Ministère de l'enseignement supérieur
et de la recherche scientifique
* * * * *
université de Sfax
* * * * *
Faculté des sciences de Sfax

Corps finis

Projet réalisé par :
Dammak Yosr & Jarraya Ahmed
Encadré par Monsieur:
Ben Ammar Mabrouk

AU : 2023-2024

Table des matières

1 Introduction

un corps fini est un corps (commutatif) qui est par ailleurs fini. À isomorphisme près, un corps fini est entièrement déterminé par son cardinal qui est toujours de la forme p^n, une puissance d'un nombre premier. Ce nombre premier n'est autre que sa caractéristique et le corps se présente comme l'unique extension du corps premier $\mathbb{Z}/\mathrm{p}\mathbb{Z}$ de dimension n.

2 Généralités

2.1 Définition:(Groupe)

On appelle groupe un ensemble A muni d'une loi interne $\times$ telle que :
• La loi $\times$ est associative : $\forall$ x, y, z de A, on a : $x \times (y \times z) = (x \times y) \times z$.
• Il existe un élément neutre e : $\forall$ x de A, $x \times e = e \times x = x$.
• Tout élément possède un symétrique : $\forall$ x de A, il existe y de A avec $x \times y = y \times x = e$.
• La loi $\times$ est commutative, on parle de groupe commutatif (ou abélien). On peut prouver qu'un groupe admet un unique élément neutre et qu'un élément x admet un unique symétrique que l'on note souvent x^{-1}.

2.2 Définition:(Anneau)

On appelle un anneau la donnée d'un ensemble A et de deux lois de composition interne notées + et $\times$ sur A vérifiant les propriétés suivantes :
• (A, +) est un groupe abélien dont le neutre sera noté 0_A
• La loi $\times$ est associative : $\forall$ a, b, c $\in$ A, $a \times (b \times c) = (a \times b) \times c$
• La loi $\times$ possède un élément neutre noté 1_A unitaire.
• La loi $\times$ est distributive par rapport à la loi +, c.-à-d. que $\forall$ a, b, c $\in$ A, $a \times (b + c) = a \times b + a \times c$ et $(b + c) \times a = b \times a + c \times a$
• La loi $\times$ est commutative, on dit que l'anneau est commutatif.
Par exemple :$(\mathbb{Z}, \times, +)$, $(\mathbb{R}, \times, +)$, $(\mathbb{C}, \times, +)$ sont des anneaux commutatifs.
$(M_n(\mathbb{R}), \times, +)$ est un anneau qui n'est pas commutatif.

2.3 Définition:(corps)

Un corps est un anneau commutatif dans lequel tout élément non réduit à 0_K dont tous les éléments non nul est inversibles

.

2.4 exemple

$(\mathbb{R}, \times, +)$, $(\mathbb{C}, \times, +)$ sont des anneaux commutatifs et un corps.
$(\mathbb{Z}, \times, +)$ est un anneau commutatif mais n'est pas un corps.
$(M_n(\mathbb{R}), \times, +)$ est un anneau qui n'est pas commutatif.

3 Caractéristique d'un corps et propriétés :

Définition Le morphisme

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow \mathrm{K} \\ \mathrm{n} &\longmapsto \mathrm{n}.1 \end{aligned}$$

est l'unique morphisme de corps de $\mathbb{Z}$ dans K. Son noyau est un idéal de l'anneau principal $\mathbb{Z}$, il existe donc un entier p tel que $\mathrm{Ker}(\phi) = \mathrm{p}\,\mathbb{Z}$. Cet entier s'appelle caractéristique de p.

3.1 Exemple

R est un corps de caractéristique nulle. $\mathbb{Z}/\mathrm{p}\mathbb{Z}$ avec p premier est un corps de caractéristique p.

3.2 Proposition

La caractéristique d'un corps est nécessairement 0 ou un nombre premier. Si elle est nulle, il s'agit d'un corps infini.

3.3 Exemple

Il est possible d'avoir un corps infini de caractéristique p premier : le corps $F_p(\mathrm{X})$ des fractions rationnelles à coefficients dans F_p.

3.4 Définitin

Dans un corps $\mathbb{K}$ de caractéristique p première, on définit le morphisme de Frobenius :

$$\begin{aligned} \sigma : \mathrm{K} &\longrightarrow \mathrm{K} \\ \mathrm{X} &\longmapsto X^p \end{aligned}$$

3.5 Proposition

Le morphisme de Frobenius est un morphisme de corps, il est donc injectif. En particulier, si $\mathrm{K} = F_p$ avec p premier, alors le morphisme de Frobenius est l'identité.

4 Corps fini

Soit $\mathbb{P}$ = 2, 3, 5, 7, ... désigne l'ensemble des nombres premiers

4.1 Introduction, propriétés

Un corps fini (un corps dont l'ensemble sous-jasent est fini). On va élucider un peu la structure générale des corps finis, et expliquer comment on peut calculer concrètement dans les corps finis. On sait déjà que pour tout nombre p premier, l'anneau quotient $\mathbb{Z}/p\mathbb{Z}$, noté aussi F_p, est un corps fini.

Proposition

Soit K un corps fini et P ∈ K[X] un polynôme irréductible. Alors l'anneau quotient L= K[X]/⟨P⟩ est un corps fini, de cardinal $card(K)_{deg(P)}$.

Proposition

Tout anneau intègre fini est un corps fini.

4.2 construction d'un corps fini

Théorème

Soit p ∈ $\mathbb{P}$ F_p[X] est un anneau principal (car F_p=$\mathbb{Z}/p\mathbb{Z}$ est un corps)
Soit, s'il existe, P ∈ F_p[X] un polynôme irréductible de degré deg(P)=n.

Proposition

Tout corps de K est une extension de Q ou de $\mathbb{Z}/p\mathbb{Z}$ (p premier).

4.3 Extension d'un corps fini :

Définition

Soit K un corps. Une extension de K est une K-algèbre (K, i) où K est un corps c'est-à-dire un couple où K est un corps et i un morphisme d'anneaux unitaires.

Définition

L ⊂ K, donc K est une extension si L est un sous-corps de K.

Exemple 1

$\mathbb{C}$ (ou plutôt ($\mathbb{C}$, i) avec i : x → x.$1_{\mathbb{C}}$) est une extension de corps de IR.

Exemple 2

1. $\mathbb{C}$ est une extension de $\mathbb{Q}$ et $\mathbb{R}$.
2. $\mathbb{Q}$ ($\sqrt{2}$) = {a + b $\sqrt{2}$: a, b ∈ $\mathbb{Q}$} est un corps tel qu'il contient $\mathbb{Q}$, alors il est une extension de $\mathbb{Q}$.

Remarque

•Le morphisme i est injectif et permet d'identifier L à un sous-corps de K.

On peut munir K d'une structure de L-espace vectoriel. Comment ? La dimension de K sur L est notée [K : L].
D'une manière générale, dans ce cours, si K est un L-espace vectoriel, on note $[K : L] = \dim_L K$.
•Une extension de degré fini est dite extension finie
Exemple : $[\mathbb{R} : \mathbb{C}] = 2$, $[\mathbb{R} : \mathbb{R}] = 1$, $[\mathbb{Q} : \mathbb{Q}] = +\infty$
•Tout corps K est un sous-corps du corps K(X) des fractions rationnelles à coefficient dans K, alors K(X) est une extension de K.
Théorème
Si A et B sont deux parties d'une extension E de K, alors :

$$K\ (A \bigcup B) = K(A)(B)$$

Preuve
$(\supset)$
Tout sous-corps de E qui contient K, A et B contient K(A) et B. Donc

$$K(A)(B) \subset K\ (A \bigcup B).$$

$(\subset)$
Tout sous-corps de E qui contient K(A) et B contient K, A et B. Donc

$$K\ (A \bigcup B) \subset K(A)(B).$$

4.4 Caractéristique et cardinal d'un corps fini :

Théorème Soit K un corps fini. Alors la caractéristique de K est un nombre premier p. Il existe en particulier une unique structure de $\mathbb{Z}/p\mathbb{Z}$-algèbre sur K, qui fait de K un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension finie. Si on note n cette dimension, le cardinal de K est p^n.
En particulier le cardinal d'un corps fini est une puissance d'un nombre premier.
Démonstration:

On sait que la caractéristique d'un corps est 0 ou un nombre premier. Mais un corps de caractéristique 0 contient $\mathbb{Z}$, donc est infini. Donc K est de caractéristique un nombre premier p. L'unique structure de F_p-algèbre sur K est alors donnée par la factorisation du morphisme $\mathbb{Z} \to K$ par $\mathbb{Z}/p\mathbb{Z} \to K$. En tant que F_p-algèbre, K hérite d'une structure de F_p-espace vectoriel. Comme K est fini, il admet une famille génératrice finie comme F_p-espace vectoriel (prendre pour famille génératrice l'ensemble K lui-même !). C'est donc, par définition, un F_p-espace vectoriel de dimension finie. Si n est sa dimension, on sait que K est isomorphe comme F_p-espace vectoriel à F_p^n. En particulier les ensembles K et F_p^n sont en bijection. Or F_p^n a pour cardinal

p^n, ce qui conclut.
Remarque
•$F_p \to$ K est une extension de deg [K : F_p] = deg(P) = n.
•car(K) = p et card(K) = p^n.

4.5 L'endomorphisme de Frobenius :

Soit K un corps (commutatif) de caractéristique car(K) = p $\in \mathbb{P}$

$$\begin{aligned} Frob_{IK} : \text{K} &\longrightarrow \text{K} \\ \text{a} &\longrightarrow a^p \end{aligned}$$

Proposition (endomorphisme de Frobenius)
$Frob_{IK}$ est un morphisme de corps et de F_p-algèbre. En particulier :
• (Pour tout x $\in F_p$) x^p=x
• (Pour tout a, b $\in$ K) $(a+b)^p$=a^p+b^p
• Si de plus card (K) $\leq \infty$, alors $Frob_{IK}$ est un automorphisme.
Démonstration
1. Petit Fermat
2. p premier donc : (pour tout k $\in$ |[1, p -1]|)
3. $Frob_{IK}$ est un morphisme de corps, donc injectif (le seul idéal $\neq$ K est {0}). Si card(K) $\leq \infty$, il est donc bijectif.

4.6 Existence d'un corps fini de cardinal p^n

(Soit n un entier strictement positif, q = p^n et L le corps de décomposition du polynôme P(X) = X^q - X sur le corps $\mathbb{F}_p$. L'ensemble des éléments invariants par l'automorphisme Frobn est une extension K de $\mathbb{F}_p$. K est exactement l'ensemble des racines de P(X). Or P(X) est scindé sur K, il est de plus séparable car premier avec son polynôme dérivé égal à 1 (cette propriété est démontrée dans le paragraphe Cas des polynômes de l'article Extension séparable). K contient donc autant de racines que son degré, c'est-à-dire p^n.
Exemple $\mathbb{F}_4$
On note, pour tout p $\in \mathbb{N}^*$ premier, et n $\in \mathbb{N}^*$, $\mathbb{F}_{p^n}$ le corps fini à p^n éléments. On a notamment, pour tout p premier : $\mathbb{F}_p = \mathbb{Z}/\text{p}\mathbb{Z}$.
1. On pose Q = X^2 + X + 1. Comme, le degré de Q est de degré inférieur ou égal à 3 et qu'il n'a pas de racines dans $\mathbb{F}_2$[X], alors Q est irréductible. Donc $\mathbb{F}_4 = \mathbb{F}_2[\text{X}]/(\mathbb{Q})$. On a : $\mathbb{F}_4$ = {0 , 1, X, X + 1}.
2. (1, X) engendre $\mathbb{F}_4$. On a : X^2 = X + 1. (car -1 = 1)

3. La loi additive du corps est :

+	0	1	X	X+1
0	0	1	X	X+1
1	1	0	X+1	X
X	X	X+1	0	1
X+1	X+1	X	1	0

4. la loi multiplicative du corps est :

x	0	1	X	X+1
0	0	0	0	0
1	0	1	X	X+1
X	0	X	X+1	1
X+1	0	X+1	1	X

5. On remarque que $\mathbb{Z}/p\mathbb{Z}$ n'est pas $\mathbb{F}_4$! En effet :

x	0	1
0	0	0
1	0	1

•$\mathbb{F}_6$ n'est pas un corps car on ne peut pas écrire sous forme un nbre première puissance un entier

•$\mathbb{F}_8$est une extension de degré 3 de $\mathbb{Z}/p\mathbb{Z}$

$\mathbb{F}_8$=$\mathbb{F}_2$[X]/$(X^3 + X^2 + 1)$ soit α et β deux racines de $X^3 + X^2 + 1$

$\mathbb{F}_8$=$\mathbb{F}_2[\alpha] \Longrightarrow \deg(\alpha) \preceq 2$

$\mathbb{F}_8$=$\{0 , 1 , \alpha , 1+\alpha , \alpha^2 , \alpha^2+1 , \alpha^2+\alpha , \alpha^2+\alpha+1\}$; $\alpha^3 = \alpha+1$; α^7=1

$\mathbb{F}_8$=$F_2[\beta] \Longrightarrow \deg(\beta) \preceq 2$

$\mathbb{F}_8$=$\{0 , 1 , \beta , 1+\beta , \beta^2 , \beta^2+1 , \beta^2+\beta , \beta^2+\beta+1\}$; β^3=β^2+1 ;β^7=1

	α^2	α	1
1	0	0	1
α	0	1	0
α^2	1	0	0
α^3	0	1	1
α^4	1	1	0
α^5	1	1	1
α^6	1	0	1

	β^2	β	1
1	0	0	1
β	0	1	0
β^2	1	0	0
β^3	0	1	1
β^4	1	1	0
β^5	1	1	1
β^6	1	0	1

5 Groupe Cyclique

Théorème 5.1 (Caractérisation des groupes cycliques)
Soit (G, .) un groupe d'ordre n $\in \mathbb{N}^*$. Soit d un diviseur de n.
Notons $E_d = \{x \in G, x^d = 1\}$

- $\forall$d un diviseur de n, $|E_d| \preceq$ d. $\iff$ Le groupe G est cyclique.

Théorème 5.2
Soit (K,+,×) un corps fini. Alors (K*,×) est un groupe cyclique
Démonstration.
Soit (K,+,×) un corps fini. Nécessairement, (K*,×) est un groupe. Il s'agit donc de démontrer qu'il est cyclique. Soit d un diviseur de l'ordre de (K*,×). $E_d \neq \emptyset$ car $1 \in E_d$. Puisque (K,+,×) est un corps, le polynôme X^d - 1 a au plus d racines sur K. Donc $|E_d| \preceq$ d. Ainsi, d'après le **théorème 5.1**, (K*,×) est cyclique.
Corollaire 5.1
Soit p un nombre premier. Alors ($(\mathbb{Z}/p\mathbb{Z})^*$,×) est un groupe cyclique. Il est isomorphe à ($\mathbb{Z}/(p - 1)\mathbb{Z}$, +).
Démonstration
Soit p un nombre premier. Alors ($\mathbb{Z}/p\mathbb{Z}$,+,×) est un corps fini. Donc, d'après le **théorème 5.2**, ($(\mathbb{Z}/p\mathbb{Z})^*$,×) est un groupe cyclique. Son ordre étant p-1, or **Tout groupe cyclique d'ordre n $\in \mathbb{N}^*$ est isomorphe à ($\mathbb{Z}/n\mathbb{Z}$, +)**. Donc il est isomorphe à ($\mathbb{Z}/(p - 1)\mathbb{Z}$, +).