UNIVERSITE CHEIKH ANTA DIOP DE DAKAR
FACULTE DES SCIENCES ET TECHNIQUES
DEPARTEMENT DE MATHEMATIQUES ET INFORMATIQUE

THÈSE DE DOCTORAT D'ÉTAT ÈS SCIENCES MATHÉMATIQUES – OPTION : ALGEBRE

Sujet de la Thèse :

FGI-ANNEAUX, I-MODULES ET SUITES RECURRENTES LINEAIRES

Présentée et soutenue publiquement le 03 Juillet 2006 à 10 H – Amphi 7

par

Monsieur Oumar DIANKHA

Pour obtenir le grade de Docteur ès Sciences Mathématiques

devant le Jury composé de :

Président :

Souleymane **NIANG**	Professeur	UCAD

Membres :

Chérif **BADJI**	Professeur	UCAD	Examinateur
Maurice **MIGNOTTE**	Professeur	Univ. Louis Pasteur (France)	Rapporteur
Mme Nouzha **EL YACOUBI**	Professeur	Univ. Mohamed V (Maroc)	Examinateur
Daouda **SANGARE**	Professeur	Univ. d'Abobo-Adjamé(Côte d'Ivoire)	Rapporteur
Mamadou **SANGHARE**	Professeur	UCAD	Directeur
Hamet **SEYDI**	Professeur	UCAD	Examinateur

Année Universitaire 2005 - 2006

Résumé

TITRE DE LA THESE : FGI – anneaux, I – Modules et Suites Récurrentes linéaires.

NATURE DE LA THESE : Thèse d'Etat

SPECIALITE : Algèbre

COMPOSITION DU JURY

Président :

Souleymane **NIANG**	Professeur	UCAD	

Membres :

Chérif **BADJI**	Professeur	UCAD	Examinateur
Maurice **MIGNOTTE**	Professeur	Univ. Louis Pasteur (France)	Rapporteur
Mme Nouzha **EL YACOUBI**	Professeur	Univ. Mohamed V (Maroc)	Examinateur
Daouda **SANGARE**	Professeur	Univ. d'Abobo-Adjamé(Côte d'Ivoire)	Rapporteur
Mamadou **SANGHARE**	Professeur	UCAD	Directeur
Hamet **SEYDI**	Professeur	UCAD	Examinateur

Date - Heure et Lieu : Le 03 Juillet 2006 à 10 H Amphi 7.

Dans cette thèse, nous avons d'abord, caractérisé les anneaux commutatifs (resp. les duo-anneaux) R pour lesquels la propriété (I) caractérise les R–modules de type fini en prouvant que ces anneaux sont des anneaux artiniens à idéaux principaux. Ces anneaux seront appelés FGI–anneaux commutatifs (resp. FGI–duo-anneaux). On dira qu'un R – module M vérifie la propriété (I) si tout endomorphisme injectif de M est un automorphisme.

Ensuite, on désigne par σ [M] la catégorie des R–modules à gauche sous–engendrés par M. On dit que le R–module M est un I–module (resp. un I_1–module) si tout R–module de la catégorie σ[M] vérifiant la propriété (I) est artinien (resp. est de longueur finie). Nous avons donné une caractérisation complète des I_1–groupes abéliens), des I_1– modules possédant un progénérateur dans σ [M] et des I-modules de type fini sur un duo– anneau.

Et enfin, nous avons étudié le rapport entre l'ordre d'une suite récurrente linéaire et celui de son polynôme caractéristique sur un corps fini K modulo un nombre premier, le degré de la plus petite extension du corps fini K dans laquelle un polynôme de K [X] se factorise complètement et nous donnons une précision sur le logarithme de ce degré et quelques généralités sur les suites aléatoires.

Mots clés : FGI-anneaux, FGI-duo-anneaux, artinien, principal, idéal, I– modules, I_1-modules σ M], type de représentation finie, progénérateur, type fini, suites récurrentes linéaires, polynômes, ordre, corps fini, irréductible et aléatoire.

FGI-ANNEAUX, I-MODULES ET SUITES RECURRENTES LINEAIRES

A mes parents, pour tout ce qu'ils ont investi pour mon éducation, ma femme et mes enfants pour leur soutien moral et leur patience.

REMERCIEMENTS

Je tiens à remercier vivement Monsieur le professeur **Souleyemane NIANG** pour l'honneur qu'il m'a fait en acceptant de présider mon jury de thèse.

Je tiens à remercier sincèrement le professeur **Mamadou SANGHARE** qui a dirigé mes travaux. Je tiens à lui exprimer ma profonde gratitude pour les conseils et les encouragements qu'il m'a prodigués tout le long de ce travail. J'ai apprécié tout particulièrement sa patience et sa grande disponibilté à mon égard.

Je remercie très sincèrement le professeur **Maurice MIGNOTTE** pour avoir accepté d'être rapporteur de cette thèse et examinateur dans ce jury. Il m'a toujours réservé un accueil très chaleureux avec beaucoup d'hospitalité et de disponibilité, pendant mes différents séjours dans son laboratoire de Mathématiques discrètes de l'Université Louis Pasteur de Strasbourg. Durant mes recherches sur les suites récurrentes linéaires, il m'a toujours prodigué de précieux conseils.
Je remercie l'Agence Universitaire de la Francophonie pour les bourses de recherche qu'elle m'a accordées.

Je remercie très sincèrement le Professeur **Daouda SANGARE** pour avoir accepté d'être rapporteur de cette thèse et examinateur dans ce jury.

J'exprime ma profonde gratitude aux Professeurs **Hamet SEYDI, Chérif BADJI** et **Mme Nouzha EL YACOUBI** pour l'honneur qu'ils me font en faisant partie du jury de cette thèse.

Je remercie tous les membres du Laboratoire d'Algèbre et de Géométrie Algébrique et Applications (LAGAA), tous mes collègues et tout le personnel administratif du Département de Mathématiques et Informatique de la Faculté des Sciences et Techniques de l'Université Cheikh Anta Diop de Dakar.

Table des matières

INTRODUCTION

Cette thèse est un ensemble de travaux consacrés essentiellement à l'étude des FGI-anneaux commutatifs, des FGI-duo-anneax, des I-modules et des suites récurrentes linéaires.

Soit R un anneau associatif non (nécessairement) commutatif, possédant un élément unité $1 \neq 0$. On dit qu'un R-module à gauche vérifie la propriété (I) si tout endomorphisme injectif de M est un automorphisme de M ; on dit qu'un R-module N est engendré par M (ou M-engendré) s'il existe un ensembre Λ et un épimorphisme $f : M^{(\Lambda)} \longrightarrow N$, où $M^{(\Lambda)}$ est la somme directe de $|\Lambda|$ copies de M ; un R-module N est dit sous-engendré par M (ou M-sous-engendré) s'il est un sous-module d'un R-module M-engendré. On note $\sigma[M]$ la catégorie dont les objets sont les modules M-sous-engendrés. $\sigma[M]$ est une sous-catégorie pleine de la catégorie des R-modules à gauche R-Mod.

Soient ENS la catégorie des ensembles et $Vect_{\mathbb{K}}$ la catégorie des $\mathbb{K}$-espaces vectoriels avec $\mathbb{K}$ un corps. On dit qu'un objet X de ENS vérifie la propriété (I) si tout morphisme (application) injectif de X est bijectif. Dans ENS, la propriété (I) caractérise les ensembles finis. On dit qu'un objet V de $Vect_{\mathbb{K}}$ vérifie la propriété (I) si tout endomorphisme injectif de V est un automorphisme de V. Dans $Vect_{\mathbb{K}}$ la propriété (I) caractérise les $\mathbb{K}$-espaces vectoriels de dimension finie

Ainsi, peut-on se poser la question suivante : comment étendre cette étude dans R-Mod et dans $\sigma[M]$?

En général, dans R-Mod, la propriété (I) ne caractérise pas les modules de type fini. Par exemple pour l'anneau $\mathbb{Z}$ des entiers, le $\mathbb{Z}$-module $\mathbb{Q}$ des nombres rationnels vérifie la propriètè (I) mais n'est pas de type fini.

Notons $\mathcal{I}_{\mathcal{R}}$ la classe des R-modules à gauche vérifiant la propriété (I) et $\mathcal{F}_{\mathcal{R}}$ la classe des R-modules à gauche de type fini. W.V. VASCONCELOS a prouvé dans [29] pour un anneau commutatif R, que $\mathcal{F}_{\mathcal{R}} \subseteq \mathcal{I}_{\mathcal{R}}$. Mais en

général cette inclusion est stricte. Par exemple pour $R = \mathbb{Z}$ l'anneau des entiers, on a l'inclusion stricte.

Nous allons donc étudier les anneaux R pour lequels tout R-module vérifiant la propriété (I) est de type fini. De tels anneaux sont appelés les FGI-anneaux ou FGI-duo-anneaux si R est un duo-anneau. La notion de FGI-anneaux a été introduite pour la première fois dans [4] paru en 1997 où les FGI-anneaux commutatifs dénombrables ont été étudiés et caractérisés. Dans [2] et [3], nous avons généralisé cette notion sur les FGI-anneaux commutatifs (non nécessairement dénombrables) et sur les FGI-duo-anneaux.

Il est bien connu que tout objet artinien de $\sigma[M]$ vérifie la propriété (I). Mais l'inverse n'est pas toujours vraie. Par exemple le $\mathbb{Z}$-module $\mathbb{Q}$ objet de $\sigma[\mathbb{Z}] = \mathbb{Z}$-Mod vérifie la propriété (I) mais n'est pas artinien. Donc il est intéressant d'étudier pour un anneau fixé R, les R-modules ${}_RM$ pour lesquels tout objet de $\sigma[M]$ vérifiant la propriété (I) est artinien (resp de longueur finie). De tels modules sont appelés I-modules (resp I_1-modules). La notion de I-module a été introduite pour la première fois dans [9] et généralisée dans [12] et [11].

Le chapitre 1 rassemble des résultats classiques et récents que nous utiliserons dans les chapitres suivants. Ce sont entre autres des résultats préliminaires que nous avons établis sur les FGI-anneaux, les FGI-duo-anneaux, les I-modules et les suites linéaires récurrentes.

L'article [2] constitue le chapitre 2. Dans ce chapitre, nous faisons une étude plus générale des FGI-anneaux commutatifs en levant la condition de dénombrabilité de l'anneau posée dans [4].

Le chapitre 3 constitué par [3], traite des FGI-duo-anneaux, ce qui nous permet de généraliser l'étude faite dans le chapitre 2.

Le chapitre 4 est constitué par [11] et [12] où nous avons donné une caractérisation complète des I_1-groupes abéliens, les I_1-modules possédant un progénérateur dans $\sigma[M]$ et les I-modules de type fini sur un duo-anneau.

Et enfin le chapitre 5 constitué par [10], est consacré à l'étude des suites récurrentes linéaires sur un corps fini. Nous étudions d'abord le rapport entre l'ordre d'une suite récurrente linéaire et celui de son polynôme caractéristique modulo un nombre premier, ensuite le degré de la plus petite extension du corps fini K dans laquelle un polynôme de $K[X]$ se factorise complètement. On montre que le logarithme de ce degré est "en général" majoré par $\frac{1}{2}\log^2 d + \frac{66}{7}(\log d)^{7/4}$ où d positif est le degré de Q, et enfin nous donnons quelques généralités sur les suites aléatoires.

Chapitre 1

PRELIMINAIRES

Ce chapitre contient essentiellement des rappels de résultats dont nous nous servirons dans cette Thèse et des notations dont nous ferons usage constamment.

Sauf mention expresse du contraire le mot anneau désignera un anneau associatif non (nécessairement) commutatif, unitaire d'élément unité $1 \neq 0$, le mot module un module à gauche unitaire et les homomorphismes d'anneaux transforment l'élément unité en l'élément unité.

On notera ${}_RM$ un R-module à gauche, R-Mod la catégorie des R-modules à gauche et $\sigma[M]$ la catégorie des R-modules sous-engendrés par M.

1.1 Notion de FGI-anneaux

Soient R un anneau et M un R-module. On dit que M vérifie la propriété (I) si tout endomorphisme injectif de M est un automorphisme de M. Un anneau R est dit duo-anneau si tout idéal à gauche ou à droite de R est bilatère. Un anneau R est un FGI-anneau si tout R-module vérifiant la propriété (I) est de type fini. Si R est un duo-anneau, on l'appelera FGI-duo-anneau.

Exemples 1.1.1. *1. Les corps (commutatifs ou non), et, plus généralement, les anneaux semi-simples sont des exemples évidents de FGI-anneaux à gauche.*

2. L'anneau $K[X]$ où K est un corps commutatif n'est pas un FGI-anneau.

Le résultat suivant est bien connu :

Proposition 1.1.1. *Soit R un anneau. Tout R-module artinien vérifie la* propriété (I).

Démonstration. Soit M un R-module artnien et f un endomorphisme injectif de M. La suite $\ldots f^n(M) \subseteq f^{n-1}(M) \subseteq \ldots \subseteq f^2(M) \subseteq f(M) \subseteq M$ étant une suite décroissante, il existe $n \in \mathbb{N}$ tel que l'on ait $:f^n(M) = f^{2n}(M)$. Soit $y \in M$, il existe $x \in M$ tel que $f^n(y) = f^{2n}(x)$. Il en résulte que $f^n(y - f^n(x)) = 0$. D'où $y = f^n(x) \in \operatorname{Im} f$. □

Remarque 1.1.1. *La réciproque du résultat de la proposition* 1.1.1 *n'est pas, en général vraie. Par exemple, si R est un anneau commutatif intègre qui n'est pas un corps, alors le corps des fractions K de R est un R-module qui vérifie la* propriété (I) *mais n'est pas artinien.*

Proposition 1.1.2. *1. L'image homomorphe d'un FGI-anneau est un FGI-anneau.*

2. Un produit direct d'anneaux $R = \prod_{i=1}^{n} R_i$ est un FGI-anneau si est seulement si chaque R_i, pour $1 \leq i \leq n$ est un FGI-anneau.

Démonstration. 1. Soit $\varphi : R \longrightarrow S$ un homomorphisme surjectif d'anneaux tel que R soit un FGI-anneau et S un anneau donné. Alors tout S-module à gauche M a une structure de R-module.
Pour tout $r \in R$, $m \in M$, $f \in \operatorname{End}({}_SM)$, nous avons :
$r \cdot m = \varphi(r) \cdot m$ et $f(r \cdot m) = f(\varphi(r) \cdot m) = \varphi(r)f(m) = r \cdot f(m)$.
Donc les R-homomorphismes de M et les S-homomorphismes de M coïncident. Les R-sous-modules de M coïncident avec les S-sous-modules de M. Par la suite, si M est un S-module vérifiant la propriété (I), alors M est de type fini.

2. Soit $p_{i_0} : R \longrightarrow R_{i_0}$ un homomorphisme surjectif. D'après 1), R_{i_0} est un FGI-anneau.
Réciproquement : Posons $R = R_1 \times R_2$, où R_1 et R_2 sont des FGI-anneaux. Soit ${}_RM$ un R-module à gauche.
Posons : $e_1 = (1_{R_1}, 0)$, $e_2 = (0, 1_{R_2})$, $1_R = 1_{R_1} + 1_{R_2} = e_1 + e_2$,
$M_1 = e_1M$, $M_2 = e_2M$ et $M = M_1 + M_2$.
Pour $x \in M$, nous avons :

$$x = 1x = (e_1 + e_2)x = e_1x + e_2x \quad \text{et} \quad R_1 \cong R_1 \times \{0\}.$$

Soient $r_1 \in R_1$, $m \in M$ et $e_1 m \in M_1$. Alors

$$r_1(e_1 m) = (r_1, 0)m = [(1,0)(r_1,0)]\, m = e_1(r_1,0)m \in M_1.$$

Donc M_1 est un R_1-module.
De même $R_2 \cong \{0\} \times R_2$ et M_2 est un R_2-module.
Considérons maintenant $f :_R M \longrightarrow_R M$ un endomorphisme de ${}_RM$, alors f induit des endomorphismes

$$f_1 : M_1 \longrightarrow M_1 \qquad \text{et} \quad f_2 : M_2 \longrightarrow M_2,$$

où $f_1 = f_{|M_1}$ et $f_2 = f_{|M_2}$.
Nous avons :
$f(e_1 m) = e_1 f(m) \in M_1$, $f(e_2 m) = e_2 f(m) \in M_2$ et
$f_1(r_1 e_1 m) = f(r_1 e_1 m) = r_1 f(e_1 m) = r_1 f_1(e_1 m)$.
Donc f_1 est R_1-linéaire. De même on montre que f_2 est R_2-linéaire.
Soit

$$\varphi_i \in End_{R_i}(M_i) \quad pour \quad i = 1, 2, \quad \text{injectifs.}$$

Nous avons
$M_1 \bigcap M_2 = \{(0,0)\}$. et $M \cong M_1 \times M_2 : x \to (e_1 x, e_2 x)$.
Posons

$$\begin{aligned} f &: M \longrightarrow M \\ x &\mapsto f(x) = \varphi_1(e_1 x) + \varphi_2(e_2 x) \end{aligned}$$

$$\begin{aligned} f(x + x') &= \varphi_1(e_1(x + x') + \varphi_2(e_2(x + x')) \\ &= [\varphi_1(e_1 x) + \varphi_2(e_2 x)] + [\varphi_1(e_1 x') + \varphi_2(e_2 x')] \\ &= f(x) + f(x'). \end{aligned}$$

Soient $r \in R$ et $x \in M$. Alors

$$\begin{aligned} f(rx) &= \varphi_1(e_1(rx)) + \varphi_2(e_2(rx)) \\ &= \varphi_1(e_1 r e_1 x) + \varphi_2(e_2 r e_2 x) \\ &= e_1 r \varphi_1(e_1 x) + e_2 r \varphi_2(e_2 x) \\ &= r e_1 \varphi_1(e_1 x) + r e_2 e_1 \varphi_1(e_1 x) + e_2 r \varphi_2(e_2 x) + e_2 r e_1 \varphi_2(e_2 x) \\ &= (r e_1 + r e_2)[\varphi_1(e_1 x + \varphi_2(e_2 x)] \\ &= r f(x). \end{aligned}$$

Comme φ_1 et φ_2 sont injectifs, alors f est injectif. Par la suite f est un automorphisme de ${}_RM$ puisque ${}_RM$ vérifie la propriété (I).

Montrons maintenant que φ_1 est surjectif.

Soit $y_1 \in M_1$, il existe x élément de M tel que $f(x) = y_1$. Ce qui impique que $y_1 = \varphi_1(e_1x) + \varphi_2(e_2x)$.

Donc $e_1y_1 = y_1 = e_1[\varphi_1(e_1x) + \varphi_2(e_2x)] = \varphi_1(e_1x)$.

Donc M_1 vérifie la propriété (I).

De même on montre que M_2 vérifie la propriété (I).

Comme R_1 et R_2 sont des FGI-anneaux, alors M_1 et M_2 sont de type fini.

Soient $x_1, \ldots, x_m \in M_1$, $y_1, \ldots, y_p \in M_2$, éléments des systèmes générateurs respectifs de M_1 et M_2. Alors

$$M_1 = \sum_{i=1}^{m} Rx_i \text{ et } M_2 = \sum_{j=1}^{p} Ry_j.$$

Donc pour tout $m \in M$, on a alors

$$m = 1.m = e_1m + e_2m = \sum_{i=1}^{m} \alpha_i x_i + \sum_{j=1}^{p} \beta_j y_j,$$

avec $\alpha_i \in R_1$ et $\beta_j \in R_2$. Donc ${}_RM$ est de type fini et $R = R_1 \times R_2$ est un FGI-anneau.

Par induction sur n, $R = \prod_{k=1}^{n} R_k$ est un FGI-anneau.

□

Soient M un R-module à gauche et $\mathrm{Ann}_R(M) = \{r \in R \,/\, \forall m \in M,\ rm = 0\}$ l'annulateur de M dans R.

Si $m \in M$, *alors* $\mathrm{Ann}_R(m) = \{r \in R \,/\, rm = 0\}$ est l'annulateur de m dans R.

Si $m_1, \ldots, m_n \in M$, $\mathrm{Ann}_R(m_1, \ldots, m_n) = \bigcap_{i=1}^{n} \mathrm{Ann}_R(m_i)$.

1.2 Notion de I-module

Soit M un R-module à gauche.

Définition 1.2.1. *Un R-module N est dit engendré par M (ou M-engendré) s'il existe un épimorphisme $\varphi : M^{(\Lambda)} \longrightarrow N$, où $M^{(\Lambda)}$ est la somme de $|\Lambda|$ copies de M.*

Un R-module K est dit sous-engendré par M (ou M-sous-engendré) si K est un sous-module d'un module M-engendré.

L'ensemble des sous-modules M-sous-engendrés forme une catégorie notée $\sigma[M]$, qui est une sous-catégorie pleine de la catégorie des R-modules à gauche R-Mod.

Si $M =_R R$, alors $\sigma[{}_RR] =$ R-Mod.

Définition 1.2.2. *Un R-module M est dit vérifier la* propriété (I) *si tout endomorphisme injectif de M est un automorphisme de M.*

On dit que M est un I-module si tout objet de $\sigma[M]$ vérifiant la propriété (I) *est artinien*

L'anneau R est dit I-anneau si le R-module ${}_RR$ est un I-module.

On dit que M est un I_1-module si tout objet de $\sigma[M]$ vérifiant la propriété (I) *est de longueur finie.*

Exemples 1.2.1. *Soit R un anneau semi-simple. Le R-module ${}_RR$ est un I-module (un I_1-module).*

1.2.1 Modules injectifs, Modules projectifs

Définition 1.2.3. *On rappelle qu'un R-module M est dit injectif (resp. projectif) si pour tout diagramme de R-modules*

$$\begin{array}{ccccc} & & M & & \\ & & \uparrow & & \\ 0 & \longrightarrow & N & \longrightarrow L & \text{respectivemement} \end{array} \qquad \begin{array}{ccccc} & & M & & \\ & & \downarrow & & \\ L & \longrightarrow & N & \longrightarrow 0, & \end{array}$$

il existe un homomorphisme $h : L \longrightarrow M$ respectivement $h : M \longrightarrow L$ qui rende respectivement les diagrammes commutatifs.

On dit qu'une extension E d'un R-module M est une *extension essentielle* de M si, pour tout sous-module N de E, la relation $N \cap M = \{0\}$ implique $N = \{0\}$. On appelle *enveloppe injective* d'un module M, toute extension essentielle injective de M. On la notera $E(M)$ ou $\widehat{M}$. Un module M est dit *uniforme* si tout sous-module non nul de M est un sous-module essentiel de M.

Chapitre 2

FGI-anneaux commutatifs

Ce chapitre est constitué par [2]. Soit R un anneau commutatif possédant un élément unité $1 \neq 0$. On dit qu'un R-module M vérifie la propriété (I) si tout endomorphisme injectif de M est un automorphisme de M. Un anneau R est un FGI-anneau si tout R-module vérifiant la propriété (I) est de type fini. Soit $\mathcal{I}_R$ la classe des R-modules vérifiant la propriété (I) et $\mathcal{F}_R$ la classe des R-modules de type fini.

Le but de ce chapitre est de caractériser les anneaux R pour lesquels $\mathcal{I}_R = \mathcal{F}_R$.

Dans la section 2.1, nous montrons que si R est un FGI-anneau alors R est de dimension zéro et que tout idéal premier de R est maximal (proposition 2.1.1). Et par la suite $J(R)$ est un nilidéal.

Dans la section 2.2, nous prouvons que si R est un anneau commutatif artinien ne possédant pas d'idéal principal, alors il existe un R-module qui vérifie la propriété (I) et qui n'est pas de type fini.

Dans la section 2.3, nous généralisons les résultats de [4] en donnant une caractérisation complète des FGI-anneaux commutatifs (théorème 5.1.3). Nous montrons que R est un FGI-anneau si et seulement si R est artinien à idéaux principaux.

2.1 Le radical de Jacobson d'un FGI-anneau est un nilidéal

Proposition 2.1.1. *Soit R un FGI-anneau. Alors, tout idéal premier de R est maximal.*

De plus l'ensemble de tous les idéaux premiers de R est fini.

Démonstration. Soient P un idéal premier de R et B le corps des fractions d'un anneau intègre R/P. Il est clair que B, considéré comme un R/P-module, satisfait la propriété (I). Comme R/P est un FGI-annneau, alors B est un R/P-module de type fini. Donc $B = R/P$ et P est maximal. Soit maintenant L l'ensemble de tous les idéaux premiers de R. Pour tout $P \in L$, R/P est un R-module simple. Si P, $P' \in L$ avec $P \neq P'$, alors nous avons $\mathrm{Hom}_R(R/P, R/P') = \{0\}$.

Donc le R-module $M = \bigoplus_{P \in L} R/P$ vérifie la propriété (I). Il en résulte que M est un R-module de type fini. D'où L est fini. □

Corollaire 2.1.1. *Soit R un FGI-anneau commutatif. Alors le radical de Jacobson $J(R)$ de R est un nilidéal et R est un anneau semi-local.*

Démonstration. Ce corollaire résulte de la proposition 2.1.1. □

Proposition 2.1.2. *Un anneau artinien à idéaux principaux est un FGI-anneau.*

Démonstration. Cette proposition résulte de ([17], Theoréme 9) □

2.2 Construction d'un module qui n'est pas de type fini et qui vérifie la propriété (I).

Pour construire ce R-module, nous supposons que l'anneau R est local artinien d'idéal maximal $J(R) = aR + bR$ avec $a^2 = b^2 = ab = 0$ et $J(R)$, le radical de Jacobson, est non principal. Alors d'après [6], il existe un sous anneau local artinien à idéaux principaux C de R avec radical de Jacobson $J(C) = aC$, où $a \neq 0$ et $a^2 = 0$.
Soient $M = \bigoplus_{i \in \mathbb{N}} C.e_i$ un C-module libre avec une base infinie dénombrable $\{e_i : i \in \mathbb{N}\}$, σ l'endomorphisme du C-module M, défini par $\sigma(e_0) = 0$, et $\sigma(e_i) = ae_{i-1}$ pour tout $i \geq 1$ et f un endomorphisme injectif du C-module M, satisfaisant $f\sigma = \sigma f$. Avec ces notations, nous avons :

Lemme 2.2.1. (i) $a\sigma = \sigma^2 = 0$
(ii) *Pour tout $i \in \mathbb{N}^*$, on a $\sigma[f(e_i)] = af(e_{i-1})$.*

Lemme 2.2.2. *Pour tout $i \in \mathbb{N}$, on a* $f(e_i) = \sum_{j<i} \alpha_j^i e_j + \alpha_i^i e_i + a\sum_{k>i} \alpha_k^i e_k$, *et α_i^i est inversible dans R.*

Démonstration. Comme f est injective, alors nous avons :

$$\sigma[f(e_0)] = f[\sigma(e_0)] = f(0) = 0, \tag{2.1}$$

et

$$af(e_0) = f(ae_0) \neq 0. \tag{2.2}$$

Soit $f(e_0) = \sum_{i=0}^{m} \alpha_i^0 e_i$. De la relation (2.1), nous avons $\sum_{i=0}^{m-1} a\alpha_{i+1}^0 e_i = 0$.
Donc $a\alpha_k^0 = 0$ pour tout $k = 1, \ldots, m$. Il en résulte que
$\alpha_k^0 \in J(C) = aC$ pour $k = 1, \ldots, m$.
La relation (2.2) implique que $a\alpha_0^0 \neq 0$ et α_0^0 est inversible.

Supposons maintenant que $f(e_i) = \sum_{j<i} \alpha_j^i e_j + \alpha_i^i + a\sum_{k>i} \alpha_k^i e_k$ avec α_i^i inversible pour tout $i \in \mathbb{N}$,
et soit $f(e_{i+1}) = \sum_{j<i+1} \alpha_j^{i+1} e_j + \alpha_{i+1}^{i+1} e_{i+1} + \sum_{k>i+1} \alpha_k^{i+1} e_k$.

D'après le Lemme 2.2.1, nous avons

$$a\sum_{j<i} \alpha e_j e_{j-1} + a\alpha_{i+1}^{i+1} e_i + a\sum_{k>i+1} \alpha_k^{i+1} e_{k-1} = a\sum_{j<i} \alpha_j^i e_j + a\alpha_i^i e_i. \tag{2.3}$$

Donc $a\alpha_k^{i+1} = 0$ pour tout $k \geq i+1$. Ce qui implique que $\alpha_k^{i+1} \in aC$.
Comme $a\alpha_{i+1}^{i+1} = a\alpha_i^i \neq 0$, alors α_{i+1}^{i+1} est inversible □

Lemme 2.2.3. *Pour tout $i \in \mathbb{N}$, $ae_i \in \operatorname{Im} f$.*

Démonstration. D'après le lemme 2.2.2, nous avons $f(e_0) = \alpha_0^0 e_0 + a\sum_{i\geq 1} \alpha_i^0 e_i$,
où α_0^0 est inversible. Par conséquent $f(ae_0) = af(e_0) = a\alpha_0^0 e_0$, donc
$ae_0 = (\alpha_0^0)^{-1} f(ae_0) = f[(\alpha_0^0)^{-1} ae_0] \in \operatorname{Im} f$

Supposons maintenant que $ae_k \in \operatorname{Im} f$ pour tout $k \leq i$.

D'après le lemme 2.2.2, nous avons

$$f(e_{i+1}) = \sum_{j\leq i} \alpha_j^{i+1} e_j + \alpha_{i+1}^{i+1} e_{i+1} + \sum_{k>i+1} \alpha_k^{i+1} e_{i+1}, \quad \text{avec} \quad \alpha_{i+1}^{i+1} \quad \text{inversible.}$$

Donc $f(ae_{i+1}) = af(e_{i+1}) = \sum_{j\leq i} a\alpha_j^{i+1} e_j + a\alpha_{i+1}^{i+1} e_{i+1}$. D'après l'hypothèse $\sum_{j\leq i} a\alpha_j^{i+1} e_j \in \operatorname{Im} f$. Donc $ae_{i+1} \in \operatorname{Im} f$ □

Lemme 2.2.4. *Pour tout $i \in \mathbb{N}$, $e_i \in \operatorname{Im} f$.*

Démonstration. D'après le lemme 2.2.2, nous avons

$$f(e_0) = \alpha_0^0 e_0 + a\sum_{k>0}\alpha_k^0 e_k \quad \text{avec} \quad \alpha_0^0 \quad \text{inversible.}$$

Il résulte du lemme 2.2.3 que $a\sum_{k>0}\alpha_k^0 e_k \in \operatorname{Im} f$. Donc $e_0 \in \operatorname{Im} f$.

Soit $i \in \mathbb{N}$. Supposons que $e_k \in \operatorname{Im} f$, pour tout $k \leq i$. Alors il résulte du lemme 2.2.2 que

$$f(e_{i+1}) = \sum_{j\geq i}\alpha_j^{i+1}e_j + \alpha_{i+1}^{i+1}e_{i+1} + a\sum_{j>i+1}\alpha_j^{i+1}e_j, \quad \text{où} \quad \alpha_{i+1}^{i+1} \quad \text{est inversible.}$$

D'après le lemme 2.2.3, nous avons $a\sum_{j>i+1}\alpha_j^{i+1}e_j \in \operatorname{Im} f$.

Donc $e_{i+1} = (\alpha_{i+1}^{i+1})^{-1}[f(e_{i+1}) - \sum_{j\leq i}\alpha_j^{i+1}e_j - a\sum_{j>i+1}\alpha_j^{i+1}e_j] \in \operatorname{Im} f$. □

La proposition suivante résulte des lemmes 2.2.1, 2.2.2, 2.2.3 et 2.2.4 :

Proposition 2.2.1. *Soit R un anneau commutatif artinien local. Si R possède un idéal non principal, alors il existe un R-module vérifiant la* propriété (I) *et qui n'est pas de type fini.*

Démonstration. Supposons que R est un anneau local avec radical de Jacobson $J(R) = aR + bR$. Dans ce cas, $a \neq 0$, $b \neq 0$ et $a^2 = ab = b^2 = 0$.

Considérons l'homomorphisme

$$\begin{aligned} \varphi : R = C \bigoplus bC &\longrightarrow \operatorname{End}_C M \\ \alpha + b\lambda &\mapsto \alpha id_M + \lambda\sigma, \end{aligned}$$

où $\alpha, \lambda \in C$ et id_M désigne l'homomorphisme identique du C-module $M = \bigoplus_{i\in\mathbb{N}} Ce_i$.

D'après φ, M a une stucture de R-module dont les endomorphismes sont les éléments f de $\operatorname{End}_C(M)$ vérifiant $f\sigma = \sigma f$. Il résulte alors des Lemmes 2.2.1, 2.2.2, 2.2.3 et 2.2.4 que le R-module M vérifie la propriété (I) et M n'est pas de type fini. □

2.3 Caractérisation des FGI-anneaux commutatifs

D'après le corollaire 2.1.1, si R est un FGI-anneau commutatif, alors le radical de Jacobson $J(R)$ est un nilidéal et R est semi-local. En particulier, tout idempotent de $R/J(R)$ se relève en un idempotent de R. Donc R est un anneau semi-parfait, c'est-à-dire c'est un produit direct fini d'anneaux locaux $R_1 \ldots, R_n$.

On sait qu'un produit d'anneaux commutatifs R_i $(1 \leq i \leq n)$ est un FGI-anneau si et seulement si chaque R_i, $(1 \leq i \leq n)$ est un FGI-anneau (proposition 1.1.2).

Donc nous supposons que R est un anneau local avec radical de Jacobson $J(R) = J$ (qui est un nilidéal). Notons S le R-module simple R/J et E l'enveloppe injective de S.

Rappelons qu'un R-module M est dit finiment annulé (noté f.a) s'il existe $m_1, \ldots, m_k \in M$ tel que $\mathrm{Ann}(M) = \mathrm{Ann}(m_1, \ldots, m_k)$, où
$\mathrm{Ann}(X) = \{a \in R : ax = 0, \forall x \in X\}$ (voir [5]).

Proposition 2.3.1. *Soit R un FGI-anneau local commutatif. Alors E est f.a.*

Démonstration. Comme E est un R-module indécomposable injectif, il vérifie la propriété (I). Donc il résulte de ([2], proposition 3.3) que E est f.a. □

Proposition 2.3.2. *Soit R un FGI-anneau commutatif local. Si N est un sous-module totalement invariant de E, alors N est f.a.*

Démonstration. Ceci résulte de ([2], propositions 3.3 et 3.4)

□

Théorème 2.3.1. *([5], théorème 2.7) Soit R un anneau avec radical premier N tel que tout sous-module de $E(R/N)$ est f.a. Les conditions suivantes sont équivalentes :*

1. *R est artinien à gauche.*
2. *Pour tout idéal premier P de R, R/P est artinien à gauche.*
3. *Tout R-module à gauche de type fini est f.a, et tout idéal premier de R est maximal.*

Démonstration. Voir [5]. □

Proposition 2.3.3. *Soit R un FGI-anneau local. Alors R est artinien.*

Démonstration. Cette proposition résulte de la proposition 2.3.2 et du théorème 2.3.1. □

Théorème 2.3.2. *Un anneau R est un FGI-anneau si et seulement si R est un anneau artinien à idéaux principaux.*

Démonstration. $\Longrightarrow$) Si R est FGI-anneau, alors d'après les propositions 2.2.1 et 2.3.3, R est anneau artinien à idéaux principaux.

$\Longleftarrow$) Si R est un anneau artinien à idéaux principaux, alors R est un FGI-anneau (voir proposition 2.1.2). □

Chapitre 3

CARACTERISATION DES *FGI*-DUO-ANNEAUX

Soit R un anneau non nécessairement commutatif possédant un élément unité $1 \neq 0$. R est dit duo-anneau si tout idéal à gauche ou à droite de R est bilatère. On dit qu'un R-module à gauche ${}_RM$ vérifie la propriété (I) si tout endomorphisme injectif de ${}_RM$ est un automorphisme de ${}_RM$. Un anneau R est dit un FGI-duo-anneau à gauche (à droite) si tout R-module à gauche (à droite) vérifiant la propriété (I) est de type fini. Un anneau R est un FGI-duo-anneau s'il est à la fois FGI-duo-anneau à gauche et FGI-duo-anneau à droite.

Soient ENS la catégorie des ensembles et $Vect_{\mathbb{K}}$ la catégorie des $\mathbb{K}$-espaces vectoriels avec $\mathbb{K}$ un corps. On dit qu'un objet X de ENS vérifie la propriété (I) si tout morphisme (application) injectif de X est bijectif. Dans ENS, la propriété (I) caractérise les ensembles finis. On dit qu'un objet V de $Vect_{\mathbb{K}}$ vérifie la propriété (I) si tout endomorphisme injectif de V est un automorphisme de V. Dans $Vect_{\mathbb{K}}$ la propriété (I) caractérise les $\mathbb{K}$-espaces vectoriels de dimension finie.

En général, dans la catégorie des R-modules à gauche R-Mod, la propriété (I) ne caractérise pas les R-modules de type fini. Par exemple pour l'anneau $\mathbb{Z}$ des entiers, le $\mathbb{Z}$-module $\mathbb{Q}$ des nombres rationnels vérifie la propriété (I) mais n'est pas de type fini. Pour $\mathcal{I}_{\mathcal{R}}$ la classe des R-modules à gauche vérifiant la propriété (I) et $\mathcal{F}_{\mathcal{R}}$ la classe des R-modules à gauche de type fini, W.V. VASCONCELOS a prouvé dans [29] pour un anneau commutatif R, que $\mathcal{F}_{\mathcal{R}} \subseteq \mathcal{I}_{\mathcal{R}}$. Mais en général cette inclusion est stricte. Par exemple le cas où $R = \mathbb{Z}$ l'anneau des entiers relatifs.

Dans le cas des FGI-anneaux commutatifs, M.BARRY, O. DIANKHA ET M. SANGHARÉ ont montré dans [2] que $\mathcal{F}_{\mathcal{R}} = \mathcal{I}_{\mathcal{R}}$.

Le but de ce chapitre constitué par [3], est de généraliser le chapitre 2 dans le cas des anneaux non nécessairement commutatifs, plus précisément les FGI-duo-anneaux. Nous avons montré pour un duo-anneau R, que tout R-module vérifiant la propriété (I) est de type fini si et seulement si R est artinien à idéaux principaux.

3.1 Définitions et caractérisations des FGI-duo-anneaux

Définition 3.1.1. *Un R-module à gauche M est dit finiment annulé (noté f.a) s'il existe $m_1, \ldots, m_n \in M$ tels que* $\mathrm{Ann}_R(M) = \mathrm{Ann}_R(m_1, \ldots, m_n)$

Proposition 3.1.1. *Si R est un FGI-duo-anneau, alors tout R-module de type fini est f.a*

Démonstration. Soient $\{m_1, \ldots, m_n\}$ est une famille génératrice de ${}_RM$, $\lambda \in \mathrm{Ann}_R(m_1, \ldots, m_n)$ et $m \in M$. Alors il existe $r_1, \ldots, r_n \in R$ tels que $m = r_1m_1 + \ldots + r_nm_n$. Il en résulte que $\lambda m = \lambda r_1 m_1 + \ldots + \lambda r_n m_n$.
Comme R est un FGI-duo-anneau, alors il existe $r'_1, \ldots, r'_n \in R$ tels que $\lambda m = r'_1 \lambda m_1 + \ldots + r'_n \lambda m_n = 0$.
Donc $\lambda \in \mathrm{Ann}_R(M)$ et $\mathrm{Ann}_R(M) = \mathrm{Ann}_R(m_1, \ldots, m_n)$. □

Proposition 3.1.2. *Soit R un FGI-duo-anneau et J un idéal de R.*
Posons $W = E(R/J)$ un R-module. Si ${}_RN$ est un sous-module à gauche de W globalement invariant, alors ${}_RN$ est de type fini.

Démonstration. Il suffit de montrer que ${}_RN$ vérifie la propriété (I).
Considérons

$$u :_R N \longrightarrow_R N \quad \text{un endomorphisme injectif de} \quad {}_RN$$

et $\tilde{u} : W \longrightarrow W$ tel que $\tilde{u}_{|N} = u$.
Montrons que $\tilde{u}$ est injectif.
Soit $x \neq 0$ un élément de W. Alors $Rx \cap N \neq 0$.
Donc il existe $r \in R$ tel que $rx \in N$.
Par conséquent $r\tilde{u}(x) = \tilde{u}(rx) = u(rx) \neq 0$.
Donc $\tilde{u}$ est injectif.

Vérifions que u est surjectif.

Soit $y \in N$. Alors il existe $x \in W$ tel que $\tilde{u}(x) = y$. Il en résulte que $x = \tilde{u}^{-1}(y) \in N$.

Donc u est surjectif et N vérifie la propriété (I). Il est donc de type fini. □

Définition 3.1.2. *Un sous-module N d'un R-module M est dit surperflu dans M si, pour tout sous-module L de M, la relation $N + L = M$ implique $L = M$.*
Soit P un R-module projectif. On dit que P est une enveloppe projective de M s'il existe un homomorphisme surjectif f de P sur M tel que ker f *soit surperflu dans P.*
On appelle anneau parfait à gauche, ou, simplement, parfait tout anneau R sur lequel tout module admet une enveloppe projective.

Lemme 3.1.1. *Soit R un FGI-duo-anneau. Si R est intègre, alors R est un anneau de division.*

Démonstration. Soit $K = S^{-1}R$ l'anneau de fractions de R, où S est l'ensemble de tous les éléments réguliers de R. Alors K est un R-module.
Soit $f : K \longrightarrow K$ une application R-linéaire. Comme f est R-linéaire, alors, pour tout $\frac{a}{s} \in K$ on a :

$$f(\frac{a}{s}) = \frac{a}{s} f(1).$$

Donc si $f(1) \neq 0$, alors f est bijectif et le R-module à gauche K vérifie la propriété (I). Par conséquent K est de type fini. Donc, il existe $\frac{a_1}{s_1}, ..., \frac{a_n}{s_n} \in K$ tels que :

$$K = \sum_{i=1}^{n} R\frac{a_i}{s_i}.$$

Comme $s_1^{-2}s_2^{-1}s_3^{-1}\dots s_n^{-1} \in K$, alors

$$s_1^{-2}s_2^{-1}\dots s_n^{-1} = \sum_{i=1}^{n} \lambda_i a_i s_i^{-1}, \quad \text{où} \quad \lambda_i,\ a_i \in R, \quad i = 1, \dots, n. \tag{3.1}$$

Posons $s_1^{-1} = \left(s_1^{-2}s_2^{-1}\dots s_n^{-1}\right) s_n s_{n-1}\dots s_2 . s_1$.

Il résulte de la relation (3.1) que

$$s_1^{-1} = \Big(\sum_{i=1}^{n} \lambda_i \; a_i \; s_i^{-1}\Big)\,(s_n \; s_{n-1} \;\; s_2 s_1)$$
$$= \sum_{i=1}^{n} \lambda_i \; a_i \; s_1^{-1} \; s_i \; \alpha, \quad \text{avec} \quad \alpha \in R \quad \text{et} \quad \sum_{i=1}^{n} \lambda_i \; a_i \alpha \in R.$$

Donc $s_1^{-1} \in R$.
De la même manière nous montrons que $s_i^{-1} \in R$ pour tout $i = 1, \ldots, n$.
Donc $K = R$ et R est un anneau de division. □

Proposition 3.1.3. *Soit R un FGI-duo-anneau, alors :*

1. *tout idéal premier de R est un idéal maximal,*
2. *R a un nombre fini d'idéaux premiers,*
3. *le radical de Jacobson $J(R)$ de R est un nilidéal.*

Démonstration. 1. Soit P un idéal premier de R. Alors l'anneau quotient R/P est un FGI-duo-anneau intègre. Soit B le corps des fractions de R/P. D'après le Lemme 3.1.1 B est un anneau de division. Par conséquent B vérifie la propriété (I) en tant que R/P-module. Alors B est de type fini. Donc $B = R/P$ et P est maximal.

2. Soit $\{P_\ell / \ell \in L\}$ l'ensemble des idéaux premiers de R.
   Pour tout $\ell \in L$, R/P_ℓ est un R-module simple. Si $\ell \neq m$, alors $\mathrm{Hom}\,(R/P_\ell \,; R/P_m) = \{0\}$. Donc le R-module $M = \bigoplus_{\ell \in L} R/P_\ell$ vérifie la propriété (I) et L est un ensemble fini.
3. Ceci résulte de 1) et 2).

□

Proposition 3.1.4. *Soit R un FGI-duo-anneau semi-simple premier, alors R est un anneau semi-simple artinien.*

Démonstration. D'après le 3) de la proposition 3.1.3, le radical de Jacobson $J(R)$ est :

$$J(R) = \bigcap_{p}^{n} P_i = \mathrm{rad}(R) = \{0\}.$$

Considérons

$$\varphi : R \longrightarrow \prod_{i=1}^{n} R/P_i$$
$$r \longrightarrow \varphi(r) = (\overline{r}^1, \overline{r}^2, \ldots, \overline{r}^n), \quad \text{où} \quad \overline{r}^i = r + p_i.$$

Alors φ est un homomorphisme d'anneaux.

$\varphi(r) = (\overline{0}, \ldots, \overline{0})$ implique que $r \in P_i$ pour tout $i \in \{1, 2, \ldots, n\}$.

Donc $r \in \mathrm{rad}(R)$. Par conséquent $r = 0$ et φ est injectif.

Soit $(\overline{s}_1, \ldots, \overline{s}_n) \in R/P_1 \times R/P_2 \times \ldots \times R/P_n$. Alors pour tout $i \neq j$, on a $P_i + P_j = R$.

Pour i fixé, pour tout $i \neq j$, il existe $\alpha_j \in P_j$, $\alpha_{i_j} \in P_i$ tels que $\alpha_j + \alpha_{i_j} = 1$. Donc

$$(\alpha_1 + \alpha_{i_1}) \times \ldots \times (\alpha_n + \alpha_{i_n}) = \alpha_i + \beta = 1,$$

où $\beta = \alpha_1 \times \alpha_2 \times \ldots \times \alpha_{i-1} \times \alpha_{i+1} \times \ldots \times \alpha_n$ et $\alpha_i = \prod_{k=1, k\neq i}^{n} \alpha_{i_k}$ sont des éléments de $\bigcap_{k=1, k\neq i}^{n} P_k$, $\alpha_i \in P_i$.

Donc nous avons :

$$P_i + \bigcap_{k=1, k\neq i}^{n} P_k = R \text{ pour tout } i, \quad 1 \leq i \leq n.$$

Soit $b_1, b_2, \ldots, b_n \in R$, cherchons $a \in R$ tels que :

$$a + P_i = b_i + P_i \quad \text{pour tout} \quad i = 1, 2, \ldots, n.$$

Nous savons que pour tout i, $1 \leq i \leq n$, il existe $\alpha_i \in P_i$ et $\beta_i \in \bigcap_{j\neq i} P_j$ tel que $\alpha_i + \beta_i = 1$.

Donc $\alpha_i + P_i = P_i$ implique $\overline{\alpha_i}^i = \overline{0}^i$ et $\alpha_i + \beta_i + P_i = \beta_i + P_i = 1 + P_i$.

Donc $\overline{\beta_i}^i = \overline{1}^i$ avec $\overline{\beta_i}^j = \overline{0}^j$ pour tout $j \neq i$.

Posons $a = b_1\beta_1 + b_2\beta_2 + \ldots + b_n\beta_n$, alors

$$a + P_i = b_1\beta_1 + b_2\beta_2 + \ldots + b_i\beta_i + b_{i+1}\beta_{i+1} + \ldots + b_n\beta_n + P_i.$$

Comme

$$b_1\beta_1 + b_2\beta_2 + \ldots + b_{i-1}\beta_{i-1}, \quad b_{i+1}\beta_{i+1} + \ldots + b_n\beta_n \in P_i,$$

alors

$$a + P_i = b_i\beta_i + P_i \quad \text{et} \quad \overline{a} = \overline{b_i\beta_i} = \overline{b_i}\,\overline{\beta_i}^{i} = \overline{b_i}\,\overline{1}^{i} = \overline{b_i}.$$

pour tout $i = 1, 2, \ldots, n$.

Donc

$$(\overline{a}, \overline{a}, \ldots, \overline{a}) = (\overline{b_1}, \ldots, \overline{b_n}) \quad \text{et} \quad R \cong \prod_{i=1}^{n} R/P_i.$$

Donc R est semi-simple artinien. □

Corollaire 3.1.1. *Si R est un FGI-duo-anneau, alors R est semi-parfait.*

Démonstration. Soit $J(R) = \text{rad}(R)$. Alors $J(R)$ est un nilidéal de R et $R/J(R)$ est un FGI-duo-anneau.

$$\text{rad}\,(R/J(R)) = \frac{\text{rad}(R)}{J(R)} = \{0\}$$

$R/J(R)$ est semi-premier puisque $J(R)$ est semi-premier. Donc R est semi-parfait. □

Corollaire 3.1.2. *Si R est un FGI-duo-anneau, alors R est isomorphe à un produit fini de FGI-duo-anneaux locaux.*

Démonstration. R est semi-parfait d'après la proposition 3.1.4 et le corollaire 3.1.1. □

Corollaire 3.1.3. *Tout FGI-duo-anneau local est un anneau de division.*

Démonstration. Ce corollaire résulte des proposition 3.1.3 et 3.1.4. □

Théorème 3.1.1. *Si R est un FGI-duo-anneau local, alors R est artnien.*

Démonstration. Ce théorème résulte de ([5], Prop 1.6 et du théorème 2.7). □

En combinant la proposition 3.1.1, la proposition 3.1.2 et ([5], Prop 1.6 et le théorème 2.7), nous obtenons le théorème suivant :

Théorème 3.1.2. *Si R est un FGI-duo-anneau, alors R est artinien.*

Remarque 3.1.1. *Soit R un duo-anneau local artinien avec radical de Jacobson $J(R)$, alors R est uniséríel ou $R/J(R)$ est un corps.*

Dans la suite R sera considéré comme un duo-anneau artinien local et $J(R) = J$, le radical de Jacobson de R vérifie $J^2 = 0$.
Il résulte de la remarque 3.1.1 que si R a un idéal non principal, alors R/J est un corps. Nous avons deux cas :

Cas 1 : R/J est un corps infini et $\dim(J/J^2) \geq 2$.

Comme R/J est infini, alors $R/J \setminus \{0\}$ est infini. Soit H l'ensemble des classes de représentants de $R/J \setminus \{0\}$. Alors H est un ensemble infini. Soit $h \in H$. Posons $I_h = R(x_1 - hx_2)$ où (x_1, x_2) est une base de $J/J^2 = J$ sur R/J et $M_h = R/I_h$. Alors M_h est un R-module.

Lemme 3.1.2. *Soit $h, h' \in H$. Si $h \neq h'$, alors $x_1 - hx_2 \notin I_{h'}$.*

Démonstration. L'hypothèse implique qu'il existe h et h' éléments de M_h tels que $x_1 - hx_2 = \alpha(x_1 - h'x_2)$. Alors $(1-\alpha)x_1 - (h - \alpha h')x_2 = \overline{0}$. Il en résulte que $1 - \alpha \in J$ et $h - \alpha h' \in J$.

Soit $m \in J$ tel que $\alpha = 1 - m$, alors $h - h' + mh' \in J$. Donc $h - h' \in J$ et $\bar{h} = \bar{h'}$. Ce qui contredit le choix de h et h'. □

Lemme 3.1.3. *Soient h et h' deux éléments de H tel que $h \neq h'$ et $g : M_h \longrightarrow M_{h'}$ une application R-linéaire. Alors $g\big(1 + I_h\big)$ n'est pas inversible dans l'anneau $M_h{}'$. Donc $g\big(1 + I_h\big) \in J/I_{h'}$.*

Notation : Nous notons un élément x_{M_h} de M_h par
$x_{M_h} = x + I_h$ où $x \in R$ et $h \in H$.

Démonstration. Nous avons :

$$\begin{aligned} 0_{M_{h'}} &= g\left(0_{M_h}\right) = g\left(x_1 - hx_2\right)_h \\ &= \left(x_1 - hx_2\right) g\left(1 + I_h\right). \end{aligned}$$

Comme $\left(x_1 - hx_2\right) g\left(1 + I_h\right) \in I_{h'}$, alors $g(1 + I_h) \in I_{h'}$ et $g(1 + I_h)$ est non inversible dans R. Par conséquent $g\left(1 + I_h\right) \in J$. Donc $g\left(1 + I_h\right) \in J/I_{h'}$. □

Corollaire 3.1.4. *Soit $f : \bigoplus_{h \in H} M_h \longrightarrow \bigoplus_{h \in H} M_h$ un endomorphisme du R-module $\bigoplus_{h \in H} M_h$. Si i_h et $p_{h'}$ sont respectivement l'injection canonique de M_h dans $\bigoplus_{h \in H} M_h$ et la projection canonique de $\bigoplus_{h \in H} M_h$ sur $M_{h'}$, alors $p_{h'} \circ f \circ i_h\left(1 + I_h\right) \in J/I_{h'}$.*

Notation :

$$M = \bigoplus_{h\in H} M_h \quad \text{où } M_h = R/I_h,\ x = \sum_{h\in H} \alpha_{h,h} e_h, \quad \alpha_{h,h} \in R, \quad e_h = 1 + I_h \in M_h$$

$$(e_h)\, f = \alpha_{h,h} e_h + \sum_{h\neq h'} \alpha_{h,h'} e_{h'} \quad \text{et} \quad \alpha_{h,h'}\, e_{h'} = (p_{h'} \circ f \circ i_h)(e_h).$$

Lemme 3.1.4. *Soit f un endomorphisme injectif de M. Alors pour tout $h \in H$, $(e_h)f = \beta_{h,h}\, e_h + \sum_{h'\neq h} \beta_{hh'} e_{h'}$ où $\beta_{h,h} \notin J$ et $\beta_{h,h'} \in J$.*

Démonstration. Soit $h \in H$. Si $h' \neq h$, alors d'après le Lemme 3.1.2

$$0_M \neq [(x_1 - h'x_2)\, e_h]\, f = (x_1 - h'x_2)\, (\beta_h, hp_h)\, f.$$

Il en résulte que $\beta_{h,h} \notin J$. □

Lemme 3.1.5. *Soit f un endomorphisme injectif de $M = \bigoplus_{h\in H} M_h$, alors $J \cdot M \subseteq \operatorname{Im} f$.*

Démonstration. Il suffit de démontrer que $\alpha e_h \in \operatorname{Im} f \quad \forall h \in H, \quad \forall \alpha \in J$. Nous avons :

$$\begin{aligned}(\alpha e_h)\, f &= \alpha \left[\beta_{h,h} e_h + \sum_{h'\neq h} \beta_{h,h'} e'_h\right] \\ &= \alpha\beta_{h,h} e_h \\ &= \beta'_{h,h} \alpha e_h \quad \text{comme } R \text{ est un duo-anneau.}\end{aligned}$$

Donc $\alpha e_h = {\beta'_{h,h}}^{-1} (\alpha e_h)\, f = \left({\beta'_{h,h}}^{-1} \alpha e_h\right) f \in \operatorname{Im} f$. □

Lemme 3.1.6. *Pour tout $h \in H$, on a $e_h \in \operatorname{Im} f$*

Démonstration.

$$\begin{aligned}(e_h)f &= \beta_{h,h} e_h + \sum_{h\neq h'} \beta_{h,h'} e_{h'} \\ &= \beta_{h,h} e_h + (V)\, f \quad \text{avec } (V)\, f = \sum_{h\neq h'} \beta_{h,h'}\, e_h \in Imf\end{aligned}$$

Donc $\beta_{h,h} e_h = (e_h - V)\, f$ et $e_h = \left[\beta_{h,h}^{-1} (e_h - V)\right] f \in \operatorname{Im} f$. □

Il résulte des lemmes 3.1.2, 3.1.3, 3.1.4, 3.1.5 et 3.1.6, le théorème suivant :

Théorème 3.1.3. *Soit R un FGI-duo-anneau local artinien d'idéal maximal J tel que $J^2 = 0$. Si R/J est un corps infini et $\dim_{R/J} J/J^2 \geq 2$, alors il existe un R - module M qui n'est pas de type fini et qui vérifie la* propriété (I).

Cas 2 : R/J est un corps fini et $\dim(J/J^2) = 2$.
Donc $R = B \oplus Bc$ où B est un sous anneau local de R, d'idéal maximal $Bb = J(B)$ qui est le radical de Jacobson de B et $b^2 = bc = cb = c^2 = 0$, $J = Bb \oplus Bc$.
Posons

$$M_R = R_R^{(\mathbb{N}*)} = \bigoplus_{i=1}^{\infty} e_i R \quad e_i = (\delta_{ij}) \qquad \text{où} \quad \delta_y = \begin{cases} 1, & \text{si} \quad i = j \\ 0, & \text{si} \quad i \neq j. \end{cases}$$

Soit l'application R - linéare

$$\begin{aligned} \sigma : M_R &\longrightarrow M_R \\ e_i &\mapsto \sigma(e_i) = \begin{cases} 0 & \text{si} \quad i = 1 \\ e_{i-1} & \text{si} \quad i \geq 2. \end{cases} \end{aligned}$$

Si $z \in R$, alors l'endomorphisme L_z de M_R défini par : pour tout $m \in M_R$ $L_z(m) = zm$.
Soit Λ le sous anneau de $End(M_R)$ engendré par $d = L_b \circ \sigma$ et les éléments L_x avec $x \in B$.
Considerons l'homomorphisme d'anneaux

$$\begin{aligned} R = B \oplus Bb &\longrightarrow \Lambda \\ x + yb &\mapsto L_x + l_y \circ d. \end{aligned}$$

Cet homomorphisme donne à M une structure de R - module à gauche défini par : $(x + yc) .m = (L_x + L_y \circ d)(m)$

Remarque 3.1.2.
- $\sigma \circ L_x = L_x \circ \sigma$.
- *pour tout $m \in M$, nous avons : $(d \cdot m)f = d(m)f$, où $d = \sigma \circ L_b$, $b \in B$.*

Lemme 3.1.7. *Pour tout $n \in \mathbb{N}^*$ nous avons :*

$$[d(e_n)]\, f = (be_{n-1})\, f \quad \textit{pour} \quad n \geq 2 \qquad \textit{et} \quad (d\ e_1)f = 0.$$

Démonstration. Nous avons :
$[d(e_n)]\, f = (b\sigma(e_n))f = (be_{n-1})f$. Et $[d(e_1)]f = (b\sigma(e_1))f = (b.0)f = 0$.
□

Lemme 3.1.8. *Pour tout $n \in \mathbb{N}^*$ nous avons :*

$(e_n)\ f = \sum_{k=1}^{\infty} \alpha_{k.n} e_k = \sum_{k<n} \alpha_{k,n} e_k + \alpha_{n,n} e_n + \sum_{k>n} \alpha_{k,n} e_k$ *où* $\alpha_{n,n}$ *inversible et* $\alpha_{k,n} \in J$ *pour tout* $k > n$.

Démonstration. Soit $(e_1)f = \alpha_{1,1}\, e_1 + \sum_{k>1} \alpha_{k,1}\, e_k$. Comme $be_1 \neq 0$ et f est injectif, alors $(b(e_1))f \neq 0$. Or $(b(e_1))f = b[(e_1)f] = b[\alpha_{11}\, e_1 + \sum_{k\geq 2} \alpha_{k,1}\, e_k]$.
Donc

$$b\ \alpha_{1,1}\ e_1 + \sum_{k>2} b\ \alpha_{k,1}\ e_k \neq 0. \tag{3.2}$$

Mais $\sigma[b\ e_1]f = b(\sigma(e_1))f = (0)\ f = \sum_{k>2} b\ \alpha_{k,1}\ e_{k-1}$.
Donc

$$0 = \sum_{k>2} b\ \alpha_{k,1}\ e_{k-1}. \tag{3.3}$$

Il résulte de (3.3) que si $b\alpha_{k,1} = 0$ pour tout $k \geq 2$, alors $\alpha_{k,1} \in J$.
D'après (3.2), comme $b\ \alpha_{11}\ e_1 \neq 0$, alors $\alpha_{1,1} \notin J$.
Considérons que :
$(e_n)\ f = \sum_{k<2} \alpha_{k,n}\ e_k + \alpha_{n,n}\ e_n + \sum_{k>2} \alpha_{k,n}\ e_k$ avec $\alpha_{n,n} \notin J$ et $\alpha_{k,n} \in J$ pour tout $k > n$.
Alors, nous avons

$$(e_{n+1})\ f = \sum_{k<n+1} \alpha_{k,n+1} + \alpha_{n+1,n+1} e_{n+1} + \sum k > n+1\ \alpha_{k,n+1}\ e_k.$$

D'après la remarque 3.1.2, $(L_b o\ \sigma)[(e_{n+1})]\ f = d[(e_{n+1})\ f] = [d(e_{n+1})]f$.
Donc

$$\begin{aligned} b(e_n)\ f &= b\left[\sum_{k<n} \alpha_{k+1,n+1}\ e_k + \alpha_{n+1,n+1} e_n + \sum_{k\geq n+1} \alpha_{k+1,n+1}\ e_k\right] \\ &= \sum_{k<n} b\ \alpha_{k+1,n+1}\ e_k + b\ \alpha_{n+1,n+1} e_n + \sum_{k\geq n+1} \alpha_{k,n+1}\ e_k. \end{aligned} \tag{3.4}$$

Mais

$$b[(e_n)\ f]\ =\ \sum_{k<n} b\ \alpha_{k,n}\ e_k\ +b\ \alpha_{n,n}\ e_n + \sum_{k\geq n} b\ \alpha_{k,n}\ e_k. \qquad (3.5)$$

D'après (3.4), (3.5) et les relations de récurrence, nous avons :

$$b\ \alpha_{n,n} = \ b\ \alpha_{n+1,n+1}.$$

Donc $\alpha_{n+1,n+1} \notin J$.
Comme $b\ \alpha_{k+1,n+1} = 0$ pour tout $k \geq n+1$, alors $\alpha_{k+1,n+1} \in J$. □

Lemme 3.1.9. *Pour tout* $n \in \mathbb{N}^*$, $\quad J \cdot e_n \subset \operatorname{Im} f$.

Démonstration. Posons $(e_1)\ f = \alpha_{11}e_1 + \sum_{k\geq 2}\alpha_{k,1}e_k$ où $\alpha_{11} \notin J$ et $\alpha_{k,1}\ \in J$ pour $k \geq 2$.
Soit $m \in J$, $\quad m = \alpha b + \beta c\ \ \alpha, \beta \in B$. Nous avons

$$\begin{aligned} m(e_1)\ f &= (L_{\alpha b} + L_\beta \circ d)[(e_1)\ f] \\ &= \ [(L_{\alpha b} + L_\beta od)(e_1)]\ f \\ &= (me_1)\ f \in \operatorname{Im} f. \end{aligned}$$

Comme R est un duo-anneau, il existe $\alpha'_{11} \in R$ tel que

$$m(e_1 f) = m\alpha_{11}e_1 = \alpha'_{11}me_1.$$

Il en résulte que $m\ e_1 = (\alpha'^{-1}_{11} m\ e_1)\ f \in \operatorname{Im} f$.
Supposons que $m\ e_s \in \operatorname{Im} f$ pour tout $s \leq n$. Alors, nous avons

$$\begin{aligned} (e_{n+1})f &= \sum_{k<n+1} \alpha_{k,n+1}e_k\ \ + \alpha_{n+1,n+1}e_{n+1} + \sum_{k>n+1} \alpha_{k,n+1}e_k \\ &= \ m[(e_{n+1})f] = (m\ e_{n+1})f \\ &= \sum_{k<n+1} m\alpha_{k,n+1}e_k\ \ + m\ \alpha_{n+1,n+1}e_{n+1} + m\sum_{k>n+1} \alpha_{k,n+1}e_k \\ &= \sum_{k<n+1} m\alpha_{k,n+1}e_k\ \ + m\ \alpha_{n+1,n+1}e_{n+1} \\ &= \sum_{k<n+1} m\alpha_{k,n+1}e_k\ \ + \alpha'_{n+1,n+1}me_{n+1}\ \ \text{où}\ \ m\alpha_{n+1,n+1} = \alpha'_{n+1,n+1}m. \end{aligned}$$

Comme $\sum_{k<n+1} m\ \alpha_{k,n+1}\ e_k \in \operatorname{Im} f$, alors $\alpha'_{n+1,n+1}\ m\ e_{n+1}\ = f(me_{n+1} - V)$.
Donc $m\ e_{n+1} = f\left[\alpha'^{-1}_{n+1,n+1}\ (m\ e_{n+1} - V)\right] \in \operatorname{Im} f$. □

Lemme 3.1.10. *Pour tout $n \in \mathbb{N}^*$, on a $e_n \in \operatorname{Im} f$.*

Démonstration. Posons $(e_1)\ f = \alpha_{11}\ e_1 + \sum_{k\geq 2} \alpha_{k,1} e_k$ $\alpha_n \notin J$ $\alpha_{k,1} \in J$ pour tout $k \geq 2$. D'après le Lemme 3.1.9, $\sum_{k\geq 2} \alpha_{k,1} e_k \in \operatorname{Im} f$. Donc

$$\alpha_{11}^{-1}\left((e_1)\ f - \sum_{k\geq 2} \alpha_{k,1}\ e_k\right) = e_1 \in \operatorname{Im} f.$$

Considérons $e_s \in \operatorname{Im} f$ pour tout $s \leq n$.

Nous avons $(e_{n+1})f = \sum_{k<n+1} \alpha_{k,n+1}\ e_k + \alpha_{n+1,n+1}\ e_{n+1} + \sum_{k>n+1} \alpha_{k,n+1}\ e_k$.

Comme $\sum_{k<n+1} \alpha_{k,n+1}\ e_k + \sum_{k>n+1} \alpha_{k,n+1}\ e_k \in \operatorname{Im} f$, alors

$$e_{n+1} = \left[\alpha_{n+1,n+1}^{-1}(e_{n+1} - u)\right]\ f \in \operatorname{Im} f \quad \text{où } f(u) = \sum_{k>n+1} \alpha_{k,n+1}\ e_k + \sum_{k<n+1} \alpha_{k,n+1}\ e_k.$$

□

Théorème 3.1.4. *Soit R un duo-anneau local arténien d'idéal maximal J tel que $J^2 = 0$. Si R/J est un corps fini et $\dim_{R/J}(J/J^2) = 2$, alors il existe un R-module qui vérifie la* propriété (I) *et qui n'est pas de type fini.*

Démonstration. Il résulte des Lemmes précédents. □

Théorème 3.1.5. *Soit R un duo-anneau, alors R est un FGI-duo-anneau si et seulement si R est artinien à idéaux principaux.*

Démonstration. [1) $\Rightarrow$ 2)] Ceci résulte des théorèmes 3.1.2, 3.1.3, et 3.1.4

[2) $\Rightarrow$ 1)] Ceci résulte de [25]. □

Chapitre 4

Sur les I_1-modules et les I-modules

Ce chapitre est constitué essentiellement par [11] et [12]. Nous introduisons ici, en utilisant la catégorie $\sigma[M]$ introduite par R. WISBAUER dans [30], la notion de I_1-module et de I-module qui généralise celle de I-anneau introduite dans [17]. Nous étudions les propriétés des I_1-modules, des I-modules et donnons d'abord une caractérisation complète des I_1-groupes abéliens (théorème 4.1.1) et des I_1-modules de type de représentation sérielle (théorème 4.1.2) et ensuite des I-modules de type fini sur un duo-anneau.

Dans ce chapitre, sans aucune autre précision, le mot anneau désigne un anneau associatif, non (nécessairement) commutatif, d'élément unité $1 \neq 0$; le mot module, désigne un module à gauche. Soit R un anneau. On désigne par R-Mod (resp. Mod-R) la catégorie des R-modules à gauche (resp. à droite). On utilisera la notation M_R pour dire que M est un R-module à droite. Soient M et N deux R-modules. On dit que N est *engendré* par M, s'il existe un ensemble Λ et un épimorphisme $f : M^{(\Lambda)} \longrightarrow N$. Un R-module K est *sous-engendré* par M si K est un sous-module d'un module engendré par M. On note $\sigma[M]$ la sous-catégorie pleine de la catégorie R-Mod, dont les objets sont les R-modules sous-engendrés par M. Si R est un anneau, alors $\sigma[R] = R$-Mod. On dit qu'un R-module M vérifie la propriété (I) si tout endomorphisme injectif de M est un automorphisme de M. Un R-module projectif de type fini générateur dans $\sigma[M]$ est appelé *progénérateur* dans $\sigma[M]$. Un R-module est dit *uniséríel* si le treillis de ses sous-modules est une chaîne; *sériel* s'il est somme directe de modules uniséríels, et de *type de représentation sérielle* si tout module de $\sigma[M]$ est sériel. Si M est de lon-

gueur finie et si dans $\sigma[M]$ il existe seulement un nombre fini de modules indécomposables non isomorphes deux à deux, on dira que M est de *type de représentation finie.* Si $n \in \mathbb{N}^*$, alors $\mathbb{Z}_n$ désigne l'anneau des entiers modulo n.

4.1 Sur les I_1-modules

Nous rappelons qu'un R-module M est dit un I_1-module, si tout module de $\sigma[M]$ vérifiant la propriété (I) est de longueur finie.

4.1.1 I_1-groupes abéliens

Théorème 4.1.1. *Soit G un groupe abélien. les conditions suivantes sont équivalentes :*

(a) *G est un I_1-groupe.*

(b) *Il existe un nombre fini d'entiers positifs $p_1 < p_2 < \ldots < p_n$ tels que tout groupe abélien M appartenant à $\sigma[G]$ s'écrit sous forme*

$$M = \bigoplus_{i=1}^{n} M_{p_i}, \quad \text{où pour tout } i,\ 1 \leq i \leq n,\ M_{p_i} \quad \text{est somme directe}$$

de p_i-groupes cycliques.

Démonstration. $(a) \Longrightarrow (b)$ Soit $x \in G$. Désignons par $\langle x \rangle$ le sous-groupe de G engendré par x. Alors $\sigma[\langle x \rangle]$ est une sous-catégorie pleine de $\sigma[G]$, et, par conséquent, $\langle x \rangle$ est un I_1-groupe. Soit $n \in \mathbb{N}$ tel que $\langle x \rangle \equiv \mathbb{Z}_n$. Alors $\sigma[\langle x \rangle] = \sigma[\mathbb{Z}_n] = \mathbb{Z}_n - \text{Mod}$. Comme $\mathbb{Z}$ n'est pas un I_1-anneau (voir [17]), on a $n \geq 1$. Il résulte que x est un élément de torsion, ce qui montre que G est un groupe de torsion. Soit

$$G = \bigoplus_{p \in P} G_p$$

la décomposition primaire de G, où P est un ensemble d'entiers premiers positifs; et $G_p \neq \{0\}$ la composante p-primaire de G. Pour tout $p \in P$, soit z_p un élément de G_p tel que $\langle z_p \rangle \equiv \mathbb{Z}$. Alors le groupe $\langle z_p \rangle$ est un élément de $\sigma[G]$, il vérifie la propriété (I). Donc

$$H = \bigoplus_{p \in P} \mathbb{Z}_p$$

est de longueur finie. Par conséquent P est fini. Soit M un élément de $\sigma[G]$. Comme $\sigma[M]$ est une sous-catégorie pleine de $\sigma[G]$, M est un I_1-groupe, donc d'après ce qui précède, M est un groupe de torsion.

Soient $p_1 < p_2 < \ldots < p_n$ les éléments de P et soit M_{p_i} pour tout entier i $(1 \leq i \leq n)$, la composante p_i-primaire de M. Alors

$$M = \bigoplus_{i=1}^{n} M_{p_i} \quad \text{pour tout } i \in \{1, 2, 3, \ldots, n\}.$$

Désignons par B_i le sous-groupe de base de M_{p_i}. Comme le groupe quotient divisible M_{p_i}/B_i est un élément de $\sigma[M]$ et vérifie la propriété (I), alors le quotient M_{p_i}/B_i est réduit à l'élément neutre. Par conséquent M_{p_i} est somme directe de p_i-groupes cycliques.
$(b) \Longrightarrow (a)$ Soit

$$N = \bigoplus_{i=1}^{n} N_{p_i}$$

un élément de $\sigma[G]$ vérifiant la propriété (I). Alors, pour tout i, $(1 \leq i \leq n)$ N_{p_i}, qui est somme directe de p_i-groupes cycliques, est nécessairement de longueur finie. Il en résulte que N est de longueur finie. □

4.1.2 I_1-modules

Proposition 4.1.1. *Soit M un R-module. Si M est un I_1-module, alors l'enveloppe M-injective de tout module uniforme appartenant à $\sigma[M]$ est de longueur finie.*

Démonstration. Soit U un module uniforme de $\sigma[M]$ et soit U_1 l'enveloppe M-injective de U. Pour montrer que U_1 est de longueur finie, il suffit de montrer qu'il vérifie la propriété (I). Soit f un endomorphisme injectif de U_1. Désignons par $\widehat{U}$ l'enveloppe injective dans R-Mod de U et $\tilde{f}$ un endomorphisme de $\widehat{U}$ prolongeant f. Comme $\widehat{U}$ est un R-module injectif indécomposable, alors $\tilde{f}$ est un automorphisme de $\widehat{U}$. Soit y un élément de U_1 et $x \in \widehat{U}$ tel que $\tilde{f}(x) = y$. On va montrer que $x \in U_1$.
Comme $U_1 = \text{trace}(M, \widehat{U}) = \sum \left\{ \text{Im}h \quad / \, h \in \text{Hom}(M, \widehat{U}) \right\}$, il existe

$m_1, m_2, \ldots, m_n \in M$ et $h_1, h_2, \ldots, h_n \in \text{Hom}(M, \widehat{U})$ tels que $\sum_{i=1}^{n} h_i(m_i) = y$.

Posons $g = (f')^{-1}$. On a

$$\sum_{i=1}^{n} g \circ h_i(m_i) = g\left(\sum_{i=1}^{n} h_i(m_i)\right) = g(y) = x.$$

Il résulte que $x \in U_1$. Par conséquent f est un automorphisme de U_1. Ainsi U_1 vérifie la propriété (I) et il en résulte que U_1 est de longueur finie. □

Proposition 4.1.2. *Soit M un R-module. Si M est un I_1-module, alors :*

1. *Dans $\sigma[M]$ il existe un nombre fini de modules simples non isomorphes deux-à-deux.*
2. *Dans $\sigma[M]$ il existe un cogénérateur injectif de longueur finie W tel que :*
   (i) *$B = \mathrm{End}_R(W)$ est un anneau artinien à droite,*
   (ii) *W_B est un cogénérateur injectif de* $\mathrm{Mod} - B$,
   (iii) *les foncteurs* $\mathrm{Hom}_R(-, W)$ *et* $\mathrm{Hom}(-, W_B)$ *définissent une dualité entre les modules de type fini de $\sigma[M]$ et les modules de type fini de* $\mathrm{Mod} - B$.

Démonstration. 1. Soit L l'ensemble des modules simples non isomorphes deux-à-deux et appartenant à $\sigma[M]$. Alors le module $N = \bigoplus_{S \in L} S$ appartient à $\sigma[M]$ et vérifie la propriété (I), donc N est de longueur finie et, par conséquent, L est un ensemble fini.

2. Soit S_1, S_2, ..., et S_n des représentants des classes d'isomorphie des modules simples de $\sigma[M]$. D'après la proposition 4.1.1, leurs enveloppes M-injectives $\widehat{S_1}$, $\widehat{S_2}$, ..., et $\widehat{S_n}$ sont de longueur finie. Il en résulte que $W = \sum_{i=1}^{n} \widehat{S_i}$ est un cogénérateur injectif de $\sigma[M]$, donc (i), (ii), et (iii) résultent de [30], Lemme 1.2.

□

Théorème 4.1.2. *Soient R un anneau dont tout idéal à gauche ou à droite est bilatère et M un R-module de type de représentation sérielle. On suppose que $\sigma[M]$ admet un progénérateur. Alors les conditions suivantes sont équivalentes :*

1. *M est un I_1-module.*

2. M est de type de représentaion finie.

Démonstration. 1) $\Longrightarrow$ 2) Soit Q un progénérateur de $\sigma[M]$ et soit $X \in Q$. On a $\sigma[RX] = R/I - \text{Mod}$, où $I = \text{Ann}(X)$. Comme le R-module RX est un I_1-module, il en résulte que l'anneau quotient R/I est un I_1-anneau. Donc d'après [26], R/I est un anneau sériel et artinien. Ce qui implique que le R-module RX est de longueur finie. Q étant un R-module de type fini, on en déduit que Q est de longueur finie. Il résulte donc de [30] que $\sigma[M] = \sigma[Q]$ et M est de type de représentation finie.
2) $\Longrightarrow$ 1) est évident. □

4.2 Sur les I-modules

Soient R un duo-anneau et M un R-module. On dit que M vérifie la propriété (I) (ou M est co-Hopfien), si tout R-endomorphisme injectif de M est un R-automorphisme de M. Dans cette section, constituée par [11], nous étudions pour un anneau fixé R, les R-modules à gauche (resp. à droite) M pour lesquels tout objet de $\sigma[M]$ vérifiant la propriété (I) est artinien. De tels modules sont appelés I-modules à gauche (resp. I-modules à droite). Nous donnons quelques propriétés de I-modules et caractérisons les I-modules de type fini fidèlement équilibrés sur R. On désigne par $\text{Gen}(M)$, la classe des modules engendrés par M.

Proposition 4.2.1. *1. L'image homomorphe d'un I-module est un I-module.*

2. (i) *Si un produit de I-modules M_i, $1 \leq i \leq n$ est un I-module, alors chaque M_i est un I-module.*
(ii) *Cependant, si $\text{Hom}(M_i, M_j) = 0$ pour tout $i \neq j$, $1 \leq i, j \leq n$, l'inverse de (i) est vraie.*

Démonstration. 1. Soit M un I-module, $M' = f(M)$ image homomorphe de M, alors $\text{Gen}(M')$ est incluse dans $\text{Gen}(M)$ (voir [1]). Ce qui implique que $\sigma[M']$ est une sous-catégorie pleine de $\sigma[M]$. Par conséquent M' est un I-module.

2. (i) Ceci résulte de 1)
(ii) Supposons que chaque M_i, pour tout $1 \leq i \leq n$, est un I-module.

Comme $\mathrm{Hom}(M_i, M_j) = 0$ pour tout $i \neq j$, $1 \leq i,\ j \leq n$, alors, d'après [28], pour tout $N \in \sigma[\prod_{i=1}^{n} M_i]$, il existe un unique $N_i \in \sigma[M_i]$ pour tout i, $1 \leq i \leq n$ tel que $N = \prod_{i=1}^{n} N_i$.

Si N vérifie la propriété (I), alors N_i la vérifie. Donc N_i est artinien. Par conséquent N est artinien et M est un I-module.

□

Un R-module M est dit *localement* de longueur finie, si tout sous-module de type fini de M est de longueur finie.

Proposition 4.2.2. *Soit M un R-module. Si M est un I-module, alors M est localement de longueur finie.*

Démonstration. Soit N un sous-module de M et $\{m_1, m_2, \ldots, m_k\}$ un sous-ensemble générateur de N.

Comme $\sigma[Rm_i]$ est une sous-catégorie pleine de $\sigma[M]$ pour tout i, $1 \leq i \leq n$, alors Rm_i est un I-module. Donc, il est artinien. Par conséquent Rm_i est de longueur finie pour tout i, $1 \leq i \leq n$.

Donc N est de longueur finie et M est localement de longueur finie. □

Proposition 4.2.3. *Soit M un R-module de type fini. Si M est un I-module, alors :*

1. *Il existe dans $\sigma[M]$ un nombre fini de modules simples non isomorphes.*
2. *Il existe un cogénérateur injectif de longueur finie W tel que :*
   (i) *$S = \mathrm{End}({}_RW)$ est anneau artinien à gauche,*
   (ii) *W_S est un cogénérateur injectif dans* $\mathrm{Mod} - S$,
   (iii) *Les foncteurs* $\mathrm{Hom}_{(-,R}W)$ *et* $\mathrm{Hom}_{(-}, W_S)$ *définissent une dualité entre les R-modules de type fini dans $\sigma[M]$ et* $\mathrm{Mod} - S$.

Démonstration.

1. Soit L un ensemble de modules simples non isomorphes dans $\sigma[M]$. Alors le sous-module $N = \bigoplus_{S \in L} S \in \sigma[M]$ et il vérifie la propriété (I). Donc N est artinien. Par conséquent L est fini.
2. Soit $S_1, S_2, \ldots, S_k$ un système de représentants de la classe des modules simples isomorphes deux-à-deux dans $\sigma[M]$. Alors les enveloppes M-injectives $\tilde{S}_1, \tilde{S}_2, \ldots, \tilde{S}_k$ sont de type fini dans $\sigma[M]$. Donc ils sont

de longueur finie .(voir Proposition 4.2.2 et [30]). Il en résulte que $W = \bigoplus_{i=1}^{k} \tilde{S}_i$ est un cogénérateur injectif de longueur finie dans $\sigma[M]$ et (i), (ii), (iii) résulte de [30], Lemme 1.2.

□

Théorème 4.2.1. *1. Si M est un module de type fini sur un anneau commutatif R, alors les conditions suivantes sont équivalentes.*
(i) *M est un I-module.*
(ii) *M est de longueur finie et tout sous-module de M est cyclique.*
(iii) *M est de de type de représentation finie.*

2. Si M est un module à gauche fidèlement équilibré sur un duo-anneau R, alors les conditions suivantes sont équivalentes
(a) *M est un I-module à gauche.*
(b) *M est de type de représentation finie.*
(c) *M est I-module à droite.*
(d) *M est uniséríel.*
(e) *M est de longueur finie et tout sous-module de M est cyclique.*

Démonstration. 1. Soit $\{m_1, m_2, \ldots, m_k\}$ un sous-système générateur de M. Considérons l'homomorphisme

$$\psi : R \to R(m_1, m_2, \ldots, m_k),$$

alors

$$\ker \psi = \mathrm{Ann}(M)$$

est un idéal de R, et M est isomorphe à $R/\mathrm{Ann}(M)$. Comme $R/\mathrm{Ann}(M)$ est un anneau commutatif, alors 1) résulte de [17], Théorème 8.

2. Désignons par $S = \mathrm{End}(_RM)$, l'anneau des endomorphismes de M.
Si M est un R-module, alors M est un S-module.
Donc, il résulte de [31] que $\sigma[M] = R/\mathrm{Ann}(M)$−Mod. Comme $R/\mathrm{Ann}(M)$ est un duo-anneau et que M est isomorphe à $R/\mathrm{Ann}(M)$, alors 2) résulte de [13], Théorème 3.3.

□

Théorème 4.2.2. *Soit M un module sur un duo-anneau R tel que $M = \bigoplus_{\Lambda} M_\lambda$ et pour tous $\lambda, \mu \in \Lambda$ distincts, $\sigma[M_\lambda] \cap \sigma[M_\mu] = 0$. Alors M est un I-module si et seulement si M est sériel.*

Démonstration. Supposons que M est un I-module et considérons l'application canonique

$\pi_\mu : M = \bigoplus_{\lambda\in\Lambda} M_\lambda \longrightarrow M_\mu$, alors d'après la proposition 4.2.1, M_μ est un I-module pour tout $\mu \in \Lambda$. Par conséquent, il résulte du Théorème 4.2.1 que M_μ est uniséríel. Donc M est sériel.

Réciproquement, On sait que M_λ est un I-module (voir Théorème 4.2.1).

Posons $N \in \sigma[M]$. Comme $\sigma[M_\lambda] \cap \sigma[M_\mu] = \{0\}$ pour tous $\lambda, \mu \in \Lambda$, alors d'après [28], il existe un unique objet $N_\lambda \in \sigma[M_\lambda]$ tel que $N = \bigoplus_{\Lambda} N_\lambda$. Comme N vérifie la propriété (I), alors N_λ est artinien puisqu'il vérifie la propriété (I). Donc N est artinien et M est un I-module. □

Chapitre 5

SUITES RECURRENTES LINEAIRES SUR UN CORPS FINI : Théorie et Applications

Introduction

Les suites récurrentes linéaires sont nées en 1202 avec l'exemple donné par FIBONACCI de la suite $1, 1, 2, 3, 5, 8, 13, \ldots$. De ce fait une littérature très abondante leur a été consacrée et il est pratiquement impossible de réaliser une bibliographie à peu près complète sur ce sujet.

Les suites récurrentes linéaires interviennent dans divers domaines théoriques et pratiques. Elles apparaissent d'abord comme un objet fondamental en théorie des langages. L'étude de la période d'une suite récurrente linéaire à valeurs dans un corps fini est un problème essentiel. On peut utiliser ces suites dans le domaine des communications (théorie des codes, cryptographie, etc ...). Elles correspondent au fonctionnement des régistres à décalage (shift-registers en anglais).

Le but de ce chapitre est de faire des études théoriques et des applications sur ces suites. Pour cela, nous donnons d'abord quelques propriétés caractéristiques de ces suites, ensuite nous étudions quelques polynômes et suites récurrentes linéaires modulo un nombre premier et enfin la relation entre l'ordre d'une suite récurrente linéaire et l'ordre de son polynôme caractéristique. Nous étudions aussi le degré de la plus petite extension d'un corps K dans laquelle un polynôme se factorise complètement et nous mon-

trons que le logarithme de ce degré est "en général" majoré par $\frac{1}{2}\log^2 n + \frac{66}{7}(\log n)^{7/4}$ où n est le degré du polynôme compagnon de la suite.

Et enfin, nous donnons des généralités sur les suites aléatoires et pseudo-aléatoires (générées par les suites récurrentes linéaires) qui établissent une connection entre les suites récurrentes linéaires et la cryptograghie ou la théorie des codes.

5.1 Définitions et Propriétés

Ce paragraphe contient des définitions et des résultats classiques et récents que nous utiliserons dans les parties suivantes.

Définition 5.1.1. *Soit R un anneau. Une suite $u_0, u_1, \ldots$ est dite récurrente linéaire d'ordre k sur R s'il existe $r_0, r_1, \ldots, r_{k-1} \in R$ tels que*

$$u_{n+k} = r_{k-1}u_{n+k-1} + r_{k-2}u_{n+k-2} + \cdots + r_0 u_n \quad \textit{pour} \quad n = 0, 1, 2, \ldots \quad (5.1)$$

alors $f(x) = x^k - r_{k-1}x^{k-1} - r_{k-2}x^{k-2} - \ldots - r_0$ est appelé le polynôme caractéristique de la suite $u_0, u_1, \ldots$ et $(u_0, u_1, \ldots, u_{k-1})$ est son vecteur inital.

Les termes $u_0, u_1, \ldots$ de la suite sont uniquement déterminés par la condition initiale.

Définition 5.1.2. *Soit S un ensemble non vide et $u_0, u_1, \ldots$ une suite d'éléments de S. S'il existe des entiers r et n_0 avec $r \geq 1$, tels que $u_{n+r} = u_n$ pour tout $n \geq n_0$, alors la suite $u_0, u_1, \ldots$ est dite ultimement périodique. La plus petite période parmi toutes les périodes possibles d'une suite ultimement périodique est appelée la période de la suite.*

Lemme 5.1.1. *Toute période d'une suite ultimement périodique est divisible par la période de la suite.*

Démonstration. Soient t une période arbitraire de suite ultimement périodique, $u_0, u_1, \ldots$ et t_1 la période de cette suite, alors on a $u_{n+t} = u_n$ pour tout $n \geq n_0$ et $u_{n+t_1} = u_n$ pour $n \geq 0$.

Supposons que t_1 ne divise pas t, alors il existe des entiers q et r tels que $t = qt_1 + r$ avec $0 \leq r < t_1$. Ce qui implique que (pour n assez grand)

$$u_{n+t} = u_n = u_{n+qt_1+r} = u_{n+(q-1)t_1+r} = \ldots = u_{n+r}$$

Par conséquent r est une période de la suite u_0, u_1, ... Contradiction avec la définition de t_1. Donc $r = 0$ et t_1 divise t. □

Définition 5.1.3. *Une suite u_0, u_1, ... est dite périodique s'il existe un entier positif t tel que $u_{n+t} = u_n$ pour $n = 0, 1, 2, \ldots$ et t est une période de la suite.*

Soit R un anneau. Considérons l'application $\varphi : \mathbb{Z} \to R, \quad n \mapsto nr$, $r \in R$, alors $\operatorname{Ker}\varphi$ est un idéal de $\mathbb{Z}$. Donc il existe un entier n tel que $\operatorname{Ker}\varphi = n\mathbb{Z}$.

Par définition, on appelle caractéristique de R (noté caract(R)), le plus petit entier positif n tel que $\operatorname{Ker}\varphi = n\mathbb{Z}$ (comme $R \neq \{0\}$, on a $n = 0$ ou $n \geq 2$).

Lemme 5.1.2. *Un anneau intègre unitaire non nul R de caractéristique positive est nécessairement de caractéristique première.*

Lemme 5.1.3. *Soit E un ensemble fini et soient*

$$f : E \longrightarrow E$$

une application et (x_n) une suite telle que $x_{n+1} = f(x_n)$ pour tout $n \geq 0$, alors la suite (x_n) est ultimement périodique, ie $x_{n+t} = x_n$ pour $t \geq l$ avec $t + l \leq \operatorname{card}(E)$.

Remarque 5.1.1. *Soit u_0, u_1, ... une suite récurrente linéaire qui vérifie la relation*

$$u_{n+h} = r_1 u_{n+h-1} + r_2 u_{n+h-2} + \cdots + r_h u_n \quad \text{pour} \quad n = 0, 1, 2, \ldots \tag{5.2}$$

Posons $U_n = (u_n, u_{n+1}, \ldots, u_{n+h-2}, u_{n+h-1}) \in R^h$. Alors on associe à cette suite la matrice A d'ordre $h \times h$ sur R définie par :

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & r_h \\ 1 & 0 & 0 & \ldots & 0 & r_{h-1} \\ 0 & 1 & 0 & \ldots & 0 & r_{h-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & r_1 \end{pmatrix}.$$

Alors nous avons

$$U_{n+1} = U_n A \quad \text{pour } n = 0, 1, 2, 3, \ldots$$

et donc $U_n = U_0 A^n$ avec $U_0 = (u_0, u_1, \ldots, u_{h-1})$.

Lemme 5.1.4. *Soit u_0, u_1, ... une suite récurrente linéaire d'ordre h sur un anneau satisfaisant la relation (5.2) avec $r_h \neq 0$, alors l'ordre de la suite (u_n) divise l'ordre de la matrice associée à (u_n).*

Démonstration. Comme $\det(A) = (-1)^{h-1} r_h \neq 0$, alors si $s = \mathrm{ord}(A)$ est fini, d'après [20] nous avons

$$U_{n+s} = U_0 A^{n+s} = U_0 A^n \times A^s = U_0 A^n = U_n \quad \text{pour} \quad n \geq 0.$$

Donc s est une période de (u_n). Il résulte du Lemme 5.1.1 que l'ordre de la suite divise s. □

Théorème 5.1.1. *Soient R un anneau et (u_n) une suite récurrente linéaire sur R définie par la relation (5.2) et telle que $I = \mathrm{Im}(u)$ soit finie, alors*

1. *(u_n) est ultimement périodique*
2. *si r_h est non diviseur de zéro, alors (u_n) est purement périodique.*

Démonstration. Posons $I = \mathrm{Im}(u)$, l'image de u, avec

$$I \subseteq R \quad \text{et} \quad I^h \subseteq R^h.$$

Considérons l'application

$$\varphi : I^h \longrightarrow I^h, \quad U_n \mapsto U_{n+1}.$$

1. Comme I^h est fini, il résulte du Lemme 5.1.3 que la suite (U_n) est ultimement périodique, donc la suite (u_n) l'est aussi.
2. On sait que (u_n) est ultimement périodique. Soit t la période minimale et n_0 tel que

   $$u_{n+t} = u_n \quad \text{pour} \quad n \geq n_0.$$

   Si $n_0 = 0$, le résultat est démontré. Sinon, d'après l'hypothèse, "le futur" de la suite détermine un terme précédent, on a plus précisément

   $$r_h u_{n_0-1} = u_{n_0+h-1} - r_1 u_{n_0+h-2} - \ldots - r_{h-1} u_n$$

   et

   $$r_h u_{n_0+t-1} = u_{n_0+h-1} - r_1 u_{n_0+h-2} - \ldots - r_{h-1} u_n.$$

   Donc $r_h(u_{n_0-1} - u_{n_0+t-1}) = 0$. Comme r_h est non diviseur de zéro, alors $u_{n_0-1} = u_{n_0+t-1}$ pour tout $n_0 \geq 0$. Ce qui contredit la définition de la prépériode n_0.
   Donc $n_0 = 0$ et la suite est périodique.

□

Théorème 5.1.2. *(théorème fondamental des suites récurrentes linéaires) Soit (u_n) une suite à valeurs dans un corps K. Alors les conditions suivantes sont équivalentes :*

1. *La suite vérifie la relation de la forme*

$$u_{n+h} = r_{h-1}u_{n+h-1} + r_{h-2}u_{n+h-2} + \ldots + r_0 u_n,$$

où les r_h sont des éléments de K et $r_0 \neq 0$.

2. *La fonction caractéristique de la suite (u_n), à savoir*

$$U(X) = \sum_{n=0}^{\infty} u_n X^n,$$

est une fonction rationnelle de la forme

$$U_(X) = \frac{P(X)}{Q^*(X)},$$

où $P(X)$ et $Q(X)$ sont des polynômes à coefficients dans K, avec $\deg(P) < h$, $Q(X) = X^h - r_{h-1}X^{h-1} - r_{h-2}X^{h-2} - \ldots - r_0$ est le polynôme caractéristique de la suite et $Q^*(X) = X^h Q(1/X)$ est le polynôme réciproque de Q.

3. *Les (u_n) sont donnés par une formule de la forme*

$$u_n = \sum_{i=1}^{k} \sum_{j=1}^{r_i} \beta_{ij} \binom{n+j-1}{j-1} \alpha_i^n,$$

où les β_{ij}, α_i^n sont des éléments d'une extension L de K et où

$$Q(X) = \prod_{i=1}^{k} (X - \alpha_i)^{r_i},$$

en fait on peut prendre $L = K[\alpha_1, \alpha_2, \ldots, \alpha_k]$.

Démonstration. 1) $\Longrightarrow$ 2)
Soit (u_n) une suite récurrente linéaire vérifiant une relation comme en 1). Considérons la fonction génératrice associée $U(X) = \sum_{n=0}^{\infty} u_n X^n$. Alors,

$$\sum_{n=0}^{\infty} u_n X^n = \sum_{n=0}^{h-1} u_n X^n + \sum_{n=h}^{\infty} \left(r_{h-1}u_{n-1} + r_{h-2}u_{n-2} + \ldots + r_0 u_{n-h}\right) X^n$$

$$= \sum_{n=0}^{h-1} u_n X^n + r_{h-1} \sum_{n=h-1}^{\infty} u_n X^{n+1} + r_{h-2} \sum_{n=h-2}^{\infty} u_n X^{n+2} + \ldots + r_0 \sum_{n=0}^{\infty} u_n X^{n+h}$$

$$= \sum_{n=0}^{h-1} u_n X^n - \left(r_{h-1} \sum_{n=0}^{h-2} u_n X^{n+1} + r_{h-2} \sum_{n=0}^{h-3} u_n X^{n+2} + \ldots + r_1 u_0 X^{h-1} \right) +$$

$$\left(r_{h-1}X + r_{h-2}X^2 + \ldots + r_0 X^h\right) U(X).$$

D'où la relation

$$U(X) = \frac{P(X)}{Q^*(X)},$$

avec

$$P(X) = \sum_{n=0}^{h-1} u_n X^n - \left(r_{h-1} \sum_{n=0}^{h-2} u_n X^{n+1} + r_{h-2} \sum_{n=0}^{h-3} u_n X^{n+2} + \ldots + r_1 u_0 X^{h-1} \right)$$

et

$$Q^*(X) = 1 - r_{h-1}X - r_{h-2}X^2 - \ldots - r_0 X^h.$$

Ce qui démontre l'implication.

2) $\Longrightarrow$ 3)

On décompose la fraction rationnelle $U(X)$ en éléments simples dans $K[\alpha_1, \alpha_2, \ldots, \alpha_k]$. On trouve ainsi

$$U(X) = \frac{P(X)}{\prod_{i=1}^{k} (1 - \alpha_i X)^{r_i}} = \sum_{i=1}^{k} \sum_{j=1}^{r_i} \frac{\beta_{ij}}{(1 - \alpha_i X)^j}.$$

On est donc ramené à développer $(1 - T)^{-j}$, nous allons montrer que

$$\frac{1}{(1-T)^j} = \sum_{n=0}^{\infty} \binom{n+j-1}{j-1} T^n,$$

ce qui démontrera le résultat cherché. Notons d'abord qu'il suffit de démontrer que cette formule est vraie sur $\mathbb{Z}$, le cas général s'en déduisant par homomorphisme. On raisonne par récurrence sur j. Pour $j = 1$ la formule est vraie.

Supposons la formule à l'ordre j, alors en désignant par D l'opérateur de dérivation

$$\begin{aligned}\frac{1}{(1-T)^{j+1}} &= \frac{1}{j} D\left(\frac{1}{(1-T)^j}\right) \\ &= \frac{1}{j} D\left(\sum_{n=0}^{\infty} \binom{n+j-1}{j-1} T^n\right) \\ &= \frac{1}{j}\left(\sum_{n=1}^{\infty} \binom{n+j-1}{j-1} T^{n-1}\right) \\ &= \frac{1}{j}\left(\sum_{n=0}^{\infty} \binom{n+j}{j-1} T^n\right) \\ &= \sum_{n=0}^{\infty} \binom{n+j}{j} T^n.\end{aligned}$$

3) $\Longrightarrow$ 1)
Posons

$$u_n = \binom{n+j-1}{j-1} \alpha^n.$$

On vérifie facilement la formule

$$v_{n+1} - \alpha v_n = \binom{n+j}{j-1} \alpha^{n+1} - \binom{n+j-1}{j-1} \alpha^{n+1} = \binom{n+j-1}{j-2} \alpha^{n+1}.$$

Un argument par récurrence montre ensuite que la suite $v = (v_n)_{n \geq 0}$ vérifie la relation

$$(S - \alpha I)^j v = 0,$$

où S désigne l'opérateur de translation (en anglais shift). Enfin, comme I et S commutent, on en conclut que la suite $u = (u_n)_{n \geq 0}$ donnée en 3) vérifie

$$\prod (S - \alpha_i I)^{r_i} u = 0,$$

ce qui correspond à la relation 1). □

Il est important de noter que la formule de la partie 3) ci-dessus qui fournit une expression de u_n a bien un sens dans tout corps K du fait que les coefficients du binôme sont des nombres entiers (il n'y a pas de dénominateurs).

Corollaire 5.1.1. *Lorsque K est de caractéristique zéro, le terme général de (u_n) d'une suite récurrente linéaire comme dans le théoréme 5.1.2 s'écrit d'une manière plus habituelle*

$$u_n = \sum_{i=1}^{k} P_i(n)\alpha_i^n,$$

où les P_i sont des polynômes à coefficients dans $\overline{K}$, extension de K, et $degP < r_i$ pour $i = 1, 2, \ldots, k$.

Définition 5.1.4. *Soit K un corps commutatif quelconque. Un polynôme F non nul à coefficients dans K est dit quadratfrei si F ne possède que des racines simples dans tout corps contenant K.*

Remarque 5.1.2.

1. *Si le corps K est fini ou est de caractéristique zéro, alors tout polynôme irréductible de $K[x]$ est quadratfrei (voir [21]).*
2. *Un corps K fini de caractéristique p contient un sous-corps qui est isomorphe au corps $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Alors K est un $\mathbb{F}_p$-espace vectoriel. Si $\dim\mathbb{F}_p = n$, alors $\mathrm{card}(K) = p^n$ et $\mathrm{card}(K^*) = p^n - 1$.*

Théorème 5.1.3. *Si un polynôme caractéristique $Q(X) \in \mathbb{F}_p[X]$ d'une suite (u_n) sur un corps fini, avec $u_n \in \mathbb{F}_p$, est irréductible de degré r, alors la période s de la suite divise $p^r - 1$.*

Démonstration. Le polynôme Q étant irréductible, il résulte de la remarque 5.1.2 que Q est quadratfrei. Par conséquent, il résulte du Théorème 5.1.2 que

$$u_n = \sum_{i=1}^{k} \lambda_i \alpha_i^n \quad \text{pour} \quad n = 0, 1, 2, \ldots$$

avec α_i racines de Q et $\lambda_i \in \mathbb{F}_q^*$ où $q = p^r$.

Pour $q = p^r$ et $\lambda_i \in \mathbb{F}_q^*$, on a alors $\alpha_i^{q-1} = 1$ dans $\mathbb{F}_q$. Donc l'ordre t de la suite divise $q - 1 = p^r - 1$. □

5.2 Polynômes et suites récurrentes linéaires modulo p

Dans cette partie, nous allons considérer les racines d'un polynôme (en particulier d'un polynôme caractéristique d'une suite récurrente linéaire) modulo un nombre premier p. Ce qui nous permet d'étudier le rapport entre

l'ordre d'une suite récurrente linéaire et celui de son polynôme caractéristique modulo p

Proposition 5.2.1. *Dans un corps K tel que* $\mathrm{card}(K) \neq 2$, *si*

$$aX^2 + bX + c = 0,\ a \neq 0, \tag{5.3}$$

et $\Delta = b^2 - 4ac$, *alors si*

- • $\Delta = 0$ *: (5.3) a une racine double,*
- • $\Delta =$ *un carré parfait non nul : (5.3) a deux racines distinctes,*
- • Δ *est différent d'un carré parfait : (5.3) possède deux racines dans une extension L de K avec $[L : K] = 2$ et $L = K[\sqrt{\Delta}]$ mais pas de racines dans K.*

Exemples 5.2.1. *On sait que $X^2 - X - 1 = 0$ est l'équation du polynôme caractéristique de la suite de Fibonacci. Alors $\Delta = 5$.*

Nous allons étudier $\Delta \bmod p$ dans les cas suivants :

Soit $t = t_p$ la période de la suite de Fibonacci (F_n) modulo p,

- • *si $p = 5$: $\Delta \equiv 0 \pmod 5$ et*

$$X^2 - X - 1 = (X - 3)^2 \pmod 5,$$

puis, par le théorème fondamental (théorème 5.1.2),

$$F_n \equiv (an + b)\,3^n \pmod 5 \quad \textit{en fait} \quad F_n \equiv 2n3^n \pmod 5,$$

donc t_5 divise $p\,(p-1) = 5 \times 4 = 20$.

n	0	1	2	3	4	5	6	7	8	9	10	11	12
mod 5	0	1	1	2	3	0	3	3	1	4	0	4	4
n	13	14	15	16	17	18	19	20	21	...			
mod 5	3	2	0	2	2	4	1	0	1	...			

On voit que $t_5 = 20$.

- • *si $p = 2$, alors on a :*

n	0	1	2	3	4	5	6	7	...
mod 2	0	1	1	0	1	1	0	1	...

on constate que $t_2 = 3$,

- • $p \neq 2, 5$ *avec* $\left(\frac{5}{p}\right) = +1$ *où* $\left(\frac{n}{p}\right)$ *est le symbole de Legendre défini, pour* n *premier avec* p, *par*

$$\left(\frac{n}{p}\right) = \begin{cases} 1, & \text{s'il existe un entier } x \text{ tel que, } x^2 \equiv n \pmod{p} \\ -1, & \text{sinon,} \end{cases}$$

alors

$$Q(X) \equiv (X - \alpha)(X - \beta) \pmod{p},$$

où α *et* β *appartiennent à* $\mathbb{Z}/p\mathbb{Z}$ *et* t *divise* $p-1$. *Par exemple si* $p = 11$, *alors on a :*

n	0	1	2	3	4	5	6	7	8	9	10	11	...
mod 11	0	1	1	2	3	5	8	2	10	1	0	1	...

$$F_n \equiv a\alpha^n + b\beta^n \pmod{p}, \quad \text{ie} \quad F_n \equiv \frac{1}{\alpha - \beta}(\alpha^n - \beta^n) \pmod{p}$$

et $t = 10$ *divise* $p - 1 = 10$.

- • $p \neq 2, 5$ *avec* $\left(\frac{5}{p}\right) = -1$

Nous avons deux racines distinctes

$$\alpha, \beta \in \mathbb{F}_p[\sqrt{5}] \quad \text{et } \alpha, \beta \notin \mathbb{F}_p,$$

dans ce cas $\left(\text{dans } \mathbb{F}_p\left[\sqrt{5}\right]\right)$

$$F_n \equiv a\alpha^n + b\beta^n \pmod{p}, \quad \text{ie} \quad F_n \equiv \frac{1}{\alpha - \beta}(\alpha^n - \beta^n) \pmod{p},$$

ce qui implique que t *divise* $p^2 - 1$.

Mieux : Comme $\alpha \notin \mathbb{F}_p$, *alors* $\alpha^p \neq \alpha$ *sinon* $\alpha^{p-1} = 1$ *qui est impossible. Comme l'équation n'a que les deux racines* α *et* β *conjuguées dans* $\mathbb{F}_p[\sqrt{5}]$, *alors* $\alpha^p = \beta$ *puisque* α^p *est clairement un conjugué de* α. *Or le produit de ces racines est* $\alpha\beta = -1$. *Par conséquent* $\alpha^p = \beta$ *implique que* $\alpha^{p+1} = \alpha\beta = -1$.

Donc $\alpha^{2(p+1)} = 1$ *et* t *divise* $2(p + 1)$.

Par exemple pour $p = 3$:

n	0	1	2	3	4	5	6	7	8	9	...
mod 3	0	1	1	2	0	2	2	1	0	1	...

On voit que $t = 8$ *divise* $2(p + 1) = 8$. *Il en résulte de cet exemple la proposition suivante :*

Proposition 5.2.2. *Soient K un corps de caractéristique p et (u_n) une suite récurrente linéaire d'ordre deux, de polynôme caractéristique $Q(X)$. Si les solutions de l'équation $Q(X) = 0$ sont dans un corps $L \neq K$, alors la période de la suite divise $(p+1)\times$(l'ordre du produit des racines)* $\pmod p$.

Exemple. — Considérons la suite récurrente linéaire (T_n) à valeurs dans $\mathbb{Z}$ définie par la relation

$$T_{n+3} = T_{n+1} + T_n \quad \text{avec } T_0 = T_1 = 0,\ T_2 = 1.$$

Soient $Q(X) = X^3 - X - 1$ son polynôme caractéristique, $\Delta(Q)$ son discriminant et p un nombre premier quelconque. Nous avons $\Delta(Q) = -23$.

(1) Le progamme suivant (en langage gp/pari) nous donne les valeurs de p comprises entre 2 et 500, pour lesquelles

$$Q(X) \equiv (X-\alpha)(X-\beta)(X-\gamma) \pmod p$$

avec α, β, γ tous distincts.

```
A=matrix(3,3) ; A[1,3]=1 ; A[2,1]=1 ; A[2,3]=1 ; A[3,2]=1
{T(p)=U0=Mod([0,0,1],p) ; U=U0 ;t=1 ; U=U*A ;
while(U<>U0,t++ ;U=U*A) ; print(p," ",t)}
wT(L) = forprime(p=2,L,T(p))
{wk(L) = forprime(p=2,L,P1=P+Mod(0,p) ; F=factor(P1) ;
print(p," ",matsize(F)[1]) ;print(F))}
{W(L) = forprime(p=2,L,P1=P+Mod(0,p) ; F=factor(P1) ;
k=matsize(F)[1] ; if(k==3,print(p)))}
W(500)
```

p	59	101	167	173	211	223	271	307	347	449	463

Par exemple :

$$Q(X) \equiv (X-17)(X-1)(X-46) \pmod{59},$$
$$Q(X) \equiv (X-81)(X-8)(X-12) \pmod{101},$$
$$Q(X) \equiv (X-33)(X-1)(X-40) \pmod{167}.$$

(2) Le programme suivant (en langage gp/pari) nous donne sous forme de tableau, pour les différentes valeurs de p comprises entre 2 et 200, les valeurs de t_p, période de la suite (T_n) modulo p.

```
A=matrix(3,3) ; A[1,3]=1 ; A[2,1]=1 ; A[2,3]=1 ; A[3,2]=1
{T(p) = U0=Mod([0,0,1],p) ; U=U0 ;t=1 ; U=U*A ;
while(U<>U0,t++ ;U=U*A) ; print(p," ",t)}
wT(L)=forprime(p=2,L,T(p))
wT(200)
```

p	2	3	5	7	11	13	17	19
t_p	7	13	24	48	120	183	288	180
p	23	29	31	37	41	43	47	53
t_p	506	871	993	1368	1723	231	2257	1404
p	59	61	67	71	73	79	83	89
t_p	58	930	4488	5113	5404	3120	2295	3960
p	97	101	103	107	109	113	127	131
t_p	3136	100	3536	2862	1485	4256	16257	17293
p	137	139	149	151	157	163	167	173
t_p	391	19461	925	1093	12324	8911	166	172
p	179	181	191	193				
t_p	32221	10920	7296	37443				

Nous avons par exemple pour :

$p = 59$, $t_p = 58 = p - 1$. De même que les autres cas avec trois facteurs distincts modulo p, t divise $p - 1$.

$p = 23$, $t_p = 506 = 23 \times 22$, puisque $23 \mid \Delta(Q)$, et

$$Q(X) \equiv (X + 13)^2(X + 20) \pmod{23}.$$

$p = 11$, $t_p = 120 = 11^2 - 1$ et

$$Q(X) \equiv (X + 5)(X^2 + 6X + 2) \pmod{11}.$$

$p = 13$, $t_p = 183$ qui divise $13^3 - 1 = 2196$ et

$$Q(X) \equiv (X^3 - X - 1) \pmod{13} \quad (\text{irréductible}).$$

Il résulte de l'exemple précédent les résultats suivants :

Proposition 5.2.3. *Soit (u_n) une suite récurrente linéaire de polynôme caractéristique $Q(X) = X^3 - aX^2 - bX - c \in \mathbb{Z}[X]$. Soit p un nombre premier et t la période de la suite modulo p. Alors les assertions suivantes sont vérifiées :*

1. *Si $Q(X)$ se factorise complètement en produit :*
   (i) *de trois facteurs tous distincts* $\pmod p$, *alors t divise $p-1$.*
   (ii) *de trois facteurs non tous distincts* $\pmod p$ *c'est-à-dire $\Delta(Q) \equiv 0 \pmod p$, alors t divise $p(p-1)$.*
2. *Si $Q(X) = (X-\alpha)(X^2+\beta X+\gamma) \pmod p$ (avec $X^2+\beta X+\gamma$ irréductible), alors t divise p^2-1.*
3. *Si Q est irréductible* $\pmod p$, *alors t divise p^3-1.*

Maintenant, soient K un corps fini, A une matrice $(n \times n)$ d'éléments dans K et Q le polynôme caractéristique de A. Alors $Q(X) \in K[X]$ représente le polynôme caractéristique d'une suite récurrente linéaire (u_n). Dans ce cas, $\mathrm{ord}(Q(X))$ divise $\mathrm{ord}(A)$ et si $Q(X)$ est irréductible, alors l'ordre de la suite est égal à $\mathrm{ord}(Q(X))$.

Proposition 5.2.4. *Soient K un corps fini, A une matrice $(n \times n)$ d'éléments dans K telle que $\det(A) \neq 0$, Q le polynôme caractéristique de A et N un entier positif. Alors*
$A^N = I$ si et seulement si $Q(X)$ divise $X^N - 1$ où I est la matrice identité.

Démonstration. Supposons que $A^N = I$ et $Q(X)$ ne divise pas $X^N - 1$. Alors n_0 l'ordre de $Q(X)$ ne divise pas N. Donc il existe des entiers α, β tels que $N = \alpha n_0 + \beta$ avec $0 < \beta < n_0$. Ce qui implique

$$A^N = A^{\alpha n_0 + \beta} = A^\beta \neq I,$$

ce qui contredit l'hypothèse. Donc $Q(X) \mid X^N - 1$.

Réciproquement. Supposons que $A^N \neq I$. Donc l'ordre de A noté t_0 ne divise pas N. Par conséquent il existe des entiers n_1, n_2 tels que

$$N = n_1 \times t_0 + n_2 \quad \text{avec} \quad 0 < n_2 < t_0.$$

Comme $n_0 = \mathrm{ord}(Q(X))$ divise t_0 alors

$$t_0 = n_0 \beta_1 \quad \text{et} \quad N = n_1 n_0 \beta_1 + n_2.$$

Donc n_0 ne divise pas N. Ce qui contredit l'hypothèse. Donc $A^N = I$. □

5.3 Etude du nombre de facteurs irréductibles d'un polynôme

Soit P un plynôme de degré n à coefficients dans un corps fini K. On se propose d'étudier le degré de la plus petite extension de K dans laquelle P se factorise complètement. Nous montrons que le logarithme de ce degré noté $D(P)$ est "en général" très voisin de $\frac{1}{2}\log^2 n$.

Lorsque n tend vers l'infini, LANDAU a montré que

$$\log g(n) \sim \sqrt{n \log n} \quad \text{avec} \quad g(n) = \max_{P \in E_n} D(P)$$

et SHAH dans [27], a amélioré ce résultat par :

$$\log g(n) = \sqrt{n \log n}\Big[1 + \frac{\log\log n}{2\log n} - \frac{1 + O(1)}{2\log n}\Big].$$

M. MIGNOTTE ET J. L. NICOLAS ont complété le résultat de LANDAU dans [22] en établissant :

$$D(P) = \frac{1}{2}\log^2 n + O(\log n)^{\frac{7}{4}}, \quad \text{"en général"}.$$

Nous allons essayer de préciser ce résultat en démontrant que :

$$D(P) \leq \frac{1}{2}\log^2 n + \frac{66}{7}(\log n)^{\frac{7}{4}}, \quad \text{"en général"}.$$

Soit (u_n) une suite récurrente linéaire de polynôme caractéristique $Q(X)$, on va étudier le type de factorisation de Q sur un corps fini, pour obtenir des informations sur la période de (u_n) modulo un nombre premier. Soient q un nombre premier, $\mathbb{F}_q$ le corps à q éléments et $\mathbb{F}_q[X]$ l'anneau des polynômes à une variable indéterminée sur $\mathbb{F}_q$. On désigne par E_n l'ensemble des polynômes unitaires de degré n de $\mathbb{F}_q[X]$. On a donc

$$\text{card}(E_n) = q^n.$$

Pour $Q(X) \in \mathbb{F}_q[X]$, on note $D(Q)$ le degré de la plus petite extension de $\mathbb{F}_q$ dans laquelle $Q(X)$ se factorise complètement. Soit $\mathcal{V}_m$ l'ensemble des polynômes irréductibles de degré m. On pose $I_m = \text{card}(\mathcal{V}_m)$, alors $\Big([22]\Big)$

$$I_m = \frac{1}{m}\sum_{l|m} \mu(l) p^{m/l}, \tag{5.4}$$

où

$$\mu(n) = \begin{cases} (-1)^k, & \text{si} \quad n = p_1 \dots p_k, \quad p_i \text{ entiers premiers distincts,} \\ 0, & \text{sinon,} \end{cases}$$

est la fonction de Mőbius.

Il en résulte l'encadrement suivant $\Big($voir [22]$\Big)$

$$\frac{q^m}{m} - \frac{2}{m} q^{m/2} \leq I_m \leq \frac{q^m}{m}. \tag{5.5}$$

Pour $H \in E_n$, on écrira sa décomposition en facteurs irréductibles :

$$H = P^{\alpha_1} P^{\alpha_2} \dots P^{\alpha_k}$$

et l'on pose pour $1 \leq i \leq k$: $\deg P_i = n_i$. On a donc :

$$\sum_{i=1}^{k} \alpha_i n_i = d \qquad \text{et} \qquad D(H) = p.p.c.m.(n_1, n_2, \dots, n_k).$$

On définit la fonction ω par :

$$\omega(H) = k = \sum_{P|H,\ P \text{ irr}} 1.$$

Alors on la proposition suivante :

Proposition 5.3.1. *Si $P(X) \in E_n$, alors $g(n)$, le plus grand degré parmi les $D(P)$ vérifie :*

$$g(n) = max\Big(p.p.c.m.\Big\{n_1, n_2, \dots, n_k; \quad n_1 + n_2 + \dots + n_k = n\Big\}\Big)$$

Démonstration. Le théorème résulte de [22], [27] et de [18]. □

Nous proposons de démontrer le théorème suivant :

Théorème 5.3.1. *Sous les hypothèses de la proposition 5.3.1, la fonction $D(P)$ vérifie l'inégalité :*

$$D(P) \leq \frac{1}{2} \log^2 n + \frac{66}{7} \Big(\log n\Big)^{\frac{7}{4}} \quad \text{“en général”.}$$

Pour démontrer ce théorème, on a besoin des lemmes suivants :

Lemme 5.3.1. *Soit T un nombre entier, $1 \leq T \leq n$. Pour $H \in E_n$ on pose*

$$\omega_T(H) = \sum_{P|H;\ H\ irr;\ \deg H \leq T} 1,$$

ainsi $\omega_T(H)$ désigne le nombre de facteurs irréductibles distincts de H dont le degré ne dépasse pas T $\Big($en particulier, si $H \in E_n$ alors $\omega_n(H) = \omega(H)\Big)$. On a

$$\sum_{H \in E_n} \omega_T(H) = q^n\Big(\log T - c\Big), \quad avec \quad -1 < c < 2,5.$$

Démonstration. On a

$$\sum_{H \in E_n} \omega_T(H) = \sum_{H \in E_n} \sum_{P|H; \deg P \leq T} 1 = \sum_{i=1}^{T} \sum_{P;\ \deg P = i} \sum_{H;\ P|H} 1 = \sum_{i=1}^{T} I_i q^{n-i},$$

où P désigne un polynôme unitaire irréductible et où H parcourt E_n.

D'après la relation (5.4), on a :

$$I_i = \frac{q^i}{i} - R_i q^{i/2} \quad \text{avec } 0 \leq R_i \leq \frac{2}{i}.$$

Donc

$$\sum_{H \in E_n} \omega_T(H) = q^n \left(\sum_{i=1}^{T} \frac{1}{i} - \sum_{i=1}^{T} R_i q^{-\frac{i}{2}} \right) = q^n \left(\log T - c \right),$$

où $c = \log T - \sum_{i=1}^{T} \frac{1}{i} + \sum_{i=1}^{T} R_i q^{-\frac{i}{2}}$.

Il est facile d'estimer c, on a d'une part

$$\log T < \sum_{i=1}^{T} \frac{1}{i} < 1 + \log T \quad \Big(\text{considérer l'intégrale } \int_1^T \log t \, dt\Big),$$

et d'autre part

$$0 < \sum_{i=1}^{T} R_i q^{\frac{-i}{2}} < 2 \sum_{i=1}^{T} \frac{\left(1/\sqrt{2}\right)^i}{i} < 2 \sum_{i=1}^{\infty} \frac{\left(1/\sqrt{q}\right)^i}{i} = -2 \log\left(1 - \left(1/\sqrt{2}\right)\right) < 2,456.$$

D'où la conclusion. □

Lemme 5.3.2. *Avec les notations du lemme 5.3.1, on a, pour tout nombre entier T, $2 \leq T \leq n$,*

$$\sum_{H \in E_n} (\omega_T(H) - \log T)^2 < 8q^n \log T.$$

Démonstration. Suivons la démonstration de Hardy et Wright dans [15] pour la fonction ω relative aux nombres entiers.

La quantité $\omega_T(H)\,(\omega_T(H) - 1)$ est le nombre de paires (P, Q) de polynômes irréductibles distincts telles P et Q divisent H (en comptant $(P, Q) \neq (Q, P)$). On a donc

$$\omega_T(H)\,(\omega_T(H) - 1) = \sum_{P \neq Q;\ \deg P, Q \leq T;\ PQ \mid H} 1,$$

ce qui implique

$$\begin{aligned}
\sum_{H \in E_n} \omega_T(H)\,(\omega_T(H) - 1) &\leq \sum_{\deg P \leq T;\ \deg P.Q \leq n} \sum_{H;\ PQ \mid H} 1 \\
&\leq \sum_{i=1}^{T} I_i \sum_{j=1}^{T} I_j q^{n-i-j} \\
&\leq q^n \left(\sum_{i=1}^{T} \frac{1}{i} \right)^2 \\
&< q^n \,(1 + \log T)^2 .
\end{aligned}$$

En utilisant la formule

$$(\omega_T(H) - \log T)^2 = \omega_T(H)\,(\omega_T(H) - 1) + (1 - 2\log T)\,\omega_T(H) + (\log T)^2$$

et le lemme 5.3.1, on a

$$\begin{aligned}
\sum_{H \in E_n} (\omega_T(H) - \log T)^2 &< q^n \left(\frac{-3}{2} + 8 \log T \right) \\
&< 8q^n \log T.
\end{aligned}$$

□

Lemme 5.3.3. *(Inégalité de Tchebytcheff pour la fonction ω)*
Pour tout nombre entier $n \geq 3$ et tout nombre réel λ strictement positif, on a l'inégalité

$$\text{Card}\left\{H \in E_n; |\omega(H) - \log n| \geq \lambda\sqrt{\log n}\right\} \leq 8q^n\lambda^{-2}.$$

Démonstration. On applique le lemme 5.3.2 avec $T = n$. □

Lemme 5.3.4. *Excepté pour au plus* $\dfrac{8}{\sqrt[4]{\log T - 2}}\, q^n$ *d'entre eux, tout polynôme $H \in E_n$ vérifie pour tout T, $e^{10000} \leq T \leq n$,*

$$|\omega_T(H) - \log T| \leq 6\,(\log T)^{\frac{3}{4}}.$$

Démonstration. Ce lemme résulte de ([22], lemme 4). □

Démonstration du Théorème 5.3.1
D'après le lemme 5.3.4

$$|\omega_T(H) - \log T| \leq 6\Big(\log T\Big)^{\frac{3}{4}} \quad \text{pour tout} \quad T,\ e^{10000} \leq T \leq n,$$

sauf au plus $\dfrac{8}{\sqrt[4]{\log T - 2}}\, q^n$ exceptions.

Donc on a :

$$\begin{aligned}\sum_{i=1}^{k} \log n_i &= \int_1^n \log T \mathrm{d}\left[\omega_T(H)\right] dT \\ &= \left[\log T \omega_T(H)\right]_1^n - \int_1^n \frac{\omega_T(H)}{T}\ \mathrm{dT} \\ &= \log^2 n + 6\,(\log)^{\frac{7}{4}} - \int_1^n \frac{\omega_T(H)}{T}\ \mathrm{dT}.\end{aligned}$$

Il résulte du lemme 5.3.4 (sauf pour au plus $\dfrac{8}{\sqrt[4]{\log T - 2}}\, q^n$ polynômes) que

$$\begin{aligned}\sum_{i=1}^{k} \log n_i &\leq \log^2 n + 6\,(\log n)^{\frac{7}{4}} - \int_1^n \frac{\omega_T(H)}{T}\ \mathrm{dT} \\ &\leq \log^2 n + 6\,(\log n)^{\frac{7}{4}} + \int_1^n \left[\frac{-\log T}{T} + \frac{6(\log T)^{\frac{3}{4}}}{T}\right]\ \mathrm{dT} \\ &\leq \frac{1}{2}\log^2 n + \frac{66}{7}\,(\log n)^{\frac{7}{4}}.\end{aligned}$$

De plus

$$D(P) = \log(\text{p.p.c.m}(n_1, n_2, \ldots, n_k)) \leq \log(n_1 n_2 \ldots n_k) = \sum_{i=1}^{k} \log n_i,$$

sauf au plus $\frac{8}{\sqrt[4]{\log T - 2}} q^n$ exceptions.

D'où le résultat, avec une majoration explicite du nombre d'exceptions, qui précise l'expression "en général".

5.4 Généralités sur les suites aléatoires

La notion de suite aléatoire est basée sur la théorie des probabilités et des statistiques. Les suites aléatoires interviennent dans divers domaines théoriques ou pratiques. Elles sont utilisées fréquemment en simulation, dans différentes applications de l'électrotechnique, en cryptographie, ...

Considérons l'expérience suivante : on jette une pièce de monnaie à plusieurs reprises. Au cours de cette expérience, on note "0" l'apparition de "Pile" et "1" celle de "Face". Les résultats de cette expérience sont alors aléatoires. Ils forment une suite de bits typiquement aléatoire. Au cours de ces jets, la fréquence limite d'un "1" ou d'un "0" est $\frac{1}{2}$, la fréquence d'avoir successivement, deux "1" ou deux "0" est $\frac{1}{4}$, la fréquence d'avoir successivement trois "1" ou trois "0" est $\frac{1}{8}$ .... On peut généraliser en considérant la fréquence d'un bloc de m bits. La fréquence d'avoir successivement m "1" ou m "0" est égale à $\frac{1}{2^m} = 2^{-m}$. Donc cette expérience peut produire des suites aléatoires que nous devrons soumettre aux tests aléatoires. Par exemple nous pouvons vérifier les quantités statistiques mentionnées ci-dessus, notamment, la fréquence relative à chaque test de distribution ou la fréquence par rapport au test période.

Un autre test populaire pour l'aspect aléatoire est le test de corrélation qui est basé sur le calcul du coefficient de corrélation

$$C_N(h) = \sum_{n=0}^{N-1} (-1)^{u_n - u_{n+h}}$$

de la suite $u_0, u_1, u_2, \ldots$ de bits. Pour que la suite puisse être considérée comme aléatoire $C_N(h)$ doit être nettement plus petit que N. Dans cette

partie, pour tester l'aspect aléatoire des suites, nous nous limitons simplement au test de corrélation.

Ces calculs effectués nous permettent de générer des suites de bits qui vont subir des tests pour estimer leur aspect aléatoire. De telles suites qui subissent ces tests avec succès sont appelées suites pseudo-aléatoires. Les suites considérées ici sont les suites de période maximale qui sont générées par la relation (5.1). Elles vont subir les différents tests décrits plus haut.

On appelle suite de période maximale d'ordre k sur un corps $\mathbb{F}_q$, toute suite $u_0, u_1, u_2, \ldots$ engendrée par une relation

$$u_{n+k} = r_{k-1}u_{n+k-1} + r_{k-2}u_{n+k-2} + \cdots + r_0 u_n \quad \text{pour} \quad n = 0, 1, 2, \ldots \quad (5.6)$$

de polynôme caractéristique $f(x) = x^k - r_{k-1}x^{k-1} - r_{k-2}x^{k-2} - \ldots - r_0$ primitif sur $\mathbb{F}_q$ et de vecteur initial $(u_0, u_1, \ldots, u_{k-1})$ non nul. Si t est la période de cette suite, alors $t = q^k - 1$. D'après [20], le test de distribution et le test périodique peuvent être traités simultanément. Par exemple, pour $b = (b_1, b_2, \ldots, b_m) \in \mathbb{F}_q^m$. Soit $Z(b)$ le nombre de n, $0 \leq n \leq t-1$ tels que $u_{n+i-1} = b_i$ pour tout i, $1 \leq i \leq m$.

Alors $m = 1$ corespond au test de distribution et $m \geq 2$ correspond au test périodique des blocs de longueur m.

Si $1 \leq m \leq k$ et $b \in \mathbb{F}_q^m$, alors pour toute suite de période maximale d'ordre k sur $\mathbb{F}_q$, on a

$$Z(b) = \begin{cases} q^{k-m} - 1, & \text{pour} \quad b = 0, \\ q^{k-m}, & \text{sinon.} \end{cases}$$

Ce résultat montre que $Z(b)$ est très proche de tq^{-m} (cf [20]).

Caractère : Soit G un groupe abélien fini (multiplicatif) d'ordre $|G|$ avec élément unité 1_G. Un *caractère* χ de G est un homomorphisme de G dans le groupe multiplicatif $\mathcal{U}$ des nombres complexes de module 1. C'est une application de G dans $\mathcal{U}$ telle que

$$\chi(g_1 g_2) = \chi(g_1)\chi(g_2), \quad \textit{pour tout} \quad g_1, g_2 \in G,$$
$$\chi(1_G) = \chi(1_G)\chi(1_G) = 1.$$

Exemples 5.4.1. *Soit G un groupe fini cyclique d'ordre n et soit g un générateur de G. Pour un entier fixe j, $0 \leq j \leq n-1$, la fonction $\chi_j(g^k) = \exp(2\pi ijk/n)$,*

pour $k = 0, 1, 2, \ldots$ *définit un caractère de* G. *Si* χ *est un caractère de* G, *alors* $\chi(g)$ *doit être une racine* $n^{\text{ième}}$ *de l'unité. Donc* $\chi(g) = \exp(2\pi ij/n)$ *avec* $0 \leq j \leq n-1$. *Il en résulte que* $\chi = \chi_j$ *et* $G^\wedge = \{\chi_0, \chi_1, \ldots, \chi_{n-1}\}$. *Si* χ *est un caractère non trivial d'un groupe abélien fini* G, *alors* $\sum_{g \in G} \chi(g) = 0$. *Si* $g \in G$ *avec* $g \neq 1_G$, *alors* $\sum_{\chi \in G^\wedge} \chi(g) = 0$. *(cf[20])*

Un caractère non trivial additif fixé de $\mathbb{F}_q$ nous permet d'étendre la définition du coefficient de corrélation $C_N(h)$:

$$C_N(h) = \sum_{n=0}^{N-1} \chi\left(u_n - u_{n+h}\right), \quad N, h \in \mathbb{N}.$$

Dans [20], R. LIDL ET H. NIEERREITER ont établi les résultats suivants :

- • Pour une suite de période maximale dans un corps $\mathbb{F}_q$ avec période minimale t

$$C_N(h) = \begin{cases} t, & \text{si} \quad h \equiv 0 \bmod t, \\ -1, & \text{sinon.} \end{cases}$$

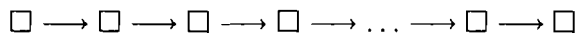
Exemples 5.4.2. *Soit* (u_n) *une suite récurrente linéaire dans* $\mathbb{F}_2$, *avec* $u_{n+5} = u_{n+2} + u_n$ *pour* $n = 0, 1, \ldots$ *et de valeurs initiales* $u_0 = u_2 = u_4 = 1$ *et* $u_1 = u_3 = 0$. *Comme le polynôme caractéristique de* (u_n) *est primitif dans* $\mathbb{F}_2$, *alors* (u_n) *est une suite de période maximale avec période minimale* $t = 2^5 - 1 = 31$. *En calculant les* 31 *bits d'une période des suites* (u_n) *et de la suite à décalage* (u_{n+3}) *on obtient* $C_n(3) = 15 - 16 = -1$ *(nombre des accords de termes correspondants– nombre de désaccords des termes correspondats)*.

- • Pour une suite de période maximale d'ordre k dans un corps $\mathbb{F}_q$ et $1 \leq N \leq t = q^k - 1$ nous avons

$$\begin{cases} C_N(h) = N, & \text{si} \quad h \equiv 0 \bmod t, \\ |C_N(h)| < q^{k/2}\left(\frac{2}{\pi}\log t + \frac{2}{5} + \frac{N}{t}\right) & \text{sinon.} \end{cases}$$

Les suites aléatoires interviennent en électronique. Dans [8], S.W. COLOMB a travaillé dans ce domaine en utilisant les suites des régistres à

décalage (en anglais Shift register sequences). On rappelle qu'un régistre à décalage est un arrangement de r tubes, dont chacun reçoit "1" identifié comme "on" ou "0" idenfié comme "off", qui décale le contenu de chaque tube au prochain tube, réglementé avec une impulsion d'horloge. (voir la figure ci-dessous)



Les suites des régistres à décalage sont périodiques, de période $t \leq 2^r - 1$ où r est le nombre de tubes qui les engendrent.

Il a ainsi utilisé l'expérience qui consiste à jeter une pièce de monnaie à plusieurs reprises en identifiant consécutivement "pile" en tant que "1" et "face" en tant que "-1".

En général les suites considérées sont binaires telles "1" et "-1" correspondent respectivement à "on" et "off" dans un système électronique. Pour caractériser l'aspect aléatoire, il a utilisé une fonction spéciale d'*autocorrélation* notée $C(\tau)$ définie de la manière suivante : pour une suite à termes réels $u_0, u_1, u_2, \ldots$, on pose

$$C(\tau) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} u_n u_{n+\tau},$$

si cette limite existe. Si (u_n) est périodique de période t, alors la somme est finie et

$$C(\tau) = \frac{1}{t} \sum_{n=1}^{t} u_n u_{n+\tau},$$

dans ce cas τ peut être considéré comme une phase à décalage de la suite.

La troisième propriété caractéristique de ces suites donne explicitement l'expression de $C(\tau)$.

$$C(\tau) = \frac{1}{t} \sum_{n=1}^{t} u_n u_{n+\tau} = \begin{cases} 1, & \text{si} \quad \tau = 0, \\ \frac{K}{t}, & \text{si} \quad 0 \leq \tau \leq t. \end{cases}$$

Remarque 5.4.1. *Une suite engendrée par r tubes d'un régistre à décalage est dite de longueur maximale si sa période est $t = 2^r - 1$. Du fait qu'on peut les utiliser pour le codage et le décodage, les suites des régistres (les suites de longueur maximale) à décalage établissent une connection entre les suites récurrentes linéaires et la théorie des codes.*

En gros, les suites de période maximale occupent une place importante dans la théorie des codes et la cryptographie. En effet, en cryptographie, plus précisément en systèmes cryptographiques, on a besoin quand on envoie un message des propriétés suivantes :

- *• Le nombre de clefs possibles doit être assez grand de sorte qu'une recherche exhaustive de clef ne soit pas possible.*
- *• Les suites infinies doivent avoir des périodes minimales dont les longueurs excédent la longueur du message.*
- *• Le texte chiffré doit sembler être aléatoire.*

Pour satisfaire ces propriétés, certaines suites récurrentes linéaires sur le corps $\mathbb{F}_2$ *seraient de bons candidats. Mais, pour construire des systèmes cryptographiques, les suites récurrentes linéaires présentent une certaine faiblesse, du fait que si on connait (on idenfie) une telle suite de polynôme caractéristique de degré* $\leq k$*, alors* $2k$ *termes consécutifs de cette suite déterminent un polynôme caractéristique. Et ainsi la suite est entièrement déterminée. Mais malgrés l'insécurité prouvée, ces suites restent populaires pour la construction des systèmes cryptographiques à cause de leurs grandes périodes* $2^k - 1$ *qui créent une illusion de force.*

En raison de cette faiblesse, on considére en général les générateurs des suites pseudo-aléatoires d'une complexité plus élevée. En combinant les suites récurrentes linéaires, on peut augmenter cette complexité et construire des suites multiplexées qui peuvent être employées comme modules dans la catégorie des chiffres. (pour plus de détails voir [20]).

PROBLEMES OUVERTS

Les résultats obtenus dans cette Thèse confirment l'intérêt qu'il y a de poursuivre l'investgation dans l'étude des FGI-anneaux, des I-modules et des suites récurrentes linéaires afin de trouver une réponse à certaines questions qui restent ouvertes et de généraliser éventuellement certains résultats dèjà établis. Des résultats intéressants ont été trouvés sur l'études des suites récurrentes linéaires sur les anneaux ou les modules. La remarque précédente montre l'importance de ces suites sur la théorie des codes et sur la cryptographie.

Nous laissons ouverts les problèmes suivants :

PROBLEME 1 : Caractériser les FGI-anneaux qui ne sont pas des duo-anneaux.

PROBLEME 2 : Poursuivre l'étude des suites récurrentes linéaires et leur application en cryptographie et en théorie des codes.

PROBLEME 3 : Soit R un anneau commutatif, C une coalgèbre sur R et $C^* = \mathrm{Hom}_R(C, R$ le dual de C qui est une R-algèbre. Alors, tout C-comodule est isomorphe au C^*-module. De plus si C est fini, alors C^* est fini. On peut donc regarder les deux questions suivantes :

- • étudier les suites récurrenntes linéaires sur les C-comodules c'est-à-dire sur les C^*-modules.

- • étudier les codes sur les C^*-modules.

PROBLEME 4 : Soit M un module sur un anneau non nécessairement un duo-anneau. Nous pouvons regarder les questions suivantes :

- • Caractériser les I-modules projectifs.

- • Caractériser les I-modules projectifs ou auto-projectif.

- • Caractériser les I-modules qui ne sont pas de type fini sur anneau non nécessairement un duo-anneau.

Bibliographie

[1] F.W ANDERSON and K.R FULLER : *Ring categories of modules*, Springer-Verlag, Berlin, 1974.

[2] M. BARRY, O. DIANKHA and M. SANGHARÉ, *Characterization of commutative FGI-ring* MATH. SCI. RES. J., 9(4) (2005), 87-91.

[3] M. BARRY, O. DIANKHA and M. SANGHARÉ : *Characterization of FGI-duo-ring*, (à paraître dans Algebras, Groups and Geometries).

[4] M. BARRY, C.T. GUÉYE and M. SANGHARÉ : *On commutative FGI-Rings*, Extracta Mathematicae vol. 12, Num. 3, 255-259, (1997).

[5] J. A. BEACH and W.D BLAIR : *Finitely annihilated modules and orders in Artinian rings*, Comm. in Algebra, Vol. 6, No. 1, (1978), 1-34.

[6] I.S COHEN : *On the structure of complete local rings*, Trans. Amer. Soc., 59 (1946), 54-106.

[7] I.S COHEN and I. KAPLANSKY : *Ring for which every module is a direct sum of cyclic modules*, Math. Zeitschr Bd., 54 (H2S), 97-101.

[8] S. W. COLOMB : *Shift rigister sequences* AEGEAN Park Press (1982).

[9] O. DIANKHA : *Etude de quelques I-modules*, Thèse de 3$^{\text{ième}}$ cycle (1998) Université Cheikh Anta Diop de Dakar.

[10] O. DIANKHA : *Suites récurrentes sur un corps fni : théorie et Applications*, (à paraître).

[11] O. DIANKHA, M. SANGHARÉ et M. SOKHNA : *Sur les I_1-modules*, Annales de l'université de Ouagadougou séries B, vol. 2, 25-30, (1999).

[12] O. DIANKHA et M. SANGHARÉ : *Sur les I-modules*, (à paraître).

[13] A.L. FALL and M. SANGHARÉ : *Sur les I-duo-ring*, Pub. Math. UFR. Sci. Tech. Besancon (2002).

[14] J. HABEB : *On Azumaya's exact rings and Artinian duo-rings*, Comm. in Algebra, 17 (01), (1989), 237-245.

[15] HARDY ET WRIHT : *An Introduction to the Theory of Numbers*, Oxford, at the Clarendon Press, 1960.

[16] I. FUCHS : *Infinite abelian groups,* II Academic press (1973).

[17] M.A KAIDI et M.SANGHARÉ : *Une caractérisation des anneaux artiniens a ideaux principaux*, in L.N.M., vol. 1328, Springer-Verlag, Berlin, 1988, 245-254.

[18] E. LANDAU : *Handbuch der Lehre von Verteilung der Primzahlen*, Leipzigund Berlin, B, G, Teubner, 1909.

[19] A. LERADJI : *On duo rings, pure semi-simplicity and finite representation type* , Comm. in Algebra 25 (12), (1997), 3947-3952.

[20] R. LIDL, H. NIEDERREITER : *Introduction to finite fields and their applications*, Cambridge University Press (1994).

[21] M. MIGNOTTE : *Mathématiques pour le calcul formel*, Presses Universitaires de France (1989).

[22] M. MIGNOTTE, J. L. NICOLAS : *Statistiques sur* $\mathbb{F}_q[X]$, Annales de l'I.H.P., section B, tome 19, n°2, (1983), p. 113-121.

[23] J. L. NICOLAS : *Ordre maximal d'un élément du groupe* S_n *des permutations et "Highly composite numbers"* Bull. Soc. math. France, 97, 1969, p. 129 à 191.

[24] H.C POP : *On the structure of Artinian rings*, Comm. in Algebra, 15(11), (1987), 2327-2348.

[25] M. SANGHARÉ : *On S-duo-rings*, Comm.in Algebra, 20 (08), (1992), 2183-2189.

[26] M. SANGHARÉ : *Sur l'artinuité des* I_1*-anneaux*, Afrika Mathematika, série 3 vol. 2 (1993), 33-37.

[27] S. M. SHAH : *An inequality for the arithmetical function* $g(x)$, J. Indian math. Soc., t. 14, 1939, p. 316-318.

[28] N. VANAJA : *All finitely generated* M*-subgenerated modules are extending*, Comm. in Algebra 24 (2), 543-572 (1996).

[29] W.V VASCONCELOS : *Injective endomorphisms of finitely generated modules*, Amer. Math. Soc., 25, (1970), 900-901.

[30] R. WISBAUER, *Decomposition properties in modules categories*, Acta. Univ. Corilia Math. Physica l26 (26), 57-68 (1985).

[31] WISBAUER : *Foundation of Module and Ring theory*, Gordon and Breach Science Publishers (1991).