N° d'ordre :18/2020-C/MT

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université des Sciences et de la Technologie Houari Boumediene
Faculté de Mathématiques

THÈSE

Présentée pour l'obtention du diplôme de Doctorat 3ième cycle (LMD)

En : Mathématiques

Spécialité : Arithmétique, Codage et Combinatoire

Par : Safia Manar Elislam BENOUMHANI

DECOMPOSITION ADDITIVE DE POLYNÔMES SUR LES ANNEAUX FACTORIELS

Soutenue publiquement le 0./06/2020, devant le jury composé de :

M. BENCHERIF Farid	Professeur	USTHB	Président
Mme CHERCHEM Leila	MCA	USTHB	Directrice de thèse
M. CHERCHEM Ahmed	MCA	USTHB	Examinateur
M. ZEKIRI Abdelmoumene	MCA	USTHB	Examinateur
M. KIHEL Omar	Professeur	Brock University	Examinateur
Mme BELKREDIM Fatma Zohra	MCA	UHBC	Examinatrice
Mme BATOUL Aicha	MCA	USTHB	Invitée

Remerciements

Mes remerciements vont tout d'abord à ma directrice de thèse, Madame Leila Benferhat. Je la remercie pour m'avoir accueillie au sein de son équipe. Qu'elle soit aussi remerciée pour sa gentillesse, sa disponibilité permanente et son aide.
Je tiens à remercier infiniment Monsieur Farid BENCHERIF, professeur à l'USTHB, pour avoir accepté de présider ce jury.
Je remercie également Madame Fatima Zohra BELKREDIM, professeur à l'université Hassiba Benbouali de Chlef, Monsieur Ahmed CHERCHEM, MCA à l'USTHB et Monsieur Abdelmoumene ZEKIRI, MCA à l'USTHB, pour l'honneur qu'ils m'ont fait en acceptant d'être rapporteurs de cette thèse. C'est un honneur qu'ils aient accepté d'évaluer mon travail.
Je remercie également Madame Aicha BATOUL, MCA à l'USTHB, pour avoir accepté mon invitation pour faire partie de mon jury de thèse.
Je tiens à remercier particulièrement Monsieur Omar KIHEL, professeur à Brock university, qui m'a accueillie, deux fois, au sein de son laboratoire. Je le remercie pour son aide appréciable.
Je remercie toutes les personnes avec qui j'ai étudié et notamment ces années de thèse.
Enfin, merci à tous les membres du laboratoire LA3C.

Abstract

This thesis consists of three chapters. The first chapter is devoted to basic definitions and elementary results in ring theory.
The second chapter discusses composed products of polynomials over finite fields introduced in the works of Brawely and Carlitz. To define these products, they introduced a binary operation denoted by $\diamond$ on the set of polynomials over finite fields of degree ≥ 1. Moreover, they showed that an irreducible over a finite field can be factored uniquely into indecomposables.
In the last chapter, we present new results with detailed proofs which were published in the journal of algebra and its application.

Keywords : Diamond product, composed product, resultant, unique factorization domain, additive decomposition.

Résumé

Cette thèse est composée de trois chapitres.
Dans le premier chapitre, nous rappelons quelques définitions et théorèmes sur les anneaux, utiles aux chapitres suivants.
Le deuxième chapitre est réservé aux produits composés de polynômes définis par Brawley et Carlitz. Pour définir ces produits, ils ont introduit une loi de composition notée $\diamond$ sur l'ensemble des polynômes, de degré ≥ 1, à coefficients dans un corps fini. Ils ont particulièrement montré l'unicité de la décomposition de polynômes irréductibles en produit de polyômes indécomposables.
Dans le dernier chapitre, Nous exposons les résultats obtenus avec des démonstrations détaillées. Cette partie a fait l'objet d'une publication dans Journal of Algebra and its Applications.

Mots clés : Produit losange, Produit composé, Résultant, Anneau factoriel, Décomposition additive.

Notations

$\mathbb{F}_q$	Un corps fini à q éléments où $q = p^s$, p un nombre premier.
Ω	Une clôture algébrique de $\mathbb{F}_q$.
$\mathbb{F}_q[x]$	L'anneau des polynômes à coefficients dans $\mathbb{F}_q$.
$A[x]$	L'anneau des polynômes à coefficients dans l'anneau A.
$deg(f)$	Le degré du polynôme f.
$M_G[q, x]$	L'ensemble de polynômes unitaires à coefficients dans $\mathbb{F}_q$ de degrés ≥ 1 et dont les racines sont dans G.
$I_G[q, x]$	Le sous-ensemble de $M_G[q, x]$, 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.
$Cont(f)$	Le contenu du polynôme f.
$cd(f)$	Le coefficient dominant du polynôme f.
$d(\alpha)$	Le degré du nombre algébrique α.
$ord_m(q)$	L'ordre multiplicatif de q modulo m.
$ord(x)$	Ordre d'un élément dans un groupe.
σ	L'automorphisme de Frobenius.

Table des matières

Introduction

Soit $\mathbb{F}_q$ un corps fini, $q = p^s$, $s \in \mathbb{N}$, et Ω sa clôture algébrique. Soit $\mathbb{F}_q[x]$, l'anneau des polynômes à coefficients dans $\mathbb{F}_q$. Soient f et g deux polyômes unitaires de $\mathbb{F}_q[x]$ tels que $deg(f) = m \geq 1$ et $deg(g) = n \geq 1$.
La somme composée de f et g, notée $f * g$, est définie par

$$f * g = \prod_{\alpha} \prod_{\beta} (x - (\alpha + \beta)),$$

où α et β sont les racines respectives de f et g dans Ω.
La multiplication composée de f et g, notée $f \circ g$, est définie par

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

où α et β sont les racines respectives de f et g dans Ω. Notons que $f * g$ et $f \circ g$ sont des polynômes de $\mathbb{F}_q[x]$ de degré mn. 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, comme on le verra dans le chapitre 2. Dans [5], 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 $pgcd(n, m) = 1$. Leur résultat nous permet de construire des polynômes irréductibles sur $\mathbb{F}_q$ de degrés assez grands. Ils ont aussi examiné l'unicité de la décomposition additive ainsi que la décomposition multiplicative. Un polynôme unitaire $f \in \mathbb{F}_q[x]$, de degré ≥ 1, est dit additivement décomposable (respectivement multiplicativement décomposable) si $f = f_1 * f_2$ (respectivement $f = f_1 \circ f_2$) tels que $f_1, f_2 \in \mathbb{F}_q[x]$ et $deg(f) > 1$, $deg(g) > 1$.
Les lois $*$ et $\circ$ peuvent être définies sur un anneau commutatif grâce à un résultat établi par Loos dans [15]. Ce résultat montre le lien entre le résultant de deux polynômes et leur produit composé.
Dans cette thèse, on s'intéresse particulièrement à la décomposition additive de polynômes à coefficients dans un anneau factoriel.

Cette thèse comporte trois chapitres :
Dans le premier chapitre, on introduit des notions de base, notamment sur les anneaux factoriels et le résultant de deux polynômes à coefficients dans un anneau commutatif.
Le deuxième chapitre est consacré aux rappels concernant le produit composé $\diamond$ 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 allons donner 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 troisième chapitre, nous exposons les résultats principaux de la thèse sur la décomposition additive de polynômes sur les anneaux factoriels. Afin de définir l'addition composée de deux polynômes sur $R[x]$, où R est un anneau commutatif, nous utilisons la définition du résultant de deux polynômes et ses propriétés pour établir une formule qui permet de calculer l'addition composée. Nous étudions la décomposition additive de polynômes irréductibles sur un anneau intègre puis sur un anneau factoriel ainsi que la décomposition de polynômes primitifs sur un anneau factoriel. Les exemples donnés dans ce chapitre ont été effectués en utilisant le logiciel Maple.
Dans ce qui suit, nous appelons unité de $(R[x], *)$, un élément de $R[x]$ qui admet un symétrique pour la loi $*$.
Les résultats obtenus sont les suivants :

Théorème 0.1 *Soit R un anneau commutatif. Le groupe des unités de $(R[x], *)$ est égal à*

$$\mathcal{U} = \{ax + b : a, b \in R, a \text{ est une unité de } R\}. \tag{1}$$

Proposition 0.2 *Soit R un anneau intègre et K son corps des fractions. Soient f, g et $h \in R[x]$ avec $f = af_1, g = bg_1$ et $h = ch_1$, où a, b et $c \in R$ et f_1, g_1 et h_1 sont des polynômes unitaires. Alors, $h = f * g$ si, et seulement si, $h_1 = f_1 * g_1$ sur K et $c = a^{\deg(g)} b^{\deg(f)}$.*

On présente maintenant quelques classes de polynômes qui ne sont pas additivement décomposables.

Théorème 0.3 *Soit R un anneau intègre. Si le coefficient dominant de $h \in R[x]$ est un élément premier p alors h n'est pas additivement décomposable sur R.*

Le théorème précédent peut être modifié pour obtenir un résultat plus général lorsque R est un anneau factoriel.

Théorème 0.4 *Soit R un anneau factoriel et soit $h \in R[x]$ un polynôme de degré supérieur à 1. Si le coefficient dominant de h est sans facteur carré et n'est pas une unité de R alors h n'est pas additivement décomposable sur R.*

Théorème 0.5 *Soit R un anneau factoriel et soit $h = ax + b \in R[x]$ où a n'est pas une unité de R. Alors $h = f_1 * ... * f_r$, où $f_1, ..., f_r \in R[x]$ sont des polynômes linéaires qui ne sont pas additivement décomposables.*

Théorème 0.6 *Soit R un anneau factoriel et soit $h \in R[x]$ un polynôme qui n'est pas une unité par rapport à $*$. Alors*

$$h = f_1 * ... * f_r,$$

où $f_1, ..., f_r \in R[x]$ ne sont pas additivement décomposables.

Corollaire 0.7 *Soit $\sigma : R \to S$ un homomorphisme d'anneaux intègres et soit $h \in R[x]$. Si $\deg \sigma(h) = \deg h$ et $\sigma(h)$ n'est pas additivement décomposable sur S, alors $h = f * l$ où $f \in R[x]$ n'est pas additivement décomposable sur R et $l \in R[x]$ est un polynôme linéaire. De plus, si le coefficient dominant de f est une unité dans R alors l est une unité par rapport à $*$, donc h n'est pas additivement décomposable.*

Théorème 0.8 *Soit R un anneau intègre et $h \in R[x]$. On suppose que $h = f * g$ est additivement décomposable. Alors, si h est un polynôme irréductible sur R, les polynômes f et g sont irréductibles sur R.*

Définition 0.9 *Soit R un anneau factoriel et $f(x) = \sum_{i=0}^{m} f_i x^i \in R[x]$. Le contenu de f est défini par*

$$Cont(f) = pgcd(a_0, ..., a_m).$$

Si $Cont(f) = 1$, on dit que f est primitif.

Le théorème suivant nous donne une condition nécessaire pour que les facteurs de la décomposition additive d'un polynôme soient primitifs.

Théorème 0.10 *Soit R un anneau factoriel et soit $h \in R[x]$. Supposons que $h = f * g$ est additivement décomposable, où $f(x) = \sum_{i=0}^{m} f_i x^i \in R[x]$ et $g(x) = \sum_{i=0}^{n} g_i x^i \in R[x]$, tels que $\deg(f) = m$ et $\deg(g) = n$. De plus, supposons que $pgcd(Cont(g), f_m) = 1$ et $pgcd(Cont(f), g_n) = 1$. Alors, si h est primitif dans $R[x]$, f et g sont primitifs dans $R[x]$.*

Chapitre 1

Préliminaires

Les notions suivantes sont classiques et peuvent être trouvées dans [11], [9], [1], [8] et [22].

1 Structure d'anneau

Définition 1.1 (Anneau) *Soit A un ensemble non vide muni de deux lois de composition internes, notées $+$ et $\cdot$.*
A est appelé anneau s'il vérifie les conditions suivantes :

1. *$(A, +)$ est un groupe abélien dont l'élément neutre est noté 0.*
2. *La multiplication est associative. c'est à dire $\forall x, y$ et $z \in A, (x \cdot y) \cdot z = x \cdot (y \cdot z)$.*
3. *Le multiplication est distributive à droite et à gauche par rapport à l'addition : $\forall x, y, z \in A, (x + y) \cdot z = x \cdot z + y \cdot z$ et $x \cdot (y + z) = x \cdot y + x \cdot z$.*
4. *La multiplication possède un élément neutre noté 1.*

Si de plus la multiplication est commutative, A est dit "anneau commutatif".

Remarque 1.2 *A est dit nul s'il est réduit à $\{0\}$.*

Pour simplifier les notations, on notera A l'anneau $(A, +, \cdot)$.
Soit A un anneau . S'il existe un élément $y \in A$ tel que $x \cdot y = y \cdot x = 1$, on dit que x est **inversible** dans A et y est son inverse. On le note x^{-1}.

Définition 1.3 (Corps) *On appelle corps commutatif, tout anneau commutatif $A \neq \{0\}$ dans lequel tout élément $x \neq 0$ est inversible.*

Définition 1.4 *Les éléments inversibles d'un anneau A sont appelés les unités de l'anneau A. L'ensemble des unités de A est noté A^*.*

Pour tout anneau non nul A, A^* est un groupe, relativement à la multiplication de A, appelé groupe des unités de A.

Exemples 1.5 *1. $\mathbb{Z}$ est un anneau commutatif pour les lois usuelles. $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps commutatifs pour les lois usuelles.*

2. L'ensemble des classes de congruences modulo n, $\mathbb{Z}\big/n\mathbb{Z} = \{\bar{0}, \bar{1}, ..., \overline{n-1}\}$, est un anneau commutatif pour les lois $+$ et $\cdot$ définies par : $\forall \bar{x}, \bar{y} \in \mathbb{Z}\big/n\mathbb{Z}$, $\bar{x} + \bar{y} = \overline{x+y}$ et $\bar{x} \cdot \bar{y} = \overline{x \cdot y}$.

1.1 Sous-anneaux

Définition 1.6 (Sous-anneau) *Soit A un anneau. Une partie non vide B de A est un sous-anneau de A si*

1. $\forall x, y \in B, x - y \in B$ et $x \cdot y \in B$.

2. $1 \in B$.

Exemple 1.7 *L'ensemble des entiers de Gauss :*

$$\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\},$$

où $i^2 = -1$ est un sous-anneau de l'anneau $\mathbb{C}$.

2 Morphisme d'anneaux

Soit A et B deux anneaux. Une application ϕ de l'anneau A dans l'anneau B est un morphisme d'anneaux si on a :

1. $\forall x, y \in A, \phi(x + y) = \phi(x) + \phi(y)$;
2. $\forall x, y \in A$, $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$;
3. $\phi(1) = 1$.

Remarque 1.8 *1. Un morphisme d'anneaux est aussi appelé **homomorphisme** d'anneaux.*

*2. Si ϕ est un homomorphisme de l'anneau A dans lui même, ϕ est appelé **endomorphisme**.*

*3. Un endomorphisme bijectif est appelé **automorphisme**.*

*4. Un homomorphisme bijectif est appelé **isomorphisme**.*

Définition 1.9 *Soit f un homomorphisme d'un anneau A dans un anneau B. Le noyau de f est noté* $\ker f$ *et est défini par :*

$$\ker f = \{x \in A / f(x) = 0\}.$$

Pour plus de propriétés des morphismes, voir [8].

Exemples 1.10 *1. Soit A' un sous-anneau d'un anneau A, l'application*

$$\begin{aligned} i : A' &\longrightarrow A \\ x &\longmapsto x \end{aligned}$$

est un morphisme injectif d'anneaux, appelée injection canonique.

2. Pour $n \in \mathbb{N}^*$, l'application

$$\begin{aligned} \pi : \mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ x &\longmapsto \overline{x} \end{aligned}$$

est un morphisme surjectif d'anneaux, appelée surjection canonique, et on a

$$\ker \pi = n\mathbb{Z}$$

3 Les idéaux d'un anneau

Soit I une partie d'un anneau A.

Définition 1.11 *On dit que I est un idéal de A si I est un sous-groupe additif de A et si $\forall x \in I, \forall a \in A$, $a \cdot x \in I$ et $x \cdot a \in I$.*

Remarque 1.12 *Un idéal est dit propre s'il est distinct de A et de $\{0\}$.*

Exemples 1.13 *1. Soit $f : A \to B$ un morphisme d'anneaux,* $\ker f$ *est un idéal de A.*

2. Les idéaux de l'anneau $\mathbb{Z}$ sont de la forme :

$$m\mathbb{Z} = \{mx : x \in \mathbb{Z}\}$$

où $m \in \mathbb{Z}$.

Définition 1.14 (Idéal premier) *Soit A un anneau commutatif et I un idéal propre de l'anneau A. On dit que I est un idéal premier si*

$$\forall a, b \in I, a \cdot b \in I \Rightarrow a \in I \text{ ou } b \in I$$

Exemple 1.15 *Dans l'anneau $\mathbb{Z}$, les idéaux premiers sont de la forme $p\mathbb{Z}$, où p est un nombre premier.*

Définition 1.16 *Soit A un anneau commutatif et I un idéal de A. On dit que I est principal s'il existe $x \in A$ tel que*

$$I = xA = \{xy : y \in A\}.$$

Dans ce cas, I est noté $\langle x \rangle$ et on dit qu'il est engendé par x.

4 Caractéristique d'un anneau

Soit A un anneau commutatif. Considérons le morphisme d'anneaux suivant :

$$\begin{aligned} \psi : \mathbb{Z} &\longrightarrow A \\ k &\mapsto k \cdot 1, \end{aligned}$$

$ker(\psi)$ est un idéal de $\mathbb{Z}$, donc soit $\ker(\psi) = \{0\}$, soit il existe un entier $n > 0$ tel que $\ker(\psi) = n\mathbb{Z}$.

Définition 1.17 *Soit A un anneau commutatif et ψ le morphisme défini ci-dessus. La caractéristique de A est l'entier positif noté $car(A)$ défini par :*

- *$car(A) = 0$ si $\ker(\psi) = 0$.*
- *$car(A) = n$ si $\ker(\psi) = n\mathbb{Z}$.*

Proposition 1.18 (Homomorphisme de Frobenius) *Soit A un anneau commutatif de caractéristique p premier.*

1. *L'application $F : A \longrightarrow A$, définie par : $F(x) = x^p$ est un homomorphisme d'anneaux, appelé homomorphisme de Frobenius.*
2. *Pour tous $x, y \in A$ et tout $k \in \mathbb{N}$: $(x + y)^{p^k} = x^{p^k} + y^{p^k}$.*

5 Anneau intègre

Définition 1.19 (Diviseur de zéro) *Soit A un anneau et $a \in A$ tel que $a \neq 0$.*

1. *On dit que a est un diviseur de 0 à gauche dans A s'il existe $b \in A$ non nul tel que $a \cdot b = 0$.*
2. *On dit que a est un diviseur de 0 à droite dans A s'il existe $b \in A$ non nul tel que $b \cdot a = 0$.*

Si a est un diviseur de zéro à gauche dans A ou un diviseur de zéro à droite dans A, on dit que a est un diviseur de zéro dans A.

Définition 1.20 (Anneau intègre) *Un anneau A est dit intègre s'il est commutatif, non nul, et sans diviseur de zéro.*

Définition 1.21 *Un anneau intègre est appelé **domaine d'intégrité**.*

Exemples 1.22
1. *$\mathbb{Z}$ est un anneau intègre .*
2. *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si, et seulement si, n est premier.*
3. *L'anneau des polynômes $\mathbb{Z}[x]$ est intègre.*
4. *L'anneau $M_2(\mathbb{Z})$ des matrices 2×2 sur $\mathbb{Z}$ n'est pas un anneau intègre.*

Théorème 1.23 *Un anneau intègre fini est un corps.*

Théorème 1.24 *Un corps commutatif est un anneau intègre.*

6 Caractéristique d'un corps

Proposition 1.25 *Si K est un corps commutatif de caractéristique n non nulle, alors n est premier.*

Démonstration 1.26 *En effet, si n n'est pas premier, alors $n = p.q$, où p et q sont des entiers tels que $1 < p < n$ et $1 < q < n$. On a $0 = n.1 = (p \cdot 1) \cdot (q \cdot 1)$, ce qui implique $p \cdot 1 = 0$ ou $q \cdot 1 = 0$ car un corps commutatif est un anneau intègre, ce qui contredit la définition de la caractéristique.*

Exemple 1.27 *L'anneau $\mathbb{Z}$, les corps $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont de caractéristique 0. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n et si p est premier, le corps $\mathbb{Z}/p\mathbb{Z}$ est de caractéristique p.*

7 Corps des fractions

Soit A un anneau intègre. Il existe un corps dont un sous-anneau est isomorphe à A qu'on appelle ***le corps des fractions*** de A. C'est le plus petit corps contenant A. Prenons par exemple le corps $\mathbb{Q}$ des rationnels qui est le corps des fractions de l'anneau $\mathbb{Z}$. La construction des corps de fractions est une généralisation de la construction de $\mathbb{Q}$. Pour plus de détails, voir [19].

8 Divisibilité

Soit A un anneau intègre.

Définition 1.28 *Soit $a, b \in A$, $a \neq 0$. On dit que a divise b et on note $a \mid b$ s'il existe $q \in A$ tel que $b = q \cdot a$.*

Définition 1.29 *Soit $a, b \in A$. On dit que a et b sont associés s'il existe $u \in A^*$ tel que $a = u \cdot b$.*

Définition 1.30 (Élément premier) *Soient $a, b \in A$. Un élément p est dit premier dans A si p est non nul, n'est pas une unité de A et si $p \mid ab$ alors p divise a ou p divise b. Deux éléments a et b de A sont dit premiers entre eux si tout diviseur commun à a et b est inversible.*

Proposition 1.31 *Soit $I = \langle p \rangle$ l'idéal de A engendré par $p \in A$. Alors, p premier dans A équivaut à I est un idéal premier.*

Définition 1.32 (Élément irréductible) *Un élément a est dit irréductible dans A s'il n'est pas inversible et si $a = xy$ entraîne $x \in A^*$ ou $y \in A^*$*

Remarque 1.33

1. *Une unité de A divise tous les éléments de A.*
2. *Les seuls diviseurs d'un élément irréductible de A sont ses associés et les unités de l'anneau A.*

Exemples 1.34

1. *Dans $\mathbb{Z}$, 5 est irréductible mais dans $\mathbb{Z}[i]$, il n'est pas irréductible car $5 = (2+i)(2-i)$.*
2. *Le polynôme $x^2 - 3$ est irréductible dans l'anneau $\mathbb{Q}[x]$ mais réductible dans $\mathbb{R}[x]$.*

Proposition 1.35 *Si p est un élément premier de A, alors il est irréductible.*

Démonstration 1.36 *Supposons que p est premier. Si p n'est pas irréductible alors p peut s'écrire sous la forme $p = a \cdot b$, où a et b ne sont pas des unités de A. Alors $p \mid a \cdot b$ et donc $p \mid a$ ou $p \mid b$. Si $p \mid a$ alors il existe $q \in A$ tel que $a = p \cdot q$. Donc*

$$p = a \cdot b = p \cdot q \cdot b \Rightarrow p \cdot (1 - q \cdot b) = 0, \tag{1.1}$$

et comme A est intègre et $p \neq 0$ alors $q \cdot b = 1$, d'où b est inversible, ce qui est impossible.
Si $p \mid b$, en effectuant le même raisonnement, on montre que a est inversible, ce qui est également impossible. Donc p est irréductible.

La réciproque est fausse en général, prenons par exemple l'anneau $A = \mathbb{Z}[i\sqrt{5}] = \{a + i\sqrt{5}b; (a, b) \in \mathbb{Z} \times \mathbb{Z}\} \subset \mathbb{C}$ qui est un sous-anneau de $\mathbb{C}$, 3 est irréductible mais non premier dans A.

Définition 1.37 *Soit a et b deux éléments non nuls de A. On dit que $d \in A$ est un plus grand diviseur commun de a et b noté $pgcd(a, b)$ si les propriétés suivantes sont vérifiées :*

1. *$d \mid a$ et $d \mid b$.*
2. *Si $c \in A, c \neq 0$, tel que $c \mid a$ et $c \mid b$ alors $c \mid d$.*

On dit que $m \in A$ est un plus petit multiple commun de a et b noté $ppcm(a, b)$ si les propriétés suivantes sont vérifiées :

1. *$a \mid m$ et $b \mid m$.*
2. *Si $c \in A$ tel que $a \mid c$ et $b \mid c$ alors $m \mid c$.*

Lemme 1.38 *Soient a, b et $x \in A$. On pose $d = pgcd(a, b)$. Si x est un autre pgcd de a et b alors x et d sont associés.*

9 Anneaux quotients

Soit A un anneau commutatif et I un idéal de A. Comme A est commutatif, I est, en particulier, un sous-groupe distingué de A, ce qui permet de définir le groupe quotient A/I et la projection canonique :

$$\begin{aligned} \pi : A &\longrightarrow A/I \\ x &\longrightarrow \bar{x} = x + I. \end{aligned}$$

On définit sur A/I l'addition et la multiplication comme suit :

$$\bar{x} + \bar{y} = \overline{x+y},$$
$$\bar{x} \cdot \bar{y} = \overline{x \cdot y}\ .$$

$(A/I, +, \cdot)$ est un anneau commutatif. On notera que, si $I = A$, alors A/I est l'anneau nul et, si $I = \{0\}$, alors $A/I = A$.

Proposition 1.39 *Soit A un anneau commutatif et I un idéal de A. On a l'équivalence suivante :*

$$I \text{ est un idéal premier dans } A \Leftrightarrow A/I \text{ est un anneau intègre} \tag{1.2}$$

10 Anneau des polynômes

On appelle polynôme à coefficients dans un anneau commutatif A toute suite $f = (a_n)_{n\in\mathbb{N}}$ d'éléments de A nulle à partir d'un certain rang.

10.1 Opérations sur les polynômes

Soit A un anneau commutatif. Soient $f = (a_n)_{n\in\mathbb{N}}$ et $g = (b_n)_{n\in\mathbb{N}}$ deux polynômes à coefficients dans un anneau commutatif A. On définit la somme et le produit de f et g comme suit :

$$f + g = (a_n + b_n)_{n\in\mathbb{N}}, \tag{1.3}$$

et

$$fg = (c_k)_{k\in\mathbb{N}}, \text{ où } c_k = \sum_{i=o}^{k} a_i b_{k-i}. \tag{1.4}$$

Si f est un polynôme à coefficients dans un anneau commutatif A. On note ce polynôme $f(x) = \sum_{i\geq 0} a_i x^i$, où $x = (0, 1, 0, \cdots)$ est appelé l'indéterminée.
L'ensemble des polynômes à coefficients dans A est noté $A[x]$.
Soit $f(x) = \sum_{i\geq 0} a_i x^i \in A[x]$.
Soit n le plus grand indice tel que $a_n \neq 0$ (s'il existe), a_n est appelé coefficient dominant de f.
On dit que f est un polynôme unitaire si le coefficient dominant est égal à 1.
Si tous les coefficients a_i sont nuls, f est appelé "**polynôme nul**", il est noté 0.
On appelle "**degré de f**" le plus grand entier i tel que $a_i \neq 0$; on le note $\deg(f)$.
Pour le degré du polynôme nul, on pose par convention $\deg(0) = -\infty$.
Un polynôme de la forme $f = a_0$ avec $a_0 \in A$ est appelé "**polynôme constant**". Si $a_0 \neq 0$, son degré est 0.

Remarque 1.40 *Comme a_i est nul à partir d'un certain rang, un polynôme de $A[x]$ peut s'écrire $\sum_{i=0}^{n} a_i x^i$.*

Proposition 1.41 *Soit A un anneau commutatif. Soient f et g deux polynômes dans $A[x]$, alors*

$$deg(f+g) \leq max(deg(f), deg(g)) \tag{1.5}$$

et

$$deg(fg) \leq deg(f) + deg(g) \tag{1.6}$$

Si A est un anneau intègre, alors $deg(fg) = deg(f) + deg(g)$.

Théorème 1.42 *Si A est une anneau intègre alors l'anneau des polynômes $A[x]$ est un anneau intègre.*

Démonstration 1.43 *Montrons que $A[x]$ n'admet pas de diviseur de zéro. Posons*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_0 \tag{1.7}$$

et

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + ... + b_0 \tag{1.8}$$

avec $a_n \neq 0$ et $b_m \neq 0$. Alors, le coefficient dominant de fg est $a_n b_m$, et $a_n b_m \neq 0$, d'où $A[x]$ est un anneau commutatif intègre.

Théorème 1.44 *Si K est un corps commutatif alors l'anneau des polynômes $K[x]$ est un anneau principal.*

10.2 Division euclidienne

Soit K un corps commutatif.

Théorème 1.45 (Division Euclidienne) *Soient f et g deux polynômes dans $K[x]$ avec g non nul. Il existe un unique couple (q, r) de $K[x] \times K[x]$ tel que :*

$$f = gq + r \text{ et } deg(r) < deg(g) \tag{1.9}$$

Théorème 1.46 (Bézout) *Soient f_1 et f_2 deux polynômes non nuls dans $K[x]$. Alors, f_1 et f_2 sont premiers entre eux si, et seulement si, il existe u et v de $K[x]$ tels que :*

$$f_1 u + f_2 v = 1. \tag{1.10}$$

Les résultats suivants sont des conséquences immédiates du théorème de Bézout.

Théorème 1.47 (Gauss) *Soient f, g et d trois polynômes de $K[x]$. Si $d \mid fg$ et $pgcd(f,d) = 1$ alors $d \mid g$.*

Proposition 1.48 *Soit f, g et h trois polynômes de $K[x]$. Si $pgcd(f,g) = 1$, $f \mid h$ et $g \mid h$ alors h est divisible par le produit fg.*

10.3 Polynômes irréductibles sur un corps commutatif

Soit K un corps commutatif.

Définition 1.49 *Un polynôme $P \in K[x]$ est dit irréductible sur K si P n'est pas constant et ses seuls diviseurs dans $K[x]$ sont les polynômes constants et ceux de la frome λP, où $\lambda \in K^*$.*

Un polynôme qui n'est pas irréductible, est dit réductible.

Proposition 1.50 *On note $\mathcal{I}_K$, l'ensemble des polynômes irréductibles sur K.*

1. *$\mathcal{I}_{\mathbb{C}} = \{P \in \mathbb{C}[x], \deg(P) = 1\}$.*
2. *Un polynôme $P \in \mathcal{I}_{\mathbb{R}}$ si, et seulement si, il est de degré un ou s'il est de degré deux et de discriminant strictement négatif.*

Théorème 1.51 *Soit $f \in K[x]$ un polynôme non nul. Le polynôme f se décompose de manière unique, à l'ordre des facteurs près, sous la forme :*

$$f = af_1^{a_1} f_2^{a_2} \dots f_r^{a_r}, \tag{1.11}$$

où les f_i sont des polynômes distincts, unitaires et irréductibles dans $K[x]$, les a_i, $i = \overline{1,r}$, sont des entiers naturels non nuls et $a \in K^*$ est le coefficient dominant de f.

Exemple 1.52 *Soit $f(x) = x^2 + 1$. Dans $\mathbb{C}[x]$, $f(x) = (x-i)(x+i)$ est réductible, mais il est irréductible dans $\mathbb{R}[x]$.*

Proposition 1.53 *Soit f et g deux polynômes non nuls de $K[x]$ et soit*

$$f = af_1^{a_1} f_2^{a_2} \dots f_r^{a_r}$$

et

$$g = bf_1^{b_1} f_2^{b_2} \dots f_r^{b_r},$$

leurs factorisations en facteurs irréductibles, où $a_i, b_i \in \mathbb{N}^*$, $i = \overline{1,r}$. Alors

$$f \mid g \Leftrightarrow a_i \leq b_i, i = \overline{1,r}$$

.

Définition 1.54 *Soit $f \in K[x]$. On dit que $\alpha \in K$ est une racine de f si $f(\alpha) = 0$. Une racine α est de multiplicité k si, et seulement si, $(x-\alpha)^k \mid f$ et $(x-\alpha)^{k+1} \nmid f$.*

11 Quelques notions sur les corps finis

Définition 1.55 *Un corps fini est un corps ayant un nombre fini d'éléments. Il est unique à isomorphisme près et est noté $\mathbb{F}_q$, où q est le nombre de ses éléments.*

Théorème 1.56 (Théorème de Wedderburn) *Tout corps fini est commutatif.*

Théorème 1.57 *Soit $\mathbb{F}_q$ un corps fini, alors q est égal à p^n, où p est un nombre premier et n un entier naturel non nul.*

Proposition 1.58 *Un corps fini $\mathbb{F}_q$, $q = p^n$, $n \in \mathbb{N}^*$, est de caractéristique p et toute extension de $\mathbb{F}_q$ est de caractéristique p.*

Théorème 1.59 *Soit m, $n \in \mathbb{N}^*$ et p un nombre premier, alors*

$$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \Leftrightarrow m \text{ divise } n. \tag{1.12}$$

Soit Ω la clôture algébrique de $\mathbb{F}_q$.

Théorème 1.60 $\Omega = \cup_{n \geq 1} \mathbb{F}_{q^n}$

Proposition 1.61 *L'application $\sigma : \Omega \to \Omega$ définie par $\sigma(x) = x^q$ est un automorphisme, appelé automorphisme de Frobenius.*

Proposition 1.62 *Soit $\mathbb{F}_q$ un corps fini, F une extension de $\mathbb{F}_q$ et $f \in F[x]$ un polynôme à coefficients dans F. Alors, $f \in \mathbb{F}_q[x]$ si, et seulement si, $f(x^q) = f(x)^q$.*

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

Théorème 1.63 *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 1.64 *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*

$$\alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}}. \tag{1.13}$$

Théorème 1.65 *Soit $q = p^n$ et posons*

$$\mu_d = \{f(x) \in \mathbb{F}_p[x] : f(x) \text{ irréductible unitaire de degré } d\}, \tag{1.14}$$

alors on a

$$x^q - x = \prod_{\substack{f(x)\in\mu_d \\ d|n}} f(x). \tag{1.15}$$

Exemple 1.66 *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 1.67 *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 1.68 *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 $x^e - 1$ et 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 1.69 *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 1.70 *Soit $f(x) \in \mathbb{F}_q[X]$ irréductible de degré m, alors $e(f)$ divise $q^m - 1$.*

12 Anneaux factoriels

Les anneaux factoriels sont les anneaux dans lesquels on peut généraliser le théorème fondamental de l'arithmétique. Rappelons le théorème fondamental de l'arithmétique.

Théorème 1.71 *Tout entier $n > 1$ se factorise de façon unique en produit de nombres premiers.*

Définition 1.72 *Soit A un anneau. On dit que A est factoriel s'il est intègre et si les deux conditions suivantes sont réalisées :*

1. *Pour tout élément non nul $a \in A$, il existe des éléments irréductibles $p_1, \ldots, p_r$ de A tels que*
$$a = \prod_{i=1}^{r} p_i. \tag{1.16}$$
2. *Si $p_1 \cdots p_r = q_1 \cdots q_s$, où les éléments $p_1, \cdots, p_r, q_1, \cdots, q_s \in A$ sont irréductibles, alors $r = s$ et il existe une permutation $\sigma \in S_r$ telle que pour tout $i \in \{1, \cdots, r\}$, p_i et $q_{\sigma(i)}$ sont associés.*

Remarque 1.73 *Dans un anneau factoriel, la notion de pgcd est bien définie, à multiplication par un élément inversible près. Par contre, il n'y a pas en général d'identité de Bézout. Par exemple, dans $\mathbb{C}[X, Y]$, le pgcd de X et de Y est 1, mais pour tous $P, Q \in \mathbb{C}[X, Y]$, le polynôme $XP + YQ$ est différent de 1.*

Exemples 1.74
1. *D'après le théorème fondamental de l'arithmétique, l'anneau $\mathbb{Z}$ est un anneau factoriel.*
2. *L'anneau $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\}$ n'est pas factoriel. L'élément 6 admet deux factorisations distinctes*
$$6 = 2 \cdot 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i).$$
En utilisant la norme, on peut montrer que $1 \pm \sqrt{5}i$ sont irréductibles dans $\mathbb{Z}[\sqrt{-5}]$.

Théorème 1.75 *Soit A un anneau factoriel. Alors*
$$p \text{ irréductible dans } A \Leftrightarrow p \text{ premier dans } A$$

Définition 1.76 (Valuation) *Soit A un anneau factoriel, K son corps des fractions et p un élément irréductible de A. Soit a un élément non nul de K. Alors il existe $u, v \in A$ non divisibles par p et un entier relatif r tels que*
$$a = p^r \frac{u}{v}.$$
Cet entier r est unique. C'est par définition la valuation en p de a, notée $v_p(a)$. Par convention, on a : $v_p(0) = -\infty$.

Proposition 1.77 *Soit A un anneau factoriel. $\forall a, b \in A$, on a :*
1. *$v_p(ab) = v_p(a) + v_p(b)$.*
2. *$v_p(a+b) \geq min(v_p(a), v_p(b))$, et si $v_p(a) \neq v_p(b)$, on a $v_p(a+b) = min(v_p(a), v_p(b))$.*

Soit A un anneau factoriel et K son corps des fractions. Une partie $\mathcal{P}$ de A est appelée système de représentants des éléments irréductibles de A si pour tout irréductible q de A, il existe p dans $\mathcal{P}$ et $u \in A^*$ uniques tels que $q = up$.
Si un tel $\mathcal{P}$ est fixé, tout élément $a \in K^*$ s'écrit de façon unique sous la forme

$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)},$$

où $u \in A^*$. On définit alors le *pgcd* et le *ppcm* dans K^* (à multiplication près par un élément de A^*) de la manière suivante :

$$pgcd(a, b) = \prod_{p \in \mathcal{P}} p^{min(v_p(a), v_p(b))}, \tag{1.17}$$

$$ppcm(a, b) = \prod_{p \in \mathcal{P}} p^{max(v_p(a), v_p(b))}. \tag{1.18}$$

On pose $pgcd(0, 0) = 0$. Plus généralement, on peut définir le *pgcd* et le *ppcm* de $a_0, \cdots, a_n \in K^*$ par

$$pgcd(a_0, \cdots, a_n) = \prod_{p \in \mathcal{P}} p^{min(v_p(a_0), \cdots, v_p(a_n))}$$

et

$$pgcm(a_0, \cdots, a_n) = \prod_{p \in \mathcal{P}} p^{max(v_p(a_0), \cdots, v_p(a_n))}$$

13 Polynômes à coefficients dans un anneau factoriel

Soit A un anneau factoriel, K son corps des fractions. Soit $f = \sum_{i=0}^{n} f_i X^i$ un polynôme non nul de degré n de $K[x]$. Le coefficient dominant de f est noté $cd(f)$. On a $cd(f) = f_n \neq 0$.

Définition 1.78 *Le contenu de $f \in K[x]$, est défini (à multiplication près par un élément de A^*) par :*

$$Cont(f) = pgcd(f_0, \cdots, f_n). \tag{1.19}$$

On pose $Cont(0) := 0$.

Définition 1.79 *On dit que $f \in K[x]$ est primitif si $Cont(f) = 1$.*

Définition 1.80 *La partie primitive $PP(f)$ d'un polynôme $f \in K[x]$ est définie (modulo une multiplication par une unité de A) par*

$$f = Cont(f)PP(f), \text{ si } f \neq 0,$$

et $PP(0) = 0$.

Théorème 1.81 *Le produit de deux polynômes primitifs de $A[x]$ est primitif.*

Démonstration 1.82 *Soient f et g deux polynômes primitifs de $A[x]$. Soit p un élément irréductible de A. Comme l'idéal pA est premier, l'anneau $D = A/pA$ est intègre, donc $D[x]$ est aussi intègre. Dans $D[x]$, la classe de f et de g modulo p sont non nulles, donc la classe de fg modulo p est non nulle. Par conséquent, p ne divise pas $Cont(fg)$. Ce qui est vrai pour tout irréductible p de A. On en déduit que $Cont(fg) = 1$.*

Corollaire 1.83 (Gauss) *Soient $A, B \in K[X]$. On a*

$$Cont(AB) = Cont(A)Cont(B), \tag{1.20}$$

et

$$PP(AB) = PP(A)PP(B). \tag{1.21}$$

Démonstration 1.84 *Si $AB = 0$, le résultat est vérifié. Sinon, on a d'une part*

$$AB = Cont(AB)PP(AB), \tag{1.22}$$

et d'autre part, en décomposant A et B séparément,

$$AB = Cont(A)Cont(B)PP(A)PP(B). \tag{1.23}$$

Les contenus étant non nuls, on déduit de l'égalité $Cont(AB) = Cont(A)Cont(B)$ que $PP(AB) = PP(A)PP(B)$.
Commençons par un cas particulier : si $R \in K^*$ et $A = \sum_{k=0}^{n} a_k x^k$ alors

$$Cont(AR) = pgcd(a_0R, \cdots, a_nR) = R.pgcd(a_0, \cdots, a_n) = Cont(R)Cont(P), \tag{1.24}$$

et le résultat est démontré dans ce cas.
Soient maintenant A et B dans $K[x]$. On note $h = PP(AB)$ et $h^* = PP(A).PP(B)$. On a l'égalité

$$AB = Cont(A)PP(B)Cont(B)PP(B) = Cont(A)Cont(B)Cont(h^*). \tag{1.25}$$

D'où

$$Cont(AB) = Cont\Big(Cont(A)Cont(B)Cont(h^*)\Big) = Cont(A)Cont(B)Cont(h^*), \tag{1.26}$$

d'après le cas particulier que nous venons de démontrer. Comme h^* est primitif, on peut conclure.

Théorème 1.85 *Soit A un anneau factoriel, K son corps des fractions. Les éléments irréductibles de $A[X]$ sont :*

1. *Les polynômes constants p, p irréductible dans A.*
2. *Les polynômes primitifs de degré ≥ 1 de $A[x]$ qui sont irréductible dans $K[X]$.*

Démonstration 1.86 *Les irréductibles de $A[X]$ de degré 0 sont clairement les éléments irréductibles p de A.*
Si P est un élément de $A[x]$ de $\deg \geq 1$, alors il est divisible par son contenu, donc les irrédutibles de $A[X]$ sont primitifs. Un polynôme P non constant et primitif qui est irréductible dans $K[X]$ l'est dans $A[X]$. En effet, par contraposée, si $P \in A[X]$, $P = P_1P_2, P_i \in A[X]$ avec les degrés de P_1 et P_2 >0 . Cette décomposition est donc aussi une décomposition dans $K[X]$ donc P est réductible dans $K[X]$.
Réciproquement, soit P un polynôme non constant, irréductible dans $A[X]$. Supposons qu'il existe P_1 et $P_2 \in K[X]$ non constants tels que $P = P_1P_2$ et d_1, d_2 les ppcm des dénominateurs des coefficients de P_1 et P_2 respectivement. On a $d_1P_1, d_2P_2 \in A[X]$ alors $d_1d_2P = d_1P_1d_2P_2$.

$$Cont(d_1d_2P) = Cont(d_1P_1d_2P_2), \tag{1.27}$$

$$d_1d_2 = Cont(d_1P_1)Cont(d_2P_2). \tag{1.28}$$

Posons $\tilde{P}_j = Cont(d_jP_j)^{-1}d_jP_j$ pour $j = 1, 2$. Alors $P = \tilde{P}_1\tilde{P}_2$. Ce qui est une contradiction car P est irréductible dans $A[x]$. Ainsi, les polynômes irréductibles de degré > 0 dans $A[X]$ sont primitifs et irréductibles dans $K[X]$.

Théorème 1.87 *Soit A un anneau factoriel. L'anneau $A[X]$ est aussi factoriel.*

Démonstration 1.88 *[22]*

Soit $f \in A[x]$ non nul et non inversible. Montrons que f est s'écrit comme un produit d'éléments irréductibles de $A[x]$. Soit K le corps des fractions de A.
Dans $K[x]$

$$PP(f) = \prod_{i=1}^{r} f_i,$$

où les f_i sont des éléments irréductibles de $K[x]$.
En prenant la partie principale du produit précédent, on obtient

$$PP(f) = \prod_{i=1}^{r} PP(f_i).$$

Les $PP(f_i)$, $i \in \{1, \cdots, r\}$, sont primitifs et irréductibles dans $K[x]$, donc irréductibles dans $A[x]$. Comme A est factoriel, on peut aussi décomposer $Cont(f)$ en produit d'éléments irréductibles de A, donc de $A[x]$. Ceci montre que f est décomposable en un produit d'éléments irréductibles de $A[x]$.
Démontrons maintenant l'unicité de la décomposition. Supposons que

$$f = \prod_{i=1}^{r} p_i \prod_{i=1}^{s} f_i = \prod_{i=1}^{t} q_i \prod_{i=1}^{u} g_i$$

où les p_i et les q_i sont des éléments irréductibles de A et où les f_i et les g_i sont des éléments irréductibles de degré ≥ 1 de $A[x]$ (donc primitifs). On en déduit que

$$Cont(f) = \prod_{i=1}^{r} p_i = \prod_{i=1}^{t} q_i.$$

Donc $r = t$ et il existe une permutation σ de S_r telle que pour tout $i \in \{1, \cdots, r\}$, p_i est associé à $q_{\sigma(i)}$. On a également

$$PP(f) = \prod_{i=1}^{s} f_i = \prod_{i=1}^{u} g_i.$$

Puisque les f_i et les g_i sont primitifs, en regardant cette égalité dans $K[x]$, il vient que $s = u$ et qu'il existe une permutation τ de S_s telle que pour tout $i \in \{1, \cdots, s\}$, f_i et $g_{\tau(i)}$ sont associés.

Corollaire 1.89 *1. Soit A un anneau factoriel. Alors, pour tout entier $n \geq 1$, l'anneau $A[X_1, ..., X_n]$ est factoriel.*

2. Soit K un corps commutatif. Alors, pour tout entier $n \geq 1$, l'anneau $K[X_1, ..., X_n]$ est factoriel.

14 Résultant de deux polynômes

Soit K un corps commutatif et soit l'ensemble $P_d = \{p \in K[x] : deg(p) < d\}$, où d est un entier positif. L'ensemble P_d est un espace vectoriel de dimension d. Soit 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 $K[x]$ tels que :

$$f(x) = \sum_{i=0}^{m} a_i x^i, \tag{1.29}$$

et

$$g(x) = \sum_{i=0}^{n} b_i x^i. \tag{1.30}$$

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 bases est la matrice carrée de taille $(n+m)$ suivante :

$$M = \begin{pmatrix} a_m & 0 & \cdots & 0 & b_n & 0 & \cdots & \cdots & 0 \\ a_{m-1} & a_m & \ddots & 0 & b_{n-1} & b_n & & & \\ \vdots & a_{m-1} & \ddots & \vdots & \vdots & b_{n-1} & \ddots & & \\ \vdots & \vdots & \ddots & a_m & b_0 & \vdots & & \ddots & \\ a_0 & \vdots & & \vdots & 0 & b_0 & & & b_n \\ 0 & a_0 & \vdots & \vdots & \vdots & \ddots & \ddots & & \\ \vdots & \ddots & \ddots & & & & & \ddots & \\ 0 & \cdots & 0 & a_0 & 0 & \cdots & \cdots & 0 & b_0 \end{pmatrix}$$

La matrice M est appelée matrice de **Sylvester** et est notée $Sylv(f,g)$. Le déterminant de M est non nul si, et seulement si, f et g sont premiers entre eux.
Remarquons que les coefficients de f sont reproduits sur m colonnes et ceux de g sur n colonnes. Le déterminant de M est une expression en fonction des coefficients de f et g et est appelé **Résultant** de f et g , noté $Res_x(f,g)$ ou simplement $Res(f,g)$. Les notions de matrice de Sylvester et de résultant se généralisent pour les polynômes à coefficients dans un anneau commutatif quelconque.

Propriétés 1.90 *Soit A un anneau commutatif. On pose*

$$f(x) = \sum_{i=0}^{m} a_i x^i \in A[x], \tag{1.31}$$

et

$$g(x) = \sum_{i=0}^{n} b_i x^i \in A[x]. \tag{1.32}$$

1. $Res(f, g) \in A$.
2. $Res(f, g) = (-1)^{mn} Res(g, f)$.
3. $\forall a \in A, Res(af, g) = a^m Res(f, g)$.
4. $\forall a \in A$, $Res(a, g) = a^n$, *où g est un polynôme non constant de degré n de* $A[x]$.

Démonstration 1.91 *Voir [15] et [12].*

Remarque 1.92 *Par convention on pose :* $Res(a, b) = 1$, $\forall a, b \in A$.

Soit A un anneau commutatif 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 $f_m(x)$. 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 $f_m(x)$. Ces relations entre les coefficients et les racines d'un polynômes interviennent dans la preuve du lemme suivant qui nous permet de démontrer des propriétés importantes des résultants.

Lemme 1.93 *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*

$$Res(f_m, g) = g(\alpha_m) Res(f_{m-1}, g). \tag{1.33}$$

Démonstration 1.94 *Voir [15], page 177.*

Théorème 1.95 *Soit A un anneau intègre. Soient $f, g \in A[x]$ tels que $f(x) = a_m \prod_{i=1}^{m} \Big(x - \alpha_i\Big)$ et $g(x) = b_n \prod_{i=1}^{n} \Big(x - \beta_i\Big)$, avec α_i et β_i les racines respectives de f et g, a_m et b_n leurs coefficients dominants respectifs, alors*

$$Res(f,g) = (-1)^{mn} b_n^m \prod_i f(\beta_i), \tag{1.34}$$

$$Res(f,g) = a_m^n b_n^m \prod_i \prod_j (\alpha_i - \beta_j), \tag{1.35}$$

$$Res(f,g) = a_m^n \prod_i g(\alpha_i). \tag{1.36}$$

Démonstration 1.96 *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 (1.34). On a vu que :*

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

alors, d'après (1.36), on obtient (1.34).

Maintenant, on prouve (1.36). 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 $f_m = \prod_{i=1}^{m} (x - \alpha_i)$ et en appliquant le lemme (1.93) sur les f_i, $1 \leq i \leq m$, nous aurons

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

On montre facilement (1.35) :

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

Remarque 1.97 *Si f et $g \in A[x,y]$, on note, $Res_x(f,g)$ le résultant dans $A[y]$ par rapport à x.*

Théorème 1.98 *Soit Kun corps commutatif. Si $f, g \in K[x]$ admettent une racine commune dans K alors $Res(f,g) = 0$.*

Démonstration 1.99 *Conséquence immédiate de (1.34).*

Les trois théorèmes suivants montrent d'autres propriétés des résultants indépendantes des racines des polynômes.

Théorème 1.100 *[15]*
Soient A un anneau factoriel, f et g deux polynômes non nuls de $A[x]$. alors

$$pgcd(f,g) \notin A \text{ si, et seulement si, } Res(f,g) = 0. \tag{1.37}$$

Théorème 1.101 *[15]*

Soit A un anneau commutatif. Soient f et g deux polynômes dans $A[x]$ de degrés positifs. Alors, il existe $S, T \in A[x]$ tels que

$$fS + gT = Res(f,g),$$

avec $deg(S) < deg(f)$ et $deg(T) < deg(g)$.

Théorème 1.102 *[15]*

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

$$Res(f, x^k g) = Res(f, g) \prod_{i=0}^{k} Res(f, x), \tag{1.38}$$

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

$$Res(f, x^k g) = (-1)^{mk} a_0^k Res(f, g). \tag{1.39}$$

Théorème 1.103 (Rüdiger Loos) *Soit A un anneau intègre et soient $f, g \in A[x]$ tels que*

$$f(x) = a_n \prod_{i=1}^{n} \Big(x - \alpha_i\Big), g(x) = b_m \prod_{j=1}^{m} \Big(x - \beta_j\Big), \tag{1.40}$$

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 nécéssairement distinctes, telles que :

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

Démonstration 1.104 *[15]*
On démontre les quatre formules en utilisant la relation (1.34).

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 1.105 *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 $\overline{cd(f)} \neq 0$. Alors $\overline{Res(f,g)} = 0 \Leftrightarrow Res(\bar{f},\bar{g}) = 0$.*

Démonstration 1.106 *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 $Sylv(\bar{f},\bar{g}) = \bar{f}I_n$. Donc $\overline{Res(f,g)}$

et $Res(\bar{f},\bar{g})$ *sont non nuls et l'équivalence est vérifiée. Supposons alors que le degré de* f *est* ≥ 1. *Si* $\bar{g}=0$ *alors* $Res(\bar{f},\bar{g})=0$ *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 2

Produit composé de polynômes à coefficients dans un corps fini

Dans ce chapitre, nous définissons le produit composé $\diamond$, appelé aussi produit losange, de deux polynômes à coefficients dans $\mathbb{F}_q$ et ses propriétés. Nous exposons une démonstration détaillée d'un théorème établi par Brawley et Carlitz [5] sur le produit composé de deux polynômes irréductibles. Ce résultat nous permet de construire des polynômes irréductibles à partir d'autres polynômes irréductibles.
À la fin du chapitre, nous donnons un algorithme qui permet de calculer ce produit.

1 Le produit losange $\diamond$ et ses propriétés

Soit Ω la clôture algébrique de $\mathbb{F}_q$. Soit G un sous-ensemble non vide de Ω. Soit σ l'automorphisme de Frobenius de Ω tel que $\sigma(x) = x^q, \forall x \in \Omega$. On supposera que G vérifie les deux conditions suivantes :

1. G est σ invariant, c'est-à-dire : $\forall \alpha \in G, \sigma(\alpha) \in G$.
2. G est muni d'une loi de composition interne $\diamond$ telle que :

$$\forall \alpha, \beta \in G, \sigma(\alpha \diamond \beta) = \sigma(\alpha) \diamond \sigma(\beta) \in G.$$

Exemples 2.1 *1.* $G = \Omega \setminus \{0\}$, $\alpha \diamond \beta = \alpha\beta$.

2. $G = \Omega$, $\alpha \diamond \beta = \alpha + \beta - c$, *où* $c \in \mathbb{F}_q$.

3. $G = \Omega \setminus \{1\}$, $\alpha \diamond \beta = \alpha + \beta - \alpha\beta$.

4. G : *Un sous-ensemble* $\sigma-$*invariant de* Ω, $\alpha \diamond \beta = f(\alpha, \beta)$, *où* $f(x, y) \in \mathbb{F}_q[x, y]$ *est un polynôme fixé de* $\mathbb{F}_q$ *tel que* $f(\alpha, \beta) \in G$, $\forall \alpha, \beta \in G$.

Remarquons que l'exemple 4 généralise les trois autres exemples. De plus, $(G, \diamond)$ est un groupe abélien dans les exemples 1, 2 et 3. Le théorème suivant a été introduit et démontré dans [7].

Théorème 2.2 *Soit G un sous-ensemble fini de Ω vérifiant les conditions précédentes. 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 2.3 *Soit $G = \{\alpha_1, \alpha_2, ..., \alpha_t\}$ un ensemble de cardinal t. D'après l'interpolation de Lagrange*

$$h(x,y) = \sum_{1 \leq i,j \leq t} \Big(\alpha_i \diamond \alpha_j\Big) \frac{S_i(x)}{W_i} \frac{S_j(y)}{W_j}, \tag{2.1}$$

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

$$h(\alpha,\beta) = \alpha \diamond \beta, \forall \alpha, \beta \in G. \tag{2.2}$$

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

$$(h(x,y))^q = h(x^q, y^q). \tag{2.3}$$

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 $h(x,y)$.

Théorème 2.4 *Soit $h(x,y) \in \mathbb{F}_q[x,y]$. Pour tout sous-ensemble S non vide de Ω, il existe un plus petit sous-ensemble G (au sens de l'inclusion) de Ω 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 2.5 *Voir [7], page 4.*

Notons $M_G[q, x]$, 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. Il est clair que si $f, g \in M_G[q, x]$, le produit $fg \in M_G[q, x]$.
Soient $f, g \in M_G[q, x]$. On définit sur $M_G[q, x]$ une loi de composition interne appelée produit composé et notée $\diamond$ comme suit

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

où α et β sont les racines respectives de f et g dans G et $\alpha \diamond \beta = h(\alpha, \beta) \in G$, $\forall \alpha, \beta \in G$, où $h(x, y) \in \mathbb{F}_q[x, y]$ est un polynôme fixé.
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 $h = f \diamond g$, alors

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

donc $h \in \mathbb{F}_q$.
Si la loi $\diamond$ est associative (respectivement commutative) dans G, alors la loi $\diamond$ est associative (respectivement commutative) dans $M_G[q, x]$.
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 $M_G[q, x]$.

2 Exemples de lois composées induites par le produit losange

Soient f et g deux polynômes de $\mathbb{F}_q[x]$, dont les factorisations dans $\Omega[x]$ 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 2.6 *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 2.7 *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 2.8 *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 2.9 *1. On a*

$$f * f = \prod_{\alpha_i\in A}\prod_{\alpha_j\in A}\Big(x-(\alpha_i+\alpha_j)\Big) = \prod_{\alpha_i=\alpha_j}\Big(x-2\alpha_i\Big)\prod_{\alpha_i\neq\alpha_j}\Big(x-(\alpha_i+\alpha_j\Big) \quad (2.4)$$

Donc,

$$f \star f = \prod_{i=1}^{n}(x-2\alpha_i)\prod_{i<j}\Big(x-(\alpha_i+\alpha_j)\Big)^2. \quad (2.5)$$

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

$$r_1 r_2 = x^2 - (\alpha_1 - \alpha_2)^2, \tag{2.6}$$

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 2.10 *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 2.11 *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 2.12 *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. $f \oslash g = Res_y\Big(g(y), f(x/y)\Big)$.

Démonstration 2.13 *Voir chapitre 01, théorème 1.103.*

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

Définition 2.14 *Soit $h \in M_G[q, x]$ 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 $M_G[q, x]$, de degrés > 1 tels que $h = f \diamond g$. Sinon, h est dit **indécomposable**.*

Remarque 2.15 *Il ne faut pas confondre le mot "indécomposable" et "irréductible". L'irréductibilité est par rapport à la multiplication usuelle. Donc un polynôme irréductible peut être décomposable.*

Soit $I_G[q, x]$ le sous-ensemble de $M_G[q, x]$ des polynômes irréductibles sur $\mathbb{F}_q$. Le théorème suivant, établi par Brawley et Carlitz [5], nous donne une condition nécessaire et suffisante pour que le produit $f \diamond g$ soit irréductible.

Théorème 2.16 *Soit $f, g \in M_G[q, x]$ tels que $\deg f = m$ et $\deg g = n$. Alors, le produit $f \diamond g$ est irréductible sur $\mathbb{F}_q$ si, et seulement si, $f, g \in I_G[q, x]$ et $pgcd(n, m) = 1$.*

Démonstration 2.17 *Supposons que $f \diamond g$ est irréductible. Alors, f et g sont nécessairement irréductibles car on a : $\forall f, g, h \in M_G[q, x]$*

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

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 mn, le

plus petit entier positif k tel que $\gamma^{q^k} = \gamma$ est $k = mn$.
On a donc :

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

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

$$\alpha^{q^{td}} \diamond \beta^{q^{td}} = \alpha \diamond \beta, \forall t \in \mathbb{N}^*. \tag{2.7}$$

Pour $t = m$, on a

$$\alpha \diamond \beta^{q^{md}} = \alpha \diamond \beta. \tag{2.8}$$

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

$$\alpha^{q^{nd}} \diamond \beta^{q^{nd}} = \alpha^{q^{nd}} \diamond \beta = \alpha \diamond \beta. \tag{2.9}$$

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 $d = mn$.

Une autre démonstration a été proposée par Munemasa et Nakamura dans [18]. Leur méthode repose sur la notion "d'annulation faible", c'est-à-dire, le produit $\diamond$ peut être non associatif. Pour plus de détails, voir [18], section 2.

3 Polynômes irréductibles et multiplication composée

On pose $G = \Omega^*$ et $M_G[q, x]$ muni de la loi $\circ$. Soient f et g deux polynômes de $M_G[q, x]$. Rappelons que

$$f \circ g = \prod_{\alpha} \prod_{\beta} \Big(x - (\alpha\beta)\Big), \tag{2.10}$$

où α , β sont les racines respectives de f et g dans G.
Soit $h \in M_G[q,x]$ tel que h n'est pas une unité. On dit que h est multiplicativement décomposable si $h = f \circ g$, où f et $g \in M_G[q,x]$ et $deg(f) > 1$, $deg(g) > 1$.
Dans [5], Brawley et Carlitz ont établi un théorème pour montrer l'unicité de la décomposition multiplicative pour les polynômes dans $I_G[q,x]$.

Par exemple, pour montrer que la décomposition multiplicative d'un polynôme unitaire de $\mathbb{F}_q[x]$ n'est pas nécessairement unique. Considérons le polynôme $f(x) = x^6 + x^3 + 1 \in \mathbb{F}_2[x]$, qui est irréductible sur $\mathbb{F}_2$ et soient

$$\begin{aligned} g_1(x) &= x^4 + x + 1, \\ g_2(x) &= x^4 + x^3 + 1, \\ g_3(x) &= x^4 + x^3 + x^2 + x + 1, \end{aligned}$$

alors

$$f \circ g_1 = f \circ g_2 = f \circ g_3 = (x^{12} + x^3 + 1)(x^{12} + x^9 + 1), \tag{2.11}$$

d'où le corollaire suivant :

Corollaire 2.18 *La décomposition multiplicative des éléments de $M_G[2,x]$, où G est le groupe multiplicatif de Ω, n'est pas unique.*

Démonstration 2.19 *D'après la relation (2.11), le polynôme réductible $x^{24}+x^{21}+x^{15}+x^{12}+x^9+x^3+1$ admet trois décompositions multiplicatives différentes.*

Théorème 2.20 *Soit G le groupe multiplicatif de Ω. Soit $f \in M_G[q,x]$ un polynôme irréductible de degré $n \geq 1$. Si f est multiplicativement décomposable dans $M_G[q,x]$ comme suit :*

$$f = f_1 \circ f_2 \circ \cdots \circ f_t = g_1 \circ \cdots \circ g_t, \tag{2.12}$$

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 2.21 *1 et 2 sont vérifiés d'après le théorème* 2.16.
Montrons 3. Soit $\alpha_i \in \mathbb{F}_{q^{n_i}}$, une racine de f_i , $1 \leq i \leq t$. D'après 2.12, g admet des racines $\beta_i \in \mathbb{F}_{q^{n_i}}$ telles que :

$$\alpha_1 \alpha_2 \ldots \alpha_t = \beta_1 \beta_2 \ldots \beta_t, \tag{2.13}$$

donc, on a :

$$\frac{\alpha_1}{\beta_1} = \frac{\beta_2}{\alpha_2} \cdots \frac{\beta_t}{\alpha_t}, \tag{2.14}$$

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 2.20, nous n'avons pas supposé l'indécomposabilté des facteurs irréductibles du polynôme f. Cependant, nous avons supposé l'égalité des degrés. Prenons par exemple le polynôme dans $M_G[2, x]$ suivant :

$$(x^6 + x^4 + x^2 + x + 1) \circ (x^5 + x^2 + 1) = (x^3 + x + 1) \circ (x^{10} + x^5 + x^4 + x^2 + 1) \tag{2.15}$$

Il est clair que les degrés des facteurs ne satisfont pas la condition du théorème 2.20. 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.
Dans ce qui suit, $d(\alpha)$ désigne le degré du nombre algébrique α.

Lemme 2.22 *Soit* α, β, γ *et* $\sigma \in \Omega$ *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* $\sigma_i \in \Omega, i = 1, 2$, *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 2.23 *Voir [5], pages 126-127.*

Théorème 2.24 *Soit $f \in \mathbb{F}_q[x]$, un polynôme irréductible de degré $n > 1$. Supposons que f est multiplicativement décomposable comme suit*

$$f = f_1 \circ f_2 \circ \cdots \circ f_t = g_1 \circ g_2 \circ ... \circ g_s, \tag{2.16}$$

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 2.25 *Posons $\deg(f_i) = n_i$ et $\deg(g_i) = m_i$ tels que : $n = \prod_{i=1}^{t} n_i = \prod_{i=1}^{s} m_i$ où les n_i (respectivement m_i) sont premiers entre eux deux à deux.*
Supposons, sans restreindre 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,

$$f' \circ F = g' \circ G, \tag{2.17}$$

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 :

$$\alpha\beta = \gamma\sigma, \tag{2.18}$$

car $\alpha\beta$ est une racine de $f' \circ F$ et $\gamma\sigma$ est une racine de $g' \circ G$. De plus, la relation [2.17] 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 2.22, $\alpha = \alpha_1\alpha_2$ 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 2.20 sont vérifiées et on en déduit que f_i et g_i sont associés.

3.1 Multiplication composée et polynômes cyclotomiques

Soit K un corps commutatif de caractéristique p où p est un nombre premier. Soit $n \in \mathbb{N}^*$ tel que $p \nmid n$.

Définition 2.26 *Le polynôme*

$$\Phi_n(x) = \prod_{\substack{i=1 \\ pgcd(i,n)=1}}^{n} \Big(x - \xi_n^i\Big), \tag{2.19}$$

où ξ_n est une racine primitive n-ième de l'unité, est appelé le n-ième polynôme cyclotomique sur K.

Remarquons que Φ_n est de degré $\varphi(n)$, où $\varphi(n)$ est la fonction d'Euler définie par : $\varphi(n) = \sum_{\substack{i=1 \\ pgcd(i,n)=1}}^{n} 1$.

Voir [14] (Chapitre 2, pages 63-66) pour plus de propriétés.

Dans le suite de cette section, on note $K = \mathbb{F}_q$ avec q une puissance d'un nombre premier. Le théorème suivant montre qu'un polynôme cyclotomique est le produit composé d'autres polynômes cyclotomiques.

Théorème 2.27 *Soit $n = p_1^{e_1} \dots p_s^{e_s}$, $n \in \mathbb{N}$. Soit*

$$\begin{aligned} \Phi_{p_1^{e_1}} &= \prod_i f_{1_i} \\ \Phi_{p_2^{e_2}} &= \prod_j f_{2_j} \\ &\vdots \\ \Phi_{p_s^{e_s}} &= \prod_k f_{s_k} \end{aligned}$$

les factorisations des Φ_i , $i \in \{p_1^{e_1}, \dots, p_s^{e_s}\}$, dans $\mathbb{F}_q[x]$. Alors

$$\begin{aligned} \Phi_n &= \Phi_{p_1^{e_1}} \circ \Phi_{p_2^{e_2}} \circ \cdots \circ \Phi_{p_s^{e_s}} \\ &= \prod_i \prod_j \cdots \prod_k \Big(f_{1_i} \circ f_{2_j} \circ \cdots \circ f_{s_k}\Big). \end{aligned} \tag{2.20}$$

De plus, si les ordres multiplicatifs de q modulo chacun des $p_i^{e_i}$ sont deux à deux premiers entre eux, alors 2.20 est la factorisation complète de Φ_n.

Démonstration 2.28 *Posons* $F = \Phi_{p_1^{e_1}} \circ \Phi_{p_2^{e_2}} \circ \cdots \circ \Phi_{p_s^{e_s}}$. *En utilisant la définition de la multiplication composée, on obtient :*

$$F = \prod_{\xi_{p_1^{e_1}}} \cdots \prod_{\xi_{p_s^{e_s}}} \Big(x - \xi_{p_1{}^{e_1}} \ldots \xi_{p_s{}^{e_s}}\Big), \tag{2.21}$$

où le produit parcourt toutes les racines primitives $p_i^{e_i}$*-ième de l'unité. Il est clair que* $\xi_{p_1^{e_1}} \ldots \xi_{p_s^{e_s}}$ *est une racine de* Φ_n.
En effet, comme $ord(\xi_{p_i^{e_i}}) = p_i^{e_i}$ *et les* p_i *sont deux à deux premiers entre eux, donc*

$$ord(\xi_{p_1^{e_1}} \ldots \xi_{p_s^{e_s}}) = p_1^{e_1} \ldots p_s^{e_s} = n.$$

Alors, $\xi_{p_1^{e_1}} \ldots \xi_{p_s^{e_s}}$ *est une racine primitive n-ième de l'unité, donc une racine de* Φ_n.
De plus, F *et* Φ *sont unitaires et*

$$\deg(F) = \prod_{i=1}^{s} \varphi(p_i^{e_i}) = \varphi(\prod_{i=1}^{s} p_i^{e_i}) = \varphi(n) = \deg(\Phi_n).$$

Rappelons que les racines d'un polynôme cyclotomique sont toutes distinctes. Si on montre que les racines de F *sont distinctes alors* $F = \Phi$. *Posons* $\xi_i = \xi_{p_i^{e_i}}$ *et montrons que les racines de* F *sont distinctes.*
On suppose que F *a deux racines égales, c'est à dire :*

$$\xi_{p_1^{e_1}}^{i_1} \ldots \xi_{p_s^{e_s}}^{i_s} = \xi_{p_1^{e_1}}^{j_1} \ldots \xi_{p_s^{e_s}}^{j_s} \tag{2.22}$$

$$\begin{aligned} \xi_1^{i_1} \ldots \xi_s^{i_s} &= \xi_1^{j_1} \ldots \xi_s^{j_s}, \\ \xi_1^{j_s - i_s} &= \xi_1^{i_1 - j_1} \ldots \xi_s^{i_{s-1} - j_{s-1}}, \\ ord(\xi_s^{j_s - i_s}) &= ord(\xi_1^{i_1 - j_1} \ldots \xi_s^{i_{s-1} - j_{s-1}}), \end{aligned}$$

ainsi, $ord(\xi_s^{j_s - i_s}) \mid p_1^{e_1} \ldots p_{s-1}^{e_{s-1}}$ *et* $ord(\xi_s^{j_s - i_s}) \mid p_s^{e_s}$, *donc*

$$pgcd(p_1^{e_1} \ldots p_{s-1}^{e_{s-1}}, p_s^{e_s}) = 1 \Rightarrow \xi_s^{j_s - i_s} = 1,$$

et comme $p_s^{e_s} > 1$ *et* $0 < i_s\ ,\ j_s < p_s^{e_s}$, *alors* $i_s = j_s$.
Par récurrence, on montre que $i_k = j_k\ ,\ 1 \leq k \leq s$, *d'où* $\Phi_n = F$.
D'après l'associativité de $\circ$ *et le fait que* $\prod f \circ g = \prod f \circ \prod g$ *et en appliquant le théorème 3.1, on en déduit facilement que les facteurs de 2.20 sont irréductibles.*

Exemple 2.29 *Soit $\mathbb{F}_{11}$ le corps à 11 éléments. Pour $n = 595 = 5 \times 7 \times 17$*
On a : $ord_5(11) = 1$, $ord_7(11) = 3$ et $ord_{17}(11) = 16$. Les ordres sont deux à deux premiers entre eux. D'après le théorème 2.27, on a

$$\Phi_{595} = \prod_i \prod_j \prod_k \Big(f_i \circ g_j \circ h_k \Big) \tag{2.23}$$

où f_i, g_j et h_k sont les facteurs irréductibles de Φ_5, Φ_7 et Φ_{17} respectivement.

Corollaire 2.30 *Soit $m, n \in \mathbb{N}$ tel que $pgcd(m, n) = 1$.*
Alors

$$\Phi_{mn} = \Phi_m \circ \Phi_n \tag{2.24}$$

De plus, soient $\Phi_m = \prod f_i$, $\Phi_n = \prod g_i$, leurs factorisations respectives sur $\mathbb{F}_q$, alors

$$\Phi_{mn} = \prod_i \prod_j f_i \circ g_j, \tag{2.25}$$

et si le $pgcd\Big(ord_m(q), ord_n(q)\Big) = 1$ alors la relation [2.25] est la factorisation complète de Φ_{mn} sur $\mathbb{F}_q$.

Tuxanidy et Wang [23] ont introduit plusieurs décompositions multiplicatives des polynômes cyclotomiques de différents degrés. Par exemple, si r est un entier impair, on a

$$\Phi_{2^n r} = \Phi_{2^n} \circ \Phi_r. \tag{2.26}$$

Donc, si les factorisations de Φ_m et Φ_n sont connues telles que $\Phi_m = \prod f_i$, $\Phi_n = \prod g_i$ et si

$$pgcd(m, n) = pgcd(ord_m(q), ord_n(q)) = 1,$$

on pourrait obtenir tous les facteurs irréductibles de Φ_{mn} en calculant $f_i \circ g_j$.
Cette méthode a été utilisée afin d'obtenir certaines factorisations des polynômes cyclotomiques. Par exemple, le théorème 3.3 dans [23] donne une factorisation de Φ_{mn} avec q une racine primitive mod (m) et

$$pgcd(m, n) = pgcd(\varphi(m), ord_m(q)) = 1.$$

Pour plus de détails, voir [23].

3.2 Un critère de décomposition multiplicative

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

Théorème 2.31 *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 2.32 *Voir [5], page 125.*

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

Corollaire 2.33 *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 comme $f \circ g$ 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 2.34

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 $\mathbb{F}_3[x]$, $E = \{7, 28, 52, 56, 91, 104, 182, 364, 728\}$ l'ensemble des ordres des polynômes irréductibles sur $\mathbb{F}_3$ de degré 6. Donc les polynômes irréductibles 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 $\Big(\varphi(52) + \varphi(104)\Big)/6 = 12$.*

4 Polynômes irréductibles et addition composée

Soit G le groupe additif Ω et $M_G[q,x]$ muni de la loi $*$. Soient f et g deux polynômes de $M_G[q,x]$. Rappelons que l'addition composée de f et g est définie comme suit :

$$f * g = \prod_{\alpha} \prod_{\beta} \Big(x - (\alpha + \beta)\Big), \tag{2.27}$$

où α, β sont les racines respectives de f et g dans G.
Soit $h \in M_G[q,x]$ tel que h n'est pas inversible. On dit que h est additivement décomposable si $h = f * g$, où f et $g \in M_G[q,x]$ et $deg(f) > 1$, $deg(g) > 1$.

Lemme 2.35 *Si le pgcd$(m,n)=1$ et $\alpha \in \mathbb{F}_{q^n}$ et $\beta \in \mathbb{F}_{q^m}$ alors*

$$\prod_{\alpha}\prod_{\beta}\Big(x-(\alpha+\beta)\Big)=\Big[(x^q-x)\otimes t_m\otimes t_n\Big]^q, \tag{2.28}$$

où $t_m(x)=x+x^q+\cdots+x^{q^{m-1}}$ et le produit symbolique $\otimes$ est défini par $(f(x)\otimes g(x))=f(g(x))$.

Démonstration 2.36 *Voir [5], page 130.*

Définition 2.37 *Soit $\gamma \in \Omega$ tel que $d(\gamma)>1$. L'élément γ est dit additivement indécomposable s 'il ne peut pas s'écrire sous la forme $\gamma=\alpha+\beta$, où $d(\alpha)>1$, $d(\beta)>1$ et $d(\gamma)=d(\alpha)d(\beta)$.*

Lemme 2.38 *Soit $\gamma \in \Omega$ avec $d(\gamma)=mn$ et pgcd$(n,m)=1$. Alors $\gamma=\alpha+\beta$, où $d(\alpha)=m$ et $d(\beta)=n$ si, et seulement si, γ est une racine du polynôme*

$$\Big(x^q-x\Big)\otimes t_m(x)\otimes t_n(x). \tag{2.29}$$

Démonstration 2.39 *Voir [5], page 131.*

Théorème 2.40 *Soit $\gamma \in \Omega \setminus \mathbb{F}_q$, γ peut s'écrire sous la forme $\gamma=\alpha_1+\cdots+\alpha_t$, où $n=d(\gamma)$, $n_i=d(\alpha_i)>1$, $n=n_1n_2\ldots n_t$, les (n_i) premiers entre eux deux à deux et les α_i additivement indécomposables. De plus, si $\gamma=\beta_1+\cdots+\beta_s$ est une autre décomposition, alors en réordonnant les β_i, on a $\beta_i=\alpha_i+c_i$,$c_i \in \mathbb{F}_q$ et $\sum c_i=0$.*

4.1 Un critère de décomposition additive

Soit $L \in \mathbb{F}_q[x]$. On dit que L est un q-polynômes si L s'écrit sous la forme $L=\sum a_i x^{q^i}$ avec $a_i \in \mathbb{F}_q$. Le polynôme L est aussi appelé polynôme linéarisé. On appelle associé ordinaire à L le polynôme $l=\sum a_i x^i$. On dit que L_1 divise symboliquement L_2 s'il existe un q-polynôme L tel que $L_1 \otimes L=L_2$. On écrit $L_1 \parallel L_2$ et on note le quotient symbolique $L=L_2//L_1$. On dit qu'un polynôme $f \in \mathbb{F}_q[x]$ appartient à un polynôme linéarisé L si, et seulement si, L est le polynôme linéarisé de plus petit degré divisible par f. Dans ce cas L est unique. On peut donc énoncer le théorème suivant :

Théorème 2.41 *Soit $h \in \mathbb{F}_q[x]$, un polynôme unitaire irréductible de degré nm tel que pgcd$(n,m)=1$. Soit L le polynôme linéarisé auquel appartient h , l le polynôme ordinaire associé à L. Alors, les propriétés suivantes sont équivalentes :*

1. *h est additivement décomposable tel que $h = f * g$ avec* $\deg f = n$ *et* $\deg g = m$.
2. $L \mid (x^{q^n} - 1) \otimes (x^{q^m} - 1)//(x^q - x)$.
3. $L \parallel (x^{q^n} - 1) \otimes (x^{q^m} - 1)//(x^q - x)$.
4. $l \mid (x^n - 1)(x^m - 1)/(x - 1)$.

Démonstration 2.42 *Voir [6], page 63.*

Le théorème 2.41 nous permet de tester si un polynôme irréductible est additivement décomposable. Le résultat suivant nous donne une formule pour évaluer le nombre de polynômes irréductibles, additivement décomposables dans $\mathbb{F}_q[x]$.

Théorème 2.43 *Soit $n > 1$ et $m > 1$ tels que : $pgcd(n, m) = 1$. Le nombre de polynômes unitaires irréductibles, de degré nm, décomposables sous la forme $f * g$, avec* $\deg f = n$ *et* $\deg g = m$, *est donné par : $\sum_{l}(\Phi(l)/nm)$ où la somme parcourt tous les polynômes l d'ordres nm qui divisent $(x^n - 1)(x^m - 1)/(x - 1)$, $\Phi(l)$ étant le nombre de polynômes unitaires de degrés $< deg(l)$, premiers à l.*

Démonstration 2.44 *Voir [6], pages 63-64 .*

Exemples 2.45

1. *Soit $h = x^6 + x^5 + x^3 + x^2 + 1 \in \mathbb{F}_2[x]$. Le polynôme h appartient au polynôme linéarisé $L = x^{16} + x^8 + x^2 + x$. Le polynôme ordinaire associé à L est $l = x^4 + x^3 + x + 1$. Soit $Q = (x^2 - 1)(x^3 - 1)/(x - 1) = x^4 + x^3 + x + 1$. Il est clair que : $l \mid Q$. D'après le théorème 2.41 , h est additivement décomposable.*
2. *Calculons le nombre de polynômes irréductibles de degré 12, additivement décomposables dans $\mathbb{F}_2[x]$. $x^{12} - 1 = (x+1)^4(x^2+x+1)^4$. Soit $D = (x^3-1)(x^4-1)/(x-1)$. Les diviseurs de D, d'ordre 12 sont : $l_1 = (x+1)^3(x^2+x+1)$ et $l_2 = (x+1)^4(x^2+x+1)$. Alors, le nombre de polynômes décomposables est : $\frac{\Phi(l_1)+\Phi(l_2)}{12} = \frac{12+24}{12} = 3$. Donc, il existe trois polynômes irréductibles, additivement décomposables, de degré 12.*

4.2 Algorithme pour f ⋄ g

Dans cette section, on présente un algorithme qui calcule le produit composé $f \diamond g$ de deux polynômes irréductibles de $I_G[q, x]$. Cet algorithme prend en entrée deux polynômes irréductibles f et g de degrés respectifs m et n, et calcul le polynôme $h \in \mathbb{F}_q[x, y]; h = f \diamond g$. On construit tout d'abord l'anneau quotient $A = \mathbb{F}_q[x, y]/\langle f(x), g(y)\rangle$, où $\langle f(x), g(y)\rangle$ est l'idéal engendré par f et g. A contient

les racines de $f(x)$ et $g(y)$ et $\mathbb{F}_q[x,y]/\langle f,g\rangle \cong \mathbb{F}_{q^{mn}}$. Ensuite, on calcule $u_i \equiv x^{q^i} mod\ f(x)$ avec $0 \leq i \leq m-1$ et $v_j \equiv y^{q^j} mod\ g(y)$ avec $0 \leq j \leq n-1$. Après, dans l'anneau $\mathbb{F}_q[x,y]/\langle f,g\rangle$, on calcule $h_{ij} = h(u_i, v_j)$ avec $0 \leq i \leq m-1$ et $0 \leq j \leq n-1$. La dernière étape est de calculer dans $A[z]$, le produit $\prod_{i=0}^{n-1}\prod_{j=0}^{m-1}\Big(z - h_{ij}\Big)$.

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 évalue et affiche $\prod_{i=0}^{n-1}\prod_{j=0}^{m-1}\Big(z - h_{ij}\Big)$.

Fin

L'algorithme 4.2 a été introduit par Brawley et al. dans [7]. Ils proposent différentes méthodes pour calculer $f * g$ et $f \circ g$ et comparent leurs complexités. D'autres algorithmes basés sur la relation entre les produits composés et les résultants peuvent être trouvés dans [3]. Ces algorithmes calculent efficacement les produits $f * g$ et $f \circ g$ dans $\mathbb{F}_q[x]$. L'algorithme le plus rapide a été introduit par Bostan et al. [3]. Leur algorithme a la meilleure complexité dans toutes les caractéristiques.

Chapitre 3

Décomposition additive sur un anneau factoriel

1 Introduction

Soit $f, g \in \mathbb{F}_q[x]$. Nous rappelons que

$$f * g = \prod_{\alpha} \prod_{\beta} (x - (\alpha + \beta)),$$

où α et β sont les racines respectives de f et g dans une clôture algébrique de $\mathbb{F}_q$ et $*$ une loi de composition interne sur l'ensemble des polynômes unitaires à coefficients dans $\mathbb{F}_q$ de degré ≥ 1. Un polynôme $h \in \mathbb{F}_q[x]$ de degré ≥ 1 est dit additivement décomposable si $h = f * g$, où $f, g \in \mathbb{F}_q[x]$ et $\deg(f) > 1$, $\deg(g) > 1$. La décomposition additive des polynômes dans $\mathbb{F}_q[x]$ a été intensivement étudiée par Brawely et Carlitz qui ont montré l'unicité de la dcomposition additive pour les polynômes unitaires irréductibles. En particulier, ils ont montré le résultat suivant :

Théorème 3.1 *Soient f et g deux polyômes à coefficients dans $\mathbb{F}_q$ tels que $deg(f) = n > 1$ et $deg(g) = m > 1$. Alors, $f * g$ est irréductible si, et seulement si, f et g sont irréductibles et $pgcd(m, n) = 1$.*

Dans ce chapitre, nous faisons une étude analogue à celle de Brawely et Carlitz sur un anneau commutatif et en particulier sur un anneau intègre et plus généralement sur un anneau factoriel. Nous donnons les résultats obtenus dans l'article [**?**].

2 Groupe des unités de $(R[x], *)$

Dans ce qui suit, une unité de $(R[x], *)$ est un élément de $R[x]$ qui admet un symétrique pour la loi $*$.
Soit $f(x) = a_m \prod_{i=1}^{m}(x - \alpha_i)$ et $g(x) = b_n \prod_{i=1}^{n}(x - \beta_i)$ deux polynômes sur un anneau commutatif intègre R, où $\alpha_1, ..., \alpha_m$ et $\beta_1, ..., \beta_n$ sont les racines du polynôme f et $g$respectivement dans une clôture algébrique du corps des fractions de R. Rappelons le résultant de f et g en x :

$$Res_x(f, g) = a_m^n \prod_{i=1}^{m} g(\alpha_i) = (-1)^{mn} b_n^m \prod_{j=1}^{n} f(\beta_j), \tag{3.1}$$

où $Res_x(f, g) \in R$ et $Res_x(f, g) = 0$ si f et g ont une racine commune.
Avant de définir l'addition composée sur un anneau commutatif R, commençons par le cas où R est un corps fini.
Soit $h \in \mathbb{F}_q[x]$, un polynôme unitaire qui est additivement décomposable, c'est à dire,

$$h = f * g.$$

Soient $\alpha_1, ..., \alpha_m$ et $\beta_1, ..., \beta_n$ les racines du polynôme f et g respectivement dans une clôture algébrique de $\mathbb{F}_q$. Remarquons que

$$\begin{aligned}(-1)^m f(x - t) &= (-1)^m (x - t - \alpha_1)...(x - t - \alpha_m) \\ &= (t - x + \alpha_1)...(t - x + \alpha_m) \\ &= (t - (x - \alpha_1))...(t - (x - \alpha_m)) \\ &= \prod_{i=1}^{m}(t - (x - \alpha_i)).\end{aligned}$$

On déduit alors que $f * g$ est lié au résultant de f et g comme suit

$$\begin{aligned}f * g &= \prod_{i=1}^{m}\prod_{j=1}^{n}(x - (\alpha_i + \beta_j)) \\ &= \prod_{i=1}^{m}\prod_{j=1}^{n}\Big((x - \alpha_i) - \beta_j\Big) \\ &= Res_t\Big((-1)^m f(x - t), g(t)\Big).\end{aligned}$$

Comme on peut calculer le résultant de deux polynômes sur un anneau commutatif, l'expression $Res_t\Big((-1)^m f(x-t), g(t)\Big)$ nous permet de définir la composition additive

de deux polynômes (pas nécessairement unitaires) sur un anneau commutatif R. Soit $h \in R[x]$. On dit que h est additivement décomposable sur R si on peut écrire $h = f * g$ où f et g sont deux polynômes de $R[x]$ qui ne sont pas des unités par rapport à la loi $*$. Dans ce cas, f et g sont appelés les facteurs de la décomposition additive de h.

Théorème 3.2 *Soit R un anneau commutatif. Le groupe des unités de $(R[x], *)$ est égal à*

$$\mathcal{U} = \{ax + b : a, b \in R, a \text{ est une unité de } R\}. \tag{3.2}$$

Démonstration 3.3 *Montrons que $\mathcal{U}$ est un groupe. En effet, posons $u(x) = x$, alors pour tout $f \in R[x]$, on a*

$$(f * u)(x) = (u * f)(x) = Res_t\Big((-1)(x-t), f(t)\Big) = Res_t\Big((t-x), f(t)\Big) = f(x).$$

Ainsi, le polynôme x est l'élément neutre qui correspond à la loi $*$.
Si $u \in \mathcal{U}$ et $v \in \mathcal{U}$ est son inverse, alors

$$1 = deg(u * v) = deg(u)deg(v),$$

et cela implique que u et v sont linéaires. Maintenant, on suppose que $u = u_1x + u_2, v = v_1x + v_2 \in R[x]$ avec u_1 et u_2 des unités de R, alors

$$u * v = (u_1v_1)x + (u_1v_2 + u_2v_1) \tag{3.3}$$

est un polynôme linéaire. En outre, si u_1 et v_1 sont des unités dans R alors u_1v_1 est aussi une unité dans R. Donc $*$ est une loi de composition interne sur $\mathcal{U}$. Si v est l'inverse de u, alors

$$u * v = (u_1v_1)x + (u_1v_2 + u_2v_1) = x, \tag{3.4}$$

donc $u_1v_1 = 1$ et $u_1v_2 + u_2v_1 = 0$. En résolvant ces équations, on aura $v_1 = u_1^{-1}$ et $v_2 = -u_2/u_1^2$.
Soient $u = u_1x + u_2, v = v_1x + v_2$ et $w = w_1x + w_2 \in \mathcal{U}$, on a

$$(u * v) * w = \Big(u_1v_1x + u_1v_2 + u_2v_1\Big) * w = (u_1v_1w_1)x + (u_1v_1w_2 + u_2v_2w_1 + u_2v_1w_1)$$

$$= (u_1x + u_2) * \Big((v_1w_1)x + (v_1w_2 + v_2w_1)\Big) = u * (v * w).$$

Donc $*$ est associative.

3 Décomposition additive

On introduit une proposition qui est une conséquence de la définition du résultant de deux polynômes.

Proposition 3.4 *Soit R un anneau intègre et K son corps des fractions. Soient f, g et $h \in R[x]$ avec $f = af_1, g = bg_1$ et $h = ch_1$, où a, b et $c \in R$ et f_1, g_1 et h_1 sont des polynômes unitaires. Alors, $h = f * g$ si, et seulement si, $h_1 = f_1 * g_1$ sur K et $c = a^{\deg(g)}b^{\deg(f)}$.*

Démonstration 3.5 *Soit*

$$f = a\prod_{i=0}^{m}(x - \alpha_i) \text{ et } g = b\prod_{i=0}^{n}(x - \beta_j).$$

Si $h_1 = f_1 * g_1$ et $c = a^n b^m$, alors on peut écrire

$$h = ch_1 = a^n b^m \prod_{i=0}^{m}\prod_{i=0}^{n}\Big(x - (\alpha_i + \beta_j)\Big) = f * g.$$

Réciproquement, si $h = f * g$, alors $h_1 = \prod_{i=0}^{m}\prod_{i=0}^{n}\Big(x - (\alpha_i + \beta_j)\Big) = f_1 * g_1$.

On présente maintenant quelques classes de polynômes qui ne sont pas additivement décomposables.

Théorème 3.6 *Soit R un anneau intègre. Si le coefficient dominant de $h \in R[x]$ est un élément premier p alors h n'est pas additivement décomposable sur R.*

Démonstration 3.7 *Supposons que h est additivement décomposable sur R. Alors, il existe $f, g \in R[x]$ avec $\deg f = m \geq 1$ et $\deg g = n \geq 1$ tels que $p = a^n b^m$, où $a, b \in R$ sont les coefficients dominants de f et g respectivement. Comme R est un anneau intègre et p est premier alors p est irréductible. D'après la proposition précédente, $p = a^n b^m$, donc l'un des deux a^n ou b^m est une unité. Supposons que a^n est une unité dans R, alors $b^m = a^{-n}p$, ce qui implique que $p \mid b^m$, et donc $p \mid b$. Posons $b = p\alpha, \alpha \in R$, on a*

$$a^{-n}p = p^m\alpha^m,$$

alors

$$p^{m-1}\alpha^m a^n = 1,$$

donc $m - 1 = 0$, sinon p^{m-1} serait une unité, ce qui est impossible. D'où, $m = 1$ et a est une unité, alors f est une unité dans $R[x]$ par rapport à $*$. Le même raisonnement si b^m est une unité dans R.

Le théorème précédent peut être modifié pour obtenir un résultat plus général lorsque R est un anneau factoriel.

Théorème 3.8 *Soit R un anneau factoriel et soit $h \in R[x]$ un polynôme de degré supérieur à 1. Si le coefficient dominant de h n'est pas une unité de R et est sans facteur carré alors h n'est pas additivement décomposable sur R.*

Démonstration 3.9 *Soit c le coefficient dominant de h. Supposons que h est additivement décomposable sur R. Donc, il existe $f, g \in R[x]$ avec $\deg f = m \geq 1$ et $\deg g = n \geq 1$ tels que $c = a^n b^m$, où $a, b \in R$ sont les coefficients dominants respectifs de f et g.*
Comme c est un élément sans facteur carré, on peut l'écrire sous la forme

$$c = up_1p_2...p_r,$$

où $p_1, p_2, ..., p_r$ sont des éléments irréductibles de R et u est une unité de R. Alors

$$a^n b^m = up_1p_2...p_r. \tag{3.5}$$

On distingue trois cas :
***Premier Cas**. Si $p_i \mid a, \forall i \in \{1, ..., r\}$, alors $a = \alpha p_1p_2...p_r$, où α est une unité de R.*
Par conséquent,

$$up_1p_2...p_r = \alpha^n(p_1p_2...p_r)^n b^m,$$

d'où

$$(p_1p_2...p_r)(u - \alpha^n(p_1p_2...p_r)^{n-1}b^m) = 0$$

avec $p_1p_2...p_r \neq 0$.
Comme R est un anneau commutatif intègre, il en résulte que $u - \alpha^n(p_1p_2...p_r)^{n-1}b^m = 0$, alors

$$u^{-1}\alpha^n(p_1p_2...p_r)^{n-1}b^m = 1.$$

Si $n = 1$, alors $m \geq 2$ et comme $\deg(h) = mn > 1$, alors $u^{-1}\alpha b^m = 1$ et cela implique que b est inversible et g est une unité de $(R[x], *)$, ce qui est impossible.
Si $n \geq 2$, alors le produit $p_1p_2...p_r$ est inversible, ce qui est aussi impossible.
***Deuxième Cas** Même raisonnement pour $p_i \mid b$, $\forall i \in \{1, ..., r\}$.*
***Troisième Cas** Si $c = up_1p_2...p_r$, où $p_1p_2...p_t \mid a$ et $p_{t+1}...p_r \mid b$, alors a et b peuvent s'écrire comme $a = \alpha p_1p_2...p_t$ et $b = \beta p_{t+1}...p_r$, où α et β sont des unités de R. Alors*

$$p_1...p_r = a^n b^m = \alpha^n(p_1...p_t)^n\beta^m(p_{t+1}...p_r)^m.$$

On a $n \geq 1, m \geq 1, mn > 1$ *et*

$$up_1p_2...p_r = \alpha^n\beta^m(p_1...p_t)(p_{t+1}...p_r)(p_1...p_t)^{n-1}(p_{t+1}...p_r)^{m-1}.$$

Par conséquent,

$$(p_1...p_r)[1 - u^{-1}\alpha^n\beta^m(p_1...p_t)^{n-1}(p_{t+1}...p_r)^{m-1}] = 0,$$

donc

$$u^{-1}\alpha^n\beta^m(p_1...p_t)^{n-1}(p_{t+1}...p_r)^{m-1} = 1$$

1. *Si* $n \geq 2$ *et* $m \geq 2$*, alors les* p_i *sont des unités, ce qui est une contradiction.*
2. *Si* $n = 1$ *et* $m \geq 2$ *alors,* $\forall i \in \{t+1, ..., r\}$*, les* p_i *sont des unités, ce qui est impossible. Même raisonnement pour* $n \geq 2$ *et* $m = 1$*.*

On conclut que $n = 1$ *et* $m = 1$*, mais ce cas est impossible car* $deg(h) > 1$*.*

Soit $\sigma : R \to S$ un homomorphisme d'anneaux intègres R et S. Cet homomorphisme peut être naturellement prolongé en l'homomorphisme $\overline{\sigma} : R[x] \to S[x]$ défini par $c_nx^n + ... + c_0 \to \sigma(c_n)x^n + ... + \sigma(c_0)$. Pour simplifier, on note $\overline{\sigma}$ par σ. Comme $Res_x(f, g)$ est un polynôme en les coefficients de f et g, on a

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

Soit $h = f * g$ et soient $a, b, c \in R$ les coefficients dominants respectifs de f, g et h. Alors $c = a^nb^m$ où $m, n \geq 1$. Si $\deg \sigma(h) = \deg h$ pour un homomorphisme d'anneaux intègres σ, alors $\sigma(a)^n\sigma(b)^m = \sigma(c) \neq 0$ donc $\sigma(a) \neq 0$ et $\sigma(b) \neq 0$.

Théorème 3.10 *Soit* $\sigma : R \to S$ *un homomorphisme d'anneaux intègres et soit* $h \in R[x]$*. Si* $\deg \sigma(h) = \deg(h)$ *et* $h = f * g$ *sur* R *alors* $\sigma(h) = \sigma(f) * \sigma(g)$ *sur* S*.*

Démonstration 3.11 *On prolonge l'homomorphisme* σ *en un homomorphisme de* $R[x, t]$ *dans* $S[x, t]$*. Notons que* $\sigma(t^n) = t^n$ *et* $\sigma((x-t)^n) = (\sigma(x-t))^n = (x-t)^n$ *car* σ *est un homomorphisme qui préserve l'unité. Comme* σ *n'envoie pas les coefficients dominants de* f *et* g *vers* 0*,* σ *fixe les degrés de* $f, g \in R[x, t] = R[x][t]$*. Ainsi*

$$\begin{aligned}
\sigma(h) &= \sigma(f * g) \\
&= \sigma(Res_t((-1)^{\deg f} f(x-t), g(t)) \\
&= Res_t(\sigma((-1)^{\deg f} f(x-t)), \sigma(g(t))) \\
&= Res_t((-1)^{\deg f}\sigma(f)(x-t), \sigma(g)(t)) \\
&= \sigma(f) * \sigma(g)
\end{aligned}$$

Le lemme suivant concernant les polynômes linéaires sera utilisé pour prouver qu'un polynôme peut être décomposé additivement en un nombre fini de facteurs additivement indécomposables.

Lemme 3.12 *Soit R un anneau factoriel et soit $h = ax + b \in R[x]$, où a n'est pas une unité dans R. Alors $h = f_1 * ... * f_r$, où $f_1, ..., f_r \in R[x]$ sont des polynômes linéaires qui ne sont pas additivement décomposables.*

Démonstration 3.13 *Si h n'est pas additivement décomposable alors le résultat est vrai en prenant $f_1 = h$.*
On suppose alors que h est additivement décomposable et on prouve le résultat par récurrence sur le nombre de diviseurs premiers (définis à un associé près) de a.
Si le nombre de diviseurs de a est égal à 1 alors a est premier et le résultat est vrai d'après le théorème 3.8.
Supposons que le résultat est vrai pour un nombre de diviseurs premiers de a inférieur ou égal à $d > 1$ et montrons que le résultat est vrai si a admet $d+1$ diviseurs premiers.
Comme h est additivement décomposable, il existe $f_1, f_2 \in R[x]$ tels que $h = f_1 * f_2$, où aucun des deux polynômes f_1 et f_2 n'est une unité par rapport à $*$. Ainsi, les coefficients dominants de f_1 et f_2 ne sont pas des unités de R. De plus ils divisent le coefficient dominant de h. Donc, le nombre de diviseurs premiers du coefficient dominant de f_1 est inférieur ou égal à d. Idem pour f_2. D'après l'hypothèse de récurrence, on peut écrire $f_1 = g_1 * ... * g_t$ et $f_2 = g_{t+1} * ... * g_r$, où les g_i, $\overline{1, r}$, ne sont pas additivement décomposables. On a par conséquent

$$\deg g_i = 1 \text{ pour tout } g_i, i = \overline{1, r}. \tag{3.6}$$

Théorème 3.14 *Soit R un anneau factoriel et soit $h \in R[x]$ un polynôme qui n'est pas une unité par rapport à $*$. Alors*

$$h = f_1 * ... * f_r,$$

où $f_1, ..., f_r \in R[x]$ ne sont pas additivement décomposables.

Démonstration 3.15 *Le cas où h n'est pas additivement décomposable est trivial, alors on suppose que h est additivement décomposable.*
Par récurrence sur le degré de h.
Si le degré de h est égal à 1 alors le résultat est vrai d'après le théorème 3.12.
Supposons que le théorème est vrai quand $1 < \deg(h) \leq k$ et montrons qu'il est vrai pour $\deg(h) = k + 1$. Comme h est additivement décomposable, alors $h = f_1 * f_2$, où f_1 et f_2 ne sont pas des unités de $R[x]$ pour la loi $*$. On considère deux cas

– *Supposons qu'il existe* f_1, $f_2 \in R[x]$ *tels que* $\deg(f_1) < \deg(h)$ *et* $\deg(f_2) < \deg(h)$. *Par hypothèse, on peut écrire,*

$$f_1 = g_1 * g_2 * ... * g_t$$

et

$$f_2 = g_{t+1} * ... * g_r,$$

où les g_i *ne sont pas additivement décomposables. Alors,* $h = g_1 * ... * g_r$ *et chaque* $g_i, i = \overline{1,r}$, *n'est pas additivement décomposable.*

– *Si* $\deg(f_1) = 1$ *et* $\deg(f_2) = \deg(h)$, *on considère le coefficient dominant de* f_2. *Si le coefficient dominant de* f_2 *est une unité, alors* f_2 *n'est pas additivement décomposable. En appliquant le lemme 3.12 sur* f_1, *on obtient le résultat. Si le coefficient dominant de* f_2 *n'est pas une unité, alors il admet un nombre fini de diviseurs premiers. Le même raisonnement utilisé pour prouver le théorème 3.12 montre que* $f_2 = g_1 * ... * g_t$, *où tous sauf un des* g_i *devrait être linéaire car* f_2 *n'admet pas de facteurs dans la décomposition additive de degré strictement compris entre* 1 *et* $deg(f_2) = deg(h)$. *En appliquant le lemme 3.12 sur* f_1 *et chaque* g_i *on obtient le résultat.*

Notons que pour un polynôme irréductible unitaire h sur un corps fini, il a été démontré dans [5] que deux décompositions additives de h sont équivalentes à une unité près par rapport à $*$, mais ce n'est pas le cas en général, comme on le voit dans l'exemple suivant.

Exemple 3.16 *Soit le polynôme irréductible*

$$h = x^6 + x^5 + x^3 + x^2 + 1 \in \mathbb{F}_2[x].$$

D'après [5], ce polynôme est additivement décomposable comme suit :

$$(x^2 + x + 1) * (x^3 + x + 1)$$

et

$$(x^2 + x + 1) * (x^3 + x^2 + 1).$$

Dans ce cas, on a

$$x^3 + x^2 + 1 = (x^3 + x + 1) * (x + 1).$$

Sur $\mathbb{Z}$, *le polynôme* $h = 36x^4$ *est additivement décomposable sous la forme* $(2x^2) * (3x^2)$ *ou* $(x^2) * (6x^2)$ *; cependant il n'existe pas un polynôme* $ax + b \in \mathbb{Z}[x]$ *tel que* $(x^2)*(ax+b) = (ax+b)^2$ *égal à* $2x^2$ *ou* $3x^2$. *Donc, deux décompositions d'un polynôme réductible non-unitaire sur un anneau* R *ne sont pas nécéssairement équivalentes à une unité près.*

Corollaire 3.17 *Soit $\sigma : R \to S$ un homomorphisme d'anneaux intègres et soit $h \in R[x]$. Si $\deg \sigma(h) = \deg h$ et $\sigma(h)$ n'est pas additivement décomposable sur S, alors $h = f * l$, où $f \in R[x]$ n'est pas additivement décomposable sur R et $l \in R[x]$ est un polynôme linéaire. De plus, si le coefficient dominant de f est une unité dans R alors l est une unité de $R[x]$ par rapport à $*$, donc h n'est pas additivement décomposable.*

Démonstration 3.18 *D'après 3.14, on a*

$$h = f_1 * ... * f_r,$$

où les $f_i \in R[x]$ ne sont pas additivement décomposables sur R. Comme $\sigma(h) = \sigma(f_1) * ... * \sigma(f_r)$ n'est pas additivement décomposable sur S alors un des $\sigma(f_i)$ n'est pas une unité par rapport à $*$. Supposons, sans restreindre à la généralité, que $\sigma(f_2), ..., \sigma(f_r)$ sont des unités par rapport à $*$. Comme $\deg f_i = \deg \sigma(f_i) = 1$ alors les f_i sont des polynômes linéaires pour $i = 2, ..., r$. Posons, $l = f_2 * ... * f_r$, alors $h = f_1 * l$, où f_1 n'est pas additivement décomposable. Si le coefficient dominant de h est une unité dans R, le coefficient dominant de l devrait être une unité de R pour que l soit une unité de $R[x]$ par rapport à $*$. Donc, h n'est pas additivement décomposable.

Soit h un polynôme unitaire irréductible sur $\mathbb{F}_q$ avec $\deg h > 1$. Le théorème 3.1 assure que si $h = f * g$, alors f et g sont irréductibles et $pgcd(\deg f, \deg g) = 1$. La conclusion sur les degrés de f et g n'est pas toujours vraie pour f et g sur un anneau R. Par exemple le polynôme $h = x^4 - 10x^2 + 1 \in \mathbb{Z}[x]$ qui est irréductible sur $\mathbb{Z}$ est décomposable comme suit $(x^2 - 2) * (x^2 - 3)$ sur $\mathbb{Z}$. Les polynômes $f(x) = x^2 - 2$ et $g(x) = x^2 - 3$ sont irréductibles dans $\mathbb{Z}[x]$ et $pgcd(\deg f, \deg g) \neq 1$.

Théorème 3.19 *Soit R un anneau intègre et $h \in R[x]$. On suppose que $h = f * g$ est additivement décomposable. Alors, si h est un polynôme irréductible sur R, les polynômes f et g sont irréductibles sur R.*

Démonstration 3.20 *Par contraposée, on montre que si f ou g est réductible sur R alors h est réductible sur R. Supposons que g est réductibe sur R. Alors, il existe $g_1, g_2 \in R[x]$ tels que $g = g_1 g_2$. Donc, d'après la propriété multiplicative du résultant, on a*

$$\begin{aligned} h = f * g &= Res_t((-1)^{\deg f} f(x-t), g_1(t)g_2(t)) \\ &= Res_t((-1)^{\deg f} f(x-t), g_1(t)) Res_t((-1)^{\deg f} f(x-t), g_2(t)) \\ &= (f * g_1)(f * g_2). \end{aligned}$$

Par conséquent, h est réductible sur R.

En général, la réciproque n'est pas vraie. On a

$$(x^2+1)*(x^2+1) = x^2(x^2+4) \text{ sur } \mathbb{Z}.$$

Soit R un anneau factoriel et $f(x) = \sum_{i=0}^{m} a_i x^i \in R[x]$. Rappelons que le contenu de f est défini par

$$Cont(f) = pgcd(a_0, ..., a_m).$$

Si $Cont(f) = 1$, on dit que f est primitif. Le théorème suivant donne une condition nécessaire pour que les facteurs de la décomposition additive d'un polynôme soient primitifs.

Théorème 3.21 *Soit R un anneau factoriel et soit $h \in R[x]$. Supposons que $h = f * g$ est additivement décomposable, où $f(x) = \sum_{i=0}^{m} f_i x^i \in R[x]$ et $g(x) = \sum_{i=0}^{n} g_i x^i \in R[x]$, tels que $\deg(f) = m$ et $\deg(g) = n$. De plus, supposons que $pgcd(Cont(g), f_m) = 1$ et $pgcd(Cont(f), g_n) = 1$. Alors, si h est primitif dans $R[x]$, f et g sont primitifs dans $R[x]$.*

Pour prouver le théorème 3.21, nous aurons besoin du lemme 1.105 du premier chapitre et du lemme suivant :

Lemme 3.22 *Soit R un anneau commutatif. Si*

$$f(x) = \sum_{i=0}^{m} f_i x^i \in R[x],$$

alors

$$f(x-t) = \sum_{i=0}^{m} (-1)^i \Big(f_i + f_{i+1} C_{i+1}^i x + ... + f_m C_m^i x^{m-i} \Big) t^i.$$

Démonstration 3.23 *Par récurrence sur le degré de f.*
Pour $m = 0$, on a $f(x-t) = f_0$.
Si $\deg(f) = m$, on a

$$f(x) = \sum_{i=0}^{m} f_i x^i \in R[x],$$

d'où

$$f(x-t) = \sum_{i=0}^{m} (-1)^i (f_i + f_{i+1} C_{i+1}^i x + ... + f_m C_m^i x^{m-i}) t^i. \tag{3.7}$$

Si $\deg(f) = m+1$. *C'est à dire, si*

$$f(x) = \sum_{i=0}^{m+1} f_i x^i \in R[x], \tag{3.8}$$

alors

$$f(x-t) = \sum_{i=0}^{m+1} (-1)^i \Big(f_i + f_{i+1} C_{i+1}^i x + ... + f_{m+1} C_{m+1}^i x^{m+1-i} \Big) t^i. \tag{3.9}$$

D'une part, on a

$$f(x) = \sum_{i=0}^{m+1} f_i x^i = \sum_{i=0}^{m} f_i x^i + f_{m+1} x^{m+1}, \tag{3.10}$$

et d'autre part

$$\begin{aligned} f(x-t) &= \sum_{i=0}^{m+1} f_i (x-t)^i \\ &= \sum_{i=0}^{m} f_i (x-t)^i + f_{m+1}(x-t)^{m+1}, \end{aligned}$$

puis

$$f(x-t) = \sum_{i=0}^{m} (-1)^i \Big(f_i + f_{i+1} C_{i+1}^i x + ... + f_m C_m^i x^{m-i} \Big) t^i + f_{m+1}(x-t)^{m+1}, \tag{3.11}$$

et comme

$$(x-t)^{m+1} = \sum_{i=0}^{m+1} C_{m+1}^i x^{m+1-i} (-t)^i = \sum_{i=0}^{m} (-1)^i C_{m+1}^i i x^{m+1-i} t^i + (-1)^{m+1} t^{m+1}, \tag{3.12}$$

en substituant 3.12 dans 3.11, on obtient

$$\begin{aligned} f(x-t) = \sum_{i=0}^{m} (-1)^i \Big(& f_i + f_{i+1} C_{i+1}^i x + ... + f_m C_m^i x^{m-i} \\ & + f_{m+1} C_{m+1}^i x^{m+1-i} \Big) t^i + (-1)^{m+1} f_{m+1} t^{m+1}, \\ = \sum_{i=0}^{m+1} (-1)^i & \Big(f_i + f_{i+1} C_{i+1}^i x + ... + f_m C_m^i x^{m-i} + f_{m+1} C_{m+1}^i x^{m+1-i} \Big) t^i. \end{aligned}$$

Démonstration 3.24 (Preuve du théorème 3.21) *Par contraposée : Nous allons prouver que si* f *ou* g *n'est pas primitif alors* $f * g$ *n'est pas primitif. Supposons que* g *n'est pas primitif, alors il existe un élément irréductible* $p \in R$ *tel que* $p \mid Cont(g)$. *On a*

$$(f * g)(x) = Res_t((-1)^m f(x-t), g(t)). \tag{3.13}$$

Posons $h_x(t) = (-1)^m f(x-t)$. *En utilisant le lemme 3.22, on a*

$$h(x,t) = (-1)^m \sum_{i=0}^{m} (-1)^i (f_i C_i^i + f_{i+1} C_{i+1}^i + f_m C_m^i x^{m-i}) t^i. \tag{3.14}$$

Remarquons que $h_x(t)$ *et* $g(t)$ *sont dans* $R[x][t]$.
Soit $j : R[x][t] \to R[x][t]/(p)$, *la surjection canonique, où* $\langle p \rangle$ *est l'idéal engendré par* p. *Comme* $p \mid Cont(g)$, *on a* $\overline{g(t)}^p = 0$, *et comme* $pgcd(Cont(g(t)), f_m) = 1$, *alors* $\overline{f_m}^p \neq 0$. *Notons que* $f(x)$ *et* $h_x(t)$ *ont le même coefficient dominant* f_m.*Donc, d'après le lemme 1.105, on a*

$$\overline{(f*g)(x)}^p = \overline{Res_t(h_x(t), g(t))}^p = Res_t(\overline{h_x(t)}^p, \overline{g(t)}^p), \tag{3.15}$$

et comme

$$Res_t(\overline{h_x(t)}^p, \overline{g(t)}^p) = Res_t(\overline{h_x(t)}^p, 0) = 0, \tag{3.16}$$

alors

$$\overline{(f*g)(x)}^p = 0, \tag{3.17}$$

ainsi, $p \mid Cont(f*g)$, *et donc* $f*g$ *n'est pas primitif.*

Remarque 3.25 *Si* f *et* g *sont primitifs,* $f*g$ *n'est pas nécessairement primitif. Par exemple* $2x^3 + 3x^2 - 11x - 6$ *et* $4x^2 - 13x - 12$ *sont des polynômes primitifs dans* $\mathbb{Z}[x]$ *alors que le polynôme*

$$f*g = -2672x^4 - 16610x^2 + 26604x^3 - 37350x + 31500 - 1728x^5 + 256x^6$$

n'est pas primitif dans $\mathbb{Z}[x]$ *car* $Cont(f*g) = 2$.

Conclusion et perspectives

Dans cette thèse, nous avons étudié la décomposition additive de polynômes sur un anneau factoriel. Pour cela, nous avons introduit la loi de composition interne $*$ sur l'ensemble des polynômes à coefficients dans un anneau commutatif et sa relation avec le résultant de deux polynômes. Nous avons montré que si un polynôme $h = f * g$ est irréductible sur un anneau intègre A alors f et g sont irréductibles sur A, un résultat analogue à celui de Brawley et Carlitz sur un corps fini. Nous avons aussi présenté des classes de polynômes additivement indécomposables sur un anneau intègre puis sur un anneau factoriel. Nous avons étudié la primitivité des facteurs d'un polynôme primitif $h = f * g$ à coefficients dans un anneau factoriel. Ce travail a été motivé par une étude faite par Brawley et Carlitz [5] sur les corps finis. D'autres lois de composition ont été définies sur l'ensemble des polynômes unitaires à coefficients dans un corps fini. L'une des perspectives serait une étude similaire par rapport à ces lois.

Bibliographie

[1] Belabas, K. *Résultant de deux polynômes*. 2012-2013.

[2] Benferhat, L., Benoumhani, S. M. E., Boumahdi, R., and Larone, J. Additive decompositions of polynomials over unique factorization domain. *Journal of Algebra and Its Applications*.

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

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

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

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

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

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

[9] Cherchem, A. *Corps Finis*. Cours de Master, USTHB, 2012-2013.

[10] 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.

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

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

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

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

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

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

[17] 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.

[18] 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.

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

[20] Salvya, A. B. P. F. B., and Schostb, É. Fast computation of special resultants.

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

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

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