REPUBLIQUE DU CAMEROUN
****
Paix-Travail-Patrie
****
UNIVERSITE DE YAOUNDE I
****
ECOLE NORMALE SUPERIEURE
DE YAOUNDE
****
DEPARTEMENT DE MATHEMATIQUES
****

N
E S

REPUBLIC OF CAMEROON
****
Peace-Work-Fatherland
****
UNIVERSITY OF YAOUNDE I
****
HIGHER TEACHER TRAINING
COLLEGE OF YAOUNDE
****
DEPARTMENT OF MATHEMATICS
****

CODES QUASI-CYCLIQUES SUR UN ANNEAU DE GALOIS

Mémoire de DI.P.E.S II de mathématiques

De

MBOK NDEBE Jacques Divine

***Matricule :* 08V0293**

Licencié en Mathématiques

Sous la direction de :

Pr MOUAHA Christophe

Maître de Conférences

Ecole Normale Supérieure, Université de Yaoundé I

Année académique : 2015-2016

CODES QUASI-CYCLIQUES SUR UN ANNEAU DE GALOIS .

MBOK NDEBE Jacques Divine

Matricule : **08V0293**

Licencié en Mathématiques pures

dirigé par le

Pr MOUAHA Christophe

Maitre de Conférences

Année Académique 2015-2016

♣ Dédicace ♣

À

Mes parents madame et monsieur **NDEBE**.

♣ Remerciements ♣

Je tiens à remercier l'éternel Dieu tout puissant pour le courage et la clairvoyance qu'il m'a donné pour mettre sur pied ce mémoire. La rédaction de ces lignes me fournit l'occasion d'exprimer ma joie d'avoir été entouré pendant toutes ces années de personnes d'une très grande richesse. Que tous trouvent ici l'expression de ma gratitude.

Ma gratitude va particulièrement au Pr Christophe MOUAHA dont la disponibilité, la pertinence des remarques et la sagacité ont été d'un apport à ne pas oublier. Il a toujours trouvé du temps à consacrer à ce travail malgré ses multiples occupations.

► Je tiens également à remercier tous les enseignants de Mathématiques de L'Université de Yaoundé I pour leur enseignement.

► Je remercie mes camarades de promotion pour leur soutien morale, académique et surtout pour leur esprit de solidarité en particulier KALDJOB KALDJOB Paul, FOUOTSA Boris, NJOUPOUAMIMCHE , SAMADINE DJALLO, GUEUDEH Franklin, KAM TSEMO, KUETE Duplex et TCHIO Serge .

► Je tiens très fortement à remercier toute ma famille en particulier mes parents monsieur et madame NDEBE, mes soeurs NDEBE Ester, NDEBE Christine et NDEBE jeanne.

► Ma gratitude va à l'endroit de ma très chére MPONGUE SOUME Gaelle pour son soutien matériel et moral, merci d'être avec moi dans les bons et les mauvais moments.

► Ma gratitude va également à l'endroit de Mme NGONO Anastasie, M MOUDIO DIBOBE Eric, M YATOU Sylvain et M NKINGUE Pascal pour leur encouragement et pour leur assistance morale et matérielle.

► Je remercie tous mes amis pour les conseils et les encouragements qu'ils ont apportés à mon endroit pendant toute ma formation.

► Je remercie enfin ceux qui de prés ou de loin ont contribué à ma formation et à la réalisation de ce travail.

Que ceux qui ne sont pas cités, trouvent dans ce travail l'expression de toute ma reconnaissance et ma profonde gratitude.

♣ Déclaration sur l'honneur ♣

Le présent travail est une oeuvre originale du candidat et n'a été soumis nulle part ailleurs, en partie ou en totalité, pour une autre évaluation académique. Les contributions externes ont été dument mentionnées et recensées en bibliographie.

Signé,
MBOK NDEBE Jacques Divine

♣ Résumé ♣

les codes s-quasi-cycliques sont des codes stables par l'action du décalage circulaire de s positions. Ils sont en fait une généralisation des codes cycliques (s=1).
Dans notre travail, nous nous intéressons aux codes quasi-cyclique de longueur $n = ls$ sur un anneau de Galois. Notre motivation de prime à bord est de généraliser les résultats obtenus sur les codes cycliques tels que la représentation polynômiale et la caractérisation des codes quasi-cycliques à base cyclique, ensuite nous montrons que les codes quasi-cycliques sur $GR(p^m, r)$ sont des $GR(p^m, r)$-sous-modules de $GR(p^m, r)^n$ et enfin, nous aborderons la notion des codes quasi-cycliques à base cyclique.

Mots clés : Codes, Anneau de Galois, Matrice génératrice, Code cyclique, Code quasi-cyclique, Relèvement de Hensel.

♣ Abstract ♣

s-quasi-cyclic codes are stable codes by the action of circular shifts of position of cyclic codes (s=1).In our work, we are interested in quasi-cyclic codes of length $n = ls$ on Galois ring. our primary motive is to generalize the results obtained on cyclic codes such as the polynomial repeesentation and the characterisation of the quasi)cyclic codes based on cyclic next, we show that quasi-cyclic codes on $GR(p^m, r)$ are $GR(p^m, r)$- sub module of $GR(p^m, r)^n$ and finaly , we discuss the notion of quasi-cyclic codes based on cyclic.

Keywords : Codes, Galois ring, Generator matrix, Cyclic code, Quasi-cyclic code, Hensel lift.

♣ Table des matières ♣

♣ Introduction générale ♣

En 1623, Francis Bacon constatait qu'un homme pouvait s'exprimer à distance au moyen de signes binaires. Mais il fallut attendre 1948, et les publications de Claude Shannon, pour que s'établisse une théorie, connue sous le nom de théorie de l'information. Cette théorie fit disparaitre "les bricolages astucieux" aux idées quelque fois préconçues, pour laisser place à de vraies techniques scientifiques.

Un des problème majeur que Shannon ([7]), étudia est la garantie d'une communication fiable, en présence des bruits. 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 communications numériques mais, le problème de la construction de "bon code" reste toujours d'actualité. Les interférences téléphoniques lors des communications et la protection des informations financières ont poussé à l'émergence des études sur le codage qui, se veut également une solution pour le problème de détection, et de correction d'erreurs de transmissions causées par les perturbations survenues sur le canal. La théorie de code correcteurs, et donc des codes linéaires au centre des préoccupations, s'est d'abord développée sur des corps finis. Ce qui fait aujourd'hui de la théorie de codage une branche active des mathématiques.

En 1994, Hammons, Kumar, Calderbank, Sloene et Solé ([11]), découvrent que plusieurs codes binaire non linéaire possédant de meilleurs propriétés proviennent des codes linéaires sur les anneaux de Galois via l'application de gray. ceci dégage encore un intérêt capital accordé à l'étude des codes linéaires sur un anneau de Galois. Notre travail qui porte sur l'étude des codes quasi-cycliques sur un anneau de Galois sera structuré comme suit :

Le chapitre premier est basé essentiellement sur les propriétés d'un anneaux de Galois, qui sont l'alphabet du codage utilisé dans notre travail. Nous montrons qu'un corps finis est un corps résiduel d'un anneau de Galois et nous parlerons du relèvement de Hensel qui est d'un intérêt capital.

Le deuxième chapitre est porté sur les propriétés algébriques et métriques des codes linéaires sur un anneau de Galois. Nous abordons partiellement les notions d'encodage ,de décodage et de correction d'erreurs par la distance minimale. Enfin nous faisons un études des codes cycliques sur un anneau de Galois.
Enfin dans le troisième chapitre nous faisons une étude des codes quasi-cycliques sur un anneau de Galois en généralisant quelques résultats obtenus des codes cycliques, puis nous donnons une caractérisation des codes quasi-cycliques à base cycliques et nous aborderons la notion de code quasi-cyclique à base cyclique.

⋆ ⋆ Chapitre Un ⋆ ⋆

ANNEAUX DE GALOIS

1.1 Préliminaires

Définition 1.1.1. *On appelle anneau la donnée d'une structure algébrique* $(A, +, \times)$ *qui vérifie les propriétés suivantes :*
- $(A, +)$ *est un groupe abélien*
- $(A, \times)$ *est un magma associatif , c'est a dire que pour tous a,b et c dans A ,*
on a, $a \times (b \times c) = (a \times b) \times c$
- $\times$ *est distributif par rapport à* $+$ *c'est a dire pour tous a,b et c dans A,*
on a, $a \times (b + c) = a \times b + a \times c$ *et* $(a + b) \times c = a \times c + b \times c$
De plus, si la multiplication est commutative on dit que l'anneau est commutatif. s'il existe un élément $1_A \in A$ *tel que pour tout* $a \in A, 1_A \times a = a \times 1_A = a$ *(où* 1_A *est l'élément neutre pour la multiplication) on dit que l'anneau est unitaire.*

Exemple 1.1.1. $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{Z}_n, \overline{+}, \overline{\times})$, sont des anneaux commutatifs unitaires.

Définitions 1.1.1. *Soient A un anneau commutatif,* $a \in A$ *et* $b \in A$.
i) L'élément a est un diviseur de zero si $a \neq 0_A$ *et s'il existe* $x \neq 0_A$ *tel que* $ax = 0_A$.
ii) L'élément b divise a si $a \in bA$.
iii) Si A est unitaire d'élément d'unité 1_A*, un élément a de A est dit inversible si* $1_A \in aA$*, dans ce cas on note* $A^\times = \mu(A)$*,l'ensemble des éléments inversibles de A.*
iv) L'élément $a \in A$ *est dit nilpotent s'il existe* $n \in \mathbb{N}^*$ *tel que* $a^n = 0_A$.
v) L'élément $a \in A$ *est dit régulier si* $a \neq 0_A$ *et pour tous* $x, y \in A$ $ax = ay$ *implique* $x = y$
vi) L'entier $n = \min\{k \in \mathbb{N}^*, a^k = 0_A\}$ *est l'indice de nilpotence de a.*

Notation 1.1.1. *$\eta(A)$ désigne l'ensemble des éléments nilpotents de A.*

Exemple 1.1.2. On a $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, ..., \overline{5}\}$, alors :
- $2, 3 \in \mathbb{Z}_6$ et $2 \times 3 = 0$; donc 2 et 3 sont les diviseurs de zero de $\mathbb{Z}_6$.
- Dans $\mathbb{Z}_6$, on a $2 = 2 \times 4$ donc 2 et 4 divisent 2.
- $\mu(\mathbb{Z}_6) = \{1, 5\}$
- Dans $\mathbb{Z}_8$, il est clair que $4 \in \mathbb{Z}_8$ et on a $4^3 = 8^2 = 0$. Donc 4 est un élément nilpotent d'indice 3.

Proposition 1.1.1. *Soit A un anneau commutatif et unitaire. Alors*
i) Tout élément nilpotent de A est diviseur de zéro.
ii) Si A est fini, alors tout élément a de A est inversible si et seulement s'il est régulier.

Preuve. *i)* soit $a \in A$ un élément nilpotent, alors $a \neq 0_A$ et il existe $n \in \mathbb{N}^*$ tel que $a^n = 0_A$, on a $aa^{n-1} = 0_A$. Si $a^{n-1} = 0_A$ cela contredit la minimalité de l'indice de nilpotence de a. Ainsi, $a^{n-1} \neq 0_A$, $a \neq 0_A$ et $aa^{n-1} = 0_A$. Donc a est un diviseur de zéro.
ii) $\Longrightarrow$) Soit $a \in A$ un élément inversible de A. On a $a \neq 0_A$ car 0_A n'est pas inversible . Pour tous $x; y \in A$ tel que $ax = ay$ on a :

$$\begin{aligned} x &= (a^{-1}a)x \\ &= a^{-1}(ax) \\ &= a^{-1}(ay) \\ &= (a^{-1}a)y \\ &= y \end{aligned}$$

D'où a est régulier.
$\Longleftarrow$) Soit $a \in A$ un élément régulier de A. Montrons que a est inversible.
considérons l'application $g_a : A \longrightarrow A$ telle que $g_a(x) = ax$. g_a dispose de deux identités à savoir $g_a(x + y) = g_a(x) + g_a(y)$ et $bg_a(x) = g_a(xb)$ pour tous $x, y, b \in A$. Ces deux identités font de $g_a(A)$ un idéal de A. En outre ; g_a est une application injective. En effet, soient $x, y \in A$ tels que $g_a(x) = g_a(y)$. On a $ax = ay$ ce qui implique $x = y$ car a est un élément régulier de A. D'où g_a est injective. De ce fait $g_a(A)$ est un idéal de A isomorphe de A ce qui donne $g_a(A) = A$. Or $g_a(A) = aA$, par suite ,$aa = A$. Comme $1_A \in A = aA$ alors $1_A = ax$, $x \in A$ ce qui fait de a un élément inversible.■

Définition 1.1.2. *soit A un anneau, un sous ensemble I de A est un idéal de A si les condition suivante sont vérifiées :*

- *pour tous $a, b \in I$, $a - b \in I$*
- *pour tout $a \in I$ et tout $x \in A$, $ax, xa \in I$*

Proposition 1.1.2. *Soit A un anneau commutatif et unitaire. Alors,*
1) *$\eta(A)$ est un idéal de A.*
2) *$\eta(A)$ est l'intersection de tous les idéaux premiers de A.*

Preuve. ([3])

Définition 1.1.3. *Soit A un anneau commutatif et unitaire.*
la caractéristique de A est définie comme suit :
(i) Si $\{k \in \mathbb{N}^* : k.1_A = 0_A\} = \emptyset$: alors $Caract(A) = 0$.
(ii) Sinon $caract(A) = \min\{k \in \mathbb{N}^* : k.1_A = 0_A\}$.

Exemple 1.1.3. $caract(\mathbb{Z}_n) = n, \forall n \geq 2$ et $caract(\mathbb{Z}) = 0$

Proposition 1.1.3. *Soit A un anneau commutatif et unitaire de caractéristique n. Alors il existe un unique monomorphisme d'anneaux unitaires de $\mathbb{Z}_n$ vers A.*

Preuve. ([3])

Proposition 1.1.4. *Soit A un anneau commutatif et unitaire de caractéristique n. Alors A possède un unique sous-anneau unitaire isomorphe à $\mathbb{Z}_n$.*

Preuve. L'application $\alpha : \mathbb{Z}_n \longrightarrow A$ telle que $\alpha(\bar{k}) = k.1_A$ est un monomorphisme d'anneaux unitaires, d'après la proposition 1.1.3. $\alpha(\mathbb{Z}_n)$ est l'unique sous-anneau unitaire de A.■

Définition 1.1.4. *Soit A un anneau commutatif et unitaire de caractéristique n. L'anneau $\mathbb{Z}_n$ est appelé sous-anneau premier de A.*

Remarque: 1.1.1. la caractéristique de A est le cardinal du sous anneau unitaire premier de A.

Définition 1.1.5. *Soit A un anneau commutatif et unitaire et I un idéal de A. Alors l'idéal I est dit maximal parmi les idéaux de A si $I \neq A$ et pour tout idéal J de A tel que $I \subseteq J \subseteq A$ on a $I = J$ ou $J = A$.*

Exemple 1.1.4. *i*) Les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$, p premier.
ii) Dans $\mathbb{Z}_8$, $\mathbb{Z}_8 = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$ est l'idéal maximal.

Théorème 1.1.1. *Soit A un anneau non nul. Alors tout idéal I de A distinct de A est contenu dans un idéal maximal de A.*

Preuve. Soit I un idéal à gauche de A tel que $I \neq A$.
Considérons $S = \{J\text{idéal à gauche de}A/I \subseteq J\}.S \neq \emptyset$ car $I \in S$ ordonnons S par l'inclusion.
Soit $\tau = \{C_\lambda/\lambda \in \Lambda\}$ chaine de S. Posons $C = \bigcup_{\lambda\in\Lambda} C_\lambda$, $C = \emptyset$.
Si $a, b \in C$ alors $\exists i; j \in \Lambda$ tels que $a \in C_i$,$b \in C_j$; or $C_i \subseteq C_j$ ou $C_j \subseteq C_i$. Donc $a-b \in C_i$ ou $a, b \in C_j$ c'est à dire $a - b \in C$. De plus, si $\gamma \in A$, $\gamma_a \in C_i$; i.e $\gamma_a \in C = \bigcup_{\lambda\in\Lambda} C_\lambda$.
D'où $C = \bigcup_{\lambda\in\Lambda} C_\lambda$ est idéal à gauche de A. Comme $I \subseteq C_i$, $\forall i \in A$, il vient que $I \subseteq \bigcup_{\lambda\in\Lambda} = C_\lambda = C$. D'autre part, $C_i \neq A, \forall i \in A$ implique que $1_A \notin C_i$, $\forall i \in \Lambda$. D'où $1_A \notin \bigcup_{\lambda\in\Lambda} C_\Lambda = C$. c'est à dire $C \neq A$. Donc $C \in S$ et $C_i \subseteq C$, $\forall i \in \Lambda$. c'est à dire C est un majorant de τ dans S, d'après la lemme de Zorn, S possède au moins un élément maximal, c'est à dire A possède au moins un idéal à gauche maximal J tel que $I \subseteq J \subseteq A$.■

Corollaire 1.1.1. *Soit A un anneau commutatif et unitaire. pour qu'un élément de A soit inversible il faut et il suffit qu'il n'appartienne à aucun idéal maximal.*

Preuve. $\Longrightarrow$) Soit $a \in A$ un élément inversible. Il existe $b \in A$ tel que $ab = 1_A$, si M est un idéal maximal de A contenant a on aura $1_A = ab \in M$ car M est un idéal d'où $M = A$ ce qui contredit le fait que M soit un idéal maximal de A. Donc a n'appartient à aucun idéal maximal de A.
$\Longleftarrow$) Soit $a \in A$ un élément de A qui n'appartient à aucun idéal maximal de A. si on suppose que a n'est pas inversible, alors $aA = A$, (Sinon avec $aA = A$,
comme $1_A \in A = aA$ alors $1_A = ax$, $x \in A$ ce qui fera de a un élément inversible) Or avec $aA \neq A$, il vient que aA est un idéal maximal de A distinct de A d'après la proposition 1.1.4, $aA \subseteq M$ où M est un idéal maximal de A. par conséquent $a \in M$ puisqu'en particulier pour $1_A \in A$, $a = a1_A \in M$ ce qui contredit $a \in T$ pour tout T idéal maximal de A. D'où a est inversible. ■

Définition 1.1.6. *un anneau commutatif unitaire est dit local s'il possède un unique idéal maximal.*

Notation 1.1.1. Si A est un anneau local, on désigne par m_A son idéal maximal.

Exemple 1.1.5. soit $n \in \mathbb{N}^*$, p un nombre premier. Alors l'anneau $\mathbb{Z}_{p^n}$ est un anneau local d'idéal maximal $p\mathbb{Z}_{p^n}$ et de corps résiduel $\mathbb{Z}_p$.

Proposition 1.1.5. *Soit A un anneau commutatif unitaire. Alors les assertions suivantes sont équivalentes :*

i) A est anneau local ;
ii) $A\backslash A^{\times}$ *le complémentaire du groupe multiplicatif* $A^{\times}$ *est un idéal maximal ;*
iii) les diviseurs de zéro de A forment un idéal.

Preuve. ([3])

Proposition 1.1.6. *Si A est un anneau local fini, alors* $m_A = \eta(A)$.

Preuve. Soit P un idéal premier de A. Alors A/P est un corps et par la suite P est un idéal maximal. Ainsi, $P = m_A$ car m_A est l'unique idéal maximal. Puisque $\eta(A)$ est l'intersection de tous les idéaux premiers de A on a :
$\eta(A) = m_A \cap m_A \cap ... \cap m_A = m_A$ donc $m_A = \eta(A)$.■

Proposition 1.1.7. *Si A est un anneau local fini, alors l'idéal maximal de A est formé de diviseurs de zéro dans A.*

Preuve. Soit $DZ(A)$ l'ensemble des diviseurs de zero de A alors, d'après la proposition 1.1.5. $DZ(A)$ est un idéal, qui est contenu dans l'unique idéal maximal m_A.
De plus, les éléments de $m_A = \eta(A)$ sont tous des diviseurs de zero, donc des éléments de $DZ(A)$. Il en résulte que $m_A = \eta(A) = DZ(A)$.■

Remarque: 1.1.2. Si A est un anneau local, on considère dans toute la suite, l'épimorphisme canonique

$$\begin{array}{rccl} \pi & : & A & \longrightarrow \overline{A} = A/m_A \\ & & a & \longmapsto a + m_A \end{array}$$

Proposition 1.1.8. *Soit A est un anneau local fini, alors* $caract(A) = p^n$, *avec* $n \in \mathbb{N}^*$ *et p un entier premier.*

Preuve. considérons l'application $\alpha : \mathbb{Z} \longrightarrow A$ telle que $\alpha(k) = k1_A$ et $\pi \circ \alpha : \mathbb{Z} \longrightarrow \overline{A}$ telle que $\pi \circ \alpha(k) = \overline{k.1}_A$. α et $\pi \circ \alpha$ sont des morphismes d'anneaux unitaires.
$caract(\overline{A}) = p$ avec p entier premier. $Ker(\alpha)$est un idéal de $\mathbb{Z}$ d'où il existe $n_0 \in \mathbb{N}^*$ tel que $Ker(\alpha) = n_0\mathbb{Z}$. Or $Ker(\alpha) \subseteq Ker(\pi \circ \ \alpha)$, d'où p divise n_0. Ainsi, p divise $caract(A)$. Si q est un autre nombre premier qui divise $caract(A)$ alors $n_0 = qt$. Par suite $\alpha(n_0) = \alpha(q)\alpha(t)$. Si $\alpha(t) = 0_A$, alors q divise 1_A ce qui est absurde car q est premier. Ainsi, $\alpha(t) \neq 0_A$ d'où $\alpha(q)$ est un diviseur de zero c'est à dire $\alpha(q) \in m_A$ et donc $\overline{\alpha}(q) = \bar{0}_A$, d'où $\pi \circ \alpha(q) = \bar{0}_A$ et ainsi p/q donc $p = q$. D'où il existe $n \in \mathbb{N}^*$, tel que $n_0 = p^n$.■

1.2 Paramètres des anneaux de Galois

Définition 1.2.1. *un anneau de Galois GR est tout anneaux local fini, non intègre tel que $m_{GR} = pGR$ avec p premier et $pGR = \{px/x \in GR\}$.*

Remarque: 1.2.1. le corps résiduel $\overline{GR} = GR/m_{GR}$ d'un anneau de Galois GR est un corps fini. Donc c'est un corps de Galois.

Exemple 1.2.1. $\mathbb{Z}/16\mathbb{Z}$ est un anneau de Galois d'idéal maximal $2\mathbb{Z}/16\mathbb{Z}$ et de corps résiduel $\mathbb{Z}/2\mathbb{Z}$.

Proposition 1.2.1. *Soit GR un anneau de Galois, $caract(GR) = p^n$. Alors,*
Si $1 \leq i \leq j \leq n-1$, alors $p^i x \in p^j GR$ implique que $x \in p^{j-i}GR$.
En particulier si $p^i x = 0$ alors $x \in p^{n-i}GR$.

Preuve. $p^i x \in p^i GR$ alors $\exists y \in GR$ tel que $p^i x = p^j y$
$p^i x = p^j y$ implique que $x = p^{j-i}y$, donc $x \in p^{j-i}GR$.■

Proposition 1.2.2. *Soit GR un anneau de Galois de caractéristique p^n alors pour tout élément non nul x de GR il existe un unique entier $t \in \{1; 2; ...; n-1\}$tel que $x = p^t u$, avec $u \in GR^\times$ et unique seulement en modulo p^{n-t}.*

Preuve. soit $a \in GR$ et $a \neq 0_{GR}$,
- si $a \in GR^\times$ prenons $t = 0$ et $u = a$
- Sinon prenons $h = \max\{i \in [\![\ 1; n-1\ ]\!]; a \in p^i GR\}$. On pose un tel ensemble car on sait au moins que $a \in pGR$. Ainsi , il existe $x \in GR$ tel que $a = p^h x$. si $x \notin GR^\times$ alors il existe $y \in GR$ tel que $x = py$ ainsi, $a = p^{h+1}y$ ce qui contredit le fait que h est maximal. si $x = p^t u = p^t v$; alors $p^t(u - v) = 0_{GR}$, d'après la proposition 1.2.1. $u - v \in p^{n-t}GR$ d'où $u = p^{n-t}\lambda + v$, Réciproquement si $u = p^{n-t}\lambda + v$, alors $p^t u = p^t v$. d'où l'unicité de u modulo p^{n-t}.■

Proposition 1.2.3. *Soit GR un anneau de Galois de caractéristique p^n, alors les idéaux de GR sont principaux et sont sous la forme $p^i GR$, $i = 0; 1; ...; n$.*

Preuve. soit I un idéal propre de GR. posons $B = \{i \in \mathbb{N}; p^i GR \subseteq I\}$, B est une partie non vide de N donc admet un plus petit élément n_0. On a $p^{n_0}GR \subseteq I$. soit $x \in I \subseteq GR$. il existe un unique couple $(h; u) \in \{0; 1; ...; n\} \times GR^\times$ tel que $x = p^h u$. On a $p^h 1_G R = xu^{-1} \in I$ d'où $p^h GR \subseteq I$ on a $n_0 \leq h$ et ainsi $x = p^h u = p^{n_0}(p^{h-n_0}) \in p^{n_0}GR$ d'où $I = p^{n_0}GR$.■

Définition 1.2.2. *(Modules) Soit A un anneau commutatif, un A- Module $(M,+,.)$ est un ensemble équipé d'une loi interne $+$ et d'une loi externe $.$ vérifiant :*

• $(M,+)$ *est un groupe abélien.*

• *On a en plus les quatre propriétés suivantes :*

1. $\alpha(m+m') = \alpha m + \alpha m'$
2. $(\alpha+\beta)m = \alpha m + \beta m$
3. $(\alpha\beta)m = \alpha(\beta m)$
4. $1.m = m.$

Pour tous $m, m' \in M$ et tous $\alpha, \beta \in A$.

Définition 1.2.3. *Soit M un A-Module, un sous-module N de M est un sous-groupe de $(M,+)$ qui est stable par la multiplication externe par tout élément de A.*
Autrement dit une partie N du A-module M est un sous-module si et seulement s'il contient 0 et si pour tous x, y de M et pour tout α de A on a $x+y \in N$ et $\alpha m \in N$.

Définition 1.2.4. *Un A-Module M est dit de type fini s'il est engendré par nombre fini d'élément c'est à dire il existe $x_1, ..., x_n \in M$ tel que $M = \sum_{i=1}^{n} Ax_i$; où $n \geq 1$*

Exemple 1.2.2. - On a $A = A1$ c'est à dire $A = (1)$ donc A est A-module fini.
- plus généralement, pour tout $n \geq 1$ la somme directe $A^n = \{(a_1, ..., a_n)/a_i \in A\}$ est un A-module de type fini.

Définition 1.2.5. *Soit M un A-module un sous ensemble B de M est une partie libre si tout les éléments de B sont linéairement indépendants sur A. C'est à dire $\forall n \geq 1$, $\forall \beta_1, ..., \beta_n$, où les β_i sont deux à deux distincts.*
$\sum_{i=1}^{n} a_i\beta_i = 0 \Longrightarrow a_i = 0,\ \forall i$

Définition 1.2.6. *Soit M un A-module un sous ensemble B est une base de M si :*
1) *B engendre M c'est à dire tout élément non nul m de M est une combinaison linéaire d'élément fini de B. Ainsi $m = \sum_{i=1}^{n} a_i\beta_i$*
2) *B est une partie libre.*

Remarque: 1.2.2. 1) et 2) de la définition précédente entraine que tout élément non nul m de M s'écrit de façon unique sous la forme :
$m = \sum_{i=1}^{n} a_i\beta_i$ avec $n \geq 1$,$a_i \in A$ et $\beta_i \in B$.

Définition 1.2.7. *un A-module M est dit libre s'il possède une base.*

Exemple 1.2.3. *i)* A est A-module libre car il possède la base 1.
ii) $A^n = \{(a_1, ..., a_n)/a_i \in A\}$ est un A-module libre car il possède la base $B = (e_1, ..., e_n)$.
Où $e_1 = (1, 0, ..., 0), e_2 = (0, 1, 0, ..., 0)...e_n = (0, 0, ..., 1)$.
1

Lemme 1.2.1. *Soit GR un anneau de Galois de caractéristique p^n,alors GR est une extension simple de $\mathbb{Z}_{p^n}$.*

Preuve. $\overline{GR}$ le corps résiduel de GR est fini d'où $\overline{GR} = F_p[\overline{\alpha}]$
avec $F = \mathbb{Z}_{p^n}$, $F_p = \overline{F} \cong \mathbb{Z}_p$, $F_p = F/pF$.
Comme $\overline{GR} = F_p[\overline{\alpha}]$ on $\{1, \overline{\alpha}, ..., \overline{\alpha}^{r-1}\}$ est une F_p- base de $\overline{GR}$.
Soit $x \in GR$, alors $x + m_{GR} \in \overline{GR}$.

$$\begin{aligned} x + m_G R &= \sum_{i=0}^{r-1} \overline{\lambda}_i \overline{\alpha}^i \ avec\ \overline{\lambda}_0, ..., \overline{\lambda}_{r-1} \in F_p \\ &= \sum_{i=0}^{r-1} (\lambda_i + pF)(\alpha + m_{GR})^i \\ &= \sum_{i=0}^{r-1} (\lambda_i \alpha^i + \lambda_i m_{GR} + pF\alpha^i + pF m_G R) \end{aligned}$$

D'où $x - \sum_{i=0}^{r-1} \lambda_i \alpha^i \in m_{GR} + p\mathbb{Z}_{p^n} G$, par suite $x \in \mathbb{Z}_{p^n}[\alpha] + p\mathbb{Z}_{p^n} GR$.
Ainsi $GR = \mathbb{Z}_{p^n}[\alpha] + p\mathbb{Z}_{p^n} GR$.
D'après le lemme 1.2.1. précédant on a donc $GR = \mathbb{Z}_{p^n}[\alpha]$. ■

Proposition 1.2.4. *Soient GR un anneau de Galois de caractéristique p^n et $\alpha \in GR$ alors $GR = \mathbb{Z}_{p^n}[\alpha]$ si et seulement si $\overline{GR} = \overline{\mathbb{Z}}_{p^n}[\overline{\alpha}]$.*

Preuve. $\Longleftarrow$) Soit $\overline{GR} = \overline{\mathbb{Z}}_{p^n}[\overline{\alpha}]$. D'après la preuve de la proposition on a $GR = \mathbb{Z}_{p^n}[\alpha]$.
$\Longrightarrow$) supposons $GR = \mathbb{Z}_{p^n}[\alpha]$.
Soit $\overline{x} \in \overline{GR}$, alors $\overline{x} = x + m_{GR}$, avec $x \in GR = \mathbb{Z}_{p^n}[\alpha]$ d'où on a :

$$\begin{aligned} \overline{x} &= x + m_{GR} \\ &= \sum_{i=0}^{r-1} \lambda_i \alpha^i + m_{GR} \\ &= \sum_{i=0}^{r-1} (\lambda_i + p\mathbb{Z}_{p^n})(\alpha^i + m_{GR}) \\ &= \sum_{i=0}^{r-1} (\lambda_i + p\mathbb{Z}_{p^n})(\alpha + m_{GR})^i \\ &= \sum_{i=0}^{r-1} \overline{\lambda}_i \overline{\alpha}^i \ avec\ \lambda_i \in \mathbb{Z}_{p^n} \end{aligned}$$

Donc $\overline{GR} = \overline{\mathbb{Z}}_{p^n[\overline{\alpha}]}$

Proposition 1.2.5. *Soit GR un anneau de Galois de caractéristique p^n.*
GR est $\mathbb{Z}_{p^n}$-module libre.

Preuve. puisque $GR = \mathbb{Z}_{p^n}[\alpha]$ il est clair que GR est un $\mathbb{Z}_{p^n}$-module libre.

Proposition 1.2.6. *Soit GR un anneau de Galois de caractéristique p^n, alors son cardinal est égal à p^{nr} et on note $\mid GR \mid = p^{nr}$, où $r \in \mathbb{N}^*$.*

Preuve. De ce qui précède GR est un $\mathbb{Z}_{p^n}$-module libre.
soit $\{1_{GR}, \alpha, ..., \alpha^{r-1}\}$ une $\mathbb{Z}_{P^n}$-base de GR. Alors $GR \cong (\mathbb{Z}_{p^n})^r$ d'où on a :

$$\begin{aligned} \mid GR \mid &= \mid (\mathbb{Z}_{p^n})^r \mid \\ &= \mid \mathbb{Z}_{p^n} \mid^r \\ &= (p^n)^r \ car \mid \mathbb{Z}_{p^n} \mid = p^n \\ &= p^{nr}.\blacksquare \end{aligned}$$

On obtient ainsi une représentation additive des éléments de GR pour tout $x \in GR$, $x = \sum_{i=o}^{r-1} \lambda_i \alpha^i$, avec $\lambda_i \in \mathbb{Z}_{p^n}$.

Proposition 1.2.7. *Un anneau de Galois GR de caractéristique p^n et de cardinal p^{nr} est unique à isomorphisme près.*

Preuve. Soit GR' un autre anneau de Galois de caractéristique p^n et de cardinal p^{nr} il ressort que $\overline{GR}$ et $\overline{GR'}$ sont des corps finis isomorphes. Soient $\overline{\alpha}$ et $\overline{\alpha'}$ les générateurs respectifs de $\overline{GR}$ et $\overline{GR'}$, alors $GR = \mathbb{Z}_{p^n}[GR]$ et $GR' = \mathbb{Z}_{p^n}[GR']$ sont isomorphes.

1.2.1 Une description polynomiale des anneaux de Galois

soit

$$\begin{aligned} \Pi : \ GR &\longrightarrow \overline{GR} \\ x &\longmapsto x + m_{GR} \end{aligned}$$

un épimorphisme canonique d'anneaux de Galois alors on peut l'étendre a un épimorphisme canonique d'anneaux des polynômes définit par :

$$\begin{aligned} \varphi : \ GR[X] &\longrightarrow \overline{GR}[X] \\ f &\longmapsto f + (P) \end{aligned}$$

Définition 1.2.8. *Un B-polynôme $g \in GR[X]$ est un polynôme irréductible unitaire tel que $\pi(f)$ soit primitif sur $\overline{GR}$.*
L'anneau $\mathbb{Z}_{p^n}[X]/(f)$ est un anneau de Galois de caractéristique p^n et de cardinal égal à p^{nr} où f est un B- polynôme de degré r.

Notation 1.2.1. *Dans la suite on notera par $GR(p^n, r)$ tout anneau de Galois isomorphe à $\mathbb{Z}_{p^n}[X]/(f)$ où $f(X) \in \mathbb{Z}_{p^n}[X]$ est un B-polynôme de degré r*

1.3 Relèvement de Hensel ([6])

Lemme 1.3.1. *soient p un nombre premier ; k un entier naturel supérieure ou égal à 2 et $P \in \mathbb{Z}_{p^k}[X]$ un polynôme unitaire, tel que*
$P \equiv QR(modp)$
pour $Q, R \in \mathbb{Z}_p[X]$, deux polynômes unitaire première entre eux, 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. $Q^{(k)} \equiv Q(modp)$ *et* $R^{(k)} \equiv R(modR)$,
3. $Q^{(k)}$ *et* $R^{(k)}$ *sont premiers entre eux.*
De plus, on a $deg(Q^{(k)}) = deg(Q)$ et $deg(R^{(k)}) = deg(R)$.
$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ est un corps car $p\mathbb{Z}$ est un idéal maximal de $\mathbb{Z}$ ainsi $\mathbb{Z}_p[X]$ est un anneau principal et donc factoriel. Par conséquent, tout les polynômes a coefficient dans $\mathbb{Z}_p$ se décompose de façon unique en produit de facteur irréductibles, c'est à dire, pour tout polynômes $P \in \mathbb{Z}_{p^k}[[X]$, P s'écrit :
$P \equiv f_1^{k_1} f_2^{k_2} ... f_l^{k_l}(modp)$ où $f_1, ..., f_l$ sont des polynômes irréductibles de $\mathbb{Z}_p[X]$ et $k_1, ..., k_l$ sont des entiers strictement positifs. D'après ce qui précède, on peut généraliser le lemme de Hensel par récurrence sur le nombre des facteurs 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 1.3.1. *soient p un nombre premier, k un entier supérieure ou égal à 2 et $P \in \mathbb{Z}_{p^k}[X]$ un polynôme irréductible, tel que :*
$P \equiv f_1^{k_1} ... f_l^k(modp)$ la factorisation de P dans $\mathbb{Z}_p[x]$, où $f_1, ..., f_l$ sont des polynômes irréductibles et $k_1, ..., k_l$ sont des entiers strictement positifs. Il existe un unique l-uplet $(g_1^{(k)}, ..., g_l^{(k)})$ de polynômes unitaires de $\mathbb{Z}_{p^k}[X]$, tel que
1. $P = g_1^{(k)} ... g_l^{(k)}$,
2. $g_i^{(k)} \equiv f_i^{(k)}(modp)$,
3. *les* $g_i^{(k)}$ *sont deux à deux premiers entre eux.*
Le théorème ci dessus permet de constater que, les polynômes de $\mathbb{Z}_{p^k}[X]$ se décomposent de façon unique en produit de polynômes du type des $g_i^{(k)}$, sont tel que réduits modulo p sont des puissances de polynômes irréductibles de $\mathbb{Z}_p[X]$. cette propriété va nous permettre de définir le relevé de Hensel d'un facteur de $X^n - 1$, où n et p sont premier entre eux.

Dans un tel cas, X^n-1 ne possède que des facteurs simples.

Définition 1.3.1. *soient Q et R deux polynômes de $\mathbb{Z}_p[X]$ tels que $X^n-1=Q(X)R(X)$ où n et p sont premiers entre eux. On appelle relevé de Hensel d'ordre k du polynôme Q, le polynôme $Q^{(k)}$ du couple $(Q^{(k)},R^{(k)})$.*

Proposition 1.3.1. *Soit $Q\in\mathbb{Z}_p[X]$, un facteur de X^n-1. Son relevé de Hensel d'ordre k divise X^n-1 dans $\mathbb{Z}_{p^k}[X]$.*

Preuve. Ceci découle du fait que $X^n-1=Q^{(k)}(X)R^{(k)}(X)$ dans $\mathbb{Z}_{p^k}[X]$. Dans la suite le cas $p=2$ fera l'objet de notre préoccupation.

Proposition 1.3.2. *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 $Q^{(k+1)}(X)=\pm(P^2(x^2)-I^2(X))$, les opérations étant faites dans $\mathbb{Z}_2^{k+1}[X]$ et le signe étant choisi pour que $Q^{(k+1)}$ soit unitaire.

Preuve. ([7]) Par construction, $P^2(X)-Q^2(X)$ n'a que des monômes de degré pair, le polynôme unitaire $f(X)\in\mathbb{Z}_{2^{k+1}}[X]$ tel que $f(X^2)=\pm(P^2(X)-Q^2(X))$ est bien défini.
On a $f(X^2)\equiv\pm(P(X^2)-Q(X^2))\equiv Q(X^2)\ (mod 2)$;
Car l'application $R(X)\longrightarrow R^2(X)$ se réduit à $R(X)\longrightarrow R(X^2)$ sur $\mathbb{Z}_2[X]$.
Donc $f(X)\equiv Q(X)(mod 2)$. il reste à vérifier que f divise $X^{2^m-1}-1$ dans $\mathbb{Z}_{2^{k+1}}[X]$.
$f(X^2)=\pm Q^{(k)}(X)Q^{(k)}(X)$ les opérations faites dans $\mathbb{Z}_{2^{k+1}}[X]$. Par hypothèse , $Q^{(k)}$ divise $X^{2^m-1}-1$ dans $\mathbb{Z}_{2^k}[X]$. On peut écrire
$X^{2^m-1}-1=Q^{(k)}(X)\Lambda(X)+2^kB(X)$,
où $\Lambda(X)$ et $B(X)$ sont deux polynômes de $\mathbb{Z}_{2^{k+1}}[X]$. cela nous donne également
$(-X)^{2^m-1}-1=Q^{(k)}(-X)\Lambda(-X)+2^kB(-X)$
Alors

$$\begin{aligned} X^{2^m-2}-1 &= (X^{2^m-1}-1)(X^{2^m-1}+1)\\ &= -(X^{2^m-1}-1)((-X)^{2^m-1}-1\\ &= -Q^{(k)}(X)Q^{(k)}(X)\Lambda(X)\Lambda(-X)-2^k(Q^{(k)}(X)\Lambda(X)B(-X)\\ &\quad -Q^{(k)}(-X)\Lambda(-X)B(X))\end{aligned}$$

Posons $Q^{(k)}=P(X)-I(X)$, $\Lambda(X)=P_a(X)-I_a(X)$ et $B(X)=P_b(X)-I_b(X)$,
où $P(X),P_a(X)etP_b(X)$ ne contiennent que des monômes de degré pair et $I(X)$,
$I_a(X)$ et $I_b(X)$,ceux de degré impair. On a ainsi

$$\begin{aligned}
Q^{(k)}(X)\Lambda(X)B(-X) - Q^{(k)}(-X)\Lambda(-X)B(X) &= (P(X) - I(X))(P_a(X) - I_a(X)) \\
&\times(P_b(-X) - I_b(-X)) \\
&+(P(-X) - I(-X))(P_a(-X) - I_a(-X)) \\
&\times(P_b(X) - I_b(X)) \\
&= (P(X) - I(X))(P_a(X) - I_a(X)) \\
&\times(P_b(X) + I_b(X)) \\
&+(P(X) + I(X))(P_a(X) + I_a(X)) \\
&\times(P_b(X) - I_b(X)) \\
&= 2(P(X)P_a(X)P_b(X) - P(X)I_a(X)I_b(X) \\
&-P_a(X)I(X)I_b(X) + I(X)I_a(x)P_b(X)) \qquad .
\end{aligned}$$

Donc on peut écrire

1.3.1 Exemple d'application

Dans $\mathbb{Z}_2[X]$, $X^7 - 1$ se factorise sous la forme

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

Posons $Q^{(1)} = X^3 + X + 1 \in \mathbb{Z}_2[X]$ et appliquons la proposition précédente pour calculer son relevé d'ordre 3. On a

$$\begin{aligned}
P(X) &= 1 \quad [mod 2] \\
Q(X) &= X^3 + X \quad [mod 2]
\end{aligned}$$

Ainsi

$$\begin{aligned}
Q^{(2)}(X^2) &= \pm(P^2(X) - I^2(X)) \quad [mod 4] \\
&= \pm(1 - X^6 - 2X^4 - X^2) \quad [mod 4] \\
&= X^6 + 2X^4 + X^2 - 1 \quad [mod 4].
\end{aligned}$$

D'où

$Q^{(2)}(X) = X^3 + 2X^2 + X - 1[mod 4]$ est le relevé d'ordre 2 du polynôme Q.

Donc

$GR(2^2, 3) = \mathbb{Z}_4[X]/id(X^3 + 2X^2 + X - 1)$. De même on a

$$\begin{aligned}
Q^{(3)}(X^2) &= \pm((2X^2 - 1)^2 - (X^3 - X)^2) \quad [mod 8] \\
&= \pm(4X^4 - 4X^2 + 1 - X^6 - 2X^4 - X^2) \quad [mod 8] \\
&= \pm(-X^6 + 2X^4 + 5X^2 + 1) \quad [mod 8] \\
&= X^6 - 2X^4 + 5X^2 - 1 \quad [mod 8] \\
&= X^6 + 6X^4 + 5X^2 + 7 \quad [mod 8].
\end{aligned}$$

Ainsi le relevé d'ordre 3 de $X^3 + X + 1$ est :

$f(X) = X^3 + 6X^2 + 5X + 7$ sur $\mathbb{Z}_8[X]$.

Donc

$GR(2^3, 3) = \mathbb{Z}_8[X]/id(X^3 + 6X^2 + 5X + 7)$

On vérifie aisément que

$f(X) \times (X^4 + 2X^3 + 7X^2 + 5X + 1) = X^7 - 1$ $[mod 8]$.

Il ressort que $X^4 + 2X^3 + 7X^2 + 5X + 1$ est le relevé d'ordre 3 de $(X - 1)(X^3 + X^2 + 1)$.

⋆ ⋆ Chapitre Deux ⋆ ⋆

CODES LINÉAIRES SUR UN ANNEAU DE GALOIS

Dans le chapitre précédent nous avons fait une étude sur les anneaux de Galois. Dans ce chapitre nous intéresserons aux codes linéaires sur un anneau de Galois.

2.1 Quelques rappels sur les codes

Dans la suite, on considèrera $GR(p^m, r)$ comme un anneau de Galois de caractéristique p^m et de cardinal p^{mr}

Définition 2.1.1. *un code linéaire de longueur n sur $GR(p^m, r)$ est un $GR(p^m, r)$-sous module de $GR(p^m, r)^n$.*
Si C est un code linéaire sur $GR(p^m, r)$ alors tout élément de C est appelé mot de ce code.

Définition 2.1.2. *On appelle distance de Hamming toute application définit par :*

$$\begin{array}{rccc} d_H : & GR(p^m,r)^n \times GR(p^m,r)^n & \longrightarrow & \mathbb{N} \\ & (x,y) & \longmapsto & \mid \{i \in [\mid 1; n \mid] / x_i \neq y_i\} \mid \end{array}$$

Avec ; $x = (x_1, ..., x_n)$ et $y = (y_1, ..., y_n)$.

Exemple 2.1.1. Soient $a = (1, 1, 1, 0, 1, 0)$ et $b = (1, 0, 1, 1, 0, 0)$ de mots de code de longueur 6 alors leur distance de Hamming est 3,c c'est à dire $d_H(a, b) = 3$.

Définition 2.1.3. *On appelle poids de Hamming d'un mot x l'entier naturel noté $w_H(x)$,où w_H est l'application définie par :*

$$\begin{array}{rccc} w_H : & GR(p^m,r)^n & \longrightarrow & \mathbb{N} \\ & x & \longmapsto & \mid \{i \in [\mid 1; n \mid] / x_i \neq 0\} \mid \end{array}$$

Exemple 2.1.2. En prenant les mots de codes de l'exemple 2.1.1 on a $w_H(a) = 4$ et $w_H(b) = 3$

Remarque: 2.1.1. pour tous $x, y \in GR(p^m, r)^n$ on a :
i) $d_H(x, y) = w_H(x - y)$
ii) $d_H(x, 0) = w_H(x)$.

Définition 2.1.4. *Soit C un code linéaire de longueur n sur $GR(p^m, r)$. On appelle distance minimale ou poids minimal de C l'entier naturel noté d tel que*
$d = min\{w_H(x); x \in C; x \neq 0_c\}$
Nous avons abordé dans le chapitre précédent, les notions de modules de type finis et modules libres. De plus nous savons que les codes linéaires sur les anneaux de Galois sont les sous modules de ces anneaux donc des modules. Le problème qui se pose est celui de savoir si les codes linéaires sur un anneau de Galois sont-ils libres ou fini ?

Proposition 2.1.1. *Les codes linéaires de longueur n sur $GR(p^m, r)$ sont de types finis*

Preuve. Soit C un code linéaire de longueur n sur $GR(p^m, r)$;par récurrence sur n.
Si $n = 1$, alors, C est un $GR(p^m, r)$- sous module de $GR(p^m, r)$, d'où C est un idéal de $GR(p^m, r)$ donc $C = (p^t), t \in [|\ 1, n\ |]$ par conséquent C est de type fini.
Supposons le résultat vrai pour tout entier strictement plus petit que n.
Posons $M_1 = \{(a, 0, 0, ..., 0)\} \in GR(p^m, r)^n / a \in GR(p^m, r)\}$, alors $C_1 = C \cap M_1$ est sous-module de $M_1 \cong GR(p^m, r)$ donc C_1 est de type fini . De plus l'application

$$\begin{array}{rccc} \varphi: & C & \longrightarrow & GR(p^m, r)^n/M_1 \\ & c & \longmapsto & \varphi(c) = \overline{c} \end{array} \text{ telle que}$$

$$\begin{aligned} Ker\varphi &= \{c \in C/\overline{c} = M_1\} \\ &= \{c \in C/c \in M_1\} \\ &= C \cap M_1 \\ &= C_1 \end{aligned}$$

$GR(p^m, r)^n/M_1 \cong GR(p^m, r)^{n-1}$ donc $\varphi(C)$ sous-module de $GR(p^m, r)^n/M_1$ est de type fini par hypothèse de récurrence.
Soit $(\overline{x_1}, \overline{x_2}, ..., \overline{x_k})$ une famille finie engendrée par $\varphi(C)$, $x_i \in GR(p^m, r)$ et $(y_1, ..., y_p)$ une famille finie engendrant C_1 comme φ est linéaire on a donc $(x_1, ..., x_k, y_1, ..., y_p)$ engendre C il en résulte que C est de type fini.■

Nous avons démontré que tout code linéaire de longueur n sur l'anneau $GR(p^m, r)$ est de type fini. Est-il aussi libre ?
Si $n = 1$ considérons les $GR(p^m, r)$-sous-modules du $GR(p^m, r)$-module libre $GR(p^m, r)$, c'est à dire les idéaux de $GR(p^m, r)$.
ces idéaux sont principaux et sont sous la forme $p^i GR(p^m, r)$; où $i \in [|\ 1, m\ |]$ et la condition $p^i\lambda = 0$ n'implique pas toujours $\lambda = 0$. A cause du caractère non intègre de

$GR(p^m, r)$ (en effet pour $\lambda \in m_G R(p^m, r)$, $\lambda \neq 0$ on a $p^{m-1}\lambda = 0$).
On peut conclure que les codes linéaires n'admettent pas toujours de base. Précisons tout de même que le problème est résolu sur les codes linéaires de longueur n sur un anneau principal A, mais notre étude sur les codes linéaires de longueur n sur l'anneau non intègre $GR(p^m, r)$ est enrichi par le module $GR(p^m, r)^n$ qui lui admet un base.

2.2 Matrice génératrice et matrice de contrôle

Un code linéaire de longueur n, de dimension k et de distance minimale d sur corps fini F_q noté $C(n, k, d)$ est sous espace vectoriel de F_q^n donc possède une base, par conséquent sa matrice génératrice est toute matrice $k \times n$ dont les k lignes forment une famille génératrice et libre de C. Cependant un code linéaire de longueur n sur $GR(p^m, r)$ en tant que $GR(p^m, r)$-sous-module de $GR(p^m, r)^n$ est de type fini mais n'admet pas toujours une base. Qu'en est-il de sa matrice génératrice ?

2.2.1 Matrice génératrice

Définition 2.2.1. *la matrice génératrice d'un code linéaire C sur $GR(p^m, r)$ est une matrice dont les lignes forment une famille génératrice minimale de C (engendrent C).*

Exemple 2.2.1. Dans $GR(2^2, 1)$,
$C = \{000, 010, 020, 030, 102, 112, 122, 132, 200, 210, 220, 230, 302, 312, 322, 332\}$ est un sous-module de $GR(2^2, 1)^3$; donc c'est un code linéaire de matrice génératrice

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

Théorème 2.2.1. *([6]) Grâce au caractère libre du $GR(p^m, r)$-module $GR(p^m, r)^n$, tout code linéaire C de longueur n sur $GR(p^m, r)$ possède ,à permutation près, une matrice génératrice dite de forme normale :*

$$G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & . & . & . & A_{0,m} \\ 0 & pI_{k_1} & pA_{1,2} & . & . & . & pA1,m \\ 0 & 0 & p^2 I_{k_2} & p^2 A_{2;3} & . & . & p^2 A_{2,m} \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ 0 & 0 & . & . & . & p^{m-1} I_{k_{m-1}} & p^{m-1} A_{m-1,m} \end{pmatrix} = \begin{pmatrix} A_0 \\ pA_1 \\ p^2 A_2 \\ . \\ . \\ . \\ p^{m-1} A_{m-1} \end{pmatrix}$$

Où les $A_{i,j}$ sont des matrices d'ordres $k_i \times l_j$ à coefficient dans $\{0, 1, ..., p-1\}$ et I_{k_i} est

la matrice identité de taille k_i avec $A_i = (I_{k_i}, A_{i,1}, ..., A_{i,m})$ et $k_m = n - \sum_{i=0}^{m-1} k_i$

on a associe à G la matrice $A = \begin{pmatrix} A_0 \\ A_1 \\ . \\ . \\ . \\ A_{m-1} \end{pmatrix}$ avec $A_i = (i_{k_i}, A_{i,1}, ..., A_{i,m})$,

$p^i A_i = (0, 0, ..., 0, p^i I_{k_i}, p^i A_{i,i+1})$.

Proposition 2.2.1. *Soit C un code linéaire de longueur n sur $GR(p^m, r)$.*
Alors $rg_{GR}(C) = \sum_{i=0}^{m-1} k_i$; où $k_i \in \mathbb{N}^*$.

Preuve. C admet une matrice génératrice G sous la formes normale comme ci-dessus et ainsi $rg_{GR(p^m,r)}(C) = \sum_{i=0}^{m-1} k_i$; où $k_i \in \mathbb{N}^*$ car les k_i lignes sont linéairement indépendants ceci découle du fait que $GR(p^m, r)^{k_i}$ est libre ■.

2.2.2 Matrice de contrôle

produit scalaire

On définit le produit scalaire sur $GR(p^m, r)$ par :
pour tous $x, y \in GR(p^m, r)^n$, $x.y = \sum_{i=0}^{n-1} x_i y_i$.
Il est appelée produit scalaire par abus car elle n'est pas défini positive.

Exemple 2.2.2. Sur $GR(2^3, 1)$, $c = (202) \neq 0$, mais

$$\begin{aligned} c.c &= 4 + 0 + 4 \\ &= 0[mod 8] \end{aligned}$$

Les opérations étant effectuées dans $GR(p^m, r)$. Ce produit scalaire permet de définir une notion de dualité sur $GR(p^m, r)$.

code dual sur $GR(p^m, r)$

Définition 2.2.2. *Soit C un code linéaire de longueur n sur $GR(p^m, r)$. On appelle code dual du code C et on note $C^\perp$, le sous-module de $GR(p^m, r)^n$ définir par :*
$C^\perp = \{x \in GR(p^m, r)^n / \forall y \in C; x.y = 0\}$

Proposition 2.2.2. *$C^\perp$ est un code linéaire de longueur n sur $GR(p^m, r)$.*

Preuve. pour tout $x \in C$, $(x,0) = 0$ d'où $0 \in C^{\perp}$.
Soient $\lambda \in GR(p^m, r)$ et $y, y' \in C^{\perp}$ pour tout $x \in C$
$(x, \lambda y) = \lambda(x,y) = 0$

$$\begin{aligned}(x, y+y') &= (x,y) + (x,y') \\ &= 0+0 \\ &= 0\end{aligned}$$

Donc $C^{\perp}$ est code linéaire.

Remarque: 2.2.1. $C^{\perp}$ étant un code linéaire, alors il possède une matrice génératrice.

Définition 2.2.3. *Soit C un code linéaire de longueur n sur $GR(p^m, r)$. On appelle matrice de contrôle du code C notée H la matrice génératrice du code dual $C^{\perp}$ de C. Lorsque la matrice génératrice du code linéaire C est sous la forme normale, la matrice génératrice du code dual se met sous la forme :*

$$H = \begin{pmatrix} B_{0,0} & B_{0,1} & . & . & . & B_{0,m-1} & I_{l_m} \\ pB_{1,0} & . & . & . & pB_{1,m-2} & pI_{l_{m-1}} & 0 \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ p^{m-1}B_{m-1,0} & p^{m-1}I_{l_1} & 0 & 0 & ... & 0 & \end{pmatrix}$$

Où les Bi,j sont de dimension $l_{m-1} \times l_j$ à coefficients dans $\{0, ..., p-1\} \subset GR(p^m, r)$. cela entraine à la conséquence suivante.

Proposition 2.2.3. *le code dual $C^{\perp}$ de C a $\prod_{i=0}^{m-1} p^{il_i}$ mots.*

Preuve. ([6])

Remarque: 2.2.2. la notion de dualité pour les codes linéaires sur $GR(p^m, r)$ est proches de celle définie pour les codes linéaires sur un corps fini.

Proposition 2.2.4. *Soit C un code linéaire sur $GR(p^m, r)$. Le code dual de $C^{\perp}$ est le code C lui même. C'est à dire*
$(C^{\perp})^{\perp} = C$.

Preuve. Soit $C^{\perp}$ le code dual de C définit tel que
$C^{\perp} = \{x / \forall y \in C, x.y = 0\}$. De même le code $(C^{\perp})^{\perp}$ est définit tel que
$(C^{\perp})^{\perp} = \{a / \forall b \in C^{\perp}, a.b = 0\}$. Or pour tout x dans C et pour tout a dans $C^{\perp}$, $x.a = 0$, donc $C \subseteq (C^{\perp})^{\perp}$.
Soit $a \in (C^{\perp})^{\perp}$. alors $\forall b \in C^{\perp}$,$a.b = 0$

Or $\forall a \in C$, $\forall b \in C^{\perp}$, $a.b = 0$. Car $C \subset (C^{\perp})^{\perp}$.
Donc $a \in C$ par conséquent $(C^{\perp})^{\perp} \subseteq C$.■

Exemple 2.2.3. Sur $\mathbb{Z}_{2^2}$ posons
$C = \{000, 010, 020, 030, 102, 112, 122, 132, 200, 210, 220, 230, 302, 312, 322, 332\}$,
C est un code linéaire sur $\mathbb{Z}_{2^2}$,son code dual est $C^{\perp} = \{000, 201, 002, 203\}$.
On vérifie aisément que $(C^{\perp})^{\perp} = C$.

2.3 Construction des codes linéaires sur un anneau de Galois.

connaissant une chaine de codes linéaires de longueur n sur un corps quelconque, nous allons donner une construction de ce code sur les anneaux de Galois.

Notation 2.3.1. Soient C un code linéaire de longueur n et $\lambda \in GR(p^m, r)$,
$(C, \lambda) = \{x \in GR(p^m, r)^n / \lambda x \in C\}$.

Proposition 2.3.1. *$(C, \lambda) = \{x \in GR(p^m, r)^n / \lambda x \in C\}$ est un code linéaire de longueur n sur $GR(p^m, r)$.*

Preuve. soient $x = (x_1, ..., x_n), y = (y_1, ..., y_n) \in (C, \lambda)$,
on a $\lambda(x + y) = \lambda\lambda x + \lambda y \in C$ car C est un code linéaire. Par ailleurs,
pour $x = (x_1, ..., x_n) \in (C; \lambda)$ et $\alpha \in GR(p^m, r)$,$\lambda(\alpha x) = \alpha(\lambda x) \in C$ car C est code linéaire. Donc (C, λ) est code linéaire de longueur n sur $GR(p^m, r)$.

Remarque: 2.3.1. $(\overline{C, \lambda}) = \{\overline{x} / x \in (C, \lambda)\}$ est un code linéaire sur $\overline{GR}(p^m, r)$ qui provient de (C, λ).

Lemme 2.3.1. *Soit C un code linéaire de matrice génératrice G dans la forme standard et A la matrice associée à G . Alors, pour $0 \leq i \leq m-1$, $(\overline{C, p^i})$ a une matrice génératrice de la forme* $\begin{pmatrix} \overline{A_0} \\ \overline{A_1} \\ . \\ . \\ . \\ \overline{A_i} \end{pmatrix}$ *et $dim(\overline{C, p^i}) = k_0 + ... + k_i$.*

Proposition 2.3.2. *Soit $E_0 \subset E_1 \subset ... \subset E'm - 1$ une chaine de codes linéaires de longueur n sur corps fini $GF(q)$,$q = p^r$.*

Alors il existe un code linéaire C de longueur n sur $GR(p^m, r)$, tel que, $(\overline{C, p^i}) = E_i$, pour tout $i \in [|\ 1, m-1\ |]$.

Preuve. Pour $GF(q)$, $q = p^r$ on construit l'anneau de Galois $GR(p^m, r)$,
tel que, $\overline{GR}(p^m, r) = GF(q)$
Posons $n_i = dim(E_i)$. chaque E_i admet une matrice $n_i \times n$ sous la forme systématique $M_{E_i} = \begin{pmatrix} L_0 \\ L_1 \\ . \\ . \\ . \\ L_i \end{pmatrix}$ c'est à dire la sous matrice constituée telle que les n_i colonnes soit la matrice identité I_{n_i}. Ainsi choisissons les matrices A_i à coefficients dans $GR(p^m, r)$ tel que $\overline{A_i} = L_i$ et définissons le code linéaire C sur $GR(p^m, r)$ de matrice génératrice $\begin{pmatrix} A_0 \\ pA_1 \\ . \\ . \\ . \\ p^{m-1}A_{m-1} \end{pmatrix}$ D'après le lemme précédent, $(\overline{C, p^i}) = E_i$, $i = 0, 1, ..., m-1$. ■

Remarque: 2.3.2. le code linéaire C n'est pas unique car dépend du choix de s A_i et les coefficients des A_i dépendent du choix des représentants des classes modulo P.

2.4 Cardinal d'un code linéaire de longueur n sur $GR(p^m, r)$.

Définition 2.4.1. *Soit C un code linéaire de longueur n sur $GR(p^m, r)$ de matrice génératrice G. On appelle encodeur l'application $\phi : GR(p^m, r)^k \longrightarrow GR(p^m, r)^n$, telle que $\phi(u) = uG = (u_0, u_0A_{0,1} + pu_1, ..., u_0A_{0,m} + ... + p^{m-1}u_{m-1}A_{m-1,m})$, pour tout $u = (u_0, ..., u_{m-1}) \in GR(p^m, r)^k$, avec $k = \sum_{i=0}^{m-1} k_i$ et $u_i \in GR(p^m, r)^{k_i}$.*

Proposition 2.4.1. *Soit C un code linéaire de longueur n sur $GR(p^m, r)$. De matrice génératrice G sous la forme standard. Alors $\phi(GR(p^m, r)^k) = C$ et $Ker(\phi) = \prod_{i=0}^{m-1} p^{m-i} GR(p^m, r)^{k_i}$.*

Preuve. pour tout $u = (u_0, ..., u_{m-1}) \in GR(p^m, r)^k$, $u_i \in GR(p^m, r)^{k_i}$,

on a $\phi(u) = uG = \sum_{i=0}^{m-1} u_i p^i A_i$. Donc uG est combinaison linéaire des éléments $p^i A_i$, $i = 0, 1, ..., m-1$, or $p^i A_i \in C$ car ce sont les lignes de la matrice génératrice G de C.
Ainsi, $\phi(u) = uG = \sum_{i=0}^{m-1} u_i p^i A_i \in C$ d'où $\phi(GR(p^m, r)^k) \subseteq C$.

Par ailleurs, si $c \in C$ alors $c = \sum_{i=0}^{m-1} \alpha_i p^i A_i$, où $\alpha = (\alpha_0, ..., \alpha_{m-1}) \in GR(p^m, r)^k$,

$\alpha_i \in GR(p^m, r)^{k_i}$. Ainsi $c = \sum_{i=0}^{m-1} \alpha_i p^i A_i = \alpha G = \phi(\alpha)$

Donc, $\phi(GR(p^m, r)^k) = C$. Il reste à montrer que $Ker(\phi) = \prod_{i=0}^{m-1} p^{m-i} GR(p^m, r)^{k_i}$ pour cela :
Soit $u = (u_0, ..., u_{m-1}) \in GR(p^m, r)^k$, $u_i \in GR(p^m, r)^{k_i}$, tel que $\phi(u) = 0$ on sait que $\phi(u) = uG = (u_0, u_0 A_{0,1} + pu_1, ..., u_0 A_{0,m} + ... + p^{m-1} u_{m-1} A_{m-1,m})(*)$; ainsi $\phi(u) = 0$ implique que $u_0 = 0$ d'où $pu_1 = 0$ et don $u_1 \in p^{m-1} GR(p^m, r)^{k_1}$, et par itération $u_i \in p^{m-i} GR(p^m, r)^{k_i}$ pour tout $i = 0, ...; m-1$. Ainsi $Ker(\phi) \subseteq \sum_{i=0}^{m-1} p^{m-i} GR(p^m, r)^{k_i}$; le calcul par $(*)$ donne $\phi(u) = 0$ d'où $x \in Ker(\phi)$ et donc $Ker(\phi) = \prod_{i=0}^{m-1} p^{m-i} GR(p^m, r)^{k_i}$. ■

Théorème 2.4.1. *Soit un code linéaire de longueur n sur $GR(p^m, r)$. Alors*
1) *les paramètres $k_0, k_1, ..., k_{m-1}$ sont les même pour une matrice génératrice G sous la forme standard.*
2) *le nombre de mots de ce code est* $| C | = | \overline{GR} | \left(\sum_{i=0}^{m-1} (m-i) k_i \right)_{ri} = p \left(\sum_{i=0}^{m-1} (m-i) k_i \right)$

Preuve. 1) Les k_i sont uniques car $k_0 = dim(\overline{C, p^0}) = dim\overline{C}$ et
$k_i = dim(\overline{C, p^i}) - dim(\overline{C, p^{i-1}})$ pour $i = 0, 1, ..., m-1$.
2) Posons $k(C) = \sum_{i=0}^{m-1} (m-i) k_i$, puisque G est la matrice génératrice de C, considérons l'application

$$\begin{array}{rccc} \phi : & GR(p^m, r)^k & \longrightarrow & GR(p^m, r)^n \\ & u & \longmapsto & \phi(u) = uG \end{array} \text{ avec } uG \in C$$

comme $Ker(\phi) = \prod_{i=0}^{m-1} p^{m-1} GR(p^m, r)^{k_i}$ alors

$$\begin{aligned} C &\cong GR(p^m,r)^k / \prod_{i=0}^{m-1} p^{m-i} GR(p^m,r)^{k_i} \\ &\cong \prod_{i=0}^{m-1} (GR(p^m,r)/p^{m-i}GR(p^m,r))^{k_i} \\ &\cong \prod_{i=0}^{m-1} (p^i GR(p^m,r))^{k_i} \end{aligned}$$

car $GR(p^m,r)/pm-iGR(p^m,r) \equiv p^i GR(p^m,r)$. comme $\mid p^i GR(p^m,r) \mid = \mid \overline{GR}(p^m,r) \mid^{m-i}$, alors

$$\begin{aligned} \overline{C} &= \prod_{i=0}^{m-1} (\mid \overline{GR}(p^m,r) \mid^{m-i})^{k_i} \\ &= \mid GR(p^m,r) \mid^{\left(\sum_{i=0}^{m-1}(m-i)k_i\right)} \end{aligned}$$

Comme $\mid \overline{GR}(p^m,r) \mid = p^{mr} alors \mid C \mid = p^{\left(\sum_{i=0}^{m-1}(m-i)k_i\right)}$.■

Notation 2.4.1. $k = k(C) = rg_G(C) = k_0(C) + ... + k_{m-1}(C) = k_0 + ... + k_{m-1}$ et $k_i = k_i(C) = dim(\overline{C, p^i}) - dim(\overline{C, p^{i-1}})$, où k_i est le nombre de ligne divisible par p^i et non par p^{i+1} dans la matrice génératrice sous forme standard.

Proposition 2.4.2. *Soient C et D deux codes linéaires de longueur n sur $GR(p^m, r)$. Tel que $C \subseteq D$ et $k_i(C) = k_i(D)$, $i = 0, 1, ..., m-1$; alors $C = D$.*

Preuve. Comme $C \subseteq D$, alors C est un $GR(p^m, r)$- sous-module de D. Ainsi on a :

$$\begin{aligned} \mid C \mid &= p^{\left(\sum_{i=0}^{m-1}(m-i)k_i(C)\right)} \\ &= p^{\left(\sum_{i=0}^{m-1}(m-i)k_i(D)\right)} \\ &= \mid D \mid . \end{aligned}$$

Donc $C = D$. ■

2.5 Décomposition d'un code linéaire de longueur n sur $GR(p^m, r)$

Proposition 2.5.1. *Tout code linéaire C de longueur n sur $GR(p^m, r)$, peut se décomposer de façon unique en somme directe comme suit.*

$C \cong \bigoplus_{i=0}^{m-1} (GR(p^m,r)/p^{m-i}GR(p^m,r))^{k_i(C)} \cong \bigoplus_{i=0}^{m-1} p^i GR(p^m,r)^{k_i(C)}$ *pour* $k_i(C) \geq 0$

Preuve. La somme directe $\bigoplus_{i=0}^{m-1} p^i GR(p^m,r)^{k_i(C)}$ est un sous-module du $\prod_{i=0}^{m-1}(p^i GR(p^m,r))^{k_i(C)}$; comme $\{0,1,...,m-1\}$ est fini, alors la somme directe coïncide avec le produit direct. ■

Remarque: 2.5.1. toute matrice génératrice d'un code linéaire C peut se mettre sous la forme standard et possède $k(C)$ lignes.

2.6 Encodage sur les codes linéaire dans un anneau de Galois

Le principe de l'encodage voudrait qu'au préalable, on code un message avant de l'envoyer. Les codes linéaires présentent plusieurs avantages dans le processus d'encodage, en ce sens qu'il suffit premièrement de stoker la matrice génératrice G du code C pour connaitre tous les mots du code. Et deuxièmement, pour envoyer un message envoyer un mot $c = c_1c_2...c_k = (c_1,...,c_k) \in GR(p^m,r)^k$, où $k \leq n$, on le code en effectuant $c.G$ qui fait passer le mot c en un mot de code et c'est ainsi que tout mot $c = c_1c_2...c_k$ sera transmis sous la forme codée cG. Ainsi on a la définition suivante :

Définition 2.6.1. *On appelle encodeur tout homomorphisme défini par :*

$$\begin{array}{rccc} \varphi: & GR(p^m,r)^k & \longrightarrow & GR(p^m,r)^n \\ & c & \longmapsto & cG \end{array}$$

Où G la matrice génératrice du code C et c est un mot de code de C.

Cependant une fois que le message codé est reçu, après avoir transité sur un canal bruité qui est susceptible de perturber le message et donc lui apporter des erreurs des problèmes se posent.

1) comment détecter les erreurs ?
2) comment les corriger ?

2.7 Détection/Correction

2.7.1 Détection

Définition 2.7.1. *Soit C un code linéaire de longueur n sur $GR(p^m,r)$ et d sa distance minimale. On dit que C détecte t erreurs si le mot $y \in GR(p^m,r)^n$ tel que $w_H(y) \leq t$ ne sont pas dans C*

Propriété 2.7.1. *Les codes linéaires détectent toujours t erreurs lorsque $t \leq d$.*

Preuve. Soit $y \in GR(p^m, r)^n$ tel que $w_H(y) \leq t$. On a $w_H(y) \leq t < d$ (*), si $y \in C$ alors $w_H(y) \geq t$ ce qui contredit (*) donc y n'appartient pas à C.■

2.7.2 Correction

Définition 2.7.2. *On dit qu'un code C corrige t erreurs si pour tout $y \in GR(p^m, r)^n$ tel que $d(y, C) \leqslant t$, il existe un unique $x \in C$ tel que $d(y, C) = d(y, x)$*

Proposition 2.7.1. *Un code C de longueur n sur GR et de distance minimale d, corrige toujours t erreurs lorsque $t \leqslant E\left(\frac{d-1}{2}\right)$ où E est la partie entière.*

Preuve. Soit $y \in GR(p^m, r)^n$ tel que $d(y, C) \leq t$
$d(y, G) = min\{d(y, x)/x \in C\}$, d'où il existe $x_1 \in C$ tel que $d(y, C) = d(Y, x_1)$, sil existe aussi $x_2 \in C$, $x_2 \neq x_1$ tel que $d(y, C) = d(y, x_2)$ alors

$$\begin{aligned} d(x_1, x_2) &\leq d(y, x_1) + d(y, x_2) \\ &\leq d(y, C) + d(y, C) \\ &< \frac{d-1}{2} + \frac{d-1}{2} \\ &< d \end{aligned}$$

Ce qui contredit la minimalité de d. Donc $x_1 = x_2$.

Définition 2.7.3. *Soit C un code linéaire de longueur n et de distance minimale d. On appelle capacité correctrice de C l'entier naturel e tel que $e = E\left(\frac{d-1}{2}\right)$.*

2.8 Codes cycliques sur $GR(p^m, r)$

Dans toute cette section on se restreint au cas où la longueur n des codes est premier avec p

Définition 2.8.1. *L'application définie par :*

$$\begin{array}{rccc} \Gamma : & GR(p^m, r)^n & \longrightarrow & GR(p^m, r)^n \\ & (x_0, x_1, ..., x_{n-1}) & \longmapsto & (x_{n-1}, x_0, ..., x_{n-2}) \end{array}$$

est un automorphisme de $GR(p^m, r)^n$ appelé opérateur de shift.

Définition 2.8.2. *Un code linéaire de longueur n sur $GR(p^m, r)$ est dit cyclique si C est stable par l'opérateur shift c'est à dire pour tout $c = (c_0, ..., c_{n-1}) \in C$ alors $\Gamma(c) \in C$.*

Remarque: 2.8.1. Un mot $c = c_0c_1...c_{n-1}$ de $GR(p^m, r)$ peut être vue comme un polynôme $c(x) = c_0 + c_1x + ... + c_{n-1}x^{n-1}$ de $GR(p^m, r)[X]$ et dans la congruence modulo

$x^n - 1$, on a $x^n - 1 = 0$ c'est à dire $x^n = 1$. Ainsi $xc(x) = c_{n-1}x^n + c_0x + ... + c_{n-2}x^{n-1}$ donc $xc(x) = c_{n-1} + c_0x + ... + c_{n-2}x^{n-1}$ car $x^n = 1$.

Considérons l'application :

$$\begin{array}{rccc} \Psi : & GR(p^m,r)^n & \longrightarrow & GR_n = GR(p^m,r)[X]/id(X^n-1) \\ & c=(c_0,...,c_{n-1}) & \longmapsto & c_0+c_1x+...+c_{n-1}x^{n-1}+<X^n-1> \end{array}$$

Où $< X^n - 1 >$ est un idéal de $GR(p^m, r)[X]$ généré par $X^n - 1$. Comme dans les corps finis Ψ est un morphisme d'anneaux, or Ψ est surjective par définition il est alors un isomorphisme de $GR(p^m, r)$-modules qui envoie les codes cycliques de $GR(p^m, r)$ sur les idéaux de $GR_n = GR(p^m, r)[X]/id(X^n - 1)$.

Proposition 2.8.1. *Soit C un code linéaire de longueur n sur $GR(p^m, r)$. Alors C est cyclique si et seulement si C est idéal de $GR_n = GR(p^m, r)[X]/id(X^n - 1)$.*

Preuve. $\Longleftarrow$) Supposons que C soit un idéal de $GR_n = GR(p^m, r)[X]/id(X^n - 1)$ et $c(x) = c_0 + c_1x + ... + c_{n-1}x^{n-1}$ un mot de code,alors $xc(x) = c_{n-1} + c_0x + ... + c_{n-2}x^{n-1}$ est également un mot de code vu que C est idéal donc $(c_{n-1}, c_0, ..., c_{n-2}) \in C$.
$\Longrightarrow$) Supposons que C est cyclique. Si $c(x) \in C$ alors $xc(x) \in C$ et par suite $x^ic(x) \in C$ pour $0 \leq i \leq n - 1$.Comme C est linéaire alors, $a(x)c(x) \in C$ pour tout polynôme $a(x)$. D'où C est idéal de $GR_n = GR(p^m, r)[X]/id(X^n - 1)$. ■

Théorème 2.8.1. *([6])*
Soient I un idéal de $GR(p^m, r)[X]/id(X^n - 1)$. Il existe une unique famille $\{\widehat{f_i}\} \subset GR(p^m, r)[X]$ de $m + 1$ polynômes unitaires deux à deux premiers entre eux, vérifiant $\widehat{f_0}...\widehat{f_m} = X^n - 1$, et telle que
$I = (f_0, pf_1, p^2f_2, ..., p^{m-1}f_{m-1})$
Où les f_i sont définies par $f_i\widehat{f_i} = X^n - 1$.D'autre part, l'élément
$g = f_0 + pf_1 + p^2f_2 + ... + p^{m-1}f_{m-1}$ *est un générateur de I et* $\mid I \mid = \prod_{i=0}^{m-1} p^{(m-i)deg(\widehat{f_i})}$.

Corollaire 2.8.1. *L'anneau $GR_n = GR(p^m, r)[X]/id(X^n-1)$ a $(m+1)^l$ idéaux distincts, où l désigne le nombre de facteurs irréductibles de $X^n - 1$ dans $GR(p^m, r)[X]$.*

Preuve. Nous savons que tout idéal de $GR(p^m, r) = \mathbb{Z}_{p^m}[X]/(f)$, avec f irréductible de degré r et facteur de $X^n - 1$,a $m + 1$ idéaux. Comme l est le nombre de facteurs irréductibles et unitaires de $X^n - 1$, le nombre d'idéaux de GR_n est $(m + 1)^l$ ■.
Dans la suite nous nous intéresserons essentiellement aux idéaux pour lesquels
$\widehat{f_1} = \widehat{f_2} = ... = \widehat{f_{m-1}} = 1$
cet intérêt provient du fait que ces idéaux s'obtiennent par relèvement de Hensel des codes

cycliques sur $GR(p^m, r)$. En effet, le générateur $g(x)$ de tout code cyclique sur $GR(p^m, r)$ est diviseur unitaire de $X^n - 1$ dans $GR(p^m, r)[X]$, sans facteur multiple puisque p ne divise pas n. On peut donc lui appliquer le relèvement de Hensel, et obtenir un diviseur unitaire $g^{(k)}(X)$ de $X^n - 1$ dans $GR(p^m, r)[X]$.

Définition 2.8.3. *Soient $g(X) \in GR(p^m, r)[X]$ un diviseur de $X^n - 1$ et $g^{(k)}(X) \in GR(p^m, r)[X]$, son relevé de Hensel d'ordre k.*
Le code $C_{p^k} =< g^{(k)}(X) > \subset GR(p^m, r)[X]/id(X^n - 1)$ est appelé code de relevé du code cyclique $C =< g(X) >$. Le polynôme $G^{(k)}(X)$ est appelé le générateur de code C_{p^k}

Propriété 2.8.1. *Soit $g^{(k)} \in GR(p^m, r)[X]$ un polynôme unitaire divisant $X^n - 1$. La famille*
$\{g^{(k)}(X), Xg^{(k)}(X), ..., X^{n-d-1}g^{(k)}(X)\}$, avec $d = deg(g^{(k)}(X))$ est une famille génératrice du code $C_{p^k} = g^{(k)}(X) \in GR(p^m, r)[X]/id(X^n - 1)$, et linéairement indépendante sur $GR(p^m, r)[X]$. C'est donc une base de C_{p^k}.

Preuve. $GR(p^m, r)[X]/id(X^n - 1)$ étant principal, alors $< g^{(k)} >$ est un idéal principal ainsi tous ses éléments s'écrivent sous la forme de combinaison linéaire sur $GR(p^m, r)$ des éléments de la famille considérée. C'est à dire forment une famille génératrice de $< g^{(k)} >$.
Montrons qu'elle est linéairement indépendante sur $GR(p^m, r)$
posons $g^{(k)}(X)h^{(k)}(X) = X^n - 1$, soit $(a_i) \in GR(p^m, r)^{n-d}$ tel que $\sum a_i X^i g^{(k)}(X) = 0 \in GR_n$
Alors $A(X) = \sum_{i=0}^{n-d-1} a_i x^i$ est un multiple de $h^{(k)}$. Or $deeg(A) \leq n-d-1$ et $deg(h^{(k)}) = n-d$.
Donc $A(X) = 0$ i.e $a_i = 0\ \forall i$.
Par conséquent la famille est libre ■.

Propriété 2.8.2. *Posons $g^{(k)} = \sum_{i=0}^{n-d} g_i^{(k)} X^i$. Alors la matrice*

$$\begin{pmatrix} g_0^{(k)} & g_1^{(k)} & . & . & . & g_{n-d}^{(k)} & 0 & . & . & . & 0 \\ 0 & g_0^{(k)} & g_1^{(k)} & . & . & . & g_{n-d}^{(k)} & 0 & . & . & 0 \\ . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . \\ 0 & . & . & . & . & g_0^{(k)} & g_1^{(k)} & . & . & . & g_{n-d}^{(k)} \end{pmatrix}$$

est une matrice génératrice de dimension $n \times (n-d)$ du code cyclique $C_{p^k} =< g^{(k)} >$ et ce code a $p^{k(n-d)}$ mots de code.

Propriété 2.8.3. *Le dual d'un code cyclique est un code cyclique.*

Preuve. Soit $x = (x_1, x_2, ..., x_n) \in C^\perp$ vérifions si $\Gamma(x) = \Gamma(x_1, x_2, ..., x_n) \in C^\perp$
Soit $c = (c_1, c_2, ..., c_n) \in C$

$$\begin{aligned}\Gamma(x)c &= \Gamma(x)\Gamma(\Gamma^{-1}(c)) \\ &= (x_n, x_1, ..., x_{n-1})(\Gamma^{-1}(c)_n, \Gamma^{-1}(c)_1, ..., \Gamma^{-1}(c)_{n-1}) \\ &= x\Gamma^{-1}(c) \\ &= 0\end{aligned}$$

car $\Gamma^{-1}(c) \in C$ d'où le résultat.

Définition 2.8.4. *Soit C un code cyclique sur $GR(p^m, r)$. Engendré par $g(X)$. On appelle polynôme de contrôle de C_{p^k} le polynôme $h^{(k)}(X) \in GR_n[X]$, tel que, $X^n - 1 = g^{(k)}(X)h^{(k)}(X)$. Le dual $C_{p^k}^\perp$ de C_{p^k} est engendré par :*

$$\begin{aligned}\overline{h}^{(k)}(X) &= \tfrac{1}{h_0} X^d h^{(k)}(X^{-1}) \\ &= \tfrac{1}{h_0} \sum_{i=0}^{d} h_{d-i}^{(k)} X^i \quad .\end{aligned}$$

ce polynôme est appelé polynôme réciproque de $h^{(k)}$.

Remarque: 2.8.2. *$deg(h^{(k)}) = n - deg(g^{(k)}) = dim(C_{p^k})$.*

Propriété 2.8.4. *Soient $C_{p^k} =< g^{(k)} > \subset GR_n$ un code cyclique et $h^{(k)}$ son polynôme de contrôle. le code dual $C_{p^k}^\perp$ est cyclique et est engendré par le polynôme réciproque de $h^{(k)}$. Par conséquent, la matrice*

$$G^\perp = \begin{pmatrix} h_{n-d}^{(k)} & h_{n-d-1}^{(k)} & . & . & . & h_0^{(k)} & 0 & . & . & . & 0 \\ 0 & h_{n-d}^{(k)} & h_{n-d-1}^{(k)} & . & . & . & h_0^{(k)} & 0 & . & . & 0 \\ . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . \\ 0 & . & . & . & 0 & h_{n-d}^{(k)} & h_{n-d-1}^{(k)} & . & . & h_0^{(k)} & 0 \\ 0 & . & . & . & 0 & 0 & h_{n-d}^{(k)} & h_{n-d-1}^{(k)} & . & . & h_0^{(k)} \end{pmatrix}$$

est la matrice génératrice de dimension $n \times d$ du code dual $C_{p^k}^\perp$ et ce code a p^{kd} mots de code.

Preuve. ([6])

Exemple 2.8.1. prenons $g^{(3)}(X) = 7 + 5X + 6X^2 + X^3$ polynôme de $\mathbb{Z}_8[X]$ facteur irréductible de $X^7 - 1$ et $C_{2^3} =< g^{(3)}(X) >$. Alors sa matrice génératrice est :

$$\begin{pmatrix} 7 & 5 & 6 & 1 & 0 & 0 & 0 \\ 0 & 7 & 5 & 6 & 1 & 0 & 0 \\ 0 & 0 & 7 & 5 & 6 & 1 & 0 \\ 0 & 0 & 0 & 7 & 5 & 6 & 1 \end{pmatrix}$$

Déterminons le polynôme générateur $\overline{h}^{(k)}$ de $C_8^{\perp}$.

On a $g^{(3)}(X^4 + 2X^3 + 7X^2 + 5X + 1) = X^7 - 1$,

d'où $h^{(k)}(X) = 1 + 5X + 7X^2 + 2X^3 + X^4$.

Ainsi

$$\begin{aligned}\overline{h}^{(k)}(X) &= 1 \times X^4 \overline{h}^{(k)}(X^{-1}) \\ &= X^4(X^{-4} + 2X^{-3} + 7X^{-2} + 5X^{-1} + 1)\ . \\ &= 1 + 2X + 7X^2 + 5X^3 + X^4\end{aligned}$$

La matrice de contrôle de C_{2^3} est :

$$\begin{pmatrix} 1 & 5 & 7 & 2 & 1 & 0 & 0 \\ 0 & 1 & 5 & 7 & 2 & 1 & 0 \\ 0 & 0 & 1 & 5 & 7 & 2 & 1 \end{pmatrix}$$

D'après ce qui précède C_{2^3} a 2^{12} mots de code et $C_{2^3}^{\perp}$ a 2^9 mots de code. Une base de $C_{2^3}^{\perp}$ est $\{1572100, 0157210, 0015721\}$.

⋆ ⋆ Chapitre Trois ⋆ ⋆

CODES QUASI-CYCLIQUES SUR LES ANNEAUX DE GALOIS

Dans le chapitre précédent il était question pour nous, de définir un codes linaires sur un anneau de Galois, donner ses paramètres et faire une étude des codes cycliques sur cet anneau. Dans ce chapitre, nous commencerons par définir et donner les propriétés générales des codes quasi-cycliques sur les anneaux de Galois avant d'aborder la notion de codes quasi-cycliques à base cyclique.

Rappelons que l'application Γ définie comme suit :

$$\begin{array}{rccc} \Gamma : & GR(p^m,r)^n & \longrightarrow & GR(p^m,r)^n \\ & (x_0,x_1,...,x_{n-1}) & \longmapsto & (x_{n-1},x_0,...,x_{n-2}) \end{array}$$

est un automorphisme de $GR(p^m,r)^n$ appelé opérateur de shift et que tout code linéaire de longueur n sur $GR(p^m,r)$ est un $GR(p^m,r)$-sous-module de $GR(p^m,r)^n$. On notera parfois $GR(p^m,r)$ par GR, s'il n'y a pas ambiguïté.

3.1 Définitions et généralités

Définition 3.1.1. *Un sous-module U de $GR(p^m,r)^n$ est dit invariant par Γ^l si $\Gamma^l(U)=U$. Où $\Gamma^l(U)=\{\Gamma^l(u)/u\in U\}$ et $l>0$*

Exemple 3.1.1. Prenons $n=4$ et $GR(p^m,r)\cong\mathbb{Z}_4$.

Soit $U=<(1,1,0,0),(0,0,1,1)>$, alors on a $\Gamma^2(U)=U$.

En effet,soit $u\in U$ alors ils existent $\alpha_1,\alpha_2\in\mathbb{Z}_4$ tel que

$$\begin{aligned} u &= \alpha_1(1,1,0,0)+\alpha_2(0,0,1,1) \\ &= (\alpha_1,\alpha_1,\alpha_2,\alpha_2) \end{aligned}$$

Ainsi $\Gamma(u)=(\alpha_2,\alpha_1,\alpha_1,\alpha_2)$

$\Gamma^2(u)=(\alpha_2,\alpha_2,\alpha_1,\alpha_1)=\alpha_2(1,1,0,0)+\alpha_1(0,0,1,1)\in U$. D'où $\Gamma^2(U)\subset U$ et comme Γ^2 est bijective, alors $\Gamma^2(U)=U$.

Par contre $\Gamma(U)\nsubseteq U$, car $\Gamma(1,1,0,0)=(0,1,1,0)$ n'appartient pas à U.

En effet, supposons qu'ils existent $\alpha\lambda \in \mathbb{Z}_4$ tel que $(\alpha, \alpha, \lambda, \lambda) = (0, 1, 1, 0)$, alors $\alpha = 0$ et $\alpha = 1$ ce qui est absurde d'où le résultat.

Définition 3.1.2. *Un code linéaire C de longueur $n = ls$, est dit quasi-cyclique sur $GR(p^m, r)$ s'il est un sous-module de $GR(p^m, r)^n$ invariant par Γ^s pour un entier $s \in [\mid 1, n \mid]$. C'est à dire $\Gamma^s(C) = C$.*

Définition 3.1.3. *Soit $C(n, k)$ un code quasi-cyclique sur $GR(p^m, r)$, $s = min\{l \in \mathbb{N}^*/\Gamma^l(C) = C\}$ est appelé indice de cyclicité (index) de C.*

Exemple 3.1.2. *i)* Soit C_1 le code tel que $C_1 =< (1, 1, 0, 0), (0, 0, 1, 1) >$, à l'exemple précédent on a montrer que $\Gamma(C_1) \nsubseteq C_1$ et $\Gamma^2(C_1) = C_1$ d'où indice de cyclicité de C_1 est 2.

ii) Soit $C_2 =< (1, 0, 1, 0), (0, 1, 0, 1) >$ alors pour tout $u \in C_2$ ils existent $\alpha_1, \alpha_2 \in \mathbb{Z}_4$ tel que

$$\begin{aligned} u &= \alpha_1(1, 0, 1, 0) + \alpha_2(0, 1, 0, 1\alpha) \\ &= (\alpha_1, \alpha_2, \alpha_1, \alpha_2) \end{aligned}$$

Ainsi $\Gamma(u) = (\alpha_2, \alpha_1, \alpha_2, \alpha_1) = \alpha_2(1, 0, 1, 0) + \alpha_1(0, 1, 0, 1\alpha) \in C_2$. D'où $\Gamma(C_2) \subset C_2$ et comme Γ est bijectif donc $\Gamma(C_2) = C_2$ par conséquent l'index de C_2 est 1.

Remarque: 3.1.1. Un code quasi-cyclique d'index 1 est un code cyclique.

Proposition 3.1.1. *si C est un code quasi-cyclique d'indice de cyclicité l invariant par Γ^n, alors l divise n.*

Preuve. considérons la division euclidienne de n par l, c'est à dire qu'ils existent $r, q \in \mathbb{N}$ tels que,$n = ql + r$ avec $0 \leq r < l$.

Ainsi,

$$\begin{aligned} \Gamma^n(C) &= \Gamma^{lq+r}(C) \\ &= \Gamma^r(\Gamma^{lq}(C)) \\ &= \Gamma^r(C) \quad (1) \end{aligned}$$

Car $\Gamma^l(C) = C$.

Puisque C est invariant par Γ^n c'est à dire $\Gamma^n(C) = C$ (2) alors (1) et (2) entrainent que $\Gamma^r(C) = C$ ce qui contredit le fait que l soit minimal. Donc $r = 0$ c'est à dire $n = lq$ par l divise n ■.

Définition 3.1.4. *Soit l un entier naturel tel que l/n . On appelle Γ^l-sous-module de GR^n, un sous-module V de GR^n invariant par Γ^l.*

Remarque: 3.1.2. l étant fixé de même que n, un code quasi-cyclique C sur GR^n sera un Γ^l-sous-module de GR^n tel son index divise l.
Donc tout Γ^l sous -module est un code quasi-cyclique mais la réciproque est fausse.

Exemple 3.1.3. Pour $n = 6$ et $l = 3$, il est clair que les sous-modules invariant par Γ^3, sont les codes quasi-cycliques d'index 1 ou 3. Mais d'après l'exemple 3.1.1 on a montre que $\Gamma^2(U) = U$ et que C est d'index 2.
Par contre $\Gamma^3(U) \nsubseteq C$, en effet $\Gamma^3((1,1,0,0)) = (1,0,0,1)$ qui n'appartient pas à U il en résulte que U n'est pas un $\Gamma^3 sous - module$.
Notons que Γ^s est aussi appelé quasi-shift dans ce cas, un code quasi-cyclique d'index s n'est rien d'autre qu'un code s-quasi-cyclique.

3.1.1 Représentation des codes quasi-cyclique comme code cyclique sur $GR(p^m, r)$

Dans cette partie, nous voyons les codes quasi-cycliques comme codes cycliques sur un anneau, en particulier sur GR. Nous utilisons le quasi-shift particulier suivant.
$\Gamma^s = ((1, s+1, ..., (l-1)s+1), (2, s+2, ..., (l-1)s+2), ..., (s, 2s, ..., ls))$.
Ainsi un code C est dit quasi-cycliques si et seulement si $\Gamma^s \in Aut(C)$.
Autrement dit soit $n = ls$ considérons l'identification

$$\begin{array}{rccc} \phi: & GR^n & \longrightarrow & GR^n \\ & (c_0, ..., c_{n-1}) & \longmapsto & ((c_0, ..., c_{s-1}), ..., (c_{(l-1)s}, ..., c_{n-1})) \end{array}$$

$C \subset GR^n$ est un code quasi-cyclique si et seulement si $\phi(C) \subset GR^n$ est cyclique.
Cette permutation correspond à un décalage circulaire par blocs de taille s et, on peut écrire une matrice génératrice de façon générale sous la forme :

$$\begin{pmatrix} A_1 & A_2 & . & . & . & A_l \\ A_l & A_1 & . & . & . & A_{l-1} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ A_2 & A_3 & . & . & . & A_1 \end{pmatrix}$$

Où les A_i sont les matrices de taille $j \times s$ avec $j \leq s$.
Ici le code est donc vu comme code cyclique par blocs cette représentation est utilisée par J.Conan et G. seguin. Par cette approche ils voient les codes quasi-cycliques comme codes sur l'anneau de polynômes $F[X]/(X^l - 1)$.

3.2 Codes quasi-cycliques à base cyclique

Définition 3.2.1. *Soit C un codes quasi-cyclique sur GR d'indice de cyclicité s. On dit que C est à base cyclique s'il existe $u \in C, u \neq 0$, tel que,*
$C =< \{u, \Gamma^s(u), ..., \Gamma^{s(l-1)}(u)\} >$, *avec* $dim(C) = l$.

Exemple 3.2.1. *i*) Tout code cyclique est un code quasi-cyclique à base cyclique dont une base est de la forme $(u, \Gamma(u), \Gamma^2(u), ..., \Gamma^{l-1}(u))$.
ii) Soit C le code de longueur 6 tel que,
$C =< (1,1,1,0,0,0), (0,1,1,1,0,0), (0,0,1,1,1,0), (0,0,0,1,1,1) >$,
posons $u =< (1,1,1,0,0,0) >$ alors $B = (u, \Gamma(u), \Gamma^2(u), \Gamma^3(u))$ est une base de C.
Donc C est un code quasi-cyclique a base cyclique.

Représentation polynomiale d'un code quasi-cyclique

Définition 3.2.2. *Soit C un code quasi-cyclique de longueur $n = ls$ et d'indice. Soit $c = (c_0, ..., c_{l-1}) \in C$. On appelle représentation polynomiale de C l'application définie par :*

$$\begin{array}{cccc} R & GR^l & \longrightarrow & GR[X] \\ & c & \longmapsto & R(c) = \sum_{i=0}^{l-1} c_i x^{si} \end{array}$$

Remarque: 3.2.1. Si C est un code quasi-cyclique à base cyclique c'est à dire
$C =< \{\Gamma^{si}(u); 0 \leqslant i \leqslant l-1\} >$ avec $dim(C) = l$, alors $R(C) =< u(x), x^s u(x), ..., x^{s(l-1)} u(x) >$.
D'où $\forall v \in C, v = \sum_{i=0}^{l-1} \lambda_i \Gamma^{si}(u)$, ainsi

$$\begin{array}{rcl} v(x) & = & \sum_{i=0}^{l-1} \lambda_i x^{si} u(x) \\ & = & (\sum_{i=0}^{l-1} \lambda_i x^{si}) u(x) \end{array}$$

Donc $v(x) \in GR[x^s]u(x)$

3.2.1 Codes quasi-cycliques comme module sur un anneau

Soit $n = ls$, on définit l'action d'un polynôme à coefficient dans $GR[X]$ sur GR par :

$$\begin{array}{cccc} GR[X] \times GR^n & \longrightarrow & GR^n \\ (P(X), u) & \longmapsto & P(X)u = P(\Gamma)u \end{array}$$

Où Γ est le décalage circulaire $\Gamma(u_0, ..., u_{n-1}) = (u_{n-1}, ..., u_{n-2})$.

Proposition 3.2.1. *Avec l'action définit ci-dessus le GR-sous-module de GR^n est un $GR[X]$-module.*

Preuve. Il suffit de montrer que les propriétés de la loi externe sont vérifiées.

► Pour tout $P(X) \in GR[X]$, pour tous $u, u' \in GR^n$:

$$\begin{aligned} P(X)(u+u') &= P(\Gamma)(u+u') \\ &= (\sum_{i=0}^{l-1} \lambda_i X^{si})(u+u') \\ &= (\sum_{i=0}^{l-1} \lambda_i X^{si})u + (\sum_{i=0}^{l-1} \lambda_i X^{si})u' \\ &= \sum_{i=0}^{l-1} \lambda_i \Gamma^{si}(u) + \sum_{i=0}^{l-1} \lambda_i \Gamma^{si}(u') \\ &= P(\Gamma)u + P(\Gamma)u' \\ &= P(X)u + P(X)u' \end{aligned}$$

► Pour tous $P_1(X), P_2(X) \in GR[X]$, pour tout $u \in GR^n$

$$\begin{aligned} (P_1(X)+P_2(X))u &= P_1(\Gamma)u + P_2(\Gamma)u \\ &= \sum_{i=0}^{l-1} \lambda_i \Gamma^{si}(u) + \sum_{i=0}^{l-1} \alpha_i \Gamma^{si}(u) \\ &= (\sum_{i=0}^{l-1} \lambda_i X^{si})u + (\sum_{i=0}^{l-1} \alpha_i X^{si})u \\ &= P_1(X)u + p_2(X)u \end{aligned}$$

► On a :

$$\begin{aligned} P_1(X)(P_2(X)u) &= P_1(\Gamma)(P_2(\Gamma)u) \\ &= (P_1(\Gamma) \circ P_2(\Gamma))u \quad \text{par composition d'applications} \\ &= (P_1(X)P_2(X))u. \end{aligned}$$

► $1u = id_{GR^n}(u) = u$ où 1 est le polynôme unité.

Cette proposition nous permet de dire que tout sous espace de GR^n est un sous-module de GR^n et comme tout Γ^n sous -module est un code quasi-cyclique il est clair que tout code quasi-cyclique est un sous-module de GR^n. Donc l'étude des codes quasi-cycliques reviendra tout simplement à l'étude des sous-modules de GR^n.

De plus pour tout vecteur $u = (u_0, u_1, ..., u_{l-1}) \in GR^l$ on peut associer un polynôme $u(X) = \sum_{i=0}^{l-1} u_i X^i \in GR[X]/ < X^l - 1 >$. Ainsi on a un $GR[X]/ < X^l - 1 >$-module provenant de l'isomorphisme entre GR^l et $GR[X]/ < X^l - 1 >$.

Puisque $GR^l \cong GR[X]/ < X^l - 1 >$ alors $GR^n \cong (GR[X]/ < X^l - 1 >)^s$.

consequence 3.2.1. *Soit C un code quasi-cyclique de longueur $n = ls$, d'indice s et on suppose qu'il soit généré par les éléments, $u_1(X); u_2(X), ..., u_r(X) \in GR[X]/ < X^l - 1 >$,*

ainsi $C = \{a_1(X)u_1(X) + a_2(X)u_2(X) + ... + a_r(X)u_r(X)/a_i(X) \in GR[X]/ < X^l - 1 >\}$
$i = 0, 1, ..., r$.
Pour un GR-sous-module de $GR[X]/ < X^l - 1 >$,
C est généré par l'ensemble $\{u_1(X), Xu_1(X), ..., X^{l-1}u_1(X), ..., u_r(X), Xu_r(X), ..., X^{l-1}u_r(X)\}$.
Si C est généré par un seul élément $u(X) \in GR[X]/ < X^l - 1 >$, *alors C est un code quasi-cyclique à base cyclique c'est à dire* $C =< \{u, \Gamma^s(u), ..., \Gamma^{s(l-1)}(u)\} >$.
En effet, soit $u(x) = u_0 + u_1X + ... + u_{l-1}X^{l-1}$ *un polynôme de* $GR[X]/X^l - 1$, *où* $u_i = u_{i,o} + u_{i,1}\alpha + ... + u_{i,s}\alpha^{s-1}$ *où* $i = 0, 1, ..., l - 1$. *Ainsi* $u(X)$ *devient un s-uplet de polynômes sur GR de degré inférieure à* $l - 1$ *avec une GR-base fixe* $\{1, \alpha, ..., \alpha^{s-1}\}$.
Par conséquent $u(x)$ *devient un élément de* $(GR[X]/ < X^l - 1 >)^s$, *il en résulte que C est un* $GR[X]/ < X^l - 1 >$*-sous-module de* $(GR[X]/ < X^l - 1 >)^s$.

Définitions 3.2.1. *i) On appelle l'ordre du sous-module C de* GR^n *le polynôme non nul de plus petit degré et unitaire* $\phi(X)$ *de tel que* $\phi(X)c = 0$ *pour tout cDans C.*
ii) L'ordre d'un élément c noté $\phi_c(X)$ *est le polynôme non nul de plus petit degré et unitaire tel que* $\phi_c(X) = 0$.

Remarque: 3.2.2. l'ordre de l'élément nul est 1.

Proposition 3.2.2. *Pour tout polynômes* $P(X)$ *de* $GR[X]$ *et pour tout élément c de* GR^n *les propriétés suivantes sont équivalentes :*
i) $P(X)c = 0$
ii) $\phi_c(X)/P(X)$

Preuve. $\Longleftarrow$) Supposons que $\phi_c(X)/P(X)$ et montrons que $P(X)c = 0$.
$\phi_c(X)/P(X)$ alors il existe $Q(X) \in GR[X]$ tel que,
$P(X) = Q(X)\phi_c(X)$. Ainsi $P(X)c = Q(X)\phi_c(X)c$ et comme $\phi_c(X)$ est l'ordre de l'élément c alors $\phi_c(X)c = 0$, donc $P(X)c = 0$.
$\Longrightarrow$) Réciproquement supposons $P(X)c = 0$ et montrons que $\phi_c(X)/P(X)$.
Soit $P(X) = Q(X)\phi_c(X) + R(X)$ avec $deg(R(X)) < deg(\phi_c(X))$ la division euclidienne de $P(X)$ par $\phi_c(X)$.

$$\begin{aligned} P(X)c = 0 &\iff Q(X)\phi_c(X)c + R(X)c = 0 \\ &\iff R(X)c = 0 \end{aligned}$$

car $\phi_c(X)c = 0$. Or $deg(R(X)) < deg(\phi_c(X))$ ce qui contredit la minimalité de $\phi_c(X)$. D'où $R(X) = 0$, donc $P(X) = Q(X)\phi_c(X)$. Il en résulte que $\phi_c(X)/P(X)$ ■.

Exemple 3.2.2. 1) L'ordre de $\mathbb{Z}_4^7$ est $X^7 - 1$.
En effet pour tout $u \in \mathbb{Z}_4^7$, on a

$$\begin{aligned}(X^7-1)u &= (\Gamma^7-1)u \\ &= \Gamma^7(u)-u\ . \\ &= u-u=0\end{aligned}$$

car $\Gamma^7(u) = id_{GR(2,1)^7}(u) = u$, donc l'ordre de $\mathbb{Z}_4$ divise X^7-1 d'après la proposition 3.2.2. D'autre part, soit un polynôme $P(X)$ tel que $deg(P(X)) < 7$, mais en prenant $c = (1,0,0,0,0,0)$, on a :

$$\begin{aligned}P(X)c &= P(\Gamma)c \\ &= \sum_{i=0}^{6}\lambda_i\Gamma^i(c) \\ &= (\lambda_0,\lambda_1,...,\lambda_6)\neq 0\end{aligned}$$

Car les (λ_i) sont non tous nuls. Donc l'ordre de $\mathbb{Z}_4^7$ est X^7-1.

2) De manière générale on a l'ordre de GR^n est $X^{n/s}-1$. Raison pour laquelle on s'occupera particulièrement de sa décomposition en facteurs premiers, qui, seront les ordres des sous-modules de GR^n correspondants.

Remarque: 3.2.3. L'ordre d'un module C est aussi appelé polynôme minimal de Γ^s sur C

Proposition 3.2.3. *Un code quasi-cyclique C de GR^n admet une base cyclique si et seulement si le degré de son polynôme minimale est égal à la dimension de C.*

Preuve. $\Longrightarrow$) Supposons que C admette une base Cyclique, alors il existe un élément non nul u de C tel que $u \in C$,$u \neq 0$ tel que $C =< \{u, \Gamma^s(u), ..., \Gamma^{s(l-1)}\} >$, alors $(\Gamma^{si})_{i=0,1,...,l}$ est une famille liée. ainsi il existe une famille de coefficient non tous nuls $(\lambda_i)_{i\in\{0,1,...,l\}}$ à valeur dans GR tel que $\sum_{i=0}^{l}\lambda_i\Gamma^{si}(u) = 0$.

Et par suite le degré du polynôme minimal de Γ^s est inférieur ou égal à l.

Si le degré est strictement inférieure à l alors $\sum_{i=0}^{l-1}\lambda_i\Gamma^{si}(u) = 0$ avec les λ_i non tous nuls ce qui contre dit le fait que $(\Gamma^{si}(u))_{i\in\{0,1,...,l\}}$ forme une base d'où le degré est exactement l.

$\Longleftarrow$) Réciproquement supposons que $dimC = l$ avec $l \geqslant 1$

considérons l'application linéaire $\Gamma^s : C \longrightarrow C$ dont la matrice de Γ^s par rapport à une base de C est une matrice carrée $l \times l$ et donc le polynôme caractéristique de Γ^s de degré l. Par conséquent le polynôme minimal de Γ^s est de degré inférieure ou égal à l. Soit $\theta(X)$ le polynôme minimal de Γ^s, supposons que degré de $\theta(X)$ soit strictement inférieure à l.

$\theta(X) = \sum_{i=0}^{k}a_iX^i$, $k \leqslant l-1$ avec $a_k \neq 0$ et $deg\theta(X) = k$, alors pour tout $u \in C$, $\theta(\Gamma)u = 0 \Longleftrightarrow \sum_{i=0}^{l-1}a_i\Gamma^{si} = 0$,d'où pour tout $u \in C$, $(\Gamma^{si})_{i=0,1,...,l}$ est liée, donc n'admet

pas de base cyclique ■.

Remarque: 3.2.4. GR^n admet une base cyclique si et seulement si $n/s = n$ c'est à dire $s = 1$ car $dimGR^n = n$ et le degré du polynôme minimal de Γ^s est n/s.
L'anneau de Galois, est un anneau non intègre, ainsi la factorisation des polynômes dans ce type d'anneau cause des problèmes à cause de ces diviseurs de zero. C'est la raison pour laquelle dans cette section nous travaillerons sur son corps résiduel. Qui est un cas particulier d'anneau de Galois.

3.2.2 Composante primaires de $(GR/m_{GR})^n = \overline{GR}^n$

Lemme 3.2.1. *Pour tout entier non nul l,* $X^l - 1 = \prod_{i=0}^{k} (f_i(X))^t$ *où* $f_i(X)$ *est irréductible pour tout* $i = 0, 1, ..., k$ *dans* $GR(p^m, r)/m_{GR}$ *où* $GR(p^m, r)/m_{GR}$ *est le corps résiduel de GR isomorphe à* F_{p^r}.

Preuve. - Si $pgcd(p^r, l) = 1$ alors on a le résultat. -sinon alors il existe un entier naturel q tel que $l = qp^r$ et $pgcd(l, p) = 1$, ainsi on a $X^l - 1 = X^{qp^r} - 1^{qp^r} = (X^q - 1)^{p^r}$ on aura $t = p^r$ ■.

Théorème 3.2.1. *Soit s un entier naturel tel que s divise n et* $X^l - 1 = \prod_{i=0}^{k} (f_i(X))^t$, *avec* $l = n/s$ *d'après le lemme 3.2.1 .*
On pose $g_i(X) = X^l - 1/(f_i(X))^t$ *et* $W_i = g_i(X)F_{p^r}^n$ *et on a les résultats suivant.*
(1) $F_{p^r}^n = W_1 \bigoplus W_2 \bigoplus, ..., \bigoplus W_k$
(2) *l'ordre de* W_i *est* $(f_i(x))^t$
(3) $W_i = \{u \in F_{p^r}^n / (f_i(X))^t.u = 0\}$
(4) W_i *est un code cyclique engendré par* $g_i(X^s)$
(5)$dimW_i = sk_it$ *où* $k_i = degf_i(X)$
(6) *tout sous module U de* $F_{p^r}^n$ *est de la forme* $U = U_1 \bigoplus U_2 \bigoplus ... \bigoplus U_k$ *où* U_i *est inclus dans* W_i, $U_i = g_i(X)U$. *Les* W_i *sont appelés les composantes primaires de* $F_{p^r}^n$.

Preuve. (1) Montrons que $F_{p^r}^n = W_1 \bigoplus W_2 \bigoplus, ..., \bigoplus W_k$
Les polynômes $g_i(X)$, $i = 0, 1, ..., k$ sont premiers entre eux et d'après le théorème de Bezout il existe $\alpha_1(X), ..., \alpha_k(X) \in \overline{GR}$ tels que :
$\alpha_1(X)g_1(X) + ... + \alpha_k(X)g_k(X) = 1$, et pour tout élément $u \in \overline{GR}^n$ on aura,
$u = \alpha_1(X)g_1(X)u + ... + \alpha_k(X)g_k(X)u$, donc $u \in W_1 + ... + W_k$
et par suite, $\overline{GR}^n = W_1 + ... + W_k$.
D'autre part si $w_1 + ... + w_k = 0$, avec $w_i \in W_i$, $i = 1, 2, ..., k$, en multipliant par $g_i(X)$,

on obtient $g_i(X)w_i = 0$, car $g_i(X)w_j = o$ pour tout $i \neq j$ $(f_j(X)/g_i(X))$ et d'où $w_i = 0$ car $w_i \neq 0$ dans à l'ordre $f_i(X)^r$, pour $1 \leq r \leq t$ et $f_i(X)/g_i(X)$. Donc $\overline{GR}^n = \bigoplus_{i=o}^{k} W_i$.

(2) montrons que L'ordre de W_i est $(f_i(X))^k$.

Soit $w_i \in W_i$,$f_i(X)w_i = 0$ car $w_i \in W_i$ est inclus dans $\overline{GR}^n$ et $X^l - 1$ étant le polynôme minimal de $\overline{GR}^n$, d'où $(f_i(X))^k$ est divisible par l'ordre de W_i et par irréductibilité de $f_i(X)$ cet ordre est exactement $(f_i(X))^k$.

(3) découle de (2)

(4) Considérons la représentation :

$$\begin{array}{ccc} \overline{GR}^n & \longrightarrow & \overline{GR}[X] \\ (u_0, ..., u_{n-1}) & \longmapsto & u_0 + u_1X + ... + u_{n-1}X^{n-1} \end{array}.$$

Par définition $W_i = g_i(X)\overline{GR}^n = \{g_i(X)u/u \in \overline{GR}^n\}$.

Soit u $\overline{GR}^n$ montrons que $\Gamma(g_i(X)\underline{u}) = Xg_i(X)\underline{u} \in \overline{GR}^n$. On a $Xg_i(X)\underline{u} = g_i(X)(x\underline{u})$, or $xu \in \overline{GR}^n$, d'où $g_i(X)(Xu) \in \overline{GR}^n$, donc $w_i =< g_i(X^s) >$.

Il reste à montrer que $\Gamma(W_i) = W_i$. Soit $W_i = (W_{0i}, ..., W_{in-1})$, on a la correspondance suivante :

$$\begin{array}{rcl} \Gamma(w) = (w_{n-1}, w_0, ..., w_{n-2}) & \longmapsto & w_{n-1} + w_0X + ... + w_{n-2}X^{n-1} \\ & \longmapsto & X(w_0 + w_1X + ... + w_{n-1}X^{n-1}) \\ & \longmapsto & \Gamma(w_i) = Xw_i \in W_i \end{array}$$

Donc $\Gamma(W_i) = W_i$ ce qui prouve que W_i est un code cyclique.

(5) On a $dim(w_i) = deg(f_i(X))^k = nk_it$, où $k_i = deg(f_i(X))$.

(6) Application immédiate de (1) ■.

Dans la suite, on notera $< c >$ le module cyclique engendré par c et définir par :

$< c >= \{P(X)c/P(X) \in \overline{GR}^n\}$

si le degré de l'ordre u est k, alors $(c, Xc, ..., X^{k-1}c)$ est une base de $< c >$.

Lemme 3.2.2. *(i)* $< c >=< w >$ *si et seulement si* $w = P(X)u$ *et* $pgcd(P(X), \phi_c(x)) = 1$
(ii) Si $C = C_1 \bigoplus ... \bigoplus C_k$, C_i *sous-modules de* $\overline{GR}^n$ *et soit* $c_i \in C_i$, $i = 1, ..., k$ *alors l'ordre de* $c = \sum_{i=1}^{k} c_i$ *est le plus petit multiple des ordres des* c_i *et de même l'ordre de* C *est le ppcm des ordres de* c_i.
(iii) Si $C = C_1 \bigoplus ... \bigoplus C_k$, *alors* C *admet une base cyclique si et seulement si* C_i *admet une base cyclique et l'ordre des* C_i *sont deux à deux premiers entre eux.*

Preuve. (i) Supposons que $< c >=< w >$, alors $w \in < c >$, donc il existe $P(X) \in \overline{GR}^n[X]$, tel que, $w = P(X)c$, d'où l'ordre $\phi_w(x)$ de w divise $pgcd(P(X), \phi_c(X))$. Et comme $deg(\phi_c(X)) = deg(\phi_w(X))$, or $< c >=< w >$ d'où on a $pgcd(\phi_c(X), P(X)) = 1$.

Réciproquement supposons que $w = P(X)c$, $P(X) \in \overline{GR}^n[X]$, alors $< w > \subset < c >$ et comme $pgcd(\phi_c(X), P(X)) = 1$, alors $\phi_c(X) = \phi_w(X)$, donc w et c ont le même ordre d'où $< c > = < w >$ d'où le résultat.

(ii) Soit $C = C_1 \bigoplus ... \bigoplus C_k$ et soit $c_i \in C_i$, $i = 1, ..., k$, posons $\overline{\phi}(X) = ppcm(\phi_{c_i}(X))$ pour tout $i = 1, ..., k$.

On a $\phi_{c_i}(X)/\overline{\phi}(X)$, donc $\overline{\phi}(X)c_i = 0$, $(\forall i)$. D'où $\overline{\phi}(X)c = 0$ et par suite $\phi_c(X)/\overline{\phi}(X)$ $(*)$. En outre $\phi_c(X)c = 0$ entraine que $\phi_c(X)c_1 + ... + \phi_c(X)c_k = 0$, d'où $\phi_c(X)c_i = 0$, $(\forall i)$ car $C = \bigoplus_{i=1}^{k} C_i$. Donc $\phi_{c_i}(X)/\phi_c(X)$, $i = 1, ..., k$,par conséquent $\overline{\phi}(X)/\phi_c(X)$ par minimalité de $\phi(c)$. $(**)$

$(*)$ et $(**)$ entraine le résultat. Par le même raisonnement, on montre que l'ordre de C est le ppcm des ordres de C_i en remplaçant c_i par C_i.

(iii) Supposons que $C_i =< c_i >$ et que $\phi_i(X) = \phi_{c_i}(X)$, $i = 1, ..., k$ soient deux à deux premiers entre eux. D'après (ii) on aura $\phi_c(X) = \prod_{i=1}^{k} \phi_i(X)$, où $c = \sum_{i=1}^{k} c_i$. D'où on a :

$$\begin{aligned} deg(\phi_c(X)) &= \sum_{i=1}^{k} deg(\phi_i(X)) \\ &= \sum_{i=1}^{k} dimC_i \\ &= dimC \end{aligned} \quad .$$

D'où $C =< c >$ et admet donc une base cyclique.

D'autre part si $C =< c >$, alors $c = \sum_{i=1}^{k} c_i$, $c_i \in C_i$, $i = 1, ..., k$. Tout élément de C est de la forme $P(X)c = \sum_{i=1}^{k} P(X)c_i$, $P(X) \in \overline{GR}^n[X]$, d'où $C =< c_1 > \bigoplus ... \bigoplus < c_k >$ et comme $c_i \in C_i$, on a $C_i =< c_i >$ et par la suite $\phi_c(X) = ppcm(\phi_{c_i}(X))$, ceci d'après (ii) et $deg(\phi_c(X)) = dimC = \sum_{i=1}^{k} deg(\phi_i(X))$, d'où $ppcm(\phi_{c_i}) = \prod_{i=1}^{k} \phi_{c_i}(X)$. Donc les $\phi_{c_i}(X)$ sont deux à deux premiers entre eux ■.

Le théorème suivant caractérise les codes quasi-cycliques à base cyclique ■.

Théorème 3.2.2. *Soit $s \in \mathbb{N}^*$ tel que S divise n et soit $W_1, ..., W_k$ les composantes primaires de $\overline{GR}^n$ suivant Γ^s et soit C un Γ^s-sous-module de $\overline{GR}^n$, tel que,*

$C = C_1 \bigoplus ... \bigoplus C_k$,avec $C_i \subset W_i$ et C_i la i^{me} composante primaire de C alors :

i) C est un code quasi-cyclique si et seulement si chacune de ses composantes C_i l'est aussi.

ii) C admet une base cyclique si et seulement si chaque C_i admet une base cyclique . et

dans ce cas si $C_i =< c_i >$ *alors* $C =< c >$ *,* *où* $c = \sum_{i=1}^{k} c_i$.

Preuve. *i*) Soit C un code quasi-cyclique d'indice de cyclicité s. Puisque $C = C_1 \bigoplus ... \bigoplus C_k$, alors $\Gamma^s(C) = \Gamma^s(C_i) \bigoplus ... \bigoplus \Gamma^s(C_i)$. En effet pour tout $c \in C$ il existe des $c_i \in C_i$, tels que,

$c = \sum_{i=1}^{k} c_i$ et $\bigcap_{i=1}^{k} c_i = \{0\}$.

$$c = \sum_{i=1}^{k} c_i \iff \Gamma^s(c) = \Gamma^s(\sum_{i=1}^{k} c_i) \quad \text{car } \Gamma^s \text{ est linéaire .}$$
$$= \sum_{i=1}^{k} \Gamma^s(c_i)$$

De plus

$$\bigcap_{i=0}^{k} c_i = \{0\} \iff \Gamma^s(\bigcap_{i=0}^{k} c_i) = \Gamma^s(\{0\}) \iff \bigcap_{i=1}^{k} \Gamma^s(c_i) = \{0\} \quad .$$

Donc $\Gamma^s(C) = \bigoplus_{i=0}^{k} \Gamma^s(C_i)$.

Supposons que C soit un code quasi-cyclique d'indice s, c'est à dire $\Gamma^s(C) = C$, et comme $\Gamma^s(C) = \bigoplus_{i=0}^{k} \Gamma^s(C_i)$ il suit que $\bigoplus_{i=0}^{k} \Gamma^s(C_i) = \bigoplus_{i=0}^{k} C_i$ car $C = \bigoplus_{i=0}^{k} C)i$.

or $Ci \subset W_i$ d'où $\Gamma^s(C_i) \subset \Gamma^s(W_i) = W_i$ car w_i est un code quasi-cyclique d'indice s. D'où $\Gamma^s(C_i) \subset W_i$ et comme $C_i \subset W_i$, par conséquent C_i est quasi-cyclique pour tout $i = 1, ..., k$.

Réciproquement supposons que C_i est quasi-cyclique d'indice s pour tout $i = 1, ..., k$, alors $\Gamma^s(C_i) = C_i$, $(\forall i)$ et donc

$$\begin{aligned} \Gamma^s(C) &= \bigoplus_{i=0}^{k} \Gamma^s(C_i) \\ &= \bigoplus_{i=0}^{k} C_i \qquad \text{car } \Gamma^s(C_i) = C_i \\ &= C \end{aligned}$$

ii) est une conséquence immédiate du lemme 3.2.2 puisque les ordres de C_i sont deux à deux premiers entre eux ■. Le théorème 3.2.2 nous permet de construire les codes quasi-cycliques à base cyclique à partir des composantes primaires de $\overline{GR}^n$, comme on va le voir dans l'exemple ci-dessous.

Exemple 3.2.3. Puisque $\overline{GR}^n = F_{p^r}$ prenons $p^r = 2$,$n = 14$ et $s = 2$. comme $n = ls$

alors $l = n/s = 7$ et on a :

$X^7 + 1 = (X + 1)(X^3 + X + 1)(X^3 + X^2 + 1)$, ainsi on a :

$g_1(X) = X^7 + 1/X + 1 = 1 + X + X^2 + X^3 + X^4 + X^5 + X^6$

$g_2(X) = X^7 + 1/X^3 + X + 1 = 1 + X + X^2 + X^4$

$g_3(X) = X^7 + 1/X^3 + X^2 + 1 = 1 + X^2 + X^3 + X^4$

Les composantes primaires de F_2^{14} sont des codes cycliques engendrés par :

$g_1(X^2) = 1 + X^2 + X^4 + X^6 + X^8 + X^{10} + X^{12}$

$g_2(X^2) = 1 + X^2 + X^4 + X^8$

$g_3(X^2) = 1 + X^4 + X^6 + X^8$

Soient W_1,W_2 et W_3 respectivement.

Donc $F_2^{14} = W_1 \bigoplus W_2 \bigoplus W_3$. Et on aura :

$dimW_1 = 2.1.1 = 2$, $dimW_2 = 2.3.1 = 6$ et $dimW_3 = 2.3.1 = 6$.

les ordres étant respectivement $f_1(X) = X+1$, $f_2(X) = X^3+X+1$ et $f_3(X) = X^3+X^2+1$.

considérons $w_2(X) = (1+X)(1+X^2+X^4+X^8) = 1+X+X^2+X^3+X^4+X^5+X^8+X^9$.

On a $w_2 \in W_2$ et engendre le module suivant :

1	1	1	1	1	1	0	0	1	1	0	0	0	0
0	0	1	1	1	1	1	1	0	0	1	1	0	0
0	0	0	0	1	1	1	1	1	1	0	0	1	1
1	1	0	0	0	0	1	1	1	1	1	1	0	0
0	0	1	1	0	0	0	0	1	1	1	1	1	1
1	1	0	0	1	1	0	0	0	0	1	1	1	1
1	1	1	1	0	0	1	1	0	0	0	0	1	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0

Sa matrice génératrice est

$$G_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

donc ce module n'est rien d'autre qu'un code quasi-cyclique à base cyclique d'indice 2 et de dimension égal à 3 dont une base est $(c_2, \Gamma^2(c_2), \Gamma^4(c_2))$ et de poids 8. On le note tout simplement $(14, 3, 8)$.

Cette fois ci considérons

$$\begin{aligned} w_3 &= (1 + X^2)(1 + X + X^6 + X^8) \\ &= 1 + X^2 + X^4 + X^{10} \end{aligned}$$

Alors on a $w_3 \in W_3$ et engendre le module suivant :

$$\begin{array}{cccccccccccccc}
1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}$$

De la même façon que le cas précédent on trouve une matrice génératrice de ce module qui est :

$$G_3 = \begin{pmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

on conclut que ce module est un code quasi-cyclique à base cyclique d'indice 2, de longueur 14 dont une base est $(c_3, \Gamma^2(c_3), \Gamma^4(c_3))$, avec $c_3 = 10101000001000$ son poids est égal à 4 . Donc on le note $(14, 3, 4)$.

D'après le théorème 3.2.2 la somme directe $W =< w_2 > \bigoplus < w_3 >$ est un codes quasi-cyclique à base cyclique de dimension 6 engendré par

$$\begin{aligned} w(X) &= w_2(X) + w_3(X) \\ &= X + X^3 + X^5 + X^8 + X^9 + X^{10}1 \end{aligned}$$

dont une matrice génératrice est :

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

une de ces bases est $(u, \Gamma^2(u), \Gamma^4(u), \Gamma^6(u), \Gamma^8(u), \Gamma^{10}(u))$, avec $u = 01010100111000$, ce code est de longueur 14 et de poids 6. On le note tout simplement $(14, 6, 6)$.

Théorème 3.2.3. *Soit C un code quasi-cyclique de longueur $n = ls$ et d'indice s sur GR. Alors C se décompose en somme directe des codes quasi-cycliques à base cyclique sur GR.*

Preuve. Soit $u \in C$, $u \neq 0$, si $C =< \{\Gamma^{si}(u), i \in [\mid 1, l-1 \mid]\} >$ c'est à dire C est à base

cyclique, alors on a le résultat.
Sinon, soit $u_1 \in C$, $u_1 \neq 0$, considérons $C_{u_1} =< \{\Gamma^{si}(u_1), i \in [|\ 1, l-1\ |]\} >$, comme C n'est pas à base cyclique alors $C_{u_1} \subset C$. Soit $u_2 \in C \backslash C_{u_1} = K$, $u_2 \neq 0$, considérons $C_{u_2} =< \{\Gamma^{si}(u_2), i \in [|\ 1, l-1\ |]\} >$ alors $C_{u_1} \bigcap C_{u_2} = \{0\}$. Si $C = C_{u_1} \bigoplus C_{u_2}$ alors on a le résultat. Sinon soit $U_3 \in C \backslash K$, $u_3 \neq 0$, considérons $C_{u_3} =< \{\Gamma^{si}(u_3), i \in [|\ 1, l-1\ |]\} >$, alors $C_{u_1} \bigcap C_{u_2} \bigcap C_{u_3} = \{0\}$, si $C = C_{u_1} \bigoplus C_{u_2} \bigoplus C_{u_3}$ alors on a le résultat . Sinon on procède de façon analogue que précédemment ainsi de suite jusqu'à un ordre k et on arrive à $C = \bigoplus_{i=1}^{k} C_{u_i}$. Car C est fini. ■

3.2.3 Dual d'un codes quasi-cyclique

Définition 3.2.3. *Soient $x = (a_0, ...a_{l-1})$ et $b = (b_1, ..., b_{l-1})$ des éléments de GR^l.*
On définit le produit euclidien de a et b comme suit : $a.b = \sum_{i=0}^{l-1} a_i.b_i$.

Définition 3.2.4. *Soit C un code quasi-cyclique à base cyclique, de longueur $n = ls$ et d'indice s sur GR. Son code dual noté $C^\perp$ est défini comme suit :*
$C^\perp = \{d \in GR^{n=ls} / d.c = 0, \forall c \in C\}$

Proposition 3.2.4. *Soit C un code quasi-cyclique de longueur $n = ls$, d'indice s sur GR alors son code dual $C^\perp$ est un code quasi-cyclique.*

Preuve. Soit C un code quasi-cyclique, d'indice s . Montrons que $\Gamma^s(C^\perp) = C^\perp$.
Soit $x = (x_1, ...x_n) \in C^\perp$, alors pour tout $C = (c_1, ..., c_n) \in C$ on a :

$$\begin{aligned} \Gamma^s(x)c &= \Gamma^s(c)\Gamma^s(\Gamma^{-s}(c)) \\ &= \Gamma^s(x\Gamma^{-s}(u)) \\ &= \Gamma^s(0) \\ &= 0 \end{aligned}$$

d'où $\Gamma^s(x) \in C^\perp$, donc $C^\perp$ est un code quasi-cyclique. ■

Remarque: 3.2.5. Nous avons démontrer que, tout codes quasi-cycliques s'écrit comme somme direct des codes quasi-cycliques à base cyclique. Puisque le dual d'un code quasi-cyclique est quasi-cyclique, alors celui-ci s'écrit comme somme directe de codes quasi-cyclique à base cyclique.

♣ Conclusion ♣

Parvenu au terme de notre travail basé sur, les codes quasi-cycliques sur un anneau de Galois, force est de constater que, les corps finis, sont des corps résiduels des anneaux de Galois. L'utilisation des anneaux de Galois comme Alphabet structuré, nous permet de généraliser la théorie des codes linéaires, sur des corps finis aux anneaux de Galois.
Dans ce travail, nous avons, utiliser les résultats obtenues des codes cycliques, pour généraliser ceux des codes quasi-cycliques. La notion de codes quasi-cycliques à base cyclique a été abordé. Nous avons montrer que les codes quasi-cycliques sont des GR-sous-module de GR^n et que, tout code quasi-cyclique s'écrit comme somme directe de codes quasi-cycliques à base cyclique.
Cependant une question se pose "le code dual d'un code quasi-cyclique à base cyclique est t-il à base cyclique ?" tel est l'objectif visé pour nos recherches futures.

♣ Bibliographie ♣

[1] M. Babier, C. Chabot, G. Quintin : 2012*on quasi-cyclic codes as a generalization of cyclic codes*, Écoles Polytechniques, Laboratoire d'informatique (Lix)21128, Palaiseau Cedex, .

[2] Christophe Chabot, 2009 :*Reconnaissance des codes, Structure des codes quasi-cycliques* , These de Doctorat $N°$ 29-2009, 21-25, 95-97, Université de Limoge.

[3] Christophe FOMEKONG, 2007 : *Anneaux et modules*, Université de Yaoundé I.

[4] Delphine Boucher, Patrick Solé, Felix Ulmer, 2008 : *codes cycliques tordus sur les anneaux de Galois*, IRMAR, UMR 6625, Université de Renne 1.

[5] Fabien Galand, 2004 : *Code $\mathbb{Z}_{2^k}$-linéaire*, Rapport de recherche $N°$ 5073 : 6-34

[6] Fabien Galand, 2004 : *construction des codes $\mathbb{Z}_{p^k}$ de bonne distance minimale fondées sur les codes de recouvrement*, Thèse de Doctorat de en mathématique, Université de CAEN, .

[7] R.Hammons, Kumar, Calderbank and P. Solé : *Kerdock, Preparata, Goethals and other codes are linear over $\mathbb{Z}_4$*, IEEE Transactions on information theory 40 : 301-319, 1994.

[8] , Northon and Salagean, *On the structure of linear and cyclic codes over finite chain ring*, Algebra in Engineering communication and computing, 489-506.

[9] Nuh Aydin and Ray-Chaudhuri, 2002 : *Quasi-cyclic codes over $\mathbb{Z}_4$ and some new binary codes*, IEEE Transaction on information on theory, Vol 48,$N°$, 1-5.

[10] Pierre-louis Cayrel, Christophe Chabot, Abdelkader, 2009 : *Codes quasi-cycliques sur des anneaux de matrice*, IRMAR-Université Renne 1.

[11] C.E. Shannon, 1949, *Communication in presence of noise* . IEEE, 37 : 10-21.