REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie
****

UNIVERSITE DE YAOUNDE I
ECOLE NORMALE SUPERIEURE
DEPARTEMENT DE MATHÉMATIQUES
****

REPUBLIC OF CAMEROUN
Peace – Work – Fatherland
****

UNIVERSITY OF YAOUNDE I
HIGHER TEACHER TRAINING COLLEGE
DEPARTMENT OF MATHEMATICS
****

CODES LINEAIRES SUR LES ANNEAUX FINIS

Présentée en vue de l'obtention du Diplôme de Professeur de l'Enseignement Secondaire deuxième grade
Mémoire de D.I.P.E.S II

Par :

NEKELEYAN DAVID

Sous la direction
Dr. NDJEYA SELESTIN
Chargé de cours

Année Académique
2015-2016

♣ Dédicace ♣

À mes parents

♣ Remerciements ♣

Ce travail est une conséquence de plusieurs erreurs de ma part et des améliorations dû à plusieurs contributions parmis lesquelles ;
- j'ai le profond plaisir d'exprimer ma gratitude à mon encadreur
le Dr NDJEYA SELESTIN qui n'a jamais cessé de me donner des conseils dans l'evolution de ce travail.
- Je remercie tous les enseignants de l'école normale supérieure de l'université
de yaoundé I.
- Merci à ma famille qui on fait de moi par leur foi en Dieu ce que je suis aujourd'hui.
- Je dit merci à mes camarades de promotion et autres qui m'ont toujours soutenu moralement.

♣ Résumé ♣

Dans ce mémoire, nous détaillons la notion de code linéaire sur un anneau fini et entre autres nous allons établir des moyens de constructions de tels codes sur des anneaux algorithquement définis qui permettrons d'optimiser ces constructions.

Mots-clés : Code linéaire, rang d'un code, code correcteur, code BCH, code Goppa, code Alternant.

♣ Abstract ♣

In this work, we detail the concept of linear code over a finite ring and among other will establish such codes constructions means an algorithment défined rings allowed optimize its construction.

Keywords : Linear code, rang code, correcteur code, BCH code, goppa code, alternant code.

♣ Table des matières ♣

♣ Introduction générale ♣

les codes linéaires sur les anneaux unitaires finis ont recenment eu un grand intérêt dans la théorie du codages algébriques et presente de nombreuse applications importantes parmis lesquelles celle du codages de l'informations. Dans ce travail, nous presentons la construction des codes cycliques, BCH, alternant, Goppa et srivastava sur des anneaux locaux finis et nous verrons que ces constructions necessitent les travaux d'extensions de galois sur un anneau donné où certaines propriétées de galois sur les corps sont triviales favavorisant ainsi la formalisation des expresions de manière générales. Dès lors, le developpement recent a contribué vers l'achevement de la fiabilité que requiert les systémes digital d'haut débit d'aujourd'hui et l'utilisation des codes correcteurs d'erreurs est devenu un modèle intégral des systémes de communications modernes et des ordinateurs. De plus, nous mentionons que l'investigation des codes sur des aphabets finis (exemple anneaux finis) est mieux approprié dans l'utilisation des ordinateurs pour la communication. Dans ce travail, nous distingons trois chapitres, le premier nous permet de rappéler des notions sur les structures d'anneaux. Par suite, le deuxième chapitre nous plonge dans la description de la théorie des codes correcteurs où nous caractérisons les propriétés d'un code MDS et nous définissons la notion de code dual d'un code linéaire donné. Enfin le troisième chapitre intitulé "Constructions des codes linéaires sur un anneau fini" est celui où nous élaborons différents types des codes et leur propriété caractéristique.

Chapitre Un

Préliminaires

1.1 Quelques éléments sur la théorie de groupes et des anneaux

1.1.1 Introduction

Au vue de l'importance des propriétés de structures algébriques (celle de groupes et d'anneaux) dans l'études des codes algébriques, il est indispensable de présenté certaines de ces propriétés associées a ces structures algébriques.

1.1.2 Généralités

Définition 1.1. .

Un groupe G est un ensemble muni d'une loi binaire "." et d'un élément appellé élément neutre de G noté e_G tel que, pour tous $x, y, z \in G$, on a :

i) $(x.y).z = x.(y.z)$ *(associativité de la loi).*

ii) Tout élement de G est symétrisable pour la loi "." c'est-à-dire que tout élément x de G possède un élément x' tel que $x.x' = e = x'.x$, l'élément x' est appellé l'inverse de x noté x^{-1}.

Proposition 1.1. .

Un sous ensemble non vide H de G est un sous groupes de G si et seulement si pour tout $x, y \in H$ $x.y \in H$ et $x^{-1} \in H$ où x^{-1} est l'inverse de x.

Exemple 1.1.1. .

Le centre d'un groupe de G noté $Z(G) = \{g \in G, gx = xg, x \in G\}$ est un sous groupe de G.

Définition 1.2. .

Soient H et G deux goupes un morphisme de groupes de G dans H est toute application

$\phi : G \longrightarrow H$ telle que pour tout $a, b \in G$, $\phi(ab) = \phi(a)\phi(b)$; par ailleurs ϕ est un monomorphisme(resp un épimorphisme), si de plus est une application injective(resp surjective) et que ϕ est un isomorphisme si de plus est une application bijective.

Définition 1.3. .

Un groupe G est monogène s'il est engendré par un seul de ses éléments de plus un tel groupe est cyclique s'il est d'ordre fini.

Soit H un sous groupe d'un groupe G, les classes à gauche respectivement à droite suivant H sont définies par $aH = \{ah, h \in H\}$, $Ha = \{ha, h \in H\}$ pour tout $a \in G$; dés lors il existe autant de classes à gauches que de classe à droite suivant H et par conséquent l'indice de H dans G se définit alors comme étant le nombre de classes distinctes à droite suivant H, il est noté $[G : H]$.

Théorème 1.1. *(lagrange).*

Soit G un groupe fini, l'ordre de tout sous groupe de G est un diviseur de l'ordre de G plus précisement on a $|G| = |H|\,[G : H]$.

Proposition 1.2. .

Un sous groupe H d'un groupe G est distingué lorsque pour tout $a \in G$, $Ha = aH$ on note $H\Delta G$. Dés lors, désignons par $\frac{G}{H}$ l'ensemble de toute les classes distintes suivant H alors $\frac{G}{H}$ est un groupe pour le produit des classes définit par $(aH).(bH) = abH$.

Preuve : $\frac{G}{H}$ est un ensemble non vide car la classe de e qui est H est l'élément neutre de $\frac{G}{H}$, de plus si (aH), (bH) sont deux éléments de $\frac{G}{H}$ alors abH est dans $\frac{G}{H}$ car $ab \in G$ donc $(aH).(bH)$ est dans $\frac{G}{H}$. Par ailleur pour tout $a \in G$, $(aH)^{-1} = a^{-1}H$ et $a^{-1} \in G$ donc $a^{-1}H$ est dans $\frac{G}{H}$, il suit par associativité et symétrique de G il s'ensuit que $\frac{G}{H}$ pour cette loi est un groupe.■

Proposition 1.3. .

Si G et K sont deux groupes et $\phi : G \longrightarrow K$ un morphisme de groupe alors $Ker(\phi)$ est un sous groupe distingué de G et $im(\phi)$ est isomorphe à $\frac{G}{Ker(\phi)}$ et on observe que si H et K sont deux sous groupes d'un groupe G tel que $K\Delta G$, alors $\frac{H}{H\cap K} \cong \frac{HK}{K}$.

Définition 1.4. .

Un ensemble A muni de deux loi + et . est un anneau si et seulement si :

i) $(A, +)$ est un groupe abélien.

ii) la loi . est associative et posséde un élément neutre noté 1_A.

iii). est distributive par rapport à l'addition.

si de plus la loi . est commutative, on dit que l'anneau A est commutatif et le neutre pour l'addition se note 0_A.

Exemple 1.1.2. .
$(\mathbb{Z}, +, .)$, $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$.

Définition 1.5. .
Soit $(A, +, .)$ un anneau unitaire, considérons la fonction $\phi : \mathbb{Z} \longrightarrow A$ tel que $\phi(n) = n.1_A$. Il vient que ϕ est un homomorphisme d'anneau et par conséquent $Ker(\phi)$ est un idéal de $\mathbb{Z}$ d'où $Ker(\phi) = k\mathbb{Z}$, $k \in \mathbb{N}$. On dit que la caractéristique de A est l'entier k.

Exemple 1.1.3. .
$caract(\mathbb{Z}) = 0$ et $caract(\mathbb{Z}_n) = n$, pour tout entier $n \in \mathbb{N}$.

Définition 1.6. .

- *Une partie B d'un anneau A contenant 0_A et stable pour les deux loi de A est un sous anneau de A ssi B muni des lois induites de celle de A est un anneau.*
- *Une partie I non vide d'un anneau A est un ideal si :*
  i) $(I, +)$ est un groupe abélien.
  ii) pour tout $a \in A$, $x \in I$; $ax \in I$, $xa \in I$.

Exemple 1.1.4. .
Dans $(\mathbb{Z}, +, .)$ les ideaux sont de la forme $(n\mathbb{Z}, +, .)$ pour tout $n \in \mathbb{N}$.

Définition 1.7. .
Soit A un anneau et $a \in A\backslash\{0\}$; a est un diviseur de zero s'il existe $b \neq 0$ tel que, $ab = 0$ et l'anneau A est intègre s'il est commutatif unitaire et ne possède pas de diviseur de zero.

Exemple 1.1.5. .
l'anneau $(\mathbb{Z}, +, .)$ est intègre.

Propriété 1.1. .

- *Soit I un ideal d'un anneau A avec $I \neq A$;*
  I est un ideal maximal si et seulement si pour tout ideal J de A, si $I \subseteq J$ alors $I \subseteq J$ ou $J = A$.
- *I est un ideal premier si et seulement si pour tout $(a, b) \in A \times A$, si $ab \in I$ alors $a \in I$ ou $b \in I$.*

Exemple 1.1.6. .
Dans $(\mathbb{Z}, +, .)$ les ideaux premiers sont les $(p\mathbb{Z}, +, .)$ avec p entier premier. Dans $(\mathbb{Z}_8, +, .)$ $\frac{2\mathbb{Z}}{8\mathbb{Z}}$ est maximal.

Théorème 1.2. .

Dans un anneaux unitaire A ; tout ideal maximal est premier.

Preuve : Soit I un idéal maximal, montrons que I est premier. En effet soit $(a, b) \in A \times A$ tel que $ab \in I$, par l'absurde supposons que $a \notin I$ et $b \notin I$ alors $I \subset (a) + I$ et $I \subset (b) + I$, Dés lors $((a) + I)((b) + I) = A^2 = A$ car A est unitaire ainsi $A \subseteq I$, Dés lors $I = A$ impossible.■

Théorème 1.3. .

Soit I un ideal d'un anneau A ; I est maximal si et seulement si $\frac{A}{I}$ est un corps.

Preuve : On sait que $\frac{A}{I}$ est un anneau unitaire car A l'est, De plus soit $a + I$ dans $\frac{A}{I}$ avec $a + I \neq I$ ainsi $a \notin I$ par suite $I \subset (a) + I$ de manière stricte ainsi $(a) + I = A$ car I est maximal, comme A est unitaire il existe $a' \in A$ et $i \in I$ tel que $1 = aa' + i$, Dés lors $aa' - 1 \in I$ c'est a dire $aa' + I = 1 + I$ en d'autre terme $(a + I)(a' + I) = 1 + I$ de ce fait, $a + I$ est inversible donc $\frac{A}{I}$ est un corps. Réciproquement, supposons que $\frac{A}{I}$ est un corps montrons que I est maximal ; il est clair que I est distint de A, soit J un ideal de A tel que $I \subseteq J, I \neq J$, soit $j \in J$ tel que $j \notin I$ comme $\frac{A}{I}$ est un corps il existe $l \notin I$ tel que $lj + I = 1 + I$; d'où $1 - lj \in I \subseteq J$ mais $j \in J$ et J un idéal donc $lj \in J$ par suite $1 \in J$. En somme $J = A$ il suit que I est un idéal maximal de A.■

Théorème 1.4. .

Soit I un ideal d'un anneau A ; I est premier si et seulement si $\frac{A}{I}$ est domaine d'intégrité.

Preuve : Suppossons que I est premier, soient a, b deux élément de A n'appatenant pas à I tel que $ab + I = I$, alors $ab \in I$ et comme I est premier il vient que $a \in I$ ou $b \in I$ c'est-à-dire que $a + I = I$ ou $b + I = I$. Dés lors, $\frac{A}{I}$ est domaine d'intégrité. Réciproquement, supposons que $\frac{A}{I}$ est un domaine d'intégrité non trivial alors il est clair que I est distint de A, soient a et b deux éléments de A tel que $ab \in I$ alors $ab + I = I$ et par hypothèse il suit que $a + I = I$ ou $b + I = I$ donc $a \in I$ ou $b \in I$ on déduit que I est premier.■

Définition 1.8. .

Soit $a, b \in A$, on dit que a divise b lorsque :

- $a \neq 0$
- *Il existe $u \in A$ tel que $b = au$.*

On dit aussi que a est un diviseur de b, ou que b est un multiple de a. On note $a \,|\, b$.

Deux éléments a et b de l'anneau A sont dit associés lorsque $a \,|\, b$ et $b \,|\, a$.

Exemple 1.1.7. .

Dans $A = \mathbb{Z}_{60}$, 5 et 25 sont associés de même 3 et 21.

Définition 1.9. .

Un élément $a \in A^*$, est dit irréductible lorsque :

- *a n'est pas inversible.*
- *pour tout $x, y \in A$ si $xy = a$ alors x est inversible ou y est inversible*

Définition 1.10. .

Un élément $b \in A^*$, est dit premier lorsque :

- *b n'est pas inversible.*
- *pour tout $x, y \in A$ si $b \,|xy$ alors $b \,|x$ ou $b \,|y$*

Définition 1.11. .

Un élément $c \in A^*$, est un pgcd(a, b) $a, b \in A^*$ lorsque :

- *$c \,|a$ et $c \,|b$.*
- *pour tout $x \in A$, $x \,|a$ et $x \,|b$ alors $x \,|c$*

Deux éléments a,b de A sont dits 1^{er} entre eux lorque tout diviseur commun de a et b est inversible.

Proposition 1.4. .

Soit A un anneau intègre

i) Un élément a de A est premier si et seulement si l'ideal (a) engendré pas a est premier et non nul.

ii) Un élément b de A est irréductible si et seulement si (b) est maximal parmi les ideaux propres principaux de A.

iii) Tout élément premier est irréductible.

Preuve : *i)* On a 'a' est premier si et seulement si

$$\begin{cases} \text{a} \neq 0\text{, a non inversible et} \\ pourtous x\text{,y} \in A \text{ si } b \,|xy \text{ alors } b \,|x \text{ ou } b \,|y \end{cases}$$

si et seulement si

$$\begin{cases} \text{a} \neq 0\text{, a non inversible et} \\ \text{xy} \in (a) \text{ alors } x \in (a) \text{ ou } y \in (a) \end{cases}$$

si et seulement si

$(a) \neq (0)$ et (a) est un ideal 1^{er}.

ii) Si b est un élément irréductible de A alors $b \neq 0$ et b non inversible ainsi l'ideal (b) engendré par b est une partie propre de A. Par ailleur si d est un élément de A tel que $(b) \subseteq (d)$ alors $b \in (d)$ dés lors il existe $u \in A$ tel que $b = du$ par conséquent d est inversible ou u est inversible(puisque b est irrréductible). Mais (d) est supposé étre un idéal propre de A il s'ensuit que $(b) = (d)$ (car pour u inversible on a $d = bu^{-1} \in (b)$). Réciproquement, supposons que (b) est maximal parmi les ideaux principaux propres alors $(o) \subseteq (b) \subseteq A$ avec $(o) \neq (b) \neq A$ ainsi $b \neq 0$ et b n'est pas inversible. Soient $x, y \in A$ tel que $b = xy$ alors $b \in (x)$ d'où $(b) \subseteq (x)$ par hypothése on déduit que $(b) = (x)$ ou $(x) = A$ par conséquent x est inversible ou $(b) = (x)$. Mais $(b) = (x) \Rightarrow \exists u \in A, x = bu$

$\Rightarrow x = xyu$

$\Rightarrow x(1 - yu) = 0$

$\Rightarrow 1 - yu = 0$ car A est un domaine d'intégrité

$\Rightarrow$ y est inversible.

iii) Soit a un élément 1^{er} de A et $x, y \in A$ tel que $a = xy$ alors $a \,|x$ ou $a \,|y$ sans nuire à la généralité supposons que $a \,|x$ alors $\exists u \in A$, $x = au$ donc $a = xy = auy$ ceci entraine que $1 = uy$ donc y est inversible. On déduit que x est invercible ou y est inversible et par conséquent a est irréductible.■

Définition 1.12. .

Un anneau A est dit principal lorsque tout ces idéaux sont principaux, c'est-à-dire que tout idéal I de A est de la forme $I = aA = \{ax, x \in A\}$ *avec* $a \in A$.

Corollaire 1.1. .

Soit ***A*** *un anneau intègre*

(*i*) *tout associé d'un élément premier(respectivement irréductible) est premier (respectivement irréductible).*

(*ii*) *les seuls diviseurs d'un élément irréductible sont ses associés et les inversibles.*

(*iii*) *Si A est un domaine principal, alors un élément est premier si et seulement si il est irréductible.*

Définition 1.13. .

Un anneau A est dit factoriel lorsque les conditions suivantes sont vérifiées

(*i*) *Tout élément non nul et non inversible a de A admet une décomposition* $a = c_0 c_1 ... c_n$, *où les* c_i *sont des irréductibles.*

(*ii*) *Si* $a = c_0 c_1 ... c_n$ *et* $a = d_0 d_1 ... d_m$ *sont deux décompositions de a en facteur d'irréductibles alors* $m = n$, $\exists \sigma \in s_{n+1}$ *tel que* $c_i = d_{\sigma(i)}$ $0 \leq i \leq n$.

Théorème 1.5. .

Tout domaine principal est factariel.

(i) Si A est intègre, alors A[X] est intègre.

(ii) Si A est factariel, alors A[X] est factoriel.

(iii) Si A est un corps, alors A[X] est un domaine principal

Exemple 1.1.8. .

$\mathbb{Z}[X]$ est un anneau factoriel qui n'est pas principal.

Définition 1.14. .

Un anneau A est dit euclidien s'il est un anneau unitaire commutative et s'il existe une application $\rho : A^* \longrightarrow \mathbb{N}$ satisfaisant les clauses suivantes :

i) Pour tout $a, b \in A$, si $ab \neq 0$ alors $\rho(ab) \geq \rho(a)$.

ii)Pour tout $a, b \in A$ si $b \neq 0$ alors il existe un unique couple $(q, r) \in A \times A$ tel que $a = bq + r$ avec $r = 0$ ou $\rho(r) \leq \rho(b)$.

Théorème 1.6. .

On a la chaîne suivante :

Tout domaine est euclidien $\Rightarrow$ tout domaine est principal $\Rightarrow$ tout domaine est factoriel.

Exemple 1.1.9. .

$\mathbb{Z}[X]$ est un anneau factoriel qui n'est pas principal, et par conséquent n'est pas Euclidien.

Définition 1.15. .

Un anneau est semi-simple s'il est isomorphe à un produit de corps.

Théorème 1.7. *(Propriété universelle des produits directs d'anneaux)*

Soit $\{A_i\}_{i \in I}$ une famille non vide d'anneaux, S un anneau et $\rho_i : S \longrightarrow A_i, i \in I$ une famille de morphisme d'anneaux, alors il existe un unique morphisme d'anneau $\rho : S \longrightarrow \prod_{i \in I} A_i$ tel que $\pi_i \rho = \rho_i$ pour tout $i \in I$.

Théorème 1.8. *(reste chinois)*

Soit $\{I_i, 0 \leq i \leq n\}$ une famille d'ideaux de A tel que pour tout $i, j \in \{0, ..., n\}$ on a $I_i + J_i = A$ alors il existe un isomorphisme entre $\frac{\boldsymbol{A}}{\cap_{0 \leq i \leq n} I_i}$ et $\frac{\boldsymbol{A}}{I_1} \times \frac{\boldsymbol{A}}{I_2} \times ... \times \frac{\boldsymbol{A}}{I_n}$

Exemple 1.1.10. .

$\mathbb{Z}$ est un anneau semi simple.

Remarque 1.1.1. .

Soient A,B deux anneaux tel que $A \subseteq B$, si $f \in A[X]$, $f = \sum_{i=0}^{n} a_i X^i$. En considérant $\hat{f}$

de B vers B tel que $\hat{f}(b) = \sum_{i=0}^{n} a_i b^i$ pour tout $b \in B$, pour tout $u \in B$, $A[u] = \{\hat{h}(u), h \in A[X]\}$ est un sous anneau de B appelé anneau engendré par u sur A. Si $u \in B$ et $\hat{f}(u) = 0$ on dit que u est une racine de f. En considérant $f' = \sum_{i=1}^{n} i a_i b^{i-1}$ la dérivée formelle de f, si $u \in B$, alors u est une racine multiple de f si et seulement si $\hat{f}(u) = 0 = \hat{f}'(u)$

Théorème 1.9. .

Soit B un anneau intègre, K un corps contenu dans B et $f \in K[X]$.
(i) Si f et f' sont premier entre eux, alors f n'admet pas de racine multiple dans B.
(ii) Si f est irréductible dans $K[X]$ et admet une racine dans B, alors f admet une racine multiple si et seulement si $f' = 0$.

Définition 1.16. .

Soit A un anneau intègre et $f = \sum_{i=0}^{n} a_i X^i$ un polynôme de $A[X]$, on dit que f est primitif losque tout pgcd de $(a_0, a_1, ..., a_n)$ est inversible dans A.

Remarque 1.1.2. (Gauss)
Si A est un domaine principal, le produit de deux polynôme primitifs est primitifs.

Théorème 1.10. .

Soit A un domaine principal K son corps des fractions et f un polynôme primitif de $A[X]$ avec $dgr(f) \geq 1$ alors f est irréductible dans $A[X]$ si et seulement si f est irréductible dans $K[X]$,

Théorème 1.11. *(Eisenstein)*

Soit A un domaine principal, K son corps de fractions et $f = \sum_{i=0}^{n} a_i X^i \in A[X]$ avec $n \geq 1$, désignons par p un élément irréductible de A tel que

$$\begin{cases} p | a_i \,,\ 0 \leq i \leq n-1 \\ \neg(p \,| a_n) \ \ et \ \neg(p^2 \,| a_0) \end{cases}$$

alors f est irréductible dans $K[X]$.

Exemple 1.1.11. .

Soit p un nombre naturel premier et n un nombre naturel non nul alors $X^n - p$ est irréductible dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$, et pour tout $a \in \mathbb{Q}^*$ on a $a(X^n - p)$ qui est irréductible dans $\mathbb{Q}[X]$.

Proposition 1.5. *(Krull)*

Soit A un anneau unitaire ; tout idéal distint de A est contenu dans un idéal maximal de A. Dés lors tout anneau posséde aumoins un idéal maximal.

Définition 1.17. .

Un anneau unitaire $(A,+,.)$ est dit local s'il admet un unique ideal maximal qu'on note M.

Exemple 1.1.12. .

Dans $(\mathbb{Z}_2,+,.)$ L'ideal null est l'unique ideal maximal.

Corollaire 1.2. .

L'ensemble des éléments non inversible d'un anneau local A constitue un idéal de A ; dans certains cas cet ensemble constitue l'idéal maximal de A.

Théorème 1.12. .

Soit I un idéal d'un anneau A, l'ensemble $\frac{A}{I}$ déduit de son groupe additif est appélé ensemble quotient de A et en considérant les opérations binaires $\bar{+}$ et $\bar{\times}$ obtenu comme suit sur $\frac{A}{I}$, on a pour tout $a,b\in A$

$$\begin{cases} (a+I)\bar{+}(b+I)=a+b+I \\ (a+I)\bar{\times}(b+I)=ab+I \end{cases}$$

Dés lors, $\frac{A}{I}$ muni des opérations binaires $\bar{+}$ et $\bar{\times}$ est appélé anneau quotient de A par l'ideal I.

Définition 1.18. .

Soit A un anneau unitaire, A est dit noethérien si tout ensemble non vide d'idéaux de A passéde un élément maximal.

Définition 1.19. .

Soit A un anneau unitaire, A est dit Artinien si tout ensemble non vide d'idéaux de A posséde un élément minimal.

Proposition 1.6. .

Soit A un anneau unitaire ; une suite croissante $I_1\subseteq I_2\subseteq I_3\subseteq ...$ d'idéaux de A est dite stationnaire s'il existe $n_0\in\mathbb{N}^*$ tel que $I_{n_0}=I_n$, pour tout $n\geq n_0$.

Théorème 1.13. .

Soit A un anneau unitaire et I un idéal de A, les assertions suivantes sont équivalentes :

i) A est un anneau noethérien

ii) Toute suite croissante d'idéaux de A est stationnaire.

iii) Tout idéal de A est finiment engendré.

iv) l'idéal I et l'anneau $\frac{A}{I}$ sont noethériens.

Preuve : Supposons que A est un anneau noethérien, soit $\{I_n\}_{n\in N}$ une suite croissante d'idéaux de A, comme $\{I_n\}_{n\in N}$ est un ensemble d'idéaux non vide et que A est un anneau noethérien, cet ensemble admet un élément maximal noté I_k, $k \in \mathbb{N}$, pour tout $n \geq k$ on a $I_k \subseteq I_n$ il suit que $I_k = I_n$ pour tout $n \geq k$ à cause de la maximalité de I_k donc la suite $\{I_n\}_{n\in N}$ est stationnaire. Réciproquement, $ii) \Rightarrow i)$, en effet, si $\mathcal{F}$ est un ensemble d'idéaux non vide de A toute chaîne d'ideaux de A est stationnaire par conséquent $\mathcal{F}$ admet un élément maximal, donc A est un anneau noethérien, dés lors $ii) \Leftrightarrow i)$. Supposons $i)$ montrons $iii)$ soit I un idéal de A, si I est trivial alors I est finiment engendré. Par contre soit $a \in I$ $a \neq 0$ on a $aA \subseteq I$ désignons par $\mathcal{F}$ l'ensemble d'idéaux finiment engendré J tel que $J \subseteq I$; il est clair que $\mathcal{F}$ est non vide et comme A est un anneau noethérien, soit K un élément maximal de $\mathcal{F}$. On a $K \subseteq I$ soit $a \in I$, $aA + K \subseteq I$ et $aA + K$ est finiment engendré donc $aA + K \in \mathcal{F}$ de plus $K \subseteq aA + K$ par maximalité de K on obtient que $K = aA + K$ d'où $a \in K$ donc $I \subseteq K$ par suite $I = K$, enfin I est un idéal finiment engendré. Réciproquement $iii) \Rightarrow ii) \Leftrightarrow i)$, en effet soit $\{I_n\}_{n\in N}$ une suite croissante d'idéaux de A, posons $G = \cup_{n\in N} I_n$ on remarque vue la croissance de la suite $\{I_n\}_{n\in N}$ que G est un idéal de A, dés lors G est finiment engendré soient $a_1, a_2, ..., a_k$ dans A tel que $G = A(a_1, a_2, ..., a_k)$ ainsi il existe $I_{n_1}, I_{n_2}, ..., I_{n_k}$ de la suite $\{I_n\}_{n\in N}$ tel que $a_i \in I_{n_i}$, pour tout $i \in \{1, ..., k\}$. Par conséquent $G = \cup_{1\leq i\leq k} I_{n_i}$ posons $l = max_{1\leq i\leq k}\{n_i\}$ on déduit par croissante de la suite $\{I_n\}_{n\in N}$ que $G = I_l$; soit $n \geq l$ $I_n \subseteq G = I_l$ c'est-à-dire que $I_n \subseteq I_l$ donc $I_n = I_l$ pour tout $n \geq l$ il vient que $\{I_n\}_{n\in N}$ est stationnaire. Donc $iii)$ $\Rightarrow i)$ ainsi $iii) \Leftrightarrow i)$. Si $ii)$ est satisfaite alors il en est le cas de $iv)$. réciproquement si $iv)$ est satisfaite alors en considérant une chaîne de $\{I_n\}_{n\in N}$, on remarque que la chaîne $\{\frac{I_n}{I_0}\}_{n\in N}$ est stationnaire dans $\frac{A}{I_0}$, soit $\frac{I_k}{I_0}$ sa station on déduit que I_k est la station de la chaîne $\{I_n\}_{n\in N}$. Donc $ii)$ est vérifié et par conséquent $iv) \Leftrightarrow ii)$. On peut conclut que les assertions $i)$,$ii)$, $iii)$ et $iv)$ sont équivalent.■

Théorème 1.14. .

Soit A un anneau unitaire et I un idéal de A, les assertions suivantes sont équivalentes :

i) A est un anneau Artinien

ii) Toute suite décroissante d'idéaux de A est stationnaire.

iii) l'idéal I et l'anneau $\frac{A}{I}$ sont artiniens.

Preuve : On prossède de la même façon que pour les anneaux noethériens pour élaboré l'équivalence des assertions précédentes.■

Exemple 1.1.13. .

Tout anneau fini est artinien et noethérien.

1.2 Anneau de Galois R et ses paramètres

Définition 1.20. .

Un anneau fini R est un anneau de galois s'il est commutatif unitaire et si l'ensemble de tous les diviseurs de zèro est de la forme pR, p étant un entier premier. Dés lors, on pourrait considérer les corps de galois comme des anneaux de galois ne contenant pas de diviseurs de zéro.

Exemple 1.2.1. .

pour $A = \mathbb{Z}_2$ et $P = x^2 + x + 1$, l'anneaux suivant $\frac{A[x]}{(x^2+x+1)}$ est un anneau de galois.

Considérons R un anneau de Galois de caractérictique p^n et $D = pR$ l'ensemble des diviseurs de zèro de R. Désignons pas "\" le symbole représentant la soustration ensembliste. le groupe multiplicatif R^* de l'anneau R est :
$R^* = R\backslash pR = R\backslash D$ car les diviseurs de zèro sont les seuls éléments non inversible dans un anneau fini. De plus l'anneau $\bar{R} = \frac{R}{D}$ est le corps de Galois $GF(q)$ (q étant une puissance de p ; p^r). Notons $\overline{1}$ l'élément neutre de $\bar{R}$. Nous avons donc $\overline{1} = 1 + D$. Posons $D^t = p^t R$ et $t \in \{0, ..., n-1\}$, on a alors $D^{n-1} \neq 0$ et $D^n = 0$ et la chaine suivante d'ideaux admet des inclusions strites : $R = D^0 \supset D = pR \supset ... \supset D^{n-1} = p^{n-1}R \supset D^n = p^n R = 0$.

Théorème 1.15. .

Le nombre d'élément de l'anneau R et du groupe multiplicatif R^* sont :

$$|R| = q^n$$

,

$$|R^*| = (q-1)q^{n-1}$$

.

Preuve : Soit $t \in \{0, ..., n-1\}$ on a l'égalité

$$\left| \frac{p^t R}{p^{t+1} R} \right| = q.$$

Car $\frac{p^t R}{p^{t+1}R}$ est isomorphe à $\bar{R} = \frac{R}{pR}$. Par ailleur posons $R_t = \frac{p^t R}{p^{t+1}R}$, R est visiblement un espace vectoriel sur $\bar{R} = GF(q)$ et on a $dim_{\bar{R}} R_t = 1$. Considérons $\alpha \in p^t R \backslash p^{t+1} R$, nous avons $R\alpha = p^t R$ et $\bar{R}\alpha = R_t$ Ainsi, $|R| = q^n$ et le cardinal de R^* découle immédiatemment puisque $|R^*| = |R| - |pR|$ et $|pR| = \frac{|R|}{q}$ et par conséquent $|R^*| = q^n - q^{n-1} = (q-1)q^{n-1}$. ■

Dés lors, l'anneau de Galois est noté $GR(p^n, r)$ où p^n est la caractéristique de ce dernier.

1.2.1 Extension d'un anneau de Galois R

$\bar{R} = \frac{R}{pR}$ est appelé corps de classe residuelle de l'anneau de galois R de caractéristique p^n. Ainsi il exite un épimorphisme d'anneau naturel $R \longrightarrow \bar{R}$ qui peut s'étendre en épimorphisme d'anneau des polynômes $R[X] \longrightarrow \bar{R}[X]$ tel que pour tout $A(X) = \sum_{k=0}^{n} a_k X^k \in R[X]$ on associe $\bar{A}(X) = \sum_{k=0}^{n} \bar{a}_k X^k \in \bar{R}[X]$.

Définition 1.21. .
Un b-polynôme (basic irreducible polynomial en anglais) $f(X) \in R[X]$ sur R est un polynôme unitaire tel que $\bar{f}(X)$ est un polynôme irréductible sur le corps $\bar{R}$.

Nous allons montrer que la donnée d'un b-polynôme f de degré m sur R permet de construire un plus gros anneau en adjoignant à R une racine de f une telle extension est appelé une G-extension de R. De plus le b-polynôme $f(X) \in R[X]$ permet de considérer la G-extension $S = \frac{R[X]}{(f(X))}$.

Théorème 1.16. .
Soit R un anneau de Galois de q^n éléments de caractéristique p^n. Soit $f(X)$ un b-polynôme de dégre m alors
l'anneau $S = \frac{R[X]}{(f(X))}$ est un anneau de galois de paramètre $caract(S) = p^n$ et $|S| = q^{nm}$.

Preuve : On sait que $caract(S) = caract(R) = p^n$ et le fait que S vue comme R-module on obtient $|S| = |R|^m = q^{nm}$, trivialement les éléments de pS sont des diviseurs de zéro puisque pR posséde la même propriété ; vérifions maintenant que les éléments de $S \backslash pS$ sont des inversibles. Soit α un élément de $S \backslash pS$, il peut s'écrire de façon unique comme suit :

$$\alpha = [A(X)]_f = A(X) + f(X)R[X]$$

, où $A(X) \in R[X]$, $deg(A(X)) < m$ et $\bar{A}(X) \neq 0$. nous avons alors $(\bar{A}(X), \bar{f}(X)) = \bar{1}$ (car $\bar{f}(X)$ est irréductible et $degr(\bar{A}(X)) < m$) et d'aprés bezout, il existe deux polynômes $U(X)$ et $V(X)$ appartenant à $R[X]$ qui vérifient l'identité $U(X)\bar{A}(X) + V(X)\bar{f}(X) = \bar{1}$ en d'autre termes, il existe $B(X) \in R[X]$ tel que $U(X)A(X) + V(X)f(X) = 1 + pB(X)$. Ainsi $[U(X)]_f[A(X)]_f = [1 + pB(X)]_f$. On voit clairement que $[1 + pB(X)]_f$ est inversible puisque $[1 + pB(X)]_f^{p^{n-1}} = [1]_f$. Enfin l'élément α est donc inversible. ■

L'anneau S peut aussi être vu comme une extension de degré m de R. il existe un b-polynôme dans $R[X]$ pour n'importe quel degré m donné. Ainsi, par le résultat pré-

cédent, nous avons les deux propriétés suivantes concernant l'existence d'un anneau de Galois R et pour tout entier m, il existe une G-extension de degré m de R.■

Propriété 1.2. .

Pour tout anneau de Galois R et tout entier m, il existe une G-extension de degré m de R.

Preuve : il suffit de remarquer que pour tout entier m il existe un b-polynôme irréductible de degré m et d'après le théorème précédent on a le resultat.■

Propriété 1.3. .

Pour tout p premier $m, n \in \mathbb{N}$, il existe un anneau de Galois S de caractéristique p^n ayant p^{nm} éléments.

Preuve : D'aprés la propriété précédente il existe un anneau de Galois R de caractéristique p^n. De plus avec l'entier m on en déduit une G-extension de dégré m de R.■

Exemple 1.2.2. .

Pour $R = \mathbb{Z}_{2^3} = \mathbb{Z}_8$ l'anneau des entiers modulo 8, Posons $S = \frac{R[X]}{(f(X))}$ avec $f(X) = X^3 + 6X^2 + 5X + 7$ le polynôme f est un b-polynôme et $\bar{f}(X) = X^3 + X + 1$; l'ensemble des diviseurs de zéro de S est $D = 2S$ de cardinal $|D| = 4^3$ et le cardinal des inversibles est $|S^*| = 8^3 - 4^3 = (2^3 - 1)4^3$; l'anneau S est une G-extension de degré 3 de R de manière générale. si l'on considère un élément α de S le sous anneau $\{A(\alpha) : A(X) \in R[X]\}$ de R est noté $R[\alpha]$.

c'est une extension de l'anneau R par α. Dans l'exemple précédent. $S = R[X]$ où α est une racine de $f(X)$. Ainsi l'anneau S peut donc s'écrire comme le module suivant $< 1, \alpha, \alpha^2 >$.

Propriété 1.4. .

Soient $A(X) \in R[X]$ et $\alpha \in S$ tels que $\bar{A}(\bar{\alpha}) = \bar{0}$ et $\bar{A}'(\bar{\alpha}) \neq \bar{0}$, alors il existe une unique racine $\beta \in S$ du polynôme $A(X)$ telle que $\bar{\alpha} = \bar{\beta}$.

Théorème 1.17. .

Soit S une G-extension de degré m de R et $f(X)$ un b-polynôme sur R de degré k alors

i) le polynôme $f(X)$ a une racine dans S ssi k divise m.

ii)si k divise m, $f(X)$ admet exactement k racines distinctes $\alpha_1, ..., \alpha_k$ dans S modulo l'ideal pS, $f(X) = (x - \alpha_1)...(x - \alpha_k)$.

iii)Pour tout élément $\alpha \in S$, on a $S = R[\alpha]$ ssi α est une racine du b-polynôme de degré m sur R.

Preuve : Voir[8].■

Corollaire 1.3. .

Soit S un anneau de Galois de caractéristique p^n et de cardinalité p^{nm} alors $S \cong \frac{\mathbb{Z}_{p^n}[X]}{(f(X))}$ où $f(X)$ est un b-polynôme de degré m sur $\mathbb{Z}_{p^n}$. Notons un tel anneau $GR(p^n, m)$, dès lors deux anneaux de Galois sont isomorphes ssi ils ont même cardinalité et caractéristique.

Remarque 1.2.1. .

$GR(p^n, 1) = \mathbb{Z}_{p^n}$, $GR(p, m) = \mathbb{F}_{p^m}$.

Théorème 1.18. .

Soit $S = GR(p^n, m)$ le groupe multiplicatif des inversibles de S peut s'écrire comme le produit direct de deux groupe $S^* = G_1 \times G_2$ où

i)G_1 est un groupe cyclique d'ordre $p^m - 1$.

ii)G_2 est un groupe d'ordre $p^{(n-1)m}$ tel que.

a) si p est impair ou si $p = 2$ et $n \leq 2$, alors G_2 est un produit direct de m groupe cyclique chacun d'ordre p^{n-1}.

b) si $p = 2$ et $n \leq 3$, alors G_2 est un produit direct d'un groupe cyclique d'ordre 2, un groupe cyclique d'ordre 2^{n-2} et $m - 1$ groupes cyclique chacun d'ordre 2^{n-1}.

Preuve : Voir[8].■

Corollaire 1.4. .

Soient $R = GR(p^n, k)$ et $R' = GR(p^n, m)$ deux anneaux de Galois, on a R' est une extension de R si et seulement si k divise m.

Preuve : Si k divise m on a $\bar{R} \subseteq \bar{R}'$ et par conséquent R' est extension de R puisqu'ils ont même caractéristique. Réciproquement, si R' est une extension de R alors $\bar{R} \subseteq \bar{R}'$ donc k divise m, d'où le résultat.■

1.3 Relèvement de Hensel-Théorème de Hensel

Lemme 1.1. *(Lemme de Hensel).*

Soit p un nombre premier k un entier supérieur ou égal à 2 et $P \in \mathbb{Z}_{p^k}[X]$ tel que $Pmodp = QR$, pour tout $Q, R \in \mathbb{Z}_p[X]$ deux polynômes unitaires et premiers entre eux alors il existe un couple $(Q^{(k)}, R^{(k)})$ de polynômes unitaires de $\mathbb{Z}_{p^k}[X]$ tel que :

i) $P = Q^{(k)}R^{(k)}$.

ii) $Q^{(k)}modp = Q$ et $R^{(k)}modp = Q$.

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

$\mathbb{Z}_p$ étant un corps on sait que $\mathbb{Z}_p[X]$ est principal et donc factoriel ainsi deux éléments $Q, R \in \mathbb{Z}_p[X]$ sont tel que $Pmodp = f_1^{n_1} f_2^{n_2} ... f_t^{n_t}$ où $f_1^{n_1}, f_2^{n_2}, ..., f_t^{n_t}$ sont des polynômes irréductibles de $\mathbb{Z}_p[X]$, $n_1, ..., n_t$ des nombres positifs. On peut donc généraliser ce lemme par réccurence sur le nombre de facteurs, afin d'obtenir une factorisation de tout polynôme de $\mathbb{Z}_{p^k}[X]$ à partir de sa factorisation dans $\mathbb{Z}_p[X]$.

Théorème 1.19. .

Soient p un nombre premier, k un entier supérieur ou égal à 2 et $P \in \mathbb{Z}_{p^k}[X]$ un polynôme unitaire, tel que $Pmodp = f_1^{n_1} f_2^{n_2} ... f_t^{n_t}$ la factorisation de P dans $\mathbb{Z}_p[X]$ où $f_1^{n_1}, f_2^{n_2}, ..., f_t^{n_t}$ sont des polynômes irréductibles de $\mathbb{Z}_p[X]$, $n_1, ..., n_t$ des nombres positifs. Alors il existe un t-uplet $(g_1^{(k)}, ..., g_t^{(k)})$ de polynômes unitaires de $\mathbb{Z}_{p^k}[X]$ tel que :
i) $P = g_1^{(k)} g_2^{(k)} ... g_t^{(k)}$.
ii) $g_i^{(k)} modp = f_i^{n_i}$.
iii) les $g_i^{(k)}$ sont deux à deux premiers entre eux.

Définition 1.22. .

Soient Q et R deux polynômes à coefficients constant dans $\mathbb{Z}_p$ tel que $X^n - 1 = QR$ où p et n sont premiers entre eux ; alors le relevé de hensel d'ordre k de Q est le polynôme $Q^{(k)}$ de $\mathbb{Z}_{p^k}[X]$ du couple $(Q^{(k)}, R^{(k)})$ tel qu'énoncé au lemme de hensel.

Proposition 1.7. .

Soit $Q \in \mathbb{Z}_p[X]$ un facteur de $X^n - 1$ dans $\mathbb{Z}_p[X]$; son relevé de hensel d'ordre k divise $X^n - 1$ dans $\mathbb{Z}_{p^k}[X]$.

Preuve : On a $(X^n - 1) modp = QR$, $R \in \mathbb{Z}_p$; par définition de $Q^{(k)}$, $X^n - 1 = Q^{(k)} R^{(k)}$ dans $\mathbb{Z}_{p^k}[X]$ où $R^{(k)}$ est le relevé d'ordre k de R dans $\mathbb{Z}_{p^k}[X]$.■

Définition 1.23. .

Lorsque Q est irréductible et primitif ses relevés sont appelés les b-polynômes.

la proposition qui suit nous décrit un algorithme itératif de calcul du relevé de hensel d'un polynôme pour $p = 2$.

Proposition 1.8. *(Calcul du relevé de Hensel binaire)*

Soient $Q \in \mathbb{Z}_2[X]$ un facteur de $X^{2^r - 1} - 1$ et $Q^{(k)} \in \mathbb{Z}_{2^k}[X]$ son relevé de hensel d'ordre k. Posons $Q^{(k)} = P(X) - I(X)$ où P est le polynôme qui contient les monômes de degrés pair et I est celui contenant les monômes de degré impair. On a alors $Q^{(k+1)}(X) = -^{+}(P^2(X) - I^2(X))$, les opérations étant faites dans $\mathbb{Z}_{2^{k+1}}[X]$ et le signe étant choisi pour que $Q^{(k+1)}(X)$ soit unitaire.

Preuve : Comme le polynôme $P^2(X) - I^2(X)$ n'a que des monômes de degré pair, on définit $f \in \mathbb{Z}_{2^{k+1}}[X]$ tel que $f(X^2) = -^+(P^2(X) - I^2(X))$. nous avons $f(X^2) = -^+(P^2(X) - I^2(X)) = Q(X^2)$ dans $\mathbb{Z}_2[X]$, car pour tout $H \in \mathbb{Z}_2[X]$ on a $H^2(X) = H(X^2)$ ainsi $f(X) mod 2 = Q^{(k)} mod 2 = Q(X)$. Il reste à vérifier que f divise $X^{2^r-1} - 1$ dans $\mathbb{Z}_{2^{k+1}}[X]$, $f(X^2) = -^+(P(X) - I(X))(P(X) + I(X)) = -^+Q^{(k)}(X)Q^{(k)}(-X)$ mais les opérations étant faites dans $Z_{2^{k+1}}[X]$ on a $Q^{(k)}$ qui divise $X^{2^r-1} - 1$ dans $Z_{2^k}[X]$ car relevé d'ordre k de $Q \in \mathbb{Z}_2[X]$. Ainsi, $X^{2^r-1} - 1 = Q^{(k)}(X)A(X) + 2^k B(X)$ où $A, B \in \mathbb{Z}_{2^{k+1}}[X]$; Dés lors on a :

$$\begin{aligned} X^{2^{r+1}-2} - 1 &= (X^{2^r-1} - 1)(X^{2^r-1} + 1) \\ &= -(X^{2^r-1} - 1)((-X)^{2^r-1} + 1) \\ &= -(Q^{(k)}(X)A(X) + 2^k B(X))(Q^{(k)}(-X)A(-X) + 2^k B(-X)) \\ &= -Q^{(k)}(X)Q^{(k)}(-X)A(X)A(-X) - 2^k(Q^{(k)}(X)A(X)B(-X) + Q^{(k)}(-X)A(-X)B(X)). \end{aligned}$$

Posons $\nabla(X) = Q^{(k)}(X)A(X)B(-X) + Q^{(k)}(-X)A(-X)B(X)$ et $A(X) = P_a(X) - I_a(X)$ et $B(X) = P_b(X) - I_b(X)$, avec P_a, P_b les polynômes ne contenant que les mônomes de dégrés pair et I_a, I_b ceux de degré impair. Par suite,

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

Ainsi, $X^{2^{r+1}-2} - 1 = Q^{(k)}(X)Q^{(k)}(-X)M(X) + 2^{k+1}N(X)$ où $M, N \in Z_{2^{k+1}}[X]$. D'où $X^{2^{r+1}-2} - 1 = f(X^2)M(X) + 2^{k+1}N(X)$ ce qui prouve que $f(X^2)$ divise $X^{2^{r+1}-2} - 1$ dans $Z_{2^{k+1}}[X]$ et par conséquent que $f(X)$ divise $X^{2^r-1} - 1$ dans $Z_{2^{k+1}}[X]$.■

1.3.1 Application : Construction des anneaux de Galois GR($2^n, r$)

Pour contruire un anneau de Galois $GR(2^n, r)$, on factorise le polynôme $X^{2^r-1} - 1$ dans $\mathbb{Z}_2[X]$ et on considére un facteur primitif et irréductible Q de degré r, puis on détermine de proche en proche son relevé de Hensel $Q^{(n)}$ d'ordre n sachant que Q est son propre relevé d'ordre 1. Par conséquent, l'anneau $\frac{\mathbb{Z}_{2^n}[X]}{id(Q^{(n)})}$ est l'anneau de Galois $GR(2^n, r)$.

Exemple 1.3.1. .

- Construction de l'anneau de Galois $GR(2^2;2)$,
  $X^3-1=(X-1)(X^2+X+1)$ dans $\mathbb{Z}_2[X]$.
  On a $Q=Q^{(1)}=X^2+X+1$, posons $P_1=X^2+1$ et $I_1=-X$, $(P_1(X))^2=X^4+2X+1 mod 4$ et $(I_1(X))^2=X^2 mod 4$, par ailleur $Q^{(2)}(X^2)=(X^4+X^2+1) mod 4$ ainsi $Q^{(2)}(X)=(X^2+X+1)$ donc $GR(2^2;2)=\frac{\mathbb{Z}_4[X]}{id(X^2+X+1)}$
- Construction des anneaux de Galois $GR(2;3)$, $GR(2^2;3)$, $GR(2^3;3)$.
  Cas de $GR(2;3)$,
  on a $X^7-1=(X-1)(X^3-X+1)(X^3+X^2+1)$.
  Posons $Q=Q^{(1)}=X^3+X^2+1$ Q est son propre relevé de Hensel d'ordre 1 et est primitif et irréductible, d'où $GR(2;3)=\frac{\mathbb{Z}_2[X]}{id(X^3-X+1)}$.
  Cas de $GR(2^2;3)$,
  posons $P_1=1$ et $I_1=-X^3-X$; $(P_1(X))^2=1 mod 4$; $(I_1(X))^2=(X^6+2X^4+X^2) mod 4$, $Q^{(2)}(X^2)=(X^6+2X^4+X^2-1) mod 4$ d'où $Q^{(2)}(X)=(X^3+2X^2+X-1) mod 4$ est le relevé d'ordre 2 de Q. Donc $GR(2^2;3)=\frac{\mathbb{Z}_4[X]}{id(X^3+2X+X-1)}$.
  Cas de $GR(2^3;3)$,
  posons $P_2=2X^2-1$ et $I_2=-X^3-X$; $(P_1(X))^2=(4X^4-4X^2+1) mod 8$ et $(I_2(X))^2=(X^6+2X^4+X^2) mod 8$, avec $Q^{(3)}(X^2)=(X^6+6X^4+5X^2+7) mod 8$ il suit que $Q^{(3)}(X^2)=(X^6+6X^4+5X^2+7) mod 8$ est le relevé d'ordre 3 de Q donc $GR(2^3;3)=\frac{\mathbb{Z}_8[X]}{id(X^3+6X^2+5X+7)}$.
  Dès lors, si on se donne un corps fini $\mathbb{F}_q$ où $q=p^r$ et qu'il est necessaire de construire un anneau de Galois dont le corps residuel est $\mathbb{F}_q$ on factorise $X^{p^r-1}-1$ dans $\mathbb{Z}_p[X]$ et par suite on considére un facteur irréductible et primitif Q de degré r, puis on détermine le relevé $Q^{(n)}$ d'ordre n de Q et on considére l'anneau $\frac{\mathbb{Z}_{2^n}[X]}{id(Q^{(n)})}$ qui est l'anneau de Galois $GR(p^n,r)$ ayant pour corps residuel $\mathbb{Z}_p[X]$. Lorsque $p=2$ nous avons un algorithme de calcul du relèvement de Hensel d'un polynôme.

Remarque 1.3.1. .

Tout corps fini est un anneau de Galois.

Chapitre Deux

Théorie des codes correcteurs d'erreurs

2.1 Introduction

La transmission d'informations dans l'air "information à envoyé par satellite par exemple où par des câbles "lecture d'un CD"est souvent lié à des pertubations. c'est pour cela qu'il convient d'introduire les codes correcteurs d'erreurs. En d'autres termes que l'on doit coder les informations à envoyer de maniére judicieuse afin de pouvoir justement détecter et corriger d'éventuels problémes sous réserve qu'ils ne soient pas trop nombreur. En fait, le technicien connaît à l'avance la qualité de la transmission et aura effectué des tests statistiques pour prévoir le nombre mais pas la position des erreurs. Dans la suite on va présenter la théorie des codes de maniére générale par suite nous donnerons certains détails sur les codes linéaires.

2.1.1 Généralités

Définition 2.1. .

Soit A un anneau

i) Un code $\mathcal{C}$ sur A de longueur n est un sous ensemble $\mathcal{C}$ de A^n.

ii) Soit $\mathcal{C}$ un code de longueur n sur A.

On appelle distance de Hamming entre deux points x et y de A^n l'application d_H défini de $A^n \times A^n \to \mathbb{N}$

$(x, y) \longmapsto d_H(x, y) = card\{i \in \{1, ..., n\}/x_i \neq y_i\}$.

Posons $d = min\{d_H(a, b); a, b \in \mathcal{C}, a \neq b\}$ appelé distance minimal du code $\mathcal{C}$. Dés lors, un tel code est noté $\mathcal{C}(n, d)$. Sa capacité théorique de correction est donnée par : $t = \left\lfloor \frac{d-1}{2} \right\rfloor$

Propriété 2.1. .

nous vérifions aisement que la distance de Hamming est bien une distance sur $\mathcal{C}$.

Preuve : Soit $x = (x_1, ..., x_n)$, $y = (y_1, ..., y_n)$ et $z = (z_1, ..., z_n)$ des mots de $\mathcal{C}$.

- $d_H(x,y) = card\{i \in \{1,...,n\}/x_i \neq y_i\} \geq 0$.
- Supposons qu'on a $d_H(x,y) = 0$, $d_H(x,y) = 0 \Leftrightarrow \forall i \in [|1;n|]$, $x_i = y_i \Leftrightarrow x = y$
- Par définition de d_H il est claire que $d_H(x,y) = d_H(y,x)$.
- Montrons enfin que $d_H(x,y) \leq d_H(x,z) + d_H(z,y)$.
  Soient $A = \{i \in \{1,...,n\}/x_i \neq y_i\}$ et $B = \{i \in \{1,...,n\}/x_i \neq z_i\}$ et $D = \{i \in \{1,...,n\}/x_i \neq z_i\}$ On a $d_H(x,y) = card(A)$, $d_H(x,z) = card(B)$, $d_H(z,y) = card(D)$. Soit $i \in \{1,...,n\}$ tel que $i \notin B \cup D$, alors $i \notin B$, $i \notin D$. D'où $x_i = z_i$ et $z_i = y_i$ donc $x_i = y_i$ et ainsi $i \notin A$ on peut donc dire qu'on a $A \subset B \cup D$; d'où $card(A) \leq card(B \cup D) \leq card(B) + card(D)$. Ainsi $d_H(x,y) \leq d_H(x,z) + d_H(z,y)$.■

Définition 2.2. *(poids de Hamming)*
Le poids de Hamming d'un mots x de $\mathcal{C}$ est sa distance de Hamming avec le mot nul.

Théorème 2.1. *(Unicité du décodage)*
Soit $\mathcal{C}$ un code de capacité théorique de correction t ; soit $x \in A^n$ un mot quelconque, alors il existe au plus un mot c du code $\mathcal{C}$ tel que $d_H(x,c) \leq t$.

Preuve : Par absurde, s'il existe x_1, x_2 de mots distints de $\mathcal{C}$ tels que $d_H(x_1,c) \leq t$ et $d_H(x_2,c) \leq t$ alors $d_H(x_1,c) + d_H(x_2,c) \leq 2t = 2\left\lfloor \frac{d-1}{2} \right\rfloor \leq d-1$ par suite on a $d \leq d-1$ car d est la distance minimal de $\mathcal{C}$ ce qui est impossible, d'où le resultat.■

Définition 2.3. .

- *Soient x et y deux mots de $\mathcal{C}$. On dit que y est une permutation de x s'il existe une permutation σ de $\{1,...,n\}$ tel que pour tout $i \in \{1,...,n\}$, $y_i = x_{\sigma(i)}$.*
- *Deux codes $\mathcal{C}$ et $\mathcal{C}'$ sont dit équivalents par permutation s'il existe une permutation σ de $\{1,...,n\}$ tel que pour tout $x \in \mathcal{C}'$, il existe $y \in \mathcal{C}$ tel que x est la permutation de y par σ.*

Définition 2.4. *(Capacité de détection)*
La capacité de détection d'un code de distance minimal d est la quantité $d-1$.

Définition 2.5. *(Code parfait)*
Un code $\mathcal{C}$ est dit parfait si l'ensemble des boules férmées de rayon t pour la distance de hamming et centrées sur les mots du codes forment une partition de A^n.

Définition 2.6. *(Eléments conjugués)*
Deux éléments α_1 et α_2 d'un corps F de l'extension $K \subseteq F$ sont dit conjugués s'il possédent le même polynôme minimal sur K.

Définition 2.7. *(Classe de conjugaisons)*
La classe de conjugaison d'un élément α d'un corps F de l'extension $K \subseteq F$ est l'ensemble des éléments conjugués à α.

Remarque 2.1.1. .
Contrairement aux espaces vectoriels, les modules n'admettent pas en général de base. Néanmoins ils possèdent une famille génératrice ; ce qui entraine que la décomposition des éléments sur cette famille n'est plus nécessairement unique.

2.2 Code linéaire

un code linéaire dispose d'une structure algébrique plus riche que celle du cadre général des codes correcteurs.

Définition 2.8. .
Un code linéaire sur un anneau A est un sous A-module de A^n.

Définition 2.9. *(Matrice génératrice)*
On appelle matrice génératrice d'un code linéaire sur A toute matrice $M(A)$ dont les lignes forment une famille génératrice minimale du codes.

Théorème 2.2. .
La matrice génératrice d'un tel code peut se mettre sous une forme particulière lorsque A est un anneaux de Galois et si on s'autorise à modifier légérement le code. Dans ce cas on dit que le code $\mathcal{C}$ admet une matrice génératrice dite de forme normale.

$$K = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & ... & A_{0,m-1} & A_{0,m} \\ 0 & pI_{k_1} & pA_{1,2} & pA_{1,3} & ... & pA_{1,m-1} & pA_{1,m} \\ 0 & 0 & p^2I_{k_2} & p^2A_{2,3} & ... & p^2A_{2,m-1} & p^2A_{2,m} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & ... & p^{m-1}I_{k_{m-1}} & p^{m-1}A_{m-1,m} \end{pmatrix}$$

où les $A_{i,j}$ sont les matrices $k_i \times k_j$ à coeficient dans A, I_{k_i} est la matrice identité de taille k_i et K est une matrice bloc donc chaque colonne est regroupée dans un bloc carré de taille $k_0, k_1, k_2, ..., k_{m-1}$, $k_m = n - \sum_{i=0}^{m-1} k_i$ avec $k_i \geq 0$ ainsi, on dit que le code $\mathcal{C}$ sur A est de type $(1)^{k_0}(p)^{k_1}(p^2)^{k_2}...(p^{m-1})^{k_{m-1}}$, De plus il ressort que $\mathcal{C}$ est de cardinal $p^r \sum_{i=0}^{m-1}(m-i)k_i$.

Définition 2.10. *(Rang)*
Soit $\mathcal{C}$ un code linéaire sur A

- *On appelle rang libre de $\mathcal{C}$ le plus grand rang des sous module libres de $\mathcal{C}$. Dans G défini précédenment le rang libre du code $\mathcal{C}$ est k_0.*
- *On définit le rang de $\mathcal{C}$ comme le nombre minimun de générateur de $\mathcal{C}$ vue comme A-module. En d'autres termes c'est le nombre de ligne de la matrice génératrice $\mathcal{C}$ linéairement indépendant, D'aprés G défini précédenment on obtient que $rang(\mathcal{C}) = \sum_{i=0}^{m-1} k_i$.*

Remarque 2.2.1. .
Un code linéaire est dit de rang libre si son rang libre est égal a son rang. Dans ce cas le code $\mathcal{C}$ est un A-module isomorphe à A^k et à pour base k éléments.

Par conséquent, un tel code est noté $\mathcal{C}(n, k, d)$ où k est le rang du code $\mathcal{C}$ vue comme sous A-module de A^n.

2.2.1 Code dual d'un code linéaire sur un anneau

Tout d'abord, définissons le produit scalaire sur A^n par $a.b = \sum_{i=0}^{n-1} a_i.b_i$ pour $a, b \in A^n$ les opérations étant éffectuées dans A ce produit scalaire permet de définir une notation de dualité sur A.

Définition 2.11. .
Soit $\mathcal{C}$ un code linéaire sur A. On appelle code dual d'un code $\mathcal{C}$ et on note $\mathcal{C}^\perp$ le sous module de A^n définit pas :

$$\mathcal{C}^\perp = \{x \in A^n; x.y = 0 \forall y \in A^n\}.$$

Théorème 2.3. .
Lorsque la matrice génératrice du code $\mathcal{C}$ est sous la forme normale défini précédenment celle de son dual se met également sous la forme normale. Soit

$$K^\perp = \begin{pmatrix} B_{0,0} & B_{0,1} & B_{0,2} & ... & ... & B_{0,m-1} & I_{k_n} \\ pB_{1,0} & pB_{1,1} & pB_{1,2} & ... & ... & pI_{k_{n-1}} & 0 \\ \vdots & \vdots & \vdots & & & \vdots & \vdots \\ p^{m-1}B_{m-1,0} & p^{m-1}I_{k_1} & 0 & ... & ... & 0 & 0 \end{pmatrix}$$

où les B_i sont les matrices blocs à coeficients dans A

Propriété 2.2. .

Avec les mêmes notation que précédenmemt, on obtient que :

i)$\left|G^{\perp}\right| = p^r \sum_{i=0}^{m-1} m_i k_i$.

De plus $G^{\perp}$ *est de type* $(1)^{k_m}(p)^{k_{m-1}}(p^2)^{k_{m-2}}...(p^{m-1})^{k_1}$ *et on a la relation :* $|G|\left|G^{\perp}\right| = p^{mrn}$.

ii) $rang(G^{\perp}) = n - k_0(\mathcal{C})$ *et* $k_0(\mathcal{C}^{\perp}) = n - k(\mathcal{C})$.

iii)$\left|G^{\perp}\right| = \frac{|A^n|}{|\mathcal{C}|}$ *et* $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$.

Corollaire 2.1. .

Soit $\mathcal{C}$ *un code linéaire les assertions suivantes sont équivalentes,*

- *c'est un code libre.*
- *Toute matrice génératrice d'un code* $\mathcal{C}$ *sous la forme précédente ce réduit à une matrice systématique* $[I_{k(\mathcal{C})}M]$ *où* M *est une matrice.*
- $k(\mathcal{C}) = k_0(\mathcal{C})$.

Définition 2.12. .

i)Si pour un code $\mathcal{C}$ *sur* A *on a* $\mathcal{C} \subseteq \mathcal{C}^{\perp}$ *alors on dit que* $\mathcal{C}$ *est faiblement autodual.*

ii)si de plus $\mathcal{C}^{\perp} = \mathcal{C}$ *on dit que* $\mathcal{C}$ *est un code auto dual.*

2.3 Code MDR sur un anneau

Définition 2.13. *(Borne de singleton)*

Comme sur les corps finis, on a également pour tout code $\mathcal{C}$ *de longueur n sur un alpabet* A

$$d_H(\mathcal{C}) \leq n - log_{|A|}(|\mathcal{C}|) + 1$$

Dés lors la partie de l'inégalité droite est appelé Borne de singleton et losqu'il est atteinte on dit que $\mathcal{C}$ *est un code MDR de plus, si* $\mathcal{C}$ *est un code linéaire de paramétre* $[n, k, d]$, *alors on a*

$$d_H(\mathcal{C}) \leq n - k + 1$$

Si on a l'égalité dans ce qui précédent, on dit que $\mathcal{C}$ *est un code MDS.*

Remarque 2.3.1. .

Un code non libre qui est MDR n'est pas forcement MDS.

Exemple 2.3.1. .

Le code linéaire sur $\mathbb{Z}_4$ de matrice génératrice (2) est un code MDR qui n'est pas MDS.

Tout code MDR libre est un code MDS.

2.3.1 Quelques propriétés des codes MDS

Théorème 2.4. .

Soit $\mathcal{C}$ un code $[n,k,d]$ libre sur A de matrice génératrice G et de matrice de contrôle H. Les propriétés suivantes sont équivalentes

i) $\mathcal{C}$ est MDS.

ii)$n-k$ colonnes de H sont linéairement indépendantes.

iii)k colonnes distinctes de G sont linéairement indépendantes.

Preuve :[10]■

Proposition 2.1. .

Lorque H est une matrice de contrôle d'un code $\mathcal{C}$ de longueur n, nous avons ; $\mathcal{C}$ a pour distance minimale d si et seulement si tout systéme de $d-1$ colonnes de H est linéairement indépendant.

Preuve : On sait qu'un mot x est dans $\mathcal{C}$ si et seulement si $H.x^t = 0$, dés lors $\mathcal{C}$ posséde un mot de poids w si et seulement si on peut trouver w colonnes de H linéairement indépendantes. De ce fait, $\mathcal{C}$ est de distance minimale d si et seulement si tout systéme de $d-1$ colonnes de H est linéairement indépendant.■

Théorème 2.5. .

Soit $\mathcal{C}$ un code $[n,k,d]$ libre sur A, de matrice génératrice G et de matrice de contrôle H si $\mathcal{C}$ est MDS alors un code dual $\mathcal{C}^\perp$ est également un code MDS.

Preuve : H étant la matrice génératrice du code $\mathcal{C}^\perp$ d'aprés le théoréme 2.4, $n-k$ colonnnes de H sont linéairement indépendants donc seul le mot nul à 0 sur chacune de ses $n-k$ coordonnées, donc $\mathcal{C}^\perp$ à une distance minimale d' plus grand que $k+1$ et d'aprés la borne singleton d'un code on obtient que $d' = k+1$ donc $\mathcal{C}^\perp$ est de paramétres $[n, n-k, k+1]$, il s'ensuit que $\mathcal{C}^\perp$ est également un code MDS.■

2.4 Détection et Correction d'erreurs

Aprés la borne singleton d'un codes linéaires obtenu par majoration de la distance minimal d'un tel code nous remarquons que la minoration de cette distance minimal posséde des propriétés suplémentaire. En effet supposons que l'anneau $A = \mathbb{F}_2$. Considérons le schema suivant qui présente la transformation d'un mots transmis dans l'espace en un moment donné

ici la reception de l'information est obtenu de manière optimisé dans la mesure où la fonction de décodage est d'une complexité abordable. D'autre part la notion d'entropie d'une source nous permet de mesurer la quantité d'information transmit conduisant à l'évaluation de sa sécurité.

Théorème 2.6. .

Soit $\mathcal{C}$ un code

- *Si $d \geq s+1$ alors $\mathcal{C}$ peut détecter au plus s erreurs.*
- *Lorsque $s = 2t$ on déduit que $\mathcal{C}$ peut corriger au plus t erreurs.*

Preuve : Supposons que m' est un mot reçu et que $m' \in \mathcal{C}$ s'il existe x tel que $d(m', x) < d$ alors l'erreur est detecté, dés lors $d(m', x) \leq d-1$ en posant $s = d(m', x)$ il suit que $d \geq s+1$ par conséquent $\mathcal{C}$ peut détecter au plus s erreurs. Par ailleurs sopposons que $s = 2t$ on déduit qu'il existe au plus un mot x de $\mathcal{C}$ tel que $d(m', x) \leq t$ et il suit que $\mathcal{C}$ peut corriger au plus t erreurs.■

Tout d'abord désignons par 'A' l'aphabet du message source. A chaque message sur A on peut calculer les fréquences d'apparition de chaque élément de l'aphabet et construire ainsi une distribution de probabilités sur A. Dés lors une source d'information est constitué du couple $S = (A, P)$ où A est l'aphabet source et $P = (p_1, ..., p_{|A|})$ est une distribution de probabilités sur S, c'est-à-dire que p_i est la probabilité d'occurence de a_i dans une emission ; par conséquent on peut construire une source d'information à partir de n'importe quel message en construisant la distribution de probabilité à partir de la fréquence des caractéres dans le méssage, une telle source d'information $S = (A, P)$ est dite sans mémoire lorsque les evenements c'est-à-dire occurences d'un symbole dans une émission sont indépendants et que leur probabilité reste stable au cours de l'émission elle est dite stationnaire. Entre autre la source est markovienne si les prababilités d'occurence des caractéres dépendent des caractéres émis précédenment de maniére simple dans le cas d'un seul prédécesseur, $P = \{p_{ij}\}$ où p_{ij} est la probabilité d'occurence de a_i sachant que a_j vient d'être émis, on a alors $p_i = \sum_j P_{ij}$ pas exemple, un texte en français est une source dont l'alpabet est l'ensemble des lettres latines et les probabilités d'occurence sont les frequences d'apparition de chaque caractére.

Définition 2.14. .

L'entropie est une notion qui permet de mesurer à la fois la quantité d'information qu'on

peut attribuer à une source et du dégrés d'ordre et de redondance d'un message qui sont utile pour la compression des messages et constituant aussi une information cruciale pour la cryptograhie.

Proposition 2.2. *l'entropie d'une source* $S = (A, P)$ *où* $A = (a_1, ..., a_{|A|})$ *et* $P = (p_1, ..., p_{|A|})$ *est* $H(S) = H(p_1, ..., p_{|A|}) = \sum_{i=1}^{|A|} p_i log_2(\frac{1}{p_i})$ *et on désigne par extension l'entropie d'un message comme l'entropie de la source induite par ce message avec la distribution de probabilités étant calculée à partir des fréquences d'apparition des caractéres dans le massage.*

Propriété 2.3. .

Pour une source $S = (A, P)$ *on a* $0 \leq H(S) \leq log_2 n$.

Preuve : théorie des codes.■

2.4.1 Entropie conjointe et conditionnelle

Nous voulons etendre la définition de l'entropie à plusieurs sources facilitant ainsi la gestion d'énorme message. Soient $S_1 = (A_1, P_1)$, $S_2 = (A_2, P_2)$ deux sources sans mémoire, dont les événements ne sont pas forcément indépendants et notons que $A_1 = (a_{11}, ..., a_{1|A_1|})$ et $P_1 = (p_1, ..., p_{|A_1|})$, $A_2 = (a_{21}, ..., a_{2|A|})$ et $P_2 = (p_1, ..., p_{2|A_2|})$ puis $P_{ij} = P(S_1 = a_{1i} \cap S_2 = a_{2j})$ est la probabilité d'occurrence conditionnelle de S_{1i} et S_{2j}.

Définition 2.15. .

L'entropie Conjointe de S_1 *et* S_2 *est la quantité* $H(S_1, S_2) = -\sum_{i=1}^{|A_1|} \sum_{j=1}^{|A_2|} p_{ij} log_2(p_{ij})$.

Par ailleurs, si les sources S_1 et S_2 sont indépendantes alors $p_{ij} = p_i p_j$ pour tout i,j et donc dans ce cas nous montrons que $H(S_1, S_2) = H(S_1) + H(S_2)$ et si les évenements de S_1 et S_2 ne sont pas indépendants et qu'on veuille connaître la quantité d'information contenue dans une source connaissant un événement de l'autre. On calcule alors l'entropie conditionnelle de S_1 relativement à la valeurs de S_2 donnée par $H(S_1|S_2 = s_{2j}) = -\sum_{i=1}^{|A_1|} p_{ij} log_2(p_{ij})$. Ensuite nous étendons cette notion à une entropie conditionnelle de S_1 connaissant S_2 qui est la quantité d'information restant dans S_1 si la loi de S_2 est connue ; on a $H(S_1|S_2) = \sum_{j=1}^{|A_2|} p_i H(S_1|S_2 = s_{2j}) = \sum_{i,j} p_{ij} log_2(\frac{p_i}{p_{ij}})$.

Remarque 2.4.1. .

Les relations suivantes sont importantes $H(S_1) \geq H(S_1|S_2)$ et l'égalité a lieu si et seulement si S_1 et S_2 sont indépendantes et encore $H(S_1|S_2) = H(S_2) + H(S_1|S_2)$ mais l'entropie d'une source sans mémoire à elle seule ne capture pourtant pas tout l'ordre ou le désordre contenu dans un message.

2.4.2 Extension d'une source

Soit S une source sans mémoire la k^{ime} extension S^k de S est le double (S^k, p^k) où S^k est l'ensemble des mots de longueur k sur S et p^k est la distribution de probabilité ainsi définie pour un mot $a = a_{i_1}...a_{i_k} \in S^k$ alors $p^k(a) = p(a_{i_1}...a_{i_k}) = a_{i_1}...a_{i_k}$.

Exemple 2.4.1. .
Pour $S = (a_1, a_2)$, $P = (\frac{1}{4}, \frac{3}{4})$ on a $S^2 = (a_1a_1, a_1a_2, a_2a_1, a_2a_2)$ et $P^2 = (\frac{1}{16}, \frac{3}{16}, \frac{3}{16}, \frac{9}{16})$ si S est une source makovienne, on définit de la même façon S^k et pour un mot $a = a_{i_1}...a_{i_k} \in S^k$ alors $p^k(a) = p_{i_1}...p_{i_k}$.

Propriété 2.4. .
Soient S une source et S^k sa k^{ime} extension $H(S^k) = kH(S)$ autrement dit, la quatité d'information d'une source étendue à k caractéres est exactement k fois celle de la source originelle.

Propriété 2.5. .
Soient M un message de taille n et S_{M^k} la source dont les probablités correspondent aux occurences des k-uplets consécutifs de M alors $H(S_{M^k}) \leq log_2(\lceil \frac{n}{k} \rceil)$.

2.4.3 Quelques protocoles de décodage d'informations

Aprés l'émission d'une information une transformation a lieu au niveau de la fonction d'encodage, la reception de cette information n'est possible qu'aprés décodage qui reduit le nombre d'erreurs possible rencontré au niveau du canal. Parmis lesquelle nous distingons le décodage au maximun de vraisemblance, décodage borné, décodage pas tableau standard, décodage par ensemble d'information.

2.4.4 Formalisme

Tout d'abord, considérons un élément $y \in A^n$ et $\mathcal{C}$ un code de capacité théorique t.
..**Décodage au maximun de vraisemblance** $(\mathcal{C}, y)$
ici il s'agit de trouver un mot $m \in \mathcal{C}$ vérifiant $d(m, y) = d(\mathcal{C}, y)$ c'est-à-dire le mot le plus proche au sens de Hamming de y. En fait, le mots qui est probablement envoyer pas l'expéditeur.
..**Décodage borné** $(\mathcal{C}, y, t)$
Il s'agit de trouver un mot $m \in \mathcal{C}$ tel que $d(m, y) \leq t$.
..**Décodage par tableau standard**

On se donne H une matrice de parité du code $\mathcal{C}$, supposons que $y = m + e$ où $m \in \mathcal{C}$, le syndrome de y est donné pas $S = Hy^T = Hm^T + He^T = He^T$. Par suite, si m est une solution du probléme de décodage borné, nous pouvons calculer m à l'aide d'un mot de poids faible de même syndrôme que y. Algorithquement on a :

-Entré G, $y = (y_1, ..., y_n)$

-Sortie $x \in \mathcal{C}$ $x \in \mathcal{C}$ tel que $d(x, y) \leq t$.

-Précalcule

calculer une matrice de parité de H associée à la matrice génératrice G. Pour un mot $e \in A^n$ de poids inférieur ou égale t calculer He^T et l'ajouter à la liste des syndrômes S.

-Décodage

calculer Hy^T et rechecher dans la liste S un mot e admettant le même syndrôme, si e existe renvoyer $c = y - e$ sinon renvoyer 'pas de solution'.

Application.

Soit $\mathcal{C}$ le code $[7, 4, 3]$ de Hamming binaire de matrice génératrice

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

$y = (11111011)$ le mot à décoder, $t = 1$.

-précalculs

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

est une matrice de contrôle de $\mathcal{C}$.

-Liste des syndrômes

Mots de poids≤ 1	syndrôme
(0 0 0 0 0 0 0 0)	$\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$
(1 0 0 0 0 0 0 0)	$\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$
(0 1 0 0 0 0 0 0)	$\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$
(0 0 1 0 0 0 0 0)	$\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$
(0 0 0 1 0 0 0 0)	$\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$
(0 0 0 0 1 0 0 0)	$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$
(0 0 0 0 0 1 0 0)	$\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$
(0 0 0 0 0 0 1 0)	$\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$

Décodage

$$Hy^T = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

le mot de poid faible de même syndrome que y est $c = (00000010)$ et le mot code cherché est alors $c = y - e = (11111111)$. L'algorithme précédent manipule une liste S contenant les syndrôme de tous les mots de poids de Hamming inférieur à t. Pour une valeur w fixée, $w \leq t$. il existe $C_t^w(q-1)^w$ mot d'un tel poids lorque $A = F_q$. Soit en tout $\sum_{w=1}^{t} C_t^w(q-1)^w$ mots de poids inférieur ou égal à t. La complexité de l'algorithme est donc exponentielle en t. regardons maintenant l'algorithme de décodage par ensemble d'information.

..**Décodage par ensemble d'information**

L'importance dévoué à un ensemble d'information est un paramétre necessaire, pour cela il oriente que les positions des mots d'un code prises pas paquet de k n'ont pas toutes la même importance. En effet k positions tirées aléatoirement ne forment pas toujours un ensemble d'information, dans les lignes qui suivent I désigne un ensemble d'information d'un code $\mathcal{C}$ de paramétre $[n, k]$, $L = \{1, 2, ..., n\}$ et J le complémentaire de I dans L.

Pour toute matrice G et tout sous ensemble d'information I de L, on note $G = (G_I|G_J)$ où G_I est la sous matrice de G constituée des colonnes étiquetées pas les éléments de I. Pour tout vecteur $x \in A^n$ on notera $x = (x_I|x_J)$ où x_I (respectivement x_J) désigne les positions du mot x étiqueté par les éléments de I(respectivement de J). Soit $\mathcal{C}$ un code $[n, k]$ de matrice génératrice G et de capacité de correction théorique t. On se donne $y = xG + e$ avec $x \in A$ on a $y = (y_I|y_J) = x(G_I|G_J) + (e_I|e_J)$ d'où $e_I = y_I - xG_I$ et $e_J = y_J - xG_J$ par conséquent si l'ensemble d'information ne contient pas de d'erreur(c'est-à-dire $e_I = 0$) on obtient $y_I = xG_I$ et $e_J = y_J - xG_J$. comme G_I est inversible par définition, le systéme s'écrit : $x = y_I G_I^{-1}$ et $e_J = y_J - xG_J$ ainsi, le vecteur $e = (e_I|e_J) = (0|y_J - y_I G^{-1})$ est la solution du probléme de décodage borné par t du code $\mathcal{C}$. Dés lors la procédure algorithmique se présente comme suit :

Algorithme : Décodage par ensemble d'information

-Input : G, $y = (y_1, ..., y_n)$ àdistance au plus t du code $\mathcal{C}$.

-Ouput : $x \in \mathcal{C}$ et e tel que $y = mG + e$

-Décodage : 1.Tirer aléatoirement un ensemble d'information I du code de matrice génératrice G.

2.Calculer $e_J = y_J - y_I R$.

Si $w(e_J) \leq t$, retourner $e = (0|e_J)$ et $x = y - e$

Si non, recommencer la procédure avec un nouveau I.

Application

Considérons le code $\mathcal{C}$ de l'application précédente et $y = (1100010)$ le mot à décoder, et que $t = 1$.

-Pour $I = \{1, 2, 3, 4\}$, on a $G_I = I_4$ et

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

$G_I^{-1} = I_4$, $R = G_I^{-1} G_J = I_4 G_J = G_J$;

$$y_I R = (1100) \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} = (100) ;$$

$e_J = y_J - y_J R = (010) - (100) = (110)$ et on a $w(e_J) = 2 > t$.

-Pour $I = \{1, 2, 3, 5\}$, on a

$$G_I = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} et G_J = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

$$G_I^{-1} = G_I,\ R = G_I^{-1} G_J = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

$$y_I R = (1100) \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} = (110)$$

$e_J = y_J - y_J R = (010) - (110) = (100)$ on a $w(e_J) = 1 \leq t$; donc $e = (0001000)$ d'où $x = y - e = (1101010)$. Nous remarquons que la probabilité pour que k éléments de L tirés aléatoirement n'étiquettent pas les t positions du vecteur d'erreur est égale à : $P = \frac{C_{n-t}^k}{C_n^k} = \frac{(n-k)!}{(n-t-k)!}$; la complexité moyenne de cette algorithme vaut $O(\frac{k^3}{P})$ multiplication dans F_q.

Chapitre Trois

Construction des codes linéaires sur un anneau fini

Dans cette section nous présentons la méthode de construction des codes BCH et alternant sur les anneaux locaux finis, premièrement nous rappelerons certains propriété necessaire des extensions de Galois sur des anneaux finis qui nous permettrons de caractériser de tel codes.

3.1 Propriétés de Galois sur les extensions de corps

Dans cette partie tout les corps considérés sont commutatifs. Soient K, F deux corps tel que $K \subseteq F$, on dit que F est une extension de K. Soit $K \subseteq F$ une extension de corps dans F. il est clair que F est un K-module (en particulier un K-espace vectoriel) donc une algébre sur K. On note $[F : K] = dim_{\mathbb{K}}F$ appélée aussi le degré de F sur K.

Définition 3.1. .
Soient K,L,F des corps tels que $K \subseteq L \subseteq F$, on dit que L est un corps intermédiaire de l'extension $K \subseteq F$.

Proposition 3.1. .
Soit L un corps intermédiaire de l'extension $K \subseteq F$, alors $[F : K] = [F : L][L : K]$ par conséquent $[F : K]$ est finie si et seulement si $[F : L]$ et $[L : K]$ sont finies.

Preuve : Trivialement si $[F : K]$ est finie alors $[F : L]$ et $[L : K]$ sont finies car $[F : K] = [F : L][L : K]$. Reciproquement, supposons que $[F : L]$ et $[L : K]$ sont finies montrons que $[F : K]$ est finie, soient $\{u_i, i \in \{1, ..., [F : L]\}\}$ une L-base de F et $\{v_i, i \in \{1, ..., [L : K]\}\}$ une K-base de L il vient que l'ensemble $\{u_i v_j, i \in \{1, ..., [F : L]\}, j \in \{1, ..., [L : K]\}\}$ est une K-base de F ; en effet soit $a_{i,j} \in K$, $(i, j) \in \{1, ..., [F : L]\} \times \{1, ..., [L : K]\}$ tel que

$\sum_{i,j} a_{i,j}u_iv_j = 0$ alors $\sum_{i,j}(a_{i,j}u_i)v_j = 0$ par conséquent pour tout $i \in \{1, ..., [F : L]\}$ $\sum_j a_{i,j}v_i = 0$ (car $a_{i,j}v_i \in L$ et $\{u_i, i \in \{1, ..., [F : L]\}\}$ est une L-base de F) et comme $\{v_i, i \in \{1, ..., [L : K]\}\}$ est une K-base de L il suit que pour tout $i \in \{1, ..., [F : L]\}$, $a_{i,j} = 0$ pour tout $j \in \{1, ..., [L : K]\}\}$ et par suite $\{u_iv_j, i \in \{1, ..., [F : L]\}, j \in \{1, ..., [L : K]\}\}$ est une K-base de F. En outre, si $x \in F$ alors $x = \sum_i a_iu_i$, $a_i \in L$ dans l'extension $L \subseteq F$; et pour tout $i \in \{1, ..., [F : L]\}$, $u_i = \sum_{i,j} b^i_j v_j$, $b_j \in K$ pour tout j, donc $x = \sum_{i,j} b^i_j u_i v_j$, $b^i_j \in K$ pour tout i,j. Ansi $\{u_iv_j, i \in \{1, ..., [F : L]\}, j \in \{1, ..., [L : K]\}\}$ est une famille génératrice de F sur K et de ce fait, on déduit que $[F : K] = [F : L][L : K]$ donc $[F : K]$ est finie d'où le resultat.■

Soit B un anneau intègre, K un corps contenu dans B et $u \in B$; $K[u]$ est le plus petit sous anneau de B contenant K et u ou encore le sous anneau de B engrendré par u sur K. Si u est inversible dans B, on a $K(u)$ est le plus petit corps contenu dans B et contenant K et u appelé corps des fractions de $K[u]$.

Définition 3.2. .

Soit $\mathbb{K} \subseteq F$ une extension.

(i) Un élément $u \in F$ est dit algébrique sur $\mathbb{K}$ lorsqu'il existe $f \in \mathbb{K}[X]$, $degr(f) \geq 1$, tel que $\hat{f}(u) = 0$, si un tel polynôme n'existe pas on dit que : u est transcendent sur $\mathbb{K}$.

(ii) F est dit algébrique sur K lorsque tout élément de F est algébrique sur $\mathbb{K}$ sinon F est transcendent sur K.

Exemple 3.1.1. .

Dans l'extension $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, $\mathbb{R}$ est transcendent sur $\mathbb{Q}$ mais $\mathbb{C}$ est algébrique sur $\mathbb{R}$.

Preuve : $\mathbb{R}$ est transcendent sur $\mathbb{Q}$ car $\pi \in \mathbb{R}$ et π n'est pas algébrique sur $\mathbb{Q}$. Pour tout $u = a + ib$ élément de $\mathbb{C}$, u est une racine du polynôme $h = X^2 - 2aX + a^2 + b^2 \in \mathbb{R}[X]$.■

Théorème 3.1. .

Soit $\mathbb{K} \subseteq F$ une extension, et $u \in F$ un élément algébrique sur K, alors il existe un polynôme unitaire f de degré minimun supérieur à 1, tel que $\hat{f}(u) = 0$ de plus ;

(i) f est irréductible et $K[u] = K(u) \cong \frac{K[X]}{(f)}$.

(ii) pour tout $g \in K[X]$, $\hat{g}(u) = 0$ alors f divise g.

(iii) Si $n = deg(f)$ alors $\{1, u..., u^{n-1}\}$ est une K-base du corps $K(u)$.

Le polynôme irréductible f est appelé le polynôme minimal de u sur K et si $deg(f) = n$ on dit aussi que u est de degré n sur K.

Preuve : (*i*) Par définition f est irréductible sinon f peut s'écrire comme produit de facteur non inversible par suite sa minimalité est contredit. En considérant l'epimorphisme

d'anneau unitaire $K[X] \xrightarrow{\alpha} K[u]$ tel que pour tout polynôme h on a $\alpha(h) = h(u)$ il vient que le noyau de α est l'idéal engendré par f et d'aprés le deuxiéme théoréme d'isomorphisme il s'ensuit que $K[u] \cong \frac{K[X]}{(f)}$ et comme $\frac{K[X]}{(f)}$ est un corps on obtient que $K[u] = K(u)$.

(ii) Soit g un polynôme de $K[X]$ tel que $g(u) = 0$ alors g est dans le noyau (f) de α donc $g = \lambda f$ par conséquent f divise g.

(iii) Supposons que $n = deg(f)$, si h est un élément de $K(u)$; on sait dans $K[X]$ $h = fq+r$ où r est un polynôme de degré strictement inférieur à n. Dés lors $h(u) = r(u)$ car $f(u) = 0$ donc $\{1, u..., u^{n-1}\}$ est une famille génératrice de $K(u)$ sur K. Par ailleur si on a λ_i $i \in \{1...n\}$ tel que $\sum_{i=0}^{n-1} \lambda_i u^i = 0$ alors le polynôme associé $p(X) = \sum_{i=0}^{n-1} \lambda_i X^i$ est nul en u sur K d'aprés (ii) on déduit f divise p donc p est nul il s'ensuit que $\lambda_i = 0$ pour tout $i \in \{1...n\}$, par conséquent $\{1, u..., u^{n-1}\}$ est une K-base du corps $K(u)$.■

Théorème 3.2. .

Soient L, M deux corps intermédiaires de l'extension $\mathbb{K} \subseteq F$.

(i) $L \vee M$ est un corps intermédiaire de l'extension $\mathbb{K} \subseteq F$.

(ii) $[L \vee M : K]$ est fini si et seulement si $[L : K]$ et $[M : K]$ sont finies.

Preuve : (i) Par définition $L \vee M$ est le plus petit corps contenant L et M, L et M sont des corps intermédiaire il s'ensuit que $L \vee M$ est un corps intermédiaire.

(ii) Si $[L \vee M : K]$ est fini comme $[L : K] \leq [L \vee M : K]$ et $[M : K] \leq [L \vee M : K]$ il s'ensuit que $[L : K]$ et $[M : K]$ sont finies. Reciproquement on a $[L \vee M : K] \leq [L : K][M : K]$ donc la quantité $[L \vee M : K]$ est fini.■

Corollaire 3.1. .

Soit $\mathbb{K} \subseteq F$ une extension et L l'ensemble des éléments de F qui sont algébrique sur K, alors L est un corps intermédiaire de l'extension $\mathbb{K} \subseteq F$.

Preuve : L est non vide car contient le 0 de K de plus les quantité $[K(u + v) : K]$, $[K(uv) : K]$, $[K(u^{-1}) : K]$, $[K(-u) : K]$ sont finis pour tout élément algébrique u, v donc $u + v$, uv, u^{-1}, $-u$ sont algébrique il s'ensuit que L est un corps intermédiaire de l'extension $\mathbb{K} \subseteq F$.■

Définition 3.3. .

Soient E, F deux corps finis contenant chacun le corps K. Soit $\alpha : F \longrightarrow E$ un morphisme de corps.

(i) Si α est un morphisme de K-espace vectoriels on dit que α est un K-morphisme.

(ii) Lorsque $F = E$ et $\alpha \in Aut(F)$ est un K-morphisme, on dit que α est un K-automorphisme de F notée $Aut_K F$ est aussi appelé le groupe de Galois de F sur K.

3.1.1 Théorème fondamental de la théorie de Galois

Soit $\mathbb{K} \subseteq F$ une extension, L un corps intermédiaire. $L' = \{\alpha \in Aut_K F, \alpha(u) = u, \forall u \in L\}$ est un sous groupe de $Aut_K F$. De même, si $H \subseteq Aut_K F$, alors $H' = \{u \in F, \alpha(u) = u, \forall \alpha \in H\}$ est un corps intermédiaire.

Lemme 3.1. .

Soit $\mathbb{K} \subseteq F$ une extension, L et M deux corps intermédiaire, H et J deux sous groupes de $Aut_K F$. alors

(i) si $L \subseteq M$ alors $M' \subseteq L'$

(ii) si $H \subseteq J$ alors $J' \subseteq H'$

(iii) si $L \subseteq L''$ alors $H \subseteq H''$

(iv) si $L''' = L'$ alors $H' = H'''$

Preuve : On se donne une extension $\mathbb{K} \subseteq F$ L et M deux corps intermédiaire, H et J deux sous groupes de $Aut_K F$,

(i) Supposons que $L \subseteq M$ et que σ est dans M', soit $u \in L$, comme $L \subseteq M$ il vient que $u \in M$ donc $\sigma(u) = u$ d'où σ est dans L' ainsi $M' \subseteq L'$.

(ii) En utilisant le même procédure on obtient que $J' \subseteq H'$ quand $H \subseteq J$.

De la même façon (iii) et (iv) sont démontrés.■

Définition 3.4. .

Soit $\mathbb{K} \subseteq F$ une extension.

(i) un corps intermédiaire L est clos losque $L'' = L$.

(ii) un sous groupe H de $Aut_K F$ est dit clos losque $H'' = H$.

(iii) l'extension $\mathbb{K} \subseteq F$ est dite galoisiènne lorsque K est clos.

Exemple 3.1.2. .

(i) Dans l'extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$; $Aut_K F = \{id, \gamma\}$ où γ est la conjugaison qui à $a+b\sqrt{2} \mapsto a - b\sqrt{2}$. Par ailleurs $u = a + b\sqrt{2} \notin \mathbb{Q}$ alors $b \neq 0$ par suite $\gamma(u) = a - b\sqrt{2} \neq u$ donc $\mathbb{Q}'' = \mathbb{Q}$ qui fait que l'extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ est galoisiènne.

(ii) Soit l'extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) = F$, on a $f = X^3 - 2$, $u = \sqrt[3]{2}(-\frac{1}{2} + i\frac{\sqrt{3}}{2})$, $n \in \{0, 1, 2\}$ on sait que $\{1, \sqrt[3]{2}, \sqrt[3]{2}\}$ est une $\mathbb{Q}$-base de F de ce fait, si $\alpha \in Aut_K F$; alors $\alpha(\sqrt[3]{2})$ est une racine de f et $\alpha(\sqrt[3]{2})$ est un élément de F il suit que $\alpha(\sqrt[3]{2}) = \sqrt[3]{2}$ par conséquent $\alpha = id_F$ donc $Aut_K F = \{id_F\}$ d'où l'extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) = F$ n'est pas Galoisienne.

Remarque 3.1.1. .

Soit $\mathbb{K} \subseteq F$ une extension et $u \in F$ un élément algébrique sur K. Si $n = deg(f_u)$, alors $\{1, u, ..., u^{n-1}\}$ est une K-base de $K[u] = K(u)$. Posons $F_0 = K[u] = K(u)$ quand $\alpha \in Aut_K F_0$, α dépend entièrement de l'expression de $\alpha(u)$ mais $\alpha(u)$ est aussi une racine de f_u, donc il y'a au plus n possibilités pour $\alpha(u)$, c'est-à-dire que $Card(Aut_K F_0) \leq n$. D'autre part, si une extension $\mathbb{K} \subseteq F$ est non galoisienne, alors $\mathbb{K}$ est strictement contenu dans $\mathbb{K}''$ en posant $\mathbb{K}_0 = \mathbb{K}''$ on obtient que $Aut_{K_0} F = Aut_K F$.

Proposition 3.2. .

Soit $\mathbb{K} \subseteq F$ une extension et $L \subseteq M$ 2 corps intermédiaires. Si $[M : L]$ est fini alors $[L' : M']$ est fini et $[L' : M'] \leq [M : L]$.

Preuve : Par la méthode de recurrence sur $n = [M : L]$

si $n = 1$, alors $M = L$ et $L' = M'$ par suite $[L' : M'] = 1$.

Soppossons que $n \geq 2$ et le resultat vrai pour tout $k < n$; soit $u \in M \backslash L$, $[M : L] = n$ impose que M est algébrique sur L, soit f_u le polynôme minimal de u sur L et $k = degr(f_u)$, $k = [L(u) : L]$, $1 < k \leq n$, $[M : L(u)] = \frac{n}{k} < n$.

$(*)$ Si $1 < k < n$, on applique l'hypothése de récurrence sur ces deux extensions pour avoir $[L' : L(u)'] \leq [L(u) : L] = k$ et $[L(u)' : M'] \leq [M : L(u)] = \frac{n}{k}$ alors $[L' : M'] = [L' : L(u)'][L(u)' : M'] \leq k\frac{n}{k} = n$.

$(**)$ Si $k = n$ alors $M = L(u)$ posons E :=ensemble des racines de f. $|E| \leq k = n = degr(f)$ il suffit de montrer que $[L' : M'] \leq |E|$ pour tout $\beta \in L'$, notons $\beta M'$ la classe de β selon M', pour tout $\sigma \in M'$, $\sigma(u) = u$ par conséquent $\beta(\sigma(u)) = \beta(u)$ notons que pour tout $\beta \in M'$ $\beta(u)$ est un élément de E car racine du polynôme minimal.

Soit $R_{M'}$ la relation d'équivalence dans L' associé à M' c'est-à-dire pour tout α, β dans L', $\alpha R_{M'} \beta$ si et seulement si $\beta^{-1}\alpha \in M'$; on a pour tout α dans L', $(\alpha M')(u) = \alpha(u)$ considérons ϕ définit de $\frac{L'}{R_{M'}}$ vers E= racine de f_u qui à $\alpha M'$ associe $\alpha(u)$ ϕ est une application injective donc $\left|\frac{L'}{R_{M'}}\right| \leq |E|$ donc $[L' : M'] \leq |E|$ par conséquent on a $[L' : M'] \leq [M : L]$ et $[L' : M']$ est fini. ■

Corollaire 3.2. .

Si $\mathbb{K} \subseteq F$ est une extension finie, alors $|Aut_K F| \leq [F : K]$.

Preuve : On a $[K' : F'] \leq [F : K]$ c'est-à-dire $[Aut_K F : id_F] \leq [F : K]$ donc on a $|Aut_K F| \leq [F : K]$.■

Proposition 3.3. .

Soit $\mathbb{K} \subseteq F$ est une extension et $H \subseteq J$ deux sous groupe de $Aut_K F$. Si $[J : H]$ est fini, alors $[H' : J'] \leq [J : H]$.

Théorème 3.3. .

Soit $\mathbb{K} \subseteq F$ une extension, et $L \subseteq M$ deux corps intermédiaires, $H \subseteq J$ deux sous groupes de $Aut_K F$.

(i) Si L est clos et $[M : L]$ est finie, alors M est clos et $[L' : M'] = [M : L]$.

(ii) Si H est clos et $[J : H]$ est fini, alors J est clos et $[H' : J'] = [J : H]$.

Corollaire 3.3. .

Soit $\mathbb{K} \subseteq F$ est une extension.

(i) Tout sous groupe fini de $Aut_K F$ est clos.

(ii) Si $\mathbb{K} \subseteq F$ est galoisinne et L un corps intermédiaire de dimension fini sur K, alors l'extension $L \subseteq F$ est galoisienne. En particulier, si $\mathbb{K} \subseteq F$ est une extension galoisienne de dimension finie, alors $[F : K] = |Aut_K F|$.

Preuve : (i) On a $\{id_F\}' = F$ donc $\{id_F\}'' = F' = F$ par suite $\{id_F\}$ est un sous groupe clos de $Aut_K F$ par ailleur si H est un sous groupe fini de $Aut_K F$ alors $[H : \{id_F\}] \leq |H|$ est fini donc H est clos.

(ii) $\mathbb{K} \subseteq F$ est galoisienne si et seulement si K est clos donc comme L un corps intermédiaire de dimension fini sur K il s'ensuit que L est clos. En particulier l'extension $\mathbb{K} \subseteq F$ est galoisienne finie implique $[F : K] = [K' : F'] = [Aut_K F : \{id_F\}] = |Aut_K F|$.■

Théorème 3.4. *(fondamental).*

Soit $\mathbb{K} \subseteq F$ une extension galoisienne finie, désignons par $Sub_K(F)$ l'ensemble des corps intermediaires et par $Sub(Aut_K F)$ l'ensemble des sous groupes de $Aut_K F$, alors l'application $\phi : Sub(Aut_K F) \longrightarrow Sub_K(F)$ tel que pour tout sous groupes H on associe $\phi(H) = H'$ est une bijection. De plus, si $H \subseteq J$ sont deux sous groupes de $Aut_K F$ alors $[H' : J'] = [J : H]$. Si $L \subseteq M$ sont deux corps intermédiaires alors $[L' : M'] = [M : L]$. En particulier, $[F : K] = |Aut_K F|$.

Corollaire 3.4. .

Soit F un corps et G un sous groupe de $Aut(F)$.

Soit $L = \{u \in F, \sigma(u) = u, \forall \sigma \in H\} = Fix(G)$ alors L est un sous corps de F, $L \subseteq F$ est une extension galoisienne et $G = Aut_L F$.

3.1.2 Normalité et stabilité

L'application $\phi : Sub(Aut_K F) \longrightarrow \mathrm{Sub}_K(F)$ induit une bijection entre les corps intermédiaires clos et les sous groupes clos, entre autre l'extension $\mathbb{K} \subseteq F$ est galoisienne si et seulement si pour tout $u \in F \backslash K$, $\exists \sigma \in Aut_K F$ tel que $\sigma(u) \neq u$.

Définition 3.5. .

Soit L un corps intermédiaire de l'extension $K \subseteq F$, on dit que L est stable dans $K \subseteq F$, lorsque pour tout $\sigma \in Aut_K F$ $\sigma(L) \subseteq L$.

Proposition 3.4. .

Soit $K \subseteq F$ une extension.

(i) Si L est un corps intermédiaire stable alors $L' = \{\alpha \in Aut_K F, \alpha(u) = u, \forall u \in L\}$ est un sous groupe normal de $Aut_K F$.

(ii) Si H est un sous groupe normal de $Aut_K F$, alors $H' = \{u \in F, \alpha(u) = u, \forall \alpha \in H\}$ est un corps intermédiaire stable.

Corollaire 3.5. .

Soit L un corps intermédiaire de l'extension $K \subseteq F$ et H un sous groupe de $Aut_K F$.

(i) Si L est stable alors L" est stable.

(ii) Si H est normal alors H" est normal.

Définition 3.6. .

Une extension $K \subseteq F$ est dite normale lorsque tout polynôme irréductible $f \in K[X]$ qui admet une racine dans F se décompose en facteurs linéaires dans $F[X]$.

Lemme 3.2. .

Tout extension galoisienne est normale.

Preuve : Soit $K \subseteq F$ une extension galoisienne, $f \in K[X]$ monique et irréductible, $u \in F$ une racine de f. Soit $\{u_1, ..., u_r\}$ les images de u par les éléments de $Aut_K F$, alors $r \leq n = degr(f)$. Considérons $g = (X - u_1)(X - u_2)...(X - u_r)$, g est un polynôme de $F(X)$ par ailleur, si $\sigma \in Aut_K F$, $\sigma_{\lceil_{\{u_1,...,u_r\}}}$ est une bijection sur $\{u_1, ..., u_r\}$ par définition de ces éléments or g s'écrit $X^r - (u_1 + u_2 + ... + u_r)X^{r-1} + (\sum_{i \neq j} u_i u_j)X^{r-2} - (\sum_{|\{i,j,k\}|=3} u_i u_j u_k)X^{r-3} + ... + (-1)^r \prod_{1 \leq i \leq r} u_i$, on remarque que les coeficients de g sont invariants par σ pour tout $\sigma \in Aut_K F$ donc les coeficients de g sont les éléments de K car l'extension $K \subseteq F$ est galoisienne d'où $g \in K[X]$; comme $u \in \{u_1, ..., u_r\}$ on a $g(u) = 0$ mais f est le polynôme minimal de u sur K, on doit avoir $f \,|g$ puisque f et g sont monique et degré(g)≤degré(f) on déduit que $f = g$ par suite l'extension $K \subseteq F$ est normale.■

Théorème 3.5. .

Soit L un corps intermédiaire de l'extension $K \subseteq F$.

(i) Si $K \subseteq F$ est galoisienne et L est stable, alors $K \subseteq L$ est galoisienne.

(ii) Si $K \subseteq L$ est algébrique et galoisienne, alors L est stable.

Définition 3.7. .

Un élément $\alpha \in Aut_K L$ est dit extensible à F lorsqu'il existe $\sigma \in Aut_K F$ tel que $\alpha = \sigma_{\restriction_L}$ de plus, si L est stable dans $K \subseteq F$, alors $Aut_L F$ est un sous groupe normal de $Aut_K F$ par conséquent l'étude de $\frac{Aut_K F}{Aut_L F}$ est nécessaire.

Proposition 3.5. .

Si le corps intermédiaire L est stable dans $K \subseteq F$, le groupe qoutient $\frac{Aut_K F}{Aut_L F}$ est isomorphe au groupe des éléments extensibles de $Aut_K L$.

Preuve : En considérant ϕ de $Aut_K F$ de vers $Aut_K L$ tel que pour tout $\sigma \in Aut_K F$ on associe $\sigma_{\restriction_L}$, ϕ est un morphisme de groupe de plus $\phi(\sigma) = id_L$ si et seulement si $\sigma(u) = u$ pour tout $u \in L$ si et seulement si $\sigma \in Aut_L F$ donc $Ker(\phi) = Aut_L F$ et $\frac{Aut_K F}{Aut_L F} \cong Im(\phi)$ mais $Im(\phi) = \{\sigma_{\restriction_{L:\sigma \in Aut_K F\}}}$ qui est l'ensemble des éléments extensibles de $Aut_K L$.

Corollaire 3.6. .

Soit $K \subseteq F$ une extension galoisienne finie,
Un corps intermédiaire L est de Galois sur K si et seulement si $Aut_L F$ est un sous groupe normal de $Aut_K F$ et dans ce cas $\frac{Aut_K F}{Aut_L F}$ est isomorphe à $Aut_K L$.

3.1.3 Corps de Décomposition

Tout d'abord remarquons qu'une extension $K \subseteq F$ est dite simple s'il existe $u \in F$ tel $F = K[u]$.

Définition 3.8. .

Soit $K \subseteq F$ une extension et $f = \sum_{i=0}^{n} a_i x^i \in K[X]$.
(i) On dit que f se décompose entièrement dans $F[X]$ (ou sur F) lorsque f peut s'écrire comme produit de facteur linéaire dans $F[X]$ c'est-à-dire que $f = u_0(X - u_1)(X - u_1)...(X - u_n)$, $u_i \in F$ pour tout $i \in \{1, ..., n\}$.
(ii) F est appélé un corps de décomposition de f sur K lorsque f se décompose entièrement dans $F[X]$ et $F = K(u_1, u_2, ..., u_r)$, où $u_1, u_2, ..., u_r$ sont des racines de f dans F.

Théorème 3.6. .

Soit $f \in K[X]$, $degr(f) = n \geq 1$ alors, il existe un corps de décomposition F de f sur K, de plus $[F : K] \leq n!$.

Preuve : Par récurrence sur le degré n de f, si $n = 1$, $f = a_0 + a_1 X = (\frac{a_0}{a_1} + X)a_1$ avec a_1 non nul dans $K[X]$ dans ce cas $F = K$.
Supposons $n \geq 1$ et f ne se decompose pas entiérement dans $K[X]$ et que le corps de

décomposition existe chaque fois pour tout polynôme h de degré stritement inférieur à n f admet un facteur irréductible f_0 dans $K[X]$ tel que degré(f_0)$\geq$ 2 il existe une extension simple $K(u)$ de K où u est une racine de f_0, et $[K(u) : K] = n_0 = degr(f_0)$ donc u est une racine de f d'où $f = (X - u)g$ où degré(g)=n-1 par hypothése de recurrence g admet un corps de décomposition F sur $K(u)$ tel que $[F : K(u)] \leq (n-1)!$ soient $v_1, v_2, ..., v_p$ des racines de g telle que $F = K(u)(u, v_1, ..., v_p)$ donc $F = K(u, v_1, ..., v_p)$, où u et les v_j sont des racines de f c'est-à-dire que F est un corps de décomposition de f sur K. $[F : K] = [F : K(u)][K(u) : K] \leq (n-1)!n_0 \leq (n-1)!n = n!$ donc le resultat est vrai.■

Proposition 3.6. .

Soit $\alpha : K \longrightarrow L$ un isomorphisme de corps, $f \in K[X]$, $degr(f) = n \geq 2$, et $h = \alpha(f)$ l'image de f dans $L(X)$. Si F est un corps de décomposition de f sur K et M est un corps de décomposition de h sur L, alors α s'étend en un isomorphisme $\bar{\alpha} : F \longrightarrow M$.

Théorème 3.7. .

Soit $K \subseteq F$ une extension finie alors, les propriétés suivantes sont équivalentes.

(i) F est un corps de décomposition sur K.

(ii) Tout polynôme irréductible $f \in K[X]$ qui admet une racine dans F se décompose entièrements sur F.

Définition 3.9. .

Soit f un polynôme irréductible sur K,

(i) f est dit séparable s'il existe un corps de décomposition de f sur K dans lequel toutes les racines sont simples(ie f n'a pas de racine multiple).

(ii) Soit $K \subseteq F$ une extension,

un élément $u \in F$ algébrique sur K est dit séparable sur K lorsque son polynôme minimal sur K est séparable, si tout élément de F est algébrique et séparable sur K on dit que l'extension $K \subseteq F$ est séparable.

Théorème 3.8. .

Soit $K \subseteq F$ une extension finie, alors les propriétés suivantes sont équivalentes.

(i) $K \subseteq F$ est une extension galoisienne.

(ii) F est séparable sur K et F est un corps de décomposition sur K.

(iii) F est le corps de décomposition d'un polynôme $f \in K[X]$ dont les facteurs irréductibles sont séparables sur K.

Corollaire 3.7. .

Soit $K \subseteq F$ une extension finie, alors il existe un corps L vérifiant les propriétés suivantes :

(i) $L \subseteq F$ et L est un corps de décomposition sur K.
(ii) Il n'existe pas de corps de décomposition M sur K tel que l'inclusion $L \subseteq M \subseteq F$ soit strite.
(iii) Si $K \subseteq L$ est séparable, alors $K \subseteq F$ est galoisienne.
(iv) Si F_0 est corps vérifiant (i) et (ii) alors F et F_0 sont K-isomorphes. Dès lors F est la clôture normal de L sur K dans (iii).

Corollaire 3.8. .
Soit $K \subseteq F$ une extension finie et séparable alors si K infini il existe $u \in L$ tel que $L = K(u)$.

3.2 Codes cycliques

Soit A un anneau commutatif unitaire la structure d'ideal sur $R = \frac{A[X]}{(X^n-1)}$ à recenment eu un grand intérêt dans le succes des applications de la théorie du codage algébrique. Nous rappelons qu'un code linéaire A de longueur n sur un anneau A est un sous A-module dans l'espace des n-uplets A^n. La notion de codes cycliques apparaît pour la première fois pas l'intermédiaire de Prange dans [9] sucitant beaucoup d'intérêt de par leur structure algébrique ils sont utilisés à la fois pour corriger les erreus isoler et les erreurs en rafale.

Définition 3.10. .
Un code linéaire $\mathcal{C}$ sur un anneau A est cyclique si pour tout n-uplet $(v_0, v_1, ..., v_{n-1})$ de $\mathcal{C}$ le n-uplet shift à droite est dans $\mathcal{C}$.

Le travail de Calderbank [6] montre que l'annneau $R = \frac{\mathbb{Z}_q[X]}{(X^n-1)}$ où $q = p^k$, p premier est un anneau principal et le travail de Interlando [11] donne la struture des idéaux principaux de l'anneaux $R = \frac{\mathbb{Z}_m[X]}{(X^n-1)}$ où m est un entier positif.

Théorème 3.9. .
Soit l'anneau $R = \frac{A[X]}{(X^n-1)}$ et φ un isomorphisme entre A^n et R tel que $\varphi(a_0, ..., a_{n-1}) = \sum_{i=0}^{n-1} a_i X^i$, un sous ensemble $\mathcal{C}$ de A^n est un code cyclique si et seulement si $\varphi(\mathcal{C})$ est un idéal de R.

Preuve : Supposons que $\mathcal{C}$ est un code cyclique alors $(\mathcal{C}, +)$ est un groupe abélien par suite $(\varphi(\mathcal{C}), +)$ est un groupe abélien. De plus, soient $P = \sum_{j=0}^{n-1} a_j X^j$ dans $(\varphi(\mathcal{C}), +)$,

$a \in A$ et $i \in \{0, ..., n-1\}$. On a :

$$\begin{aligned}(aX^i)P &= (aX^i)\sum_{j=0}^{n-1} a_j X^j \\ &= \sum_{j=0}^{n-1} aa_j X^{j+i}\end{aligned}$$

de cette dernière égalité, il s'ensuit que pour tout $i \in \{0, ..., n-1\}$; $(aX^i)P$ est dans $\varphi(\mathcal{C})$ car modulo n le n-uplet $(aa_0, ..., aa_{n-1})$ est shifté à droite chaque fois et $\mathcal{C}$ est code cyclique. Comme A est commutatif, on en déduit pour tout $P \in \varphi(\mathcal{C})$, $Q \in \frac{A[X]}{(X^n-1)}$ $PQ \in \varphi(\mathcal{C})$ $QP \in \varphi(\mathcal{C})$.
Reciproquement si $\varphi(\mathcal{C})$ est un idéal de R alors $(\varphi(\mathcal{C}), +)$ est groupe abélien donc $(\mathcal{C}, +)$ est un groupe abélien. Soit $a \in A$ et $(a_0, ..., a_{n-1}) \in \mathcal{C}$,

$$\begin{aligned}a(a_0, ..., a_{n-1}) &= a\varphi^{-1}(\sum_{i=0}^{n-1} a_i X^i) \\ &= \varphi^{-1}(a\sum_{i=0}^{n-1} a_i X^i)\end{aligned}$$

et $a\sum_{i=0}^{n-1} a_i X^i \in \varphi(\mathcal{C})$ car $\varphi(\mathcal{C})$ est un idéal donc $a(a_0, ..., a_{n-1}) \in \mathcal{C}$ par suite $\mathcal{C}$ est linéaire de plus, soit $(a_0, ..., a_{n-1}) \in \mathcal{C}$ et $i \in \{0, ..., n-1\}$; Posons $v^{(i)} = \varphi^{-1}(X^i \sum_{j=0}^{n-1} a_j X^j)$, on a $X^i \sum_{j=0}^{n-1} a_j X^j \in \mathcal{C}$ (puisque $\sum_{j=0}^{n-1} a_j X^j$ est dans $\varphi(\mathcal{C})$ et $\varphi(\mathcal{C})$ est un ideal) dès lors, $v^{(i)}$ est dans $\mathcal{C}$; donc $\mathcal{C}$ est un code cyclique.■

Plus généralement, considérons $R = \frac{A[X]}{(f(X))}$ l'ensemble des classes modulo le polynôme unitaire f de dégrée n sur A. Nous representerons les éléments de R par les polynômes de la forme $\overline{a}(X) = \sum_{j=0}^{n-1} \overline{a}_j X^j$, nous distingons les ideaux principaux de R c'est-à-dire idéal engendré par un élément $g(X)$ de R appelé polynôme générateur et l'etude d'un code cyclique à partir de ce générateur est notre préoccupation.

Théorème 3.10. .
Soit B un idéal de l'anneau R, si le coefficient dominant d'un polynôme de B est inversible dans A, alors il existe un unique pôlynome unitaire de degré minimal dans B.

Preuve : Soit $\bar{g} = \sum_{i=0}^{m} a_i X^i \in B$ tel que $\bar{a}_m \in \mathcal{U}(A)$; comme B est un idéal, $g_1(X) = a_m^{-1} g(X) \in B$ et g_1 est un pôlynome unitaire de même degré que g. D'ailleur si $\bar{m}_1$ et $\bar{m}_2$ sont des polynômes unitaire de degré minimal m de B il vient que $\bar{m}_1 - \bar{m}_2$ est de degré inférieur à m dans B ainsi $\bar{m}_1 - \bar{m}_2 = 0$ d'où $\bar{m}_1 = \bar{m}_2$.■

Théorème 3.11. .

Soit B un idéal de l'anneau R si le coefficient dominant d'un polynôme $\bar{g}(X)$ de plus petit degré dans B est inversible dans A alors $B =< \bar{g}(X) >$ c'est-à-dire B est un idéal principal.

Preuve : Si $\bar{a}(X) \in B$ par définition de $\bar{g}$ il existe un unique $b(X)$, $r(X) \in A[X]$ tel que $\bar{a}(X) = q(X)\bar{g}(X) + \bar{r}(X)$ et $deg(r(X)) < deg(\bar{g}(X))$ on a $r(X) = \bar{a}(X) - q(X)\bar{g}(X) \in B$ (puisque B est un idéal) la minimalité du degré de $\bar{g}$ impose que $r(X) = 0$ d'où $\bar{a}(X) \in <$ $\bar{g}(X) >$ par suite on a $B =< \bar{g}(X) >$.■

Lemme 3.3. .

Soit $r(X)$ un polynôme sur A. Si $r(X) \neq 0$ et $degr(r(X)) < degr(f(X))$ alors $\bar{r}(X) \neq \bar{0}$ dans R.

Preuve : Supposons que $\bar{r}(X) = \bar{0}$, alors $r(X) = g(X)f(X)$, $g(X) \in A[X]$ mais $r(X) \neq 0$ et f unitaire donc $degr(r(X)) = degr(g(X)) + degr(f(X)) \geq degr(f)$ ce qui est impossible par hypothése donc $\bar{r}(X) \neq \bar{0}$ dans R.

Théorème 3.12. .

Soit B un idéal de l'anneau R, soit $g(X)$ un polynôme sur A tel que $degr(g(X)) < degr(f(X))$ et le coefficient dominant de g est inversible dans A. Si $\bar{g}(X) \in B$ et son dégré est le plus petit dans B alors $g(X)$ divise $f(X)$.

Preuve : On sait que $degr(g(X)) < degr(f(X))$ est le coefficient dominant de g est inversible dans A, il existe $q(X)$, $r(X)$ sur A tel que d'aprés l'algarithme d'euclide $f(X) = q(X)g(X) + r(X)$ et $deg(r(X)) < deg(g(X))$ ainsi on obtient $\bar{r}(X) = \bar{f}(X) - \bar{q}(X)\bar{g}(X) = -\bar{q}(X)\bar{g}(X)$ par suite $\bar{r}(X) = \bar{0}$ et $deg(r(X)) < deg(g(X)) < deg(f(X))$ comme le coefficient domminant de f est inversible il suit que $r(X) = 0$ par conséquent $r(X) = 0$.■

Exemple 3.2.1. .

Considérons R l'anneau $R = \frac{\mathbb{Z}_4[X]}{<f(X)>}$ où $f(X) = X^2 - 1$ et $B = \{\bar{0}, \bar{1}X + \bar{1}, \bar{2}X + \bar{2}, \bar{3}X + \bar{3}\}$ est un idéal de R on a : $B =< \bar{3}X + \bar{3} >$ d'aprés le théoréme 3.11 et 3.12 on a $g(x) = 3X + 3$ qui divise $X^2 - 1$.

Théorème 3.13. .

Soit B un idéal de l'anneau R, si $g(X)$ divise $f(X)$ et $\bar{g}(X) \in B$, alors $\bar{g}(X)$ est le plus petit degré dans $< \bar{g}(X) >$.

Preuve : Soit $\bar{c}(X)$ dans $< \bar{g}(X) >$ tel que $deg(\bar{c}(X)) < deg(\bar{g}(X))$; comme $\bar{c}(X)$ est dans $< \bar{g}(X) >$, alors $\bar{c}(X) = \bar{k}(X)\bar{g}(X)$, $\bar{k}(X) \in R$ ainsi $c(X) - g(X)k(X)$ est dans

$< f(X) >$ c'est-à-dire $c(X) - g(X)k(X) = f(X)e(X)$ pour $e(X)$ dans $A[X]$. De ce fait, nous avons $c(X) = g(X)k(X) + f(X)e(X)$. Par hypothése $g(X)$ divise $f(X)$, il s'ensuit que $g(X)$ divise $g(X)k(X) + f(X)e(X)$ ce qui implique que $g(X)$ divise $c(X)$ impossible car $deg(c(X)) < deg(g(X))$ on déduit que $\bar{g}(X)$ est le plus petit degré dans $< \bar{g}(X) >$.■

Exemple 3.2.2. .
Soit R un anneau $R = \frac{\mathbb{Z}[X]}{<X^3+X^2+X+1>}$ et B est un idéal tel que $\bar{g}(X) = \bar{1}X + \bar{1}$ est B. Nous avons $g(X) = X + 1$ divise $f(X) = X^3 + X^2 + X + 1$ et d'aprés le théorème 3.13 on obtient que $\bar{g}(X)$ est de plus petit degré dans $< \bar{g}(X) >$.

Théorème 3.14. .
Tout code cyclique de longueur n sur $\frac{A[X]}{X^n-1}$ posséde un générateur et un seul qui est un diviseur de $X^n - 1$ dans $A[X]$ et dont le coefficient dominant est 1.

Preuve : Il suffit d'aprés le théorème 3.12 de prendre $f(X) = X^n - 1$ pour déduire que tout générateur de code linéaire sur $\frac{A[X]}{X^n-1}$ divise $X^n - 1$.

Tout d'abord, considérons $\mathcal{C}$ un code cyclique de longueur n sur A, et soit $g(X)$ le générateur de degré u de $\mathcal{C}$. Tout polynôme associé à $\mathcal{C}$ $m(X)$ est de la forme $a(X)g(X)$; il s'ensuit la representation suivante $(a_0+a_1X+...+a_sX^s)g(X) = a_0g(X)+a_1Xg(X)+...+a_sX^sg(X)$, $0 \leq s \leq n-1$ les polynômes $g(X)$, $Xg(X)$,...,$X^{n-1}g(X)$ forment donc une famille génératrice de $m(X)$ dont on peut extraire une base.■

Théorème 3.15. .
La dimension d'un code cyclique de longueur n dont le générateur est $g(X)$ est $k = n - deg(g(X))$.

Théorème 3.16. .
Soit $g(X) = c_0 + c_1X^1 + ... + c_tX^t$ le générateur d'un code cyclique $\mathcal{C}$ de longueur n sur A. La matrice M à k lignes et n colonnes suivante, où $t = deg(g(X)) = n - k$ est une matrice génératrice du code $\mathcal{C}$. On a

$$M = \begin{pmatrix} c_0 & c_1 & c_2 & \cdots & c_t & 0 & \cdots & \cdots & 0 & 0 \\ 0 & c_0 & c_1 & c_2 & \cdots & c_t & 0 & \cdots & 0 & 0 \\ \vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & c_0 & c_1 & c_2 & \cdots & c_t & 0 \\ 0 & 0 & 0 & \cdots & 0 & c_0 & c_1 & c_2 & \cdots & c_t \end{pmatrix}$$

Le codage consiste à multiplier $g(X)$ par des polynômes de degré au plus $k - 1$.

Définition 3.11. .

Soit $g(X)$ le générateur d'un code cyclique $\mathcal{C}$ et $u = deg(g(X))$ l'orthogonal de $\mathcal{C}$ a pour pour dimension $n - dim\mathcal{C} = n - (n - t) = t$ et son polynôme de contrôle est le polynôme $h(X)$ tel que $X^n - 1 = g(X)h(X)$.

Théorème 3.17. .

Soit $\mathcal{C}$ un code cyclique.

-i)L'orthogonal d'un code cyclique $\mathcal{C}$ est un code cyclique.

-ii)Si $h(X)$ est le polynôme de contrôle de $\mathcal{C}$, alors le générateur de l'orthogonal de $\mathcal{C}$ est $X^k h(X^{-1})$.

Théorème 3.18. .

La distance minimal d'un code cyclique $\mathcal{C}$ de matrice génératrice $g(X)$ de degré t est d avec $d \leq t + 1$.

Preuve : On sait que la distance minimal de $\mathcal{C}$ est inférieur ou égal à $n - k + 1$ où n est sa longueur et k sa dimension et comme t est le degré de sa matrice génératrice $g(X)$ qui vaut $n - k$ il s'ensuit que $d \leq t + 1$.■

3.3 Codes BCH

Dans cette partie nous supposons que A est un anneau local fini commutatif et unitaire. Désignons pas M l'idéal maximal de A et posons $\mathbb{K} = \frac{A}{M} \equiv GF(p^m)$ où p est un entier avec $A[X]$ l'anneau des polynômes à variable X sur A. Considérons $\mu : A[X] \to \mathbb{K}[X]$ tel que $\mu(a(X)) = \bar{a}(X)$, soit $f(X)$ un polynôme de degré h dans $A[X]$ tel que $\mu(f(X))$ est irréductible dans $\mathbb{K}[X]$ alors $f(X)$ est irréductible dans $A[X]$. Soit R l'anneau $\frac{A[X]}{f(X)}$ ainsi R est un anneau commutatif local unitaire fini appellé anneau de galois sur A de degré h. En considérant $\mathbb{K}_1 = \frac{A}{M_1} \equiv GF(p^{mh})$ où $\bar{M_1}$ est un idéal maximal de R et $\mathbb{K}_1^*$ le groupe multiplicatif sur $\mathbb{K}_1$ qui est d'ordre $p^{mh} - 1$. Par suite R^* étant le groupe des éléments inversible de R, il s'ensuit que R^* est un groupe abélien et donc on peut l'exprimer comme produit direct de groupes cyclique. De ce fait, nous sommes intéressés pas le sous groupe maximal de R^* que nous noterons $\mathcal{G}_s$ tel que ces éléments soient racine du polynôme $x^s - 1$ et s est un entier tel que $pgcd(s, p) = 1$. Ici, le seul sous groupe à un ordre relativement premier avec p. Ce groupe cyclique est d'ordre $s = p^{mh} - 1$.

Définition 3.12. .

Un code BCH $\mathcal{C}(n,\eta)$ de longueur $n = s$ est un code sur A de matrice de parité

$$H = \begin{pmatrix} \alpha_1 & \alpha_2 \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 \cdots & \alpha_n^2 \\ \vdots & \ddots & \vdots \\ \alpha_1^r & \alpha_2^r \cdots & \alpha_n^r \end{pmatrix}$$

Pour $r \geq 1$, $\eta = (\alpha_1, \alpha_2, ...\alpha_n) = (\alpha^{k1}, \alpha^{k2}, ...\alpha^{kn})$ est constitué d'éléments distinct de $\mathcal{G}_s$, lorque n est un entier inférieur à s on dit que $\mathcal{C}(n,\eta)$ est un petit code BCH.

Lemme 3.4. .
Soit α un élément de $\mathcal{G}_s$ d'ordre s la difference $\alpha^{l_1} - \alpha^{l_2}$ est inversible dans R si $0 \leq l_1 \neq l_2 \leq s-1$.

Preuve : Considérons $\alpha^{l_1} - \alpha^{l_2}$ nous pouvons l'écrire comme suit $\alpha^{l_2}(1 - \alpha^{l_1 - l_2})$ où 1 est l'unité dans R. la quantité α^{l_2} est inversible dans R et pour le second facteur soit $j \in \{1, ..., s-1\}$, par l'absurde si $1 - \alpha^j$ est non inversible dans R alors $1 - \alpha^j \in \bar{M}$ ainsi $\mu'(\alpha)^j = \mu'(1)$ pour $j < s$ impossible par définition de $\mathcal{G}_s$ il s'ensuit que $1 - \alpha^j \in R^*$, pour tous $1 \leq j \leq s-1$. Dés lors $(1 - \alpha^{l_1 - l_2})$ est inversible dans R comme produit d'élément inversible il suit que $\alpha^{l_1} - \alpha^{l_2}$ est inversible dans R.■

Théorème 3.19. .
La distance minimum de hamming d'un code BCH $\mathcal{C}(n,\eta)$ satisfait $d \geq r + 1$.

Preuve : considérons C un mot non nul de $\mathcal{C}(n,\eta)$ tel que $w_H \leq 2t$. Ainsi $cH^T = 0$. dés lors $n - 2t$ colonne de H correspond au zéro il s'ensuit que la nouvelle matrice obtenu est H' est de vandermonde d'aprés le lemme 3.4 le déterminant obtenu est inversible dans R par suite la seule possibilité pour c est que c soit nul. On en déduit que $d - 1 \geq w_H(c)$ dès lors $d \geq w_H(c) + 1 \geq r + 1$.■

Exemple 3.3.1. .
Soit $f(X) = X^3 + X + 1$ un polynôme irréductible sur $GF(2)$ et $A = GF(2)[i]$ où $i^2 = -1$, considérons l'anneaux $R = \frac{A[X]}{(f(X))}$ nous avons si α est un générateurs de $\mathcal{G}_s$ et $s = 2^3 - 1 = 7$, soit $\eta = (\alpha^5, \alpha, 1, \alpha^4, \alpha^2, \alpha^6)$ un vecteur si $r = 2$ alors la matrice

$$H = \begin{pmatrix} \alpha^5 & \alpha & 1 & \alpha^4 & \alpha^2 & \alpha^6 \\ \alpha^3 & \alpha^2 & 1 & \alpha & \alpha^4 & \alpha^5 \end{pmatrix}$$

de code BCH $\mathcal{C}(6,\eta)$ de longueur 6 et la distance minimun de hamming est inférieur à 3.

3.4 Codes alternant

Définition 3.13. .

Un code alternant $\mathcal{C}(n, \eta, w)$ de longueur $n = s$ est un code sur A de matrice de parité

$$H = \begin{pmatrix} w_1 & w_2 \cdots & w_n \\ w_1\alpha_1 & w_2\alpha_2 \cdots & w_n\alpha_n \\ \vdots & \ddots & \vdots \\ w_1\alpha_1^{r-1} & w_2\alpha_2^{r-1} \cdots & w_n\alpha_n^{r-1} \end{pmatrix}$$

où r est un entier positif, $\eta = (\alpha_1, \alpha_2, ..., \alpha_n) = (\alpha_1^{k1}, \alpha_2^{k2}, ...\alpha_n^{kn})$ est un vecteur constitué d'élément de $\mathcal{G}_s$. ce code est dit petit lorsque n est un entier inférieur ou égale à s.

Théorème 3.20. .

Un code alternant $\mathcal{C}(n, \eta, w)$ a une distance minimun $d \geq r + 1$.

Preuve : Soit c un mot non nul de $\mathcal{C}(n, \eta, w)$ tel que $w_H(c) \leq r$, $cH^T = c(XY)^T = 0$. Posons $b = cY^T$ nous avons $w_H(b) = w_H(c)$ avec Y invercible. Dés lors $bX^T = 0$ ce qui entraine que $n - r$ colonne de X correspond à des zéro du mot du code ainsi la nouvelle matrice X' de vandermonde du lemme 3.4 nous permet d'en déduire que le déterminant est inversible dans R par suite la seule possibilité de c est qu'il soit null impossible ce qui en déduire le resultat.■

Exemple 3.4.1. .

Considérons $\eta = (\alpha, \alpha^4, 1, \alpha^3, \alpha^2)$ un vecteur sur R, $w = (\alpha^5, \alpha, 1, \alpha^4, \alpha^2)$ et $r = 2$ alors la matrice

$$H = \begin{pmatrix} \alpha^5 & \alpha & 1 & \alpha^4 & \alpha^2 \\ \alpha^6 & \alpha^5 & 1 & 1 & \alpha^4 \end{pmatrix}$$

est une matrice du code alternant $\mathcal{C}(5, \eta, w)$ de longueur 5 et sa distance minimum de Hammming est inférieur à 3.

3.5 Codes de Goppa et de Srivastava

Dans cette section premiérement nous sommes interessés par les sous classes des codes altenant sur les anneaux locaux finis qui est similaire par ceux proposé par Goppa sur un corps. Maintenant nous savons que les codes cycliques sont déterminé par un polynôme générateur, mais le probléme repose sur la difficulté à estimé la distance de Hamming, par suite les codes de Goppa permet de décrire les polynômes de Goppa $g(x)$. Considérons

A, R, et $\mathcal{G}_s$ définie précédenment et α un élément primitif du groupe cyclic $\mathcal{G}_s$ où $s = p^{mh} - 1$ considérons $g(z) = \sum_{i=0}^{n} g_i z^i$ sur R un polynôme avec $g_r \neq 0$. Considérons $L = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ un ensemble constitué d'élément distint de $\mathcal{G}_s$ tel que $g(\alpha_i)$ est inversible dans R pour $i = 1, 2, ..., n$.

Définition 3.14. .

Un code de Goppa $\mathcal{C}(L, g)$ de longueur $n = s$ est un code sur A de matrice carrée

$$H = \begin{pmatrix} g(\alpha_1)^{-1} & \cdots & g(\alpha_1)^{-1} \\ \alpha_1 g(\alpha_1)^{-1} & \cdots & \alpha_n g(\alpha_n)^{-1} \\ \vdots & \ddots & \vdots \\ \alpha_1^{r-1} g(\alpha_1)^{-1} & \cdots & \alpha_n^{r-1} g(\alpha_n)^{-1} \end{pmatrix}$$

où r est un entier positive $\eta = (\alpha_1, \alpha_2, ...\alpha_n) = (\alpha_1^{k1}, \alpha_2^{k2}, ...\alpha_n^{kn})$ est un vecteur constitué d'élément de $\mathcal{G}_s$ et $w = (g(\alpha_1)^{-1}, ...g(\alpha_n)^{-1})$ est un vecteur constitué d'élément de $\mathcal{G}_s$. lorsque n est un entier inférieur à s l'on dit que c'est un petit Goppa code.

Définition 3.15. .

Soit $\mathcal{C}(L, g)$ un code de Goppa

- *si $g(z)$ est irréductible alors $\mathcal{C}(L, g)$ est appelée irréductible Goppa code.*
- *si $c = (c_1, c_2, ...c_n) \in \mathcal{C}(L, g)$ et $c' = (c_n, c_{n-1}, ...c_1) \in \mathcal{C}(L, g)$ alors $\mathcal{C}(L, g)$ est un code de Goppa reversible.*
- *si $g(z) = (z - \alpha)^r$ alors $\mathcal{C}(L, g)$ est un code de Goppa commutative.*
- *si $g(z)$ n'a pas de zero multiple alors $\mathcal{C}(L, g)$ est appelée un code de Goppa séparable.*

Remarque 3.5.1. .

Soit $\mathcal{C}(L, g)$ un code de Goppa

- $\mathcal{C}(L, g)$ est un code linéaire
- sa matrice génératrice sur A est obtenu en remplaçant les entrées de H par les vecteurs de longueur h sur A.
- Pour un codes de Goppa de polynôme $g_l(z) = (z - \beta_l)^{rl}$, où $\beta_l \in \mathcal{G}_s$ nous avons

$$H_l = \begin{pmatrix} (\alpha_1 - \beta_l)^{-rl} & (\alpha_2 - \beta_l)^{-rl} & \cdots & (\alpha_n - \beta_l)^{-rl} \\ \alpha_1(\alpha_1 - \beta_l)^{-rl} & \alpha_2(\alpha_2 - \beta_l)^{-rl} & \cdots & \alpha_n(\alpha_n - \beta_l)^{-rl} \\ \vdots & \ddots & \vdots & \\ \alpha_1^{rl-1}(\alpha_1 - \beta_l)^{-rl} & \alpha_2^{rl-1}(\alpha_2 - \beta_l)^{-rl} & \cdots & \alpha_n^{rl-1}(\alpha_n - \beta_l)^{-rl} \end{pmatrix}$$

ce qui équivaut à

$$H_l = \begin{pmatrix} (\alpha_1-\beta_l)^{-rl} & (\alpha_2-\beta_l)^{-rl} & \cdots & (\alpha_n-\beta_l)^{-rl} \\ (\alpha_1-\beta_l)^{-(rl-1)} & (\alpha_2-\beta_l)^{-(rl-1)} & \cdots & (\alpha_n-\beta_l)^{-(rl-1)} \\ \vdots & \ddots & \vdots & \\ (\alpha_1-\beta_l)^{-1} & (\alpha_2-\beta_l)^{-1} & \cdots & (\alpha_n-\beta_l)^{-1} \end{pmatrix}$$

par conséquent, si $g(z) = \prod_{i=0}^{k}(z-\beta_l)^{rl} = \prod_{i=0}^{k} g_l(z)$ alors le code de Goppa est l'intersection des codes avec $g_l(z) = (z-\beta_l)^{rl}$, pour $l = 1, 2, ..., k$ et sa matrice de controle est donné par

$$H = \begin{pmatrix} H_1 \\ H_2 \\ \vdots \\ H_k \end{pmatrix}$$

– Les codes BCH sont des cas particuliers des codes de Goppa. choisissons $g(z) = z^r$ et $L = \{\alpha_1, \alpha_2, ..., \alpha_n\}$, où $\alpha_i \in \mathcal{G}_s$ pour $i = 1, 2, ..., n$. alors pour

$$H = \begin{pmatrix} \alpha_1^{-r} & \alpha_2^{-r} & \cdots & \alpha_n^{-r} \\ \alpha_1^{1-r} & \alpha_2^{1-r} & \cdots & \alpha_n^{1-r} \\ \vdots & \ddots & \vdots & \\ \alpha_1^{-1} & \alpha_2^{-1} & \cdots & \alpha_n^{-1} \end{pmatrix}$$

redevient la matrice génératrice du code BCH quand α_i^{-1} est remplacé par β_i, $i = 1, 2, ..., n$.

Théorème 3.21. .

Le code de Goppa $\mathcal{C}(L, g)$ a une distance minimum de hamming $d \geq r + 1$.

Preuve : nous savons que $\mathcal{C}(L, g)$ est un codes alternant $\mathcal{C}(n, \eta, w)$ avec $\eta = (\alpha_1, \alpha_2, ...\alpha_n)$ et $w = (g(\alpha_1)^{-1}, g(\alpha_2)^{-1}, ...g(\alpha_n)^{-1})$ maintenant le théorème 3.20 nous permet d'en déduire que $\mathcal{C}(L, g)$ à une distance minimum $d \geq r + 1$.■

Exemple 3.5.1. .

Soit $A = GF(2)[i]$ et $R = \frac{A[X]}{(f(X))}$ où, $f(X) = X^4 + X + 1$ est irréductible sur A. Ainsi pour $s = 15$ et $\mathcal{G}_s$ de générateur α, où $\alpha^4 = \alpha + 1$. soit $g(X) = X^4 + X^3 + 1$, $L = \{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}\}$ et $w = \{\alpha^{12}, \alpha^{10}, \alpha^7, \alpha^3, \alpha^{11}, \alpha^6, \alpha^9, \alpha^5, \alpha^{14}, \alpha^{13}\}$, La matrice

$$H = \begin{pmatrix} 1 & \alpha^{12} & \alpha^{10} & \alpha^{7} & \alpha^{3} & \alpha^{11} & \alpha^{6} & \alpha^{9} & \alpha^{5} & \alpha^{14} & \alpha^{13} \\ 1 & \alpha^{14} & 1 & \alpha^{4} & \alpha^{11} & \alpha^{2} & \alpha^{7} & \alpha^{13} & 1 & \alpha^{8} & \alpha \\ 1 & \alpha & \alpha^{5} & \alpha & \alpha^{4} & \alpha^{8} & \alpha^{8} & \alpha^{2} & \alpha^{13} & \alpha^{2} & \alpha^{2} \\ 1 & \alpha^{3} & \alpha^{10} & \alpha^{13} & \alpha^{12} & \alpha^{14} & \alpha^{9} & \alpha^{6} & \alpha^{5} & \alpha^{11} & \alpha^{7} \end{pmatrix}$$

est la matrice génératrice d'un code de Goppa sur $GF(2)[i]$ de longueur 11 et de distance minimum de Hamming inférieur à 5. Maintenant nous sommes intéressé par d'autre sous classe des codes alternant sur les anneaux finis local qui sont simillaire par ceux proposé par Srivastava en 1967 dans unpublished work tel que la matrice génératrice est de la forme

$$H = \{\frac{\alpha_j^l}{1-\alpha_i\beta_j}, 1 \leq i \leq r, 1 \leq j \leq n\}$$

où $\alpha_1, \alpha_2, ..., \alpha_r$ sont des éléments distinct sur $GF(q^m)$ et β_1, β_2,...,β_n sont des éléments de $GF(q^m)$.

Définition 3.16. .

Un code de Srivastava de longueur $n = s$ est un code sur A de matrice de contrôle

$$H = \begin{pmatrix} \frac{\alpha_1^l}{\alpha_1-\beta_1} & \frac{\alpha_2^l}{\alpha_2-\beta_1} \cdots & \frac{\alpha_n^l}{\alpha_n-\beta_1} \\ \frac{\alpha_1^l}{\alpha_1-\beta_2} & \frac{\alpha_2^l}{\alpha_2-\beta_2} \cdots & \frac{\alpha_n^l}{\alpha_n-\beta_2} \\ \vdots & \ddots & \vdots \\ \frac{\alpha_1^l}{\alpha_1-\beta_r} & \frac{\alpha_2^l}{\alpha_2-\beta_r} \cdots & \frac{\alpha_n^l}{\alpha_i-\beta_j} \end{pmatrix}$$

où r,l sont entier positive et $\alpha_1, \alpha_2, ..., \alpha_r$,$\beta_1$, β_2,...,β_n sont $n + r$ éléments distinct de $\mathcal{G}_s$. un tel code est dit petite lorque n est inférieur ou égale à s.

Théorème 3.22. .

Un code de Srivastava a une distance minimun $d \geq r + 1$.

Preuve : Tout d'abord remarquons que la distance minimun de ce code est inférieur à $r + 1$ si et seulement si toute conbinaison de moin de r colonne de H sont linéairement indépendant sur R ou la sous matrice

$$H_1 = \begin{pmatrix} \frac{\alpha_{i_1}^l}{\alpha_{i_1}-\beta_1} & \frac{\alpha_{i_2}^l}{\alpha_{i_2}-\beta_1} \cdots & \frac{\alpha_{i_r}^l}{\alpha_{i_r}-\beta_1} \\ \frac{\alpha_{i_1}^l}{\alpha_{i_1}-\beta_2} & \frac{\alpha_{i_2}^l}{\alpha_{i_2}-\beta_2} \cdots & \frac{\alpha_{i_r}^l}{\alpha_{i_r}-\beta_2} \\ \vdots & \ddots & \vdots \\ \frac{\alpha_{i_1}^l}{\alpha_{i_1}-\beta_r} & \frac{\alpha_{i_2}^l}{\alpha_{i_2}-\beta_r} \cdots & \frac{\alpha_{i_r}^l}{\alpha_{i_r}-\beta_r} \end{pmatrix}$$

est singulier. le déterminant de la matrice est exprimé comme suit :

$$det(H_1) = (\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3}, ..., \alpha_{i_r})^l det(H_2)$$

où la matrice est donné par

$$H_2 = \begin{pmatrix} \frac{1}{\alpha_{i_1}-\beta_1} & \frac{1}{\alpha_{i_2}-\beta_1}\cdots & \frac{1}{\alpha_{i_r}-\beta_1} \\ \frac{1}{\alpha_{i_1}-\beta_2} & \frac{1}{\alpha_{i_2}-\beta_2}\cdots & \frac{1}{\alpha_{i_r}-\beta_2} \\ \vdots & \ddots & \vdots \\ \frac{1}{\alpha_{i_1}-\beta_r} & \frac{1}{\alpha_{i_2}-\beta_r}\cdots & \frac{1}{\alpha_{i_r}-\beta_r} \end{pmatrix}$$

Dés lors le $det(H_2)$ est de cauchy d'ordre r on peut conclure que le déterminant de la matrice H_1 est donné par $det(H_1) = (\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3}, ..., \alpha_{i_r})^l \frac{(-1)^{r_2}\phi(\alpha_{i_1},\alpha_{i_2},\alpha_{i_3},...,\alpha_{i_r})\phi(\beta_1,\beta_2,\beta_3,...,\beta_r)}{\nu(\alpha_{i_1})\nu(\alpha_{i_2})...\nu(\alpha_{i_r})}$ où $\phi(\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3}, ..., \alpha_{i_r}) = \prod_{i_j \leq i_h}(\alpha_{i_j} - \alpha_{i_h})$ et $\nu(x) = (x-\beta_1)(x-\beta_2)...(x-\beta_r)$ ainsi par le théorème7 [4] nous avons $det(H_1)$ est inversible dans R et maintenant $d \geq r+1$.■

Définition 3.17. *Supposons $r = kl$ et soient $\alpha_1, \alpha_2, \alpha_3, ..., \alpha_n$, $\beta_1, \beta_2, \beta_3, ..., \beta_k$, $n+k$ élément distinct de $\mathcal{G}_s$, $w_1, w_2, w_3, ..., w_k$ est un éléments de $\mathcal{G}_s$. Un code de Srivastava généralisé de longueur $n \leq s$ est un code sur A de matrice génératrice.*

$$H = \begin{pmatrix} H_1 \\ H_2 \\ \vdots \\ H_k \end{pmatrix}$$

où

$$H_j = \begin{pmatrix} \frac{w_1}{\alpha_1-\beta_j} & \frac{w_2}{\alpha_2-\beta_j}\cdots & \frac{w_n}{\alpha_n-\beta_j} \\ \frac{w_1}{(\alpha_1-\beta_j)^2} & \frac{w_2}{(\alpha_2-\beta_j)^2}\cdots & \frac{w_n}{(\alpha_n-\beta_j)^2} \\ \vdots & \ddots & \vdots \\ \frac{w_1}{(\alpha_1-\beta_j)^l} & \frac{w_2}{(\alpha_2-\beta_j)^l}\cdots & \frac{w_n}{(\alpha_n-\beta_j)^l} \end{pmatrix}$$

pour j=1,2,...,k.

Théorème 3.23. .

Un code de Srivastava généralisé ainsi définit à une distance minimum de Hamming $d \geq kl+1$.

Preuve : Il suffit de prendre $g(z) = \prod_{i=1}^{k}(z-\beta_i)^l$, et appliquée le théorème précédent pour conclure.■

Exemple 3.5.2. .

$n = 7$, $r = 6$, $k = 2$, $l = 3$; $\{\alpha_1, \alpha_2 ..., \alpha_n\} = \{\alpha^4, \alpha^3, \alpha^5, \alpha, \alpha^7, \alpha^{12}, \alpha^{10}\}$, $\{\beta_1, \beta_2\} =$

$\{\alpha^9, \alpha^6\}$, $\{w_1, ..., w_7\} = \{\alpha, \alpha, \alpha^2, \alpha^4, \alpha^7, \alpha^{10}, \alpha^9\}$ alors la matrice

$$H = \begin{pmatrix} \frac{\alpha}{\alpha^4-\alpha^9} & \frac{\alpha}{\alpha^3-\alpha^9} & \frac{\alpha^2}{\alpha^5-\alpha^9} & \frac{\alpha^2}{\alpha-\alpha^9} & \frac{\alpha^5}{\alpha^7-\alpha^9} & \frac{\alpha^{10}}{\alpha^{10}-\alpha^9} & \frac{\alpha^9}{\alpha^{10}-\alpha^9} \\ \frac{\alpha}{(\alpha^4-\alpha^9)^2} & \frac{\alpha}{(\alpha^3-\alpha^9)^2} & \frac{\alpha^2}{(\alpha^5-\alpha^9)^2} & \frac{\alpha^2}{(\alpha-\alpha^9)^2} & \frac{\alpha^5}{(\alpha^7-\alpha^9)^2} & \frac{\alpha^{10}}{(\alpha^{10}-\alpha^9)^2} & \frac{\alpha^9}{(\alpha^{10}-\alpha^9)^2} \\ \frac{\alpha}{(\alpha^4-\alpha^9)^3} & \frac{\alpha}{(\alpha^3-\alpha^9)^3} & \frac{\alpha^2}{(\alpha^5-\alpha^9)^3} & \frac{\alpha^2}{(\alpha-\alpha^9)^3} & \frac{\alpha^5}{(\alpha^7-\alpha^9)^3} & \frac{\alpha^{10}}{(\alpha^{12}-\alpha^9)^3} & \frac{\alpha^9}{(\alpha^{10}-\alpha^6)^3} \\ \frac{\alpha}{\alpha^4-\alpha^6} & \frac{\alpha}{\alpha^3-\alpha^6} & \frac{\alpha^2}{\alpha^5-\alpha^6} & \frac{\alpha^2}{\alpha-\alpha^6} & \frac{\alpha^5}{\alpha^7-\alpha^6} & \frac{\alpha^{10}}{\alpha^{12}-\alpha^9} & \frac{\alpha^9}{\alpha^{10}-\alpha^6} \\ \frac{\alpha}{(\alpha^4-\alpha^9)^2} & \frac{\alpha}{(\alpha^3-\alpha^9)^2} & \frac{\alpha^2}{(\alpha^5-\alpha^9)^2} & \frac{\alpha^2}{(\alpha-\alpha^9)^2} & \frac{\alpha^5}{(\alpha^7-\alpha^9)^2} & \frac{\alpha^{10}}{(\alpha^{10}-\alpha^9)^2} & \frac{\alpha^9}{(\alpha^{10}-\alpha^9)^2} \\ \frac{\alpha}{\alpha^4-\alpha^6} & \frac{\alpha}{\alpha^3-\alpha^6} & \frac{\alpha^2}{\alpha^5-\alpha^6} & \frac{\alpha^2}{\alpha-\alpha^6} & \frac{\alpha^5}{\alpha^7-\alpha^6} & \frac{\alpha^{10}}{\alpha^{12}-\alpha^9} & \frac{\alpha^9}{\alpha^{10}-\alpha^6} \end{pmatrix}$$

est une matrice génératrice du codes de Srivastava avec une distance minimum inférieur à 7.

♣ Intérêt pédagogique ♣

Nous savons que les structures algébriques nous permettent d'avoir une compréhension général sur les structures élémentaires tels que l'addition et la multiplication, dès lors ce concept nous permet de définir les relations entre éléments favorisant l'interprétation d'une configuration donnée. Par ailleur cette théorie facilite la compréhension du fontionnement d'un systéme de codage tel que le téléphone, l'ordinateur.

♣ Conclusion et perspectives ♣

Dans notre travail, l'investigation des structures algébriques nous a permi d'élaborer de manière déductive certaines propriétés dans la théorie du codage algébrique favorisant ainsi leur interprétation mais plusieurs dificultés s'etend aux niveau de la caractérisation de la distance minimale d'un code (qui est une pièce indispensable dans la définition de tels codes). Nous détaillons dans ce mémoire la notion de code sur un anneau fini et entre autre nous établissons des liens entre differents codes, donnant ainsi une relation d'éfficacité entre de tels codes. Au vu de la confidentialité d'un message qui est un élément majeur dans la notion du codage, la notion d'entropie est cruciale en cryptographie. En effet, il est trés important que tous les messages cryptés aient une entropie forte, pour ne pas que les traces d'organisations dans un message donnent des informations sur la manière dont il a été crypté. Mais il est aussi important que l'entropie reste forte si on arrive à connaître des informations dépendantes, par exemple la connaissance d'un message et de son cryptage ne devrait pas donner d'information sur la clef utilisée.

♣ Bibliographie ♣

[1] A.A Andrade and R.Palazzo Jr ; Codigos de bloco lineares sobre anéis comutativos finitos com identidade, Rev. Mat. Estat, 16 (1998), 161-172

[2] A.A Andrade et M.G.C Andrade, A note on principal ideal rings, Rev. Mat. Estat, 18 (2000), 207-212.

[3] A.A Andrade and R.Palazzo Jr, Construction and decodind of BCH codes over finite commutative rings, Linear Algebra Applic, 286 (1999), 69-85.

[4] A.A Andrade and R.Palazzo Jr, A note on units of a local finite rings, Rev. de Mat, Estat, 18 (2000), 213-222

[5] A.A Andrade, J.C.Interlando and R.Palazzo Jr, Alternant, and BCH code over certains rings, Computational and Appllied Mathematics, 22 No.2 (2003),233-247.

[6] A.R.Cadlderbank and N.J.A Sloane, Modular and p-adic cyclic codes, des codes Cryptogr 6 (1995), 21-35.

[7] V.D.Goppa, A new class of linear error-correcting codes, Preblach.Inform, 6, No.3(1970),24-30.

[8] A.A. Nechaev.Kerdock code in a cyclic form. Discrete Mathematics Appl.,1 :365-384, 1991.

[9] Eugene prange Clyclic Error correcting codes in ttwo symbols. Air Force

cambridge Research center. 1957

[10] G.H.Norton and A. Salagean on the Hamming of linear codes over a finite chain rings, IEEE Trans.Inform. Theory, $vol.46\ No.3$ (2000) PP.$1060-1067$

[11] J.C. Interlando and R. Palazzo Jr. A note on cyclic codes over $\mathbb{Z}_m$, Latin Amer. Appl. Res, $25/S$ (1995) $83-85$.