N° d'ordre :

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université des Sciences et de la Technologie Houari Boumediène

Faculté de Mathématiques

THESE DE DOCTORAT

Présentée pour l'obtention du **grade** de **DOCTEUR**

En : MATHEMATIQUES

Spécialité : Arithmétique, codage et combinatoire

Par : OULD MOHAMED Rezki

Sujet

COMPOSITION MULTIPLICATIVE ET POLYNÔMES RÉDUCTIBLES MODULO p

Soutenue publiquement, le 13 / 04 /2023, devant le jury composé de :

Mme. SELMAN Shehrazad	Professeur	à l'USTHB	Présidente
Mme. BENFERHAT Leila	Professeur	à L'ENSIA	Directrice de thèse
M. KIHEL Omar	Professeur	à Brock University	Co- Directeur de thèse
Mme. BATOUL Aicha	Professeur	à L'USTHB	Examinatrice
Mme. GUENDA Kenza	Professeur	à L'USTHB	Examinatrice
Mme. KEBLI Salima	Maître de Conférence/A	à L'université Oran 1	Invitée

Remerciements

J'aimerais remercier très particulièrement ma directrice de thèse, Professeure Leila BENFERHAT, pour toute l'aide qu'elle m'a apporté. Je suis ravi d'avoir été son étudiant car outre son appui scientifique, elle a été toujours là pour me conseiller et me soutenir au cours de l'élaboration de cette thèse.
Un très grand merci à mon Co-directeur de thèse, Professeur Omar KIHEL, pour sa grande contribution et pour m'avoir accueilli si chaleureusement au sein de son université. Je le remercie en particulier pour sa disponibilité et son soutien scientifique et moral. "Thank you so Much"
Un très grand merci à Mme SELMANE Schehrazad, Professeure à l'USTHB, qui m'honore en présidant ce jury.
Un grand merci à Mme BATOUL Aicha, Professeure à l'USTHB, et à Mme GUENDA Kenza, Professeure à l'USTHB, pour avoir accepté d'examiner ma thèse.
Un grand merci à Dr. KEBLI Salima d'avoir accepté mon invitation.
Je remercie le CERIST et tous mes collègues de la division (DTISI) qui m'ont accueilli au sein de leur équipe.
À toute personne qui a participé de près ou de loin à l'élaboration de cette thèse.
Je remercie toute ma famille et mes amis pour leur soutien moral.
À mon très cher papa saïd qui m'a soutenu tout au long de ma vie.
À mon grand frère ABDEL GHANI qui est toujours à mes côtés.
À ma très chère femme MANAR à qui je dois beaucoup.

À ma Mère et à ma Grande Mère...

Résumé

Cette thèse est composée de quatre chapitres.
Dans le premier chapitre, nous donnons quelques rappels sur les anneaux et les corps finis.
Le deuxième chapitre est consacré au résultant de deux polynômes sur un anneau commutatif ainsi que ses propriétés que nous utiliserons dans le dernier chapitre.
Le troisième chapitre est la partie clé de notre travail. Nous rappelons la notion de produit composé de deux polynômes défini par Brawley et Carlitz ainsi que les propriétés de ce produit. Nous donnons aussi un des résultats importants des travaux de ces deux mathématiciens sur les polynômes irréductibles sur un corps fini.
Dans le dernier chapitre, nous exposons les résultats obtenus avec des démonstrations détaillées. En utilisant la composition multiplicative de polynômes sur un anneau intègre, nous construisons des polynômes entiers irréductibles sur $\mathbb{Z}$ et réductibles sur $\mathbb{F}_p$ pour tout nombre premier p. Ce travail a fait l'objet d'une publication dans TARA MOUNTAINS Mathematical Publications [4].

Mots clés : Composition multiplicative, résultant, polynômes sur un corps fini, polynôme irréductible.

Abstract

This thesis contains four chapters.
In the first chapter introduces definitions and preliminaries in rings theory and finite fields.
The second chapter is devoted to the resultatnt of two polynomials in a commutative ring and his properties which will be used in the last chapter.
The third chapter is the main part of our work. We recall the definition of the composed product of two polynomials defined by Brawley and Carlitz and the properties of this product. We also give one of the important results of these two mathematicians on irreducible polynomials on a finite fields.
In the last chapter, we expose our results with proofs. Using the multiplicative composition of polynomials on an integral domain, we build somme irreducible polynomials on $\mathbb{Z}$ which are reducible on F_p for any prime number p. This work has been published in TARA MOUNTAINS Mathematical Publications[4].

Keywords : Multiplicative composition, resultant, polynomials over finite fields, irreducible polynomials .

ملخص

تحتوي هذه اطروحة على أربعة فصول.

الفصل الأول يقدم بعض التعاريف المتعلقة بالحلقات و الحقول المتنهية.

الفصل الثاني يتطرق لكثيرات الحدود داخل الحلقات التبادلية و خصائصها المستخدمة في الفصل التالي. في الفصل الثالث نستعرض المحصل المركب ، الدراسة التي قام بها العالمان براولي و كارلتز ، خصائصه و كثيرات الحدود الغير قابلة للاختزال في الحقول المتنهية. الفصل الأخير مخصص لدراسة التي قمنا بها للمحصل المركب لكثيرات الحدود على المجالات ذات التفكيك الوحيد.

النتائج تتضمن أيضا بناء كثيرات حدود غير قابلة للاختزال في حقل الأعداد الصحيحة و لكن يمكن تفكيكها في أي حقل متنهي Fp من أجل p عدد أولي، تم نشر هذه الدراسة مع البراهين في المجلة العلمية Tatra mountains mathematical publications

الكلمات المفتاحية : كثيرات حدود غير قابلة للاختزال ، المحصل المركب ، الحقول المتنهية .

Notations

$\mathbb{F}_q$	Un corps fini à q éléments.
Γ_q	Une clôture algébrique de $\mathbb{F}_q$.
$\mathbb{F}_q[x]$	L'anneau des polynômes à coefficients dans $\mathbb{F}_q$.
$R[x]$	L'anneau des polynômes à coefficients dans l'anneau R.
$deg(f)$	Le degré du polynôme f.
P_G	L'ensemble de polynômes unitaires à coefficients dans $\mathbb{F}_q$ de degrés ≥ 1 et dont les racines sont dans G.
I_G	Le sous-ensemble de P_G, de polynômes unitaires irréductibles à coefficients dans $\mathbb{F}_q$ et dont les racines sont dans G.
$Res_x(f,g)$	Le résultant en x des polynômes f et g.
C_f	Le coefficient dominant du polynôme f.
$d(\alpha)$	Le degré du nombre algébrique α.
$\mathcal{A}^*$	Le groupe des unités de $\mathcal{A}$.
$Aut(\mathbb{K})$	Le groupe des automorphismes de $\mathbb{K}$.

Table des matières

Introduction

Soient $f, g \in \mathbb{F}_q[x]$ deux polynômes unitaires sur un corps fini. Soient $\alpha_1, ..., \alpha_m$ et $\beta_1, ..., \beta_n$ toutes les racines de f et g respectivement dans une clôture algébrique de $\mathbb{F}_q$. La composition additive de f et g est donnée par :

$$f * g = \prod_{i=1}^{m} \prod_{j=1}^{n} (x - (\alpha_i + \beta_j))$$

et la composition multiplicative de f et g est donnée par :

$$f \circ g = \prod_{i=1}^{m} \prod_{j=1}^{n} (x - \alpha_i \beta_j)$$

En 1987, Brawley et Carlitz ont défini une notion plus générale de produit composé, noté $f \diamond g$, où $f * g$ et $f \circ g$ sont des cas particuliers. Dans [9], ces deux mathématiciens ont étudié de façon détaillée ce produit composé. Ils montrent que si f et g sont deux polynômes à coefficients dans $\mathbb{F}_q$ tels que $\deg f = n \geq 1$ et $\deg g = m \geq 1$, alors le produit $f \diamond g$ est irréductible sur $\mathbb{F}_q$ si, et seulement si, f et g sont irréductibles sur $\mathbb{F}_q$ et $pgcd(n, m) = 1$. Ce résultat nous permet de construire des polynômes irréductibles sur $\mathbb{F}_q$ de degrés assez grands. Ils ont également examiné l'unicité de la décomposition de polynômes en produit composé de polynômes. Un polynôme unitaire $f \in \mathbb{F}_q[x]$, de degré ≥ 1, est dit décomposable si $f = f_1 \diamond f_2$ tels que $f_1, f_2 \in \mathbb{F}_q[x]$ et $deg(f) > 1$, $deg(g) > 1$.
Le produit composé de deux polynômes peut être défini sur un anneau commutatif grâce à un résultat établi par Loos dans [20]. Ce résultat montre le lien entre le résultant de deux polynômes et leur produit composé.
Dans cette thèse, en utilisant la composition multiplicative et le résultant de deux polynômes sur un anneau commutatif intègre, nous construisons des polynômes irréductibles sur $\mathbb{Z}$ et réductibles sur $\mathbb{F}_p$ pour tout nombre premier p.
Cette thèse est composée de quatre chapitres.

Dans le premier chapitre, Nous donnons quelques rappels sur les anneaux et les corps finis.
Le deuxième chapitre est consacré au Résultant de deux polynômes sur un anneau commutatif ainsi que ses propriétés que nous utiliserons dans le dernier chapitre.
Le troisième chapitre est la clé de notre travail qui est liée à la multiplication composée de deux polynômes dans $\mathbb{F}_q[x]$. Brawley et Carlitz ont montré que la loi $\diamond$ est une loi de composition interne sur l'ensemble des polynômes unitaires à coefficients dans $\mathbb{F}_q$ de degré ≥ 1. Nous donnons le résultat établi par ces deux derniers sur le produit composé de deux polynômes unitaires irréductibles à coefficients dans un corps fini et sa démonstration. Ensuite, nous abordons l'addition et la multiplication composées de deux polynômes à coefficients dans un corps fini ainsi que la décomposition de polynômes par rapport à ces deux lois sur $\mathbb{F}_q$. Nous donnons également des méthodes qui permettent de calculer l'addition et la multiplication composées et un algorithme à la fin du chapitre.
Dans le dernier chapitre, nous présentons une construction de polynômes entiers irréductibles sur $\mathbb{Z}$ et réductibles sur $\mathbb{F}_p$ pour tout nombre premier p.
Pour établir cette construction, nous avons introduit la composition multiplicative que nous noterons $\diamond$ de deux polynômes sur un anneau intègre R et nous donnons le groupe des unités de $R[X]$ pour la loi $\diamond$. Nous introduisons également la notion de polynômes presque indécomposables. Les résultats sont donnés comme suit :

Théorème 0.1 *Le groupe $G_\diamond$ des unités de $R[x]$ pour la loi $\diamond$ est égal exactement à l'ensemble des polynômes linéaires $u = u_1x + u_0$ avec $u_1, u_0 \in R^*$, et l'inverse d'un tel u est donné par : $u_1^{-1}x + u_0^{-1}$.*

Définition 0.2 *Soit $f \in R[x]$. S'il existe $f_1, f_2 \in R[x] \setminus G_\diamond$ tels que $f = f_1 \diamond f_2$, alors on dit que f est multiplicativement décomposable. Sinon, On dit que f est multiplicativement indécomposable.*
Si f admet une décomposition de la forme $f = f_1 \diamond f_2$ avec f_1 ou f_2 linéaire, alors on dit que f est presque indécomposable sur R.

Théorème 0.3 *Si $f \in R[x]$ est de degré p premier, alors f est presque indécomposable sur R.*

Théorème 0.4 *Si $f \in R[x]$ avec $\deg f > 1$ et de coefficient dominant p premier, alors f est presque indécomposable sur R. De plus, le coefficient dominant de tout facteur linéaire de la décomposition est une unité de R.*

Théorème 0.5 *Soit $f \in R[x]$. Alors $f = f_1 \diamond f_2 \diamond \cdots \diamond f_r$, où les $f_i \in R[x]$ sont des polynômes presque indécomposables $f_i \in R[x]$.*

Un homomorphisme d'anneaux $\sigma : R \to S$ peut être naturellement prolongé en un homomorphisme d'anneaux de $R[x]$ à $S[x]$ par l'application $a_m x^m + \cdots + a_0 \to \sigma(a_m)x^m + \cdots + \sigma(a_0)$. Si $\sigma : R[x] \to S[x]$ préserve les degrés de f et $g \in R[x]$, alors

$$\sigma(Res_x(f,g)) = Res_x(\sigma(f), \sigma(g)).$$

Comme $Res_x(f,g)$ est un polynôme dont les coefficients sont des produits et sommes des coefficients de f et de g. alors nous pouvons énoncer le résultat suivant :

Théorème 0.6 *Soit $\sigma : R \to S$ un homomorphisme d'anneaux, et soit $f \in R[x]$ tel que $f(0)$ et $C_f \notin \ker\sigma$. Si σf est presque indécomposable sur S, alors f est presque indécomposable sur R.*

Lemme 0.7 *Soit K le corps des fractions de l'anneau intègre R. Soit $f, f_1, f_2 \in R[x]$ et soit $f = C_f F, f_1 = C_{f_1} F_1$ et $f_2 = C_{f_2} F_2$, où $C_f, C_{f_1}, C_{f_2} \in R$ et $F, F_1, F_2 \in K[x]$ sont des polynômes unitaires. Alors $f = f_1 \diamond f_2$ sur R si, et seulement, si $F = F_1 \diamond F_2$ sur K and $C_f = C_{f_1}^{\deg f_2} C_{f_2}^{\deg f_1}$.*

Ainsi, nous obtenons les deux résultats principaux suivants :

Théorème 0.8 *Soit m un idéal maximal de R tel que le corps des résidus R/m est fini, et soit $f \in R[x]$ un polynôme de degré au moins 2 et dont les coefficients dominant et terme constant ne s'annulent pas modulo m. Si l'image de f modulo m est irréductible dans $R/m[x]$, alors f est le produit composé d'au plus $\omega(deg f)$ de polynômes presque indécomposables de degrés au moins 2 sur R, où $\omega(n)$ désigne le nombre de nombres premiers apparaissant dans la décomposition de n en produit de nombres premiers.*

Corollaire 0.9 *Soient $f_1, f_2, ..., f_r \in \mathbb{Z}[x]$ de degrés au moins 2. Si*

$$\omega(\deg f_1 ... \deg f_r) < r,$$

alors $f_1 \diamond ... \diamond f_r$ est réductible modulo p quelque soit p premier qui ne divise pas leur coefficients dominants et leurs termes constants.

Exemple 0.10 *Les polynômes ci-dessous sont irréductibles sur $\mathbb{Z}$ mais réductibles sur $\mathbb{F}_p$ quelque soit p premier :*

1. $x^{12} - x^{10} + 3x^8 + 4x^6 + 3x^4 + 2x^2 + 1 = (x^2+1) \diamond (x^2+x+1) \diamond (x^3+x^2+1)$,

2. $x^8 + 2x^4 + x^2 + 1 = (x^2 + 1) \diamond (x^4 + x + 1)$,
3. $x^4 + (a^2 - 2)x^2 + 1 = (x^2 + 1) \diamond (x^2 + ax + 1)$ *où* $a \notin \{0, \pm 2\}$,
4. $x^4 + (a^2 + 2)x^2 + 1 = (x^2 + 1) \diamond (x^2 + ax - 1)$ *où* $a \neq 0$.

L'irréductiblité des polynômes précédents sur $\mathbb{Z}$ peut être vérifiée par un logiciel de calcul. Notons que le polynôme $f \diamond g$ n'est pas toujours irréductible sur $\mathbb{Z}$. Par exemple le polynôme $f = x^2 + 1$ et $g = x^2 + x - 2$ vérifient les conditions du corollaire 0.9, mais le polynôme

$$f \diamond g = (x^2 + 1) \diamond (x^2 + x - 2) = x^4 + 5x^2 + 4 = (x^2 + 4)(x^2 + 1)$$

est réductible sur $\mathbb{Z}$.

Chapitre 1

Rappels sur les anneaux et les corps finis

Dans ce chapitre, nous donnons quelques rappels et résultats sur les anneaux et les corps finis.

1 Définition d'un anneau

Définition 1.1 *Un anneau est un ensemble $\mathcal{A}$ muni de deux lois de composition internes notées $+$ et $\cdot$, respectivement, vérifiant :*

1. *$(\mathcal{A}, +)$ est un groupe abélien*
2. *La loi $\cdot$ est associative et admet un élément neutre appelé l'unité de $\mathcal{A}$.*
3. *La loi $\cdot$ est distributive par rapport à la loi $+$.*

Si de plus, la loi $\cdot$ est commutative, on dira que l'anneau est commutatif.
Un anneau muni de deux lois $+$ et $\cdot$ sera noté $(\mathcal{A}, +, \cdot)$.

Remarque 1.2 *Les propriétés suivantes découlent immédiatement de la définition d'un anneau :*

1. *$0.a = a.0 = 0$. Pour tout $a \in \mathcal{A}$. (On dit que 0 est absorbant)*
2. *Si $1 = 0$, alors l'anneau est trivial, ie $\mathcal{A} = \{0\}$.*

Dans un anneau $(\mathcal{A}, +, \cdot)$, un élément $a \in \mathcal{A}, a \neq 0$, est dit inversible s'il existe $b \in \mathcal{A}$ tel que $a \cdot b = b \cdot a = 1$. Dans ce cas b est unique, on l'appelle l'inverse de a et on le note a^{-1}. Un élément inversible de $\mathcal{A}$ est aussi appelé unité de $\mathcal{A}$. Le groupe des unités de $\mathcal{A}$ est noté $\mathcal{A}^*$.

Exemple 1.3 *1. Les éléments inversibles de $\mathbb{Z}$ sont 1 et -1.*

2. les éléments inversibles de $\mathbb{Z}/3\mathbb{Z}$ sont $\overline{1}$ et $\overline{2}$.

3. Les éléments inversibles de $\mathbb{R}[x]$ sont les polynômes constants non nuls.

4. Les éléments inversibles de $\mathbb{Z}[x]$ sont les polynômes constants 1 et -1.

Définition 1.4 *Un corps est un anneau non trivial contenant au moins deux éléments dans lequel tout élément non nul est inversible. Autrement dit un corps est un anneau $\mathcal{A}$ tel que $\mathcal{A} \setminus \{0\} = \mathcal{A}^*$.*

Exemple 1.5 *$\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps commutatifs pour l'addition et la multiplication usuelles. L'anneau des polynômes $\mathbb{K}[x]$ n'est pas un corps. L'anneau $\mathbb{Z}/3\mathbb{Z}$ est un corps commutatif et plus généralement, si p est un nombre premier alors $\mathbb{Z}/p\mathbb{Z}$ est un corps commutatif.*

Définition 1.6 *Un anneau intègre est un anneau commutatif $\mathcal{A}$ dans lequel la propriété suivante est vérifiée :*

$$\forall a, b \in \mathcal{A}, a \cdot b = 0 \Rightarrow a = 0 \text{ ou } b = 0.$$

Remarque 1.7 *Dans un anneau intègre $\mathcal{A}$, il n'y a pas de diviseur de 0.*
On dit qu'un élément $a \in \mathcal{A} \setminus \{0\}$ est un diviseur de 0 s'il existe $b \in \mathcal{A} \setminus \{0\}$ tel que $a \cdot b = 0$ ou $b \cdot a = 0$.
Un corps commutatif est un anneau intègre. Si un anneau $\mathcal{A}$ est intègre, alors l'anneau des polynômes $\mathcal{A}[X]$ est intègre.

Proposition 1.8 *Les trois propriétés suivantes sont équivalentes :*

1. *$\mathbb{Z}/p\mathbb{Z}$ est un corps*
2. *$\mathbb{Z}/p\mathbb{Z}$ est un anneau intègre*
3. *p est premier*

2 Sous-anneaux, anneaux engendrés

Définition 1.9 *Un sous-anneau d'un anneau $(\mathcal{A}, +, \cdot)$ est un sous-ensemble $\mathcal{A}' \subset \mathcal{A}$ tel que les lois $+$ et $\cdot$ sont des lois de composition internes dans $\mathcal{A}'$ et $(\mathcal{A}', +, \cdot)$ est un anneau ayant pour unité $1_{\mathcal{A}}$, l'unité de $\mathcal{A}$.*

Exemple 1.10 *1. Le seul sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$ lui même.*

2. $\mathbb{R}[X]$ *est un sous-anneau de* $\mathbb{C}[X]$.

Proposition 1.11 *Soit* $(\mathcal{A}_i)_{i\in I}$ *une famille de sous-anneaux d'un anneau* $\mathcal{A}$. *Alors* $\bigcap_{i\in I}\mathcal{A}_i$ *est un sous-anneau de* $\mathcal{A}$.

Remarque 1.12 *Contrairement à l'intersection, l'union de deux sous-anneaux n'est pas nécessairement un sous -anneau.*

Définition 1.13 *Soit* $\mathbb{E}$ *un sous-ensemble d'un anneau* $\mathcal{A}$. *L'intersection de tous les sous-anneaux de* $\mathcal{A}$ *qui contiennent* $\mathbb{E}$ *est un sous-anneau de* $\mathcal{A}$ *appelé sous-anneau engendré par* $\mathbb{E}$. *Il s'agit du plus petit sous-anneau de* $\mathcal{A}$ *(au sens de l'inclusion) contenant* $\mathbb{E}$.

3 Morphismes d'anneaux, Anneaux produits

Définition 1.14 *Soient* $\mathcal{A}$ *et* $\mathcal{B}$ *deux anneaux. Un morphisme (ou homomorphisme) de* $\mathcal{A}$ *dans* $\mathcal{B}$ *est une application* $\varphi : \mathcal{A} \to \mathcal{B}$ *: vérifiant*

1. $\varphi(1_{\mathcal{A}}) = 1_{\mathcal{B}}$
2. $\varphi(a+b) = \varphi(a) + \varphi(b)$ *et* $\varphi(ab) = \varphi(a)\varphi(b)$, $\forall a, b \in \mathcal{A}$.

Un isomorphisme d'anneaux est un morphisme bijectif.
Il découle immédiatement de la définition d'un morphisme $\varphi : \mathcal{A} \to \mathcal{B}$ *tel que* $\varphi(0_{\mathcal{A}}) = 0_{\mathcal{B}}$, $\varphi(-x) = -\varphi(x)$ *et que si* x *est inversible alors* $\varphi(x)$ *est inversible avec* $\varphi(x^{-1}) = (\varphi(x))^{-1}$.

Proposition 1.15 *Si* $\varphi : \mathcal{A} \to \mathcal{B}$ *est un isomorphisme d'anneaux alors* $\varphi^{-1} : \mathcal{B} \to \mathcal{A}$ *est un isomorphisme d'anneaux de* $\mathcal{B}$ *dans* $\mathcal{A}$.

Exemple 1.16
1. *L'application* $\varphi : \mathbb{R}[x] \to \mathbb{R}$ *définie par* $\varphi(P) = P(0)$ *est un morphisme qui n'est pas un isomorphisme.*
2. *L'application* $\varphi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ *définie par* $\varphi(a + b\sqrt{2}) = a - b\sqrt{2}$ *est un isomorphisme.*
3. *Il n'existe pas de morphisme d'anneaux entre* $\mathbb{Z}[\sqrt{2}]$ *et* $\mathbb{Z}[\sqrt{3}]$.

Proposition 1.17 *Supposons qu'il existe un isomorphisme* φ *entre deux anneaux* $\mathcal{A}$ *et* $\mathcal{B}$. *Alors on a :*

1. $\mathcal{A}$ *est commutatif* $\Leftrightarrow$ $\mathcal{B}$ *est commutatif.*
2. $\mathcal{A}$ *est intègre* $\Leftrightarrow$ $\mathcal{B}$ *est intègre.*

3. *Un élément $a \in \mathcal{A}$ est inversible $\Leftrightarrow$ $\varphi(a)$ est inversible.*
4. *Un élément $a \in \mathcal{A}$ est nilpotent $\Leftrightarrow$ $\varphi(a)$ est nilpotent.*
5. *Un élément $a \in \mathcal{A}$ est idempotent $\Leftrightarrow$ $\varphi(a)$ est idempotent.*

Définition 1.18 *Soit $\varphi : \mathcal{A} \to \mathcal{B}$ un morphisme d'anneaux. On définit le noyau de φ, noté $\ker\varphi$, par*

$$\ker\varphi = \{x \in \mathcal{A} / \varphi(x) = 0_{\mathcal{B}}\}.$$

On définit l'image de φ, notée $Im\varphi$, par

$$Im\varphi = \{\varphi(x) / x \in \mathcal{A}\}.$$

Nous avons la proposition suivante :

Proposition 1.19 *Soit $\varphi : \mathcal{A} \to \mathcal{B}$ un morphisme d'anneaux. Alors on a :*

1. *$\ker\varphi$ est un sous-anneau de $(\mathcal{A}, +)$.*
2. *$Im\varphi$ est un sous-anneau de $\mathcal{B}$.*
3. *φ est injective si, et seulement si, $\ker\varphi = \{0_{\mathcal{A}}\}$.*

4 Divisibilité dans les anneaux

Définition 1.20 *Soient $a, b \in \mathcal{A}$.*

— *On dit que b divise a s'il existe $c \in \mathcal{A}$ tel que $a = bc$ et on notera dans ce cas $b \mid a$. On dit également que a est un multiple de b.*

— *On dit que a et b sont associés et on notera $a \sim b$ si $a \mid b$ et $b \mid a$.*

Il est facile de voir que la relation $a \sim b$ est une relation d'équivalence sur $\mathcal{A}$. Lorsque l'anneau $\mathcal{A}$ est intègre, on a la caractérisation suivante :

Proposition 1.21 *Si $\mathcal{A}$ est intègre, deux éléments a et b sont associés si et seulement si, il existe $u \in \mathcal{A}^*$ tel que $a = ub$.*

Définition 1.22 *On dit qu'un élément $a \in \mathcal{A}$ est irréductible s'il est non inversible et les seuls diviseurs de a dans $\mathcal{A}$ sont les éléments inversibles de $\mathcal{A}$ et les éléments associés à a.*

Définition 1.23 *On dit qu'un élément $a \in \mathcal{A} \setminus \{0\}$ est premier s'il est non inversible et lorsqu'il divise le produit de deux éléments de $\mathcal{A}$, il doit diviser au moins l'un des deux. Autrement dit :*

$$a \mid bc \Rightarrow a \mid b \text{ ou } a \mid c.$$

Proposition 1.24 *Soit $\mathcal{A}$ un anneau intègre. Si $a \in \mathcal{A}$ est premier alors il est irréductible.*

La réciproque est fausse en général voir l'exemple ci-dessous :

Exemple 1.25 *Considérons dans l'anneau $\mathbb{Z}[\sqrt{-3}]$. On peut montrer que 2 est irréductible dans $\mathbb{Z}[\sqrt{-3}]$ mais il n'est pas premier. En effet, 2 est un diviseur de 4 et $4 = (1+\sqrt{-3})(1-\sqrt{-3})$.*

Définition 1.26 *Deux éléments $a, b \in \mathcal{A}$ sont dits premiers entre eux si les seuls diviseurs communs sont les éléments inversibles de $\mathcal{A}$. On dit qu'ils sont étrangers s'il existe $x, y \in \mathcal{A}$ tel que $xa + yb = 1$.*

Proposition 1.27 *Si a et b sont étrangers alors ils sont premiers entre eux.*

La réciproque est fausse comme le montre l'exemple ci-dessous

Exemple 1.28 *Dans l'anneau $\mathbb{Z}[X]$ les polynômes $P = 3$ et $\mathbb{Q} = X$ sont premier entre eux mais pas étrangers.*

5 Idéaux

Soit $\mathcal{A}$ un anneau commutatif.

Définition 1.29 *Un idéal de $\mathcal{A}$ est un sous-ensemble $\mathcal{I} \subset \mathcal{A}$ vérifiant*

1. *$(\mathcal{I}, +)$ est un sous-groupe de $\mathcal{A}$*
2. *Pour tout $a \in \mathcal{I}$ et pour tout $x \in \mathcal{A}$, on a $ax \in \mathcal{I}$.*

Exemple 1.30

1. *Dans un anneau $\mathcal{A}$, il y a au moins deux idéaux : l'idéal trivial $\{0\}$ et $\mathcal{A}$.*
2. *Dans l'anneau $\mathbb{Z}$ le sous-ensemble $n\mathbb{Z} = \{nk, k \in \mathbb{Z}\}$ avec $n \in \mathbb{N}$, sont des idéaux.*
3. *Si φ est un morphisme d'anneaux, alors $\ker\varphi$ est un idéal de $\mathcal{A}$.*
4. *Il découle directement de la définition que pour tout idéal $\mathcal{I}$ de $\mathcal{A}$, $0 \in \mathcal{I}$, et que si $1 \in \mathcal{I}$ alors $\mathcal{I} = \mathcal{A}$.*

Nous avons la caractérisation suivante des idéaux :

Proposition 1.31 *Un sous-ensemble non vide $\mathcal{I} \subset \mathcal{A}$ est un idéal si et seulement si $a_1 x + \cdots + a_k x^k \in \mathcal{I}$ pour tout $a_1, \cdots, a_k \in \mathcal{I}$ et tout $x, \cdots, x^k \in \mathcal{A}$.*

Remarque 1.32 *Pour tout élément $a \in \mathcal{A}$, $\langle a \rangle = \{ax : x \in \mathcal{A}\}$ est un idéal de $\mathcal{A}$, appelé idéal engendré par a.*

Proposition 1.33 *$\mathcal{A}$ est un corps si, et seulement si, les seul idéaux de $\mathcal{A}$ sont l'idéal trivial $\{0\}$ et $\mathcal{A}$.*

Définition 1.34 *Un idéal $\mathcal{I}$ de $\mathcal{A}$ est dit principal s'il existe $a \in \mathcal{A}$ tel que $\mathcal{I} = \langle a \rangle$*

Exemple 1.35
1. *Tout les idéaux de l'anneau $\mathbb{Z}$ sont principaux car tous les sous-groupe de $(\mathbb{Z}, +)$ sont de la forme $p\mathbb{Z}, p \in \mathbb{N}$.*
2. *Dans l'anneau $\mathbb{Z}[x]$, l'idéal $\mathcal{I} = \{2P + QX : P, Q \in Z[X]\}$ n'est pas principal.*

Proposition 1.36 *Si $\mathbb{K} = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, tout idéal de l'anneau $\mathbb{K}[X]$ est principal.*

Définition 1.37 *Soit $\mathbb{E}$ un sous-ensemble de $\mathcal{A}$. L'intersection de tous les idéaux contenant $\mathbb{E}$ est un idéal de $\mathcal{A}$, appelé l'idéal engendré par $\mathbb{E}$. C'est le plus petit idéal de $\mathcal{A}$ contenant $\mathbb{E}$, il est noté $\langle \mathbb{E} \rangle$.*

Remarque 1.38 *Si $\mathcal{I}$ et $\mathcal{J}$ sont des idéaux de $\mathbb{A}$, l'ensemble $\mathcal{I} \cup \mathcal{J}$ n'est pas un idéal en général. On peut vérifier néanmoins que l'idéal engendré par $\mathcal{I} \cup \mathcal{J}$ est $\mathcal{I} + \mathcal{J}$.*

Exemple 1.39 *Dans $\mathbb{Z}$ l'union des deux idéaux $2\mathbb{Z}$ et $3\mathbb{Z}$ n'est pas un idéal car par exemple $3 - 2 = 1 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$. L'idéal engendré par $2\mathbb{Z} \cup 3\mathbb{Z}$ est $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$.*

6 Anneau quotient

Si $\mathcal{I}$ est un idéal de $\mathcal{A}$, la relation $\mathcal{R}$ définie sur $\mathcal{A}$ par :

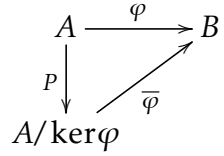
$$x \mathcal{R} y \Leftrightarrow x - y \in \mathcal{I}.$$

est une relation d'équivalence sur $\mathcal{A}$. Soit $\mathcal{A}/\mathcal{I}$, l'ensemble des classes d'équivalence. On définit sur $\mathcal{A}/\mathcal{I}$, l'addition et la multiplication comme suit :

$$\overline{x} + \overline{y} = \overline{x + y} \textbf{ et } \overline{xy} = \overline{xy}.$$

Proposition 1.40 *$\mathcal{A}/\mathcal{I}$, muni de l'addition et de la multiplication définies ci-dessus est un anneau commutatif. De plus la projection canonique $P : \mathcal{A} \to \mathcal{A}/\mathcal{I}$ définie par $P(x) = \overline{x}$ est un morphisme d'anneaux qui est surjectif et dont le noyau est $\mathcal{I}$.*

Théorème 1.41 *(théorème de factorisation)*
Soit $\varphi : \mathcal{A} \to B$ un morphisme d'anneaux. Alors il existe un unique morphisme d'anneaux injectif $\overline{\varphi} : \mathcal{A}/\ker\varphi \to B$ vérifiant le diagramme commutatif suivant :



En particulier, $\overline{\varphi} : \mathcal{A}/\ker\varphi \to Im\varphi$ est un isomorphisme d'anneaux. Le diagramme est dit commutatif si $\varphi = \overline{\varphi} \circ P$. De plus, $Im\overline{\varphi} = Im\varphi$.

Exemple 1.42 *Soit $\mathcal{A} = \mathbb{R}[X]$ et soit $\varphi : \mathcal{A} \to \mathbb{R}$ définie par $\varphi(P) = P(0)$. On a $\ker\varphi = \langle X \rangle$ et $Im\varphi = \mathbb{R}$. Ainsi, on a $\mathbb{R}[X]/\langle X \rangle \cong \mathbb{R}$.*

Théorème 1.43 *(Théorème d'isomorphisme)*
Si $\mathcal{I}$ est un idéal de $\mathcal{A}$, alors les idéaux de $\mathcal{A}/\mathcal{I}$ sont de la forme $\mathcal{J}/\mathcal{I}$, où $\mathcal{J}$ est un idéal de $\mathcal{A}$ tel que $\mathcal{I} \subset \mathcal{J}$. De plus le morphisme canonique $f : \mathcal{A}/\mathcal{I} \to \mathcal{A}/\mathcal{J}$ est surjectif et induit d'après le théorème précédent un isomorphisme $\overline{f} : (\mathcal{A}/\mathcal{I})/(\mathcal{J}/\mathcal{I}) \to \mathcal{A}/\mathcal{J}$. Ainsi, on a

$$(\mathcal{A}/(\mathcal{I})/(\mathcal{J}/\mathcal{I}) \cong \mathcal{A}/\mathcal{J}.$$

Définition 1.44 *Deux idéaux $\mathcal{I}, \mathcal{J}$ de $\mathcal{A}$ sont dit étrangers si $\mathcal{I} + \mathcal{J} = \mathcal{A}$.*

Il découle directement de la définition que deux idéaux $\mathcal{I}$ et $\mathcal{J}$ sont étrangers s'il existe $a \in \mathcal{I}$ et $b \in \mathcal{J}$ tel que $a + b = 1$.

6.1 Idéaux maximaux, Idéaux premiers

Définition 1.45 *Un idéal $\mathcal{M}$ de $\mathcal{A}$ est dit maximal s'il est distinct de $\mathcal{A}$ et si pour tout idéal $\mathcal{I}$ de $\mathcal{A}$ on a*

$$\mathcal{M} \subset \mathcal{I} \Rightarrow \mathcal{I} = \mathcal{M} \text{ ou } \mathcal{I} = \mathcal{A}.$$

Proposition 1.46 *Un idéal $\mathcal{M}$ de $\mathcal{A}$ est maximal si l'anneau $\mathcal{A}/\mathcal{M}$ est un corps.*

Proposition 1.47 *Si $\mathcal{M}_1$ et $\mathcal{M}_2$ sont deux idéaux maximaux de $\mathcal{A}$ alors ils sont étrangers.*

Théorème 1.48 *(Théorème de Krull)*
Tout idéal propre est contenue dans un idéal maximal.

Corollaire 1.49 *Pour qu'un élément de $\mathcal{A}$ soit inversible il faut et il suffit qu'il n'appartiennent à aucun idéal maximal de $\mathcal{A}$.*

Définition 1.50 *Un idéal $\mathcal{I} \neq \mathcal{A}$ est dit premier si*

$$\forall x, y \in \mathcal{A}, xy \in \mathcal{I} \Rightarrow x \in \mathcal{I} \text{ ou } y \in \mathcal{I}.$$

Exemple 1.51
1. *Dans $\mathbb{Z}$ un idéal (non trivial) est premier si, et seulement si, il est de la forme $p\mathbb{Z}$ avec p premier.*
2. *Dans tout anneau intègre $\mathcal{A}$, l'idéal trivial $\{0\}$ est premier.*

Proposition 1.52 *Soit I un idéal de $\mathcal{A}$,*

$$\mathcal{I} \text{ est un ideal premier de } \Leftrightarrow \mathcal{A}/\mathcal{I} \text{ est intègre .}$$

En particulier tout idéal maximal est premier.

Exemple 1.53
1. *Soit $\mathcal{A}$ un anneau intègre mais non trivial, alors l'idéal $\{0\}$ est premier mais non maximal.*
2. *Dans l'anneau $\mathbb{Z}[X]$, l'idéal $\langle X \rangle$ est premier puisque $\mathbb{Z}[X]/\langle X \rangle \cong \mathbb{Z}$ et $\mathbb{Z}$ est intègre. Comme $\mathbb{Z}$ n'est pas un corps, alors $\langle X \rangle$ n'est pas maximal.*
3. *Si $\varphi : \mathcal{A} \to \mathcal{B}$ est un morphisme d'anneau avec $\mathcal{B}$ intègre , alors $\ker \varphi$ est un idéal premier de $\mathcal{A}$*
4. *Si $\varphi : \mathcal{A} \to \mathcal{B}$ est un morphisme d'anneau, alors pour tout idéal premier $\mathcal{I} \subset \mathcal{B}$, $f^{-1}(\mathcal{I})$ est un idéal premier de $\mathcal{A}$.*

7 Anneau Euclidien

Définition 1.54 *Un anneau $\mathcal{A}$ est dit euclidien si il est intègre et si il existe une application $N : \mathcal{A}\setminus\{0\} \to \mathbb{N}$ tel que pour tout $a \in \mathcal{A}$ et $b \in \mathcal{A}\setminus\{0\}$, il existe $(q, r) \in \mathcal{A}\times\mathcal{A}$ vérifiant*

$$a = ba + r \textbf{ et } N(r) < N(b) \text{ si } r \neq 0.$$

Proposition 1.55 *L'anneau $\mathcal{A}[x]$ est euclidien si, et seulement si, $\mathcal{A}$ est un corps.*

Exemple 1.56
1. *$\mathbb{Z}[X]$ n'est pas euclidien car $\mathbb{Z}$ n'est pas un corps.*
2. *$\mathbb{Z}/p\mathbb{Z}[X]$ est euclidien si, et seulement si, p est premier*

8 Anneau principal

Définition 1.57 *Un anneau $\mathcal{A}$ est dit principal s'il est intègre et tout idéal de $\mathcal{A}$ est principal.*

Exemple 1.58
— *$\mathbb{Z}$ est un anneau principal*
— *$\mathbb{R}[X]$, et plus généralement $\mathbb{K}[X]$ avec $\mathbb{K}$ un corps, est principal.*
— *$\mathbb{Z}[X]$ n'est pas principal car par exemple $\mathcal{I} = 2P + XQ, P, Q \in \mathbb{Z}[X]$ n'est pas principal.*

Proposition 1.59 *Dans un anneau principal, un idéal non nul est premier si, et seulement si, il est maximal.*

Proposition 1.60 *Tout anneau euclidien est principal*

Proposition 1.61 *(Lemme D'Euclide)*
Dans un anneau principal un élément est premier si, et seulement si, il est irréductible.

9 Anneau factoriel

Définition 1.62 *Un anneau $\mathcal{A}$ est dit factoriel s'il est intègre et vérifie les deux conditions suivante :*

1. *Tout élément $a \in \mathcal{A}$ non nul et non inversible se décompose en produit d'éléments irréductibles, c'est à dire qu'il existe $p_1, ..., p_r \in \mathcal{A}$ qui sont irréductibles tels que $a = p_1 \dots p_r$.*
2. *La décomposition précédente est unique dans le sens suivant : si $a = p_1, ..., p_r = q_1, ..., q_s$ avec $a = p_1, ..., p_r$ et $q_1, ..., q_s$ irréductibles, alors $r = s$ et il existe une permutation σ de l'ensemble $\{1, ..., r\}$ telle que $p_i = q_{\sigma(i)}$ pour tout $i = 1, \dots, r$.*

Proposition 1.63 *Tout anneau principal est factoriel.*

Proposition 1.64 *Dans un anneau factoriel un élément est premier si, et seulement si, il est irréductible.*

Définition 1.65 *Soit $\mathcal{A}$ un anneau factoriel et soit $P = a_0 + a_1 X + \dots + a_n X^n \in \mathcal{A}[X]$. On appelle le contenu de P, noté $c(P)$, le pgcd de ses coefficients.*

Définition 1.66 *On dit qu'un polynôme $P \in \mathcal{A}[X]$ est primitif si son contenu est inversible.*

Proposition 1.67 *Pour tout $P, Q \in \mathcal{A}[X]$, on a $c(PQ) = c(P)c(Q)$. En particulier, si P et Q sont primitifs, alors PQ est primitif.*

Théorème 1.68 *Si $\mathcal{A}$ est factoriel alors $\mathcal{A}[X]$ est factoriel.*

Exemple 1.69 — *L'anneau $\mathbb{Z}[X]$ est factoriel*
— *L'anneau $\mathcal{A}[X]$ avec $\mathcal{A} = \mathbb{Z}[\sqrt{-3}]$ n'est pas factoriel.*

Théorème 1.70 *Soit $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$ et soit p un nombre premier, $p \in \mathbb{N}$.*
On suppose que $\overline{a}_n \neq \overline{0}$ dans $\mathbb{Z}/p\mathbb{Z}$ et que le polynôme $\overline{P} = \overline{a}_0 + \overline{a}_1X + \cdots + \overline{a}_nX^n \in \mathbb{Z}/p\mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$. Alors P est irréductible dans $\mathbb{Q}[X]$. Si de plus P est primitif, alors il est irréductible dans $\mathbb{Z}[X]$.

On en déduit le corollaire suivant :

Corollaire 1.71 *(Critère D'Eisenstein)*
Soit $P = a_0+a_1X+\cdots+a_nX^n \in \mathbb{Z}[X]$ avec $\deg P \geqslant 1$. On suppose qu'il existe un nombre premier p tel p divise a_i pour tout $i = 0, \ldots, n-1$, avec p qui ne divise pas a_n et p^2 ne divise pas a_0. Alors P est irréductible dans $\mathbb{Q}[X]$ et si de plus P est primitif, alors il est irréductible dans $\mathbb{Z}[X]$.

10 Anneau Local et corps des résidus

Définition 1.72 *Un anneau $\mathcal{A}$ est dit Local si il admet exactement un idéal maximal M et $\mathcal{A}/M$ est son corps des résidus.*

Exemple 1.73 *Un corps $\mathbb{K}$ est dit local si $\{0\}$ est son seul idéal maximal et $\mathbb{K} \cong \mathbb{K}/\{0\}$ est son propre corps des résidus.*

11 Corps finis

Définition 1.74 *Un corps fini est un corps ayant un nombre fini d'éléments.*

Théorème 1.75 (Théorème de Wedderburn) *Tout corps fini est commutatif.*

Théorème 1.76 *$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier*

11.1 Cardinal et caractéristique d'un corps fini

Soit $\mathbb{K}$ un corps fini. Posons

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{K} \\ n &\longrightarrow n.1 \end{aligned}$$

$$\text{où } \ n.1 = \begin{cases} 1+1+\cdots+1 & (n \text{ fois }) \quad si \ \ n>0, \\ 0 & si \quad n=0, \\ (-1)+(-1)+\cdots+(-1) & (-n \text{ fois }) \quad si \ \ n<0. \end{cases}$$

L'application f est un morphisme d'anneaux et on a

$$\ker f \ = \{m \in \mathbb{Z} \ : m.1 = 0\}.$$

Comme $\ker f$ est un idéal de $\mathbb{Z}$, il est donc de la forme $p\mathbb{Z}$, $p \in \mathbb{N}$, d'où $\mathbb{Z}/\ker f \ = \mathbb{Z}/p\mathbb{Z} \simeq f(\mathbb{Z})$. Comme $\mathbb{K}$ est un corps fini, il est intègre et tout sous-anneau de $\mathbb{K}$ est intègre, d'où $f(\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$ est intègre. On en déduit que p est premier.

Donc tout corps fini $\mathbb{K}$ contient une copie de $\mathbb{Z}/p\mathbb{Z}$, où p est un nombre premier. Autrement dit, $\mathbb{K}$ est une extension de $\mathbb{Z}/p\mathbb{Z}$. Remarquons que le nombre premier p est la caractéristique du corps $\mathbb{K}$, i.e., le plus petit entier strictement positif tel que $p.1 = 0$.

Théorème 1.77 *Soit $\mathbb{K}$ un corps fini, alors le cardinal de $\mathbb{K}$ est égal à p^n, où p est un nombre premier et n est un entier naturel non nul.*

Définition 1.78 *Le nombre premier p est appelé caractéristique du corps $\mathbb{K}$ et $\mathbb{Z}/p\mathbb{Z}$ est appelé corps premier de $\mathbb{K}$.*

Théorème 1.79 *a) Pour tout nombre premier p et pour tout $n \in \mathbb{N}^*$, il existe un corps fini à p^n éléments.*
b) Deux corps finis ayant le même nombre d'éléments sont isomorphes.

11.2 Exemples de construction de corps finis

Pour construire un corps fini à p^n éléments, on se donne un polynôme unitaire irréductible $f(x)$ sur $\mathbb{F}_p$, de degré n, puis on considère l'anneau quotient $\mathbb{F}_p[x]/(f(x))$ qui est un corps à p^n éléments. On rappelle que $(f(x))$ désigne l'idéal de $\mathbb{F}_p[x]$ engendré par le polynôme $f(x)$ et que l'on a l'isomorphisme de corps

$$\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_p[\alpha],$$

où α est une racine de $f(x)$ dans une clôture algébrique de $\mathbb{F}_p$. Dans la suite, après avoir choisi un polynôme unitaire et irréductible de degré n, on écrira simplement

$$\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha].$$

Exemple 1.80 *Le corps* $\mathbb{F}_8$.
Le polynôme $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ *est irréductible car il est de degré* 3 *et n'admet pas de racine dans* $\mathbb{F}_2$ *puisque* $f(0) = f(1) = 1$. *On a donc*

$$\mathbb{F}_8 = \mathbb{F}_2[\alpha] = \{a\alpha^2 + b\alpha + c : a, b, c \in \mathbb{F}_2 \text{ et } \alpha^3 + \alpha + 1 = 0\}.$$

Exemple de calcul dans $\mathbb{F}_8$ *:*

$$\begin{aligned} \text{On a } (\alpha^2 + \alpha + 1)(\alpha^2 + \alpha) &= \alpha + \alpha^2 + \alpha^2 + \alpha^3 + \alpha^3 + \alpha^4 = \alpha + \alpha^4. \\ &= \alpha + \alpha(\alpha^3) = \alpha + \alpha(\alpha + 1) = \alpha + \alpha^2 + \alpha. \\ &= \alpha^2. \end{aligned}$$

Remarquons que :

$$\alpha^3 = 1 + \alpha, \alpha^4 = \alpha + \alpha^2, \alpha^5 = 1 + \alpha + \alpha^2, \alpha^6 = 1 + \alpha^2 \text{ et } \alpha^7 = 1.$$

Exemple 1.81 *Le corps* $\mathbb{F}_{16}$.
Le polynôme $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ *est irréductible. En effet,* $f(0) = f(1) = 1 \neq 0$, *donc* $f(x)$ *n'a pas de racine dans* $\mathbb{F}_2$ *; de plus* $(x^2+x+1)^2 = x^4+x^2+1 \neq f(x)$, *et* x^2+x+1 *est le seul polynôme irréductible de degré* 2 *sur* $\mathbb{F}_2$. *On a donc*

$$\mathbb{F}_{16} = \mathbb{F}_2[\alpha] = \{a\alpha^3 + b\alpha^2 + c\alpha + d : a, b, c, d \in \mathbb{F}_2\}.$$

11.3 Automorphismes d'un corps fini

Il est facile de vérifier que l'ensemble des automorphismes d'un corps $\mathbb{K}$ forme un groupe pour la composition des applications. Ce groupe est noté $Aut(\mathbb{K})$.

Proposition 1.82 *Soit* $\mathbb{F}$ *un corps fini de caractéristique p. Alors l'application* $\sigma : \mathbb{F} \to \mathbb{F}$ *définie par* $\sigma(a) = a^p$ *est un automorphisme de* $\mathbb{F}$.

Définition 1.83 *L'automorphisme* φ *est appelé automorphisme de Frobenius.*

Théorème 1.84 *Soit* $q = p^n, p$ *premier. Alors le groupe des automorphismes de* $\mathbb{F}_q$ *est un groupe cyclique d'ordre n engendré par l'automorphisme de Frobenius. Autrement dit :*

$$Aut\left(\mathbb{F}_q\right) = \left\{\sigma, \sigma^2, \cdots, \sigma^n = id\right\}.$$

Exemple 1.85 *Le groupe des automorphismes $G = Aut(\mathbb{F}_{16})$ du corps $\mathbb{F}_{16} = \mathbb{F}_{2^4}$ est donné par*

$$G = \left\{\sigma, \sigma^2, \sigma^3, \sigma^4 = id\right\},$$

où σ est l'automorphisme de Frobenius défini par $\sigma(a) = a^2$, pour tout $a \in \mathbb{F}_{16}$. Comme G est cyclique, alors il possède un unique sous-groupe propre, qui est d'ordre 2 : $H = \left\{id, \sigma^2\right\}$. Ce sous-groupe correspond à l'unique sous-corps propre de $\mathbb{F}_{16}$:

$$\begin{aligned} K &= \{a \in \mathbb{F}_{16} : g(a) = a, \forall a \in \mathbb{F}_{16}\} \\ &= \left\{a \in \mathbb{F}_{16} : a^{2^2} = a, \forall a \in \mathbb{F}_{16}\right\} = \mathbb{F}_4. \end{aligned}$$

11.4 Polynômes irréductibles sur $\mathbb{F}_q$

Théorème 1.86 *Soit $f(x)$ un polynôme irréductible de degré m dans $\mathbb{F}_q[x]$. Alors le corps de décomposition (ou corps des racines) de $f(x)$ sur $\mathbb{F}_q$ est $\mathbb{F}_{q^m}$. En particulier deux polynômes irréductibles $f(x)$ et $g(x)$ de même degré sur $\mathbb{F}_q[x]$ admettent le même corps de décomposition, à isomorphisme près.*

Théorème 1.87 *Tout polynôme irréductible $f(x)$ de $\mathbb{F}_q[x]$ de degré m possède exactement m racines distinctes dans $\mathbb{F}_{q^m}$. Si α est l'une de ses racines, toutes les autres racines sont données par*

$$\alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}}. \tag{1.1}$$

Théorème 1.88 *Soit $q = p^n$ et posons*

$$\mu_d = \left\{f(x) \in \mathbb{F}_p[x] : f(x) \text{ irréductible unitaire de degré } d\right\}, \tag{1.2}$$

alors on a

$$x^q - x = \prod_{\substack{f(x) \in \mu_d \\ d|n}} f(x). \tag{1.3}$$

Exemple 1.89 *Sur $\mathbb{F}_2$, on a*

$$\begin{aligned} x^{16} - x &= x^{2^4} - x = \prod_{\substack{f(x) \in \mu_d \\ d|4}} f(x) = \prod_{f(x) \in \mu_1} f(x) \prod_{f(x) \in \mu_2} f(x) \prod_{f(x) \in \mu_4} f(x) \\ &= x(x+1)\left(x^2 + x + 1\right)\left(x^4 + x + 1\right)\left(x^4 + x^3 + 1\right)\left(x^4 + x^3 + x^2 + x + 1\right). \end{aligned}$$

Lemme 1.90 *Soit $f(x) \in \mathbb{F}_q[X]$ de degré m avec $f(0) \neq 0$, alors il existe un entier $e \leq q^m - 1$ tel que $f(x)$ divise $x^e - 1$.*

Définition 1.91 *Soit $f(x) \in \mathbb{F}_q[X]$, $f(x) \neq 0$. Si $f(0) \neq 0$, le plus petit entier e tel que $f(x)$ divise $x^e - 1$ est appelé ordre de $f(x)$, on le note $e(f)$. Si $f(0) = 0$, on écrit $f(x) = x^k g(x)$ avec $g(x) \neq 0$, et on pose par définition $e(f) = e(g)$.*

Théorème 1.92 *Soit $f(x) \in \mathbb{F}_q[X]$ irréductible de degré m, tel que $f(0) \neq 0$. Alors l'ordre de $f(x)$ est égal à l'ordre d'une racine de $f(x)$ dans le groupe multiplicatif $\mathbb{F}_{q^m}^*$.*

Corollaire 1.93 *Soit $f(x) \in \mathbb{F}_q[X]$ irréductible de degré m, alors $e(f)$ divise $q^m - 1$.*

Chapitre 2

Résultant de deux polynômes sur un anneau commutatif

Dans ce chapitre, nous rappelons la définition du résultant de deux polynômes sur un anneau commutatif ainsi que ses propriétés que nous utiliserons dans le dernier chapitre.

1 Résultant de deux polynômes

Soit A un anneau commutatif et soit l'ensemble $P_k = \{p \in K[x] : deg(p) < k\}$, où k est un entier positif. L'ensemble P_k est un espace vectoriel de dimension sur k. Soient m et n deux entiers naturels et l'application

$$\begin{aligned} \phi : P_n \times P_m &\longrightarrow P_{n+m} \\ (s,t) &\mapsto sf + tg, \end{aligned}$$

où f et g sont des polynômes de $A[x]$ tels que :

$$f(x) = \sum_{i=0}^{m} a_i x^i, \tag{2.1}$$

et

$$g(x) = \sum_{i=0}^{n} b_j x^j. \tag{2.2}$$

Soient $\mathcal{B} = \{(x^{n+m}, x^{n+m-1} \ldots, 1)\}$ une base de P_{n+m} et

$$\mathcal{B}' = \{(x^{n-1}, 0), (x^{n-2}, 0) \ldots, (1,0), (0, x^{m-1}), (0, x^{m-2}), \ldots, (0,1)\}$$

une base de $P_n \times P_m$.
La matrice associée à ϕ pour ces deux bases est la matrice carrée de taille $(n+m)$, appelée matrice de Sylvester de f et g, et notée $Sylv(f,g)$, elle est définie par

$$Sylv(f,g) = \begin{pmatrix} a_m & 0 & \cdots & 0 & b_n & 0 & \cdots & \cdots & 0 \\ a_{m-1} & a_m & \ddots & 0 & b_{n-1} & b_n & & & \\ \vdots & a_{m-1} & \ddots & \vdots & \vdots & b_{n-1} & \ddots & & \\ \vdots & \vdots & \ddots & a_m & b_0 & \vdots & & \ddots & \\ a_0 & \vdots & & \vdots & 0 & b_0 & & & b_n \\ 0 & a_0 & \vdots & \vdots & \vdots & \ddots & \ddots & & \\ \vdots & \ddots & \ddots & & & & & \ddots & \\ 0 & \cdots & 0 & a_0 & 0 & \cdots & \cdots & 0 & b_0 \end{pmatrix}.$$

Remarquons que les coefficients de f sont reproduits sur m colonnes et ceux de g sur n colonnes. Le déterminant de $Sylv(f,g)$ est donné en fonction des coefficients de f et g et est appelé **Résultant** de f et g , noté $Res_x(f,g)$ ou simplement $Res(f,g)$.

Propriétés 2.1 *Soit A un anneau commutatif. On pose*

$$f(x) = \sum_{i=0}^{m} a_i x^i \in A[x], \tag{2.3}$$

et

$$g(x) = \sum_{j=0}^{n} b_j x^j \in A[x]. \tag{2.4}$$

1. $Res(f,g) \in A$.
2. $Res(f,g) = (-1)^{mn} Res(g,f)$.
3. $\forall a \in A, Res(af,g) = a^m Res(f,g)$.

Démonstration 2.2 *Voir [20] et [17].*

Par définition, on pose :

1. $Res(a,b) = 1$, $\forall a, b \in A$.
2. $\forall a \in A, Res(a,g) = a^n$

2 Polynômes symétriques des racines

Soit A un anneau intègre et $f_m(x) = \prod_{i=1}^{m}\left(x-\alpha_i\right) = \sum_{i=0}^{m} a_i^{(m)} x^i \in A[x]$, où les α_i , $0 \leq i \leq m$, sont les racines de $f_m(x)$ dans une clôture algébrique du corps des fractions de A. On définit

$$\begin{aligned} a_m^{(m)} &= S_m = 1, \\ -a_{m-1}^{(m)} &= S_{m-1} = \alpha_1 + \alpha_2 + \cdots + \alpha_m, \\ a_{m-2}^{m} &= S_{m-2} = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \cdots + \alpha_{m-1}\alpha_m, \\ &\vdots \\ (-1)^m a_0^{(m)} &= S_0 = \alpha_1\alpha_2 \ldots \alpha_m. \end{aligned}$$

Les S_i, $0 \leq i \leq m$, sont appelés les polynômes symétriques élémentaires des racines de $f_m(x)$.

Les coefficients $a_i^{(m)}$ sont linéaires en α_m. On pose $f_{m-1}(x) = \dfrac{f_m(x)}{x-\alpha_m}$. Entre les coefficients de f_m et f_{m-1} considérés comme des polynômes en α_i, on a la relation

$$a_{i-1}^{(m-1)}(\alpha_1, \cdots, \alpha_{m-1}) = a_i^{(m)}(\alpha_1, \cdots, \alpha_{m-1}, 0). \tag{2.5}$$

Lemme 2.3 *Soient A un anneau intègre et $g \in A[x]$ tel que* $\deg(g) > 0$. *Soit m un entier tel que $m > 1$. On pose $f_m(x) = \prod_{i=1}^{m}(x-\alpha_i)$ et $f_{m-1}(x) = \dfrac{f_m(x)}{x-\alpha_m}$, alors*

$$Res(f_m, g) = g(\alpha_m) Res(f_{m-1}, g). \tag{2.6}$$

Démonstration 2.4 *Pour $1 \leq i < m+n$, on ajoute à la dernière colonne de la matrice de sylvester $Sylv(f_m, g) = M$, α_m^{m+n-1} fois la ième colonne. Appelons la matrice obtenue M_1. On a* $\det(M_1) = \det(M)$ *et les éléments de la dernière colonne de haut-en-bas sont : $\alpha_m^{n-1} f_m(\alpha_m), \cdots, \alpha_m^0 f_m(\alpha_m), \alpha_m^{m-1} g(\alpha_m), \cdots, \alpha_m^0 g(\alpha_m)$. Comme $f_m(\alpha_m) = 0$, faisons sortir le facteur $g(\alpha_m)$ de la dernière colonne et on obtient la matrice M_2 dont la dernière colonne est $0, \cdots, 0, \alpha_m^{m-1}, \cdots, \alpha_m^0$ et*

$$Res(f_m, g) = Det(M) = Det(M_1) = g(\alpha_m) Det(M_2). \tag{2.7}$$

Considérons les deux membres de l'égalité (2.7) *comme des polynômes en α_m. Comme M admet n lignes constituées des coefficients de $f(\alpha_m)$ qui sont au plus linéaires en α_m, le membre de gauche de l'égalité est de degré inférieur ou égal à n en α_m. Dans le*

membre de droite, le facteur $g(\alpha_m)$ est déjà de degré n. Comme R est un anneau intègre $\det(M_2)$ *est de degré* 0 *en* α_m. *Considérons* $\det(M_2)$ *en* $\alpha_m = 0$, *la dernière colonne sera égal à* $0, \cdots, 0, \cdots, 1$ *et les coefficients de* f_m *sont remplacés par les coefficients de* f_{m-1}, *d'après la relation* (2.5). *En développant* $\det(M_2)\,|_{\alpha_m=0}$ *suivant la dernière colonne, on obtient une matrice* $(m+n-1)\times(m+n-1)$ *avec* $\det(M_3) = \det(M_2) = Res(f_{m-1}, g)$ *et en utilisant la propriété* 3, *on a la preuve du lemme.*

Théorème 2.5 *Soit A un anneau intègre. Soient* $f, g \in A[x]$ *tels que* $f(x) = a_m \prod_{i=1}^{m} \left(x - \alpha_i\right)$ *et* $g(x) = b_n \prod_{j=1}^{n} \left(x - \beta_j\right)$, *avec* α_i *et* β_i *les racines respectives de* f *et* g, a_m *et* b_n *leurs coefficients dominants respectifs, alors*

$$Res(f, g) = (-1)^{mn} b_n^m \prod_i f(\beta_i), \tag{2.8}$$

$$Res(f, g) = a_m^n b_n^m \prod_i \prod_j (\alpha_i - \beta_j), \tag{2.9}$$

$$Res(f, g) = a_m^n \prod_i g(\alpha_i). \tag{2.10}$$

Démonstration 2.6 *Si* $m = 0$ *ou* $n = 0$, *les relations sont vraies avec la convention* $\prod_{i=k}^{l} (x - \alpha_i) = 1$, *pour* $l < k$. *Montrons (2.8). On a vu que :*

$$Res(f, g) = (-1)^{nm} \cdot Res(g, f),$$

alors, d'après (2.10), on obtient (2.8).

Maintenant, on prouve (2.10). En calculant le résultant de $f_1 = x - \alpha_1$ *et g, on a*

$$Res(f_1, g) = g(\alpha_1).$$

On sait que $Res(af, g) = a^n Res(f, g)$.

Posons $f_n = \prod_{i=1}^{n}(x-\alpha_i)$ *et en appliquant le lemme (2.3) sur les* f_i, $1 \leq i \leq n$, *nous aurons*

$$\begin{aligned} Res(f,g) &= a_n^m Res(f_n,g), \\ &= a_n^m g(\alpha_1) Res(f_{n-1},g), \\ &= a_n^m g(\alpha_1) g(\alpha_2) Res(f_{n-2},g), \\ &\vdots \\ &= a_n^m g(\alpha_1)\dots g(\alpha_n), \\ &= a_n^m \prod_{i=1}^{n} g(\alpha_i). \end{aligned}$$

On montre facilement (2.9) :

$$\begin{aligned} Res(f,g) &= a_n^m \prod_{i=1}^{n} g(\alpha_i), \\ &= a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}\left(\alpha_i - \beta_j\right). \end{aligned}$$

Remarque 2.7 *Si* f *et* $g \in A[x,y]$, *on note,* $Res_x(f,g)$ *le résultant dans* $A[y]$ *par rapport à* x.

Théorème 2.8 *Soit* K *un corps commutatif. Si* $f,g \in K[x]$ *admettent une racine commune dans* K *alors* $Res(f,g) = 0$.

Démonstration 2.9 *Conséquence immédiate de (2.8).*

Théorème 2.10 *[20] Soit* A *un anneau intègre et soient* f, g_1 *et* g_2 *des polynômes dans* $A[x]$. *Alors*

$$Res(f, g_1 g_2) = Res(f,g_1) Res(f,g_2).$$

Le théorème 2.10 nous permet de calculer facilement le résultant de deux polynômes si on connait la factorisation de l'un d'entre eux. Par exemple,

$$Res(f, x^k g) = Res(f,g) \prod_{i=0}^{k} Res(f,x), \tag{2.11}$$

et comme $Res(f,x) = (-1)^m f(0) = (-1)^m a_0$, alors

$$Res(f, x^k g) = (-1)^{mk} a_0^k Res(f,g). \tag{2.12}$$

Théorème 2.11 (Rüdiger Loos) *Soit A un anneau intègre et soient $f, g \in A[x]$ tels que*

$$f(x) = a_n \prod_{i=1}^{n} \Big(x - \alpha_i\Big), g(x) = b_m \prod_{j=1}^{m} \Big(x - \beta_j\Big), \tag{2.13}$$

et $deg(f) = n > 0$, $deg(g) = m > 0$, α_i, β_j leurs racines respectives. Alors, le polynôme

$$r(x) = (-1)^{mn} Z a_n^m b_m^n \prod_{i} \prod_{j} \Big(x - \gamma_{ij}\Big)$$

est de degré nm et admet nm racines, pas nécessairement distinctes, telles que :

1. $r(x) = Res(f(x-y), g(y)), \gamma_{ij} = \alpha_i + \beta_j, Z = 1.$
2. $r(x) = Res(f(x+y), g(y)), \gamma_{ij} = \alpha_i - \beta_j, Z = 1.$
3. $r(x) = Res(y^m f(x/y), g(y)), \gamma_{ij} = \alpha_i \beta_j, Z = 1.$
4. $r(x) = Res(f(xy), g(y)), \gamma_{ij} = \alpha_i / \beta_j, Z = (-1)^{nm} g_0^m \Big/ b_m^n$ *où* $g_0 = \beta_1 \beta_2 \cdots \beta_m$.

Démonstration 2.12 *[20]*
On démontre les quatre formules en utilisant la relation (2.8).

1.

$$\begin{aligned} Res_y(f(x-y), g(y)) &= (-1)^{nm} b_m^n \prod_{j=1}^{m} f(x - \beta_j) \\ &= (-1)^{nm} a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} \Big(x - \beta_j - \alpha_i\Big) \\ &= (-1)^{nm} a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} \Big(x - (\alpha_i + \beta_j)\Big). \end{aligned}$$

2.

$$\begin{aligned} Res_y(f(x+y), g(y)) &= (-1)^{nm} b_m^n \prod_{j=1}^{m} f(x + \beta_j) \\ &= (-1)^{nm} a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} \Big(x + \beta_j - \alpha_i\Big) \\ &= (-1)^{nm} a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} \Big(x - (\alpha_i - \beta_j)\Big). \end{aligned}$$

3.

$$\begin{aligned} Res_y\Big(y^n f(x/y), g(y)\Big) &= (-1)^{nm} b_m^n \prod_{j=1}^{m} \beta_j^n f(x/\beta_j) \\ &= (-1)^{nm} a_n^m b_m^n \prod_{j=1}^{m}\prod_{i=1}^{n} \beta_j^n (\frac{x}{\beta_j} - \alpha_i) \\ &= (-1)^{nm} a_n^m b_m^n \prod_{j=1}^{m}\prod_{i=1}^{n} \Big(x - \alpha_i\beta_j\Big). \end{aligned}$$

4.

$$\begin{aligned} Res_y\Big(f(xy), g(y)\Big) &= (-1)^{nm} b_m^n \prod_{j=1}^{m} f(x\beta_j) \\ &= (-1)^{nm} b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m} (x\beta_j - \alpha_i) \\ &= (-1)^{nm} a_n^m \Big(\prod_{i=1}^{n} b_m\Big)\Big(\prod_{j=1}^{m} \beta_j\Big)\prod_{j=1}^{m}\Big(x - \frac{\alpha_i}{\beta_j}\Big) \\ &= (-1)^{nm} a_n^m g_0^m \prod_{j=1}^{m}\prod_{i=1}^{n}\Big(x - \frac{\alpha_i}{\beta_j}\Big) \end{aligned}$$

Lemme 2.13 *Soit A un anneau intègre. Soient $f, g \in A[x]$ deux polynômes non nuls. Soit I un idéal de A. Soit $a \in A$. On note par $\overline{a}$ la classe de a modulo I. On suppose que $\overline{C_f} \neq 0$. Alors*

$$\overline{Res(f,g)} = 0 \Leftrightarrow Res(\bar{f}, \bar{g}) = 0.$$

Démonstration 2.14 *Soient $f = \sum_{i=0}^{m} f_i x^i \in A[x]$ et $g = \sum_{j=0}^{j=n} g_j x^j \in A[x]$, de degrés respectifs m et n.*
Si le degré de f est nul alors $Sylv(f,g) = fI_n$ et $Sylv(\overline{f},\overline{g}) = \overline{f}I_n$. Donc $\overline{Res(f,g)}$ et $Res(\overline{f},\overline{g})$ sont non nuls et l'équivalence est vérifiée. Supposons alors que le degré de f est ≥ 1. Si $\overline{g} = 0$ alors $Res(\overline{f},\overline{g}) = 0$ et les m dernières colonnes de $Sylv(f,g)$ qui contiennent les g_i s'annulent modulo I. On a donc $\overline{Res(f,g)} = 0$.
Si $\overline{g} \neq 0$. Soit i le plus petit indice tel que $\overline{g_{n-i}} \neq 0$, alors $\overline{Sylv(f,g)}$ est de la forme

$$\begin{pmatrix} T & 0 \\ U & V \end{pmatrix},$$

où T est une matrice carrée de taille i et triangulaire inférieure avec des $\overline{f_m}$ sur la diagonale, et V est une matrice carrée de taille $n-i$. On en déduit que $\overline{Res(f,g)} = \overline{f_m^i} Res(\overline{f},\overline{g})$. D'où le résultat.

Chapitre 3

Produit composé de polynômes à coefficients dans un corps fini

Soient $f(x)$ et $g(x)$ deux polynômes à coefficients dans $\mathbb{F}_q$ de degrés respectifs m et n alors la composition additive de f et g notée $f * g$, est un polynôme de degré mn dont les racines sont les sommes des racines de f et g. La composition multiplicative de f et g notée $f \circ g$, est un polynôme de degré mn dont les racines sont les produits des racines de f et des racines de g. En 1987, Brawley et Carlitz ont défini une notion plus générale de la composition des polynômes, notée $f \diamond g$, pour laquelle $f * g$ et $f \circ g$ sont des cas particuliers. Dans ce chapitre, nous définissons le produit composé $\diamond$ de deux polynômes à coefficients dans $\mathbb{F}_q$ et ses propriétés. Nous donnons quelques exemples de lois composées induites par le produit composé. Nous exposons une démonstration détaillée d'un théorème établi par Brawley et Carlitz [9] sur le produit composé de deux polynômes irréductibles. À la fin du chapitre, nous donnons un algorithme qui permet de calculer ce produit.

1 Le produit composé $\diamond$ et ses propriétés

Soit $\mathbb{F}_q$ un corps fini, $q = p^n$. Soient $f(x)$ et $g(x)$ deux polynômes unitaires dans $\mathbb{F}_q[x]$. La composition multiplicative de f et g est définie par

$$f \circ g = \prod_{\alpha} \prod_{\beta} (x - \alpha\beta).$$

Le produit est calculé sur toutes les racines de f et toutes les racines de g.
Dans l'article de Brawley et Carlitz, cette notion a été généralisée comme suit.

Soit G un sous-ensemble non vide de la clôture algébrique Γ_q de $\mathbb{F}_q$ avec la propriété que G est invariant par l'automorphisme de Frobenius $\alpha \longrightarrow \sigma(\alpha) = \alpha^q$. On définit sur G une loi interne notée $\diamond$, vérifiant

$$\forall \alpha, \beta \in G, \sigma(\alpha \diamond \beta) = \sigma(\alpha) \diamond \sigma(\beta) \in G. \tag{3.1}$$

Exemples 3.1

1. $G = \Gamma_q \setminus \{0\}$, $\alpha \diamond \beta = \alpha\beta$.
2. $G = \Gamma_q$, $\alpha \diamond \beta = \alpha + \beta - c$, *où* $c \in \mathbb{F}_q^*$.
3. $G = \Gamma_q \setminus \{1\}$, $\alpha \diamond \beta = \alpha + \beta - \alpha\beta$.
4. G : *Un sous-ensemble* $\sigma-$*invariant de* Γ_q, $\alpha \diamond \beta = f(\alpha, \beta)$, *où* $f(x, y) \in \mathbb{F}_q[x, y]$ *est un polynôme fixé de* $\mathbb{F}_q[x]$ *tel que* $f(\alpha, \beta) \in G$, $\forall \alpha, \beta \in G$.

$(G, \diamond)$ est un groupe abélien dans les trois premiers exemples et le dernier exemple généralise les trois autres exemples.
Soit G un sous-ensemble non vide de la clôture algébrique Γ_q de $\mathbb{F}_q$, invariant par l'automorphisme de Frobenius $\alpha \longrightarrow \sigma(\alpha) = \alpha^q$. Notons P_G, l'ensemble de tous les polynômes unitaires f à coefficients dans $\mathbb{F}_q$ tels que $deg(f) \geq 1$ dont les racines sont dans G.
Soient $f, g \in P_G$, le produit composé, noté $f \diamond g$, est le polynôme défini par

$$f \diamond g = \prod_{\alpha} \prod_{\beta} (x - \alpha \diamond \beta), \tag{3.2}$$

où le produit est calculé sur toutes les racines de f et toutes les racines de g.
On a

$$degf \diamond g = (degf)(degg).$$

La loi $\diamond$ est une loi de composition interne. En effet, comme σ permute les racines de n'importe quel polyôme de $\mathbb{F}_q[x]$, donc si $k = f \diamond g$, alors

$$(k(x))^q = \prod_{\alpha} \prod_{\beta} (x^q - (\alpha^q \diamond \beta^q)) = \prod_{\alpha} \prod_{\beta} (x^q - (\alpha \diamond \beta)) = k(x^q),$$

donc $k \in \mathbb{F}_q[x]$.
Si la loi $\diamond$ est associative (respectivement commutative) dans G, alors la loi $\diamond$ est associative (respectivement commutative) dans P_G.
Si e est l'élément neutre de G, alors $\alpha \diamond e = e \diamond \alpha = \alpha$, $\forall \alpha \in G$. Donc $\sigma(\alpha) \diamond \sigma(e) = \sigma(e) \diamond \sigma(\alpha) = \sigma(\alpha)$, et comme σ est un isomorphisme et $\sigma(e) = e$, donc $e \in \mathbb{F}_q$. Alors, $x - e$ est l'élément neutre de P_G.

Théorème 3.2 *Soit $(G,\diamond)$ un sous-ensemble fini de Γ_q vérifiant la condition (1.3). Alors, il existe $h(x,y) \in \mathbb{F}_q[x,y]$ tel que $h(\alpha,\beta) = \alpha \diamond \beta$, $\forall \alpha,\beta \in G$.*

Démonstration 3.3 *Soit $G = \{\alpha_1, \alpha_2, ..., \alpha_t\}$ un ensemble de cardinal t. D'après l'interpolation de Lagrange*

$$h(x,y) = \sum_{1\leq i,j\leq t} \Big(\alpha_i \diamond \alpha_j\Big) \frac{S_i(x)}{W_i} \frac{S_j(y)}{W_j}, \tag{3.3}$$

où $S_i(x) = \prod\limits_{\substack{\alpha\in G \\ \alpha\neq\alpha_i}} (x-\alpha)$ et $W_i = \prod\limits_{\substack{\alpha\in G \\ \alpha\neq\alpha_i}} (\alpha_i - \alpha)$.

On a

$$h(\alpha,\beta) = \alpha \diamond \beta, \forall \alpha,\beta \in G. \tag{3.4}$$

Montrons que $h(x,y) \in \mathbb{F}_q[x,y]$. Comme G est $\sigma-$invariant, σ induit une permutation des éléments de G, alors comme la somme se fait sur tous les couples (i,j), on a

$$\begin{aligned}(h(x,y))^q &= \sum_{(i,j)} \left(\Big(\alpha_i \diamond \beta_j\Big) \frac{S_i(x)}{W_i} \frac{S_j(y)}{W_j}\right)^q \\ &= \sum_{(i,j)} \alpha_{\sigma(i)} \diamond \beta_{\sigma(i)} \frac{S_{\sigma(i)}(x^q)}{W_{\sigma(i)}} \frac{S_{\sigma(j)}(y^q)}{W_{\sigma(j)}},\end{aligned}$$

où $\alpha_i^q = \alpha_{\sigma(i)}$ et $\beta_j^q = \beta_{\sigma(j)}$ et comme σ permute les éléments de G, alors

$$(h(x,y))^q = h(x^q, y^q). \tag{3.5}$$

Donc, les coefficients de $h(x,y)$ sont dans $\mathbb{F}_q$.

Réciproquement. étant donné un polynôme $h(x,y) \in \mathbb{F}_q[x,y]$, on peut définir une loi de composition interne $\diamond$ sur un sous-ensemble G adéquat de la clôture algébrique de $\mathbb{F}_q$ en utilisant $h(x,y)$ comme le stipule le théorème suivant :

Théorème 3.4 *Soit $h(x,y) \in \mathbb{F}_q[x,y]$. Pour tout sous-ensemble S non vide de Γ_q, il existe un plus petit sous-ensemble G (au sens de l'inclusion) de Γ_q contenant S tel que :*

1. *G est σ-invariant.*
2. *La loi $\diamond$ définie par $\alpha \diamond \beta = h(\alpha,\beta)$ est une loi de composition interne satisfaisant $\sigma(\alpha \diamond \beta) = \sigma(\alpha) \diamond \sigma(\beta), \forall \alpha,\beta \in G$.*

De plus, si S est fini, G est fini.

Démonstration 3.5 *Voir [11], page 4.*

2 Exemples de lois composées induites par le produit composé

Soient f et g deux polynômes de $\mathbb{F}_q[x]$, dont les factorisations dans $\Gamma_q[x]$ sont les suivantes : $f = \prod_{\alpha}(x-\alpha)$ et $g = \prod_{\beta}(x-\beta)$. On définit sur $\mathbb{F}_q[x]$ les lois de composition suivantes :

$$f * g = \prod_{\alpha}\prod_{\beta}\Big(x-(\alpha+\beta)\Big), \textbf{ appelée l'addition composée,}$$

$$f \ominus g = \prod_{\alpha}\prod_{\beta}\Big(x-(\alpha-\beta)\Big), \textbf{ appelée la soustraction composée,}$$

$$f \circ g = \prod_{\alpha}\prod_{\beta}\Big(x-(\alpha\beta)\Big), \textbf{ appelée la multiplication composée,}$$

$$f \oslash g = \prod_{\alpha}\prod_{\beta}\Big(x-\frac{\alpha}{\beta}\Big), g(0)\neq 0, \textbf{ appelée le quotient composé.}$$

Théorème 3.6 *Soient $f \in \mathbb{F}_q[x]$, $q = p^s$, dont les racines sont dans $\mathbb{F}_p$. On suppose qu'il existe $g \in \mathbb{F}_p[x]$, de degré > 1 tel que $g \mid f$. Alors, $g \diamond g \mid f \diamond f$.*

Démonstration 3.7 *Si β est une racine de g alors β est aussi une racine de f car $g \mid f$. Donc $\beta_i \diamond \beta_j$, les racines de $g \diamond g$, sont aussi des racines de $f \diamond f$, d'où $g \diamond g \mid f \diamond f$.*

Théorème 3.8 *Soit $f \in \mathbb{F}_q[x]$ un polynôme de degré $n \geq 1$. On pose $f(x) = \prod_{i=1}^{n}(x-\alpha_i)$, sa factorisation dans une clôture algébrique de $\mathbb{F}_q$, alors*

1. $f * f = \prod_{i=1}^{n}\Big(x-2\alpha_i\Big)\prod_{i<j}\Big(x-(\alpha_i+\alpha_j)\Big)$,
2. $f \ominus f = x^n \prod_{i<j}\Big(x^2-(\alpha_i-\alpha_j)\Big)$,
3. $f \circ f = \prod_{i=1}^{n}\Big(x-\alpha_i^2\Big)\prod_{i<j}\Big(x-(\alpha_i\alpha_j)^2\Big)$,
4. $f \oslash f = \Big(x-1\Big)^n \prod_{i<j}(x^2-(\frac{\alpha_i}{\alpha_j}+\frac{\alpha_j}{\alpha_i})x+1)$, $f(0)\neq 0$.

De plus, tous ces polynômes sont de degré n^2.

Démonstration 3.9 *1. On a*

$$f * f = \prod_{\alpha_i \in A} \prod_{\alpha_j \in A} \Big(x - (\alpha_i + \alpha_j)\Big) = \prod_{\alpha_i = \alpha_j} \Big(x - 2\alpha_i\Big) \prod_{\alpha_i \neq \alpha_j} \Big(x - (\alpha_i + \alpha_j\Big) \tag{3.6}$$

Donc,

$$f * f = \prod_{i=1}^{n} (x - 2\alpha_i) \prod_{i<j} \Big(x - (\alpha_i + \alpha_j)\Big)^2. \tag{3.7}$$

2. On pose $r_1 = x - (\alpha_1 - \alpha_2)$ et $r_2 = x - (\alpha_2 - \alpha_1)$, donc

$$r_1 r_2 = x^2 - (\alpha_1 - \alpha_2)^2, \tag{3.8}$$

alors,

$$\begin{aligned} f \ominus f &= \prod_{\alpha_i = \alpha_j} (x - (\alpha_i - \alpha_j)) \prod_{\alpha_i \neq \alpha_j} (x - (\alpha_i - \alpha_j)), \\ &= x^n \prod_{i<j} (x^2 - (\alpha_i - \alpha_j)^2). \end{aligned}$$

3. On a

$$\begin{aligned} f \circ f &= \prod_i \prod_j (x - \alpha_i \alpha_j), \\ &= \prod_i (x - \alpha_i^2) \prod_{i \neq j} (x - \alpha_i \alpha_j). \end{aligned}$$

4. On a

$$\begin{aligned} f \oslash f &= \prod_{i=j} (x - \frac{\alpha_i}{\alpha_j}) \prod_{i \neq j} (x - \frac{\alpha_i}{\alpha_j}), \\ &= (x-1)^n \prod_{i<j} (x^2 - (\frac{\alpha_i}{\alpha_j} + \frac{\alpha_j}{\alpha_i})x + 1). \end{aligned}$$

Théorème 3.10 *Soit f un polynôme de degré $n \geq 1$, où n est un entier positif sans facteur carré, alors*

$$\begin{aligned} f * f &= \prod_{\alpha} f(x-\alpha), \\ f \ominus f &= \prod_{\alpha} f(x+\alpha), \\ f \circ f &= f(0)^n \prod_{\alpha} f(x\alpha^{-1}), \\ f \oslash f &= f(0)^{-n} \prod_{\alpha} f(x\alpha). \end{aligned}$$

Démonstration 3.11 *Les résultats sont obtenus en appliquant les définitions des opérations $*, \circ, \ominus$ et $\oslash$.*

Les produits composés peuvent être exprimés en fonction du résultant. Ce dernier nous permet de calculer les produits composés sans avoir à calculer les racines de f et g.

Théorème 3.12 *[20] Soit $f, g \in \mathbb{F}_q[x]$, alors*

1. $f * g = Res_y\Big(g(y), f(x-y)\Big)$,
2. $f \ominus g = Res_y\Big(g(y), f(x+y)\Big)$,
3. $f \circ g = Res_y\Big(g(y), f(xy)\Big)$,
4. $f \oslash g = Res_y\Big(g(y), f(x/y)\Big)$.

3 Polynômes irréductibles et multiplication composée

Dans la suite, on suppose que G muni de la loi $\diamond$ est un groupe abélien et un élément de P_G admettant un symétrique pour la loi $\diamond$ est appelé unité de P_G.

Définition 3.13 *Soit $h \in P_G$ tel que h n'est pas une unité. Le polynôme h est dit **décomposable** par rapport à la loi $\diamond$ s'il existe deux polynômes f et g dans P_G, de degrés > 1 tels que $h = f \diamond g$. Sinon, h est dit **indécomposable**.*

Remarque 3.14 *Il ne faut pas confondre l'indécomposabilité et l'irréductibilité. L'irréductibilité est par rapport à la multiplication usuelle. Donc un polynôme irréductible peut être décomposable.*

Soit I_G le sous-ensemble de P_G des polynômes irréductibles sur $\mathbb{F}_q$. Le théorème suivant, établi par Brawley et Carlitz [9], nous donne une condition nécessaire et suffisante pour que le produit $f \diamond g$ soit irréductible.

Théorème 3.15 *Soit $f, g \in P_G$ tels que $\deg f = n$ et $\deg g = m$. Alors, le produit $f \diamond g$ est irréductible sur $\mathbb{F}_q$ si, et seulement si, $f, g \in I_G$ et $pgcd(n, m) = 1$.*

Démonstration 3.16 *Supposons que $f \diamond g$ est irréductible. Alors, f et g sont nécessairement irréductibles car on a :*

$$f \diamond (g \times h) = (f \diamond g) \times (f \diamond h),$$

où $\times$ est la multiplication usuelle.
Supposons que $pgcd(m, n) = d > 1$. Soient r et s deux entiers premiers entre eux, tels que : $m = dr$ et $n = ds$. Soit $\gamma = \alpha \diamond \beta$ où α est une racine de f et β une racine de g. Donc γ est une racine de $f \diamond g$ et comme $f \diamond g$ est irréductible de degré nm, le plus petit entier positif k tel que $\gamma^{q^k} = \gamma$ est $k = mn$.
On a donc :

$$\begin{aligned} \gamma^{q^{drs}} &= \left(\alpha \diamond \beta\right)^{q^{drs}}, \\ &= \alpha^{q^{drs}} \diamond \beta^{q^{drs}}, \\ &= \alpha^{q^{ms}} \diamond \beta^{q^{nr}}, \\ &= \alpha \diamond \beta = \gamma, \end{aligned}$$

et comme $drs < mn$, on a une contradiction.

Supposons que f et g sont irréductibles avec $pgcd(m, n) = 1$. Soient α et β des racines respectives de f et g. Alors, $\gamma = \alpha \diamond \beta$ est une racine de $f \diamond g$.
Le polynôme $f \diamond g$ est irréductible si, et seulement si, le polynôme minimal de γ sur $\mathbb{F}_q$ est de degré nm. Montrons que le plus petit entier d tel que $\gamma^{q^d} = \gamma$ est $d = mn$.
On a $\gamma^{q^{mn}} = \alpha^{q^{mn}} \diamond \beta^{q^{mn}} = \alpha \diamond \beta = \gamma \Rightarrow d \leq nm$.
Comme $\gamma^{q^d} = \gamma$, alors $\alpha^{q^d} \diamond \beta^{q^d} = \alpha \diamond \beta$. En élevant à la puissance q^d t fois, on obtient

$$\alpha^{q^{td}} \diamond \beta^{q^{td}} = \alpha \diamond \beta, \forall t \in \mathbb{N}^*. \tag{3.9}$$

Pour $t = m$, on a

$$\alpha \diamond \beta^{q^{md}} = \alpha \diamond \beta. \tag{3.10}$$

Comme G est un groupe alors $\beta^{q^{md}} = \beta$. Par conséquent, $n \mid md \Rightarrow n \mid d$ car $pgcd(m,n) = 1$.
De la même manière, en prenant $t = n$, on aura

$$\alpha^{q^{nd}} \diamond \beta^{q^{nd}} = \alpha^{q^{nd}} \diamond \beta = \alpha \diamond \beta. \tag{3.11}$$

Alors $\alpha^{q^{nd}} = \alpha$ et donc $m \mid nd$ et par conséquent $m \mid d$. Comme $mn \mid d$, on en déduit que $mn \leq d$, donc $d = mn$.

On pose $G = \Gamma_q^*$ et P_G muni de la loi $\circ$. Soient f et g deux polynômes de P_G. Rappelons que

$$f \circ g = \prod_{\alpha} \prod_{\beta} \big(x - \alpha\beta\big), \tag{3.12}$$

où α , β sont les racines respectives de f et g dans G.
Soit $h \in P_G$ tel que h n'est pas une unité. On dit que h est multiplicativement décomposable si $h = f \circ g$, où f et $g \in P_G$ et $degf) > 1$, $deg(g) > 1$.
Dans [9], Brawley et Carlitz ont établi un théorème pour montrer l'unicité de la décomposition multiplicative pour les polynômes dans I_G.

Théorème 3.17 *Soit G le groupe multiplicatif de Γ_q. Soit $f \in I_G$ un polynôme irréductible de degré $n \geq 1$. Si f est multiplicativement décomposable dans I_G comme suit :*

$$f = f_1 \circ f_2 \circ \cdots \circ f_t = g_1 \circ \cdots \circ g_t, \tag{3.13}$$

où $\deg(f_i) = \deg(g_i) = n_i$ *, $i = 1, \ldots, t$, alors*

1. *Les n_i sont deux à deux premiers entre eux.*
2. *f_i et g_i sont irréductibles et,*
3. *$\forall i$, f_i et g_i sont associés.*

Démonstration 3.18 *1 et 2 sont des cas particuliers du théorème 3.15.*
Montrons 3. Soit $\alpha_i \in \mathbb{F}_{q^{n_i}}$, une racine de f_i , $1 \leq i \leq t$. D'après 3.13, g admet des racines $\beta_i \in \mathbb{F}_{q^{n_i}}$ telles que :

$$\alpha_1 \alpha_2 \ldots \alpha_t = \beta_1 \beta_2 \ldots \beta_t, \tag{3.14}$$

donc, on a :

$$\frac{\alpha_1}{\beta_1} = \frac{\beta_2}{\alpha_2} \ldots \frac{\beta_t}{\alpha_t}, \tag{3.15}$$

et $\left(\frac{\alpha_1}{\beta_1}\right) \in \mathbb{F}_{q^{n_1}}$ *et* $\left(\frac{\alpha_1}{\beta_1}\right) \in \mathbb{F}_{q^{n/n_1}}$.
Comme $pgcd(n_1, \frac{n}{n_1}) = 1$ *alors* $\alpha_1 = c\beta_1$ *où* $c \in \mathbb{F}_q$. *Ceci implique que* $f_1 = (x-c) \circ g_1$, *donc* f_1 *et* g_1 *sont associés.*
D'une manière similaire, on trouve que f_i *et* g_i *sont associés ,* $2 \leq i \leq t$.

Dans le théorème 3.17, nous n'avons pas supposé l'indécomposabilté des facteurs irréductibles du polynôme f. Cependant, nous avons supposé l'égalité des degrés. On a la décomposition suivante dans $\mathbb{F}_2[x]$, où tous les facteurs sont irréductibles :

$$(x^6 + x^4 + x^2 + x + 1) \circ (x^5 + x^2 + 1) = (x^3 + x + 1) \circ (x^{10} + x^5 + x^4 + x^2 + 1) \quad (3.16)$$

Il est clair que les degrés des facteurs ne satisfont pas la condition du théorème 3.17. De plus, les polynômes de degré 6 et 10 sont décomposables. Donc, pour supprimer la condition d'égalité des degrés, nous allons exiger que les facteurs multiplicatifs soient indécomposables.
Si $d(\alpha)$ désigne le degré du nombre algébrique α. Nous avons le lemme suivant :

Lemme 3.19 *Soit* α, β, γ *et* $\sigma \in \Gamma_q$ *tels que :*

1. $\alpha\beta = \gamma\sigma$.
2. $d(\alpha) = a$, $d(\beta) = b$, $d(\gamma) = c$ *et* $d(\sigma) = d$
3. $pgcd(a, b) = 1 = pgcd(c, d)$.

Alors, il existe des entiers m, n, r *et* s, *premiers entre eux deux à deux tels que :* $a = mn$, $b = rs$, $c = mr$, $d = ns$, *et pour chacune des factorisations, il existe* $\alpha_i, \beta_i, \gamma_i$ *et* $\sigma_i \in \Gamma_q, i = 1, 2$, *tels que :* $\alpha = \alpha_1\alpha_2$, $\beta = \beta_1\beta_2$, $\gamma = \gamma_1\gamma_2$ *et* $\sigma = \sigma_1\sigma_2$, *où*

$$\begin{aligned} d(\alpha_1) = m, d(\alpha_2) = n, \\ d(\beta_1) = r, d(\beta_2) = s, \\ d(\gamma_1) = m, d(\gamma_2) = r, \\ d(\sigma_1) = n, d(\sigma_2) = s. \end{aligned}$$

Démonstration 3.20 *Voir [9], pages 126-127.*

Théorème 3.21 *Soit* $f \in \mathbb{F}_q[x]$, *un polynôme irréductible de degré* $n > 1$. *Supposons que* f *est multiplicativement décomposable comme suit*

$$f = f_1 \circ f_2 \circ \cdots \circ f_t = g_1 \circ g_2 \circ ... \circ g_s, \quad (3.17)$$

avec $f_i, g_i \in \mathbb{F}_q[x]$ sont indécomposables pour la loi $\circ$. Alors, $s = t$ et les f_i et g_i sont associés (en réordonnant les g_i) , $1 \leq i \leq t$.

Démonstration 3.22 *Posons* $\deg(f_i) = n_i$ *et* $\deg(g_i) = m_i$ *tels que :* $n = \prod_{i=1}^{t} n_i = \prod_{i=1}^{t} m_i$ *où les n_i (respectivement m_i) sont premiers entre eux deux à deux.*
Supposons, sans restreindre à la généralité, que $t < s$. Montrons le résultat par récurrence sur t.
Pour $t = 1$, f est trivialement indécomposable. On suppose donc, $t > 1$. On réarrange les f_i et les g_i tels que $1 < n_1 < n_2 < \cdots < n_t$ et $1 < m_1 < m_2 < \cdots < m_s$. Nous affirmons que $s = t$ et $n_i = m_i$, $\forall i$. Supposons que $s \geq t$ et qu'il existe n_i tel que $n_i \neq m_j$, $j = 1, \ldots, s$. Choisissons le plus petit des n_i et notons le a. Comme $n = \prod_{i=1}^{t} n_i = \prod_{i=1}^{t} m_i$, il existe un certain m_j qu'on note c tel que $pgcd(a, c) \neq 1$ et $a \neq c$.
Posons $b = \frac{n}{a}$ et $d = \frac{n}{c}$ alors $ab = cd$ et $pgcd(a, b) = pgcd(c, d) = 1$.
Soit $f' \in \mathbb{F}_q[x]$ le polynôme f_i tel que $deg(f_i) = a$ et $g' \in \mathbb{F}_q[x]$ le polynôme g_i tel que $deg(g_i) = c$. Alors,

$$f' \circ F = g' \circ G, \tag{3.18}$$

où F (respectivement G) est le produit des f_i restants (respectivement des g_i restants). De plus, F et G sont des polynômes irréductibles de degré b (repectivement d). Soit α, β, γ et σ les racines respectives de f', F, g' et G. On a donc :

$$\alpha\beta = \gamma\sigma, \tag{3.19}$$

car $\alpha\beta$ est une racine de $f' \circ F$ et $\gamma\sigma$ est une racine de $g' \circ G$. De plus, la relation [3.18] montre que $d(\alpha) = a, d(\beta) = b, d(\gamma) = c$ et $d(\sigma) = d$ où $a > 1$, $b > 1$, $c > 1$ et $d > 1$, puisque $2 \leq t \leq s$.
Posons $m' = pgcd(a, c) > 1$ alors $a = m'n'$ et $c = m'r'$, $n', r' \in \mathbb{N}$, $n' > 1$ ou $r' > 1$. Pour $n' > 1$, en appliquant le lemme 3.19, $\alpha = \alpha_1\alpha_2$ où $d(\alpha_i) = n' > 1$ et $d(\alpha_2) = m' > 1$. Donc $f = h_1 \circ h_2$, où h_1 et h_2 sont les polynômes minimaux de α_1 (respectivement α_2), ce qui est une contradiction car f est décomposable. Ainsi $s = t$ et $m_i = n_i$, $1 \leq i \leq t$. Alors les conditions du théorème 3.17 sont vérifiées et on en déduit que f_i et g_i sont associés.

3.1 Un critère de décomposition multiplicative

Le théorème suivant donne une condition pour qu'un polynôme irréductible sur $\mathbb{F}_q$ soit multiplicativement décomposable.

Théorème 3.23 *Soit $h \in \mathbb{F}_q[x]$ un polynôme irréductible de degré nm et d'ordre e avec $pgcd(n,m) = 1$. Alors $h = f \circ g$, où f et g sont irréductibles dans $\mathbb{F}_q[x]$, de degrés respectifs n et m si, et seulement si, $e \mid (q^n-1)(q^m-1)/(q-1)$.*

Démonstration 3.24 *Voir [9], page 125.*

Le corollaire suivant donne le nombre de polynômes irréductibles multiplicativement décomposables.

Corollaire 3.25 *Soit $n, m \in \mathbb{N}$ avec $pgcd(n,m) = 1$. Soit E l'ensemble des ordres des polynômes irréductibles sur $\mathbb{F}_q[x]$ de degré nm. Le nombre N de polynômes irréductibles, de degré nm, décomposables sous la forme $f \circ g$ avec $\deg f = n$ et $\deg g = m$ est donné par $N = \sum_{e \in E} \varphi(e)/nm$ avec $e \mid (q^n-1)(q^m-1)/(q-1)$.*

Exemple 3.26

1. *Dans $\mathbb{F}_2[x]$. On considère les polynômes irréductibles de degré $nm = 6$ avec $n = 2$ et $m = 3$. Les ordres de ces polynômes sont $9, 21$ et 63. Donc, les polynômes irréductibles décomposables de degré 6 sont d'ordre 21 et le nombre de ces polynômes est $N = \frac{\varphi(21)}{6} = 2$.*
2. *Dans $\mathbb{F}_3[x]$, $E = \{7, 28, 52, 56, 91, 104, 182, 364, 728\}$. Donc les polynômes irréductibles f avec $f(0) \neq 0$ décomposables dans $\mathbb{F}_3[x]$ sont ceux d'ordres 52 et 104. Ainsi, le nombre de polynômes irréductibles décomposables de degré 6 dans $\mathbb{F}_3[x]$ est $\Big(\varphi(52) + \varphi(104)\Big)/6 = 12$.*

3.2 Algorithme pour le calcul du produit composé

On définit le produit composé de $f \diamond g = \prod_{\alpha}\prod_{\beta}(x - (\alpha \diamond \beta)$, où α et $\beta \in G$ sont les racines des polynômes unitaires f et g dans G. Supposons que le produit $\diamond$ est représenté par $h(x,y) \in F_q[x,y]$, c'est à dire, $\alpha \diamond \beta = h(\alpha, \beta), \forall \alpha, \beta \in G$. Le but est de calculer $f \diamond g$. On suppose que f et g sont irréductibles de degré m et n, respectivement, et $\gcd(f,g) = 1$. Les racines de f et de g appartiennent à une extension du corps $\mathbb{F}_q$. Le plus petit corps contenant les racines de f et g est $\mathbb{F}_{q^{mn}}$ et peut être construit comme $\mathbb{F}_{q^m}[y]/\langle g(y)\rangle$ où $\mathbb{F}_{q^m} = \mathbb{F}_q[x]/\langle f(x)\rangle$. Autrement dit, $\mathbb{F}_{q^{mn}} \simeq R = \mathbb{F}_q[x,y]/I$, où $I = \langle f(x), g(y)\rangle$. C'est l'idéal de $\mathbb{F}_q[x,y]$ engendré par les polynômes $f(x)$ et $g(y)$.

Dans R, toutes les racines de $f(z)$ sont de la forme $\overline{x}^{q^i}, 0 \leqslant i \leqslant m-1$, et toutes les racines de $g(z)$ sont de la forme $\overline{y}^{q^j}$, avec $0 \leqslant j \leqslant n-1$. En calculant dans R, on réduit les puissances de x modulo $f(x)$ et les puissances de y modulo $g(y)$. La composition de $f \diamond g$ peut être calculée par l'algorithme suivant :

3.3 Algorithme pour f $\diamond$ g

Algorithm 1 f $\diamond$ g

Entrée f , $g \in \mathbb{F}_q[x]$ et $h \in \mathbb{F}_q[x,y]$.
Sortie $f \diamond g$.
Début

1. La construction de $A = \mathbb{F}_q[x,y]/\langle f(x), g(y)\rangle$.
2. On calcule $u_i \equiv x^{q^i} \mod f(x)$ avec $0 \leq i \leq m-1$ et $v_j \equiv x^{q^j} \mod g(x)$ avec $0 \leq j \leq n-1$.
3. Dans A, on calcule $h_{ij} = h(u_i, v_j)$ avec $0 \leq i \leq n-1$ et $0 \leq j \leq m-1$.
4. Dans $A[z]$, on calcule et affiche le polynôme $\prod_{i=0}^{n-1}\prod_{j=0}^{m-1}\left(z - h_{ij}\right)$.

Fin

L'algorithme 3.3 a été introduit par Brawley et al. dans [11]. Cet algorithme calcule efficacement le produit composé de $f \diamond g$ dans $\mathbb{F}_q[x]$. Ces calculs peuvent être réalisés à l'aide d'un logiciel de calculs comme Sage math, Maple, ...etc. L'algorithme le plus rapide a été introduit par Bostan et al. [7]. Leur algorithme a la meilleure complexité dans toutes les caractéristiques.

Chapitre 4

Composition multiplicative et polynômes irréductibles sur $\mathbb{Z}$

1 Introduction

Soient $f, g \in \mathbb{F}_q[x]$ deux polynômes unitaires sur $\mathbb{F}_q$. Brawley et Carlitz [9] ont étudié le produit composé $f \diamond g$ de deux polynômes, et en particulier, le produit composé induit par la multiplication et l'addition définies sur une clôture algébrique de $\mathbb{F}_q$. L'un des résultats importants de Brawley et Carlitz est le suivant :

Théorème 4.1 *Soient f et g deux polynômes unitaires à coefficients dans $\mathbb{F}_q$ avec* $\deg f = m$ *et* $\deg g = n$. *Alors $f \diamond g$ est irréductible si, et seulement si, f et g sont irréductibles et* $\gcd(m, n) = 1$.

Soit R un anneau commutatif. On rappelle que le résultant de deux polynômes $f, g \in \mathbb{F}_q[x]$, noté $Res_x(f, g)$, est le déterminant de leur matrice de Sylvester. Ayad [1] a montré que si les polynômes unitaires $f, g \in \mathbb{Z}[x]$ satisfont des propriétés supplémentaires, alors le polynôme

$$Res_y(f(y), g(x-y))$$

est irréductible sur $\mathbb{Q}$ mais réductible sur $\mathbb{F}_p$ pour tout nombre premier p. Le polynôme ci-dessus est lié à la composition additive de f et g par :

$$\prod_{i=1}^{m}\prod_{j=1}^{n}(x-(\alpha_i+\beta_j)) = Res_y(f(y), g(x-y)),$$

où $\alpha_1, ..., \alpha_m$ et $\beta_1, ..., \beta_n$ sont les racines respectives de f et g dans $\mathbb{C}$.
Dans ce chapitre, en utilisant la composition multiplicative, nous présentons une

construction de polynômes entiers irréductibles sur $\mathbb{Z}$ et réductibles sur $\mathbb{F}_p$ pour tout nombre premier p. Ce travail a fait l'objet d'une publication dans TATRA MOUNTAINS, Mathematical Publications [4].
Dans toute la suite, pour la composition multiplicative, nous utiliserons la notation $\diamond$ au lieu de $\circ$.

1.1 Préliminaires

Dans tout ce qui suit, R et S sont des anneaux intègres.
Soit,

$$g = b_n x^n + b_{n-1}x^{n-1} + ... + b_1 x + b_0 \in R[x], \text{ avec } b_n \neq 0.$$

L'homogénéisation de g , noté ${}^h g(y,x)$, est le polynôme défini par :

$${}^h g(y,x) := b_n x^n + b_{n-1}x^{n-1}y + ... + b_1 x y^{n-1} + b_0 y^n.$$

C'est un polynôme homogène dans $R[x,y]$ de degré $n = \deg g$ tel que ${}^h g(1,x) = g(x)$. Une comparaison directe montre que

$$y^n g(x/y) = b_n x^n + b_{n-1}x^{n-1}y + ... + b_1 x y^{n-1} + b_0 y^n =^h g(y,x).$$

Si $\alpha_1, ..., \alpha_m$ et $\beta_1, ..., \beta_n$ sont les racines respectives de f et g, dans une clôture algébrique du corps des fractions de R et si C_f et C_g sont les coefficients dominants respectifs de f et g, alors on a :

$$\begin{aligned} C_f^n C_g^m \prod_{i=1}^{m}\prod_{j=1}^{n}(x - \alpha_i\beta_j) &= C_f^n \prod_{i=1}^{m}\left(\alpha_i^n C_g \prod_{j=1}^{n}(x/\alpha_i - \beta j)\right) \\ &= C_f^n \prod_{=1}^{m}(\alpha_i^n g(x/\alpha_i)) \\ &= Res_y(f(y), y^n g(x/y) = Res_y(f(y),^h g(y,x)) \end{aligned}$$

Cette égalité entraine la définition suivante :

Définition 4.2 *Soient $f, g \in R[x]$. On définit le produit composé de f et g par*

$$(f \diamond g)(x) := Res_y(f(y),^h g(y,x)).$$

Le produit composé est une opération binaire associative et commutative sur $R[x]$. Elle peut être facilement vérifiée en considérant les racines des polynômes

dans une clôture algébrique du corps de fractions de R. Ce produit composé est commutatif car le produit est commutatif dans une clôture algébrique du corps des fractions de R. L'associativité est vérifiée puisque $f \diamond (g \diamond h)$ et $(f \diamond g) \diamond h$ sont égaux à

$$C_f^{\deg g \deg h} C_g^{\deg f \deg h} C_h^{\deg f \deg g} \prod_{\alpha,\beta,\gamma} (x - \alpha\beta\gamma),$$

où α, β et γ sont les racines respectives de f, g et h. Il est clair, par définition, que si $f = f_1 \diamond f_2$, alors

$$C_f = C_{f_1}^{\deg f_2} C_{f_2}^{\deg f_1}.$$

On pose

$$g = b_n x^n + b_{n-1} x^{n-1} + ... + b_1 x + b_0 \in R[x],$$

et f un polynôme, $f \in R[x]$, de degré m. Alors
Si $b_0 \neq 0$ alors,

$$\begin{aligned}(f \diamond g)(0) &= Res_y(f(y),^h g(y,0)) \\ &= Res_y(f(y), b_0 y^n) \\ &= (-1)^{mn} Res_y(b_0 y^n, f(y)).\end{aligned}$$

En utilisant une des propriétés du résultant de deux polynômes, on a

$$(f \diamond g)(0) = (-1)^{mn} b_0^m f(0)^n.$$

Si $b_0 = 0$, alors

$$(f \diamond g)(0) = Res_y(f(y),^h g(y,0) = Res_y(f(y),0) = 0.$$

Donc,

$$(f \diamond g)(0) = (-1)^{mn} f(0)^n g(0)^m.$$

On en déduit que le produit composé est une loi de composition interne dans $R[x]$. Il serait donc intéressant de déterminer les inverses pour la loi $\diamond$.
Remarquons que le polynôme $l := x - 1 \in R[x]$ est l'élément neutre pour la loi $\diamond$. En effet, pour tout $f \in R[x]$, on a

$$(l \diamond f)(x) = Res_y(l(y),^h f(y,x)) =^h f(1,x) = f(x)$$

et

$$(f \diamond l)(x) = Res_y(f(y), x - y) = (-1)^m Res_y(x - y, f(y)) = (-1)^{2degf} f(x) = f(x).$$

Si $u, v \in R[x]$ sont inverses l'un de l'autre, alors $u = u_1 x + u_0$ et $v = v_1 x + v_0$. On a

$$x - 1 = l(x) = (u \diamond v)(x) = u_1 v_1 x - u_0 v_0.$$

D'où, par identification, on obtient $u_1 v_1 = u_0 v_0 = 1$. C'est à dire que u_1 et u_0 sont inversibles et $v = u_1^{-1} x + u_0^{-1}$. Comme le produit composé et associatif dans $R[x]$, il l'est également sur le sous-ensemble des polynômes linéaires.
Dans le théorème suivant, R^* désigne le groupe des unités de R pour la multiplication.

Théorème 4.3 *Le groupe $G_\diamond$ des unités de $R[x]$ pour la loi $\diamond$ est égal exactement à l'ensemble des polynômes linéaires $u = u_1 x + u_0$ avec $u_1, u_0 \in R^*$, et l'inverse d'un tel u est donné par : $u_1^{-1} x + u_0^{-1}$.*

Proposition 4.4 *Soit $G_\diamond$ le groupe des unités de $R[x]$ muni de la loi $\diamond$. Alors $G_\diamond \simeq R^* \oplus R^*$.*

Démonstration 4.5 *On note $(\overline{R}, +, *)$ l'anneau induit par l'anneau $(R, +, \cdot)$, où $*$ est la loi définie par $x * y := -(x.y)$. Notons que l'élément neutre de $\overline{R}$ pour la loi $(*)$ est -1, 1 étant l'élément neutre de R pour la loi $(\cdot)$. L'application $\phi : R \to \overline{R}$ définie par $\phi(x) = -x$ est un morphisme d'anneaux. En effet,*

1. $\phi(x + y) = -(x + y) = (-x) + (-y) = \phi(x) + \phi(y), \forall x, y \in R.$
2. $\phi(x \cdot y) = -(x \cdot y) = x * y.$
3. $\phi(1) = -1$

L'application ϕ est injective et surjective, donc un isomorphisme. Comme R et $\overline{R}$ sont des anneaux isomorphes et on note $R \simeq \overline{R}$, alors leurs groupes des unités respectifs R^* et $\overline{R}^*$ sont isomorphes.
On définit l'application $\psi : G_\diamond \to R^* \oplus \overline{R}^*$ par $\psi(u_1 x + u_0) = (u_1, u_0)$, on a :

$$G_\diamond \simeq R^* \oplus \overline{R}^* \simeq R^* \oplus R^*,$$

$R^* \oplus \overline{R}^*$, étant muni de la loi produit $\times$. En effet, ψ est un morphisme de groupes car $\forall u = u_1 x + u_0, v = v_1 x + v_0 \in G_\diamond$, on a

$$\psi(u \diamond v) = \psi(u_1 v_1 x - u_0 v_0) = (u_1 v_1, -u_0 v_0) = (u_1 \cdot v_1, u_0 * v_0) = (u_1, u_0) \times (v_1, v_0).$$

On a $ker\psi = \{u = u_1 x + u_0 \in G_\diamond, \psi(u) = (1, -1)\} = x - 1$.
L'application ψ est surjective par construction.

Définition 4.6 *Soit $f \in R[x]$. S'il existe $f_1, f_2 \in R[x] \setminus G_\diamond$ tels que $f = f_1 \diamond f_2$, alors on dit que f est multiplicativement décomposable. Dans le cas contraire, On dit que f est multiplicativement indécomposable.*
Si f admet une décomposition de la forme $f = f_1 \diamond f_2$ avec f_1 ou f_2 linéaire, alors on dit que f est presque indécomposable sur R.

1.2 Polynômes indécomposables

Dans cette partie, nous donnons quelques résultats sur les polynômes indécomposables. Par définition, un polynôme indécomposable est presque indécomposable, et ces deux notions coïncident sur un corps.

Lemme 4.7 *Soit $f \in R[x]$ un polynôme presque indécomposable sur R. Si le coefficient dominant et le terme constant de f sont des unités de R, alors f est indécomposable sur R.*

Démonstration 4.8 *Nous savons que si f est presque indécomposable, alors on peut écrire $f = f_1 \diamond f_2$, $f_1, f_2 \in R[x]$, avec f_1 ou f_2 linéaire. On pose $\deg f_2 = n$. Sans restreindre la généralité, on suppose que f_1 est linéaire. On a*

$$C_f = C_{f_1}^n C_{f_2}$$

et

$$f(0) = (f_1 \diamond f_2)(0) = (-1)^n f_1(0)^n f_2(0).$$

D'après les égalités précédentes, si C_f et $f(0)$ sont des unités de R, alors $C_{f_1}, f_1(0)$ sont des unités de R. Donc $f_1 = C_{f_1} x + f_1(0) \in G_\diamond$, d'où f est indécomposable.

Théorème 4.9 *Soit $f \in R[x]$ avec $\deg f = n \geq 1$. Supposons que $f(0) \in R^*$ et C_f est premier. Si f est presque indécomposable sur R, alors f est indécomposable sur R.*

Démonstration 4.10 *Supposons que f est presque indécomposable, alors $f = f_1 \diamond f_2$ avec $f_1, f_2 \in R[x]$, f_1 où f_2 linéaire. Posons $\deg f_2 = n$. Sans restreindre la généralité, supposons que f_1 est linéaire. On pose $f_1 = C_{f_1} x + f_1(0)$. On a d'une part,*

$$f(0) = (f_1 \diamond f_2)(0) = (-1)^n f_1(0)^n f_2(0)$$

Comme $f(0)$ est une unité de R, alors $f_1(0)$ et $f_2(0)$ sont des unités de R. D'autre part $C_f = C_{f_1}^n C_{f_2}$. Comme C_f est premier dans R, donc irréductible dans R. On en déduit que C_{f_1} où C_{f_2} est inversible.
Si C_{f_1} est inversible, alors f est indécomposable car $f_1(0)$ est aussi inversible. Si C_{f_2}

est inversible, alors $C_{f_1}^n = C_f C_{f_2}^{-1}$ *implique que* C_f *divise* C_{f_1}. *Posons* $C_{f_1} = C_f \alpha, \alpha \in R$, *alors on a*

$$(C_f \alpha)^n C_{f_2} = C_f,$$

d'où $C_f^{n-1} \alpha^n C_{f_2} = 1$. *Dans le cas où* $n \geq 2$, *on déduit que* $C_f \alpha$ *est inversible, donc* C_{f_1} *l'ai aussi alors* f *est indécomposable. Dans le cas ou* $n = 1$ *on en déduit que* C_{f_2} *est inversible, et comme* $f_2(0)$ *est aussi inversible on en conclut que* f *est encore indécomposable.*

1.3 Polynômes presque indécomposable

Dans cette partie, on présente deux classes de polynômes presque indécomposables.

Théorème 4.11 *Si* $f \in R[x]$ *est de degré p premier, alors* f *est presque indécomposable sur R.*

Démonstration 4.12 *Supposons que* $f = f_1 \diamond f_2$ *avec* $f_1, f_2 \in R[x]$ *de degrés m et n, respectivement. Comme* $p = \deg f = mn$, *on en déduit que* f_1 *ou* f_2 *est linéaire.*

Théorème 4.13 *Si* $f \in R[x]$ *avec* $\deg f > 1$ *et de coefficient dominant p premier, alors* f *est presque indécomposable sur R. De plus, le coefficient dominant de tout facteur linéaire de la décomposition est une unité de R.*

Démonstration 4.14 *Supposons que* $f = f_1 \diamond f_2$ *avec* $f_1, f_2 \in R[x]$ *de de degrés m et n, respectivement. On a* $p = C_{f_1}^n C_{f_2}^m$. *Sans restreindre la généralité, supposons que p divise* $C_{f_1}^n$. *Alors p divise* C_{f_1}, *donc on a* $C_{f_1} = pa$ *avec* $a \in R$, *cela implique que* $p = p^n a^n C_{f_2}^m$, *donc* $0 = p(p^{n-1} a^n C_{f_2}^m - 1)$, *ce qui entraine que* $p^{n-1} a^n C_{f_2}^m = 1$. *D'où* p^{n-1} *divise* 1, *ce qui est impossible sauf si* $n = 1$. *On conclut que* $\deg f_2 = 1$ *et* $aC_{f_2}^m = 1$.

Notons que si le polynôme $f = f_1 \diamond f_2 \diamond \cdots \diamond f_r \in R[x]$ est presque indécomposable, alors au plus un facteur de la composition n'est pas linéaire. En effet, s'il existe au moins deux polynômes non linéaires f_i et f_j parmi les facteurs de la composition alors nous pouvons écrire $f = f_i \diamond (f_j \diamond g)$, où g est la composition des facteurs restants, Cela pourrait contredire le fait que f est presque indécomposable.
Si un polynôme n'est pas presque indécomposable, alors on pourrait se poser la question sur la possibilité d'une décomposition en polynômes presque indécomposables.

Théorème 4.15 *Soit $f \in R[x]$. Alors $f = f_1 \diamond f_2 \diamond \cdots \diamond f_r$, où les $f_i \in R[x]$ sont des polynômes presque indécomposables $f_i \in R[x]$.*

Démonstration 4.16 *Le cas où f est lui même indécomposable est trivial. Supposons alors que f est décomposable et procédons par induction sur le degré de f. Comme chaque polynôme linéaire est presque indécomposable, l'hypothèse est vérifiée si* $\deg f = 1$. *On suppose alors, par hypothèse d'induction, que le résultat est vérifié pour tous les polynômes de degré inférieur ou égal au degré de f.*
Comme nous avons supposé que f est décomposable alors on peut écrire $f = f_1 \diamond f_2$ avec $f_1, f_2 \in R[x] \setminus G_\diamond$. Si f_1 ou f_2 est linéaire, alors f est presque indécomposable par définition. Si on a une décomposition avec $degf_1 < degf$ et $degf_2 < degf$, alors par hypothèse $f_1 = g_1 \diamond \cdots \diamond g_t$ et $f_2 = g_{t+1} \diamond \cdots \diamond g_r$, où les $g_i \in R[x]$ sont des polynômes presque indécomposables, d'où $f = g_1 \diamond \cdots \diamond g_r$, ce qui termine la démonstration.

Un homomorphisme d'anneaux $\sigma : R \to S$ peut être naturellement prolongé en un homomorphisme d'anneaux de $R[x]$ à $S[x]$ par l'application $a_m x^m + \cdots + a_0 \to \sigma(a_m)x^m + \cdots + \sigma(a_0)$. Si $\sigma : R[x] \to S[x]$ préserve les degrés de f et $g \in R[x]$, alors

$$\sigma(Res_x(f,g)) = Res_x(\sigma(f), \sigma(g)).$$

Comme $Res_x(f,g)$ est un polynôme dont les coefficients sont des produits et sommes des coefficients de f et de g. alors nous pouvons énoncer le résultat suivant :

Théorème 4.17 *Soit $\sigma : R \to S$ un homomorphisme d'anneaux, et soit $f \in R[x]$ tel que $f(0), C_f \notin \ker\sigma$. Si $f = f_1 \diamond f_2$ sur R, alors $\sigma f = \sigma f_1 \diamond \sigma f_2$ sur S et* $\deg \sigma f_1 = \deg f_1$, $\deg \sigma f_2 = \deg f_2$.

Démonstration 4.18 *On prolonge naturellement σ à un homomorphisme d'anneaux de $R[x,y]$ à $S[x,y]$. Par hypothèse, σ n'annule pas C_f et $f(0)$. Soient m et n les degrés respectifs de f_1 et f_2. Alors $C_f = C_{f_1}^n C_{f_2}^m$ implique que*

$$0 \neq \sigma(C_f) = \sigma(C_{f_1})^n \sigma(C_{f_2})^m.$$

Comme $f(0) = (-1)^{mn} f_1(0)^n f_2(0)^m$, alors

$$0 \neq \sigma(f_1(0))^n \sigma(f_2(0))^m.$$

Comme σ n'annule pas les coefficients dominants et les termes constants de f_1 et f_2, il préserve les degrés de ces deux polynômes ainsi que les polynômes ${}^h f_1(y,x)$ et ${}^h f_2(y,x)$. Donc,

$$\sigma(f_1 \diamond f_2) = \sigma(Res_y(f_1(y), {}^h f_2(y,x))) = Res_y(\sigma f_1(y), {}^h \sigma f_2(y,x)) = \sigma f_1 \diamond \sigma f_2.$$

Théorème 4.19 *Soit $\sigma : R \to S$ un homomorphisme d'anneaux, et soit $f \in R[x]$ tel que $f(0)$ et $C_f \notin \ker\sigma$. Si σf est presque indécomposable sur S, alors f est presque indécomposable sur R.*

Démonstration 4.20 *Par le théorème 4.15, $f = f_1 \diamond \cdots \diamond f_r$, où chaque $f_i \in R[x]$ est presque indécomposable sur R. Alors $\sigma f = \sigma f_1 \diamond \cdots \diamond \sigma f_r$ est presque indécomposable sur S, tous sauf l'un des σf_i est linéaire, soit f_t pour $t \in \{1,\dots,r\}$. Comme $\deg f_i = \deg \sigma f_i = 1$, il s'ensuit que f_i est linéaire quelque soit $i \in \{1,\dots,r\} \setminus \{t\}$. Posons $l_1 := f_1 \diamond \cdots \diamond f_{t-1}$ et $l_2 := f_{t+1} \diamond \cdots \diamond f_r$, donc $f = l_1 \diamond f_t \diamond l_2$. Par conséquent, f est presque indécomposable .*
la preuve de ce résultat nécessite un lemme, qui découle immédiatement de la définition du produit composé :

Lemme 4.21 *Soit K le corps de fractions de l'anneau intègre R. Soit $f, f_1, f_2 \in R[x]$ et soit $f = C_f F, f_1 = C_{f_1} F_1$ et $f_2 = C_{f_2} F_2$, où $C_f, C_{f_1}, C_{f_2} \in R$ et $F, F_1, F_2 \in K[x]$ sont des polynômes unitaires. Alors $f = f_1 \diamond f_2$ sur R si, et seulement, si $F = F_1 \diamond F_2$ sur K and $C_f = C_{f_1}^{\deg f_2} C_{f_2}^{\deg f_1}$.*

2 Résultats principaux

Théorème 4.22 *Soit m un idéal maximal de R tel que le corps des résidus R/m est fini, et soit $f \in R[x]$ un polynôme de degré au moins 2 et dont les coefficients dominant et terme constant ne s'annulent pas modulo m. Si l'image de f modulo m est irréductible dans $R/m[x]$, alors f est le produit composé d'au plus $\omega(deg f)$ de polynômes presque indécomposables de degrés au moins 2 sur R, où $\omega(n)$ désigne le nombre de nombres premiers apparaissant dans la décomposition de n en produit de nombres premiers.*

Démonstration 4.23 *Supposons que $f = f_1 \diamond \dots \diamond f_r$ où chaque $f_i \in R[x]$ est presque indécomposable de degré au moins 2 sur R. On définit $\sigma : R \to R/\mathfrak{m}$ par $a \to a \pmod{\mathfrak{m}}$ qu'on peut étendre à un homomorphisme d'anneaux de polynômes.*

Supposons que $r > \omega(\deg f)$. Le coefficient dominant et le terme constant de f ne sont pas réduits à zero modulo $\mathfrak{m}$, alors par le Théorème 4.17 chaque $\deg f_i = \deg \sigma f_i$ divise $\deg f = \deg \sigma f$. D'après le principe des tiroirs, il s'ensuit qu'au moins 2 des $\deg \sigma f_i$ partagent un facteur premier du $\deg \sigma f$, soit $\deg \sigma f_1$ et $\deg \sigma f_2$ sans restreindre la généralité. Posons $\sigma g := \sigma f_2 \diamond \dots \diamond \sigma f_r$ alors $\sigma f = \sigma f_1 \diamond \sigma g$. On suppose que les polynômes σf_1 et σf_2 sont unitaires, sinon nous divisons simplement par leurs coefficients dominants, et la relation est vérifiée par le lemme4.21 . Si σf est irréductible sur $R/\mathfrak{m}$, donc $pgcd(\deg \sigma f_1, \deg \sigma g) = 1$ par le théorème4.1, ce qui contredit le fait que les deux degrés partagent un facteur premier, donc on conclut que $r < \omega(\deg f)$.

Corollaire 4.24 *Soient $f_1, f_2, ..., f_r \in \mathbb{Z}[x]$ de degrés au moins 2. Si*

$$\omega(\deg f_1 ... \deg f_r) < r,$$

alors $f_1 \diamond ... \diamond f_r$ est réductible modulo p quelque soit p premier qui ne divise pas leur coefficients dominants et leurs termes constants.

Démonstration 4.25 *Quelque soit $i \in \{1, \dots, r\}$, on écrit f_i sous la forme*

$$f_i = f_{i,1} \diamond \cdots \diamond f_{i,k_i}$$

, où $k_i \geq 1$, et $f_{i,j}$ est un polynôme presque indécomposable de degré minimum 2 pour chaque $j \in \{1, \dots, k_i\}$. Posons

$$f := (\diamond_{i=1}^{r} f_i) = (\diamond_{i=1}^{r} \diamond_{j=1}^{k_i} f_{i,j}).$$

Comme par hypothèse $\omega(\deg f_1 \dots \deg f_r) < r$ on a :

$$k := \sum_{i=1}^{r} k_i \geq r > \omega\left(\prod_{i=1}^{r} \deg f_i\right) = \omega\left(\prod_{i=1}^{r} \prod_{j=1}^{k_i} \deg f_{i,j}\right) = \omega(\deg f).$$

Donc $\omega(\deg f)$ est strictement inférieur à k, où k est le nombre de polynômes non linéaires presque indécomposables dans sa factorisation. Pour tout nombre premier p qui ne divise pas $f(0)$ et C_f, la supposition que f soit irréductible modulo p impliquerait que $k \leq \omega(\deg f)$ d'après le Théorème 4.22, ce qui est une contradiction.

Exemple 4.26 *Les polynômes ci-dessous sont irréductibles sur $\mathbb{Z}$ mais réductibles sur $\mathbb{F}_p$ quelque soit p premier :*

1. $x^{12} - x^{10} + 3x^8 + 4x^6 + 3x^4 + 2x^2 + 1 = (x^2 + 1) \diamond (x^2 + x + 1) \diamond (x^3 + x^2 + 1)$,
2. $x^8 + 2x^4 + x^2 + 1 = (x^2 + 1) \diamond (x^4 + x + 1)$,
3. $x^4 + (a^2 - 2)x^2 + 1 = (x^2 + 1) \diamond (x^2 + ax + 1)$ *où* $a \notin \{0, \pm 2\}$,
4. $x^4 + (a^2 + 2)x^2 + 1 = (x^2 + 1) \diamond (x^2 + ax - 1)$ *où* $a \neq 0$.

L'irréductibilité des polynômes précédents sur $\mathbb{Z}$ peut être vérifiée par un logiciel de calcul. Notons que le polynôme $f \diamond g$ n'est pas toujours irréductible sur $\mathbb{Z}$. Par exemple le polynôme $f = x^2+1$ et $g = x^2+x-2$ vérifient les conditions du corollaire 4.24, mais le polynôme

$$f \diamond g = (x^2 + 1) \diamond (x^2 + x - 2) = x^4 + 5x^2 + 4 = (x^2 + 4)(x^2 + 1)$$

est réductible sur $\mathbb{Z}$.

Remarque 4.27 *Les exemples 3 et 4 précédents peuvent être utilisés pour produire un résultat plus faible sur la décomposition des polynômes sur un corps fini. Par exemple, il est connu que le polynôme* $x^4 + 1$ *est irréductible sur* $\mathbb{Z}$ *mais réductible sur* $\mathbb{F}_p$*, pour tout nombre premier* p*. En considérant la classe plus générale des polynômes* $x^4 + (a^2 \pm 2)x^2 + 1$ *avec* $a \neq 0$*, et en utilisant l'homomorphisme d'anneaux* $f : \mathbb{Z} \to \mathbb{Z}/P\mathbb{Z}[X]$*, on peut déduire que : les polynômes* $x^4+(a^2-2)x^2+1$ *sont irréductibles sur* $\mathbb{Z}$ *mais réductibles sur* $\mathbb{F}_p$ *pour* $p = 2$ *et* $p \equiv \pm 1(mod 8)$ *et les polynômes* $x^4+(a^2+2)x^2+1$ *avec* $a \neq 0$ *sont irréductibles sur* $\mathbb{Z}$ *mais réductible sur* $\mathbb{F}_p$ *pour* $p = 2$ *et* $p \equiv 1(mod 8)$ *ou* $p \equiv 3(mod 8)$*. Il en suit que les polynômes* $x^4+(a^2-2)x^2+1$ *avec* $a \neq 0$ *sont irréductibles au moins sur* $\mathbb{F}_{p^2}$ *pour chaque* $p \equiv \pm 1(mod 8)$ *et les polynômes* $x^4 + (a^2 + 2)x^2 + 1$ *avec* $a \neq 0$ *sont irréductibles au moins sur* $\mathbb{F}_{p^2}$ *pour* $p \equiv 1(mod 8)$ *ou* $p \equiv 3(mod 8)$*.*

Conclusion et perspectives

La factorisation des polynômes est un des problèmes fondamentaux du calcul formel, sur lequel beaucoup de progrès significatifs ont été faits ces dernières années. Dans notre travail de recherche, on s'est inspiré du produit composé de polynômes définis sur un corps fini étudié par Brawley et Carlitz et sa relation avec le résultant. Ce qui nous a permis de construire des polynômes irréductibles sur $\mathbb{Z}$ et réductibles modulo p pour tout nombre premier p. Notre sujet est d'actualité et a nécessité plusieurs lectures et discussions pour aboutir à ces résultats. Dans la suite, nous souhaitons élargir les travaux de Brawley et Carlitz à des polynômes définis sur des anneaux factoriels.

Bibliographie

[1] Ayad, M. On irreducible polynomials over q which are reducible over f p for all p. *The Rocky Mountain Journal of Mathematics* (2010), 1377–1389.

[2] Belabas, K. Résultant de deux polynômes. *Préparation à l'agrégation, Université Bourdeaux 1* (2012-2013).

[3] Benferhat, L., Benoumhani, S. M. E., Boumahdi, R., and Larone, J. Additive decompositions of polynomials over unique factorization domains. *Journal of Algebra and Its Applications* (2019), 2050150.

[4] Benferhat, L., Kihel, O., Larone, J., and Ould Mohamed, R. Irreducibility and multiplicative composition of polynomials over finite fields. *Tatra Mountains, Mathematical Publications*.

[5] Benoumhani, S. M. E. *Decomposition additive de polynômes sur les anneaux factoriels.* PhD thesis, Université des sciences et de la technologie Houari-Boumédiène (USTHB), 2020.

[6] Bostan, A., Flajolet, P., Salvy, B., and Schost, E. Fast computation with two algebraic numbers.

[7] Bostan, A., Flajolet, P., Salvy, B., and Schost, É. Fast computation of special resultants. *Journal of Symbolic Computation 41*, 1 (2006), 1–29.

[8] Brawley, J. V., and Brown, D. Composed products and module polynomials over finite fields. *Discrete mathematics 117*, 1-3 (1993), 41–56.

[9] Brawley, J. V., and Carlitz, L. Irreducibles and the composed product for polynomials over a finite field. *Discrete Mathematics 65*, 2 (1987), 115–139.

[10] Brawley, J. V., and Carlitz, L. A test for additive decomposability of irreducibles over a finite field. *Discrete mathematics 76*, 1 (1989), 61–65.

[11] Brawley, J. V., Gao, S., and Mills, D. Computing composed products of polynomials. *Contemporary mathematics 225* (1999), 1–16.

[12] Calais, J. *Éléments de théorie des anneaux : anneaux commutatifs ; niveau L3*. Ellipses Éd. Marketing, 2006.

[13] Cherchem, A. Corps finis. *Cours de Master, USTHB* (2012-2013).

[14] Cohen, H. *A course in computational algebraic number theory*, vol. 138. Springer Science & Business Media, 2013.

[15] Dvornicich, R., and Traverso, C. Newton symmetric functions and the arithmetic of algebraically closed fields. In *International Conference on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes* (1987), Springer, pp. 216–224.

[16] Gallian, J. *Contemporary abstract algebra*. Nelson Education, 2012.

[17] Gerhard, J., and Von zur Gathen, J. *Modern computer algebra*. Cambridge University Press, 2013.

[18] Glasby, S. On the tensor product of polynomials over a ring. *Journal of the Australian Mathematical Society 71*, 3 (2001), 307–324.

[19] Lidl, R., and Niederreiter, H. *Introduction to finite fields and their applications*. Cambridge university press, 1994.

[20] Loos, R. Computing in algebraic extensions. In *Computer algebra*. Springer, 1982, pp. 173–187.

[21] Marquis, D. *Deterministic factorization of polynomials over finite fields*. PhD thesis, Carleton University, 2015.

[22] Menezes, A. J., Blake, I. F., Gao, X., Mullin, R. C., Vanstone, S. A., and Yaghoobian, T. *Applications of finite fields*, vol. 199. Springer Science & Business Media, 2013.

[23] Munemasa, A., and Nakamura, H. A note on the brawley-carlitz theorem on irreducibility of composed products of polynomials over finite fields. In *International Workshop on the Arithmetic of Finite Fields* (2016), Springer, pp. 84–92.

[24] Querré, J. *Cours d'Algèbre*. Masson, 1876.

[25] Shoup, V. Fast construction of irreducible polynomials over finite fields. *Journal of Symbolic Computation 17*, 5 (1994), 371–391.

[26] Stichtenoth, H. A note on composed products of polynomials over finite fields. *Designs, codes and cryptography 73*, 1 (2014), 27–32.

[27] Szpirglas, A. *Mathématiques L3 : cours complet avec 400 tests et exercices corrigés. Algèbre*. Pearson Education France, 2009.

[28] Tuxanidy, A., and Wang, Q. Composed products and factors of cyclotomic polynomials over finite fields. *Designs, codes and cryptography 69*, 2 (2013), 203–231.