

# Remerciements

*Avant tout je remercie Allah, le tout puissant d'avoir, éclaire notre vie, renforce notre courage et notre volenté pour finie ce travail.*

*Je remercie monsieur N.GHADBANE pour m'avoir proposé ce sujet et d'avoir accepté de m'encadrer.*

*La gentillesse et la disponibilité dont il a fait preuve à mon égard m'ont beaucoup touchée.*

*Je remercie également les professeurs*

*Mr.D.MIHOUBI*

*Mr.L.HEBOUB*

*qui m'ont faite l'honneur d'être membres du jury.*

*Merci à tous les enseignants et les étudiants de département mathématique pour leurs dévouement et leurs générosité.*

*Je tiens aussi à exprimer ma profonde gratitude envers mes parents surtout mon père pour le soutien qu'ils m'ont apporté au fil des ans dans la poursuite de mes études et pour m'avoir permis de devenir tout ce que je suis aujourd'hui.*

*Enfin, Un grand merci à ma famille, à mes proches et à mes collègues et pour leurs encouragements et pour leurs amitiés.*

# Dédicace

*Je dédie ce modeste travail à :*

*Les parents les plus chers au monde, mon père Brahim et ma mère Aicha, que dieu  
les garde et les protège.*

*Mon frère walid, mes sœurs Nabila, Samiha, Feriel.*

*Les enfants de ma sœur Loai, Assil, Imade.*

*Ma chère amie Imane LEGMA.*

*Toutes mes amies, particulièrement : Marwa, Khaoula, Saàdia, Halima, Djazia.*

*Toute la promotion 2019 de Université Mohamed Boudiaf de M'sila.*

*A tous ceux qui sont proches de mon cœur et dont je n'ai pas cité le nom.*

*Je demande à Dieu de préserver leur vie.*

# Résumé

Ce mémoire de master Algèbre et Mathématiques discrètes s'inscrit dans le cadre de la théorie des anneaux de polynômes à plusieurs variables et leurs applications en cryptographie asymétrique.

On donne tout d'abord des notions générales sur les anneaux et les corps.

Par suite, on fait une étude sur l'anneau de polynômes à plusieurs variables.

D'autre part, nous avons étudié La cryptographie asymétrique.

Enfin, on s'intéresse au protocole cryptographique asymétrique sur l'anneau de polynômes à plusieurs variables.

**Mots clés :** Anneau, corps, idéal, l'anneau de polynômes à plusieurs variables, la cryptographie asymétrique.

# Abstract

This master thesis Algebra and Discrete Mathematics is part of the theory of multi-variable polynomial rings and their applications in asymmetric cryptography.

First, general notions about rings and bodies are given.

As a result, we study the ring of polynomials with different variables.

On the other hand, we studied asymmetric cryptography.

Finally, we are interested in the asymmetric cryptographic protocol on the ring of multivariate polynomials.

**Keywords :** Ring, ideal, ideal, ring of polynomials to more variables, asymmetric cryptography.

# Notations

- $\mathbb{K}[x_1, \dots, x_n]$  : l'ensemble des polynômes à  $n$  variables  $x_1, \dots, x_n$  à coefficients dans  $\mathbb{K}$ .
- $GL_n(\mathbb{F}_q)$  (resp  $GL_u(\mathbb{F}_q)$ ) : l'ensemble des matrices inversibles de  $\mathcal{M}_{n,n}(\mathbb{F}_q)$  (resp  $\mathcal{M}_{n,u}(\mathbb{F}_q)$ ).
- $\underline{c}$  : le  $n$ -uplet de variables  $c_1, \dots, c_n$ .
- $\mathcal{P}$  : les mots en clair.
- $\mathcal{C}$  : les mots codés.
- $\mathcal{K}$  : l'espace des clefs.
- $\mathbb{F}_q$  : le corps fini à  $q = p^m$  ( $p$  premier,  $m > 0$ ) éléments.

# Table des matières

<b>Introduction</b>	<b>1</b>
<b>1 Notions élémentaires sur les anneaux et les corps</b>	<b>2</b>
1.1 Les anneaux . . . . .	2
1.1.1 Calculs dans un anneau . . . . .	3
1.1.2 Produit fini d'anneaux . . . . .	4
1.1.3 Anneaux euclidienne . . . . .	7
1.1.4 Algorithme d'Euclide . . . . .	8
1.1.5 Sous-anneau . . . . .	8
1.1.6 Morphisme d'anneau . . . . .	9
1.2 Idéaux . . . . .	10
1.2.1 Opérations sur les idéaux . . . . .	11
1.3 Les corps . . . . .	13
1.3.1 Sous-corps . . . . .	14
<b>2 Etude sur l'anneau de polynômes à plusieurs variables</b>	<b>16</b>
2.1 La division dans l'anneau des polynômes à plusieurs variables . . . . .	16
2.1.1 Polynômes . . . . .	16
2.2 S-polynôme . . . . .	22
2.3 Anneaux des polynômes sur un corps . . . . .	22
2.4 Idéaux dans un anneau de polynôme à plusieurs variables . . . . .	26
2.4.1 Idéaux premiers . . . . .	27
2.4.2 Idéaux maximaux . . . . .	28
2.4.3 Idéaux monomiaux . . . . .	28
2.4.4 Algorithme de division de polynômes . . . . .	28
<b>3 La cryptographie asymétrique</b>	<b>31</b>
3.1 Préambules mathématique . . . . .	32
3.1.1 Identité de Bézout . . . . .	32
3.1.2 Congruences . . . . .	32
3.1.3 L'exponentiation rapide . . . . .	34
3.2 L'arithmétique pour RSA . . . . .	34
3.2.1 Description du cryptosystème RSA : . . . . .	35
3.2.2 Protocole d'envoi d'un message en RSA : . . . . .	35
3.3 El Gamal . . . . .	37

3.3.1	Description du cryptosystème El Gamal . . . . .	37
<b>4</b>	<b>Protocole cryptographique asymétrique sur l’anneau de polynômes à plusieurs variables</b>	<b>39</b>
4.1	Transformations affines . . . . .	39
4.2	Principe général . . . . .	40
4.3	Exemples de trappes . . . . .	42
4.3.1	Extension de corps . . . . .	43
	<b>Conclusion</b>	<b>44</b>
	<b>Bibliographie</b>	<b>44</b>

# Introduction

L'objet de la cryptographie est de fournir les outils pour assurer la protection des données. La sécurité cryptographique repose sur la difficulté de retrouver un certain secret (clé secrète). La cryptographie asymétrique utilise une clé dite publique et une clé privée [DH76]. Dans les schémas classiques, on utilise des problèmes issus de la théorie des nombres comme factoriser un grand entier pour RSA [RSA78] ou résoudre le problème du logarithme discret (ElGamal [ElG85]) qui sont largement utilisés.

Le problème de résoudre un système d'équations polynomiales non-linéaires en plusieurs variables (POSSO) à été montré NP-difficile [GJ79].

Dans la cryptographie multivariée, la clé publique se présente sous la forme d'un système de polynômes  $\{g_1, \dots, g_m\} \in \mathbb{F}_q[x_1, \dots, x_n]$  à coefficient dans un corps  $K$ .

Dans ce mémoire nous allons étudier la cryptographie à clé publique basé sur la difficulté de résoudre un système polynômiels à plusieurs variables.

Ce travail est composé de quatre chapitres :

Le premier chapitre consiste à un rappel des notions élémentaires sur les anneaux et les corps.

Dans le deuxième chapitre nous allons étudier l'anneau de polynômes à plusieurs variables.

Dans le troisième chapitre nous intéressons à la cryptographie asymétrique et quelques propriétés.

A la quatrième chapitre, nous allons étudier un protocole cryptographique asymétrique sur l'anneau de polynômes à plusieurs variables.

# Chapitre 1

## Notions élémentaires sur les anneaux et les corps

Ce premier chapitre contient les définitions et les propriétés des outils que nous utiliserons par la suite

### 1.1 Les anneaux

#### Définition 1.1

On appelle anneau tout triplet  $(A, +, \times)$  formé d'un ensemble  $A$  et de deux lois de composition internes usuellement notées "  $+$  " et "  $\times$  " sur  $A$  vérifiant :

1.  $(A, +)$  est un groupe abélien de neutre  $0_A$  .
2. "  $\times$  " est associative.
3. "  $\times$  " est distributive sur "  $+$  "  
i.e.,  $\forall a, b, c \in A, a(b + c) = ab + ac$  et  $(b + c)a = ba + ca$ .

#### Notation 1.1    *Dans un anneau $A$*

- On note  $0$  (ou  $0_A$ ) l'élément neutre pour  $+$ .
- On note  $1$  (ou  $1_A$ ) l'élément neutre pour  $\times$ .
- On note couramment  $x \cdot y$  ou même  $xy$  à la place de  $x \times y$ .



### Remarque 1.1

- 1) Si la loi "  $\times$  " possède un éléments neutre noté "1" on dit que  $A$  est un anneau unitaire et "1" est l'unité de  $A$ .
- 2) Si la loi "  $\times$  " est commutative on dit que l'anneau  $A$  est commutatif.

### Exemple 1.1

- $(\mathbb{Z}, +, \times), (\mathbb{R}, +, \times), (\mathbb{C}, +, \times)$  sont des anneaux commutatifs unitaires.
- Soient  $A$  est un anneau et  $X$  un ensemble et  $\mathcal{F}(X, A)$  l'ensemble des fonctions de  $X$  vers  $A$ .  $(\mathcal{F}(X, A), +, \times)$  est un anneau de neutres  $\tilde{0}$  et  $\tilde{1}$  (fonctions constantes). En particulier, si  $X = \mathbb{N}$ , l'ensemble  $A^{\mathbb{N}}$  des suites d'éléments de  $A$  est un anneau commutatif unitaire.

#### 1.1.1 Calculs dans un anneau

##### Proposition 1.1

$$\forall a, b \in A, 0_A \times a = a \times 0_A = 0_A, (-a)b = -(ab) = a(-b).$$

$$\text{Plus généralement, } \forall n \in \mathbb{Z}, (n.a) \times b = n.(ab) = a \times (n.b).$$

##### Théorème 1.2

Si  $a$  et  $b$  sont deux éléments commutant (i.e.  $ab = ba$ ) d'un anneau  $A$  on a pour tout  $n \in \mathbb{N}$

$$(ab)^n = a^n b^n, (a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}.$$

Et

$$a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-1-k}.$$

##### Définition 1.2

Un élément  $a$  d'un anneau  $(A, +, \times)$  est dit inversible s'il existe  $b \in A$  tel que  $ab = ba = 1$ . Cet élément  $b$  est alors unique, on l'appelle inverse de  $a$  et il est noté  $a^{-1}$ .

**Exemple 1.2**

$1_A$  est inversible et  $1_A^{-1} = 1_A$ .

**Théorème 1.3**

*L'ensemble  $U(A)$  des éléments inversibles de l'anneau  $(A, +, \times)$  est un groupe multiplicatif.*

**Exemple 1.3**

$$U(\mathbb{Z}) = \{1, -1\}.$$

**1.1.2 Produit fini d'anneaux**

Soit  $(A_1, +, \times), \dots, (A_n, +, \times)$  des anneaux et  $A = A_1 \times \dots \times A_n$ .

On définit des lois  $+$  et  $\times$  sur  $A$  en posant

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) \stackrel{\text{déf}}{=} (x_1 + y_1, \dots, x_n + y_n).$$

Et

$$(x_1, \dots, x_n) \times (y_1, \dots, y_n) \stackrel{\text{déf}}{=} (x_1 \times y_1, \dots, x_n \times y_n).$$

**Théorème 1.4**

*L'ensemble  $A$  muni des lois  $+$  et  $\times$  définies ci-dessus est un anneau de neutres*

$$0_A = (0_{A_1}, \dots, 0_{A_n}) \text{ et } 1_A = (1_{A_1}, \dots, 1_{A_n}).$$

*De plus, un élément  $(a_1, \dots, a_n) \in A$  est inversible si et seulement si les  $a_1, \dots, a_n$  le sont et son inverse est alors  $(a_1^{-1}; \dots; a_n^{-1})$ .*

**Corollaire 1.1**

$$U(A) = U(A_1) \times \dots \times U(A_n).$$

**Exemple 1.4**

$(\mathbb{Z}^2, +, \times)$  est un anneau commutatif où  $(a, b) + (c, d) = (a + c, b + d)$  et  $(a, b) \times (c, d) = (ac, bd)$ .

On a  $U(\mathbb{Z}^2) = \{(1, 1), (1, -1), (-1, 1), (-1, -1)\}$ .

### Définition 1.3

Soient  $(A, +, \times)$  un anneau commutatif unitaire  $a \in A$ .

- On dit que  $a$  est un diviseur de zéro dans  $A$ , s'il existe  $b \in A$  et  $b \neq 0$  telle que  $b \times a = a \times b = 0$ .
- L'anneau  $(A, +, \times)$  est intègre s'il ne possède pas de diviseur de zéro, c'est à dire  $a \times b = 0 \Rightarrow a = 0$  ou  $b = 0$ .
- On dit que  $a$  est irréductible si et seulement si  $a \notin U(A)$  et pour tout  $x, y \in A$   $x \times y = a \Rightarrow (x \in U(A) \text{ ou } y \in U(A))$  où  $U(A)$  est le groupe des éléments inversibles de l'anneau  $A$ .
- Un anneau intègre est principale si tout idéal de cet anneau est principale.
- Soit  $A$  un anneau commutatif, on dit que  $A$  est factoriel s'il intègre et vérifier les deux conditions suivantes : existence(1) et unicité (2) de la décomposition en facteurs irréductible. Autrement dit :

1. tout  $x \in A^*$  non inversible s'écrit  $x = p_1 \dots p_r$ , où  $r \geq 1$  et les  $p_i$  sont éléments irréductible de  $A$  non nécessairement distincts.

Deux élément  $a, b \in A$  sont associés et on écrit  $a \sim b$  si  $a \mid b$  et  $b \mid a$

2. la décomposition précédente est unique au sens suivant : si l'on a deux décompositions  $x = p_1 \dots p_r = q_1 \dots q_s$  où les  $p_i$  et les  $q_i$  sont irréductible, alors  $s = r$  et il existe une permutation  $\sigma$  de  $[1 \dots r]$  telle que  $p_i$  et  $q_{\sigma(i)}$  soient associés.

- On dit que  $a$  divise  $b$ , et on écrit  $a \mid b$  s'il existe  $x \in A$  telle que  $b = a \times x$  ( $a$  diviseur de  $b$ ,  $b$  multiple de  $a$ ).
- Soit  $a, b \in A$ , on appelle un pgcd (plus grand commun diviseur) de  $a$  et  $b$  noté  $\text{pgcd}(a, b) = a \wedge b$  un élément de  $A$  vérifiant :

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

### Exemples

1.  $\mathbb{Z}, \mathbb{Q}, \mathbb{C}, \mathbb{R}$  sont des anneaux intègres.
2.  $A = M_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in \mathbb{Z} \right\}$ .

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \text{ sont des diviseurs de zéro donc } M_2(\mathbb{Z}) \text{ est non int\`egre.}$$

3.  $\mathbb{Z}/7\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ ,  $\mathbb{Z}/7\mathbb{Z}$  est int\`egre.

4. Dans  $\mathbb{Z}$ , les \`elements irr\'eductible sont les nombres premiers.

5. L'anneau  $(\mathbb{Z}, +, \times)$  est factoriel.

6.  $A = \mathbb{Z}$ ,  $2 \mid 4$ ,  $2 \mid 6$ ,  $-3 \mid 9$ .

7.  $A = \mathbb{Z}/7\mathbb{Z}$ ,  $\bar{2} \sim \bar{3}$ ,  $\bar{2} \mid \bar{3}$  car  $\bar{2} \times \bar{5} = \bar{3}$  et  $\bar{3} \mid \bar{2}$  car  $\bar{3} \times \bar{3} = \bar{2}$ .

8. 3 est un  $\text{pgcd}$  de 15, 9 dans  $\mathbb{Z}$ .

### Proposition 1.2

*Dans un anneau int\`egre  $(A, +, \times)$  :*

$\forall a, b, c \in A, (ab = ac \text{ et } a \neq 0_A) \Rightarrow b = c$

*Et*

$\forall a, b, c \in A, (ab = ac \text{ et } a \neq 0_A) \Rightarrow b = c$

### Preuve.

Si  $ab = ac$  alors  $ab - ac = 0_A$  et donc  $a(b - c) = 0_A$ .

Si de plus  $a \neq 0_A$  alors, par int\'egrit\'e,  $b - c = 0_A$  et donc  $b = c$ . ■

### D\'efinition 1.4 "Anneau de B\'ezout"

Soit  $A$  un anneau commutatif int\`egre, on dit que  $A$  est un anneau de B\'ezout si, et seulement si une des deux propositions \'equivalentes suivantes est v\'erifi\'ee :

1. La somme de deux id\'eaux principaux de  $A$  est toujours un id\'eal principal.
2. Tous les id\'eaux de type fini de  $A$  sont principaux.

### Th\'eor\`eme 1.5 "\'Egalit\'e de B\'ezout"

*Soit  $A$  un anneau de B\'ezout,  $a$  et  $b$  deux \`elements de  $A$  et  $d = \text{pgcd}(a, b)$ . Il existe alors un couple  $(u, v) \in A^2$  tels que :  $au + bv = d$ .*

### **Théorème 1.6**    "*Théorème de Bézout*"

Soit  $A$  un anneau de Bézout,  $a$  et  $b$  deux éléments de  $A$  sont premier entre eux si, est seulement si  $\exists (u, v) \in A^2$ ,  $au + bv = 1_A$ .

#### **Preuve.**

Dans le sens " $\Rightarrow$ " : Immédiat grâce à **l'égalité de Bézout**.

Dans le sens " $\Leftarrow$ " : (réciproquement)

On suppose que  $\exists (u, v) \in A^2$ ,  $au + bv = 1_A$

Si  $d = \text{pgcd}(a, b)$  alors  $d$  divise  $a$  et  $b$  donc  $d$  divise  $au + bv$ .

Donc  $d$  divise  $1_A$ . On a bien  $d = 1_A$ . ■

### **1.1.3 Anneaux euclidienne**

#### **Définition 1.5**

Soit  $A$  anneau commutatif unitaire intègre.

Une division euclidienne sur  $A$  est une application  $\varphi : A^* \rightarrow \mathbb{N}$ , vérifiant :

1.  $\forall a, b \in A^* : \varphi(a) \leq \varphi(ab)$ .
2.  $\forall a, b \in A : b \neq 0$ , il existe  $(q, r) \in A \times A$  telle que :  $a = bq + r$  avec  $r = 0$  ou  $\varphi(r) \leq \varphi(b)$ .

#### **Exemple 1.5**

L'anneau  $\mathbb{Z}$  muni de l'application  $\varphi(n) = |n|$  est euclidien.

#### **Définition 1.6**

Un anneau euclidien est un anneau intègre muni d'une division euclidienne.

#### **Définition 1.7**

Tout anneau euclidien est un anneau principal.

#### **Exemple 1.6**

$(\mathbb{Z}, +, \times)$ .

#### **Définition 1.8**

Tout anneau euclidien est factoriel.

### 1.1.4 Algorithme d'Euclide

Soit  $a$  et  $b$  ( $b \neq 0$ ). deux entiers, on effectue les divisions euclidiennes successives des quotients par leurs restes, jusqu'à arriver à un reste nul, alors le dernier reste non nul est un diviseur commun de  $a$  et  $b$  de degré minimal, ce reste une fois normalisé, s'appelle le  $\text{pgcd}$  de  $a$  et  $b$  et se note  $a \wedge b$ .

$$a = bq_1 + r_1, r_1 = 0 \text{ ou } \varphi(r_1) < \varphi(b)$$

$$b = r_1q_2 + r_2, r_2 = 0 \text{ ou } \varphi(r_2) < \varphi(r_1)$$

$$r_1 = r_2q_3 + r_3, r_3 = 0 \text{ ou } \varphi(r_3) < \varphi(r_2)$$

.

.

.

$$r_{n-2} = r_{n-1}q_n + r_n, r_n = 0 \text{ ou } \varphi(r_n) < \varphi(r_{n-1})$$

$$r_{n-1} = r_nq + 0.$$

Donc on a :  $r_n = \text{pgcd}(a, b)$ , inversement on trouve  $x, y \in A$  ( $A$  anneau euclidienne) telle que :

$$r_n = a \cdot x + b \cdot y. \text{ (identité de Bézout).}$$

### 1.1.5 Sous-anneau

Dans cette section  $(A, +, \times)$  désigne un anneau.

#### Définition 1.9

On appelle sous-anneau de  $(A, +, \times)$  toute partie  $B$  de  $A$  vérifiant :

1.  $\forall x, y \in B; x - y \in B;$
2.  $\forall x, y \in B, xy \in B;$

#### Exemple 1.7

Considérons  $\mathbb{Z}[i] = \{a + ib / a, b \in \mathbb{Z}\}$  et montrons que  $(\mathbb{Z}[i], +, \times)$  est un anneau commutatif.

Montrons que  $\mathbb{Z}[i]$  un sous-anneau de l'anneau commutatif  $(\mathbb{C}, +, \times)$ .

On a évidemment  $\mathbb{Z}[i] \in \mathbb{C}$ .

$1 = 1 + i.0 \in \mathbb{Z}[i]$ . Pour  $x, y \in \mathbb{Z}[i]$ , on peut écrire  $x = a + ib$  et  $y = c + id$  avec  $a, b, c, d \in \mathbb{Z}$ . On a  $x - y = (a - c) + i(b - d) \in \mathbb{Z}[i]$  car  $a - c, b - d \in \mathbb{Z}$  et  $xy = (ac - bd) + i(ad + bc) \in \mathbb{Z}[i]$ .

Ainsi,  $\mathbb{Z}[i]$  est un sous-anneau de  $(\mathbb{C}, +, \times)$  et donc  $(\mathbb{Z}[i], +, \times)$  est un anneau commutatif.

### **Théorème 1.7**

*Si  $B$  est un sous-anneau de  $(A, +, \times)$  alors  $B$  peut être muni des lois "  $+$  " et "  $\times$  " définies par restriction des lois sur  $A$  et  $(B, +, \times)$  est alors un anneau de mêmes neutres que  $A$ .*

#### **Preuve.**

$B$  est un sous-groupe du groupe abélien  $(A, +)$  donc  $(B, +)$  est un groupe abélien.

$B$  est stable par "  $\times$  " donc on peut définir la restriction de la loi "  $\times$  " sur  $B$ .

Celle-ci est associative sur  $A$  et possède un neutre  $1_A \in B$  donc "  $\times$  " est associative sur  $B$  et  $y$  possède un neutre.

Enfin, "  $\times$  " est distributive sur "  $+$  " sur  $A$  donc a fortiori aussi sur  $B$ . ■

### **Proposition 1.3**

1. Toute intersection de sous-anneau est un sous-anneau.
2. Tout sous-anneau d'anneau commutatif (respectivement intègre) est commutatif (respectivement intègre).

### **Remarque 1.2**

Une réunion de sous-anneau n'est pas forcément un sous-anneau.

## **1.1.6 Morphisme d'anneau**

### **Définition 1.10**

Soient  $(A, +, \times)$  et  $(B, +, \times)$  on dit que  $f : A \longrightarrow B$  est un morphisme d'anneaux si :

1.  $\forall (a, b) \in A^2, f(a + b) = f(a) + f(b)$ .

2.  $\forall (a, b) \in A^2, f(a \times b) = f(a) \times f(b)$ .
3.  $f(1_A) = 1_B$ .

### Exemple 1.8

L'application identité  $\text{Id}_A : A \rightarrow A$  est un morphisme de l'anneau  $(A, +, \times)$  vers lui-même.

## 1.2 Idéaux

### Définition 1.11

Soit  $(A, +, \times)$  un anneau et soit  $I \subset A$ .

$I$  est un idéal à gauche (respectivement à droite) de  $A$  si et seulement si :

- a.  $\forall x, \forall y \in I, x - y \in I$ .
- b.  $\forall a \in A : a \times x \in I$  (resp.  $x \times a \in I$ ).

### Exemple 1.9

$n\mathbb{Z}$  est un idéal de  $(\mathbb{Z}, +, \times)$ .

### Remarque 1.3

- La condition (a) veut dire que  $(I, +)$  est un sous-groupe de  $(A, +)$ .
- Si l'anneau  $A$  est commutatif l'une des condition  $a \times x \in I$  ou  $x \times a \in I$  suffit.

### Définition 1.12

1.  $I$  est un idéal bilatère si et seulement si  $I$  est un idéal à gauche et à droite.
2.  $I$  est un idéal strict ou propre si  $I \neq A$ .

### Définition 1.13

$I$  est un idéal premier ssi  $\forall x, y \in A, x.y \in I \Rightarrow x \in I$  ou  $y \in I$ .

L'ensemble des idéaux premiers est le spectre de  $A$ , noté  $\text{Spec}(A)$ .



**Exemple 1.10**

Si  $A = \mathbb{Z}$ ,  $I = n\mathbb{Z}$  est premier si et seulement si  $n = 0$  ou  $n$  premier.

**Définition 1.14**

Si  $I$  est un idéal bilatère. On dit que  $I$  est maximal s'il est strict et s'il n'est contenu dans aucun autre idéal que l'anneau tout entier.

L'ensemble des idéaux maximaux de  $A$  est le spectre maximal de  $A$ , noté  $Max(A)$ .

**Exemple 1.11**

Les idéaux maximaux de  $\mathbb{Z}$  sont les  $p\mathbb{Z}$  pour  $p$  est premier.

**Corollaire 1.2**

*Tout idéal maximal est premier.*

**Proposition 1.4**

*Soit  $(A, +, \times)$  un anneau unitaire. Soit  $I$  un idéal de  $A$ .*

*Si  $I$  contient l'élément unité de  $A$  ou un élément inversible de  $A$  alors  $I = A$ .*

**1.2.1 Opérations sur les idéaux****Somme et produit d'idéaux**

Les opérations d'addition et de multiplication d'idéaux sont triviales :

**Définition 1.15**

Soit  $(A, +, \times)$  et soient  $I$  et  $J$  des idéaux dans  $A$ . Alors :

la somme de  $I$  et  $J$ , noté  $I + J$ , est définie par :

$$I + J = \{f + g : f \in I \text{ et } g \in J\}.$$

le produit de  $I$  et  $J$ , noté  $I \cdot J$ , est définie par :

$$I \cdot J = \{f \cdot g : f \in I \text{ et } g \in J\}.$$

**Définition 1.16**

Soit  $(A, +, \times)$  un anneau unitaire et soit  $I$  un idéal de  $A$ .

1.  $I$  est dit principal s'il est engendré par un seul élément.

( $I$  est de la forme  $I = s.A$  ou  $A.s$  où  $s \in A$ ).

2.  $I$  est dit de type fini si il existe  $S \subset A$  finie engendrant  $I$

(c'est-à-dire :  $I = S.A$  ou  $A.S$ ). On le notera  $(S)$  quand l'idéal est bilatère.

**Définition 1.17**

Soit  $A$  un anneau. On dit que  $A$  est noethérien lorsqu'il possède les propriétés équivalentes suivantes :

1. Toute suite croissante d'idéaux  $I_0 \subset I_1 \subset \dots \subset I_n \subset \dots$  est stationnaire autrement dit il existe  $n \geq 0$  tel que  $I_m = I_n$  pour  $m \geq n$ .
2. Toute famille non vide d'idéaux admet un élément maximal.

**Proposition 1.5**

Soit  $f : A \longrightarrow B$  un morphisme d'anneaux

1. Si  $I$  est un idéal bilatère alors  $f^{-1}(I)$  est un idéal bilatère.
2. Si  $I$  est un idéal premier alors  $f^{-1}(I)$  est un idéal premier.

**Théorème 1.8**

Si  $A$  est un anneau euclidien, tout idéal de  $A$  est engendré par un élément.

**Preuve.** Soit  $A$  un anneau euclidien, muni d'un algorithme euclidien  $\varphi$ , et soit  $I$  un idéal de  $A$ . Si  $I$  est nul, il est engendré par 0, on a  $I = \langle 0 \rangle$ . Si  $I$  est non nul, alors  $\varphi(I - \{0\})$  est une partie non vide de  $\mathbb{N}$ , elle a donc un plus petit élément  $n$ . Soit  $b \in I - \{0\}$ , tel que  $\varphi(b) = n$ . Tout élément  $a$  de  $I$  s'écrit  $a = bq + r$ , avec  $r = 0$  ou  $\varphi(r) < \varphi(b) = n$ . Or  $r = a - bq \in I$ , donc par minimalité de  $n$ , on ne peut pas avoir  $\varphi(r) < n$ , d'où nécessairement  $r = 0$ . Par suite, tout élément  $a$  de  $I$  s'écrit  $a = bq$ , ainsi  $I = \langle b \rangle$ .

■

## 1.3 Les corps

### Définition 1.18

On appelle corps tout anneau  $(K, +, \times)$  vérifiant

1.  $(K, +, \times)$  est commutatif .
2.  $K$  est non réduit à  $\{0_K\}$ .
3. Tous les éléments de  $K$ , sauf le nul, sont inversibles.

### Exemple 1.12

$(\mathbb{Q}, +, \times)$ ,  $(\mathbb{R}, +, \times)$ ,  $(\mathbb{C}, +, \times)$  sont des corps usuels.

### Proposition 1.6

*Tout corps est intègre.*

#### Preuve.

Soit  $K$  un corps.  $K$  est commutatif et non réduit à  $\{0_K\}$ . Pour  $a, b \in K$ , si  $ab = 0_K$  et  $a \neq 0_K$  alors on peut introduire  $a^{-1}$  et on  $ab = a^{-1}(ab) = 0_K$ . Ainsi,  $K$  ne possède pas de diviseurs de zéro. Il est donc intègre. ■

### Proposition 1.7

*Soit  $(A, +, \times)$  un anneau commutatif et  $I$  un idéal de  $A$  distinct de  $A$ , alors les deux énoncés suivants sont équivalents :*

1.  $I$  est maximal dans  $A$ .
2. Le triplet  $(A/I, +, \times)$  est un corps.

#### Preuve.

Supposons d'abord (1) et montrons alors que l'anneau quotient  $A/I$  est un corps i.e; que tout élément non nul de  $A/I$  est inversible dans  $(A/I, +, \times)$ .

Soit donc  $\bar{x} \in A/I$ ,  $\bar{x} \neq 0$ , c'est-à-dire,  $x$  n'appartenant pas à  $I$ ; dans ces conditions l'idéal engendré par  $I$  et  $\{x\}$ , c'est-à-dire :  $I + xA = \{j + ax; j \in I; a \in A\}$

contient strictement  $I$  ; il est donc égal à  $A$ , ainsi on peut trouver  $x'$  dans  $A$  et  $j$  dans  $I$  tels que :  $xx' + j = e$  (élément neutre multiplicatif de  $A$ ).

Dans ces conditions :  $xx' = e$  ce qui prouve (2).

Réciproquement supposons (1) et soit  $J$  un idéal de  $A$ , contenant strictement  $I$  ; on peut donc trouver  $x \in J$ ,  $x \notin I$ ,  $x$  est donc dans  $A = I$  un élément non nul et de ce fait, puisque on dispose d'un corps, inversible ; ainsi il existe  $x' \in A$  tel que :  $xx' = e$  ou encore :  $xx' - e \in I \subset J$ .

Comme  $xx'$  appartient à  $J$  (puisque  $J$  est un idéal) l'élément neutre  $e$  est aussi dans  $J$  ; cela impose :  $J = A$  et achève la preuve de la proposition. ■

### Définition 1.19

Soit  $K$  un corps et  $k$  un sous-corps. On dit que  $K$  est une extension de  $k$ .

### Définition 1.20

Soit un corps fini  $\mathbb{F}_{p^m}$  à  $p^m$  éléments,  $p$  premier et  $m$  positif, alors :

- le nombre premier  $p$  est appelé caractéristique du corps.
- le nombre entier  $m$  est appelé degré de l'extension  $\mathbb{F}_{p^m}$  sur  $\mathbb{F}_p$ .

## 1.3.1 Sous-corps

Soit  $(K, +, \times)$  un corps.

### Définition 1.21

On appelle sous-corps d'un corps  $(K, +, \times)$  toute partie  $L$  de  $K$  vérifiant :

1.  $L$  est un sous-anneau de  $(K, +, \times)$ .
2.  $\forall x \in L; x \neq 0_K \Rightarrow x^{-1} \in L$ .

### Exemple 1.13

$\mathbb{Q}$  est un sous-corps de  $(\mathbb{R}, +, \times)$ .

**Définition 1.22**

Soit  $A$  un anneau commutatif, le corps  $(A \times A^*)/\mathfrak{R}$  tel que  $\mathfrak{R}$  est une relation définie sur  $(A \times A^*)$  par :

$$(a, b)\mathfrak{R}(c, d) \Leftrightarrow ad = bc$$

s'appelle corps des fractions de  $A$ .

**Exemple 1.14**

Le corps des fractions de  $\mathbb{Z}$  est  $\mathbb{Q}$ .

# Chapitre 2

## Etude sur l'anneau de polynômes à plusieurs variables

### 2.1 La division dans l'anneau des polynômes à plusieurs variables

Dans cette section,  $\mathbb{K}$  désignera un corps commutatif.

#### 2.1.1 Polynômes

##### Définition 2.1

Un Monôme en  $x_1, \dots, x_n$  est un produit de la forme  $x_1^{\alpha_1} \dots x_n^{\alpha_n}$  où  $\alpha_i \in \mathbb{N}$ ,  $1 \leq i \leq n$ . On note aussi  $x^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}$ , où  $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ . Le degré total de  $x^\alpha$  est  $|\alpha| = \alpha_1 + \dots + \alpha_n$ .

##### Remarque 2.1

Si  $\alpha = (0, \dots, 0)$ , on note  $x^\alpha = 1$ .

##### Définition 2.2

Un polynôme  $P$  en  $x_1, \dots, x_n$  avec les coefficients dans  $\mathbb{K}$  est une combinaison linéaire finie des monômes  $P = \sum_{\alpha} a_{\alpha} x^{\alpha}$  où les  $a_{\alpha} \in \mathbb{K}$  sont presque tous nuls, i.e. la somme porte sur un ensemble fini de n-uplets  $(\alpha_1, \dots, \alpha_n)$ .

### Définition 2.3

Soit  $P = \sum_{\alpha} a_{\alpha} x^{\alpha}$ ;  $a_{\alpha} \in \mathbb{K}$ , un polynôme dans  $\mathbb{K}[x_1, \dots, x_n]$ .

1. On appelle  $a_{\alpha}$  le coefficient du monôme  $x^{\alpha}$ .
2. Si  $a_{\alpha} \neq 0$ , alors on appelle  $a_{\alpha} x^{\alpha}$  un terme de  $P$ .
3. Le degré totale de  $P$  noté  $\deg(P)$  est le maximum des  $|\alpha|$  tel que  $a_{\alpha} \neq 0$ .

### Exemple 2.1

Soit  $A = \mathbb{K}[x, y, z]$ , où  $\mathbb{K}$  est corps commutatif.

Prenons le polynôme  $P = 4xy^2 + 2y^3z^4$  de  $A$  le premier terme de  $P$  est  $4xy^2$  et le deuxième terme est  $2y^3z^4$ . et le  $\deg(P) = 7$ , le premier coefficient de  $P$  est 4 et le deuxième coefficient est 2.

### Proposition 2.1

Etant donnés deux polynômes  $P$  et  $Q \in \mathbb{K}[X]$ , on a :

1.  $\deg(P + Q) \leq \max(\deg P, \deg Q)$ , avec égalité  $\deg P \neq \deg Q$ .
2.  $\deg(PQ) = \deg(P) + \deg(Q)$ .

### Preuve.

1. Si  $P = Q = 0$ , alors  $P + Q = 0$  et le résultat est évident.

Sinon posons  $n = \max(\deg P, \deg Q) \in \mathbb{N}$ ; on peut alors écrire :  $P = \sum_{\alpha=0}^n a_{\alpha} X^{\alpha}$  et  $Q = \sum_{\alpha=0}^n b_{\alpha} X^{\alpha}$ , ce qui donne  $P + Q = \sum_{\alpha=0}^n (a_{\alpha} + b_{\alpha}) X^{\alpha}$  et prouve  $\deg(P + Q) \leq n$  de plus, le terme de degré  $n$  est  $a_n + b_n$ . Si  $\deg P \neq \deg Q$ , par exemple  $\deg P < \deg Q$ , alors  $a_n = 0$  et  $b_n \neq 0$ , et par suite  $a_n + b_n \neq 0$ , ce qui prouve que  $P + Q$  est de degré  $n$ .

2. Si  $P = 0$  ou  $Q = 0$ , alors  $PQ = 0$  et :  $\deg(PQ) = \deg(0) = -\infty = \deg P + \deg Q$ . car avec l'extension des opérations arithmétiques sur  $\overline{\mathbb{R}}$ , on a pour tout  $n \in \mathbb{N} \cup \{-\infty\}$  :  $n + (-\infty) = -\infty + n = -\infty$ .

Sinon, soit  $p_0 = \deg P$  et  $q_0 = \deg Q$ .

- Les coefficients de  $PQ$  d'indice strictement supérieur à  $p_0 + q_0$  sont nuls, ce qui donne  $\deg(PQ) \leq p_0 + q_0$ .

- Le coefficient de  $PQ$  d'indice  $p_0 + q_0$  vaut  $a_{p_0}b_{q_0}$  qui est donc non nul, puisque c'est le produit de deux éléments non nuls d'un corps. Donc  $\deg(PQ) = p_0 + q_0$ .

■

### Remarque 2.2

1. Si  $\lambda \in \mathbb{K}$  et  $A \in \mathbb{K}[X]$ , alors :  $\deg(\lambda A) = \begin{cases} \deg(A) & \text{si } \lambda \neq 0. \\ -\infty & \text{si } \lambda = 0. \end{cases}$
2. Si  $(\lambda, \mu) \in \mathbb{K}^2$  et  $(A, B) \in \mathbb{K}[X]^2$ , alors :  $\deg(\lambda A + \mu B) \leq \max(\deg A, \deg B)$ .

### Définition 2.4

Un polynôme est dit homogène de degré  $d \in \mathbb{N}$  si tous les monômes qui apparaissent avec un coefficient non nul ont même degré total.

### Exemple 2.2

Le polynôme  $4x^3 + 5x^2y - z^3$  est homogène dans  $\mathbb{K}[x, y, z]$ .

Le polynôme  $4x^3 + 5x^2y - z^6$  n'est pas homogène dans  $\mathbb{K}[x, y, z]$ .

### Définition 2.5

Nous appellerons composante homogène de degré  $d \in \mathbb{N}$  de  $P$ , notée  $P^{(d)}$ , la somme des termes de degré total  $d$  de  $P$ .

Voyons donc maintenant quelques propriétés des polynômes homogènes :

#### propriété 2.1

Un polynôme  $P \in \mathbb{F}_q[x_1, \dots, x_n]$  de degré total  $D \in \mathbb{N}$  se décompose de manière unique comme la somme de ses composantes homogènes non nulles. Autrement dit :  $P = \sum_{\{d, 0 \leq d \leq D: P^{(d)} \neq 0\}} P^{(d)}$ .

On appelle polynôme homogénéisé (ou simplement homogénéisé) de  $P$ , le polynôme :

$$\begin{aligned} F(x_1, \dots, x_n, z) &= \sum_{d=0}^D P^{(d)}(x_1, \dots, x_n) z^{D-d} \\ &= P^{(D)}(x_1, \dots, x_n) + P^{(D-1)}(x_1, \dots, x_n)z + \dots + P^{(0)}(x_1, \dots, x_n)z^D. \end{aligned}$$

Ce polynôme homogénéisé peut aussi être calculé en utilisant la formule :

$$F(x_1, \dots, x_n, z) = z^D \cdot P\left(\frac{x_1}{z}, \dots, \frac{x_n}{z}\right).$$

Remarquons que :  $F(x_1, \dots, x_n, 1) = P(x_1, \dots, x_n)$ .



**Exemple 2.3**

Soit  $P \in \mathbb{F}_q[x_1, x_2, x_3]$ ,  $P = 5x_1^3 + 6x_1x_2x_3 + 2x_1x_2^2 + 3$  et le degré totale  $D = 3$  pour  $d = 0$ ,  $P^{(0)} = 3$ ,  $d = 1$ ,  $P^{(1)} = 0$ ,  $d = 2$ ,  $P^{(2)} = 0$ ,  $d = 3$ ,  $P^{(3)} = 5x_1^3 + 6x_1x_2x_3 + 2x_1x_2^2$ .

$$\begin{aligned}
\text{Alors } P(x_1, x_2, x_3, z) &= \sum_{d=0}^3 P^{(d)}(x_1, x_2, x_3) z^{3-d} \\
&= P^{(0)}(x_1, x_2, x_3) z^3 + P^{(1)}(x_1, x_2, x_3) z^2 + P^{(2)}(x_1, x_2, x_3) z^1 + \\
&\quad P^{(3)}(x_1, x_2, x_3) z^0 \\
&= P^{(0)}(x_1, x_2, x_3) z^3 + P^{(3)}(x_1, x_2, x_3) z^0 \\
&= z^3 + 5x_1^3 + 6x_1x_2x_3 + 2x_1x_2^2.
\end{aligned}$$

**Définition 2.6**

Soit  $A = \mathbb{K}[x_1, \dots, x_n]$ , où  $\mathbb{K}$  est un corps commutatif. Un ordre monomial sur  $A$  est une relation  $>$  sur  $\mathbb{Z}_{n \geq 0}^n = \mathbb{N}_n$ , ou de manière équivalente, une relation  $>$  sur l'ensemble des monômes  $x^\alpha$  de  $A$ , avec  $\alpha \in \mathbb{Z}_{n \geq 0}^n$ , satisfaisant les trois conditions suivantes :

1.  $>$  est un ordre total sur  $\mathbb{Z}_{n \geq 0}^n$ .
2. Si  $\alpha > \beta$ , alors  $\alpha + \gamma > \beta + \gamma$ , avec  $\alpha, \beta, \gamma \in \mathbb{Z}_{n \geq 0}^n$ .
3.  $>$  est un bon ordre sur  $\mathbb{Z}_{n \geq 0}^n$ .

**Définition 2.7**

Soit  $A = \mathbb{K}[x_1, \dots, x_n]$ .

Soient  $P = a_dx^d + a_{d-1}x^{d-1} + \dots + a_1x + a_0$  un polynôme de  $A$ , où  $a_i \in \mathbb{K}$ ,  $a_d \neq 0$ , pour  $i = 1, \dots, n$  et  $t$  est un ordre monomial sur  $A$ .

Soit  $d$  le degré du polynôme, et noté  $\deg(P)$  Nous dirons que  $a_dx^d$  est le terme dominant de  $P$ , selon  $t$  et nous le noterons  $LT(P)$  (pour leading term). Nous dirons aussi que  $a_d$  est le coefficient dominant de  $P$ , selon  $t$  et nous le noterons  $LC(P)$  (pour leading coefficient). Finalement, nous dirons que  $x^d$  est le monôme dominant de  $P$ , selon  $t$  et nous le noterons  $LM(P)$  (pour leading monomial).

**Exemple 2.4**

Soit  $A = \mathbb{K}[x, y]$ , où  $\mathbb{K}$  est un corps commutatif.

Prenons le polynôme  $P = 5x^3y^2 - 6x^2y + 3y - 1$  de  $A$ .

Nous avons que  $LT(P) = 5x^3y^2$ ,  $LC(P) = 5$ , et  $LM(P) = x^3y^2$ .

### Définition 2.8

Soient  $\alpha = (\alpha_1, \dots, \alpha_n)$ ,  $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$ .

Nous dirons que  $\alpha >_{lex} \beta$  si, dans le vecteur différence  $(\alpha - \beta) \in \mathbb{Z}_{\geq 0}^n$ , la coordonnée non nulle la plus à gauche est positive. Si  $\alpha >_{lex} \beta$ , alors nous pourrions dire que  $x^\alpha >_{lex} x^\beta$ .

### Exemple 2.5

Soit  $A = \mathbb{K}[x, y, z]$ , où  $\mathbb{K}$  est un corps commutatif. Prenons le polynôme  $P = 4xy^2 + 2y^3z^4$  de  $A$ . Le premier terme de  $P$  est  $4xy^2$  avec  $\alpha = (1, 2, 0)$  et le deuxième terme de  $P$  est  $2y^3z^4$  avec  $\beta = (0, 3, 4)$ .

On obtient donc le vecteur différence  $(\alpha - \beta) = (1, -1, -4)$ . Puisque sa coordonnée non nulle la plus à gauche est positive, on a que  $\alpha >_{lex} \beta$ . C'est donc dire que  $4xy^2 >_{lex} 2y^3z^4$ .

### Proposition 2.2

*Soit  $g$  un polynôme non nul de  $\mathbb{K}[x]$ . Pour tout  $f \in \mathbb{K}[x]$ , il existe  $q, r \in \mathbb{K}[x]$  tels que  $f = qg + r$  avec  $q, r \in \mathbb{K}[x]$  et  $r = 0$  ou  $\deg(r) < \deg(g)$ . Les polynômes  $q$  et  $r$  sont uniques.*

### Preuve.

Si  $f = 0$  rien faire.

Si  $f \neq 0$ , on initialise :  $q = 0$ ;  $r = f$  si  $LT(g)$  divise  $LT(r)$  alors

$$q = q + LT(r)/LT(g)$$

$$r = r - (LT(r)/LT(g))g$$

On refait tant que  $r \neq 0$  et  $LT(r)/LT(g)$ .

■

### Définition 2.9

Soit  $A = \mathbb{K}[x_1, \dots, x_n]$ , où  $\mathbb{K}$  est un corps commutatif, et soient  $f, g$  deux polynômes de  $A$ .

Le plus petit commun multiple (*ppcm*) entre  $f$  et  $g$  est un polynôme  $h \in A$  tel que  $f \mid h$  et  $g \mid h$  et tel que si  $f \mid h'$  et  $g \mid h'$ , alors  $h \mid h'$ , avec  $h' \in A$ .  $f \mid h$  veut dire que  $f$  divise  $h$ , c'est-à-dire qu'il existe  $p \in A$  tel que  $h = fp$ .

Le plus petit commun multiple est déterminé à un multiple inversible près d'un élément de  $A$ .

### Exemple 2.6

Soit  $A = \mathbb{K}[x, y]$ , où  $\mathbb{K}$  est un corps commutatif.

Le *ppcm*( $2x^2y^3, x^3y$ ) est un polynôme de la forme  $ax^3y^3$ , où  $a$  est inversible dans  $A$ , c'est-à-dire que  $a$  est une constante non nulle.

Par convention, on prendra  $a = 1$ . Donc *ppcm*( $2x^2y^3; x^3y$ ) =  $x^3y^3$ .

### Définition 2.10

Un plus grand commun diviseurs des polynômes  $f_1, \dots, f_s \in \mathbb{K}[x]$  est un polynôme unitaire  $h$  tel que :

1.  $h$  divise  $f_1, \dots, f_s$ .
2. Si  $p$  divise  $f_1, \dots, f_s$  alors  $p$  divise  $h$ .

On écrit  $h = \Delta(f_1, \dots, f_s)$ .

### Proposition 2.3

Soient  $f_1, \dots, f_s$  des polynômes dans  $\mathbb{K}[x_1, \dots, x_n]$  alors :

1.  $\Delta(f_1, \dots, f_s)$  existe et il est unique.
2.  $\Delta(f_1, \dots, f_s)$  est un générateur de l'idéal  $\langle f_1, \dots, f_s \rangle$ .
3. Pour  $s \geq 3$ ,  $\Delta(f_1, \dots, f_s) = \Delta(f_1, \Delta(f_2, \dots, f_s))$ .
4. Il y a un algorithme pour obtenir  $\Delta(f_1, \dots, f_s)$  appelé algorithme d'Euclide.

## 2.2 S-polynôme

### Définition 2.11

Soit  $A = \mathbb{K}[x_l, \dots, x_n]$ , où  $\mathbb{K}$  est un corps commutatif et soient  $f, g$  deux polynômes non nuls de  $A$  et soit  $t$  un ordre monomial fixé. Le S-polynôme de  $f$  et  $g$  est, par définition,  $S(f, g) = \frac{ppcm(LM(f), LM(g))}{LT(f)} \cdot f - \frac{ppcm(LM(f), LM(g))}{LT(g)} \cdot g$ , où les  $LT$  et  $LM$  sont calculés selon  $t$ .

Le S-polynôme est utilisé, dans les calculs, afin d'annuler les termes dominants.

### Exemple 2.7

Soit  $A = \mathbb{K}[x_l, \dots, X_n]$ , où  $\mathbb{K}$  est un corps commutatif

Prenons  $f = x^3y^2 - x^2y^3 + x$  et  $g = 3x^4y + y^2$ , deux polynômes de  $A$

On peut calculer le S-polynôme de  $f$  et  $g$ , selon l'ordre lexicographique

$$S(f, g) = \frac{x^4y^2}{x^3y^2} \cdot (x^3y^2 - x^2y^3 + x) - \frac{x^4y^2}{3x^4y} \cdot (3x^4y + y^2) = -x^3y^3 + x^2 - \frac{1}{3}y^3.$$

## 2.3 Anneaux des polynômes sur un corps

### Définition 2.12

L'anneau des polynômes à coefficients dans  $\mathbb{K}$ , noté  $\mathbb{K}[X]$ , est l'ensemble des suites finies d'éléments de  $\mathbb{K}$ ,  $P = P(X) = (a_0, a_1, \dots, a_n)$ .

### Définition 2.13

Deux polynômes  $P(X) = (a_0, a_1, \dots, a_n) \in \mathbb{K}[X]$ ,  $Q(X) = (b_0, b_1, \dots, b_m) \in \mathbb{K}[X]$  (avec  $m \geq n$ ) sont égaux si  $a_i = b_i$  pour  $0 \leq i \leq n$  et  $b_j = 0$  pour  $n+1 \leq j \leq m$ , en particulier :

$$P(X) = (a_0, a_1, \dots, a_n) = \underbrace{(a_0, a_1, \dots, a_n, 0, 0, \dots, 0)}_{n+h \text{ éléments}}.$$

### Exemple 2.8

Soit les coefficients :

$$P(X) = (1, 2, 3) \in \mathbb{K}[X] \text{ et } Q(X) = (1, 2, 3, 0, 0) \in \mathbb{K}[X], \text{ donc } P(X) = Q(X).$$

**Notation 2.1** On adopte les notations classiques suivantes :

- Le polynôme  $(0, 0, \dots, 0)$  sera noté  $0$  et on a  $P(X) + 0 = 0 + P(X) = P(X)$  et  $0 \times P(X) = P(X) \times 0 = 0$ .
- Le polynôme  $(1, 0, 0, \dots, 0)$  sera noté  $1$  et on a  $1 \times P(X) = P(X) \times 1 = P(X)$ .
- Le polynôme  $P(X) = (0, 1, 0, \dots, 0)$  sera noté  $X$  et appelé l'indéterminée ou la variable.
- Le polynôme  $\underbrace{P(X) = (0, 1, 0, \dots, 0) \times \dots \times (0, 1, 0, \dots, 0)}_{n \text{ facteurs}}$  sera noté  $X^n$ .

**Définition 2.14**

L'addition et la multiplication munissent l'ensemble des polynômes en  $x_1, \dots, x_n$  d'une structure d'anneau commutatif intègre noté  $\mathbb{K}[x_1, \dots, x_n]$ .

Le corps des fractions de  $\mathbb{K}[x_1, \dots, x_n]$  est noté  $\mathbb{K}(x_1, \dots, x_n)$  et est appelé corps des fractions rationnels à  $n$  indéterminés :

$$\mathbb{K}(x_1, \dots, x_n) = \left\{ \frac{P}{Q} \mid P, Q \in \mathbb{K}[x_1, \dots, x_n], Q \neq 0 \right\}.$$

**La somme des polynômes**

**Définition 2.15**

Soit  $P(X) = (a_0, a_1, \dots, a_n) \in \mathbb{K}[X]$ ,  $Q(X) = (b_0, b_1, \dots, b_n) \in \mathbb{K}[X]$ .

On définit la somme  $P(X) + Q(X)$  par :

$$P(X) + Q(X) = R(X) = (c_0, c_1, \dots, c_n) = ((a_0 + b_0), (a_1 + b_1), \dots, (a_n + b_n)).$$

**La multiplication des polynômes**

**Définition 2.16**

Soit  $P(X), Q(X) \in \mathbb{K}[X]$ , On définit le produit  $P(X) \times Q(X) = P \cdot Q = PQ$  par :

$$P(X) \times Q(X) = (d_0, d_1, \dots, d_{m+n}) = ((a_0 b_0), (a_0 b_1 + a_1 b_0), \dots, \underbrace{(a_j b_0 + a_{j-1} b_1 + \dots + a_{j-k} b_k + \dots + a_0 b_j)}_{\text{avec } a_l=0 \text{ si } l>n, \ b_\lambda=0 \text{ si } \lambda>m}) + \dots + (a_n b_m)).$$

## Composition des polynômes

### Définition 2.17

Étant donnés  $P = \sum_{\alpha=0}^{\infty} a_{\alpha} x^{\alpha} \in \mathbb{K}[X]$  et  $A \in \mathbb{K}[X]$ , on définit :

$$P \circ A = P(A) = \sum_{\alpha=0}^{\infty} a_{\alpha} A^{\alpha} = \sum_{\alpha=0}^n a_{\alpha} A^{\alpha} \text{ pour tout } n \geq \deg(P).$$

### Racine d'un polynôme

### Définition 2.18

Soit  $P$  un polynôme à coefficient dans  $\mathbb{K}$ , un élément  $\alpha$  de  $\mathbb{K}$  est racine du polynôme si  $P(\alpha) = 0$ .

### Proposition 2.4

*Un élément  $\alpha$  de  $\mathbb{K}$  est racine de  $P$  si, et seulement si,  $(X - \alpha)$  divise  $P$ .*

**Preuve.** Le polynôme  $(X - \alpha)$  divise  $P$  si, et seulement si,  $P(\alpha)$  reste de la division euclidienne de  $P$  par  $(X - \alpha)$ , est nul. ■

### Définition 2.19 "Division euclidienne"

Si  $A(X)$  et  $B(X)$  sont deux polynômes de  $\mathbb{K}[X]$  ( $B \neq 0$ ) il existe un unique couple de polynômes  $Q(X)$  et  $R(X)$  tel que

$$A(X) = B(X)Q(X) + R(X) \text{ et } \begin{cases} \text{ou bien } R=0. \\ \text{ou bien } 0 \leq \deg(R) \leq \deg(B)-1. \end{cases}$$

On dit que  $B(X)$  est un diviseur de  $A(X)$  s'il existe  $Q(X) \in \mathbb{K}[X]$  tel que :

$$A(X) = B(X)Q(X), \text{ on note } B(X)|A(X).$$

On dit que deux polynômes non nuls  $A(X)$  et  $B(X)$  sont associés s'il existe  $a \in \mathbb{K}^*$  tel que  $A(X) = a \times B(X)$ .

Tout polynôme  $A(X) = a_0 + a_1X + \dots + a_nX^n$  a au moins comme diviseurs les éléments non-nuls de  $\mathbb{K}$  et lui-même car si  $a \neq 0 \in \mathbb{K}$  alors  $a^{-1}$  existe et on a  $A(X) = a((a_0a^{-1}) + (a_1a^{-1})X + \dots + (a_na^{-1})X^n)$ ,  $A(X) = 1 \times A(X)$ . Mais il peut en avoir d'autres par exemple :  $X^2 - 1 = (X - 1)(X + 1)$ .  $X^2 - 1$  a donc comme diviseurs les constantes non nulles ( $= \mathbb{K}^*$ ), les polynômes  $X - 1$  et  $X + 1$  à une constante multiplicative non nulle près et lui-même à une constante multiplicative non nulle près. Un polynôme,  $P(X)$ , est appelé une unité de  $\mathbb{K}[X]$  s'il est réduit à un élément de  $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ , autrement dit si  $P^{-1}$  existe dans  $\mathbb{K}[X]$ .

## Définition 2.20

Un polynôme  $P(X) \in \mathbb{K}[X]$  est appelé un polynôme premier ou polynôme irréductible si ses seuls diviseurs sont lui-même et les éléments de  $\mathbb{K}^*$ .

## Exemple 2.9

Dans  $\mathbb{Q}[X]$  le polynôme  $X^2 + 1$  est irréductible, par contre dans  $\mathbb{F}_2[X]$  il ne l'est pas car sur  $\mathbb{F}_2$  on a  $X^2 + 1 = (X + 1)^2$ .

## Proposition 2.5

Tout polynôme non nul  $A(X) \in \mathbb{K}[X]$  possède une décomposition en un produit de polynômes premiers  $A(X) = a \cdot P_1(X)P_2(X)\dots P_m(X)$  où  $a \in \mathbb{K}^*$ ,  $P_j(X)$  premier pour  $1 \leq j \leq m$ .

Cette décomposition est unique à l'unité  $a$  près et à l'ordre près des facteurs  $P_j$ . Si l'on regroupe tous les polynômes  $P_j$  associés, la décomposition en produit de polynômes premiers prend la forme suivante

$A(X) = a \cdot P_1(X)^{\alpha_1} P_2(X)^{\alpha_2} \dots P_\ell(X)^{\alpha_\ell}$ ,  $\alpha_i \in \mathbb{N}$ , où  $a \in \mathbb{K}^*$ ,  $P_j(X)$  premier pour  $1 \leq j \leq \ell$ ,  $P_i$  et  $P_j$  ne sont pas associés pour  $i \neq j$  sous cette forme la décomposition est unique à l'ordre des facteurs si on choisit les  $P_j$  unitaires et les  $\alpha_i \geq 1$  (c'est 'à dire qu'on s'interdit des exposants nuls).

**Preuve.** La preuve repose sur l'algorithme de division euclidienne, cf. [13]. ■

## Théorème 2.2 "Théorème de Bézout"

Soit  $A(X), B(X) \in \mathbb{K}[X]$ , alors il existe des polynômes  $U(X), V(X) \in \mathbb{K}[X]$  tels que :  $A(X)U(X) + B(X)V(X) = A(X) \wedge B(X) = D(X)$

**Preuve.**

On reprend l'algorithme du PGCD (13.12 cf[5]page 190-191) à partir de la fin. On écrit avec les notations précédentes

$$\begin{aligned} D &= R_{j+1} = R_{j-1} - Q_j R_j = R_{j-1} U_{j-1}(1) - R_j V_j(Q_j) \\ &= R_{j-1} - Q_j (R_{j-2} - Q_{j-1} R_{j-1}) \\ &= R_{j-1} (1 + Q_j Q_{j-1}) - Q_j R_{j-2} \\ &= -U_{j-2}(Q_j) R_{j-2} + R_{j-1} V_{j-1}(Q_{j-1}, Q_j) \\ &= (R_{j-3} - Q_{j-2} R_{j-2}) (1 + Q_j Q_{j-1}) - Q_j R_{j-2} \end{aligned}$$

$$\begin{aligned}
&= R_{j-3}(1 + Q_j Q_{j-1}) - R_{j-2}(Q_{j-2}(1 + Q_j Q_{j-1}) + Q_j) \\
d &= R_{j-3}U_{j-3}(Q_j, Q_{j-1}) - R_{j-2}V_{j-2}(Q_{j-2}, Q_{j-1}, Q_j) \\
&\vdots \\
&= (-1)^{j+1}aU_0(Q_1, \dots, Q_j) + (-1)^j bV_0(Q_0, \dots, Q_j) \\
\text{On a une relation de récurrence facile sur } U_j \text{ et } V_j \\
U_{j+1} &= U_{j-1} - Q_{j+1}U_j. \\
V_{j+1} &= V_{j-1} - Q_{j+1}V_j. \blacksquare
\end{aligned}$$

### Définition 2.21

Si  $P(X) \in \mathbb{K}[X]$  et si  $A(X), B(X)$  appartiennent à  $\mathbb{K}[X]$  on dit que  $A$  et  $B$  sont congrus modulo  $P$  s'il existe  $Q \in \mathbb{K}[X]$  tel que  $A - B = PQ$ . On écrira  $A \equiv B \pmod{P}$  et on dira que  $A$  et  $B$  appartiennent à la même classe d'équivalence modulo  $P$ .

### Proposition 2.6

*L'addition et la multiplication sont compatibles à la relation de congruence sur les polynômes ; autrement dit si  $P(X)$  est un polynôme fixé et si  $A(X), B(X) \in \mathbb{K}[X]$  alors :*

$$\begin{aligned}
((A(X) \pmod{P(X)}) + (B(X) \pmod{P(X)}) \pmod{P(X)}) &= (A(X) + B(X) \pmod{P(X)}). \\
((A(X) \pmod{P(X)}) \times (B(X) \pmod{P(X)}) \pmod{P(X)}) &= (A(X) \times B(X) \pmod{P(X)}).
\end{aligned}$$

**Preuve.** Pour la preuve cf. [13].  $\blacksquare$

## 2.4 Idéaux dans un anneau de polynôme à plusieurs variables

### Définition 2.22

Soit  $f_1, \dots, f_s \in \mathbb{K}[x_1, \dots, x_n]$ .

On note  $\langle f_1, \dots, f_s \rangle = \{p_1 f_1 + \dots + p_s f_s, p_i \in \mathbb{K}[x_1, \dots, x_n], i = 1, \dots, s\}$ .

#### Exemples

- $\langle 0 \rangle = \{0\}$ ,
- $\langle 1 \rangle = \mathbb{K}[x_1, \dots, x_n]$ ,
- $\langle x, y \rangle = \mathbb{K}[x, y] - \mathbb{K}^*$ ,



### Définition 2.23

Soit  $I \subset \mathbb{K}[x_1, \dots, x_n]$  un ensemble non vide.

L'ensemble  $I$  est un idéal de  $\mathbb{K}[x_1, \dots, x_n]$  si :

1.  $0 \in I$ .
2.  $\forall f, \forall g \in I, f + g \in I$ .
3.  $\forall f \in I, \forall p \in \mathbb{K}[x_1, \dots, x_n], pf \in I$ .

### Exemple 2.10

Dans  $\mathbb{K}[x, y]$ , les ensembles suivants sont des idéaux :  $\{0\}$ ,  $\mathbb{K}[x, y]$ ,  $\mathbb{K}[x, y] - \mathbb{K}^*$ .

### Lemme 2.1

Si  $f_1, \dots, f_s \in \mathbb{K}[x_1, \dots, x_n]$  alors l'ensemble  $\langle f_1, \dots, f_s \rangle = \{ \sum_{i=1}^s h_i f_i; h_1, \dots, h_s \in \mathbb{K}[x_1, \dots, x_n] \}$ , est un idéal de  $\mathbb{K}[x_1, \dots, x_n]$  appelé l'idéal engendré par  $f_1, \dots, f_s$  (c'est le plus petit idéal contenant  $f_1, \dots, f_s$ ).

### Preuve.

1.  $0 \in \langle f_1, \dots, f_s \rangle$  puisque  $0 = \sum_{i=1}^s 0 f_i$ .
2. Soit  $f = \sum_{i=1}^s p_i f_i, p_i \in \mathbb{K}[x_1, \dots, x_n]$  et  $g = \sum_{i=1}^s q_i f_i, q_i \in \mathbb{K}[x_1, \dots, x_n]$ .  
On a  $f + g = \sum_{i=1}^s (p_i + q_i) f_i \in \langle f_1, \dots, f_s \rangle$  car  $p_i + q_i \in \mathbb{K}[x_1, \dots, x_n]$ .
3. Soit  $h \in \mathbb{K}[x_1, \dots, x_n]$  on a  $hf = \sum_{i=1}^s (hp_i) f_i$  où  $hp_i \in \mathbb{K}[x_1, \dots, x_n]$ , donc  $hf \in \langle f_1, \dots, f_s \rangle$ .

■

## 2.4.1 Idéaux premiers

### Définition 2.24

Soit  $A = \mathbb{K}[x_1, \dots, x_n]$ , où  $\mathbb{K}$  est un corps commutatif. Un idéal  $I$  de  $A$  est dit idéal premier si et seulement si il satisfait les deux conditions suivantes :

1.  $I$  est un idéal propre de  $A$ , c'est-à-dire que  $I \neq A$ .
2. Si  $f \in A, g \in A$  et  $(f.g) \in I$ , alors ou bien  $f \in I$  ou bien  $g \in I$ .

## 2.4.2 Idéaux maximaux

### Définition 2.25

Soit  $A = \mathbb{K}[x_1, \dots, x_n]$ , où  $\mathbb{K}$  est un corps commutatif. Un  $I$  de  $A$  est dit idéal maximal si  $I \neq A$  et si tout idéal  $J$  de  $A$ , contenant  $I$  est tel que  $I = J$  ou bien  $J = A$ .

### Lemme 2.2

Soit  $A = \mathbb{K}[x_1, \dots, x_n]$ , où  $\mathbb{K}$  est un corps commutatif. Tout idéal  $I$  de  $A$ , de la forme  $I = \langle x_1 - a_1, \dots, x_n - a_n \rangle$  est un idéal maximal, avec  $a_1, \dots, a_n \in \mathbb{K}$ .

**Preuve.** Voir [4](Cox, 1996) page 198. ■

## 2.4.3 Idéaux monomiaux

### Définition 2.26

Soit  $A = \mathbb{K}[x_1, \dots, x_n]$ , où  $\mathbb{K}$  est un corps commutatif. Un idéal  $I$  de  $A$  est dit idéal monomial s'il existe un sous ensemble  $E \subset \mathbb{Z}_{n \geq 0}^n$ , possiblement infini, tel que l'idéal  $I$  est composé de tous les polynômes qui sont des sommes finies de la forme  $\sum_{e \in E} h_e x^e$ , où  $h_e \in A$ .

Dans ce cas, nous notons  $I = \langle x^e \mid e \in E \rangle$ .

## 2.4.4 Algorithme de division de polynômes

Soit  $A = \mathbb{K}[x_1, \dots, x_n]$ , où  $\mathbb{K}$  est un corps commutatif et soit  $t$  un ordre monomial sur  $A$  et soient  $f_1, \dots, f_s$  des éléments de  $A$ .

Prenons un polynôme  $f$  de  $A$ ,  $(f_1, \dots, f_s)$  une suite de polynômes de  $A$  et  $t$  un ordre monomial sur  $A$ . Calculons d'abord  $LT(f)$  et  $LT(f_i)$  pour  $i = 1, \dots, s$ , selon  $t$ .

Posons  $r = 0$  et  $a_1 = \dots = a_s = 0$ .

Trouvons le plus petit  $i$  tel que  $LT(f_i) \mid LT(f)$ , s'il existe. Alors  $LT(f_i) \mid LT(f)$  deviendra notre premiers terme de  $a_i$ . Cela fera en sorte que  $f := f - \frac{LT(f)}{LT(f_i)} f_i$  et  $a_i = a_i + \frac{LT(f)}{LT(f_i)}$ .

S'il n'existe pas de tel  $i$ , on a  $r := r + LT(f)$  et  $f := f - LT(f)$ . Recommençons tout, cette fois, avec notre nouveau polynôme  $f$ .

L'algorithme se terminera quand  $f = 0$ .

### Exemple 2.11

Soit  $A = \mathbb{K}[x, y]$ , où  $\mathbb{K}$  est un corps commutatif. Prenons  $f = xy^2 + 1 \in A$  et deux polynômes  $(xy + 1, y + 1)$  de  $A$ .

$LT(f) = xy^2$ ,  $LT(xy + 1) = xy$ ,  $LT(y + 1) = y$ , selon l'ordre lexicographique.

$LT(xy + 1) \mid LT(f)$ , puisque  $xy \mid xy^2 = y$ .

Donc  $a_1 = y$  et  $f := f - (y(xy + 1)) = -y + 1$ .

Prenons  $f = -y + 1$  et  $(xy + 1, y + 1)$ ,  $LT(f) = -y$ ,  $LT(xy + 1) = xy$ ,

$LT(y + 1) = y$ , selon l'ordre lexicographique.

$LT(xy + 1) \nmid LT(f)$ , puisque  $xy \nmid -y$ . Mais  $LT(y + 1) \mid LT(f)$ ,

puisque  $y \mid -y = -1$ . Donc  $a_2 = -1$  et  $f := f - (-1(y + 1)) = 2$ .

Prenons  $f = 2$  et  $(xy + 1, y + 1)$ ,  $LT(xy + 1) \nmid LT(f)$ , puisque  $xy \nmid 2$  et

$LT(y + 1) \nmid LT(f)$ , puisque  $y \nmid 2$ .

Donc  $r = 2$  et  $f = 0$ .

Nous avons terminé et nous obtenons

$f = xy^2 + 1 = y(xy + 1) - (y + 1) + 2$ .

### Définition 2.27

Soit  $A = \mathbb{K}[x_1, \dots, x_n]$  où  $\mathbb{K}$  est un corps commutatif et soit  $I$  un idéal non nul de  $A$ .

– Notons par  $LT(I)$  l'ensemble des termes dominants des éléments de  $I$ .

Autrement dit,  $LT(I) = \{a_d x^d \mid \text{il existe } f \in I \text{ avec } LT(f) = a_d x^d\}$ .

– Notons par  $\langle LT(I) \rangle$  l'idéal engendré par les éléments de  $LT(I)$ .

### Proposition 2.7

Soit  $A = \mathbb{K}[x_1, \dots, x_n]$  où  $\mathbb{K}$  est un corps commutatif et soit  $I$  un idéal non nul de  $A$ . On a que

–  $\langle LT(I) \rangle$  est un idéal monomial.

– Il existe  $f_1, \dots, f_s \in I$  tel que  $\langle LT(I) \rangle = \langle LT(f_1), \dots, LT(f_s) \rangle$ .

**Lemme 2.3**

Soient  $A = \mathbb{K}[x_1, \dots, x_n]$ , où  $\mathbb{K}$  est un corps commutatif et  $I = \langle x^e \mid e \in E \rangle$  un idéal monomial de  $A$ , où  $E$  est un sous ensemble de  $\mathbb{Z}_{\geq 0}^n$ , possiblement infini, tel que Vu dans la définition (2.26).

Alors, un monôme  $x^\beta$  est dans l'idéal  $I$  si et seulement si  $x^\beta$  est divisible par un  $x^e$ , pour  $e \in E$ .

**Théorème 2.3 "Théorème de base de Hilbert"**

*Soit  $A = \mathbb{K}[x_1, \dots, x_n]$ , où  $\mathbb{K}$  est un corps commutatif.*

*Tout idéal  $I$  de  $A$  a un nombre fini de générateurs. Il s'écrit sous la forme*

*$I = \langle f_1, \dots, f_s \rangle$ , pour  $f_1, \dots, f_s$  des éléments de  $I$ .*

**Preuve.**

Si  $I = \{0\}$ , on prendra l'ensemble de générateurs  $\{0\}$  qui est assurément fini, puisqu'il contient un seul élément.

Si  $I \neq \{0\}$  et si  $I$  contient des polynômes non nuls, alors un ensemble de générateurs  $\{f_1, \dots, f_s\}$  de  $I$  peut être construit de la manière suivante.

On sait, qu'il y a  $f_1, \dots, f_s \in I$  tels que  $\langle LT(I) \rangle = \langle LT(f_1), \dots, LT(f_s) \rangle$  Nous supposons que  $I = \langle f_1, \dots, f_s \rangle$ .

Il est évident que  $\langle f_1, \dots, f_s \rangle \subset I$ , puisque chaque  $f_i$  est dans  $I$ .

Inversement, soit un polynôme  $f \in I$ . Si nous appliquons l'algorithme de division de polynômes pour diviser  $f$  par  $(f_1, \dots, f_s)$ , alors nous obtenons une expression de la forme  $f = a_1 f_1 + \dots + a_s f_s + r$  où aucun terme de  $r$  n'est divisible par  $LT(f_1), \dots, LT(f_s)$ .

Nous supposons que  $r = 0$ . Pour montrer cela, notons que

$$r = f - a_1 f_1 - \dots - a_s f_s \in I.$$

Si  $r \neq 0$ , alors on aurait  $LT(r) \in \langle LT(I) \rangle = \langle LT(f_1), \dots, LT(f_s) \rangle$  et par le lemme (2.3), il s'ensuivrait que  $LT(r)$  devrait être divisible par un des  $LT(f_i)$  ce qui contredit la définition même du reste  $r$ . Par conséquent,  $r = 0$ .

Donc,  $f = a_1 f_1 + \dots + a_s f_s + 0 \in \langle f_1, \dots, f_s \rangle$ , ce qui montre que  $I \subset \langle f_1, \dots, f_s \rangle$ . ■

# Chapitre 3

## La cryptographie asymétrique

Du préfixe français «crypto» («kruptos» en grec) qui signifie «caché», et du suffixe «graphie» pour «écriture».

La cryptographie est la science qui utilise les mathématiques pour le cryptage et le décryptage de données.

### LEXIQUE :

- **Cryptanalyse** : l'art de retrouver un message clair à partir du message chiffré, sans connaître la clé.
- **Cryptologie** : science des messages secrets. Se décompose en Cryptographie + Cryptanalyse.
- **Cryptogramme** : message chiffré ou codé.
- **Cryptosystème** : ensemble regroupant les méthodes cryptographiques, les textes clairs, les textes chiffrés ainsi que toutes les clés possibles. (B.Schneier)
- **Décrypter** : action de retrouver le message clair à partir du message chiffré sans la clé.
- **Chiffrer=Crypter** : transformer un message afin qu'il ne soit lisible qu'à l'aide d'une clef.
- **Clef** : dans un système de chiffrement, elle correspond à un nombre, un mot, une phrase, etc. qui permet, grâce à l'algorithme de chiffrement, de chiffrer ou de déchiffrer un message.

## 3.1 Préambules mathématique

On appelle indicatrice d'Euler d'un entier  $n$  et on note  $\varphi(n)$  le nombre entiers compris entre 1 et  $n$  qui sont premiers avec  $n$

$$\varphi(n) = \text{card} \{j \in \{1..n\} : \text{pgcd}(j, n) = 1\}.$$

On a  $\varphi(1) = 1$  et pour un entier premier  $p$ ,  $\varphi(p) = p - 1$ ,

une méthode de calcul de  $\varphi(n)$  est de décomposer  $n$  en produit de facteurs premier

$$n = \prod_{p/n, p \text{ premier}} p^{\alpha_p} \text{ alors, } \varphi(n) = \prod_{p/n, p \text{ premier}} (p^{\alpha_p} - p^{\alpha_p-1}) = n \prod_{p/n, p \text{ premier}} \left(1 - \frac{1}{p}\right)$$

par exemple :  $\varphi(12) = (4 - 2) \times (3 - 1) = 12 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right)$ .

### Corollaire 3.1

Soit  $m \in \mathbb{N}$  et soit  $a \in \mathbb{N}$  tel que  $a \wedge m = 1$  alors le plus petit entier  $e \geq 1$  tel que  $a^e \equiv 1 \pmod{m}$  est un diviseur de  $\varphi(m)$ .

#### Preuve.

Supposons que  $e$  ne soit pas un diviseur de  $\varphi(m)$  et écrivons l'identité de la division euclidienne de  $\varphi(m)$  par  $e$

$\varphi(m) = e \times q + r$  avec  $0 < r \leq e - 1$  on a  $r \neq 0$  car  $e$  ne divise pas  $\varphi(m)$ . Alors

$$a^r = a^{\varphi(m) - eq} = a^{\varphi(m)} \times a^{-eq} = a^{\varphi(m)} \times (a^e)^{-q} \equiv 1 \pmod{m}$$

Or comme  $1 \leq r \leq e - 1$  ceci contredit la définition de  $e$ . ■

### 3.1.1 Identité de Bézout

si  $a$  et  $b$  sont premiers entre eux, il existe  $x$  et  $y$  tel que  $a \times x + b \times y = 1$ .

### 3.1.2 Congruences

On dit que «  $a$  est congru à  $b$  modulo  $n$  », et l'on note  $a \equiv b \pmod{n}$  si  $a$  peut s'écrire :

$$a = n \times q + b \text{ avec } 0 \leq b < n$$

- $r$  est le reste de la division de  $a$  par  $n$ .
  - $q$  est le quotient.
- ex :**  $15 = 7 \times 2 + 1$  donc  $15 \equiv 1[7]$ .

**Théorème 3.1**     *"Petit théorème de Fermat"*

Si  $p$  est un nombre premier et  $a \in \mathbb{Z}$  alors

$$a^p \equiv a \pmod{p}.$$

**Corollaire 3.2**     *Si  $p$  ne divise pas  $a$  alors*

$$a^{p-1} \equiv 1 \pmod{p}.$$

**Théorème 3.2**     *"Petit théorème de Fermat amélioré"*

Soient  $p$  et  $q$  deux nombres premiers distincts et soit  $n = p \times q$ . Pour tout  $a \in \mathbb{Z}$  tel que  $\text{pgcd}(a, n) = 1$  alors :

$$a^{(p-1)(q-1)} \equiv 1 \pmod{n}.$$

**Preuve.** Notons  $c = a^{(p-1)(q-1)}$ . Calculons  $c$  modulo  $p$  :

$c \equiv a^{(p-1)(q-1)} \equiv (a^{p-1})^{q-1} \equiv 1^{q-1} \equiv 1 \pmod{p}$  où l'on applique le petit théorème de Fermat :  $a^{p-1} \equiv 1 \pmod{p}$ , car  $p$  ne divise pas  $a$ . Calculons ce même  $c$  mais cette fois modulo  $q$  :

$c \equiv a^{(p-1)(q-1)} \equiv (a^{q-1})^{p-1} \equiv 1^{p-1} \equiv 1 \pmod{q}$ , où l'on applique le petit théorème de Fermat :  $a^{q-1} \equiv 1 \pmod{q}$ , car  $q$  ne divise pas  $a$ . Conclusion partielle :  $c \equiv 1 \pmod{p}$  et  $c \equiv 1 \pmod{q}$ . Nous allons en déduire que  $c \equiv 1 \pmod{pq}$ . Comme  $c \equiv 1 \pmod{p}$  alors il existe  $\alpha \in \mathbb{Z}$  tel que  $c = 1 + \alpha p$ ; comme  $c \equiv 1 \pmod{q}$  alors il existe  $\beta \in \mathbb{Z}$  tel que  $c = 1 + \beta q$ . Donc  $c - 1 = \alpha p = \beta q$ . De l'égalité  $\alpha p = \beta q$ , on tire que  $p \mid \beta q$ . Comme  $p$  et  $q$  sont premiers entre eux (car ce sont des nombres premiers distincts) alors par le lemme de Gauss on en déduit que  $p \mid \beta$ . Il existe donc  $\beta' \in \mathbb{Z}$  tel que  $\beta = \beta' p$ . Ainsi  $c = 1 + \beta q = 1 + \beta' p q$ . Ce qui fait que  $c \equiv 1 \pmod{pq}$ , c'est exactement dire  $a^{(p-1)(q-1)} \equiv 1 \pmod{n}$ . ■

### 3.1.3 L'exponentiation rapide

Nous aurons besoin de calculer rapidement des puissances modulo  $n$ . Pour cela il existe une méthode beaucoup plus efficace que de calculer d'abord  $a^k$  puis de le réduire modulo  $n$ . Il faut garder à l'esprit que les entiers que l'on va manipuler ont des dizaines voir des centaines de chiffres.

Voyons la technique sur l'exemple de  $5^{11} \pmod{14}$ . L'idée est de seulement calculer  $5, 5^2, 5^4, 5^8 \dots$  et de réduire modulon à chaque fois. Pour cela on remarque

que  $11 = 8 + 2 + 1$ . Donc  $5^{11} = 5^8 \times 5^2 \times 5^1$ .

Calculons donc les  $5^{2^i} \equiv \pmod{14}$  :

$$5 \equiv 5 \pmod{14}$$

$$5^2 \equiv 25 \equiv 11 \pmod{14}$$

$$5^4 \equiv 5^2 \times 5^2 \equiv 11 \times 11 \equiv 121 \equiv 9 \pmod{14}$$

$$5^8 \equiv 5^4 \times 5^4 \equiv 9 \times 9 \equiv 81 \equiv 11 \pmod{14}$$

à chaque étape est effectuée une multiplication modulaire. Conséquence :

$$5^{11} \equiv 5^8 \times 5^2 \times 5^1 \equiv 11 \times 11 \times 5 \equiv 11 \times 55 \equiv 11 \times 13 \equiv 143 \equiv 3 \pmod{14}.$$

Nous obtenons donc un calcul de  $5^{11} \pmod{14}$  en 5 opérations au lieu de 10 si on avait fait  $5 \times 5 \times 5 \dots$ .

## 3.2 L'arithmétique pour RSA

Le système RSA est nommé d'après le nom de ses inventeurs : Rivest, Shamir, Adleman en 1978.

Pour un entier  $n$ , sachant qu'il est le produit de deux nombres premiers, il est difficile de retrouver les facteurs  $p$  et  $q$  tels que  $n = p \times q$ . Le principe du chiffrement RSA, chiffrement à clé publique, repose sur cette difficulté. Dans cette partie nous mettons en place les outils mathématiques nécessaires pour le calcul des clés publique



et privée ainsi que les procédés de chiffrement et déchiffrement RSA.

### 3.2.1 Description du cryptosystème RSA :

On a un ensemble  $(A_i)_{i \in I}$  de correspondants (personnes physiques ou ordinateurs). le principe du cryptosystème RSA est le suivant

#### Principe de RSA

- On choisit 2 grand nombre premiers  $p$  et  $q$ .
- On calcule  $n = p \times q$ , ce sera le module.
- On prend  $e$ , premier avec  $(p - 1) \times (q - 1)$ , ce sera l'exposant.
- On peut alors calculer  $d$  tel que  $e \times d = 1 \bmod (p - 1) * (q - 1)$
- $(n, e)$  est la clé publique.
- $(n, d)$  est la clé privée.
- **Chiffrement**
  - Pour un message  $M < n$ .
  - $C = M^e \bmod n$ .
- **Déchiffrement**
  - Pour un message chiffré  $C$ .
  - $M = C^d \bmod n$ .
- **Décryptage**
  - Si on veut calculer  $d$  avec  $e$  et  $n$ , il nous faut  $p$  et  $q$  C'est à dire factoriser  $n$ , ce qui est très difficile.
- **Comment ça marche ?**

Posons  $C = M^e \bmod n$  et  $M = C^d \bmod n$ . On a alors :

$$C^d \equiv (M^e)^d \bmod n \equiv M^{e \times d} \bmod n, \text{ or } e \times d \equiv 1 \bmod (\varphi n),$$

$$\text{donc } e \times d \equiv k \times \varphi(n) + 1.$$

$$\text{Alors } C^d \equiv M^{k \times \varphi(n) + 1} \bmod n \equiv M \times \underbrace{(M^{\varphi(n)})}_{\text{Euler+ Fermat} \hookrightarrow \equiv 1 \bmod n} \bmod n \equiv M \bmod n$$

### 3.2.2 Protocole d'envoi d'un message en RSA :

Alice veut envoyer un message  $\mathcal{M}$  à Bob . La clef publique d'Alice (resp Bob ) est  $(n_a, e_a)$ , (*resp.*  $(n_b, e_b)$ ), sa clef secrète est  $(p_a, q_a, d_a)$  (*resp.*  $(p_b, q_b, d_b)$ ).

Elle suit le protocole suivant :

1. Alice commence par transformer le message en une suite de chiffres, par exemple en remplaçant les lettres et les différents symboles utilisés par des chiffres.
2. Alice regarde dans l'annuaire public la clé de chiffrement  $n_b, e_b$  de Bob . Elle découpe le message  $\mathcal{M}$  en blocs  $\mathcal{M}$  de taille approximativement  $n_b$ .
3. Elle calcule

$$f_b(M) = M^e \equiv M^{e_b} \text{ mod } n_b,$$

et envoie  $M^e = f_b(M)$  à Bob.

4. Pour récupérer le texte en clair Bob calcule

$$f_b^{-1}(M^e) = (M^e)^{d_b} = f_b(M)^{d_b} \equiv M^{e_b d_b} = M^{1+k_b \varphi(n_b)} \text{ mod } n_b.$$

D'après le théorème d'Euler on a

$$M^{\varphi(n_b)} \equiv 1 \text{ mod } n_b.$$

Et par conséquent

$$f_b^{-1}(M^e) \equiv M \text{ mod } n_b.$$

Si la taille de  $M$  est adaptée à celle de  $n_b$ , il n'y a pas d'ambiguïté, et Bob récupère donc bien le message d'Alice.

### Exemple 3.1

1. Prenons  $p = 53$  et  $q = 97$ .
2. Prenons  $e = 7$  (premier avec  $52 \times 96$ ).
3. Nous avons  $n = 53 \times 97 = 5141$ .
4.  $M = \text{BONJOUR} = 2 \quad 15 \quad 14 \quad 10 \quad 15 \quad 21 \quad 18$ .
5. On découpe  $M = 2 \ 151 \ 410 \ 152 \ 118$ .

- $C1 = 2^7 \bmod 5141$ .
- $C2 = 151^7 \bmod 5141$ .
- $C3 = 401^7 \bmod 5141$ .
- $C4 = 152^7 \bmod 5141$ .
- $C5 = 118^7 \bmod 5141$ .

### 3.3 El Gamal

Le cryptosystème El Gamal est basée sur la fonction à sens unique logarithme discret. On considère un groupe cyclique fini,  $G$ , de cardinal  $n$  engendré par un générateur,  $g$ . Donc  $G = \{g^i \mid 0 \leq i \leq n-1\}$ .

On suppose que le calcul de  $g^i$  est “facile”, “rapide” “calculatoirement facile” (c’est à dire faisable en temps polynomial en fonction de la taille des données) mais que le calcul de  $i$  connaissant  $g^i$  n’est “pas facile”, est “lent”, “calculatoirement difficile” (c’est à dire : n’est pas faisable en temps polynomial en fonction de la taille des données). Si  $a = g^i$ ,  $i$  est appelé le logarithme discret de  $a$ .

#### 3.3.1 Description du cryptosystème El Gamal

On considère le cryptosystème suivant : Soit  $p$  un nombre premier tel que le problème du logarithme discret dans  $\mathbb{Z}/p\mathbb{Z}$  soit difficile. Soit  $g$  une racine primitive modulo  $p$ , (cf.[5] le théorème (13.3.17 page 172)), c’est à dire que  $g$  est un générateur du groupe cyclique  $(\mathbb{Z}/p\mathbb{Z})^*$ .

Soit  $\mathcal{P} = (\mathbb{Z}/p\mathbb{Z})^*$ , les messages en clair, et soit  $\mathcal{C} = (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^*$  les messages cryptés et enfin soit l’espace des clefs.

$$\mathcal{K}_b = \{(p, g, \alpha, \beta); \beta \equiv g^\alpha \bmod p\} \text{ où } \begin{cases} (p, g, \beta) \text{ est la clef publique.} \\ \alpha \text{ est la clef secrète.} \end{cases}$$

Alice veut transmettre un message  $\mathcal{M}$ , à Bob.

1. Bob choisit un grand nombre premier  $p_b$ , un générateur  $g_b$  du groupe cyclique multiplicatif  $\mathbb{Z}/p_b\mathbb{Z}$  et un entier  $\alpha_b$  inférieurs à  $p_b - 1$ .
2. Bob calcule  $\beta_b = g_b^{\alpha_b}$ ; alors le triplet  $(p_b, g_b, \beta_b)$  constitue sa clef publique,  $\alpha_b$  est sa clef secrète.

3. Alice découpe le message  $\mathcal{M}$  en blocs  $M$  de taille inférieure à  $p_b$ , elle choisit un entier  $k_a$  (inférieur à  $p_b - 1$ ) pour chacun des blocs  $M$  et calcule  $y_1 \equiv g_b^{k_a} \pmod{p_b}$  et  $y_2 = \beta_b^{k_a} M$ .

La paire  $e_{K_b}(M, k_a) = (y_1, y_2)$  est le message codé qu'Alice envoie à Bob.

Pour décoder

Bob calcule  $M \equiv y_2(y_1^{\alpha_b})^{-1} \pmod{p_b}$ , comme  $y_1^{\alpha_b} = g_b^{k_a \alpha_b} \pmod{p_b}$  on a :

$d_K(y_1, y_2) = y_2(y_1^{\alpha_b})^{-1} \equiv \beta_b^{k_a} M (g_b^{k_a \alpha_b})^{-1} \equiv g_b^{\alpha_b k_a} M g_b^{-\alpha_b k_a} \equiv M \pmod{p_b}$  et comme  $M$  est inférieur à  $p_b$  il n'y a pas d'ambiguïté dans le décodage. Pour une bonne sécurité, Alice doit changer souvent  $k_a$ .

### Exemple 3.2

Alice et Bob veulent correspondre en employant le système El-Gamal. Alice choisit comme paramètres :  $p_a = 263$ ,  $g_a = 5$ ,  $\alpha_a = 47$ . Bob choisit comme paramètres  $p_b = 257$ ,  $g_b = 5$ ,  $\alpha_b = 67$ .

On vérifie facilement que  $p_a$  et  $p_b$  sont des nombres premiers, que  $g_a$  et  $g_b$  sont respectivement des générateurs des groupes cycliques  $\mathbb{Z}/p_a\mathbb{Z}$  et  $\mathbb{Z}/p_b\mathbb{Z}$ . Il suffit pour cela de vérifier (par exemple à l'aide d'une table ou d'un système de calcul faisant de l'arithmétique modulaire) que  $\begin{cases} g_a^e \not\equiv 1 \pmod{p_a} & \forall 1 < e < p_a - 1 \text{ divisant } p_a - 1. \\ g_b^e \not\equiv 1 \pmod{p_b} & \forall 1 < e < p_b - 1 \text{ divisant } p_b - 1. \end{cases}$

En effet d'après le corollaire (3.1) le plus petit entier non nul  $e$  tel que  $g_a^e \equiv 1 \pmod{p_a}$  est un diviseur de  $p_a - 1$ . Ici  $p_a - 1 = 262 = 2 \times 131$ , donc il suffit de vérifier que  $g_a^{131} \not\equiv 1 \pmod{263}$  et  $p_b - 1 = 256 = 2^8$ , donc il suffit de vérifier que  $g_b^{128} \not\equiv 1 \pmod{257}$ . Alice calcule  $\beta_a = p_a^{\alpha_a} \pmod{p_a} = 40$  et sa clef publique est  $K_a = (p_a = 263, g_a = 5, \beta_a = 40)$  et sa clé secrète est  $\alpha_a = 47$ .

Bob calcule  $\alpha_b = p_b^{\alpha_b} \pmod{p_b} = 201$  et sa clef publique est  $K_b = (p_b = 257, g_b = 5, \beta_b = 201)$  et sa clé secrète est  $\alpha_b = 67$ .

# Chapitre 4

## Protocole cryptographique asymétrique sur l'anneau de polynômes à plusieurs variables

### 4.1 Transformations affines

#### Définition 4.1

Soient  $n, m \in \mathbb{N} - \{0\}$ , une application  $T : \mathbb{R}^n \rightarrow \mathbb{R}^m$  est appelée transformation linéaire si elle satisfait les deux conditions suivantes :

1.  $T(u + v) = T(u) + T(v)$ .
2.  $T(\alpha u) = \alpha T(u)$ .

Pour tous  $u, v \in \mathbb{R}^n$  et tout  $\alpha \in \mathbb{R}$  Intuitivement, ces conditions signifient que la structure d'espace vectoriel est préservée en passant de  $\mathbb{R}^n$  à  $\mathbb{R}^m$  par l'application  $T$ .

Une transformation affine  $f$  s'obtient en combinant la transformation linéaire  $T$  avec une translation du vecteur  $\vec{b} \in \mathbb{R}^m$  i.e.  $f = T + \vec{b}$ .

Une transformation affine  $f$  agit sur les points de l'espace affine. À tout point  $M$  de l'espace elle associe un point  $M'$  tel que  $f(M) = M'$ .

#### Exemple 4.1

Soit  $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$  une transformation affine, Soit  $(O, \vec{i}, \vec{j}, \vec{k})$  le repère,  $(x, y, z)$  les coordonnées du point  $M$ ,  $(x', y', z')$  les coordonnées du point  $M'$  et

$\vec{b} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} \in \mathbb{R}^3$ . On a  $f(M) = M'$  si, et seulement si  $\overrightarrow{OM'} = f(\overrightarrow{OM}) + \vec{b}$  ce qui donne sous forme matricielle :

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}.$$

## 4.2 Principe général

Nous décrivons de manière générale les trois opérations fondamentales en cryptographie multivariée à clé publique.

### Génération des clés publiques et privées :

Soit  $\mathcal{F}$  une application définie comme :

$$\begin{aligned} \mathcal{F} &: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m \\ (v_1, \dots, v_n) &\mapsto (f_1(v_1, \dots, v_n), \dots, f_m(v_1, \dots, v_n)), \end{aligned}$$

avec  $\{f_1, \dots, f_m\} \in \mathbb{F}_q[x_1, \dots, x_n]$ . Les polynômes  $f_1, \dots, f_m$  sont en général de degré 2 et le système sera muni d'une certaine structure.

Ainsi, il faudra publier une version « masquée » du système. On définit  $Aff_n(\mathbb{F}_q) \simeq GL_n(\mathbb{F}_q) \times \mathbb{F}_q^n$  comme l'ensemble des transformations affines inversibles de  $\mathbb{F}_q^n$ .

Soient deux transformations  $\mathcal{S} \in Aff_n(\mathbb{F}_q)$  et  $\mathcal{T} \in Aff_n(\mathbb{F}_q)$ . On construit l'application  $\mathcal{G} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$  définie comme :

$$\begin{aligned} \mathcal{G} &: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m \\ (v_1, \dots, v_n) &\mapsto (g_1(v_1, \dots, v_n), \dots, g_m(v_1, \dots, v_n)), \end{aligned}$$

avec  $\{g_1, \dots, g_m\} \in \mathbb{F}_q[x_1, \dots, x_n]$ . Les polynômes  $g_1, \dots, g_m$  sont de même degré que les polynômes  $f_1, \dots, f_m$ .

Soit  $(\mathbf{S}, \underline{s}) \in GL_n(\mathbb{F}_q) \times \mathbb{F}_q^n$  (resp.  $(\mathbf{T}, \underline{t}) \in GL_n(\mathbb{F}_q) \times \mathbb{F}_q^m$ ) le couple représentant l'application  $\mathcal{S}$  (resp.  $\mathcal{T}$ ) alors on construit :

$$(g_1, \dots, g_m) = (f_1(x'_1, \dots, x'_n), \dots, f_m(x'_1, \dots, x'_n)) \mathbf{T} + \underline{t};$$

avec  $(x'_1, \dots, x'_n) = (x_1, \dots, x_n) \mathbf{S} + \underline{s}$ . Les données privées sont les applications  $\mathcal{F}$ ,  $\mathcal{S}$  et  $\mathcal{T}$  et la clé publique l'application  $\mathcal{G}$ . L'idée est de masquer la structure de  $\mathcal{F}$  avec les applications  $\mathcal{S}$  et  $\mathcal{T}$ . On pourra aussi utiliser des transformations linéaires pour  $\mathcal{S}$  et  $\mathcal{T}$ .

### Chiffrement :

Dans un schéma multivarié, les messages vivent dans l'espace vectoriel  $\mathbb{F}_q^n$  et les chiffrés dans  $\mathbb{F}_q^m$ . Pour chiffrer un message  $\underline{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ , il suffit de calculer

$$\underline{c} \in \mathbb{F}_q^m = (c_1, \dots, c_m) = (g_1(a_1, \dots, a_n), \dots, g_m(a_1, \dots, a_n)).$$

Le nombre d'opérations nécessaires pour chiffrer un message dépend du degré des polynômes publics  $g_1, \dots, g_m$ .

### Déchiffrement :

Le possesseur de la clé secrète peut déchiffrer  $\underline{c} \in \mathbb{F}_q^m$  en inversant séparément chaque application qui compose la clé publique. Soient  $\mathcal{F}$ ,  $\mathcal{S}$ ,  $\mathcal{T}$  la clé privée correspondant à  $\mathcal{G}$ . On a bien que

$$\underline{a} = \mathcal{G}^{-1}(\underline{c}) = \mathcal{S}^{-1} \circ \mathcal{F}^{-1} \circ \mathcal{T}^{-1}(\underline{c}).$$

L'application  $\mathcal{F}$  est munie d'une certaine structure qui va permettre un déchiffrement efficace. On peut noter que le déchiffrement ne peut être unique que si  $m \geq n$ . En général, le nombre d'opérations nécessaires pour le déchiffrement dépend de la trappe choisie pour construire l'application  $\mathcal{F}$ .

### Exemple 4.2

On considère les trois applications :

$$\mathcal{F} : \mathbb{R}^2 \rightarrow \mathbb{R}^2, (x, y) \mapsto (x + y, 2y) \text{ et } \mathcal{S} : \mathbb{R}^2 \rightarrow \mathbb{R}^2, (x, y) \mapsto (x + 2, y + 3)$$

$$\text{On a } \mathcal{S}(x, y) = S \begin{pmatrix} x \\ y \end{pmatrix} + \underline{s} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix}.$$

$\mathcal{T} : \mathbb{R}^2 \rightarrow \mathbb{R}^2, (x, y) \mapsto (x + 4, y + 5).$

On a  $\mathcal{T}(x, y) = T \begin{pmatrix} x \\ y \end{pmatrix} + \underline{t} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 4 \\ 5 \end{pmatrix}.$

On calcul,  $(x', y') = (x, y)S + \underline{s} = (x + 2, y + 3).$

Soit l'application  $\mathcal{G} : \mathbb{R}^2 \rightarrow \mathbb{R}^2,$

$(x, y) \mapsto (g_1(x, y), g_2(x, y)) = (f_1(x', y'), f_2(x', y'))T + \underline{t}$

$= (x + y + 5, 2y + 6) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 4 \\ 5 \end{pmatrix}$

$\mathcal{G}(x, y) = (x + y + 9, 2y + 11).$

### Chiffrement

On considère  $\underline{a} = (1, -1)$ , par suite  $\underline{c} = \mathcal{G}(1, -1) = (9, 9).$

### Déchiffrement

On calcule  $(\mathcal{S}^{-1} \circ \mathcal{F}^{-1} \circ \mathcal{T}^{-1})(9, 9).$

On a  $\mathcal{T}^{-1} : \mathbb{R}^2 \rightarrow \mathbb{R}^2, (x, y) \mapsto (x - 4, y - 5).$

Donc  $\mathcal{T}^{-1}(9, 9) = (5, 4).$

$\mathcal{F}^{-1} : \mathbb{R}^2 \rightarrow \mathbb{R}^2, (x, y) \mapsto (x - \frac{1}{2}y, \frac{1}{2}y), \mathcal{F}^{-1}(5, 4) = (3, 2).$

$\mathcal{S}^{-1} : \mathbb{R}^2 \rightarrow \mathbb{R}^2, (x, y) \mapsto (x - 2, y - 3), \mathcal{S}^{-1}(3, 2) = (1, -1).$

Finalement  $(\mathcal{S}^{-1} \circ \mathcal{F}^{-1} \circ \mathcal{T}^{-1})(\underline{c}) = (\mathcal{S}^{-1} \circ \mathcal{F}^{-1} \circ \mathcal{T}^{-1})(9, 9) = \underline{a} = (1, -1).$

Le concept de chiffrement à clef publique repose sur la notion de fonction à sens unique avec trappe. Intuitivement, une fonction à sens unique avec trappe est une fonction facile à calculer, mais difficile à inverser, sauf lorsque l'on connaît une information supplémentaire (la trappe).

## 4.3 Exemples de trappes

Nous présentons brièvement les principales familles de trappes que l'on trouve en cryptographie multivariée. Celles-ci ont été répertoriées notamment par C. Wolf par exemple dans [Wol05, WP05c].



### Systèmes triangulaires :

Dans cette famille, le système secret  $f_1, \dots, f_m$  a une structure qui permet d'inverser  $\mathcal{F}$  composante par composante. Soit  $n = m$ , on considère

$$\left\{ \begin{array}{l} f_1(x_1, \dots, x_n), \\ f_2(x_2, \dots, x_n), \\ \vdots \\ f_{m-1}(x_{n-1}, x_n), \\ f_m(x_n). \end{array} \right.$$

Inverser le système consiste à trouver une racine du polynôme univarié  $f_m$  puis étape par étape on spécialise la valeur de  $x_n$  dans le polynôme  $f_{m-1}$  et ainsi de suite jusqu'à  $f_1$ . Ce principe peut se généraliser : à chaque étape, on résout un petit nombre d'équations en un petit nombre de variables qui peuvent éventuellement posséder une trappe.

#### 4.3.1 Extension de corps

L'idée dans cette famille de trappes est d'utiliser un morphisme  $\varphi$  entre le corps  $\mathbb{F}_{q^n}$  et l'espace vectoriel  $\mathbb{F}_q^n$ . Ainsi, on construit une application  $\mathcal{F}^*$  facile à inverser dans  $\mathbb{F}_{q^n}$  et on publie l'application vue dans  $\mathbb{F}_q^n$  masquée par les transformations  $\mathcal{S}$  et  $\mathcal{T}$ .

L'exemple historique utilisant cette construction est le schéma  $C^*$  de Matsumoto et Imai [MI88]. Dans ce schéma, on a  $m = n$  et on construit une application  $\mathcal{F}^*$  dans l'extension  $\mathbb{F}_{q^n}$ .  $\mathcal{F}^* : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n}$ ,  $V \mapsto V^{1+q^i}$ , telle que  $\gcd(1+q^i, q^n-1) = 1$ . Il faut donc choisir pour  $q$  une puissance de 2. Grâce à cette structure, on peut facilement inverser l'application puisque  $\mathcal{F}^{*-1}(X) = X^t$  avec  $t(1+q^i) \equiv 1 \pmod{q^n-1}$ . On obtient finalement l'application dans le petit corps  $\mathcal{F} = \varphi \circ \mathcal{F}^* \circ \varphi^{-1}$  qu'on peut voir comme l'évaluation d'un système  $(f_1, \dots, f_n) \subset (\mathbb{F}_q[x_1, \dots, x_n])^n$  d'équations de degré 2. En effet, la mise à la puissance  $q^i$  est linéaire sur  $\mathbb{F}_q$ . Par conséquent  $X^{1+q^i}$  se transforme en système quadratique.

# Conclusion

Ce mémoire de master Algèbre et Mathématiques discrètes s'inscrit dans le cadre de la théorie des anneaux de polynômes à plusieurs variables et leurs applications en cryptographie asymétrique.

On donne tout d'abord des notions générales sur les anneaux et les corps. Par suite, on fait une étude sur l'anneau de polynômes à plusieurs variables. D'autre part, nous avons étudié la cryptographie asymétrique. Enfin, on s'intéresse au protocole cryptographique asymétrique sur l'anneau de polynômes à plusieurs variables..

# Bibliographie

- [1] **A. Khelili**, Mémoire pour l'oboration du diplome de magister en Mathématiques intitulé Base de gröbner, Université d'oran, le 30 janvier 2013.
- [2] **B. Magalie**, Travaux d'Etudes et de Recherches :CRYPTOGRAPHIE, le 11 juin 2005, [http ://mp.cpgedupuydelome.fr](http://mp.cpgedupuydelome.fr).
- [3] **D. Cox, J. Little, D. O'Shea**, Undergraduate texts in Mathematics, Springer 1997.
- [4] **D. Cox, J. Little et D. O'Shea**. 1996. Ideals, VaTieties, and Algorithms, An Introduction to Computational Algebraic Geometry and Commutative Algebra. Springer. Second Edition.
- [5] **D. Barsky & G. Dartois**, Cours Cryptographie, Paris 13(version 2010/2011), le 1 octobre 2010.
- [6] **D. Delaunay**, Cours Mathématiques MP, 1<sup>er</sup> mai 2015.
- [7] **D. Mihoubi**, Cours de cryptographie, 2018/2019.
- [8] **[ElG85] :T. ElGamal**. A public key cryptosystem and a signature scheme based on discrete logarithms. In Advances in Cryptology, volume 196 of Lecture Notes in Computer Science, pages 10–18. Springer, 1985.
- [9] **F. Moulin, JF. Ruaud, A.Miquel, J-C.Sirfe**, Mathématiques tout-en-un 1<sup>er</sup>année, DUNOD 2<sup>e</sup> édition.
- [10] **J-Ch. Faugère**, Calcul efficace des bases de Gröbner et Applications, February 9, 2007.
- [11] **K. Hossen et F. Duchene**, Introduction à la cryptographie, Ecole nationale superieure d'informatique et de mathématiques appliquées de grenoble, 2011.

- [12] **L. Ladjlat**, *Cours Master1, Les anneaux*, Université M.Boudiaf de Msila. Année univ 2017-2018.
- [13] **L. MARCOTTE**, Mémoire présenté comme exigence partielle de la maîtrise en mathématiques, Université du québec à Montréal, Avril 2008.
- [14] **L. Schwartz**, Mathématiques pour la Licence, Algèbre, Dunod, Paris, 1998.
- [15] **L. Perret**, Étude d'outils algébriques et combinatoires pour la cryptographie à clef publique, Thèse, Université de Marne-la-Vallée, le 17 Octobre 2005.
- [16] **L. Bettale**, Cryptanalyse algébrique (outils et applications), Thèse, l'Université Pierre et Marie Curie - Paris 6, le 3 Octobre 2011.
- [17] **N. Perrin**, Algèbre effective, Université de Versailles Saint-Quentin-en-Yvelines, Année 2017-2018.
- [18] **[RSA78] :Ronald L. Rivest, A.Shamir, and L.Adleman**. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2) :120–126, 1978.
- [19] **W. Adams et P. Loustau**, An introduction to Gröbner bases, Graduate studies in Mathematics 3 AMS, 1994.