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 : Mathématiques Discrètes.

Par:

REGOUID AFAF

BAHACHE MESSAOUDA

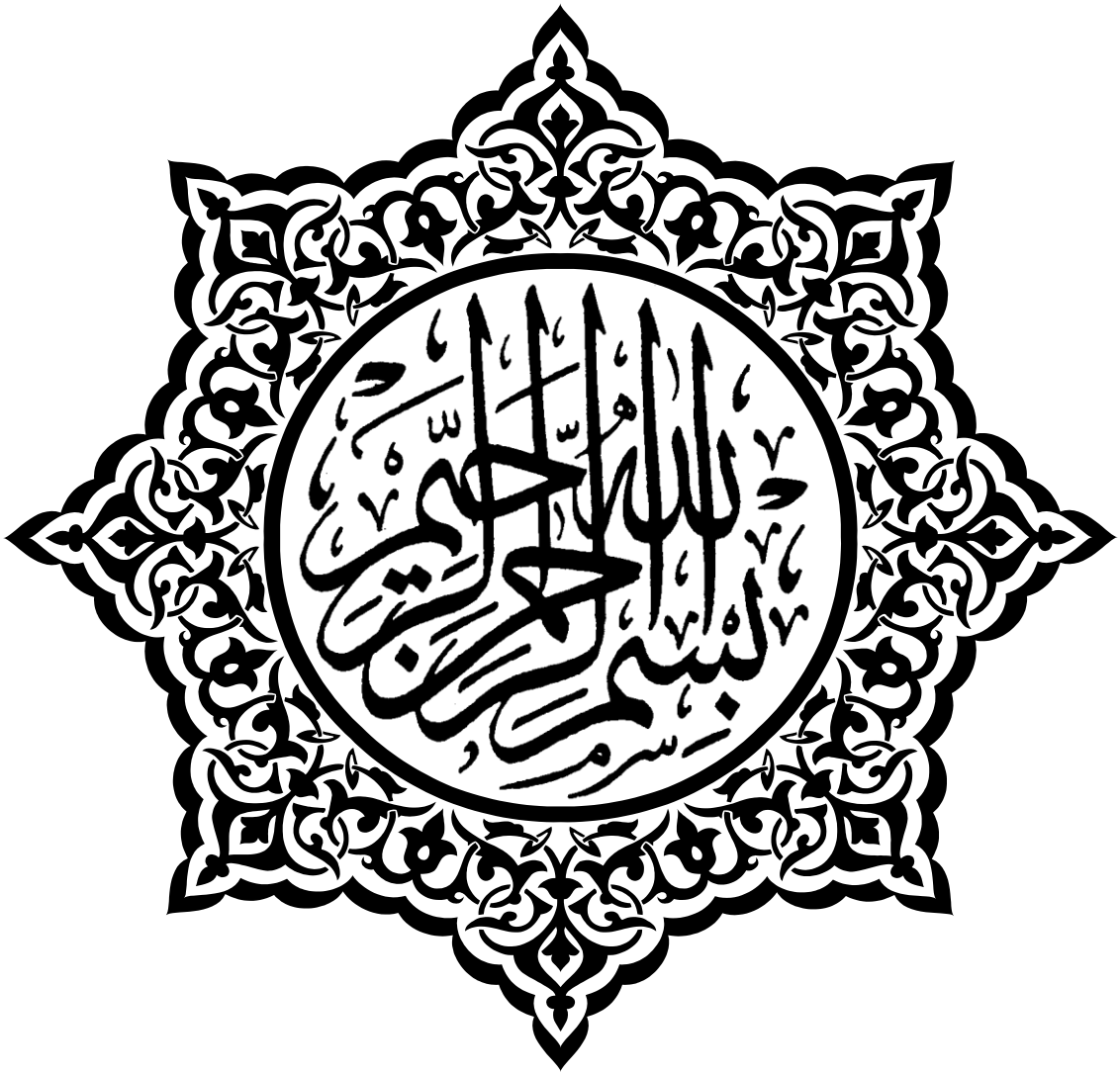
Sujet

SUR LES CODES CYCLIQUES MINIMAUX

Devant le jury :

Mr MIHOUBI Douadi	Prof.	Univ de M'sila	Président
Mr GHADBANE Nacer	M.C.B.	Univ de M'sila	Examinateur
Mr HABOUB Lakhdar	M.A.A.	Univ de M'sila	Rapporteur

Promotion : 2016 / 2017


بسم الله الرحمن الرحيم

Remerciement

Nous voulons exprimer par ces quelques lignes de remerciement notre gratitude envers tous ceux qui par leur présence, leur soutien, leur disponibilité et leur conseils, nous avons eu courage d'accomplir ce travail de mémoire de master 2 mathématiques.

Nous commençons par remercier ***Mr Heboub.L*** *qui nous a fait l'honneur d'être notre encadreur. Nous le remercions profondément pour ses conseils intéressants, son encouragement continu ainsi que le temps qu'il nous a réservé malgré ses grandes occupations.*

Nous remercions également ***Mr Frehtia.N*** *et* ***Mr Merzougui.D*** *pour leurs directives qu'ils nous ont fournies car leur aide précieuse était indispensable pour la réussite de notre projet de fin d'étude.*

Nous tenons d'autre part à remercier les respectueux membres du jury ***Mr Mihoubi.D*** *et* ***Mr Ghadeban.N*** *pour bien vouloir nous accorder de leur temps précieux pour commencer, discuter et juger notre travail.*

Enfin, nous ne pouvons achever ce mémoire sans exprimer notre gratitude à tous les professeurs des mathématiques discrètes pour leur dévouement et leur assistance tout au long de nos études universitaires et à tous ceux qui nous ont appris à lire et à écrire.

Dédicace

C'est avec profonde gratitude et sincères mots,
que nous dédions ce modeste travail de fin d'étude à
nos chers parents ; qui ont sacrifié leur vie pour
notre réussite et nous ont éclairé le chemin par
leurs conseils judicieux.
Nous espérons qu'un jour,
nous pourrons leurs rendre un peu de ce qu'ils ont
fait pour nous, que dieu leur prête bonheur et longue vie.
Nous dédions aussi ce travail à nos frères et
sœurs, nos familles, nos amis,
tous nos professeurs qui nous ont enseigner
et à tous ceux qui nous sont chers.

Notations

$|G|$: L'ordre d'un groupe fini ou le cardinal d'un ensemble fini G.

N : L'ensemble des entiers naturels.

Z : L'ensemble des entiers relatifs.

R : L'ensemble des nombres rééls.

Q : L'ensemble des nombres rationneles.

$\mathbf{Z}/p\mathbf{Z}$: L'ensemble des entiers modulo p.

$C(n,k)$: Code correcteur de longueur n et dimension k.

$\overline{X}$: La classe de X modulo une relation d'équivalence.

k^* : Le groupe multiplicatif d'un corps k avec K^*= K-{0}

F_q : Un corps fini de cardinal q.

$A[x]$: L'anneau des polynômes à une déterminée x sur un anneau.

$(f(x))$: L'idéal engendré par $f(x)$ dans $A[x]$.

$\cong$: Isomorphisme de groupe, de corps, d'espaces vectoriels.

$w(x)$: Le poids de Hamming d'un mots x.

rgH: Le rang d'une matrice H.

$\ker H$: L'espace nul d'une matrice H.

$d(x,y)$: Distance de Hamming entre x et y.

$C^{\perp}$: Le code dual du code considéré.

Table des matières

Introduction

Le transfert d'informations prend de plus en plus d'importance dans notre société que ce soit pour la transmission de photographies de planètes éloignées, pour des communications entre ordinateurs ou encore pour la lecture de nos disques lasers.

Les codes correcteurs d'erreurs sont utilisés pour corriger des erreurs quand les messages sont transmis par le biais d'un canal de communication comportant des parasites.

Dans ce mémoire, on s'intéresse à l'étude de quelques techniques sur les codes cycliques minimaux.

Le premier chapitre est un chapitre d'introduction où nous présentons les notions et les propriétés fondamentales nécessaires pour la réalisation de ce travail tels que : rappel sur les anneaux, anneaux principaux, anneaux des polynômes, corps finis et construction d'un corps finis. Les notions citées dans ce chapitre représentent l'outil mathématique utilise pour l'étude des codes cycliques.

Le deuxième chapitre est consacré à l'étude les codes et étude les codes linéaires, nous étudions les définitions et les propriétés des codes linéaire, puis on va présenter les codes cycliques et aussi nous étudions les définitions et les propiétés sur les codes cycliques.

Enfin, dans le troisième chapitre, on va étudier les codes cycliques minimaux et on achevera nôtre travail par l'étude des éléments minimaux d'une famille, les codes minimaux et les codes cycliques minimaux de longueur $p^n q$ et dimension, polynôme générateur de code minimal de longueur $p^n q$.

Chapitre 1

Les corps finis

Ce chapitre est un chapitre de préliminaires. Il s'agit ici de présenter la terminologie est les principales notations, tout en ciblant les objets étudiés. Les définitions et résultats enoncés constituent la base pour explorer ces objets. D'autre part les corps finis, extension d'un corps fini et enfin construction d'un corps fini.

1.1 Rappel sur les anneaux

Définition 1.1

Un anneau $(A, +, \cdot)$ est un ensemble A muni de deux opérations binaires (lois) notées « + » et « · » telles que :

1. $(A, +)$ soit un groupe abélien.
2. La loi « · » est associative :

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \text{ pour tout } a, b, c \in A.$$

3. La loi « · » est distributive par rapport à « + » :

$$a \cdot (b + c) = a \cdot b + a \cdot c \; et \; (b + c) \cdot a = b \cdot a + c \cdot a \text{ pour tout } a, b, c \in A.$$

Remarque 1.1

a) Les opérations « + » et « · » ne sont pas nécessairement les opérations usuelles sur les nombres.

b) Par convention, on utilise 0_A (appelé « zéro ») pour désigner l'élément neutre du groupe abélien $(A, +)$. L'opposé (l'inverse pour l'addition) de a est noté $-a$. Aussi, $a + (-b)$ est l'abréviation de $a - b$.

c) On écrira ab au lieu of $a \cdot b$, sauf s'il y a un risque d'ambiguité.

Définition 1.2

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

1. A est un anneau unitaire si A posséde un élément neutre e_A pour la loi « $\cdot$ », un élément e est tel que $e \cdot a = a \cdot e = a$ pour tout a de A et appelé « l'unité » de A. On écrira fréquemment 1_A pour désigner l'élément e_A.
2. A est un anneau commutatif si l'opération « $\cdot$ » est commutative.
3. A est un anneau intégre s'il est commutatif (avec élément unité $e \neq 0$) et si l'équation $ab = 0$ implique $a = 0$ ou $b = 0$ pour tout $(a, b) \in A^2$. Cette propriété se traduit en disant que A n'admet pas de diviseurs de zéro.

Exemples 1.1

1. $(\mathbb{Z}, +, .)$ est un anneau commutatif unitaire de même $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$.
2. $2\mathbb{Z} = \{2k \setminus k \in \mathbb{Z}\}$, $(2\mathbb{Z}, +, .)$ anneau commutatif non unitaire.

Idéal d'un anneau

Définition 1.3

Soit A un anneau commutatif. On dit que I est un idéal de A si les deux conditions suivantes sont vérifiées :

1. I est un sous-groupe additif de A.
2. Pour tout $x \in I$ et $y \in A$, le produit $xy \in I$.

Un idéal de A est dit propre s'il est différent de A.

Théorème 1.1

Soit A un anneau ; tout idéal propre de A est inclus dans un idéal maximal.

Idéaux premiers et maximaux

Définition 1.4

Un idéal I de A est premier si $I \neq A$ et $\forall x, y \in A \; x, y \in I \Longrightarrow x \in I$ ou $y \in I$.

Proposition 1.1

A anneau commutatif unitaire intégre, I idéal de A.

$$I \text{ premier} \Longleftrightarrow A/I \text{ intégre.}$$

Définition 1.5

L'idéal I est maximale dans A si $I \neq A$ et si $I \subset J$ alors $J = I$ ou $J = A$.

Exemple 1.2

Les idéaux maximaux dans $\mathbb{Z}$ sont les idéaux $p\mathbb{Z}$ avec p premier. En effet, on a $p\mathbb{Z} \subset d\mathbb{Z}$ si et seulement si $d \mid p$. Donc $p\mathbb{Z}$ est maximal si et seulement s'il n'a pas d'autres diviseurs que $p, -p, 1$ et -1. ce qui équivaut à p premier.

Proposition 1.2

A anneau commutatif unitaire intégre, I idéal de A.

$$I \text{ maximal} \Longrightarrow I \text{ premier.}$$

1.2 Anneaux principaux

Définition 1.6

Soit A un anneau commutatif unitaire.

1. Soient A un anneau et I un idéal de A. On dit que I est principal s'il est engendré par un élément (*i.e.* $\exists\ a \in A$ tel que $I = (a)$).
2. Un anneau A est principal s'il est intègre et si tout idéal de A est principal.

Par exemples $\mathbb{Z}$ et $\mathbb{k}[x]$ (quand $\mathbb{k}$ est un corps) sont principaux.
$A[x]$ = L'ensemble des polynôme en x et à cofficients dans A.

Définition 1.7

Soit A un anneau commutatif unitaire intégre est dit euclidien s'il existe une application : $\varphi : A \setminus \{0\} \to \mathbb{N}$ tel que

i) $\forall\ a, b \in A,\ b \neq 0$, il existe uniqe $(q, r) \in A \times A$ tel que $a = bq + r$, avec $r = 0$ ou $\varphi(r) < \varphi(b)$.

ii) $\varphi(ab) \geq \varphi(a)$.

Exemples 1.3

1. L'anneau $\mathbb{Z}$ est euclidien pour la fonction $\varphi(n) = |n|$.
2. Si $\Bbbk$ est un corps, l'anneau $\Bbbk[x]$ est euclidien pour la fonction '$\varphi(P) = \deg(P)$.

Théorème 1.2

Un anneau euclidien est principal.

Preuve.

Soit I un idéal de A.

Si $I = \{0\}$, alors $I = (0)$.

Supposons que $I \neq \{0\}$, soit $a \in I - \{0\}$ tel que $\varphi(a) = \min\{\varphi(x), x \in I - \{0\}\}$ $a \in I$ alors $(a) \subset I$ ..... (1)

Soit $x \in I$, $\exists\ q, r \in A$ tell que $x = a \cdot q + r$ avec $r = 0$ ou $\varphi(r) < \varphi(a)$.

On a $r = x - a \cdot q \in I$ car I est un idéal et on a $\varphi(r) < \varphi(a)$ est impossible par définition de a .

Donc $r = 0$ d'ou $x = a \cdot q$ et donc $x \in (a)$ alors $I \subset (a)$.....(2)

De (1) et (2) on a $I = (a)$, alors A est principal.

Proposition 1.3

Si A est un anneau intègre, alors tout élément premier non nul est irréductible.

Preuve.

Puisque l'idéal (a) est premier, on a $(a) \neq A$, donc a est non inversible dans A. Si $a = bc$, alors $b \in (a)$ ou $c \in (a)$ puisque (a) est un idéal premier. Si $b \in (a)$, alors $b = ua$, d'où $a = bc = uac$ et $a(1 - uc) = 0$. Puisque l'anneau A est intègre, on a $(1 - uc) = 0$, cequi signifieque c est inversible. Si c'est c qui appartient à (a), le même raisonnement montre que b est inversible.

Proposition 1.4

Soient A un anneau intègre et $a \neq 0$ un élément de A.

1. *Si l'idéal (a) est maximal, l'élément a est irréductible.*
2. *Si A est principal et si a est irréductible, l'idéal (a) est maximal.*

Preuve.

(i) Si l'idéal (a) est maximal il est premier, l'élément a est donc premier, et par conséquent irréductible.

(ii) Supposons que l'élément a soit irréductible et que l'anneau A soit principal.

Supposons qu'il existe un idéal $I = (b)$ de A tel que $(a) \subseteq I$. Alors $a = bc$ et, puisque a est irréductible, b ou c est inversible. Si b est inversible, alors $(b) = A$ et si c est inversible, alors $b = ac - 1$ et $(b) = (a)$. On en déduit que l'idéal (a) est maximal.

Le groupe $(\mathbb{k}^*, \cdot)$ est commutatif (car tout corps fini est commutatif, c'est le théorème de WEDDERBURN) et fini.

1.3 Anneau des polynômes

A anneau commutatif unitaire, x une indéterminée (un symbole).

$$P(x) = a_0 + a_1 x + ... + a_n x^n,\ a_i \in A,\ n \in \mathbb{N}$$

$P(x)$ polynôme d'indéterminée x et à cofficients dans A.

• Si $a_n \neq 0$, on dit que $P(x)$ est de degré n, et on note $d^\circ p = \deg p = n$.

• Si $a_0 = a_1 = ... = a_n = 0$, $P(x) = 0 =$ le polynôme nul, alors par convention $d^\circ p = -\infty$, si $d^\circ p = 0$, p est le polynôme constant.

Anneau quotient

Définition 1.8

A anneau (commutatif unitaire), I un idéal de A.

A/I muni des opération $\oplus$ et $\odot$ est un anneau (commutatif et unitaire) appelé l'anneau quotient de A modulo I.

Exemple 1.4

Soit $\mathbb{k}$ un corps commutatif. On disine par $A = \mathbb{k}[x]$ l'anneau des polynômes à cofficient dans le corps $\mathbb{k}$, $f(x) \in \mathbb{k}[x]$ de dégré n, $I = (f(x)) = \{h(x)f(x) / h(x) \in A\}$. impliqe $A/I = \mathbb{k}[x]/(f(x))$ anneau quotient.

1. $\deg(g) < n = \deg(f)$ donc $\overline{g}(x) = g(x) + I \in A/I$.
2. $\deg(g) \geq n$ Par la dévision euclidienne de g par f dans $\mathbb{k}[x]$, il existe $q(x)$, $r(x) \in \mathbb{k}[x]$ tel que : $g(x) = q(x) \cdot f(x) + r(x)$ $\deg r < \deg f = n$ dans $\mathbb{k}[x]/f$,

$$\overline{g(x)} = \overline{q(x) \cdot f(x)} + \overline{r(x)} = \overline{0} + \overline{r(x)} = \overline{r(x)}.$$

En résumant :

$$\Bbbk[x]/(f) = \{g(x) + I \ / \deg g < \deg f\} = a_0 + a_1 x + ... + a_{n-1}x^{n-1} + I / \ a_i \in \Bbbk\}$$

1.4 Corps finis

Définition 1.9

Un corps est un anneau commutatif unitaire non réduit 0 dans lequel tout élément $x \neq 0$ possède un inverse.

Exemples 1.5

1. L'ensemble des nombres rationnels $\mathbb{Q}$, l'ensemble des nombres réels $\mathbb{R}$ et l'ensemble des nombres complexes $\mathbb{C}$ sont des corps commutatifs.
2. l'ensemble des nombres (réels ou complexes) constructibles à partir de $\{0, 1\}$ est un corps qui contient le corps des nombres rationnels $\mathbb{Q}$.

Définition 1.10

On appelle sous-corps d'un corps $\Bbbk$, un sous-ensemble de $\Bbbk$ qui est lui méme un corps par rapport à l'addition et à la multiplication de $\Bbbk$.

Définition 1.11

Un corps fini est un corps qui posséde un nombre fini d'éléments.

Exemples 1.6

Pour tout entier p premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps à p éléments.

1. Le cardinal de $\Bbbk$ est une puissance de p.
2. Réciproquement, pour tout $n \in \mathbb{N}^*$, il existe un corps $\Bbbk$ de cardinal p^n. De plus, $\Bbbk$ est unique à isomorphisme près.

1.4.1 Caractéristique et cardinal

1. Caractéristique d'un corps

Définition 1.12

Soit $\Bbbk$ un corps commutatif, la caractéristique de $\Bbbk$ est :

Soit le plus petit entier $n > 0$ vérifiant $n \cdot 1_k = 0$ (s'il existe). Soit le zéros (0) dans le cas contraire avec

$$n \cdot 1_k = \underbrace{1 + 1 + ... + 1}_{n\ fois}$$

1_k élément neutre de "$\cdot$" dans $\Bbbk$. *car* $(k) \in \mathbb{N}$.

Théorème 1.3

L'anneau $(\mathbb{Z}_p, +, .)$ *est un corps si et seulement si* p *est un nombre premier.*

Preuve.

$\Rightarrow$) $(\mathbb{Z}_p, +, .)$ est un corps. Si $p = ab$, avec $1 < a, b < n$, alors $b = a^{-1}ab = a^{-1}p = 0\ mod\ p$, contradiction.

$\Leftarrow$) p est un nombre premier. Tout nombre $1 \leq q \leq p-1$ est premier avec p. D'après le théorème de Bezout il existe des entiers u et v tels que $up + vq = 1$ d'où en passant à $\mathbb{Z}_p$, $\overline{vq} \equiv \overline{1}$ et $\overline{q}$ est inversible, donc $(\mathbb{Z}_p, +, .)$ est un corps.

Exemples 1.7

1. $\Bbbk = \mathbb{Q}$, *car* $(\mathbb{Q}) = 0$, $\Bbbk = \mathbb{R}$, *car* $(\mathbb{R}) = 0$, $\Bbbk = \mathbb{C}$, *car* $(\mathbb{C}) = 0$.
2. $\Bbbk = \mathbb{Z}/p\mathbb{Z}$, $p \cdot \overline{1} = \overline{0}$. $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{p-1}\}$

Proposition 1.5

Soit $\Bbbk$ *un corps fini de caractéristique* p *premier.* $\Bbbk$ *a nécessairement* $q = p^n$ *éléments, pour* $n \geq 1$. $\Bbbk$ *contient* $\mathbb{Z}/p\mathbb{Z}$ *appelé le sous-corps premier de* $\Bbbk$. $\Bbbk$ *est un espace vectoriel de dimension* n *sur* $\mathbb{Z}/p\mathbb{Z}$.

Il existe donc une base de n *éléments de* $\Bbbk$ $(e_1, ..., e_n)$ *telle que pour tout* x *dans* $\Bbbk$ *il existe un unique* $(\alpha_1, ..., \alpha_n)$ *dans* $\mathbb{Z}/p\mathbb{Z}$ *tel que*

$$x = \sum_{i=1}^{n} \alpha_i e_i$$

Réciproquement, pour tout nombre premier p *et tout* $n \geq 1$, $q = p^n$, *il existe un corps fini et un seul (à isomorphisme près) à* q *éléments. On le note* $\mathbb{F}_q$, *ou* $GF(q)$.

Proposition 1.6

Soit $\mathbb{F}_q$ *un corps fini avec* $q = p^n$ *, alors on a* $(x + y)^p = x^p + y^p$ *pour tout* $x, y \in \mathbb{F}_q$.

L'application $f : x \longrightarrow x^p$ *est un automorphisme dit de Frobenius :* $f(x+y) = f(x) + f(y)$, $f(xy) = f(x) f(y)$ *et* f *est une bijection. Les éléments tels que* $f(x) = x$ *sont exactement les éléments de* $\mathbb{F}_p \subset \mathbb{F}_q$.

Théorème 1.4

Soit $\Bbbk$ *un corps fini de cardinal* q.

Le groupe multiplicatif $(\Bbbk^*, \cdot)$ *est cyclique d'ordre* $q-1$.

Preuve.

Le groupe $(\Bbbk^*, \cdot)$ est commutatif (car tout corps fini est commutatif, c'est le théorème de WEDDERBURN) et fini. D'après le théorème précédent, ils existent des groupes cycliques $H_1, ..., H_r$ tel que :

$$\Bbbk^* \cong H_1 \times H_2 \times ... \times H_r$$

et pour tout $i = 1, 2, ..., r-1, |H_i|$ divise $|H_{i+1}|$

L'entier $s = |H_r|$ est donc un exposant de chaque élément de $\Bbbk^*$, donc pour tout $x \in \Bbbk^*$, $x^s = 1$; en d'autre terme tout les élément de $\Bbbk^*$ sont racine du polynôme $x^s - 1 \in \Bbbk[x]$ or ce polynôme admet au plus s racines donc

$$|\Bbbk^*| \leq s$$

Mais $|H_r| = s$ divise $|\Bbbk^*|$, d'ou $|H_r| = |\Bbbk^*|$, et comme $\Bbbk^*$ est fini cela entraîne que $\Bbbk^* = H_r$.

2. Cardinal d'un corps finis

Théorème 1.5

Soit $\mathbb{F}$ *un corps fini de caractéristique* p. *Le nombre des élément de* $\mathbb{F}$ *est de la forme*

$$|\mathbb{F}| = p^n.$$

Preuve.

$\mathbb{F}$ est un $\mathbb{F}_p$-espace vectoriel et par hypothèse $\mathbb{F}$ est fini, par conséquent, la dimension de $\mathbb{F}$ en tant que $\mathbb{F}_P$-espace vectoriel est forcement finie. D'ou $|\mathbb{F}_p| = |\mathbb{F}|^n = p^n$.

Donc, un corps fini a forcement p^n éléments où p est un nombre premier.

Remarque 1.2

1. Le cardinal d'un corps fini est une puissance d'un nombre premier.
2. Si $\mathbb{F}_q$ est un corps fini alors $\mathbb{F}_q - \{0\} = \mathbb{F}_q^*$.

Corollaire 1.6

Tout corps $\mathbb{F}$ d'ordre premier p est isomorphe à $\mathbb{Z}_p$.

Elément primitif d'un corps fini

Définition 1.13

Un générateur du groupe multiplicatif $\mathbb{F}_q^*$ est appelé un élément primitif du corps fini $\mathbb{F}_q$.

Soit α un élément primitif d'un corps fini $\mathbb{F}_q$ alors :

$$\mathbb{F}_q = \left\{0, 1, \alpha, \alpha^2, ..., \alpha^{q-2}\right\}.$$

Avec $\alpha^{q-1} = 1$ de plus α^k est primitif si et seulement si k et $q-1$ sont premiers entre eux.

Proposition 1.7

Soit $\mathbb{F}_q$ un corps fini à $q = p^n$ élément, $car(\mathbb{F}_q) = p$, $n \geq 1$ si $a, b \in \mathbb{F}_q$, alors :

$$(a+b)^{p^i} = a^{p^i} + b^{p^i}, \forall i \in \mathbb{N} \ldots\ldots (*)$$

Preuve.

On démontre par récurrence sur i :

$\star$pour $i = 0$ c'est clair

$$\begin{aligned} (a+b)^{p^0} &= a^{p^0} + b^{p^0}. \\ (a+b)^1 &= a^1 + b^1 \cdot (p^0 = 1) \end{aligned}$$

$\star$supposonsque $(*)$ est vraie pour i

$$(a+b)^{p^{i+1}} = \left[(a+b)^{p^i}\right]^p = (a^{p^i} + b^{p^i})^p = (a^{p^i})^p + (b^{p^i})^p = a^{p^{i+1}} + b^{p^{i+1}}.$$

Proposition 1.8

Soient $m, n \in \mathbb{N}^*$, p est premier, on a :

$$\mathbb{F}_{P^m} \subset \mathbb{F}_{P^n} \iff m \mid n.$$

Preuve.

$\Longrightarrow$) On a : $\mathbb{F}_q \subset \mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$

$[\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n}:\mathbb{F}_{q^m}] \cdot [\mathbb{F}_{qm}:\mathbb{F}_q]$

$n = [\mathbb{F}_{q^n}:\mathbb{F}_{q^m}] \cdot m$

$\Longrightarrow m \mid n$

$\Longleftarrow$) $m \mid n \Longrightarrow q^m - 1 \mid q^n - 1$

$\Longrightarrow x^{q^m-1} - 1 \mid x^{q^n-1} - 1$

$\Longrightarrow x^{q^m} - x \mid x^{q^n} - x$

donc $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$.

Exemple 1.8

1. $\mathbb{F}_{2^2} \subset \mathbb{F}_{2^4}$ par contre $\mathbb{F}_{2^2} \nsubseteq \mathbb{F}_{2^3}$ car $2 \nmid 3$.
2. Les sous corps de $\mathbb{F}_{2^{12}}$ sont les sous corps $\mathbb{F}_{2^k}$ tels que $k \mid 12$

   Les diviseurs de 12 sont $1, 2, 3, 4, 6, 12$.

Alors les sous corps de $\mathbb{F}_{2^{12}}$ sont $\mathbb{F}_2$,$\mathbb{F}_{2^2}$,$\mathbb{F}_{2^3}$,$\mathbb{F}_{2^4}$,$\mathbb{F}_{2^6}$,$\mathbb{F}_{2^{12}}$.

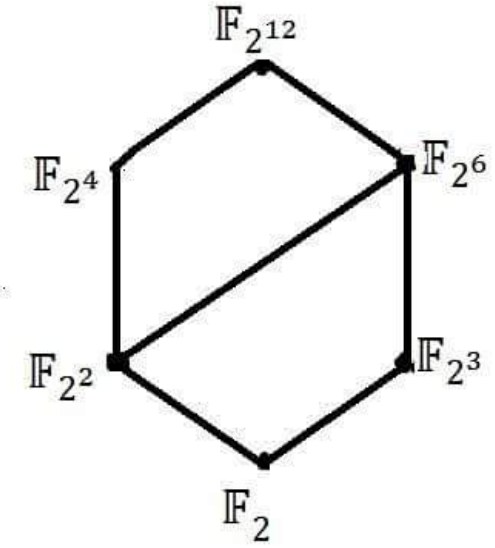


Figure 1.1

1.4.2 Polynômes irréductibles sur un corps fini

Définition 1.14

Un polynôme p de deg ≥ 1 qui n'admet pas de diviseurs propres (autres que lidentité et lui même est appelé un polynôme irréductible).

Exemples 1.9

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

Les polynômes constants ne sont donc ni réductible, ni irréductible.

Proposition 1.9

Un polynome de degré 2 *ou* 3 *sur un corps est irréductible si est seulement si il n'ademet pas des racines.*

Exemple 1.10

$x^2 + x + 1$ est lunique polynome irréductible de degré 2 sur $\mathbb{F}_2$. Donc tout polynome n'ademettent pas des racines dans $\mathbb{F}_2$ et distinct de $(x^2 + x + 1)^2 = 1 + x^2 + x^4$ est irréductible.

1.4.3 Racine de l'unité,polynômes cyclotomiques

Racine de l'unité

Définition 1.15

Soit ζ un nombre complexe, on dit que c'est une racine n-ièmes de l'unité s'il existe un entier n tel que $\zeta^n = 1$. On note μ_n l'ensemble des racines n-ièmes de l'unité.

Cette définition s'étend évidemment au cas d'un corps quelconque.

Définition 1.16

On appelle racine primitive n-ièmes de l'unité un élément de μ_n qui est d'ordre n, c'est-à-dire un générateur de μ_n. On note μ_n^* l'ensemble des racines primitives n-ièmes de l'unité, cet ensemble est de cardinal $\varphi(n)$, où on rappelle que φ est la fonction d'Euler.

L'indicateur d'Euler

Soit n un entier > 0. On note $\varphi(n)$ le nombre des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$, soit

$$\varphi(n) = \#\left((\mathbb{Z}/n\mathbb{Z})^*\right),$$

c'est-à-dire encore le nombre des entiers a premiers à n et tels que $0 \leq a < n$, soit

$$\varphi(n) = \#\{a \ /0 \leq a < n,\ a \text{ premier à } n\}.$$

Dans les lignes précédentes et dans tout le livre, on désigne par $\#E$ le nombre des éléments d'un ensemble fini E. La fonction φ s'appelle l'indicateur d'Euler.

On a

$$\varphi(1) = 1,\ \varphi(2) = 1,\ \varphi(3) = 2,\ \varphi(4) = 2, ...$$

On a toujours $\varphi(n) < n$, sauf pour $n = 1$, et la condition $(n) = n - 1$ équivaut au fait que $\mathbb{Z}/n\mathbb{Z}$ est un corps, donc à la primalité de n.

Polynômes cyclotomiques

Le polynôme ϕ_n

Dans le corps $\mathbb{C}$ des nombres complexes, les racines de l'unité sont les $e^{2\pi ir}$, avec $r \in \mathbb{Q}$. Dire que $e^{2\pi ir}$ est une racine n-ièmes de l'unité signifie que $nr \in \mathbb{Z}$, dire que c'est une racine primitive n-ièmes de l'unité signifie que n est le dénominateur de la fraction r mise sous forme irréductible. Notons que, pour $k \in \mathbb{Z}$, $e^{2\pi ik/n}$ ne dépend que de la classe de k *modulo* n, cela permet de donner un sens à l'expression $e^{2\pi ik}$, n avec $k \in \mathbb{Z}/n\mathbb{Z}$. On obtient ainsi lorsque k parcourt $\mathbb{Z}/n\mathbb{Z}$ les n racines n-ièmes de l'unité, les racines primitives correspondent aux éléments k qui sont inversibles dans $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire aux $\varphi(n)$ éléments du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$.

Définition 1.17

Soit n un entier > 0. On appelle n-ièmes polynôme cyclotomique et on note $\phi_n(x)$ le produit $\prod_{\zeta}(x - \zeta)$ où ζ

parcourt les racines primitives n-ièmes de l'unité dans $\mathbb{C}$.

On a donc

$$\phi_n(x) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^*} \left(x - e^{2\pi ik/n}\right),$$

à comparer avec

$$x^n - 1 = \prod_{k \in \mathbb{Z}/n\mathbb{Z}} \left(x - e^{2\pi i k/n}\right).$$

Proposition 1.10

a) *Le polynôme ϕ_n est un polynôme unitaire à coefficients entiers, de degré $\varphi(n)$.*

b) *On a :* $x^n - 1 = \prod_{d|n} \phi_d(x)$.

Preuve.

La partie a) est claire : il suffit de regrouper les racines n-ièmes de l'unité suivant leur ordre. Par ailleurs, ϕ_n est unitaire et de degré $\varphi(n)$.

La partie b) permet de calculer les $\phi_n(x)$ par récurrence. On obtient par exemple

$$\begin{aligned}
\phi_1(x) &= x - 1 \\
\phi_2(x) &= x + 1 \\
\phi_3(x) &= x^2 + x + 1 \\
\phi_4(x) &= x^2 + 1 \\
\phi_5(x) &= x^4 + x^3 + x^2 + x + 1
\end{aligned}$$

$\star$Si p est premier on a :

$$x^p - 1 = \prod_{d|p} \phi_d(x) = \phi_1(x) \cdot \phi_p(x) = (x-1)\,\phi_p(x)$$

alors

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = \frac{(x-1)\left(x^{p-1} + x^{p-2} + ... + x + 1\right)}{(x-1)} = x^{p-1} + x^{p-2} + ... + x + 1$$

$\star$Si p un nombre premier impair on a :

$x^{2p} - 1 = \prod_{d|2p} \phi_d(x) = \phi_1(x) \cdot \phi_2(x) \cdot \phi_p(x) \cdot \phi_{2p}(x)$

alors

$$\begin{aligned}\phi_{2p}(x) &= \frac{x^{2P}-1}{\phi_1(x)\cdot\phi_2(x)\cdot\phi_P(x)} = \frac{(x^p-1)(x^p+1)}{\phi_2(x)(x^p-1)} \\ &= \frac{x^p+1}{x+1} \\ &= x^{p-1}-x^{p-2}+x^{p-3}-...+x^2-x+1 \\ &= \phi_p(-x)\end{aligned}$$

Définition 1.18

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

$$\phi_n = (x-\alpha_1).....(x-\alpha_{\varphi(n)}) \in \mathbb{F}(\alpha)[x]$$

ou $\alpha_1, \alpha_2, ..., \alpha_{\varphi(n)}$ sont les racines primitives $n^{iéme}$ de l'unité dans $\mathbb{F}(\alpha)$, est appelé le $n^{iéme}$ polynôme cyclotomique sur $\mathbb{F}$, c'est-à-dire ϕ_n à ses coefficient dans $\mathbb{F}_p$. Soit α une racine primitive $n^{iéme}$ de l'unité, alors il résulte que :

$$\phi_n = \prod_i (x-\alpha^i)$$

ou le produit est formé pour tout i avec $p\gcd(i,n)=1$. Le polynôme ϕ est de degré $\varphi(n)$. Soit $n=kd$ ainsi α^k d'ordre d, car $\left(\alpha^k\right)^d = \alpha^{kd} = \alpha^n = 1$, et est une racine primitive $d^{iéme}$ de l'unité. Le $d^{iéme}$ polynôme cyclotomique est de la forme :

$$\phi_d = \prod_{p\gcd(i,n)=1} (x-\alpha^{ik})$$

Toute racine $n^{iéme}$ de l'unité est une racine primitive $n^{iéme}$ de l'unité pour exactement un seul d.

Exemple 1.11

Soit $n=8$ et $\mathbb{F}=\mathbb{F}_3$, et considérons le polynôme x^2+x+2 qui est irréductible sur $\mathbb{F}_3$, pour cela il suffit de voir que tous les éléments de $\mathbb{F}_3$ ne sont pas des racines de ce polynôme. On se donne la peine de trouver une racine primitive huitième de l'unité dans $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+x+2)$, soit α une racine du polynôme

x^2+x+2 c'est à dire $\alpha^2+\alpha+2=0$, d'ou sur $\mathbb{F}_3$, $\alpha^2=2\alpha+1$. Calculons α^k pour $k=3,4,...,8$.

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

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

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

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

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

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

Ainsi

$$\begin{aligned}\mathbb{F}_9 &= \{0,1,2,\alpha,2\alpha,1+\alpha,1+2\alpha,2+\alpha,2+2\alpha\}.\\ \mathbb{F}_9 &= \left\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7\right\}.\end{aligned}$$

Donc α est une racine primitive huitième. Et comme

$$\begin{aligned}\varphi(8) &= |\{m\ /\ 1\leq m\leq n \text{ et } (m,n)=1\}|\\ &= |\{1,3,5,7\}|=4\end{aligned}$$

Les autres racines primitives huitième de l'unité sont $\alpha^3,\alpha^5,et\ \alpha^7$. Ainsi on trouve :

$$\begin{aligned}\phi_8 &= (x-\alpha^1)\left(x-\alpha^3\right)\left(x-\alpha^5\right)\left(x-\alpha^7\right)\\ \phi_8 &= x^4+1.\end{aligned}$$

La factorisation du polynôme x^n-1 joue un rôle important dans la recherche de tous les codes cyclique de longueur n sur $\mathbb{F}_q$. Comme le polynôme générateur d'un code cyclique de longueur n sur $\mathbb{F}_q$ est un diviseur de x^n-1, on est intéressé à déterminer les facteurs.

Théorème 1.7

$$x^n-1=\prod_{d\backslash n}\phi_d \text{ (décomposition cyclotomique)}$$

Un résultat important se déduit pour le polynôme ϕ_{p^m}, pour p premier et m entier positif.

Corollaire 1.8

$$\phi_{p^m} = 1 + x^{p^{m-1}} + \ldots + x^{(p-1)^{m-1}}$$

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

$$\begin{aligned} x^{p^m} - 1 &= \prod_{d \backslash p^m} \phi_d = \phi_1 \phi_p \ldots \phi_{p^m} \\ \phi_{p^m} &= \frac{x^{p^m} - 1}{\phi_1 \phi_p \ldots \phi_{p^{m-1}}} \\ &= \frac{x^{p^m} - 1}{x^{p^{m-1}} - 1} \\ &= 1 + x^{p^{m-1}} + \ldots + x^{(p-1)^{m-1}} \end{aligned}$$

Exemple 1.12

Soit le polynôme $x^{15} - 1$ dans $\mathbb{F}_2$, donnons sa décomposition cyclotomique, comme suivant :

$$x^{15} - 1 = \prod_{d/15} \phi_d = \phi_1 \phi_3 \phi_5 \phi_{15}$$

Où $\phi_1 = x + 1, \phi_3 = x^2 + x + 1, \phi_5 = x^4 + x^3 + x^2 + x + 1$ et $\phi_{15} = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1$.

En effet, de la formule

$$\phi_n = \prod_i \left(x - \alpha^i\right), \text{ ou } p \gcd(i, n) = 1, \text{ avec } 1 \leq i \leq n$$

et comme

$$\varphi(n) = |\{m \ / \ 1 \leq m \leq n \text{ et } (m, n) = 1\}| = |\{1, 2, 4, 7, 8, 11, 13, 14\}| = 8$$

Et la caracteristique 2 de $\mathbb{F}_2$ ne divise pas $1, 3, 5$ et 15 on a d'aprés le définition précédent :

$deg\phi_1 = \varphi(1) = 1$ et $\phi_1 = x + 1$, $deg\phi_3 = \varphi(3) = 2$, et

$$\begin{aligned} \phi_3 &= \frac{x^{3^1} - 1}{x^{3^{1-1}} - 1} \\ &= \frac{x^3 - 1}{x - 1} \\ &= x^2 + x + 1 \end{aligned}$$

$deg\phi_5 = \varphi(5) = 4$, et

$$\begin{aligned}\phi_3 &= \frac{x^{5^1}-1}{x^{5^{1-1}}-1} \\ &= \frac{x^5-1}{x-1} \\ &= x^4+x^3+x^2+x+1\end{aligned}$$

ϕ_1, ϕ_3, ϕ_5 sont irréductible sur $\mathbb{F}_2$. Comme $15/\left(2^4-1\right)$ et $deg\phi_{15} = \varphi\left(15\right) = 8$, on conclut que est le produit de deux polynôme irréductibles de $deg = 4$ à savoir :

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

D'ou l'écriture du polynôme en produit de polynômes irréductibles sur $\mathbb{F}_2$.

1.5 Extension d'un corps fini

Définition 1.19

Soient E et $\mathbb{F}$ deux corps, E est dit extension de $\mathbb{F}$ si E contient un sous-corps isomorphe à $\mathbb{F}$. i.e $\mathbb{F} \subset E$.

Exemples 1.13

$\mathbb{C}$ est une extension de $\mathbb{R}$, $\mathbb{R}$ est une extension de $\mathbb{Q}$. Plus généralement, tout corps commutatif est une extension de son corps premier. $\mathbb{C}$ est donc une extension de $\mathbb{Q}$ s'il est de caractéristique 0 ou une extension de $\mathbb{Z} = p\mathbb{Z}$ s'il est de caractéristique p.

Soit E une extension de $\mathbb{F}$, alors E peut être considérer comme espace véctoriel sur $\mathbb{F}$ selons les lois suivantes :

1. $E \times E \to E$ (addition de E)
   $(x, y) \mapsto x + y$
2. $E \times E \to E$
   $(\lambda, x) \mapsto \lambda x$

C'est-a-dire, E est un $\mathbb{F}$-espace vectoriel.

Définition 1.20

Tout corps $\Bbbk$ contenant le corps $\mathbb{F}$ s'appelle extension de $\mathbb{F}$. $\Bbbk$ est un espace vectoriel sur $\mathbb{F}$ et on a sa dimension $[\Bbbk : \mathbb{F}]$.

Théorème 1.9

Soit $\mathbb{F}$ un corps. Alors ou bien $\mathbb{F}$ est une extension du corps $\mathbb{Q}$ des nombre rationnels, ou bien $\mathbb{F}$ est une extension de $\mathbb{Z}_p$ pour un nombre premier p uniquement dèterminé.

Proposition 1.11

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

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

et

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

alors :

1. *$\mathbb{F}[\alpha]$ est le plus petite 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.*

Proposition 1.12

Soit $\mathbb{F}$ un corps fini et E extention de $\mathbb{F}$ avec $[E:\mathbb{F}] = d$ on a alors $|E| = |\mathbb{F}|^d$.

Preuve.

En effet, soit $\{\alpha_1, \alpha_2, ..., \alpha_d\}$ une base de E sur $\mathbb{F}$, chaque élément de E s'écrit d'une manièire unique comme une combinaisons linéaire de la forme

$$a_1\alpha_1 + a_2\alpha_2 + ... + a_d\alpha_d \text{ avec } \alpha_i \in \mathbb{F}$$

Comme il y a $|\mathbb{F}|$ possibilités pour chaque a_i $(i = 1, 2, ..., d)$ donc on aura $|\mathbb{F}|^d$ combinaisons linéaires différentes est par conséquent

$$|E| = |\mathbb{F}|^d.$$

Extension algébrique

Définition 1.21

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

Exemples 1.14

1. $\mathbb{C} = \mathbb{R}(i)$ est une extension algébrique sur $\mathbb{R}$, $[\mathbb{R}(i) : \mathbb{R}] = 2$.
2. $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ est de même une extension algébrique de degré 4 sur $\mathbb{Q}$.

Extension simple

Définition 1.22

Soit E une extension d'un corps $\mathbb{F}$ et soit α un élement de E n'appartenant pas à $\mathbb{F}$. On appelle extension simple de E le plus petit sous corps de E contenant $\mathbb{F}$ et α, on note $\mathbb{F}(\alpha)$.

Définition 1.23

Une extension simple $E \to \mathbb{F}$ est une extension engendrée par un élément α de $\mathbb{F}$, c'est-à-dire que $\mathbb{F}$ est égal au sous-corps de $\mathbb{F}$ engendré par E et α. Une telle extension est notée $\mathbb{F} = E(\alpha)$.

Exemples 1.15

1. $\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} \setminus a, b \in \mathbb{Q}\right\}$ est une extension simple de $\mathbb{Q}$.
2. Le corps $\mathbb{Q}(i)$ est une extension simple de $\mathbb{Q}$ engendrée par $i \in \mathbb{C}$.
3. Le corps $K[x]$ des fractions rationnelles à une variable sur K est une extension simple de E engendrée par x.

Extension par adjonction

Définition 1.24

Soit E une extension de $\mathbb{F}$, soit S une partie de E, il existe au moins un sous corps de E qui 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 1.3

1. Si $S \subset \mathbb{F}$ alors $\mathbb{F}(S) = \mathbb{F}$.
2. Si $S = \{a_1, a_2, ..., a_n\}$ alors $\mathbb{F}(S)$ note $\mathbb{F}(a_1, a_2, ..., a_n)$.

Exemple 1.16

$\mathbb{C} = \mathbb{R}(i)$, $\mathbb{Q}\left(\sqrt{2}\right)$ extension simple de $\mathbb{Q}$ par adjonction de $\sqrt{2}$. .

Extension finie

Définition 1.25

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

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

Exemples 1.17

1. $[\mathbb{C} : \mathbb{R}] = 2$.
2. $[\mathbb{F}(\alpha) : \mathbb{F}] = \deg \mathbb{F}(\alpha) = \deg(p(x))$ ou $p(x)$ est le polynôme minimale de α.

1.6 Corps de décomposition

Définition 1.26

Le corps L est un corps de décomposition pour le polynôme P et $K[x]$ sur le corps K si les conditions suivantes sont satisfaites :

1. K est un sous-corps de L.
2. P est scindé sur L. c'est-à-dire, en notant $n = \deg(P)$ et en appelant c le coefficient de x^n dans P. qu'il existe des $\lambda_1, ...\lambda_n$ dans L tels que

$$P(x) = c\prod_{i=1}^{n}(x - \lambda_i).$$

3. L est minimal pour cette propriété, c'est-à-dire que s'il existe L' tel que $K \subset L' \subset L$ et que P est scindé sur L', alors $L' = L$. La condition 3 peut aussi se dire $L = K(\lambda_i, ..., \lambda_n)$.

Exemple 1.18

$\mathbb{F}_2$ est un corps de décomposition de $x^2 + x + 1$ sur $\mathbb{F}_2$.

1.7 Construction d'un corps fini

Pour déterminer les éléments d'un corps $\mathbb{F}_q$ on utilise l'anneau quotient $\mathbb{F}_p[x]/(f(x))$, où $f(x)$ est un polynôme irréductible de degré n sur $\mathbb{F}_p$.

Soit un corps fini et $f(x) \in \mathbb{F}_p[x]$un polynôme irréductible de degré n. Alors :

$$\mathbb{F}_p[x]/(f(x)) = \left\{a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + (f(x)) : a_i \in \mathbb{F}_p\right\}$$

est un espace véctoriel sur $\mathbb{F}_p$ de dimension n et de base $\{1, \alpha, \ldots, \alpha^{n-1}\}$, avec $\alpha = [x] = \bar{x} = x + (f(x))$ ou $\bar{\alpha} = 0$.
On sait que le corps fini $\mathbb{F}_{p^n}$ est un espace vectoriel de dimension n sur $\mathbb{F}_p$, de plus, est une extension simple, c-à-d $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$, est tous les $(n+1)$ éléments de $\mathbb{F}_{p^n}$ seront linéarement dépandants.
Donc ils existent $a_0, a_1, \ldots, a_n \in \mathbb{F}_p$ telque :

$$a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$$

Ce qui montre que α est une racine de polynôme

$$a_0 + a_1x + \ldots + a_nx^n \in \mathbb{F}_p[x]$$

Soit $f(x)$un polynôme minimal de α (irréductible unitaire)

$$\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha) \cong \mathbb{F}_p[x]/(f(x))$$

On détermine un polynôme irréductible unitaire de degré n sur $\mathbb{F}_p$, et on construit $\mathbb{F}_p[x]/(f(x))$

Exemple 1.19

Pour déterminer les élément de $\mathbb{F}_{2^3}$ on regarde $\mathbb{F}_{2^3}$ comme une extension simple de degré 3 sur le corps fini $\mathbb{F}_2$, alors cette extension est obtenue par adjonction à $\mathbb{F}_2$ de à $\mathbb{F}_2$ de la racine d'un polynôme de degré 3 irréductible sur $\mathbb{F}_2$. Par exemple, $x^3 + x + 1$ et $x^3 + x^2 + 1$ sont irréductibles sur $\mathbb{F}_2$, par conséquent

$$\mathbb{F}_{2^3} \simeq \mathbb{F}_2[x]/\left(x^3 + x + 1\right) \text{ et aussi } \mathbb{F}_{2^3} \simeq \mathbb{F}_2[x]/x^3 + x^2 + 1)$$

Soit α une racine de $f = x^3 + x + 1$, alors $\{1, \alpha, \alpha^2\}$ forment une base de $\mathbb{F}_{2^3}$ sur $\mathbb{F}_2$, les éléments de $\mathbb{F}_{2^3}$ sont

$$a + b\alpha + c\alpha^2, \text{ où } a, b, c \in \mathbb{F}_2 \text{ et } \alpha^3 + \alpha + 1 = 0$$

Formellement, les polynômes sont les différentes suites finis (, ,) qu'on peut former avec 0 et 1.

	comme un polynôme	comme une puissance de α
000	0	0
100	1	1
010	α	α
001	α^2	α^2
110	$1+\alpha$	α^3
011	$\alpha+\alpha^2$	α^4
111	$1+\alpha+\alpha^2$	α^5
101	$1+\alpha$	α^6

avec $\alpha^3+\alpha+1=0$ et $\alpha^7=1$.

On peut aussi utiliser $g=x^3+x^2+1$ pour déterminer les éléments de $\mathbb{F}_{2^3}$.

Soit β une racine de g, donc $\beta^3+\beta^2+1=0$, et comme $\beta+1$ est une racine de f et $f=x^3+x+1$ dans $\mathbb{F}_2[x]/(g)$ (c-à-d $(\beta+1)^2+(\beta+1)^2=\beta^3+\beta+1$).

L'application Ψ définie par $\Psi(\alpha)=\beta+1$ est un isomorphiseme entre $\mathbb{F}_2[x]/(x^3+x+1)$ et $\mathbb{F}_2[x]/(x^3+x^2+1)$ et $\Psi/\mathbb{F}_2$ est l'identité. Les éléments $\left\{1,\beta+1,(\beta+1)^2\right\}$ forment une base de $\mathbb{F}_2[x]/(g)$ sur $\mathbb{F}_2$.

$$\Psi\left(a+b\alpha+c\alpha^2\right)=a+b(\beta+1)+c(\beta+1)^2, avec\ a,b,c\in\mathbb{F}_2$$

Donc

$$\begin{aligned} F_2[x]/(g) &= \left\{0,1,\beta,\beta+1,\beta^2,\beta^2+\beta,\beta^2+1,\beta^2+\beta+1\right\} \\ &= \left\{0,1,\beta,\beta^2,\beta^3,\beta^4,\beta^5,\beta^6\right\} \end{aligned}$$

avec $\beta^3+\beta^2+1=0$ et $\beta^7=1$.

Exemple 1.20

$\mathbb{F}_{3^2}\simeq\mathbb{F}_3[x]/(g)$, où $g=x^2+x+2$, comme g est irréductible sur $\mathbb{F}_3$, on a $\mathbb{F}_3[x]/(g)=\{a+b\alpha : a,b\in\mathbb{F}_3\}$ et $\alpha^2+\alpha+2=0$, donc les éléments de $\mathbb{F}_3$ sont :

	comme un polynôme	comme une puissance de α

00	0	0
10	1	1
01	α	α
12	$1+2\alpha$	α^2
22	$2+2\alpha$	α^3
20	2	α^4
02	2α	α^5
21	$2+\alpha$	α^6
11	$1+\alpha$	α^7

avec $\alpha^2+\alpha+2=0$ et $\alpha^8=1$.

Polynôme minimal

Définition 1.27

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 1.13

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

Rappelons que l'ordre de α (dans le groupe multiplicatif $\mathbb{F}^*_{q^m}$) est le plus petit entier positif non nul l tel que $\alpha^l=1$.

Lemme 1.10

Soit $\alpha \in \mathbb{F}_{q^m}$. Soit l l'ordre de α. Soit d un entier positif non nul. Alors d est le plus petit entier positif non nul tel que $\alpha^{q^d}=\alpha$ si et seulement si $d=ord_l(q)$.

Preuve.

Notons $r=ord_l(q)$. D'aprés la définition de l'ordre de q modulo l, nous avons $l \mid q^r-1$. Mais $\alpha^l=1$, donc $\alpha^{q^r-1}=1$ et $\alpha^{q^d}=\alpha$. Et r est le plus petit entier positif non nul avec cette propriété, compte tenu de la même définition. Donc r est égal à d si et seulement si d est le plus petit entier positif non nul tel que $\alpha^{q^d}=\alpha$.

Corollaire 1.11

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

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

Preuve.

C'est une conséquence directe de la proposition et du lemme précédent.

Proposition 1.14

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 $\left\{\alpha, \alpha^q, \alpha^{q^2}, \alpha^{q^3}, \ldots, \alpha^{q^{ord_l(q)-1}}\right\}$ est l'ensemble des racines de $M_\alpha(x)$.

Remarque 1.4

La proposition et la corollaire précédent nous montrent que

$$\alpha^{q^{ord_l(q)}} = \alpha.$$

Proposition 1.15

Soit $\alpha \in \mathbb{F}_{q^m}$. Toutes les racines de $M_\alpha(x)$ sont de même ordre.

Conjugaison

Définition 1.28

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

$$\alpha R \beta \quad \text{si} \quad M_\alpha(x) = M_\beta(x) \ .$$

Proposition 1.16

La conjugaison dans $\mathbb{F}_{q^m}$ est une relation d'equivalence.

Définition 1.29

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

Proposition 1.17

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

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

Ils sont distincts deux à deux.

Preuve.

C'est une conséquence directe de la définition précédent et de la proposition dans polynôme minimal.

Remarque 1.5

En résumé, tous les éléments de $\mathbb{F}_{q^m}$ sont divisés en classes d'équivalence pour la conjugaison. Une classe déquivalence est composée de toutes les racines d'un polynôme minimal sur $\mathbb{F}_q$ Donc :

- il y a autant des classes d'équivalence que de polynômes minimaux différents des éléments de il y a autant des classes de $\mathbb{F}_{q^m}$.
- le cardinal de toute classe est égal au degré du polynôme minimal correspondant.

Racines de l'unité

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

Définition 1.30

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

Les racines n-ièmes de l'unité sur $\mathbb{F}_q$ forment un sous groupe du 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, $\left(\beta^{-1}\right)^n = (\beta^n)^{-1} = 1$. Donc les racines n-ièmes de l'unité sur $\mathbb{F}_q$ forment un sous groupe de $\mathbb{F}_{q^m}^*$. Comme $\mathbb{F}_{q^m}^*$ est cyclique, ce sous groupe est aussi cyclique.

Soit u l'entier tel que $n = q^m - 1$. Soit α un 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^u est égal à

$\frac{q^m-1}{(q^m-1,u)} = \frac{q^m-1}{u} = n$. Donc β est un générateur de ce sous-groupe qui est dordre n.

Ce sous-groupe est composé de toutes les racines de x^n-1, i.e. la décomposition de $x^n - 1$ sur $\mathbb{F}_{q^m}$ 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 polynômes minimaux différents des racines n-ièmes de l'unité sur $\mathbb{F}_q$.
- le cardinal de toute classe est égal au degré du polynôme minimal 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

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

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

Cas général Prenons 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 grande 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.

Puisque r est premier avec p, nous pouvons décomposer x^r-1 comme ci-dessus,

et en déduire la décomposition de $x^n - 1$. Plus précisément, si β est une racine r-ième primitive de l'unité sur $\mathbb{F}_q$, alors

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

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,

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

où γ parcourt un ensemble de représentants des classes d'équivalence par conjugaison des racines r-ièmes de l'unité sur $\mathbb{F}_q$.

Classes cyclotomiques

Soit $(n, q) = 1$.

Soit β une racine n-ièmes primitive de l'unité sur $\mathbb{F}_q$. La relation d'équivalence sur les racines n-ièmes de l'unité sur $\mathbb{F}_q$, induit une relation d'équivalence dans l'ensemble $\mathbb{Z}_n$ comme suit : $i, j \in \mathbb{Z}_n$ sont dans la même classe d'équivalence si et seulement si β^i et β^j sont dans la même classe. À la classe de $\gamma = \beta^j$, i.e. la classe $\left\{\gamma, \gamma^q, \gamma^{q^2}, \gamma^{q^3}, \ldots, \gamma^{q^{r-1}}\right\} = \left\{\beta^j, \beta^{jq}, \beta^{jq^2}, \beta^{jq^3}, \ldots, \beta^{jq^{r-1}}\right\}$, correspond la classe des exposants $\{j, qj, q^2j, \ldots, q^{r-1}j\}\ mod\ n$, où r est le nombre de conjugués distincts de β^j. Nous savons que r est le plus petit entier positif non nul tel que $(\beta^j)^{q^r} = \beta^j$, autrement dit, tel que $jq^r \equiv j\ mod\ n$.

Définition 1.31

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

$$Cl(j) = \left\{j, qj, q^2j, \ldots, q^{r-1}j\right\} mod\ n,$$

où r est le plus petit entier positif non nul tel que $jq^r \equiv j\ mod\ n$.

Nous pouvons donc réécrire les résultats. Nous avons que

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

où l est l'ordre de β^j, nous obtenons 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 polynômes minimaux différents des racines n-ièmes de l'unité sur $\mathbb{F}_q$. La formule nous donne

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

où j parcourt un ensemble de représentants des classes cyclotomiques modulo n sur $\mathbb{F}_q$. Donc le nombre de classes cyclotomiques 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 1.32

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 $ord_n(a)$.

Si $a \geq 1$, l'order $ord_n(a)$ de a modulo n est l'order de a dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$.

algorithme de décomposition

1. Détermination du plus petit entier m tel que n divise $q^m - 1$. On en déduit le corps des racines n-ièmes de l'unité sur $\mathbb{F}_q$, soit $L = \mathbb{F}_{q^m}$;
2. Détermination des différentes classes cyclotomiques $(i, iq, iq^2, ..., iq^j, ...)$. Leur nombre est celui des facteurs irréductibles cherchés, et le nombre d'éléments dans une classe est le degré du polynôme correspondant ;
3. Pour chaque classe cyclotomique, détermination du polynôme correspondant. (En utilisant les opérations dans le corps L).

Exemple 1.21

Considérons $x^7 - 1$ sur $\mathbb{F}_2$ on a $n = 7$, $q = 2$ et $m = 3$ car $7 = 2^3 - 1$

Pour les classes cyclotomique modulo 7 on a :

$$\begin{aligned} C_0 &= \left\{0, 2^j\right\} = \{0\} \\ C_1 &= \left\{1, 2^j\right\} = \{1, 2, 4\} = C_2 \\ C_3 &= \left\{3, 2^j\right\} = \{3, 5, 6\} \end{aligned}$$

Les trois polynôme minimaux sont :

$$\begin{aligned} M_0(x) &= (x-1) \\ M_1(x) &= \prod_{j \in C_1} \left(x - \alpha^j\right) = (x-\alpha)\left(x-\alpha^2\right)\left(x-\alpha^4\right) \\ M_3(x) &= \prod_{j \in C_3} \left(x - \alpha^j\right) = \left(x-\alpha^3\right)\left(x-\alpha^5\right)\left(x-\alpha^6\right) \end{aligned}$$

(α une racine 7-ième primitive de l'unité sur $\mathbb{F}_2$).

Pour déterminierles cofficients binaire de $M_1(x)$ et $M_3(x)$, il faut faire des calculs dans $\mathbb{F}_8$, puis que $8 = 2^3$, nous considéronsun polynôme binaire de degré 3 irréductible sur $\mathbb{F}_2$, par exemple $f(X) = x^3 + x + 1$ si α racine primitive de $f(x)$, alors $f(\alpha) = 0$.

On a donc

$$\alpha^3 = \alpha + 1, \alpha^4 = \alpha^2 + \alpha, \alpha^5 = \alpha^2 + \alpha + 1, \alpha^6 = \alpha^2 + 1, \alpha^7 = 1$$

Alors

$$\begin{aligned} M_1(x) &= (x-\alpha)\left(x-\alpha^2\right)\left(x-\alpha^4\right) = x^3 + \left(\alpha + \alpha^2 + \alpha^4\right)x^2 + \left(\alpha^3 + \alpha^5 + \alpha^6\right)x + \alpha^7 \\ &= x^3 + x + 1 \end{aligned}$$

Et on trouve de maniére analogue que

$$M_3(x) = x^3 + x^2 + 1$$

Et la factorisation de $x^7 - 1$ sur $\mathbb{F}_2$

$$x^7 - 1 = (x+1)\left(x^3 + x^2 + 1\right)\left(x^3 + x + 1\right)$$

Chapitre 2

Les codes linéaires et les codes cycliques

Nous rappelons, dans ce chapitre, queleques notions sur la théorie des codes. On à donner la définition des codes, les codes linéaires et aussi les codes cycliques.

2.1 Les codes

Définition 2.1

Soit $A = \{a_1, a_2, \ldots, a_q\}$ un ensemble que nous rappellerons un alphabet de code et soit A^n l'ensemble de toutes les chaines de longueur n sur A.
Nous dirons que chaque sous-ensemble $C \subset A^n$ s'appelle un code. Chacune des chaines c de C est appelée mot du code. De plus, nous dirons qu'un code $C \subset A^n$ est de cardinalité M si $M = |C|$.

La dimension n de A^n est appelée la longeur du code. Un code de longueur n contenant M mots sera appelé un (n, M) code. Le corps fini à q élément sera noté $\mathbb{F}_q$. L'éspace vectoriel de dimension n sur $\mathbb{F}_q$ sera noté $\mathbb{F}_{q^n}$.

Exemples 2.1

i) $C_1 = \{122, 211, 111\}$ est un code de longeur 3 et de cardinale 3 sur $A_1 = \{1, 2\}$.

ii) $C_2 = \{aaaa, zrtu, bcde, aabb\}$ est un code de longeur 4 et de cardinal 4 sur A l'alphabet de la langue Latin.

iii) exemple pour le code de répitition : Soit C un code de longueur $n = kr$, de cardinal $M = q^k$ et de distance minimal $d = r$. Il détecté $r - 1$ erreurs, et il corrige $\left[\frac{r-1}{2}\right]$.

On prend : $q = 2$, $r = 3$, $k = 3$, le message $101 \in \mathbb{F}_2^3$ est codé par le mot de code 111000111, il détecté 2 erreurs et il corrige *une* erreur.

Distance de Hamming

Définition 2.2

La distance de Hamming entre deux mots $x = (x_1, x_2, \ldots, x_n)$ et $y = (y_1, y_2, \ldots, y_n)$, que l'on notera $d(x, y)$ est le nombre d'indice i tels que $x_i \neq y_i$, c'est-à-dire :

$$d(x, y) = |\{i \ / \ x_i \neq y_i\}| .$$

On remareque que la distance de Hamming est une vraie distance au sens numérique de terme. Rappelons briévement les propiétés d'un distance $d(x, y)$, faciles à vérifié sur d.

1. $d(x, y) = d(y, x) \geq 0$
2. $d(x, y) = 0$ si et seulement si $x = y$.
3. $d(x, y) \leq d(x, z) + d(z, y)$.

Exemples 2.2

i) Nous avons $d(122, 111) = 2$ et $d(211, 111) = 1$ pour l'exemple 2.1.i).

ii) $d(aaaa, aabb) = 2$ et $d(zrtu, bcde) = 4$ pour l'exemple 2.1.ii).

Distance minimale d'un code

Définition 2.3

La distance minimale d'un code C est la distance minimum entre deux mots distincts de code. On la note d :

$$d = \min\{d(x, y)/x, y \in C \text{ et } x \neq y\}$$

Par exemple, $d(0011, 0010) = 1$, $d(1120, 2200) = 3$.

Le poids de Hamming

Définition 2.4

Le poids de Hamming d'un mots $x = (x_1, x_2, \ldots, x_n)$, noté $\omega(x)$, est le nombre d'indices i tels que $x_i \neq 0$

$$\omega(x) = |\{i \ / \ x_i \neq 0\}|$$

Nous pouvons remarquer que le poids $\omega(x) = d(x, 0)$.

Par exemple, dans $\mathbb{F}_{2^4}$. Nous avons $\omega(1101) = 3$ et $\omega(0011) = 2$.

Proposition 2.1

Un code C de distance minimale d corrige au plus $e = \left[\frac{d-1}{2}\right]$ erreurs et en détecte $d-1$.

2.2 Codes linéaires

Définition 2.5

Un code linéaire de dimension k et de longueur n sur $\mathbb{F}_q$ est un sous espace vectoriel de dimension k de $\mathbb{F}_{q^n}$.

Si la distance minimale de C est d, on dit que C est un code de paramètre $[n, k, d]$, et si $q = 2$ le code C est dit code binaire.

Pour un code linéaire C, on retrouve la distance de Hamming par la formule $d(x, y) = \omega(x - y)$, et la distance minimale du code C par

$$d = \min\{\omega(x)/x \in C \ et \ x \neq 0\}$$

Matrice génératrice

Définition 2.6

Une matrice génératrice du code C est une matrice G à k lignes et n colonnes, dont les lignes formet une base de C, tels que

$$C = \left\{c \in \mathbb{F}_{q^n} \ / \ \exists x \in \mathbb{F}_{q^k} : c = xG\right\}$$

Définition 2.7

La matrice G est appelée la matrice génératrice de C et tout les vecteurs de C sont appelés les mots code de C .

Remarque 2.1

- Le rang de la matrice génératrice G est k.
- À partir de la matrice génératrice G, on peut aussi considérer la code linéaire $C = C(n,k)$ comme l'image d'un application linéaire f telle que

$$\begin{array}{lll} f : \mathbb{F}^n & \rightarrow & \mathbb{F}^n \\ a & \rightarrow & f(a) = aG \end{array}$$

L'application f est appelée la fonction de codage et a la mot d'information.

Exemple 2.3

Soit G la matrice génératrice du $[4,2]$ code binaire C telle que :

$$G = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Déterminions

$$\begin{array}{lll} C & = & \{c_1(0,1,1,1) + c_2(1,0,0,1) / c_1, c_2 \in \mathbb{F}_2\} \\ C & = & \{0000, 1001, 0111, 1110\} \end{array}$$

Ainsi le code C est de paramètre $[4,2,2]$ et $|C| = q^k = 2^2 = 4$, et par exemple le message 11 est codé par $c = 11G = 1110$

Matrice de contrôle

On peut aussi se donner un sous -espace vectoriel par un système d'équations indépendants. Une matrice de contrôle d'un code linéaire C est la matrice d'un système d'équations linéaires homogénes indépendantes dont l'éspace des solutions est C.

Définition 2.8

Une matrice de contrôle H d'un code linéaire C est une matrice de taille $n \times (n-k)$ et de rang $(n-k)$ vérifiant :

$$C = \left\{ \ c \in \mathbb{F}_{q^n} \ \setminus \ H \ {}^t c = 0 \right\}$$

Exemple 2.4

Pour obtenir le code C a partir de la matrice de contrôle H on calcul tout d'abord l'espace nul de G, $y \in \mathbb{F}_{2^4}$. Alors $y \in$ l'espace nul de G ssi $Gy^t = 0$

$$Gy^t = 0 \Leftrightarrow \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = 0 \Leftrightarrow \begin{cases} y_1 + y_2 = 0 \\ y_2 + y_3 + y_4 = 0 \\ y_1 + y_3 = 0 \end{cases} = 0$$

Les solutions du système sont $\{0000, 1110\}$.

Donc la base est $\{1110\}$et la matrice $H = [1110]$

Soit

$$\varphi_H \quad : \quad \mathbb{F}_{2^4} \quad \rightarrow \quad \mathbb{F}_2$$

$$(x_1, x_2, x_3, x_4) \rightarrow (1110) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

$$\varphi_H (x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3$$

et par conséquent, on a

$$C = \ker \varphi_H = \{x \in \mathbb{F}_{2^4} : x_1 + x_2 + x_3 = 0\} \text{ on a par exemple}$$

$$1111 \notin C \text{ car } 1+1+1 \neq 0, \ 0111 \in C \text{ car } 0+1+1 = 0.$$

Proposition 2.2

La distance minimale d'un code linéaire $C = C(n,k)$ est le plus petit poids des mots code non nul

$$d = \min_{u \in C - \{0\}} \omega(u)$$

Code dual

La contrainte de la linéarité sur le code donne naturellement naissance à la notion de code dual d'un code linéaire. Puisque C est un espace vectoriel, on peut considérer l'ensemble des formes qui s'annulent sur C. Cet ensemble est un espace vectoriel que l'on appelle code dual de C.

Définition 2.9

Soit C un $[n, k, d]$-code linéaire. Soit $\langle ., . \rangle$ le produit scalaire euclidien usuel : $\langle u, v \rangle = \sum_{i=1}^{n} c_i v_i$. Le code dual note $C^{\perp}$ est donc un code linéaire de la même longueur. Sa dimension est $n - k$

$$C^{\perp} = \{v \in \mathbb{F}_{q^n} \ : \ \forall c \in C : \langle u, v \rangle = 0\}$$

Il découle directement des définitions que si H est une matrice génératrice de $C^{\perp}$, elle est communément appelée matrice de contrôle du code C. De même, une matrice génératrice de C est une matrice de contrôle de $C^{\perp}$.

Exemple 2.5

Soit le code $C = \{000, 011, 101, 110\}$ de longueur 3 sur F_2 le dual $C^{\perp}$ de C est

$$C^{\perp} = \{y \in \mathbb{F}_{2^3} \ : y = abc \ , \forall c \in C : \langle c, y \rangle = 0\}$$

donc $y = 111$ ou $y = 000$ d'ou $C = \{000, 111\}$

2.3 Codes cycliques

Les codes cycliques forment une sous-classe des codes linéaires, et sont les plus utilisés en pratique. Ils conjugent en effet de nombreux avantages : leur mise en ouvre (codage / décodage) est facile, ils offerent une gamme étendue de code, avec de nombreux choix de paramètre $[n, k, d]$, et enfin permettent de corriger différents types d'erreurs .

On définit la fonction " décalage" sur $\mathbb{F}_{q^n}$, qui est une permutation circulaire des coordonnées :

$$\begin{array}{lcl} \mathbb{F}_{q^n} & \rightarrow & \mathbb{F}_{q^n} \\ \sigma : (c_0, c_1, c_2, ..., c_{n-1}) & \rightarrow & (c_{n-1}, c_0, c_1, c_2, ..., c_{n-2}) \end{array}$$

Définition 2.10

Un code linéaire C de longueur n est cyclique s'il vérifier la propriété suivante :

$$\text{Si } x_1...x_n \in C, \text{ alors } x_n x_1...x_{n-1} \in C$$

Définition 2.11

Soit C un code linéaire sur $\mathbb{F}_{q^n}$. On dit que C est cyclique si $\sigma(C) = C$.

La transformation σ est d'ordre n, c'est à dire n la plus petit entier tel que $\sigma^n = id$.

Exemples 2.6

1. le code $C = \{000, 110, 011, 101\}$ est un code cyclique.
2. Le code $C = \{0000, 1001, 0110, 1111\}$ n'est pas cyclique. Il est cependant équivalent à un code cyclique (il faut échanger les troisième et quatrième coordonnées).

Tout mot $c = (c_0, c_1,..., c_{n-1})$ d'un code C sur $\mathbb{F}$ peut être identifié à un polynôme $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ de $\mathbb{F}[x]$. Pour pouvoir construire des codes cycliques, l'anneau à considérer est $R_n = \mathbb{F}[x]/(x^n - 1)$.

En effet, dans cet anneau, on peut réduire tout polynôme modulo $x^n - 1$ en remplaçant simplement x^n par 1, x^{n+1} par x et ainsi de suite. Le code C est alors un sous ensemble de R_n. Observons ce qu'il se passe lorsque l'on multiplie $c(x)$ par x dans R_n :

$$\begin{aligned} x.c(x) &= c_0x + c_1x^2 + \cdots + c_{n-1}x^n \\ &= c_{n-1} + c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1}. \end{aligned}$$

La multiplication par x correspond à un décalage circulaire. La multiplication par x^m correspond à m décalages circulaires.

Théorème 2.1

Un code cyclique de $\mathbb{F}_{q^n}$ est un idéal de l'anneau $\mathbb{F}_q[x]/(x^n - 1)$.

Preuve.

Soit l'application

$$\begin{aligned} \varphi &: \mathbb{F}_{q^n} \to \mathbb{F}_q[x] \to \mathbb{F}_q[x]/(x^n-1) \\ &: c \to c(x) \to c(x) \mod x^n - 1 \end{aligned}$$

qui associe à un mot

$$c = (c_0, c_1, .., c_{n-1})$$

le polynôme

$$c(x) = c_0 + c_1 x + ... + c_{n-1} x_{n-1}$$

φ est un isomorphisme de $\mathbb{F}_q$-espaces vectoriels.

Dans $\mathbb{F}_q[x]/(x^n-1)$, la multiplication par x correspond à la permutation circulaire des cofficients. Ainsi, pour tout $u \in \mathbb{F}_{q^n}$, on a

$$\varphi(\sigma(u)) = x\varphi(u)$$

un code C est stable par σ si et seulement si

$$x\varphi(C) = \varphi(C)$$

Comme d'autre part un code linéaire et aussi un $\mathbb{F}_q$-espace vectoriel, il est stable par σ si et seulement si son image par φ est un idéal de $\mathbb{F}_q[x]/(x^n-1)$.

Exemple 2.7

1. Le code linéaire

   $$C = \{000, 011, 101, 110\}$$

   est un code cyclique car $011 \in C \Rightarrow 101 \in C$, $101 \in C \Rightarrow 110 \in C$ et $110 \in C \Rightarrow 011 \in C$. La représentation polynomiale de 011 est $x + x^2$.

2. Le code linéaire C=$\{01010, 10101, 11111, 00000\}$ n'est pas cyclique. Par example, $01010 \in C$ mais $00101 \notin C$.

Rappelons aussi que

$$(f(x)) = \{r(x)f(x) \ / \ r(x) \in R_n\}$$

L'idéal engendre par $f(x)$.

Théorème 2.2

Pour tout $f(x) \in R_n$ l'ensemble $(f(x))$ est un code cyclique dit engendré par $f(x)$.

Preuve.

1. si $a(x)f(x) \in (f(x))$ et $b(x)f(x) \in (f(x))$ alors $a(x)f(x) + b(x)f(x) = (a(x) + b(x))\, f(x) \in (f(x))$.
2. si $a(x)f(x) \in (f(x))$ et $r(x) \in R_n$ alors $r(x)\,(a(x)f(x)) = (r(x)a(x))f(x) \in (f(x))$.

Code engendré par le polynôme de contrôle

Définition 2.12

Le code engendré par $h(x)$ est équivalent au code dual de C. C'est un code cyclique de dimension $n - dimC = \deg g(x)$. Pour

$$h(x) = h_0 + h_1 x + ... + h_k x^k$$

on peut construire sa matrice H :

$$H = \begin{pmatrix} 0 & \dots & \dots & 0 & h_k & \dots & h_1 & h_0 \\ 0 & \dots & 0 & h_k & \dots & h_1 & h_0 & 0 \\ \vdots & \ddots & & & & & \ddots & \vdots \\ 0 & & & & & & & \\ h_k & \dots & & h_1 & h_0 & 0 & \dots & 0 \end{pmatrix}$$

Théorème 2.3

Soit C un code cyclique dans R_n

1. *il existe un polynôme unique (unitaire) $g(x)$ de degré minimal dans C.*
2. *$C = (g(x))$*
3. *$g(x)$ est facteur de $x^n - 1$.*

Preuve.

1. supposons $g(x)$ et $h(x)$ deux polynômes unitaire de degré minimales alors $h(x), g(x) \in C$ et ayant un degré minimal ceci conduit à une contradiction. Si $g(x) \neq h(x)$ ainsi $g(x)h(x)$ est dans C et de degré inférieur à $\deg g(x)$.
2. Supposons $a(x) \in C$, par l'algorithme de division par $g(x)$, $a(x) = q(x)g(x) + r(x)$ où $\deg r(x) < \deg g(x)$ mais $r(x) = a(x) - q(x)g(x) \in C$. On doit avoir $r(x) = 0$ et ainsi $a(x) \in (g(x))$.
3. En appliquant l'algorithme de division :

$$x^n - 1 = q(x)g(x) + r(x) \text{ ou } \deg r(x) < \deg g(x)$$

mais

$$r(x) = -q(x)g(x) \pmod{x^n - 1} \text{ et ainsi } r(x) \in (g(x)).$$

Pour la minimalité de degré de $g(x)$, on doit avoir $r(x) = 0$ ce qui implique $g(x)$ est un facteur de $x^n - 1$.

Théorème 2.4

Soit C un code cyclique de polynôme générateur $g(x) = g_0 + g_1x + g_2x^2 + \ldots + g_rx^r$ avec $\deg g(x) = r$.

Alors, $\dim C = k = n - r$ et sa matrice génératrice est :

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \ldots & g_t & 0 & \ldots & \ldots & 0 \\ 0 & g_0 & g_1 & \ldots & \ldots & g_t & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & g_0 & g_1 & g_2 & \ldots & g_t & 0 \\ 0 & \ldots & \ldots & 0 & g_0 & g_1 & g_2 & \ldots & g_t \end{pmatrix} = \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ \vdots \\ x^{k-1}g(x) \end{bmatrix}$$

Preuve.

Les $n - r$ lignes de la matrice G sont nécessairement linéairement indépendantes. Ces $n-r$ lignes représentent les mots du code, $g(x), xg(x), \ldots\ldots, x^{n-r-1}g(x)$.

Il reste à montrer que chaque mot de code dans C s'exprime à l'aide déceux-ci.

Le théorème précédent montre que si $a(x)$ est un mot de code on $a(x) = g(x)q(x)$, pour un polynôme $q(x)$ et que ceci est une égalité de polynôme dans $\mathbb{F}_q[x]$, qui ne requiert aucune réduction modulo $x^n - 1$ ainsi $\deg a(x) \prec n$ il s'en

suit que $\deg q(x) \prec n-r$ d'où :

$$\begin{aligned} g(x)q(x) &= \left(q_0, q_1x, \ldots\ldots, q_{n-r-1}x^{n-r-1}\right) g(x) \\ &= q_0g(x) + q_1xg(x) + \ldots\ldots + q_{n-r-1}x^{n-r-1}g(x). \end{aligned}$$

Laquelle est la combinaison linéaire désirée.

Exemple 2.8

Le code de Hamming de paramètre $(7, 4, 3)$ et de polynôme générateur $g(x) = 1 + x + x^3$ admet pour matrice génératrice :

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Théorème 2.5

Soit $h(x)$ le polynôme de contrôle d'un code linéaire cyclique C dans R_n.

a) *le code C peut être représenté par :*

$$C = \{p(x) \in R_n \ / \ p(x)h(x) = 0\}$$

b) *soit $h(x) = h_0 + h_1x + \ldots + h_{n-r}x^{n-r}$ alors une matrice de contrôle du code C est donnée par*

$$H = \begin{bmatrix} h_{n-r} & \ldots & & \ldots & h_0 & 0 & \ldots & \ldots & 0 \\ 0 & h_{n-r} & \ldots & \ldots & \ldots & h_0 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & h_{n-r} & \ldots & & \ldots & h_0 & 0 \\ 0 & \ldots & \ldots & 0 & h_{n-r} & \ldots & & \ldots & h_0 \end{bmatrix}$$

Exemple 2.9

Considérons le code binaire $C\,(7, 4)$ généré par $g(x) = 1 + x + x^3$ sa matrice génératrice est composée à partir du polynôme générateur

$$g(x) = g_0 + g_1x + g_2x^2 + \ldots + g_rx^r$$

est

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & g_3 & 0 & 0 & 0 \\ 0 & g_0 & g_1 & g_2 & g_3 & 0 & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & g_3 & 0 \\ 0 & 0 & 0 & g_0 & g_1 & g_2 & g_3 \end{pmatrix}$$

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Calculer la matrice de contrôle à partir de la matrice génératrice n'est pas en généralaisé, par contre, on peut facilement trouver le polynôme de contrôle $h(x)$ qui est telque :

$$h(x)g(x) = 0$$

et donc

$$\begin{aligned} h(x) &= \frac{x^7 - 1}{1 + x + x^3} \\ &= x^4 + x^2 + x + 1 \end{aligned}$$

et la matrice de contrôle correspondant est

$$\begin{aligned} H &= \begin{pmatrix} h_4 & h_3 & h_2 & h_1 & h_0 & 0 & 0 \\ 0 & h_4 & h_3 & h_2 & h_1 & h_0 & 0 \\ 0 & 0 & h_4 & h_3 & h_2 & h_1 & h_0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \end{aligned}$$

Pour encoder 0111 en utilisant le produit polynomial, on doit multiplier le polynôme $m(x) = x^3 + x^2 + x$ correspondant par $g(x) = 1 + x + x^3$.

On obtient

$$\begin{aligned} c(x) &= m(x)g(x) = \left(x^3 + x^2 + x\right)\left(1 + x + x^3\right) \\ &= x^6 + x^5 + x \\ &= c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0 \end{aligned}$$

Qui correspondant au mot code $c_0c_1c_2c_3c_4c_5c_6 = 0100011$.

2.4 Construction d'un code cyclique

Pour construire un code cyclique de longueur n, il est utile de connaître la décomposition de $x^n - 1$ en polynômes irréductibles sur le corps de base $\mathbb{F}$:

$$x^n - 1 = \prod_i f_i(x).$$

En l'absence d'un logiciel (maple, magma,...), on peut déterminer les classes cyclotomiques modulo n. Le nombre de classes donne le nombre de facteurs irréductibles. La donnée d'un polynôme irréductible diviseur de $x^n - 1$ permet alors de connaître tous les autres facteurs. Le polynôme générateur du code est un produit d'un certain nombre de facteurs trouvés.

Exemple 2.10

Combien peut-on construire de codes cycliques $[31, 21]$ sur $\mathbb{F}_2$?

Il suffit de déterminer les classes cyclotomiques modulo 31. Il existe 7 classes cyclotomiques, chacune contenant 5 éléments

$$\begin{aligned} C_0 &= \{0\} \\ C_1 &= \{1, 2, 4, 8, 16\} \\ C_3 &= \{3, 6, 12, 24, 17\} \\ C_5 &= \{5, 10, 20, 9, 18\} \\ C_7 &= \{7, 14, 28, 25, 19\} \\ C_{11} &= \{11, 22, 13, 26, 21\} \\ C_{23} &= \{23, 15, 30, 29, 27\} \end{aligned}$$

Il existe 6 facteurs de degré 5 et un facteur de degré 1 : $(x - 1)$. Le polynôme générateur d'un code $[31, 21]$ doit être de degré 10. Il y a $\binom{6}{2} = 15$ possibilités. Pour pouvoir factoriser effectivement $x^{31} - 1$ il faut connaître un polynôme irréductible de degré 5 (en effet $31 = 2^5 - 1$). Il existe des tables qui donnent des polynômes irréductibles ou primitifs de degré donné sur $\mathbb{F}_2$.

Chapitre 3

Les codes cycliques minimaux

3.1 Éléments minimaux d'une famille

Définition 3.1

Dans cette partie, nous considérons un corps fini $\mathbb{F}$ (pas nécéssairemment $\mathbb{F}_2$ ou une extension) et un entier naturel n. Soit ξ une famille de sous ensembles de $\mathbb{F}^n$. Ici, nous n'imposons pas que les éléments sont des codes (des sous espace vectoriels). Par contre, nous imposons que $C \in \xi$.

Nous munissons cette famille de la relation d'ordre la plus naturelle, l'inclusion $\subset$. Nous obtenons ainsi une famille partiellement ordonnée $(\xi, \subset)$.

Définition 3.2

Soit C un élément de $\xi \setminus \{0\}$. C est appelé un élément minimal de ξ si :

$$(D \subset C \text{ et } D \in \xi) \Longrightarrow (D = C \text{ ou } D = \{0\}).$$

En d'autres mots, C est un élément minimal de ξ s'il n'existe pas de code entre C et $\{0\}$ dans $(\xi, \subset)$.

Remarque 3.1

Notons que, puisque ξ est une famille finie, le nombre d'éléments minimaux de ξ est fini.

Définition 3.3

On note $\xi_{\min} = \{C_1, ..., C_r\}$ l'ensemble des éléments minimaux de $(\xi, \subset)$.

Remarque 3.2

Si ξ n'est pas réduit à $\{0\}$, ξ possède au moins un élément minimal.

Proposition 3.1

Soit C un élément de ξ $(C \neq \{0\})$.Alors, il existe $i \in \{1, ..., r\}$ tel que :

$$C_i \subset C.$$

Ce résultat découle de la définition d'élément minimal.

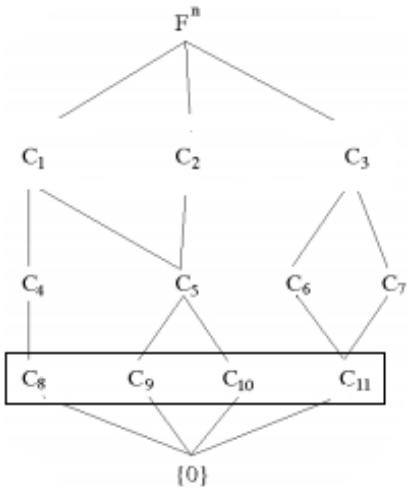


Figure 3.1

Exemple 3.1

Ce schéma se lit de la maniére suivante : un élément C est relié à un élément D placé plus haut si et seulement si $C \subset D$.

Dans cet exemple, $\{0\} \subset C_8 \subset C_4 \subset C_1 \subset \mathbb{F}^n$.

3.2 Codes minimaux

Définition 3.4

Si $x^n - 1 = g_1 ... g_t$ est la factorisation complete de $x^n - 1$, on facteur irréductible diffirent sur $\mathbb{F}_q$, alors les codes cycliques $\left(\frac{x^n-1}{g_i}\right)$ engendres par les polynômes $\frac{x^n-1}{g_i}$ sont appelés les codes cycliques minimaux.

Définition 3.5

Soit C une famille de codes linéaires sur $\mathbb{F}$ de longueur n contenant le code trivial $\{0\}$.

L'inclusion $\subset$ est une relation d'ordre sur C. On a donc la notion d'éléments minimaux : un élément $c \in C$ est dit minimal si, dés que l'on a $c \subsetneq D$ et $D \in C$, alors $D = \{0\}$.

Soit $C_{\min} = \{C_1, C_2, \ldots, C_r\}$ l'ensemble des élément minimaux de $(C, \subset)$.

Ainsi, pour tout $c \in C$, $c \neq 0$, il existe $i \in \{1, \ldots\ldots, r\}$ telque

$$c_i \subset c$$

On a la bijection suivante :

$$\begin{array}{lcl} \phi : \{\text{diviseurs de } x^n - 1\} & \rightarrow & \{\text{codes cycliques de longeur } n\} \\ g(x) & \mapsto & \langle g(x) \rangle \end{array}$$

Si on considère C la famille des codes cycliques de longeur n,

$$C_{\min} = \phi \left(\langle \frac{x^n - 1}{g(x)} \rangle \right), \ g(x) \text{ polynôme irréductible}$$

Si on note $g_1(x), \ldots\ldots, g_r(x)$ les facteurs irréductibles de $x^n - 1$, alors

$$C_{\min} = \left\{ c_i := \ \langle \frac{x^n - 1}{g_i(x)} \rangle, \ i = 1 \ldots r \right\}$$

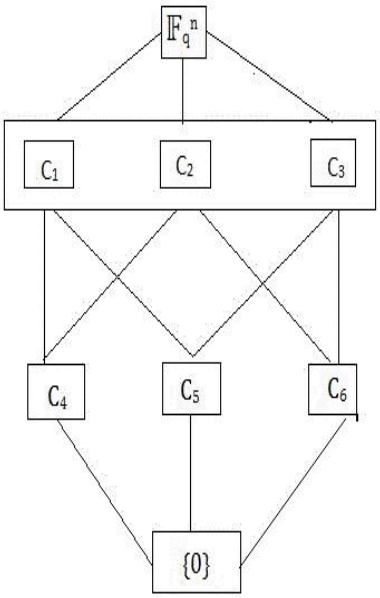


Figure 3.2 - Codes minimaux.

Exemple 3.2

Prenons $n = 7$ et $\mathbb{F} = \mathbb{F}_2$. $x^7 - 1$ se factorise de la façons suivante :

$$x^7 - 1 = (x+1)\left(x^3 + x + 1\right)\left(x^3 + x^2 + 1\right)$$

Les trois facteurs étant irréductibles. Ainsi, les codes cycliques minimaux de longeur 7 sont exactement les $\langle \mathcal{M}_1(x) \rangle$, $\langle \mathcal{M}_2(x) \rangle$, $\langle \mathcal{M}_3(x) \rangle$ avec

$$\begin{aligned}
\mathcal{M}_1(x) &= \frac{x^7 - 1}{g_1(x)} \quad \text{tel que} \quad g_1(x) = (x+1) \\
\mathcal{M}_2(x) &= \frac{x^7 - 1}{g_2(x)} \quad \text{tel que} \quad g_2(x) = \left(x^3 + x^2 + 1\right) \\
\mathcal{M}_3(x) &= \frac{x^7 - 1}{g_3(x)} \quad \text{tel que} \quad g_3(x) = \left(x^3 + x + 1\right)
\end{aligned}$$

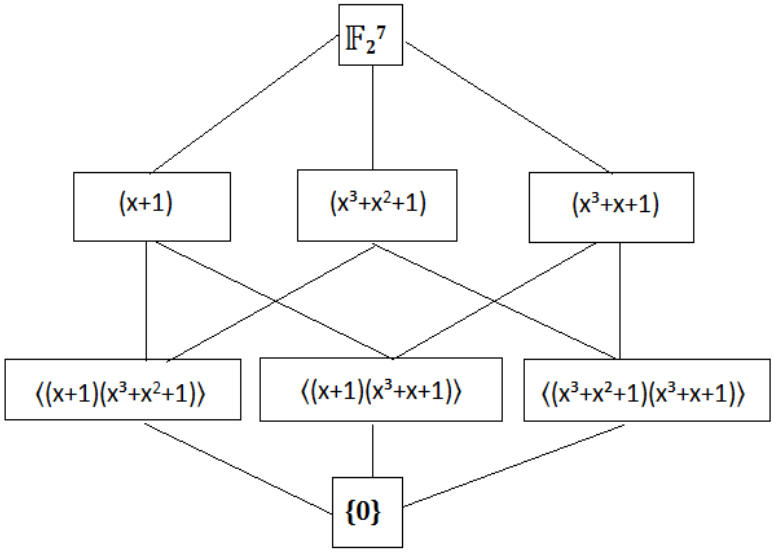


Figure 3.3

Exemple 3.3

Les codes cycliques minimaux de longueur 7 sur $\mathbb{F}_2$.

polynôme générateur	paramètres de code
$(x+1)(x^3+x+1) = 1+2x+x^2+x^3+x^4$	$[7,3]$
$(x+1)(x^3+x^2+1) = 1+x+x^2+2x^3+x^4$	$[7,3]$
$(x^3+x+1)(x^3+x^2+1) = 1+x+x^2+3x^3+x^4+x^5+x^6$	$[7,1]$

Exemple 3.4

Factor $[-1+x^{13},\ modulus \to 3]$ On utilisent le logiciel mathématica, on trouve

$$x^{13}-1 = (2+x)\left(2+2x+x^3\right)\left(2+x^2+x^3\right)\left(2+x+x^2+x^3\right)\left(2+2x+2x^2+x^3\right).$$

Les codes cycliques minimaux de longueur 13 sur $\mathbb{F}_3$

polynôme générateur	paramètres de code
$1+2x+x^2+2x^4+2x^5+x^6+x^7+x^8+x^{10}$	$[13,3]$
$1+2x+2x^3+x^5+x^6+x^7+2x^8+x^9+x^{10}$	$[13,3]$
$1+x+2x^2+x^3+x^4+x^5+2x^7+2x^9+x^{10}$	$[13,3]$
$1+x^2+x^3+x^4+2x^5+2x^6+x^8+2x^9+x^{10}$	$[13,3]$
$1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{11}+x^{12}$	$[13,1]$

3.3 Les codes cycliques minimaux de longueur $p^n q$ sur le corps $\mathbb{F}_l$

Soit $\mathbb{F}_l$ le corp fini est m un entier ≥ 1, (avec l, m, p, q sont des entiers premiers impairs).

Théorème 3.1

Si $m = p^n q$, $d = p \gcd(\phi(p^n), \phi(q))$, $p \nmid (q-1)$, l *est une racine primitive* $\bmod p^n$ *et* $\bmod q$, *alors il existe* $n(d+1)+2$ *classes cyclotomiques* $\bmod p^n q$ *données par*

$$\begin{aligned} C_0 &= \{0\}, \\ C_{p^n} &= \left\{p^n, p^n l, p^n l^2, \ldots, p^n l^{\phi(q)-1}\right\}, \end{aligned}$$

et pour $0 \leq i \leq n-1$, $0 \leq k \leq d-1$,

$$\begin{aligned} C_{p^i q} &= \left\{p^i q, p^i q l, \ldots, p^i q l^{\phi\left(p^{n-i}\right)-1}\right\}, \\ C_{a^k p^i} &= \left\{a^k p^i, a^k p^i l, \ldots, a^k p^i l^{\frac{\phi\left(p^{n-i}q\right)}{d}-1}\right\}. \end{aligned}$$

Preuve.

Comme l est une racine primitive $\bmod q$, $\{1, l, l^2, \ldots, l^{q-1}\}$ forme un systeme de classe reduit $\bmod q$. Aussi $p^n l^{q-1} \equiv p^n \pmod{p^n q}$. Danc la classe cyclotomique contient p^n est $C_{p^n} = \{p^n, p^n l, p^n l^2, \ldots, p^n l^{q-2}\}$.

Comme l est une racine primitive $\bmod p^{n-i}$ pour tout i, $0 \leq i \leq n-1$, et $p^i q l^{\phi\left(p^{n-i}\right)} \equiv p^i q \pmod{p^n q}$, la classe cyclotomique contenantt $p^i q$ est $C_{p^i q} = \left\{p^i q, p^i q l, \ldots, p^i q l^{\phi\left(p^{n-i}\right)-1}\right\}$.

$C_{a^k p^i}$ et $C_{a^h p^j}$ sont disjoints pour tout $k \neq h$ ou $i \neq j$. Pour k fixé , $0 \leq k \leq d-1$, et i fixée, $0 \leq i \leq n-1$, $a^k p^i l^{\frac{\phi\left(p^{n-i}q\right)}{d}} \equiv a^k p^i \pmod{p^n q}$. Donc, la classe cyclotomique contient $a^k p^i$ est $C_{a^k p^i} = \left\{a^k p^i, a^k p^i l, \ldots, a^k p^i l^{\frac{\phi\left(p^{n-i}q\right)}{d}-1}\right\}$.

Finalement, ce sont toute les classes cyclotomiques $\bmod p^n q$ est les seules car

$$\begin{aligned}
|C_0| + |C_{p^n}| + \sum_{i=0}^{n-1} \left|C_{p^i q}\right| + \sum_{k=0}^{d-1}\sum_{i=0}^{n-1} \left|C_{a^k p^i}\right| &= 1 + (q-1) + \sum_{i=0}^{n-1} \phi\left(p^{n-i}\right) + \sum_{k=0}^{d-1}\sum_{i=0}^{n-1} \frac{\phi\left(p^{n-i} q\right)}{d} \\
&= 1 + (q-1) + (p^n - 1) + \sum_{k=0}^{d-1} \left(\frac{\phi(q)}{d}\left(p^n - 1\right)\right) \\
&= p^n q.
\end{aligned}$$

Remarque 3.3

On obeserve

$$\begin{aligned}
C_1 &= \left\{1, l, l^2, \ldots, l^{\frac{\phi(p^n q)}{d} - 1}\right\} \\
C_a &= \left\{a, al, al^2, \ldots, al^{\frac{\phi(p^n q)}{d} - 1}\right\}, \ldots, C_{a^{d-1}} = \left\{a^{d-1}, a^{d-1} l, a^{d-1} l^2, \ldots, a^{d-1} l^{\frac{\phi(p^n q)}{d} - 1}\right\}
\end{aligned}$$

Donc, $C_1 \cup C_a \cup \ldots\ldots \cup C_{a^{d-1}}$ est un systeme reduce $\bmod p^n q$.

3.4 Dimension et polynôme générateur de code minimal de longueur $p^n q$ sur le corps $\mathbb{F}_l$

polynôme générateur de code $M_{p^j q}$

le polynôme minimal de $\alpha^{p^j q}$ pour $0 \leq j \leq n-1$ est

$$M^{\left(p^j q\right)}(x) = 1 + x^{p^{n-j-1}} + x^{2p^{n-j-1}} + \ldots + x^{(p-1)p^{n-j-1}}.$$

Aussi pour $0 \leq j \leq n-1$, on trouve

$$\begin{aligned}
\left(x^{p^n q} - 1\right) &= \left(x^{p^{n-j}} - 1\right)\left(1 + x^{p^{n-j}} + x^{2p^{n-j}} + \ldots + x^{(p-1)p^{n-j}}\right) \\
&= \left(x^{p^{n-j-1}} - 1\right)\left(1 + x^{p^{n-j-1}} + x^{2p^{n-j-1}} + \ldots + x^{(p-1)p^{n-j-1}}\right) \\
&\quad \times \left(1 + x^{p^{n-j}} + x^{2p^{n-j}} + \ldots + x^{\left(p^j q - 1\right)p^{n-j}}\right)
\end{aligned}$$

le polynôme générateur de $M_{p^j q}$ est donnée par

$$\left(x^{p^{n-j-1}} - 1\right)\left(1 + x^{p^{n-j}} + x^{2p^{n-j}} + \ldots + x^{\left(p^j q - 1\right)p^{n-j}}\right)$$

Donc, le code $M_{p^j q}$ un code de répétition dans le code de longueur p^{n-j} générée par $\left(x^{p^{n-j-1}}-1\right)$.

Polynôme générateur de code $M_{a^k p^i}$

Pour $0 \leq j \leq n-1$, on trouve

$$\begin{aligned}(x^{p^n q}-1) &= \left(x^{p^{n-j}q}\right)^{p^j}-1 \\ &= (x^{p^{n-j}q}-1)\left(1+x^{p^{n-j}q}+x^{2p^{n-j}q}+\ldots+x^{(p-1)p^{n-j}q}\right) \\ &= \left(x^{p^{n-j-1}q}-1\right)\left(1+x^{p^{n-j-1}q}+x^{2p^{n-j-1}q}+\ldots+x^{(p-1)p^{n-j-1}q}\right) \\ &\quad \times\left(1+x^{p^{n-j}q}+x^{2p^{n-j}q}+\ldots+x^{\left(p^j-1\right)p^{n-j}q}\right)\end{aligned}$$

on note

$$M_{p^j q}(x)\prod_{k=0}^{d-1}M_{a^k p^j}=\left(1+x^{p^{n-j-1}q}+x^{2p^{n-j-1}q}+\ldots+x^{(p-1)p^{n-j-1}q}\right)$$

on obtient

$$\begin{aligned}\frac{x^{p^n q}-1}{\prod_{k=0}^{d-1}M_{a^k p^j}(x)} &= \left(x^{p^{n-j-1}q}-1\right)\left(1+x^{p^{n-j-1}}+x^{2p^{n-j-1}}+\ldots+x^{(p-1)p^{n-j-1}}\right) \\ &\quad \times\left(1+x^{p^{n-j}q}+x^{2p^{n-j}q}+\ldots+x^{(p-1)p^{n-j}q}\right)\end{aligned}$$

Exemples 3.5

On considère deux exemples :

1. On prend $p=5$, $q=17$, $n=1$, $l=3$.

(a) Le polynôme minimal correspondant pour toute classe cyclotomique est obtient suivant :

$$\left(x^{85}-1\right)=\prod_s M_s(x),$$

$M_0(x)=x-1,$

$M_1(x)=x^{16}+x^{14}+x^{12}-x^{11}-x^{10}-x^9+x^6+x^4+x^3+x^2-x+1,$

$M_2(x)=x^{16}-x^{15}-x^{12}-x^{11}-x^9+x^8+x^7+x^6+x^5-x^2+x+1,$

$$M_4(x) = x^{16} - x^{15} + x^{14} + x^{13} + x^{12} + x^{10} - x^7 - x^6 - x^5 + x^4 + x^2 + 1,$$

$$M_5(x) = x^{16} + x^{15} + x^{14} + ... + x^2 + x + 1,$$

$$M_8(x) = x^{16} + x^{15} - x^{14} + x^{11} + x^{10} + x^9 + x^8 - x^7 - x^5 - x^4 - x + 1,$$

$$M_{17}(x) = x^4 + x^3 + x^2 + x + 1.$$

(b) Si $g_s(x)$ est le polynôme générateur de $\mathcal{M}_s$ alors :

$$g_0(x) = x^{84} + x^{83} + ... + x + 1,$$

$$\begin{aligned} g_1(x) = (&x^{69} - x^{67} + x^{64} - x^{63} - x^{62} - x^{60} + x^{59} - x^{58} + x^{57} - x^{56} - x^{55} + x^{52} + x^{51} - \\ &x^{49} - x^{48} - x^{45} + x^{44} + x^{43} - x^{39} + x^{37} - x^{35} + x^{34} - x^{33} - x^{31} - x^{30} + x^{29} - x^{27} - \\ &x^{25} - x^{24} + x^{23} - x^{22} - x^{17} - x^{16} + x^{15} - x^{14} - x^{11} - x^7 + x^6 + x^4 - x^3 - x - 1), \end{aligned}$$

$$\begin{aligned} g_2(x) = (&x^{69} + x^{68} + x^{67} + x^{66} - x^{65} + x^{64} - x^{60} + x^{59} - x^{58} + x^{57} + x^{56} + x^{55} + \\ &x^{54} + x^{53} + x^{52} - x^{51} + x^{50} + x^{49} + x^{48} - x^{46} - x^{44} - x^{42} - x^{41} + x^{40} + x^{39} + \\ &x^{38} + x^{37} + x^{36} - x^{35} + x^{34} - x^{33} + x^{32} - x^{30} + x^{28} + x^{27} + x^{25} + x^{24} + x^{22} + \\ &x^{20} + x^{18} - x^{16} + x^{12} - x^{11} + x^9 - x^8 + x^7 + x^6 + x^4 + x^2 + x - 1), \end{aligned}$$

$$\begin{aligned} g_4(x) = &x^{69} + x^{68} + x^{66} - x^{65} - x^{63} + x^{62} + x^{58} + x^{55} - x^{54} + x^{53} + x^{52} + x^{47} - x^{46} + \\ &x^{45} + x^{44} + x^{42} - x^{40} + x^{39} + x^{38} + x^{36} - x^{35} + x^{34} - x^{32} + x^{30} - x^{26} - x^{25} + x^{24} + \\ &x^{21} + x^{20} - x^{18} - x^{17} + x^{14} + x^{13} - x^{12} + x^{11} - x^{10} + x^9 + x^7 + x^6 - x^5 + x^2 - 1), \end{aligned}$$

$$g_5(x) = (x^{69} - x^{68} + x^{52} - x^{51} + x^{35} - x^{34} + x^{18} - x^{17} + x - 1,$$

$$\begin{aligned} g_8(x) = (&x^{69} - x^{68} - x^{67} - x^{65} - x^{63} - x^{62} + x^{61} - x^{60} + x^{58} - x^{57} + x^{53} - x^{51} - \\ &x^{49} - x^{47} - x^{45} - x^{44} - x^{42} - x^{41} + x^{39} - x^{37} + x^{36} - x^{35} + x^{34} - x^{33} - x^{32} - \\ &x^{31} - x^{30} - x^{29} + x^{28} + x^{27} + x^{25} + x^{23} - x^{21} - x^{20} - x^{19} + x^{18} - x^{17} - x^{16} - \\ &x^{15} - x^{14} - x^{13} - x^{12} + x^{11} - x^{10} + x^9 - x^5 + x^4 - x^3 - x^2 - x - 1), \end{aligned}$$

$$\begin{aligned} g_{17}(x) = (&x^{81} - x^{80} + x^{76} - x^{75} + x^{71} - x^{70} + x^{66} - x^{65} + x^{61} - x^{60} + x^{56} - x^{55} + \\ &x^{51} - x^{50} + x^{46} - x^{45} + x^{41} - x^{40} + x^{36} - x^{35} + x^{31} - x^{30} + x^{26} - x^{25} + x^{21} - \\ &x^{20} + x^{16} - x^{15} + x^{11} - x^{10} + x^6 - x^5 + x - 1). \end{aligned}$$

(c) La dimension est donné par :

Code	$\mathcal{M}_0$	$\mathcal{M}_1$	$\mathcal{M}_2$	$\mathcal{M}_4$	$\mathcal{M}_5$	$\mathcal{M}_8$	$\mathcal{M}_{17}$
Dimension	1	16	16	16	16	16	16

2. On prend $p = 7$, $q = 19$, $n = 1$, $l = 3$.

(a) Le polynôme minimal correspondant pour toute classe cyclotomique est obtient suivant :

$$\left(x^{133} - 1\right) = \prod_s M_s(x),$$

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

$$M_1(x) = x^{18} + x^{16} - x^{14} + x^{13} - x^{12} - x^{11} - x^{10} - x^8 - x^7 - x^6 + x^5 - x^4 + x^2 + 1,$$

$$M_2(x) = x^{18} - x^{17} - x^{16} - x^{15} + x^{12} - x^{11} + x^{10} + x^8 - x^7 + x^6 - x^3 - x^2 - x + 1,$$

$$M_4(x) = x^{18} - x^{16} + x^{15} + x^{14} + x^{13} - x^{12} - x^{10} - x^9 - x^8 - x^6 + x^5 + x^4 + x^3 - x^2 + 1,$$

$$M_7(x) = x^{18} + x^{17} + ... + x^2 + x + 1,$$

$$M_8(x) = x^{18} + x^{17}x^{15} - x^{14} + x^{12} + x^{10} - x^9 + x^8 + x^6 - x^4 + x^3 + x + 1,$$

$$M_{16}(x) = x^{18} - x^{17} - x^{16} - +x^{15} - x^{13} + x^{11} - x^{10} - x^8 + x^7 - x^5 + x^3 - x^2 - x + 1,$$

$$M_{19}(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

$$M_{32}(x) = x^{18} - x^{14} + x^{11} - x^{10} + x^9 - x^8 + x^7 - x^4 + 1.$$

(b) Si $g_s\,(x)$ est le polynôme générateur de $\mathcal{M}_s$ alors :

$$g_0(x) = x^{132} + x^{131} + ... + x^2 + x + 1,$$

$$\begin{aligned} g_1(x) = (&x^{115} - x^{113} - x^{111} - x^{110} + x^{109} + x^{107} - x^{106} - x^{104} - x^{101} + x^{100} - x^{99} + \\ &x^{98} + x^{97} + x^{96} - x^{95} - x^{94} + x^{93} + x^{92} - x^{91} - x^{90} - x^{89} + x^{88} + x^{85} - x^{84} - \\ &x^{83} + x^{82} - x^{80} + x^{79} + x^{78} + x^{76} + x^{75} - x^{73} + x^{69} - x^{67} - x^{66} + x^{65} + x^{61} - \\ &x^{60} + x^{58} - x^{57} + x^{55} - x^{54} - x^{50} + x^{49} + x^{48} - x^{46} + x^{42} - x^{40} - x^{39} - x^{37} - \\ &x^{36} + x^{35} - x^{33} + x^{32} + x^{31} - x^{30} - x^{27} + x^{26} + x^{25} + x^{24} - x^{23} - x^{22} + x^{21} + \\ &x^{20} - x^{19} - x^{18} - x^{17} + x^{16} - x^{15} + x^{14} + x^{11} + x^9 - x^8 - x^6 + x^5 + x^4 + x^2 - 1), \end{aligned}$$

$$\begin{aligned} g_2(x) = (&x^{115} + x^{114} - x^{113} + x^{112} + x^{111} + x^{110} - x^{109} + x^{108} - x^{107} - x^{106} - x^{105} - \\ &x^{104} - x^{103} - x^{101} + x^{98} - x^{97} - x^{96} + x^{94} - x^{93} + x^{91} + x^{88} + x^{87} + x^{86} - x^{84} - \\ &x^{82} - x^{80} + x^{79} - x^{77} - x^{74} - x^{73} + x^{72} + x^{71} - x^{68} - x^{65} + x^{64} - x^{63} + x^{61} + \\ &x^{59} - x^{58} + x^{57} - x^{56} - x^{54} + x^{52} - x^{51} + x^{50} + x^{47} - x^{44} - x^{43} + x^{42} + x^{41} + \\ &x^{38} - x^{36} + x^{35} + x^{33} + x^{31} - x^{29} - x^{28} - x^{27} - x^{24} + x^{22} - x^{21} + x^{19} + x^{18} - \\ &x^{17} + x^{14} + x^{12} + x^{11} + x^{10} + x^9 + x^8 - x^7 + x^6 - x^5 - x^4 - x^3 + x^2 - x - 1), \end{aligned}$$

$$\begin{aligned} g_4(x) = (&x^{115} + x^{113} - x^{112} + x^{109} + x^{107} - x^{106} - x^{105} + x^{103} - x^{102} - x^{101} - x^{100} + \\ &x^{99} - x^{96} + x^{95} + x^{94} - x^{93} - x^{92} + x^{90} + x^{88} - x^{87} - x^{85} + x^{84} + x^{83} + x^{81} + x^{80} - \\ &x^{78} + x^{77} + x^{76} + x^{75} + x^{73} + x^{72} - x^{71} + x^{70} + x^{68} + x^{64} - x^{63} + x^{62} + x^{61} + x^{60} + \\ &x^{59} + x^{58} - x^{57} - x^{56} - x^{55} - x^{54} - x^{53} + x^{52} - x^{51} - x^{47} - x^{45} + x^{44} - x^{43} - x^{42} - \\ &x^{40} - x^{39} - x^{38} + x^{37} - x^{35} - x^{34} - x^{32} - x^{31} + x^{30} + x^{28} - x^{27} - x^{25} + x^{23} + x^{22} - \\ &x^{21} - x^{20} + x^{19} - x^{16} + x^{15} + x^{14} + x^{13} - x^{12} + x^{10} + x^9 - x^8 - x^6 + x^3 - x^2 - 1), \end{aligned}$$

$$g_7(x) = x^{115} - x^{114} + x^{96} - x^{95} + x^{77} - x^{76} + x^{58} - x^{57} + x^{39} - x^{38} + x^{20} - x^{19} + x - 1,$$

$$\begin{aligned} g_8(x) = (&x^{115} - x^{114} + x^{113} + x^{112} + x^{111} - x^{109} - x^{108} - x^{106} + x^{102} - x^{101} - x^{100} + \\ &x^{99} - x^{98} + x^{97} - x^{93} + x^{92} + x^{90} - x^{89} + x^{88} + x^{87} + x^{86} + x^{85} + x^{83} + x^{82} - \end{aligned}$$

$$x^{81}+x^{80}-x^{78}+x^{76}-x^{75}-x^{74}-x^{73}+x^{72}+x^{70}-x^{68}+x^{66}+x^{65}-x^{61}-$$
$$x^{58}+x^{57}+x^{54}-x^{50}-x^{49}+x^{47}-x^{45}-x^{43}+x^{42}+x^{41}+x^{40}-x^{39}+x^{37}-$$
$$x^{35}+x^{34}-x^{33}-x^{32}-x^{30}-x^{29}-x^{28}-x^{27}+x^{26}-x^{25}-x^{23}+x^{22}-x^{18}+$$
$$x^{17}-x^{16}+x^{15}+x^{14}-x^{13}+x^{9}+x^{7}+x^{6}-x^{4}-x^{3}-x^{2}+x-1),$$

$$g_{16}(x)=(x^{115}+x^{114}-x^{113}-x^{112}+x^{110}-x^{108}+x^{106}+x^{105}+x^{104}-x^{102}-x^{101}+$$
$$x^{99}+x^{98}+x^{96}-x^{95}+x^{92}+x^{91}+x^{90}+x^{89}+x^{86}+x^{85}-x^{83}-x^{77}-x^{76}+$$
$$x^{75}+x^{70}-x^{66}-x^{63}-x^{62}+x^{60}+x^{58}-x^{57}-x^{55}+x^{53}+x^{52}+x^{49}-x^{45}-$$
$$x^{40}+x^{39}+x^{38}+x^{32}-x^{30}-x^{29}-x^{26}-x^{25}-x^{24}-x^{23}+x^{20}-x^{19}-x^{17}-$$
$$x^{16}+x^{14}+x^{13}-x^{11}-x^{10}-x^{9}+x^{7}-x^{5}+x^{3}+x^{2}-x-1),$$

$$g_{19}(x)=(x^{127}-x^{126}+x^{120}-x^{119}+x^{113}-x^{112}+x^{106}-x^{105}+x^{99}-x^{98}+x^{92}-$$
$$x^{91}+x^{85}-x^{84}+x^{78}-x^{77}+x^{71}-x^{70}+x^{64}-x^{63}+x^{57}-x^{56}+x^{50}-x^{49}+$$
$$x^{43}-x^{42}+x^{42}+x^{36}-x^{35}+x^{29}-x^{28}+x^{22}-x^{21}+x^{15}-x^{14}+x^{8}-x^{7}+x-1),$$

$$g_{32}(x)=(x^{115}+x^{111}-x^{108}-x^{107}-x^{106}+x^{105}+x^{102}+x^{101}-x^{100}+x^{99}-x^{98}+$$
$$x^{96}-x^{95}-x^{93}+x^{92}-x^{89}-x^{87}-x^{86}-x^{85}+x^{84}-x^{83}+x^{82}+x^{81}+x^{80}+$$
$$x^{76}-x^{74}-x^{73}-x^{72}-x^{71}-x^{68}+x^{67}+x^{66}+x^{65}+x^{64}-x^{62}-x^{61}-x^{60}+$$
$$x^{58}-x^{57}+x^{55}+x^{54}+x^{53}-x^{51}-x^{50}-x^{49}-x^{48}+x^{47}+x^{44}+x^{43}+x^{42}+$$
$$x^{41}-x^{39}-x^{35}-x^{34}-x^{33}+x^{32}-x^{31}+x^{30}+x^{29}+x^{28}+x^{26}-x^{23}+x^{22}+$$
$$x^{20}-x^{19}+x^{17}-x^{16}+x^{15}-x^{14}-x^{13}-x^{10}+x^{9}+x^{8}+x^{7}-x^{4}-1).$$

(c) La dimension est donné par :

Code	$\mathcal{M}_0$	$\mathcal{M}_1$	$\mathcal{M}_2$	$\mathcal{M}_4$	$\mathcal{M}_7$	$\mathcal{M}_8$	$\mathcal{M}_{16}$	$\mathcal{M}_{19}$	$\mathcal{M}_{32}$
Dimension	1	18	18	18	18	18	18	6	18

conclusion

Dans cette mémoire on a présenté les codes cycliques minimaux pour certaines longueurs dans les corps finis $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_l$(tel que l un nombre premier impair).

De plus, on a pu utiliser le logiciel mathematica pour les codes cycliques minimaux.

Bibliographie

[1] **Abdous.F**, *Codes auto-duaux sur $\mathbb{F}_q$ et $\mathbb{Z}_4$*, Mémoire présenté pour l'obtention du diplôme de magistèr Université de el hadj lakhdar-batena, 2007.

[2] **Arnault.F and all,** *Mathématiques L3 Algèbre Cours complet avec 400 tests et exercices corrigés,* Pearson Education France, 2009.

[3] **Bonnecaze.A**, Introduction à l'algèbre pour les Codes Cycliques, Marseille Université, 2006-2007.

[4] **Christophe.C**, *Reconnaissance de code, structure des codes quasi-cyclique*, Mémoire présenté pour obtention le grade de docteur de L'*université* de Limoges, 2009.

[5] **Demazure.M**, *Cours d'algèbre. Primalité, divisibilité, codes*, Nouvelle bibliothèque mathématique, Cassini, 1997.

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

[7] **G.K. Bakshi, Madhu Raka**, *Minimal cyclic codes of length $p^n q$*, Finite Fields Appl. 9 (2003) 432–448.

[8] **Heboub.L**, *Etude de techniques de décodage des codes linéaires*, Mémoire présenté pour l'obtention du diplôme de magistèr Université de m'sila, 2009.

[9] **Ladjlat.L**, *Etudes de l'équivalence de deux codes sur un corps finis*, Mémoire présenté pour l'obtention du diplôme de magistèr Université de m'sila, 2004.

[10] **Lidl.R et Pilz.G**, *Applied Abstract Algebra*, springer verlag, New York-Berlin-Heidelberg, October 1997.

[11] **Mihoubi.C**,*Classification des codes linéaires tertiaires optimaux [n,n/2]*, Mémoire présenté pour l'obtention du diplôme de doctorat en sciences Université de el hadj lakhdar-batena, 2012.

[12] **Mihoubi.C,** *Etude sur l'irréductibilité d'un polynôme sur un corps fini*, Mémoire présenté pour l'obtention du diplôme de magistèr Université de m'sila, 2001.

[13] **Saadi.A**, *Etude sur les bornes des codes correcteurs d'erreurs*, Mémoire présenté pour l'obtention du diplôme de magistèr Université de m'sila, 2000.

[14] **Schwartz.L**, *Algébre $3^{\text{éme}}$ année 2^{e} édition, Université de Paris-Nord*, Dunod, avril 2003.

ملخص

يندرج هذا العمل في إطار نظرية الشفرات المصححة للأخطاء أكثر دقة دراسة الشفرات الدورية الأصغرية.

الشفرة الدورية التي طولها n على الحقل المنتهي F_q هي مثالي رئيسي في حلقة حاصل القسمة $R_n = \mathrm{F}_q[x] \big/ \langle x^n - 1 \rangle$ حيث $\mathrm{F}_q[x]$ هو حلقة كثيرات الحدود التي معاملاتها من F_q و $(x^n - 1)$ هو المثالي الرئيسي المولد بكثير الحدود $\langle x^n - 1 \rangle$

في هذا البحث نهتم بدراسة المثاليات الأصغرية في حلقة حاصل القسمة R_n ، هذه المثاليات تمثل الشفرات الدورية الأصغرية R_n.

الكلمات المفتاحية : الحقول المنتهية، الشفرات الدورية.

Résumé

Ce travail se situe dans le cadre de la théorie des codes correcteurs d'erreurs. Plus précisément l'étude de codes cycliques minimaux.

Un code cyclique de longueur n sur le corps fini F_q est un idéal principal de l'anneau quotient $R_n = \mathrm{F}_q[x] \big/ \langle x^n - 1 \rangle$ où $\mathrm{F}_q[x]$ est l'anneau des polynômes à coefficients dans le corps fini F_q et $\langle x^n - 1 \rangle$ est l'idéal principal engendré par le polynôme $(x^n - 1)$.

Dans cette mémoire on s'intéresse aux idéaux minimaux de l'anneau quotient R_n, ces idéaux représentent les codes cycliques minimaux de R_n.

Mots clés: Corps finis, codes cycliques.

Abstract

This work is included in the frame of the theory of error -correcting codes. More precisely the study of minimal cyclic codes.

A cyclic code of length n on the finite field F_q is a principal ideal of the quotient ring $R_n = \mathrm{F}_q[x] \big/ \langle x^n - 1 \rangle$ where $\mathrm{F}_q[x]$ is the ring of polynomials with coefficients in the finite field F_q and $\langle x^n - 1 \rangle$ is the principal ideal generated by the polynomial $(x^n - 1)$.

In this memory we are interested in the minimal ideals of the ring quotient R_n, these ideals represent the minimal cyclic codes of R_n.

Keywords: Finite fields , cyclic codes.