

# Table des matières

<b>Introduction</b>	<b>4</b>
<b>1 Etude sur les corps finis</b>	<b>5</b>
1.1 Généralités . . . . .	5
1.1.1 Groupe: . . . . .	5
1.1.2 Anneaux: . . . . .	6
1.2 Corps finis . . . . .	6
1.3 Description des corps finis . . . . .	7
1.4 Cardinal et groupe multiplicatif d'un corps fini . . . . .	8
1.4.1 Cardinal d'un corps fini . . . . .	8
1.4.2 Groupe multiplicatif d'un corps fini . . . . .	9
1.5 Groupe d'automorphisme d'un corps fini . . . . .	9
1.6 Extension de corps . . . . .	10
1.6.1 Existence et unicité des extensions $F_q \subseteq F_{q^n}$ . . . . .	11
1.7 Existence et Unicité du corps $F_q$ . . . . .	12
1.7.1 Existence du corps $F_q$ . . . . .	12
1.7.2 Unicité du corps $F_q$ . . . . .	13
1.8 Construction des corps finis . . . . .	14
1.9 Quelques propriétés . . . . .	15
1.9.1 Représentation d'un corps fini en puissance de $\alpha$ . . . . .	16
<b>2 Etude des polynômes sur un corps fini</b>	<b>18</b>
2.1 Anneaux des polynômes . . . . .	18

2.1.1	Opérations sur les polynômes . . . . .	18
2.2	Polynômes irréductibles . . . . .	22
2.2.1	Irréductibilité des polynômes de degré 1 . . . . .	22
2.2.2	Polynômes irréductibles . . . . .	23
2.2.3	Critère d'irréductibilité d'un polynôme sur $\mathbb{Q}$ . . . . .	24
2.2.4	Période d'un polynôme . . . . .	26
2.3	Anneau quotient . . . . .	26
2.3.1	Idéaux . . . . .	26
2.3.2	L'anneau $F_q[X] \setminus (P)$ . . . . .	27
2.3.3	Quelque propriétés dans L'anneau $F_q[X] \setminus (P)$ . . . . .	27
<b>3</b>	<b>Divisibilité des trinômes <math>x^{am} + x^{bs} + 1</math> par un polynôme irréductible sur <math>F_2</math></b>	<b>31</b>
3.1	Introduction . . . . .	31
3.2	Divisibilité d'un trinômes sur un corps fini . . . . .	31
3.2.1	Primitivité d'un polynôme irréductible sur un corps fini . . . . .	31
3.2.2	Théorèmes de base sur la divisibilité des trinômes $x^{am} + x^{bs} + 1$ par un polynôme irréductible sur $F_2$ . . . . .	32
3.2.3	Condition nécessaire de divisibilité des trinômes $x^{am} + x^{bs} + 1$ par un polynôme irréductible sur $F_2$ . . . . .	33
3.3	Recherche des trinômes irréductible sur $F_2$ de degré $\leq 100$ . . . . .	36
	<b>Bibliographie</b>	<b>40</b>

# NOTATION

$F_q$  : corps fini d'ordre  $q$

$(a, b) : p \gcd(a, b)$

$\cong$  : isomorphe

$Deg(f)$  : degré  $f$

$\langle p \rangle$  : idéal engendré par  $p$

$[K' : K]$  : dimension de  $K'$  sur  $K$

$F^* : F \setminus \{0\}$

$m \equiv m' \pmod{n} : m - m'$  divisible par  $n$

$A$  : Anneau de polynômes

$I$  : idéal de  $A$

$F_q[X] / (p)$  : anneau des classes modulo  $p(x)$

$F_q^n$  : espace vectoriel des vecteurs de longueur  $n$  sur  $F_q$

$|F|$  : cardinal de  $F$

$A[X]$  : anneau des polynômes à coefficients dans  $A$

$m_n(p)$  : nombre des polynômes irréductible sur  $F_p[X]$

$F_2$  : corps fini à deux éléments

$K/F$  : une extension finie de corps finis

# Introduction

L'objectif dans ce mémoire est l'étude de la divisibilité des trinômes en général par un polynôme irréductible de degré quelconque, cette divisibilité est un problème d'actualité, en particulier la divisibilité de ces trinômes sur  $F_2$ .

Les trinômes sont des polynômes de la forme  $x^{am} + x^{bs} + 1$ . Ils ont une application dans la théorie de corps finis et en théorie du codage. Beaucoup de factorisations des trinômes et des trinômes irréductibles ont été publiés.

Notre travail est organisé en trois chapitres:

1- Dans le premier Chapitre: Nous étudions les corps finis, en particulier le corps fini à deux éléments.

2- Le deuxième est consacré à la recherche des polynômes irréductible sur  $F_2$  de degré  $\leq 100$ .

3- Dans le troisième nous étudions la divisibilité (*Algorithme*) des Trinômes  $x^{am} + x^{bs} + 1$  sur  $F_2$  par un polynôme irréductible de degré quelconque.

# Chapitre 1

## Etude sur les corps finis

La structure de corps fini intervient dans divers domaines des mathématiques, en particulier dans la théorie de Galois sur la résolution des équations algébriques où ils sont introduits pour la première fois. Pour cette raison, en hommage au mathématicien français Evariste Galois (1811-1832), ces corps sont appelés les corps de Galois. Dans ce chapitre nous allons étudier de ces corps finis

### 1.1 Généralités

#### 1.1.1 Groupe:

**Définition 1.1.1** *Un ensemble  $G$  est un groupe si il est muni d'une loi de composition interne vérifiant les trois propriétés suivantes:*

- *Existence d'un élément neutre  $e$ :  $\forall x \in G, e * x = x * e = x$ .*
- *Associativité de la loi  $*$ :  $\forall x, y, z \in G, (x * y) * z = x * (y * z) = x * y * z$ .*
- *Existence d'un symétrique pour tout  $x$  de  $E$ :  $\forall x \in G, \exists y \in G$  tel que  $x * y = y * x = e$ .*

*Si de plus la loi de composition interne est commutative  $\forall x, y \in G : x * y = y * x$  alors le groupe  $(G, *)$  est dit commutatif (ou abélien). Dans ce cas la loi  $*$  sera souvent notée  $+$ , le neutre  $e$  noté  $0$  et le symétrique  $y$  noté  $-x$*

### 1.1.2 Anneaux:

**Définition 1.1.2** Soit  $A$  un ensemble muni de deux lois de composition interne notées  $+$  et  $\times$  on dit que  $(A, +, \times)$  est un anneau lorsque:

1.  $(A, +)$  est un groupe commutatif
2.  $\times$  est associative
3. il y a dans  $A$  un élément neutre pour  $\times$
4.  $\times$  est distributive par rapport à  $+$  ie :

$$\forall (x, y, z) \in A^3, \begin{cases} (x + y) \times z = x \times z + y \times z \\ x \times (y + z) = x \times y + x \times z \end{cases}$$

## 1.2 Corps finis

**Définition 1.2.3** Soit  $(A, \times, +)$  un anneau. Un élément  $a \in A$  est dit inversible s'il possède un symétrique pour la multiplication c'est à dire si :  $\exists a' \in A, a' \times a = a \times a' = 1_A$ .

Un anneau (commutatif)  $K$  est appelé un corps si tout élément non nul de  $K$  est inversible.

- l'anneau  $\mathbb{Z}$  n'est pas un corps (par exemple 2 n'est pas inversible)
- les anneaux  $\mathbb{Q}, \mathbb{R}$  et  $\mathbb{C}$  sont des corps

**Définition 1.2.4** On appelle sous corps, d'un corps  $(K, +, \times)$ , tout sous ensemble  $K'$  de  $K$  que, muni des restrictions des lois  $+$  et  $\times$  est un corps.

**Proposition 1.2.5**  $K' \subset K$  est un sous corps de  $(K, +, \times)$  si et seulement si

- $K' \neq \emptyset$ .
- $\forall a, b \in K', a - b$  et  $a \times b^{-1} \in K'$ .

✱ On dit qu'un corps  $K$  est fini s'il n'a qu'un nombre fini d'éléments

✱ un exemple de corps finis est l'ensemble  $F_2 = \{0, 1\}$  avec la règle  $1 + 1 = 0$ .

## 1.3 Description des corps finis

Dans toute la suite, étant donné un entier  $p \in \mathbb{N}^*$ , nous noterons  $\mathbb{Z}_p$  le groupe  $\mathbb{Z}/p\mathbb{Z}$  qui est un corps si et seulement si  $p$  est premier.

**Théorème 1.3.6** (Wedderburn) *Tout corps fini est commutatif.*

**Théorème 1.3.7** *Soit  $F$  un corps fini. Il existe un plus petit entier  $p$  tel que  $p.1 = 0$ . De plus,  $p$  est un nombre premier et  $\mathbb{Z}_p$  est un sous-corps de  $F$ .*

**Preuve.** Comme  $F$  est fini, les éléments  $1, 2.1, 3.1, \dots$  ne sont pas tous distincts, donc il existe deux entiers  $n$  et  $m$  tels que  $n.1 = m.1$  avec  $n < m$ . Par conséquent, par simplification,  $(m - n).1 = 0$ . Soit  $p$  le plus petit entier non nul tel que  $p.1 = 0$ . L'ensemble  $K = \{0, 1, 2.1, \dots, (p-1).1\}$  est un sous-corps de  $F$  à  $p$ -éléments et  $K \simeq Fp = \mathbb{Z}/p\mathbb{Z}$ . Donc  $p$  est premier et  $F_p$  est un sous-corps de  $F$ . ■

**Proposition 1.3.8** *L'entier  $p$  est appelé caractéristique de  $F$  et le sous-corps engendré par 1 (qui est isomorphe à  $F_p$ ) est le sous-corps premier de  $F$ .*

On dira d'un tel  $F_p$  (avec  $p$  premier) que c'est un corps premier de caractéristique  $p$  (par convention,  $\mathbb{Q}$  est un corps premier de caractéristique 0). Comme  $F_p$  est un sous-corps de  $F$ ,  $F$  peut être vu comme un  $F_p$ -espace vectoriel

**Théorème 1.3.9** *Soit  $F$  un corps fini de caractéristique  $p$ ,  $F$  est un  $F_p$  espace vectoriel de dimension finie (disons  $n$ ) et par conséquent,*

$$\#(F) = p^n$$

(où  $\#(F)$  désigne le cardinal de  $F$ ).

**Preuve.**  $F$  est un  $F_p$ -espace vectoriel et, par hypothèse,  $F$  est fini. Par conséquent, la dimension de  $F$  en tant que  $F_p$ -espace vectoriel est forcément finie (disons  $n$ ). D'où  $\#(F)$

$= (\#(F_p))^n = p^n$ . Donc un corps fini a forcément  $p^n$  éléments où  $p$  est un nombre premier.

■

**Proposition 1.3.10** *Soit  $F_q$  un corps fini de cardinal  $q$ , il existe un nombre premier  $p$  tel que :*

1.  $F_p \subset F_q$  ( $F_p = \mathbb{Z}/p\mathbb{Z}$ )
2.  $q = p^n$  pour un certain  $n \in \mathbb{N}^*$
3.  $\forall x \in F_q$ , on a  $x^q = x$ .

## 1.4 Cardinal et groupe multiplicatif d'un corps fini

### 1.4.1 Cardinal d'un corps fini

Soit  $K$  un corps fini. Son sous-corps premier est fini donc  $K$  est de caractéristique  $p > 0$ . On identifiera son sous corps premier à  $F_p = \mathbb{Z}/p\mathbb{Z}$ . Tout corps contenant  $K$  à même sous-corps premier, donc est aussi de caractéristique  $p$ .

**Lemme 1.4.11** *Soient  $K, K'$  deux corps finis, de cardinal  $q$  et  $q'$  respectivement.*

- 1) Soit  $n = [K' : K]$ . Alors  $q' = q^n$ .
- 2) Par conséquent, si  $p = \text{car}(K)$  et  $m = [K : F_p]$ , alors  $q = p^m$  et  $q' = p^{mn}$ .

**Preuve.** 1) Comme  $K'$  est fini, c'est un  $K$ -espace vectoriel de dimension finie  $n$ . Alors  $K' \cong K^n$  comme  $K$ -espace vectoriel, et donc  $|K'| = |K|^n \implies q' = q^n$ . Ceci prouve 1).

2)  $F_p \subseteq K$  et comme  $K$  est finie, c'est un  $F_p$  espace vectoriel de dimension finie  $m$ . Alors  $K \cong F_p^m$ , comme  $K$  espace vectoriel et donc  $|K| = |F_p|^m \implies q = p^m$  et  $(q')^n = (p^m)^n \implies q' = p^{mn}$ . ■

**Corollaire 1.4.12** *Si  $K$  est un corps fini de caractéristique  $p$ , alors le cardinal de  $K$  est une puissance de  $p$ .*



### 1.4.2 Groupe multiplicatif d'un corps fini

La propriété suivante des corps finis joue un rôle important en cryptographie ainsi que pour la construction de certains codes correcteurs d'erreurs

**Théorème 1.4.13** *Soit  $k$  un corps fini de cardinal  $q = p^n$ . Le groupe multiplicatif  $F_q^* = F_q \setminus \{0\}$  est un groupe cyclique d'ordre  $q - 1$ .*

**Preuve.** Par définition,  $F^*$  est un groupe multiplicatif. Soit  $\alpha \in F^*$ . Comme  $|F^*| = p^m - 1$ ,  $\alpha^i$  a au plus  $p^m - 1$  valeurs différentes. Il existe donc  $r$ ,  $1 \leq r \leq p^m - 1$ , tel que  $\alpha^r = 1$ . Le plus petit  $r$  vérifiant cette propriété est appelé l'ordre de  $\alpha$ . Soit  $\alpha$  un élément de  $F^*$  d'ordre  $r$  maximal. Montrons que l'ordre  $l$  de tout élément de  $F^*$  divise  $r$ . Soit  $\pi$  premier tel que  $r = \pi^a r'$  et  $l = \pi^b l'$  avec  $\text{pgcd}(r', \pi) = \text{pgcd}(l', \pi) = 1$ .  $\alpha^{\pi^a}$  a pour ordre  $r'$  et  $\beta^{l'}$  a pour ordre  $\pi^b$ , donc  $\alpha^{\pi^a} \beta^{l'}$  a pour ordre  $\pi^b r'$ . Par conséquent,  $\pi^b r' \leq r = \pi^a r'$ , soit  $b \leq a$ . Cela montre que  $l$  divise  $r$ . Pour tout  $\beta \in F^*$ , est donc solution de  $X^r - 1 = 0$ .  $\prod_{\beta \in F^*} (X - \beta)$  divise  $X^r - 1$ , donc  $r \geq p^m - 1$ , et donc  $r = p^m - 1$  et  $F^*$  est cyclique. ■

**Définition 1.4.14** *Les générateurs de  $F_q$  sont appelés éléments primitifs de  $F_q^*$ .*

## 1.5 Groupe d'automorphisme d'un corps fini

**Proposition 1.5.15 (Frobenius)**

Soit  $K$  un corps de caractéristique  $p > 0$ . L'application  $x \mapsto x^p$  est un homomorphisme de corps appelé homomorphisme de Frobenius.

**Proposition 1.5.16** *Soit  $K$  un corps de caractéristique  $p > 0$ .*

- Soit  $x \in k$  Alors  $x \in F_2$  si et seulement si  $x^p = x$ .
- Soit  $Q \in K[X]$ . Alors  $Q \in F_p[X]$  si et seulement si  $Q(X^p) = (Q(X))^p$ .

**Preuve.** Soit  $x \in K$ . Si  $x \in F_p$  alors par le théorème de Lagrange  $x^p = x$ . Réciproquement, le polynôme  $X^p - X$  a au plus  $p$  racines, or les éléments de  $F_p$  au nombre de  $p$  sont tous racines. Si  $Q \in F_p[X]$  alors d'après l'homomorphisme de Frobenius

$Q(X^p) = (Q(X))^p$ . Réciproquement si  $Q(X^p) = (Q(X))^p$  alors par l'homomorphisme de Frobenius les coefficients de  $Q$  vérifient l'équation  $x^p = x$  donc appartiennent à  $F_p$ . ■

**Proposition 1.5.17** *Soit  $K$  un corps de caractéristique  $p \neq 0$ . L'application  $F : x \rightarrow x^p$  est un endomorphisme de la  $\mathbb{Z}/p\mathbb{Z}$ -algèbre  $K$ , appelé **endomorphisme de Frobenius de  $K$** . De plus, si  $K$  est fini,  $F$  est un automorphisme. En particulier, si  $K = \mathbb{Z}/p\mathbb{Z}$ ,  $F$  est l'identité.*

**Proposition 1.5.18** *Soit  $K$  un corps fini de caractéristique  $p$ . Si  $\alpha \in K$  est de degré  $r$  sur  $F_p$ , alors  $r$  est le plus petit entier tel que  $\alpha^{p^r} = \alpha$ , les  $\alpha^{p^i}$  sont distincts, pour  $0 \leq i \leq r$  et le polynôme minimal de  $\alpha$  sur  $F_p$  est  $\prod_{0 \leq i \leq r} (X - \alpha^{p^i})$ .*

**Proposition 1.5.19** *Soit  $q = p^n$ , avec  $p$  premier. Le groupe des automorphismes de  $F_q$  est cyclique d'ordre  $n$  engendré par l'automorphisme de Frobenius  $F : x \rightarrow x^p$ .*

## 1.6 Extension de corps

Soit  $K$  un corps fini et soit  $L$  une extension du corps  $K$ . Ceci veut dire que  $L$  contient  $K$  comme sous-ensemble et que l'addition et la multiplication dans  $L$  prolongent celles de  $K$ , en d'autres termes, si  $x, y \in K$ ,  $x + y$  et  $xy$  désignent le même élément (de  $K$ ) que les opérations soient prises dans  $(K, +, \times)$  ou dans  $(L, +, \times)$ . On note l'extension par  $L/K$  ou  $L : K$ .

Le corps  $L$  est muni d'une structure d'espace vectoriel sur  $K$ . Si cet espace vectoriel est de dimension finie on note  $[L : K]$  sa dimension, on dit que l'extension  $L/K$  est finie, et on appelle  $[L : K]$  le degré de l'extension.

**Définition 1.6.20** *Soient  $F$  et  $E$  des corps, si  $F$  est un sous corps de  $E$ , on dit alors que  $E$  est une extension de  $F$ .*

**Proposition 1.6.21** *Toute extension finie de corps finis est normale et séparable.*

**Démonstration.** Soient  $K/F$  une extension finie de corps finis,  $q$  le nombre d'éléments de  $K$ ,  $F_p$  le sous-corps premier. Le corps  $K$  est le corps de décomposition sur  $F_p$  (donc sur  $F$ ) du polynôme  $X^q - X$ , par conséquent l'extension  $K/F_p$  est normale, et donc  $K/F$  aussi. Si  $\alpha$  est un élément de  $K$ , il est algébrique sur  $F$ , son polynôme irréductible sur  $F$  divise  $X^q - X$ , il est totalement décomposé sur  $K$ , sans racine multiple (noter que  $p$  ne divise pas  $q - 1$ ), donc il est séparable. ■

### 1.6.1 Existence et unicité des extensions $\mathbf{F}_q \subseteq \mathbf{F}_{q^n}$

**Théorème 1.6.22** Soient  $p$  un nombre premier,  $q = p^d$  et  $q' = p^n$  deux puissances de  $p$ .

1) S'il existe une extension  $F_q \subseteq F_{q'}$  alors  $q'$  est une puissance de  $q$  c.-à-d  $n$  est un multiple de  $d$ .

2) Réciproquement, si  $n = rd$ , c.-à-d., si  $q' = q^r$ , alors le corps  $F_{q'}$  contient un **unique** sous-corps de cardinal  $q$ , c'est le sous-corps des invariants de  $Fr_q$ .

**Preuve.** 1) On a déjà vu (lemme 1.4.11) que si  $\mathbf{F}_q \subseteq \mathbf{F}_{q'}$  alors  $\mathbf{F}_{q'}$  est un  $F_q$ -espace vectoriel de dimension finie  $r$ , d'où  $q' = q^r$ , c.-à-d  $n = dr$ .

2) Réciproquement, supposons  $n = dr$ , c.-à-d.,  $q' = q^r$ . Le polynôme  $X^{q'} - X = X^{q^r} - X$  est scindé dans  $F_{q'}$  et ses racines, deux à deux distinctes, sont exactement les éléments de  $F_{q'}$ . D'autre part,

$$\begin{aligned} X^{q^r} - X &= X^q - X + X^{q^2} - X^q + \dots + X^{q^r} - X^{q^{r-1}} \\ &= X^q - X + (X^q - X)^q + \dots + (X^q - X)^{q^{r-1}} \end{aligned}$$

Donc  $X^q - X$  divise  $X^{q^r} - X$  et a aussi toutes ses racines dans  $F_{q'}$ . Ces racines sont exactement les points fixes dans  $F_{q'}$  de l'endomorphisme de Frobenius  $Fr_q$ , donc forment un sous-corps  $K$  de cardinal  $q$ , isomorphe à  $F_q$ . Enfin, supposons que  $L$  soit un autre sous-corps de  $F_{q'}$  de cardinal  $q$ . D'après le **théorème 1.4.13**, le groupe multiplicatif  $L^\times$  est cyclique, d'ordre  $q - 1$ . Donc, tout élément  $x \in L^\times$  vérifie

$$x^q - 1 = 1 \text{ et donc } x^q = x.$$

Par conséquent, les éléments de  $L = L^\times \cup \{0\}$  sont exactement les racines dans  $F_{q'}$  du polynôme  $X^q - X$ . Il en résulte  $L = K$ . ■

**Lemme 1.6.23** Soit  $K$  un corps de caractéristique  $p > 0$ . Notons  $F$  l'application  $K \rightarrow K$  définie par  $F(x) = x^p$  ( $F$  s'appelle le morphisme de Frobenius). Alors :

1.  $F$  est un morphisme de corps ( injectif).
2. Si  $K$  est fini, c'est un automorphisme (i.e. il est bijectif).
3. Pour  $x \in K$ ,  $F(x) = x$  si et seulement si  $x \in F_p$ .

**Preuve.** On a évidemment  $F(xy) = F(x)F(y)$  et  $F(1) = 1$ , ce qui implique que  $F(x^{-1}) = (F(x))^{-1}$  pour  $x \neq 0$ . Pour l'addition, écrivons la formule du binôme :

$$(x + y)^p = x^p + \binom{p}{1} x^{p-1}y + \cdots + \binom{p}{i} x^{p-i}y^i + \cdots + y^p$$

D'après le théorème 1.9.29 la formule du binôme devient donc:  $(x + y)^p = x^p + y^p$ , ce qui montre 1.  $F$  étant un morphisme de corps, il est injectif et donc bijectif si le cardinal de  $K$  est fini. Enfin on a  $x^{p-1} = 1$  pour tout  $x \in F_p$  non nul (car  $F_p^*$  est de cardinal  $p - 1$ ) et donc  $x^p = x$  pour  $x \in F_p$ . Les éléments de  $F_p$  sont les seuls vérifiant cette équation, puisque l'équation  $X^p - X = 0$  a au plus  $p$  racines dans le corps  $K$ . ■

## 1.7 Existence et Unicité du corps $F_q$

### 1.7.1 Existence du corps $F_q$

**Théorème 1.7.24** Soient  $p$  un nombre premier,  $n \in \mathbb{N}^*$ . On pose  $q = p^n$ . On considère le polynôme  $X^q - X$  comme à coefficients dans  $F_p$ . Alors le corps de décomposition du polynôme  $X^q - X$  sur  $F_p$  est un corps à  $q$  éléments noté  $F_q$ .

**Preuve.** Soit  $K$  le corps de décomposition de  $X^q - X$  sur le corps  $F_p$ . L'ensemble  $A \subset K$  des racines de  $X^q - X$  est un corps car si  $x \in A$  et  $y \in A$ , on a  $x^q = x$  et  $y^q = y$ , d'où  $(xy)^q = xy$  et  $(x + y)^q = x + y$  car  $q$  étant égal à  $p^n$ , l'application  $x \rightarrow x^q$  de  $K$  dans  $K$  est le morphisme de Frobenius itéré  $n$  fois. On a donc  $xy \in A$  et  $x + y \in A$ . De plus si  $x \in A$ ,  $x \neq 0$ , on a évidemment  $1/x \in A$ , et  $A$  contient  $F_p$ . On a donc  $A = K$  puisque par définition  $K$  est engendré sur  $F_p$  par les racines de  $X^q - X$ . D'autre part si l'on pose

$P = X^q - X$ , on a  $P' = qX^{q-1} - 1 = -1$  puisque la caractéristique  $p$  de  $K$  divise  $q$ . Cela entraîne que les racines de  $P$  sont simples (puisque pour toute racine  $\alpha$  de  $P$  dans  $K$  on a  $P'(\alpha) = -1 \neq 0$ ), et donc que  $A = K$  est un corps à  $q$  éléments (puisque le polynôme  $X^q - X$  a alors exactement  $q$  racines dans  $K$ ). En particulier, si  $q = p$  on a  $K = F_p$ . ■

### 1.7.2 Unicité du corps $F_q$

**Proposition 1.7.25** *Soit  $k$  un corps fini à  $q = p^n$  éléments. Alors il est isomorphe au corps  $F_q$  (par un  $F_p$ -isomorphisme).*

**Preuve.** Comme  $|k| = q = p^n$ , le corps  $k$  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

$$F_q = \{ \alpha_0 + \alpha_1 a + \dots + \alpha_{n-1} a^{n-1}, \alpha_i \in F_p \}$$

puisque  $F_q \simeq \frac{F_p[X]}{(q_a(X))}$ .

Comme  $|K| = q$ , les éléments de  $K$  vérifient aussi l'équation  $X^q - X = 0$  et  $K$  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  $b \in K$  tel que  $q_a$  soit le polynôme minimal de  $b$  ( $b$  est une racine dans  $K$  du polynôme  $q_a$ ). Considérons l'application  $f : F_q \rightarrow K$  :

$$\alpha_0 + \alpha_1 a + \dots + \alpha_{n-1} a^{n-1} \longmapsto \alpha_0 + \alpha_1 b + \dots + \alpha_{n-1} b^{n-1}$$

Il est immédiat de vérifier que  $f$  est un isomorphisme (en fait un  $F_p$ -isomorphisme) de corps. ■

Étudions maintenant les sous-corps de  $F_q$ .

**Proposition 1.7.26** *Posons  $q = p^n$  avec  $p$  premier.*

1. Pour tout entier  $d$  tel que  $d|n$ , il y a un unique corps  $K$  de cardinal  $p^d$  tel que :

$$F_p \subset K \subset F_q$$

Ce corps  $K$  est l'ensemble des  $x \in F_q$  tels que  $x^{p^d} = x$  est isomorphe à  $F_{q'}$  avec  $q' = p^d$ .

2. Réciproquement, tout corps  $K$  tel que  $F_p \subset K \subset F_q$  est de cardinal  $p^d$  avec  $d|n$ .

**Démonstration.** Soit  $d$  un entier tel que  $d|n$ . Montrons l'existence de  $K$ . Soit  $K$  l'ensemble des racines (dans  $F_q$ ) du polynôme  $X^{p^d} - X$ , il a déjà été démontré que  $K$  était un corps (démonstration de théorème de l'existence). ■

## 1.8 Construction des corps finis

Ainsi, comme les corps finis de même cardinal  $q = p^n$  sont tous isomorphes, il suffit d'en connaître un pour les connaître. Par exemple soit  $P$  un polynôme irréductible de degré  $n$  dans  $\mathbb{Z}/p\mathbb{Z}$ , l'ensemble  $\frac{\mathbb{Z}/p\mathbb{Z}}{P}$  peut être muni d'une structure de corps et est de cardinal  $p^n$ . Une construction classique de l'arithmétique dans un corps fini est donc d'implémenter  $\mathbb{Z}/p\mathbb{Z}$ , de rechercher un polynôme irréductible  $P$  dans  $\mathbb{Z}/p\mathbb{Z}$  de degré  $n$ , puis de représenter les éléments de  $GF[p^n]$  par des polynômes ou des vecteurs, et d'implémenter les opérations arithmétiques comme des opérations modulo  $p$  et  $P$ .

Le théorème pour la construction d'un corps fini à  $q = p^n$  éléments est le suivant:

**Théorème 1.8.27** Soit  $\alpha \in F/K$  et soit  $g$  le polynôme minimal de  $\alpha$  sur  $K$  Alors:

- 1)  $K(\alpha)$  est isomorphe à  $K[x]/(g)$ .
- 2) Une base de  $K(\alpha)$  sur  $K$  est  $\{1, \alpha, \alpha^2, \dots, \alpha^{\deg(g)-1}\}$ .

**Exemple 1.8.28** Soit  $P = X^2 + X + 1$  le seul polynôme irréductible de degré 2 de l'algèbre  $F_2[X]$ . On note  $\alpha$  une de ses racines, on a

$$F_2(\alpha) \sim F_2[x]/\langle p \rangle$$

On sait, que  $F_2[X]/\langle p \rangle$  est un corps et que si désigne la classe d'équivalence du polynôme  $X$  dans  $F_2[X]/\langle p \rangle$ , alors,  $F_2[X]/\langle p \rangle = \{a + b \mid a, b \in F_2\} = \{0, 1, \alpha, 1 + \alpha\}$ , et  $\{1, \alpha\}$  est une base de  $F_2(\alpha)$

**La table de multiplication de  $F_2[X]/\langle p \rangle$**  s'écrit, compte tenu de l'égalité  $P(\alpha) = 0$ , c'est-à-dire  $\alpha^2 = \alpha + 1$

$\times$	0	1	$\alpha$	$1 + \alpha$
0	0	0	0	0
1	0	1	$\alpha$	$1 + \alpha$
$\alpha$	0	$\alpha$	$1 + \alpha$	1
$1 + \alpha$	0	$1 + \alpha$	1	$\alpha$

On y voit par exemple que l'inverse de  $\alpha$  est  $(1 + \alpha)$ .

La table de l'addition de  $F_2[X]/\langle p \rangle$  s'écrit

+	0	1	$\alpha$	$1 + \alpha$
0	0	1	$\alpha$	$1 + \alpha$
1	1	0	$1 + \alpha$	$\alpha$
$\alpha$	$\alpha$	$1 + \alpha$	0	1
$1 + \alpha$	$1 + \alpha$	$\alpha$	1	0

**Puissance de  $\alpha$  dans  $F_2[x]/(x^2 + x + 1)$**

$i$	0	1	2	3
$\alpha^i$	1	$\alpha$	$1 + \alpha$	1

- $\alpha$  est un élément primitif, et  $x^2 + x + 1$  un polynôme primitif dans  $F_2[x]$

## 1.9 Quelques propriétés

**Théorème 1.9.29** Dans tout corps fini  $F$  ayant  $q = p^n$  éléments ( $p$  premier), pour tout  $x, y \in F$

on a

$$(x + y)^p = x^p + y^p$$

**Preuve.** comme  $F$  est de caractéristique  $p$ , dans  $F$  on a la formule du binôme de Newton donne

$$(x + y)^p = \sum_{k=0}^p C_p^k x^k y^{p-k}$$

Montrons que pour tout  $1 \leq k \leq p-1$  on a  $p/C_p^k$ . on a

$$C_p^k = \frac{p \times (p-1) \dots (p-k+1)}{k}$$

Montrons tout d'abord que  $\text{pgcd}(k, p) = 1$ . Comme  $p$  est premier,  $\text{pgcd}(k, p) = 1$  ou  $p$ , si  $\text{pgcd}(k, p) = p$ , comme  $p$  est premier, d'après Gauss, il faudrait que  $p$  divise l'un des facteurs de  $k$  ce qui est impossible puisqu'ils sont tous strictement inférieurs à  $p$ . Donc  $\text{pgcd}(k, p) = 1$ .

or, comme  $C_p^k$  est entier, on a  $k/p \cdot (p-1) \dots (p-k+1)$  puis  $C_p^k = p \underbrace{\frac{(p-1) \dots (p-k+1)}{k}}_{\text{entier}}$

Donc pour  $1 \leq k \leq p-1$ , on a  $p/C_p^k$  puis  $C_p^k = 0$  dans  $F$ . Ainsi, dans la somme (1), seuls le premier et le dernier termes sont non nuls, c'est à dire  $(x + y)^p = x^p + y^p$ . ■

**Corollaire 1.9.30** si  $\alpha$  est une racine de  $P \in F_p[x]$ , alors  $\alpha^p, \alpha^{p^2}, \dots, \alpha^{p^n}$  sont aussi des racines de  $P$ .

**Lemme 1.9.31**  $\mathbb{Z}/n\mathbb{Z}$  est un corps  $\Leftrightarrow n$  est premier  $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}$  est un anneau intègre. De plus  $\mathbb{Z}/p\mathbb{Z}$  est l'unique corps (à isomorphisme près) de cardinal  $p$ .

### 1.9.1 Représentation d'un corps fini en puissance de $\alpha$

**Exemple 1.9.32** Soit  $\alpha \in F_{16}$  une racine du polynôme irréductible  $x^4 + x + 1$  sur  $F_2$  (on peut faire la division par  $x + 1$  et  $x^2 + x + 1$ ), c'est à dire que  $\alpha^4 + \alpha + 1 = 0$ . Signalons que  $\alpha$  est primitif (ie  $\alpha^{15} = 1$ ),  $F_{16}$  est représenté par les polynômes de  $\deg < 4$  dont tout élément est combinaison linéaire des éléments  $1, \alpha, \alpha^2$  et  $\alpha^3$ . Voilà les différentes représentations des éléments de  $F_{16}$ .



En puissance de $\alpha$	En polynôme	En 4 uples
0	0	(0, 0, 0, 0)
1	1	(1, 0, 0, 0)
$\alpha$	$\alpha$	(0, 1, 0, 0)
$\alpha^2$	$\alpha^2$	(0, 0, 1, 0)
$\alpha^3$	$\alpha^3$	(0, 0, 0, 1)
$\alpha^4$	$1 + \alpha$	(1, 1, 0, 0)
$\alpha^5$	$\alpha + \alpha^2$	(0, 1, 1, 0)
$\alpha^6$	$\alpha^2 + \alpha^3$	(0, 0, 1, 1)
$\alpha^7$	$1 + \alpha + \alpha^3$	(1, 1, 0, 1)
$\alpha^8$	$1 + \alpha^2$	(1, 0, 1, 0)
$\alpha^9$	$\alpha + \alpha^3$	(0, 1, 0, 1)
$\alpha^{10}$	$1 + \alpha + \alpha^2$	(1, 1, 1, 0)
$\alpha^{11}$	$\alpha + \alpha^2 + \alpha^3$	(0, 1, 1, 1)
$\alpha^{12}$	$1 + \alpha + \alpha^2 + \alpha^3$	(1, 1, 1, 1)
$\alpha^{13}$	$1 + \alpha^2 + \alpha^3$	(1, 0, 1, 1)
$\alpha^{14}$	$1 + \alpha^3$	(1, 0, 0, 1)

$F_{16}$  vu comme espace vectoriel sur  $F_2$  de dimension 4,  $\{1, \alpha, \alpha^2, \alpha^3\}$  étant une base ou  $\alpha$  vérifié  $\alpha^4 + \alpha + 1 = 0$

# Chapitre 2

## Etude des polynômes sur un corps fini

### 2.1 Anneaux des polynômes

Soit  $A$  un anneau commutatif, on rappelle qu'un polynôme  $P$  à une variable à coefficients dans l'anneau  $A$  est la donnée d'une suite  $P = (a_0, a_1, \dots, a_n, \dots)$  d'éléments de  $A$ , dont tous les termes sont nuls à partir d'un certain rang. L'ensemble de ces polynômes est noté  $A[X]$ .

**Définition 2.1.33** *L'anneau  $A[X]$  est appelé anneau des polynômes à coefficients dans  $A$ .*

Nous allons maintenant étudier quelques propriétés de l'anneau  $A[X]$

#### 2.1.1 Opérations sur les polynômes

**Définition 2.1.34** *Soit  $P = (a_0, a_1, \dots, a_n, \dots)$  et  $Q = (b_0, b_1, \dots, b_n, \dots)$  deux polynômes de  $A[X]$ . On définit la somme et le produit de  $P$  et  $Q$  respectivement par*

$$(1) \ P + Q = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, \dots)$$

$$(2) \ PQ = (c_0, c_1, \dots, c_n, \dots),$$

$$\text{où pour chaque indice } i \geq 0, c_i = \sum_{k=0}^i a_k b_{i-k}.$$

Un polynôme dont les termes  $a_i$  sont nuls pour tout  $i \geq 1$  est appelé polynôme constant. On identifie tout élément  $a \in A$  au polynôme constant  $(a, 0, 0, \dots)$ , ce qui permet d'écrire

$$aP = (aa_0, aa_1, \dots, aa_n, \dots)$$

Il est clair que le polynôme  $1 = (1, 0, 0, \dots)$  est l'élément neutre de la multiplication et le polynôme  $0 = (0, 0, 0, \dots)$  celui de l'addition.

Un polynôme à une variable sur un corps  $A$  est une expression  $a_0 + a_1X + \dots + a_nX^n$  où les  $a_i$  sont des éléments de  $A$  (les coefficients du polynôme).

**Définition 2.1.35** Soit  $A$  un anneau. Soit  $f \in A[X]$ ,  $f \neq 0$ . Puisque  $f \neq 0$ , on peut écrire  $f = a_dX^d + a_{d-1}X_{d-1} + \dots + a_0$ , avec  $a_i \in A$ ,  $a_d \neq 0$ . L'entier  $d \geq 0$  est appelé le degré de  $f$ , et est noté  $\deg(f)$ . Par convention, on pose  $\deg(0) = -\infty$  on a donc  $\deg(f) \geq 0$  si et seulement si  $f$  est non nul.

Le coefficient  $a_d$  est appelé le coefficient *dominant* de  $f$ . On dit qu'un polynôme est unitaire si son coefficient dominant est égal à 1.

Contrairement au cas des polynômes à coefficients dans un corps, l'anneau  $A[X]$  n'est pas nécessairement intègre. Le lemme suivant donne des conditions nécessaires et suffisantes pour cela soit le cas.

**Lemme 2.1.36 :** Soit  $A$  un anneau. Alors, les propriétés suivantes sont équivalentes :

- (1) l'anneau  $A[X]$  est intègre .
- (2) l'anneau  $A$  est intègre .
- (3) pour tous  $f, g \in A[X]$ , on a  $\deg(fg) = \deg(f) + \deg(g)$ .

**Preuve.**

(1)  $\Rightarrow$  (2). C'est immédiat car un sous-anneau d'un anneau intègre est intègre.

(2)  $\Rightarrow$  (3). Si  $f$  ou  $g$  est nul, l'égalité est triviale. Supposons maintenant que  $f$  et  $g$  soient non nuls, et écrivons

$$f = a_nX^n + \dots + a_0, g = b_mX^m + \dots + b_0, a_n \neq 0, b_m \neq 0$$

En utilisant la définition, on voit que l'on a

$$fg = a_nb_mX^{n+m} + \text{des termes en } X^i, i < n+m ,$$

Comme  $A$  est intègre, on a  $a_n b_m \neq 0$ , ce qui démontre l'égalité

$$\deg(fg) = n + m = \deg(f) + \deg(g)$$

(3)  $\Rightarrow$  (1). Puisque  $A$  est commutatif non trivial, il en est de même de  $A[X]$ .

Soient  $f$  et  $g$  deux polynômes non nuls. On a donc  $\deg(f) \geq 0$  et  $\deg(g) \geq 0$ . Mais alors, on a

$$\deg(fg) = \deg(f) + \deg(g) \geq 0,$$

ce qui entraîne que  $fg$  est non nul, d'où l'intégrité de  $A[X]$ . ■

On continue ce paragraphe en expliquant comment diviser deux polynômes.

**Théorème 2.1.37** *Soit  $A$  un anneau. Soient  $f, g \in A[X]$ ,  $g \neq 0$ ,  $\deg(f) \geq \deg(g)$ . On suppose que le coefficient dominant de  $g$  est un élément inversible de  $A$ . Alors il existe deux polynômes  $Q, R \in A[X]$ , avec  $\deg(R) < \deg(g)$  tels que  $f = Qg + R$ . Si de plus  $A$  est intègre,  $Q$  et  $R$  sont uniques.*

### Démonstration

On démontre l'existence de  $Q$  et  $R$  par récurrence sur  $\deg(f)$ . Soit  $(H_n)$  la propriété :

$(H_n)$  : Pour tous  $f, g \in A[X]$ ,  $g \neq 0$  tels que  $\deg(g) \leq \deg(f) \leq n$ , et tels que le coefficient dominant de  $g$  soit inversible, il existe  $Q, R \in A[X]$ , tels que  $\deg(R) < \deg(g)$  et  $f = gQ + R$ .

Si  $f$  est nul, c'est clair, car on prend  $Q = R = 0$ . Si  $\deg(f) = 0$ , alors  $\deg(g) = 0$ . On a donc  $f = a, g = b, a, b \in A, b \in A^\times$ . On pose alors  $Q = b^{-1}a$  et  $R = 0$  dans ce cas. Ainsi  $(H_0)$  est vraie.

Supposons  $(H_n)$  vraie pour un  $n \geq 0$ , et montrons  $(H_{n+1})$ . Si  $\deg(f) \leq n$ , alors  $Q$  et  $R$  existent car  $(H_n)$  est vraie, donc on peut supposer que  $\deg(f) = n + 1$ . Ecrivons

$$f = a_{n+1}X^{n+1} + \dots + a_1X + a_0, g = b_mX^m + \dots + b_1X + b_0$$

Par hypothèse, on a  $n + 1 \geq m$ .

Soit  $Q_1 = b_m^{-1} a_{n+1}X^{n+1-m}$  et  $R_1 = f - b_m^{-1}a_{n+1}X^{n+1-m}g$ . Remarquons que  $b_m^{-1}$  à un sens dans  $A$ , puisque  $b_m \in A$ . Puisque  $f, g \in A[X]$ , on a aussi  $Q_1, R_1 \in A[X]$ . Par construction,

le coefficient en  $X^{n+1}$  de  $R_1$  est 0, donc  $\deg(R_1) \leq n$ . Si  $\deg(R_1) < \deg(g)$ , on a fini, car on peut écrire

$$f = b_m^{-1}a_m X^{n+1-m}g + R_1,$$

et donc poser  $R = R_1$  et  $Q = b_m^{-1}a_m X^{n+1-m}$ .

Supposons maintenant que  $\deg(R_1) \geq \deg(g)$ . Comme  $\deg(g) \leq \deg(R_1) \leq n$ , on peut appliquer  $(H_n)$ , et donc il existe  $Q_2, R_2 \in A[X]$  tels que  $R_1 = gQ_2 + R_2$ , avec  $\deg(R_2) < \deg(g)$ .

Ainsi, on a  $f = (b_m^{-1}a_m X^{n+1-m} + Q_2)g + R_2$ , et  $\deg(R_2) < \deg(g)$ . Maintenant, il suffit de poser  $Q = b_m^{-1}a_m X^{n+1-m} + Q_2$  et  $R = R_2$ .

Ainsi,  $(H_{n+1})$  est vraie, ce qui achève la récurrence. Montrons maintenant l'unicité de  $Q$  et  $R$  dans le cas où  $A$  est intègre. Supposons  $f = Q_1g + R_1 = Q_2g + R_2$ , avec  $Q_i, R_i \in A[X]$  et  $\deg(R_i) < \deg(g)$ . Alors, on a  $g(Q_1 - Q_2) = R_2 - R_1$ . Puisque  $A$  est intègre, on a

$$\deg(g(Q_1 - Q_2)) = \deg(g) + \deg(Q_1 - Q_2)\deg(g).$$

Néanmoins, il est facile de constater que  $\deg(R_2 - R_1) < \deg(g)$ , d'où une contradiction, sauf si  $\deg(R_2 - R_1) = -\infty$ , c'est-à-dire  $R_1 - R_2 = 0$ . Ainsi  $R_1 = R_2$ , et donc  $g(Q_1 - Q_2) = 0$ . Comme  $A$  est intègre, il en est de même de  $A[X]$ , et puisque  $g \neq 0$ , on obtient  $Q_1 = Q_2$ .

**Définition 2.1.38** *Si  $A$  est intègre, les polynômes  $Q$  et  $R$  s'appellent respectivement le quotient et le reste de la division de  $f$  par  $g$ .*

En pratique, la meilleure façon de calculer  $Q$  et  $R$  est de procéder comme dans le cas où  $A = \mathbb{R}, \mathbb{C}$ .

**Attention !** Ce résultat n'est pas vrai dans le cas général. Par exemple,  $X, 2X \in \mathbb{Z}[X]$ , mais le quotient de  $X$  par  $2X$  est  $\frac{1}{2}$ , qui n'est pas dans  $\mathbb{Z}[X]$ .

Si  $\mathbb{k}$  est un corps, on peut donc diviser n'importe quel polynôme par un polynôme non nul, et on obtient que  $\mathbb{k}[X]$  est un anneau euclidien dans ce cas. Nous reviendrons sur ce point dans un paragraphe ultérieur.

## 2.2 Polynômes irréductibles

### 2.2.1 Irréductibilité des polynômes de degré 1

Nous allons commencer à nous intéresser à l'irréductibilité des polynômes à coefficients dans un anneau. Nous examinerons dans ce paragraphe le cas des polynômes de degré 1. Avant de continuer, signalons que la notion usuelle d'irréductibilité d'un polynôme à coefficients dans un corps concide avec la notion d'irréductibilité plus générale introduite précédemment.

**Remarque:**

Si  $K$  est un corps, alors  $f \in \mathbb{k}[X]$  est irréductible si et seulement s'il n'est pas constant et ne peut pas s'écrire comme produit de deux polynômes non constants, ce qui est la définition classique de l'irréductibilité d'un polynôme.

En effet, si  $f$  est constant, alors il est soit nul, soit inversible car  $\mathbb{k}^\times[X] = K^\times = \mathbb{k} \setminus \{0\}$ . Dans ce cas, il n'est pas irréductible. Si  $f = f_1 f_2$  avec  $f_1, f_2 \in \mathbb{k}[X]$  non constants, alors  $f$  n'est pas irréductible non plus, puisque  $f_1, f_2 \in \mathbb{k}[X]^\times = K^\times = \mathbb{k} \setminus \{0\}$ . Inversement, supposons que  $f$  ne soit pas irréductible, et supposons qu'il soit non constant. Alors, en particulier il est non nul et non inversible, et donc nécessairement, on a  $f = f_1 f_2$ , avec  $f_1, f_2 \in \mathbb{k}[X]$  et donc non constants. Ceci devient faux pour des coefficients quelconques. Par exemple,  $2X \in \mathbb{Z}[X]$  ne peut pas s'écrire comme produit de deux polynômes non constants, mais il n'est pas irréductible, puisque ni 2, ni  $X$  ne sont inversibles (en effet,  $\mathbb{Z}[X]^\times = \mathbb{Z} \setminus \{0\}$ ).

Lorsque  $\mathbb{k}$  est un corps, tout polynôme de degré 1 à coefficients dans  $\mathbb{k}$  est irréductible. Plus généralement, on a le résultat suivant:

**Lemme 2.2.39** *Soit  $A$  un anneau intègre. Alors, pour tout  $a \in A$ , le polynôme  $X - a$  est irréductible.*

**Démonstration:**

Soit  $a \in A$ . Alors,  $X - a$  est non nul, et non inversible, car  $A$  étant intègre, on a  $A[X]^\times = A^\times$ . Supposons que l'on puisse écrire  $X - a = fg$ ,  $f, g \in A[X]$ . Remarquons que  $f$  et  $g$  sont non nuls. Comme  $A$  est intègre, on a  $\deg(X - a) = 1 = \deg(f) + \deg(g)$

En particulier,  $f$  ou  $g$  est constant, disons  $f$ . Dans ce cas,  $g$  est de degré 1. Écrivons  $f = b$  et  $g = cX + d$ . En identifiant les coefficients dominants, on obtient  $bc = 1$ . Ainsi,  $f = b \in A$  et  $X - a$  est bien irréductible.

L'exemple suivant montre que ce résultat n'est plus valable si  $A$  n'est plus intègre.

**Lemme 2.2.40** *Soit  $A$  un anneau, soit  $f \in A[X]$ , et soit  $a \in A$ . Alors,  $f$  est irréductible si et seulement si  $f(X - a)$  est irréductible.*

## 2.2.2 Polynômes irréductibles

**Définition 2.2.41** *Soit  $K$  un corps, et  $P(X) \in K[X]$  un polynôme. Le polynôme  $P$  est irréductible s'il ne peut pas se mettre sous la forme d'un produit de deux polynômes de degré au moins égal à 1. Les polynômes irréductibles sont aux polynômes ce que sont les nombres premiers aux nombres entiers.*

On peut particulier montrer que tout polynôme se décompose de manière unique (à l'ordre près des facteurs et à un coefficient multiplicatif constant près) en un produit de polynômes irréductibles.

### Exemple 2.2.42

1.  $P(X) = x^2 + x + 1$  est irréductible sur  $F_2$
2. Les polynômes de degré 3 irréductibles dans  $F_2[X]$  sont  $X^3 + X^2 + 1$  et  $X^3 + X + 1$ .
3. De manière générale, tout polynôme de degré 1 est irréductible dans  $K[X]$  et ceci quelque soit le corps, fini ou non.
4. Dans  $R[X]$  les polynômes irréductibles sont tous les polynômes de degré 1 et les polynômes de degré 2 dont le discriminant (le fameux  $\Delta = b^2 - 4ac$ ) est négatif.
5. Dans  $C[X]$  les polynômes irréductibles sont tous les polynômes de degré 1 et eux seulement.

Dans le cas des corps finis, on admettra le théorème suivant qui donne l'existence de polynômes irréductibles de tout degré.

**Théorème 2.2.43** *Soit  $p$  un nombre premier. Pour tout entier  $n \geq 1$  il existe un polynôme irréductible à coefficients dans  $F_p$  de degré  $n$ .*

Le théorème suivant donne une condition nécessaire et suffisante pour qu'un polynôme à coefficient dans un corps fini soit irréductible.

**Théorème 2.2.44** *Soit  $F_q$  un corps à  $q$  élément, un polynôme  $P \in F_q[X]$  de degré  $n \geq 1$  est irréductible si et seulement si*

1.  $P$  divise le polynôme  $X^{q^n} - X$ .
2.  $\text{pgcd}(X^{q^{n/t}} - X, P) = 1$  pour tout diviseur premier  $t$  de  $n$ .

### 2.2.3 Critère d'irréductibilité d'un polynôme sur $\mathbb{Q}$

**Définition 2.2.45** *Soit*

$$P = a_0 + a_1X + \dots + a_dX^d.$$

*Un polynôme à coefficients entiers. On définit le contenu de  $P$  comme le nombre*

$$c(P) = \text{PGCD}(a_0, a_1, \dots, a_d)$$

**Proposition 2.2.46** « *Lemme de Gauss* » *Soit  $P \in \mathbb{Z}[X]$  un polynôme primitif. Alors  $P$  est irréductible dans  $\mathbb{Q}[X]$  si et seulement s'il est irréductible dans  $\mathbb{Z}[X]$ .*

**Lemme 2.2.47** *Soient  $P, Q \in \mathbb{Z}[X]$ . Alors  $c(PQ) = c(P)c(Q)$ .*

**Théorème 2.2.48** (*Critère d'Eisenstein*). *Soit  $P \in \mathbb{Z}[X]$ ,  $P = a_nX^n + \dots + a_0$ .*

*Soit  $p$  un nombre premier. On suppose:*

1.  $p \nmid a^n$ .
2.  $p \mid a_i$ , pour  $i \leq n - 1$ .
3.  $p^2 \nmid a_0$ .



Alors  $P$  est irréductible sur  $Q$  (et donc dans  $Z$  pourvu que  $P$  soit primitif).

**Démonstration:**

En divisant par  $c(P)$  on peut supposer  $P$  primitif. Il suffit alors de montrer que  $P$  est irréductible dans  $\mathbb{Z}[X]$  par la **proposition 2.2.46**. Raisonnons par l'absurde : supposons que  $P = P_1 P_2$  dans  $\mathbb{Z}[X]$ , avec  $P_1$  et  $P_2$  non constants. Si  $Q = c_0 + \dots + c_q X^q \in \mathbb{Z}[X]$  et si  $p$  est un nombre premier, notons  $\overline{Q} = \overline{c_0} + \dots + \overline{c_q} X^q$  le polynôme de  $F_p[X]$  obtenu en prenant les classes des coefficients modulo  $p$  (« réduction de  $Q$  modulo  $p$  »).

Rappelons que  $F_p$  désigne le corps premier  $\mathbb{Z}/p\mathbb{Z}$ . L'égalité  $P = P_1 P_2$  donne par réduction modulo  $p$  la relation  $\overline{P} = \overline{P_1 P_2}$  dans  $F_p[X]$  (car il est immédiat de voir que  $\overline{P_1 P_2} = \overline{P_1} \cdot \overline{P_2}$  puisque l'application  $a \rightarrow \overline{a}$  de  $\mathbb{Z}$  dans  $F_p$  est un morphisme d'anneaux). Mais par hypothèse  $\overline{P} = \overline{a_d} X^d$ . Notons  $\alpha_0$  et  $\beta_0$  les coefficients constants de  $P_1$  et  $P_2$ , on en déduit que  $\overline{\alpha_0} = \overline{\beta_0} = 0$  dans  $F_p$ , on a en effet  $\overline{\alpha_0 \beta_0} = \overline{a_0} = 0$ , d'où  $\overline{\alpha_0} = 0$  ou  $\overline{\beta_0} = 0$  puisque  $F_p$  est un corps. Si par exemple  $\overline{\alpha_0} = 0$ , notons  $\overline{\alpha_r} X^r$  le monôme non nul de plus bas degré de  $\overline{P_1}$ , on a alors  $\beta_0 \overline{\alpha_r} = \overline{a_r} = 0$  d'où  $\overline{\beta_0} = 0$ . On en déduit que  $p \mid \alpha_0$  et  $p \mid \beta_0$ , et donc que  $p^2 \mid \alpha_0 \beta_0$ , soit  $p^2 \mid a_0$ , ce qui est contraire à l'hypothèse 3.

**Théorème 2.2.49** (réduction modulo  $p$ ). Soit  $p$  un nombre premier et soit

$P \in \mathbb{Z}[X]$ ,  $P = a^n X^n + \dots + a_0$ . On pose  $\overline{P} = C_p(a_n) X^n + \dots + C_p(a_0)$ . Si  $P$  est irréductible dans  $\mathbb{Z}/p\mathbb{Z}[X]$ , alors  $P$  est irréductible dans  $\mathbb{Q}[X]$  (et donc dans  $\mathbb{Z}[X]$  si il est primitif).

**Remarque:**

1- Il existe beaucoup de polynômes irréductibles de degré  $n$  dans  $F_p[x]$ , puisque leur nombre  $m_n(p)$  est encadré par

$$\frac{p^n - p^{\lfloor n/2 \rfloor + 1}}{n} \leq m_n(p) \leq \frac{p^n}{n}. \quad [15]$$

2- Si  $p$  un nombre premier.  $X^p - X - 1$  est irréductible sur  $\mathbb{Z}$ . [11]

3- Si  $p$  est un nombre premier,  $X^{p-1} + \dots + X + 1$  est irréductible sur  $\mathbb{Z}$  et  $\mathbb{Q}$ . (appliquer Eisenstein à  $P(X+1)$ ). [11]

### 2.2.4 Période d'un polynôme

\* Tout polynôme à une période, et la période d'un polynôme irréductible de degré  $n$  est  $2^m - 1$  sur  $F_2$ .

\* Tout polynôme irréductible sur  $GF(2)$  de degré  $m$  divise  $x^l + 1$  avec  $l = 2^m - 1$ .

\*  $x^3 + x + 1$  divise  $x^7 + 1$  on effet  $2^3 - 1 = 7$

\*  $x^7 + 1 = (x^4 + x^2 + x + 1)(x^3 + x + 1)$

## 2.3 Anneau quotient

### 2.3.1 Idéaux

Soit  $(A, +, \times)$  un anneau.

**Définition 2.3.50** On appelle idéal à droite (respectivement à gauche) de l'anneau  $A$ , tout ensemble  $I \subset A$  tel que

1.  $I$  est un sous groupe de  $(A, +)$ .
2.  $\forall x \in A, \forall y \in I, xy \in I$  (respectivement  $y \times x \in I$ ).

Si  $I$  est idéal à droite et à gauche de  $A$ , on dit que  $I$  est un idéal bilatère de  $A$ . Si l'anneau  $A$  est commutatif, tout idéal de  $A$  est bilatère, et dans ce cas on parle seulement d'idéal sans préciser s'il l'est à droite, à gauche ou bilatère.

**Exemple 2.3.51** Soit  $(A, +, \times)$  un anneau, alors  $I = \{O_A\}$  est un idéal bilatère de  $A$ .

**Proposition 2.3.52** Soit  $I$  un idéal à gauche (ou à droite) d'un anneau unitaire  $(A, +, \bullet)$ , alors  $1_A \in I \Leftrightarrow I = A \Leftrightarrow \exists x \in I, x$  est inversible.

**Définition 2.3.53** Soient  $A$  un anneau commutatif non nul et  $I$  un idéal de  $A$ . Alors la relation définie par:

$$x \Re y \Leftrightarrow x - y \in I$$

est une relation d'équivalence sur  $A$ , compatible avec les deux lois de  $A$ . L'ensemble quotient noté  $A/I$  (*muni des deux lois quotients*) est un anneau commutatif appelé anneau quotient de  $A$  par  $I$ . Il est clair que :

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

### 2.3.2 L'anneau $F_q[X] / (P)$

**Définition 2.3.54** Soit  $P$  un polynôme de  $F_q[X]$ . Soit  $A, B \in F_q[X]$ , on dit que  $A$  est congru à  $B$  modulo  $P$ , si  $P$  divise  $A - B$ . Cette propriété se note  $A \equiv B \pmod{P}$  ou  $A \equiv B[P]$ .

**Définition 2.3.55** Soit  $P \in F_q[X]$ . La relation  $A \Re B \Leftrightarrow A \equiv B[P]$  est une relation d'équivalence. On note  $F_q[X] / (P)$  l'ensemble quotient de  $F_q[X]$  par cette relation d'équivalence.

### 2.3.3 Quelques propriétés dans L'anneau $F_q[X] / (P)$

**Proposition 2.3.56** L'addition, la multiplication et la multiplication par un scalaire, définies sur l'ensemble quotient  $K[X] / \langle P \rangle$  par

$$\forall (A, B) \in K[X]^2, \begin{cases} \overline{A + B} = \overline{A} + \overline{B}, \\ \overline{AB} = \overline{A}\overline{B}, \\ \forall a \in \mathbb{k}, a\overline{A} = \overline{aA}, \end{cases}$$

font de  $K[X] / \langle P \rangle$  une  $\mathbb{k}$ -algèbre dans laquelle l'élément neutre de l'addition est  $\bar{0}$ , classe du polynôme  $0 \in \mathbb{k}[x]$ , et l'élément neutre de la multiplication est  $\bar{1}$ , classe du polynôme  $1 \in \mathbb{k}[x]$ . Alors  $(K[X] / \langle P \rangle, \bar{+}, \bar{\times})$  est un anneau.

**Proposition 2.3.57** Les éléments inversibles de  $F_q[X] / (P)$  sont les classes des polynômes premiers avec  $P$ .

**Proposition 2.3.58** L'anneau  $(F_q[X] / (P), \bar{+}, \bar{\times})$  est un corps si et seulement si  $P$  est irréductible sur  $F_q[X]$ .

**Théorème 2.3.59** Soit  $P \in K[X]$  un polynôme non constant. La classe  $\overline{A} \in K[X]/\langle P \rangle$  d'un polynôme  $A \in K[X]$  est inversible dans  $K[X]/\langle P \rangle$  si et seulement si  $A$  est premier avec  $P$ .

**Exemple 2.3.60** (Construction des corps finis)

- Le corps fini  $F_{2^3}$

On considère le polynôme  $P(X) = X^3 + X + 1$  de  $F_2[X]$ ,  $P$  est irréductible. Alors  $F_2[X]/(P(X))$  est un corps.

$$F_2[\alpha]/(P(\alpha)) = \{a\alpha^2 + b\alpha + c \mid a, b, c \in F_2\}.$$

$$F_2[\alpha]/(P(\alpha)) = \{0, 1, \alpha, \alpha^2, 1 + \alpha, 1 + \alpha^2, \alpha + \alpha^2, 1 + \alpha + \alpha^2\}.$$

$$\#F_2[\alpha]/(P(\alpha)) = 8 = 2^3.$$

$$F_2[\alpha]/(P(\alpha)) = F_{2^3}$$

### Addition

L'addition dans  $F_{2^3}$  se fait modulo 2 avec  $1 + 1 = 0$ .

$$(1 + \alpha^2) + (\alpha + \alpha^2) = 1 + \alpha, \quad (1 + \alpha^2) + (1 + \alpha^2) = 0.$$

### Multiplication

La multiplication dans  $F_{2^3}$  se fait modulo 2 et  $X^3 + X + 1$ , avec  $\alpha^3 = -\alpha - 1 = \alpha + 1$ .

$$\begin{aligned} (1 + \alpha^2) \times (\alpha + \alpha^2) &= \alpha + \alpha^2 + \alpha^3 + \alpha^4 \\ &= \alpha + \alpha^2 + (\alpha + 1) + (\alpha^2 + \alpha) \\ &= 1 + \alpha \end{aligned}$$

$\times$	1	$\alpha$	$1 + \alpha$	$\alpha^2$	$1 + \alpha^2$	$\alpha + \alpha^2$	$1 + \alpha + \alpha^2$
1	1	$\alpha$	$1 + \alpha$	$\alpha^2$	$1 + \alpha^2$	$\alpha + \alpha^2$	$1 + \alpha + \alpha^2$
$\alpha$	$\alpha$	$\alpha^2$	$\alpha + \alpha^2$	$1 + \alpha$	1	$1 + \alpha + \alpha^2$	$1 + \alpha^2$
$1 + \alpha$	$1 + \alpha$	$\alpha + \alpha^2$	$1 + \alpha^2$	$1 + \alpha + \alpha^2$	$\alpha^2$	1	$\alpha$
$\alpha^2$	$\alpha^2$	$1 + \alpha$	$1 + \alpha + \alpha^2$	$\alpha + \alpha^2$	$\alpha$	$1 + \alpha^2$	1
$1 + \alpha^2$	$1 + \alpha^2$	1	$\alpha^2$	$\alpha$	$1 + \alpha + \alpha^2$	$1 + \alpha$	$\alpha + \alpha^2$
$\alpha + \alpha^2$	$\alpha + \alpha^2$	$1 + \alpha + \alpha^2$	1	$1 + \alpha^2$	$1 + \alpha$	$\alpha$	$\alpha^2$
$1 + \alpha + \alpha^2$	$1 + \alpha + \alpha^2$	$1 + \alpha^2$	$\alpha$	1	$\alpha + \alpha^2$	$\alpha^2$	$1 + \alpha$

- Le corps fini  $F_{3^2}$

Le polynôme  $X^2 + X + 2$  de  $F_3[X]$ ,  $P$  est irréductible sur  $F_3[X]$ . Alors  $F_3[X]/(P(X))$  est un corp.

Soit  $\alpha$  racine de  $P$  dans  $F_3$

$F_9 = F_{3^2}$  est un espace vectoriel sur  $F_3$  de dimension  $n = 2$  don  $\{1, \alpha\}$  est une base

$$F_3[X]/(P(X)) = \{a + b\alpha \mid a, b \in F_3\}$$

$$= \{0, 1, 2, 1 + \alpha, 1 + 2\alpha, 2 + \alpha, 2 + 2\alpha, \alpha, 2\alpha\}$$

on  $\alpha^2 + \alpha + 2 = 0$ ,  $\alpha^2 = -\alpha - 1 = 2\alpha + 1$ .

### Addition

L'addition dans  $F_{3^2}$  se fait modulo 3 avec  $1 + 1 + 1 = 0$

$$(1 + \alpha) + \alpha = 1 + 2\alpha \quad 2\alpha + \alpha = 3\alpha = 0 \quad (2 + 2\alpha) + 2\alpha = 2 + 4\alpha = 2 + \alpha.$$

### Multiplication

La multiplication dans  $F_{3^2}$  se fait modulo 3 et  $\alpha^2 + \alpha + 2$ , avec  $\alpha^2 = -\alpha - 2 = 2\alpha + 1$   
calcul de  $\alpha^3$

$$\begin{aligned} \alpha^3 &= \alpha^2 \cdot \alpha = (1 + 2\alpha) \cdot \alpha = \alpha + 2\alpha^2 \\ &= \alpha + 2(1 + 2\alpha) = \alpha + 2 + 4\alpha \\ &= 2 + 2\alpha \end{aligned}$$

$$(2 + \alpha) \cdot (2 + 2\alpha) = 4 + 4\alpha + 2\alpha + 2\alpha^2 = 1 + 2\alpha^2$$

$$= 1 + 2(1 + 2\alpha)$$

$$= 4\alpha = \alpha$$

$\times$	1	2	$\alpha$	$1 + \alpha$	$2 + \alpha$	$2\alpha$	$1 + 2\alpha$	$2 + 2\alpha$
1	1	2	$\alpha$	$1 + \alpha$	$2 + \alpha$	$2\alpha$	$1 + 2\alpha$	$2 + 2\alpha$
2	2	1	$2\alpha$	$2 + 2\alpha$	$1 + 2\alpha$	$\alpha$	$2 + \alpha$	$1 + \alpha$
$\alpha$	$\alpha$	$2\alpha$	$1 + 2\alpha$	1	$1 + \alpha$	$2 + \alpha$	$2 + 2\alpha$	2
$1 + \alpha$	$1 + \alpha$	$2 + 2\alpha$	1	$2 + \alpha$	$2\alpha$	2	$\alpha$	$1 + 2\alpha$
$2 + \alpha$	$2 + \alpha$	$1 + 2\alpha$	$\alpha + 1$	$2\alpha$	2	$2 + 2\alpha$	1	$\alpha$
$2\alpha$	$2\alpha$	$\alpha$	$2 + \alpha$	2	$2 + 2\alpha$	$1 + 2\alpha$	$1 + \alpha$	1
$1 + 2\alpha$	$1 + 2\alpha$	$2 + \alpha$	$2 + 2\alpha$	$\alpha$	1	$1 + \alpha$	2	$2\alpha$
$2 + 2\alpha$	$2 + 2\alpha$	$1 + \alpha$	2	$1 + 2\alpha$	$\alpha$	1	$2\alpha$	$2 + \alpha$

# Chapitre 3

## Divisibilité des trinômes $x^{am} + x^{bs} + 1$ par un polynôme irréductible sur $F_2$

### 3.1 Introduction

Les polynômes irréductibles sur les corps finis ont beaucoup d'application dans la théorie des nombres et sont souvent utilisés dans la construction des codes correcteurs d'erreurs. Les trinômes irréductibles présentent un grand défi pour les chercheurs malgré les résultats qui paraissent régulièrement. Dans cette partie on étudie la divisibilité des trinômes du type

$$x^{am} + x^{bs} + 1$$

par un polynôme irréductible de degré  $r$ , sur le corps fini  $F_2$ , pour  $a, b$  des entiers quelconques et  $m, s$  des entiers à déterminer.

### 3.2 Divisibilité d'un trinôme sur un corps fini

#### 3.2.1 Primitivité d'un polynôme irréductible sur un corps fini

**Définition 3.2.61** Soit  $T$  un polynôme irréductible de degré  $r > 1$  sur  $F_2$ . La primitivité de  $T$  est le plus petit entier positif  $t$  tel que  $T$  divise  $x^t - 1$ .

**Exemple 3.2.62**

1- Soit le polynôme  $T = x^4 + x^3 + x^2 + x + 1$  irréductible sur  $F_2$  et faisons les divisions de  $x^t - 1$  par  $T$  pour  $t = 2, 3, 4, 5, \dots$ , sur  $F_2$

$$x^2 + 1 \equiv x^2 + 1 \pmod{(T)}$$

$$x^3 + 1 \equiv x^3 + 1 \pmod{(T)}$$

$$x^4 + 1 \equiv x^3 + x^2 + 1 \pmod{(T)}$$

$$x^5 + 1 \equiv (x + 1)(x^4 + x^3 + x^2 + x + 1) \pmod{(T)}$$

$$x^5 + 1 \equiv 0 \pmod{(T)}$$

Ainsi la primitivité du polynôme  $T$  est  $t = 5$

2- Soit le polynôme  $T' = x^2 + x + 1$  irréductible sur  $F_2$  et faisons les divisions de  $x^t - 1$  par  $T'$  pour  $t = 2, 3, 4, \dots$  sur  $F_2$

$$x^2 - 1 \equiv x \pmod{(T')}$$

$$x^3 - 1 \equiv (x - 1)(x^2 + x + 1) \pmod{(T')}$$

$$x^3 - 1 \equiv 0 \pmod{(T')}$$

Alors la primitivité du polynôme  $T'$  est  $t = 3$

**3.2.2 Théorèmes de base sur la divisibilité des trinômes  $x^{am} + x^{bs} + 1$  par un polynôme irréductible sur  $F_2$**

**Théorème 3.2.63** [6] *Soit  $T$  un polynôme irréductible de degré  $r > 1$  sur  $F_2$ , ayant  $\alpha$  comme racine dans une extension.  $T$  divise un certain trinôme si et seulement si ils existent des entiers distincts  $i$  et  $j$  tels que  $\alpha^i + \alpha^j = 1$ .*

**Preuve.** Le trinôme  $h(x) = x^i + x^j + 1$  est divisible par  $T$  si et seulement si  $h(\alpha) = \alpha^i + \alpha^j + 1 = 0$  c'est à dire  $\alpha^i + \alpha^j = 1$ . ■

**Théorème 3.2.64** [6] *Soit  $T$  un polynôme irréductible de degré  $r > 1$  sur  $F_2$  et de primitivité  $t$ , ayant  $\alpha$  comme racine dans une extension. Si  $T$  divise un trinôme quelconque, alors il divise infiniment des trinômes.*



**Preuve.** supposons que le polynôme  $T$ , de primitivité  $t$ , divise le trinôme  $x^m + x^s + 1$ . Alors  $T$  divise aussi la famille des trinômes  $x^{m+\mu t} + x^{s+vt} + 1$  pour tous les entiers positifs  $\mu$  et  $v$ . ■

**Théorème 3.2.65** [6] *Soit  $T$  un polynôme irréductible de degré  $r > 1$  sur  $F_2$ , ayant  $\alpha$  comme racine dans une extension. Si  $T$  divise des trinômes quelconque, alors il divise un certain trinôme de degré  $< t$ .*

**Preuve.** Si  $T$  divise  $x^m + x^s + 1$ , nous avons  $\alpha^m + \alpha^s + 1 = 0$ . Comme  $\alpha^t = 1$ , ce qui donne  $\alpha^{m'} + \alpha^{s'} + 1 = 0$  où  $m \equiv m' \pmod{t}$  et  $s \equiv s' \pmod{t}$ , pour lequel  $m'$  et  $s'$  sont dans l'ensemble  $\{0, t, \dots, t-1\}$ . Alors  $T$  doit diviser un certain trinôme  $x^{m'} + x^{s'} + 1$  de degré  $< t$ . ■

### 3.2.3 Condition nécessaire de divisibilité des trinômes $x^{am} + x^{bs} + 1$ par un polynôme irréductible sur $F_2$

Dans cette section nous considérons que les conditions de divisibilité des trinômes  $x^{am} + x^{bs} + 1$  par un polynôme irréductible de degré donné sur  $F_2$ . Soit  $f$  un polynôme irréductible de degré  $n$  sur  $F_2$  et  $a$  et  $b$  entiers positifs, il a été prouvé que s'ils existent entiers positifs  $m$  et  $s$  tel que  $f$  divise  $x^{am} + x^{bs} + 1$ , alors  $a$  et  $b$  ne sont pas divisible par  $2^n - 1$ . ci dessus nous donnons un raffinement de ce resultat

**Théorème 3.2.66** [8] *Soit  $f$  un polynôme irréductible d'ordre  $e > 1$  sur  $F_2$  et  $a, b$  des entiers positifs. S'il existe des entiers positifs  $m, s$  tels que  $f$  divise trinômes  $x^{am} + x^{bs} + 1$  ( $am > bs$ ), alors  $am, bs$  et  $am - bs$  ne sont pas divisible par  $e$ .*

**Preuve.** Soit  $\alpha$  une racine de  $f$  dans une certaine extension de  $F_2$ . Si  $am$  est divisible par  $e$ , alors  $\alpha^{am} = 1$ , donc  $f$  divise un polynôme  $x^{am} + 1$ . Comme  $e > 1$ ,  $f(0) \neq 0$  et donc  $f$  ne divise pas  $x^{bs}$ . Par conséquent  $f$  ne peut pas diviser le trinôme  $x^{am} + x^{bs} + 1$ . Le cas où  $bs$  est divisé par  $e$  est très similaire. supposer  $am - bs$  est divisée par  $e$ . Ensuite, de la même façon que ci-dessus, nous voyons facilement que  $x^{am-bs} + 1$  est divisé par  $f$  et donc  $x^{am} + x^{bs} + 1 = x^{bs} (X^{am-bs} + 1) + 1$  est ne divise pas par  $f$ .

Si  $f$  est un polynôme irréductible de l'ordre  $e$  et degré  $n$  sur  $F_2$ , Alors  $e$  est un diviseur de  $2^n - 1$ . Ainsi, le théorème ci-dessus découle directement le résultat dans [3], et si  $a = b = 1$  et  $f = x^2 + x + 1$  alors l'inverse de théorème est également vrai. ■

**Corollaire 3.2.67** [8] *Le trinôme  $x^n + x^k + 1$  ( $n > k$ ) est divisé par  $x^2 + x + 1$  si et seulement si  $n$ ,  $k$ , et  $n - k$  ne sont pas divisés par 3.*

**Preuve.** Depuis l'ordre du  $x^2 + x + 1$  qui est 3, la nécessité est clair d'après le théorème ci-dessus. Supposons que  $n$ ,  $k$ , et  $n - k$  ne sont pas divisés par trois. Alors nous obtenons deux cas

$$n \equiv 2(\text{mod } 3), k \equiv 1(\text{mod } 3), n - k \equiv 1(\text{mod } 3)$$

ou

$$n \equiv 1(\text{mod } 3), k \equiv 2(\text{mod } 3), n - k \equiv 2(\text{mod } 3)$$

1- Soit  $\alpha$  soit une racine de  $x^2 + x + 1$ , puis dans le premier cas, nous avons

$$\alpha^n + \alpha^k + 1 = \alpha^{3n_1+2} + \alpha^{3k_1+1} + 1 = \alpha^2 + \alpha + 1 = 0$$

Ainsi  $x^2 + x + 1$  divise  $x^n + x^k + 1$ . Le deuxième cas est similaire ■

Enfin, nous considérons que le critère pour tester si un polynôme irréductible divise trinômes de type  $X^{am} + X^{bs} + 1$  sur  $F_2$ .

**Théorème 3.2.68** (*Critère de Welch*) [6]

*Pour tout entier impair  $t$ , les polynômes irréductibles de primitivité  $t$  divisent des trinômes si et seulement si le pgcd  $[1 + x^t, 1 + (1 + x^t)]$  est de degré supérieur à 1.*

**Preuve.** Soit

$$c_t(x) = \frac{x^t - 1}{x - 1} = f_1(x) f_2(x) \dots f_r(x)$$

la factorisation de  $c_t(x)$  en facteurs irréductible. Alors

$$1 + x^t = (1 + x) c_t(x)$$

(sur  $F_2$ ) et

$$1 + (1 + x)^t = x c_t(1 + x)$$

Ainssi, excepté pour des facteurs linéaires possibles,

$$\text{pgcd} [1 + x^t, 1 + (1 + x)^t] = \text{pgcd} [c_t(x), c_t(1 + x)]$$

Alors collectivement les racines de  $f_1(x), f_2(x), \dots, f_r(x)$  sont

$$\alpha, \alpha^2, \alpha^3, \dots, \alpha^{t-1}$$

où  $\alpha \neq 0$  et  $\alpha^t = 1$ .

Par conséquent, les racines des facteurs irréductibles de  $c_t(1 + x)$  sont

$$1 + \alpha, 1 + \alpha^2, 1 + \alpha^3, \dots, 1 + \alpha^{t-1}$$

Ainssi, le pgcd en question est de degré supérieur à 1 si et seulement si les racines  $1 + \alpha^j$  de  $c_t(1 + x)$  sont égales aux racines  $\alpha^i$  de  $c_t(x)$ , c'est à dire

$$1 + \alpha^j = \alpha^i$$

qui est précisément la condition qu'un facteur de  $c_t(x)$  ayant  $\alpha$  comme racine divise le trinôme  $x^i + x^j + 1$ . ■

**Théorème 3.2.69** [9] *Soit  $T$  un polynôme irréductible de degré  $n > 1$  sur  $F_2$  et soient  $a, b$  des entiers non nuls. S'ils existent  $m, s$  des entiers positifs tels que  $T$  divise  $x^{am} + x^{bs} + 1$ , alors  $a$  et  $b$  ne sont pas divisible par  $2^n - 1$ .*

**Preuve.** Supposons que  $a$  ou  $b$  est divisible par  $(2^n - 1)$  et nous voulons montrer que le polynôme  $T$ , irréductible de degré  $n$ , ne divise pas  $x^{am} + x^{bs} + 1$  quels que soient les entiers  $m$  et  $s$ .

1- Si  $a = 0 \pmod{(2^n - 1)}$  a s'écrit  $a \equiv a_1(2^n - 1)$  et sachant que  $(x^{2^n-1} - 1) \equiv 0 \pmod{(T)}$  alors  $x^{2^n-1} \equiv 1 \pmod{(T)}$  d'où  $(x^{2^n-1} - 1)^{a_1 m} \equiv (1)^{a_1 m} \pmod{(T)} \equiv 1 \pmod{(T)}$  c'est à dire que  $(x^{2^n-1})^{a_1 m} + 1 \equiv 0 \pmod{(T)}$ . Mais le polynôme  $T$  ne divise pas le monôme  $x^{bs}$  ( $n > 1$ ), ainsi le polynôme  $T$  ne divise pas le trinôme  $x^{am} + x^{bs} + 1$  quelques soient  $m, s$  entiers.

2- Si  $b = 0 \pmod{(2^n - 1)}$ , b s'écrit  $b \equiv b_1(2^n - 1)$ , alors  $(x^{2^n-1})^{b_1 s} + 1 \equiv 0 \pmod{(T)}$ . Mais le polynôme  $T$  ne divise pas le monôme  $x^{am}$  ( $n > 1$ ), ainsi le polynôme  $T$  ne divise le trinôme  $x^{am} + x^{bs} + 1$  quelques soient  $m, s$  entiers.

Donc le polynôme  $T$  ne divise pas le trinôme  $x^{am} + x^{bs} + 1$  quelques soient  $m, s$  si  $a$  ou  $b$  est divisible par  $(2^n - 1)$ . ■

### 3.3 Recherche des trinômes irréductible sur $F_2$ de degré $\leq 100$

Voici le programme Maple de recherche des trinômes irréductibles sur  $F_2$  pour des valeurs de a,b et M une borne fixée

```
> search3 := proc(a, b, p, M)
> local m, s, nb, total, f, B;
> nb := 0;
> total := 0;
> for m from 1 while a*m <= M do
>   for s from 1 while b*s < a*m do
>     f := x^(am) + x^(bs) + 1;
>     B := Irreduc(f) mod p;
>     total := total + 1;
>     if B True then nb := nb + 1, print(f) fi;
>   od
> od;
> nb, total, evalf(nb/total)
> end;
```

**Les trinômes  $x^{am} + x^{bs} + 1$  irréductible sur  $F_2$  pour:**

$(a, b) = (3, 7)$ ,  $(a, b) = (5, 3)$ ,  $(a, b) = (3, 5)$ ,  $(a, b) = (7, 5)$  de degré  $\leq 100$ .

**Résultats pratiques**

<i>search3</i> (3, 7, 2, 100)	<i>search3</i> (5, 3, 2, 100)	<i>search3</i> (3, 5, 2, 100)	<i>search3</i> (7, 5, 2, 100)
$x^{12} + x^7 + 1$	$x^5 + x^3 + 1$	$x^6 + x^5 + 1$	$x^{14} + x^5 + 1$
$x^{15} + x^7 + 1$	$x^{10} + x^3 + 1$	$x^9 + x^5 + 1$	$x^{28} + x^{15} + 1$
$x^{15} + x^{14} + 1$	$x^{20} + x^3 + 1$	$x^{12} + x^5 + 1$	$x^{28} + x^{25} + 1$
$x^{18} + x^7 + 1$	$x^{20} + x^{15} + 1$	$x^{18} + x^{15} + 1$	$x^{42} + x^{35} + 1$
$x^{21} + x^7 + 1$	$x^{25} + x^3 + 1$	$x^{33} + x^{10} + 1$	$x^{49} + x^{15} + 1$
$x^{21} + x^{14} + 1$	$x^{25} + x^{18} + 1$	$x^{33} + x^{20} + 1$	$x^{49} + x^{40} + 1$
$x^{30} + x^{21} + 1$	$x^{30} + x^9 + 1$	$x^{36} + x^{15} + 1$	$x^{63} + x^5 + 1$
$x^{36} + x^{21} + 1$	$x^{30} + x^{21} + 1$	$x^{36} + x^{25} + 1$	$x^{63} + x^{35} + 1$
$x^{39} + x^{14} + 1$	$x^{35} + x^{33} + 1$	$x^{39} + x^{25} + 1$	$x^{84} + x^5 + 1$
$x^{39} + x^{35} + 1$	$x^{55} + x^{24} + 1$	$x^{39} + x^{35} + 1$	$x^{84} + x^{35} + 1$
$x^{42} + x^7 + 1$	$x^{55} + x^{48} + 1$	$x^{42} + x^{35} + 1$	$x^{84} + x^{45} + 1$
$x^{42} + x^{35} + 1$	$x^{60} + x^9 + 1$	$x^{54} + x^{45} + 1$	$x^{84} + x^{75} + 1$
$x^{54} + x^{21} + 1$	$x^{60} + x^{15} + 1$	$x^{57} + x^{25} + 1$	
$x^{57} + x^7 + 1$	$x^{60} + x^{45} + 1$	$x^{57} + x^{35} + 1$	
$x^{57} + x^{35} + 1$	$x^{60} + x^{51} + 1$	$x^{57} + x^{50} + 1$	
$x^{60} + x^{49} + 1$	$x^{65} + x^{18} + 1$	$x^{60} + x^{15} + 1$	
$x^{63} + x^{28} + 1$	$x^{65} + x^{33} + 1$	$x^{60} + x^{45} + 1$	
$x^{66} + x^{35} + 1$	$x^{90} + x^{27} + 1$	$x^{63} + x^5 + 1$	
$x^{66} + x^{63} + 1$	$x^{90} + x^{63} + 1$	$x^{63} + x^{35} + 1$	
$x^{81} + x^{35} + 1$	$x^{95} + x^{78} + 1$	$x^{81} + x^{35} + 1$	
$x^{81} + x^{77} + 1$	$x^{95} + x^{84} + 1$	$x^{81} + x^{65} + 1$	
$x^{84} + x^{35} + 1$	$x^{100} + x^{15} + 1$	$x^{84} + x^5 + 1$	
$x^{84} + x^{49} + 1$	$x^{100} + x^{51} + 1$	$x^{84} + x^{35} + 1$	
$x^{90} + x^{63} + 1$	$x^{100} + x^{63} + 1$	$x^{84} + x^{45} + 1$	
$x^{93} + x^{91} + 1$	$x^{100} + x^{75} + 1$	$x^{84} + x^{75} + 1$	
	$x^{100} + x^{81} + 1$		
25, 222, 0.01126126126	26, 337, 0.07715133531	25, 317, 0.07886435331	12, 139, 0.08633093525

**Pour  $(a, b) = (1, 1)$  et de degré  $\leq 40$**

*Search* (1, 1, 2, 40)

$x^2 + x + 1$	$x^{14} + x^5 + 1$	$x^{21} + x^{19} + 1$	$x^{31} + x^6 + 1$
$x^3 + x + 1$	$x^{14} + x^9 + 1$	$x^{22} + x + 1$	$x^{31} + x^7 + 1$
$x^3 + x^2 + 1$	$x^{15} + x + 1$	$x^{22} + x^{21} + 1$	$x^{31} + x^{13} + 1$
$x^4 + x + 1$	$x^{15} + x^4 + 1$	$x^{23} + x^5 + 1$	$x^{31} + x^{18} + 1$
$x^4 + x^3 + 1$	$x^{15} + x^7 + 1$	$x^{23} + x^9 + 1$	$x^{31} + x^{24} + 1$
$x^5 + x^2 + 1$	$x^{15} + x^8 + 1$	$x^{23} + x^{14} + 1$	$x^{31} + x^{25} + 1$
$x^5 + x^3 + 1$	$x^{15} + x^{11} + 1$	$x^{23} + x^{18} + 1$	$x^{31} + x^{28} + 1$
$x^6 + x + 1$	$x^{15} + x^{14} + 1$	$x^{25} + x^3 + 1$	$x^{33} + x^{10} + 1$
$x^6 + x^3 + 1$	$x^{17} + x^3 + 1$	$x^{25} + x^7 + 1$	$x^{33} + x^{13} + 1$
$x^6 + x^5 + 1$	$x^{17} + x^5 + 1$	$x^{25} + x^{18} + 1$	$x^{33} + x^{20} + 1$
$x^7 + x + 1$	$x^{17} + x^6 + 1$	$x^{25} + x^{22} + 1$	$x^{33} + x^{23} + 1$
$x^7 + x^3 + 1$	$x^{17} + x^{11} + 1$	$x^{28} + x + 1$	$x^{34} + x^7 + 1$
$x^7 + x^4 + 1$	$x^{17} + x^{12} + 1$	$x^{28} + x^3 + 1$	$x^{34} + x^{27} + 1$
$x^7 + x^6 + 1$	$x^{17} + x^{14} + 1$	$x^{28} + x^9 + 1$	$x^{35} + x^2 + 1$
$x^9 + x + 1$	$x^{18} + x^3 + 1$	$x^{28} + x^{13} + 1$	$x^{35} + x^{33} + 1$
$x^9 + x^4 + 1$	$x^{18} + x^7 + 1$	$x^{28} + x^{15} + 1$	$x^{36} + x^9 + 1$
$x^9 + x^5 + 1$	$x^{18} + x^9 + 1$	$x^{28} + x^{19} + 1$	$x^{36} + x^{11} + 1$
$x^9 + x^8 + 1$	$x^{18} + x^{11} + 1$	$x^{28} + x^{25} + 1$	$x^{36} + x^{15} + 1$
$x^{10} + x^3 + 1$	$x^{18} + x^{15} + 1$	$x^{28} + x^{27} + 1$	$x^{36} + x^{21} + 1$
$x^{10} + x^7 + 1$	$x^{20} + x^3 + 1$	$x^{29} + x^2 + 1$	$x^{36} + x^{25} + 1$
$x^{11} + x^2 + 1$	$x^{20} + x^5 + 1$	$x^{29} + x^{27} + 1$	$x^{36} + x^{27} + 1$
$x^{11} + x^9 + 1$	$x^{20} + x^{15} + 1$	$x^{30} + x + 1$	$x^{39} + x^4 + 1$
$x^{12} + x^3 + 1$	$x^{20} + x^{17} + 1$	$x^{30} + x^9 + 1$	$x^{39} + x^8 + 1$
$x^{12} + x^5 + 1$	$x^{21} + x^2 + 1$	$x^{30} + x^{21} + 1$	$x^{39} + x^{14} + 1$
$x^{12} + x^7 + 1$	$x^{21} + x^7 + 1$	$x^{30} + x^{29} + 1$	$x^{39} + x^{25} + 1$
$x^{12} + x^9 + 1$	$x^{21} + x^{14} + 1$	$x^{31} + x^3 + 1$	$x^{39} + x^{31} + 1$
			$x^{39} + x^{35} + 1$

105, 780, 0.1346153846

# Conclusion

Dans ce mémoire nous avons étudié la divisibilité des trinômes de la forme

$$x^{am} + x^{bs} + 1$$

par un polynôme irréductible de degré quelconque, en particulier la divisibilité de ces trinômes sur  $F_2$ , cette divisibilité est un problème d'actualité.

Les trinômes irréductible de degré  $n$  sur  $F_2$  n'existe pas toujours et dans le cas où il n'y a pas de trinôme irréductible de degré  $n$ , il peut être efficace d'utiliser des trinômes avec un facteur irréductible de degré  $n$ .

Dans notre travail, nous considérons certaines conditions dans lesquelles les polynômes irréductible divisent des trinômes sur  $F_2$ , l'extension du critère de Welch pour tester si un polynôme irréductible divise les trinômes  $x^m + x^s + 1$  vers les trinômes  $x^{am} + x^{bs} + 1$  est présentée.

La condition nécessaire de divisibilité des trinômes par un polynôme irréductible sur  $F_2$  est la suivante:

Soit  $P$  un polynôme irréductible de degré  $n$  sur  $F_2$  et  $a, b$  entiers positifs, il a été prouvé que s'ils existent entiers positifs  $m, s$  telque  $P$  divise  $x^{am} + x^{bs} + 1$ , alors  $a$  et  $b$  ne sont pas divisible par  $2^n - 1$ .

# Bibliographie

- [1] G.BERHUY, Anneaux des polynômes, (cours général) .
- [2] A, BRUASSE-BAC ESIL, Corps finis, (cours général) .
- [3] H. CHAPDELAINE, Théorie des anneaux commutatifs, Hiver, 2013.
- [4] J. P. CHERDIEU, Introduction aux corps finis et aux sommes de Gauss et Jacobi, Ecole du CIMPA UNSA ICTP UNESCO ICIMAF, 2000
- [5] Z. GILLES, Arithmétique 1: corps finis et applications, Master CSI, 11 Décembre 2006..
- [6] W. GOLOMB AND PEY-FENG LEE. Irreducible Polynomials Wich divide Trinomials Over  $GF(2)$ , IEEE Vol. 53. pp. 768-774. 2007.
- [7] R. JEAN JACQUES & B.PASCAL, Algèbre Pour La licence 3, Dunod, Paris, 2006.
- [8] R. KIM, W.KOEPEF, Divisibilité of Trinômials by Irreductible Polynmials over  $F_2$ , International Journal of Algèbre,vol 3, no 4, 189-197, 2009.
- [9] C. MIHOUBI, Condition nécessaire de la divisibilité de trinômes  $x^{am} + x^{bs} + 1$  par un polynôme irréductible de degré r sur  $GF(2)$ , International Journal of Algèbre, 2 (13) (2008), 645-648.
- [10] D. OLIVIER, Algèbre2, Ecole Normal Supérieure, 2012-2013.
- [11] L. PIERRE, Anneaux  $\mathbb{Z}/n\mathbb{Z}$ . Application, Decembre 18, 2009.
- [12] L. PIERRE, Corps fini. Application, May 6, 2010.



- [13] D. PERRIN. Cours d'algèbre, Ellipses, 1990.
- [14] L. PIERRE, Polynômes irréductibles. Corps de repture. Exemples et applications, janaury 4, 2010.
- [15] É. WEGRZYŃOWSKI, Corps finis, Licensce et Master mention informatique, USTL, 15 mars 2007.

# Résumé

Ce travail porte sur la divisibilité des trinômes de la forme  $x^{am} + x^{bs} + 1$  par un polynôme irréductible de degré quelconque sur  $F_2$ . Le contenu est composé de trois chapitres:

1- Le premier est consacré à l'étude des corps finis. Ils sont à la base de nombreuses applications algorithmiques, notamment en cryptographie et en codage de l'information.

2- Le deuxième consiste en la recherche des polynômes irréductibles sur un corps fini à deux éléments.

3- Dans le troisième nous étudions la divisibilité de ces trinômes par un polynôme irréductible dans un corps à deux éléments, nous concluons le resultat suivant [9]:

- Soit  $T$  un polynôme irréductible de degré  $n$  sur  $F_2$  et  $a, b$  entiers positifs, il a été prouvé que s'ils existent des entiers positifs  $m, s$  telque  $T$  divise  $x^{am} + x^{bs} + 1$ , alors  $a$  et  $b$  ne sont pas divisible par  $2^n - 1$ .

# Abstract

This work deals with divisibility trinomials of the form  $x^{am} + x^{bs} + 1$  by an irreducible polynomial of any degree of  $F_2$ . The content is divided into three chapters:

1. The first is devoted to the study of finite fields. They are the basis of many algorithmic applications, including cryptography and coding information.
2. The second is the search for irreducible polynomials over a finite field of two elements
3. In the third we study the divisibility of these trinomials by an irreducible polynomial in a field with two elements, we conclude the following result [9]:
  - Let  $T$  be an irreducible polynomial of degree  $n$  over  $F_2$  and  $a, b$  positive integers, it has been proven that they exist positive integers  $m, s$  telque  $T$  divides  $x^{am} + x^{bs} + 1$ , then  $a$  and  $b$  are not divisible by  $2^n - 1$ .