REPUBLIQUE DU CAMEROUN
****
Paix – travail – Patrie
****
UNIVERSITÉ DE YAOUNDÉ I
****
ECOLE NORMALE SUPERIEURE DE YAOUNDE
****
DEPARTEMENT DE MATHEMATIQUES

N
E S

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

CODES SUR LES ANNEAUX DE GALOIS

Mémoire présenté et soutenu publiquement en vue de l'obtention du DIPES II en Mathématiques

Par:

BIKAÏ-BI-NYEMB VALERY MERVEIL

Matricule: 10S12759

Licencié en Mathématiques

Sous la direction de :

Pr. MOUAHA Christophe

Maître de Conférences

École Normale Supérieure, Université de Yaoundé 1

Année académique : 2018-2019

Dédicace

A toute ma famille

Remerciements

Mes remerciements vont tout d'abord à l'endroit de mon directeur de mémoire le Pr MOUAHA CHRISTOPHE qui n'a ménagé aucun effort pour me conduire dans ce travail , ensuite à tous mes enseignants de l'Ecole Normale supérieure de Yaoundé ,ainsi qu'à ceux de l'Université de Douala plus précisément du département de mathématiques et informatique.

Je remercie particulièrement mes parents M.et Mme MAKOUMAG pour le soutient incommensurable qu'ils ne cessent de m'apporter.

Je rémercie tout aussi mes camarades de l'Ecole Normale supérieure de yaoundé plus particulièrement ceux de mon groupe de récherche pour la franche et bénéfique collaboration. Je citerai nomement mes amis : IROUME, KAMTO, TCHOMTE, KAMGA, EBANDA, ACHABA, DONGMO, TCHAGNA, MPONO, DJACHEUN, TEGA, NGWEM et bien d'autres pour les bon moments qu'on a eu à partager ensemble.

Déclaration sur l'honneur

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

Signature du candidat

BIKAÏ-BI-NYEMB VALERY MERVEIL

Résumé

Dans ce travail , Il a été question pour nous de parcourir la notion d'anneau de Galois , de faire la présentation d'une famille particulière de codes linéaires , les codes cycliques . En outre , notre travail nous a conduit à présenter et proposer des métriques dont l'une sur les codes quaternaires, qui sont les codes sur l'anneau $\mathbb{Z}_4$.'Ces métriques sont d'un apport significatif dans la théorie du décodage.

Mots-clé : codes linéaires , codes cycliques , anneaux de Galois

Abstract

This work aimed to present and propose metric on linear code .To attend this objective we have started by showing sumarise of notion of the Galois ring with great interest on linear codes and particulary on cyclic code.
keywords : linear code , cyclic code , Galois ring.

Sommaire

Introduction

Il est indéniable que les nouvelles technologies de l'information et de la communication ont embrasé le monde dans son entièreté et plus particulièrement notre pays le **CAMEROUN** .Cette mouvance existe depuis un certain nombre d'années.

Malgré la simplicité , la flexibilité, et même l'opérationalité de ces mutations, elles s'accompagnent de quelques difficultés liées à un certain nombre d'aléas tels que la mauvaise qualité du signal ou du réseau.Il est préalablement à noter que la transmission des messages et autres informations est rendue possible par un système dont les outils majeurs sont les codes.

Les difficultés rencontrées sont donc liées aux erreurs sur des codes de transmission.

Cette proximité des technologies de l'information et de la communication avec certains outils mathématiques , les *codes linéaires* a poussé notre curiosité et suscité notre intérêt pour ceux-ci.

Dans ce document qui va s'articuler en trois chapitres, nous nous intéresserons particulièrement à l'étude des anneaux de Galois et aux codes sur les anneaux de Galois .

Au premier chapitre nous allons faire quelques rappels sur les groupes , les anneaux et les corps ; nous y évoquerons aussi quelques éléments importants sur les modules.

Au deuxième chapitre nous entrerons de plein pied dans la notion d'anneaux de Galois afin de parcourir certaines constructions de tels types d'anneaux .

Pour terminer nous donnerons la définition de codes avant d'y établir des métriques dont l'une est intimement liée à la famille des codes quaternaires.

Chapitre 1

PRÉLIMINAIRES.

1.1 Introduction

Au vue de l'encrage de l'étude que nous allons mener sur des structures algébriques il nous a semblé optimal de proposer quelques rappels sur les notions de groupes, d'anneaux et de corps.

1.2 Quelques éléments constitutifs sur les groupes , les anneaux et corps

Définition 1.1. *On appelle groupe un couple $(G, .)$ où G est un ensemble quelconque non vide et "." est une loi de composition interne vérifiant :*

1. *il existe un élément que l'on notera "e_G" tel que : $\forall x \in G, x.e_G = e_G.x = x$;*
2. *$\forall x, y, z \in G; x.(y.z) = (x.y).z$;*
3. *$\forall x \in G \; \exists y \; tel \; que \; x.y = y.x = e_G$.*

Remarque 1.1. *Le 1. traduit l'existence d'un élément neutre pour le groupe ; le 2. traduit l'associativité de la loi composition interne et enfin le 3. renseigne que tout élément est symétrisable.*

N.B *: Si l'on n'est sur le coup d'aucune ambiguité l'on désignera simplement le groupe par G.*

Définition 1.2. *Soit H un sous ensemble non vide de G , on dit que H est un sous-groupe du groupe G si H devient un groupe lorsqu'on le muni de la loi "." de G . Il suffit donc que :*

$$\forall x \in H, \; x^{-1} \in H \tag{1.1}$$

$$\forall x, y \in H, \; x.y \in H \tag{1.2}$$

Exemple 1.1. *$\mathbb{Z}$ muni de la loi $+$ est un sous-groupe de $\mathbb{R}$*

Définition 1.3. *Soient G un groupe et A une partie de G , le sous-groupe K engendré par A est le plus petit sous-groupe de G contenant A.*
*Si A a un seul élément alors K est dit **monogène** ; si de plus K est fini alors on dira que K est **cyclique**.*

Définition 1.4. *Soit H un sous-groupe d'un groupe G , les classes à gauche respectivement les classes à droite suivant H sont données par : $aH = \{ah \ , h \in H\}$, $Ha = \{ha \ , h \in H\}$ pour $a \in G$.*

Remarque 1.2. *Si G est un groupe fini, il existe donc de ce fait autant de classes à gauche que celles à droite suivant le sous-groupe H. On définit par conséquent l'indice de H comme le nombre commun de classes à gauche et de classes à droite suivant H et 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 . On a en effet $|G| = |H|[G : H]$*

Définition 1.5. *Le centre d'un groupe G est le sous-groupe de G noté $Z(G)$ et défini par :*
$Z(G) = \{x \in G \ ; \ x.y = y.x \ \forall y \in G\}$

Définition 1.6. *On dit qu'un sous-groupe H du groupe G est un sous-groupe distingué ou normal de G si*

$$\forall g \in G \ et \ \forall h \in H \ , \ g.h.g^{-1} \in H \tag{1.3}$$

Remarque 1.3. *C'est-à-dire que l'ensemble des classes à gauche est égale celui des classes à droite.*
On remarque que le centre $Z(G)$ du groupe G est un sous-groupe distingué de G.

Preuve : Soit G un groupe , soient $g \in G$ et h un élément de $Z(G)$. On a pour tout x dans G ,

$$\begin{aligned} g.h.g^{-1}.x &= g.g^{-1}.h.x \ (\ car \ h \in Z(G)) \\ &= h.x \\ &= x.h \\ &= x.h.g.g^{-1} \\ &= x.g.h.g^{-1} \end{aligned}$$

donc $g.h.g^{-1}$ est un élément de $Z(G)$ ce qui achève la preuve. ■

Définition 1.7. *On appelle morphisme de groupes , une application γ d'un groupe G dans un autre groupe H vérifiant :*

- *pour tout a et b appartenant à G , $\gamma(a.b) = \gamma(a).\gamma(b)$;*
- $\gamma(e_G) = e_H$.

*On dira que γ est un **endomorphisme** si $G = H$ et dans ce cas il sera appelé **monomorphisme** s'il est injectif et **épimorphisme** s'il est surjectif.*
*S'il est à la fois injectif et surjectif il est appelé **automorphisme**.*

Exemple 1.2. *l'application γ définie par :*

$$\begin{array}{rcl} \gamma : (\mathbb{Z}, +) & \longrightarrow & (\mathbb{Z}, +) \\ a & \longmapsto & 2a \end{array}$$

est un monomorphisme.
On a ; $\gamma(0) = 0$ en effet $\gamma(0) = 20 = 0$.
Soient a et b dans $\mathbb{Z}$,

$$\begin{array}{rcl} \gamma(a+b) & = & 2(a+b) \\ & = & 2a + 2b \\ & = & \gamma(a) + \gamma(b) \end{array}$$

d'où γ est un morphisme de groupes et de plus

$$\begin{array}{rcl} \gamma(a) = \gamma(b) & \Longrightarrow & 2a = 2b \\ & \Longrightarrow & a = b; \end{array}$$

ce qui entraine que γ est injectif.

1.2.1 Anneaux et corps [1]

Définition 1.8. *On appelle anneau , un triplet (A,+,.) où A est un ensemble , " $+$ " et " . " sont les lois de composition internes telles que (A,+) soit un groupe abélien et " . " vérifie :*

- " . " *est distributive par rapport à " $+$ " ;*
- " . " *est associative ;*
- " . " *admet un élément neutre qu'on pourra noter 1_A.*

L'anneau A sera dit *commutatif* si $\forall x, y \in A\ ,\ x.y = y.x$

Comme pour les groupes on peut désigner simplement l'anneau par son ensemble sous-jasent A.

Dans la suite les anneaux seront considérés commutatifs sauf mention du contraire.

Propriété 1.1. *soit A un anneau et soit δ le morphisme d'anneaux de $\mathbb{Z}$ dans A défini par :*
$\delta(n) = n1_A$; le noyau de cet homomorphisme est un idéal de $\mathbb{Z}$ alors il existe
$n_0 \in \mathbb{Z}$ tel que $Ker(\delta) = n_0\mathbb{Z}$

Définition 1.9. *On désigne par caractéristique de l'anneau A; l'entier n_0 donné dans propriété précédente.*

Définition 1.10. *Un élément non nul x d'un anneaux A est dit inversible dans A s'il existe un autre élément non nul y dans A tel que :*
$x.y = y.x = 1_A$. L'élément y qui est l'inverse de x est noté x^{-1}
L'ensemble des éléments inversibles de A est noté $U(A)$ et appelé groupe des unités de A.

Proposition 1.1. *L'ensemble $U(A)$ est un groupe lorsqu'on le muni de la deuxième loi de A.*

Définition 1.11. *Soit $a \in A - \{0\}$, a est dit élément **irréductible** de A si :*

1. *$a \notin U(A)$;*
2. *pour tout $x, y \in A$,$xy = a \Longrightarrow x$ est inversible ou y est inversible.*

Définition 1.12. *L'élément $p \in A - \{0\}$ p est dit élément **premier** de A si :*
1) $p \notin U(A)$;
2) pour tout x,$y \in A$ $p|xy \Longrightarrow p|x$ ou $p|y$.

Proposition 1.2. *Dans un anneau intègre tout élément premier est irréductible.*

Preuve :

Soit p un élément premier de A ,alors p est non inversible .

Supposons de plus pour $x\ ,\ y \in A$ tels que $xy = p$; alors $p|x$ ou $p|y$ supposons sans nuire à la généralité que $p|y$;alors $\exists u \in A$ tel que : $upx = p$

il suit que $x|1_A$ d'où le résultat. ■

Exemple 1.3. *Les éléments irréductibles de l'anneau $\mathbb{Z}$ sont les nombres premiers et leur opposé.*

En effet soit $p \in \mathbb{Z}$ tel que p irréductible alors :

1. *p est non inversible c'est-à-dire que $p \notin U(\mathbb{Z}) = \{1, -1\}$*
2. *$\forall a \; et \; b \in \mathbb{Z}$ tels que $ab = p$ avec p supposé irréductible par hypothèse , alors $a \in U(\mathbb{Z})$ ou $b \in U(\mathbb{Z})$ c'est-à-dire $p = \pm a$ ou $p = \pm b$ ce entraine que p est premier ou l'opposé d'un nombre premier.*

Définition 1.13. *Un sous ensemble non vide B de A est un sous-anneau de A si :*
i) B est un sous-groupe de $(A, +)$;
ii) $\forall a, b \in B \; a.b \in B$.

Définition 1.14. *Soit A un anneau commutatif ; on définit sur A une relation notée $\sim$.*
Soient $x \; et \; y \in A \; x \sim y$ si et seulement si $\exists u \in U(A)$ tel que $x = uy$.

Si deux éléments x et y sont en rélation c'est-à-dire $x \sim y$ alors on dira que x et y sont associés.
" $\sim$ " ainsi définie est une relation d'équivalence .
Preuve : Montrons que " $\sim$ " est une relation d'équivalence. Soient $x, y \; et \; z \in A$ on a :

1. $x \sim x$ car $x = 1_A.x$ et 1_A est inversible ;
2. supposons $x \sim y$ alors il existe $u \in U(A)$ tel que $x = uy$ ce qui entraine que $y = u^{-1}x$; comme $u \in U(A)$ alors $u^{-1} \in U(A)$, d'où $y \sim x$
3. supposons que $x \sim y$ et $y \sim z$ alors il existe $u \; et \; v \in U(A)$ tels que $x = uy$ et $y = vz$ ce qui entraine que

$$\begin{aligned} x &= u(vz) \\ &= (uv)z \;\; (car \; A \; est \; un \; anneau) \end{aligned}$$

et comme $U(A)$ est un groupe multiplicatif d'où $uv \in U(A)$ et par conséquent $x \sim z$.

■

Propriété 1.2. *soient p et p' deux éléments d'un anneau A.*
A1) Si p est irréductible et $p \sim p'$ alors p' est irréductible.
A2) Si p est premier et $p \sim p'$ alors p' est premier.

Preuve :

A1) soit p un élément irréductible de A supposons que $p \sim p'$:soient donc $a \; et \; b$ deux éléments

de A tels que $p' = ab$ alors comme par hypothèse $p \sim p'$ $\exists u \in U(A)$ tel que $p = up'$ il suit que $p = uab$ or p est irréductible donc $ua \in U(A)$ ou $b \in U(A)$ c'est-à-dire $a \in U(A)$ ou $b \in U(A)$ donc p' est irréductible.

A2) soit p un élément premier de A supposons que $p \sim p'$: soient donc $a\ et\ b$ deux éléments de A tels que $p'|ab$ alors comme par hypothèse $p \sim p'$ $\exists u \in U(A)$ tel que $p = up'$ il suit que $p|ab$ car u est inversible ,or p est premier par hypothèse d'où $p|a\ ou\ p|b$.

Il suit que $p'|a\ ou\ p'|b$ donc p' est premier ■

Définition 1.15. *On dira qu'un sous ensemble non vide I d'un anneau A est un idéal si :*

i) I est un sous-groupe de $(A, +)$;

ii) $\forall a \in A$ et $i \in I$, $a.i \in I$ et $i.a \in I$.

*Si I est différent de A alors I est dit **propre**.*

Définition 1.16. *Soient A un anneau et I un idéal de A , on définit sur A la relation binaire R_I par : $(x, y) \in R_I$ si et seulement si $x - y \in I$.*

Il est immédiat que R_I est une relation d'équivalence.

l'ensemble des classes des éléments de A modulo R_I que nous noterons A/I est un anneau lorsqu'on le muni des lois $\bar{+}$ et $\bar{\times}$ définies par :

$$\forall x\ , y \in A\ \ \bar{x} := x + I$$

- $\bar{x}\ \overline{\times}\ \bar{y} = \overline{xy}$
- $\bar{x}\ \overline{+}\ \bar{y} = \overline{x + y}$

Définition 1.17. *Soient A un anneau et I un idéal de A. I est dit idéal premier si :*

- $\forall x\ et\ y \in A,\ xy \in I \Longrightarrow (x \in I\ ou\ y \in I)$

Exemple 1.4. *L'anneau A et l'ensemble $\{0\}$ sont des idéaux premiers de A.*

Définition 1.18. *Soient A un anneau et M un idéal propre de A . M est dit **idéal maximal** de A si :*

- $\forall J$ *idéal propre de A tel que $M \subset J \Longrightarrow J = M$*

Remarque 1.4.

- *Si p est irréductible alors l'idéal engendré par p noté (p) est **maximal** parmi les idéaux principaux.*
- *Si x est premier alors l'idéal engendré par x est un idéal **premier**.*

Définition 1.19. *Un anneau est dit **local** s'il possède un unique idéal maximal ; et **semi-local** s'il possède un nombre fini d'idéaux maximaux.*

Exemple 1.5. *Posons $A = \mathbb{Z}/p^n\mathbb{Z}$ tel que p est premier et $n \in \mathbb{N}, n \geq 2$; cet anneau anneau est local.*

Preuve : On sait que les idéaux de A sont sous la forme $I/p^n\mathbb{Z}$ où I est un idéal de $\mathbb{Z}$ tel que $p^n\mathbb{Z} \subset I$; comme $\mathbb{Z}$ est principal alors $I = m\mathbb{Z}$ ce qui conduit à $p^n\mathbb{Z} \subset m\mathbb{Z}$ c'est-à-dire $m|p^n$. On écrira donc dans ce cas $I/p^n = m\mathbb{Z}/p^n\mathbb{Z} = (\bar{m})$.
Donc A est principal et les seuls idéaux maximaux sont engendrés par les irréductibles de A qui sont les $\bar{t}$ tels que t irréductible dans $\mathbb{Z}$ et $t|p^n$; or les irréductibles de $\mathbb{Z}$ sont les nombres premiers .
D'où **le seul idéal maximal** de A est celui engendré par $\bar{p}$ c'est-à-dire : $p\mathbb{Z}/p^n\mathbb{Z}$. ■

Définition 1.20. *soient $(A, +, .)$ et $(B, +, .)$ deux anneaux ; l'application λ est dite morphisme d'anneaux si :*

- *λ est un morphisme de groupes ;*
- *$\forall x \in A$ et $\forall y \in A$, $\lambda(x.y) = \lambda(x).\lambda(y)$.*

Remarque 1.5. *Le couple $(U(A), .)$ est un groupe.*

Preuve : Soient x, y deux éléments de $U(A)$ on a :

— $(x.y).(y^{-1}.x^{-1}) = (y^{-1}.x^{-1}).(x.y) = 1_A$; ce qui conduit au fait que $x.y$ soit inversible c'est-à-dire un élément de $U(A)$;

— ensuite $x^{-1}.x = x.x^{-1} = 1_A$ ce qui prouve que x^{-1} est un élément de $U(A)$.

Ces deux assertions suffisent pour affirmer que $U(A)$ est un groupe car "." est déjà associative et admet pour élément neutre 1_A . ■

Définition 1.21. *Lorsque tous les éléments non nuls d'un anneau sont inversibles , il s'agit d'un **corps**.*

Définition 1.22. *Un anneau A est dit intègre si :*
$\forall a, b \in A \; a.b = 0 \Rightarrow (a = 0 \; ou \; b = 0)$.
*Un élément x de A qui a la propriété : $\exists y \in A \; ; x.y = 0$,est un **diviseur de zéro**.*

Exemple 1.6. *L'anneau $\mathbb{Z}$ est intègre car $\forall x \; et \; y \in \mathbb{Z}$, $xy = 0 \Longrightarrow (x = 0 \; ou \; y = 0)$. Par contre l'anneau $\mathbb{Z}/8\mathbb{Z}$ n'est pas intègre car $\bar{2} \neq \bar{0}$ et $\bar{4} \neq \bar{0}$ mais $\bar{2}.\bar{4} = \bar{8} = \bar{0}$.*

Remarque 1.6. *On remarque qu'un anneau intègre ne possède pas de diviseur de zéro.*

Théorème 1.2. *Soit A un anneau et I un idéal de A*
I est maximal si at seulement si A/I est un corps

Preuve : Comme A est unitaire on a A/I l'est aussi soit donc $a+I \in A/I$ tel que $a+I \neq I$ ainsi $a \notin I$ d'où $I \subset (a)+I$ avec $I \neq (a)+I$ ce qui conduit à $a+I=A$ car I idéal maximal ; de plus comme A est unitaire $\exists a' \in A \ et \ i \in I$ tels que $1 = a'a + i$ ce qui entraine que $1 - a'a \in I$ ce qui veut dire que $a'a + I = 1 + I$ ce qui signifie que $(a' + I)(a + I) = 1 + I$ donc $a + I$ est inversible et par suite A/I est un corps.
Réciproquement supposons que A/I est un corps alors $I \neq A$ car sinon on aurait $A/I = \{I\}$ serait un corps absurde il n'admet aucun élément non nul. Soit donc J un idéal de A contenant strictement I et soit $j \in J$ tel que $j \notin I$. comme A/I est un corps, il $x \notin I$ tel que $jx+I = 1+I$ il suit que $1 + jx \in I \subset J \ xj \in J$ car$J$ idéal et par suite $1 \in J$ d'où $J = A$ et I idéal maximal.
■

Définition 1.23. *On dit qu'un anneau A est un anneau principal si :*

- *A est commutatif intègre ;*
- *tout idéal de A est engendré par un élément.*

Théorème 1.3. *Soit A un anneau commutatif et I un idéal de A ;*
I est premier si et seulement si A/I est un domaine intègre.

Preuve : Supposons que I est un idéal premier de l'anneau A comme A est commutatif il suit que A/I l'est aussi.Soit $a + I$ et $b + I$ deux éléments de non nuls de A/I tels que $(a + I)(b + I) = I$ c'est-à-dire $ab + I = I$ alors $ab \in I$.
Or I est un idéal premier d'où $a \in I$ ou $b \in I$ ce qui conduit à $a + I = I$ ou $b + I = I$ .Il en résulte que A/I est un domaine d'intégrité.
Réciproquement si A/I est un domaine d'intégrité non trivial alors I est un idéal propre de A.
Soit a et b deux éléments de A tels que $ab \in I$ alors $ab+I = I$ or A/I est un domaine d'intégrité d'où $a + I = I$ ou $b + I = I$ donc $a \in I$ ou $b \in I$ il suit que I est premier . ■

Proposition 1.3. *Soit A un anneaux , alors les propriétés suivantes sont équivalentes :*

1) *Tout idéal de A est engendré par un nombre fini d'éléments.*
2) *Toute suite croissante d'idéaux (pour l'inclusion) est stationnaire.*
3) *Toute famille non vide d'idéaux de A admet un élément maximal.*

Preuve : montrons que $1) \Rightarrow 2)$.

Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante alors $I = \cup_{n\in\mathbb{N}} I_n$ est un idéal et selon $1)$ $\exists x_1, ..., x_n$ tels que $I = (x_1, ..., x_n)$; chaque x_i est dans l'un des I_n .

Soit n_0 le plus grand indice tel que tous les x_i appartiennent à I_{n_0} , alors pour tout $n \geq n_0$ on a : $I_{n_0} = I_n = I$.

Montrons ensuite que $2) \Rightarrow 3)$.

faisons le par contra-posée . Soit une famille Δ non vide d'idéaux de A qui n'admet pas d'élément maximal.

Donc $\exists I_1 \in \Delta$ et comme Δ n'a pas d'idéal maximal, $\exists I_2$ tel que $I_1 \subset I_2$

et ainsi de suite on aura une famille croissante (au sens de l'inclusion) ne saurait être stationnaire d'où le résultat.

Montrons $3) \Rightarrow 1)$

Soit I un idéal de A posons :

$E = \{J : J\ est\ de\ type\ fini\ et\ J \subset I\}$, $E \neq \emptyset$ car $\{0\} \in E$ soit J_0 l'élément maximal.

Si $J_0 \neq I$,$\exists x \in I - J_0$ et on aura $J_0 + (x)$ contient J_0

or $J_0 + (x)$ est de type fini , ce qui contredit la maximalité de J_0 ;

donc $J_0 = I$. Ce qui entraine que tout idéal de A est de type fini.ce qui achève la preuve. ■

Définition 1.24. *Un anneau A est dit noethérien s'il vérifie l'une des trois propriétés énoncées dans la* ***proposition 1.3****.*

Définition 1.25. *Soit A un anneau on dit qu'il est factoriel s'il vérifie les propriétés suivantes :*

(O) A est intègre ;

(E) Tout élément non nul x de A s'écrit sous la forme : $x = u\prod_{p\in\mathcal{P}} \mathrm{p}^{\mathrm{v_p(x)}}$, avec $\mathcal{P}$ un système de représentants d'irréductibles ,$u \in U_A$ et $v_p(x)$ la valuation p-adique de x.

1.2.2 Anneaux des polynômes. [1]

Introduction

Nous venons de donner une définition générale de la notion d'anneaux . Intéressons nous à une famille particulière d'anneaux . Nous nous limiterons ici aux anneaux des polynômes à une indéterminée.

Définition 1.26. *L'ensemble des polynômes à une indéterminée et à coefficients dans un anneau quelconque A noté $A[X]$ devient aussi anneau lorsqu'on le muni des deux lois suivantes ;*

pour toute paire de polynômes $P(X)$ et $Q(X)$ dans $A[X]$ de degrés respectifs m et n tels que :
$P(X) = \sum_{i=0}^{m} a_i X^i$ *et* $Q(X) = \sum_{i=0}^{n} b_i X^i$ *;*
1) $P(X) + Q(X) = \sum_{i=0}^{max(m,n)} (a_i + b_i) X^i$ *;*
2) $P(X)Q(X) = (\sum_{i=0}^{m} a_i X^i)(\sum_{j=0}^{n} b_j X^j) = \sum_{l=0}^{m+n} (\sum_{i+j=l} a_i b_j) X^l$

Proposition 1.4. *Soient $P(X)$ et $Q(X)$ de degrés respectifs m et n on a toujours :*

- *le degré de $P(X)Q(X)$ au moins égal à mn.*
- *de plus si l'anneau A est intègre alors il y'a égalité et par suite $A[X]$ est aussi intègre.*

Preuve : Soit $P(X) \in A[X]$, posons $deg(P)$ son degré.

L'inégalité $deg(PQ) \leq m + n$ résulte du **2)** de la **définition1.13**.

Supposons que A est intègre ;

comme $deg(P) = m$ et $deg(Q) = n$ alors $a_m \neq 0$ et $b_n \neq 0$

alors $a_m b_n \neq 0$ et est le coefficient de X^{m+n}, ce qui entraine que $deg(PQ) = m + m$.

De plus si $P(X)$ et $Q(X)$ sont tous non nuls alors $a_m \neq 0$ $et; b_n \neq 0$ d'où $P(x)Q(X) \neq 0$ et par conséquent $A[X]$ est intègre. ■

Le théorème suivant est connu sous le nom de

transfert de HILBERT.

Théorème 1.4. *Soit A un anneau :*

Si A est noethérien alors $A[X]$ l'est aussi.

Définition 1.27. *Soient A un anneau factoriel et $A[X]$ son anneau de polynôme associé . Soit P un élément de $A[X]$.*

*On appel **contenu** de P et note $C(P)$ le pgcd de ses coefficients .*

*On dira qu'un polynôme est **primitif** si son contenu est un élément inversible de A.*

Lemme 1.1. *(Gauss) Considérons l'anneau $A[X]$; soient P et $Q \in A[X]$;on a $c(PQ) = c(P)c(Q)$.*

Preuve :

Supposons d'abord que P et Q sont primitifs. Dans ce cas il est immédiat que PQ l'est aussi car sinon on aura un élément irréductible p qui divise tous les coefficients de PQ ;

or comme P et Q sont primitifs ,il va exister au moins un coefficient a_{i_0} de P et b_{j_0} un coefficient de Q tels que.

$$p \nmid a_{i_0}$$

et

$$p \nmid b_{j_0}.$$

Le coefficient d'indice $i_0 + j_0$ de PQ est somme des termes divisibles par p et de $a_{i_0}b_{j_0}$ donc n'est pas divisible par p car l'idéal engendré par p est premier ce qui contredit l'hypothèse selon laquelle tous les coefficients de PQ sont divisibles par p.
Dans le cas général si on a deux polynômes P et Q on peut obtenir deux polynômes Q_1 et P_1 primitifs en faisant :

$$P_1 = \frac{P}{c(P)}$$

et

$$Q_1 = \frac{Q}{c(Q)}.$$

Par suite selon ce qu'on a fait au premier cas P_1Q_1 est primitif,ce qui achève la preuve. ■

Critères d'irréductibilité d'un polynôme.[1]

Soit l'anneau des polynômes à une indéterminée $A[x]$; il existe différents critères d'irréductibilité. Nous en donnerons un.

Théorème 1.5. *(critère d'Einsentein) Soient A un anneau factoriel , P un polynôme non constant c'est-à-dire $P \in A[x] - A$, p irréductible dans A*
on pose $P = \sum_{k=0}^{n} a_k x^k$ est irréductible dans $K[X]$ où K est le corps de fractions de A Si :

1) p ne divise pas a_n ;

2) p divise les a_k pour $0 \leq k \leq n-1$;

3) p^2 ne divise pas a_0.

Si de plus P est primitif alors il est irréductible dans $A[X]$.

Proposition 1.5. *Soit A un anneau commutatif et B un anneau contenant A ; on dira alors que B est un sur-anneau de A ou une extension de A .*
Il clair qu'on puisse bâtir sur B une structure de A-module .

Définition 1.28. *Soient B une extension d'un anneau A et α un élément de B ; on dira que*

- α *est* ***algébrique*** *sur* A *s'il existe* $P \in A[X]$ *non constant tel que* $P(\alpha) = 0$.
- α *est* ***transcendant*** *sur* A *s'il n'est pas algébrique sur* A.

1.3 Modules

1.3.1 Introduction

La notion de module vient généraliser celle d'espace vectoriel.

1.3.2 Généralités sur les modules

Définition 1.29. *Soit* A *un anneau commutatif; Un* A*-module est un groupe abélien* M *muni d'une application :*

$$\begin{aligned} A \times M &\longrightarrow M \\ (a, m) &\mapsto am, \end{aligned}$$

vérifiant les trois propriétés suivantes :

$\forall m, m' \in M$ *et* $\forall a, b \in A$ *:*

- $a(m + m') = am + amet(a + b)m = am + bm$
- $a(bm) = (ab)m$
- $1_A m = m$

Définition 1.30. *Un sous ensemble* N *de* M *est un sous-*A*-module si :*

1) N *est un sous-groupe de* M *;*

2) $\forall (a, n) \in A \times N$ *,*$an \in N$.

Exemple 1.7. *1) Un anneau* A *est un* A*-module . En effet dans la définition de l'anneau la deuxième loi de composition interne vérifie les trois propriétés de la* ***définition 2.1*** *.Il en va de même pour un idéal de* A.

2) Un groupe abélien G *est un* $\mathbb{Z}$*-module. Soit* $n \in \mathbb{Z}$*,*$x \in G$ *on pose :*

$nx = x + x + ... + x$*(n fois) si* $n > 0$ *;*

$(-n)x = (-x) + (-x) + ... + (-x)$ *si* $n < 0$

et si $n = 0$ $nx = 0x = 0_G$ *de plus* $0_{\mathbb{Z}}x = 0_G$.

L'application $\mathbb{Z} \times G \to G$ *définie par :*$(n, x) \mapsto nx$ *vérifie aisément les trois propriétés de la* ***définition 2.1*** *.*

Définition 1.31. *Soient $MetN$ deux A-modules ,une application f de M dans N est un morphisme de A-modules si :*

1. *f est un morphisme de groupes.*
2. *f vérifie :$\forall(a,x) \in A \times M$, $f(ax) = af(x)$.*

Proposition 1.6. *Soit M un A-module et S une partie de M ;l'ensemble des $m \in M$ tels que $m = \sum_{i=1}^{n} a_i s_i$ où les $s_i \in S$ et les $a_i \in A$ est le sous-A-module engendré par S.*
Il est noté (S) ; c'est le plus petit module contenant les éléments de S.
Si S est une partie finie c'est-à-dire $S = \{s_1, ..., s_n\}$,alors (S) est dit de type fini et on note :
$(S) = As_1 + ... + As_n$.
Si $(S) = M$ alors la partie S sera dite génératrice .

Définition 1.32. *Soit M un A-module et soit B une partie de M .On dit que B est une partie libre de M si les éléments de B sont linéairement indépendants c'est-à-dire si la proposition suivante est vérifiée :*
Pour $n > 1$ si $\sum_{i=1}^{n} \lambda_i s_i = 0 \Rightarrow \lambda_i = 0, s_i \in B$, $\forall i \in \{1, ..., n\}$

1.3.3 Modules libres

Définition 1.33. *Soit M un A-module et B une partie de M ; B est une base de M si les deux propriétés suivantes sont vérifiées :*

1. *B est une partie génératrice de M ou B engendre M.*
2. *B est une partie libre de B.*

Ce qui entraine que tout $m \neq 0 \in M$ s'écrit comme suit :
$m = \sum_{i=1}^{n} a_i b_i$ avec $a_i \in A$ et $b_i \in B$ $\forall i \in \{1, ..., n\}$.
On dit que M est un module libre si M possède une base.

Exemple 1.8.

1. *Un anneaux A est un A-module libre de base $B = \{1_A\}$.*
2. *pour n>1 on a $A^n = \{(a_1, ..., a_n) : a_{i \in A}\}$ est un A-module libre de base $B = \{e_i : 1 \leq i \leq n\}$ où $e_1 = (1, ..., 0)$,...,$e_n = (0, ..., 1)$.*
   En effet tout module libre de base à n éléments est isomorphe à A^n.

Remarque 1.7. *À la suite de cette définition, une question survient .Toutes les bases d'un module libre M ont-elles le même nombre d'éléments ? la réponse est non sauf s'il s'agit d'un module sur un anneau commutatif ou noethérien et dans ce cas ce nombre est appelé le* ***rang*** *de M.*

Proposition 1.7. *Soient A un anneau principal et M un A-module ;M est un module libre de rang fini n si et seulement si :*

⋆ *il existe une famille finie $(M_i)_i$ à n éléments telle que :*

$M_0 = \{0\} \subset M_1 \subset ... \subset M_n = M$ *avec* $M_{i+1}/M_i \simeq A$ *pour* $1 \leq i \leq n-1$

Preuve : Supposons que M est libre alors il existe une base $B = \{e_i \ ; 1 \leq i \leq n\}$ alors prendre $M_i = Ae_1 \oplus ... \oplus Ae_i$, pour $1 \leq i \leq n$, car avec cette construction, $M_0 = \{0\}$ et en définissant , θ_i de A_{i+1}/A_i vers A pour $1 \leq i \leq n-1$ définie par :$\theta_i(a + A_i) = a_{i+1}$ on a bien les θ_i qui sont des isomorphismes.
Réciproquement supposons que M vérifie les propriétés précédentes, on a les : M_{i+1}/M_i qui sont des A-modules libres de rang 1.on aura donc pour $1 \leq i \leq n-1$, $M_{i+1}/M_i = A\bar{e}_{i+1}$ on a alors :

$$M_{i+1} = Ae_{i+1} \oplus M_i;$$

en effet si $x \in M_{i+1}$ $\bar{x}$=$\lambda\bar{e}_{i+1}$ de sorte qu'on ait : $x = \lambda e_{i+1} + y$ avec $y \in M_i$ d'où ; $M_{i+1} = e_{i+1} \oplus M_i$ de plus si $x \in M_i \cap Ae_{i+1}$ ce qui entraine que $\lambda e_{i+1} \in M_i$ et par suite $\bar{x} = M_i = \bar{0}$ et en itérant cette construction sur i on a bien M qui est un A-module libre. donc l'une des bases est $(e_i)_i$,$1 \leq i \leq n$. ■

Proposition 1.8. *Soient A un anneau principal et M un A-module libre de rang n ; tout sous-module M' de M est libre et de rang $m \leq n$.*

Preuve : Comme M est libre par hypothèse, considérons une famille $(M_i)_i$ avec $0 \leq i \leq n$ telle que :
$M_0 = \{0\} \subset M_1 \subset ... \subset M_n = M$ avec $M_{i+1}/M_i \simeq A$ pour $1 \leq i \leq n-1$,posons $M'_i = M_i \cap M'$, et soit donc $m \leq n$ le plus petit entier tel que $M_m \cap M' = M'$ on a donc $M'_0 = \{0\} \subset M'_1 \subset ... \subset M'_m = M'$;de plus le morphisme canonique entre M'_{i+1}/M'_i et M_{i+1}/M_i est injectif donc d'image un idéal de A donc M'_{i+1}/M'_i est isomorphe à A et par suite M' est libre de rang m. ■

Chapitre 2

ANNEAUX DE GALOIS

Introduction

Nous allons présenter dans ce chapitre la notion d'anneau de Galois en donnant quelques définitions et propriétés.

2.1 Généralités

2.1.1 Définitions et propriétés préliminaires

Définition 2.1. *[2] Soit A un anneau fini commutatif unitaire non intègre. On dira que A est un anneau de Galois si :*

- *A est un anneau local*
- *A a pour caractéristique p^n avec p un nombre premier et $n \in \mathbb{N}$ tel que $n \geq 2$*

Son corps résiduel est un corps de Galois.

Proposition 2.1. *Soit A un anneau de Galois son unique idéal maximal est son nilradical. Il correspond à l'ensemble D de ses diviseurs de zéro.*

Exemple 2.1. *Les anneaux $\mathbb{Z}/p^n\mathbb{Z}$ avec p premier et n un entier au moins égale à 2 sont un exemple d'anneaux de Galois.*
En effet ils sont commutatifs unitaires et les diviseurs de zéro de ce type d'anneaux sont les éléments de la forme px avec $x \in \mathbb{Z}/p^n\mathbb{Z}$ c'est-à-dire $D = p\mathbb{Z}/p^n\mathbb{Z}$.
nous avons montré dans le chapitre précédent que D ainsi défini est l'unique idéal maximal de $\mathbb{Z}/p^n\mathbb{Z}$.

Propriété 2.1. *Soit A un anneau de Galois de caractéristique p^n avec p un nombre premier et $n \in \mathbb{N}$ tel que $n \geq 2$, alors A contient un sous-anneau isomorphe à $\mathbb{Z}/p^n\mathbb{Z}$*

Preuve :

Soit l'application θ de $\mathbb{Z}$ dans A définie par : $\theta(n) = n1_A$. θ ainsi définie est un morphisme d'anneaux et $ker(\theta) = p^n\mathbb{Z}$ d'où $\mathbb{Z}/p^n\mathbb{Z} \simeq Im(\theta) \subset A$ ■

Proposition 2.2. *Soit A un anneau de Galois de caractéristique p^n et M son idéal maximal . On sait que $M = D = pA$ où D est l'ensemble de ses diviseurs de zéro.*
L'anneau quotient A/D est un corps car D est un idéal maximal. A/D ainsi donné est le corps résiduel de A et $|A/D| = q = p^r$ on notera cet anneau par $GR(p^n, r)$. Considérons la famille $D^i = p^iA$ pour $0 \leq i \leq n-1$ alors on obtient la chaine ci-après :

$$A = D^0 \supset D = pR \supset ... \supset D^{n-1} \supset D^n = \{0\}$$

et par suite $|A| = q^n$

Preuve : Il est clair que les D^k/D^{k+1} pour $0 \leq i \leq n-1$ sont isomorphes à A/D de plus la chaine ci- dessus donnée entraine que A est un sous-module libre de rang n sur l'anneau A/D d'où $|A| = q^n$ ■

Corollaire 2.1. *Les anneaux de Galois sont des $\mathbb{Z}/p^n\mathbb{Z}$-modules libres à un isomorphisme prês.*

2.1.2 Extension d'un anneau de Galois

Définition 2.2. *[2] Soient A un anneau de Galois de caractéristique p^n et R son corps des classes résiduelles .Soient de plus $R = A/pA$ et π l'épimorphisme canonique de A sur $R = A/pA$.*
*On peut donc prolonger cet épimorphisme en un épimorphisme d'anneaux des polynômes de $A[X]$ sur $R[X] \simeq A[X]/pA[X]$ qui à un polynôme $P(X) = \sum_i a_i x^i$ associe $\bar{P}(X) = \sum_i \bar{a}_i x^i$. Un polynôme $P(X)$ de $A[X]$ est dit **b-polynôme** s'il est unitaire tel que $\bar{P}(X)$ irréductible dans $R[X]$.*

Proposition 2.3. *Les b-polynômes sur les anneaux de Galois permettent de construire des extensions d'anneaux de Galois qui sont des anneaux de Galois plus grands.*
En effet soient A un anneau de Galois et $P[X]$ un b-polynôme admettant une racine α.
*En adjoignant α à A on obtient un anneau de Galois plus grand,il s'agit alors de la **G-extension** $A[X]/(P[X])$*

Théorème et définition 2.1. *Soient A un anneau de Galois de caractéristique p^n de q^n éléments et $P[X]$ un b-polynôme sur A de degré m, alors la G-extension*

$$S = A[X]/(P(X))$$

est un anneau de Galois de caractéristique p^n et de q^{nm} éléments. S est appelé G-extension de A.

Preuve : Il existe une une inclusion entre A et S donc S a la même caractéristique p^n que A et de plus l'anneau S peut être vu comme une extension de degré m sur A d'où $|S| = q^{nm}$.
Par suite, il est immédiat que les éléments de pS sont les diviseurs de zéro de A ; il reste donc à montrer que $\forall \alpha \in S - pS\ ,\ \alpha$ est irréductible.
Soit $\alpha \in S - pS$, on a :$\alpha = [T(X)]_P = T(X) + (P(X))$ avec $T(X) \in A[X]$ tel que $deg(T(X)) < m$ et $\bar{T}(X) \neq 0$ nous avons alors : $pgcd(\bar{P}(X), \bar{T}(X)) = \bar{1}$ et d'après Bezout il existe $U(X)$ et $V(X)$ deux polynômes de $A[X]$ qui vérifie l'égalité :

$$\bar{U}(X)\bar{T}(X) + \bar{V}(X)\bar{P}(X) = \bar{1}$$

ce qui veux dire qu'il existe $B(X) \in A[X]$ tel que

$$U(X)T(X) + V(X)P(X) = 1 + pB(X)$$

ainsi on a :

$$[U(X)]_P[T(X)]_P = [1 + pB(X)]$$

et $[1 + pB(X)]$ est inversible car

$$[1 + pB(X)]_P^{p^{n-1}} = [1]_P$$

D'où α est inversible . Ainsi par le résultat précédent nous avons les deux propriétés suivantes concernant l'existence d'un anneau de Galois. ■

Lemme 2.1. *Pour tout anneau de Galois A et pour tout entier naturel m il existe une G-extension S de degré m de A.*

Lemme 2.2. *Pour tout nombre premier p ,n et m deux entiers naturels ,il existe un anneau de Galois R de caractéristique p^n et p^{nm} éléments.*

Exemple 2.2. *$A = \mathbb{Z}/8\mathbb{Z}$ est un anneau de Galois de caractéristique $8 = 2^3$ et d'idéal maximal $D = 2A$.*
posons $P(X) = X^3 + 6X^2 + 5X + 7$, $P(X)$ est un b-polynôme car $\bar{P}(X) = X^3 + X + 1$ est irréductible dans $A[X]/2A[X]$.Ainsi

$$S = A[X]/(P(X))$$

est une G-extension de A de degré 3 de même caractéristique que A de $2^{3.3}$ éléments.

De manière générale si on a S une G-extension de A et $\alpha \in S$, alors l'anneau $A[\alpha]$ défini par :

$$A[\alpha] = \{P(\alpha) \ : \ P(X) \in A[X]\}$$

est une extension de A.
Dans l'exemple précédent on aura :

$$S = A[\alpha]$$

avec α une racine de $P(X)$ d'où S est le module engendré par $\{1, \alpha, \alpha^2\}$.

Théorème 2.1. *Soit S une G-extension de degré m de l'anneau de Galois A,$P(X)$ un b-polynôme de degré k .Alors*

- *Le polynôme $P(X)$ admet une racine dans S si et seulement si k divise m.*
- *Si k divise m alors le polynôme $P(X)$ possède exactement k racines distinctes $\alpha_1, ..., \alpha_k$dans S modulo l'idéal pS et $P(X) = (X - \alpha_1)...(X - \alpha_k)$.*
- *Pour tout élément α on a, $S = A[\alpha]$ si et seulement si α est une racine du b-polynôme $P(X)$.*

Ce théorème entraine un corollaire très important.

Corollaire 2.2. *Soit S un anneau de Galois de caractéristique p^n et de cardinal p^{nm} où p est un entier premier et $n, m \in \mathbb{N}$;on a :*

$$S \simeq \mathbb{Z}_{p^n}[X]/(P(X))$$

avec $P(X)$ un b-polynôme d'ordre m dans $\mathbb{Z}_{p^n}[X]$,un tel anneau sera noté $GR(p^n, m)$.Ce qui conduit à dire que deux anneaux de Galois ayant la même caractéristique et le même nombre d'éléments sont isomorphes.

Corollaire 2.3. *Soit a un entier naturel impaire , le polynôme $X^a - 1$ admet une factorisation unique dans S.*

Ce corollaire est une conséquence du lemme suivant.

Lemme 2.3. *Soient $P(X) \in A[X]$ et α tels que $\bar{P}(\alpha) = \bar{0}$ et $\bar{P}'(\alpha) \neq \bar{0}$ alors il existe une unique racine β de $P(X)$ dans S telle que $\bar{\beta} = \bar{\alpha}$.*

Proposition 2.4. *[2] Soit $G(p^k, m)$ un anneau de Galois , un élément α de $G(p^k, m)$ peut s'écrire de manière unique sous deux formes.*

Représentation additive :

$$\alpha = \sum_{i=0}^{m-1} \lambda_i x^i;$$

avec les λ_i les éléments de $\mathbb{Z}_{p^k}$.

Représentation multiplicative :

$$\alpha = \sum_{i=0}^{k-1} \alpha_j p^j;$$

avec les α_j les éléments de $\mathcal{T}$ et $\mathcal{T} = \{0\} \cup \mathcal{T}^*$ est appelé ensemble de Teichmuller.

Preuve : La représentation additive du fait qu'un anneau de Galois est un $\mathbb{Z}_{p^k}$-module grâce à son structure d'anneau quotient .

L'existence et l'unicité de l'écriture multiplicative découlent de l'algorithme que nous détaillerons ci-dessous.

Il n'est pas aisé de représenter tout $\alpha \in GR(p^k, m)$ multiplicativement car l'addition de deux représentations multiplicatives ne donne pas toujours une représentation multiplicative.Il faut donc faire recours à une conversion.Ce changement permet de donner la forme additive des éléments de l'ensemble de Teichmuller, On obtient de façon itérative :

Supposons x^j décomposé de façon additive par $x^{j-1} = \sum_{i=0}^{m-1} a_{j-1,i} x^i$, pour $j > m$

$$\begin{aligned} x^j &= x^{j-1}x, \\ &= a_{j-1,o}x + a_{j-1,1}x^2 + ... + a_{j-1,m-1}x^m \\ &= a_{j-1,m-1}a_{m,0} + \sum_{i=1}^{m-1}(a_{j-1,m-1}a_{m,i} + a_{j-1,i})x^i. \end{aligned}$$

(la forme additive de x^m et des puissances inférieures de x étant donnée par le b-polynôme avec lequel on construit cet anneau de Galois). On pourra donc passer plus aisément de l'écriture

multiplicative à celle additive.

En effet pour $\alpha = \sum_{j=0}^{k-1} \alpha_j p^j$ il suffit de remplacer pour tout $0 \leq j \leq k-1$ α_j par sa représentation additive donnée dans la table précédente. Pour $0 \leq j \leq k-1$ posons : $\alpha_j = \sum_{i=0}^{m-1} u_{j,i} x^i$,on aura

$$\begin{aligned} \alpha &= \sum_{j=0}^{k-1} \alpha_j p^j \\ &= \sum_{j=0}^{k-1} (\sum_{i=0}^{m-1} u_{j,i} x^i) p^j \\ &= \sum_{i=0}^{m-1} (\sum_{j=0}^{k-1} p^j u_{j,i}) x^i \end{aligned}$$

Le retour à la forme multiplicative se fait de la manière suivant :

Désignons tout d'abord par π l'épimorphisme de $GR(p^k, m)$ dans GF_{p^m} définie par :$\pi(\alpha) = \alpha + (p)$

Nous énumérons alors deux cas :

cas 1 $\pi(\alpha) = (p)$ ce qui veut dire que $\alpha \in (p)$ et donc $\exists \alpha' \in GR(p^k, m)$ tel que $\alpha = p\alpha'$

cas 2 $\pi(\alpha)$ est non nul. Dans ce cas $\pi(x)$ étant un élément primitif de $GF(p^m)$,alors il existe un unique entier k ,$0 \leq k \leq p^{m-2}$ tel que $\pi(\alpha) = \pi(x)^k$ d'où $(\alpha - x^k) \in \ker(\pi)$ c'est-à-dire $\alpha - x^k \in (p)$ car π est un morphisme d'anneaux.ce qui entraine que α se met sous la forme $x^k + p\alpha'$

Dans les deux cas ci-dessus mentionnés,on peut écrire $\alpha = \alpha_0 + p\alpha'$ avec $\alpha_0 \in \mathcal{T}$ et $\alpha' \in GR(p^k, m)$.α' étant dans $GR(p^k, m)$ on aura $\alpha' = \alpha_1 + p\alpha''$ et en itérant m fois on obtient une écriture multiplicative. ■

Exemple 2.3. *Considérons l'anneau* $GR(2^3, 3) = \mathbb{Z}_{2^3}[X]/(X^3 + 6X^2 + 5X + 7)$ *posons* $\alpha = 5 + 3x^2$ *et* $\beta = x$ *avec biensûr* $x = X + (X^3 + 6X^2 + 5X + 7)$.*Nous allons donner les représentations additives et multiplicatives de* α *et* β *et calculer* $\beta + \alpha$ *et* $\alpha\beta$ *On a les tables suivantes :*

$x = x$

$x^2 = x^2$

$x^3 = -6x^2 - 5x - 7 = 2x^2 + 3x + 1$

$x^4 = xx^3 = 2x^3 + 3x^2 + x = 7x^2 + 7x + 2$

$x^5 = 7x^3 + 7x^2 + 2x = 5x^2 + 7x + 7$

$$x^6 = 5x^3 + 7x^2 + 7x = x^2 + 6x + 5$$

$$x^7 = x^3 + 6x^2 + 5x = 1.$$

L'application π modulo l'idéal (2) nous donne :

$$\pi(x) = x$$

$$\pi(x^2) = \pi(x^2)$$

$$\pi(x^3) = \pi(x) + 1$$

$$\pi(x^4) = \pi(x^2) + \pi(x)$$

$$\pi(x^5) = \pi(x^2) + \pi(x) + 1$$

$$\pi(x^6) = \pi(x^2) + 1$$

$$\pi(x^7) = 1$$

On obtient donc :

- *En représentation additive :*
  $\alpha = 5 + x^2$ *,* $\beta = x$ *et* $\alpha\beta = (5 + 3x^2)x = 5x + 3x^3$ *ce qui conduit à* $\alpha\beta = 6x^2 + 6x + 3$ *de même* $\alpha + \beta = (5 + 3x^2) + x = 3x^2 + x + 5$
- *En représentation multiplicative* $\pi(\alpha) = 1 + \pi(x^2)$ *et grâce à la seconde table on a :* $\pi(\alpha) = \pi(x^6)$ *et en évaluant* $\alpha - x^6$ *on obtient :*

$$\begin{aligned} \alpha - x^6 &= 5 + 3x^2 - (5 + 6x + x^2) \\ &= 2x + 2x^2 \\ &= 2(x + x^2); \end{aligned}$$

d'où

$$\alpha = x^6 + 2(x + x^2).$$

En itérant avec $\alpha' = x + x^2$ *on a finalement :*

$$\alpha = x^6 + 2(x^4 + 2x^5)$$

L'élément β étant déjà à la fois sous forme multiplicative et sous forme additive , on a plus besoin de faire des conversions.La somme $\alpha + \beta$ se fait en utilisant les formes additives puis en passant à la forme multiplicative comme dans le cas de α

$$\begin{aligned} \alpha + \beta &= (x^6 + 2x^4 + 4x^2) + (x) \\ &= 5 + 3x^2 + x \end{aligned}$$

et en conversion multiplicative ;

$$\alpha + \beta = x^5 + 2x^5 + 4x^4.$$

Il est plus aisé de calculer $\alpha\beta$ car le produit de deux formes multiplicatives donne une forme multiplicative.
Ainsi on a :

$$\begin{aligned} \alpha\beta &= (x^6 + 2x^4 + 4x^5)(x) \\ &= 1 + 2x^5 + 4x^6 \end{aligned}$$

2.1.3 Relèvement de Hensel [2]

Lemme 2.4. *(Lemme de Hensel) Soit p un nombre premier, k un entier supérieur ou égal à 2 et $P \in \mathbb{Z}_{p^k}[X]$ un polynôme unitaire tel que :*

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

avec Q et $R \in \mathbb{Z}_p[X]$ deux polynômes unitaires premiers entre eux alors, il existe un unique couple $(Q^{(k)}, P^{(k)})$ de polynômes unitaires de $\mathbb{Z}_{p^k}[X]$ tels que

- $P = Q^{(k)}R^{(k)}$
- $Q^{(k)} \equiv Q\ mod(p)$ *et* $P^{(k)} \equiv P\ mod(p)$
- $P^{(k)}$ *et* $Q^{(k)}$ *sont premiers entre eux.*

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

L'anneau $\mathbb{Z}_p[X]$ est un anneau principal donc factoriel et par conséquent tout tout polynôme de $\mathbb{Z}_p[X]$ s'écrit de façon unique à permutation près en produit d'irréductibles .
On a donc pour tout $P \in \mathbb{Z}_{p^k}[X]$ on a :

$$P \equiv f_1^{e_1}...f_r^{e_r}\ mod(p)$$

où $f_1, ..., f_r$ sont des polynômes irréductibles de $\mathbb{Z}_p[X]$ et $e_1, ..., e_r$ sont des entiers strictement positifs.
avec le lemme précédent et par induction on obtient le nombre de facteurs de P dans $\mathbb{Z}_{p^k}$.

Théorème 2.2. *(Relèvement de Hensel) Soit p un nombre premier et k un entier supérieur ou égal à 2 et $P \in \mathbb{Z}_{p^k}[X]$ un polynôme unitaire . Il existe un unique r-uplet $(P_1^{(k)}, ..., P_r^{(k)})$ de polynômes unitaires de $\mathbb{Z}_{p^k}[X]$ tels que :*

- $P = P_1^{(k)}...P_r^{(k)}$
- $P_i^{(k)} \equiv f_i^{e_i} mod(p)$ *pour* $1 \leq i \leq r$
- *les* $P_i^{(k)}$ *sont premiers entre eux.*

Ce qui veut dire les polynômes unitaires de $\mathbb{Z}_{p^k}[X]$ se décomposent en des g_i^k des polynômes qui réduits modulo p sont des puissances de polynômes irréductibles .
Cette propriété va nous permettre de définir le relevé de Hensel d'un facteur de $X^n - 1$ avec n et p premiers entre eux.En effet dans ce cas $X^n - 1$ ne possède que de facteurs simples.

Définition 2.3. *(Relevé de Hensel) Soient* n *un entier naturel premier avec* p *et deux polynômes* P *et* $Q \in \mathbb{Z}_p[X]$ *tels que* $X^n - 1 = PQ$ *. On appelle relevé de Hensel d'ordre* k *de* Q *, le polynôme* Q^k *du couple* $(P^{(k)}, Q^{(k)})$*.*

Proposition 2.5. *Soit* $Q \in \mathbb{Z}_p[X]$ *un facteur de* $X^n - 1$ *, son relevé de Hensel d'ordre* k *divise* $X^n - 1$ *dans* $\mathbb{Z}_{p^k}[X]$

Remarque 2.1. *Lorsque* Q *est irréductible et primitif , les relevés de Hensel de* Q *sont des b-polynômes.*

Étudions le cas binaire où $p = 2$

Proposition 2.6. *(calcul du relevé de Hensel binaire) Soient* $Q \in \mathbb{Z}_2[X]$ *un facteur de* $X^{2^n-1}-1$ *et* $Q^{(k)} \in \mathbb{Z}_{2^k}[X]$ *son relevé de Hensel d'ordre* k *.*
Posons $Q^{(k)}(X) = P(x) - I(X)$ *tel que* P *et* I *contiennent respectivement les monômes de degrés pairs et ceux de degrés impairs.On a alors* $Q^{(k+1)}(X^2) = \pm(P^2(X) - I^2(X))$ *, les opérations étant faites dans* $\mathbb{Z}_{2^{k+1}}[X]$ *et le signe choisi pour que* $Q^{(k+1)}$ *soit unitaire.*

Preuve : Soit $f(X) \in \mathbb{Z}_{2^{k+1}}[X]$ le polynôme unitaire tel que $f(X) = \pm(P^2(X) - I^2(X))$ et f ainsi construit dans $Z_{2^{k+1}}[X]$ est bien définie.On a

$$f(X^2) \equiv P(X^2) - I(X^2) \equiv Q(X^2) mod(2)$$

or l'application $R(X) \mapsto R(X^2)$ se réduit à $R(X) \mapsto R^2(X)$ d'où $f(X) \equiv Q(X) mod(2)$
Il reste donc à vérifier que f divise $X^{2^{n-1}-1}$ dans $Z_{2^{k+1}}[X]$ .Or

$$f(X^2) = \pm Q^{(k)}(X)Q^{(k)}(-X)$$

, les opérations étant faites dans $Z_{2^{k+1}}[X]$.
Par hypothèse on a $Q^{(k)}(X)$ divise $X^{2^n-1} - 1$ dans $Z_{2^k}[X]$, on peut donc écrire

$$X^{2^n-1} - 1 = Q^{(k)}(X)A(X) + 2^k B(X)$$

avec $A(X)$ et $B(X)$ des éléments de $Z_{2^{k+1}}[X]$ et

$$(-X)^{2^n-1} - 1 = Q^{(k)}(-X)A(-X) + 2^k B(-X)$$

. Ainsi

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

Posons $Q^{(k)}(X) = P(X) - I(X)$,$A(X) = P_a(X) + I_a(X)$ et $B(X) = P_b(X) + I_b(X)$ où ,$P(X)$,$P_a(X)$,$P_b(X)$ ne contiennent que les monômes de degrés pairs des polynômes $Q^{(k)}(X)$, $A(X)$ $B(X)$ et $I(X)$,$I_a(X)$,$I_b(X)$ ceux de degré impairs.On a ainsi

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

Il en résulte que $f(X^2)$ divise $x^{2^{n+1}-2} - 1$ dans $\mathbb{Z}_{2^{k+1}}[X]$ donc $f(X)$ divise $x^{2^n-1} - 1$ dans $\mathbb{Z}_{2^{k+1}}[X]$. ■

Exemple 2.4. *Considérons* $\mathbb{Z}_2[X]$ $X^7 - 1 \in \mathbb{Z}_2[X]$ *, on a :* $X^7 - 1 = (X^3 + X + 1)(X^3 + X^2 + 1)(X - 1)$ *une factorisation de* $X^7 - 1$ *sur* $\mathbb{Z}_2[X]$.

Comme les facteurs de $X^7 - 1$ sont 2 à 2 premiers entre eux on bien pour $Q = (X^3 + X + 1)$ le relevé de Hensel d'ordre 1 de Q défini par $Q^{(1)} = Q$ dans $\mathbb{Z}_2[X]$. Déterminons le relevé de Hensel d'ordre 3 de Q.

En utilisant la proposition précédente on a :

$$P_1(X) = 1 \ mod(2)$$

et

$$I_1(X) = X^3 + X \ mod(2)$$

donc

$$P_1^2(X) = 1 \ mod(4);$$

$$I_1^2(X) = X^6 + 2X^4 + x^2 \ mod(4)$$

D'où

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

c'est-à-dire

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

Ainsi on obtient

$$P_2(X) = 2X^2 - 1 \ mod(4);$$

$$I_2(X) = X^3 + X \ mod(4).$$

Ce qui entraine que

$$P_2^2(X) = 4X^4 - 4X^2 + 1;$$

$$I_2^2(X) = X^6 + 2X^4 + X^2.$$

Par suite

$$Q^{(3)}(X^2) = X^6 - 2X^4 - 3X^2 - 1$$

enfin

$$Q^{(3)}(X) = X^3 - 2X^2 - 3X - 1$$

ou tout simplement

$$Q^{(3)}(X) = X^3 + 6X^2 + 5X + 7.$$

On vérifie aisément que :

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

D'où $Q^{(3)}(X)$ est un diviseur de $X^7 - 1$ dans $\mathbb{Z}_8[X]$.

Proposition 2.7. *Soit $Q^{(k)}$ le relevé de Hensel d'ordre k d'un facteur irréductible de $X^{p^m-1} - 1$ alors ;*

le polynôme $Q^{(k)}$a exactement $d = deg(Q^{(k)})$ racines dans $GR(p^k, m)$ et ses racines sont de la forme

α , α^{p^2} , α^{p^3}, ..., $\alpha^{p^{d-1}}$ où α est un élément non nul de l'ensemble de Teichmuller.

Chapitre 3

CODES SUR LES ANNEAUX DE GALOIS

Introduction

Dans ce chapitre nous allons donner une définition d'un code sur les anneaux de Galois , ensuite nous énoncerons quelques propriétés complémentaires tout en s'intéressant aux codes linéaires sur les anneaux de Galois et enfin nous proposerons une étude de métrique sur l'anneau $\mathbb{Z}_4$ et code construit sur cet anneau.

3.1 Définitions , propriétés et exemples.

Définition 3.1. *Soit A un anneau de Galois , on appelle code de longueur n sur l'anneau A est tout sous-ensemble C de A^n .*

Dans ce cas A est appelé alphabet de C.

Définition 3.2. *Soient A un anneau de Galois et C un code de longueur n sur l'anneau A . On sait que A^n est doté d'une structure de A-module . On dira donc que C est un code linéaire de longueur n sur A si C est un sous-module de A^n*

On définit sur un code C de longueur n sur A une distance.

Définition 3.3. *L'application définie par :*

$$\begin{aligned} d_H : C^2 &\longrightarrow \mathbb{R}_+ \\ (a,b) &\longmapsto \textit{card}\,\{i \in \{1,...,n\}/a_i \neq b_i\} \end{aligned}$$

est appelée définie est la distance de Hamming.

Preuve : Montrons par la suite que d_H est une distance sur C.
Soient $a, b \in C$, posons $a = (a_1, a_2, ..., a_n)$ et $b = (b_1, b_2, ..., b_n)$

$(\star)$ il est clair par définition de d_H que $d_H(a,b) \in \{1, 2, ..., n\}$ donc $d_H(a,b) \geq 0$

$(\star\star)$ $d_H(a,a) = card\{i \in \{1,2,...,n\}/a_i \neq a_i\}$ d'où $d_H(a,a) = 0$ Supposons que $d_H(a,b) = 0$ alors pour tout $i \in \{1,2,...,n\}$ $a_i = b_i$ ce qui entraine que $a = b$, de plus par définition de d_H , $d_H(a,b) = d_H(b,a)$

$(\star\star\star)$ soit $c \in C$, montrons que $d_H(a,b) \leq d_H(a,c) + d_H(c,b)$

Posons $\mathcal{A} = \{i \in \{1,2,...,n\}/a_i \neq b_i\}$, $\mathcal{B} = \{i \in \{1,2,...,n\}/a_i \neq c_i\}$ et $\mathcal{F} = \{i \in \{1,2,...,n\}/c_i \neq b_i\}$ on remarque que $d_H(a,b) = card(\mathcal{A})$, $d_H(a,c) = card(\mathcal{B})$ et $d_H(c,b) = card(\mathcal{F})$ Soit donc $i \in \{1,2,...n\}$ $i \notin \mathcal{B} \cup \mathcal{F}$ alors $i \notin \mathcal{B}$ et $i \notin \mathcal{F}$ c'est-à-dire $a_i = c_i$ et $c_i = b_i$ d'où $a_i = b_i$ et par suite $i \notin \mathcal{A}$.

Ce qui entraine que $\mathcal{A} \subset \mathcal{B} \cup \mathcal{F}$ et par suite $card(\mathcal{A}) \leq card(\mathcal{B} \cup \mathcal{F}) \Rightarrow card(\mathcal{A}) \leq card(\mathcal{B}) + card(\mathcal{F})$ car $card(\mathcal{B} \cup \mathcal{F}) \leq card(\mathcal{B}) + card(\mathcal{F})$; en d'autres termes ; $d_H(a,b) \leq d_H(a,c) + d_H(c,b)$.

$(\star)$, $(\star\star)$ et $(\star\star\star)$ entrainent que d_H est une distance . ■

Définition 3.4. *Soit a un mot du code C , le poids de Hamming de a qu'on notera w_H est la quantité $d_H(a,0)$ où 0 est le mot nul donné par :* $0 = (0,0,...,0)$.

Définition 3.5. *Soient A un anneau de Galois , et C un code sur cet anneau ;la distance minimale du code C de longueur n sur l'anneau A est la quantité* $d = \min\{d_H(a,b) \ : \ a,b \in C \ et \ a \neq b\}$ *On pourra donc noter un tel code* $c(n,d)$.

Définition 3.6. *Le polynôme distribution de poids P_C d'un code linéaire C est le polynôme donné par :*

$$P_C(z) = \sum_{x \in C} z^{w_H(x)}$$

On obtient par suite que :

$$P_C(z) = \sum_{i=0}^{n} A_i z^i$$

où A_i est le nombre de mots de poids i.

Ce polynôme ainsi défini permet d'améliorer le décodage.

En effet ce polynôme renseigne sur le nombre total de mots du code C et peut permettre au récepteur du code de détecter une quelconque érreur liée au nombre de mots du code.

Définition 3.7. *Soit C un code de distance minimale d ; sa capacité théorique de correction est donnée par :* $t = E(\frac{d-1}{2})$

Définition 3.8. *Considérons le code C. Soient $a, b \in C$. a est dit permutation de b s'il existe une permutation σ de $\{1, 2, ..., n\}$ telle que $a_i = b_{\sigma(i)}$. Ainsi la relation $\mathcal{R}$ définie par :*
$\forall (a, b) \in C^2$, $(a, b) \in \mathcal{R}$ si et seulement si b est une permutation de a est une relation d'équivalence.

Preuve : Soient a , d et b trois mots de C .On a :

1. $(a, a) \in \mathcal{R}$ car a est une permutation de a (prendre pour permutation l'application identité).
2. Supposons que : $(a, b) \in \mathcal{R}$ alors par définition il existe $\sigma \in S_n$ telle que $\forall i \in \{1, 2, ..., n\}$, $b_i = a_{\sigma(i)}$ ce qui entraine que $a_i = b_{\sigma^{-1}(i)}$ d'où b est une permutation de a et donc $(b, a) \in \mathcal{R}$.
3. Supposons enfin que $(a, b) \in \mathcal{R}$ et $(b, d) \in \mathcal{R}$ alors il existe $\sigma_1 \in S_n$ et $\sigma_2 \in S_n$ telles que $\forall i \in \{1, 2, ..., n\}$, $b_i = a_{\sigma_1(i)}$ et $d_i = b_{\sigma_2(i)}$ ce qui entraine que $d_i = a_{\sigma_1(\sigma_2(i))} = a_{\sigma_1 \circ \sigma_2(i)}$ d'où d est une permutation de a et par conséquent $(a, d) \in \mathcal{R}$

Les trois dernières phrases montrent que $\mathcal{R}$ est une relation d'équivalence. ■

Définition 3.9. *Deux codes C et C' sont dit équivalents par permutation s'il existe une permutation σ de $\{1, ..., n\}$ telle que pour tout mot $x \in C'$ il existe $y \in c$ tel que x est une permutation de y par σ .*

Définition 3.10. *Une application f de A^n dans lui même est dite monomiale si , elle est linéaire et sa matrice dans une base de A^n est telle que chaque ligne et chaque colonne possède un unique élément non nul.*

En général , deux codes linéaires C et C' sont dit équivalents s'il existe une application monomiale f qui transforme C en C' . supposons que la matrice de f est $M(f)$ et G et G' sont les matrices génératrices respectives de C et C' alors on aura :

$$G' = GM(f)$$

Définition 3.11. *La capacité de détection d'un code de distance minimale d est la quantité $d-1$*

Définition 3.12. *Un code C est dit parfait si l'ensemble des boules fermées de rayon t pour la distance Hamming et centrées sur les mots du codes forment une partition ; en d'autres termes*

$$A^n = \bigcup_{x \in C} B(x, t)$$

Définition 3.13. *Soit A un anneau de Galois d'idéal maximal D et soit l'application ϕ_H définie Par :*

$$\begin{aligned} \phi_H : A &\longrightarrow \mathbb{R}_+ \\ x &\longmapsto \phi_H(x) = \begin{cases} 0 \; si \; x \in D \\ 1 \; sinon. \end{cases} \end{aligned}$$

L'application ci-dessus définie est le ***poids Homogène*** *sur l'anneau A.*

Proposition 3.1. *Cette application génère une autre sur A^2 qui est à une propriété près une métrique l'anneau A . Il s'agit de $\mathcal{M}$ définie par*

$$\mathcal{M}(x, y) = \phi_H(y - x)$$

En effet elle est positive , symétrique et vérifie l'inégalité triangulaire.

Preuve : Soient $x \; et \; y \in A \; \mathcal{T}(x, y) = \phi_H(y - x)$, et par définition $\phi_H(y - x) \geq 0$.
Ensuite , on a :

$$\begin{aligned} \mathcal{M}(x, y) &= \phi_H(y - x) \\ &= \phi_H(x - y) \\ &= \mathcal{M}(y, x) \end{aligned}$$

Car si $y - x \in D$ alors $x - y \in D$ .On remarquera que si $x - y = -(y - x)$ et D est un idéal. De plus si $y - x \notin D$ alors $y - x$ est inversible et son opposé l'est aussi. Il reste à montrer que $\mathcal{M}$ admet l'inégalité triangulaire.
Soient $x \; , \; y \; et \; z \in A$, montrons que :

$$\mathcal{M}(x, y) \leq \mathcal{M}(x, z) + \mathcal{M}(z, y);$$

- si $\mathcal{M}(x, y) = 0$ alors on a le résultat ;
- si $\mathcal{M}(x, y) = 1$, alors supposons que $\mathcal{M}(x, z) = 0$ et $\mathcal{M}(z, y) = 0$ ce qui va entrainer que par définition de $\mathcal{M}$ que $z - x \in D$ et $y - z \in D$ et par suite comme D est un idéal alors $(y - z) + (z - x) \in D$ c'est-à-dire $x - y \in D$ d'où $\mathcal{M}(x, y) = 0$ ce qui contredit l'hypothèse de départ .donc $\mathcal{M}(x, z) = 1$ ou $\mathcal{M}(z, y) = 1$ ce qui achève la preuve.

■ L'application $\mathcal{M}$ nous permet de définir sur l'anneau quotient A/D une distance.

Proposition 3.2. *L'application $\tilde{\mathcal{M}}$ définie par :*

$$\begin{aligned} \tilde{\mathcal{M}} : A/D \times A/D &\longrightarrow \mathbb{R}_+ \\ (\bar{x}, \bar{y}) &\longmapsto \mathcal{M}(x, y) \end{aligned}$$

avec $\bar{x} = x + D$, est une distance .

Preuve : vérifions d'abord si $\tilde{\mathcal{M}}$ est bien définie . Soient $x, x', y \; et \; y' \in A$ tels que $x' \in \bar{x}$ et $y' \in \bar{y}$ montrons que $\tilde{\mathcal{M}}(\bar{x}, \bar{y}) = \tilde{\mathcal{M}}(\bar{x'}, \bar{y'})$.
On a :$\tilde{\mathcal{M}}(\bar{x}, \bar{y}) = \mathcal{M}(x, y)$

— si $y - x \in D$ alors $\tilde{\mathcal{M}}(\bar{x}, \bar{y}) = 0$ et dans ce cas $\bar{x} = \bar{y}$ ce qui entraine que $\bar{x'} = \bar{y'}$ car

$$\begin{aligned} \bar{x'} &= \bar{x} \\ &= \bar{y} \\ &= \bar{y'} \end{aligned}$$

ce résultat nous permet de dire que dire que $\overline{y' - x'} = \bar{0} = D$ d'où $y' - x' \in D$ et par définition de $\tilde{\mathcal{M}}$, $\tilde{\mathcal{M}}(\bar{x'}, \bar{y'}) = 0 = \tilde{\mathcal{M}}(\bar{x}, \bar{y})$

— si $y - x \notin D$ alors $\tilde{\mathcal{M}}(\bar{x}, \bar{y}) = 1$ et dans ce cas $\overline{y - x} \neq D$ c'est-à-dire $\bar{y} - \bar{x} \neq D$ et comme $x' \in \bar{x}$ et $y' \in \bar{y}$ alors on obtient

$$\begin{aligned} \bar{y'} - \bar{x'} \neq D &\implies \overline{y' - x'} \neq D \\ &\implies y' - x' \notin D \\ &\implies \tilde{\mathcal{M}}(\bar{x'}, \bar{y'}) = 1 \end{aligned}$$

$$\tilde{\mathcal{M}}(\bar{x'}, \bar{y'}) = \tilde{\mathcal{M}}(\bar{x}, \bar{y});$$

ce qui prouve que $\tilde{\mathcal{M}}$ est bien définie . Montrons ensuite que ce qui prouve que $\tilde{\mathcal{M}}$ est une distance sur A/D.

Par définition de $\tilde{\mathcal{M}}$ $\forall \bar{x}, \bar{y} \; et \; \bar{z} \in A/D$

1. $\tilde{\mathcal{M}}(\bar{x}, \bar{y}) \geq 0$
2. $\tilde{\mathcal{M}}(\bar{x}, \bar{y}) = \tilde{\mathcal{M}}(\bar{y}, \bar{x})$
3. $\tilde{\mathcal{M}}(\bar{x}, \bar{y}) \leq \tilde{\mathcal{M}}(\bar{x}, \bar{z}) + \tilde{\mathcal{M}}(\bar{z}, \bar{y})$
4. $\tilde{\mathcal{M}}(\bar{x}, \bar{x}) = 0$

il reste à montrer que $\forall \bar{x}, \bar{y} \in A/D$, $\tilde{\mathcal{M}}(\bar{x}, \bar{y}) = 0 \Longrightarrow \bar{x} = \bar{y}$.
Par définition $\tilde{\mathcal{M}}(\bar{x}, \bar{y}) = 0$ veut dire que $y - x \in D$ ce qui conduit à $\bar{x} = \bar{y}$. D'où $\tilde{\mathcal{M}}$ est une

distance sur A/D ■

L'application $\tilde{\mathcal{M}}$ permet d'établir une distance sur le A/D-espace vectoriel $(A/D)^n$ où n est un entier naturel.

Proposition 3.3. *L'application γ définie par :*

$$\begin{aligned} \gamma : (A/D)^n \times (A/D)^n &\longrightarrow \mathbb{R}_+ \\ (a,b) &\longmapsto \sum_{i=1}^{n} \tilde{\mathcal{M}}(\bar{a}_i, \bar{b}_i) \end{aligned}$$

est une distance sur A/D.

Preuve : Soient $a, b \; et \; c \in A/D$,on a :$\tilde{\mathcal{M}}(a,a) = 0$ car $\forall i \in \{1,2,...n\}$, $\bar{a}_i - \bar{a}_i = D$ de la même manière les autres propriétés de distance découlent du fait que $\tilde{\mathcal{M}}$ est une distance sur A/D. ■

3.2 Codes linéaires

Un code linéaire dispose d'une structure algébrique plus riche qu'un code dans le cadre général . Dans la définition 3.2 on vu qu'un code de longueur n sur un anneau de Galois A est dit linéaire s'il est un sous-A-module de A^n.

On sait que les modules ne possèdent pas toujours une base comme dans le cas des espaces vectoriels . Il y existe néanmoins des familles génératrices que nous avons définie dans le chapitre précédent . Ces familles nous permettent de définir les matrices génératrices d'un code .

Définition 3.14. *On appelle matrice génératrice d'un code linéaire sur A toute matrice M dont les lignes forment une famille génératrice minimale du code .*

Théorème 3.1. *Lorsque A est un anneau de Galois la matrice d'un code linéaire C de longueur n sur A , si l'on s'autorise une légère modification de C se met sous la forme :*

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

où les $A_{i,j}$ sont les matrices à k_i lignes et k_j colonnes à coefficients dans A , les I_{k_i} sont les matrices identité d'ordre k_i et K est une matrice bloc dont chaque colonne est regroupée dans un bloc carré de taille k_0,k_1,k_2,...,k_m tels que :

$$n = \sum_{i=0}^{m} k_i \ , \ k_i \geq 0$$

De cette manière on dira que le code C sur A est de type :$(1)^{k_0}(P)^{k_1}, (P^2)^{k_2}...(p^{m-1})^{k_{m-1}}$ et de plus

$$|C| = p^r \sum_{i=0}^{m-1}(m-i)k_i$$

Définition 3.15. *Soit C un code linéaire de longueur n sur A*

1. *On appelle rang libre de C le plus grand rang des sous-modules libres de C . Dans l'exemple précédent , le rang libre du code C est k_0.*
2. *On définit le rang de C comme le cardinal de la famille génératrice minimale de C vu comme un A-module.Il s'agit en d'autres termes du nombre de lignes de la matrice génératrice linéairement indépendantes*

Dans l'exemple précédent on obtient

$$rang(C) = \sum_{i=0}^{m-1} k_i$$

Remarque 3.1. *Un code linéaire est dit de rang libre si son rang libre est égal à son rang. Dans ce cas C est un sous-A-module libre de A^n isomorphe à $A^{rang(C)}$*

3.2.1 Code dual d'un code linéaire sur un anneau de Galois.

Définissons dans un premier temps la forme bilinéaire symétrique ϕ sur A^n par $\phi(a,b) = \sum_{i=0}^{n-1} a_i b_i$, elle nous permet de définir une nouvelle notion . Celle de dualité.

Définition 3.16. *Soit C un code linéaire sur A de longueur n ; On appelle code dual d'un code C et on note $C^{\perp}$ le sous-A-module défini par :*

$$C^{\perp} = \{a \in A^n \ ; \ ab = 0 \ ; \ \forall b \in A^n\}$$

Théorème 3.2. *Lorsque la matrice du code linéaire C est définie sous la forme normale comme précédemment , celle de son dual se met également sous forme normale . On pourra la notée $K^{\perp}$ définie par :*

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

où les B_i sont les matrices blocs à coefficients dans A.

Définition 3.17. *Soit C un code linéaire de matrice génératrice G , la matrice génératrice $G^{\perp}$ de son dual est sa matrice de contrôle.*

Définition 3.18.

1. *Si pour un code C sur A alors on a $C \subset C^{\perp}$ alors on dit que C est faiblement auto dual.*
2. *Si de plus $C^{\perp} \subset C$ c'est-à-dire $C^{\perp} = C$ alors C est dit auto dual.*

3.2.2 Codes cycliques [4]

Soit A un anneau de Galois , il existe une famille intéressante de codes linéaires que nous définirons plus bas.

Définition 3.19. *L'application shift à droite donne à tout n-uplet $(a_0, a_1, ..., a_{n-1})$ l'image $(a_{n-1}, a_0, ..., a_{n-2})$*

Définition 3.20. *Un code linéaire C de longueur n sur un anneau A est cyclique si pour tout $a = (a_{n-1}, a_0, ..., a_{n-2})$ l'image par le shift à droite de a est un élément de C.*

Définition 3.21. *Soit C un code linéaire sur un anneau de Galois A .On appelle représentation polynômiale d'un mot $a = (a_0, a_1, ..., a_{n-1})$ le polynôme $P(x)$ de $A/(x^n - 1)$ donné par :*

$$P(x) = \sum_{i=0}^{n-1} a_i x^n$$

Il est d'ailleurs immédiat que l'application ϕ de A^n vers $A/(x^n - 1)$ qui à tout mot a de A^n associe sa représentation polynômiale est un isomorphisme.Ce qui veut dire en d'autre termes que tout code linéaire est identifiable à une partie de $A[X]/(X^n - 1)$.

Le théorème qui va suivre donne une définition algébrique d'un code cyclique.

Théorème 3.3. *Un sous ensemble C de A^n est un code cyclique si et seulement si son image par ϕ est un idéal de $A[x]$ où $x = X + Id(X^n - 1)$*

Preuve : Supposons que C est un code cyclique , alors $(C, +)$ est un groupe abélien car C est linéaire ce qui entraine que $(\phi(C), +)$ est un groupe abélien . De plus soient $P(x) = \sum_{i=0}^{n-1} a_i x^n \in (\phi(C), +)$,
de plus soient $a \in A$ et $i \in \{0, ..., n-1\}$ on obtient :

$$\begin{aligned} ax^i P(x) &= (ax^i) \sum_{j=0}^{n-1} a_j x^j \\ &= \sum_{j=0}^{n-1} a a_j x^{j+i}; \end{aligned}$$

de cette manière on le polynôme est $ax^i P(x)$ est la représentation polynômiale du shifté d'ordre $i + j - (n-1)$ du mot $(aa_0, ..., aa_{n-1})$ et comme C est un code cyclique donc linéaire alors $(aa_0, ..., aa_{n-1}) \in C$ et par suite $ax^i P(x) \in \phi(C)$. On en déduit du fait que A soit commutatif que pour tout $P(x) \in \phi(C)$ et $Q(x) \in A[X]/(x^n - 1)$ on a $P(x)Q(x) \in \phi(C)$.
Réciproquement , si $\phi(C)$ est un idéal de R alors $(\phi(C), +)$ est un groupe abélien ce entraine directement que (C,+) l'est aussi. Soient $a \in A$ et $(a_0, ..., a_{n-1}) \in C$, alors

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

or $\phi(C)$ est un idéal $a \sum_{i=0}^{n-1} a_i x^i \in \phi(C)$ d'où $a(a_0, ..., a_{n-1})$ ce qui montre bien que C est linéaire de plus on sait que $x \sum_{i=o}^{n-1} a_i x^i$ est la représentation polynômiale du shifté à droite du mot $(a_0, ..., a_{n-1})$ et comme $\phi(C)$ est un idéal alors $x \sum_{i=o}^{n-1} a_i x^i \in \phi(C)$ d'où le shifté à droite de $(a_0, ..., a_{n-1})$ est un élément de C et donc C est cyclique. ■

3.2.3 construction d'un code cyclique [4]

Dans cette section nous considérons que $A = \mathbb{Z}_{2^k}$ avec $k \in \mathbb{N}$ tel que $k \geq 2$ pour garder le fait que A soit un anneau de Galois.
Les codes que nous utiliserons seront de longueur n avec n impair.
Comme dans le cas général , un code de longueur n sur A que l'on notera C_{2^k} est dit cyclique

s'il est linéaire et stable par l'opérateur shift droit.
En plus sa représentation polynômiale est un idéal de $\mathbb{Z}_{2^k}[X]/(X^n-1)$.
Notre travail consiste ici à déterminer les idéaux de $\mathbb{Z}_{2^k}[X]/(X^n-1)$.
Comme dans le cas des corps fini l'anneaux $\mathbb{Z}_{2^k}[X]/(X^n-1)$ est principal.Il cependant plus complexe de déterminer ses idéaux.

Théorème 3.4. *Tout idéal de $\mathbb{Z}_{2^k}[X]/(X^n-1)$ admet de manière unique un générateur de forme :*

$$g = f_0 + 2f_1 + 2^2 f_1 + ... + 2^{k-1} f_{k-1}$$

avec

$$f_{k-1}|f_{k-2}|...|X^n - 1$$

Nous allons mettre en évidence une famille plus restreinte d'idéaux de $\mathbb{Z}_{2^k}[X]/(X^n-1)$ en utilisant le relèvement de Hensel .
En effet le générateur $g(X)$ de tout code cyclique binaire est est un diviseur de unitaire de X^n-1 dans $GF(2)[X]$, on peut donc lui appliquer le relèvement de Hensel , ce qui nous conduit à un diviseur unitaire de X^n-1 dans $\mathbb{Z}_{2^k}[X]$ qui est donc selon le théorème précédent le générateur d'un idéal de $\mathbb{Z}_{2^k}[X]/(X^n-1)$ de la forme $f_1 = f_2 = ... = f_{k-1} = g^{(k)}$

Définition 3.22. *Soient $g(X) \in GF(2)[X]$ un diviseur de X^n-1 et $g^{(k)}(X)$ son relevé de Hensel d'ordre k.Le code $C_{2^k} = (g^{(k)}(X)) \subset \mathbb{Z}_{2^k}[X]/(X^n-1)$ est appelé le code relevé du code cyclique binaire $C = (g(X)) \subset GF(2)[X]/(X^n-1)$*

Soit m le plus petit entier tel que $g^{(k)}(X)|X^{2^m-1}-1$. le polynôme $g^{(k)}(X)$ peut s'écrire comme produit de facteurs irréductibles de $X^{2^m-1}-1$, donc par la (proposition 2.7) $g^{(k)}(X)$ a tous ses zéros dans l'anneau de Galois $GR(2^k, m)$ et ils sont au nombre de $deg(g)$.

Définition 3.23. *Soient $g^{(k)}$ un diviseur unitaire de X^n-1 et c_{2^k} le code engendré par $g^{(k)}$. On appelle zéros de c_{2^k} l'ensemble des zéros de $g^{(k)}$ dans $GR(2^k, m)$.*

Proposition 3.4. *Soit $g^{(k)} \in \mathbb{Z}_{2^k}[X]$ un polynôme unitaire divisant X^n-1. la famille*

$$\{g^{(k)} \ , \ Xg^{(k)} \ , \ ... \ , X^{n-d-1}g^{(k)}\}$$

avec $d = deg(g^{(k)})$, est une base du code $C_{2^k} = (g^{(k)})$.

Preuve : La famille ci-dessus est une famille génératrice de $C_{2^k} \subset \mathbb{Z}_{2^k}[X]/(X^n-1)$ car en effet pour tout polynôme $P(x)$ de C_{2^k} il existe $Q(X)$ tel que $P(X) = Q(X)g^{(k)}(X)$ et comme $P(x) \in \mathbb{Z}_{2^k}[X]/(X^n-1)$ alors $deg(P(X)) \leq n-1$ d'où $deg(Q(X)) \leq n-d-1$ et par conséquent

$$P(X) = \sum_{i=0}^{n-d-1} a_i X^i g^{(k)}(X)$$

d'où cette famille est génératrice.

Montrons ensuite qu'elle est libre sur $\mathbb{Z}_{2^k}$. posons $X^n - 1 = g^{(k)}(X)h^{(k)}(X)$ et supposons qu'il existe $n-d$ éléments de $\mathbb{Z}_{2^k}$ tels que $\sum_i a_i X^i g^{(k)}(X) = 0$ alors comme $\sum_i a_i X^i g^{(k)}(X) \in \mathbb{Z}_{2^k}[X]/(X^n-1)$ alors $\sum_i a_i X^i g^{(k)}(X) = X^n - 1$ c'est-à-dire $A(X) = \sum_i a_i X^i$ est un multiple de $h^{(k)}(X)$ or $deg(h^{(k)}(X)) = n-d$ et mais $deg(A(X)) \leq n-d-1$ donc $A(X) = 0$, ce qui entraine que les a_i choisis plus haut sont tous nuls . ■

3.2.4 codes quaternaires [2]

Dans la suites notre alphabet sera $\mathbb{Z}_4$

Définition 3.24. *On appelle code quaternaire , un code sur* $\mathbb{Z}_4$.

Un tel code s'il est linéaire de longueur n est un sous-module de $\mathbb{Z}_4$.

La poids de Hamming défini plus haut n'est pas suffisamment précis sur l'anneau $\mathbb{Z}_4$ car il ne différencie pas véritablement les éléments de $\mathbb{Z}_4$.

Le poids le plus adapté est le poids de Lee défini sur $\mathbb{Z}_4$ par :

$$\begin{aligned} W_{Lee} : \mathbb{Z}_4 &\longrightarrow \{0,1,2\} \\ \bar{0} &\longmapsto 0 \\ \bar{1} &\longmapsto 1 \\ \bar{2} &\longmapsto 2 \\ \bar{3} &\longmapsto 1 \end{aligned}$$

Il faut dire qu'en général sur $\mathbb{Z}_p$, W_{Lee} est définie par :

$$W_{Lee}(x) = \begin{cases} x \ si \ x \leq \lfloor \frac{p}{2} \rfloor \\ \\ -x \ sinon \end{cases}$$

où $-x$ est l'inverse additif de x dans $\mathbb{Z}_p$.

Définition 3.25. *Le poids de Lee d'un vecteur $u \in \mathbb{Z}_4^n$ est donné par l'égalité :*

$$W_L(u) = \sum_{i=1}^{n} W_{Lee}(u_i).$$

Ce poids nous permet de définir une nouvelle distance sur $\mathbb{Z}_4^n$ donnée par :

$$\forall u, v \in \mathbb{Z}_4^n \ , \ d_L(u, v) = W_L(u - v)$$

Preuve :

Soient $a, b, c \in \mathbb{Z}_4^n$ on a $d_L(a, b) = W_L(a - b) \geq 0$ par définition de W_L

$$\begin{aligned} d_L(a,b) &= W_L(a-b) \\ &= \sum_{i=1}^{n} W_{Lee}(a_i - b_i) \\ &= \sum_{i=1}^{n} W_{Lee}(b_i - a_i) \ car \ pour \ x \in \mathbb{Z}_4 \ , \ W_{Lee}(-x) = W_{Lee}(x) \\ &= d_L(b,a); \end{aligned}$$

par suite on a $d_L(a, a) = 0$ par définition de d_L

$$\begin{aligned} d_L(a,b) = 0 &\implies \sum_{i=1}^{n} W_{Lee}(a_i - b_i) = 0 \\ &\implies W_{Lee}(a_i - b_i) = 0 \ pour \ tout \ i. \ car \ W_{Lee} \ est \ positive \\ &\implies a_i = b_i \ pardfinition \ de \ W_{Lee} \\ &\implies a = b \end{aligned}$$

Remarque 3.2. *de part la construction de W_{Lee} on remarque que pour tout $x, y \in \mathbb{Z}_4$ $W_{Lee}(x + y) \leq W_{Lee}(x) + W_{Lee}(y)$*

ce qui entraine que :

$$\begin{aligned} d_L(a,b) &= \sum_{i=1}^{n} W_{Lee}(a_i - b_i) \\ &= \sum_{i=1}^{n} W_{Lee}((a_i - c_i) + (c_i - b_i) \\ &\leq \sum_{i=1}^{n} W_{Lee}(a_i - c_i) + \sum_{i=0}^{n} W_{Lee}(c_i - b_i) \ (\ par \ la \ remarque \ ci - dessus \ ) \end{aligned}$$

ce qui conduit à

$$d_L(a,b) \leq d_L(a,c) + d_L(c,b)$$

. donc d_L est bien une métrique sur $\mathbb{Z}_4^n$.

■

APPORT DIDACTIQUE

L'élaboration de notre travail nous a permis de consolider quelques notions importantes d'algèbre linéaire dont la maîtrise est nécessaire pour le jeune enseignant de mathématiques afin de mieux conduire ses enseignements au lycée . De plus le document que nous avons produit est un rendu de plusieurs recherches dans des bibliothèques , médiathèques et en laboratoire ; ce travail est en effet une transposition didactique . Il s'agit la aussi d'une tâche qui sera incontournable au lycée et/ou collège pour un enseignant , et lorsqu'elle est bien faite , elle sera bénéfique pour ses élèves .

Nous rappelons que la transposition didactique est la transformation d'un savoir savant en un savoir enseigné.Il s'agit ici de rendre un savoir souvent sophistiqué plus accessible .

Que dire alors des méthodes de rédaction que nous avons expérimentées à l'occasion de la confection de ce document ; une merveille pour la rédaction des documents de mathématiques ; l'éditeur LaTeX qui à l'ère du numérique nous permettra d'affronter la nouvelle donne et produire les documents et épreuves de qualité pour le bonheur de nos futurs élèves.

Pour conclure nous dirons que notre travail , sans être spécifique à la didactique , nous a plongé dans les réalités quotidiennes d'un enseignant de mathématiques.

Conclusion

Au terme de notre travail , il apparait que la notion de code sur un anneau de Galois et plus particulièrement de code linéaire est fortement riche et ne saurait se resumer à cet ouvrage qui s'est limité juste à une présentation introductive . Notons par ailleurs que nous avons travaillé sur les anneaux de Galois ; nous détaillons en effet dans ce mémoire la notion de codes sur les anneaux de Galois . Cependant nous restons curieux de découvrir les avantages que l'on peut engranger si notre alphabet est un anneau intègre voire un corps au sens mathématique.
En perspective nous nous proposons de faire une étude plus complète sur les anneaux de chaine ; de parcourir leurs propriétés générales et celles des codes sur ce type d'anneaux.

Bibliographie

[1] Christian Blanchet. *Cours d'algébre*. Paris-Diderot, 2011-2012.

[2] Alexis BONNECAZE. *Codes sur des anneaux finis et reseaux arithmétiques*. PhD thesis, Université de Nice Sophia Antapolis et l'école doctorale Science Pour L'ingenieur, 1995.

[3] NEKELEYAN DAVID. *Codes linéaires sur les anneaux finis*. Higher teacher training college of Yaoundé, 2015-2016.

[4] YEMEN OLFA. *Application des codes cycliques tordus*. PhD thesis, Université de Nice Sophia Antapolis, 2013.