

Remerciements

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

Je tiens à exprimer mes sentiments respectueux à mes chers parents à qui je dédie ce travail pour leur grand soutien.

Je remercie particulièrement mon directeur de thèse Monsieur Nacer Ghadbane, pour toute l'aide qu'il m'a apporté et leur patience leurs conseils et pour avoir guidé ce travail avec beaucoup d'intérêt.

Remercie également les professeurs Mr.D. MIHOUBI, Mr.L. HEBOUB qui m'ont fait l'honneur d'être membres du jury.

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

Enfin, mes remerciements s'adressent à tous les enseignants du département de mathématique pour leurs dévouements et leurs générosités.

Dédicace

Au nom de Allah clément et le miséricordieux.

-Je dédie ce modeste travail.

A Ma Mère

Avec tout mon amour pour ton soutien et tes encouragements. j'espère rester à la hauteur de tes espoirs que Dieu te protège et t'accorde santé et longue vie

- A Mon père

Tes sacrifices et tes Prières m'ont permis de vivre ce jour. Rien ne saurait exprimer la fierté, la reconnaissance et l'amour que je te porte. que Dieu le tout puissant te procure, santé et longue vie.

-A toute la famille

Surtout mes frères Khaled et Daoud.

-A toute nos amies.

-A mes collègue en particulier :

Sara, Siham, Halima, Chaima, Soumia pour leurs gentillesse et leurs soutien.

- Je tiens à remercier l'ensemble de tous les étudiants et étudiantes de ma promotion,

Enfin je dédie ce mémoire à mes collègues et tous ceux qui me sont cher.

Notations

- $A = \mathbb{K}[x_1, \dots, x_n]$: l'anneau de polynômes à coefficients dans \mathbb{K} (\mathbb{K} : un corps).
- $\langle a \rangle$: l'idéal bilatère engendré par a .
- \mathcal{R} : une relation binaire sur E .
- \leq : une relation d'ordre.
- $\text{multideg}(f)$: le multidegré de f .
- $\mathcal{M}(x_1, \dots, x_n)$: l'ensemble des monômes en les indéterminées x_1, \dots, x_n .
- $|\alpha|$: le degré total de monome $x_1^{\alpha_1} \dots x_n^{\alpha_n}$ avec $\alpha_i \in \mathbb{N}$.
- $x^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}$ telque $x^\alpha \in \mathcal{M}(x_1, \dots, x_n)$ et $\alpha = (\alpha_1, \dots, \alpha_n)$.
- " \preccurlyeq " : un ordre monomial sur \mathcal{M} .
- $LT(f)$: le terme dominant de f , selon " \preccurlyeq " (pour leading term).
- $LC(f)$: le coefficient dominant de f , selon " \preccurlyeq " (pour leading coefficient).
- $LM(f)$: le monôme dominant de f , selon " \preccurlyeq " (pour leading monomial).
- $LT(I)$: l'ensemble des termes dominants des éléments de I .
- $\langle LT(I) \rangle$: l'idéal engendré par les éléments de $LT(I)$.
- \preccurlyeq_{lex} : l'ordre lexicographique.
- \preccurlyeq_{revlex} : l'ordre lexicographique inversé.
- " \preccurlyeq_{deglex} " : l'ordre lexicographique gradué.
- " $\preccurlyeq_{degrevlex}$ " : l'ordre lexicographique gradué inversé.
- $f \xrightarrow{G} r$: la forme normale du polynôme f par la division par G .
- \mathbb{F}_p : corps fini de p élément.
- $\overline{\mathbb{F}_q}$: la clôture algébrique de \mathbb{F}_q .
- $F(x_1, \dots, x_n, z)$: le polynôme homogénéisé (ou simplement homogénéisé) de f .
- $\mathbf{V}(f_1, \dots, f_m)$: la variété affine de f_1, \dots, f_m .
- $\mathbf{V}(I)$: le sous-ensemble de \mathbb{K}^n de l'idéal I de $\mathbb{K}[x_1, \dots, x_n]$.

Table des matières

Introduction	1
1 Notions élémentaires sur les anneaux et la relation d'ordre.	3
1.1 Généralités sur les anneaux.	3
1.1.1 Anneaux et idéaux.	3
1.2 La relation d'ordre.	14
1.2.1 Généralités sur la relation d'ordre.	14
1.2.2 Ordre réciproque, ordre induit, ordre produit.	17
1.2.3 Morphismes et isomorphisme d'ensembles ordonnés.	18
2 Etude sur les ordres monomiaux.	20
2.1 L'ordre monomial.	20
2.2 Quelques ordres monomiaux.	21
2.2.1 L'ordre lexicographique.	21
2.2.2 L'ordre lexicographique inversé	22
2.2.3 L'ordre lexicographique gradué	22
2.2.4 L'ordre lexicographique gradué inversé	23
2.3 Idéal monomial.	24
3 Etude sur le problème de l'appartenance d'un polynôme à un idéal.	29
3.1 Algorithme de division des polynômes à plusieurs variables.	29
3.2 Base de Gröbner.	31
3.2.1 Propriétés des bases de Gröbner	32
3.3 Problème de l'appartenance à un idéal.	33
4 Etude sur les variétés algébriques.	34
Conclusion	39
Bibliographie	39

Introduction

En algèbre appliquée, de nombreux problèmes de modélisation se formulent en termes d'équations polynomiales. L'étude des idéaux de polynômes à plusieurs indéterminées permet de résoudre des systèmes d'équations polynomiales à plusieurs inconnues, grâce à des méthodes algorithmiques. L'ensemble des polynômes à plusieurs indéterminées forme un anneau commutatif, noté $\mathbb{K}[x_1, \dots, x_n]$. Un idéal de $\mathbb{K}[x_1, \dots, x_n]$ est un sous-ensemble de cet anneau, stable pour l'addition et la multiplication. On peut définir des idéaux de $\mathbb{K}[x_1, \dots, x_n]$ à partir d'une famille de polynômes, appelée base de l'idéal. L'idéal correspond alors à l'ensemble des combinaisons de polynômes de la base. Cette définition invite au problème suivant : comment savoir si un polynôme donné appartient à l'idéal engendré par une base donnée ? (Le problème de l'appartenance à un idéal). La division euclidienne peut répondre à cette question. Mais cette méthode n'est pas toujours opérationnelle. Pour résoudre ce problème, une méthode consiste à trouver, pour un idéal donné, une base qui respecte cette équivalence entre la nullité du reste de la division d'un polynôme par cette base et l'appartenance de ce polynôme à l'idéal. On appellera base de Gröbner. La théorie des bases de Gröebner pour les anneaux de polynômes à plusieurs indéterminées a été développée en 1965 en Autriche. Le père de cette théorie est Bruno Buchberger, il a donné à ces bases le nom de son directeur d'études, Wolfgang Groebner. Le mathématicien Buchberger a créé un algorithme qui, pour tout idéal, calcule une base de Gröbner. Cet algorithme termine avec succès en un nombre fini d'étape.

Ce mémoire est réparti en quatre chapitres :

Dans le premier chapitre, nous allons donner quelques notions élémentaires sur les anneaux et la relation d'ordre.

Dans le deuxième chapitre, on fait une étude sur les ordres monomiaux.

Dans le troisième chapitre, nous présentons les bases de Gröbner et le problème de l'appartenance d'un polynôme à un idéal.

A le quatrième chapitre, nous intéressons à quelques propriétés sur les variétés algébriques.

Chapitre 1

Notions élémentaires sur les anneaux et la relation d'ordre.

1.1 Généralités sur les anneaux.

1.1.1 Anneaux et idéaux.

Anneaux

Définition 1.1

Un groupe $(G, *)$ est un ensemble G muni d'une loi interne (ou loi de composition interne), c'est -à-dire une application $G \times G \rightarrow G, (x, y) \rightarrow x * y$ Possédant les propriétés suivantes :

1. La loi est associative : $\forall x, y, z \in G, (x * y) * z = x * (y * z)$.
2. Il existe un élément $e \in G$, appelé élément neutre de G , tel que :

$$\forall x \in G, x * e = e * x = x.$$

3. pour tout élément $x \in G$, il existe $x' \in G$, appelé symétrique de x , tel que :

$$x * x' = x' * x = e.$$

Si, de plus, la propriété suivante $\forall (x, y) \in G \times G, x * y = y * x$ est vérifiée, le groupe G est dit commutatif ou abélien.

Exemple 1.1

$(\mathbb{Z}, +)$ est un groupe.

Définition 1.2

On appelle sous-groupe d'un groupe $(G, *)$ toute partie H de G vérifiant :

1. $e \in H$.
2. $\forall x, y \in H, x * y' \in H$.

Exemple 1.2

$\{e\}$ et G sont des sous-groupes de $(G, *)$.

Définition 1.3

Un anneau A est un ensemble muni de deux opérations " + " (addition) et " \times " (multiplication) telles que :

1. $(A, +)$ est un groupe abélien.
2. La multiplication est associative : $\forall a, b, c \in A, (a \times b) \times c = a \times (b \times c)$

et distributif par rapport à l'addition :

$$\forall a, b, c \in A, a \times (b + c) = a \times b + a \times c \text{ et } (a + b) \times c = a \times c + b \times c.$$

On ne regarde ici que des anneaux commutatifs :

$$\forall a, b \in A, a \times b = b \times a.$$

Muni d'une unité $1_A : \forall a \in A, 1_A \times a = a \times 1_A = a$.

Exemple 1.3

$(\mathbb{Z}, +, \times), (\mathbb{R}, +, \times), (\mathbb{C}, +, \times), (\mathbb{Q}, +, \times)$ sont des anneaux commutatifs unitaire.

Définition 1.4

Un sous-ensemble S d'un anneau A est un sous-anneau, si S est un sous-groupe pour l'addition, stable par multiplication et $1_A \in S$.

Exemple 1.4

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

Définition 1.5

Soient A, B deux anneaux. Une application $f : A \rightarrow B$ est un homomorphisme d'anneaux, si :

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

Exemple 1.5

Soit $f : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, x \longrightarrow \bar{x}, n \in \mathbb{N}^*,$ définie par $f(x) = \bar{x},$ on a :

1. $f(x + y) = \overline{x + y} = \bar{x} + \bar{y} = f(x) + f(y).$
2. $f(xy) = \overline{xy} = f(x)f(y).$
3. $f(1_{\mathbb{Z}}) = \overline{1_{\mathbb{Z}/n\mathbb{Z}}}.$

Donc, f un homomorphisme d'anneaux.

Définition 1.6

Soit A anneau commutatif d'unité $1_A.$

1. $x \in A$ est un diviseur de zéro si, $\exists y \neq 0, y \in A$ tel que $x \times y = 0.$
2. $x \in A$ est inversible si, $\exists y \in A$ tel que $x \times y = 1_A.$

L'ensemble d'éléments inversibles de A est un groupe, appelé groupe des unités de A et noté $\mathbb{U}(A).$

3. On dit que A est intègre si, A n'a pas de diviseurs de zéro sauf 0.

Exemple 1.6

1. $\mathbb{Z}_{6\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}, 0 = \bar{0}, 1 = \bar{1},$ on a $\bar{2} \times \bar{3} = \bar{6} = \bar{0}$ donc, $\bar{2}$ et $\bar{3}$ des diviseurs de zéro, et $\mathbb{Z}_{6\mathbb{Z}}$ n'est pas intègre.
2. Soit p premier. Les éléments inversibles de \mathbb{F}_p sont les classes de $1, 2, \dots, p - 1.$
 $\mathbb{U}(\mathbb{Z}) = \{1, -1\}, \mathbb{U}(\mathbb{K}) = \mathbb{K}^*.$
3. Les anneaux \mathbb{Z}, \mathbb{F}_p (p premier), $\mathbb{K}[x_1, \dots, x_n]$ (\mathbb{K} un corps) sont intègres.

Corps

Définition 1.7

On appelle corps tout anneau $(\mathbb{K}, +, \times)$ vérifiant :

1. $(\mathbb{K}, +, \times)$ est commutatif.

2. \mathbb{K} est non réduit à $\{0_{\mathbb{K}}\}$.
3. Tous les éléments de \mathbb{K} , sauf le nul, sont inversibles.

Exemple 1.7

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

Proposition 1.1

Tout corps est intègre.

Preuve.

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

Sous corps

Définition 1.8

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

1. \mathbb{L} est un sous-anneau de $(\mathbb{K}, +, \times)$.
2. $x \in \mathbb{L}, x \neq 0_{\mathbb{K}} \implies x^{-1} \in \mathbb{L}$.

Exemple 1.8

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

Théorème 1.1

Si \mathbb{L} est un sous-corps de $(\mathbb{K}, +, \times)$, alors $(\mathbb{L}, +, \times)$ est un corps.

Preuve.

Puisque \mathbb{L} est un sous-anneau de l'anneau commutatif $(\mathbb{K}, +, \times)$, on peut affirmer que $(\mathbb{L}, +, \times)$ est un anneau commutatif. Puisque $1_{\mathbb{K}} \in \mathbb{L}$, on peut affirmer que l'anneau $(\mathbb{L}, +, \times)$ n'est pas réduit à $0_{\mathbb{K}}$. Enfin, puisque l'inverse d'un élément non nul de \mathbb{L} est élément de \mathbb{L} , on peut affirmer que tout élément non nul de l'anneau \mathbb{L} est inversible dans celui-ci. ■

Exemple 1.9

Considérons $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} / a, b \in \mathbb{Q}\}$. Montrons que $(\mathbb{Q}[\sqrt{2}], +, \times)$ est un

corps. Pour cela montrons que $\mathbb{Q}[\sqrt{2}]$ est un sous-corps du corps $(\mathbb{R}, +, \times)$. On a évidemment $\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$. $1 = 1 + 0 \times \sqrt{2} \in \mathbb{Q}[\sqrt{2}]$.

Pour $x, y \in \mathbb{Q}[\sqrt{2}]$, on peut écrire $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$ avec $a, b, c, d \in \mathbb{Q}$.

On a alors, $x - y = (a - c) + (b - d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$.

et $xy = (ab + 2dc) + \sqrt{2}(ad + bc) \in \mathbb{Q}[\sqrt{2}]$. Enfin, si $x \neq 0$,

$$x^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

$$\text{car } \frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \in \mathbb{Q}.$$

Idéaux

Définition 1.9

Une partie I d'un anneau A est un idéal à gauche (resp. à droite, resp. bilatère) si I est un sous-groupe abélien de A pour l'addition et si

$$\forall x \in I, \forall a \in A, a.x \in I \text{ (resp, } x.a \in I, \text{ resp, } a.x \in I \text{ et } x.a \in I).$$

Remarque 1.1

1. Si l'anneau A est commutatif, il y a équivalence entre idéal à gauche, idéal à droite et idéal bilatère. Dans ce cas, on dira que I est un idéal.
2. Il est évident que si I est un idéal à gauche (resp. à droite, resp. bilatère) d'un anneau A et si $1_A \in I$, alors $I = A$.

Exemple 1.10

Soient A et $\{0\}$ sont des idéaux bilatères de A .

Définition 1.10

Si I et J sont deux idéaux à gauche (resp. à droite, resp. bilatères) d'un anneau A , alors : $I + J = \{x + y \mid x \in I, y \in J\}$ est un idéal à gauche (resp. à droite, resp. bilatère) de A , appelé somme des idéaux I et J .

$IJ = \left\{ \sum_{finie} x_i y_i \mid x_i \in I, y_i \in J \right\}$ est un idéal à gauche (resp. à droite, resp. bilatère) de A , appelé produit des idéaux I et J .

Proposition 1.2

Si $\{I_j\}_{j \in J}$ une famille non vide d'idéaux à gauche (resp. à droite, resp. bilatères) d'un anneau A , alors $\bigcap_{j \in J} I_j$ est un idéal à gauche (resp. à droite, resp. bilatère) de A .

Définition 1.11

Soient A un anneau et S une partie de A . On appelle idéal à gauche (resp. à droite, resp. bilatère) de A engendré par S le plus petit idéal à gauche (resp. à droite, resp. bilatère) de A contenant S . C'est l'intersection des idéaux à gauche (resp. à droite, resp. bilatères) de A contenant S .

Proposition 1.3

Soient A un anneau et S une partie de A . L'idéal à gauche de A engendré par S est formé des éléments de A s'écrivant : $\sum_{finie} a_i s_i$, $a_i \in A, s_i \in S$.

On écrire de la même manière l'idéal à droite (resp. bilatère) engendré par S .

Notation 1.2

Si la partie S est réduite à un élément, $S = \{a\}$, on note $\langle a \rangle$ l'idéal bilatère engendré par a .

Définition 1.12

Un idéal (à gauche, à droite, bilatère) I d'un anneau A est dit propre si $I \neq \{0\}$ et $I \neq A$.

Proposition 1.4

Un anneau commutatif A est un corps, si et seulement s'il ne possède aucun idéal propre.

Preuve.

Soient A un corps et I un idéal non nul de A . Il existe un élément $a \neq 0$ dans I .

L'élément a , étant non nul, est inversible dans A et, puisque I est un idéal, $a^{-1}a = 1_A$ appartient à I . On en déduit que $I = A$.

Supposons que A soit un anneau commutatif sans idéal propre. Pour tout élément $a \neq 0$ de A , L'idéal $\langle a \rangle$ engendré par a est non nul, donc égal à A . Par conséquent, il existe un élément b de A tel que $ab = 1_A$. Cela montre que tout élément non nul de A est inversible, donc que A est un corps. ■

Définition 1.13

Soient A un anneau et I un idéal de A . On dit que I est principal s'il est engendré par un élément (i.e., $\exists a \in A$ tel que $I = \langle a \rangle$).

Définition 1.14

Un anneau intègre est principal si tout idéal de cet anneau est principal.

Remarque 1.2

1. Si l'élément $a \in A$ est inversible, alors $aa^{-1} = 1_A \in \langle a \rangle$.
2. Dans un anneau intègre, $\langle a \rangle = \langle a' \rangle$ est équivalent à $a' = ua$ avec u élément inversible de A . En effet, si $\langle a \rangle = \langle a' \rangle$, il existe $u \in A$ et $v \in A$ tels que $a' = ua$ et $a = va'$: on a donc $a' = uva'$, d'où $(1_A - uv) = 0$ et, puisque l'anneau A est intègre, $uv = 1_A$. Si $a' = ua$, alors $\langle a' \rangle \subset \langle a \rangle$. Si u est inversible, on a $a = u^{-1}a'$, d'où $\langle a \rangle \subset \langle a' \rangle$.

Autrement dit, dans un anneau principal, tous les générateurs d'un idéal quelconque sont « égaux entre eux, aux éléments inversibles près ».

Anneaux Euclidien**Définition 1.15**

Soient A un anneau commutatif, a et b deux éléments de A . On dit que a divise b , ou que a est un diviseur de b , et on écrit $a|b$, s'il existe un élément $c \in A$ tel que $b = ac$.

Définition 1.16 (Anneau de Bézout)

Soit A un anneau commutatif intègre, on dit que A est un anneau de Bézout si, et seulement si une des deux propositions équivalentes suivantes est vérifiée :

1. La somme de deux idéaux principaux de A est toujours un idéal principal.
2. Tous les idéaux de type fini de A sont principaux.

Théorème 1.3 (*Égalité de Bézout*)

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

Théorème 1.4 (théorème de Bézout)

Soit A un anneau de Bézout, a et b deux éléments de A sont premier entre eux si, et 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 $d = 1_A$. ■

Définition 1.17

Soit A anneau commutatif unitaire intègre. Une division Euclidienne sur A est une application $\varphi : A - \{0\} \rightarrow \mathbb{N}$, $x \rightarrow \varphi(x)$, vérifiant :

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

Algorithme d'Euclide**Algorithm 1.5**

Soit A anneau euclidien. On calcul le pgcd de a et $b \in A$ ($b \neq 0$).

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

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

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

$$\vdots$$

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

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

donc on a, $r_n = \text{pgcd}(a, b)$, inversement on trouve $x, y \in A$ tels que $r_n = ax + by$.

Définition 1.18

Un anneau Euclidien est un anneau commutatif A vérifiant les deux propriétés suivantes :

1. A est intègre, i.e., pour tous éléments a et b de A ,

$$ab = 0 \Rightarrow (a = 0 \text{ ou } b = 0).$$

2. Il existe sur A un algorithme Euclidien, i.e., une application $\varphi : A - \{0\} \rightarrow \mathbb{N}$, telle que, pour tout $a \in A$ et tout $b \in A - \{0\}$, il existe $q \in A$ et $r \in A$, tels que

$$a = bq + r, \text{ avec } \varphi(r) < \varphi(b) \text{ ou } r = 0.$$

Théorème 1.6

Un anneau Euclidien est principal.

Idéaux maximaux, idéaux premiers

Définition 1.19

1. Un idéal $I \subset A, I \neq A$ est premier si $x \times y \in I$ implique soit $x \in I$, soit $y \in I$.
2. Un idéal $M \subset A, M \neq A$ est maximal si pour un d'idéal I tel que $I \supset M$, on a soit $I = M$, soit $I = A$.

Algèbre des polynômes.

Définition 1.20

Soit A un anneau, l'ensemble des polynômes à une indéterminée à coefficients dans A muni de l'addition et de la multiplication définies ci-dessus est un anneau commutatif. On note $A[X]$.

Proposition 1.5

Si A est intègre alors pour tout $P, Q \in A[X]$ on a :

$$\deg(PQ) = \deg(P) + \deg(Q) \text{ et } \deg(P + Q) \leq \deg(P) + \deg(Q).$$

Preuve.

Si un des deux polynômes est nul alors $PQ = 0$ et l'égalité devient $-\infty = -\infty$ ce qui est « vrai ». On suppose donc que P et Q sont non nuls. Soit $n = \deg(P)$ et $m = \deg(Q)$. On pose $P = \sum a_i X^i$ et $Q = \sum b_i X^i$ où $a_i, b_i \in A$. Alors le coefficient

du terme dominant de PQ est a_nb_m , Or $a_n \neq 0$ et $b_m \neq 0$ et donc, puisque A est intègre, $a_nb_m \neq 0$. Ce qui implique $\deg(PQ) = n + m$. ■

Définition 1.21

Un monôme en x_1, \dots, x_n est un produit de la forme $x_1^{\alpha_1} \dots x_n^{\alpha_n}$ avec $\alpha_i \in \mathbb{N}$, le degré total de ce monôme est la somme des α_i , il est noté $|\alpha|$.

Définition 1.22

Un polynôme f en x_1, \dots, x_n avec les coefficients dans \mathbb{K} est une combinaison linéaire finie des monômes, on écrit : $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$; $a_{\alpha} \in \mathbb{K}$.

Définition 1.23

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

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

Définition 1.24

Un polynôme est dit homogène si tous les monômes apparaissant avec un coefficient non nul ont le même degré total.

Exemple 1.11

Le polynôme $x_1 x_2 x_3 + x_2^3 - 10x_1^2 x_3$ est homogène.

Le polynôme $x_1^2 + x_2$ n'est pas homogène.

Définition 1.25

Un ensemble $I \subseteq \mathbb{K}[x_1, \dots, x_n]$ est un idéal si et seulement si :

1. $0 \in I$.
2. Si $f, g \in I$, alors $f - g \in I$.
3. Si $f \in I$ et $h \in \mathbb{K}[x_1, \dots, x_n]$ alors $hf \in I$.

Lemme 1.1

Si $f_1, \dots, f_s \in \mathbb{K}[x_1, \dots, x_n]$ alors l'ensemble :

$$\langle f_1, \dots, f_s \rangle = \left\{ \sum_{i=1}^s h_i f_i; h_1, \dots, h_s \in \mathbb{K}[x_1, \dots, x_n] \right\}$$

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.

$0 \in \langle f_1, \dots, f_s \rangle$ puisque $0 = \sum_{i=1}^s 0f_i$.

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 $p_i - q_i \in \mathbb{K}[x_1, \dots, x_n]$.

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 $hf \in \langle f_1, \dots, f_s \rangle$.

Soit I un idéal de $\mathbb{K}[x_1, \dots, x_n]$ tel que $\{f_1, \dots, f_s\} \subseteq I$, on montre que $\langle f_1, \dots, f_s \rangle \subseteq I$.

Soit $f \in \langle f_1, \dots, f_s \rangle$, i.e, $f = \sum_{i=1}^s p_i f_i, p_i \in \mathbb{K}[x_1, \dots, x_n]$, on a $\{f_1, \dots, f_s\} \subseteq I$ et comme I est un idéal de $\mathbb{K}[x_1, \dots, x_n]$, alors $f \in I$. ■

Définition 1.26

Soit g un polynôme non nul de $\mathbb{K}[x_1, \dots, x_n]$. Pour tout $f \in \mathbb{K}[x_1, \dots, x_n]$,

il existe $q, r \in \mathbb{K}[x_1, \dots, x_n]$ tels que $f = qg + r$ avec $q, r \in \mathbb{K}[x_1, \dots, x_n]$ et $r = 0$ ou $\deg(r) < \deg(g)$. Les polynômes q et r sont uniques.

Définition 1.27 (plus grand commun diviseur)

un plus grand commun diviseur des polynômes $f_1, \dots, f_s \in \mathbb{K}[x_1, \dots, x_n]$ 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 1.6

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.

1.2 La relation d'ordre.

Définition 1.28 (Produit cartésien)

Soient E et F des ensembles, on note $E \times F$ et on appelle Le produit cartésien de E et F l'ensemble de tous les couples dont la première composante appartient à E et le seconde à F : $E \times F = \{(x, y) : (x \in E) \wedge (y \in F)\}$.

Définition 1.29 (Relation binaire sur un ensemble)

Soit E un ensemble quelconque, une relation binaire \mathcal{R} sur E est une partie de E^2 , c'est-à-dire $\mathcal{R} = \{(a, b) : (a, b) \in E^2\}$. Si \mathcal{R} une relation binaire sur un ensemble E et $(a, b) \in \mathcal{R}$, on dit que a est en relation avec b selon \mathcal{R} et on écrit $a\mathcal{R}b$.

Définition 1.30 (L'image directe et l'image réciproque)

Soit \mathcal{R} une relation binaire sur un ensemble E , et soit X, Y des parties de E .

On appelle image directe de X par \mathcal{R} , et on note $\mathcal{R}(X)$, le sous-ensemble de E : $\mathcal{R}(X) = \{y \in E \mid \exists x \in X : x\mathcal{R}y\}$. Cas particulier, si la partie $X = \{a\}$ (singleton) on note $\mathcal{R}(X)$ par $\mathcal{R}(a)$.

On appelle image réciproque de Y par \mathcal{R} , et on note $\mathcal{R}^{-1}(Y)$, le sous-ensemble de E : $\mathcal{R}^{-1}(Y) = \{x \in E \mid \exists z \in Y : x\mathcal{R}z\}$. Cas particulier, si la partie $Y = \{b\}$ (singleton) on note $\mathcal{R}^{-1}(Y)$ par $\mathcal{R}^{-1}(b)$.

Exemple 1.12

Soient l'ensemble $E = \{1, 2, 3\}$ et $\mathcal{R} = \{(1, 1); (2, 1); (3, 2)\}$ une relation binaire sur E . $X_1 = \{1, 3\}$, $X_2 = \{3\}$, $Y_1 = \{1, 2\}$ et $Y_2 = \{2\}$ sont des parties de E .

$\mathcal{R}(X_1) = \{1, 2\} = Y_1$ et $\mathcal{R}(X_2) = \mathcal{R}(3) = \{2\} = Y_2$.

$\mathcal{R}^{-1}(Y_1) = \{1, 3\} = X_1$ et $\mathcal{R}^{-1}(Y_2) = \mathcal{R}^{-1}(2) = \{3\} = X_2$.

1.2.1 Généralités sur la relation d'ordre.

Définition 1.31

Une relation binaire \mathcal{R} dans un ensemble non vide E est dite relation d'ordre sur E si, et seulement si elle vérifie les trois propriétés suivantes :

1. Réflexivité : pour tout x , $x\mathcal{R}x$.
2. Antisymétrie : si $x\mathcal{R}y$ et $y\mathcal{R}x$, alors $x = y$.

3. Transitivité : si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $x\mathcal{R}z$.
4. \mathcal{R} est dite irréflexive si $(x, x) \notin \mathcal{R}$, pour tout $x \in E$.

D'une façon générale une relation d'ordre sera notée $x \leq y$ (x inférieur à y), au lieu de $x\mathcal{R}y$. En cas de confusion possible on pourra préciser cette notation : $x \leq_E y$ ou $x \leq_1 y$ (s'il y a plusieurs relations d'ordre).

Définition 1.32

Un ensemble E muni d'une relation d'ordre sera dit un ensemble ordonné.

Exemple 1.13

1. L'ensemble \mathbb{N}^* muni de la relation de divisibilité : x/y (x divise y) définie par : il existe $a \in \mathbb{N}$ tel que $y = ax$.
2. $\mathcal{P}(E)$ muni de la relation d'inclusion : $X \subset Y$ (E étant un ensemble quelconque).

Notation 1.7

On utilisera également les notations suivantes :

1. $x \not\leq y$: x non inférieur à y .
2. $x < y$: x strictement inférieur à y , c'est-à-dire $x < y$ et $x \neq y$.

Définition 1.33

Soit \mathcal{R} une relation binaire de E vers F , on appelle complémentaire de \mathcal{R} et on noté $\overline{\mathcal{R}}$ ou \mathcal{R}^c la relation binaire définie par :

$$\forall (x, y) \in E \times F; (x, y) \in \mathcal{R}^c \implies (x, y) \notin \mathcal{R}.$$

Définition 1.34

Soient \mathcal{R} et \mathcal{S} deux relations binaires sur un ensemble E .

1. On appelle réunion de \mathcal{R} et \mathcal{S} et on note $\mathcal{R} \cup \mathcal{S}$, la relation binaire définie sur E par : $\forall (x, y) \in E^2, (x, y) \in \mathcal{R} \cup \mathcal{S} \iff (x, y) \in \mathcal{R} \vee (x, y) \in \mathcal{S}$.
2. On appelle intersection de \mathcal{R} et \mathcal{S} et on note $\mathcal{R} \cap \mathcal{S}$, la relation binaire définie sur E par : $\forall (x, y) \in E^2, (x, y) \in \mathcal{R} \cap \mathcal{S} \iff (x, y) \in \mathcal{R} \wedge (x, y) \in \mathcal{S}$.
3. On appelle compose de \mathcal{R} et \mathcal{S} et on note $\mathcal{S} \circ \mathcal{R}$, la relation binaire définie sur E par : $\forall (x, y) \in E^2, (x, y) \in \mathcal{S} \circ \mathcal{R} \iff \exists z \in E : (x, z) \in \mathcal{R} \text{ et } (z, y) \in \mathcal{S}$.

Exemple 1.14

Soit $E = \{a, b, c, d\}$. $\mathcal{R} = \{(a, b), (b, c), (c, d)\}$. on a $\mathcal{R} \circ \mathcal{R} = \{(a, c), (b, d)\}$.

Proposition 1.7

Soit \mathcal{R} une relation binaire sur E .

1. \mathcal{R} est réflexive, alors, \mathcal{R}^c aussi.
2. \mathcal{R} est transitive, si et seulement si, $\mathcal{R} \circ \mathcal{R} \subset \mathcal{R}$.
3. Si \mathcal{R} est transitive alors, $\mathcal{R} \circ \mathcal{R}$ aussi.
4. \mathcal{R} est antisymétrique, si et seulement si, $\mathcal{R} \cap \mathcal{R}^c \subset \Delta_E$ où $\Delta_E = \{(x, x) / x \in E\}$.

Preuve.

1. Si \mathcal{R} réflexive alors pour tout $x \in E$, $(x, x) \in \mathcal{R}$, donc $(x, x) \in \mathcal{R}^c$, par suite \mathcal{R}^c est réflexive.

2. On suppose que \mathcal{R} est transitive et on montre $\mathcal{R} \circ \mathcal{R} \subseteq \mathcal{R}$. Soit $(x, y) \in \mathcal{R} \circ \mathcal{R} \iff \exists z \in E : (x, z) \in \mathcal{R} \text{ et } (z, y) \in \mathcal{R}$, donc $(x, y) \in \mathcal{R}$.

Inversement : soient x, y et $z \in E$ tels que $(x, y) \in \mathcal{R}$ et $(y, z) \in \mathcal{R}$, donc $(x, y) \in \mathcal{R} \circ \mathcal{R}$, comme $\mathcal{R} \circ \mathcal{R} \subset \mathcal{R}$, on $(x, y) \in \mathcal{R}$, i.e, \mathcal{R} est transitive

3. Si \mathcal{R} une relation d'ordre transitive, On a $\mathcal{R} \circ \mathcal{R} \subset \mathcal{R}$.

Soient x, y et $z \in E$ tels que $(x, y) \in \mathcal{R} \circ \mathcal{R}$ et $(y, z) \in \mathcal{R} \circ \mathcal{R}$, i.e,

il existe $(u, v) \in E^2$ tels que $(x, u) \in \mathcal{R}$, $(u, y) \in \mathcal{R}$, $(y, v) \in \mathcal{R}$ et $(v, z) \in \mathcal{R}$.

Comme \mathcal{R} est transitive, on a $(x, y) \in \mathcal{R}$ et $(y, z) \in \mathcal{R}$, par définition on a $(x, z) \in \mathcal{R} \circ \mathcal{R}$.

4. On suppose que \mathcal{R} est antisymétrique, i.e,

$\forall (x, y) \in E^2 : (x, y) \in \mathcal{R} \text{ et } (y, x) \in \mathcal{R} \text{ implique } x = y$. Et on vérifie que

$\mathcal{R} \cap \mathcal{R}^c \subseteq \Delta_E$, soit $(x, y) \in \mathcal{R} \cap \mathcal{R}^c$, i.e., $(x, y) \in \mathcal{R}$ et $(y, x) \in \mathcal{R}^c$, donc

$(x, y) \in \mathcal{R}$ et $(y, x) \in \mathcal{R}$ implique $x = y$ et par suite $\mathcal{R} \cap \mathcal{R}^c \subseteq \Delta_E$.

Inversement : si $\mathcal{R} \cap \mathcal{R}^c \subseteq \Delta_E$, alors $(x, y) \in \mathcal{R}$ implique $x = y$.

■

Définition 1.35

1. Deux éléments x et y sont dits comparables si $x \leq y$ ou $y \leq x$, sinon ils sont dits incomparables, c'est-à-dire $x \not\leq y$ et $y \not\leq x$.

2. Une relation d'ordre dans un ensemble E est dite totale si tous les éléments sont deux à deux comparables.
3. Un ensemble E muni d'une relation d'ordre totale est dit totalement ordonné, on dit aussi que E est une chaîne.

Exemple 1.15

1. \mathbb{N}^* avec la relation de divisibilité n'est pas une chaîne.
2. $\mathcal{P}(E)$ avec la relation d'inclusion n'est pas une chaîne (si E a au moins deux éléments).
3. \mathbb{N} avec l'ordre ordinaire est une chaîne.

Définition 1.36

Une relation binaire \mathcal{R} sur un ensemble E est dite ordre strict si elle est irréflexive et transitive. Dans ce cas le couple (E, \mathcal{R}) est dit ensemble strictement ordonné.

Remarque 1.3

Un ordre strict $<$ est nécessairement antisymétrique. En effet : si on imagine $((a < b)$ et $(b < a))$, avec $a \neq b$, la transitivité de $<$ entraîne $a < a$, ce qui est contredit l'irréflexivité de $<$.

1.2.2 Ordre réciproque, ordre induit, ordre produit.

L'ordre réciproque

Définition 1.37

Soit un ensemble ordonné (E, \leq) on peut définir sur E une nouvelle relation, notée $x \geq y$, comme étant équivalente à $y \leq x$. On vérifie immédiatement que c'est aussi une relation d'ordre sur E .

La relation $x \geq y$ (x supérieur à y) est dite la relation d'ordre réciproque de $x \leq y$. On notera également : $x \not\geq y$: x non supérieur à y .

$x > y$: x strictement supérieur à y , c'est-à-dire $x > y$ et $x \neq y$.

Remarque 1.4

Une relation d'ordre et sa relation réciproque ne sont identiques que dans le seul cas de la relation d'égalité.

L'ordre induit

Définition 1.38

Soit (E, \leq) un ensemble ordonné et soit A une partie non vide de E . La trace sur $A \times A$ de la relation \leq est une relation d'ordre sur A qui sera notée $x \leq_A y$, elle est donc définie par : $x \in A$ et $y \in A$ et $x \leq y$. Cette relation sera appelée relation d'ordre induite par \leq sur A .

Exemple 1.16

Soit l'ensemble ordonné $(\mathbb{N}^*, /)$ et soit $A = \{1, 2, 8, 64\}$. On remarque que A est une chaîne pour l'ordre induit, bien que la relation d'ordre ne soit pas totale sur \mathbb{N}^* .

L'ordre produit.

Définition 1.39

Considérons une famille d'ensembles ordonnés $((E_i, \leq_i))_{i \in I}$. Sur l'ensemble produit $E = \prod_{i \in I} E_i$ on peut définir la relation : $(x_i) \leq (y_i)$ pour tout $i \in I, x_i \leq_i y_i$.

Il est clair que ceci est une relation d'ordre sur E qui est appelée relation d'ordre produit.

1.2.3 Morphismes et isomorphisme d'ensembles ordonnés.

Définition 1.40

Soit $\mathcal{F}(E, F)$ l'ensemble des applications d'un ensemble E dans un ensemble F . Si F est un ensemble ordonné on peut alors muni $\mathcal{F}(E, F)$ de la relation d'ordre induit : $f \leq g$ si, et seulement si, pour tout $x \in E, f(x) \leq g(x)$.

Définition 1.41

Soient deux ensembles ordonnés $(E, <)$ et $(F, <)$, une application $f : E \rightarrow F$ sera dite un morphisme d'ordres ou encore une application croissante, si quels que soient x et y dans $E : x < y$ implique $f(x) < f(y)$. On définira également :

1. Application décroissante : $x < y$ implique $f(x) > f(y)$. (c'est un morphisme en munissant F de l'ordre réciproque).
2. Application strictement croissante : $x < y$ implique $f(x) < f(y)$.

3. Application strictement décroissante : $x < y$ implique $f(x) > f(y)$.

Remarque 1.5

1. Une application constante est à la fois croissante et décroissante, mais la réciproque est inexacte.
2. Une application croissante et injective est strictement croissante, mais une application strictement croissante n'est pas nécessairement injective.
3. Si f est une bijection croissante, l'application réciproque f^{-1} n'est pas nécessairement croissante.

Exemple 1.17

1. $E = \{2, 3, 4, 9\}$ ordonné par divisibilité, $F = \mathbb{N}$ avec l'ordre naturel, on définit f par $f(2) = f(4) = 1$ et $f(3) = f(9) = 2$, f est croissante et décroissante mais n'est pas constante.
2. Avec les mêmes ensembles que précédemment, $f(2) = 1$, $f(3) = f(4) = 2$, et $f(9) = 3$, f est strictement croissante mais n'est pas injective.
3. L'application identique de $(\mathbb{N}^*, |)$ sur (\mathbb{N}^*, \leq) est une bijection croissante, mais l'application réciproque n'est pas croissante.

Définition 1.42

Une application $f : E \rightarrow F$ est dite un isomorphisme d'ordres si : f est bijective et $x < y$ équivaut à $f(x) < f(y)$. Cela signifie donc que f et f^{-1} sont toutes les deux croissantes, par suite étant injectives elles seront strictement croissantes.

Chapitre 2

Etude sur les ordres monomiaux.

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

2.1 L'ordre monomial.

Nous noterons $\mathcal{M}(x_1, \dots, x_n)$, ou \mathcal{M} s'il n'y a pas de confusion, l'ensemble des monômes en les indéterminées x_1, \dots, x_n :

$$\mathcal{M}(x_1, \dots, x_n) = \{x^\alpha \mid \alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n\}.$$

Définition 2.1

Soit $A = \mathbb{K}[x_1, \dots, x_n]$, où \mathbb{K} est un corps commutatif. Un ordre monomial sur \mathcal{M} est une relation " \preccurlyeq " vérifiant les assertions suivantes :

1. " \preccurlyeq " est un ordre total sur \mathcal{M} .
2. Si $x^\alpha \preccurlyeq x^\beta$, alors $x^\alpha x^\gamma \preccurlyeq x^\beta x^\gamma$, pour tous x^α, x^β et $x^\gamma \in \mathcal{M}$.
3. $1 \preccurlyeq x^\alpha$, pour tout $x^\alpha \in \mathcal{M}$, tel que $x^\alpha \neq 1$.

Proposition 2.1

Soit X un ensemble ordonné non vide. Les assertions suivantes sont équivalentes :

1. *la relation \leq est un bon ordre.*
2. *X est totalement ordonné et ne contient pas de suite strictement décroissante pour la relation \leq .*

Preuve.

Supposons que la condition (2) est satisfaite. Soit x_0 un élément de X . Si \leq n'est pas un bon ordre, alors puisque X est totalement ordonné, il existe x_1 dans X tel que $x_1 < x_0$. De même x_1 ne peut être un plus petit élément il existe un x_2 dans X tel que $x_2 < x_1$. Par récurrence, on construit donc une suite strictement décroissante, ce qui contredit (2).

Réciproquement supposons que la condition (1) est satisfaite. Alors a fortiori X est totalement ordonnée. Si (x_n) est une suite décroissante, alors $\{x_0, x_1, \dots\}$ est non vide donc admet un plus petit élément. Cela assure que la suite est stationnaire, et prouve que X ne contient pas de suite strictement décroissante pour la relation \leq . ■

Proposition 2.2

Soit \preccurlyeq un ordre monomial sur \mathcal{M} . Soient x^α et x^β deux monômes de \mathcal{M} , tels que x^α divise x^β , alors $x^\alpha \preccurlyeq x^\beta$.

Preuve.

Si le monôme x^α divise le monôme x^β , il existe alors un monôme x^γ dans \mathcal{M} , tel que $x^\beta = x^\alpha x^\gamma$. L'ordre \preccurlyeq étant monomial, on a $1 \preccurlyeq x^\gamma$, d'où $x^\alpha \preccurlyeq x^\alpha x^\gamma = x^\beta$. ■

2.2 Quelques ordres monomiaux.

Soient $\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$, et $|\alpha| = \sum_{i=1}^n \alpha_i, |\beta| = \sum_{i=1}^n \beta_i$.

2.2.1 L'ordre lexicographique.

Définition 2.2

L'ordre lexicographique noté " \preccurlyeq_{lex} " est défini par :

$x^\alpha \preccurlyeq_{lex} x^\beta \Leftrightarrow$ le premier coefficient non nul de $\beta - \alpha$ est positif.

Proposition 2.3

L'ordre lexicographique " \preccurlyeq_{lex} " est un ordre monomial sur \mathbb{N}^n .

Preuve.

Que l'ordre lexicographique soit total découle immédiatement que l'ordre usuel sur \mathbb{N} est total. Supposons que $\alpha \preccurlyeq_{lex} \beta$ et soit $\gamma \in \mathbb{N}^n$. Comme $\beta + \gamma - (\alpha + \gamma) = \beta - \alpha$

il résulte de la définition que $\alpha + \gamma \preceq_{lex} \beta + \gamma$. Finalement donnons nous une suite décroissante d'éléments α_i de \mathbb{N}^n pour l'ordre lexicographique. La suite des $\alpha_{i,1}$ est décroissante dans \mathbb{N} donc stationnaire, il existe donc $N \geq 1$ tel que $\alpha_{i,1} = \alpha_{N,1}$ pour $i \geq N$. On en déduit qu'à partir de N , La suite de $\alpha_{i,2}$ est décroissante. Quitte à prendre un N plus grand, on a donc $\alpha_{i,1} = \alpha_{N,1}$ et $\alpha_{i,2} = \alpha_{N,2}$ pour $i \geq N$. De prêche en prêche on conclut que la suite des α_i est stationnaire. Notons que si on change l'ordre des variables, l'ordre lexicographique obtenu est différent. Par conséquent il y a $n!$ ordres lexicographiques. ■

Exemple 2.1

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

Prenons le polynôme $f = 4xy^2 + 2y^3z^4$ de A . Le premier terme de f est $4xy^2$ avec $\alpha = (1, 2, 0)$ et le deuxième terme de f 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 $\beta \preceq_{lex} \alpha$. C'est donc dire que $2y^3z^4 \preceq_{lex} 4xy^2$.

2.2.2 L'ordre lexicographique inversé

Définition 2.3

L'ordre lexicographique inversé noté " \preceq_{revlex} " est défini par :

$x^\alpha \preceq_{revlex} x^\beta \Leftrightarrow$ le dernier coefficient non nul de $\beta - \alpha$ est positif.

Exemple 2.2

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

Prenons le polynôme $f = 4xy^2 + 2y^3z^4$ de A . Le premier terme de f est $4xy^2$ avec $\alpha = (1, 2, 0)$ et le deuxième terme de f est $2y^3z^4$ avec $\beta = (0, 3, 4)$. On obtient donc le vecteur différence $(\beta - \alpha) = (-1, 1, 4)$. Puisque sa coordonnée non nulle la plus à gauche est positive, on a que $\alpha \preceq_{lex} \beta$. C'est donc dire que $4xy^2 \preceq_{revlex} 2y^3z^4$.

2.2.3 L'ordre lexicographique gradué

Définition 2.4

L'ordre lexicographique gradué noté " \preceq_{deglex} " est défini par :

$$x^\alpha \preceq_{deglex} x^\beta \Leftrightarrow \begin{cases} |\alpha| < |\beta|; \\ \text{ou} \\ |\alpha| = |\beta| \text{ et } x^\alpha \preceq_{lex} x^\beta. \end{cases}$$

Remarque 2.1

Avec l'ordre lexicographique gradué, on compare d'abord les degrés puis on applique l'ordre lexicographique. Par exemple, avec $y < x$, on a

$$1 \preceq_{deglex} y \preceq_{deglex} x \preceq_{deglex} y^2 \preceq_{deglex} xy \preceq_{deglex} x^2 \preceq_{deglex} y^3.$$

Proposition 2.4

L'ordre lexicographique gradué " \preceq_{deglex} " est un ordre monomial sur \mathbb{N}^n .

Preuve.

Similaire au cas de l'ordre lexicographique. ■

Exemple 2.3

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

Prenons le même polynôme $f = 4xy^2 + 2y^3z^4$ de A que dans l'exemple précédent. Le premier terme de f est $4xy^2$ avec $|\alpha| = 3$ et le deuxième terme de f est $2y^3z^4$ avec $|\beta| = 7$. On obtient que $|\alpha| < |\beta|$ et donc $\alpha \preceq_{deglex} \beta$. C'est donc dire que $4xy^2 \preceq_{deglex} 2y^3z^4$.

2.2.4 L'ordre lexicographique gradué inversé

Définition 2.5

L'ordre lexicographique gradué inversé noté " $\preceq_{degrevlex}$ " est défini par :

$$x^\alpha \preceq_{degrevlex} x^\beta \Leftrightarrow \begin{cases} |\alpha| < |\beta|; \\ \text{ou} \\ |\alpha| = |\beta| \text{ et } x^\alpha \succ_{revlex} x^\beta \end{cases}$$

On compare d'abord les degrés puis on applique l'opposé d'ordre lexicographique inversé

Remarque 2.2

Une définition équivalente de l'ordre lexicographique gradué inverse est la suivante :

$$x^\alpha \preceq_{\text{degrevlex}} x^\beta \iff \begin{cases} |\alpha| < |\beta|; \\ \text{ou} \\ |\alpha| = |\beta| \text{ et le dernier coefficient non nul de } \beta - \alpha \text{ est } < 0. \end{cases}$$

Exemple 2.4

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

Prenons le polynôme $g = 2xy^5z^2 - x^4yz^3$ de A . Le premier terme de g est $2xy^5z^2$ avec $\alpha = (1, 5, 2)$, $|\alpha| = 8$ et le deuxième terme de g est $-x^4yz^3$ avec $\beta = (4, 1, 3)$, $|\beta| = 8$. On doit donc examiner le vecteur différence $(\alpha - \beta) = (-3, 4, -1)$. Puisque sa coordonnée non nulle la plus à droite est négative, on a que $\beta \preceq_{\text{degrevlex}} \alpha$. C'est donc dire que $-x^4yz^3 \preceq_{\text{degrevlex}} 2xy^5z^2$.

2.3 Idéal monomial.

Définition 2.6

Un idéal I de $\mathbb{K}[x_1, \dots, x_n]$ est dit monomial s'il est engendré par des monômes, autrement dit s'il existe une partie non vide $E \subset \mathbb{N}^n$, possiblement infini, telle que I soit l'ensemble des polynômes qui s'écrivent comme somme finie de la forme $\sum_{\alpha} h_{\alpha} x^{\alpha}$ avec $h_{\alpha} \in \mathbb{K}[x_1, \dots, x_n]$. Dans ce cas, nous notons $I = \langle x^{\alpha} / \alpha \in E \rangle$.

Exemple 2.5

L'idéal $I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle$ est un idéal monomial de $\mathbb{K}[x, y]$.

L'idéal $I = \langle x - y \rangle$ n'est pas monomial.

Remarque 2.3

Des idéaux monomiaux sont égaux si et seulement si ils contiennent les mêmes monômes.

Définition 2.7

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

et soient $f = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$ un polynôme de A , où $a_i \in \mathbb{K}$, $a_d \neq 0$, pour $i = 1, \dots, n$ et " \preceq " est un ordre monomial sur A . Soit d le degré du polynôme.

Nous dirons que $a_d x^d$ est le terme dominant de f , selon " \preccurlyeq " et nous le noterons $LT(f)$ (pour leading term).

Nous dirons aussi que a_d est le coefficient dominant de f , selon " \preccurlyeq " et nous le noterons $LC(f)$ (pour leading coefficient).

Nous dirons que x^d est le monôme dominant de f , selon " \preccurlyeq " et nous le noterons $LM(f)$ (pour leading monomial).

Exemple 2.6

Prenons le polynôme $f = 5x^3y^2 - 6x^2y + 3y - 1$ de A et l'ordre lexicographique.

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

Remarque 2.4

On dit que f est unitaire si son coefficient dominant est 1.

Définition 2.8

Fixons un ordre monomial \preccurlyeq sur $\mathcal{M}(x_1, \dots, x_n)$. Tout polynôme non nul f de $\mathbb{K}[x_1, \dots, x_n]$ peut s'écrire sous la forme : $f = a_1 x^{\alpha_{i_1}} + a_2 x^{\alpha_{i_2}} + \dots + a_d x^{\alpha_{i_d}}$,

où les a_K sont des scalaires non nul, les $x^{\alpha_{i_k}}$ des monômes de $\mathcal{M}(x_1, \dots, x_n)$ deux à deux distincts et $a_d x^{\alpha_{i_d}} \preccurlyeq \dots \preccurlyeq a_2 x^{\alpha_{i_2}} \preccurlyeq a_1 x^{\alpha_{i_1}}$.

Le n -uplet α_{i_1} est appelé le multidegré de f , on le note $\text{multideg}(f)$: $\text{multideg}(f) = \alpha$ tel que x^α est le plus grand monôme apparaissant dans f .

Proposition 2.5

On fixe un ordre monomial sur $\mathcal{M}(x_1, \dots, x_n)$. Soient f et g des polynômes non nuls de $\mathbb{K}[x_1, \dots, x_n]$. Le multidegré vérifie les propriétés suivantes :

1. $\text{multideg}(fg) = \text{multideg}(f) + \text{multideg}(g)$.
2. Si $f + g$ est non nul, alors $\text{multideg}(f + g) \leq \max(\text{multideg}(f), \text{multideg}(g))$ et si, de plus $\text{multideg}(f) \neq \text{multideg}(g)$, on a l'égalité.

Définition 2.9

Ces définitions s'étendent aisément à un ensemble $F \subset \mathbb{K}[x_1, \dots, x_n]$. Ainsi :

1. $LT(F) = \{LT(f) : f \in F\}$.
2. $LC(F) = \{LC(f) : f \in F\}$.

3. $LM(F) = \{LM(f) : f \in F\}$.

Notation 2.1

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 .

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

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

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

Proposition 2.6

Soit $I = \langle x^\alpha \mid \alpha \in E \rangle$ un idéal monomial. Un monôme x^β est dans I si, et seulement si, x^β est divisible par x^α , pour un $\alpha \in E$.

Preuve.

Si x^β est divisible par un monôme $x^\alpha, \alpha \in E$, alors, il existe un polynôme h de $\mathbb{K}[x_1, \dots, x_n]$, tel que $x^\beta = h x^\alpha$, d'où $x^\beta \in I$. Supposons que x^β soit un monôme de I . Il existe alors une décomposition $x^\beta = h_{\alpha(1)} x^{\alpha(1)} + \dots + h_{\alpha(s)} x^{\alpha(s)}$, où $h_{\alpha(i)} \in \mathbb{K}[x_1, \dots, x_n]$ et $\alpha(i) \in E$. En développant chaque polynôme $h_{\alpha(i)}$, le terme de droite se décompose en une combinaison linéaire de monômes, et chaque monôme est divisible par un $x^{\alpha(i)}$. Par suite, x^β est divisible par un $x^{\alpha(i)}$. ■

Remarque 2.5

Supposons que $I = \langle f_1, \dots, f_s \rangle$, pour tout $i \in [1, s]$, on a

$LT(f_i) \in LT(I) \subset \langle LT(I) \rangle$, par suite $\langle LT(f_1), \dots, LT(f_s) \rangle \subset \langle LT(I) \rangle$.

Il est cependant possible que cette inclusion soit stricte, comme l'illustre l'exemple suivant.

Exemple 2.7

On fixe l'ordre lexicographique sur les monômes de $\mathbb{R}[x, y]$, avec $y < x$.

Soient $I = \langle f_1, f_2 \rangle$ l'idéal de $\mathbb{R}[x, y]$ engendré par les polynômes $f_1 = xy + 1$ et $f_2 = y^2 - 1$. Considérons le polynôme $f = xy^2 - x$, on a :

$xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y)$, et $xy^2 - x = x(y^2 - 1) + 0(xy + 1) + 0$.

La seconde équation montre que $f \in I$ et d'après la première équation, on a :

$-x - y = f - y f_1 \in I$. Ainsi $x + y \in I$ et $LT(x + y) = x \in \langle LT(I) \rangle$. Or

$x \notin \langle LT(f_1), LT(f_2) \rangle = \langle xy, y^2 \rangle$ car x n'est pas divisible par xy ou y^2 . L'inclusion $\langle LT(f_1), LT(f_2) \rangle \subset \langle LT(I) \rangle$.

Proposition 2.7

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

On a que :

- $\langle LT(I) \rangle$ est un idéal monomial.
- Il existe $f_1, \dots, f_s \in I$ tel que $\langle LT(I) \rangle = \langle LT(f_1), \dots, LT(f_s) \rangle$.

Preuve.

Voir (Cox, 1996) page 73. ■

Remarque 2.6

Soit I un idéal monomial. Un polynôme $f \in \mathbb{K}[x_1, \dots, x_n]$ appartient à I si et seulement si f est une combinaison linéaire des monômes appartenant à I .

Théorème 2.2 (Lemme de Dickson)

Soit I un idéal monomial et $E \subset \mathbb{N}^n$ une partie non vide tels que les monômes x^α engendrent I . Il existe alors des éléments $\alpha_1, \dots, \alpha_s$ dans E tels que les monômes $x^{\alpha_1}, \dots, x^{\alpha_s}$ engendrent I . En particulier I est de type fini.

Remarque 2.7

Un ensemble de générateurs d'un idéal est parfois appelé base d'un idéal.

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, par la proposition (2.7), 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 la proposition (2.6), 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

Etude sur le problème de l'appartenance d'un polynôme à un idéal.

3.1 Algorithme de division des polynômes à plusieurs variables.

Définition 3.1

Soit $A = \mathbb{K}[x_1, \dots, x_n]$, où \mathbb{K} est un corps commutatif et soit \preccurlyeq un ordre monomial sur A et soient f_1, \dots, f_s des éléments de A . Soient l'idéal $I = \langle f_1, \dots, f_s \rangle$ de A et une permutation σ de l'ensemble $\{1, \dots, s\}$. L'algorithme de division de polynômes sert à diviser un polynôme f de A par une suite de polynômes $F = (f_1, \dots, f_s)$ de A . Ce qui permet d'exprimer f sous la forme :

$$f = a_1 f_1 + \dots + a_s f_s + r$$

où les a_i , appelés quotients, sont des polynômes de A et r appelé reste, est aussi un polynôme de A . L'écriture de f sous la forme $f = a_1 f_1 + \dots + a_s f_s + r$, où aucun terme de r n'est divisible par un des $LT(f_i)$, pour $i = 1 \dots s$, est unique. r est le reste de la division de f par F et ce, quelque soit la permutation σ . En effet, le reste de la division de f par (f_1, \dots, f_s) est égal au reste de la division de I par $(f_{\sigma(1)}, \dots, f_{\sigma(s)})$.

Nous verrons plus tard que si le reste n'est pas nul, alors le polynôme f à diviser n'est pas dans l'idéal I . L'inverse n'est pas toujours vrai. Notons par f^{-F} , le reste de la division de f par les f_i de F .

Algorithme 3.1 (*Algorithme de division de polynômes*)

Prenons un polynôme f de A , (f_1, \dots, f_s) une suite de polynômes de A et \preccurlyeq un ordre monomial sur A . Calculons d'abord $LT(f)$ et $LT(f_i)$ pour $i = 1, \dots, s$, selon \preccurlyeq .

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 :

$$f := f - \frac{LT(f)}{LT(f_i)} f_i \text{ et } a_i := a_i + \frac{LT(f)}{LT(f_i)}.$$

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 $f = 0$.

Pour voir que l'algorithme se termine, observons qu'à chaque fois que la variable f est redéfini, soit son degré baisse, soit elle devient nulle. Ainsi, $f = 0$ arrivera forcément après un nombre fini d'étapes de l'algorithme et il se terminera.

Exemple 3.1

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

3.2 Base de Gröbner.

Définition 3.2

Un ordre monomial étant fixé, un sous-ensemble fini $G = \{g_1, \dots, g_t\}$ d'un idéal I est appelé base de Gröbner (ou base standard) si $\langle LT(g_1), \dots, LT(g_t) \rangle = \langle LT(I) \rangle$.

Exemple 3.2

On fixe l'ordre lexicographique sur les monômes de $\mathbb{R}[x, y]$ avec l'ordre alphabétique $y < x$. Soient $I = \langle f_1, f_2 \rangle$ l'idéal de $\mathbb{R}[x, y]$ engendré par les polynômes $f_1 = xy + 1$ et $f_2 = y^2 - 1$. On a vu dans l'exemple (2.7) que l'inclusion $\langle LT(f_1), LT(f_2) \rangle \subset \langle LT(I) \rangle$, est stricte, par suite $\{f_1, f_2\}$ n'est pas une base de Gröbner de I .

Exemple 3.3

Considérons les polynômes $g_1 = z + x$ et $g_2 = y - x$ de $\mathbb{Q}[x, y, z]$. On utilise l'ordre lexicographique sur $\mathbb{Q}[x, y, z]$ avec $x < y < z$. Montrons que $G = \{g_1, g_2\}$ est une base de Gröbner de l'idéal $I = \langle g_1, g_2 \rangle$. Supposons le contraire, c'est-à-dire qu'il existe $f \in I$, tel que $LT(f) \notin \langle LT(g_1), LT(g_2) \rangle = \langle z, y \rangle$.

Alors z ne divise pas $LT(f)$ et y ne divise pas $LT(f)$. En raison de l'ordre lexicographique, z et y n'apparaissent pas non plus dans les autres termes de f . Par suite, f est un polynôme en la seule indéterminée x . Par ailleurs, on a $f = h_1(z + x) + h_2(y - x)$, avec $h_1, h_2 \in \mathbb{Q}[x, y, z]$. On a alors pour tous $a, c \in \mathbb{Q}$, $f(a, a, c) = h_1(a, a, c)(a + c)$.

Comme \mathbb{Q} est infini et y n'apparaît pas dans les termes de f , on en déduit que $f = h_1(x, x, z)(x + z)$. Par suite $z + x$ divise f , qui est contradictoire avec le fait que f est d'une seule indéterminée x . Ainsi, G est une base de Gröbner de I .

Théorème 3.2

Tout idéal $I \subset \mathbb{K}[x_1, \dots, x_n]$ non nul possède une base de Gröbner. De plus toute base de Gröbner de I engendre I .

Preuve.

Nous avons vu l'existence d'une base de Gröbner avec la proposition (2.7). Reste à voir qu'une base de Gröbner $\{g_1, \dots, g_t\}$ engendre I .

On a bien évidemment $\langle g_1, \dots, g_t \rangle \subset I$ puisque g_i sont dans I . Montrons l'inclusion réciproque. Soit f un élément de I . L'algorithme de division de f par $\{g_1, \dots, g_t\}$ permet d'écrire $f = a_1g_1 + \dots + a_tg_t + r$ avec a_1, \dots, a_t des polynômes et r un polynôme

dont les termes ne sont divisibles par aucun $LT(g_i)$.

Supposons $r \neq 0$. Dans ce cas puisque $r \in I$, on voit que

$$LT(r) \in \langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle.$$

La proposition (2.6) assure que l'un des $LT(g_i)$ divise $LT(r)$, ce qui est absurde. On voit donc que r est nul, ce qui prouve que f appartient bien à $\langle g_1, \dots, g_t \rangle$. ■

3.2.1 Propriétés des bases de Gröbner

Proposition 3.1

Soient $G = \{g_1, \dots, g_t\}$ une base de Gröbner d'un idéal non nul $I \subset \mathbb{K}[x_1, \dots, x_n]$ et $f \in \mathbb{K}[x_1, \dots, x_n]$. Il existe un unique $r \in \mathbb{K}[x_1, \dots, x_n]$ satisfaisant aux deux propriétés suivantes :

1. Les termes de r ne sont divisibles par aucun $LT(g_i)$.
2. Il existe $g \in I$ tel que $f = g + r$.

Le reste est appelé la forme normale du polynôme f par la division par G . On note $f \xrightarrow{G} r$.

Preuve.

Divisons le polynôme f par $\{g_1, \dots, g_t\}$, d'après la définition(3.1), il existe des polynômes u_1, \dots, u_t et r , tels que $f = u_1g_1 + \dots + u_tg_t + r$, où r satisfait à l'assertion 1). En posant, $g = u_1g_1 + \dots + u_tg_t$, le polynôme r satisfait aussi à l'assertion 2).

Montrons l'unicité de r . Supposons qu'il existe r et r' satisfaisant les deux assertions : $f = g + r = g' + r'$. Alors $r - r' = g' - g \in I$.

Ainsi, si $r \neq r'$, on a $LT(r - r') \in \langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$.

Par suite, $LT(r - r')$ est divisible par un $LT(g_i)$. Or, ceci est impossible puisque aucun terme de r et r' n'est divisible par $LT(g_1), \dots, LT(g_t)$. Par suite, $r - r'$ doit être nul, ce qui montre l'unicité.

La dernière assertion de la proposition est une conséquence de l'unicité du reste. Attention, même si le reste est unique, les quotients u_1, \dots, u_s peuvent être différents d'une décomposition à l'autre. ■

3.3 Problème de l'appartenance à un idéal.

Étant donné un idéal $I = \langle f_1, \dots, f_s \rangle$ et un polynôme f de $\mathbb{K}[x_1, \dots, x_n]$, déterminer si $f \in I$.

Proposition 3.2

Soit I un idéal de $\mathbb{K}[x_1, \dots, x_n]$ et soit $G = \{f_1, \dots, f_t\}$ une base de Gröbner de I . Un polynôme f de $\mathbb{K}[x_1, \dots, x_n]$ est un élément de I , si et seulement si, le reste de la division de f par G est égal à 0.

Autrement dit, $f \in I$, si et seulement si, $f \xrightarrow{G} 0$.

Preuve.

Si le reste est nul, alors $f \in I$. Inversement, étant donné $f \in I$, alors, on a une décomposition $f = f + 0$ satisfaisant les deux assertions de proposition (3.1). Par suite, 0 est le reste de la division de f par G . ■

Exemple 3.4

Considérons l'idéal $I = \langle f_1, f_2 \rangle$ de $\mathbb{Q}[x, y, z]$, avec $f_1 = xy - y^2$, $f_2 = x^2 - z^2$.

Soit $f = 2x^3y - xyz^2 - y^2z^2$, a-t-on $f \in I$? Considérons l'ordre lexicographique gradué, avec $z < y < x$, on a les réductions $xy \xrightarrow{f_1} y^2$, $x^2 \xrightarrow{f_2} z^2$.

L'ensemble $\{f_1, f_2\}$ n'est pas une base de Gröbner de I , car la paire critique

$x^2y \xrightarrow{f_1} xy^2 \xrightarrow{f_1} y^3$ et $x^2y \xrightarrow{f_2} yz^2$ n'est pas confluyente. Pour obtenir une base de Gröbner,

il suffit de compléter cette paire critique, car il n'apparaît pas d'autre paire critique

non confluyente. L'ensemble $G = \{f_1, f_2, f_3\}$, avec $f_3 = y^3 - yz^2$, est une base de

Gröbner de I . Pour tester l'appartenance de f à I , il suffit alors de diviser f par G ,

on a $f = 2xyf_1 + z^2f_2$. Le reste de cette division est nul, ainsi $f \in I$. Cela revient à

réduire le polynôme f par f_1 et f_2 et tester si la forme normale obtenue est nulle :

$$\begin{aligned} 2x^3y - xyz^2 - y^2z^2 &\xrightarrow{f_1} 2x^2y^2 - xyz^2 - y^2z^2 \xrightarrow{f_1} 2xy^3 - xyz^2 - y^2z^2 \xrightarrow{f_1} 2y^4 - xyz^2 - \\ &y^2z^2 \xrightarrow{f_1} 2y^4 - y^2z^2 - y^2z^2 \xrightarrow{f_3} 2y^2z^2 - 2y^2z^2 = 0. \end{aligned}$$

L'ordre d'application des réductions n'a pas d'influence sur le résultat, car G étant une base de Gröbner, le système est confluyente.

Ainsi, tout polynôme f tel que $LT(f)$ n'est pas dans l'idéal $\langle LT(G) \rangle = \langle xy, x^2, y^3 \rangle$

n'est pas dans I . Par exemple, le polynôme $f = zy - y^2$ n'est pas dans I , car il est

en forme normale par réduction par G .

Chapitre 4

Etude sur les variétés algébriques.

Définition 4.1

Soit $f = \sum_{(\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n} c_{\alpha_1 \dots \alpha_n} x_1^{\alpha_1} \dots x_n^{\alpha_n} \in \mathbb{F}_q[x_1, \dots, x_n]$, alors :

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

Exemple 4.1

Soit $\mathbb{F}_q[x, y, z]$, et $f = 4x^2 + 12xy - 10yz + 1$. On a f n'est pas homogène de degré total $d = 2$. Le composante homogène de degré $d = 2$ est : $f^{(2)} = 4x^2 + 12xy - 10yz$.

propriété 4.1

Un polynôme $f \in \mathbb{F}_q[x_1, \dots, x_n]$ de degré total $D \in \mathbb{N}$ se décompose de manière unique comme la somme de ses composantes homogènes non nulles. Autrement dit :

$$f = \sum_{\{d, 0 \leq d \leq D: f^{(d)} \neq 0\}} f^{(d)}.$$

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

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

Ce

polynôme homogénéisé peut aussi être calculé en utilisant la formule :

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

Exemple 4.2

Soit $f \in \mathbb{F}_q[x, y, z]$, $f = 4x^2 + 12xy - 10yz + 1$ et $D = 2$. pour $d = 0$, $f^{(0)} = 1$,
 $d = 1$, $f^{(1)} = 0$, $d = 2$, $f^{(2)} = 4x^2 + 12xy - 10yz$

$$\begin{aligned} \text{alors, } F(x, y, z, t) &= \sum_{d=0}^2 f^{(d)}(x, y, z) t^{2-d}. \\ &= f^{(0)}(x, y, z) t^2 + f^{(2)}(x, y, z) t^0. \\ &= t^2 + 4x^2 + 12xy - 10yz. \end{aligned}$$

Remarque 4.1

On remarquons que : $F(x_1, \dots, x_n, 1) = f(x_1, \dots, x_n)$.

Définition 4.2

Soient \mathbb{F} une extension de corps de \mathbb{F}_q et $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$. La variété affine (ou simplement variété), sur \mathbb{F} associée à f_1, \dots, f_m est définie comme l'ensemble des solutions à coefficients dans \mathbb{F} du système :

$$\left\{ \begin{array}{l} f_1(x_1, \dots, x_n) = 0; \\ f_2(x_1, \dots, x_n) = 0; \\ \vdots \\ f_m(x_1, \dots, x_n) = 0. \end{array} \right. \quad (*)$$

Cette variété sera notée :

$$\mathbf{V}_{\mathbb{F}}(f_1, \dots, f_m) = \{(z_1, \dots, z_n) \in \mathbb{F}^n : f_i(z_1, \dots, z_n) = 0, \text{ pour tout } i, 1 \leq i \leq m\}.$$

Nous dirons que le système (*) est de dimension zéro (ou zéro-dimensionnel) si,

$$|\mathbf{V}_{\overline{\mathbb{F}_q}}(f_1, \dots, f_m)| < \infty, \overline{\mathbb{F}_q} \text{ désignant la clôture algébrique de } \mathbb{F}_q.$$

Définition 4.3

Soient F_1, \dots, F_m les polynômes homogénéisés de f_1, \dots, f_m respectivement. Nous dirons que le système (*) est de dimension zéro à l'infini, si le système suivant l'est :

$$\left\{ \begin{array}{l} F_1(x_1, \dots, x_n, z) = 0; \\ F_2(x_1, \dots, x_n, z) = 0; \\ \vdots \\ F_m(x_1, \dots, x_n, z) = 0. \end{array} \right. \quad (\Delta)$$

Remarque 4.2

En homogénéisant les polynômes du système $(*)$, on peut faire apparaître des solutions à l'infini, c'est-à-dire des solutions de (Δ) pour lesquelles $z = 0$ qui ne sont pas des solutions du système de départ $(*)$. D'autre part, les solutions du système (Δ) pour lesquelles $z = 1$ correspondent exactement aux solutions de $(*)$.

Lemme 4.1

Soient \mathbb{F} une extension de corps de \mathbb{F}_q et $f_1, \dots, f_m, g_1, \dots, g_t$, des polynômes de $\mathbb{F}_q[x_1, \dots, x_n]$.

Alors : $\mathbf{V}_{\mathbb{F}}(f_1, \dots, f_m, g_1, \dots, g_t) = \mathbf{V}_{\mathbb{F}}(f_1, \dots, f_m) \cap \mathbf{V}_{\mathbb{F}}(g_1, \dots, g_t)$.

Ce lemme traduit simplement le fait qu'une solution, sur \mathbb{F} , du système polynomial : $f_1 = 0, \dots, f_m = 0, g_1 = 0, \dots, g_t = 0$, est un zéro commun, sur \mathbb{F} , des polynômes f_1, \dots, f_m et des polynômes g_1, \dots, g_t .

Remarque 4.3

Dans la suite, nous noterons plus simplement $\mathbf{V}(f_1, \dots, f_m)$ la variété $\mathbf{V}_{\mathbb{F}_q}(f_1, \dots, f_m)$.

Exemple 4.3

Soient $f_1 = y - x^2, f_2 = z - x^3 \in \mathbb{R}[x, y, z]$ et le système suivant :
$$\begin{cases} y - x^2 = 0; \\ z - x^3 = 0. \end{cases}$$

Alors, la variété affine de ce système est :

$$\mathbf{V}(f_1, f_2) = \{(a_1, a_2, a_3) \in \mathbb{R}^3 : f_i(a_1, a_2, a_3) = 0, \text{ pour tout } i, 1 \leq i \leq 2\}.$$

On peut $x = t$ alors,

$$\begin{cases} y - x^2 = 0; \\ z - x^3 = 0. \end{cases} \implies \begin{cases} y = x^2; \\ z = x^3. \end{cases} \implies \begin{cases} y = t^2; \\ z = t^3. \end{cases}$$

Donc $\mathbf{V}(f_1, f_2) = \{(t, t^2, t^3) : t \in \mathbb{R}\} \subset \mathbb{R}^3$.

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

Définition 4.4

Soit I un idéal de $\mathbb{K}[x_1, \dots, x_n]$. On note $\mathbf{V}(I)$ le sous-ensemble de \mathbb{K}^n défini par :

$$\mathbf{V}(I) = \{(a_1, \dots, a_n) \in \mathbb{K}^n \mid f(a_1, \dots, a_n) = 0, \text{ pour tout } f \in I\}.$$

Proposition 4.1

Pour tout idéal I de $\mathbb{K}[x_1, \dots, x_n]$, $\mathbf{V}(I)$ est un ensemble algébrique affine. En particulier, si $I = \langle f_1, \dots, f_s \rangle$, alors $\mathbf{V}(I) = \mathbf{V}(f_1, \dots, f_s)$.

Remarque 4.4

Il faut observer que I contient plus d'informations que $\mathbf{V}(I)$: par exemple considérons le système en une variable et une équation : $x_1^2 = 0$ dans $\mathbb{K} = \mathbb{C}$. l'idéal associé est $I_1 = \langle x_1^2 \rangle$ et la variété associée à I_1 est $\mathbf{V}(I_1) = \{0\}$.

Donc les idéaux I_1 et $I_2 = \langle x_1 \rangle$ ont la même variété algébrique associée $\{0\}$.

Remarque 4.5

On peut ainsi décrire $\mathbf{V}(I)$ à partir de toute base de I , en particulier avec une base de Gröbner calculée avec l'ordre lexicographique.

Exemple 4.4

On considère le système d'équations
$$\begin{cases} x^2 + y^2 + z^2 = 1 \\ x^2 + z^2 = y \\ x = z \end{cases}$$

dans \mathbb{C}^3 . Ces équations déterminent l'idéal

$$I = \langle x^2 + y^2 + z^2 - 1, x^2 + z^2 - y, x - z \rangle.$$

L'objectif est de décrire l'ensemble algébrique affine $\mathbf{V}(I)$. On calcule une base de Gröbner $G = \{g_1, g_2, g_3\}$ de l'idéal I en utilisant l'ordre lexicographique induit par l'ordre alphabétique $z < y < x$:

$$g_1 = x - z, g_2 = -y + 2z^2, g_3 = z^4 + \frac{1}{2}z^2 - \frac{1}{4}.$$

On a $\mathbf{V}(I) = \mathbf{V}(g_1, g_2, g_3)$. L'équation $g_3 = 0$ est de degré 4 en z , ses racines sont : $z = \pm \frac{1}{2}\sqrt{\pm\sqrt{5}-1}$. Des équations $g_1 = 0$ et $g_2 = 0$, on déduit alors les valeurs de x et de y .

Définition 4.5

Soit \mathbf{W} un ensemble de \mathbb{K}^n . Alors,

$I(\mathbf{W}) = \{f \in \mathbb{K}[x_1, \dots, x_n] \mid f(a_1, \dots, a_n) = 0, \forall (a_1, \dots, a_n) \in \mathbf{W}\}$ est un idéal.

Définition 4.6

Si I est un idéal, alors $\sqrt{I} = \{f \in \mathbb{K}[x_1, \dots, x_n] \mid \exists k \in \mathbb{N} \text{ tel que } f^k \in I\}$.

Théorème 4.1 (*Hilbert Nullstellensatz*)

Si I est un idéal de $\mathbb{K}[x_1, \dots, x_n]$ alors $I(\mathbf{V}_{\mathbb{K}}(I)) = \sqrt{I}$.

Si \mathbf{V} est une variété algébrique sur \mathbb{K} alors $\mathbf{V}_{\mathbb{K}}(I(\mathbf{V})) = \mathbf{V}$.

Définition 4.7

Une variété \mathbf{V} est dite irréductible si dans toute expression de \mathbf{V} comme union de deux variétés $\mathbf{V}_1 \cup \mathbf{V}_2$ on a $\mathbf{V} = \mathbf{V}_1$ ou $\mathbf{V} = \mathbf{V}_2$.

Proposition 4.2

Soit \mathbf{V} une variété algébrique. \mathbf{V} est irréductible, si et seulement si, $I(\mathbf{V})$ est premier.

Théorème 4.2

1. Si I est un idéal alors il existe J_1, \dots, J_K des idéaux premiers tels que $\sqrt{I} = \bigcap_{i=1}^K J_i$.
2. Si \mathbf{V} est une variété algébrique, il existe $\mathbf{V}_1, \dots, \mathbf{V}_K$ des variétés algébriques irréductibles telles que $\mathbf{V} = \bigcup_{i=1}^K \mathbf{V}_i$.

Conclusion

Dans ce mémoire, on s'intéresse à l'étude des ordres monomiaux et les variétés algébriques. Nous avons donné dans le premier chapitre quelques notions élémentaires sur les anneaux et la relation d'ordre.

Dans le deuxième chapitre, nous avons fait une étude sur les ordres monomiaux, quelques ordres monomiaux et l'idéal monomial.

Ensuite nous avons étudié la base de Gröbner et le problème de l'appartenance d'un polynôme à un idéal. Nous avons utilisé la base de Gröbner à le grand avantage de ramener l'étude des idéaux polynomiaux à l'étude des idéaux monomiaux, plus faciles à appréhender, ainsi que résoudre le problème de l'appartenance d'un polynôme à un idéal.

Finalement nous intéressons à quelques propriétés sur les variétés algébriques.

Bibliographie

- [1] **A. Amroun**, Cours Master1, *théorie des relations*, Université M.Boudiaf de Msila, année univ 2017-2018.
- [2] **P. Chris**, *Algèbre approfondie*, Notes de M2 (1995–1996), Université de Grenoble I Saint-Martin d’Hères, France, 26 Mai, 1997.
- [3] **D. Delaunay**, Cours Mathématiques KP, 1^{er} mai 2015, <http://mp.cpgedupuydelome.fr>.
- [4] **JCh. Faugère**, *Résolution des systèmes polynômiaux en utilisant les bases de Gröbner*, thèse de doctorat, INRIA (POLSYS) / UPMC / CNRS/ LIP6.
- [5] **N. Ghadbane**, Cours Mastre1, *Semi groupe et Automates fini*, Université M.Boudiaf de Msila, année univ 2017-2018.
- [6] **D. Guin**, *Algèbre II Anneaux, modules et algèbre multilinéaire*, collection enseignement SUP - Mathématiques, 17, avenue du Hoggar Parc d’activités de Courtabœuf, BP 112 91944 Les Ulis Cedex A, France.
- [7] **A. Kehaili**, *Bases de Grobner*, Mémoire pour l’obtention du diplôme de amgister en mathématiques, Université d’oran, Soutenu le 30 janvier 2013, Année univ 2012-2013.
- [8] **L. Ladjlat**, *Cours Master1, Algèbre (anneaux)*, Université M.Boudiaf de Msila. Année univ 2017-2018.
- [9] **M. Laurence**, *les bases de Grobner et les ordres monomiaux*, Mémoire de maitre, Université du Québec à Montréal, Avril 2008.
- [10] **P. Ludovic**, *Etude d’outils algébriques et combinatoires pour la cryptographie à clef publique*, Thèse de doctorat, Université de Marne-la-Vallée, 17 Octobre 2005.

- [11] **D. Mihoubi**, *Cours licence, théorie de groupe*, Université M.Boudiaf de Msila.
Année univ 2016-2017.
- [12] **N. Perrin**, Master 2 Algèbre appliquée, *Algèbre effective*, Université Paris-Saclay, année univ 2017-2018.
- [13] **D. Ponasse, JC.Carrega** , *Algèbre et Topologie Booléennes*, Paris New York
Barcelone Milan : MASSON, 1979.