N° D'ordre : 05/2013-D/MT

Ministère de l'enseignement Supérieur et de la Recherche Scientifique

Université des Sciences et de la Technologie Houari Boumediene

Faculté de Mathématiques

Département d'Algèbre et Théorie des Nombres

Thèse

Présentée pour l'obtention du diplôme de DOCTORAT

En MATHEMATIQUES

Spécialité : Algèbre et Théorie des Nombres

BATOUL Aicha

Thème

Construction des Codes Auto-Duaux

Soutenue publiquement, le 18/04/2013. Devant le jury composé de :

Mr B. BENZAGHOU	Professeur à l'USTHB	Président
Mme A. LAOUDI	Maitre de conférence à l'USTHB	Directrice de thèse
Mr K .BETINA	Professeur à l'USTHB	Examinateur
Mr A.DERBAL	Professeur à l'ENS de Kouba	Examinateur
Mme F.Z.BELKREDIM	Maitre de conférence à l'U.Chlef	Examinatrice
Mme F.MAMACHE	Maitre de conférence à l'USTHB	Examinatrice
Mr S.REZAOUI	Maitre de conférence à l'USTHB	Examinateur

Résumé

Dans cette thèse, nous nous sommes intéressés à l'étude des codes correcteurs auto-duaux sur les anneaux principaux finis. Nous avons établi des conditions nécessaires et suffisantes pour l'existence des codes cycliques auto-duaux sur ces anneaux et nous avons donné une nouvelle construction de ces codes. En utilisant les propriétés des codes duadiques, nous avons trouvé une famille infinie de codes cycliques auto-duaux sur les corps finis de caractéristique 2. La généralisation de cette définition aux anneaux finis nous a permis de trouver une autre famille infinie de codes auto-duaux définis sur les anneaux. Nous avons prouvé qu'il n'existe pas de codes cycliques libres auto-duaux sur les anneaux de caractéristique impaire comme nous avons calculé le nombre de codes cycliques ainsi que le nombre de codes cycliques auto-duaux sur ces anneaux. Nous avons montré qu'il n'existe pas de codes cycliques auto-duaux sur ces anneaux dont l'idéal maximal a pour générateur un élément qui a pour indice de nilpotence un entier impair. Nous avons généralisé ce résultat aux anneaux principaux dont au moins un idéal maximal a pour indice de stabilité un entier impair. Bien que notre travail ait principalement une motivation théorique, on peut espérer que cette étude servira de base sur laquelle des résultats en théorie de l'information peuvent être établis, comme de nombreuses perspectives sont possibles pour l'étendre.

Mots clés : Anneaux principaux, Anneaux à chaine finis, Codes correcteurs définis sur les anneaux finis, Codes libres, Codes cycliques, Codes auto-duaux, Résidus quadratiques.

Remerciements

Je remercie **Allah**, le miséricordieux, de m'avoir accordé la connaissance, et m'avoir donné la volonté et le courage afin d'accomplir ce modeste travail.

Je tiens à remercier le Professeur Benzaghou d'avoir accepté d'examiner mon travail et de présider le jury.

Je remercie ma Directrice de thèse, Mme Laoudi pour son encadrement, ses conseils ses encouragements et sa confiance.

Comme je remercie le Professeur Betina Directeur du Laboratoire d'Algèbre et Théorie des Nombres (LATN) de la Faculté de Mathématiques de l'USTHB au sein duquel a été réalisé cette thèse.

J'adresse mes sincères remerciements au membres du jury pour avoir accepté d'évaluer ce travail, à savoir : Mesdames et Messieurs le Professeur Mr Derbal et les Maitres de conférences Mme Belkredim, Mme Mamache et Mr Rezaoui.

Mes remerciements vont également à Mme Guenda qui a toujours répondu à mes questions et en qui j'ai trouvé une vraie amie. Je te remercie pour tes conseils, ton soutien, ton aide et ta collaboration durant toutes ces années de travail. Tu as su m'entrainé dans la recherche avec passion.

Je suis redevable au Professeur T.A.Gulliver de l'Université Victoria du Canada pour sa collaboration.

Comme je remercie tous mes collègues enseignants pour l'inestimable soutien qu'ils n'ont cessé de m'apporter ces derniers temps et particulièrement un grand merci à Mme Selmane pour son amitié et ses conseils.

Je tiens à remercier toutes les personnes qui ont contribué de près ou de loin à l'aboutissement de ce travail.

Ce travail n'aurait jamais abouti sans le soutien moral de ma famille et belle famille surtout les "Prières" de mes parents et les encouragements de mon mari, mes frères, sœurs et mes enfants. Je vous en remercie tous. *aicha Batoul*

Table des matières

Notations

$\mathbb{F}_q$ =: Le corps fini à q éléments.

$\min(E)$ =: Le plus petit élément de E.

Pour a et $b \in \mathbb{N}$ et p un nombre premier,

$p^a//b$ =: a est la plus grande puissance de p qui divise b.

$\mathbb{Z}_n$ =: $\mathbb{Z}/n\mathbb{Z}$.

C_i =: La $i$ème classe cyclotomique mod n.

$ppcm(a, b)$ =: Le plus petit commun multiple de a et b.

$[n]$ =: L'ensemble $\{1, \ldots, n\}$.

$q \equiv \square \mod n$ =: q est un résidu quadratique modulo n.

$\phi(.)$ =: La fonction indicatrice d'Euler.

S_n =: Le groupe symétrique d'un ensemble à n éléments.

$\mathcal{R}$:= Un anneaux fini.

$\langle\gamma\rangle$ =: Un idéal principal engendré par γ

e =: indice de nilpotence de γ

$(n, q) = 1$ signifit que n et q sont premiers entre eux.

Introduction

Ces dernières années, la demande de systèmes de transmission numériques fiables a énormément augmenter . L'explosion de l'échange d'informations a accentué cette tendance. Les systèmes de communication modernes exigent des débits de plus en plus élevés afin de traiter des volumes d'informations qui ne cessent d'augmenter. Le codage des informations à transmettre, permet la détection ou la correction d'éventuelles erreurs de transmission. Parmi les principales techniques existantes, les codages en bloc et les codages convolutifs sont prédominants. La stratégie de base du codage consiste à ajouter une quantité contrôlée de redondance à la série d'informations à envoyer. L'informatique est un domaine jeune , en plein essor domaine et vaste dont les codes correcteurs en est une branche. Cette branche est reliée à celle d'un autre arbre, beaucoup plus vaste, l'arbre des mathématiques. Les codes correcteurs reposent bien souvent sur de l'algèbre, de l'arithmétique, de la géométrie et la liste ne se veut pas exhaustive. Nous sommes donc à la frontière entre informatique et mathématiques. L'objectif des codes correcteurs est de " sécuriser " les données numériques contre des " ennemis ". L'absence de contexte rend cette définition vague et impropre.

Il a fallu attendre 1948 et les publications de Claude Shannon pour que s'établisse une théorie des communications numérique rigoureuse. Cette théorie, connue sous le nom de théorie de l'information fit disparaitre des (bricolages astucieux) aux (idées quelquefois préconçues) pour laisser place à de vraie méthodes scientifiques.

Un des problèmes majeurs que Shannon étudia est la garantie d'une communication fiable en présence de bruit. Ce problème est intimement lié à la notion de codage.

Cependant, la théorie se contente de prédire l'existence de codes et ne donne aucun moyen de les construire. Depuis les années cinquante, des progrès considérables ont été effectués en matière de conception de systèmes de communication numériques. Mais le problème de la construction de bons codes reste toujours d'actualité.

La problématique du codage correcteur est : Comment protéger un message contre les erreurs ? Un message est composé d'une suite d'éléments appartenant à un ensemble fini (ou alphabet) appelés symboles d'information. L'alphabet est le plus souvent binaire. Lors de la transmission d'un message, il arrive occasionnellement que surviennent des erreurs.

Celle-ci peuvent être la conséquence de bruit sur le canal et peuvent affecter la qualité de la transmission. Pour prévenir ce risque, on adjoint à un bloc de k symboles d'information (le message à transmettre) un certain nombre de symboles calculés en fonction du message par l'intermédiaire d'une fonction φ fixée à l'avance. Cela revient à ajouter une redondance au message à transmettre.

Cette concaténation des k symboles d'information avec la redondance représente un " mot de code" x de longueur $n > k$. L'ensemble de tous les mots obtenus de cette façon forme un code en bloc de longueur n.

Connaissant la fonction φ, il est facile de vérifier l'appartenance d'un mot au code et de détecter d'éventuelles erreurs. Un "bon code" doit compter un grand nombre de mots distincts les uns des autres. Il doit donc permettre d'envoyer des messages variées et de réduire la possibilité de confusion entre les mots.

Le codage peut-être aussi schématisé comme étant une suite d'opérations mathématiques inversibles qui modifie le message et le rallonge. Le message codé ne contient pas seulement l'information brute mais aussi de la redondance. Cette redondance peut permettre (ou non) au destinataire de reconstituer l'information en cas de dégradation. En contrepartie, la transmission des messages codés prend davantage de temps puisqu'il y a plus de données à transmettre. Cette capacité de pouvoir corriger ou non des erreurs dépend des propriétés du code.

Les codes correcteurs sont utilisés notamment dans les télécommunications ou pour

le stockage d'informations. Ils permettent alors de détecter et de corriger des erreurs. On entend par le terme " erreur " , une altération ou une perte partielle ou totale de l'information. Ces erreurs sont 'l'ennemi' du codeur. Des causes multiples peuvent être à l'origine de ces erreurs. Des poussières ou des rayures peuvent dégrader les données contenues sur un disque Blu-ray ou un DVD. Des perturbations électromagnétiques peuvent détériorer les données dans les communications satellitaires ou téléphoniques. Les codes correcteurs sont encore utilisés dans diverses technologies de communication (ADSL, fibre optique et USB entre autres).

La plupart du temps, et pour des raisons pratiques, on utilise des codes linéaires. Concrètement, un code linéaire de longueur n sur un corps fini $\mathbb{F}$ est un sous espace vectoriel de $\mathbb{F}^n$ sur $\mathbb{F}$. Ces codes permettent de travailler sur des matrices et non sur des ensembles. Ils sont donc plus pratiques à étudier, à coder et à décoder. Cependant, la linéarité induit une structure qui limite quelquefois la cardinalité du code. Pour maximaliser le nombre de mots du code , avec une longueur et une capacité de correction données, il est souvent nécessaire de considérer des codes non linéaires. Les codes non linéaires les plus célèbres sont les codes de Preparata ,Kerdock et Nordstrom- Robinson. Ils contiennent deux fois plus de mots que les meilleurs codes linéaires de même paramètres. Les codes de Preparata Kerdock sont d'une certaine manière "duaux" l'un de l'autre bien que l'absence de linéarité ne permette pas de parler de dualité algébrique. En 1992 Hammons et al.[34] donnerent une explication à cette dualité formelle définissant les codes de Preparata Kerdock sur l'anneau des entiers modulo quatre, $\mathbb{Z}_4$. Sur cet anneau, ces codes sont linéaires et algébriquement duaux.
L'application "**Gray** " permet de passer de la représentation quaternaire à la représentation binaire. Elle joue un rôle fondamental dans l'étude des codes quaternaires. C'est une isométrie qui préserve la propriété de distance invariante mais pas la linéarité.
De là, a commencé l'intérêt pour les codes linéaires définis sur les anneaux finis et spécialement, **Les Codes sur les Anneaux Principaux finis**.
Dans cette thèse, nous abordons les différents aspects des codes linéaires auto-duaux

sur les anneaux finis, en particuliers, les codes cycliques. En plus de leur importance théorique ,les codes auto-duaux ont aussi une application pratique, ils ont une relation avec les réseaux unimodulaires et leurs groupes d'automorphismes sont parfois d'un grand intérêt [9, 13]. Plusieurs chercheurs ont travaillé sur les codes sur les anneaux [21, 23, 28].

La structure des codes cycliques sur $\mathbb{Z}_{p^a}$ a été donnée premièrement par Calderbank et Sloane [17] en suite par Kanwar [37]. Cela a motivé d'autres chercheurs comme [1, 11, 59]), pour donner la structure des codes cycliques et négacycliques sur les anneaux à chaine finis .

Norton et Sualugean [45], Dinh et lopez-Permouth [21]ont généralisé cette structure au codes cycliques sur les anneaux à chaine finis .

Récemment,la structure a été donnée dans [21] et généralisée aux codes constacycliques [32]. Motivé par un problème ouvert par Jia et al. [35] sur la structure des codes cycliques auto-duaux sur les anneaux finis, nous donnons des conditions nécessaires et suffisantes sur l'existence des codes cyclique auto-duaux non triviaux sur les anneaux à chaine finis.

Nous utilisons la définition des codes duadiques [36] sur les corps finis, pour construire une famille infinie de codes cycliques auto-duaux sur les corps finis de caractéristiques 2. Nous généralisons cette définition sur les anneaux à chaine finis pour construire une famille de codes cycliques auto-duaux sur ces anneaux. Nous montrons que dans le cas où la nilpotence du générateur de l'idéal maximal est paire. Il existe un code cyclique non trivial auto-dual de longueur n impair si et seulement si $ord_n(p^r)$ est impair, où p^r est le cardinal du corps résiduel de l'anneau à chaine fini $\mathcal{R}$. Nous montrons également qu'il n'existe pas de codes cycliques libres auto-duaux définis sur les anneaux à chaine finis, tel que p soit impair,où p est la caractéristique de son corps résiduel.

Nous donnons aussi une expression explicite du nombre de codes cycliques auto-duaux sur les anneaux à chaine finis et nous illustrons par des exemples . Ce résultat est une extension de Jia et al [35] concernant le nombre des codes cyclique auto-duaux

sur le corps $\mathbb{F}_{2^i}$.

Cette thèse est organisée comme suit : Une introduction , quatre chapitres, une conclusion et un appendice consacré aux préliminaires mathématiques nous permettant une compréhension plus aisée des autres chapitres.
Le chapitre un est consacré aux rappels sur les notions de base des codes correcteurs d'erreurs. Nous donnons une brève introduction sur la théorie des codes. Nous rappelons les notions de base et les propriétés des codes correcteurs d'erreurs linéaires ainsi que les paramètres qui permettent de les caractériser.Nous donnons quelques bornes sur ces paramètres, telle que les bornes de singleton et de Hamming. On rappelle les notions d'extension par terme de parité,ainsi que les définitions des codes auto-duaux pour le produit défini sur $\mathbb{F}_q^n$.

Le chapitre deux est consacré au codes cycliques en général et aux codes duadiques en particulier , sur les corps finis par exemple code de Harmming, Résidue quadratique, code BCH , code Reed-solomon et les codes duadiques.

En utilisant les propriétés des codes duadiques, nous donnons une Construction d'une famille infinie de codes auto-duaux définis sur les corps finis de caractéristique 2. Nous clôturons ce chapitre par des exemples qui illustrent nos résultats.

Dans le chapitre trois, on définit les codes linéaires de longueur n sur un anneau commutatif fini $\mathcal{R}$ par un sous-module du module $\mathcal{R}^n$ sur $\mathcal{R}$.On montre que tout anneau principal fini est équivalent à une somme directe d'anneaux à chaine finis. Donc pour étudier les codes sur les anneaux principaux il suffit de les étudier sur les anneaux à chaine finis. Comme exemples de codes linéaires définis sur des anneaux finis ,nous étudions de plus prés les codes linéaires définis sur les anneaux à chaine finis à quatre éléments et les anneaux de Galois.

Le but essentiel du chapitre quatre est l'étude des codes cyclique définis sur les an-

neaux à chaine finis. A l'aide d'un certain isomorphisme d'anneaux, nous montrons que cette classe de codes est isomorphisme à une classe plus générale qui est la classe des codes constacycliques. Dinh et López-Permouth [21] ont montré que les codes négacycliques de longueur impair sont isomorphes aux codes cycliques de même longueur.
Nous avons prouvé que cet isomorphisme reste vrai pour un cas plus général.
Nous donnons des conditions nécessaires et suffisantes pour l'existence des codes cycliques auto-duaux sur les anneaux finis. Nous montrons qu'il n'existe pas de codes cycliques sur un anneau à chaine fini d'indice de nilpotence impair.et nous généralisons ce résultat aux codes cycliques définis sur les anneaux principaux dont au moins un idéal maximal a pour indice de stabilité un entier impair. Nous avons calculé le nombre de codes cycliques et celui des codes cycliques auto-duaux définis sur les anneaux à chaine finis. Nous avons généralisé la définition des codes duadiques définis sur les corps finis aux anneaux à chaine finis qui nous a permis de construire une famille infinie de codes cycliques auto-duaux.

Nous clôturons ce chapitre par des exemples où nous avons utilisé nos résultats pour calculer des codes cycliques auto-duaux sur quelques anneaux à chaine finis. La conclusion et les perspectives clôtureront cette thèse.

Chapitre 1

Codes Linéaires Définis sur les Corps Finis

1.1 Introduction

Un code peut être considéré comme un dictionnaire avec des mots inintelligibles, les mots du code. Ces mots ont pourtant un sens bien qu'il soit dissimulé. Ils révèlent leur sens par le biais de ce que l'on appelle le décodage. Les mots de code peuvent bien être décodés puisque le codage est une suite d'opérations inversibles. Le décodage d'un mot de code nous fournit dès lors un mot de notre bon vieux dictionnaire. Chaque code possède plusieurs caractéristiques fondamentales. Certains codes permettent de corriger beaucoup d'erreurs, mais cela ne suffit pas. Si l'on envoie trois fois un message, le destinataire a plus de chances de le recevoir. Mais, on aura envoyé trois fois plus de données, ce qui n'est généralement pas acceptable. Cet exemple est celui du code de répétition. Les codeurs cherchent des codes " optimaux " pour chaque contexte. Il faut faire un compromis entre plusieurs contraintes. L'objectif initial est de corriger des erreurs. On ne veut pas que le codage et le décodage prennent trop de ressources (mémoire, temps). On ne souhaite pas non plus que la taille du message augmente excessivement. Les codes optimaux sont des objets mathématiques structurés comme

nous le verrons par la suite.

1.2 Généralités sur les codes

Dans ce qui va suivre, nous avons tenté de résumer quelques notions fondamentales sur les codes correcteurs définis sur les corps finis . Le lecteur peut consulter [20],[48],[40],[46] , pour de plus amples informations sur ce sujet .

1.2.1 Définitions

Soit $\mathcal{A}$ un alphabet, k, m et n des entiers positifs.

Définition 1. *(**Code correcteur**) Un code correcteur est l'image d'une application injective définie de $\mathcal{A}^k$ et à valeurs dans $\mathcal{A}^n$. Le terme mot de code désigne un élément de cet ensemble.*

Par abus de langage, nous utiliserons le mot code pour désigner les codes correcteurs d'erreurs, à ne pas confondre (ces codes là) avec les " codes secrets " utilisés en cryptographie.

Il existe également des codes détecteurs. Leur rôle consiste à détecter la présence d'érreurs et le cas échéant, à retransmettre le message erroné.

Nous traiterons uniquement des codes correcteurs d'erreurs. Une erreur désigne une modification d'un symbole en un autre. Il existe encore les codes correcteurs d'erreurs en rafale ainsi que les codes correcteurs d'effacements. Le rôle de ces derniers consiste à reconstituer un mot de code émis à partir de l'ensemble des symboles reçus. Un effacement désigne la disparition d'un symbole.

Nous traiterons uniquement des codes en blocs, pour lesquels, les opérations de codage et décodage d'un bloc dépendent uniquement des symboles d'information de ce bloc. L'autre famille de codes est celle des codes convolutifs. Pour ces derniers, le codage et le décodage d'un bloc dépendent des symboles d'information d'autres blocs

(généralement de blocs précédemment transmis). On peut naturellement faire l'analogie avec le chiffrement par blocs et le chiffrement à flot en cryptographie.

Définition 2. *(**Code linéaire**). Un code linéaire est l'image d'une application linéaire injective définie sur $\mathbb{F}_q^k$ et à valeurs dans $\mathbb{F}_q^n$.*

Les entiers k et n désignent respectivement la dimension et la longueur du code. il est dit q-aire. En particulier, le code est dit binaire si $q = 2$ et ternaire si $q = 3$.

Proposition 1. *Un code linéaire est un $\mathbb{F}_q$-sous-espace vectoriel de l'espace vectoriel $\mathbb{F}_q^n$ de dimension k.*

Exemple 1. *1. $\{0\}$, $\mathbb{F}_q^n$ sont des codes linéaires dits triviaux.*

2. Dans $\mathbb{F}_3^3$ le code linéaire engendré par $(1, 0, 2)$ et $(1, 1, 2)$ sur $\mathbb{F}_3$ est

$$C = \{000, 102, 112, 201, 221, 211, 020, 122, 010\}$$

Les mots d'un code linéaire peuvent s'écrire de plusieurs manières selon le choix d'une base du code. On représente une base d'un code linéaire sous forme matricielle.

1.2.2 Paramètres d'un code

Soit C Un q-aire code linéaire de dimension k et de longueur n.

Définition 3. *(**Matrice génératrice**). Une matrice génératrice de C est une matrice notée généralement G de type (k, n) et à coefficients dans $\mathbb{F}_q$ dont les lignes forment une base de C.*

Propriétés 1. *Pour toute matrice inversible M d'ordre k et à coefficients dans $\mathbb{F}_q$, MG est une matrice génératrice de C.*

Définition 4. *Une matrice génératrice d'un code est dite **sous forme systématique** si et seulement si $G = (I_k|A)$, où I_k est la matrice identité $k \times k$ et A une matrice $k \times (n - k)$.*

Proposition 2. *Tout code linéaire C peut se mettre sous forme systématique à permutation près.*

Définition 5. *(**Distance de Hamming**) La distance de Hamming de deux mots x et y de longueur fixe est*

$$d(x,y) = |\{i|\ 0 \leq\ i\ \leq\ n-1, x_i \neq y_i\}|.$$

Définition 6. *(**Espace de Hamming**). L'espace $\mathbb{F}_q^n$ munie de la distance de Hamming est appelé espace de Hamming.*

Définition 7. *(**Support d'un mot**). Le support d'un mot $x = (x_1, x_2, \ldots, x_n)$ deF_q^n est l'ensemble d'indices i tels que $x_i \neq 0$.*

Définition 8. *(**Support d'un code**). Le suppport d'un code est l'union des supports de ses mots.*

Définition 9. *(**Poids de Hamming**). Le poids de Hamming d'un mot est le cardinal de son support. On notera $w(x)$ le poids de Hamming d'un mot x.*

Propriétés 2. *Pour tout x , $y \in F_q^n$, $d(x,y) = w(x-y)$.*

Remarque 1. *La distance de Hamming est une métrique ou distance (au sens mathématique du terme) sur F_q^n*

Nous utiliserons seulement cette métrique pour les codes définis sur les corps finis, néanmoins il en existe d'autres. On pourra citer la métrique rang, la métrique de Lee, la métrique arithmétique ainsi que la métrique de Hamming généralisée.

Définition 10. *(**Distance minimale**). La distance minimale d d'un code est le plus petit poids non nul d'un mot du code.*

Définition 11. *(**Capacité de détection**). La capacité de détection d'un code est la quantité* $d-1$.

Définition 12. *(**Capacité de correction**). La capacité de correction* t *d'un code est la quantité* $\lfloor \frac{d-1}{2} \rfloor$.

Elle désigne le nombre maximal d'erreurs que peut corriger un code sans ambiguïté. Corriger signifie dans notre contexte, choisir le mot de code le plus proche, en termes de distance de Hamming, du mot reçu. On parle de décodage suivant la règle du plus proche voisin. Il y a ambiguïté s'il existe plusieurs possibilités de correction. Auquel cas, on peut soit choisir un mot au hasard parmi les mots de code les plus proches du mot reçu, soit demander une retransmission.

Remarque 2. *Il existe d'autres types de décodage ; on citera le décodage à vraisemblance maximale et le décodage en liste [48].*

1.2.3 Propriétés d'un code

On note par $[n, M, d]_q$ un code q-aire C de longueur n, de cardinal M et de distance minimale d. Un code linéaire $[n, k, d]_q$ est un q-aire code linéaire de longueur n, de dimension k et de distance minimale d. On a l'égalité : $|M| = q^k$.

Il existe plusieurs critères d'optimalité sur les paramètres du code.

Définition 13. ***Borne de Hamming*** *Soient* n *et* d *deux entiers positifs et* $t = \lfloor \frac{d-1}{2} \rfloor$. *Soit* $\mathcal{A}_q(n, d)$ *le nombre maximum de mots que peut contenir un code de longueur* n *et de distance minimale* d *alors*

$$\mathcal{A}_q(n, d) \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-1)^i}$$

Définition 14. *(**Code parfait**). Un code* $[n, M, d]_q$ *est dit parfait si l'ensemble des boules fermées de rayon* t *centrées sur les mots du code forment une partition de* $\mathbb{F}_q^n$, *pour la distance de Hamming.*

Autrement dit, on a l'égalité suivante

$$|C| = \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i}$$

Intuitivement, cela signifie que toute erreur détectée est corrigée. Cela ne signifie néanmoins pas que l'erreur soit correctement corrigée.

Théorème 1. ***(Borne de Singleton)*** *soit C un $[n,k,d]_q$ code, alors*

$$d \leq n - k + 1$$

Définition 15. ***(Isométrie linéaire)*** *Soit F_q un corps fini et d la distance de Hamming définie sur F_q^n. Une isométrie ,est une application linéaire*

$$f : F_q^n \longrightarrow F_q^n$$

qui est une isométrie pour d.

Théorème 2. *soit $f : F_q^n \longrightarrow F_q^n$ une application .Les assertions suivantes sont équivalentes :*

i) f est une isométrie linéaire.

ii) Il existe une permutation $\sigma \in \mathcal{S}_n$ et des scalaires non nuls $\lambda_1, \lambda_2, \ldots, \lambda_n$ tels que pour tout $x = (x_1, x_2, \ldots, x_n) \in F_q^n$, on a :

$$f(x_1, x_2, \ldots, x_n) = (\lambda_1 x_{\sigma(1)}, \lambda_2 x_{\sigma(2)}, \ldots, \lambda_n x_{\sigma(n)}) \tag{1.1}$$

Une application de la forme 1.1 est dite **Monômiale** .Si P est la matrice dans la base canonique d'une telle application ,alors chaque ligne et chaque colonne de P contient un seul coefficient non nul .

Définition 16. ***(Codes equivalents)*** *Deux codes linéaires C et C' de longueur n sur F_q sont dits équivalents ,s'il existe une isométrie linéaire f de F_q^n telle que $f(C) = C'$.*

Remarque 3. *Deux codes linéaires équivalents ont les mêmes propriétés métriques et les mêmes propriétés linéaires.*

Définition 17. *(**Code MDS**). Un code $[n, k, d]_q$ est dit MDS (maximum distance separable) si on a l'égalité*

$$d = n - k + 1$$

La quantité $n - k + 1$ est appelée la borne du singleton.

1.3 Codes dérivés

Dans ce paragraphe, nous allons construire de nouveaux codes à partir d'un code linéaire donné. Il existe d'autres constructions, On pourrait également combiner des codes entre eux (e.g. les codes concaténés, les codes produits, les turbo-codes).

Soit C un code linéaire de paramétres $[n, k, d]_q$.

Définition 18. *(**Produit sur** F_q) Par analogie avec le produit scalaire usuel ,on définit un produit sur $\mathbb{F}_q^n$, pour $x, y \in F_q^n$ on a*

$$x.y = \sum_{i=1}^{i=n} x_i y_i$$

Définition 19. *(**Code Dual**). Le dual de C est l'orthogonal $C^\perp$ de C dans $\mathbb{F}_q^n$.*

Exemple 2. *Sur $\mathbb{F}_2$ si $C = \{000, 111\}$ alors $C^\perp = \{000, 011, 110, 101\}$.*

Remarque 4. *Il s'agit d'un code linéaire $[n, n-k]_q$. On a l'égalité $dim(C)+dim(C^\perp) = n$. On ne sait pas en revanche exprimer la distance minimale du dual en fonction des paramètres de C. D'autre part, la dimension du dual est parfois appelée la codimension du code.*

Définition 20. *(**auto-dual**). Le code C est auto-dual si $C = C^\perp$.*

Définition 21. *(**auto-orthogonal**). Le code C est auto-orthogonal si $C \subset C^\perp$.*

Définition 22. *(**Hull**). Le hull de C est l'intersection de C et de$C^\perp$.*

Définition 23. *(**Matrice de parité**). Une matrice de parité de C est une matrice notée généralement H de type $(n-k, n)$ dont les lignes forment une base de$C^{\perp}$. Il s'agit d'une matrice génératrice de $C^{\perp}$.*

Remarque 5. *Un code linéaire peut être défini par sa matrice génératrice ou sa matrice dite **matrice de contrôle de parité** de C donné par :*

$$C = \{x \in \mathbb{F}_q^n / Hx^t = 0\}.$$

Pour tout $1 \leq i \leq n$, on notera c_i la i-ème composante d'un mot de longueur n. L'ensemble E désignera un sous-ensemble de $\{c_1, \ldots, c_n\}$.

Définition 24. *(**Code étendu**). Le code étendu $\hat{C}$ d'un code q-aire C défini est :*

$$\hat{C} = \{((c_1, \ldots, c_n, c_{n+1} = -\sum_{i=1}^{i=n} c_i), (c_1, \ldots, c_n) \in C\}$$

Remarque 6. *Pour $q = 2$, la dernière coordonnée de$C$ est celle du bit de parité. Le code $\hat{C}$ est linéaire et admet pour paramètres $[n+1, k, \hat{d}]$ avec $\hat{d} = d$ ou $d+1$. Dans le cas binaire, si d est impaire alors $\hat{d} = d + 1$.*

Définition 25. *(**Code de poids pair**). Un code binaire est un code de poids pair si tous ses mots ont un poids pair.*

Exemple 3. *Le code étendu d'un code binaire est un code de poids pair.*

Soit Ω un ensemble de cardinal n. Nous indexons les coordonnées des mots de $\mathbb{F}_q^n$ par cet ensemble, par exemple, $x = (x_\gamma)_{\gamma \in \Omega}$.

Définition 26. *(**Code poinçonné**) Le code poinçonné de C en J est composé de tous les mots de code de C avec les coordonnées indexées par J remplaçées par zéros où J est un sous-ensemble de Ω.*

Définition 27. *(**Code raccourci**) Le code raccourci de C en e est obtenu en poinçonnant en e, le sous-code de C contenant les mots dont toutes les composantes dans e valent 0.*

On peut également construire des codes sur $\mathbb{F}_q$ à partir de plusieurs codes définis sur $\mathbb{F}_q$, telle que l'intersection, la réunion , la somme directe ... , d'un nombre fini de codes linéaires (puisque on peut les considérer comme des sous -espaces vectoriels d'un meme espace vectoriel).

1.4 Conclution

Dans ce chapitre nous avons donné des notions de bases sur les codes correcteurs définis sur les corps finis, cela nous sera utile pour étudier un cas particulier de ces codes qui sont les codes cycliques.

Chapitre 2

Codes Cycliques Définis sur les Corps Finis

2.1 Rappels sur les corps finis

Nous rappelons dans cette section quelques notions sur les corps finis et leurs extensions qui seront utiles par la suite. Les énoncées donnés ici sont largement inspirés de ([20],[48],[46]) ouvrages auquels nous renvoyons le lecteur s'il désire les preuves complètes des résultats exposés ci-dessous.

2.1.1 Corps finis et extensions

Définition 28. *Soit $p > 1$ un nombre premier. On note $\mathbb{F}_p$ le corps fini à p éléments $\mathbb{Z}/p\mathbb{Z}$.*

Définition 29. *Soient K un sous-corps du corps K_0 et k la dimension de K_0 en tant que K-espace vectoriel. On dit que K_0 est une extension de degré k de K.*

Théorème 3. *1) Soit $\mathbb{F}$ un corps fini de cardinal q, $q > 1$. Alors $q = p^m$, où p est un nombre premier et m un entier positif.*

2) $\mathbb{F}$ est unique à isomorphisme prés.

Le corps de cardinal $q = p^m$, noté $\mathbb{F}_q$ est une extension de degré m du corps premier $\mathbb{F}_p$.

Proposition 3. *Pour tout entier $m > 1$, $\mathbb{F}_{q^m}$ est une extension de degré m de $\mathbb{F}_q$.*

Théorème 4. *Le groupe multiplicatif de $\mathbb{F}_q$, noté $\mathbb{F}_q^*$ muni de la multiplication est un groupe cyclique.*

Définition 30. *Un générateur de $\mathbb{F}_q^*$ est appelé élément primitif de $\mathbb{F}_q$.*

Théorème 5. *Soit $f(x) \in \mathbb{F}_q[x]$ un polynôme irréductible de degré m. Alors $f(x)$ possède une racine α dans F_{q^m} . De plus les racines de $f(x)$ sont simples et sont données par les éléments distincts suivants $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots \alpha^{q^{m-1}}\}$ des éléments de $\mathbb{F}_{q^m}$ qui sont appelés les conjugés de α pour F_q .*

Remarque 7. *Si α est un élément primitif de $\mathbb{F}_{q^m}$, alors ses conjugés sont aussi des éléments primitifs. On dira alors que $f(x)$ est un polynôme primitif.*

Théorème 6. *Soit $\mathbb{F}_q$ un corps fini, et soient m_1 et m_2 deux entiers strictement positifs. $\mathbb{F}_{q^{m_2}}$ est isomorphe à un sous-corps de $F_{q^{m_1}}$ si et seulement si m_2/m_1.*

2.1.2 Représentation polynômiale d'un corps fini

Si $f(x) \in \mathbb{F}_q[x]$, on note $(f(x))$ l'idéal de $\mathbb{F}_q[x]$ engendré par $f(x)$.

Proposition 4. *Soient un entier $m > 1$ et $f(x) \in \mathbb{F}_q[x]$, un polynôme irréductible de degré m. Alors l'anneau quotient $\mathbb{F}_q[x]/(f(x))$ est un corps fini de cardinal q^m, isomorphe à F_{q^m} .*

Cette proposition nous fournit une représentation des éléments de F_{q^m} par des polynômes à coéfficient dans F_q de degré au plus $m-1$ en une racine α de $f(x)$.

Nous allons maintenant nous intéresser à la factorisation du polynôme $x^n - 1$ sur $\mathbb{F}_q$.

2.1.3 La factorisation de $x^n - 1$

La factorisation du polynôme $x^n - 1$ joue un rôle important dans la recherche des codes cycliques de longueur n définis sur $\mathbb{F}_q$. 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 $\mathbb{F}_q$:

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

Pour cela on détermine les classes cyclotomiques modulo n,le nombre de classes donne le nombre de facteurs irréductibles. La donnée d'un polynôme irréductible diviseur particulier 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.
La factorisation de $x^n - 1$ s'écrit :

$$x^n - 1 = (x-1)f_1.f_2...f_r \quad avec \quad \sum_{i=1}^{r} degf_i = n - 1$$

si $f_i = a_0 + a_1x + ... + a_{k-1}x^{k-1} + a_kx^k \Rightarrow degf_i = k$ (plus haut degré de f_i) où les f_i sont des polynômes irréductibles, et sont également les polynômes minimaux correspondants aux classes cyclotomiques modulo n sur $\mathbb{F}_q$.

Les racines n-ièmes de l'unité

Soit $\mathbb{F}_q$ un corps fini de caractéristique p et $n = mp^h$, avec $(m, p) = 1$, alors le polynôme $x^n - 1$ admet la décomposition suivante :

$$x^n - 1 = x^{mp^h} - 1 = (x^m - 1)^{p^h}$$

Pour cela on se restreint au cas où n et q sont premiers entre eux.
On dénote par $\mathbb{F}_{q^s}$ le corps de décomposition de $x^n - 1$ sur $\mathbb{F}_q$, c'est l'extension de $\mathbb{F}_q$ qui contient toutes les racines du polynôme $x^n - 1$. Comme $(n, q) = 1$, la dérivée de $x^n - 1$ est égale à nx^{n-1} et donc $x^n - 1$ n'a aucune racine double, donc il admet n racines distinctes dans $\mathbb{F}_{q^s}$. Ces racines sont appelées **racines n-ièmes de l'unité** sur $\mathbb{F}_q$, elles forment le sous groupe E^n de $\mathbb{F}_{q^s}^*$ de cardinal n. Comme $\mathbb{F}_{q^s}^*$ est cyclique alors E^n est

cyclique d'ordre n. Un élément primitif de E^n est appelé **racine primitive n-ième de l'unité**. Donc si α est une racine primitive n-ième de l'unité, on a alors :

$$\alpha \in \mathbb{F}_{q^s} \Rightarrow \alpha^{q^s} = \alpha \Rightarrow \alpha^{q^s-1} = 1 \Rightarrow n|(q^s - 1).$$

L'entier s est appelé *l'ordre* de q modulo n et on le note par $s = ord_n q$, c'est le plus petit entier qui vérifie $q^s \equiv 1 \ mod \ n$.

Puisque tout groupe cyclique d'ordre n admet $\phi(n)$ éléments d'ordre n, alors il existe exactement $\phi(n)$ racines primitives n-ièmes de l'unité sur $\mathbb{F}_q$. En particulier puisque $\phi(n) > 0$, donc il existe une racine primitive n-ième de l'unité sur $\mathbb{F}_q$ pour tout entier positif n qui est relativement premier à q.

Le résultat suivant nous permet de trouver les racines primitives n-ièmes de l'unité.

Proposition 5. *Soit β un élément primitif du corps de décomposition $\mathbb{F}_{q^s}$ de $x^n - 1$, alors les racines primitives n-ièmes de l'unité sur $\mathbb{F}_q$ sont exactement les éléments de l'ensemble suivant :*

$$\{\beta^k \ / \ k = \frac{q^s - 1}{n} u, \ u < n, \ (u, n) = 1\}.$$

D'après cette proposition, si on a un élément primitif β de $\mathbb{F}_{q^s}$ avec $s = ord_n q$, alors on obtient une racine primitive n-ième de l'unité $\alpha = \beta^{\frac{q^s-1}{n}}$, donc les racines de $x^n - 1$ sont données par $1, \alpha, ..., \alpha^{n-1}$, d'où la décomposition de $x^n - 1$ dans $\mathbb{F}_{q^s}$:

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i). \tag{2.1}$$

Puisque les α^i sont distinctes, alors $x^n - 1$ n'est rien d'autre que le produit des polynômes minimaux de ces racines.

On rappelle la définition du polynôme minimal.

Définition 31. *Soit $\gamma \in \mathbb{F}_{q^s}$. Le **polynôme minimal** de γ sur $\mathbb{F}_q$ est le polynôme unitaire de plus bas degré $M_\gamma(x)$ dans $\mathbb{F}_q[x]$, vérifiant $M_\gamma(x) = 0$.*

Proposition 6. *Soient $\gamma \in \mathbb{F}_{q^s}$ et $M_\gamma(x)$ son polynôme minimal. Alors deg $M_\gamma(x) = d$ si et seulement si d est le plus petit entier positif vérifiant $\gamma^{q^d} = \gamma$.*

De la définition de l'ordre de q modulo l nous déduisons le corollaire suivant :

Corollaire 1. *Si $\gamma \in \mathbb{F}_{q^s}$ tel que l est l'ordre de γ, alors deg $M_\gamma(x) = ord_l\ q$.*

La proposition suivante donne la forme de $M_\gamma(x)$.

Proposition 7. *Soit α une racine primitive n-ième de l'unité de F_{q^s} et $\gamma = \alpha^j$. Alors le polynôme minimal de γ est donné par*

$$M_\gamma(x) = \prod_{i=0}^{ord_l q-1} (x - \alpha^{jq^i}). \tag{2.2}$$

La forme de $M_\gamma(x)$ donnée par cette proposition nous suggère de noter $M_\gamma(x)$ simplement par $M_j(x)$. à l'ensemble $\{\alpha^j, \alpha^{jq}, ..., \alpha^{jq^{ord_l q-1}}\}$ nous pouvons associer l'ensemble

$$C_j = \{j, jq, ..., jq^{ord_l\ q-1}\} mod\ n.$$

Cet ensemble est appelé **la classe cyclotomique** de j modulo n, et alors $r = ord_l\ q$ est le plus petit entier positif tel que $jq^r = j\ mod\ n$. Les entiers j et l sont reliés par le fait que l est l'ordre de $\gamma = \alpha^j$, i.e. $l = \dfrac{n}{(n, j)}$.

Remarque 8. *L'ordre de q modulo n vérifie les propriétés suivantes :*

1. *Si $n > 1$, alors $ord_n\ q$ est l'ordre de q dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$.*
2. *Si m est tel que $q^m = 1\ mod\ n$ alors $ord_n\ q$ divise m.*

De la proposition 7 et l'équation 2.2 nous obtenons la factorisation de $x^n - 1$ suivante :

$$x^n - 1 = \prod_{j \in K} M_j(x)$$

où K est un ensemble de représentants modulo n.

Remarque 9. *Si α est une racine primitive n-ième de l'unité, son polynôme minimal est M_1 et donc $ord_n\ q = |C_1| = deg\ M_1$.*

Définition 32. *Soient $i \in \mathbb{Z}_n$ et C_i la classe cyclotomique de i modulo n sur $\mathbb{F}_q$. Alors C_i est dite **réversible** si elle satisfait,*

$$C_i = C_{-i}.$$

Dans ce qui suit nous démontrons le lemme suivant :

Lemme 1.

Si C_1 est réversible, alors $\forall j \in \mathbb{Z}_n, C_j$ est réversible.

Preuve: Si C_1 est réversible, alors il existe k, $1 \leq k \leq ord_n(q)$ tel que $q^k \equiv -1 \mod n$, il s'ensuit que $jq^k \equiv -j \mod n$, d'où $C_j = C_{-j}$. □

Lemme 2. *S'il existe $i > 0$ tel que $q^i \equiv -1 \mod n$, alors C_1 est réversible.*

Preuve: Puisque $C_1 = \{1, q, \ldots, q^{r-1}\} \mod n$, où $r = ord_n q$, alors il suffit de vérifier l'existence d'un entier k, $1 \leq k \leq ord_n q$, tel que $q^k \equiv -1 \mod n$. Nous avons $i \equiv j \mod n$. Pour $j > 0$ il suffit de prendre $k = j$. Pour $j < 0$ il suffit de prendre $k = j + ord_n q > 0$. □

Exemple 4. *On prend $n = 7$ et $q = 2$. Les classes cyclotomiques correspondantes à 2 modulo 7 sont les classes suivantes :*

$$C_0 = \{0\},\ C_1 = \{1, 2, 4\},\ C_3 = \{3, 5, 6\}$$

Puisque $x^7 - 1 = M_0(x).M_1(x).M_3(x)$, où les $M_j(x)$ sont les polynômes minimaux respectifs, on a :
$M_0(x) = x - 1$ correspond à la classe cyclotomique C_0.
$M_1(x) = x^3 + x + 1$ correspond à la classe cyclotomique C_1.
$M_3(x) = x^3 + x^2 + 1$ correspond à la classe cyclotomique C_3.
Donc la factorisation de $x^7 - 1$ s'écrit $x^7 - 1 = (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1)$.

2.2 Structure des codes cycliques définis sur les corps finis

Les codes cycliques représentent la famille de codes la plus importante. D'un point de vue pratique, ce sont les codes les plus utilisés car leur mise en oeuvre est facile et ils admettent de bons algorithmes de décodage. D'un point de vue théorique, ils possèdent

une structure algébrique intéressante. Les codes cycliques les plus connus sont les codes de Hamming, BCH, Reed-Solomon, Résidus quadratiques,Duadiques, etc.

Définition 33. *Un code linéaire C de longueur n sur $\mathbb{F}_q[x]$ est dit* ***cyclique*** *si l'ensemble de ses mots est invariants par décalage circulaire à droite :*

$$(c_0, c_1..., c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, ..., c_{n-2}) \in C$$

Ainsi, par deux décalages circulaires successifs on a :

$$(c_{n-1}, c_0, c_1, ..., c_{n-2}) \in C \Rightarrow (c_{n-2}, c_{n-1}, c_0, c_1, ..., c_{n-3}) \in C$$

De manière général, par m décalages circulaires successifs on a :

$$(c_{n-m+1}, ..., c_{n-1}, c_0, ..., c_{n-m}) \in C \Rightarrow (c_{n-m}, ..., c_{n-1}, c_0, ..., c_{n-m-1}) \in C$$

Exemple 5. *1. Les codes triviaux $\{0\}$ et $\mathbb{F}_q^n$ sont cycliques.*

2. Le code binaire $C = \{000, 101, 011, 110\}$ est un code cyclique.

3. Le code binaire $C = \{0000, 1001, 0110, 1111\}$ n'est pas cyclique.

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

$$x.c(x) = c_0x + c_1x^2 + ... + c_{n-1}x^n = c_{n-1} + c_0x + ... + c_{n-2}x^{n-1}$$

Ce dernier polynôme correspond au mot $(c_{n-1}, c_0, c_1, ..., c_{n-2}) \in C$ obtenu par un décalage circulaire.

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

$$x^m c(x) = c_0x^m + c_1x^{m+1} + ... + c_{n-m}x^n = c_{n-m} + c_0x^m + ... + c_{n-m-1}x^{n-1}$$

Ce dernier polynôme correspond au mot $(c_{n-m}, ..., c_{n-1}, c_0, ..., c_{n-m-1}) \in C$ obtenu par m décalages circulaires à droite.

On peut donc traduire la cyclicité d'un code C en concidérant l'ensemble $C(x)$ des polynômes associés aux mots du code C et en demandant que cet ensemble $C(x)$ soit fermé pour les deux opérations suivantes :

- Si $c_1(x)$ et $c_2(x) \in C(x) \subset \mathbb{F}[x]$ alors $c_1(x) + c_2(x) \in C(x)$ (linéarité).
- Si $c(x) \in C(x)$ alors $x.c(x)$ *mod* $(x^n - 1)$ est encore dans $C(x)$ (cyclicité).

Ce qui précède se résume en disant que l'image de $C(x)$ dans l'anneau $R_n = \mathbb{F}_q[x]/x^n - 1$ est un idéal de R_n.

Théorème 7. *C est cyclique si et seulement si $C(x)$ est un idéal de $\mathbb{F}_q[x]/(x^n - 1)$*

Remarque 10.
- *Si $(n, q) = 1$ on appelle les codes cycliques de longueur n définis sur F_q ,* ***codes cycliques à racines simples***
- *Si $(n, q) \neq 1$ on appelle les codes cycliques de longueur n définis sur F_q ,****codes cycliques à racines multiples***

2.2.1 Polynôme générateur et polynôme de contrôle

Si $f(x)$ est irréductible sur $\mathbb{F}_q$ alors $\mathbb{F}[x]/(f(x))$ est un corps,donc ses seuls idéaux sont $\langle o \rangle$ ou $\langle 1 \rangle$. On déduit par le théoreme des restes chinois, que R_n est un anneau principal, donc C est un idéal principal engendré par un polynôme $g(x)$.

Définition 34. *Le polynôme* ***générateur*** *$g(x)$ d'un code cyclique C est un polynôme non nul unitaire de plus bas degré de C.*

Proposition 8. *Le polynôme générateur est unique.*

Preuve: Supposons que g_1 et g_2 soient deux polynômes générateurs. Alors $g_1 - g_2$ est un polynôme générateur (le code est linéaire) de degré strictement inférieur au degré des g_i. Contradiction.

Proposition 9. *Tout mot d'un code cyclique est un multiple du polynôme générateur. On note* $C =< g(x) >$.

Preuve: Soit $c(x) \in C$ on effectue la division euclidienne de $c(x)$ par $g(x)$: $c(x) = a(x)g(x)+r(x)$ avec $deg\ (r(x)) < deg\,(g(x))$. Or, le reste $r(x)$ qui est la différence de deux mots du code appartient au code. Si $r(x) \neq 0$, on contredit l'hypothèse sur le degré minimum de $g(x)$.

Proposition 10. *Le polynôme générateur divise* $x^n - 1$.

Preuve: On a $x^n - 1 = ag + r$ avec $deg\ (r) < deg\ (g)$ et on conclut comme précédemment que r doit être nul (après réduction modulo $x^n - 1$).

Proposition 11. *La dimension* k *du code cyclique* C *est* $n - r$*, où* $r = deg\ (g)$.

Preuve: Tout mot du code peut être vu comme un polynôme de degré au plus $n - 1$, multiple d'un polynôme de degré $deg\,(g)$. Ces polynômes peuvent donc s'écrire sous la forme $g(x).h(x)$ pour $deg\ (h) \leq n-1-deg\ (g)$, il y a donc exactement $q^{n-deg(g)}$ mots possibles qui par constructions sont tous distincts et donc la dimension du code est $k = n - deg\,(g)$.

Réciproquement, tout polynôme unitaire $g(x)$ de degré $n - k$, divisant $x^n - 1$ est le polynôme générateur d'un code cyclique de longueur n et de dimension k.

Remarque 11. *D'après ce qui précède, il découle que pour déterminer les codes cycliques de longueur* n *de dimension* k *sur un corps* $\mathbb{F}_q$*, il suffit de déterminer les polynômes unitaires de degré* $n - k$ *divisant* $x^n - 1$ *dans* $\mathbb{F}_q[x]$.

Définition 35. *Soit* C *un code cyclique de longueur* n *et de dimension* k *sur* $\mathbb{F}_q$*, de polynôme générateur* g*. On appelle* ***polynôme de contrôle*** *de* C *le polynôme* h *tel que* $h(x) = \dfrac{x^n - 1}{g(x)}$*. Comme* g *est unitaire de degré* $n - k$*, le polynôme de contrôle* h *est unitaire de degré* k.

Réciproquement, tout polynôme unitaire h de degré k, divisant x^n-1 est le polynôme de contrôle d'un code cyclique de longueur n et de dimension k.

2.2.2 Représentation matricielle

Soit C un code cyclique de longueur n et de dimension k sur $\mathbb{F}_q$.

Soient $g = \sum_{i=0}^{r} g_i x^i$ et $h = \sum_{i=0}^{k} h_i x^i$ respectivement le polynôme générateur et le polynôme de contrôle de C. On a vu que tout mot $c \in C$ peut s'obtenir en multipliant g (de degré r) par un polynôme a sans avoir à réduire modulo $x^n - 1$: $c(x) = a(x)g(x)$. Puisque $deg\,(c(x)) < n$ et $deg\,(g(x)) = r$, on obtient $deg\,(a(x)) < n - r$.

Utilisons maintenant la notation matricielle. On a : $c = aG$ où $c = (c_0, ..., c_{n-1})$, $a = (a_0, ..., a_{n-r})$ et G est une matrice circulaire $k \times n$ donnée par :

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \dots & g_r & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & g_2 & \dots & g_r & 0 & \dots & 0 \\ 0 & 0 & g_0 & g_1 & \dots & \dots & g_r & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & g_0 & g_1 & \dots & g_r \end{pmatrix}$$

G est appelée **matrice génératrice** du code C de longueur n et de dimension $k = n - r$ où $r = deg\,(g(x))$

Une matrice de contrôle du code C est donnée par :

$$H = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & h_{k-2} & \dots & h_0 & 0 & \dots & 0 \\ 0 & 0 & h_k & h_{k-1} & h_{k-2} & \dots & h_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & h_k & h_{k-1} & \dots & h_0 \end{pmatrix}$$

2.2.3 Dual d'un code cyclique

Définition 36. ***Polynôme réciproque*** *soit $f(x)$ un polynôme de degré n on définit son polynôme réciproque par*

$$f^\star(x) = x^n f(\frac{1}{x})$$

Proposition 12. *Soit C un code cyclique de dimension k engendré par le polynôme $g(x)$ de degré r, alors le code $C^{\perp}$ dual de C est un code cyclique engendré par $g^{\perp}(x) = h^*(x) = x^k h(x^{-1})$, avec $h(x) = \dfrac{x^n - 1}{g(x)}$.*

Exemple 6. *Déterminons les codes cycliques binaires de longueur 7.*
La factorisation en produit de polynômes irréductibles de $x^7 - 1$ sur $\mathbb{F}_2$ est $x^7 - 1 = (x-1)(x^3 + x + 1)(x^3 + x^2 + 1)$. On obtient alors $2^3 = 8$ codes cycliques binaires de longueur 7. dont, par exemple :

- *Le code C_1 engendré par $g_1 = 1$, $h_1 = x^n - 1$ est $\mathbb{F}_q^n$.*
- *Le code C_2 engendré par $g_2 = x - 1$, $h_2 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, est le code de contrôle de parité.*
- *Le code C_3 engendré par $g_3 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, est le code répétition.*
- *Le code C_4 engendré par $g_4 = x^3 + x^2 + 1$, a pour polynôme de contrôle $h_4 = (x-1)(x^3 + x + 1) = x^4 + x^3 + x^2 + 1$. Une matrice génératrice G et une matrice de contrôle H sont donc*

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

C'est un code de Hamming, qui est donc un code cyclique.
Soit $C_4^{\perp}$ le dual du code C_4, alors $g_4^{\perp} = x^4 h_4(x^{-1}) = x^4 + x^2 + x + 1$ est le polynôme générateur de $C_4^{\perp}$.

Il existe une autre manière de définir un code cycliques par ce que l'on appelle l'ensemble de définition :

Soit α est une racine primitive n-ième de l'unité sur le corps F_q, et codes cycliques de longueur n sur F_q, et soit $S \subset \{0, 1, ..., n-1\}$.On peut défini un code C de longueur n sur F_q comme ce suit :

$$c(x) \in C \; ssi \; c(\alpha^i) = 0, i \in S$$

On appelle **ensemble de définition** du code C, un sous ensemble de $Z_n = \{1, ..., n\}$ défini par :

$$T = \left\{ i \in Z_n \mid g(\alpha^i) = 0 \right\}.$$

Quelques propriétés de l'ensemble de définition d'un code cyclique sont données par la proposition suivante :

Proposition 13. *soit T l'ensemble de définition d'un code cyclique C engendré par g, alors on a :*

- *$T = \cup C_s$, la réunion est sur toutes les classes cyclotomiques C_s telle que M_s divise g.*
- *deg $g = |T|$ et alors dim $C = n - |T|$.*
- $C = \left\{ f(x) \ mod \ (x^n - 1) \mid f(\alpha^i) = 0 \ \forall i \in T \right\}.$

L'ensemble de définition de code dual $C^{\perp}$ est défini par :

$$T^{\perp} = \{ s \in Z_n | \ n - s \notin T \} = Z_n / (-T).$$

Remarque 12. *Soit $f(x)$ un polynôme de $\mathbb{F}_q[x]$ tel que $f(0) \neq 0$. Puisque $f^*(x) = x^{deg(f)} f(x^{-1})$ alors si T est le domaine de définition de $f(x)$,$-T$ est le domaine de $f^*(x)$.*

2.2.4 Distance minimale d'un code cyclique

Le taux de correction (k/n) d'un code cyclique est difficile à calculer. Cependant, nous donnons ci-après le théorème suivant qui permet de garantir une minoration de la distance minimale d'un code cyclique et par suite une minoration du taux de détection. Ce théorème est de plus constructif :
il permet la construction de codes cycliques ayant un taux de correction garanti.

On suppose que n est premier avec q. Soit alors α une racine primitive de $x^n - 1$ dans $\mathbb{F}_q[x]$; soit C un code cyclique de polynôme générateur $g(x)$ divisant $x^n - 1$, on a $g(x) = \prod_{j \in K} (x - \alpha^j)$ où $K \subset \{0, 1, ..., n-1\}$ est la réunion de classes cyclotomiques

relatives à q modulo n. Le théorème suivant montre que l'analyse de K permet d'avoir une minoration de la distance minimale d du code C.

Théorème 8. *On suppose que n est premier avec q.*
Si il existe un entier a tel que $\{a+1, a+2, ..., a+s\} \subset K$ alors $d \geq s+1$.
Le code C est donc au moins s-détecteur et $[s/2]$-correcteur.

Exemple 7. *Nous avons vu que les classes cyclotomiques relatives à 2 modulo 7 sont :*

- $C_0 = \{0\}$ *;* $M_0 = x - 1$.
- $C_1 = \{1, 2, 4\}$ *;* $M_1 = (x^3 + x + 1)$.
- $C_3 = \{3, 6, 5\}$ *;* $M_3 = (x^3 + x^2 + 1)$.

On a : $\{1, 2\} \subset C_1$. *Ici,* $s = 2$ *: le code* $(7, 4)$ *associé à* M_1 *est donc au moins* 1*-correcteur.*
De la même façon, on a $\{5, 6\} \subset C_3$ *; le code* $(7, 4)$ *associé à* M_3 *est donc aussi au moins* 1*-correcteur (c'est un code de Hamming).*
Considérons maintenant le code C associé au polynôme $g = M_1.M_3$; comme g est de degré 6*, C est un code* $(7, 1)$ *qui comporte* 6 *bits de redondance. Il est caractérisé par la classe* $k = C_1 \cap C_3 = \{1, 2, 3, 4, 5, 6\}$ *; ici,* $s = 6$. *Ce code est donc au moins* 3*-correcteur.*

2.2.5 Borne BCH

La borne BCH est par la suite utilisé pour la définition des codes BCH ;
Soit C un code cyclique ; on rappelle que l'on nomme ensemble de définition T du code C l'ensemble des i tels que α^i est un zéro de C.
On dira qu'il contient un ensemble de s éléments consécutifs s'il existe un ensemble $\{b, b+1, ..., b+s-1\}$ d'entiers consécutifs tel que

$$\{b, b+1, ..., b+s-1\} \ (mod\ n) \ \subset \ T.$$

Théorème 9. *Soit C un code cyclique de longueur n sur $\mathbb{F}_q$ avec un ensemble de définitions T si l'on note d la distance minimale du code C et si T contient $\delta - 1$ éléments consécutifs, alors $\leq \delta \ \leq \ d$.*

Remarque 13. *La valeur δ est une distance construite du code .*
δ constitue une minoration de la vraie distance minimale d du code ; en pratique, il y a souvent très peu de différence entre δ et d.

Comme exemple de codes cycliques nous allons voir les codes BCH.

2.2.6 Les Codes BCH

Dans cette section, on examine un membre très important de la famille des codes cycliques, c'est bien les codes BCH.
en même temps que les codes BCH ont été apparu, *Reed* et *Solomon* ont publié leur travail sur les codes qui ont pris leurs noms.

Définition 37. *Soient n et q deux entiers premier entre eux, et soit α une racine n-ième de l'unité sur $\mathbb{F}_q^{(ord\, n\, /q)}$.*
soit δ un entier avec $2 \leq \delta \leq n$, un code BCH sur $\mathbb{F}_q$ de longueur n et de distance construite δ est un code cyclique avec l'ensemble de définitions

$$T = C_b \cup C_{b+1} \cup ... \cup C_{b+\delta-2}$$

ou C_i désigne la $q-classe$ cyclotomique modulo n contenant i.

Pour différentes indices b on obtient des codes différents. Pour $b = 1$ on parle de code BCH au sens strict, si de plus n est de la forme $q^t - 1$ avec t quelconque on parle de code BCH primitif.

Théorème 10. *Soit C un code BCH $[n,k]_q$ de distance construite δ, alors :*

1) $k \geq n - ord(n).(\delta - 1)$

2) si $q = 2$ et si C est un code BCH au sens strict, alors on peut restreindre δ au cas ou δ est impaire ; de plus, si l'on écrit $\delta = 2w + 1$, alors $k \geq n - ord_q(n).w$

Théorème 11. *Pour $i = 1$ et 2*

Soit C_i un code BCH sur $\mathbb{F}_q$ avec domaine de définition

$$T_i = C_b \cup C_{b+1} \cup ... \cup C_{b+\delta_i-2}$$

où $\delta_1 < \delta_2$ alors, $C_1 \subseteq C_2$

Exemple 8. *Prenons la longueur 15 sur $\mathbb{F}_2$, des codes BCH au sens strict qui sont primitifs .*

$* \delta = 3$ *donne* $T = C_1 \cup C_2 = C_1 = \{1, 2, 4, 8\}$ *soit* $[15, 11, d \geq 3]$

$* \delta = 4$ *donne* $T = C_1 \cup C_2 \cup C_3 = C_1 \cup C_3 = \{1, 2, 3, 4, 6, 8, 9, 12\}$ *soit* $[15, 7, d \geq 5]$

$* \delta = 5$ *n'ajoute rien par rapport au cas* $\delta = 4$

$* \delta = 6$ *et* $\delta = 7$ *donnent* $T = C_1 \cup C_3 \cup C_5$ *soit* $[15, 5, d \geq 7]$

$* \delta = 8$ *et plus donne* $[15, 1, 15]$ *; car il n y a plus de classe cyclotomique à ajouter (à part* 0*).*

2.2.7 Les codes de Reed-Solomon

Définition 38. *[40] Un code de Reed-Solomon est un code BCH sur F_q de longueur $n = q - 1$.*

Proposition 14. *Les codes de Reed-Solomon sont MDS.(voir chapitre 1)*

2.2.8 L'idempotent d'un code cyclique

Tous les codes cycliques sur $F_q$sont engendrés par des polynômes générateurs. Il y a d'autre polynômes très particuliers appelés idempotents générateurs, qu'on peut utiliser pour engendrer un code cyclique.

Définition 39. *Un générateur e(x) d'un idéal de R_n qui vérifie $e^2(x) \equiv e(x)$ est appelé idempotent générateur.*

Exemple 9. *On a par exemple* $x^3 + x^5 + x^6$ *est un idempotent générateur dans* $R_7 = F_2[x]/(x^7 - 1)$ *; car*

$$(x^3 + x^5 + x^6)^2 \equiv x^3 + x^5 + x^6$$

Par la suite nous allons énumérer quelques propriétés ([46] chapitre 4, section 3) de l'idempotent :

Soit C un code cyclique dans R_n, alors

- Il existe un unique idempotent $e(x) \in C$ tel que $C = \langle e(x) \rangle$
- Un code cyclique est engendré par $e(x)$, alors pour chaque mot $c(x)$ de code C on peut l'écrire comme $c(x)e(x)$.
- Si e(x) est un idempotent non nul dans C, alors $C = \langle e(x) \rangle$ si et seulement si $e(x)$ est un élément inversible.
- le polynôme générateur g(x) du code C d'idempotent e(x) est obtenu par :

$$g(x) = p.g.c.d(e(x), x^n - 1).$$

Théorème 12. *([46] page 135) Soit* C_1 *et* C_2 *deux codes cycliques de longueur n sur* F_q *avec les polynômes générateurs* $g_1(x)$, $g_2(x)$ *et les idempotents générateurs* $e_1(x), e_2(x)$*tel que :*

i) $C_1 \cap C_2$ *est de polynôme générateur égale le* $ppcm(g_1(x), g_1(x))$ *a un idempotent* $e_1(x)e_2(x)$.

ii) $C_1 + C_2$ *est de polynôme générateur égale le* $pgcd(g_1(x), g_1(x))$ *et un idempotent* $e_1(x) + e_2(x) - e_1(x)e_2(x)$.

Pour calculer les idempotents générateurs d'un code cyclique de longueur n on suit les étapes suivantes :

1. On calcule $h(x)$ tel que $h(x) = (x^n - 1)/g(x)$.
2. On cherche $r(x)$ et $s(x)$ par l'algorithme d' Euclide telle que

$$r(x)g(x) + s(x)h(x) = 1$$

3. $e(x) = r(x)g(x)$.

Exemple 10. *Dans La table suivante on donne tous les codes cycliques C_i, de la longueur 9 sur F_2 avec leurs polynômes générateurs $g_i(x)$ et leurs idempotents générateurs $e_i(x)$:*

i	dim	$g_i(x)$	$e_i(x)$
0	0	$1 + x^9$	0
1	1	$1 + x + ... + x^8$	$1 + x + ... + x^8$
2	2	$1 + x + x^3 + x^4 + x^6 + x^7$	$x + x^2 + x^4 + x^5 + x^7 + x^8$
3	3	$1 + x^3 + x^6$	$1 + x^3 + x^6$
4	6	$1 + x^3$	$x^3 + x^6$
5	7	$1 + x + x^2$	$1 + x + x^2 + x^4 + x^5 + x^7 + x^8$
6	8	$1 + x$	$x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8$
7	9	1	1

Soit α une racine primitive n-ième de l'unité sur le corps F_q, et soit C est un code cyclique de longueur n sur F_q avec l'ensemble de définition $T = \left\{ i \in Z_n \mid g(\alpha^i) = 0 \right\}$.

Théorème 13. *Si $e(x) \in R_n$, alors $e(x)$ est un idempotent de C si et seulement si*

$$e(\alpha_i) = 0 \text{ si } i \in T, \text{ et } e(\alpha_i) = 1 \text{ si } i \in \{0, 1, ..., n-1\} / T.$$

Remarque 14. *Pour avoir les idempotent générateurs nous ne somme pas obligé de fctoriser $x^n - 1$ sur $\mathbb{F}_q$.*

2.3 Codes Résidus Quadratiques

On présente dans cette section,les codes Résidus Quadratiques qui sont un cas particulier de codes cycliques et qui ont des propriétés très importants. Mais avant de donner la définition exacte de ces codes on commence par quelques propriétés des résidus quadratiques.

2.3.1 Résidus Quadratiques modulo un nombre premier

Définition 40. *Soit p un nombre premier impair. Un entier a est* ***un résidu quadratique*** *si et seulement si a est premier avec p et il existe x tel que*

$$a \equiv x^2 (mod p)$$

en d'autre terme on dit que a est un résidu quadratique modulo p si a est une racine carrée modulo p.

Exemple 11. *2 est un résidu quadratique modulo 17 car :*

$$2 \equiv 6^2 (mod\ 17).$$

L'ensemble des résidus quadratiques modulo p est une partition de l'ensemble $Z_p^* = \{1, 2, .., p-1\}$, noté **QR**, un entier a premier avec p qui n'est pas un résidu quadratique est appelé un non-résidu quadratique,et de même l'ensemble des non-résidus quadratiques est une partition de Z_p^*,noté **NQR**. On a alors

$$Z_p = \{0\} \cup QR \cup NQR.$$

Ces deux ensembles vérifies quelques propriétés sont données par le lemme suivant :

Lemme 3. *([46]page 237) Soit p un nombre premier impair. Alors on a :*

i) $|QR| = |NQR| = (p-1)/2$.

ii) Modulo p, on a $QR\, a = QR$; $NQR\, a = NQR$;

$QR\, b = NQR$; $NQR\, b = QR$

tel que : $a \in QR$, $b \in NQR$.

Exemple 12. *Les résidus quadratiques modulo 11 sont :*

$$1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 16 \equiv 5, 5^2 = 25 \equiv 3.$$

Alors $QR = \{1, 3, 4, 5, 9\}$; $NQR = \{2, 6, 7, 8, 10\}$

2.3.2 Symbole de Legendre

Définition 41. *Soit p un nombre premier impair, et a un entier tel que $(a,p)=1$. On appelle* ***Symbole de Legendre*** *noté $(\frac{a}{p})$, et défini par :*

$$(\frac{a}{p}) = \begin{cases} 1 & \text{si } a \text{ est résidu quadratique} \\ -1 & \text{si } a \text{ est non-réidu quadratique} \end{cases}$$

Nous résumons les propriétés du Symbole de Legendre dans le théorème suivant :

Théorème 14. *([48]) Soit p, q deux nombres premiers impairs tel que $p \neq q$, et $(a,p)=(b,p)=1$.*

1) $(\frac{1}{p}) = (\frac{a^2}{p}) = 1$.
2) *Si $a \equiv b \ mod\ p$, alors $(\frac{a}{p}) = (\frac{b}{p})$.*
3) *L'écriture d'Euler : $(\frac{a}{p}) \equiv a^{(p-1)/2} \ mod\ p$.*
4) $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.
5) $(\frac{-1}{p}) = 1$ *si seulement si* $p \equiv 1 \ mod\ 4$.
6) $(\frac{2}{p}) = 1$ *si seulement si* $p \equiv \pm 1 \ mod\ 8$.
7) $(\frac{3}{p}) = 1$ *si seulement si* $p \equiv \pm 1 \ mod\ 12$.

Exemple 13.

$$(\frac{-a^2}{p}) = (\frac{-1}{p})(\frac{a^2}{p}) = (\frac{-1}{p}) = (-1)^{(p-1)/2}$$

alors on a $x^2 = -a^2 \ mod\ p$a une solution si seulement si $p \equiv 1 \ mod\ 4$.

Exemple 14. *On considère le congruence*

$$x^2 = 15 \ mod\ 19$$

On a

$$(\frac{15}{19}) = (\frac{-4}{19}) = (\frac{-1}{19})(\frac{2}{19})^2 = (\frac{-1}{19}) = -1$$

Mais on a $19 \equiv 1 \ mod\ 4$ alors pas de solution dans cette congruence.

2.3.3 les codes Résidus Quadratiques

Soit α est une racine primitive n-ième de l'unité sur le corps F_q, soit QR et NQR l'ensemble des résidus quadratiques et résidus non-quadratiques alors on peut définir deux classes cyclotomiques avec ces deux ensembles et par suite on obtient deux polynômes minimaux définis comme suit :

$$Q(x) = \prod_{i \in QR} (x - \alpha^i)$$

et

$$N(x) = \prod_{j \in NQR} (x - \alpha^j)$$

La factorisation de $x^p - 1$ dans F_q est

$$x^p - 1 = (x - 1)Q(x)N(x)$$

On peut maintenant présenter les codes résidus quadratiques comme suit :

Définition 42. *Soit p un nombre premier impair,et q une puissance d'un nombre premier tel que* $(p, q) = 1$.
Le code cyclique sur F_q *engendré par l'un des Polynômes suivent :*

$$Q(x), (x - 1)Q(x)$$

$$N(x), (x - 1)N(x)$$

de longueur p dans

$$R_n = F_q[x]/(x^n - 1)$$

est appelé un code résidu quadratique.

2.3.4 L'existence des codes Résidus Quadratiques

Théorème 15. *[?] Un code résidu quadratique de longueur un nombre premier p impair défini sur le corps* F_q *existe si seulement si* $q \in QR$.

2.3.5 Exemples de codes résidus quadratiques

1) Soit $p = 7$ et $q = 2$. Soit α est une racine primitive 7-ième de l'unité sur le corps F_2.

$$QR = \{1, 2, 4\}$$

$$NQR = \{3, 5, 6\}$$

on retrouve ces polynômes minimaux.

$$Q = (x - \alpha)(x - \alpha^2)(x - \alpha^4) = (x^3 + x + 1)$$

$$N = (x - \alpha^3)(x - \alpha^5)(x - \alpha^6) = (x^3 + x^2 + 1)$$

Les codes Résidus Quadratiques de longueur 7 sur $\mathbb{F}_2$ sont :

$$\left\langle (x^3 + x + 1) \right\rangle \ , \ \left\langle (x^3 + x^2 + 1) \right\rangle$$

$$\left\langle (x - 1)(x^3 + x + 1) \right\rangle \ , \ \left\langle (x - 1)(x^3 + x^2 + 1) \right\rangle$$

2) Soit $p = 11$ et $q = 3$. Soit α est une racine primitive n-ième de l'unité sur le corps F_3 on a

$$QR = \{1, 4, 5, 9, 3\}$$

$$NQR = \{2, 8, 10, 7, 6\}$$

alors les polynômes minimaux sur F_3 sont :

$$Q(x) = \prod_{i \in QR} (x - \alpha^i)$$

$$= (x - \alpha)(x - \alpha^4)(x - \alpha^5)(x - \alpha^9)(x - \alpha^3)$$

$$= 2 + x^2 + 2x^3 + x^4 + x^5.$$

et

$$N(x) = \prod_{j \in NQR} (x - \alpha^j)$$

$$= (x - \alpha^2)(x - \alpha^8)(x - \alpha^{10})(x - \alpha^7)(x - \alpha^6)$$

$$= 2 + 2x + x^2 + 2x^3 + x^5.$$

La factorisation de $x^{11} - 1$ dans F_3est :

$$x^{11} - 1 = (x - 1)(2 + x^2 + 2x^3 + x^4 + x^5)(2 + 2x + x^2 + 2x^3 + x^5).$$

Les codes Résidus Quadratiques de longueur 11 sur $\mathbb{F}_3$ sont :

$$\left\langle (2 + x^2 + 2x^3 + x^4 + x^5) \right\rangle \ , \ \left\langle (2 + 2x + x^2 + 2x^3 + x^5) \right\rangle$$

$$\left\langle (x - 1)(2 + x^2 + 2x^3 + x^4 + x^5) \right\rangle \ , \ \left\langle (x - 1)(2 + 2x + x^2 + 2x^3 + x^5) \right\rangle$$

2.4 Codes Duadiques définis sur les corps finis

La famille des codes duadiques, qui contient les codes résidus quadratiques (QR), a été introduite par J.S Leon et al [36]. Leurs distances minimales (pour des longueurs $n \leq 241$) ont été données par [55]. Les codes duadiques contiennent beaucoup de codes qui ont les meilleurs paramètres connus à ce jour. Soient q une puissance d'un nombre premier et n un entier impair premier avec q.

Pour un entier s premier avec n on appelle **multiplicateur** une application

$$\mu_s : \frac{\mathbb{F}_q[x]}{x^n - 1} \longmapsto \frac{\mathbb{F}_q[x]}{x^n - 1}$$

définie par :

$$\mu_s(c(x)) = c(x^s)(\mod (x^n - 1)).$$

Au fait l'application μ_s est un automorphisme d'anneaux de $\dfrac{\mathbb{F}_q[x]}{x^n - 1}$.
Si C est un code cyclique, on définit $\mu_s(C) = \{\mu_s(c(x)) = c(x^s) | c(x) \in C\} = \{c(x^s) \,|\, c(x) \in C\}$.

μ_s induit aussi une permutation sur $\mathbb{Z}_n$, définie par :

$$\mu_s : i \longmapsto is \mod n.$$

L'ensemble de définition de $\mu_s(C)$ est donné par le lemme suivant :

Lemme 4. *[46, corollaire 4.4.5] Soit C un code cyclique de longueur n sur $\mathbb{F}_q$, ayant pour ensemble de définition T, alors $\mu_s(C)$ est un code cyclique d'ensemble de définition $s^{-1}T$.*

Dans ce qui suit on donnera un rappel des définitions et des propriétés connues sur les codes duadiques. On commence par la définition du splitting donné comme suit :

Soient S_1 et S_2 des réunions de classes cyclotomiques modulo n, tels que :

1. $S_1 \cap S_2 = \emptyset$,
2. $S_1 \cup S_2 = \mathbb{Z}_n \setminus \{0\}$ et
3. $\mu_s(S_i \mod n) = S_{(i+1) \mod 2}$.

Le triplet μ_s, S_1, S_2 est appelé **splitting** modulo n. Ce splitting donne un quadriplet de codes ; deux codes cycliques sur $\mathbb{F}_q$, D_1 et D_2 ayant pour ensembles de définitions respectifs S_1 et S_2 et qui sont appelés **les codes duadiques odd-like** et deux codes cycliques C_1 et C_2 sur $\mathbb{F}_q$ admettant pour ensembles de définitions respectifs $\{0\} \cup S_1$ et $\{0\} \cup S_2$ et qui sont appelés **les codes duadique even-like**.

De la dernière propriété nous obtenons que $|S_1| = |S_2|$, et alors $|S_i| = \dfrac{n-1}{2}$ ce qui justifie le choix de n impair.

Autrement, si on considère une racine primitive $n$ième de l'unité α de $\mathbb{F}_q$, les codes D_i sont des codes cycliques de polynômes générateurs

$$g_i = \prod_{j \in S_i} (x - \alpha^j),$$

les codes C_i ont pour polynômes générateurs $g_i(x-1)$ et alors $\dim D_i = \dfrac{n+1}{2}$ et $\dim C_i = \dfrac{n-1}{2}$.

Remarque 15. *Nous avons une caractéristique des mots des codes D_i et C_i, en effet :*

$$\forall \mathsf{x} = (x_1, \ldots, x_n) \in D_i, \text{ alors } \mathsf{x} \text{ vérifie } \sum x_i \neq 0$$

$$\forall \mathsf{x} = (x_1, \ldots, x_n) \in C_i, \text{ alors } \mathsf{x} \text{ vérifie } \sum x_i = 0.$$

Le théorème suivant prouvé par M. Smid [55] donne une condition nécessaire et suffisante sur l'existence des codes duadiques sur $\mathbb{F}_q$.

Théorème 16. *Les codes duadiques de longueur n sur $\mathbb{F}_q$ existent si et seulement si $q \equiv \square \mod n$, i.e., si $n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$, alors il existe un code duadique sur $\mathbb{F}_q$ si et seulement si $q \equiv \square \mod p_i$ avec $i \in \{1, 2, \dots, s\}$.*

Exemples :

5 est un résidu quadratique modulo 11 ($5 = 4^2 \mod 11$). Nous avons les classes cyclotomiques suivantes :

$$S_0 = \{0\}, S_1 = \{1, 3, 4, 5, 9\} \text{ et } S_2 = \{2, 6, 7, 8, 10\},$$

ce qui donne que

Exemple 15. *$n = 11$, $q = 4$ sur le corps F_4*
Il existe deux classes cyclotomiques : $C_1 = S_1 = \{1, 4, 5, 9, 3\}$ et $C_2 = S_1 = \{2, 8, 6, 10, 7\}$ on remarque que $S_1 \cup S_2 = Z_{11}^*$ et $S_1 \cap S_2 = \emptyset$, et on a la permutation μ_6 fait l'échange entre S_1 et S_2 alors

$$\mu_6 : S_1 \overset{\rightarrow}{\leftarrow} S_2.$$

un splitting modulo 11.

Remarque 16. *Les codes duadiques sont une généralisation des codes dits **résidus quadratiques**. construit comme suit :*

Soient n un nombre premier impair tel que $q = \square \mod n$, $S_1 = \{0 < i < n \,|\, i = \square \mod n\}$ et $S_2 = \{0 < i < n \,|\, i = \square \mod n\}$, pour un $a \in S_2$ $\mu_a : S_1 \leftrightarrow S_2$ est un splitting modulo n et les codes correspondants sont appelés les codes résidus quadratiques, (car le produit de deux non résidues est un résidu).

Les codes duadiques sont importants en pratique à cause de leurs distances minimales qui est large et aussi à cause de leurs lien avec les codes auto-duaux, ce lien est donné par le théorème suivant.

Théorème 17. *([55])*

Soit C un code cyclique de longueur n sur $\mathbb{F}_q$. Supposons que l'étendu de C soit un code auto-dual, alors C est un code duadique et le splitting est donné par μ_{-1}.

2.4.1 L'existence des codes duadiques

L'existence des codes duadiques de longueur n sur F_q dépend de l'existence des splittings modulo n. Soit q une puissance d'un nombre premier.

Théorème 18. *Soit $n = p_{m_1}^1 p_{m_2}^2 \cdots p_{m_k}^k$ la décomposition en facteur premiers du nombre impair n.*

Un splitting mod n existe si et seulement si q est carré mod $p_i \forall i \in \{1, 2, \ldots, k\}$; i.e

$$\exists\, x \in Z_{p_i} \text{ tel que } q \equiv x^2 \ mod\ p_i,\ i = 1, 2, \ldots, k.$$

Théorème 19. *([46] p221) Soit $n = p_{m_1}^1 p_{m_2}^2 \cdots p_{m_k}^k$ tel que $p_1 p_2 \cdots p_r$ des nombres premiers impairs distincts. on a les proprietés suivantes :*

i) les codes duadiques de longueur n sur F_2 existent si et seulement si

$$p_i \equiv \pm 1 (mod\ 8)\ pour\ 1 \leq i \leq k.$$

ii) les codes duadiques de longueur n sur F_3 existent si et seulement si

$$p_i \equiv \pm 1 (mod\ 12)\ pour\ 1 \leq i \leq k.$$

iii) les codes duadiques de longueur n sur F_4 existent pour tout n impair.

2.4.2 Exemples de codes duadiques

1) nous avons vu que les codes QR de longueur impaire sur le corps fini F_q sont des codes duadiques.
2) Soit $n = 15$ et $q = 4$; (15,4)=1. Alors la décompsition de n en facteur peremier est $n = 15 = 3 * 5$.

   On a $4 \equiv 1\ mod\ 3 \equiv 1^2\ mod\ 3$ alors 4 est carré modulo 3,

et $4 \equiv 4 \; mod \; 5 \equiv 2^2 \; mod \; 5$ alors 4 est carré modulo 5,

d'après (Théorème 18) il existe un splitting mod 15, et d'après (Théorème **??**) $q = 4$ est un carré modulo $n = 15$.

Alors le code de longueur $n = 15$ sur F_4 est un code duadique.

2.4.3 Propriétés des codes duadiques

Soit $\mu_a : S_1 \overrightarrow{\leftarrow} S_2$ un splitting mod n, et soit α est une racine primitive n-ième de l'unité sur le corps F_q.

Soit C_k les codes duadiques de longueur n sur F_q avec l'ensemble de définition $T_{S_k} = \{i \in S_k |\; g(\alpha^i) = 0\}$, et avec un sous-code even-like D_k.

Nous avons le résultat suivant sur la distance minimale des codes duadiques.

Théorème 20. *[46] Soient D_1 et D_2 une paire de codes duadiques odd-like de longueur n sur F_q. Alors D_1 et D_2 ont la même distance minimale d et on a :*

i) $d^2 \geq n$. *On suppose que le splitting donne par μ_{-1} alors*

ii) $d^2 - d + 1 \geq n$

2.5 L'existence des splittings

Dans cette section, nous donnons des conditions sur l'existence du splitting μ_{-1}. Comme conséquences, nous déduisons des résultats et des propriétés des codes duadiques sur $\mathbb{F}_q$.

2.5.1 Le splitting μ_{-1}

Le problème d'existence du spliting μ_{-1} est un ancien problème, la solution est liée à l'existence des codes duadiques cycliques comme dans notre cas ou plus généralement les codes duadiques d'algèbre de groupe. Récemment la réponse a été donné dans [2].

Il est évident que si une classe cyclotomique modulo n est fixé par μ_{-1} est alors réversible.

Théorème 21. *[55] Soit $n = p_{m_1}^1 p_{m_2}^2 \cdots p_{m_k}^k$ la décomposition en facteur premiers du nombre impair n. On suppose que :*

$$\exists\, x \in Z_{p_i} \text{ tel que } q \equiv x^2 \bmod p_i,\ i = 1, 2, \ldots, k.$$

1) *Si $p_i \equiv -1 \bmod 4,\ \forall i, i = 1, 2, ..., k.$ alors tous les splittings mod n sont donnés par μ_{-1}*
2) *Si $\exists i \in \{1, 2, ..., k\}$ tel que $p_i \equiv 1 \bmod 4$, alors il existe un splitting qui n'est pas donné par μ_{-1}.*

Théorème 22. *[49] Soit n un entier impair et q une puissance d'un nombre premier p alors μ_{-1} donne un splitting si et seulement si $ord_n(q)$ est impair.*

Corollaire 2. *Si $ord_n(q)$ est pair il ne peut exister de codes cycliques de longueur n sur $\mathbb{F}_q$ ou cycliques étendus qui soient auto-orthogonaux ou qui contiennent leurs duaux.*

Lemme 5. *Soient q et n des entiers différents de zéro avec n impair alors l'ordre de q modulo n est impair si et seulement si l'ordre de q modulo chaque entier premier p divisant n est impair.*

Preuve: Soit p un nombre premier divisant n alors $ord_p q \ / \ ord_n q$ donc si $ord_n q$ est impair alors

$ord_p q$ est aussi impair .

réciproquement : si $ord_p q$ est impair alors $ord_{p^\alpha} q$ est impair on a q^i congru à 1 mod p donc $q^{ip^{\alpha-1}}$ congru à 1 mod p^α donc $ord_{p^\alpha} q$ divise $ip^{\alpha-1}$ qui est impair d'où$ord_{p^\alpha} q$ est impair

si $n = p_1 p_2$ alors

$$ord_{p_1 p_2} q \ = \ lcm(ord_{p_1} q \ , ord_{p_2} q)$$

si $n = p_1^{\alpha_1} p_2^{\alpha_2}$ alors

$$ord_n q \ = \ lcm(ord_{p_1^{\alpha_1}} q \ , ord_{p_2^{\alpha_2}} q)$$

2.5.2 L'Orthogonalité des codes duadiques

Les codes duadiques sont importants en pratique à cause de leurs lien avec les codes auto-duaux, ce lien est donné par les théorèmes suivants :

Théorème 23. *[46] Les codes C_k et D_k sont duaux l'un de l'autre si et seulement si μ_{-1} donne un splitting ($k = 1, 2$).*

Théorème 24. *[49] Soit C un code cyclique de longueur n sur F_q. Supposons que l'étendu de C soit un code auto-dual, alors C est un code duadique et le splitting est donné par μ_{-1}.*

Théorème 25. *[46] Si C_1 et C_2 sont des codes duadiques even-like sur F_q, avec des codes duadiques odd-like associe D_1 et D_2. on a les propositions suivantes sont equivalents :*

- $C_1^{\perp} = D_1$.
- $C_2^{\perp} = D_2$.
- $C_1\mu_{-1} = C_2$
- $C_2\mu_{-1} = C_1$

Théorème 26. *[46] Si C_1 et C_2 sont des codes duadiques even-like sur F_q, avec des codes duadiques odd-like associe D_1 et D_2. On a les proposition suivant sont equivalents :*

- $C_1^{\perp} = D_2$.
- $C_2^{\perp} = D_1$.
- $C_1\mu_{-1} = C_1$
- $C_2\mu_{-1} = C_2$

Lemme 6. *[7] Soit q une puissance d'un nombre premier et un entier impair n tel que $(n, q) = 1$ Supposons que q ait un ordre impair modulo n et soit f_i un polynôme irreductible non-trivial (ie différent de $(x-1)$) diviseur de $x^n - 1$ sur F_q in $F_{q^{ord_n q}}$ alors $f_i \neq f_i^{\star}$*

Preuve: Supposons que $f_i = f_i^{\star}$ pour un certain facteur nontrivial irréductible ($ie\, f_i \neq (x-1)$) de $x^n - 1$ et classe correspondante C_i. Soit $j \in C_i$ le plus petit entier

tel que $q^j i \equiv -i \,(mod\, n)$ (un tel j existe puisque $C_i = C_{-i}$ si l est l'ordre de i dans Z_n alors l est impair et donc l'ordre de q modulo l est $2j$. Mais ceci contredit le fait que q ait un ordre impair modulo n . □

2.6 Construction de codes auto-duaux définis sur F_{2^r}

Soit $q = 2^r$ alors la caracteristique de F_q est 2 alors $-x = x$. soit $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, $2^r \equiv \square mod m$ si r est pair et $2^r \equiv 2 mod m$ si r est impair . donc si r est pair il existe des codes Duadiques de longueur $\forall\, m$ et si r est impair il existe des codes duadiques si et seulement si $p_i \equiv \pm 1 \, mod\, 8$, $\forall i \in \{1, 2, \dots s\}$

Exemple 16. *Soit* $m = 21 = 3 \cdot 7$,$7 \equiv -1 \, mod\,(8)$ *et* $3 \equiv 3 \, mod\,(8)$.

D'où il n'existe pas de codes duadiques de longueur 21 *sur* F_2 *et* F_8*mais il existe des codes duadiques de longueur* 21 *sur* F_4 *et* F_{16}.

Théorème 27. *[7] Soit* m *un entier impair tel que* $2^r \equiv \square mod\ m$ *et soient* $D_1 = \langle f_1(x) \rangle$, $D_2 = \langle f_2(x) \rangle$ *une pair de codes duadiques odd like de longueur* m *définis sur* F_{2^r}.

Soit $n = 2^a m$ *so* $x^n - 1 = x^{2^a m} - 1 = (x^m - 1)^{2^a} = (x-1)^{2^a} f_1^{2^a}(x) f_2^{2^a}(x)$. *et soit*

$$g_1(x) = (x-1)^{2^{a-1}} f_1^{2^a}(x) \tag{2.3}$$

$$g_2(x) = (x-1)^{2^{a-1}} f_2^{2^a}(x) \tag{2.4}$$

les codes cycliques de longueur $2^a m$ *définis sur* F_{2^r} *engendrés par* $g_i(x)$ $i \in \{1, 2\}$ *sont auto-duaux ou duaux l'un de l'autre.*

Preuve: D'aprés le lemme 6 et le théorème 21, nous avons deux cas possibles :

i) $f_i^\star(x) = \epsilon f_j(x)$ pour $i \neq j$ si le splitting est donné par μ_{-1}.

ii) $f_i^\star(x) = \epsilon f_i(x)$ avec $\epsilon = \pm 1$ dans F_{2^r} si le splitting n'est pas donné par μ_{-1}.

Donc on déduit :

1) Si $f_i^\star(x) = \pm f_j(x)$ pour $i \neq j$. Soit $C_i = \langle g_i(x)\rangle$ alors $C_i^\perp = \langle g_i^\star(x)\rangle = \langle((x-1)^{2^{a-1}})^\star(f_j^{2^a}(x))^\star\rangle = \langle\pm((x-1)^{\star 2^{a-1}})(f_j^{\star 2^a}(x))\rangle = \langle\pm(x-1)^{2^{a-1}} f_i^{2^a}(x)\rangle = C_i$. D'où C_i est un code cyclique auto dual.

2) Si $f_i^\star(x) = \pm f_i(x)$ pour $i \in \{1,2\}$. Soit $C_i = \langle g_i(x)\rangle$ alors $C_i^\perp = \langle g_i^\star(x)\rangle = \langle((x-1)^{2^{a-1}})^\star(f_j^{2^a}(x))^\star\rangle = \langle\pm((x-1)^{\star 2^{a-1}})(f_j^{\star 2^a}(x))\rangle = \langle\pm(x-1)^{2^{a-1}} f_j^{2^a}(x)\rangle = C_j = \langle\pm(x-1)^{2^{a-1}}(f_i^{\star 2^a}(x))\rangle$.

□

Dans ce qui suit nous donnons quelques exemples de codes auto-duaux définis sur $\mathbb{F}_2$:

Exemple 17. *considérons le cas* $n = 14$,$q = 2$ *nous avons* $m = 7$ *et* $7 \equiv -1\,(mod, 8)$ *donc il existe deux paires de codes duadiques de longueur* 7 *sur* $\mathbb{F}_2$ *la factorisation de* $x^{14} - 1$ *sur* $\mathbb{F}_2$ *est*

$$(x-1)^2(x^3+x+1)^2(x^3+x^2+1)^2$$

puisque $7 \equiv -1\,mod\,(4)$ *alors* (x^3+x+1) *est le polnôme réciproque de* (x^3+x^2+1).

Le polynôme $x^7 - 1$ *engendre le code auto dual trivial de longueur* 14 *sur* $\mathbb{F}_2$

et les codes

$$C_1 = \langle(x-1)(x^3+x+1)\rangle$$

$$C_2 = \langle(x-1)(x^3+x^2+1)\rangle$$

sont des codes cycliques auto-duaux de longueur 14 *sur* F_2

Exemple 18. *considérons le cas* $n = 34$,$q = 2$ *nous avons* $m = 17$ *et* $17 \equiv 1\,(mod, 8)$ *donc il existe deux paires de codes duadiques de longueur* 17 *sur* $\mathbb{F}_2$ *la factorisation de* $x^{34} - 1$ *sur* $\mathbb{F}_2$ *est*

$$(x-1)^2(x^8+x^5+x^4+x^3+1)^2(x^8+x^7+x^6+x^4+x^2+x+1)^2$$

puisque $17 \equiv 1\,mod\,(4)$ *alors* $(x^8+x^5+x^4+x^3+1)$ *n'est pas le polnôme réciproque de* $(x^8+x^7+x^6+x^4+x^2+x+1)$.

Le polynôme $x^{17} - 1$ *engendre le code auto dual trivial de longueur* 34 *sur* $\mathbb{F}_2$

et les codes

$$C_1 = \langle (x-1)(x^8+x^7+x^6+x^4+x^2+x+1) \rangle$$

$$C_2 = \langle (x-1)(x^8+x^5+x^4+x^3+1) \rangle$$

sont des codes cycliques duaux l'un de l'autre de longueur 34 *sur* F_2

Exemple 19. *considérons le cas* $n = 46$ *,*$q = 2$ *nous avons* $m = 23$ *et* $23 \equiv -1\,(mod, 8)$ *donc il existe deux paires de codes duadiques de longueur* 23 *sur* $\mathbb{F}_2$.
La factorisation de $x^{46}-1$ *sur* $\mathbb{F}_2$ *est*

$$(x-1)^2(x^{11}+x^9+x^7+x^6+x^5+x+1)^2(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)^2$$

puisque $23 \equiv -1\, mod\,(4)$ *alors* $(x^{11}+x^9+x^7+x^6+x^5+x+1)$ *est le polnôme réciproque de* $(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)$.

Le polynôme $x^{23}-1$ *engendre le code auto dual trivial de longueur* 46 *sur* $\mathbb{F}_2$
et les codes

$$C_1 = \langle (x-1)(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1) \rangle$$

$$C_2 = \langle (x-1)(x^{11}+x^9+x^7+x^6+x^5+x+1) \rangle$$

sont des codes cycliques auto-duaux de longueur 46 *sur* $\mathbb{F}_2$

Exemple 20. *considérons le cas* $n = 62$ *,*$q = 2$ *nous avons* $m = 31$ *et* $31 \equiv -1\,(mod, 8)$ *donc il existe deux paires de codes duadiques de longueur* 31 *sur* $\mathbb{F}_2$.
La factorisation de $x^{62}-1$ *sur* $\mathbb{F}_2$ *est* $(x-1)^2((x^5+x^2+1)(x^5+x^3+x^2+x+1)(x^5+x^4+x^2+x+1))^2$
$((x^5+x^3+1)(x^5+x^4+x^3+x^2+1)(x^5+x^4+x^3+x+1))^2$
et puisque $31 \equiv -1\, mod\,(4)$ *alors* $(x^5+x^2+1)(x^5+x^3+x^2+x+1)(x^5+x^4+x^2+x+1)$ *est le polnôme réciproque de* $(x^5+x^3+1)(x^5+x^4+x^3+x^2+1)(x^5+x^4+x^3+x+1)$.

Le polynôme $x^{31}-1$ *engendre le code auto dual trivial de longueur* 62 *sur* $\mathbb{F}_2$
et les codes

$$C_1 = \langle (x-1)(x^5+x^2+1)(x^5+x^3+x^2+x+1)(x^5+x^4+x^2+x+1) \rangle$$

$$C_2 = \langle (x-1)(x^5+x^3+1)(x^5+x^4+x^3+x^2+1)(x^5+x^4+x^3+x+1) \rangle$$

sont des codes cycliques auto-duaux de longueur 62 *sur* $\mathbb{F}_2$

Exemple 21. *Considérons le cas* $n = 142$ *,*$q = 2$ *nous avons,* $m = 71$ *et* $71 \equiv -1\,(mod, 8)$ *donc il existe deux paires de codes duadiques de longueur* 71 *sur* $\mathbb{F}_2$*.*
La factorisation de $x^{142}-1$ *sur* $\mathbb{F}_2$ *est*
$(x-1)^2(x^{35}+x^{33}+x^{28}+x^{27}+x^{26}+x^{25}+x^{24}+x^{17}+x^{13}+x^8+x^7+x^5+x^4+x+1)^2(x^{35}+x^{34}+x^{31}+x^{30}+x^{28}+x^{27}+x^{22}+x^{18}+x^{11}+x^{10}+x^9+x^8+x^7+x^2+1)^2$
puisque $71 \equiv -1\, mod\,(4)$ *alors*
$(x^{35}+x^{33}+x^{28}+x^{27}+x^{26}+x^{25}+x^{24}+x^{17}+x^{13}+x^8+x^7+x^5+x^4+x+1)$
est le polynôme réciproque de
$(x^{35}+x^{34}+x^{31}+x^{30}+x^{28}+x^{27}+x^{22}+x^{18}+x^{11}+x^{10}+x^9+x^8+x^7+x^2+1)$.

Le polynôme $x^{23}-1$ *engendre le code auto dual trivial de longueur* 142 *sur* $\mathbb{F}_2$
et les codes

$$C_1 = \langle (x-1)(x^{35}+x^{33}+x^{28}+x^{27}+x^{26}+x^{25}+x^{24}+x^{17}+x^{13}+x^8+x^7+x^5+x^4+x+1) \rangle$$

$$C_2 = \langle (x-1)(x^{35}+x^{34}+x^{31}+x^{30}+x^{28}+x^{27}+x^{22}+x^{18}+x^{11}+x^{10}+x^9+x^8+x^7+x^2+1)) \rangle$$

sont des codes cycliques auto-duaux de longueur 142 *sur* $\mathbb{F}_2$

Chapitre 3

Codes Linéaires Définis sur les Anneaux Finis

3.1 introduction

La théorie des anneaux occupe un role trés important dans la résolution de certains problèmes liés à la théorie des codes correcteurs d'erreurs. D'ailleurs, on a construit de bons codes sur l'anneau à quatre éléments Z_4, ce qui a motivé notre travail sur d'autres classes d'anneaux.

Remarque 17. *[4] La structure d'anneaux est moins restrictive que celles des corps donc plus nombreux. D'ailleurs, nous avons un seul corps à isomorphisme prés à* 4 *éléments alors qu'ils existent* 9 *différents anneaux commutatifs à* 4 *éléments. Parmi ces anneaux ils existent* 3 *qui sont locaux (*$\mathbb{Z}/4\mathbb{Z}, GF(2^2), (\mathbb{Z}/2\mathbb{Z})[X]/(X^2)$ *, donc on peut construire plus de* ***Codes*** *sur les anneaux.*

Au début des années 1990, Hammons, Kumar, Calderbank,Solé donnèrent une construction très simple de certains codes binaires,c'est à dire définis sur le corps à deux éléments,non linéaires figurant parmi les meilleurs connus.Il s'agit notamment des codes de Kerdock et de Preparata.Cette construction est également à l'origine de l'explication algébrique d'une curieuse relation entre codes de Kerdok et de Preparata,à savoir leurs

dualité formelle.
Quelque années auparavant,certains chercheurs ont été amenés à introduire un nouvel alphabet pour construire des codes.Contrairement à la tradition, cet alphabet de quatre éléments admet une structure d'anneau et non de corps.C'est $\mathbb{Z}_4$,l'anneau des entiers modulo quatre.L'introduction de ces codes dits aussi quaternaires a alors été perçu comme un événement considérable au sein de la communauté des codeurs.

L'objectif était de construire et d'étudier de bon codes sur Z_4 puis les transformer en codes binaires,les codes ainsi-obtenu sont dit $\mathbb{Z}_4$-linéaires.
La transformée des codes linéaires sur Z_4 en codes binaires s'opère à l'aide de l'application de **Gray** qui va de $\mathbb{Z}_4$ dans $\mathbb{Z}_2^2$,étendue coordonnée par coordonnée grâce aux propriétés de cette application.Depuis lors,une généralisation d'étude et de construction de codes a été faite sur les anneaux finis.

3.2 Préliminaires

Dans ce qui suit on donne quelque définitions nécessaires pour la compréhension du reste pour plus de détails (voir l'appendice).

Définition 43. *Un anneau $\mathcal{R}$ est appelé anneau local si $\mathcal{R}$ a un unique idéal maximal.*

Définition 44. *Un anneau à chaine fini est un anneau commutatif $\mathcal{R}$ fini tel que $1 \neq 0$ et tel que tous ses idéaux sont ordonnés par l'inclusion.*

Soit $\mathfrak{m}$ l'idéal maximal de l'anneau à chaine fini $\mathcal{R}$. Puisque $\mathcal{R}$ est principal (voir chapitre 4), il existe un générateur $\gamma \in \mathcal{R}$ de $\mathfrak{m}$, alors γ est nilpotent d'indice de nilpotence un certain entier e. Les idéaux de $\mathcal{R}$ forment la chaine suivante

$$< 0 >= \langle \gamma^e \rangle \subsetneq \langle \gamma^{e-1} \rangle \subsetneq \ldots \subsetneq \langle \gamma \rangle \subsetneq \mathcal{R}.$$

Le nilradical de $\mathcal{R}$ est $\langle \gamma \rangle$.
D'où tous les éléments de $\langle \gamma \rangle$ sont nilpotents donc les éléments de $\mathcal{R}/\langle \gamma \rangle$ sont des unités.
Puisque $\langle \gamma \rangle$ est un idéal maximal, le corps résiduel noté $\mathcal{R}/\langle \gamma \rangle$ sera noté par $\mathcal{K}$.

Considérons l'homomorphisme surjectif $(-)$:

$$\begin{aligned} - : \mathcal{R} &\longrightarrow \mathcal{K} \\ a &\longmapsto \overline{a} = a \pmod{\gamma} \end{aligned} \tag{3.1}$$

$|\mathcal{K}| = q = p^r$ pour un certain entier r, alors

$$|\mathcal{R}| = |\mathcal{K}| \cdot |\langle\gamma\rangle| = |\mathcal{K}| \cdot |\mathcal{K}|^{e-1} = |\mathcal{K}|^e = p^{er}. \tag{3.2}$$

Dans le cas d'un anneau à chaine fini,on utilisera l'abus de langage suivant : anneau à chaine de caractéristique p au lieu d'anneau à chaine dont le corps résiduel a pour caractéristique p.

3.3 Codes linéaires définis sur les anneaux finis

Définition 45. *Soit $\mathcal{R}$ un anneau fini Un code linéaire C de longueur n sur $\mathcal{R}$ est un sous-module du $\mathcal{R}$-module $\mathcal{R}^n$,Qui peut être libre ou pas.*
Les vecteurs de C sont appelés les mots du code C.

Exemple 22. *Soit le code C_1 dans $\mathbb{Z}_4^3$ tel que :*

$$C_1 = \{000, 121, 202, 323\}, \textit{alors } C_1 \textit{ est linéaire car :}$$
$$121 + 202 = 323 \in C_1$$
$$121 + 323 = 000 \in C_1$$
$$202 + 323 = 121 \in C_1$$

Soit le code C_2 dans $\mathbb{Z}_4$ tel que :

$$C_2 = \{000, 011, 203\} \textit{ est non linéaire car :}$$
$$011 \textit{ et } 203 \in C_2 \textit{ mais } 011 + 203 = 210 \textit{ n'est pas dans } C_2$$

On munit $\mathcal{R}^n$ du produit suivant : $v \cdot w = \sum v_i w_i$. Le code dual $C^\perp$ de C est définit par

$$C^\perp = \{v \in \mathcal{R}^n \mid v \cdot w = 0 \text{ for all } w \in C\}. \tag{3.3}$$

Si $\mathcal{C} \subseteq \mathcal{C}^\perp$, on dit que le code C est auto-orthogonal et si $C = C^\perp$, on dit que le code C est auto-dual.

Dans ce qui suit on donne la forme standard d'une matrice génératrice d'un code linéaire défini sur un anneau à chaine fini ce qui n'est pas possible pour n'importe quel anneau fini.

3.4 Matrice génératrice d'un code linéaire défini sur un anneau à chaine fini

Soit $\mathcal{R}$ un anneau à chaine fini d'idéal maximal $\langle\gamma\rangle$, e l'indice de nilpotence de γ, de corps résiduel $\mathbb{F}_q = \mathbb{F}_{p^r}$ où p est un nombre premier et $(n, p) = 1$

Définition 46. *Soit C un code linéaire sur $\mathcal{R}$ de rang k.La matrice génératrice de C est une matrice $k \times n$,dont ces lignes engendrent C,et aucune d'elles ne peut s'écrire comme combinaison linéaire des autres lignes de G .*
En particulier : $C = \{xG; x \in \mathcal{R}\}$

Théorème 28. *[45] Soit C un code linéaire sur $\mathcal{R}$,à une permutation prés des coordonnées ,C admet une matrice génératrice G sous la forme standard suivante :*

$$G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \dots & A_{0,e-1} & A_{0,e} \\ 0 & \gamma I_{k_1} & \gamma A_{1,2} & \gamma A_{1,3} & \dots & \gamma A_{1,e-1} & \gamma A_{1,e} \\ 0 & 0 & \gamma^2 I_{k_2} & \gamma^2 A_{2,3} & \dots & \gamma^2 A_{2,e-1} & \gamma^2 A_{2,e} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & \gamma^{e-1} I_{k_{e-1}} & \gamma^{e-1} A_{e-1,e} \end{pmatrix} \tag{3.4}$$

où tous les éléments dans $\gamma^i A_{i,j}$ $(0 \leq i \leq e-1, 1 \leq j \leq e)$ sont dans $\langle \gamma^i \rangle$

On dit que C est de type $\{k_0, k_1, \ldots, k_{e-1}\}$. Ce qui implique que son cardinal est : $|C| = |\mathcal{R}/\langle\gamma\rangle|^{\sum_{i=0}^{e-1}(e-1)k_i} = |\mathbb{F}_q|^{\sum_{i=0}^{e-1}(e-1)k_i}$

On définit $k_e = n - \sum_{i=0}^{e-1} k_i$

Le rang de C est définit par :

$$k(C) = \sum_{i=0}^{e-1} k_i. \tag{3.5}$$

Il est clair que $k(C)$ est le nombre minimum de vecteurs d'une famille génératrice de C. De plus, nous avons une relation entre C et son dual $C^\perp$.

$$|C||C^\perp| = q^{\sum(e-i)(k_i+k_i^\perp)} = q^{en} = |R|^n, \text{ and } (C^\perp)^\perp = C. \tag{3.6}$$

Remarque 18. *De (3.6), Il existe un code auto-dual de longueur n sur $\mathcal{R}$ si et seulement si en est pair. Si e est pair , il existe un code auto-dual de longueur n appelé le code aoto-dual trivial donné par sa matrice génératrice : $G = \gamma^{\frac{e}{2}} I_n$.*

Le rang de C est le cardinal de sa plus petite famille génératrice. Le rang libre de C est défini comme le plus grand rang des sous modules libres de C. Un code linéaire est dit dit libre si son rang libre est égal à son rang . Dans ce cas Le code est un R sous module libre isomorphe au sous module $R^{k(C)}$, et a comme base à $k(C)$ éléments. Donc dans ce cas une matrice génératrice de C dans la forme standard est donné par $(I_k\ M)$ pour une certaine matrice M.

Lemme 7. *([17]) Soit C un code linéaire de matrice génératrice G dans la forme standard (**??**). Then if for Alors si $0 \leq i < j \leq e$, $B_{i,j} = -\sum_{k=i+1}^{j-1} B_{i,k} A^{tr}_{e-j,e-k} - A^{tr}_{e-j,e-i}$, nous avons*

$$H = \begin{pmatrix} B_{0,e} & B_{0,e-1} & \ldots & B_{0,1} & I_{n-k} \\ \gamma B_{1,e} & \gamma B_{1,e-1} & \ldots & \gamma I_{k_{e-1}} & 0 \\ \gamma^2 B_{2,e} & \gamma B_{2,e-1} & \ldots & \gamma I_{k_{e-2}} & 0 \\ \vdots & & & & \\ \gamma^{e-1} B_{e-1,e} & \gamma^{e-1} I_{k_{e-1}} & \ldots & 0 & 0 \end{pmatrix}, \tag{3.7}$$

est une matrice pour $C^{\perp}$. *De plus* $k_i(C^{\perp}) = k_{e-i}(C)$, *for* $i = 1, \ldots, e-1$, *et* $k_0(C^{\perp}) = n - k(C)$.

Lemme 8. *[26] Soit* C *un code de type* $\{k_0, k_1, \ldots, k_{e-1}\}$ *alors* $C^{\perp}$ *son dual est un code de type* $\{k_e, k_{e-1}, k_{e-2}, \ldots, k_1\}$

3.5 Les paramètres d'un code linéaire défini sur $\mathcal{R}$

On définit sur $\mathcal{R}^n$ une métrique appelée **distance de Hamming** notée $d(x, y)$ entre deux vecteurs $(x, y) \in \mathcal{R}^n$ donnée par le nombre de leurs coordonnées différentes :

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

Le poids de Hamming qu'on note $w_H(c)$ d'un mot $c \in \mathcal{R}$ est le nombre de coordonnées non nulles de c :

$$w_H(c) = d(c, 0)$$

La distance minimale notée $d_H(c)$ d'un code C définit sur $\mathcal{R}$ la plus petite distance entre les différents mots de code,i.e., :

$$d_H(c) = \{\min d(x, y) \mid x, y \in \mathcal{R}^n\}$$

Le poids minimal d'un code C est le poids minimum non nul de code :

$$w(C) = \{\min w(x) \mid x \in C, x \neq 0\}$$

Exemple 23. *On reprend l'exemple* 2.1 *:*

$$d(121, 202) = 3$$
$$d(121, 323) = 2$$
$$d(202, 323) = 3$$
$$et\ d_H(C) = 2$$
$$w(121) = 3$$
$$w(202) = 2$$
$$w(323) = 3$$
$$et\ w_H(C) = 2$$

Remarque 19. *Pour un code linéaire, la distance minimale et le poids minimal sont égaux.*

3.6 Les différents poids et distances sur l'anneau de Galois $\mathbb{Z}_q$

Soit C un code linéaire sur $GR(p^m, r)$ de longueur n,et soit $G(C)$ sa matrice génératrice.

Soit $x = (x_1, ..., x_n) \in GR(p^m, r)^n$.

On a déjà défini le poids de Hamming $w_H(x)$ comme étant le nombre de composantes non nulles de x.

Si on est dans l'anneau de Galois $\mathbb{Z}_q$ tel que q est une puissance d'un nombre premier p,alors on peut associer à un vecteur x différents poids et différentes distances autres que le poids de Hamming et la distance de Hamming.

Le poids Euclidien est :

$$w_E(x) = \sum_{i=1}^{n} \min\{x_i^2, (q - x_i)^2\}$$

Le poids de Lee est :

$$w_L(x) = \sum_{i=1}^{n} \min\{|x_i|, |q - x_i|\}$$

De meme pour la distance, on définit ces trois distances :

La distance de Hamming :

$$d_H(x, y) = w_H(x - y)$$

La distance de Lee :

$$d_L(x, y) = w_L(x - y)$$

La distance Euclidienne :

$$d_E(x, y) = w_E(x - y)$$

Définition 47. *Soit C un code sur $GR(p^m, r)$ de longueur n et de rang $k = \sum_{i=0}^{m-1} k_i$ et de distance minimal d alors il est dit $[n, k, d]$-code.*

Enumérateur de poids

Pour un code de longueur n,on appelle énumérateur de poids le polynôme :

$$W_c(x) = \sum_{i=0}^{n} A_i(C)x^i$$

où A_i est égale au nombre de mots de poids i du code C.

En remplaçant x par x/y et en multipliant par y^n,le polynôme $W_c(x)$ peut être transformé en un polynome à deux variables x et y comme suit :

$$W_c(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$$

L'introduction de ces codes, dit aussi *codes quaternaires*, a été considérée comme une première au sein de la communauté des chercheurs. En effet, de par leurs propriétés remarquables, les codes sur $\mathbb{Z}_4$ devinrent rapidement une nouvelle voie de recherche.

L'objectif était de construire et d'étudier de bons codes sur $\mathbb{Z}_4$ et plus généralement sur des anneaux finis. Certains codes révèlent en effet leur vraie structure lorsqu'ils sont définis sur un alphabet approprié.

3.7 Codes linéaires sur l'anneau $\mathbb{Z}_4$

Définition 48. *Un code linéaire sur $\mathbb{Z}_4$ de longueur n est un sous-groupe additif de $\mathbb{Z}_4^n$. Un tel sous groupe est un* ***sous-module*** *de $\mathbb{Z}_4$, qui peut être libre ou pas. On rappel qu'un $\mathbb{Z}_4$-module M est libre s'il existe un sous ensemble B de M tels que chaque élément de M peut être exprimer sous forme de $\mathbb{Z}_4$ combinaison linéaire d'éléments de B*

Remarque 20. *Si v est un vecteur de $\mathbb{Z}_4^n$ de composantes égale à 0 ou 2, alors $2v = 0$, ce qui implique qu'un tel vecteur ne peut pas être un vecteur de base d'un module libre de $\mathbb{Z}_4$.*

Exemple 24. *On peut montrer que l'ensemble des mots suivants de $\mathbb{Z}_4$ est un $\mathbb{Z}_4$-linéaire code de longueur 4 :*

$$\begin{array}{cccccccc} 0000 & 1113 & 2222 & 3331 & 0202 & 1311 & 2020 & 3133 \\ 0022 & 1131 & 2200 & 3313 & 0220 & 1333 & 2002 & 3111 \end{array}$$

C'est un sous groupe additif de $\mathbb{Z}_4^4$. Si c'est un $\mathbb{Z}_4$-module libre alors, il va exister une base de deux vecteurs b_1 et b_2 ayant au moins une composante égale à 1 ou 3. Tous les mots avec une composante égale à 1 ou 3 vérifient $2b_1 = 2b_2 = 2222$. Alors $\{b_1, b_2\}$ ne peuvent pas former une base ce qui implique que C n'est pas libre. Cependant on peut montrer que tout mot de C peut s'écrire sous la forme :

$$xc_1 + yc_2 + zc_3$$

avec $c_1 = 1113$, $c_2 = 0202$, $c_3 = 0022$, $x \in \mathbb{Z}_4$, y et $z \in \{0, 1\}$.

3.7.1 Matrice génératrice

Soit C le code de $\mathbb{Z}_4$ donné par l'exemple 1, on peut montrer que

$$G = \begin{pmatrix} 1 & 1 & 1 & 3 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{pmatrix}$$

est une matrice génératrice de C : dans le sens où tout mot de C peut s'écrire comme étant $(xyz)G$ pour certain $x \in \mathbb{Z}_4$, y et $z \in \mathbb{Z}_2$.

Tout mot de C peut s'écrire sous la forme de

$$\sum_{i=1}^{k_1} a_i c_i + \sum_{i=k_1}^{k_1+k_2} b_i c_i$$

avec $a_i \in \mathbb{Z}_4$ pour $1 \leq i \leq k_1$ et $b_i \in \mathbb{Z}_2$ pour $k_1 + 1 \leq i \leq k_1 + k_2$. En plus chaque c_i admet une composante égale à 1 ou 3 pour $1 \leq i \leq k_1$ et tout c_i est égale à 0 ou 2 pour $k_1 + 1 \leq i \leq k_1 + k_2$. Si $k_2 = 0$, le code C est un $\mathbb{Z}_4$-module libre.

Définition 49. *La matrice qui admet pour ligne c_i pour $1 \leq i \leq k_1 + k_2$ est appelée* ***matrice génératrice*** *de C. Le code C admet $4^{k_1}2^{k_2}$ mots et il est dit* ***de type*** *$4^{k_1}2^{k_2}$. Le code de l'exemple 1 est de type $4^1 2^2$.*

Toute matrice d'un $\mathbb{Z}_4$-code linéaire peut s'exprimer sous la forme de

$$G = \begin{pmatrix} I_{k_1} & A & B_1 + 2B_2 \\ O & 2I_{k_2} & 2C \end{pmatrix}$$

avec A, B_1, B_2 et C sont des matrice à coefficients dans $\mathbb{Z}_2$, et O est une matrice $k_2 \times k_1$ matrice nulle. Le code C est de type $4^{k_1}2^{k_2}$.

Théorème 29. *Tout code linéaire sur $\mathbb{Z}_4$ est équivalent à un code avec une matrice génératrice sous sa forme standard.*

3.7.2 Dual d'un code sur $\mathbb{Z}_4$

Définition 50. *Il existe un produit scalaire modulo 4 sur $\mathbb{Z}_4^n$ défini par :*

$$x.y = x_1y_1 + ... + x_ny_n \ (mod\ 4)$$

avec $x = x_1...x_n$ et $y = y_1...y_n$. On peut définir le code ***dual*** *de C par*

$$C^{\perp} = \{x \in \mathbb{Z}_4^n | x.c = o \ pour \ tout \ c \in C\}$$

Définition 51. *Un $\mathbb{Z}_4$-linéaire est un code* ***auto-orthogonal*** *s'il vérifie $C \subset C^{\perp}$, il est dit* ***auto-dual*** *s'il vérifie $C = C^{\perp}$.*

Si C est un code dans sa forme standard, alors $C^{\perp}$ admet pour matrice génératrice :

$$G^{\perp} = \begin{pmatrix} -(B_1 + 2B_2)^t - C^t A^t & C^t & I_{n-k_1-k_2} \\ 2A^t & 2I_{k_2} & O \end{pmatrix}$$

où O est la matrice $k_2 \times (n - k_1 - k_2)$ zéro matrice. En particulier, $C^{\perp}$ est de type $4^{n-k_1-k_2}2^{k_2}$.

3.7.3 Poids et distances d'un code sur $\mathbb{Z}_4$

Sur $\mathbb{Z}_4$, il existe différents poids pour un vecteur de $\mathbb{Z}_4^n$ et alors différentes distances minimales. Soit $x \in \mathbb{Z}_4^n$, supposons que $n_a(x)$ le nombre de composantes de x égale à a pour $a \in \mathbb{Z}_4$.
Le poids de Hamming, le poids de Lee et le poids Euclidien sont respectivement :

$$wt_H(x) = n_1(x) + n_2(x) + n_3(x)$$
$$wt_L(x) = n_1(x) + 2n_2(x) + n_3(x)$$
$$wt_E(x) = n_1(x) + 4n_2(x) + n_3(x)$$

La distance de Hamming, la distance de Lee respectivement la distance Euclidienne entre x et y sont :

$$d_H(x, y) = wt_H(x - y)$$
$$d_L(x, y) = wt_L(x - y)$$
$$d_E(x, y) = wt_E(x - y)$$

Théorème 30. *Soient C un code linéaire de $\mathbb{Z}_4$ qui est auto-orthogonal avec $c \in C$. Alors :*

1. $wt_L(c) \equiv 0 \ (mod\ 2)$, *et*
2. $wt_E(c) \equiv 0 \ (mod\ 4)$

Exemple 25. *Soit le vecteur* $v = 120203303$*,alors ;*

$$w_H(x) = 6$$

$$w_L(v) = 8$$

$$w_E(v) = 12$$

3.7.4 Codes binaires obtenus à partir des codes sur $\mathbb{Z}_4$

L'importance des codes quaternaire est sans nul doute liée à l'application "Gray" qui a l'origine servait à encoder des séquences avec le système QPSK (Quadrature Phase-Shift Keying).Définissons les trois applications α, β, γ de $\mathbb{Z}_4$ sur $\mathbb{Z}_2$ par

c	$\alpha(c)$	$\beta(c)$	$\gamma(c)$
0	0	0	0
1	1	0	1
2	0	1	1
3	1	1	0

Ces applications peuvent s'étendre à des vecteurs de longueurs n,de $\mathbb{Z}_4^n$ vers $\mathbb{Z}_2^{2n}$. L'application Gray $\varphi : \mathbb{Z}_4^n \longrightarrow \mathbb{Z}_2^{2n}$ est donnée par

$$\varphi(c) = (\beta(c), \gamma(c)), c \in \mathbb{Z}_4^n$$

Remarque 21. *Le code binaire formé des mots* $(\alpha(c), \beta(c), \gamma(c))$ *pour* $c = 0, 1, 2, 3$*, est linéaire et tous poids sont pairs.*

L'application est aussi Gray de $\mathbb{Z}_4^n$ vers $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$

$$(a_1, \cdots, a_n) \longmapsto ((u_1, \cdots, u_n), (v_1, \cdots, v_n))$$

où pour tout $i \in \{1, \cdots, n\}, a_i = 2u_i + (u_i + v_i \ mod\ 2)$.

L'image d'un code quaternaire C_4 de longueur n est un code binaire C de longueur $2n$.

Le code C est appelé image binaire de C_4, n'est pas forcément linéaire. Cependant, lorsque C est linéaire et la matrice génératrice de C_4 est de la forme (2.1) alors la matrice génératrice de C est de la forme

$$\begin{bmatrix} I_{k_1} & A & \alpha(B_1+2B_2) & I_{k_1} & A & \alpha(B_1+2B_2) \\ 0 & I_{k_2} & C & 0 & I_{k_2} & C \\ 0 & 0 & \beta(B_1+2B_2) & I_{k_1} & A & \gamma(B_1+2B_2) \end{bmatrix}$$

L'application Gray permet donc de construire des codes binaires à partir des codes quaternaires. Sa propriété essentielle est d'être une isométrie. Ainsi nous allons voir que si la disposition des mots dans l'image binaire C ne lui permet pas en général d'être linéaire, C est tout de même de distance invariante.

3.7.5 Propriétés de l'application Gray

Définition 52. *Une application $f : X \to Y$ est appelée isométrie si*

$$\forall x \in X, y \in Y, d(f(x), f(y)) = d'(x, y)$$

Théorème 31. *L'application Gray est une isométrie*

$(\mathbb{Z}_4^n, \textit{lee distance}) \longrightarrow \left(\mathbb{Z}_2^{2n}, \textit{Hamming distance}\right)$. A partir de la définition de la métrique de Lee on a

$$w_H(\varphi(c)) = w_L(c), c \in \mathbb{Z}_4^n,$$

$$d_H(\varphi(c_1)\varphi(c_2)) = d_L(c_1, c_2), c_1, c_2 \in \mathbb{Z}_4^n,$$

Où wt_H et d_H représentent respectivement le poids et la distance de Hamming pour les mots binaires □

L'application φ ne conserve pas la propriété de linéarité. Cependant elle conserve la propriété de distance invariante car c'est une isométrie.

Théorème 32. *[46] Soit C_4 un code linéaire sur $\mathbb{Z}_4$ de distance de Lee d_L, alors son image binaire $\varphi(C_4) = C$ est un code binaire de distance de Hamming $d_H = d_L$.*

Ainsi, l'image binaire d'un code quaternaire est de distance invariante. Un code $C \in \mathbb{Z}_2^{2n}$ est dit $\mathbb{Z}_4-$linéaire s'il peut être défini comme étant l'image par l'application Gray d'un code quaternaire, c'est à dire si

$$\exists C_4 \in \mathbb{Z}_4^n; \varphi(C_4) = C.$$

On a alors la propriété sur les distributions de poids

$$Ham_C(W, X) = Lee_{C_4}(W, X).$$

Puisque l'image binaire d'un code quaternaire $\varphi(C_4) = C$ n'est pas toujours linéaire, elle n'admet pas de dual au sens algébrique du terme. On définit alors le $\mathbb{Z}_4-$dual de C qui est $C^\perp = \varphi(C_4^\perp)$. Ainsi, nous avons le diagramme suivant :

$$\begin{array}{lll} C_4 & \xrightarrow{\varphi} & C = \varphi(C_4) \\ Dual \downarrow & & \\ C_4^\perp & \xrightarrow{\varphi} & C^\perp = \varphi(C_4^\perp) \end{array}$$

Il n'est pas possible de rajouter une flèche notée "dual" dans la partie droite du diagramme car les 2 codes binaires ne sont que $\mathbb{Z}_4-$duaux. Cependant, la propriété de $\mathbb{Z}_4-$dualité est plus forte qu'on pourrait le penser à première vue

3.8 Codes linéaires définis sur l'anneau $R_{2,2} = \mathbb{F}_2 + u\mathbb{F}_2$

Récemment, les codes sur l'anneau $\mathbb{F}_2 + u\mathbb{F}_2$ ont eu beaucoup d'attention dans le domaine de la théorie des codes car l'anneau $\mathbb{F}_2 + u\mathbb{F}_2$ partage les propriétés de $\mathbb{Z}_4$ et $\mathbb{F}_4$, il a été introduit par Bachoc pour la construction des réseaux unimodulaires. Dans cette section on va introduire quelques définitions et notions de base sur $\mathbb{F}_2 + u\mathbb{F}_2$. On définit les poids de Lee des éléments de $\mathcal{R}$, $0, 1, u, 1+u$ par $0, 1, 2, 1$ respectivement. Sur

$\mathcal{R}^n$ on définit la distance de Lee des vecteurs x et y comme le poids de Lee de $x - y$. On définit la distance minimale de Lee d'un code C comme la distance minimale de Lee entre chaque deux mots du code C.

3.8.1 Définitions et préliminaires

$\mathbb{F}_2 + u\mathbb{F}_2$ est un anneau commutatif, l'ensemble des éléments de $\mathbb{F}_2 + u\mathbb{F}_2$ est $\{0, 1, u, \bar{u} = 1 + u\}$ avec $u^2 = 0$.
Il est facile de vérifier que c'est bien un anneau local d'idéal maximal donné par $\{0, u\}$; L'addition et la multiplication dans cet anneau sont données par les deux tableaux suivants :

+	0	1	u	$\bar{u}$
0	0	1	u	$\bar{u}$
1	1	0	$\bar{u}$	u
u	u	$\bar{u}$	0	1
$\bar{u}$	$\bar{u}$	u	1	0

.	0	1	u	$\bar{u}$
0	0	0	0	0
1	0	1	0	$\bar{u}$
u	0	u	0	u
$\bar{u}$	0	$\bar{u}$	u	1

La table de multiplication coïncide avec la table de $\mathbb{Z}_4$ quand $\{u, 1 + u\}$ sont remplacés par 2 et 3, par contre la table d'addition est différente de la table de $\mathbb{Z}_4$, mais elle est similaire au corps de Galois $\mathbb{F}_4 = \left\{0, 1, \beta, \beta^2 = 1 + \beta\right\}$ quand u et $u+1$ sont remplacés par β et β^2 respectivement .

Définition 53. *[14] (code linéaire) Soit C un code de longueur n, C est un code linéaire sur $\mathbb{F}_2 + u\mathbb{F}_2$ s'il est un sous module de $(\mathbb{F}_2 + u\mathbb{F}_2)^n$ sur $\mathbb{F}_2 + u\mathbb{F}_2$*

On donne quelques définitions des distances et des poids les plus utiles. Pour les codes sur $\mathbb{F}_2 + u\mathbb{F}_2$; il y a trois distances *Hamming*,*Lee* et *Euclide*. On a constaté que la distance de *Lee* et la distance d'Euclide ont des applications remarquables sur les codes binaires non linéaires et les réseaux unimodulaires.

Le poids de *Lee* pour le mots du code $x = (x_1, x_2, ..., x_n)$ est définie par

$$wt_L(x) = \sum_{i=1}^{n} wt_L(x_i)$$

où

$$wt_L(x_i) = \begin{cases} 0 & si \;\; x_i = 0 \\ 1 & si \;\; x_i = 1 \;\; ou \;\; 1+u \\ 2 & si \;\; x_i = u \end{cases}$$

La distance de *Lee* entre deux vecteurs x et $y \;\; \in (\mathbb{F}_2 + u\mathbb{F}_2)^n$ est définie par :

$$d_L(x, y) = \sum_{i=1}^{n} wt_L(x_i - y_i)$$

par suite

$$d_L(x - y) = wt_L(x - y)$$

Le poids d'Euclide est donné par la relation suivante :

$$wt_E(x) = \sum_{i=1}^{n} wt_E(x_i)$$

ou

$$wt_E(x_i) = \begin{cases} 0 & si \;\; x_i = 0 \\ 1 & si \;\; x_i = 1 \;\; ou \;\; 1+u \\ 4 & si \;\; x_i = u \end{cases}$$

La quantité

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

est appelée la distance minimale de C

Tout code linéaire non nul C sur $\mathbb{F}_2 + u\mathbb{F}_2$ est équivalent à un code qui a pour matrice génératrice la matrice suivante :

$$G = \begin{bmatrix} I_{k_1} & A & B \\ 0 & uI_{k_2} & uD \end{bmatrix}$$

où A et B sont des matrices sur $\mathbb{F}_2 + u\mathbb{F}_2$, D est une matrice sur $\mathbb{F}_2$.

Le code C contient tout mot du code $[v_0, v_1]\, G$ *où* v_0 est un vecteur de $\mathbb{F}_2 + u\mathbb{F}_2$ de

longueur k_1 et v_1 et un vecteur de $\mathbb{F}_2$ de longueur k_2.

Le code C contient $4^{K_1} * 2^{K_2}$ mots du code.

Les paramètres de C sont $\left[n, 4^{k_1} * 2^{k_2}, d_L\right]$ ou d_L représente la distance minimale de *Lee*.

On associe au code C deux codes binaires

le code résidu $C_1 = \{x \in \mathbb{F}_2^n / \exists\, y \in \mathbb{F}_2^n : x + uy \in C\}$

le code tortion $C_2 = \{x \in \mathbb{F}_2^n / ux \in C\}$

L'application *Gray* joue un role très intéressent sur les codes définis sur l'anneau $\mathbb{F}_2 + u\mathbb{F}_2$ cette application est définie de $\mathbb{F}_2 + u\mathbb{F}_2$ sur $\mathbb{F}_2^2$ par : $\Phi(x + yu) = (y, x + y)$ ou x et $y \in \mathbb{F}_2$

L'application *Gray* appliquée aux codes sur $\mathbb{F}_2 + u\mathbb{F}_2$ est analogue au cas de cette dernière appliquée aux codes sur $\mathbb{Z}_4$ *c.à.d* :

$$\begin{cases} 0 \longrightarrow 00 \\ 1 \longrightarrow 01 \\ u \longrightarrow 11 \\ 1 + u \longrightarrow 10 \end{cases}$$

À partir de cette définition et la définition du poids de *Lee*, on a les lemmes suivants :

Lemme 9. *[14] Si un code C est linéaire, le poids minimal de Lee de C est égal au poids minimal de Hamming de $\Phi(C)$.*

Lemme 10. *[14] Le poids minimal de Lee du code C est donné par* $\min(d_1, 2d_2)$ *où d_1 et d_2 les distances minimales des codes residus et tortions respectivement.*

Corollaire 3. *[14] Soit C un code linéaire sur $\mathbb{F}_2 + u\mathbb{F}_2$,*
alors $d_H \geq \left\lceil \frac{d_L}{2} \right\rceil$

3.9 Codes linéaires définis sur les anneuax principaux

Soit $\mathcal{R}$ un anneau principal fini.

Lemme 11 ([10], p. 54, Proposition 6)**.** *Soit* $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ *des idéaux de* $\mathcal{R}$*,premiers entre eux deux à deux et soit* $\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{a}_i$*. Pour tout* $\mathcal{R}$*-module* M*, l'homomorphisme canonique* $M \to \prod_{i=1}^{n} (M/\mathfrak{a}_i M)$ *est surjectif et son noyau est* $\mathfrak{a}M$*.*

Soit $\mathfrak{a}_i$ un idéal d'un anneau $\mathcal{R}$, et notons $\mathcal{R}_i = \mathcal{R}/\mathfrak{a}_i$. Donc nous avons un épimophisme canonique

$$\psi_i : \mathcal{R} \to \mathcal{R}_i$$

.

Proposition 15. *soit* $\mathcal{R}$ *un anneau commutatif fini . Alors les propositions suivantes sont equivalentes.*

(i) $\mathcal{R}$ *est un anneau principal .*

(ii) $\mathcal{R}$ *est isomorphe à un produit fini d'anneaux à chaine finis.*

De plus , la décomposition dans (ii) est unique . Elle est de la forme $\mathcal{R} \cong \prod_{i=1}^{k} R/\mathfrak{m}_i^{t_i}$*, où* $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_k$ *sont des idéaux maximaux de* $\mathcal{R}$*, et* $t_1, t_2, \ldots, t_k$ *sont les indices de stabilité respectives .*

Remarque 22. *Soit* $\mathcal{R}_i = \mathcal{R}/\mathfrak{m}_i^{t_i}$ *alors* $\mathcal{R}_i$ *est un anneau à chaine fini d'idéal maximal* $\mathfrak{m}_i/\mathfrak{m}_i^{t_i}$ *Pour* $i = 1, \ldots, k$*, soit* C_i *un code linéaire sur* R_i *de longueur* n *et soit*

$$C = CRT(C_1, C_2, \ldots, C_k) = \Psi^{-1}(C_1 \times \cdots \times C_k) = \{\Psi^{-1}(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k) \mid \mathbf{v}_i \in C_i\}.$$

avec

$$\psi : \mathcal{R} \to \prod_{i=1}^{k} \mathcal{R}_i, \quad \psi(u) = (\psi_1(u), \ldots, \psi_k(u))$$

On désigne par C *le code* ***Produit Chinois des Codes*** $C_1, C_2, \ldots, C_k$*.*

Pour avoir les propiriétés de C il suffit d'avoir les propriétés des C_i.

Exemple 26. *On utilise cette méthode pour étudier les codes linéaires définis sur* $\mathbb{Z}_n$ *avec* $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ *où les* p_i *sont des entiers premiers.*

3.10 Conclution

Dans ce chapitre nous avons donné des notions de bases sur les codes correcteurs définis sur les anneaux finis. Cela nous sera utile pour étudier un cas particulier de ces codes qui sont les codes cycliques et constacycliques définis sur les anneaux finis.

Chapitre 4

Codes Cycliques Définis sur les Anneaux Finis

4.1 Introduction

Le but de ce chapitre est de généraliser l'étude de Calderbank et Sloane sur les codes cycliques sur $\mathbb{Z}_{p^m}$.On parlera des codes cycliques sur les anneaux à chaine finis et les anneaux principaux plus précisement où la longueur n du code n'est pas divisible par la caractéristique p de son corps résiduel $\overline{\mathcal{R}}$. Tous les anneaux considérés sont commutatifs unitaires.

Les résultats suivants qui sont dans Mac Donald [41] résument quelques propriétes des anneaux commutatif à chaine finis.

4.2 Préliminaires

Pour la classe des anneaux commutatifs finis nous avons les équivalences suivantes :

Proposition 16. *Soit $\mathcal{R}$ un anneau commutatif fini les conditions suivantes sont équivalentes.*

i) *$\mathcal{R}$ est un anneau local et son ideal maximal M est principal.*

ii) $\mathcal{R}$ *est un anneau local principal.*

iii) $\mathcal{R}$ *est un anneau à chaine.*

Preuve:

i)$\Rightarrow$ ii) Soit I un idéal de $\mathcal{R}$ si $I = \mathcal{R}$ alors I est engendré par 1.
Si $I \subsetneq \mathcal{R}$ alors $I \subseteq M$ par i) M est engendré par un élément, par exemple $M =< \gamma >$, donc $I =< \gamma^k >$ pour un certain k d' où $\mathcal{R}$ est anneau local principal.
ii)$\Rightarrow$ iii) Soit $\mathcal{R}$ un anneau local principal d'idéal maximal M, $M =< \gamma >$, et $A,\ B$ deux idéaux propres de $\mathcal{R}$, alors $A,\ B \subseteq M$ donc ils existent des entiers $l,\ m$ tel que $A =< \gamma^l >$, $B =< \gamma^m >$ ($l,\ m \leq$ la nilpotence de γ) donc soit $A \subseteq B$ ou $B \subseteq A$ d'où $\mathcal{R}$ est un anneau à chaine fini.
iii)$\Rightarrow$ i) Supposons $\mathcal{R}$ un anneau à chaine fini, alors il est clair que $\mathcal{R}$ est local, pour prouver que l'ideal maximal M est principal, supposons le contraire que M est engendré par plus d'un élément par exemple $b,\ c$ tels que $b \notin c\mathcal{R}$ et $c \notin b\mathcal{R}$ alors $< b > \subsetneq < c >$ et $< c > \subsetneq < b >$ ce qui est absurde avec la supposition que $\mathcal{R}$ est un anneau à chaine d'où M est principal. □

Dans la suite on utilisera les équivalences vu ci-dessus.
Soit γ un générateur d'un idéal maximal M alors γ est nilpotent et on note par e son indice de nilpotence. Les idéaux de $\mathcal{R}$ forment une chaine,

$$\mathcal{R} = \langle \gamma^0 \rangle \supsetneq \langle \gamma^1 \rangle \supsetneq \ldots \supsetneq \langle \gamma^{e-1} \rangle \supsetneq \langle \gamma^e \rangle = \langle 0 \rangle.$$

Soit $\overline{\mathcal{R}} = \mathcal{R}/\langle \gamma \rangle$. On note par

$$- : \mathcal{R}[x] \longrightarrow \overline{\mathcal{R}}[x]$$

l'homomorphisme d'anneaux qui à x nous donne $x + \langle \gamma \rangle$ et à la variable x nous donne x.

Proposition 17. *Soit $\mathcal{R}$ un anneau commutatif à chaine fini d'idéal maximal, $M = \langle \gamma \rangle$ et d'indice de nilpotence e (ie $\gamma^e = 0$) alors*

a/ *Pour un certain entier premier p et des entiers positifs $k,\ r$ $(k \geq r)$; $|\mathcal{R}| = p^k$, $|\overline{\mathcal{R}}| = p^r$, et les caractéristiques de $\mathcal{R}$ et $\overline{\mathcal{R}}$ sont des puissances de p.*

b/ *Pour* $i = 0, \ldots e$,

$$|\langle \gamma^i \rangle| = |\overline{\mathcal{R}}|^{e-i}$$

en particulier $|\mathcal{R}| = |\overline{\mathcal{R}}|^e$ *ie* $k = re$

Définition 54. *Deux polynômes* $f_1, f_2 \in \mathcal{R}[x]$ *sont premiers entre eux si*

$$\langle f_1 \rangle + \langle f_2 \rangle = \mathcal{R}[x]$$

Ce qui est équivalent à $\exists g_1, g_2 \in \mathcal{R}[x]$ *tels que* $f_1 g_1 + f_2 g_2 = 1$.

Définition 55. i) *Un polynôme* $f \in \mathcal{R}[x]$ *est appelé un b-polynôme si* $\overline{f}$ *est irreductible dans* $\overline{\mathcal{R}}[x]$.

ii) *Un polynôme* $f \in \mathcal{R}[x]$ *est appele régulier si il n'est pas diviseur de 0 dans* $\mathcal{R}[x]$.

Proposition 18. *Soit* $f = a_0 + a_1 x + \ldots + a_n x^n \in \mathcal{R}[x]$ *nous avons les equivalences suivantes.*

i) f *est régulier*

ii) $\langle a_0, a_1, ..., a_n \rangle = \mathcal{R}$

iii) a_i *est inversible dans* $\mathcal{R}$ *pour un certain* i, $0 \leq i \leq n$

iv) $\overline{f} \neq 0$

Proposition 19. *Soient* f *et* g *deux polynômes réguliers dans* $\mathcal{R}[x]$ *alors*
f *et* g *sont premiers entre eux dans* $\mathcal{R}[x]$ *si et seulement si* $\bar{f}$ *et* $\bar{g}$ *sont premiers entre eux dans* $\bar{\mathcal{R}}[x]$

Preuve: Si f et g sont premiers entre eux dans $\mathcal{R}[x]$ alors il existe f_1 , $g_1 \in \mathcal{R}[x]$ tels que $f f_1 + g g_1 = 1$ et puisque $\bar{f} \neq 0$ et $\bar{g} \neq 0$ (f et g sont réguliers) alors on a $\bar{f}\vec{f_1} + \bar{g}\bar{g_1} = 1$ donc $\bar{f}$ et $\bar{g}$ sont premiers entre eux dans $\bar{\mathcal{R}}$.
Inversement, si $\bar{f}$ et $\bar{g}$ sont premiers entre eux dans $\bar{\mathcal{R}}$ alors il existe f_1 , $g_1 \text{et} v \in \mathcal{R}[x]$ tels que

$$f(x) f_1(x) + g(x) g_1(x) = 1 + \gamma^i v(x)$$

pour un certain $0 < i \leq e$ et puisque $1 + \gamma^i v(x)$ est un élément inversible dans $\mathcal{R}[x]$ alors $1 \in \langle f(x) \rangle + \langle g(x) \rangle$ par conséquent f et g son premiers entre eux dans $\mathcal{R}[x]$. $\square$

Le lemme suivant appelé lemme de Hensel, nous permet de relever la factorisation d'un polynôme $\overline{P(x)}$ en produit de facteurs irreductibles dans $\bar{\mathcal{R}}[x]$ en une factorisation similaire sur $\mathcal{R}$.
Pour $P(x)$ où $\overline{P(x)}$ est l'image de $P(x)$ par la réduction $(-)$ vu au paravant.

Lemme 12. *[lemme de Hensel] Soit f un polynôme sur $\mathcal{R}[x]$, supposons que $\overline{f} = g_1 g_2 ... g_r$ où $g_1, g_2, ..., g_r$ sont des polynômes sont des polynômes premiers entre eux deux à deux dans $\bar{\mathcal{R}}[x]$ alors ils existent des polynômes premiers entre eux deux à deux $f_1, f_2, ..., f_r$ dans $\mathcal{R}[x]$ tels que $f = f_1 f_2 ... f_r$ et $\overline{f_i} = g_i$ pour $i = 1, 2, ..., r$*

Soit D l'ensemble des polynômes $f \in \mathcal{R}[x]$ tels que $\overline{f}$ soit sans racine multiples dans une clôture algebrique de $\overline{\mathcal{R}}$.
La proposition suivante nous donne la relation entre polynômes irreductibles et b-polynomes réguliers de D.

Proposition 20. *(Mac Donald [41]) Soit f un polynôme régulier dans $\mathcal{R}[x]$, alors :*

i) *Si f est un b-polynôme , $\bar{f}$ est irréductible.*

ii) *Si f est irréductible , $\overline{f} = u.g^k$ où $u \in \overline{\mathcal{R}^*}$ et g est un polynôme unitaire irréductible dans $\overline{\mathcal{R}}[x]$*

iii) *Si $f \in D$ alors f est irréductible si seulement si f est un b-polynome.*

Définition 56. *Un idéal $I \subseteq \mathcal{R}$ est primaire si $I \neq \mathcal{R}$ et dés que $ab \in I$ alors soit $a \in I$ ou $\exists k \in \mathbb{N}$ tel que $b^k \in I$.*
Un polynôme $f \in \mathcal{R}[x]$ est dit primaire si $\langle f \rangle$ est un idéal primaire.

Proposition 21. *Si $f(x) \in \mathcal{R}[x]$ est un b-plynôme, alors $f(x)$ est un polynôme primaire.*

Preuve: Supposons que $f(x)$ soit un b-polynôme et $g(x)h(x) \in \langle f(x) \rangle$.

Alors $\overline{f}(x)$ est irréductible dans $\mathbb{F}_q[x]$, donc $(\overline{f}(x), \overline{g}(x)) = 1$ ou $\overline{f}(x)$. Si $(\overline{f}(x), \overline{g}(x)) = 1$, alors d'aprés la Proposition 19 f et g sont premiers entre eux, donc il existe f_1 et g_1 dans $\mathcal{R}[x]$ such that tels que $1 = f(x)f_1(x) + g(x)g_1(x)$. Donc $h(x) = f(x)h(x)f_1(x) + g(x)h(x)g_1(x)$. Puisque $g(x)h(x) \in \langle f(x)\rangle$, ce qui implique que $h(x) \in \langle f(x)\rangle$. Si $(\overline{f}(x), \overline{g}(x)) = \overline{f}(x)$, alors il existe $f_1(x), g_1(x) \in \mathcal{R}[x]$ tels que $g(x) = f(x)f_1 + \gamma^i g_1(x)$ pour un certain $i < e$. Alors pour $k > i$, on a $g^k(x) \in \langle f(x)\rangle$, et donc $f(x)$ est un plynôme primaire. □

Définition 57. *i) Soit $f_1(x),\ f_2(x) \in \mathcal{R}[x]$, $f_1(x)$ est dit associé à $f_2(x)$ si il existe un element inversible $r \in \mathcal{R}$ tel que $f_1(x) = r f_2(x)$ $(f_1(x) = f_2(x))$*

ii) Un polynôme $f(x) \in \mathcal{R}[x]$ est dit irréductible si $f(x) = g(x)h(x)$ où $g(x),\ h(x) \in \mathcal{R}[x]$ alors $g(x)$ ou $h(x)$ est un élément inversible dans $\mathcal{R}[x]$

Remarque 23. *L'irreductibilité d'un polynôme depend de l'anneau $\mathcal{R}$. Par exemple $x^2 + 1$ est irréductible sur $\mathbb{Z}$ mais est réductible sur $\mathbb{Z}_2$*

Proposition 22. *[41] Soit f un polynôme régulier dans $\mathcal{R}[x]$, alors $f = ug_1g_2...g_r$ où u est un élément inversible et $g_1, g_2, ..., g_r$ sont des polynômes réguliers primaires premiers entre eux deux à deux.*
De plus $g_1, g_2, ..., g_r$ sont uniques dans le sens où si

$$f = ug_1g_2...g_r \tag{4.1}$$
$$= vh_1h_2...h_s \tag{4.2}$$

où u, v sont inversibles,$\{g_i\}$ et $\{h_i\}$ sont des polynômes réguliers primaires premiers entre eux deux à deux dans $\mathcal{R}[x]$ alors $r = s$ et aprés réarrangement on obtient $\langle g_i\rangle = \langle h_i\rangle$, $1 \leq i \leq n$.

Proposition 23. *Un polynôme $f \in \mathcal{R}[x]$ est primaire si et seulement si $\overline{f}$ est primaire dans $\overline{\mathcal{R}}[x]$. Ce qui est équivalent à $\overline{f} = u.\overline{g}^n$ où $u \in \overline{\mathcal{R}}^*$ et $\overline{g}$ est un polynôme irreductible dans $\overline{\mathcal{R}}[x]$*

Proposition 24. *[21] Si f est un polynôme unitaire dans $\mathcal{R}[x]$ tel que $\overline{f}$ est sans racine multiples alors f admet une factorisation unique en produit de b-polunômes unitaires, premiers entre eux deux à deux.*

Proposition 25. *[41] Soient $f,\ g$ deux polynômes $\neq 0$ dans $\mathcal{R}[x]$ si g est régulier alors ils existent des polynômes $q,\ r \in \mathcal{R}[x]$ tels que $f = gq + r$ et $deg(r) < deg(g)$.*

Théorème 33 (critère d'Eisenstein)**.** *[21] Soit $n \geq 1$ et*

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$$

si il existe un entier premier p tel que

$$p/a_0, \ldots p/a_{n-1}, \ \ et \ \ p/a_n, p^2/a_0$$

alors $f(x)$ est irréductible dans $\mathbb{Q}[x]$

Remarque 24. *le critère d'Eisenstein n'est pas vrai dans $\mathbb{Z}_k[X]$*

Exemple 27. *$f(x) = x^2 + 10x + 5 \in \mathbb{Z}_{20}[X]$, $p = 5$ satisfait le critere mais $f(x) = x^2 + 10x + 5 = (x+5)^2$ donc n'est pas irreductible dans $\mathbb{Z}_{20}[X]$.*

4.3 Structure des codes cycliques définis sur les anneaux à chaine finis

On a déja vu (chapitre 3) qu'un sous ensemble $C \subseteq \mathcal{R}^n$ est appelé un code linéaire de longueur n sur $\mathcal{R}$. Si C est un $\mathcal{R}$-sous-module de $\mathcal{R}^n$.
C est dit cyclique si pour tout mot $x = (x_0, x_1, \ldots, x_{n-1}) \in C$ son cyclique décalage à droite $(x_{n-1}, x_0, \ldots, x_{n-2})$ est aussi dans C.
Un n-uples $C = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{R}^n$ est identifié à sa representation polynômiale $c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$ dans $\mathcal{R}[x]/\langle x^n - 1\rangle$
On montre [21] qu'un code cyclique C de longueur n sur $\mathcal{R}$ est cyclique si et seulement

si l'ensemble des representations polynômiales de ses mots est un idéal de $\mathcal{R}[x]/\langle x^n-1\rangle$.

Soient $x=(x_0,x_1,\ldots,x_{n-1}),\quad y=(y_0,y_1,\ldots,y_{n-1})\in\mathcal{R}^n$ on définit leurs produit par $x\cdot y=x_0y_0+x_1y_1+\ldots+x_{n-1}y_{n-1}\in\mathcal{R}$

$*$ Deux mots $x,\ y$ sont dits orthogonaux si $x\cdot y=0$

Pour un code linéaire C sur $\mathcal{R}$ son code dual

$$C^{\perp}=\{x\in\mathcal{R}^n/\ x\cdot y=0,\ \forall y\in C\}$$

Un code C est dit auto-dual si $C=C^{\perp}$.

Pour un anneau à chaine fini $\mathcal{R}$ d'idéal maximal $\langle\gamma\rangle$ avec l'indice de nilpotence e de γ pair.

Le code $\langle\gamma^{e/2}\rangle$ un code auto-dual appelé le code auto-dual trivial.

Proposition 26. *[37] Le nombre des mots de code d'un code C de longueur n sur $\mathbb{Z}_p^m$ est p^k pour un certain $k\in\{0,1,\ldots,mn\}$ de plus le code dual $C^{\perp}$ a p^l mots de code où $k+l=mn$.*

On utilisant la même démonstration utilisée pour la proposition 26 on montre que :

Proposition 27. *[21] Soit $\mathcal{R}$ un anneau fini d'ordre p^{α}. Le nombre des mots d'un code C de longueur n sur $\mathcal{R}$ est p^k pour un certain $k\in\{0,1,\ldots,\alpha n\}$ de plus le code dual $C^{\perp}$ a p^l mots de code où $k+l=\alpha n$.*

Proposition 28. *Soit $\mathcal{R}$ un anneau commutatif fini et*

$$\begin{aligned} a(x) &= a_0+a_1x+\ldots+a_{n-1}x^{n-1}\\ b(x) &= b_0+b_1x+\ldots+b_{n-1}x^{n-1}\in\mathcal{R}[X]\end{aligned}$$

alors $a(x)b(x)=0$ dans $\mathcal{R}[x]/\langle x^n-1\rangle$ si et seulement si $(a_0,a_1,\ldots,a_{n-1})$ est orthogonl à $(b_{n-1},b_{n-2},\ldots,b_0)$ et tout ses cycliques décalages à droite.

Preuve: Soit ξ le décalage à droite des mots de longueur n ie , pour $(x_0, x_1, \ldots, x_{n-1}) \in \mathcal{R}^n$

$$\xi(x_0, x_1, \ldots, x_{n-1}) = (x_{n-1}, x_0, \ldots, x_{n-2})$$

donc

$$\xi^i(b_{n-1}, b_{n-2}, \ldots, b_0), \quad i = 1, 2, \ldots, n$$

sont tous les décalage à droite de $(b_{n-1}, b_{n-2}, \ldots, b_0)$
Soit $c(x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} = a(x)b(x) \in \mathcal{R}[x]/\langle x^n - 1\rangle$ alors pour $k = 0, 1, \ldots, n-1$

$$\begin{aligned} c_k &= \sum_{i+j=k \text{ ou } i+j=n+k} a_i b_j, \qquad 0 \leq i,\ j \leq n-1 \\ &= (a_0, a_1, \ldots, a_{n-1}) \cdot (b_k, b_{k-1}, \ldots, b_{k+1}) \\ &= (a_0, a_1, \ldots, a_{n-1})\xi^{k+1}(b_{n-1}, b_{n-2}, \ldots, b_0) \end{aligned}$$

donc $c(x) = 0$ si et seulement si $c_k = 0$ pour $k = 0, 1, \ldots, n-1$ si et seulement si $(a_0, a_1, \ldots, a_{n-1})\xi^{k+1}(b_{n-1}, b_{n-2}, \ldots, b_0) = 0$ pour $k = 0, 1, \ldots, n-1$ si et seulement si $(a_0, a_1, \ldots, a_{n-1})$ est orthogonal à $(b_{n-1}, b_{n-2}, \ldots, b_0)$ et tous ses décalages à droite. Conclusion : Le code dual d'un code cyclique est un code cyclique.

4.4 Structure des codes cycliques définis sur les anneaux à chaine finis

Soit $\mathcal{R}$ un anneau à chaine fini d'idéal maximal $\langle\gamma\rangle$ et e l'indice de nilpotence de γ. De la proposition 17, il existe un nombre premier p et un entier r tel que $|\overline{\mathcal{R}}| = p^r$ et $|\mathcal{R}| = p^{re}$, les caractéristiques de $\mathcal{R}$ et $\overline{\mathcal{R}}$ sont des puissances de p dans cette partie, on suppose que n est un entier positif qui n'est pas divisible par p. D'où $\overline{x^n - 1}$ est sans racines multiples dans $\overline{\mathcal{R}}[x]$. ($(x^n - 1)' = nx^{n-1} \neq 0$ dans $\overline{\mathcal{R}}[x]$). Donc $x^n - 1$ a une unique décomposition en produit de b-polynômes unitaires premiers entre eux deux à deux dans $\mathcal{R}[x]$ (proposition 24)

Lemme 13. *[21] Soit $\mathcal{R}$ un anneau à chaine fini d'idéal maximal $\langle\gamma\rangle$ et e l'indice de nilpotence de γ. Si f est un b-polynôme de $\mathcal{R}[x]$ alors $\mathcal{R}[x]/\langle f\rangle$ est aussi un anneau à chaine fini, avec comme chaine d'idéaux :*

$$\mathcal{R}[x]/\langle f\rangle = \langle 1+\langle f\rangle\rangle \supseteq \langle \gamma+\langle f\rangle\rangle \supseteq \cdots \supseteq \langle \gamma^{e-1}+\langle f\rangle\rangle \supseteq \langle \gamma^{e}+\langle f\rangle\rangle = \langle 0\rangle$$

pour un polynôme $f(x)$ de degre k son polynôme réciproque $x^k f(x^{-1})$ est noté par f^* par exemple.
Si

$$f(x) = a_0 + a_1 x + \ldots + a_{k-1}x^{k-1} + a_k x^k$$

alors

$$\begin{aligned} f^*(x) &= x^k(a_0 + a_1 x^{-1} + \ldots + a_{k-1}x^{-(k-1)} + a_k x^{-k}) \\ &= a_k + a_{k-1}x + \ldots + a_1 x^{-(k-1)} + a_0 x^k \end{aligned}$$

de plus si $f(x)$ est un facteur de x^n-1 on note $\hat{f}(x) = x^n - 1/f(x)$

Théorème 34. *Soit $\mathcal{R}$ un anneau à chaine fini d'idéal maximal $\langle\gamma\rangle$ et e l'indice de nilpotence de γ ($\gamma^e = 0$). Soit $x^n-1 = f_1 f_2 \ldots f_r$ factorisation unique en b-polynômes premiers entre eux deux à deux dans $\mathcal{R}[x]$, alors tout idéal de $\mathcal{R}[x]/\langle x^n-1\rangle$ est somme d'idéaux de la forme $\langle \gamma^j \hat{f}_i + \langle x^n-1\rangle\rangle$ où $0 \le j \le e$ et $0 \le i \le r$.*

Preuve: Le théorème des restes chinois nous donne

$$\mathcal{R}[x]/\langle x^n-1\rangle = \mathcal{R}[x]/\bigcap_{i=1}^{r}\langle f_i\rangle \approx \oplus\sum_{i=1}^{r}\mathcal{R}[x]/\langle f_i\rangle$$

donc tout idéal I dans $\mathcal{R}[x]/\langle x^n-1\rangle$ est de la forme $\oplus\sum_{i=1}^{r} I_i$ où I_i est un idéal de $\mathcal{R}[x]/\langle f_i\rangle$ (lemme 13) pour $0 \le i \le r$, $I_i = 0$ où

$$I_i = \sum\langle \gamma^k + \langle f_i\rangle\rangle$$

dans $\mathcal{R}[x]/\langle x^n-1\rangle$. Par conséquant I est une somme d'idéaux de la forme $\langle \gamma^j \hat{f}_i + \langle x^n-1\rangle\rangle$

Théorème 35. *[21] Soit C un code cyclique de longueur n sur l'anneau à chaine fini $\mathcal{R}$ d'idéal maximal $\langle\gamma\rangle$ d'indice de nilpotence e et $(n,q)=1$ où q est le cardinal de son corps résiduel, alors il existe une famille unique de polynomes premiers entre eux deux à deux unitaires $F_0, F_1, ..., F_e$ dans $\mathcal{R}[x]$ tels que $F_0F_1...F_e = x^n - 1$ et*

$$C = \langle \hat{F}_1, \gamma\hat{F}_2, \ldots, \gamma^{e-1}\hat{F}_e \rangle$$

de plus

$$|C| = (|\bar{\mathcal{R}}|)^{\sum_{i=0}^{e-1}(e-i)\deg F_{i+1}}$$

Dans ce qui suit nous donnons une méthode calculatoire pour avoir le relevé de Hensel d'un polynôme,appelée aussi méthode de Graeffe.

4.5 Relèvement de Hensel

Nous présentons le relèvement de Hensel, qui permet d'obtenir (relever), sous certaines conditions, une factorisation d'un polynôme dans l'anneau $\mathbb{Z}_{p^k}[X]$ à partir d'une factorisation dans $\mathbb{Z}_p[X]$. Cela nous servira dans deux cadres différents : en premier lieu, cela permet une construction effective des anneaux de Galois ; en second lieu, le relèvement de Hensel sera une technique de construction de codes cycliques sur $\mathbb{Z}_{p^k}$. Nous illustrons le fonctionnement du relèvement par un algorithme de calcul dans le cas $p = 2$.

Lemme 14. *[41] **(Lemme de Hensel)** Soient p un nombre premier, k un entier supérieur ou égal à 2 et $P \in \mathbb{Z}_{p^k}[X]$ un polynôme unitaire, tel que*

$$P \equiv QR \ (mod\ p),$$

pour $Q, R \in \mathbb{Z}_p[X]$, deux polynômes unitaires premiers entre eux. Alors, il existe un unique couple $(Q^{(k)}, R^{(k)})$ de polynômes unitaires de $\mathbb{Z}_{p^k}[X]$, tel que

1. $P = Q^{(k)}R^{(k)}$,
2. $Q^{(k)} \equiv Q(mod\ p)$ *et* $R^{(k)} \equiv R(mod\ p)$,

3. $Q^{(k)}$ *et* $R^{(k)}$ *sont premiers entre eux.*

De plus, on a $deg(Q^{(k)}) = deg(Q)$ *et* $deg(R^{(k)}) = deg(R)$.

L'anneau $\mathbb{Z}_p[X]$ étant factoriel,donc tout polynôme à coefficients dans $\mathbb{Z}_p$ se décompose de manière unique en produit de facteurs irréductibles. On a pour tout polynôme $P \in \mathbb{Z}_{p^k}[X]$:

$$P \equiv f_1^{e_1}...f_l^{e_l} \ (mod\ p),$$

où $f_1, ..., f_l$ sont des polynômes irréductibles de $\mathbb{Z}_p[X]$ et $e_1, ..., e_l$ des entiers strictement positifs. Il est donc possible, par récurrence sur le nombre de facteurs, de généraliser le lemme 1.3 afin d'obtenir la factorisation de tout polynôme de $\mathbb{Z}_{p^k}[X]$ à partir de sa factorisation dans $\mathbb{Z}_p[X]$.

Théorème 36. *[41] Soient* p *un nombre premier,* k *un entier supérieur ou égal à* 2 *et* $P \in \mathbb{Z}_{p^k}[X]$ *un polynôme unitaire. Soit* $P \ mod\ p = f_1^{e_1} \cdots f_l^{e_l}$ *la factorisation de* P *dans* $\mathbb{Z}_p[X]$*, où* $f_1, \ldots, f_l$ *sont des polynômes irréductibles et* $e_1, \ldots, e_l$ *des entiers strictement positifs. Il existe un unique* l*-uplet* $(g_1^{(k)}, \ldots, g_l^{(k)})$ *de polynômes unitaires de* $\mathbb{Z}_{p^k}[X]$*, tel que*

1. $P = g_1^{(k)}...g_l^{(k)}$,
2. $g_i^{(k)} \equiv f_i^{e_i} \ (mod\ p)$,
3. *les* $g_i^{(k)}$ *sont deux à deux premiers entre eux.*

En d'autres termes, les polynômes unitaires de $\mathbb{Z}_{p^k}[X]$ se décomposent -de manière unique- en produits de polynômes du type $g_i^{(k)}$, Réduits modulo p, ils sont des puissances d'un polynôme irréductible. Cette propriété va nous permettre de définir le relevé de Hensel d'un facteur de $X^n - 1$ où n est premier avec p. En effet, dans ce cas, $X^n - 1$ ne comporte que des facteurs simples.

Définition 58. ***(Relevé de Hensel)*** *Soient* Q *et* R *deux polynômes à coefficients dans* $\mathbb{Z}_p$ *tels que* $X^n - 1 = Q(X)R(X)$ *où* n *est un entier premier avec* p*. On appelle* ***relevé de Hensel*** *d'ordre* k *du polynôme* Q*, le polynôme* $Q^{(k)}$ *du couple* $(Q^{(k)}, R^{(k)})$.

Proposition 29. *Soit $Q \in \mathbb{Z}_p$ un facteur de $X^n - 1$. Son relevé de Hensel d'ordre k divise $X^n - 1$ dans $\mathbb{Z}_{p^k}[X]$.*

Le cas le plus important dans la suite est le cas binaire, i.e. $p = 2$. La proposition suivante décrit un algorithme itératif de calcul du relevé de Hensel d'un polynôme pour $p = 2$.

Proposition 30. *[30] **(Calcul du relevé de Hensel binaire)** Soient $Q \in \mathbb{Z}_2[X]$ un facteur de $X^{2^m-1} - 1$ et $Q^{(k)} \in \mathbb{Z}_{2^k}[X]$ son relevé de Hensel d'ordre k. Posons $Q^{(k)}(X) = P(X) - I(X)$ où P contient les monômes de degré pair et I ceux de degré impair. On a alors $Q^{(k+1)}(X^2) = \pm(P^2(X) - I^2(X))$, les opérations étant faites dans $Z_{p^{k+1}}[X]$ et le signe étant choisi pour que Q^{k+1} soit unitaire.*

Exemple 28. *Reprenons notre code de Hamming avec $m = 3$ et $a = 7$. La factorisation de $X^7 - 1$ modulo 2 donne*

$$X^7 - 1 = (X - 1)(X^3 + X^2 + 1)(X^3 + X + 1)$$

Posons $Q = Q^{(1)}(X) = X^3 + X + 1 \in \mathbb{Z}_2[X]$ et appliquons la proposition 1.30 pour calculer son relevé d'ordre 3 (un b-polynôme avec notre définition). On a

$$\begin{aligned} P_1(X) &= 1 && mod\ 2, \\ I_1(X) &= X^3 + X && mod\ 2, \end{aligned}$$

donc

$$\begin{aligned} (P_1(X))^2 &= 1 && mod\ 4, \\ (I_1(X))^2 &= X^6 + 2X^4 + X^2 && mod\ 4, \end{aligned}$$

d'où

$$Q^{(2)}(X^2) = -X^6 - 2X^4 - X^2 + 1 \quad mod\ 4$$

Ainsi, le relevé de Hensel d'ordre 2 du polynôme $Q(X)$ est

$$Q^{(2)}(X) = X^3 + 2X^2 + X - 1 \quad mod\ 4,$$

De même, pour calculer $Q^{(3)}$ *on décompose* $Q^{(2)}$ *sous la forme :*

$$\begin{aligned} P_2(X) &= 2X^2 - 1 \qquad mod\ 4, \\ I_2(X) &= X^3 + X \qquad mod\ 4, \end{aligned}$$

ce qui donne

$$\begin{aligned} (P_2(X))^2 &= 4X^4 - 4X^2 + 1 \qquad mod\ 8, \\ (I_2(X))^2 &= X^6 + 2X^4 + X^2 \qquad mod\ 8, \end{aligned}$$

On a donc

$$Q^{(3)}(X^2) = X^6 - 2X^4 + 5X^2 - 1 \quad mod\ 8,$$

soit, finalement

$$Q^{(3)}(X) = X^3 + 6X^2 + 5X + 7 \quad mod\ 8$$

On peut alors vérifier que $Q^{(3)}$ *est bien un diviseur de* $X^7 - 1$ *dans* $\mathbb{Z}_8[X]$*, en effet*

$$Q^{(3)}(X)(X^4 + 2X^3 + 7X^2 + 5X + 1) = X^7 - 1 \quad mod\ 8.$$

Bien entendu, $X^4 + 2X^3 + 7X^2 + 5X + 1$ *est le relevé de Hensel d'ordre* 3 *du polynôme* $(X^3 + X^2 + 1)(X - 1)$*.*

Dans la suite nous donnons des exemples de codes cycliques définis sur les anneaux à quatre éléments.

4.6 Codes cycliques définis sur $\mathbb{Z}_4$

$\mathbb{Z}_4$ est un anneau à chaine fini à quatre éléments ,d'idéal maximal $2\mathbb{Z}_4$, d'indice de nilpotence 2 et de corps résiduel $\mathbb{Z}_2$.

4.6.1 Polynôme générateur d'un code cyclique sur $\mathbb{Z}_4$

Corollaire 4. *[46] Soit* n *un entier impair,* $x^n - 1$ *le produit de* k *polynômes sur* $\mathbb{Z}_4$ *alors il y a* 3^k *codes cycliques de longueur* n *sur* $\mathbb{Z}_4$ *.*

Théorème 37. *[46] Soit C un code cyclique sur $\mathbb{Z}_4$ de longueur n, alors il existe des polynômes unitaires uniques f, g et h tels que $x^n - 1 = fgh$ et $C = \langle fh \rangle \oplus \langle 2fg \rangle$ de plus C est de type $4^{deg\ g}.2^{deg\ h}$*

1) Si $h = 1$,$C = \langle f \rangle$ et $|C| = 4^{n-deg\ f}$

2) Si $g = 1$, $C = \langle 2f \rangle$ et $|C| = 2^{n-deg\ f}$.

Exemple 29. *Par La méthode de Greaffe $(x-1)(x^3+2x^2+x-1)(x^3-x^2+2x-1)$ est la factorisation de (x^7-1) en facteurs irréductibles dans $\mathbb{Z}_4[x]$. $x^7-1 = g_1(x)g_2(x)g_3(x)$ où*

$$f(x) = g_1(x) = x - 1$$

$$g(x) = g_2(x) = x^3 + 2x^2 + x - 1$$

$$h(x) = g_3(x) = x^3 - x^2 + 2x - 1$$

sont les facteurs unitaires irréductibles de $x^7 - 1$. D'après le corolaire précédant il y a $3^3 = 27$ codes cycliques sur $\mathbb{Z}_4$ de longueur 7. On a $C = \langle f(x)h(x) \rangle \oplus \langle 2f(x)g(x) \rangle$.
On prend $g_1(x)g_3(x) = (x-1)(x^3 - x^2 + 2x) = 1 + x + 3x^2 + 2x^3 + x^4$
$g_1(x)g_2(x) = (x-1)(x^3 + 2x^2 + x - 1)$
il est de type $4^3.2^3$ sa matrice génératrice est la suivante

$$G = \begin{bmatrix} 1 & 1 & 3 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 3 & 2 & 1 & 0 \\ 0 & 0 & 1 & 1 & 3 & 2 & 1 \\ 2 & 0 & 2 & 2 & 2 & 0 & 0 \\ 0 & 2 & 0 & 2 & 2 & 2 & 0 \\ 0 & 0 & 2 & 0 & 2 & 2 & 2 \end{bmatrix}$$

4.7 Codes cycliques définis sur $\mathbb{F}_2 + u\mathbb{F}_2$

Nous avons déja vu la définition de l'anneau $\mathbb{F}_2 + u\mathbb{F}_2$, (voir chapitre 3) qui est un anneau à chaine fini. Nous donnons dans ce qui suit des exemples de codes cycliques définis sur cet anneau.

Le nombre de codes cycliques sur $\mathbb{F}_2 + u\mathbb{F}_2$ est 3^r où r est le nombre de b-polynômes facteurs de $x^n - 1$ sur $\mathbb{F}_2 + u\mathbb{F}_2$.
Par le théorème 35 les codes cycliques sur $\mathcal{R}$ sont donné par la description de leur polynôme générateur.
La factorisation de $x^n - 1$ en facteur irréductible sur $\mathbb{F}_2$ donne :

$$x^n - 1 = f_1 f_2 ... f_r$$

Les codes cycliques sur $\mathbb{F}_2 + u\mathbb{F}_2$ sont obtenus en partitionnant les facteurs de $x^n - 1$ en trois blocs f,g et h par exemple $f = f_1 f_2$, $g = f_3 f_4 f_5$ et $h = f_6 ... f_r$; en plus f,g,h peuvent prendre la valeur de 1.

Soit C un code cyclique de longueur n sur $\mathcal{R}$, alors d'aprés le théorème 35, il existe des b-polynômes unitaires uniques f, g, h tel que $C = (fh, ufg)$ où $fgh = (x^n - 1)$ et $|c| = 4^{deg(g)} 2^{deg(h)}$
ou a :

a) Si $h = 1$,$C = (f)$ et $|C| = 4^{n-deg(f)}$

b) Si $g = 1$,$C = (uf)$ et $|C| = 2^{n-deg(f)}$

Exemple 30. *La factorisation de* $x^7 - 1$ *dans* $\mathbb{F}_2 + u\mathbb{F}_2$ *est* $f_1 f_2 f_3$ *où*
$f_1(x) = x + 1$, $f_2(x) = x^3 + x + 1$, $f_3(x) = x^3 + x^2 + 1$

TABLE 4.1 – Codes cycliques définis sur $\mathbb{F}_2 + u\mathbb{F}_2$ de longueur 7

Générateur	Ordre	d_{Lee}	Paramètres du code binaire image
(uf_2f_3)	2	14	$[14, 1, 14]$
(uf_1f_3)	2^3	8	$[14, 3, 8]$
(uf_3)	2^4	6	$[14, 4, 6]$
(uf_1f_2)	2^3	8	$[14, 3, 8]$
(uf_2)	2^4	6	$[14, 4, 6]$
(uf_1)	2^6	4	$[14, 6, 4]$
(u)	2^7	2	$[14, 7, 2]$
(f_2f_3)	4	7	$[14, 2, 7]$
(f_2f_3, uf_1f_3)	4.2^3	6	$[14, 5, 6]$
(f_2f_3, uf_1f_2)	4.2^3	6	$[14, 5, 6]$
(f_2f_3, uf_1)	4.2^6	2	$[14, 8, 2]$
(f_1f_3)	4^3	4	$[14, 6, 4]$
(f_1f_3, uf_2f_3)	$4^3.2$	4	$[14, 7, 4]$
(f_1f_3, uf_1f_2)	$4^3.2^3$	4	$[14, 9, 4]$
(f_1f_3, uf_2)	$4^3.2^4$	2	$[14, 10, 2]$
(f_3)	4^4	3	$[14, 8, 3]$
(f_3, uf_1f_2)	$4^4.2^3$	2	$[14, 11, 2]$
(f_1f_2)	4^3	4	$[14, 6, 4]$
(f_1f_2, uf_2f_3)	$4^3.2$	4	$[14, 7, 4]$
(f_1f_2, uf_1f_3)	$4^3.2^3$	4	$[14, 9, 4]$
(f_1f_2, uf_3)	$4^3.2^4$	2	$[14, 10, 2]$
(f_2)	4^4	3	$[14, 8, 3]$
(f_2, uf_1f_3)	$4^4.2^3$	2	$[14, 12, 2]$
(f_1)	4^6	2	$[14, 12, 2]$
(f_1, uf_2f_3)	$4^6.2$	2	$[14, 13, 2]$

Il existe une autre forme des générateurs de codes cyclique définis sur $\mathcal{R}$ donnée par le théorème suivant

Théorème 38. *[21] Soit C un code cyclique de longueur n sur l'anneau à chaine fini $\mathcal{R}$ d'idéal maximal $\langle\gamma\rangle$ et d'indice de nilpotence e ($\gamma^e = 0$), alors ils existent des polynômes $g_0, g_1, ..., g_{e-1}$ dans $\mathcal{R}[x]$ tels que*

$$C = \langle g_0, \gamma g_1, \ldots, \gamma^{e-1} g_{e-1} \rangle$$

et

$$g_{e-1}/g_{e-2}/.../g_1/g_0/(x^n - 1)$$

Théorème 39. *[21] Soit C un code cyclique de longueur n avec les notations du théorème 35*

$$F = \hat{F}_1 + \gamma \hat{F}_2 + \cdots + \gamma^{e-1} \hat{F}_e$$

alors F est un générateur de C ie $C = \langle F \rangle$

Du théorème 35 on déduit le corollaire suivant :

Corollaire 5. *$\mathcal{R}[x]/\langle x^n - 1\rangle$ est un anneau principal.*

Ce qui n'est pas le cas pour $(n, p) \neq 1$ (exemple les codes sur $\mathbb{Z}_4$ de longueur paire) ne sont pas tous principaux.Voir comme exemple [1]

Dans ce qui suit, on verra une famille de codes plus générale que les codes cycliques qui sont les codes constacycliques.

4.8 les codes constacycliques

Pour un élément inversible $\lambda \in \mathcal{R}$, un code C est dit constacyclique ou plus généralement λ-constacyclique si $(\lambda c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$ dés que $(c_0, c_1, \ldots, c_{n-1}) \in C$. Par exemple, les cycliques et les negacycliques correspond à $\lambda = 1$ et respectivement à $\lambda = -1$.

Théorème 40. *Soit λ un élément inversible dans un anneau à chaine fini, $\mathcal{R}$ de caratéristique p. Où $(n,p)=1$. Le polynôme $x^n-\lambda$ admet une unique factorisation en b-polynômes unitaires premiers entre eux deux à deux sur $\mathcal{R}$. De plus, il existe une correspondance biunivoque entre l'ensemble des b-polynômes facteurs de $x^n-\lambda$ dans $\mathcal{R}[x]$ et l'ensemble des polynômes irréductibles diviseurs de $\overline{x^n-\lambda}$ dans $\bar{\mathcal{R}}=\mathbb{F}_q=\mathbb{F}_{p^r}$.*

Preuve: Si $(n,p)=1$ on déduit que $\overline{x^n-\lambda}$ est sans racines multiples dans $\mathbb{F}_q[x]$. Par le lemme 24, $x^n-\lambda$ admet une unique factorisation en b-polynômes unitaires premiers entre eux deux à deux dans $\mathcal{R}[x]$
$x^n-\lambda=f_1f_2\dots f_s$, puisque $\mathbb{F}_q[x]$ est un anneau factoriel alors,

$x^n\bar{-}\lambda$ admet une unique factorisation en polynômes unitaires irréductibles dans $\mathbb{F}_q[x]$,
$x^n\bar{-}\lambda=h_1h_2\dots h_k$. Ces polynômes sont premiers entre eux ($(n,p)=1$). Par le lemme de Hensel 12, il existe des polynômes $\tilde{h_i}$ dans $\mathcal{R}[x]$ tels que $\bar{\tilde{h_i}}=hi$ et $x^n-\lambda=\tilde{h}_1\tilde{h}_2\dots\tilde{h}_k$. Donc $\tilde{h}_i$ pour $1\leq i\leq k$ sont des b-polynômes unitaires de $\mathcal{R}[x]$ premiers entre eux deux à deux. De l'unicité de la décomposition de $x^n-\lambda$ dans $\mathcal{R}[x]$, on déduit que $\tilde{h}_i=f_i$ et $k=s$.

□

Dinh et López-Permouth [21] ont montré que les codes négacycliques de longueur impair sont isomorphes aux codes cycliques de même longueur si $(n,p)=1$.
Nous allons montré que cet isomorphisme reste vrai pour un cas plus général .

Proposition 31. *[6] Soit n un entier positif impair et λ un élément inversible tel que $\lambda^2=1\in\mathcal{R}^*$. Soit μ l'application*

$$\mu:\mathcal{R}[x]/\langle x^n-1\rangle\longrightarrow\mathcal{R}[x]/\langle x^n-\lambda\rangle.$$

définie par $\mu(c(x))=c(\lambda x)$. Alors μ est un isomorphisme d'anneau.

Preuve: Il est clair que μ est un homomorphisme d'anneaux, on montre seulement

que μ est bijective.Pour cela, soit $f(x)$ et $g(x)$ deux polynomes dans $\mathcal{R}[x]$ tels que

$$f(x) \equiv g(x) \pmod{x^n - 1}.$$

Ce qui est équivalent à l'existence de $h(x) \in \mathcal{R}[x]$ tel que $f(x) - g(x) = h(x)(x^n - 1)$. La derniere egalité est vraie si $f(\lambda x) - g(\lambda x) = h(\lambda x)((\lambda x)^n - 1)$ est vraie,car $\lambda^n = \lambda$ et $\lambda^2 = 1$,ce qui est equivalent à $f(\lambda x) - g(\lambda x) = \lambda h(\lambda x)(x^n - \lambda)$si et seulement si$f(\lambda x) - g(\lambda x) \equiv 0 \mod x^n - \lambda$. Ce qui implique que f et g sont dans $\mathbb{R}[x]/\langle x^n - 1\rangle$,nous avons $f(x) = g(x)$ si et seulement si $\mu(f(x)) = \mu(g(x))$. d'où μ est un isomorphisme. □

Les ideaux de $\mathcal{R}[x]/\langle x^n - \lambda\rangle$ sont principaux alors le corollaire suivant est une conséquence directe de la Proposition 31

Corollaire 6. *[6] Soit $\mathcal{R}$ un anneau à chaine fini et λ un élément inversible dans $\mathcal{R}$. Un sous ensemble I dans $\mathcal{R}[x]$ est un idéal dans $\mathcal{R}[x]/\langle x^n - 1\rangle$ ce qui implique que C est un code cyclique de longueur n sur un anneau à chaine fini $\mathcal{R}$, si et seulement si $\mu(C)$ est un λ-constacyclique code de longueur n sur $\mathcal{R}[x]$.*

Exemple 31. *les codes $(1 \pm \gamma^{e-1})$-constacycliques sur $\mathbb{F}_2 + \gamma\mathbb{F}_2 + \ldots \gamma^{e-1}\mathbb{F}_2$ sont equivalents aux codes cycliques puisque $(1 \pm \gamma^{e-1})^2 = 1$.*

Dans la suite, on donne des conditions nécessaires et suffisantes pour l'existence des codes cycliques auto-duaux sur les anneaux finis.

4.9 Les codes duaux des codes cycliques

Dans [39], on donne une caratérisation des codes auto-duaux cycliques sur $\mathbb{Z}_p^m$. Dans [21] on généralise cette caratérisation aux codes cycliques sur les anneaux à chaine finis.

Théorème 41. *Soit C un code cyclique sur $\mathcal{R}$ avec*

$$C = \langle \hat{F}_1, \gamma\hat{F}_2, \ldots, \gamma^{e-1}\hat{F}_e \rangle$$

et

$$|C| = (|\bar{\mathcal{R}}|)^{\sum_{i=0}^{e-1}(e-i)\deg F_{i+1}},$$

où $F_0F_1...F_e = x^n - 1$ *et* $F_{e+1} = F_0$ *alors et*

$$C^{\perp} = \langle \hat{F}_0^{\star}, \gamma \hat{F}_e^{\star}, \ldots, \gamma^{e-1} \hat{F}_2^{\star} \rangle$$

$$|C^{\perp}| = (|\bar{\mathcal{R}}|)^{\sum_{i=1}^{e} e \deg F_{i+1}}$$

Exemple 32. *Code cycliques de longueur* $n = 6$ *sur* $\mathbb{Z}_{49}$.
La factorisation de $x^6 - 1$ *sur* $\mathbb{Z}_{49}$ *en produit de b-polynômes ppremiers entre eux sur* $\mathbb{Z}_{49}$ *est :*

$$x^6 - 1 = (x-1)(x+1)(x+18)(x-18)(x+19)(x-19).$$

Pour $f(x) = x - 18$, $f^{\star}(x) = -18(x-19)$, *donc* $x^6 - 1 = g(x)f(x)f^*(x)$ *avec* $g(x) = -18(x-1)(x+1)(x+18)(x+19)$. *Si*

$$C = (f^*g, 7ff^{\star})$$

alors

$$C^{\perp} = ((f^*)^*g^*, 7ff^*) = C$$

Lemme 15. *Soit* $F_0F_1...F_e = x^n - 1$ *et*

$$C = \langle \hat{F}_1, \gamma \hat{F}_2, \ldots, \gamma^{e-1} \hat{F}_e \rangle$$

alors dans $\mathcal{R}[x]/\langle x^n - 1 \rangle$

a) $\hat{F}_i^* \hat{F}_i^* = 0$

b) $\hat{F}_i^*, \hat{F}_i^*$ *,sont premiers entre eux* $\forall i \in \{0, 1, \ldots, e\}$

Théorème 42. *Avec les mêmes notations que le théorème 41*

$$G = \hat{F_0}^{\star} + \gamma \hat{F_e}^{\star} + \cdots + \gamma^{e-1} \hat{F_2}^{\star}$$

alors G *est un polynôme générateur de* C *ie* $C = \langle G \rangle$

Proposition 32. *[21] Soit* $F_0F_1...F_e = x^n - 1$ *et*

$$C = \langle \hat{F}_1, \gamma\hat{F}_2, \ldots, \gamma^{e-1}\hat{F}_e \rangle$$

35 alors C *est un code auto-dual si et seulement si* F_i *et* F_j^* *sont associés pour tout* $i, j \in \{0, 1, \ldots, e\}$ *tels que* $i + j \equiv 1 \, mod(e+1)$

Lemme 16. i) *Si* $degf \geq degg$ *alors* $(f(x) + g(x))^* = f^*(x) + x^{degf - degg} g^*(x)$

ii) $(f(x)g(x))^* = f^*(x)g^*(x)$

iii) *Si* f *est unitaire alors* $(\bar{f^*}) = (\bar{f})^*$

Théorème 43. *Supposons* e *un entier pair alors il existe un code cyclique non trivial auto-dual sur* $\mathcal{R}$ *si et seulemnet si il existe un b-polynôme* $f \in \mathcal{R}[x]$ *facteur de* $x^n - 1$ *tel que* f *et* f^* *ne soient pas associés.ie* $((f) \neq (f^*))$

Permounth a donné une construction pour l'existence de codes auto-duaux [21], nous donnons une autre construction.

Preuve: Supposons qu'il existe un b-polynôme $f \in \mathcal{R}[x]$ diviseur de $x^n - 1$ tel que f et f^* ne soient pas associés, alors puisque le terme constant de f est différent de zero,alors $degf = degf^*$ et f^* est aussi diviseur de $x^n - 1$ de plus ff^* est un facteur de $x^n - 1$ on ecrit $x^n - 1 = ff^*g$

dans la factorisation $x^n - 1 = F_0F_1 \ldots F_e$ on prend $F_0 = f$, $\mathbb{F}_1 = f^*$ et $F_{e/2+1} = g$

Conçidérons

$$C = \langle fg, \gamma^{e/2} ff^* \rangle$$

puis que $1 - x^n = (x^n - 1)^* = (ff^*g)^* = f^*fg^*$ on a $ff^*g = -ff^*g$, ce qui implique $g = -g^*$ par le théorème 41 et lemme 16

$$\begin{aligned} C^\perp &= \langle \hat{F_0}^*, \gamma^{e/2}\hat{F}^*_{e/2+1} \rangle && (4.3) \\ &= \langle (f^*g)^*, \gamma^{e/2}(ff^*)^* \rangle && (4.4) \\ &= \langle -fg^*, \gamma^{e/2} f^*f \rangle && (4.5) \\ &= \langle fg, \gamma^{e/2} ff^* \rangle = C && (4.6) \end{aligned}$$

Inversement, supposons qu'il existe un code cyclique auto-dual C, par le théorème 35

$$C = \langle \hat{F}_1, \gamma \hat{F}_2, \ldots, \gamma^{e-1} \hat{F}_e \rangle$$

où $F_0, F_1, \ldots, F_e$ sont des polynômes unitaires dans $\mathcal{R}[x]$ tel que $F_0 F_1 \ldots F_e = x^n - 1$. Supposons que $\forall f \diagup x^n - 1$ f et f^* soient associés. alors F_i et F_i^* sont aussi associés pour $i = 0, \ldots e$.

Puisque C est auto-dual (proposition 32) on déduit que $\forall i, j \in 0, \ldots e$ tels que $i + j \equiv 1 \mod (e+1)$.

F_i est associé avec F_j^* et donc associé avec F_j puisque $x^n - 1$ n'a pas de racine multiples ceçi implique que pour $i, j \in 0, \ldots e$ avec $i + j \equiv 1 \mod (e+1)$ soit $F_i = F_j = 1$ soit $F_i = F_j$ donc $F_i = 1, \ \forall i, \in 0, \ldots e \diagdown \dfrac{e}{2} + 1$ et $F_{\frac{e}{2}+1} = x^n - 1$ donc $C = \langle \gamma^{e/2} \rangle$ qui est le code auto-dual trivial contradiction. □

Ce qui implique que l'on doit avoir l'existence d'un b-polynôme facteur de $x^n - 1$ dans $\mathcal{R}[x]$ tel que f et f^* ne soient pas associes.

En utilisant la factorisation de $x^n - 1$ sur $\mathbb{F}_q$ et les propriétes des classe cyclotomiques, on arrive a cette condition nécéssaire et suffisante d'existence des codes cycliques auto-duaux non triviaux sur $\mathcal{R}$.

Théorème 44. *Soit $\mathcal{R}$ un anneau à chaine fini d'idéal maximal $\langle \gamma \rangle$ $|\mathbb{R}| = p^{le}$ où $|\bar{\mathbb{R}}| = p^l$ et e l'indice de nilpotence de γ. Alors il existe un code cyclique auto-dual de longueur n sur $\mathcal{R}$ si et seulement si $q^i \ncong -1 (mod\ n)$ $\forall i$ positif.*

Preuve: Soit C_v la classe cyclotomique modulo n contenant v et α une racine n-ieme primitive de 1 si $g(x)$ est un b-polynôme unitaire diviseur de $x^n - 1$ alors il existe une classe cyclotomique C_u telle que

$$\bar{g}(x) = \prod_{i \in C_u} (x - \alpha^i)$$

et par la suite

$$\bar{g}^*(x) = \prod_{i \in C_u} \alpha^i \prod_{i \in C_{n-u}} (x - \alpha^i) = u \prod_{i \in C_{n-u}} (x - \alpha^i)$$

où $u = \prod_{i \in C_u} \alpha^i$ est un élément inversible dans $\mathcal{R}$.
Donc par la proposition 31 il existe un code cyclique auto-dual de longueur n sur $\mathcal{R}$ si et seulemnet si il existe un b-polynôme $f(x)$ facteur de $x^n - 1$ tel que f et f^* ne soient pas associés, si et seulemnet si il existe une classe cyclotomique C_u qui ne soit pas reversible (ie $C_u \neq C_{n-u}$), donc si $C_1 \neq C_{-1}$ ce qui implique $q^i \ncong -1(mod\ n)\ \ \forall i$

inversement si $q^i \ncong -1(mod\ n)\ \ \forall i$ alors $C_1 \neq C_{-1}$ d'où il existe un b-polynôme associé à la classe cyclotoique C_1 et qui n'est pas associé à son polynôme réciproque.

Si $p = 2$, les entiers n, où $2^i \ncong -1(mod\ n)\ \ \forall i$ ont été etudiés par Moree [42]. Dans [21] on donne quelques exemples de non existence de codes cyclique auto-duaux. Nous allons donner une condition nécéssaire et suffisante d'existence de codes auto-duaux non triviaux, définis sur les anneaux à chaine finis.

Lemme 17. *Soit n et s deux entiers positifs et q une puissance d'un nombre premier alors*

i) *Si $q^s \equiv -1(mod\ n)$ alors $ord_n(q)$ est pair*

ii) *Si n est premier alors, $ord_n(q)$ est pair $\Longleftrightarrow \exists i\ /\ q^i \equiv -1(mod\ n)$*

Preuve:

i) $q^s \equiv -1(mod\ n) \Longrightarrow q^{2s} \equiv 1(mod\ n) \Longrightarrow ord_n(q)/2s$, si $Ord_n(q)$ est impair $\Longrightarrow ord_n(q)\ /\ s$ (contradiction avec la définition de l'ordre)

ii) Supposons que $ord_n(q) = 2w$ est pair donc $q^{2w} \equiv 1 \bmod n$.
d'où $n/(q^w - 1)(q^w + 1)$. Puisque n est premier et ne peut pas divisé $q^w - 1$ (àcause de l'ordre), nous avons $q^w = -1 \bmod n$. l'autre implication se déduit de (i).

Dans ce qui suit nous donnons une condition nécéssaire et suffisante d'existence de codes cycliques auto-duaux non triviaux sur les anneaux à chaine finis.

Théorème 45. *[6] Soit $\mathcal{R}$ un anneau à chaine fini d'idéal maximal $\langle\gamma\rangle$ d'indice de nilpotence pair e et $|\mathcal{R}| = p^{er}$ où $|\bar{\mathcal{R}}| = |\mathcal{K}| = p^r$ alors il existe un code cyclique non*

trivial de longueur impaire n puissance d'un nombre premier sur $\mathcal{R}$ si et seulement si $ord_n(p^r)$ est impair.

Preuve: Si on suppose qu'il n'existe pas de code cyclique auto-duaux sur $\mathcal{R}$ par le théorème 44 il existe un entier i tel que $(p^r)^i \equiv -1(mod\ n)$ donc par la partie i) du lemme 17 on a $ord_n(p^r)$ est pair.
Inversement supposons qu'il existe un code cyclique non-trivial auto-dual donc par le théorème 44 il n'existe pas d'entier i tel que $(p^r)^i \equiv -1(mod\ n)$ (ie $\forall i, \quad (p^r)^i \not\equiv -1)(mod\ n)$ on va montrer que dans ce cas $ord_n(p^r)$ est pair et pour cela on considère les cas suivants :

(i) Si n est premier impair alors par ii) du lemme 17 on a $ord_n(p^r)$ est impair.

(ii) $n = q^\alpha$ Supposons que $ord_q^\alpha(p^r)$ soit pair. On montre premierèment l'implication suivante.
$ord_{q^\alpha}(p^r)$ pair $\Longrightarrow ord_q(p^r)$ pair.
Supposons $ord_{q^\alpha}(p^r)$ est pair et $ord_q(p^r)$ est impair alors il existe $i > 0$ impair tel que

$$\begin{aligned} p^{ri} &\equiv 1(mod\ q) \Longleftrightarrow p^{ri} = 1 + kq \\ \text{donc} \quad p^{riq^{\alpha-1}} &= (1+kq)^{q^{\alpha-1}} \equiv 1(mod\ q^\alpha) \\ \text{car} \quad (1+kq)^{q^{\alpha-1}} &\equiv 1 + kq^\alpha (mod\ q^{\alpha+1}) \\ \text{donc} \quad p^{riq^{\alpha-1}} &\equiv 1(mod\ q^\alpha) \end{aligned}$$

Nous avons i impair et $q^{\alpha-1}$ impair d'où, $ord_{q^\alpha}(p^r)$ est impair, car $ord_{q^\alpha}(p^r)/iq^{\alpha-1}$ ce qui est absurde, donc $ord_q(p^r)$ est pair, d'où il'existe un entier j tel que $0 < j < ord_q(p^r)$ et $p^{rj} \equiv -1(mod\ q)$ d'où de (4.7) on a $p^{rjq^{\alpha-1}} \equiv -1(mod\ q^\alpha)$ ce qui donne que la classe cyclotomique C_1 est reversible et par le théorème 44 ceçi est impossible.

Remarque 25. *On note que l' $ord_n(p^r)$ impair est une condition suffisante pour tout n d'existence de codes auto-duaux non triviaux sur Rr.*

On donne quelques exemples de codes auto-duaux non triviaux .

Exemple 33. – *Longueur 22 sur* $\mathbb{Z}_{25}$.

Nous avons $ord_{22}(5) = 5$ *est impair. La factorisation de* $x^{22}-1$ *sur* $\mathbb{Z}_{25}$ *en produit de b-polynomes sur* $\mathbb{Z}_{25}$ *est donnée par*

$$\begin{aligned} x^{22}-1 &= (x-1)(x+24)(x^5+16x^4+24x^3+24x^2+8x+1) \\ &\quad (x^5+17x^4+24x^3+x^2+16x+1)(x^5+8x^4+24x^3+24x^2+16x+1) \\ &\quad (x^5+9x^4+24x^3+x^2+16x+1) \\ &= f_1(x)f_2(x)f_3(x)f_4(x)f_5(x)f_6(x), \end{aligned}$$

et on a $f_3^\star = f_5$, *d'où* f_3 *n'est pas associé avec son réciproque. Soit* $g = f_1f_2f_4f_6$. *Alors nous avons le code cyclique auto-dual suivant :*

$$C = (f_3^\star g, 5f_3f_3^\star).$$

– *Longueur* 13 *sur* $\mathbb{Z}_9$.

Dans ce cas $ord_{13}(3) = 3$, *alors il existe un code cyclique auto-dual de longueur 13 sur* $\mathbb{Z}_9$. *La factorisation de* $x^{13}-1$ *en produit de b-polynômes sur* $\mathbb{Z}_9$ *est donnée par*

$$x^{13}-1 = (x-1)(x^3+6x^2+2x+8)(x^3+7x^2+3x+8)(x^3+4x^2+7x+8)(x^3+2x^2+7x+8).$$

Pour $f(x) = x^3+6x^2+2x+8$ *nous avons* $f^\star(x) = -(x^3+7x^2+3x+8)$ *et* $x^{13}-1 = f(x)f^\star(x)g(x)$ *avec* $g(x) = -(x-1)(x^3+4x^2+7x+8)(x^3+2x^2+7x+8)$. *Alors nous avons le code cyclique auto-dual suivant :*

$$C = (f^\star g, 3ff^\star).$$

– *Longueur 11 sur* $\mathbb{Z}_{25}$.

Nous avons $ord_{11}(5) = 5$ *est impair. La factorisation de* $x^{11}-1$ *sur* $\mathbb{Z}_{25}$ *en produit de b-polynômes sur* $\mathbb{Z}_{25}$ *est donnée par*

$$x^{11}-1 = (x-1)(x^5+17x^4+24x^3+x^2+16x+24)(x^5+9x^4+24x^3+x^2+8x+24),$$

qui est égale à $g(x)f(x)f^\star(x)$ *with* $g(x) = -(x-1)$. *Alors nous avons le code cyclique auto-dual suivant :*

$$C = (f^\star g, 5ff^\star).$$

– *Longueur 6 sur* $\mathbb{Z}_{49}$.

Nous avons $ord_6(7) = 1$ *est impair .La factorisation de* $x^6 - 1$ *sur* $\mathbb{Z}_{49}$ *en produit de b-polynômes sur* $\mathbb{Z}_{49}$ *est donnée par*

$$x^6 - 1 = (x-1)(x+1)(x+18)(x-18)(x+19)(x-19).$$

Pour $f(x) = x - 18$, $f^\star(x) = -18(x+19)$, *d'où* $x^6 - 1 = g(x)f(x)f^\star(x)$ *avec* $g(x) = 19(x-1)(x+1)(x+18)(x-19)$. *Alors nous avons le code cyclique auto-dual suivant :*

$$C = (f^\star g, 7ff^\star).$$

Corollaire 7. *[7] Soit* $\mathcal{R}$ *un anneau à chaine fini d'idéal maximal* $\langle\gamma\rangle$ *d'indice de nilpotence pair e et* $|\mathbb{R}| = p^{er}$ *où* $|\bar{\mathbb{R}}| = |\mathcal{K}| = p^r$ *.Soit* $n = km$ *produit de deux entiers positifs où* m *est une puissance d'un nombre premier ipmair.*
Si $ord_m(p^r)$ *est impair alors il existe un code cyclique auto-dual sur* $\mathcal{R}$ *de longueur* n

Preuve: Si $ord_m(p^r)$ est impair alors d'aprés le théorème 45.

$$\begin{aligned} \forall i, \quad & p^{ri} \ncong -1 (mod\ m) \\ \text{d'où} \quad \forall i, \quad & p^{ri} \ncong -1 (mod\ km) \\ \text{sinon} \quad \exists i \quad & p^{ri} \equiv -1 (mod\ km) \\ \text{ce qui implique} \quad & p^{ri} \equiv -1 (mod\ m) \end{aligned}$$

d'où $ord_m(p^r)$ est pair. □

Exemple 34. $n = 22, \quad \mathbb{R} = \mathbb{Z}_{25}$, $ord_{11}(5^2) = ord_{11}(5) = 5$ *est impair alors il existe un code cyclique auto-dual de longueur* 22 *sur* $\mathbb{Z}_{25}$.

Pour la suite la notation $q \equiv \square mod\ n$ siqnifit que q est un residue quadratique modulo n.

Corollaire 8. *[6] Soit $\mathcal{R}$ un anneau à chaine fini d'idéal maximal $\langle\gamma\rangle$ d'indice de nilpotence pair e et de corps résiduel K tel que $|\mathcal{K}| = p^r$, alors si $p_1p_2\dots p_s$ est la décomposition de n en facteurs premiers impairs tels que $p^r \equiv \square mod\ p_i$*
et $p_i \equiv -1 mod\ 4 \quad \forall i,\ 1 \leq i \leq s$ alors il existe un code cyclique auto-dual non trivial de longueur n sur $\mathcal{R}$ si seulement si $ord_n(p^r)$ est impair.

Preuve: On a $ord_n(p^r) = ppcm(ordp_i(p^r))$ puisque $p^r \equiv \square mod\ p_i$ alors $ord_{p_i}(p^r)$ divise $\frac{p_i - 1}{2}$. donc $ord_{p_i}(p^r)$ est impair sinon $p_i \equiv 1 mod\ 4$ d'où $ord_n(p^r)$ est impair, et par le théorème 45 nous avons l'existence d'un code cyclique auto-dual non trivial sur $\mathcal{R}$. □

Corollaire 9. *[6] avec les notations déjà utilisées.*
Si n est premier impair tel que $n \equiv -1 mod\ 4$ alors il existe un code cyclique auto-dual non trivial si seulement si

$$p \equiv \square mod\ n$$

Preuve: la conditions necéssaire est donnée par ([21] Corollaire 8) pour la réciproque. Si on suppose $p \equiv \square mod\ n$ alors $p^r \equiv \square mod\ n$ et on a le resultat par le corolaire 9 □

Exemple 35. *On a $11 \equiv -1$ [4] et $3 \equiv \square mod\ 11$ alors il existe un code cyclique auto-dual non trivial de longueur 11 sur $\mathbb{Z}_9$. dans ce cas on a aussi $ord_{11}(3) = 5$ impair.*
La factorisation de $x^{11} - 1$ en produit de b-polynomes sur $\mathbb{Z}_9$ est donnée par

$$x^{11} - 1 = (x-1)(x^5 + 3x^4 + 8x^3 + x^2 + 2x - 1)(x^5 - 2x^4 - x^3 + x^2 - 3x - 1) = (x-1)f_1f_1^\star$$

on obtient le code cyclique auto-dual non trivial de longueur 11 sur $\mathbb{Z}_9$ suivant :

$$C = \langle (x-1)f_1, 3f_1f_1^\star \rangle$$

Nous avons vu que les codes cycliques définis sur les anneaux finis étaient des sous modules donc qui n'ont pas obligatoirement de bases. nous allons voir par la suite sous quelles conditions, ces sous modules admettent-ils une base.

4.10 Les codes cycliques libres définis sur les anneaux à chaine finis

Théorème 46. *([32, Theorem 4.20]) Soit C un code cyclique de longueur n sur un anneau à chaine fini $\mathcal{R}$ de caractéristique p,tel que $(p, n) = 1$. Alors C est un code libre de rang k si et seulement si il existe un polynôme $f(x) \in \mathcal{R}[x]$ tel que $f(x)/(x^n - 1)$ qui engendre C et dans ce cas on a $k = n - deg(f)$.*

Théorème 47. *[6] Soit $\mathcal{R}$ un anneau à chaine fini d'idéal maximal $\langle\gamma\rangle$, d'indice de nilpotence e, de caractéristique p tel que $(n, p) = 1$, alors si p est impair il n'existe pas de code cyclique auto-dual libre de longueur n défini sur $\mathcal{R}$.*

Preuve: Soit C un code cyclique libre auto-dual sur $\mathcal{R}$ de longueur n. D'aprés le théorème 46, C est engendre par un diviseur $g(x)$ facteur de $x^n - 1$ dans $\mathcal{R}[x]$.
Puisque C est auto-dual on a $g(x) = g^{\perp}(x)$ avec $g^{\perp}(x) = \hat{g}^*(x)$ et la reduction modulo γ est un homorphisme d'anneau on obtient

$$\overline{g^*}\,\overline{g} = \overline{x^n - 1}$$

Et puisque $(n, p) = 1$, par le théorème 34, $\bar{\hat{g}}(x)$ est un diviseur de $\overline{x^n - 1}$ dans $\mathcal{K}[x]$, de plus par le lemme 16, on a $\overline{g^*} = \overline{g}^*$. Donc C est un code cyclique auto-dual sur $\mathcal{K}$ ([35]) nous montre qu'il n'existe pas de code cyclique auto-dual sur un corps fini $\mathcal{K}$ de caractéristique impair. D'où le résultat. □

Il existe une une autre manière de définir les codes cycliques sur les anneaux finis qui est utilisée pour les anneaux de Galois (voir appendice pour la définition d'un anneau de Galois).

4.11 Codes cycliques définis par les racines de l 'unité

Les éléments inversibles de $\mathcal{R} = GR(q,l)$ forment un groupe multiplicatif qui est un produit direct $\langle\xi\rangle \times G$ où$\langle\xi\rangle$ est un groupe cyclique d'ordre $p^l - 1$ engendré par un élément primitif ξ de $\mathcal{R}$;et $G = \{1 + \pi\,; \pi \in \langle p\rangle\}$ est un groupe d'ordre $p^{(r-1)l}$.
Soit n un entier positif tel que $n \,/\, p^m - 1$ alors l'anneau de Galois $GR(q,m)$ contient toutes les racines de $x^n - 1$.
Maintenant soit m le plus petit entier positif tel que l/m et $n/p^m - 1$ alors $GR(q,m)$ est la plus petite extension de $\mathcal{R}$ qui contient une n-ième racine primitive de l'unité ξ.Si ζ est un élément primitif de $GR(q,m)$ alors $\xi = \zeta^{(p^m-1)/n}$ est une racine n-ième primitive de l'unité dans $GR(q,m)$.
Une racine n-ième de l'unité dans $GR(q,m)$ peut aussi etre obtenue comme suit :
Soit β une racine n-ième de l' unité dans le corps résiduel F_{p^m} de $GR(q,m)$,puisque $(p,n) = 1$ β est une racine simple de $x^n - 1$ dans F_{p^m}. alors par [41] il existe un unique élément $\xi \in GR(q,m)$ tel que $\bar{\xi} = \beta$ et ξ est une racine de $x^n - 1$ dans $GR(q,m)$. On a aussi par [41] ordre de (ξ) = ordre de ($\bar{\xi}$ et donc ξ est une racine n-ième primitive de l'unité dans $GR(q,m)$. Un code cyclique C de longueur n sur $\mathcal{R}$ peut aussi etre défini par les racines n-ième de l'unités
Soient $\xi^{i_1}, \xi^{i_2}, \ldots, \xi^{i_k}$ des racines n-ième de l' unité dans $GR(q,m)$ alors le code cyclique correspondant C est défini par

$$\{c(x) \in \mathcal{R}[x]/(x^n - 1) \;/\, c(\xi^{i_j}) = 0\,;\; 1 \leq j \leq k\}$$

Le polynôme générateur $g(x)$ de C est le plus petit multiple commun des polynomes minimaux de ξ^{i_j} , $1 \leq j \leq k$ evidement $g(x) \,/\, x^n - 1$. Donc un tel code cyclique est libre sur $\mathcal{R}$.

Proposition 33. *On Suppose que le polynôme générateur $g(x)$ d'un code cyclique C de longueur n sur $\mathcal{R} = GR(q,m)$ divisant $x^n - 1$ a ses racines $\xi^b, \xi^{b+1}, \ldots, \xi^{b+\delta-2}$ où ξ est une n-ième racine de l'unité dans une extension approprié de $\mathcal{R}$ alors*

$$d(C) \geq \delta$$

où $d(C)$ est la distance minimale de Hamming de C. La preuve est la même que celle pour les codes sur les corps , on considere que $\bar{C}$ est un code sur F_{p^m}.

Exemple 36. *Le polynôme* $h(x) = x^3 + x^2 + 1$ *est un facteur irréductible de* $x^n - 1$ *sur* F_2 *qui est aussi un polynôme primitif sur* F_2. *le relevé de Hensel de* $h(x)$ *à* $\mathbb{Z}_4$ *est* $f(x) = x^3 - x^2 + 2x - 1$

Soit ξ *une racine de* $f(x)$ *,alors* ξ *est un élément primitif de* $GR(4,3)$ *ie un élément d''ordre* $2^3 - 1 = 7$ *dans* $GR(4,3)$. *Soit le polynôme générateur sur* $\mathbb{Z}_4$ *défini par* $g(x) = lcm(M_0(x), M_1(x), M_2(x))$ *où*$(M_0(x), M_1(x)$ *et* $M_2(x))$ *sont respectivement les polynomes minimaux de* 1 *,*ξ *et* ξ^2 *.Maintenant* $M_0(x) = x - 1$ *et* $M_1(x) = M_2(x) = f(x)$. *donc* $g(x) = x^4 + 2x^3 - x^2 + x + 1$ *;* $g(x) \,/\, x^7 - 1$ *sur* $\mathbb{Z}_4$. *par suite* C *est un code cyclique libre de longueur* 7 *sur* $\mathbb{Z}_4$ *de rang* 3 *et de distance minimale* $4 \leq d$ *au moins* 4.

Une matrice génératrice de C *est*

$$G = \begin{pmatrix} 1 & 1 & 3 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 3 & 2 & 1 & 0 \\ 0 & 0 & 1 & 1 & 3 & 2 & 1 \end{pmatrix}$$

La première ligne de G *est un vecteur de poids* 4. *Donc* C *a une distance minimale égale exactement à* 4.

4.12 Nombre de codes cycliques et cycliques auto-duaux définis sur un anneau àchaine fini

On calcul le nombre de codes cycliques et celui des codes auto-duaux définis sur les anneaux à chaine finis .

Le théoreme suivant donne le nombre de codes cycliques et cycliques libres définis sur les anneaux à chaine finis.

Théorème 48. *[6] Soit* $\mathcal{R}$ *un anneau à chaine fini, d'indice de nilpotence e et de corps*

résiduel F_q, avec $q = p^r$ éléments. Soit $C_q(n)$ le nombre de q-classes cyclotomiques modulo n avec $(n, q) = 1$. alors on a :

(i) le nombre de codes cycliques définis sur $\mathcal{R}$ est égale à $(e+1)^{C_q(n)}$,

(ii) le nombre de codes cycliques libres définis sur $\mathcal{R}$ est egale à $2^{C_q(n)}$.

On note que le Théoreme 48 est aussi vrai pour les codes cycliques définis sur les corps finis, puisque les corps finis sont aussi des anneaux à chaine finis d'indice de nilpotence $e = 1$ Le résultat suivant donne $C_q(n)$ dans le théorème 48.

Proposition 34. *[52] Soit $C_q(n)$ le nombre des q-classes cyclotomiques modulo n avec $(n, q) = 1$. alors on a :*

$$C_q(n) = \sum_{l|n} \frac{\Phi(l)}{ord_l(q)},$$

où $\Phi(.)$ est la fonction d'Euler.

Théorème 49. *([21, Theorem 3.2]) Soit $\mathcal{R}$ un anneau à chaine fini d'idéal maximal $\langle\gamma\rangle$ et l'indice de nilpotence de γ est e . Soit $x^n - 1 = f_1 f_2 \dots f_k$ la factorisation de $x^n - 1$ en produit de b-polynômes premiers entre eux deux à deux dans $\mathcal{R}[x]$. Alors tout idéal dans $\frac{\mathcal{R}[x]}{\langle x^n-1\rangle}$ est de la forme $\bigoplus \sum_{i=1}^{k} I_i$, où $I_i = 0$, or $I_i = \langle \gamma^j \hat{f}_i + \langle x^n - 1\rangle\rangle$, où $0 \le j \le e, 1 \le i \le k$.*

Concidérons maintenant le polynôme $x^n - 1$ sur l'anneau à chaine fini $\mathcal{R}$.

Du Theorem 40, ce polynôme se décompose en forme unique en produit de b-polynômes unitaires f_i tels que $1 \le i \le k$. on a aussi $k = C_q(n)$. Notons les facteurs f_i dans la factorisation de $x^n - 1$ qui sont associés à leurs réciproques par $g_1, \dots g_s$, et le reste f_j groupés en paires $h_1, h_1^*, \dots, h_t, h_t^*$. donc $k = s + 2t$, et

$$x^n - 1 = g_1 \dots g_s h_1 h_1^\star \dots h_t h_t^\star. \tag{4.7}$$

En utilisant la décomposition de $x^n - 1$ donnée dans (4.7) et le Théorème 49,on obtient que tout idéal de $\frac{\mathcal{R}[x]}{\langle x^n-1\rangle}$ est de la forme $\sum_{i=1}^{k} I_i$, où $I_i = 0$ ou $I_i = \sum_{r=1}^{s} I_r \bigoplus \sum_{j=1}^{t} (I_j + I_j^\star)$ avec $I_i = \langle \gamma^l \hat{g}_i + \langle x^n - 1\rangle\rangle, 1 \le i \le s$ and I_j (respectivement $I_j^\star$), $1 \le j \le t$, est donnée par $I_j = \langle \gamma^l \hat{h_j} + \langle x^n - 1\rangle\rangle$, (respectivement $I_j^* = \gamma^l \hat{h_j^*} + \langle x^n - 1\rangle$), et $0 \le l \le e$.

Corollaire 10. *[6] Soit $\mathcal{R}$ un anneau à chaine fini d'idéal maximal $\langle\gamma\rangle$ et l'indice de nilpotence de γ est e . Alors le nombre de codes cycliques auto-duaux définis sur $\mathcal{R}$ de longueur n et $(1+e)^t$, où t est le nombre de paires de facteurs dans l'unique factorisation de x^n-1 en produit de b-polynômes unitaires premiers entre eux deux à deux qui ne sont pas associés à leurs polynômes réciproques .*

On note le nombre t donné dans le Corollaire 10 par $t(n,r)$ puisque il dépend de n et r. Il a été mensioné dans Jia et al. [35, p. 2247] que dans le cas général il est difficile de trouver une expression simple de $t(n,r)$. Ce nombre est bien sur égale à $\dfrac{C_n(q)-s}{2}$, meme l'expression de $C_n(q)$ donnée dans la Proposition 34 est difficile à calculer par Skersy [52]. Jia et al. donnent $t(n,r)$ dans le cas où caracteristique est 2. Pour le reste on utilise, le resultats de Jia et al. [35] pour généraliser cette expression pour d'autres anneaux et d'autres caractéristiques.

On rappelle que l'on considère un anneau à chaine fini $\mathcal{R}$ avec comme corps résiduel $\mathbb{F}_q$, où $q=p^r$ est une puissance d'un nombre premier.

Définition 59. *Soit l et r deux nombres positifs avec l impair. la paire (l,r) est appelée efficace si il existe un nombre positif j tel que l divise $(p^r)^j+1$, et non efficace sinon.On définit la fonction suivante sur (l,r)*

$$\chi(l,r)=\begin{cases} 0 & \textit{si } (l,r) \textit{ est efficace,}\\ 1 & \textit{sinon.}\end{cases}$$

Lemme 18. *[35] Si la paire (l,r) est une paire efficace alors tous les fateurs irreductibles du polynôme cyclotomique $Q_l(x)$ sont associés à leurs réciproques , sinon aucun d'eux l'est.*

Si une paire (l,r) est efficace ,Du Lemme 18 tous les facteurs de $Q_l(x)$ sont associés à leurs réciproques, donc aucun facteurs intervient dans $t(n,r)$. Sinon, tous les facteurs $Q_l(x)$ intervient dans $t(n,r)$, puisque le nombre des paires des facteurs de $Q_l(x)$ de la Proposition 34 est egale à $\dfrac{\Phi(l)}{2ord_l(p^r)}$.
Alors nous avons le théorème suivant.

Théorème 50. *Soit $\mathcal{R}$ un anneau à chaine fini avec comme corps résiduel $\mathbb{F}_q$ où $q = p^r$ et comme indice de nilpotence e. Alors le nombre de codes auto-duaux sur $\mathcal{R}$ de longueur n avec $(n, p) = 1$ est egale à $(e+1)^{t(n,r)}$, où $t(n, r)$ est le nombre de facteurs irreductibles diviseurs de $x^n - 1$ donné dans (4.7). De plus, on a*

$$t(n, r) = \frac{1}{2} \sum_{l|n} \chi(l, r) \frac{\Phi(l)}{ord_l(p^r)}.$$

Remarque 26. *Le Théorème 50 est une généralisation du [35, Théorème 3] aux anneaux à chaine finis.*

Maintenant du Théorème 50 et [35, Le théorème 5], on obtient une version similaire de [35, Corollaire 2] pour les anneaux à chaine finis.

Théorème 51. *[6] Soit $\mathcal{R}$ un anneau àchaine fini avec comme corps résiduel F_{2^m}, et n un entier impair dont aucun de ses facteurs est congru à 1 modulo 8.*

1. *Si m est impair , il existe un unique code cyclique auto dual si et seulement si tous les diviseurs premiers de n sont congruent à 3 modulo 8, ou tous les diviseurs premiers de n sont congruent à 5 modulo 8.*
2. *Si $m \equiv 2 \pmod 4$, il existe un unique code cyclique auto dual si et seulement si tous les diviseurs premiers de n sont congruent à to 5 modulo 8.*
3. *Si $m \equiv 0 \pmod 4$, il existe au moins deux codes cycliques auto duaux.*

En utilisant les résultats précédants , on donne dans la Table suivante le nombre de codes cycliques et cycliques auto duaux sur $\mathbb{Z}_4$. $N = (e+1)^{C_n(q)}$ est le nombre de codes cycliques , et $N_t = (e+1)^t$ est le nombre de codes cycliques auto-duaux sur $\mathbb{Z}_4$. Dans e cas , $e = 2$ and $p = 2$.

TABLE 4.2 – Le nombre de codes cycliques et cycliques auto-duaux sur $\mathbb{Z}_4$ pour $n < 100$.

n	t	N	N_t	n	t	N	N_t
1	0	1	1	51	2	3^8	9
3	0	9	1	53	0	9	1
5	0	9	1	55	1	3^5	3
7	1	27	3	57	0	3^5	1
9	0	27	1	59	0	9	1
11	0	9	1	61	0	9	1
13	0	9	1	63	5	3^{13}	3^5
15	1	81	3	65	0	3^7	1
17	0	27	1	67	0	9	1
19	0	9	1	69	2	3^8	9
21	2	3^6	9	71	1	27	3
23	1	27	3	73	4	3^9	81
25	0	27	1	75	2	3^8	9
27	0	81	1	77	2	3^6	9
29	0	9	1	79	1	27	3
31	3	3^7	27	81	0	3^5	1
33	0	3^5	1	83	0	9	1
35	2	3^6	9	85	4	3^{12}	3^4
37	0	9	1	87	1	3^{11}	1
39	1	3^5	3	89	4	3^9	81
41	0	27	1	91	4	3^{10}	3^4
43	0	81	1	93	6	3^{14}	3^6
45	2	3^7	9	95	1	3^5	3
47	1	27	3	97	0	27	1
49	2	3^5	9	99	0	3^7	1

4.13 Codes cycliques définis sur un anneau à chaine fini d'indice de nilpotence impair

Dans ce qui suit on montre qu'il n'existe pas de code cyclique simple auto-dual défini sur un anneau à chaine fini dont l'indice de nilpotence de son idéal maximal est un entier impair.

Théorème 52. *[8] Soit $\mathcal{R}$ un anneau à chaine fini où $\langle\gamma\rangle$ est son idéal maximal d'indice de nilpotence e.Si e est impair et q une puissance d'un nombre premier alors il n'existe pas de code cyclique non-trivial auto-dual de longueur n sur $\mathcal{R}$,tel que $(n,q)=1$.*

Preuve: Soit C un code cyclique non trivial de longueur n sur $\mathcal{R}$ alors ils existent des polynomes unitaires premiers entre eux deux à deux, $F_0, F_1, \ldots, F_{e-1}, F_e$ tels que

$$x^n - 1 = F_0 F_1 \ldots F_{e-1} F_e$$

et $C = \langle \hat{F}_1, \gamma\hat{F}_2, \ldots, \gamma^{e-1}\hat{F}_e\rangle$. Si C est auto-dual,donc de [21, Proposition 4.1] F_i est associé avec $F_j^\star$ pour $i,j \in \{0,1,\ldots e\}$ et $i+j \equiv 1 \pmod{e+1}$. Alors $F_i = \epsilon F_j^\star$ pour tous les $i,j \in \{0,\ldots e\}$ $i+j \equiv 1 \pmod{e+1}$, ϵ est un élément inversible dans $\mathcal{R}$. D'où $F_i \neq F_j^\star$ puisque e est impair et il ne peut pas vérifier $i+i \equiv e+2$, ce qui implique

$$x^n - 1 = F_0 F_0^\star F_2 F_2^\star F_3 F_3^\star \ldots F_{\frac{e+1}{2}} F_{\frac{e+1}{2}}^\star.$$

Donc aucun F_i n'est associé à son réciproque, or le polynôme $(x-1)$ est un facteur de x^n-1, donc il existe un $0 \leq i_0 \leq e$ tel que $F_{i_0} = (x-1)g(x)$ pour un certain $g(x)$. D'où

$$F_{i_0}^\star = (x-1)^\star g(x)^\star = (x-1)g(x)^\star = F_{1-i_0 \pmod{1+e}},$$

Ce qui est impossible puisque pour tout $0 \leq i \leq e$ les F_i sont premiers entre eux, et x^n-1 n'a pas de racines multiples puisque $(n,q)=1$.

Exemple 37. *Il n'existe pas de code cyclique auto-dual non trivial de longueur premiere avec 3 sur $\mathbb{Z}_{27}$.*

Dans ce qui suit on généralise le théorème 52 aux anneaux principaux finis.

4.14 Codes cycliques auto-duaux définis sur les anneaux principaux

Lemme 19 ([10], p. 54, Proposition 6)**.** *Soit $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ des idéaux de $\mathcal{R}$,premiers entre eux deux à deux et soit $\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{a}_i$. Pour tout $\mathcal{R}$-module M, l'homomorphisme canonique $M \to \prod_{i=1}^{n} (M/\mathfrak{a}_i M)$ est surjectif et son noyau est $\mathfrak{a}M$.*

Soit $\mathfrak{a}_i$ un idéal d'un anneau $\mathcal{R}$, et notons $\mathcal{R}_i = \mathcal{R}/\mathfrak{a}_i$. Donc nous avons epimophisme canonique

$$\psi_i : \mathcal{R} \to \mathcal{R}_i$$

.

Proposition 35. *[19] soit $\mathcal{R}$ un anneau commutatif fini . Alors les propositions suivantes sont equivalentes.*

(i) $\mathcal{R}$ est un anneau principal .

(ii) $\mathcal{R}$ est isomorphe à un produit fini d'anneaux à chaine finis.

De plus , la décomposition dans (ii)est unique . Elle est de la forme $\mathcal{R} \cong \prod_{i=1}^{k} R/\mathfrak{m}_i^{t_i}$, où $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_k$ sont des idéaux maximaux de $\mathcal{R}$, et $t_1, t_2, \ldots, t_k$ sont les indices de stabilité respectives .

Remarque 27. *Soit $\mathcal{R}_i = \mathcal{R}/\mathfrak{m}_i^{t_i}$ alors $\mathcal{R}_i$ est un anneau à chaine fini d'idéal maximal $\mathfrak{m}_i/\mathfrak{m}_i^{t_i}$*

Si $\mathcal{R}$ est un anneau principal fini ,on dit que la décomposition de $\mathcal{R}$ en produit d'anneaux à chaine finis, donnée en (ii), est un *décomposition canonique de $\mathcal{R}$*. Les idéaux $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_k$ dans ce cas sont appelés *décomposition directe de $\mathcal{R}$*. Soit $\mathcal{R}$ un anneau fini et $(\mathfrak{m}_i)_{i=1}^{n}$ une décomposition directe de $\mathcal{R}$. Soit

$$\Psi : \mathcal{R}^n \to \prod_{i=1}^{k} \mathcal{R}_i^n$$

l'isomorphisme canonique de $\mathcal{R}$-modules . Pour $i = 1, \ldots, k$ soit C_i un code sur $\mathcal{R}_i$ de longueur n et soit

$$C = CRT(C_1, C_2, \ldots, C_k) = \Psi^{-1}(C_1 \times \cdots \times C_k) = \{\Psi^{-1}(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k) \mid \mathbf{v}_i \in C_i\}.$$

On note C comme *Produit Chinois des Codes* $C_1, C_2, \ldots, C_k$ [25].

Théorème 53. *[8] Avec les notations ci-dessus , soient $C_1, C_2, \ldots, C_k$ des codes de longueur n, avec C_i un code défini sur $\mathcal{R}_i$, et soit $C = CRT(C_1, C_2, \ldots, C_k)$. alors nous avons*

(i) C est un code cyclique si et seulement si chaque C_i est cyclique ;

(ii) $C_1, C_2, \ldots, C_k$ sont auto-duaux si et seulement si C est un code auto-dual .

Preuve:

i) Puisque $\mathcal{R}_i$ est un anneaux à chaine fini ,soit $\mathbb{F}_{q_i}$ son corps résiduel et n un entier positif tel que $(n, q_i) = 1 \, \forall i \in \{1, 2, \ldots, k\}$. En plus, soit

$$\phi_i : \mathcal{R}[x]/(x^n - 1) \longrightarrow \mathcal{R}_i[x]/(x^n - 1),$$

et on définit :

$$\phi_i(a_0 + a_1 x + \cdots a_{n-1}x^{n-1}) = \psi_i(a_0) + \psi_i(a_1)x + \cdots + \psi_i(a_{n-1})x^{n-1}.$$

on définit en plus :

$$\phi : R[x]/(x^n - 1) \longrightarrow R_1[x]/(x^n - 1) \times R_2[x]/(x^n - 1) \times \cdots \times R_k[x]/(x^n - 1)$$

Où

$$\phi(f(x)) = (\phi_i(f(x)), \phi_2(f(x)), \cdots, \phi_k(f(x))).$$

Si I est un idéal de $\mathcal{R}[x]/(x^n - 1)$,alors $\phi_i(I)$ est un idéal de $\mathcal{R}_i[x]/(x^n - 1)$. inversement pour tout idéal I_i dans $R_i[x]/(x^n - 1)$ on définit

$$\phi^{-1}(I_1, I_2, \ldots, I_k).$$

On note que

$$I = CRT(I_1, I_2, \ldots, I_k)$$

est l'unique idéal dans $\mathcal{R}[x]/(x^n - 1)$ qui est congru à I_i dans $\mathcal{R}_i$. Par la généralisation du théorème des restes chinois cette application est bien définie, Ce qui imlique que

$$I = CRT(I_1, I_2, \ldots, I_k)$$

est un idéal de $\mathcal{R}[x]/(x^n - 1)$. En Associant a un code cyclique son idéal correspondant on obtient que :

$$CRT(C_1, C_2, \ldots, C_k)$$

un code cyclique sur $\mathcal{R}$ si et seulement si C_i est cyclique sur $\mathcal{R}_i$.

ii) Premiérement notons que

$$CRT(C_1, C_2, \ldots, C_k)^{\perp} = CRT(C_1^{\perp}, C_2^{\perp}, \ldots, C_k^{\perp}).$$

Alors si $C = CRT(C_1, C_2, \ldots, C_k)$ nous avons

$$C^{\perp} = CRT(C_1^{\perp}, C_2^{\perp}, \ldots, C_k^{\perp}) = CRT(C_1, C_2, \ldots, C_k) = C,$$

et le code C est auto-dual.

□

De ce qui précede on déduit :

Théorème 54. *[7] Soit $\mathcal{R} \cong \prod_{i=1}^{k} \mathcal{R}/\mathfrak{m}_i^{t_i}$,un anneau principal fini, et C un code cyclique défini sur $\mathcal{R}$. Alors si un des t_i est impair , C n'est pas un code auto-dual.*

On généralise maintenant la définition des codes duadiques définis sur les corps aux anneaux à chaine finis pour construire des codes auto-duaux non triviaux définis sur ces anneaux.

4.15 Codes duadiques définis sur les anneaux à chaine finis

Soit $\mathcal{R}$ un anneau à chaine fini où $\langle\gamma\rangle$ est l'idéal maximal d'indice de nilpotence e. On sait que $\mathcal{R}/\langle\gamma\rangle \simeq \mathbb{F}_q$ et $q = p^r$. Soit n un entier impair tel que $(p, n) = 1$ et $q \equiv \square mod(n)$ alors il existe une paire de codes duadiques odd-like sur $\mathbb{F}_q$, $\langle f_1(x)\rangle$ et $\langle f_2(x)\rangle$ où

$$x^n - 1 = (x - 1)f_1(x)f_2(x)$$

sur F_q . puisque $x - 1$, $f_1(x)$ et $f_2(x)$ sont des facteurs unitares irréductibles premiers entre eux deux à deux de x^n-1 sur $\mathbb{F}_q$. Par le lemme de Hensel il existe des b-polynomes $g_1(x), g_2(x)$ unitaires premiers entre eux tels que, $x - a$, $g_1(x)$, $g_2(x)$ sont des facteurs de $x^n - 1$ dans $\mathcal{R}[x]$
tels que $x - \bar{a} = x - 1$, $\bar{g_1}(x) = f_1(x)$ et $\bar{g_2}(x) = f_2(x)$
$x^n - 1 = (x - a)g_1(x)g_2(x)$ dans $\mathcal{R}[x]$. En remplaçant $x = 1$ dans l'équation çi dessus on obtient

$$(1 - a)g_1(1)g_2(1) = 0$$

puisque $\bar{g_1}(1) = f_1(1) \neq 0$ et $\bar{g_2}(1) = f_2(1) \neq 0$ alors $g_1(1), g_2(1)$ sont tous les deux inversibles dans $\mathcal{R}$ donc $a = 1$ et on obtient
$x^n - 1 = (x - 1)g_1(x)g_2(x)$ dans $\mathcal{R}[x]$. On peut définir maintenant

- Des codes duadiques odd-like libres sur $\mathcal{R}$ par $D_1 = \langle g_1(x)\rangle$, $D_2 = \langle g_2(x)\rangle$
- Des codes duadiques even-like libres sur $\mathcal{R}$ par $C_1 = \langle(x - 1)g_1(x)\rangle$, $C_2 = \langle(x - 1)g_2(x)\rangle$

Et si e est pair, on définit des codes duadiques non libres sur $\mathcal{R}$ par :

$$E_1 = \langle(x - 1)g_1(x), \gamma^{\frac{e}{2}}g_1(x)g_2(x)\rangle \tag{4.8}$$

$$E_2 = \langle(x - 1)g_2(x), \gamma^{\frac{e}{2}}g_1(x)g_2(x)\rangle \tag{4.9}$$

En utilisant la définition ci-dessus on construit des codes cycliques auto-duaux définis sur les anneaux à chaine finis comme suit :

4.16 Construction de codes auto-duaux définis sur les anneaux à chaine finis

Théorème 55. *[7] Soient E_1 et E_2 définis comme ci-dessus si le splitting est donné par μ_{-1} alors E_1 et E_2 sont auto-duaux ,sinon E_1 et E_2 sont duaux l'un de l'autre.*

Preuve: Soit$\mathcal{R}$ un anneau à chaine fini où $\langle\gamma\rangle$ est son idéal maximal d' indice de nilpotence e un entier pair, tel que $\mathcal{R}/\langle\gamma\rangle \simeq \mathbb{F}_q$ et $q = p^r$. Soit n un entier impair tel que $(p, n) = 1$ et $q \equiv \square mod(n)$ alors il existe une paire de codes duadiques odd-like sur $\mathbb{F}_q$, $\langle f_1(x)\rangle$ and $\langle f_2(x)\rangle$ où

$$x^n - 1 = (x - 1)f_1(x)f_2(x)$$

sur $\mathbb{F}_q$.

i) Si le splitting est donné par μ_{-1} alors $f_1^\star(x) = \pm f_2(x)$ et $f_2^\star(x) = \pm f_1(x)$ alors par [6] leurs relevés de Hensel ont les mêmes propriétés, donc on obtient, $g_1^\star(x) = \alpha g_2(x)$ et $g_2^\star(x) = \beta g_1(x)$ avec α et β des éléments inversibles dans $\mathcal{R}$ tels que $\bar{\alpha} = \pm$ et $\bar{\alpha} = \pm$ Donc soit

$$E_1 = \langle (x - 1)g_1(x), \gamma^{\frac{e}{2}} g_1(x)g_2(x)\rangle$$

alors par [21] nous avons

$$E_1^\perp = \langle (x - 1)^\star g_2^\star(x), \gamma^{\frac{e}{2}} g_1^\star(x)g_2^\star(x)\rangle$$

=

$$\langle (x - 1)g_1(x), \gamma^{\frac{e}{2}} g_1(x)g_2(x)\rangle$$

D'où E_1 est un code auto-dual et avec la même preuve on obtient que E_2 est aussi un code auto dual sur $\mathcal{R}$

ii) Si le splitting n'est pas donné par μ_{-1} donc $f_1^\star(x) = \pm f_1(x)$ and $f_2^\star(x) = \pm f_2(x)$ alors par [6] leurs relevés de Hensel ont les mêmes propriétés donc on obtient,

$g_1^\star(x) = \alpha g_1(x)$ and $g_2^\star(x) = \beta g_2(x)$ avec α et β des éléments inversibles dans $\mathcal{R}$ tels que $\bar{\alpha} = \pm$ et $\bar{\alpha} = \pm$ D'où soit

$$E_1 = \langle (x-1)g_1(x), \gamma^{\frac{e}{2}} g_1(x)g_2(x) \rangle$$

alors par [21] nous avons

$$E_1^\perp = \langle (x-1)^\star g_2^\star(x), \gamma^{\frac{e}{2}} g_1^\star(x)g_2^\star(x) \rangle$$

=

$$\langle (x-1)g_2(x), \gamma^{\frac{e}{2}} g_1(x)g_2(x) \rangle$$

$= E_2$ Ce qui implique que E_1 et E_2 sont des codes cycliques duaux l'un de l'autre sur $\mathcal{R}$.

□Nous donnons dans la suite quelques exemples de codes auto-duaux définis sur les anneaux finis.

Exemple 38. *Pour* $n = 11 \equiv -1 \mod 4$ *et* $q = 3 \equiv \square \mod 11$.
Il existe une paire de codes duadiques impaires sur $\mathbb{F}_3$ *engendrés respectivement par* $f_1(x),\ f_2(x)$.
Soient $g_1(x),\ g_2(x)$ *leurs relevés de Hensel sur* $\mathbb{Z}_9$.

$$x^{11} - 1 = (x-1)(x^5 + 3x^4 + 8x^3 + x^2 + 2x - 1)(x^5 - 2x^4 - x^3 + x^2 - 3x - 1).$$

Pour $g_1(x) = x^5 + 3x^4 + 8x^3 + x^2 + 2x - 1$, *on a* $g_1^*(x) = -(x^5 - 2x^4 - x^3 + x^2 - 3x - 1) = -g_2(x)$

$$C = \langle (x-1)g_i(x), 3g_i(x)g_j^*(x) \rangle \text{ est auto-dual.}$$

Exemple 39. *Pour* $n = 31$, $31 \equiv -1$ *mod* 8
$x^{31} - 1 = (x-1)(x^5 + x^2 + 1)(x^5 + x^3 + 1)(x^5 + x^3 + x^2 + x + 1)(x^5 + x^4 + x^2 + x + 1)(x^5 + x^4 + x^3 + x + 1)(x^5 + x^4 + x^3 + x^2 + 1)$ *dans* $\mathbb{F}_2[x]$. *Le code cyclique de longueur* 31 *défini sur* $\mathbb{F}_2 + u\mathbb{F}_2$ *:*

$$\langle (x-1)(x^5 + x^2 + 1)(x^5 + x^3 + 1)(x^5 + x^3 + x^2 + x + 1), u\frac{x^{31} - 1}{(x-1)} \rangle \text{ est auto-dual.}$$

Exemple 40. *Pour* $n = 23 \equiv -1 \mod 4$ *et* $q = 2 \equiv \square \mod 23$.

Il existe une paire de codes duadiques impaires sur $\mathbb{F}_2$ *engendrés respectivement par* $f_1(x),\ f_2(x)$.

Soient $g_1(x),\ g_2(x)$ *leurs relevés de Hensel sur* $\mathbb{Z}_4$.

$$x^{23}-1 = (x-1)(x^{11}+2x^{10}+3x^9+3x^7+3x^6+3x^5+2x^4+x+3)(x^{11}+3x^{10}+2x^7+x^6+x^5+x^4+x^2+2x+3)$$

Pour $g_1(x) = (x^{11} + 2x^{10} + 3x^9 + 3x^7 + 3x^6 + 3x^5 + 2x^4 + x + 3)$,
on a $g_1^*(x) = -(x^{11} + 3x^{10} + 2x^7 + x^6 + x^5 + x^4 + x^2 + 2x + 3) = -g_2(x)$

$$C = \langle (x-1)g_i(x), 2g_i(x)g_j^*(x) \rangle \text{ est un code cyclique auto-dual sur.}$$

Exemple 41. *Pour* $n = 31 \equiv -1 \mod 4$ *et* $q = 2 \equiv \square \mod 31$.

Il existe une paire de codes duadiques impaires sur $\mathbb{F}_2$ *engendrés respectivement par* $f_1(x),\ f_2(x)$.

Soient $g_1(x),\ g_2(x)$ *leurs relevés de Hensel sur* $\mathbb{Z}_4$.

$x^{31} - 1 = (x-1)(x^5 + 3x^2 + 2x + 3)(x^5 + 2x^4 + 3x^3 + x^2 + 3x + 3)(x^5 + 3x^4 + x^2 + 3x + 3)(x^5 + 2x^4 + x^3 + 3)(x^5 + x^4 + 3x^3 + x + 3)(x^5 + x^4 + 3x^3 + x^2 + 2x + 3)$

Pour $g_1(x) = (x^5+3x^2+2x+3)(x^5+2x^4+3x^3+x^2+3x+3)(x^5+3x^4+x^2+3x+3)$
on a $g_1^*(x) = -(x^5+2x^4+x^3+3)(x^5+x^4+3x^3+x+3)(x^5+x^4+3x^3+x^2+2x+3) = -g_2(x)$

$$C = \langle (x-1)g_i(x), 2g_i(x)g_j^*(x) \rangle \text{ est un code cyclique auto-dual.}$$

Exemple 42. *Pour* $n = 47 \equiv -1 \mod 4$ *et* $q = 2 \equiv \square \mod 47$.

Il existe une paire de codes duadiques impaires sur $\mathbb{F}_2$ *engendrés respectivement par* $f_1(x),\ f_2(x)$.

Soient $g_1(x),\ g_2(x)$ *leurs relevés de Hensel sur* $\mathbb{Z}_4$.

$x^{47} - 1 = (x+3)(x^{23} + 2x^{21} + x^{19} + x^{18} + 2x^{16} + x^{14} + 3x^{13} + 3x^{12} + 2x^{11} + 3x^{10} + 3x^9 + x^7 + 3x^6 + 3x^5 + 2x^4 + x^3 + x^2 + 3x + 3)(x^{23} + x^{22} + 3x^{21} + 3x^{20} + 2x^{19} + x^{18} + x^{17} + 3x^{16} + x^{14} + x^{13} + 2x^{12} + x^{11} + x^{10} + 3x^9 + 2x^7 + 3x^5 + 3x^4 + 2x^2 + 3)$

Pour $g_1(x) = (x^{23} + 2x^{21} + x^{19} + x^{18} + 2x^{16} + x^{14} + 3x^{13} + 3x^{12} + 2x^{11} + 3x^{10} + 3x^9 + x^7 + 3x^6 + 3x^5 + 2x^4 + x^3 + x^2 + 3x + 3)$

on a $g_1^*(x) = -(x^{23} + x^{22} + 3x^{21} + 3x^{20} + 2x^{19} + x^{18} + x^{17} + 3x^{16} + x^{14} + x^{13} + 2x^{12} + x^{11} + x^{10} + 3x^9 + 2x^7 + 3x^5 + 3x^4 + 2x^2 + 3) = -g_2(x)$

$C = \langle (x-1)g_i(x), 2g_i(x)g_j^*(x) \rangle$ *est un code cyclique auto-dual.*

Appendice

4.17 Généralités sur les Anneaux Finis et les Modules.

4.17.1 Introduction

Pour commencer, nous allons devoir définir ce qu'est une structure algébrique : Un ensemble est muni d'une structure algébrique si une ou plusieurs lois de composition sont définies sur cet ensemble.

De très nombreuses structures algébriques ont été étudiées. Il n'est pas question ici de toutes les recenser. On peut néanmoins citer quelques unes : les groupes, les anneaux, les corps et les espaces vectoriels.

Mais, nous nous intéressons essentiellement, dans ce chapitre, à la structure d'anneau ainsi qu'à certaines définitions et propriétés qui en découlent.

4.18 Anneaux, corps et idéaux

Un anneau est un ensemble $\mathcal{R}$, muni de deux lois, notées en général par $+$ et $\times$ telles que $(\mathcal{R}, +)$ soit un groupe abélien, $(\mathcal{R}, \times)$ un monoïde (ie. la loi est associative) et vérifiant de plus une propriété de distributivité de l'addition par rapport à la multiplication. Si, de plus, la multiplication admet un élément neutre, noté 1 en général, on dira que l'anneau $\mathcal{R}$ est unitaire et si cette même multiplication est commutative, on dira que l'anneau est commutatif.
En fait, dans toute la suite , sauf mention contraire, tous les anneaux considérés seront

commutatifs unitaires. Donnons quelques définitions utiles :

Définition 60. *Un élément inversible de $\mathcal{R}$ est un élément $x \neq 0$ de $\mathcal{R}$ qui "divise" 1. En d'autres termes, on a $xy = 1$ pour un certain $y \neq 0$ dans $\mathcal{R}$.*

Définition 61. *Un élément a d'un anneau $\mathcal{R}$ est un diviseur de zéro si et seulement s'il est non nul et s'il existe $b \in \mathcal{R}$ non nul tel que $ab = 0$.*

Définition 62. *Un anneau $\mathcal{R}$ est intègre si et seulement si $\mathcal{R} \neq \{0\}$ et si $\mathcal{R}$ n'a pas de diviseur de zéro ,autrement dit si on a :*

$$ab = 0 \Rightarrow (a = 0 \text{ ou } b = 0).$$

Définition 63. *Un corps est un anneau dont tout élément non nul est inversible.*

Exemple 43.
- *$\mathbb{Z}$ est intègre*
- *un corps $\mathcal{K}$ est intègre*
- *$\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre.*

Homomorphisme d'anneaux

Soit $\mathcal{A}$ et $\mathcal{B}$ deux anneaux. Une application $f : \mathcal{A} \to \mathcal{B}$ est un homomorphisme d'anneaux si et seulement si :

1. $f(a + b) = f(a) + f(b)$ pour tous $a, b \in \mathcal{A}$
2. $f(ab) = f(a)f(b)$ pour tous $a, b \in \mathcal{A}$
3. $f(1_{\mathcal{A}}) = 1_{\mathcal{B}}$

Caractéristique d'un anneau

Définition 64. *Soit $\mathcal{R}$ un anneau.S'il existe un entier n non nul tel que $n1_R = 0$, on pose $c = inf\{n \in \mathbb{N}^*/n1_{\mathcal{R}} = 0\}$ et l'on dit que $\mathcal{R}$ est un anneau de caractéristique c . Dans le cas contraire , on dit que $\mathcal{R}$ est de caractéristique 0 (ou infinie).*
La caractéristique d'un anneau $\mathcal{R}$ se note $car(\mathcal{R})$.

Exemple 44. – *La caractéristique du corps $\mathbb{Z}_p$ est p pour tout entier p premier.*

– *La caractéristique de $\mathbb{Q}$,$\mathbb{R}$,$\mathbb{C}$ est nulle.*

4.18.1 Idéaux et anneaux quotients

Nous pourrions donner la définition générale dans le cas d'anneaux non commutatifs d'idéal à droite,à gauche et bilatère, mais, comme rappelé ci-dessus,les anneaux considérés par la suite seront commutatifs.

Définition 65. *Une partie I d'un anneau $\mathcal{R}$ est appelée idéal si et seulement si :*

– *I est un sous groupe de $(\mathcal{R}, +)$;*

– *$\forall a \in \mathcal{R}, \forall x \in I : ax \in I$.*

Exemple 45. *i) Si $\mathcal{K}$ est un corps $\mathcal{K}$ n'a que deux idéaux $\{0\}$ et lui-même.*

ii) Si $f : \mathcal{A} \to \mathcal{B}$ est un homomorphisme d'anneaux,alors $Ker(f)$ et $Imf(f)$ sont respectivement des idéaux de $\mathcal{A}$ et $\mathcal{B}$.

Définition 66. *Un idéal I de $\mathcal{R}$ est dit propre dans R, s'il n'est pas égal à l'anneau tout entier.*

Définition 67. *Soit $\mathcal{R}$ un anneau et I un idéal de $\mathcal{R}$. On définit l'anneau quotient comme :*

$$\mathcal{R}/I = \{r + I : r \in \mathcal{R}\}$$

Idéaux premiers et idéaux maximaux

Définition 68. *(**Idéal premier**) Soit $\mathcal{R}$ un anneau et I un idéal de $\mathcal{R}$. L'ideal I est un idéal premier de $\mathcal{R}$ si et seulement si :*

$$\forall (a, b) \in \mathcal{R} \times \mathcal{R}\ a.b \in I \Rightarrow a \in I \text{ ou } b \in I$$

Exemple 46. *1. Les idéaux premiers de $\mathbb{Z}$ sont $\{0\}$ et les $n\mathbb{Z}$ pour n premier.*

2. *L'image réciproque d'un idéal premier par un morphisme d'anneaux est un idéal premier.*

Théorème 56. *Soit $\mathcal{R}$ un anneau commutatif unitaire, et $I \neq \mathcal{R}$ un idéal propre de $\mathcal{R}$, alors $\mathcal{R}/I$ est un anneau intègre si et seulement si I est un idéal premier de $\mathcal{R}$.*

Exemple 47. *$\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre ($2.3 = 0$) car 6 n'est pas premier*

Théorème 57. *Soit $\mathcal{R}$ un anneau commutatif unitaire, un idéal M de R est dit maximal si et seulement si $\mathcal{R}/M$ est un corps.*

Exemple 48.
1. *Si $\mathcal{K}$ est un corps,alors son seul idéal maximal est $\{0\}$.*
2. *Dans l'anneau $\mathbb{Z}$, l'ideal $\{0\}$ est un idéal premier.*
   - *$H_4 = \{4n, n \in \mathbb{Z}\}$ on peut le voir comme un idéal maximal dans l'anneau des entier pair E.*
   - *H_4 n'est pas premier car $2.2 = 4 \in H_4$ mais 2 n'appartient pas à H_4 et aussi n'est pas maximal car $4\mathbb{Z} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$.*

Théorème 58. *Tout idéal propre I de $\mathcal{R}$ est inclus dans un idéal maximal de $\mathcal{R}$.*

Lemme 20. *(**Lemmede Zorn**) Tout ensemble inductivement ordonné non vide admet des éléments maximaux.*

Corollaire 11. *Tout élément non inversible de $\mathcal{R}$ est contenu dans un idéal maximal.*

Définition 69. *(**Idéal principal**) Un idéal I d'un anneau $\mathcal{R}$ est dit principal s'il existe un élément $a \in I$ tel que $I =< a >$,où*

$$< a >= \{ax : x \in \mathcal{R}\}$$

L'élément a est dit générateur de I et I est dit engendré par a. Un anneau intègre dans lequel tout idéal est principal est dit principal.

Définition 70. *(**Anneau factoriel**)*

Un anneau $\mathcal{R}$ est factoriel si tout élément $x \in \mathcal{R}$ peut s'écrire :

$$x = x_1^{e_1}.x_2^{e_2}...x_k^{e_k}$$

où les x_i sont des éléments irréductibles de $\mathcal{R}$ et les exposants e_i des entiers positifs. Cette factorisation est unique.

Remarque 28. *si $\mathcal{R}$ n' est pas intègre cette factorisation n'est pas toujours unique.*

Définition 71. *(**Anneau local**) Un anneau $\mathcal{R}$ est dit anneau local si et seulement s'il admet un seul idéal maximal.*

Ainsi les assertions suivantes sont équivalentes :

1. A est un anneau local.
2. A admet exactement un idéal maximal.
3. Les diviseurs de zéro de A sont contenus dans un idéal propre.
4. Les diviseurs de zéro de A forment un idéal.
5. Les diviseurs de zéro de A forment un groupe commutatif additif.
6. Pour tout x dans A, un des deux éléments de l'ensemble $\{x, 1+x\}$ est inversible.

Définition 72. *(**Idéal primaire**) Un idéal I d'un anneau $\mathcal{R}$ est dit primaire si $\forall a, b \in \mathcal{R}$ si $ab \in I$ et $a \notin I$ entraine qu'il existe un entier n tel que $b^n \in I$.*

Théorème 59. *Si I est un idéal primaire d'un anneau $\mathcal{R}$, son radical $\sqrt{I}$ est premier et c'est le plus petit idéal premier contenant I.*

Exemple 49. *Les idéaux primaires de $\mathbb{Z}$ sont (0) et $p^n\mathbb{Z}$ avec p un entier premier , en effet, ce sont les seuls idéaux de $\mathbb{Z}$ avec un radical premier et il est immédiat qu'ils sont primaires.*

Théorème 60. *Dans un anneau principal $\mathcal{R}$, un élément $p \neq 0$ est irréductible, si et seulement si l'idéal $p\mathcal{R}$ est premier.*

Corollaire 12. *Dans un anneau principal, tout idéal premier non nul est maximal.*

Théorème 61. *Dans un anneau principal, toute suite croissante d'idéaux est stationnaire.*

4.18.2 Idéaux étrangers et théorème chinois

[18] Soient $I_1, I_2, \ldots, I_n$ des ideaux de $\mathcal{R}$. l'ideal $I_1 + I_2 + \cdots I_n$ est l'idéal formé des sommes $x_1 + x_2 + \cdots + x_n$ où $x_i \in I_i$ pour $j = 1, \ldots, n$.

Définition 73. *1. On dit que $I_1, I_2, \ldots, I_n$ sont étrangers si l'on a $I_1 + I_2 + \cdots I_n = \mathcal{R}$.*

2. On dit que $I_1, I_2, \ldots, I_n$ sont étrangers deux à deux si I_r et I_s sont étrangers pour tout $r \neq s$.

Théorème 62. *On suppose que $I_1, I_2, \ldots, I_n$ sont des idéaux étrangers deux à deux. Alors le morphisme d'anneaux*

$$\psi : \mathcal{R} \longrightarrow \mathcal{R}/I_1 \oplus \cdots \oplus \mathcal{R}/I_n$$

induit un isomorphisme d'anneaux

$$\mathcal{R}/(I_1 \cap I_2 \cap \ldots \cap I_n) \longrightarrow \bigoplus_{r=1}^{n} \mathcal{R}/I_r$$

Nilradical, radical et radical de Jacobson

Définition 74. ***(Elément nilpotent, Nilradical)***

i) Un élément a d'un anneau $\mathcal{R}$ est dit nilpotent s'il existe un entier $n \neq 0$ tel que $a^n = 0$

*ii) L'ensemble des éléments nilpotents de $\mathcal{R}$ est appelé le **Nilradical** de $\mathcal{R}$ et noté $Nil(\mathcal{R})$.*

Proposition 36. *L'ensemble $\mathfrak{N}$ de tout les éléments nilpotents dans un anneau $\mathcal{R}$ est un idéal, et $A/\mathfrak{N}$ n'admet aucun élément nilpotent $\neq 0$.*

La proposition suivante nous donne le lien entre $Nil(\mathcal{R})$ et les idéaux premiers de l'anneau :

Proposition 37. *Le nilradical de $\mathcal{R}$ est l'intersection de tout les idéaux premiers de $\mathcal{R}$.*

Plus généralement, on définit le **radical** d'un idéal I de $\mathcal{R}$ par la formule :

$$\sqrt{I} = \{a \in A;\ il\ existe\ n \geq 1,\ a^n \in I\}$$

c'est un idéal de A qui contient I.
On déduit alors que le nilradical de $\mathcal{R}$ est égal au radical de l'idéal nul.

Définition 75. *Un idéal I d'un anneau $\mathcal{R}$ est dit maximal si et seulement si $I \neq \mathcal{R}$ et si J est un idéal de $\mathcal{R}$ distinct de $\mathcal{R}$ tel que : $I \subset J$ alors $J = I$.*

Définition 76. *Le **radical de Jacobson** de $\mathcal{R}$ noté $\mathfrak{J}(\mathcal{R})$ est l'intersection de tout les idéaux maximaux de $\mathcal{R}$.*

Il peut être caractérisé comme suit :

Proposition 38. *$x \in \mathfrak{J}(\mathcal{R}) \Leftrightarrow 1 - xy$ est inversible dans $\mathcal{R}$ pour tout $y \in \mathcal{R}$.*

Proposition 39. *Tout anneau intègre fini est un corps.*

Proposition 40. *L'idéal maximal d'un anneau fini local est nilpotent.*

Preuve: comme $\mathcal{R}$ est un anneau fini alors il admet un nombre fini d'idéaux premiers $\{P_1, P_2, \ldots, P_s\}$, donc $\mathcal{R}/P_i$ avec $1 \leq i \leq s$ sont des anneaux intègres . Or un anneau fini intègre est un corps , donc les P_i sont des idéaux maximaux pour $1 \leq i \leq s$. Ce qui entraine $Nil(\mathcal{R}) = \bigcap P_i = P = M = \mathfrak{J}(\mathcal{R})$.

4.18.3 Polynômes et anneaux de polynômes

Définition 77. *Un polynôme à une inconnue sur un anneau unitaire est une fonction $f : \mathbb{R} \to \mathbb{R}$ définie par une expression du type :*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$$

*où x est appelé **indéterminée** du polynôme supposé être distinct de tout élément de l'anneau $\mathcal{R}$. Les éléments $a_0, ..., a_n \in \mathcal{R}$ sont appelés les **coefficients** de $f(x)$.*
*Si $a_n \neq 0$, n est appelé le **degré** de $f(x)$ et est noté $deg(f(x))$.*

Définition 78. *Un polynôme $a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ est dit unitaire si et seulement si $a_n = 1$, c'est à dire que le coefficient de la variable de plus haut degré est égal à 1 (l'élément neutre pour la multiplication de$\mathcal{R}$).*

Définition 79. *(**Anneau de polynômes**) L'ensemble des polynômes sur $\mathcal{R}$ muni des deux opérations, l,addition et la multiplication, admet une structure d'anneau commutatif unitaire noté $\mathcal{R}[x]$.*

Proposition 41. *Si l'anneau $\mathcal{R}$ est intègre alors l'anneau $\mathcal{R}[x]$ l'est aussi .*

c'est à dire si P et Q sont deux polynômes tels que $P.Q$ est le polynôme nul alors soit P est nul ou Q est nul.

Soient $f(x), g(x)$ et $d(x)$ des polynômes dans $\mathcal{R}[x]$, si $d(x)$ divise $f(x)$ et $g(x)$, et si tout polynôme divisant $f(x)$ et $g(x)$ divise aussi $d(x)$, alors $d(x)$ est le **plus grand diviseur commun** de $f(x)$ et $g(x)$.On note $d(x) = pgcd(f(x), g(x))$.
Si $pgcd(f(x), g(x)) = 1$, on dit que $f(x)$ et $g(x)$ sont **premier entre eux**.

Définition 80. *(**Polynôme constant**) Un polynôme constant est un polynôme constitué d'un unique monôme de degré 0, il s'identifie avec un élément de l'anneau $\mathcal{R}$.*
*On écrit souvent $p(x) = a_0$. Les autres polynômes sont dits **non constants**.*

Définition 81. *(**Polynôme irréductible**) Un polynôme non constant $f(x) \in \mathcal{R}[x]$ est dit irréductible sur $\mathcal{R}$ si les seuls polynômes différents de $f(x)$ qui le divise sont constants. Sinon, le polynôme $f(x)$ est **réductible**.*

Définition 82. *(**Racine d'un polynôme**) Un élément a est une racine (ou un zéro) du polynôme $f(x)$ si $f(a) = 0$.*

Dans la suite, on va voir une famille particuliere d'anneaux .

4.19 Anneau de Galois

Nous abordons ici les anneaux de Galois, Il semble que c'est Krull qui a initié l'étude des anneaux de Galois en 1924 , et plus tard, ces anneaux ont été redécouvert indépendamment par Janusz en 1966, et Raghavendran en 1969. Depuis lors ,les anneaux de

Galois ont été révélés applicable dans de nombreuses branches mathématiques comme la combinatoire et la théorie des codes.

Définition 83. *$\mathcal{R}$ est un anneau de Galois s'il est commutatif, unitaire, et si l'ensemble de ces diviseurs de zéro est de la forme pR, où p est un nombre premier.*

Les corps de Galois peuvent donc être considérés comme des anneaux de Galois ne contenant pas de diviseurs de zéro. L'exemple le plus utilisé en théorie de codes est $\mathcal{R} = \mathbb{Z}_{p^m}$, l'anneau des entiers modulo p^m.
La *caractéristique* noté $car\mathcal{R}$ est l'ordre additif de l'élément neutre pour la multiplication 1.
Ainsi $(\mathbb{Z}_m, +, .)$ est un anneau de caractéristique m, puisque 1 est d'ordre m dans $(\mathbb{Z}_m, +)$.
La caractéristique d'un anneau $\mathcal{R}$ de Galois est

$$carR = p^m, m \in \mathbb{N}$$

Nous allons voir que d'une manière générale, l'anneau $\mathbb{Z}_{p^m}$ est un anneau local pour p premier. C'est de plus un anneau de Galois.

Exemple 50. *$\mathcal{R} = \mathbb{Z}_{p^n}$ l'anneau des entiers modulo p^n.*

La caractéristique de l'anneau de Galois $\mathcal{R}$ est : $carR = p^n$, $n \in \mathbb{N}$.

4.19.1 Paramètres d'un anneau de Galois

Notons "\" le symbole représentant la soustraction ensembliste.Le groupe multiplicatif R^* de l'anneau est

$$R^* = R \backslash pR = R \backslash D,$$

Puisque les diviseurs de zéro sont les seuls éléments non inversibles dans un anneau fini. Les éléments de R^* sont donc les inversibles de $\mathcal{R}$ et $M = pR$ est l'unique idéal maximal

de $\mathcal{R}$.

De plus l'anneau

$$\overline{R} = R/M$$

est le corps de Galois $GF(q)$ (q étant une puissance de p, p^n). Notons $\overline{1}$ l'élément neutre de $\overline{\mathcal{R}}$. Nous avons donc $\overline{1} = 1 + M$.

Posons $M^e = p^e\mathcal{R}$ et $\{0, ..., m-1\}$. On a alors

$$M^{m-1} \neq 0 \; et \; M^m = 0,$$

Et la chaine suivante d'idéaux admet des inclusions strictes :

$$\mathcal{R} = M^0 \supset M = pR \supset ...M^{m-1} = p^{m-1}R \supset M^m = p^mR = 0$$

Tout comme la caractéristique , le cardinal de l'anneau est important pour la détermination de $\mathcal{R}$.

Nous verrons que ces deux paramètres déterminent complètement, à isomorphe près, l'anneau de Galois. Nous allons prouver que le nombre d'éléments de l'anneau $\mathcal{R}$ et du groupe multiplicatif $\mathcal{R}^*$ sont

$$|\mathcal{R}| = q^m, \qquad |R^*| = (q-1)q^{m-1}.$$

Il suffit pour cela de prouver que pour chaque $e \in \{0, ..., n-1\}$, nous avons l'égalité

$$|p^eR/p^{e+1}R| = q.$$

Posons $R_e = p^tR/p^{t+1}R$. Il est facile de voir que R est un espace vectoriel sur $\overline{R} = GF(q)$. De plus $\dim_{\overline{R}} R_t = 1$.

En effet considérons $\alpha \in p^tR \backslash p^{t+1}R$,nous avons $R\alpha = p^tR$ et $\overline{R}\alpha = R_t$. Ainsi $|R| = q^m$ et le cardinal de R^* découle immédiatement.

4.19.2 Extension de l'anneau de Galois $\mathcal{R}$

Nous allons montrer que la donnée d'un b- polynôme f de degré r sur R permet de construire un gros anneau en adjoignant à R une racine de f . Nous appelons cette

extension une G-extension de R. Le b-polynôme $f(x) \in R[x]$ permet de construire la G-extension $S = Rr[x]/(f(x))$ qui est un anneau de Galois.

Théorème 63. *Soit Rr un anneau de Galois de q^m éléments et de caractéristique p^m. Soit $f(x)$ un b-polynôme sur R de degré r . Alors l'anneau quotient*

$$S = R[x]/(f(x))$$

est un anneau de Galois de paramètres :

$$carS = p^m \qquad |S| = p^{mr}$$

Preuve: Si le calcul des paramètres de l'anneau ne pose aucune difficulté, il convient de prouver que S est un anneau de Galois. Les éléments de pS sont des diviseurs de zéro. Il faut donc vérifier que tous les éléments de $S\backslash pS$ sont des inversibles.
Considérons α un élément de $S\backslash pS$ .Il peut s'écrire de façon unique

$$\alpha = [A(X)]_f = A(X) + f(X)R[X],$$

où $A(X) \in R[X], \deg A(X) < m$ et $\overline{A}(X) \neq 0$.
Nous avons alors $(\overline{A}(X), \overline{f}(X)) = \overline{1}$ et d'après Bezout il existe deux polynomes $U(X)$ et $V(X)$ appartenant à $R[X]$ qui vérifient l'identité

$$\overline{U}(X)\overline{A}(X) + \overline{V}(X)\overline{f}(X) = \overline{1}.$$

En d'autre termes, il existe $B(X) \in R[X]$ tel que

$$U(X)A(X) + V(X)f(X) = 1 + pB(X)$$

Ainsi

$$[U(X)]_f[A(X)]_f = [1 + pB(X)]_f.$$

Il est facile de voir que $[1|pB(X)]_f$ est inversible puisque

$$[1 + pB(X)]_f^{p^{n-1}} = [1]_f$$

L'élément α est donc inversible. □ L' existence d'un anneau de Galois se déduit du résultat précédant.

Lemme 21. *Pour tout anneau de Galois R et tout entier r il existe une G-extension de degré r de R .*

Lemme 22. *Pour tout p premier ,$r, m \in \mathbb{N}$, il existe un anneau de Galois S de caractéristique p^m ayant p^{mr} éléments .*

Exemple 51. *Soit l'anneau des entier modulo* 8, $R_8 = \mathbb{Z}_{2^3} = \mathbb{Z}_8$.
Posons $S_8 = R_8[X]/(f(x))$ *avec* $f(x) = x^3 + 6x^2 + 5x + 7$
Le polynôme f est un b-polynôme et $\overline{f(x)} = x^3 + x + 1$

$$car S = 8 \qquad |S| = 64$$

L'anneau S_8 est une G-extension de degré 3 de R_8.

En régle général, si l'on considère un élément α de S , le sous anneau

$$\{A(\alpha) : A(X) \in R[X]\}$$

de R est noté $R[\alpha]$. C'est une extension de l'anneau R par α . Dans l'exemple précédant, $S_8 = R_8[\alpha]$ où α et une racine de $f(x)$. L'anneau S_8 peut s'écrire en tant que module $\langle 1, \alpha, \alpha^2 \rangle$

Corollaire 13. *Soit S un anneau de Galois de caractéristique p^m et de cardinal p^{mr} alors :*

$$S \approx \mathbb{Z}_{p^m}[x]/(f(x))$$

où $f(x)$ est un b-polynôme de degré r sur $\mathbb{Z}_{p^m}$, notons un tel anneau de Galois $GR(p^m, r)$. Ainsi ,deux anneaux de Galois sont isomorphes si et seulement s'ils ont même cardinale et caractéristique.

Remarque 29. $GR(p^m, 1) = \mathbb{Z}_{p^m}$ *et* $GR(p, r) = \mathbb{F}_{p^r}$

Corollaire 14. *Soit a un entier impair, alors $X^a - 1$ admet une factorisation unique dans S.*

Soit l'anneau de Galois :

$$GR(p^m, r) = \mathbb{Z}_{p^m}[\xi] = \mathbb{Z}_{p^m}[x]/(G_{(p,r)}(x)),$$

où ξ est une racine d'un b-polynôme unitaire, $G_{(p,r)}(x) \in \mathbb{Z}_{p^m}[x]$, déterminé par le lemme de Hensel à partir d'un polynôme primitif $g_{(p,r)}(x) \in \mathbb{Z}_p[x]$ de degré r tel que :

$$\mathbb{F}_{p^r} = GF(p^r) = \mathbb{F}_p[x]/(g_{(p,r)}(x)) \cong \mathbb{Z}(\theta),$$

Avec $g_{(p,r)}(\theta) = 0$ et $g_{(p,r)}(x) \equiv G_{(p,r)}(x) \pmod{p}$. Ainsi le polynome $G_{(p,r)}(x)$ est lié à $g_{(p,r)}(x)$ par l'épimorphisme :

$$\mu : \mathbb{Z}_{p^m}[x] \to \mathbb{Z}_p[x],$$

i.e., $\mu(G_{(p,r)})(x) = g_{(p,r)}(x) \in \mathbb{Z}_p[x]$.
Si $g_{(p,r)}(x)$ est un polynome unitaire, irréductible de la forme :

$$g_{(p,r)}(x) = x^r + a_{r-1}x^{r-1} + ... + a_0.$$

Dans ce cas là, on a :

$$G_{(p,r)}(x) = x^r + (p^m - p + a_{r-1})x^{r-1} + ... + (p^m - p + a_0) \in \mathbb{Z}_{p^m}[x].$$

$$GR(p^m, r) = \{\sum_{j=0}^{r-1} b_j \xi^j \ b_j \in \mathbb{Z}_{p^m}, 0 \leq j \leq r-1\},$$

Son idéal maximal est $pGR(p^m, r)$ de corps résiduel

$$GR(p^m, r)/pGR(p^m, r) \cong \mathbb{F}_{p^r}.$$

Avec $G_{(p,r)}(\xi) = 0$.
Notons que les éléments de l'idéal maximal s' écrivent de manière unique :

$$pGR(p^m, r) = \{p\sum_{j=0}^{r-1} b_j \xi^j \mid b_j \in \mathbb{Z}_{p^m}, 0 \leq j \leq r-1\},$$

Plus précisement :

$$pGR(p^m, r) = \{\sum_{j=0}^{r-1} b_j \xi^j \mid b_j \in p\mathbb{Z}_{p^m}, 0 \leq j \leq r-1\}.$$

Exemple 52. *Dans l'anneau $\mathbb{Z}_8$, $p = 2$, $m = 3$ et prenons $r = 3$. Rappelons que :*

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3 + x + 1) = \{a + b\xi + c\xi^2 \mid a, b, c \in \mathbb{F}_2\},$$

Où $\xi^3 = \xi + 1$,i.e

$$\mathbb{F}_8 = \{0, 1, \xi, \xi^2, 1 + \xi, 1 + \xi^2, \xi + \xi^2, 1 + \xi + \xi^2\}.$$

Le polynome $g_{(2,3)}(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$ est un polynôme primitif utilisé pour l'extension de corps $\mathbb{F}_2 \subset \mathbb{F}_8$. D'après le lemme de Hensel :
$G_{(2,3)}(x) = x^3+(8-2+0)x^2+(8-2+1)x+(8-2+1)x+(8-2+1) = x^3+6x^2+7x+7 \in \mathbb{Z}_8[x]$.
On peut donc voir l'anneau de Galois $GR(2^3, 3)$ comme :

$$GR(8, 3) = \{b_0 + b_1\xi + b_2\xi^2 \mid b_i \in \mathbb{Z}_8\},$$

où ξ est une racine de $G_{(2,3)}(x) \in \mathbb{Z}_8$ i.e. $\xi^3 = 2\xi^2 + \xi + 1$, et l'idéal maximal M de $\mathbb{Z}_8$ est $2\mathbb{Z}_8 = \{0, 2, 4, 6\}$ et $\mu(x^3 + 6x^2 + 7x + 7) = x^3 + x + 1$.
On considère l'application

$$\widetilde{\mu} : GR(8, 3) = \mathbb{Z}_8/(x^3 + 6x^2 + 7x + 7) \to \mathbb{Z}_2[x]/(x^3 + x + 1)$$

Les éléments de l'idéal maximal sont de la forme :

$$2GR(8, 3) = \{2(b_0 + b_1\xi + b_2\xi^2) : b_0, b_1, b_2 \in \mathbb{Z}_8\}$$

avec $\xi^3 = 2\xi + \xi + 1\xi$ Or les coefficients $2b_0, 2b_1, 2b_2$ sont dans $M = 2\mathbb{Z}_8$.
Donc on peut écrire $2GR(8, 3) = \{\lambda_0 + \lambda_1\xi + \lambda_2\xi^2/\lambda_i \in M, 0 \leq i \leq 2\}$,
avec $\xi^3 = 2\xi + \xi + 1$

Définition 84. *[30] Soit $GR(p^m, r)^*$ le groupe multiplicatif de $GR(p^m, r)$. Alors :*
si p est impair, ou $p = 2$ et $m \leq 2$, alors

$$GR(p^m, r)^* \simeq \mathbb{Z}_{p^r-1} \times \mathbb{Z}_{p^{m-1}} \times \mathbb{Z}_{p^{m-1}} \ldots \times \mathbb{Z}_{p^{m-1}}, \tag{4.10}$$

Avec r copies de $\mathbb{Z}_{p^{m-1}}$.

Si $p = 2$ et $m \geq 3$,alors

$$GR(2^m, r)^* \simeq \mathbb{Z}_{2^r-1} \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}} \times \mathbb{Z}_{2^{m-1}} ... \times \mathbb{Z}_{2^{m-1}}, \tag{4.11}$$

avec $r-1$ copies de $\mathbb{Z}_{2^{m-1}}$.

4.19.3 Sous-anneau d'un anneau de Galois

Tout sous-anneau de $GR(p^m, r)$ est un anneau de la forme $GR(p^m,)$ où l divise r. Inversement, si l divise r alors $GR(p^m, r)$ contient une seule copie de $GR(p^m, l)$.
Cela veut dire que le nombre de sous-anneaux de $GR(p^m, r)$ est le nombre de diviseurs positives de r.

4.19.4 Les inversibles de $GR(p^m, r)$

Théorème 64. *[30] Soit $S = GR(p^m, r)$. Le groupe multiplicatif de S peut s'écrire comme le produit direct de deux groupes :*

$$S^* = G_1 \times G_2$$

où

1. *G_1 est un groupe cyclique d'ordre $p^r - 1$*
2. *G_2 est un groupe d'ordre $p^{(m-1)r}$ tel que*
   - *Si p est impair ,ou si $p = 2$ et $m \leq 2$,alors G_2 est un produit direct de m groupes cycliques chacun d'ordre p^{m-1}.*
   - *Si $p = 2$ et $m \leq 3$, alors G_2 est un produit direct d'un groupe cyclique d'ordre 2, un groupe cyclique d'ordre 2^{m-2} et $r-1$ groupes cyclique chacun d'ordre 2^{m-1}*

Exemple 53. *Prenons l'exemple précédant : $R = \mathbb{Z}_8$ et $S_8 = R[X]/(f(X))$ avec*

$$f(X) = X^3 + 6X^2 + 5X + 7.$$

Alors $f(X)$ divise $X^7 - 1$ dans $\mathbb{Z}_8[X]$. Soit α une racine primitive de $f(X)$, l'ordre de α est $2^3 - 1 = 7$.
Notons H le groupe cyclique engendré par α et K le corps résiduel de S, on a alors :

$$H \approx (K, \times).$$

Soit $U = 1 + 2S_8 + 4S_8$ alors $(U, \times) \approx (S_4, +)$ où $S_4 \approx \mathbb{Z}_4/(f(X) \mod 4)$. Ainsi

$$S_8^* \approx (K, \times) \times (S_4, +).$$

Il s'ensuit que l'ordre multiplicatif maximal d'un élément de S_8^* est $4(2^r - 1) = 28$.

4.19.5 L'anneau de Galois $R = GR(4, r)$

On sait que l'anneau $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ des entier modulo 4 est un anneau local. Son unique idéal maximal $2\mathbb{Z} = \{0, 2\}$ est composé de diviseurs de zéro. Soit $f \in \mathbb{Z}_4[X]$, définissons l'application projection μ comme suit :

$$\mu \colon \mathbb{Z}_4[X] \to GF(2)[X]$$

Qui réduit modulo 2 les coefficients de $f(x) \in \mathbb{Z}_4[X]$.
Ainsi un b-polynôme $f \in \mathbb{Z}_4[X]$ est un polynôme unitaire tel que $\mu(f)$ est irréductible sur $\mathbb{Z}_2$.

Lemme 23. *Le polynome $X^a - 1$ (a impair et strictement positif) admet une factorisation unique sur $\mathbb{Z}_4[x]$. Cette factorisation établit une correspondance biunivoque avec la factorisation sur $\mathbb{Z}_2$.*

Définition 85. *Soit f un b-polynôme de degré r sur $\mathbb{Z}_4$.*
L'anneau de Galois $R = GR(4, r)$ est défini à un isomorphisme près comme étant $\mathbb{Z}_4[X]/(f)$.

Soit β une racine primitive de $f(X)$ et $f(X)$ un facteur primitif de $X^{2^r-1} - 1$ (les facteurs primitifs qui divisent $X^a - 1$ mais pas $X^{a'} - 1$ pour $a > a'$ sont appelés des

facteurs primitifs). Alors l'anneau de Galois $R = GR(4, r)$ peut être défini comme étant l'extension $R = \mathbb{Z}_4[\beta]$. Les diviseurs de zéro forment le sous groupe $2R$.Le groupe des inversible $R^* = R\backslash 2R$ est un produit direct de deux groupes G_1 et G_2. D'après le théorème1.5, le sous groupe G_1 est un groupe cyclique d'ordre a, que l'on va noter T^*, appelé **système de Teichmuller** lorsqu'on lui adjoint 0, posons $T = T^* \cup \{0\}$. Alors on a :

$$T = \{0, 1, \beta^2, ..., \beta^{2^m-2}\}.$$

Les éléments de R admettent une représentation unique **'multiplicative'** ou **'additive'**. Dans la première représentation , un élément $c \in R$ s'écrit $c = a + 2b$ où a et b appartiennent à T. Pour la représentation additive, un élément $c \in R$ s'écrit :

$$c = \sum_{t=0}^{r-1} b_t \beta^t \qquad b_t \in \mathbb{Z}_4$$

Exemple 54. *Soit $h(x) = X^3 + 2X^2 + X - 1$ et β une racine de h. Alors*

$$\begin{aligned}
\beta^3 &= 2\beta^2 + 3\beta + 1 \\
\beta^4 &= 3\beta^2 + 3\beta + 2 \\
\beta^5 &= \beta^2 + 3\beta + 3 \\
\beta^6 &= \beta^2 + 2\beta + 1 \\
\beta^7 &= 1
\end{aligned}$$

Ainsi , l'élément $c = 1 + 3\beta^5$ s'écrit dans la représentation additive $2 + \beta + 3\beta^2$:

$$\begin{aligned}
c &= 1 + 3\beta^5 \\
&= 1 + 3(3 + 3\beta + \beta^2) \\
&= 1 + 1 + \beta + 3\beta^2 \\
&= 2 + \beta + 3\beta^2
\end{aligned}$$

4.20 Modules

4.20.1 Modules et sous-modules

Définition 86. *Soit $(M,+)$ un groupe commutatif , on dit que M est un A-module s'il existe une application : $A \times M \to M$, où on note ax l'image de (a,x), telle que :*

1. *$a(x+y) = ax + ay$ pour $a \in A$ et $x, y \in M$,*
2. *$(a+b)x = ax + bx$ pour $a, b \in A$ et $x \in M$,*
3. *$1x = x$ et $a(bx) = (ab)x$ pour $a, b \in A$ et $x \in M$.*

Si l'anneau A est un corps K , on dit que M est un K-espace vectoriel.

Exemple 55.

1. *Si A est un anneau commutatif unitaire alors A est un A-module*
2. *Si I est un idéal de A, alors I est un A-module*
3. *Un groupe commutatif est un $\mathbb{Z}$-module*
4. *$A^n = A \times A \times ... \times A$,muni des deux opérations :*
   - *$\lambda(a_1, ..., a_n) = (\lambda a_1, ..., \lambda a_n)$*
   - *$(a_1, ..., a_n) + (b_1, ..., b_n) = (a_1 + b_1, ..., a_n + b_n)$*

   est un A-module
5. *Soit $f : A \to B$ un homomorphisme d'anneaux. Alors B muni de l'opération $ab = f(a)b$ pour $a \in A$ et $b \in B$,est un A-module.*

Définition 87. *Soit M un A-module . Un sous groupe N de M tel que $ax \in N$ pour $a \in A$ et $x \in N$ est un sous-module de M.*
Il est claire qu'un sous-ensemble N de M est un sous-module de M si et seulement si $x, y \in N$ et $a, b \in A$ impliquent $ax + by \in N$, autrement dit si et seulement si N est stable par combinaison linéaire .

Exemple 56. *Soit A un anneau commutatif unitaire, alors A est un A-module et les sous modules de A sont les idéaux de A.*

4.20.2 Module de type fini

Définition 88. *On dit qu'un A-module M est de* ***type fini*** *s'il est engendré par un nombre fini d'éléments ,i.e., s'il existe $x_1, x_2, ..., x_n \in M$ tel que :*

$$M = Ax_1 + ... + Ax_n$$

i.e., si tout $m \in M$ s'écrit : $m = a_1x_1 + ... + a_nx_n$ avec $a_i \in A$

Exemple 57. *1. Le A-module A est de type fini : il est engendré par l'élément 1 puisque $a = a1$ pour tout $a \in A$.*

2. Plus généralement , pour tout $n \geq 1$, la somme directe

$$A^n = \{(a_1, ..., a_n) \mid a_i \in A\}$$

est un A-module de type fini. En effet, introduisons les éléments :

$$e_1 = (1, 0, ..., 0), ..., e_n = (0, ..., 0, 1),$$

alors tout élément $a = (a_1, ..., a_n)$ de A^n s'écrit (de façon unique)

$$a = a_1e_1 + ... + a_ne_n.$$

4.20.3 Module libre

Définition 89. *Soit M un A-module et soit B un sous-ensemble de M .On dit que B est une* ***partie libre*** *de M si les éléments de B sont linéairement indépendants sur A ,i.e., si la propriété suivante est vérifiée : pour tout $n \geq 1$ si $\beta_1, ..., \beta_n \in B$ sont deux à deux distincts et si : $a_1\beta_1 + ... + a_n\beta_n = 0$,alors $a_i = 0$ pour tout $i = 1, ..., n$.*

Définition 90. *Soit M un A-module. On dit qu'un sous ensemble B de M est une* ***base*** *de M s'il vérifie les deux propriétés suivantes :*

1. *B engendre M , i.e., tout $x \in M$ s'écrit comme combinaison A-linéaire d'un nombre fini d'éléments de B ,i.e., sous la forme :*

$$m = \sum_{i=1}^{n} a_i\beta_i$$

avec $n \in \mathbb{N}^*, \beta_i \in B$ et $a_i \in A$

2. B est une partie libre de M

Il résulte de 1) *et* 2) *que tout $m \neq 0$ dans M s'écrit de façon* ***unique*** *, comme une somme finie : $m = \sum_{i=1}^{n} a_i \beta_i$ où $n \geq 1, \beta_i \in B$ et $a_i \neq 0$ pour tout $i = 1, ..., n$*

Définition 91. *On dit que M est un A-module* ***libre*** *s'il possède une base.*

Exemple 58. *1. Le A-module A possède la base $\{1\}$. Donc A est un A-module libre.*

2. Plus généralement, pour tout $n \geq 1$, le A-module

$$A^n = \{(a_1, ..., a_n) \mid a_i \in A\}$$

est un A-module libre, il admet comme base $B = (e_1, ..., e_n)$ où

$$e_1 = (1, 0, .., 0), ..., e_n = (0, ..., 0, 1)$$

3. Considérons l'anneau $A = \mathbb{Z}$ et le $\mathbb{Z}$-module $M = \mathbb{Z}/n\mathbb{Z}$ ($on > 1$). Alors M ne possède pas de base comme $\mathbb{Z}$-module. En effet , $\forall x \in M$ on a $nx = 0$, donc la condition "2" de la définition n'est pas vérifiée pour aucun sous-ensemble B de M. Donc $\mathbb{Z}/nZ$ n'est pas un Z-module libre.

4.20.4 Rang d'un module de type fini :

Définition 92. *On dit que M est un A-module libre de* ***rang*** *n s'il est libre et admet une base formée de n éléments, i.e, si $M \cong A^n$.*

Lemme 24. *Si M est un A-module libre, alors toutes les bases de M sont formées d'un nombre fini d'éléments.*

Conclusion et Perspectives

Ce travail a permis de résoudre certains problèmes ouverts dans la théorie des codes correcteurs, spécialement la déterminantion des conditions d'existence des codes cycliques auto-duaux, leurs construction et leur nombre.
Nous avons pu construire des familles infinis de codes auto-duaux qui ont un lien trés important avec la construction de réseaux unimodulaires qui sont utilisés en informatique.

Nous proposons des questions dont certaines sont un prolongement possible de notre travail.

- Il serait intéressant de déterminer des réseaux unimodulaires à partir des codes auto-duaux que nous avons trouvé.
- Pour les codes définis sur les anneaux,nous avons travaillé dans le cas où la caractéristique de l'anneau fini est première avec la longueur du code,il serait intéressant de voir l'autre cas.

Bibliographie

[1] T. Abualrub and R. Oehmke, On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e, IEEE Trans. Inform. Theory, 49(9) 2126–2133, Sept. 2003.

[2] S. A. Aly, A. Klappenecker and P. K. Sarvepalli, Duadic Group Algebra Codes, Proc. IEEE Intern. Sym. Inform. Theory, Seattle, USA, 2096-2100, 2006.

[3] S. A. Aly, A. Klappenecker and P. K. Sarvepalli, Remarkable degenerate quantum stabilizer codes derived from duadic codes, Proc. IEEE Intern. Sym. Inform. Theory, Seattle, USA, 1114-1118, 2006.

[4] M.F.Atiya and I.G.Macdonald. Introduction to commutative algebra. Addition-Wesley, 1969.

[5] N. Aydin, I. Siap and D. J. Ray-Chaudhuri, *The structure of 1-generator quasi-twisted codes and new linear codes*, Des. Codes Cryptogr. 24(3), 313–326, 2001.

[6] A. Batoul, K. Guenda, and T. A. Gulliver, "On self-dual cyclic codes over finite chain rings,"Available online. Des. Codes Cryptogr 2012 :

[7] A. Batoul, K. Guenda, and T. A. Gulliver, Construction of Self-Dual and Isodual Cyclic Codes over Finite Chain Rings. The Algerian-Turkish International days on Mathematics 2012, ATIM2012.

[8] A. Batoul, K. Guenda, and T. A. Gulliver, On Self-dual Cyclic Codes over Finite Principal Rings. .International Colloquy of Algebra and Number Theory, US-THB,2012, ICANT12.

[9] E. Bannai, S. T. Dougherty, M. Harada and M. Oura, Type II codes, even unimodular lattices and invariant rings, IEEE Trans. Inform. Theory, 45(4) 1194–1205, May 1999.

[10] N. Bourbaki, Commutative Algebra, Springer-Verlag, New-York, 1989.

[11] T. Blackford, Cyclic codes over $\mathbb{Z}_4$ of oddly even length, Appl. Discr. Math., 128 27–46, 2003.

[12] T. Blackford, Negacyclic codes over $\mathbb{Z}_4$ of even length, IEEE. Trans. Inform. Theory, 49(6) 1417–1424, June 2003.

[13] A. Bonnecaze, P. Solé, and A. R. Calderbank, Quaternary quadratic residue codes and unimodular lattices, IEEE Trans. Inform. Theory, 41(2) 366–377, Mar. 1995.

[14] A. Bonnecaze et P. Udaya,cyclic codes and self-Dual codes over $F_2 + uF_2$, 1998.

[15] A.Bonnecaze, Codes sur les anneaux finis et réseaux arithmétiques, thése de Doctorat, Université de Nice et l'Ecole doctorale Science pour l'ingénieur, nov.1995.

[16] A.R. Calderbank and N.J.A. Sloane, Modular and p-adic cyclic codes, Designs, Codes, Cryptogr., 6(1) 21–35, 1996.

[17] A.R. Calderbank and N.J.A. Sloane, Modular and p-adic cyclic codes, Designs, Codes, Cryptogr., 6, 1995, 21–35.

[18] A.Chambert-Loir,Algèbre commutative cours à l'université de Rennes 1 (2006-2007).

[19] S.T. Dougherty, M. Harada and P. Solé, Self-dual codes over rings and the Chinese remainder theorem, Hokkaido Math Journal, Volume 28, 1999.

[20] M. Demazure, Cours D'Algèbre : Primalité, Divisibilité, Codes, Cassini, Paris, 1997.

[21] H. Dinh and S. R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans Inform Theory, 50(8) 1728–1744, Aug. 2004.

[22] S.T. Dougherty, T.A. Gulliver and J.N.C. Wong, Self-dual codes over $\mathbb{Z}_8$ and $\mathbb{Z}_9$, Designs, Codes, Crypt., 41(3) 235–249, 2006.

[23] S.T. Dougherty, H. Liu, and Y.H. Park, Lifted codes over finite chain rings, Math. J. Okayama University, 53 39–53, Jan. 2010.

[24] S.T. Dougherty, J. L. Kim and H. Kulosman, MDS codes over finite principal ideal rings, Designs, Codes and Cryptography, 50, 77–92, 2009.

[25] S.T. Dougherty and K. Shiromoto, MDR Codes codes over Z_k, IEEE Trans. Inform. Theory, vol. 46, no. 1, 2000, 265–269.

[26] S.T. Dougherty, M. Harada, and P. Solé, Self-dual codes over rings and the Chinese remainder theorem, Hokkaido Math Journal, 28 253–283, 1999.

[27] S.T.Dougherty,T.A.Gulliver,and J.Wang, Self-dual codes over $\mathbb{Z}_8$ and $\mathbb{Z}_9$,Designs, codes and Crypthography,vol. 41(2006) pp. 235-249.

[28] S. T. Dougherty and J. L. Kim, Construction of self-dual codes over chain rings, Int. J. Inform. and Coding Theory, 1(2) 171–190 2010.

[29] H.Q.Dinh. Constacyclic codes of length 2^s over $\mathbb{Z}_{2^a}$. IEEE Trans. Inform. Theory,53(1) :147-161, 2007.

[30] Gilberto Bini and Flaminio Flamini, Finite commutative rings and their a pplications, University of Michigan, Universita degli Studi Roma Tre,U.S.A and Italy, 2002.

[31] K. Guenda, New MDS self-dual codes over finite fields, Des. Codes and Cryptography, 62(1), pp. 31-42, 2012.

[32] K. Guenda and T. A. Gulliver, MDS and self-dual codes over rings, Finite Fields Appl., 2011.

[33] K.Guenda, Sur l'equivalence des codes, 2010.

[34] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, The Z_4 linearity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. Inform. Theory, 40(2) 301–319, Mar. 1994.

[35] Y. Jia, S. Ling, and C. Xing, On self-dual cyclic codes over finite fields, IEEE Trans. Inform. Theory, 57(4) 2243–2251, Apr. 2011.

[36] J.S.Leon,J.M.Masley,and V.Pless,Duadic codes IEEE Trans.Inform. Theory IT-30 (1984),709-714.

[37] P. Kanwar and S. R. López-Permouth, Cyclic codes over the integers modulo p^m, Finite Fields Appl., 3(4) 334–352, Oct. 1997.

[38] A.Klapper and M.Goresky,An introduction to abstract algebra.

[39] S. R. López-Permouth and S. Szabo, Repeated root cyclic and negacyclic codes over Galois rings, Applied Algebra, Albebraic Algorithms and Error-Correcting Codes, Springer Lecture Notes in Computer Science, 5527 219–222, 2009.

[40] F. J. Macwilliams and N.J.A Sloane, *Thetheory of error correcting-codes,* Benjamin, Inc. Amsterdam,North-Holland, 1977

[41] B.R.McDonald, Finite Rings with identity, Pure and Applied Mathematics, vol.28. Marcel Dekker,Inc.New York,(1974).

[42] P. Moree and P. Solé, Around the Pellikán's conjecture on very odd sequences, Manuscripta Math. 117 219–238, 2005.

[43] C. S. Nedeloaia, Etude des énumérateurs des poids des codes linéaires utilisant des formes décomposées des matrices génératrices, 2005.

[44] G. Ganske and B. R. McDonald, *Finite local rings,* Rocky Mountain J. Math. 3(4), 521-540, 1973.

[45] G. H. Norton and A. Sălăgean, On the structure of linear and cyclic codes over a finite chain ring, Appl. Algebra Engr. Comm. Comput., 10(6) 489–506, 2000. S. Ling et C. Xing,Coding Theory, Cambridge, 2004.

[46] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes,* Cambridge, 2003.

[47] E. Rains and N.J.A. Sloane, Self-dual codes, in Handbook of Coding Theory, V.S. Pless and W.C. Huffman, eds., Elsevier, Amsterdam, 177–294, 1998.

[48] S. Roman, Coding and Information Theory, Graduate Texts in Mathematics, 134, Springer-Verlag, New-York, 1992.

[49] J. J. Rushanan, *Duadic codes and difference sets,* J. Combin. Theory Ser. A, 57 : 254-261, 1991.

[50] J. H. van Lint,"Repeated-root cyclic codes," *IEEE Trans. Inform. Theory*, vol. 37, no. 2, pp. 343–345, Mar. 1995.

[51] S.Ling et P. Solé,Duadic Codes over $F_2 + uF_2$, Springer-Verlag, 2001.

[52] G. Skersys, Calcul du group d'automorphismes des codes, PhD Thesis, Laco, Limoges, 1999.

[53] N. J. A. Sloane and J. G. Thompson, Cyclic self-dual codes, IEEE. Trans. Inform. Theory, 29(3) 364–366, May 1983.

[54] Solé P. Open problem 2 : cyclic codes over rings and p-adic fields. Coding theory and applications (Toulon, 1988), 329, Lecture Notes in Comput Sci, 388, New York : Springer, 1989

[55] M. H. M. Smid, *Duadic codes,* IEEE. Trans. Inform. Theory, 29(2), 1983.

[56] J.Cannon and C.Playoust, An introduction to Magma, University of Sydney, Sydney, Australia, (1994)

[57] V.Pless and Z.QianCyclic codes and quadratic codes over $\mathbb{Z}_4$IEEE trans.Inform.Theory 42 (1996),1594-1600.

[58] V.Pless,P.Solé and Z.QianCyclic self-dual $\mathbb{Z}_4$ codes Finite Fields Appl. 3 (1997),48-69.

[59] J. Wolfmann, Negacyclic and cyclic codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory, 45(7) 2522–2532, Nov. 1999.

[60] J. L. Yucas and G. L. Mullin, Self-reciprocal irreducible polynomials over finite fields, Designs, Codes, Crypt., 33(3) 275–281, 2004.

[61] O. Zariski and P. Samuel, Commutative Algebra. New York : Van Nostrand, 1958