UNIVERSITE MOHAMED BOUDIAF DE M'SILA

Faculté des Mathématiques et de l'Informatique

Département de Mathématiques

MEMOIRE DE FIN D'ETUDE

Présenté pour l'obtention du Diplôme de **MASTER**

Domaine : Mathématiques et Informatique

Filière Mathématiques**:**

Option : Algèbre et Mathématiques Discrètes

Par

Houichi Loubna

Sujet

Sur les polynômes irréductibles

Date de soutenance 20/06 /2018

Devant le jury :

Mr.D .Mihoubi. Prof. Univ de M'sila Président

Mr.L.Heboub . M.A.A Univ de M'sila Rapporteur

Mr.K.Saadaui. M.A.A Univ de M'sila Examinateur

Promotion : 2017 / 2018

Remerciements

Je remercie mon dieu **ALLAH** qui est toujours présent avec moi

dans le meilleur et dans le pire·

Je remercie **Mr Heboub Lakhdar** pour son encadrement et pour l'aide qu'il m'a apportée·

Je tiens à remercier Monsieur **D. Mihoubi** pour l'intérêt qu'il a

porté à mon travail. C'est pour moi un honneur qu'il a accepté de présider le jury.

Je suis très reconnaissant a messieur **k. Saadaui** d'avoir accepter d'examiner ce travail et de me faire l'honneur de participer au jury.

Enfin je remercie tous les professeurs de département de Mathématique

DÉDICACE

A mon Père et ma Mère, à qui je dois tout et qui m'ont soutenu jusqu'au bout.
A mes Frères et mes Soeurs, à qui je souhaite beaucoup de réussite dans leurs vies.
A tous mes neveux et nièces sans oublier mes beaux frères.
A toute ma grande famille.
A tous mes amis qui ont une place spéciale dans ma vie et à qui je souhaite beaucoup de bonheur et de réussite.
A tous ceux qui ont contribué de loin ou de prés à ce travail.

.

Résumé:

Ce travail se situe dans le cadre des polynômes irréductibles sur un corps fini $\mathbb{F}_q$.

Dans cette mémoire on s'intéresse aux polynômes irréductible et certaines de ses propriétés comme nous avons discuté de factorisation de x^n-1 sur un corps fini$\mathbb{F}_q$.

Mots clés : corps fini, polynômes irréductible sur un corps fini.

Abstract:

This Work is included in the frame irréductible polynomial over finite field $\mathbb{F}_q$.

In this memory we are intersted irréductible polynomial and some of its propretés and factorization of x^n-1 over finite field $\mathbb{F}_q$.

Key words : finite field , irréductible polynomial over finite field $\mathbb{F}_q$.

Notations :

Les notations suivantes seront utilisées le long de ce mémoire:

- (a, b) : pgcd(a, b)
- $\deg p$: degré de p
- (p) : idéal engendré par p
- $\overline{p}$: fonction polynômaile induite par p
- $car\ F$: caractéristique de F
- $[K : F]$: dimention de K sur F minimal
- F^* : $F \setminus \{0\}$
- $a \setminus b$: a divise b
- $a \equiv b \,(\mathrm{mod}\, n)$: $(a - b)$ divisible par n
- $\mathbb{F}_q$: corps fini d'ordre q
- $\phi\,(n)$: indicateur d'euler
- Φ_n : le n^{ieme} polynôme cyclotomique
- m_α : le polynôme minimal de α
- μ : fonction de Mobius

Table des matières

Introduction

Les polynômes sur un corps fini qui ont beaucoup d'applications dans la théorie des nombres· La question centrale pour les polynômes dans $\mathbb{F}[x]$, $\mathbb{F}$ corps, est de décider quand un polynôme donné est irréductible ou non sur $\mathbb{F}$· Pour notre intension, les polynômes irréductibles sur $\mathbb{F}_p$,p premier sont d'une particularité interéssante· Pour déterminer tous les polynômes unitaires irréductibles sur $\mathbb{F}_p$, de degré fixé n, une possibilité est de rechercher tous les polynômes unitaires réductiubles dans $\mathbb{F}_p[x]$ de degré n et de les éliminer de l'ensemble des polynômes dans $\mathbb{F}_p[x]$ de degré n·

Dans ce mémoire, on s'intéresse à l'étude sur les polynômes irréductibles·

Le premier chapitre est un chapitre d'introduction de anneau de polynôme où présenté quelque définition et propriétés fondamentales pour ce tratravail tel que: anneau et corps, définition et quelques propriétes est etude l'irréductibilité d'un polynome·

Le deuxiéme chapitre est consacré à l'étude les polynômes irréductibles nous étudions les extension d'un corps fini, construction d'un corps fini, propriétes des polynômes irréductibles, racines $n^{iéme}$ de l'unité est teste d'irréductibilité d'un polynôme sur un corps fini·

En fin, dans le troisieme chapitre on va étude les décomposition des polynômes et on achevera nôtre travail par l'étude les factorisation du polynome $x^n - 1$ sur $\mathbb{F}_q$ est factorisation de $x^{4p^n} - 1$ sur $\mathbb{F}_q$·

Chapitre 1

Anneau de polynôme

Dans ce chapitre, on rappelle les notions de base dont aura besoin par la suite, anneau et corps, définitions et quelques propriétés est etude l'irréductibilité d'un polynôme·

1.1 Rappels de théorie des nombres

Définition 1.1.1

La fonction d'Euler $\phi(n)$ est définie comme le nombre d'entier positifs non nuls inférieur ou égaux à n, premiers avec n, i·e·,

$$\phi(n) = \sum_{\substack{1 \leq i \leq n \\ (i,n)=1}} 1 = |\{i \ / \ 1 \leq i \leq n, \ \ (i,n) = 1\}| \cdot$$

Notez que $\phi(1) = 1$·

Proposition 1.1.1

(i) La fonction ϕ est une fonction multiplicative, c'est–à–dire si $(a, n) = 1$,
$alors\ \phi(na) = \phi(n)\,\phi(a)$ ·
(ii) Si p est un nombre premier, alors $\phi(p) = p - 1$·
(iii) Si p est un nombre premier et i est un entier positif non nul,
alors $\phi(p^i) = p^{i-1}(p-1)$ ·

(iv)

$$\phi(n) = n \prod_{\substack{p/n \\ p \text{ premier}}} \left(1 - \frac{1}{p}\right) \cdot$$

(v)

$$\sum_{d/n} \phi(d) = n \cdot$$

Théorème 1.1.1 (**Euler – Ferrmat**)

Si $(n, a) = 1$, alors $\mathrm{a}^{\phi(n)} \equiv 1 \mod n \cdot$

Définition 1.1.2

Soit $(n, a) = 1 \cdot$ Le plus petit entier positif non nul r tel que

$$a^r \equiv 1 \mod n$$

est appelé l'order de a modulo n est noté $\mathrm{ord}_n(a) \cdot$

Remarque 1.1.1

1) Notez que $\mathrm{ord}_n(a) = 1$ pour tout a dans $\mathbb{N}^* \cdot$

2) Notez encore que $\mathrm{a}^r \equiv 1 \mod n$ s'ecrit aussi $\mathrm{n} \mid \mathrm{a}^r - 1 \cdot$

3) Si $\mathrm{n} \geq 1$, l'ordre $\mathrm{ord}_n(a)$ de a modulo n est l'order de a dans le group multiplicatif $(\mathbb{Z}/n\mathbb{Z})^* \cdot$

Définition 1.1.3

Soit $(n, a) = 1 \cdot$ Si $ord_n(a) = \phi(n)$, nous appelons a racine primitive modulo $n \cdot$

Théorème 1.1.2

Soit p un nombre premier, $p > 2 \cdot$ Si a est une racine primitive modulo p^2,
alors a est une racine primitive modulo p^i pour tout $i \geq 1 \cdot$

1.2 Anneau et corps

Définition 1.2.1

Un anneau $(A, +, \cdot)$ est la donnée d'un ensemble non vide A muni de deux lois de composition internes, notées "$+$" et "$\cdot$" (appelées respectivement addition et multiplication), telles que :

1) $(A, +)$ est un groupe abélien

2) La loi " $\cdot$ " est associative i.e. $\forall x, y, z \in A,\ x \cdot (y \cdot z) = (x \cdot y) \cdot z$

3) La loi "$\cdot$" est distributive par rapport à la loi "$+$" $\forall x, y, z \in A, x \cdot (y+z) = x \cdot y + x \cdot z$ et $(x + y) \cdot z = x \cdot z + y \cdot z$

Remarque 1.2.1

1) Si la loi " $\cdot$ " est commutative i.e $\forall x, y \in A,\ x \cdot y = y \cdot x$, on dit que l'anneau A est commutatif.

2) Si la loi " $\cdot$ " posséde un élément neutre 1, on dit que A est un anneau unitaire et 1 s'appelle l'unite de A.

Exemple 1.2.1

1) $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ et $(\mathbb{C}, +, \cdot)$ sont des anneaux commutatifs unitaires.

2) L'ensemble des entiers relatifs $\mathbb{Z}$ muni de l'addition et de la multiplication useulles est un anneau commutatif·

Définition 1.2.2

Dans un anneau A, un idéal I est dit principal s'il existe un élément $a \in A$ qui engendre I ·

En d'autres termes : $I = (a) = \{ar : r \in A\}$ ·

L'idéal I est dit maximal s'il n'est pas contenu dans un autre idéal J différent de l'anneau A · Un idéal $I \neq A$ est dit premier si pour tout $a,\ b \in A$ *on* $a : ab \in I \Rightarrow a \in I$ *ou* $b \in I$·

L'ensemble des classes résiduélles d'un anneau A modulo un idéal I forme un anneau noté A/I est dite anneau quation dont les deux opération sont définies par :

1) $(a + I) + (b + I) = (a + b) + I$

2) $(a + I)(b + I) = ab + I$

Définition 1.2.3

Un corps est un anneau unitaire dans lequel tout élément non nul est invérsible·

La caractéristique d'un corps $\mathbb{F}$ est le plus petit entier positif n tel que : $nr = 0$ por tout $r \in \mathbb{F}$ · S'il n'existe pas d'entier positif n le corps $\mathbb{F}$ est dit de caractéristique 0 ·

Le corps $\mathbb{Z}/p\mathbb{Z}$, p premier, est de caractéristique p, les corps $\mathbb{Q}$ et $\mathbb{R}$ sont de caractéristique 0 ·

Proposition 1.2.1

Dans un corps $\mathbb{F}$ de caractéristique p, p premier, on a :

$$(a+b)^p = a^p + b^p\cdot$$

Preuve.

Nous utiliserons le fait que dans la formule du binome les coéfficients C sont divisibles par p pour $0 < i < p$ et que le facteur p dans $C_p^i = \frac{p(p-1)\cdots(p-i+1)}{1\times 2\times\cdots\times i}$ n'est pas supprimé, donc tous ces termes sont nuls, et il ne reste dans la formule $(a+b)^p$ que le premier et le dernier terme, d'où le résultat · ■

Remarque 1.2.2

On a le même résultat pour $p = p^n$, en faisant le raisonnement par récurrence sur n · C'est à dire que :

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}\cdot$$

1.3 Définitions et quelques propriétés

Définition 1.3.1

Soit A un anneau commutatif unitaire ·Tout suit d'élément de A n'ayant q'un nombre fini de termes non nul est dit polynôme à coéfficient dans A· L'ensemble des polynomes sur A est noté $A[x]$ ·

Dans $A[x]$ on définit l'addition et la multiplication comme suit :

$(a_0,\ a_1,\ \cdots\ ) + (b_0,\ b_1,\ \cdots) = (a_0 + b_0,\ a_1 + b_1,\ \cdots)$

$(a_0,\ a_1,\ \cdots\ )(b_0,\ b_1,\ \cdots) = (c_0,\ c_1,\ \cdots)$ *où* $c_k \sum_{i=0}^{k} a_i b_{k-i}$.

Proposition 1.3.1

Soient p et q deux polynômes non nuls a coéfficient de $\mathbb{k}$ ·

$\deg(p \times q) = \deg p + \deg q$

$\deg\ (p+q) \leq Max\ \ (\deg\ \ p, \deg\ \ q)$ ·

Définition 1.3.2

Un élément a d'un anneau A admet un inverse s'il existe un élément b de A tel que $ab = 1$ · Un élément a est inversible s'il admet un inverse (*unique*) · On note alors a^{-1} son inverse et $U(A)$ l'ensemble des élément inversibles de A ·

Exemple 1.3.1

$U(\mathbb{Z}) = \{1, -1\}$

Division euclidienne des polynômes

Soit U et V deux polynômes de $A[x]$ ($A[x]$ l'anneau des polynômes à coefficients dans A) ·

Supposons que le coefficient dominant de V soit inversible dans A·

Il existe alors deux polynôme Q et R, uniquement déterminés, tel que $U = VQ + R$ avec $\deg(R) < \deg(V)$ · f

Définition 1.3.3

Soit $p(x),\ q(x) \in A[x]$, on dit que $p(x)$ divise $q(x)$ et on note $p(x)\ /\ q(x)$ *si* $q(x) = p(x)\, r(x)$ avec $r(x) \in A[x]$ *et* $\deg p(x) < \deg q(x)$, $p(x)$ est alors appelé un diviseur propre de $q(x)$ ·

Définition 1.3.4

Un polynôme q de deg ≥ 1 qui n'a pas de diviseurs propres et appelé un polynôme irréductible ·

Exemple 1.3.2

1· $x^2+1=(x-i)(x+i)$ est réductible dans $\mathbb{C}[x]$ mais est irréductible dans $\mathbb{R}[x]$ ·

2· $x^2-2=\left(x-\sqrt{2}\right)\left(x+\sqrt{2}\right)$ est réductible dans $\mathbb{R}[x]$ mais est irréductible dans $\mathbb{Q}[x]$ ·

3· Les polynômes constants ne sont donc ni réductible, ni irréductible·

1.4 Etude de l'irréductibilité d'un polynôme

1.4.1 L'irréductibilité d'un polynôme sur un corps de caractéristique zéro

Corollaire 1.4.1

Soit $f(x)$ un polynôme unitaire, de deg ≥ 1 sur un corps $\mathbb{F}$ alors, les propriétes suivantes sont équivalentes:

i) $f(x)$ est irréductuble sur $\mathbb{F}$

ii) $\forall a \in \mathbb{F}$, $f(x+a)$ est irréductible sur $\mathbb{F}$

iii) $f(x+1)$ est irréductible sur $\mathbb{F}$·

Corollaire 1.4.2

Si un polynôme est irréductible sur $\mathbb{Z}$, il l'est sur $\mathbb{Q}$·

1.4.2 Critère d'irréductibilité D'EISENTEIN d'un polunôme

Proposition 1.4.1

Soit $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$, un polynôme unitaire sur $\mathbb{Z}$ dont tous les coéfficients sont divisibles par un certain nombre premier p, et a_0 n'est pas divisible par p^2, alors $f(x)$ est irréductible sur $\mathbb{Q}$·

Exemple 1.4.1

Le polynôme $\mathrm{x}^4+9x^3-27x^2+15x+3$ est irréductible sur $\mathbb{Q}\cdot$ (prendre $p=3$)

Exemple 1.4.2

Pour tout nombre premier p, le polynome $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ est irréductible sur $\mathbb{Q}\cdot$ En effet, il suffit de voir l'irréductibilité du polynome $f(x+1)\cdot$

$$\begin{aligned} f(x+1) &= \frac{(x+1)^p - 1}{(x+1) - 1} \\ &= \frac{C_p^p x^p + C_p^{p-1} x^{p-1} + \cdots + C_p^2 x^2 + C_p^2 x + C_p^0 - 1}{x} \\ &= x^{p-1} + C_p^{p-1} x^{p-2} + \cdots + C_p^2 x + C_p^1\cdot \end{aligned}$$

Or p divise tous les coéfficients C_p^i pour $1 \leq i \leq p-1$, mais p^2 ne divise pas le coéfficient $C_p^1 = p\cdot$Ansi $f(x+1)$ est irréductible par le critère D'EISENTTEIN et par suit $f(x)$ est irréductible sur $\mathbb{Q}\cdot$

Théorème 1.4.1

Les polynômes irréductibles dans $\mathbb{C}[x]$ sont précisement les seuls polynômes de deg $= 1\cdot$ Les polynômes irréductibles dans $\mathbb{R}[x]$ sont les polynômes de deg $= 1$ et les polynômes $a_0 + a_1 x + a_2 x^2$ *avec* $a_1^2 - 4a_0 a_1 < 0\cdot$

Théorème de la factorisation unique

Théorème 1.4.2

Soit $\mathbb{F}$ un corps $\cdot$ Alors tout polynôme $p \in \mathbb{F}[x]$ a une représentation unique (à l'ordre prés) de la forme:

$$p = r p_1 p_2 \cdots p_k$$

où $r \in \mathbb{F}$ *et* $p_1,\ p_2,\ \cdots, p_k$ sont des polynômes unitaires irréductibles sur $\mathbb{F}\cdot$

Ce théorème affirme l'existence de l'édriture unique d'un polynôme comme produit de polynômes unitaires irréductibles mais n'indique pas comment construire décomposition en facteurs premiers $\cdot$

Remarque 1.4.1

Soit $\mathbb{F}$ un corps et $p = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{F}[x]$ *alors*, $\overline{p} : \mathbb{F} \longrightarrow \mathbb{F}$; $\alpha \mapsto a_0 + a_1\alpha + \cdots + a_n\alpha^n$ est appelée la fonction polynômaile induite par p ·

Si $\mathbb{F}$ est un corps de caractéristique 0, alors $\mathbb{F}[x] \cong P(\mathbb{F})$ ·Mais ce résultat n'est pas vrai si $\mathbb{F}$ est un anneau fini, ainsi dans $\mathbb{Z}/p\mathbb{Z}$,le polynômes $p = x(x+1)\cdots(x+(n-1))$ est de degré n, mais $\overline{p}$ est la fonction nulle, en effet :

$$\overline{p}(0) = \overline{p}(1) = \cdots \cdot \overline{p}(n-1) = 0\cdot$$

Définition 1.4.1

Un élément $r \in \mathbb{F}$ est appelé racine du polynôme $p \in \mathbb{F}_q[x]$ *si* $\overline{p}(r) = 0\cdot$

Il y a une relation entre la non existence de racines et l'irréductibilité d'un polynôme $p \in \mathbb{F}[x]$ · Si p est un polynôme irréductible dans $\mathbb{F}[x]$ *de* deg ≥ 2 alors il n'admet pas de racines dans $\mathbb{F}$ · La réciproque tient pour des polynômes de deg = 2 ou 3, mais pas necéssairement pour des polynômes de degré élevé·

Proposition 1.4.2

Un polynôme $p \in \mathbb{F}[x]$ de degré 2 ou 3 est irréductible dans $\mathbb{F}[x]$ si et seulement si p n'admet pas de racines dans $\mathbb{F}$·

Preuve.

La condition necéssaire est déja notée· Inversement, si p n'admet de racines dans $\mathbb{F}$ et est réductible dans $\mathbb{F}[x]$, on peut écrire $p = gh$ avec $g, h \in \mathbb{F}[x]$ *et* $1 \leq \deg g \leq \deg h$·Mais deg g + deg h = deg $p \leq 3$, par conséquent deg g=1, et $g(x) = a_1x + a_0$ avec $a_0, a_1 \in \mathbb{F}$, *et* $a_1 \neq 0$ ·Alors $-a_0a_1^{-1}$est un racine de g, et par suite elle est racine de p dans $\mathbb{F}$,

on a une contradiction avec le fait que p n'admet pas de racines·

Dans le cas géneral, pour $n \geq 4$ ce résultat n'est pas vrai, en effet, dans $\mathbb{R}[x]$,le polynôme $p = x^4 + x^2 + 1$ n'admet de racines sur $\mathbb{R}$ mais il est réductible : $x^4 + x^2 + 1 = (x^2 - x + 1)(x^2 + x + 1)\cdot$ ■

Exemple 1.4.3

$x^2 + x + 1$ est l'unique polynôme irréductible de degré 2 sur $\mathbb{F}_2$·

Chapitre 2

polynôme sur un corps fini

Dans ce chapitre, on rappelle les notions de base dont aura besoin par la suite, Extensions d'un corps fini, construction d'un corps fini, propriétes des polynômes irréductibles, racines n^{iémes} de l'unité, nombre de polynômes unitaire irréductibles de degré fixésur un corps fini et test d'irréductibilité d'un polynôme sur un corps fini·

2.1 Extensions d'un corps fini

Extension de corps

Définition 2.1.1

Soient $\mathbb{F}$ et E deux corps commutatifs· Si $\mathbb{F} \subseteq E$ on dit que E est une extension de $\mathbb{F}$·

Exemple 2.1.1

a) Tout corps de caractéristique 0 est extension du corps $\mathbb{Q}$·

b) Tout corps de caractéristique p$\neq$ 0 est extension du corps $\mathbb{Z}/p\mathbb{Z}$, p premie·

c) $\mathbb{R}$ est un extension de $\mathbb{Q}$·

Proposition 2.1.1

Soient E une extension de $\mathbb{F}$ et $\alpha \in E$, si on définit :

$$\mathbb{F}[\alpha] = \{f(\alpha) \mid f(x) \in \mathbb{F}[x]\}$$

et

$$\mathbb{F}(\alpha) = \{f(\alpha) \ / \ g(\alpha) \mid f(x), \ g(x) \in \mathbb{F}[x] \text{ avec } g(\alpha) \neq 0\}$$

alors :

1) $\mathbb{F}[\alpha]$ est le plus petit sous anneau de E qui contient à la fois $\mathbb{F}$ et α.

2) $\mathbb{F}(\alpha)$ est le plus petit sous corps qui contient à la fois $\mathbb{F}$ et α.

Extension algébrique

Définition 2.1.2

Soit E un une extension du corps $\mathbb{F}$. Un élément α de Eest dit algébrique sur $\mathbb{F}$ s'il ya un polynôme non nul g avec les coéfficient dans $\mathbb{F}$ tel que $g(\alpha) = 0$.

Exemple 2.1.2

$\mathbb{C} = \mathbb{R}(i)$ est une extension algébrique sur $\mathbb{R}$.

Extension finie

Définition 2.1.3

Une extension E de $\mathbb{F}$ est dite finie si la dimension de $\mathbb{F}$ -espace vectoriel E est finie.

Le degré d'extension de $\mathbb{F}$ est noté

$$[E : \mathbb{F}] = \dim_{\mathbb{F}} E.$$

Exemple 2.1.3

1) $[\mathbb{C} : \mathbb{R}] = 2$.

2) $[\mathbb{F}(\alpha) : \mathbb{F}] = \deg \mathbb{F}(\alpha) = \deg(p(x))$ ou $p(x)$ le polynôme minimal de α .

Extension simple

Définition 2.1.4

Soit E une extension d'un corps $\mathbb{F}$ et soit α un élément de E n'appartenant pas à $\mathbb{F}\cdot$ On apelle extension simple de E le plus petit sous corps de E contenant $\mathbb{F}$ et $\alpha\cdot$ C'est à dire $\mathbb{F}(\alpha)\cdot$

Exemple 2.1.4

$\mathbb{Q}(\sqrt{2}) = \left\{a + b\sqrt{2} \mid a,\ b \in \mathbb{Q}\right\}$ est un extension simple de $\mathbb{Q}\cdot$

Définition 2.1.5

Soit E une extension de $\mathbb{F}$, un élément α est dit algébrique sur $\mathbb{F}$ si il existe un polynôme non nul $f \in \mathbb{F}[x]$ tel que $f(\alpha) = 0\cdot$

α est dit transcendent dans le cas contraire, c'est à dire s'il n'existe aucun polynôme $f\ \in \mathbb{F}[x]$ tel que $f(\alpha) = 0$ autre que le polynôme nul $\cdot$

Théorème 2.1.1

Soit E une extension de $\mathbb{F}$ et soit $\alpha \in E$ un élément algébrique sur $\mathbb{F}$, alors il existe un polynôme normalisé $p(X) \in \mathbb{F}[X]$ tel que :

(1) $p(\alpha) = 0$

(2) $p(X)$ est irréductible

(3) si il existe $f\ (x) \in \mathbb{F}[x]$ tel que $f(\alpha) = 0$ alors $p(X)$ divise $f(X)\cdot$

Définition 2.1.6

Le degré de α sur $\mathbb{F}$ est par définition le degré du polynôme minimal $p(X)$ et on ecrit

$$\deg_{\mathbb{F}}(\alpha) = \deg(p(X))\cdot$$

Théorème 2.1.2

soient E une extension de $\mathbb{F}$ et $\alpha \in E$ un élément algébrique sur $\mathbb{F}$ avec $\deg_{\mathbb{F}}(\alpha) = \mathrm{n}$ et soit $p(X)$ est le polynôme minimal de α sur $\mathbb{F}$, alors :

(1) $\mathbb{F}(\alpha) \simeq \mathbb{F}[X]\ /\ \langle p(X)\rangle\cdot$

(2) $\{1,\ \alpha,\ \alpha^2,\ \cdots,\ \alpha^{n-1}\}$ est une base de l'espace vectoriel $\mathbb{F}(\alpha)$ sur $\mathbb{F}\cdot$

(3) $\dim_{\mathbb{F}}(\mathbb{F}(\alpha)) = \deg_{\mathbb{F}}(\alpha) = \deg(p(X))\cdot$

Extension par adjonction

Définition 2.1.7

Soit E une extension de $\mathbb{F}$, soit S une partie de E, il existe au moins un sous corps de E contient à la fois $\mathbb{F}$ et la partie S·

L'intersection de tous les sous corps de E contenant à la fois $\mathbb{F}$ et S est un sous corps noté $\mathbb{F}(S)$ ·

Remarque 2.1.1

1- Si $S \subset \mathbb{F}$ alors $\mathbb{F}(S) = \mathbb{F}$·

2- Si $S = \{\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n\}$ alors $\mathbb{F}(S)$ note $\mathbb{F}(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n)$ ·

Exemple 2.1.5

$\mathbb{Q}\left(\sqrt{2}\right)$ extension simple de $\mathbb{Q}$ par adjonction de $\sqrt{2}$·

2.2 Construction d'un corps fini

Pour déterminer les éléments d'un corps fini $\mathbb{F}_q$ on peut suivre une des méthodes suivantes :

1- Soit en utilisant l'anneau quations $\mathbb{F}_q[x]\ /\ (f(x))$ où $f(x)$ est un polynôme irréductible sur $\mathbb{F}_q$·

2- Soit en utilisant le fait que $\mathbb{F}_q^*$ est un groupe cyclique où chaque élément est une puissance d'un élément générateur α appartient à $\mathbb{F}_q^*$·

Théorème 2.2.1

Soit $\mathbb{F}_q$ un corps et $f(x) \in \mathbb{F}_q[x]$, alors $\mathbb{F}_q[x]\ /\ (f(x))$, est un corps si et seulement si $f(x)$ est irréductible sur $\mathbb{F}_q[x]$ ·

La preuve de ce théorème montre non seulement que $\mathbb{F}_q[x]\ /\ (f(x))$ est un corps, mais nous donne aussi la facon d'obtenir ses éléments·

Preuve.

On note par I l'idéal principal$(f(x))$, supposons que $f(x)$ est irréductible sur $\mathbb{F}_q$,c·a·d $f(x) = a(x)\,b(x)$ tel que $a(x), b(x)$, ont des degrés inférieur au degré de f(x) ·

On montre dans ce cas que $\mathbb{F}_q[x] \ / \ (f(x))$ n'est pas un corps· Le degré de tout polynôme non nul de I doit être supérieur où égal au degré de $f(x)$, donc $a(x) \notin I,\ b(x) \notin I,$ par conséquent $I + a(x),\ I + b(x)$ sont des élément non nul de $\mathbb{F}_q[x] \ / \ I$·

Mais on a :

$$(I + a(x))(I + b(x)) = I + f(x) = I$$

ce qui montre que $\mathbb{F}_q[x] \ / \ I$ ne peut être un corps donc $f(x)$doit être irréductible sur $\mathbb{F}_q$·

Inversement, supposons que maintenant que $f(x)$ est irréductible sur $\mathbb{F}_q$·

$\mathbb{F}_q[x] \ / \ I$ est un anneau commutatif d'élément unité $I + e$ (ou e est l'unité de $\mathbb{F}_q$),

il suffit donc de démontre que tout élément non nul de $\mathbb{F}_q[x] \ / \ I$ admet un inverse dans $\mathbb{F}_q[x] \ / \ I$·

Soit $I+p(x) \in \mathbb{F}_q[x]$ différent de zéro(c · à · d différent de I), donc $p(x) \notin I,$ ce qui montre que $p(x)$ n'est pas multiple de $f(x)$, comme $f(x)$ est irréductible, alors $f(x)$ et $p(x)$

sont premiers entre eux et donc d'aprés le théorème de bézout

$\exists, u(x),\ v(x) \in \mathbb{F}_q[x] \ / \ (f(x))$ tel que

$$f(x)u(x) + p(x)v(x) = e$$

alors on a :

$$e - p(x)v(x) = f(x)u(x) \in I$$

et par conséquent

$$I + e = I + p(x)v(x) = (I + p(x))(I + v(x)) = e$$

c·à·d $I + v(x)$ est l'élément inverse de $I + p(x\cdot)$ ■

Exemple 2.2.1

1) Pour construire $\mathbb{F}_4$, j'ai besion d'une polynôme de degré 2 irréductible sur$\mathbb{F}_2$· je vérifie immédaitement que $x^2 + x + 1$ convient parce qu'il n'a pas de racine, donc $\mathbb{F}_4 = \mathbb{F}_2 \ / \ (x^2 + x + 1) = \{0,\ 1,\ j,\ 1 + j\}$, où $j = x$ ·

Il y a que deux élément à taster, à savoir j et $1 + j$ ·

Les deux conviemment :$j^3-1=(j+1)(1+j^2+j)=0$ donc $j^3=1,$ et j est d'ordre 3 donc engendre $\mathbb{F}_4^*$ ·Comme $1+j=j^2$ est l'autre racine de $x^2+x+1,$ on a le même résultat ·En fait, sans même calculer,

comme $\phi(3)=2$ il était granti qu'ils engendre le groupe multiplicatif·

2) Soit $\mathbb{F}$ un corps de 5 éléments · Aucun des élément de $\mathbb{F}$ est une racine du polynôme $f(x)=x^2+2$ et donc $f(x)$ est irréductible en $\mathbb{F}[x]$ ·d'où

$$\Bbbk=\mathbb{F}[x]\ /\ \langle f(x)\rangle$$

est un corps d'ordre 25 ·Un élément de $\Bbbk$ est de forme

$$aX+b+\langle f(x)\rangle \qquad a,b\in\mathbb{F}$$

écrire $X+\langle f(x)\rangle\ =\alpha$·Les puissance de α sont alors déterminées comme suit : $\alpha^2=3,\ \alpha^3=3\alpha,\ \alpha^4=4,\ \alpha^5=4\alpha,\ \alpha^6=2,\ \alpha^7=2\alpha,\ \alpha^8=1$·Donc α n'est pas un élément primitif de $\Bbbk$·

Pose $\beta=\alpha+4$ donne

$$\begin{aligned}
\beta^2 &= \alpha^2+3\alpha+1=3\alpha+4\\
\beta^3 &= (3\alpha+4)(\alpha+4)=\alpha\\
\beta^4 &= 4\alpha+\alpha^2=4\alpha+3\\
\beta^5 &= (\alpha+4)(4\alpha+3)=4\alpha+4\\
\beta^6 &= (4\alpha+4)(\alpha+4)=3\\
\beta^7 &= 3\alpha+2\\
\beta^8 &= (3\alpha+2)(\alpha+4)=4\alpha+2\\
\beta^9 &= (4\alpha+2)(\alpha+4)=3\alpha\\
\beta^{10} &= 3\alpha^2+2\alpha=2\alpha+4\\
\beta^{11} &= (2\alpha+4)(\alpha+4)=2\alpha+2\\
\beta^{12} &= (2\alpha+2)(\alpha+4)=4
\end{aligned}$$

donc l'ordre de β dans le groupe multiplicatif de $\Bbbk$ est supérieur à 12 et donc β est un élément primitiuf de $\Bbbk$·

Calculs résiduels sur les polynômes

Soit $f(x) \in \mathbb{F}_q[x]$, $f(x)$ fixé($\mathbb{F}_q$ corps) et soit $g(x)$, $h(x) \in \mathbb{F}_q[x]$,
les deux polynôme $g(x)$ et $h(x)$ sont dits congrus modulo $f(x)$ en notion
g$(x) \equiv h(x)\,[f(x)]$ *si* $g(x) - h(x)$ est divisible par $f(x)$ ·
$\forall a(x) \in \mathbb{F}_q[x]$ on a : $a(x) \equiv r(x)\,[f(x)]$
Avec $a(x) \equiv q(x) f(x) + r(x)$ et $r(x) = 0$ ou $\deg r(x) \leq \deg f(x)$ ·
⋆ Si $a(x)$, $h(x) \in \mathbb{F}_q[x]$ / $(f(x)) = \mathbb{F}_q[x]$ / I, $I = (f(x))$
1- $a(x) + h(x) \in \mathbb{F}_q[x]$ / I
2- le produit a$(x)\,h(x)$ est calculé modulo $f(x)$ ·

Exemple 2.2.2

Dans $\mathbb{F}_2[x]$ / $(x^2 + x + 1)$ on a

$$(x+1)^2 = x^2 + 2x + 1 = x^2 + 1 \equiv x \left(\mathrm{mod}\, x^2 + x + 1\right) \cdot$$

Addition et multiplication dans $\mathbb{F}_2[x]$ / $(x^2 + x + 1)$ ·

+	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	0
$1+x$	$1+x$	x	1	1

×	0	1	x	$1+x$
0	0	0	0	0
1	0	x	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

Théorème 2.2.2

Soit $\mathbb{F}$ un corps et $p \in \mathbb{F}[x]$ de degré k alors :

$$\mathbb{F}[x] \,/\,(p) = \left\{\alpha_0 + \alpha_1 x + \cdots + \alpha_{k-1} x^{k-1} + (p) \;/\alpha_i \in F\right\}$$

est un espace véctoriel sur $\mathbb{F}$ de base $\left\{1,\ \alpha,\ \alpha^2, \cdots,\ \alpha^{k-1}\right\}$, où $\alpha = [x] = x + (p)$ ·On a $\overline{p}(\alpha) = 0$ et $\mathbb{F}[x] \,/\,(p)$ est un corps si et seulement si p est irréductible·

Exemple 2.2.3

Soit p$(x) = x^2 + x + 1$, irréductible sur $\mathbb{F}_2$, alors :

$$\mathbb{F}_2[x] \,/\,(p) = \{a_0 + a_1\alpha \;/\; a_0,\ a_1 \in F_2\}$$

d'où : $\mathbb{F}_2[x] \,/\,(p) = \{0,\ 1,\ \alpha,\ \alpha + 1\}$ est un corps de quatre éléments·

2.3 Propriétes des polynômes irréductibles

Dans cette partie on discutera des propriétes de base des polynômes irréductibles sur un corps fini $\mathbb{F}_q$.

Lemme 2.3.1

Soit f un polynôme irréductible sur $\mathbb{F}_q$, est α une racine de f dans un extension de $\mathbb{F}_q$. Alors si $g \in \mathbb{F}_q[x]$, on a $g(\alpha) = 0$ si et seulement si $f \mid g$.

Exemple 2.3.1

Soient $f(x) = x^2 + x + 1$, irréductible sur $\mathbb{F}_2$, et $g(x) = x^5 + x^4 + 1 \in \mathbb{F}_2[x]$.

Soit α une racine de f dans $\mathbb{F}_{2^2}$,c'est à dire $\alpha^2 + \alpha + 1 = 0$, d'où $\alpha^2 = \alpha + 1$ ainsi : $g(\alpha) = \alpha^5 + \alpha^4 + 1$ mais

$$\alpha^3 = \alpha^2 \cdot \alpha = (\alpha + 1)\alpha = \alpha^2 + \alpha = (\alpha + 1) + \alpha = 2\alpha + 1 = 1.$$

Et $\alpha^4 = \alpha^3 \cdot \alpha = \alpha$, d'où $\alpha^5 = \alpha^2 = \alpha + 1 = \alpha^4 + 1$, ce qui donne $\alpha^5 + \alpha^4 + 1 = 0$.

C'est à dire que α est racine du polynôme g est on a $f \mid g$ car $g(x) = f(x) \cdot (x^3 + x + 1)$.

Inversement si $f \mid g$ et $f(\alpha) = 0$ on a directement $g(\alpha) = 0$.

Théorème 2.3.1

Pour tout corps fini $\mathbb{F}_q$, et un entier positif k, il existe un polynôme irréductible f de degré k sur $\mathbb{F}_q$.

En effet, soit β un élément primitif de $\mathbb{F}_{q^k}$.Alors $\mathbb{F}_q(\beta) = \mathbb{F}_{q^k}$, et comme

$$[\mathbb{F}_q(\beta) : \mathbb{F}_q] = \left[\mathbb{F}_{q^k} : \mathbb{F}_q\right] = k$$

alors le polynôme minimal de β,irréductible sur $\mathbb{F}_q$, doit être de degré k .

2.4 Racines n$^{\text{iémes}}$ de l'unité

2.4.1 Polynômes cyclotomiques

Racines n$^{\text{iémes}}$ de l'unité

Sachant que dans $\mathbb{C}$, les racines $n^{iémes}$ de l'unité sont $z_k = \exp\left(\frac{2\pi ki}{n}\right),\ k = 0,\ 1,\ \cdots n-1,$ et que tout les z_k avec $\text{pgcd}(k,n)\ = 1$ sont des générateurs, en particulier z_1·Elles sont appelées les racines $n^{iémes}$ primitive de l'unité ·Pour un corps quelconque nous définitions :

Définition 2.4.1

Soit $\mathbb{F}$ un corps · Une racine de $x^n - 1$ dans $\mathbb{F}[x]$ est appelée une racine n^{iemes} de l'unité · L'order d'une racine n^{iemes} de l'unité est le plus petit entier positif k tel que :$\alpha^k = 1$ · Une racines n^{ieme} de l'unité d'order n est dite primitive, le corps de décomposition S_n de $x^n - 1$ est appelé le corps cyclotomique associé·

Dans la suit on aura besoin de la fonction ϕ de $\mathbb{N}$ dans $\mathbb{N},$ dite D'EULER, qui est définie par :

$$\phi(n) = |\{m\ /1 \leq m \leq n\ et\ \ (m,n) = 1\ \}|$$

Pour m, n des entiers positifs · Si $n = p_1^{t_1} \cdots p_k^{t_k}$ où les p_i sont des entiers premiers distincts, alors $\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$ ·

Polynômes cyclotomiques

Définition 2.4.2

Soit n une entier positif et $\mathbb{F}$ un corps dont la caractéristique ne divise pas n, et α une racine primitive n^{ieme} de l'unité· Le polynôme :

$$\Phi_n = (x - \alpha_1) \cdots \left(x - \alpha_{\Psi(n)}\right)\ \ \in\ \ F(\alpha)[x]$$

où $\alpha_1, \cdots, \alpha_{\Psi_{(n)}}$ sont les racines primitives $n^{iémes}$ de l'unité dans $\mathbb{F}(\alpha)$, est appelé le $n^{iémes}$ polynôme cyclotomique sur $\mathbb{F}$·

Remarque 2.4.1

Le polynôme Φ_n ne dépend pas de $\alpha\cdot$

Exemple 2.4.1

Soit $n = 8$ et $\mathbb{F} = \mathbb{F}_3\cdot$Comme $n = 3^2 - 1,\ n$ n'est pas divisible par 3, et considérons le polynôme x^2+x+2 qui est irréductible sur $\mathbb{F}_3,$ pour sela il suffit de voire que tous les éléments de $\mathbb{F}_3$ ne sont pas des racines de ce polynôme $\cdot$ On se donne la peine de trouver une racin primitive huitiéme de l'unité dans $\mathbb{F}_9 = \mathbb{F}_3[x]\ /(x^2 + x + 1)$, soit α une racine du polynôme $x^2 + x + 1$ c'est à dire $\alpha^2 + \alpha + 1 = 0,$ d'où sur $\mathbb{F}_3,\ \alpha^2 = 2\alpha + 1\ \cdot$Calculons α^k pour $k = 3,\ 4, \cdots,\ 8\cdot$

$\alpha^3 = \alpha^2 \cdot \alpha = (2\alpha + 1) \cdot \alpha = 2\alpha^2 + \alpha = 2(2\alpha + 1) + \alpha = 2\alpha + 2\cdot$

$\alpha^4 = \alpha^3 \cdot \alpha = (2\alpha + 2) \cdot \alpha = 2\alpha^2 + 2\alpha = 2(2\alpha + 1) + 2\alpha = 2\cdot$

$\alpha^5 = \alpha^4 \cdot \alpha = 2\alpha\cdot$

$\alpha^6 = \alpha^5 \cdot \alpha = 2\alpha^2 = 2(2\alpha + 1) = \alpha + 2\cdot$

$\alpha^7 = \alpha^6 \cdot \alpha = (\alpha + 2) \cdot \alpha = \alpha^2 + 2\alpha = (2\alpha + 1) + 2\alpha = \alpha + 1\cdot$

$\alpha^8 = \alpha^7 \cdot \alpha = (\alpha + 1) \cdot \alpha = \alpha^2 + \alpha = (2\alpha + 1) + \alpha = 1\cdot$

Ainsi $\mathbb{F}_9 = \{0,\ 1,\ 2,\ \alpha,\ 2\alpha,\ \alpha + 1,\ 2\alpha + 1,\ 2 + \alpha,\ 2\alpha + 2\}$

$\mathbb{F}_9 = \{0,\ 1,\ \alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4,\ \alpha^5,\ \alpha^6,\ \alpha^7\}\cdot$

Donc α est une racine primitive huitiéme de l'unité$\cdot$

Et comme $\phi(8) = |\{m\ \in \mathbb{N}\ /1 \leq m \leq 8\ et\ \ (m, 8) = 1\}| = |\{1,\ 3,\ 5,\ 7\}| = 4\cdot$

Les autres racines primitives huitiéme de l'unité sont $\alpha^3,\ \alpha^5,\ et\ \alpha^7\cdot$ Ainsi on trouve: $\Phi_8 = (x - \alpha)(x - \alpha^3)(x - \alpha^5)(x - \alpha^7)\cdot$

En developpant ceci et en tenant compte que la multiplication dans $\mathbb{F}_9$, en sa représentation en puissance de α , se fait en observant que : $\alpha^i \cdot \alpha^j = \alpha^{i+j(\mathrm{mod}\,8)}$

on trouve que $\Phi_8 = x^4 + 1\cdot$par la suite Φ_8 n'est pas dans $\mathbb{F}_9$ mais dans $\mathbb{F}_3[x]\cdot$

Remarque 2.4.2

Le polynôme cyclotomique $\Phi_n(x)$ est de dégrè $\phi_n\cdot$

Pour notre exemple $\Phi_8(x)$ est de degré $\varphi_n = 4\cdot$

On va voir dans les pages qui suivent que ce fait surprenant est toujour vrai :

Φ_n a ses coéfficient dans $\mathbb{F}_p$ · Soit α une racine primitive $n^{iémes}$ de l'unité alors :

$$\Phi_n = \prod_i \left(x - \alpha^i\right)$$

où le produit est formé pour tout i avec pgcd $(i, n) = 1$· Le polynômeΦ_n est degré $\phi(n)$·

Soit $n = kd$ ainsi α^k est d'order d , car$\left(\alpha^k\right)^d = \alpha^{kd} = \alpha^n = 1,$ et est une racine primitive d *iémes* de l'unité· Le d *ieme* polynôme cyclotomique est de la forme :

$$\Phi_d = \prod_{pgcd(i,d)=1} \left(x - \alpha^{ik}\right) \cdot$$

Tout racine $n^{iéme}$ de l'unité est une racine primitive d^{ieme} de l'unité pour exactement un seul d· Par conséquent, on peut regrouper les racines $n^{iémes}$ de l'unité ensemble et on obtient le résultat suivant :

Théorème 2.4.1

$$x^n - 1 = \prod_{d/n} \Phi_d \,(\text{décomposition cyclotomique})$$

Un résultat important se déduit pour le polynôme cyclotomiqueΦ_{p^m} , pour p premier et m un entier positif, a savoir :

$$\Phi_{p^m} = 1 + x^{p^{m-1}} + \cdots + x^{(p-1)p^{m-1}}.$$

En effet, du théorème précédent et sachant que les diviseurs de p^m, p premier, sont 1, p, $p^2, \cdots, p^m$ *alors* :

$$\begin{aligned} x^{p^m} - 1 &= \prod_{d/p^m} \Phi_d = \Phi_1 \cdot \Phi_p \cdots \Phi_{p^m} \\ \Phi_{p^m} &= \frac{x^{p^m} - 1}{\Phi_1 \cdot \Phi_p \cdots \Phi_{p^{m-1}}} \\ &= \frac{x^{p^m} - 1}{x^{p^{m-1}} - 1} \\ &= 1 + x^{p^{m-1}} + \cdots + x^{(p-1)p^{m-1}}. \end{aligned}$$

Exemple 2.4.2

Soit dans $\mathbb{F}_2$, le polynome $x^{15}-1$, donnons sa décomposition cyclotomique ·

Comme les diviseur de 15 sont: 1, 3, 5, 15, ona

$$x^{15}-1=\prod_{d/15}\Phi_d=\Phi_1\Phi_3\Phi_5\Phi_{15}$$

On $\Phi_1=x+1,\ \Phi_3=x^2+x+1,\ \Phi_5=x^4+x^3+x^2+x+1\ et\ \Phi_{15}=x^8+x^7+x^5+x^4+x^3+x+1$·

En effet, de la formule $\Phi_n=\prod_i(x-\alpha^i)$, où pgcd $(i,n)=1$, avec $1\leq i\leq n$,et comme

$\phi(15)=|\{m\in\mathbb{N}\ /\ 1\leq m\leq 15\ et\ (m,15)=1\}|\ =|\{1,\ 2,\ 4,\ 7,\ 8,\ 11,\ 13,\ 14\}|=8$·

Et la caracteristique 2 de $\mathbb{F}_2$ ne divide pas 1, 3, 5 et 15 on a d'apres le corollaire divide diviseur

deg $\Phi_1=\phi(1)=1\ et\ \Phi_1=x+1$·

deg $\Phi_3=\phi(3)=2,\ et$

$$\begin{aligned}\Phi_3 &= \frac{x^{3^1}-1}{x^{3^{1-1}}-1}\\ &= \frac{x^3-1}{x-1}\\ &= x^2+x+1\cdot\end{aligned}$$

deg $\Phi_5=\phi(5)=4$, et

$$\begin{aligned}\Phi_5 &= \frac{x^{5^1}-1}{x^{5^{1-1}}-1}\\ &= \frac{x^5-1}{x-1}\\ &= x^4+x^3+x^2+x+1\cdot\end{aligned}$$

$\Phi_1,\ \Phi_3,\ \Phi_5$ sont irréductible sur $\mathbb{F}_2$·Comme $15/(2^4-1)\ et$ deg $\Phi_{15}=\phi(15)=8$, on conclut que Φ_{15} est le produit de deux polynôme irréductible de deg =4 à savoir:

$$\Phi_{15}=\left(x^4+x+1\right)\left(x^4+x^3+1\right)$$

D'où l'écriture du polynome $x^{15}-1$ en produit de polynomes irréductibles sur $\mathbb{F}_2$·

2.4.2 Critère d'irréductibilité d'un polynôme cyclotomique sur un corps fini

Définition 2.4.3

Soit $p > 1$, le polynôme f $=\frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1$ est irréductible sur $\mathbb{F}_q$ si et seulement si p est premier et q est une racine primitive $(p-1)$ iéme de l'unité modulo p $(ie\ q^{p-1} \equiv 1 \pmod p)$ ·

Preuve.

Supposons f irréductible alors, l'ordre de f doit diviser q^{p-1}· Mais l'ordre de f est par définition le plus petit entier naturel e tel que f divise $x^e - 1$, *or* f divise $x^p - 1$ (car $x^p - 1 = (x-1) f(x)$) ·Et comme $\deg f = p-1$ ce qui implique que $e = p$, d'ou on a: p divise $q^{p-1} - 1$,c'est à dire $q^{p-1} - 1 \equiv 0 \pmod p$, ainsi $q^{p-1} = 1 \pmod p$

et p est premier par le petit théorème de fermat·Invérsement,

sioent p un nombre premier et q un entier positif qui vérifier $q^{p-1} \equiv 1 \pmod p$,

montrons que le polynome f est irréductible sur F_q, en effet

$\frac{x^p-1}{x-1} = \frac{\prod_{d/p} \Phi_d}{x-1} = \frac{\Phi_1 \cdot \Phi_2}{x-1} = \frac{(x-1)\Phi_p}{x-1} = \Phi_p$, et comme p est premier on a $\phi(p) = p-1$ *et* $q^{p-1} \equiv 1 \pmod p$, par

lemme:$\Phi_n[x] \in F_q[x]$ est irréductible si, seulement si l'ordre multiplicatif de q modulo n est $\phi(n)$,

c'est à dire si $q^{\varphi(n)} \equiv 1 \pmod n$ ·

le polynôme cyclotomique Φ_p est irréductible sur $\mathbb{F}_q$,d'où le résultat· ■

Exemple 2.4.3

Le polynôme $f = \frac{x^7-1}{x-1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ est irréductible sur $\mathbb{F}_3$, car $p = 7$ est premier et $3^6 \equiv 1 \pmod 7$ ·

Définition 2.4.4

On appelle fonction de **MOBIUS**, l'application

$$\begin{aligned} \mu &: \mathbb{N}^* \to \mathbb{N}^* \\ d &\mapsto \mu(d) \end{aligned}$$

tell que

$$\begin{aligned} \mu(1) &= 1 \\ \mu(d) &= (-1)^k, \text{ si } d \text{ est produit de } k \text{ nombre premier distincts} \cdot \\ \mu(d) &= 0, \text{ si } d \text{ est divisible par le carré d'une nombre premier} \end{aligned}$$

Proposition 2.4.1

Pour tout entier $n > 0$ on a :

$$\sum_{d/n} \mu(d) = \begin{cases} 1 & si\ n = 1 \\ 0 & si\ n > 0 \end{cases}$$

Démonstration. ■

On montre la formule

$$\sum_{d/n} \mu(d) = \begin{cases} 1 & si\ n = 1 \\ 0 & si\ n > 0 \end{cases}$$

la formule est triviale si $n = 1\cdot$

Supposons $n > 1$ est notons $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$la décomposition de $n \cdot$ Les diviseur de n s'écrivent $d = p_1^{\beta_1} p_2^{\beta 2} \cdots p_k^{\beta_k}$ avec $\beta_i \leq \alpha_i,$ et l'on a $\mu(d) = 0$ si l'un des exposants β_i est $\geq 2 \cdot$ Si t exposants de la décomposition de d valent 1, les autres étant nuls, $\sum_{d/n} \mu(d) = \sum_{t=0}^{k} C_k^t (-1)^t = (1-1)^k = 0\cdot$

Etant donné un corps $\mathbb{k}$ est un entier $n > 0$ si $\Phi_n(x)$ est le $n^{iéme}$ polynôme cyclotomique sur $\mathbb{F},$ alors

$$\Phi_n(x) = \prod \left(x^{\frac{n}{d}} - 1\right)^{\mu(d)}$$

où μ est la fonction de mobius $\cdot$

Exemple 2.4.4

1) Pour trouver le polynôme cyclotomique $\Phi_8(x)$ sans utiliser les racine $8^{iémes}$ de l'unité

$$\begin{aligned} \Phi_8(x) &= \left(x^8-1\right)^{\mu(1)} \left(x^4-1\right)^{\mu(2)} \left(x^2-1\right)^{\mu(4)} (x-1)^{\mu(8)} \\ &= \left(x^8-1\right)\left(x^4-1\right)^{-1} \\ &= x^4+1 \end{aligned}$$

2.4.3 Décomposition des polynômes cyclotomiques dans un corps fini

D'après ce qu'on a vu, tout corps fini peut se construire en adjoignant à un corps premier $\mathbb{F}_p$ un élément algébrique bien choisi, racine d'un polynôme irréductible $p \in \mathbb{F}_p[x]\cdot$ Mais comme tout élément non nul d'un corps fini, cet élément est nécessairement un racine de l'unité, et donc p est un facteur irréductible d'un polynôme $x^n - 1\cdot$ Or, on a vu qu'un tel polynôme se décomposait déjà dans $\mathbb{Z}[x]$ en produit des polynômes cyclotomiques Φ_d, pour d divisant $n\cdot$ Parconséquent, p est un facteur irréductible (dans $\mathbb{F}_p[x]$)d'un des polynomes cyclotomiques $\Phi_d\cdot$ Il existe ainsi une relation directe entre la construction des corps fini de caractéristique p et la décomposition des polynômes cyclotomiques dans $\mathbb{F}_p[x]\cdot$

Soient p un nombre premier et n un entier $> 0\cdot$ Bien que le polynôme Φ_n soit irréductible sur $\mathbb{Q}$ comme on vient de le prouver, il n'en n'est pas nécessairement de même lorsqu'on le réduit modulo $p\cdot$ Par exemple, si $\Phi_7 = 1 + x + \cdots + x^6$ est bien irréductible sur $\mathbb{Q}$, il ne l'est plus modulo 2, puisqu'on a

$$1 + X + \cdots + X^6 \equiv \left(1 + X + X^3\right)\left(1 + X^2 + X^3\right)[\mathrm{mod}\,2]\cdot$$

Proposition 2.4.2

Soit $\Bbbk$ un corps fini à q élément, et soit $n > 0$ un entier premier à $q\cdot$ Notons r l'ordre de la classe de q dans le groupe $(\mathbb{Z}/p\mathbb{Z})^*$, c'est-à-dire le plus petit entier $r > 0$ tel que $q^r \equiv 1\,[\mathrm{mod}\,n]\cdot$ Alors le polynôme cyclotomique $\Phi_n(x)$ se décompose dans $\Bbbk[x]$ en produit de polynômes unitaire irréductibles de degré r, tous différents·

Exemple 2.4.5

Soit $q = 3$ et $n = 11$, on a $r = 5$, et le polynôme $\Phi_{11} = 1 + X + \cdots + X^{10}$ se décompose dans le corps $\mathbb{F}_3$ en produit de deux polynômes irréductibles de degré 5·

Corollaire 2.4.1

Soit $\Bbbk$ un corps fini à q éléments, et soit n un entier positif premier à q· Pour que le polynome cyclotomique Φ_n soit irréductible sur $\Bbbk$, il faut et il suffit que la classe de q engendre le groupe $(\mathbb{Z}/p\mathbb{Z})^*\cdot$

Exemple 2.4.6

Puisque la classe de 2 est un générateur de $(\mathbb{Z}/3\mathbb{Z})^*$ (resp $(\mathbb{Z}/5\mathbb{Z})^*$) , le polynôme Φ_3 ($resp$ Φ_5) est irréductible sur $\mathbb{F}_2$·

Corollaire 2.4.2

Dans l'anneau $\mathbb{F}_p$, le polynôme Φ_{p^r-1} est un produit de polynômes unitaires irréductibles de degré r, tous différents·

On trouve ainsi pour $p = 2$ et $r = 3$ la décomposition

$$1 + X + \cdots + X^6 = \left(1 + X + X^3\right)\left(1 + X^2 + X^3\right) \in \mathbb{F}_2[x] \cdot$$

Proposition 2.4.3

Pour tout nombre premier p et tout entier $r > 0$, il existe dans $\mathbb{F}_p[x]$ des polynômes primitifs de degré r·

2.5 Nombre de polynômes unitaire irréductibles, de degré fixé, sur un corps fini

Formule d'invérsion de MOBIUS

Cette formule est une méthode d'invertions de certains type de sommes· La forme classique est originallement développée en 1935, indépendament par **P·HAL**L et **L·WEINER** .

Cependant en 1964, **GAIN–GARLO ROTA** généralise la forme classique pour d'autres situations· L'importance de la fonction μ est contenue dans le résultat suivant :

Théorème 2.5.1

Soit f , g deux applications de $\mathbb{N}$ dans un groupe A

Si A est additif abélien alors :

$$f(n) = \sum_{d/n} g(d) \iff g(n) = \sum_{d/n} \mu\left(\frac{n}{d}\right) f(d) \tag{1}$$

Si A est multiplicatif abélien alors :

$$f(n) = \prod_{d/n} g(d) \iff g(n) = \prod_{d/n} f(d)^{\mu\left(\frac{n}{d}\right)} \tag{2}$$

Preuve.

Compte tenu de la modification citée, une sommation dirécte sur les n divisant m des deux membres de (1) multipliés par $\mu\left(\frac{m}{n}\right)$, donne:

$$\begin{aligned}\sum_{n/m} \mu\left(\frac{m}{n}\right) f(n) &= \sum_{n/m} \mu\left(\frac{m}{n}\right) \sum_{d/m} g(d) \\ &= \sum_{d/m} g(d) \sum_{d/(n/m)} \mu\left(\frac{m}{n}\right) \\ &= g(m)\end{aligned}$$

Un simple changement de désignation conduit à la formul

$$g(n) = \sum_{d/n} \mu\left(\frac{n}{d}\right) f(d)$$

la réciproque se fait de la même maniére

Pour la formule (2) il convient d'éffféctuer les mêmes calculs formels:

$$\begin{aligned}\prod_{n/m} f(n)^{\mu\left(\frac{m}{n}\right)} &= \prod_{n/m} \prod_{d/n} g(d)^{\mu\left(\frac{m}{n}\right)} \\ &= \prod_{d/m} \prod_{d/(n/m)} g(d)^{\mu\left(\frac{m}{n}\right)} \\ &= \prod_{d/m} g(d)^{\sum\limits_{d/(n/m)} \mu\left(\frac{m}{n}\right)} \\ &= g(m)\end{aligned}$$

En modification légérement les désignations, on aboutit au résultat · ■

Exemple 2.5.1

La fonction ϕ D'EULER, définie par

$$\phi(n) = |U(\mathbb{Z}/n\mathbb{Z})|$$

(l'ordre du groupe des élément invérsibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$) ·

Sachant que $n = \sum_{d/n} \phi(d)$ et en utilisant la forme additive de la formule d'invérsion de **MOBIUS** on obtient :

$$\begin{aligned} \phi(n) &= \sum_{d/n} \mu\left(\frac{n}{d}\right) \cdot d \qquad\qquad (ici\ f(n) = n) \\ &= \sum_{d/n} \mu\left(\frac{n}{d}\right) \cdot \frac{n}{d} \\ &= n \sum_{d/n} \frac{\mu(d)}{d} \end{aligned}$$

Si $n = p_1^{m_1} \cdots p_r^{m_r}$ alors:

$$\begin{aligned} \sum_{d/n} \frac{\mu(d)}{d} &= 1 - \sum_i \frac{1}{pi} + \sum_{i \prec j} \frac{1}{p_i p_j} - \cdots + (-1)^r \frac{1}{p_1 \cdots p_r} \\ &= \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) \end{aligned}$$

D'où

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) \cdot$$

Exemple 2.5.2

Du théorème de la décomposition cyclotomique

$$x^n - 1 = \prod_{d/n} \Phi_d$$

En appliquant la forme multiplicative de la formule d'invérsion de **MOBIUS** on obtient une expréssion explicite pour

$$\Phi_n = \prod_{d/n} \left(x^d - 1\right)^{\mu\left(\frac{n}{d}\right)} \qquad (3)$$

pour de faibles valeurs de n on a :

$\Phi_1 = \prod_{d/1} \left(x^d - 1\right)^{\mu\left(\frac{1}{d}\right)} = (x^1 - 1)^{\mu\left(\frac{1}{1}\right)} = x - 1$ *car* $\mu(1) = 1$

$\Phi_2 = \prod_{d/2} \left(x^d - 1\right)^{\mu\left(\frac{2}{d}\right)} = (x^1 - 1)^{\mu\left(\frac{2}{1}\right)} (x^2 - 1)^{\mu\left(\frac{2}{2}\right)} = \frac{x^2-1}{x-1} = x + 1 \cdot$car $\mu(2) = -1$

$\Phi_3 = \prod_{d/3} \left(x^d - 1\right)^{\mu\left(\frac{3}{d}\right)} = (x^1 - 1)^{\mu\left(\frac{3}{1}\right)} (x^3 - 1)^{\mu\left(\frac{3}{3}\right)} = \frac{x^3-1}{x-1} = x^2+x+1 \cdot$puisque $\mu(3) = -1$

$\Phi_4 = \prod_{d/4} \left(x^d - 1\right)^{\mu\left(\frac{4}{d}\right)} = (x^1 - 1)^{\mu\left(\frac{4}{1}\right)} (x^2 - 1)^{\mu\left(\frac{4}{2}\right)} (x^4 - 1)^{\mu\left(\frac{4}{4}\right)} = \frac{x^4-1}{x^2-1} = x^2 + 1 \cdot$

car $\mu(4) = 0$

avec les même calculs on trouve :

$\Phi_8 = x^4 + 1$

$\Phi_9 = x^6 + x^3 + 1$

$\Phi_{12} = x^4 - x^2 + 1$

Calcul du nombre de polynômes unitaires irréductibles, de degré fixé, sur un corps fini

Soit $N_q(n)$ le nombre de polynômes unitaires irréductibles de degré n sur le corps $\mathbb{F}_q$. La formule $x^{q^n} - x = \prod f_i$ on montre que le degré du produit de tout les polynômes irréductibles unitaires sur $\mathbb{F}_q$ dont le degré divise n est égal à $\sum_{d/n} N_q(d) \cdot d$ et comme le polynôme $x^{q^n} - x$ est de degré q^n, on a:

$$q^n = \sum_{d/n} N_q(d) \cdot d$$

En appliquant la forme additive de la formule d'invérsion de **MOBIUS** et en posant $f(n) = q^n$ et $g(n) = n \cdot N_q(n)$, on obtient:

$$n \cdot N_q(n) = \sum_{d/n} \mu\left(\frac{n}{d}\right) q^d \qquad (4)$$

c'est à dire que

$$N_q(n) = \frac{1}{n} \sum_{d/n} \mu\left(\frac{n}{d}\right) q^d \qquad (5)$$

Exemple 2.5.3

On calcule, sur $\mathbb{F}_2$, le nombre exacte de polynômes irréductibles de deg $= 2,\ 3,\ 4,\ 5,\ 6\cdot$

$N_2(2) = \frac{1}{2}\left[\mu\left(\frac{2}{1}\right)2^1 + \mu\left(\frac{2}{2}\right)2^2\right] = \frac{1}{2}\left(2^2 - 2^1\right) = 1\cdot$

$N_2(3) = \frac{1}{3}\left[\mu\left(\frac{3}{1}\right)2^1 + \mu\left(\frac{3}{3}\right)2^3\right] = \frac{1}{3}\left(2^3 - 2^1\right) = 2\cdot$

$N_2(4) = \frac{1}{4}\left[\mu\left(\frac{4}{1}\right)2^1 + \mu\left(\frac{4}{2}\right)2^2 + \mu\left(\frac{4}{4}\right)2^4\right] = \frac{1}{4}\left(2^4 - 2^2\right) = 3\cdot$

$N_2(5) = \frac{1}{5}\left[\mu\left(\frac{5}{1}\right)2^1 + \mu\left(\frac{5}{5}\right)2^5\right] = \frac{1}{5}\left(2^5 - 2^1\right) = 6\cdot$

$N_2(6) = \frac{1}{6}\left[\mu\left(\frac{6}{1}\right)2^1 + \mu\left(\frac{6}{2}\right)2^2 + \mu\left(\frac{6}{3}\right)2^3 + \mu\left(\frac{6}{6}\right)2^6\right] = \frac{1}{6}\left(2^6 - 2^3 - 2^2 + 2^1\right) = 9\cdot$

La formule (5) montrre que pour tout $q = p^n,\ p$ premier, il existe un polynôme irréductible de degré $n\ \cdot$

Voici un tableau donnant le nombre de polynômes unitaires irréductibles,de degré $\leq\ 14$, sur $\mathbb{F}_2$

n	6	7	8	9	10	11	12	13	14
$N_q(n)$	9	18	30	56	99	186	335	630	1161

Malgré qu'on connait le nombre de polynômes unitaires irréductibles, de degré n, sur un corps fini $\mathbb{F}_q\cdot$On ne peut pas, en général, les expliciter tous si les deux entier positifs n et q deviénnent assez grands, cependant on peut calculer leur produit:

Corollaire 2.5.1

Le produit $I(q,n)$ de tous les polynômes unitaires irréductibles sur $\mathbb{F}_q$, de degré n, est donné par :

$$I(q,n) = \prod_{d/n}\left(x^{q^n} - x\right)^{\mu\left(\frac{n}{d}\right)}$$

Preuve.

on a $x^{q^n} - x = \prod_{d/n} I(q,n)\cdot$En posant $f(n) = I(q,n)$ et $g(n) = x^{q^n} - x$ pour tout $n \in \mathbb{N},$ et en appliqaunt la forme multiplicative de la formule d'inversion de MOBIUS on obtient :

$$\begin{aligned} g_n &= \prod_{d/n} f(d) \iff f(n) = \prod_{d/n} g(d)^{\mu\left(\frac{n}{d}\right)} \\ &\iff I(q,n) = \prod_{d/n}\left(x^{q^n} - x\right)^{\mu\left(\frac{n}{d}\right)} \end{aligned}$$

■

Exemple 2.5.4

Calculons le produit de tous les polynômes unitaires irréductibles, de deg = 4, sur $\mathbb{F}_2$.

$$\begin{aligned} I(2,4) &= \prod_{d/4} \left(x^{2^4} - x\right)^{\mu\left(\frac{4}{d}\right)} \\ &= \left(x^2 - x\right)^{\mu\left(\frac{4}{1}\right)} \left(x^{2^2} - x\right)^{\mu\left(\frac{4}{2}\right)} \left(x^{2^4} - x\right)^{\mu\left(\frac{4}{4}\right)} \\ &= \frac{x^{16} - x}{x^4 - x} = \frac{x^{15} - 1}{x^3 - 1} \\ &= x^{12} + x^9 + x^6 + x^3 + 1. \end{aligned}$$

Et ceci car $\mu(1) = 1,\ \mu(2) = -1,\ \mu(4) = 0$.

Et on a : $$\begin{aligned} x^{16} - x &= I(2,1)\ I(2,2)\, I(2,4) \\ &= (x^2 - x)(x^2 + x + 1)(x^{12} + x^9 + x^6 + x^3 + 1). \end{aligned}$$

2.6 Test d'irréductibilité d'un polynôme sur un corps fini

Proposition 2.6.1

Un polynôme $f \in \mathbb{F}_p$ de degré n est irréductible si les deux conditions suivant sont vérifiéés:

i) $x^{p^n} - x \equiv 0 \pmod{f(x)}$

ii) Et pour tout q premier qui divise n, $\left(x^{p^{n/q}} - x, f(x)\right) = 1$.

Exemple 2.6.1

Sur $\mathbb{F}_2$, soit le polynôme $f = x^4 + x^3 + 1$, montrons qu'il est irréductible, vérifions alors s'il réalise les deux conditions (dans $\mathbb{F}_2$ on a $: -1 = 1$)

i) $x^{2^4} + x \equiv 0 \pmod{x^4 + x^3 + 1}$, en effet

$x^{2^4} + x = (x^4 + x^3 + 1)(x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^5 + x^4 + x)$

ii) et comme 2 est le seul nombre premier qui divise 4 on a :

$x^{2^{4/2}} + x = x^4 + x$ et $\text{pgcd}(x^4 + x, x^4 + x^3 + 1) = 1$.

Chapitre 3

Décomposition des polynômes

Dans ce chapitre, on rappelle les notions de base dont aura besoin par la suite, factotisation du polynômes $x^n - 1$ *sur* $\mathbb{F}_q$ est factorisation de $x^{4p^n} - 1$ sur $\mathbb{F}_q$·

3.1 Factorisation du polynomes x^n-1 sur $\mathbb{F}_q$

Polynôme minimal

Définition 3.1.1

Soit $\alpha \in \mathbb{F}_{q^m}$· Le polynôme minimal de α sur $\mathbb{F}_q$ est le polynôme unitaire de plus bas degré $f(x) \in \mathbb{F}_q[x]$ vérifiant $f(\alpha) = 0$·Nous le notons $M_\alpha(x)$·

Proposition 3.1.1

Soit $\alpha \in \mathbb{F}_{q^m}$·Soit d un entier positif non nul·Le degré deg $M_\alpha(x)$ du polynôme minimal $M_\alpha(x)$ de α sur $\mathbb{F}_q$ est égal à d si et seulement si d est le plus petit entier positif non nul tel que $\alpha^{q^d} = \alpha$·

Corollaire 3.1.1

Soit $\alpha \in F_{q^m}$· Soit l l'ordre de α·Alors

$$\deg\ M_\alpha(x) = ord_l(q)\cdot$$

Proposition 3.1.2

Soit $\alpha \in \mathbb{F}_{q^m}$· Soit l l'ordre de α·Alors

$$M_\alpha(x) = \prod_{i=0}^{ord_l(q)-1} \left(x - \alpha^{q^i}\right),$$

C'est–à–dire $\left\{\alpha,\ \alpha^q,\ \alpha^{q^2}, \cdots,\ \alpha^{q^{ord_l(q)-1}}\right\}$ est l'ensemble des racines de $M_\alpha(x)$

Proposition 3.1.3

Soit $\alpha \in \mathbb{F}_{q^m}$·Tout les racine de $M_\alpha(x)$ sont de même ordre·

Conjugaison

Définition 3.1.2

La conjugaison dans $\mathbb{F}_{q^m}$ est le relation $\Re$ définie par

$$\alpha \Re \beta \quad si\ M_\alpha(x) = M_\beta(x)$$

Proposition 3.1.4

La conjugaison dans $\mathbb{F}_{q^m}$ est un relation d'équivalence ·

Définition 3.1.3

Les conjugués d'un élément α de $\mathbb{F}_{q^m}$ sont les élément de la classe d'équivalence de α pour le conjugaison dans $\mathbb{F}_{q^m}$·

Proposition 3.1.5

Soit $\alpha \in \mathbb{F}_{q^m}$·Soit l l'ordre de α·La conjugués de α sont

$$\alpha,\ \alpha^q,\ \alpha^{q^2},\ \alpha^{q^3}, \cdots, \alpha^{q^{ord_l(q)-1}}$$

Ils sont distincts deux à deux ·

Racines de l'unité

Rappelons que $(n, q) = 1$·Soit m un entier positif non nul tel que $n \ / \ q^m - 1$·

Définition 3.1.4

On appelle racine n –ièmes de l'unité sur $\mathbb{F}_q$, un élément de $\mathbb{F}_{q^m}$ dont l'ordre divise n, on appelle racine n –ièmes primitive de l'unité sur $\mathbb{F}_q$, un élément de $\mathbb{F}_{q^m}$ d'ordre n ·

En particulier si $n = q^n$–1, une racine primitive n–ièmes de l'unité sur $\mathbb{F}_q$ est un élément primitif de $\mathbb{F}_{q^m}$·

Les racine n –ièmes de l'unité sur $\mathbb{F}_q$ forment un sous groupe multiplicatif $\mathbb{F}^*_{q^m}$·

En effet, si β et γ sont deux racines n-ièmes de l'unité sur $\mathbb{F}_q$, $(\beta\gamma)^n = \beta^n\gamma^n = 1$ et donc $\beta\gamma$ est aussi une racine n-ièmes de l'unité sur $\mathbb{F}_q$·

D'ailleurs, $\left(\beta^{-1}\right)^n = (\beta^n)^{-1} = 1$ un sous group de $\mathbb{F}^*_{q^m}$·

Comme $\mathbb{F}^*_{q^m}$ est cyclique, ce sous groupe est aussi cyclique ·

Soit μ l'entier tel que $n = q^m - 1$ ·Soit α une élément primitif de $\mathbb{F}_{q^m}$·Alors β est une racine n-ièmes primitive de l'unité sur $\mathbb{F}_q$, car l'ordre de α^μ est égal à $\frac{q^m-1}{(q^m-1,\mu)} = \frac{q^m-1}{\mu} = n$·Donc β est un générateur de ce sous groupe qui est d'ordre n·

Ce sous groupe est composé de toutes les racines de $x^n - 1$, i·e·la décomposition de $x^n - 1$ sur F_q est

$$x^n - 1 = \prod_{i=0}^{n-1} \left(x - \beta^i\right)$$

Soit γ une racine n –ièmes de l'unité sur $\mathbb{F}_q$, ses conjugués dans $\mathbb{F}_{q^m}$ sont les puissances de γ, donc ils sont aussi des racines n –ièmes de l'unité sur $\mathbb{F}_q$·La conjugaison dans $\mathbb{F}_{q^m}$ définit donc une relation d'équivalence dans l'ensemble des racines n–ièmes de l'unité sur $\mathbb{F}_q$·On peut alors dire les mêmes choses comme dans la remarque précédent chaque classe d'équivalence est composée de toutes les racines d'un polynôme minimal, et

* il y a autant des classes d'équivalence que de polynôme minimaux différents des racines n–ièmes de l'unité sur $\mathbb{F}_q$·

* le cardinal de toute classe est égal au degré du polynôme correspondant

Nous obtenons aussi que

$$x^n - 1 = \prod_{\gamma} M_\gamma(x)$$

où parcourt un ensemble de représentants des classes d'équivalence, et compte tenu de la proposition dans la partie polynôme minimal, que le polynôme minimal de $\gamma = \beta^j$, $j \in$

$\mathbb{Z}_n$ est égal à

$$M_\gamma(x) = \prod_{i=0}^{ord_\ell(q)-1} \left(x - \gamma^{q^i}\right) = \prod_{i=0}^{ord_\ell(q)-1} \left(x - \beta^{jq^i}\right)$$

où ℓ est l'ordre de γ, $\ell = \frac{n}{(n,j)}$.

Cas générale prenon maintenant le cas général ou n et q ne sont pas forcément premiers entre eux. Soit $n = rp^s$, ou r est premier avec p et $s \geq 0$

(p^s est la plus grand puissance de p qui divise n) .Alors

$$x^n - 1 = x^{rp^s} - 1 = (x^r - 1)^{p^s},$$

car nous travaillons sur le corps $\mathbb{F}_q$ de caractéristique p.

Puis que r est premier avec p, nous pouvons décomposer $x^n - 1$ comme si dessus, et en déduire la décomposition de $x^n - 1$. Plus précisément, si β est un racine r–ièmes primitive de l'unité sur $\mathbb{F}_q$, alors

$$x^n - 1 = \prod_{i=0}^{r-1} \left(X - \beta^i\right)$$

et donc

$$x^n - 1 = (x^r - 1)^{p^s} = \left(\prod_{i=0}^{r-1} \left(x - \beta^i\right)\right)^{p^s} = \prod_{i=0}^{r-1} \left(x - \beta^i\right)^{p^s}$$

De même,

$$x^n - 1 = (x^r - 1)^{p^s} = \left(\prod_{\gamma} M_\gamma(x)\right)^p = \prod_{\gamma} M_\gamma(x)^{p^s}$$

où parcourt un ensemple de rprésentants des classes d'équivalence par conjugaison des racines r–ièmes de l'unité sur F_q.

Classes cyclotomiques

Soit $(n, q) = 1$.

Soit β une racine n^{iéme} primitive de l'unité sur $\mathbb{F}_q$. $\mathbb{Z}_n$ les ensemble de relation d'équivalence.

Définition 3.1.5

Pour tout entier j, $j \in \mathbb{Z}_n$, nous définissons la classe yclotomique de j modulo n sur $\mathbb{F}_q$ comme l'ensemble

$$cl(j) = \left\{j,\ jq,\ jq^2, \cdots,\ jq^{r-1}\right\} \bmod n,$$

où r est le plus petit entier positif non nul tel que $jq^r = j \bmod n$·

Nous pouvons donc récrire les résultat· Nous avons que

$$r = \deg M_{\beta^j}(x) \equiv ord_\ell(q),$$

où ℓ est l'ordre de β^j, nous obtenus que le polynôme minimal de $\gamma = \beta^j,\ j \in \mathbb{Z}_n$ est

$$M_\gamma(x) = \prod_{i \in cl(j)} \left(x - \beta^i\right)$$

Le nombre de classes cyclotomiques modulo n sur $\mathbb{F}_q$ est égal au nombre de polynomes minimaux dfférents des racines n–ièmes de l'unité sur $\mathbb{F}_q$· La formule nous donne

$$x^n - 1 = \prod_\gamma M_{\beta^j}(x),$$

ou j parcourt un ensemble de représentants des classes cyclotomiques modulo n sur $\mathbb{F}_q$·Donc le nombre de classes cyclotomique modulo n sur $\mathbb{F}_q$ est égal au nombre de diviseurs irréductibles de $x^n - 1$ sur $\mathbb{F}_q$·

Décomposition de $x^n - 1$ sur $\mathbb{F}_q$

Définition 3.1.6

Soit $(n, a) = 1$·Le plus petit entier positif non nul r tel que $a^r \equiv 1 \bmod n$ est appelé l'ordre de a modulo n et noté $\mathrm{ord}_n(a)$·

Si $a \geq 1$, l'ordre $\mathrm{ord}_n(a)$ de a modulo n est l'ordre de a dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$

Algoritheme de décomposition

1· Détermination du plus petit entier m tel que n divise $q^n - 1$·On en déduit le corps des racine n–ièmes de l'unité sur $\mathbb{F}_q$,soit $L = \mathbb{F}_{q^m}$;

2· Détermination des differents classes cyclotomique$(i,\ iq,\ iq^2, \cdots iq^j, \cdots)$ leur nombre est celui des facteurs irréductible cherché, et le nombre d'éléments dans une classes est le degré du polynôme correspondant;

3· Pour chaque classe cyclotomique, détermination du polynôme correspondant

(en utilisant les opèration dand le corps L)·

Exemple 3.1.1

(i) Considérons x^3-1 sur $\mathbb{F}_2$ on a $n=3,\ q=2$ et $m=2$ car $2^2-1=3$

pour les classes cyclotomique modulo 3 on a :

$$\begin{aligned} C_0 &= \left\{0, 2^j\right\} = \{0\} \\ C_1 &= \left\{1, 2^j\right\} = \{1, 2\} \end{aligned}$$

Les deux polynômes minimaux sont:

$M_0(x) = (x-1)$

$M_1(x) = \prod_{j \in C_1} (x-\alpha^j) = (x-\alpha)(x-\alpha^2)$

(α une racine 3-ièmes primitive de l'unité sur F_2)

Pour déterminie le coeficient binaire de $M_1(x)$, il faut faire des calcule dans $\mathbb{F}_4$, puis que 4=2^2, nous considérons polynômes de degré 2 irréductible sur $\mathbb{F}_2$, par exemple $f(x)$=x^2+x+1 si α racine de $f(x)$ alors $f(\alpha)=0$ on a donc $\alpha^2=\alpha+1$ alors

$$M_1(x) = (x-\alpha)\left(x-\alpha^2\right) = x^2 + \left(\alpha+\alpha^2\right)x + 1 = x^2+x+1$$

Donc la factorisation de x^3-1 sur $\mathbb{F}_2$ est

$$x^3-1 = (x-1)\left(x^2+x+1\right)$$

(ii) Considérons x^{21}–1 sur $\mathbb{F}_2$·Il est facile de vérifier que $\{0,\ 1,\ 3,\ 5,\ 7,\ 9\}$ est un ensemble complet de représentants des classes cyclotomique de 2 modulo 21· Puis que 21est un diviseur de 2^6–1, nous considérons le corps $\mathbb{F}_{64}$·Soit α une racine de $1+x+x^6$·On peut vérifier que α est un élément primitif de $\mathbb{F}_{64}$ (vérifier que $\alpha^3 \neq 1,\ \alpha^7 \neq 1,\ \alpha^9 \neq 1$ est $\alpha^{21} \neq 1$) ·Nous listons les classes cyclotomique de 2 modulo 3 contenant des multiples de 3 :

$C_0 = \{0\}$, $\quad C_3 = \{3,\ 6,\ 12,\ 24,\ 48,\ 33\}$,

$C_9 = \{9,\ 18,\ 36\}$, $\quad C_{15} = \{15,\ 30,\ 60,\ 57,\ 51,\ 39\}$,

$C_{21} = \{21,\ 42\}$, $\quad C_{27} = \{27,\ 54,\ 45\}$·

Par conséquent, nous obtenons

$$\begin{aligned}
M_0(x) &= 1+x,\\
M_3(x) &= \prod_{j\in C_3}\left(x-\alpha^j\right) = 1+x+x^2+x^4+x^6,\\
M_9(x) &= \prod_{j\in C_9}\left(x-\alpha^j\right) = 1+x^2+x^3,\\
M_{15}(x) &= \prod_{j\in C_{15}}\left(x-\alpha^j\right) = 1+x^2+x^4+x^5+x^6,\\
M_{21}(x) &= \prod_{j\in C_{21}}\left(x-\alpha^j\right) = 1+x+x^2,\\
M_{27}(x) &= \prod_{j\in C_{27}}\left(x-\alpha^j\right) = 1+x+x^3\cdot
\end{aligned}$$

Donc la factorisation de x^{21}–1 sur $\mathbb{F}_2$ en polynômes irréductible:

$$\begin{aligned}
x^{21}-1 &= M_0(x)\,M_3(x)\,M_9(x)\,M_{15}(x)\,M_{21}(x)\,M_{27}(x)\\
&= (1+x)\left(1+x+x^2+x^4+x^6\right)\left(1+x^2+x^3\right)\left(1+x^2+x^4+x^5+x^6\right)\\
&\quad \left(1+x+x^2\right)\left(1+x+x^3\right)\cdot
\end{aligned}$$

(*iii*) Considérons x^{13}–1 sur $\mathbb{F}_3$·Il est facile de vérifier que $\{0,\ 1,\ 2,\ 4,\ 7\}$ est un ensemble complet de représentants des classes cyclotomique de 3 modulo 13· Puis que 13est un diviseur de 3^3–1, nous considérons le corps F_{27}·Soit α une racine de 1+2x+x^3 · α est un élément primitif de $\mathbb{F}_{27}$ · *les classes cyclotomique de* 3 modulo 26 contenant des multiples de 2 ·*Par conséquent, nous obtenons*

$$\begin{aligned}
M_0(x) &= 2+x,\\
M_2(x) &= \prod_{j\in C_2}\left(x-\alpha^j\right) = \left(x-\alpha^2\right)\left(x-\alpha^6\right)\left(x-\alpha^{18}\right) = 2+x+x^2+x^3,\\
M_4(x) &= \prod_{j\in C_4}\left(x-\alpha^j\right) = \left(x-\alpha^4\right)\left(x-\alpha^{12}\right)\left(x-\alpha^{10}\right) = 2+x^2+x^3,\\
M_8(x) &= \prod_{j\in C_8}\left(x-\alpha^j\right) = \left(x-\alpha^8\right)\left(x-\alpha^{12}\right)\left(x-\alpha^{24}\right) = 2+2x+2x^2+x^3,\\
M_{14}(x) &= \prod_{j\in C_{14}}\left(x-\alpha^j\right) = \left(x-\alpha^{14}\right)\left(x-\alpha^{16}\right)\left(x-\alpha^{22}\right) = 2+2x+x^3\cdot
\end{aligned}$$

Donc la factorisation de x^{13}-1 sur $\mathbb{F}_3$ est :

$$\begin{aligned} x^{13}-1 &= M_0(x)\,M_2(x)\,M_4(x)\,M_8(x)\,M_{14}(x) \\ &= (2+x)\left(2+x+x^2+x^3\right)\left(2+x^2+x^3\right)\left(2+2x+2x^2+x^3\right)\left(2+2x+x^3\right)\cdot \end{aligned}$$

3.2 Factorisation de x^{4p^n}-1 sur $\mathbb{F}_q$

On considérons que q une puissance d'un nombre premier impair et p un nombre premier impair, premier avec q ·Pour n'importe quel entier s, la classe cyclotomique de s modulo $4p^n$ est l'ensemble

$$C_s = \left\{s,\ sq,\ sq^2,\ \cdots,\ sq^{n_s-1}\right\}$$

où n_s le plus petit entier positif tel que $\mathrm{sq}^{n_s} \equiv s \pmod{4p^n}$ · Notez que n_s l'ordre multiplicatif de q modulo $\frac{4p^n}{\gcd(s,4p^n)}$ ·Soit α une racine $4p^n - ième$ primitive de l'unité dans un extension de corps $\mathbb{F}_q$ ·Il est bien que

$$M_s(x) = \prod_{i\in C_s}\left(x-\alpha^i\right)$$

est le polynôme minimal de α^ssur $\mathbb{F}_q$ et m

$$x^{4p^n}-1 = \prod M_s(x)$$

donne la factorisation de $x^{4p^n}-1$ en facteurs irréductibles sur $\mathbb{F}_q$, où par tout un ensemble de réprésentants de classes q-cyclotomiques modulo $4p^n$·

Pour tout entier $m \geq 1$, on note $O_m(q)$ l'ordre multiplicatif de q modulo m ·Pour tout ensemble s on noté par $|s|$ le cardinal de s · Soit

$$f = O_p(q)\ \ et\ e = \frac{\phi(p)}{f}$$

où ϕ indique la fonction d'euler ·Nous écrivons

$$q^f = 1 + p^d c, \quad p \nmid c,\ d \geq 1$$

si $q^2 \equiv 1 \pmod 4$ nous trouvons pour tout entier ℓ $1 \leq \ell \leq n$,

$$O_{p^\ell}(q) = O_{2p\ell}(q) = fp^{\max(\ell-d,0)}$$

et

$$O_{4p^l}(q) = \begin{cases} fp^{\max(\ell-d,0)} & si\ q \equiv 1 \pmod 4, \\ fp^{\max(\ell-d,0)} & si\ q \equiv 3 \pmod 4 \text{ avec } f \text{ pair}, \\ 2fp^{\max(\ell-d,0)} & si\ q \equiv 3 \pmod 4 \text{ avec } f \text{ impair}\cdot \end{cases}$$

pour $1 \leq l \leq n$, soit

$$\lambda(\ell) = fp^{\max(\ell-d,0)} \text{ et } \delta(\ell) = \frac{\phi\left(p^\ell\right)}{\lambda(\ell)} = \frac{\lambda\left(p^\ell\right)}{fp^{\max(\ell-d,0)}} = ep^{\min(\ell,d)-1}.$$

Soit ℓ la plus grande puissance de p divisant $\frac{4p^n}{PGCD(s,4p^n)}$, i·e·soit $n-\ell$ la plus grande puissance de p divisant s ·Soit $s = p^{n-\ell}s'$, $p \nmid s'$ alors

$$\deg\left(M_{p^{n-\ell}s'(x)}\right) = \left|C_{p^{n-\ell}s'}\right| = \begin{cases} fp^{\max(\ell-d,0)} & si\ q \equiv 1 \pmod 4, \\ fp^{\max(\ell-d,0)} & si\ q \equiv 3 \pmod 4 \text{ avec soit } f \text{ ou } s' \text{ pair}, \\ 2fp^{\max(\ell-d,0)} & si\ q \equiv 3 \pmod 4 \text{ avec } f \text{ ou } s' \text{ impair}\cdot \end{cases}$$

Soit r une racine primitive modulo p telle que $\text{pgcd}\left(\frac{r^{p-\ell}-1}{p}, p\right) = 1$·Comme p est impaire, il existe un entier x tel que

$$xp^2 \equiv 1 - r \pmod 4 \cdot$$

on pose $g = r+xp^2$·Alors $g^{p-1}-1 \equiv (r+xp^2)^{p-1}-1 \equiv r^{p-1}-1 \pmod{p^2}$·Donc $\gcd\left(\frac{g^{p-1}-1}{p}, p\right) = \gcd\left(\frac{r^{p-1}-1}{p}, p\right) = 1$, ce qui donne que g est un racine primitive modulo p^ℓ pour tout $\ell \geq 1$ on trouve,

$$g \equiv 1 \pmod 4 \cdot$$

nous prouvons ce qui suit

Théorème 3.2.1

Soit $\mathbb{F}_q$ un corps fini à q élément et p un nombre premier impair avec q ·Soit n $\geq$ 1un entier avec $\delta(\ell)$, $1 \leq \ell \leq n$ et g défini ci-dessus·

(i) Si $q \equiv 1 \pmod 4$,

$$x^{4p^n} - 1 = M_0(x) M_{p^n}(x) M_{-p^n}(x) M_{2p^n}(x) \prod_{a\in R} \prod_{\ell=1}^{n} \prod_{k=0}^{\delta(\ell)-1} M_{ap^{n-l}g^k}(x),$$

ou $R = \{1, -1, 2, 4\}$·

(ii) Si $q \equiv 3 \pmod 4$ et f pair,

$$x^{4p^n} - 1 = M_0(x) M_{p^n}(x) M_{2p^n}(x) \prod_{\ell=1}^{n} \prod_{k=0}^{\delta(\ell)-1} M_{p^{n-l}g^k}(x) \prod_{i=1}^{2} \prod_{\ell=1}^{n} \prod_{k=0}^{\delta(\ell)-1} M_{2^i p^{n-l}g^k}(x) \cdot$$

(iii) Si $q \equiv 3 \pmod 4$ et f impair,

$$x^{4p^n} - 1 = M_0(x) M_{p^n}(x) M_{2p^n}(x) \prod_{i=0}^{2} \prod_{\ell=1}^{n} \prod_{k=0}^{\delta(\ell)-1} M_{2^i p^{n-\ell}g^k}(x) \cdot$$

Pour de prouver le théorème, nous démontrons d'abord quelques lemmes ·

Lemme 3.2.1

Si $q \equiv 1 \pmod 4$, alors tous les classes q cyclotomique distinct modulo $4p^n$ sont donnés par

$C_0 = \{0\}$, $C_{p^n} = \{p^n\}$, $C_{-p^n} = \{-p^n\}$, $C_{2p^n} = \{2p^n\}$,

$C_{ap^{n-\ell}g^k} = \left\{ap^{n-\ell}g^k,\ ap^{n-\ell}g^k q, \cdots,\ ap^{n-\ell}g^k q^{\lambda(\ell)-1}\right\}$ pour $a \in R = \{1,\ -1,\ 2,\ 4\}$, $0 \leq k \leq \delta(\ell) - 1$ *est* $1 \leq \ell \leq n$·

Preuve.

Nous affirmons que le classe cyclotomique $\mathrm{C}_{ap^{n-l}g^k}$, $0 \leq k \leq \delta(\ell)-1$, $1 \leq \ell \leq n$, $a \in R = \{1,\ -1,\ 2,\ 4\}$ sont distinct ·suppose $C_{a_1 p^{n-l_1} g^{k_1}} = C_{a_2 p^{n-l_2} g^{k_2}}$, pour certains $\ell_i,\ k_i,\ a_i,\ 1 \leq \ell_i \leq n,\ 1 \leq k_i \leq \delta(\ell_i) - 1,\ a_i \in R = \{1,\ -1,\ 2,\ 4\},\ i = 1,\ 2$·ensuite nous avons

$$a_1 p^{n-\ell_1} g^{k_1} \equiv a_2 p^{n-\ell_2} g^{k_2} q^j \pmod{4p^n}$$

pour un certain nombre j · Nous devons donc avoir

$$\gcd\left(a_1 p^{n-\ell_1} g^{k_1}, 4p^n\right) = \gcd\left(a_2 p^{n-\ell_2} g^{k_2} q^j, 4p^n\right) = \gcd\left(a_2 p^{n-\ell_2} g^{k_2}, 4p^n\right),$$

comme q est premier a $4p$ · Cela donne $\ell_1 = \ell_2 = \ell$ et soit $a_1 = a_2$ *ou* $a_1 = -a_2 = \pm 1$·

Si $a_1 = -a_2 = \pm 1$donne

$$-p^{n-\ell} g^{k_1} \equiv p^{n-\ell} g^{k2} q^j \pmod{4p^n}$$

ce qui donne plus

$$-1 \equiv g^{k_2 - k_1} q^j \left(\mathrm{mod}\, 4p^\ell\right) \cdot$$

comme g $\equiv 1 \pmod 4$ et $q \equiv 1 \pmod 4$, $-1 \equiv 1 \pmod 4$, une contradiction·

Si $a_1 = a_2 = a$, donne

$$ap^{n-\ell}g^{k_1} \equiv p^{n-\ell}g^{k2}q^j \pmod{4p^n}$$

pour certains j, ce qui donne

$$g^{k_2-k_1} \equiv q^j \left(\mathrm{mod}\, 4p^\ell\right)$$

élever les deux puissance $\lambda(\ell)$, nous obtenons

$$g^{(k_1-k_2)\lambda(l)} \equiv q^{j\lambda(l)} \equiv 1 \left(\mathrm{mod}\, 4p^l\right) \cdot$$

comme g est un racine primitive modulo p^l, cela donne ca $\phi\left(p^\ell\right)$ divise $(k_1 - k_2)\lambda(\ell)$, $i \cdot e\cdot$, $\delta(\ell)$ divise $(k_1 - k_2)$ depuis·$0 \leq k_1, k_2 \leq -1$·

c'est possible si et seulement si $k_1 = k_2$·

cela prouve l'affirmation ·en outre, ce sont tout les classe cyclotomique modulo $4p^n$, on a

$$\begin{aligned} & |C_0| + |C_{p^n}| + |C_{-p^n}| + |C_{2p^n}| + \sum_{a\in R}\sum_{\ell=1}^{n}\sum_{k=0}^{\delta(\ell)-1} \left|C_{ap^{n-\ell}g^k}\right| \\ = \;& 4 + \sum_{a\in R}\sum_{\ell=1}^{n}\sum_{k=0}^{\delta(\ell)-1} \lambda(\ell) \\ = \;& 4 + \sum_{a\in R}\sum_{\ell=1}^{n} \delta(\ell)\lambda(\ell) \\ = \;& 4 + 4\sum_{\ell=1}^{n} \phi\left(p^\ell\right) = 4p^n\cdot \end{aligned}$$

■

Lemme 3.2.2

Si $q \equiv 3 \pmod 4$ est f est pair, alors tous les classes cyclotomiques distincts modulo $4p^n$ sont donnés par

$C_0 = \{0\}$, $C_{p^n} = \{p^n, p^n q\}$, $C_{2p^n} = \{2p^n\}$, $C_{p^{n-l}g^k} = \left\{p^{n-\ell}g^k,\ ap^{n-\ell}g^k q, \cdots,\ ap^{n-\ell}g^k q^{\lambda(\ell)-1}\right\}$

pour $0 \leq k \leq 2\delta(\ell)-1$, $1 \leq \ell \leq n$; *est* $C_{2^i p^{n-l}g^k} = \left\{2^i p^{n-\ell}g^k,\ 2^i p^{n-\ell}g^k q,\ \cdots,\ 2^i p^{n-\ell}g^k q^{\lambda(\ell)-1}\right\}$,

pour $i = 1,\ 2$, $0 \leq k \leq \delta(\ell) - 1,\ 1 \leq \ell \leq n$ ·

Preuve.

Si $C_{2^{i}p^{n-l_1}g^{k_1}} = C_{2^{i}p^{n-l_2}g^{k_2}}$ pour certains $k_1, k_2, \ell_1, \ell_2,$ avec $0 \leq k_i \leq 2\delta(\ell) - 1,\ 1 \leq \ell_i \leq n,$ est $i_1, i_2 \in \{0, 1, 2,\ \}$ puis travailler comme dans le lemma $(3 \cdot 2 \cdot 1)$,

on voit ca $\ell_1 = \ell_2 = \ell$ *et* $a_1 = a_2 = a \cdot$

Si $i = 1$ ou 2 est $0 \leq k_i \leq \delta(\ell) - 1,$ puis $C_{2^{i}p^{n-l}g^{k_1}} = C_{2^{i}p^{n-\ell}g^{k_2}}$ implique $2^{i}p^{n-\ell}g^{k_1} \equiv 2^{i}p^{n-\ell}g^{k_2}q^{j} \pmod{4p^n}$ pour certains $j;$ ce qui donne la congruence à savoir

$$g^{k_1-k_2} \equiv q^{j} \left(\mathrm{mod}\, 4p^{\ell}\right) \cdot$$

Travaille maintenant comme dans le lemme$(3 \cdot 2 \cdot 1)$, nous obtenons k_1=k_2·

Si $i = 0$, puis $C_{p^{n-\ell}g^{k_1}} = C_{p^{n-\ell}g^{k_2}}$ implique

$$p^{n-\ell}g^{k_1} \equiv p^{n-\ell}g^{k_2}q^{j} \pmod{4p^n}$$

pour certains $j,$ qui donne

$$g^{k_1-k_2} \equiv q^{j} \pmod{4}$$

puisque $g \equiv 1 \pmod{4}$ *est* $q \equiv 3 \pmod{4}$ nous devons avoir ce j est pair ·Soit $j = 2j'$·cela donne

$$g^{k_1-k_2} \equiv q^{2j'} \left(\mathrm{mod}\, p^{l}\right) \cdot$$

puisque f est pair, nous avons $\lambda(\ell)$ est pair et donc les deux congruence a la puissance $\frac{\lambda(\ell)}{2}$ nous obtenons

$$g^{(k_1-k_2)\frac{\lambda(\ell)}{2}} \equiv q^{j\lambda(\ell)'} \equiv 1 \left(\mathrm{mod}\, p^{\ell}\right) \cdot$$

comme g est un racine primitive modulo $p^{\ell},$ cela donne que $\phi\left(p^{\ell}\right)$ divise $(k_1 - k_2)\frac{\lambda(\ell)}{2},\ i \cdot e \cdot,\ 2\delta(\ell)$ divise $(k_1 - k_2)$ ·car $0 \leq k_1, k_2 \leq 2\delta(\ell) - 1,$ c'est possible si et seulement si $k_1 = k_2$·

En oura, ce sont tous les classes cyclotomiques modulo $4p^n$, on donne

$$\begin{aligned}
& |C_0| + |C_{p^n}| + |C_{2p^n}| + \sum_{\ell=1}^{n}\sum_{k=0}^{2\delta(\ell)-1} \left|C_{ap^{n-\ell}g^{k}}\right| + \sum_{i=1}^{2}\sum_{\ell=1}^{n}\sum_{k=0}^{2\delta(\ell)-1} \left|C_{2^{i}p^{n-\ell}g^{k}}\right| \\
= \ & 4 + \sum_{\ell=1}^{n}\sum_{k=0}^{2\delta(\ell)-1} \lambda(\ell) + \sum_{i=1}^{2}\sum_{\ell=1}^{n}\sum_{k=0}^{\delta(\ell)-1} \lambda(\ell) \\
= \ & 4 + \sum_{\ell=1}^{n} 2\delta(\ell)\lambda(\ell) + 2\sum_{l=1}^{n} \delta(\ell)\lambda(\ell) \\
= \ & 4 + \sum_{l=1}^{n} 2\phi\left(p^{\ell}\right) + 2\sum_{l=1}^{n} \phi(p\ell) \\
= \ & 4 + 4\sum_{l=1}^{n} \phi\left(p^{\ell}\right) = 4p^{n} \cdot
\end{aligned}$$

■

Lemme 3.2.3

Si $q \equiv 3 \pmod 4$ est f est impair, alors tous les classe cyclotomique distincts modulo $4p^n$ sont donnés par

$C_0 = \{0\}$, $C_{p^n} = \{p^n, p^n q\}$, $C_{2p^n} = \{2p^n\}$, $est\, C_{p^{n-l}g^k} = \left\{p^{n-\ell}g^k,\ p^{n-\ell}g^k q, \cdots,\ p^{n-\ell}g^k q^{2\lambda(\ell)-1}\right\}$,

$C_{2^i p^{n-\ell}g^k} = \left\{2^i p^{n-\ell}g^k,\ 2^i p^{n-\ell}g^k q,\ \cdots,\ 2^i p^{n-\ell}g^k q^{\lambda(\ell)-1}\right\}$, pour $i = 1,\ 2,\ 0 \leq k \leq \delta(\ell) - 1,\ 1 \leq \ell \leq n$.

Preuve. Si $C_{2^{i_1}p^{n-l_1}g^{k_1}} = C_{2^{i_2}p^{n-l_2}g^{k_2}}$ pour certains $k_1, k_2, \ell_1, \ell_2,$ avec $0 \leq k_i \leq \delta(\ell)-1,\ 1 \leq \ell_i \leq n,$ et $i_1, i_2 \in \{0, 1, 2,\ \}$, puis travailler comme dans le lemma $(3 \cdot 2 \cdot 1)$, on voit ca $\ell_1 = \ell_2 = \ell$ et $i_1 = i_2 = i$.

En outre Si $i = 1$ ou 2 est 0 Travaille maintenant comme dans le lemme$(3 \cdot 2 \cdot 2)$, nous obtenons k_1=k_2.

Si $i = 0$, puis $C_{p^{n-l}g^{k_1}} = C_{p^{n-l}g^{k_2}}$ implique

$$p^{n-\ell}g^{k_1} \equiv p^{n-\ell}g^{k_2}q^j \pmod{4p^n}$$

pour certains $j,$ ce qui donnela congruence a savoire

$$g^{k_1-k_2} \equiv q^j \left(\operatorname{mod} p^l\right).$$

Travaille maintenant comme dans le lemme$(3 \cdot 2 \cdot 1)$, nous obtenons k_1=k_2.

En oura, ce sont tous les classes cyclotomiques modulo $4p^n,$ on donne

$$\begin{aligned}
& |C_0| + |C_{p^n}| + |C_{2p^n}| + \sum_{i=1}^{2}\sum_{\ell=1}^{n}\sum_{k=0}^{2\delta(\ell)-1} \left|C_{2^i p^{n-\ell}g^k}\right| \\
= \ & 4 + \sum_{\ell=1}^{n}\sum_{k=0}^{2\delta(\ell)-1} 2\lambda(\ell) + \sum_{i=1}^{2}\sum_{l=1}^{n}\sum_{k=0}^{\delta(\ell)-1} \lambda(\ell) \\
= \ & 4 + \sum_{\ell=1}^{n} 2\delta(\ell)\lambda(\ell) + \sum_{i=1}^{2}\sum_{l=1}^{n} \delta(\ell)\lambda(\ell) \\
= \ & 4 + \sum_{\ell=1}^{n} 2\phi\left(p^\ell\right) + 2\sum_{\ell=1}^{n} \phi\left(p^\ell\right) \\
= \ & 4 + 4\sum_{\ell=1}^{n} \phi\left(p^\ell\right) = 4p^n.
\end{aligned}$$

$$g^{k_1-k_2} \equiv q^j \,(\mathrm{mod}\, 4)$$

puisque g $\equiv 1\,(\mathrm{mod}\, 4)$ est $q \equiv 3\,(\mathrm{mod}\, 4)$ nous devons avoir ce j est pair ·Soit $j = 2j'$·cela donne

$$g^{k_1-k_2} \equiv q^{2j'} \left(\mathrm{mod}\, p^\ell\right) \cdot$$

puisque f est pair, nous avons $\lambda(\ell)$ est pair et donc les deux congruence a la puissance $\frac{\lambda(\ell)}{2}$ nous obtenons

$$g^{(k_1-k_2)\frac{\lambda(\ell)}{2}} \equiv q^{j\lambda(\ell)'} \equiv 1 \left(\mathrm{mod}\, p^\ell\right) \cdot$$

comme g est un racine primitive modulo p^ℓ, cela donne que $\phi\left(p^\ell\right)$ divise $(k_1 - k_2)\frac{\lambda(\ell)}{2}$, i·e·, $2\delta(\ell)$ divise $(k_1 - k_2)$ ·car $0 \leq k_1, k_2 \leq 2\delta(\ell) - 1$, c'est possible si et seulement si $k_1 = k_2$·

En oura, ce sont tous les classes cyclotomiques modulo 4 p^n, on donne

$$\begin{aligned}
& |C_0| + |C_{p^n}| + |C_{2p^n}| + \sum_{\ell=1}^{n} \sum_{k=0}^{2\delta(\ell)-1} \left|C_{ap^{n-\ell}g^k}\right| + \sum_{i=1}^{2} \sum_{\ell=1}^{n} \sum_{k=0}^{2\delta(\ell)-1} \left|C_{2^i p^{n-\ell}g^k}\right| \\
= \;& 4 + \sum_{\ell=1}^{n} \sum_{k=0}^{2\delta(\ell)-1} \lambda(\ell) + \sum_{i=1}^{2} \sum_{\ell=1}^{n} \sum_{k=0}^{\delta(\ell)-1} \lambda(\ell) \\
= \;& 4 + \sum_{\ell=1}^{n} 2\delta(\ell)\lambda(\ell) + 2\sum_{l=1}^{n} \delta(\ell)\lambda(\ell) \\
= \;& 4 + \sum_{\ell=1}^{n} 2\phi\left(p^\ell\right) + 2\sum_{\ell=1}^{n} \phi\left(p^\ell\right) \\
= \;& 4 + 4\sum_{\ell=1}^{n} \phi\left(p^\ell\right) = 4p^n \cdot
\end{aligned}$$

■

Exemple 3.2.1

Nous donnons maintenant quelques exemples illustratifs avec logiciel matimalica

1) Si $q = 5,\ p = 3,\ n = 1$, alors on trouve

$x^{12}-1 = (1+x)(2+x)(3+x)(4+x)(1+x+x^2)(4+2x+x^2)(4+3x+x^2)(1+4x+x^2)$·

2) Si $q = 3,\ p = 5,\ n = 1$, alors on trouve

$x^{20} - 1 = (1+x)(2+x)(1+x^2)(1+2x+x^3+x^4)(1+x+x^2+x^3+x^4)$

$(1+x+2x^3+x^4)(1+2x+x^2+2x^3+x^4)\cdot$

3) Si $q = 3,\ p = 7,\ n = 1$, alors on trouve

$x^{28}-1 = (1+x)(2+x)(1+x^2)(1+x+x^3+x^5+x^6)(1+x+x^2+x^3+x^4+x^5+x^6)$

$(1+2x+2x^3+2x^5+x^6)(1+2x+x^2+2x^3+x^4+2x^5+x^6)\cdot$

Conclusion

Dans ce mémoire on a présenté les polynômes irréductibles dans le corps fini $\mathbb{F}_q$ et on présenté les cas suivant :

- ▶ définition est quelque proprité de polynôme irréductible·
- ▶ Polynôme irréductible sur un corps fini $\mathbb{F}_q$·
- ▶ Factorisation de $\mathrm{x}^n - 1$ sur $\mathbb{F}_q$ (en cas particuler factorisation de $x^{4p^n} - 1$ sur $\mathbb{F}_q$) ·

Bibliographie

[1] **Bakshi·G·K, Raca·M**, self-dual self-orthogonal megacyclique codes of lenth $2p^n$ over a finite field, Finite fieldes App·19 (1) (2013) 39 − 54·

[2] **Ben bachire·M**, Extension galoisien et quelques applications, Mémoire présenté pour l'obtention du diplôme de master, université de m'sila, 2016·

[3] **Bahache·M et Regouid·A,** Sur les codes cycliques minimaux , Mémoire présenté pour l'obtention du diplôme de master, université de m'sila, 2017·

[4] **Demazure·M**, Cours d'algebre·Primalité, divisibilité, codes, Nouvelle bibloithéque mathématique, Cassini, 1997·

[5] **Gintaras·S**, Calcul du groupe d'automorphismes des codes·Détermination de l'équivalence des codes, Université de limoges, 1999·

[6] **Heboub·L**, Etude de technique de décodage des codes linéaires,Mémoire présenté pour l'obtention du diplôme de magistèr université de m'sila, 2009·

[7] **Larry Joel Galdstein**: Abstact Algebra· A first Course-Printice-Hall, Inc; Englewood Cilffs, New Jersey, 1973·

[8] **Mangalo·C,** Algébre 1· De la théorie de Galois-Edicef-pusaf, paris·1987·

[9] **Mihoubi·C**, Etude sur l'irréductibilité d'une polynôme sur un corps fini, Mémoire présenté pour l'obtention du diplôme de magistèr université de m'sila, 2001·

[10] **Josette·C**: Extension de corps, Théorie de Galois, Elllepses Edition Marcting S·A·2006·

ملخص

يندرج هذا العمل في إطار كثيرات الحدود الغير القابلة للتفكيك على حقل منتهي IF_q.

في هذا البحث نهتم بدراسة كثيرات الحدود الغير القابلة للتفكيك وبعض خواصها كما نتطرق إلى تحليل $x^n - 1$ على حقل منتهي IF_q.

الكلمات المفتاحية : حقل منتهي , كثيرات الحدود الغير القابلة للتفكيك.

Résumé

Ce travail se situe dans le cadre des polynômes irréductibles sur un corps fini IF_q .

Dans cette mémoire on s'intéresse aux polynômes irréductible et certaines de ses propriétés comme nous avons discuté de factorisation de $x^n - 1$ sur un corps finiIF_q .

Mots clés : corps fini, polynômes irréductible sur un corps fini.

Abstract

This Work is included in the frame irréductible polynomial over finite field IF_q .

In this memory we are intersted irréductible polynomial and some of its propretés and factorization of $x^n - 1$ over finite field IF_q .

Key words : finite field , irréductible polynomial over finite field IF_q .