$ engendré par $K$ et $\alpha$ est égal au corps $K(\alpha)$, donc $\alpha$ est inversible dans $A$. Réciproquement, supposons que tout anneau $A$ vérifiant $K \subset A \subset E$ soit un corps. Pour tout élément $\alpha \in E$ on a $K \subset K[\alpha] \subset E$, donc $K[\alpha]$ est un corps et $\alpha$ est inversible dans $K[\alpha]$, i.e. il existe $f(x) \in K[X]$ tel que $\alpha^{-1} = f(\alpha)$. On a donc $\alpha f(\alpha) - 1 = 0$, i.e. $\alpha$ est algébrique. ■

**Théorème 2.2.1** *Soient $E\ /K$ une extension et $\alpha \in E$ un élément algébrique sur $K$.Alors,*
*1) Il existe un unique polynôme irréductible unitaire $M_\alpha(X) \in K[X\ ]$ tel que $M_\alpha(\alpha) = 0$.*
*2) Tout polynôme $P(X) \in K[X]$ tel que $P(\alpha) = 0$ est divisible par $M_\alpha(X)$.*
*3) Le corps $K(\alpha)$ est isomorphe à $K[X]\ /(M_\alpha(X))$ et $[K(\alpha) : K]$ est égale au degré du polynôme $M_\alpha(X\ )$. En posant ce degré égal à $n$, les éléments $1, \alpha, ..., \alpha^{n-1}$ forment une base du $K$ espace vectoriel $K(\alpha)$*

**Démonstration.** cf [5]. ■

**Polynôme minimal**

**Définition 2.2.3** *Le polynôme $M_\alpha(X)$ est appelé* ***le polynôme minimal*** *de $\alpha$ sur $K$. L'entier $\deg(M_\alpha(X)) = [K(\alpha) : K]$ est appelé le degré de $\alpha$ sur $K$.*

**Remarque 2.2.1** *1) L'extension $A\ /\mathbb{Q}$ étant algébrique, $A$ est dénombrable.*
*2) On remarque que tout polynôme irréductible unitaire de $K\ [X\ ]$est un polynôme minimal de ses racines dans une extension $E$ de $K$ (s'il admet des racines dans $E$). Une question, importante dans la suite, est de savoir, lorsque ce polynôme admet des racines dans $E$, si elles sont simples.*

### 2.2.2 Extensions Trancsendantes

**Définition 2.2.4** *Soit $E$ /$K$ une extension. Un élément de $E$ qui n'est pas algébrique sur $K$ est dit* ***transcendant*** *sur $K$. Si l'extension $E$ n'est pas algébrique elle est dite* ***transcendante*** *(sur $K$).*

**Remarque 2.2.2** *Un élément $\alpha \in E$ est transcendant sur $K$ si et seulement si les éléments $\alpha^n, n \in \mathbb{N}$, sont linéairement indépendants sur $K$. Dans ce cas, $dim_K K(\alpha) = +\infty$ :il en est donc de même pour $dim_K E$.*

#### Extension trancsendantes pure

**Définition 2.2.5** *Une extension $E$ /$K$ est dite extension* ***transcendante pure*** *de $K$ s'il existe une famille $(\alpha_i)_{i\in I}$ d'éléments de $E$, algébriquement libre sur $K$ et telle que $E = K(\alpha_i)_{i\in I}$. Une telle famille est appelée* ***base pure*** *de $E$ sur $K$.*

**Théorème 2.2.2** *Pour qu'une extension $E$ /$K$ soit transcendante pure, de base pure $(\alpha_i)_{i\in I}$, il faut et il suffit que $E$ soit isomorphe au corps $K(X_i)_{i\in I}$ des fractions rationnelles sur $K$.*

**Démonstration.**

i) Si $I = \emptyset, K$ est une extension transcendante pure de $K$.

ii) Si $I \neq \emptyset$,alors $\varphi : K\ [X_i]_{i\in I} \longrightarrow K\ [\alpha_i]_{i\in I}$ définie par $f \longrightarrow f\ (\alpha_i)$ est un isomorphisme, car surjective par définition de $K\ [\alpha_i]_{i\in I}$ et injective puisque les $(\alpha_i)_{i\in I}$ sont algébriquement libres. La propriété universelle du corps des fractions d'un anneau intègre montre que le corps des fractions de $K\ [\alpha_i]_{i\in I}$ est $E = K(\alpha_i)_{i\in I}$, d'où $K(\alpha_i)_{i\in I} \backsimeq K(X_i)_{i\in I}$. La réciproque est évidente. ■

#### Base de transcendance

**Définition 2.2.6** *Soit $E$ /$K$ une extension. On appelle* ***base de transcendance*** *de $E$ sur $K$ un élément maximal de l'ensemble, ordonné par inclusion, des parties de $E$ algébriquement libres sur $K$.*

**Degré de transcendance**

**Définition 2.2.7** *Soit $E/K$ une extension ayant une base de transcendance sur $K$ qui est finie. On appelle* ***degré de transcendance*** *de $E$ sur $K$ le cardinal d'une base de transcendance de $E$ sur $K$.*

**Remarque 2.2.3** *Il résulte de ce qui précède que si $E/K$ est une extension de degré de transcendance $n$, alors :*
*1) Tout système de générateurs a au moins $n$ éléments. S'il en existe un ayant $n$ éléments, c'est une base pure*
*(et $E$ est donc une extension pure de $K$).*
*2) Toute partie de $E$ algébriquement libre sur $K$ a au plus $n$ éléments. S'il en existe une ayant $n$ éléments, c'est une base de transcendance de $E$ sur $K$.*

# Chapitre 3

# Corps finis

## 3.1 Introduction

**Définition 3.1.1** *Un corps fini $K$ est un corps de cardinal fini.*
*ie* $card\,(k) = n \in \mathbb{N}$.

**Théorème 3.1.1** *L'anneau $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $n$ est un nombre premier.*

**Démonstration.** cf [8] . ■

**Notation 3.1.1** *On note $p$ nombre premier et $F_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.*

**Lemme 3.1.1** *Soit $K$ un corps fini de caractéristique $p$. Alors $K$ contient un sous corps isomorphe à $F_p$ (que l'on identifie à $F_p$), et son cardinal est de la forme $p^n$ avec $n \geq 1$.*

**Démonstration.** Soit $\varphi : \mathbb{Z} \longrightarrow k$ est un homomorphisme d'anneaux définit par $\varphi(n) = n.1 = 1 + ... + 1$.
Par le premier théorème d'isomorphisme on obtient que l'image de $\varphi$ était isomorphe à $F_p$. Identifions $Im\varphi$ et $F_p$. Le corps $K$ est un espace vectoriel sur $F_p$ de dimension finie $n$. Son $card\,(K)$ est donc bien $p^n$. ■

## 3.2 Caractéristique d'un corps fini

**Lemme 3.2.1** *Soit un corps $K$ son sous corps premier est isomorphe à un corps premier tel que*

*$car(k) = 0$ si et seulement si, si le sous corps premier de $K$ est isomorphe à $\mathbb{Q}$*

*$car(k) = p$ si et seulement si, si le sous corps premier de $K$ est isomorphe à $F_p$.*

**Théorème 3.2.1** *Soit $K$ un corps fini à $q$ éléments, de caractéristique $p$.*

*1) Si $n$ est la dimension de l'espace vectoriel $K$ sur $F_p$, on a $q = p^n$.*

*2) Tout élément $x$ de $K^*$ vérifie $x^{q-1} = 1$, ce qui implique $x^{-1} = x^{q-2}$.*

*3) Tout élément $x$ de $K$ vérifie $x^q = x$.*

*4) Soit $\alpha$ un élément primitif de $K$. La famille*

$$B = \left\{1, \alpha, \alpha^2, ..., \alpha^n\right\}$$

*est une base de l'espace vectoriel $K$ sur $F_p$, c'est-à-dire que tout élément $x$ de $K$ s'écrit d'une façon unique*

$$x = R(\alpha) \ \ avec\ R \in F_p[X]^{(n)}.$$

**Démonstration.**

1) $K$ est un espace vectoriel sur $F_p$ .Cet espace vectoriel est nécessairement de dimension finie puisque $K$ est fini. Soit $n$ cette dimension, et soit $\{b_1, b_2, ..., b_n\}$une base de $K$ sur $F_p$. Tout élément $x$ de $K$ s'écrit de façon unique

$$x = \alpha_1 b_1 + \alpha_2 b_2 + ... + \alpha_n b_n,$$

où chaque $\alpha_i$ de $F_p$ peut prendre $card F_p$ de valeurs distincts.

(2) et (3) Le groupe $K^*$ est d'ordre $(q-1)$ donc tout élément $x$ de $K^*$ vérifie

$$x^{q-1} = 1 = xx^{q-2},$$

d'où l'on déduit $x^q = x$, relation qui est aussi vérifie par 0.

4) Le corps $K$ étant un espace vectoriel de dimension $n$ sur $F_p$, montrons que la famille $B = \{1, \alpha, \alpha^2, ..., \alpha^n\}$ est libre.Supposons le contraire, une combinasion linéaire non identiquement nulle entre les $\alpha^i$ équivaut à l'existence d'un polynôme non constant $P$ de $F_p[X]^{(n)}$

tel que $p(\alpha) = 0$.

Soit $\lambda$ le sous $F_p$ espace vectoriel de $K$ engendré par la famille $B$. D'après notre hyppothèse, $\dim(\lambda) < n$ donc $\lambda$ est strictement inclus dans $K$. On en deduit que $(\lambda \setminus \{0\})$ est strictement inclus dans $K^*$.

Si l'on montre que $\lambda$ est une anneau, l'ensemble $(\lambda \setminus \{0\})$, qui contient $\alpha$, contiendra toutes la puissances positives de $\alpha$ et cela impliquera que $\alpha$ n'est pas un générateur de $K^*$, d'où contradiction.

par definition $\lambda$, on peut écrire $\lambda = \left\{ R(\alpha) \,|R \in F_p[X]^{(n)} \right\}$ .Possons

$$A = \{Q(\alpha) \,|Q \in F_p[X]\}.$$

Comme $A$ est un anneau, il suffit de montrer que $\lambda = A$.

Or il est clair que $\lambda \subseteq A$.Réciproquement, soit $Q$ un polynôme de $F_p[X]$, la division euclidienne de $Q$ par $p$ s'écrit

$$\begin{Bmatrix} Q = pQ_1 + R_1, \\ R_1 \in F_p[X]^{(n)}. \end{Bmatrix}$$

Comme $p(\alpha) = 0$, on voit que $Q(\alpha) = R_1(\alpha)$ appartient à $\lambda$ puisque $R_1$ est dans $F_p[X]$, ce qui prouve que $A \subseteq \lambda$, donc l'égalité. ■

**Théorème 3.2.2** *Soit $k$ un corps fini tel que $cardK = q$ Si $K$ est de caractéristque $p$, alors*

*1) $K$ est une extension de $F_p$ de degré $[k : F_p] = n$ et $q = p^n$.*

*2) Le sous corps premier de $K$ est isomorphe à $F_p$.*

**Démonstration.**

1) $k$ est un corps de caractéristique $p \neq 0$, donc $k$ est une extenstion de $F_p$ on peut supposer $F_p \subseteq k$, alors

$$F_p \subseteq k \text{ et } card(K) < \infty \implies [k : F_p] < \infty.$$

Posons $n = [k : F_p]$ ; ainsi $k$ est un espace vectoriel de dimension finie, $n$, sur $F_p$; d'où $k \backsimeq F_p^n$, ce qui implique $card(k) = p^n$.

2) evident. ■

**Remarque 3.2.1** *1) Tout corps fini (c'est-à-dire de cardinal) est nécessairement de caractéristique non nulle.*

*2) Le corps $\mathbb{Z}/p\mathbb{Z}$ est de cardinal $p$ et de caracteristique $p$, pour tout nombre premier $p$.*

*3) Si $V$ est un espace voctoriel sur un corps $K$ alors*:

$$\dim_k V = n \ < \infty \Longleftrightarrow V \backsimeq k^n.$$

## 3.3 Construction des corps finis

L'anneau $F_p[X]$ est un anneau principal car $F_p$ est un corps.

**Théorème 3.3.1** *Pour tout $p$ nombre premier et tout entier $n > 0$, il existe un polynôme irréductible de degré $n$ dans l'anneau $F_p[X]$.*

**Démonstration.** cf [5]. ■

**Théorème 3.3.2** *Soit $n \in \mathbb{N}^*$, on pose $q = p^n$ alors il existe un corps $k$ à $q$ élément, c'ést le corps de composition du polynôme $x^q - X$*
*on le note $F_q$.*

***Démonstration.*** *Si $K$ est un corps à $q$ éléments et si $x \in K$, alors $x^{q-1} = 1$*
*( Lagrange), donc tout élément de $K$ est racine de $X^q - X$. Or $X^q - X$ est à coefficients dans $F_p$ le sous corps premier de $K$. Donc $K$ est bien le corps de décomposition de $X^q - X$ sur $F_p$.*
*Réciproquement, soit $K$ le corps de décompisotion de $X^q - X$ sur $F_p$ et soit $k \subset K$ l'ensemble des racines de $X^q - X$. Alors $k$ est un corps. D'autre part le polynôme dérivé de $X^q - X$ est toujours non nul donc $X^q - X$ n'admet que des racines simples, donc $card(k) = q$. D'où $k = K$.* ■

On déduit, pour tout $n > 0$, l'existence d'un polynôme irréductible de degré $n$.
Soit $P(x) \in F_p[X]$ on a,

$$\pi : F_p[X] \to k = F_p[X]/(P)$$

alors $k$ est une extension de degré $[k : F_p] = n$ et d'apres le théoreme (3.2.2) $k$ corps à $p^n$ éléments.

**Théorème 3.3.3** *Soit $P$ un polynôme irréductible de degré $n$ de $F_p[X]$ et soit $k$ le corps $F_p[X]/(P)$. On désigne par $\alpha$ la classe d'équivalence du polynôme $X$ dans $k$.*
*Alors*
*1) Pour tout élément $x$ de $k$, il existe un polynôme $g$ de $F_P[X]$ et un seul, de degré au plus égal à $(n-1)$ tel que*

$$x = g(\alpha).$$

*2) La famille*

$$\left\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\right\}$$

*est une base, appelée base canonique, de l'espace vectoriel $k$ sur $F_p$.*
*3) Le corps $k$ posséde $p^n$ éléments.*

**Preuve.** cf [8] ■

**Exemple 3.3.1** ***( Le corps*** $F_8$*)*
*Soit $p(X) = X^3 + X + 1$.ce polynôme est irréductible sur le corps à deux éléments $F_2$.le quotient de l'anneau $\mathbb{Z}_2[X]$ des polynomes à coefficent dans $\mathbb{Z}_2$ par l'idéal engendré par $P$ est un corps que nous noterons $F_8$.*

## 3.4 L'endomorphisme de Frobenius

**Définition 3.4.1** *Soit $K$ un corps commuttif de caractéristique $p$, alors l'application*
$F : K \longrightarrow K$
$\alpha \longrightarrow \alpha^p$
*est un endomorphisme de $K$, appelé endomorphisme de Frobenius.*

**Remarque 3.4.1** *Si le corps $K$ est fini, alors $F$ est un automorphisme de $K$*
*et si $K = F_p$ alors , $F = id_{F_p}$.*

**Proposition 3.4.1** *Soit $K$ un corps fini de caractéristique $p$.*
$\forall (x, y) \in K^2$ *on a*
*i)* $(x+y)^p = x^p + y^p$.
*ii)* $(x+y)^{p^i} = x^{p^i} + y^{p^i}$ *pour tout* $i \geq 2$.

*iii)* $F_p = \{x \in K \ / \ x = x^p\}$ .

*iv) Soit* $G$ *un polynôme de* $K[X]$ *.On a l'équivalence*

$$(G \in F_p[X]) \Leftrightarrow (G(X^p) = G(X)^p).$$

**Démonstration.**

i) On développe $(x+y)^p$ par la formule du binôme de netwton, puis le coefficient binomial $C_p^k$ est divisible par $p$, donc est nul dans $F_p$.

iii) Le groupe $F_p^*$ est d'ordre $(p-1)$, tout élément $x$ de $F_p^*$ vérifie donc $x^{p-1} = 1$, d'où $x^p = x$, relation aussi verifiée par 0, donc $F_p \subseteq \{x \in K / x = x^p\}$ .

Réciproquement, le polynôme $X^p - X$ posséde au plus $p$ racines dans $K$, on a l'inégalité

$$card\{x \in K / x = x^p\} \leq card F_p.$$

iv) Soit $G(X) = \alpha_0 + \alpha_1 X + ... + \alpha_n X^n$ D'apres (i). on a

$$G(X)^p = \alpha_0^p + \alpha_1^p X^p + ... + \alpha_n^p (X^n)^p,$$

le résultat découle alors de (iii). ■

## 3.5 Propriétés des corps finis

**Théorème 3.5.1** *Si* $k$ *est un corps finis, alors toute extension de degré fini sur* $k$ *est une extension simple .*

**Preuve.** cf [5] . ■

**Corollaire 3.5.1** *Toute corps fini de la forme* $F_{p^n}$ *est une extension simple de* $F_p$.

**Théorème 3.5.2** *Si* $k$ *est un corps finis, alors le groupe multiplicatif* $k^*$ *est cyclique.*

**Démonstration.** Pour chaque diviseur $d$ de l'ordre du groupe $k^*$, l'enssemble

$$U_d = \left\{x \in k^* / x^d = 1\right\}$$

coïncide avec l'ensemble des racines distinctes du polynôme $\left(X^d - 1\right)$. On deduit que $cardU_d \leq d$.

Il en résulte que si $k$ est un corps à $q$ éléments, le groupe cyclique $k^*$, qui est d'ordre $(q-1)$, possède $f(q-1)$ générateurs.

Ces générateurs du groupe $k^*$en termes des $(q-1)$ premières puissances de $\alpha$, puisque

$$k^* = \{\alpha_i \ / \ i = 1, 2, ..., q-1\}.$$

Cela implique en particulier que si sous-corps $L$ de $k$ contient un élément primitif $\alpha$ de $k$, alors $L = k$. ■

**Théorème 3.5.3** *Deux corps finis qui ont méme nombre d'éléments sont isomorphes.*

**Preuve.** Soit $K$ et $K'$ deux corps à $p^n$ éléments, soit $\alpha$ un élément primitif de $K$, et soit $p$ le polynôme minimal de $\alpha$. On sait que $p$ apartient à $F_p[X]$ et est irréductible de degé $n$. de plus, $K$ est isomorphe au corps $F_p[X]/(p)$.

que $p$ admet $n$ racines distinctes dans le corps $K'$, soit $\beta$ l'une d'elles etant irréductible dans $F_p[X], p$ est le polynôme minimal de $\beta$. Ainsi $\beta$ est de degré $n$ sur $F_p$, cela signifie que $K'$ est isomorphe au corps $F_p[X]/(p)$.

L'isomorphisme de $K$ sur $K'$ n'a rien de canonique, il dépend du choix d'un élément primitif $\alpha$ de $K$ et d'un élément $\beta$ de degré algébrique $n$ de $K'$, mais attention, ce choix n'est pas unique. ■

## 3.6 Sous corps d'un corps fini

**Théorème 3.6.1** *Soit $K$ un corps de caractéristique $p$, à $q = p^n$ éléments.*

*1) Le nombre d'éléments de tout sous corps de $K$ est de la forme $p^r$, où $r$ divise $n$.*

*2) Réciproquement, pour chaque diviseur $r$ de $n$, l'ensemble des éléments de $K$ vérifiant*

$$x^{p^r} = x$$

*est l'unique sous corps de $K$ à $p^r$ éléments .*

**Démonstration.**

1) Le nombre d'éléments d'un sous corps de $K$ est de la forme $p^r$ d'après le théoréme (2) (dans caractéristique d'un corps fini) ,$p^n$ est une puissance de $p^r$ donc $r$ divise $n$.

2) Soit $r$ un diviseur de $n$. l'entier $(p^r - 1)$ divise l'ordre $(p^n - 1)$ du groupe cyclique $K^*$. Que les éléments de $K^*$ vérifiant $X^{p^r} = 1$ constituent un sous-groupe d'ordre $(p^r - 1)$ de $K^*$.

$$L = \{x \in K | x^{p^r} = x\}$$

posséde $p^r$ éléments.

Comme $L^*$ est un groupe multiplucatif, il reste à montre qui $L$ est un groupe additif.

On sait que $L$ est stable pour l'addition et que $0 \in L$. Soit $x$ un élément de $L$, montrons que $-x \in L$.

i) Si $p = 2$, on a $-x = x \in L$.

ii) Si $p > 2, p^r$ impair :

$$(-x)^{p^r} = -x^{p^r} = -x$$

c'est-à-dire $-x \in L$.

Ainsi $L$ est bien un corps . L'unicité vient du fait que si $L_1$ est un sous-corps à $p^r$ éléments de $K$, le groupe $L_1^*$ est d'ordre $(p^r - 1)$ donc tout élément $x \in L_1$ vérifie $x^{p^r} = x$, ce qui fait que $L_1 \subset L$ donc $L_1 = L$. ■

## 3.7 Existence et unicité de corps finis

### 3.7.1 Existence de corps finis

**Théorème 3.7.1** *Pour tout entier $n > 0$ et tout nombre premier $p$, il existe effectivement un corps ayant $q = p^n$ éléments.*

**Démonstration.** Montrons que le corps de décomposition $L$ du polynôme $p = x^q - x$ sur $F_p$ répond à la question. Pour cela notons $E$ l'ensemble des racines de $p$ dans $L$. Comme le polynôme dérivé de $p$ est égal à $-1$, les racines de $p$ sont simples, donc $card\,(E) = q$.On va montrer que $L$ coincide avec $E$. Si a et b sont deux racines de $p$, on a

$(a + b)^q = (a + b)^{p^n} = a^{p^n} + b^{p^n} = a^q + b^q = a + b$, ce qui prouve que $a + b \in E$ et d'autre

part, $(ab)^q = a^q b^q = ab$, ce qui prouve que $ab \in E$.
En fin, il est clair que $0, 1 \in E$ et que $a^{-1}E$.par conséquent, $E$ est un corps, donc $E = L$. ■

**Corollaire 3.7.1** *Pour tout entier $n > 0$ et tout nombre premier $p$, il existe un polynôme irréductible de degré $n$ dans $F_p[x]$.*

**Démonstration.** Le théoréme montre l'existence d'un corps $K$ à $p^n$ éléments, extension de degré $n$ de $F_p$.Soit $x$ un générateur de $K^*$ et notons $f : F_p[x] \to K$ l'homomorphisme défini par $f(x) = x$; $f$ est surjectif; son noyau est l'idéal des pôlynomes de $F_p[x]$.On a donc un isomorphisme $\varphi : \frac{F_p[x]}{(p)} \to K$. par conséquent, $p$ est un polynôme irréductible de degré $n$ dans $F_p[x]$, pour construire un corps de $p^n$ éléments, il suffit donc de savoir trouver un polynôme irréductible de degré $n$ dans $F_p[x]$. ■

### 3.7.2 Unicité de corps finis

**Proposition 3.7.1** *Soit $L$ un corps fini à $q = p^n$ éléments. Alors il est isomorphe au corps $F_q$ .*

**Démonstration.** Comme $card(L) = q = p^n$, le corps $L$ est de caractéristique $p$. Il contient donc le corps $F_p$. Soit $a \in F_q$ un élément primitif, $q_a \in F_p[X]$ son polynôme minimal. Le polynôme $q_a$ est de degré $n$, et

$$F_q = \{\lambda_0 + \lambda_1 a + \cdots + \lambda_{n-1} a^{n-1}, \lambda_i \in F_p\},$$

puisque $F_q \simeq \frac{F_p[x]}{(q_a(x))}$.
Comme $card(L) = q$, les éléments de $L$ vérifient aussi l'équation $x_q - x = 0$, et $L$ s'identifie aussi à l'ensemble des solutions de l'équation $x_q - x = 0$. Comme $q_a$ est un diviseur irréductible sur $F_p$ de $x_q - x$, il existe $b \in L$ tel que $q_a$ soit le polynôme minimal de $b$ ($b$ est une racine dans $L$ du polynôme $q_a$). Considérons l'application $f : F_q \longrightarrow L$ :

$$\lambda_0 + \lambda_1 a + ... + \lambda_{n-1} a^{n-1} \longrightarrow \lambda_0 + \lambda_1 b + ... + \lambda_{n-1} b^{n-1}.$$

Il est immédiat de vérifier que $f$ est un isomorphisme de corps. ■

# Bibliographie


[1] **Amara HITTA;** COURS D'ALGEBRE ET EXERCICES; OFFICE DES PUBLICATIONS UNIVERSITIARES; 07-2006.

[2] **A-NITTAJ.**Introduction aux courbes elliptiques. Université de Caen, Rabat. 29 octobre 2008.

[3] **Daniel GUIN et Thomas HAUSBERGER;** Algebre I. GROUPES; COURPS ET THÉORIE DE GALOIS; EDP sciences France.

[4] **Jean-Jaque RISLER et BOYER Pascal;** ALGÈBRE POUR LA LICENCE 3; Groupes, anneaux, corps; dunod Paris 2006.

[5] **Josette CALAIS** Extensions de corps; Théorie de Galois; niveau M1-M2.

[6] **J.Lelong FERRAND et J-M ARNAUDIÉS**; Cours de mathématiques; 1. Algébre; LES COURS DE RÉFÉRENCE; dunod mars 2003 Belgique.

[7] **Jean-Marie MOUNIER;** ALGÈBRE MPSI; Cours; méthodes et exercices corrigés; dunod; juin 2006 France.

[8] **Josette CALAIS** Extensions de corps; Théorie de Galois; niveau M1-M2.

[9] **Pierre WASSE** ; Arithmetique; Vuibert 2009 Paris.

## Résumé

Dans ce mémoire on a fait une étude superficielle sur le corps fini et ses caractéristique en donnant des définitions, des théorèmes, des démonstrations et des exemples.

Le corps fini est utilisé dans plusieurs domaines comme par exemple : les polynômes et les théorèmes de l'arithmétique numérique.



**Mots clés :** corps finis, nombre premier , extension de corps, isomorphisme de Frobenius.



## Abstract

In our project, we have studied; briefly, the finite field and its characteristics by giving definitions, theories, proofs and examples.

The finite field is used in many domain a such as: the study of polynomial; theories of informatics the theories of algebraic numerical



**Keywords:** finite field, prime number, expansion of the field, the isomorphism Frobenius.



## الملخص

لقد تطرقنا في هذه المذكرة إلى دراسة سطحية حول الحقل المنتهي وخصائصه بإعطاء تعاريف ، نظريات ، براهين وأمثلة .

يستعمل الحقل المنتهي في كثير من المجالات نذكر منها : دراسة كثيرات الحدود، نظريات الإعلام الآلي، النظريات الجبرية العددية .



**الكلمات المفتاحية :** الحقل المنتهي، الأعداد الأولية، توسعة الحقل ، تشاكل فروبينيس .