UNIVERSITÉ MOHAMED BOUDIAF DE M'SILA
Faculté des Mathématiques et de l'Informatique
Département de Mathématiques

Présenté pour l'obtention du diplôme de MASTER

Domaine : Mathématiques et de L'informatique

Filière : Mathématiques

Option : Algèbre et Mathématiques Discrètes

Présenté par
ZOUID Lina, GOUMIDA Sabah

Sujet

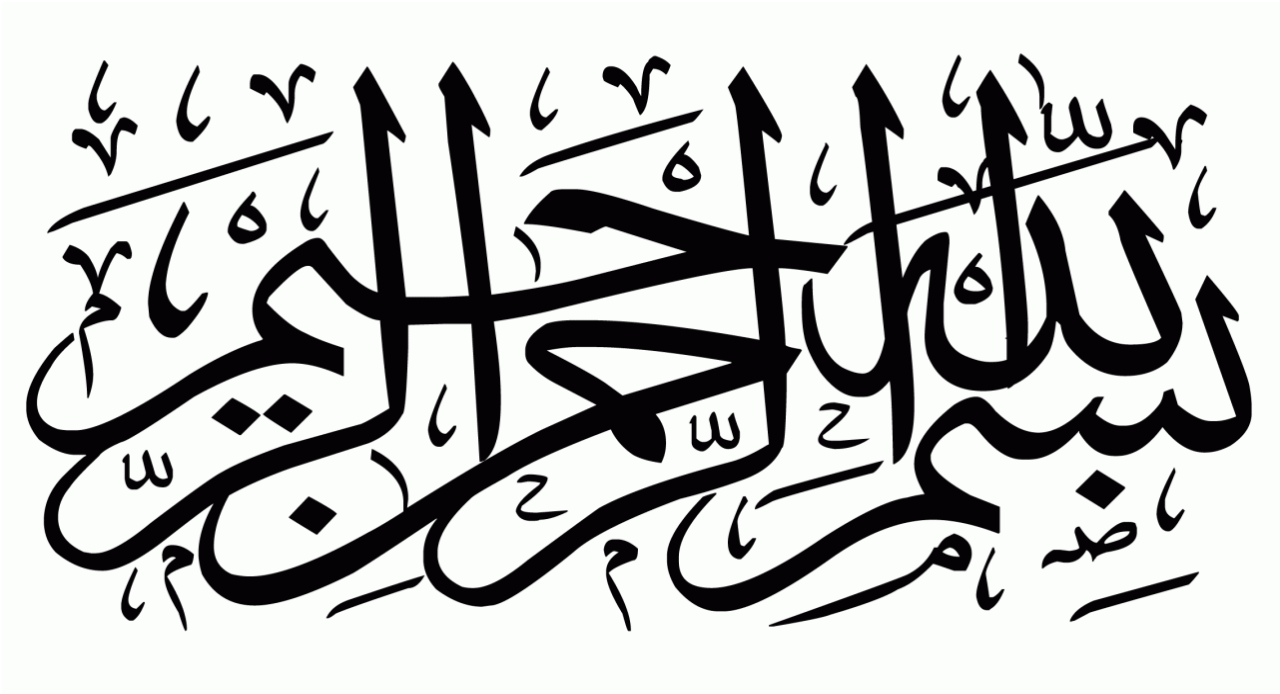
Sur l'anneau des polynômes en plusieurs indéterminées

Soutenu le :28/06/2022

Devant le jury :

Mr. Khadraoui Abdelmalek	M.A.A. Univ de M'sila	Président
Mr. Ladjelat Lahcene	M.A.A. Univ de M'sila	Encadreur
Mr. Dechoucha Noureddine	M.A.A. Univ de M'sila	Examinateur
Mr. Berrabah Imadeddine	E.Doct. Univ de M'sila	Invité

Promotion : 2021/2022


بسم الله الرحمن الرحيم

IL Y A DEUX CHOSES IMPORTANTES DANS NOTRE VIE :

APPRENDRE LES MATHÉMATIQUES

ET

ÉTUDIER LES MATHÉMATIQUES.

Remerciment

Avant tout, je remercie Dieu Tout-Puissant d'éclairer nos vies et de renforcer notre courage et notre courage pour terminer ce travail.

Je remercie Monsieur **L.LADJLET** de nous avoir proposé ce sujet et d'avoir accepté de nous encadrer.

Son énergie et sa confiance ont été pour nous des moteurs. Nous vous remercions pour tout.

Je tiens également à exprimer notre plus profonde gratitude à nos parents pour le soutien qu'ils nous ont apporté au fil des ans dans la poursuite de études et pour nous permettre de devenir ce que nous sommes aujourd'hui.

Enfin, un grand merci à nos familles, amis et collègues pour leurs encouragements et leur amitié.

Merci Beaucoup

Dédicace

Je dédie ce modeste travail à :

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

Mon deuxième père Saddam hocine,

Mes frère ; Ibrahim, Amer, Micho, et Abdelbasset.

Mes sœurs ; Guermia, Massaouda, Fadhila,

Toutes mes ameis, particulièrement : Lina , Chaima, Yousra , Achwaq, Chahinez, Ranya, Amel, Lamya.

tout ma famille «**GOUMIDA** » et « **BAKROU** ».

Toute la promotion 2022 de Université Mohamed Boudiaf (M'sila). Surtout le spécialité Algèbre et mathématique discret **(AMD)**

Goumida Sabah

Dédicace

Je dédie ce modeste travail :

-A mes chèrs parents "**Abdesselam et Hassina**",

-A mon chèrs frères : Mahfoud, Boularbah, Hamza,

-A mes chèrs sœurs : Razika, Aya,

-A toute la famille **Zouid**,

-A toute la famille **Hachrouf**,

-A tous mes amis : Aid Safia, Djenidi Dounia, Sahraoui Souheyla, Bouzina Amira, Hamidi Lobna, Salme Fatiha, Salamani Chaima, Massaouda, Khawla, Hayat, Karima, Nada, hassiba,.....,

-toute ma famille de département de Mathématiques,

-A toutes mes adorables que j'ai connu pendant toute ma vie . . .

Zouid Lina

Notations

- $(G, *)$: groupe minu par la loi interne "$*$ ".
- S_n : groupe symétrique de $\{1, 2, 3, ..., n\}$.
- $(A, +, *)$: Anneau minu par les deux lois de composition " $+$ "," $*$ ".
- $P(X)$: Un polynôme.
- $A[X]$: L'ensemble de polynôme à une indetermineé X et a coefficient dans A.
- $A[X_1, ..., X_n]$: L'anneau des polynômes en plusieurs indéterminеés.
- $\Bbbk[x_1, ..., x_n]$: L'ensemble des polynômes à n variables $x_1, ..., x_n$ à coefficients dans $\Bbbk$.
- $\deg_X(P)$: Degrè de polynôme à l'indeterminée X.
- $\mathbf{MD}(f)$: Le monôme directeur de f .
- $discP = \Delta_n$: Discriminant du polynôme de degré n.

Table des matières

Introduction

Les mathématiques sont l'une des sciences fondamentales à partir desquelles un grand nombre d'autres sciences ont émergé, et elles suscitent toujours beaucoup d'intérêt de la part des masses d'érudits et de chercheurs dans ce domaine.

La branche de l'algèbre est considérée comme la branche la plus complète de les mathématiques et l'arithmétique, car cela dépend de la formulation d'équations composées de variables et de catégories et néglige les nombres. Le sujet des anneaux et des polynômes en algèbre est un sujet nouveau et important (Abraham Fraenkel ,1914), souvent, le terme " polynôme en anneau" désigne implicitement le cas particulier d'un anneau polynomial dans un indéfini sur un corps. Ces anneaux polynomiaux ont le grand nombre de propriétés qu'ils ont en commun avec l'anneau entier.

Dans ce travail, qui traitera de anneau des polynômes en plusieurs indéterminées , il sera étudié en trois chapitres, la première chapitre portera sur les concepts initiaux de définitions, théories, et propriétés des anneaux, groupes, polynômes, et autres, tandis que la deuxième chapitre portera sur concernera les polynômes en plusieurs indéterminées et les polynômes symétriques, et nous étudierons ce dernier, sa structure et certaines de ses propriétés Quant à la dernière chapitre, elle inclura quelques applications des polynômes symétriques.

Chapitre 1

Notions élémentaires

1.1 Groupe

Définition 1.1.1 *Soit G un ensemble non vide, et soit la loi de composition intrene"$*$"*

$$\begin{array}{ccccccc} * & : & G & \times & G & \to & G \\ & & (& x,y &) & \mapsto & x*y \end{array}$$

*on dit que $(G,*)$ est un **groupe** s'il vérifie les conditions suivantes :*

i) *Pour tout $(x,y,z) \in G^3$, $(x*y)*z = x*(y*z)$.*

ii) *Il existe un élément $\mathbf{e} \in G$ tel que : pour tout $x \in G \quad x*e = x*e = x$.*

iii) *Pour tout $x \in G$, il existe $x^{'} \in G$ tel que : $x*x^{'} = x^{'}*x = \mathbf{e}$.*

De plus, si ;

$$\text{pour tout} \quad (x,y) \in G^2 : x*y = y*x$$

le groupe G est dit commutatif ou abélien.

Exemple 1.1.1 ***1)*** *l'ensemble des entiers relatif $\mathbb{Z}$, muni de l'addition usuelle est un groupe commutatif.*

Soient $(x,y,z) \in \mathbb{Z}$, $(x+y)+z = x+y+z = x+(y+z)$.

il existe $\mathbf{e} = 0$ tel que pour tout $x \in \mathbb{Z}$, $x+0 = 0+x = x$, pour tout $x \in \mathbb{Z}$, il existe $x\prime = -x$ tel que :

$$x+(-x) = x-x = (-x)+x = 0$$

on a :

$$\textit{pour tout } (x,y) \in \mathbb{Z}, \quad x+y = y+x.$$

Donc $(\mathbb{Z},+)$ *est un groupe commutatif.*
2) *Soit l'ensemble* $M(2,\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, (a,b,c,d\ ) \in \mathbb{Z}^4 \right\}$ *avec l'addition est un groupe.*
Soient N, G *et* K *des matrices de* $M(2,\mathbb{Z})$ *tel que :*

$$N = \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ G = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \textit{ et } K = \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}$$

$$\begin{aligned}
(N+G)+K &= \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \right) + \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} \\
&= \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d'' \end{pmatrix} + \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} \\
&= \begin{pmatrix} a+a'+a'' & b+b'+b'' \\ c+c'+c'' & d+d''+d''' \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a'+a'' & b'+b'' \\ c'+c'' & d+d''' \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} + \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} \right) \\
&= N + (G+K)
\end{aligned}$$

il existe $\mathbf{e} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ *tel que pour tout* $N \in M(2,\mathbb{Z})$ *on a :*

$$\mathbf{e}+N = N+e = N$$

pour tout $N \in M(2,\mathbb{Z})$*, il existe* $N' \in M(2,\mathbb{Z})$ *,* $N^{'} = -N$ *tel que :*

$$N+N' = N'+N = \mathbf{e}$$

pour tout $N, G \in M(2,\mathbb{Z})$ *on a :*

$$\begin{aligned} N+G &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \\ &= \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d'' \end{pmatrix} \\ &= \begin{pmatrix} a'+a & b'+b \\ c'+c & d'+d \end{pmatrix} \\ &= \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &= G+N \end{aligned}$$

Donc $(M(2,\mathbb{Z}),+)$ *est un groupe commutatif.*

3) pour tout $n>0$, $(\mathbb{Z}/n\mathbb{Z},+)$ *est un groupe commutatif tel que :* $\mathbb{Z}/n\mathbb{Z}=\left\{\overline{1},\overline{2},\overline{3},...,\overline{n-1}\right\}$.

Soient $(x,y,z)\in\mathbb{Z}/n\mathbb{Z}$ $(\overline{x}+\overline{y})+\overline{z}=\overline{x+y}+\overline{z}=\overline{x+y+z}=\overline{x}+\overline{y+z}=\overline{x}+(\overline{y}+\overline{z})$

il existe $\mathbf{e}=\overline{0}$ *tel que :*

$\forall x\in\mathbb{Z}/n\mathbb{Z}$,$\overline{x}+\overline{0}=\overline{x+0}=\overline{0+x}=\overline{x}$.

pour tout $x\in\mathbb{Z}/n\mathbb{Z}$, *il existe* $x'=\overline{-x}$ *tel que :*

$$\overline{x}+x'=\overline{x+(-x)}=\overline{x-x}=\overline{-x+x}=\overline{0}$$

on a , $\forall x,y\in\mathbb{Z}/n\mathbb{Z}$

$$\overline{x}+\overline{y}=\overline{y+x}=\overline{y}+\overline{x}$$

Donc $(\mathbb{Z}/n\mathbb{Z},+)$ *est un groupe commutatif .*

1.1.1 Sous-groupe

Définition 1.1.2 *Soient* $(G,*)$ *un groupe, et* H *un ensemble non vide. On dit* H *est* ***sous-groupe*** *de* G, *s'elle vérifie les conditions suivantes :*

i) *pour tout* $x,y\in H$, $x*y\in H$.

ii) *l'élément neutre* $\mathbf{e}\in H$.

iii) *pour tout* $x \in H, \quad x' \in H$.

Exemple 1.1.2 *1)* $(\mathbb{R}_+^*, \times)$ *est un sous-groupe de* $(\mathbb{R}^*, \times)$.

$1 \in \mathbb{R}_+^*$

si $x, y \in \mathbb{R}_+^*$ *alors* $x \times y \in \mathbb{R}_+^*$

si $x \in \mathbb{R}_+^*$ *alors* $x' = \frac{1}{x} \in \mathbb{R}_+^*$

2) $U = \{z \in \mathbb{C}, |z| = 1\}$ *est un sous-groupe* $(\mathbb{C}^*, \times)$.

$1 \in U$

si $z_1, z_2 \in U \quad |z_1 \times z_2| = |z_1| \times |z_2| = 1 \times 1 = 1$

si $z \in U \quad \left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$

3) L'ensemble des matrices $GL_n(\mathbb{R})$ *de déterminant* $\det(A) = 1$ *est un sous-groupe de* $(GL_n(\mathbb{R}), \times)$.

$$I_n \in H \qquad \det \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = 1$$

si $A, B \in H \qquad car \ \det(A, B) = 1 \times 1 = 1$

si $A \in H \quad \det(A) = 1 \quad \det(A^{-1}) = \frac{1}{\det(A)} = 1$

1.1.2 sous-groupe engendré

Définition 1.1.3 *Soient* $(G, *)$ *un groupe et un ensemble* $E \subset G$, ***le sous-groupe engendré*** *par* E *est le plus petit sous-groupe de* G *contenant* E.

Exemple 1.1.3 *Le groupe* $(\mathbb{R}^*, \times)$ *et* $E = \{2\}$ *le sous-groupe engendré par* E *est* $H = \{2^n \quad n \in \mathbb{Z}\}$.

1.1.3 Groupe symétrique

Définition 1.1.4 *Soit* E *un ensemble. Une bijection* f *de* E *vers* E *est appelée une permutation de* E.

L'ensemble des permutation de E *muni par la loi de composition des applications est un*

groupe, appelé le groupe symétrique de E, et noté S_E ou $S(E)$.

On note S_n le groupe symétrique de $\{1,2,3,...,n\}$, $n \in \mathbb{N}^*$, et on dit que S_n est le groupe symétrique de degré n. $Card(S_n) = n!$.

Soit f une permutation, tel que $f : \{1,2,3,...,n\} \longrightarrow \{1,2,3,...,n\}$

$$f = \begin{bmatrix} 1 & 2 & 3 & ... & n \\ f(1) & f(2) & f(3) & ... & f(n) \end{bmatrix}$$

L'inverse : $f^{-1} : \{1,2,3,...,n\} \longrightarrow \{1,2,3,...,n\}$

$$\begin{bmatrix} 1 & 2 & 3 & ... & n \\ f(1) & f(2) & f(3) & ... & f(n) \end{bmatrix} \uparrow f^{-1}$$

Composition de deux permutations :

Soient f ,g deux permutations :

$$f = \begin{bmatrix} 1 & 2 & 3 & ... & n \\ f(1) & f(2) & f(3) & ... & f(n) \end{bmatrix}, \quad g = \begin{bmatrix} 1 & 2 & 3 & ... & n \\ g(1) & g(2) & g(3) & ... & g(n) \end{bmatrix}$$

$$\begin{aligned} f \circ g &= \begin{bmatrix} 1 & 2 & 3 & ... & n \\ g(1) & g(2) & g(3) & ... & g(n) \\ f(g(1)) & f(g(2)) & f(g(3)) & ... & f(g(n)) \end{bmatrix} \\ &= \begin{bmatrix} 1 & 2 & 3 & ... & n \\ f(g(1)) & f(g(2)) & f(g(3)) & ... & f(g(n)) \end{bmatrix} \end{aligned}$$

Exemple 1.1.4 *Le groupe S_3 des permutations de $\{1,2,3\}$ à $3! = 6$ élémenets.*

$S_3 = \{id, \tau_1, \tau_2, \tau_3, \sigma, \sigma^{-1}\}$

$$id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \qquad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\tau_1 \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \tau_2 \ et \qquad \sigma \circ \tau_1 = \tau_3$$

$\sigma \circ \tau_1 \neq \tau_1 \circ \sigma$

alors le groupe ($S_3, \circ$) n'est pas commutatif.

1.2 Anneau

Définition 1.2.1 *Soit* **A** *un ensemble non vide , et soient les deux lois de compositions interne, notées "+" l'addition et "∗" la multiplication. On dit que le triplet* $(A,+,*)$ *est un* ***anneau*** *si :*

1) $(A,+)$ *est un groupe abélien .*

2) *pour tout* $(x,y,z)\in A^3 \quad (x*y)*z = x*(y*z)$.

3) *Il existe* $1_A \in A$, *pour tout* $x\in A$, $\quad x*1_A = 1_A*x = x$.

4) *pour tout* $(x,y,z)\in A^3 \quad x*(y+z) = x*y+x*z$, *et* $\quad (y+z)*x = y*x+z*x$.

Si la loi "∗" est commutative, on dit que A est un ***anneau commutatif unitaire .***

Exemple 1.2.1

1) *l'ensemble des entiers relatifs* $\mathbb{Z}$, *muni de l'addition et de la multiplication usuelles, est anneau commutatif :*

i) $(\mathbb{Z},+)$ *est un groupe commutatif* ***(1,1).***

ii) $\forall (a,b,c)\in\mathbb{Z}^3 \quad (a\times b)\times c = a\times b\times c = a\times(b\times c)$.

iii) $\exists e = 1\in\mathbb{Z}$, $\forall a\in\mathbb{Z} \qquad 1\times a = a\times 1 = a$.

iv) $\forall (a,b,c)\in\mathbb{Z}^3 \quad a\times(b+c) = a\times b + a\times c$, $(b+c)\times a = b\times a + c\times a$.

De plus on a :

$$\forall (a,b)\in\mathbb{Z}^2, \quad a\times b = b\times a.$$

2) *l'ensemble* $\mathbb{Z}/n\mathbb{Z}$ $(n>0)$, *muni par l'addition et de la multiplication usuelles, est un anneau unitaire commutatif .*

$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{1},\overline{2},\overline{3},...,\overline{n-1}\right\}$ *tel que :*

$$\begin{cases} \overline{x}+\overline{y} = \overline{x+y}. & \text{pour tout } x,y\in\mathbb{Z}/n\mathbb{Z} \\ \overline{x}\times\overline{y} = \overline{x\times y}. & \text{pour tout } x,y\in\mathbb{Z}/n\mathbb{Z} \end{cases}$$

i) $(\mathbb{Z}/n\mathbb{Z},+)$ *est un groupe commutatif* ***(def 1.1.1).***

ii) $\forall x,y,z\in\mathbb{Z}/n\mathbb{Z} \qquad (\overline{x}\times\overline{y})\times\overline{z} = \overline{x\times y}\times\overline{z} = \overline{x\times y\times z} = \overline{x}\times\overline{y\times z} = \overline{x}\times(\overline{y}\times\overline{z})$.

iii) $\exists\ e = \overline{1}\in\mathbb{Z}/n\mathbb{Z}$ *pour tout* $x\in\mathbb{Z}/n\mathbb{Z}$ *on a* $\overline{1}\times\overline{x} = \overline{x\times 1} = \overline{1\times x} = \overline{x}$

iv) $\forall x,y,z\in\mathbb{Z}/n\mathbb{Z} \qquad \overline{x}\times(\overline{y}+\overline{z}) = \overline{x}\times\overline{y}+\overline{x}\times\overline{z}$. *et* $(\overline{y}+\overline{z})\times\overline{x} = \overline{y}\times\overline{x}+\overline{z}\times\overline{x}$.

de plus on a :

$\forall x, y \in \mathbb{Z}/n\mathbb{Z} \qquad \overline{x} \times \overline{y} = \overline{x \times y} = \overline{y \times x} = \overline{y} \times \overline{x}$.

1.2.1 Sous-anneau

Définition 1.2.2 *Soit $(A, +, *)$ un anneau, B une partie non vide de A. On dit que B est un **sous-anneau** de A si et seulement si :*

$$\text{pour tout } x, y \in B : \quad \begin{cases} x - y \in B \\ x * y \in B \\ 1_A \in B \end{cases}$$

Exemple 1.2.2

$A = (\mathbb{Z}, +, \times)$

$B = n\mathbb{Z} = \{nx \qquad x \in \mathbb{Z}\}$

$B \neq \emptyset$ *car* $0 \in B$

$a = nx \ , b = ny \qquad x, y \in \mathbb{Z}$

1) $a - b = nx - ny = n(x - y) \quad = nt \qquad t = x - y \in \mathbb{Z}$

Donc $a - b \in B$

2) $a \times b = nx \times ny = n(xny) = nu \qquad u = xny \in \mathbb{Z}$

Donc $a \times b \in B$

B *sous-anneau de* $(\mathbb{Z}, +, \times)$

1.2.2 Ideaux

Définition 1.2.3 *Soit $(A, +, *)$ un anneau, et I un partie non vide de A. On dit que I un **idéal** de A si :*

i) *pour tout* $x, y \in A$, $\quad x - y \in I$.

ii) *pour tout* $x \in A$, *pour tout* $a \in I$, $ax \in I$ *et* $xa \in I$.

Exemple 1.2.3 ***1)*** $(\mathbb{Z}, +, \times)$ *n'est pas un idéal de* $(\mathbb{Q}, +, \times)$ *car :* $4 \in \mathbb{Z}$ *et* $\frac{2}{5} \in \mathbb{Q}$ *alors que* $4 \times \frac{2}{5} \notin \mathbb{Z}$.

2) K *cops comutatif,* X *indétèrminée sur* K , $f \in K[X]$

$< f(X) >= f\ K[X] = \{f \cdot g\ ,\quad g \in K[X]\ \}$ *est un idéal de* $K[X]$.

3) *K cops comutatif,* $K[X,Y]$

$(X,Y) = \{X \cdot f + Y \cdot g \qquad f,g \in K[X,Y]\}$

est un idéal de $K[X,Y]$.

Idéal propre :

Définition 1.2.4

Un idéal I d'un anneau est dit propre si : $I \neq \{\emptyset\}, \quad I \neq A.$

Exemple 1.2.4 $2\mathbb{Z}$ *est un idéal propre d'un anneau* $(\mathbb{Z},+,\times)$.
Si A est un anneau, $\{0\}$ *et A sont des idéaux de A, appelés idéaux triviaux. On appelle idéal propre tout idéal différent de A.*

Idéal premier :

Définition 1.2.5 *Un idéal I d'un anneau est dit premier si :*

$$\textit{pour tout}\ \ x,y \in A,\ x * y \in I\ \textit{alors}\ x \in I\ \textit{ou}\ y \in I\ .$$

Exemple 1.2.5 *Les idéaux premiers de* $(\mathbb{Z},+,\times)$ *sont les* $\{0\}$ *et les* $n\mathbb{Z}$ *pour n premier. Les idéaux* (X_1) *et* (X_1,X_2) *sont tous deux premiers dans* $K[X_1,X_2]$.

Idéal maximale :

Définition 1.2.6 *Un idéal I d'un anneant est dit maximale :*
s'il n'existe pas un idéal J distinct de A et I tel que $I \subset J$**.**

Exemple 1.2.6 *p premier,* $(p) = p\mathbb{Z}$ *est maximal de* $\mathbb{Z}$.
$p\mathbb{Z} \subset a\mathbb{Z} \Longrightarrow p \in a\mathbb{Z} \quad a/p \Longrightarrow a = 1$ *(donc* $a\mathbb{Z} = \mathbb{Z}$*) ou* $a = p$ *(*$a\mathbb{Z} = p\mathbb{Z}$*).*

Idéal engendré par une partie :

Définition 1.2.7 *L'idéal* ***engendré par une partie*** *de A, est l'ideal en particulier*:

$$< B >= (B) = \left\{ \sum_{i=1}^{n} a_i b_i \qquad a_i \in A, b_i \in B \right\}$$

Exemple 1.2.7 .
Pour un anneau commutatif A et un élément $a \in A$, l'idéal engendré par $\{a\}$ est aA.
l'idéal de $\mathbb{Z}$ engendré par $\{n\}$ est $n\mathbb{Z}$.

Idéal de type fini :

Définition 1.2.8 *Soit I un idéal d'un anneau A, I est dit de type fini s'il est engendré par un nombre fini d'éléments.*

Idéal principal :

Définition 1.2.9 *Un l'ideal I est principal s'il est engendré par un seul élément c'est à dire sous la forme,*

$$(a) = \{ax \quad \setminus \ x \in A\} = aA.$$

Exemple 1.2.8 *Dans $K[X]$, tout idéal est principal. Soit en effet I un idéal non trivial de $K[X]$. Soit $P_0 \in I$ non nul de degré minimum. Nous allons voir que $I = (P_0)$. Puisque $P_0 \in I$, il est clair que $(P_0) \subset I$. Soit réciproquement $P \in I$. On effectue la division euclidienne $P = QP_0 + R$. Alors $R = P - QP_0 \in I$. Mais comme $\deg R < \deg P_0$, le choix de P_0 (minimalité du degré) entraîne que $R = 0$, donc $P = QP_0 \in (P_0)$.*

1.2.3 Quelques exemples d'anneau

Anneau intègre :

Définition 1.2.10 *On dit que l'anneau A* ***intègre*** *si :*

$$pour\ tout\ (x, y) \in A^2 \qquad (x * y = 0) \Rightarrow (x = 0\ ou\ y = 0)$$

Exemple 1.2.9 ***1)*** $\mathbb{Z}$ *est un anneau intègre.*
2) $\mathbb{Z}/6\mathbb{Z}$ *est un anneau non intègre.*

Anneau noethérien :

Définition 1.2.11 *A est un anneau noethérien si, tout ses idéaux de A est engendré par sous- ensemble fini.*
si I est un ***idéal*** *de A, il existe a sous- ensemble fini* $S \subset A$ *tel que :* $(S) = I$.

Exemple 1.2.10 $\mathbb{Z}$ *est nœthérien : si*

$$n_0\mathbb{Z} \subset n_1\mathbb{Z} \subset ...$$

alors $n_i|\ n_{i-1}$ *donc* $|n_0| > ... > |n_i| > ....$

Anneau principal :

Définition 1.2.12 *Soit A un anneau.On dit que A est* ***principal*** *si et seulement si :*
1) *il est un intègre.*
2) *tout idéal de A est principal.*

Exemple 1.2.11 $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$ *des anneaus principaux.*

anneau factoriel :

Définition 1.2.13 *Un anneau commutatif intègre est appelé anneau* ***factoriel****, s'il vérifie les deux axiomes suivantes :*
Pour tout a non nul et non inversible :
i) $a = up_1p_2...p_m$ *avec* $u \in U(A)$,$m \in \mathbb{N}^*$ *et* $p_1, p_2, ..., p_m$ *des élément irréductible de A.*
ii) *Si* $a = vq_1q_2...q_m$ *avec* $v \in U(A)$, $m \in \mathbb{N}^*$ *et* $q_1q_2...q_m$ *irréductible dans A, alors* $n = m$ *et il existe une parmutation* σ *de* S_m *tel que :*

$$\text{pour tout } i = 1....n : \qquad q_i \sim p_{\sigma(i)}$$

Exemple 1.2.12 *l'anneau* $(\mathbb{Z}, +, \times)$ *est un anneau factoriel.*

Anneau quotient :

Définition 1.2.14 *Soit $(A,+,*)$ un anneau et I est un idéal de A.*
pour tout $a \in A$,definit la partie $a+I$ par :

$$a+I=\{a+i, \quad i \in I\}$$

appelée classe de a modulo I.

Proposition 1.2.1 *$(a+I)=(b+I)$ si et seulement si : $(a-b) \in I$, $0+I=I$.*

Soit l'ensemble A on defini la relation $\sim$ par :

$$a \sim b \Longleftrightarrow a+I=b+I \Longleftrightarrow (a-b) \in I.$$

$\sim$ est une relation d'equivalence sur A, de plus on a $\overline{a}=[a]=a+I$.

$$(A/\sim)=(A/I)=\{a+I, \quad a \in A\},$$

*sur A/I on définit les deux lois "**internes**" :*

i) L'addition : $(a+I)+(b+I)=(a+b)+I$.

ii) La multiplication : $(a+I)\times(b+I)=(a\times b)+I$.

$(A/I,+,\times)$ définit une structure d'anneau commutatif appele l'anneau quotien.

Exemple 1.2.13 $A=\mathbb{Z}, \quad I=n\mathbb{Z}, \quad A/I=\mathbb{Z}/n\mathbb{Z}$
Soit $(A,+,\times)$ un anneau commutatif et I est un idéal de $(A,+,\times)$
pour tout $a \in A$, $I=\{0\}$ $\quad a+\{0\} \longrightarrow a, \quad A \equiv A/I$

$I=A \qquad A/I=\{0\}$

$a+I=I \Longleftrightarrow a \in I$

$1 \in I \Longleftrightarrow I=A$

$x \in U(A)$: $\quad x \in I \Longleftrightarrow I=A$

1.2.4 Morphisme d'anneau

Définition 1.2.15

Soient $(A,+,\times),(B,+,\times)$,et soit l'application $f : A \to B$,on dit que f est un morphisme d'anneau si :

1) *pour tou t* $x,y \in A \quad f(x+y) = f(x)+f(y)$.

2) *pour tou t* $x,y \in A \quad f(x\times y) = f(x)\times f(y)$.

3) $f(1_A) = 1_B$.

Exemple 1.2.14 *Soit A un anneau, l'application identité :*

$$\begin{array}{rccc} \mathrm{Id_A}: & A & \to & A \\ & x & \longmapsto & x \end{array}$$

est un morphisme anneau.

1.3 Corps

Définition 1.3.1

On appelle corps tout anneau $(K,+,*)$ vérifiant :

1. *$(K,+,*)$ est commutatif.*

2. *K est non réduit à $\{0_K\}$.*

3. *Tous les éléments de K, sauf le nul, sont des éléments inversibles.*

Exemple 1.3.1

$(\mathbb{R},+,\times),(\mathbb{Q},+,\times),(\mathbb{C},+,\times)$ *munis par les opérations usuelles sont des corps.*

Remarque 1.3.1 *Tout anneau intègre fini est un corps .*

1.3.1 Caractérisation d'un corp fini

Définition 1.3.2 *Soit $(K,+,*)$ un corps fini. le Caractérisation d'un corp fini est un nombre premier p tel que $card(K) = p^n$ pour $n \in \mathbb{N}_0$.noteé par* ***Char*** $K = p$.

Exemple 1.3.2 *Soit $p \in \mathbb{N}$ premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps fini de p élément.*

Théorème 1.3.1 *Soit p un nombre premier.*

Pour chaque $r \in \mathbb{N}$ il existe un corps K de $q = p^r$ éléments.

1.3.2 Sous-Corps

Définition 1.3.3 *Soit $(K, +, \times)$ un corps, k est dite sous- corps si :*

1. *k est sous- anneau de $(K, +, \times)$.*
2. *Pour tout $x \in k$, $x \neq 0_K$, $x\prime \in k$.*

Exemple 1.3.3 *Q est un sous-corps de $(R, +, \times)$.*

1.3.3 Corps de fraction

Définition 1.3.4 *Soit A un anneau commutatif intègre est le plus petit corps commutatif contenant A, On définit sur $E = A \times A\backslash\{0\}$ deux lois internes et une relation d'équivalence $\Re$ compatible avec ces deux lois :*
pour tout (a, b) et (c, d) de E,

$$(a, b) + (c, d) = (ad + cb, bd) \ .$$

pour tout $(a, b)et\ (c, d)$ de E,

$$(a, b).(c, d) = (ac, bd) \ .$$

pour tout (a, b) et (c, d) de E,

$$(a, b)\Re(c, d) \Longleftrightarrow ad = bc$$

s'appelle corps des fractions de A. noteé par $F(A)$, $Frac(A)$.

Proposition 1.3.1 *Soit A un anneau intègre. Dans l'ensemble $K = A \times A^*$, la relation $\sim$ définie par :*
pour tout $a, b, c, d \in K$ on a :

$$(a, b) \sim (c, d) \text{ si et seulement si } ad = bc.$$

est une relation équivalence.

Exemple 1.3.4 $\mathbb{Q}$ *est le corps des fractions de* $\mathbb{Z}$.

1.4 Polynômes sur un corps

Définition 1.4.1 *Soit* $(A, +, \times)$ *un corps , X indetermineé, un polynôme* $P(X)$ *est une décomposition linéaire sous la forme*

$$\begin{aligned} P(X) &= a_n X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + ... + a_2X^2 + a_1X^1 + a_0 \\ &= \sum_{i=0}^{n} a_i X^i \quad tel\ que: \qquad a_i \in A,\ n \in \mathbb{N} \end{aligned}$$

.

i) *les* a_i *sont appelés* ***les coefficients*** *du polynôme.*

ii) *le coefficient* a_n*est appelé* ***le coefficients dominant .***

iii) *Si tout les coefficients* a_i *sont nuls,* P *est le polynôme* ***nul****, noté* 0.

iv) $P = a_0$*, est appelé un polynôme* ***constant.***

v) *Un élément* c *de* A *est appelé* ***racine*** *de* $P(X)$ *si :* $P(c) = 0$.

vi) *L'ensemble des polynômes à coefficients dans* A *est noté* $A[X]$.

vii) *le degré de* P *non nul note* $deg(P)$ *est l'entier* $d = sup\{i \quad \backslash a_i \neq 0\}$.

Remarque 1.4.1 *Soient* $P(X),\ Q(X)$ *deux polynômes de* $A[X]$ *on a :*

1) ***a)*** *degré de polynôme nul est* $(-\infty)$.

b) $\deg(P+Q) \leq \sup\{\deg(P), \deg(Q)\}$

c) *Si* $\deg(P) \neq \deg(Q), \deg(P+Q) = \sup\{\deg(P), \deg(Q)\}$

d) $\deg(PQ) = \deg(P) + \deg(Q)$

e) $\deg(P \circ Q) = \deg(P) \times \deg(Q)$

f) *Si* $\lambda \in K \quad et \quad A \in K[X]$, *alors :*

$$\deg(\lambda A) = \begin{cases} \deg(A) & si \ \ \lambda \neq 0 \\ -\infty & si\ \lambda = 0 \end{cases}$$

Si $(\lambda, \mu) \in K^2 et\ \ (A, B) \in K[X]^2$, *alors :* $\deg(\lambda A + \mu B) \leq \max(\deg A, \deg B)$.

2) a) Égalité :

$P = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X^1 + a_0$

$Q = b_nX^n + b_{n-1}X^{n-1} + ... + b_1X^1 + b_0$

$P = Q \quad ssi \quad a_i = b_i$ *pour tout* $i \in \mathbb{N}$.

b)Addition :

$P + Q = (a_n + b_n)X^n + (a_{n-1} + b_{n-1})X^{n-1} + ... + (a_1 + b_1)X^1 + (a_0 + b_0)$

c) Multiplication :

$P = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X^1 + a_0$

$Q = b_mX^m + b_{m-1}X^{m-1} + ... + b_1X^1 + b_0$

$P \cdot Q = c_rX^r + c_{r-1}X^{r-1} + ... + c_1X^1 + c_0$

avec $r = n + m$ *et* $c_k = \sum_{i+j=k} a_ib_j$ *pour* $k \in \{0, ..., r\}$.

d) Multiplication par un scalaire : *Soit* $\lambda \in A$, $\lambda \cdot P$ *est le polynôme dont le i-ème coefficient est* λa_i .

Exemple 1.4.1

$P = aX^4 + bX^3 + cX^2 + dX + e$, $Q = \alpha X^2 + \beta X + \gamma$

$\deg(P) = 4, \ \deg(Q) = 2$

$P + Q = aX^4 + bX^3 + (c + \alpha)X^2 + (d + \beta)X + (e + \gamma)$

$\deg(P + Q) = \sup\{\deg(P), \deg(Q)\} = \sup\{4, 2\} = 4 \qquad P \times Q = (a\alpha)X^6 + (a\beta + b\alpha)X^5 +$

$(a\gamma + b\beta + c\alpha)X^4 + (b\gamma + c\beta + d\alpha)X^3 + (c\gamma + d\beta + c\alpha)X^2 + (d\gamma + c\beta)X + (c\gamma)$

$\deg(P \times Q) = \deg(P) + \deg(Q) = 4 + 2 = 6$

$P = Q$ *si et seulement si* $a = 0$,$b = 0$,$c = \alpha$,$d = \beta$ *et* $e = \gamma$.

3) La division euclidienne de $P(X)$ par $Q(X)$ tel que $Q \neq 0$, alors il existe deux polynômes uniques $(Q(X), R(X)) \in (A[X])^2$ s'ecrit $P(X) = G(X)Q(X) + R(X)$ et $\deg(R) < \deg(G)$.

Exemple 1.4.2 $P(X) = X^3 + X^2 + 1$, $Q(X) = X - 1$

$P(X) = (X - 1)(X^2 + 2X + 2) + 3 \quad$ *tel que :* $G(X) = X^2 + 2X + 2$, $R(X) = 3$.

4) $P(X)$ est un **polynôme irréduclible** s'il est non constant et si les seule diviseurs de $P(X)$ sont les $\lambda \in A^*$ et les μP , ou $\mu \in A^*$.

Exemple 1.4.3

$f(x) = x^2 + 1$ *irréductible dans* $\mathbb{R}[X]$, *mais réductible dans* $\mathbb{C}[X]$.

Preuve. (1,b)

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 : $P(X) = \sum_i^n p_i X^i$ et $Q(X) = \sum_{i=0}^n q_i X^i$, ce qui donne $P(X) + Q(X) = \sum_i^n (p_i + q_i) X^i$, et prouve $\deg(P + Q) \leq n$. de plus, le terme de degré n est ($p_n + q_n$).

Si $\deg(P(X)) = \deg(Q(X))$.

(supose que : $\deg(P(X)) < \deg(Q(X))$), alors $p_n = 0$ et $q_n \neq 0$; et par suite $p_n + q_n \neq 0$, ce qui prouve que $P(X) + Q\ (X)$ est de degré n. ■

Définition 1.4.2 *Soit $A[X]$, où A est un corps commutatif, et soient $f(X)$ et $g(X)$ deux polynômes de $A[X]$.*

Un polynôme $D(X) \in A[X]$ est un plus grand commun diviseur ($p\gcd$) de $f(X)$ et $g(X)$ si les deux conditions suivants sont vérifées :

a) $D(X) \mid f(X)$ *et* $D(X) \mid g(X)$.

b) *si ;* $D'(X) \mid f(X)$ *et* $D'(X) \mid g(X)$, *alors* $D'(X) \mid D(X)$

on notée $p\gcd(f, g)$, (f, g), $f \wedge g$.

Exemple 1.4.4 $f(X) = x^5 + x +^4 2x^3 - 2x + 3$

$g(X) = x^4 + 3x^3 + 7x^2 + 8x + 6$

$p\gcd(f(X), g(X)) = x^2 + x + 3.$

Remarque 1.4.2 *soient $f(X), g(X)$ deux polynômes de $A[X]$, on dit que $f(X)$ et $g(X)$ sont premiers entre eux si :*

$$pgcd(f, g) = 1$$

Corollaire 1.4.1 *(relation de Bézout)*

Deux polynômes $f(X)$, $g(X)$ de $A[X]$, sont premiers si et seulement si : $C(X)$*et* $D(X) \in A[X]$ *, tels que :*

$$C(X)f(X) + D(X)g(X) = 1$$

Définition 1.4.3 *Soit $A[X]$, où A est un corps commutatif, et soient $f(X), g(X)$ deux polynômes de $A[X]$.*

Un polynôme $P(X) \in \mathbf{A}[\mathbf{X}]$ est le plus petit commun multiple (ppcm) de $f(X)$ et $g(X)$ si les deux condition suivants sont vérifées :

a) $f(X) \mid P(X)$ *et* $g(X) \mid P(X)$.

b) *si;* $f(X) \mid P'(X)$ *et* $g(X) \mid P'(X)$, *alors* $P(X) \mid P'(X)$

on notée ppcm (f, g), $[f, g]$, $f \vee g$.

Exemple 1.4.5

$p(x) = 3x^3 - 6x^2 - 9x$

$q(x) = 7x^4 + 21x^3 + 14x^2$

$ppcm(p(x), q(x)) = 21x^2(x + 1)(x - 3)(x + 2)$.

Définition 1.4.4 *Soit* $P(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$, *le contenu de P, noté cont(P), est par définition* $pgcd(a_0, ..., a_n)$.

Proposition 1.4.1 *(Lemme de G a u s s) :*
Soient P, Q $\in A[X]$, *on a :*

$$cont(PQ) = cont(P)cont(Q).$$

1.4.1 Les éléments irreductibles

Définition 1.4.5 *Un élément a d'un anneau intègre A est appelé irréductiple s'il n'est pas inversible et si une relation de la forme $a = bc$ implique que b ou c est inversible.*

Exemple 1.4.6 0 *n'est pas irréductible car* $0 = 0 \times 0$ *et* 0 *n'est pas inversible.*
Les élément rréductible de $\mathbb{Z}$ *sont de la forme* $\pm p$ *avec p premier.*

1.4.2 Les polynômes irreductibles

Définition 1.4.6 *Soit* $P(X)$ *un élément de* $A[X]$*de degré supérieur ou égal à* 1.
$P\ (X)$ *est irréductible sur* $A[X]$ *si et seulement s'il n'existe pas deux polynômes A et B, de*

degré supérieur ou égal à 1, *tel que :*

$$P = AB$$

Remarque 1.4.3 *Par défitnition : tout les polynôme de degré* 1 *sont irréductibles sur* A

Un polynôme $f(X)$ *irréductible sur* A; *ssi ; Pour tout* $g(X), h(X) \in A[X]$

$$(f(X) = g(X) \cdot h(X) \Longrightarrow (\deg g(X) = 0 \ ou \ \ \deg h(X) = 0).$$

Un polynôme qui n'a pas de racine dans A *n'est pas nécessairement irréductible sur* A.

Les polynômes de $\mathbb{R}[X]$, *irréductibles sur* $\mathbb{R}$, *sont les polynômes de degré* 2 *à discriminant strictement négatif.*

Exemple 1.4.7 $K = \mathbb{R}[X], \quad f(X) = x^2 + 1$ *irréductible sur* $\mathbb{R}$.
$K = \mathbb{Q}[X], \quad f(X) = x^3 - x + 1$ *irréductible sur* $\mathbb{Q}$.

Théorème 1.4.1 ***(Théorème de D'alembert-Gauss)***
Les polynômes irréductibles sur $\mathbb{C}$ *sont les polynômes de degré* 1.

Définition 1.4.7 *Soit* P *un polynôme de* $A[X]$, $\deg P \geq 1$.
P *est* ***scindé*** *sur* A *si et seulement si* P *est un produit de polynômes de degré* 1 *à coefficients dans* A.

Exemple 1.4.8 *le polynôme* $P = 2(X-1)^2(X-2) = (2X-2)(X-1)(X-2)$ *est scindé sur* $\mathbb{R}$.
Le polynôme $X^2 + 1$ *n'est pas scindé sur* $\mathbb{R}$.

1.5 L' anneau $A[X]$

Définition 1.5.1 *Soit* $(A, +, \times)$ *un anneau commutatif .*
$A[X]$ *l'ensemble de polynôme à indetermineé* X *et à coefficient dans* A, *muni des lois :*

1) *L'addition des polynômes :* $P + Q = (a_n + b_n)X^n + (a_{n-1} + b_{n-1})X^{n-1} + ... + (a_1 + b_1)X^1 + (a_0 + b_0)$.

2) *La multiplication des polynômes :*

$P \times Q = c_r X^r + c_{r-1} X^{r-1} + ... + c_1 X^1 + c_0.$

Proposition 1.5.1 $(A[X], +\times)$ *muni par l'addition et la multiplication des polynômes définit une structure d'anneau commutatif unitaire.*

Preuve.

1) On montre que $(A[X], +)$ est un groupe abélien.

i) La loi " + " est interne :

$P(X), Q(X) \in A[X] \Rightarrow P(X) + Q(X) \in A[X]$

Soient $P(X), Q(X) \in A[X]$

$$P(X) = \sum_{i=0}^{n} a_i X^i \qquad Q(X) = \sum_{i=0}^{n} b_i X^i \qquad a_i, b_i \in A$$

$$P(X) + Q(X) = \sum_{i=0}^{n} (a_i + b_i) X^i \qquad a_i + b_i \in A$$

Donc $P(X) + Q(X) \in A[X]$.

ii) La loi " + " est associative :

$$(P(X) + Q(X)) + G(X) = P(X) + (Q(X) + G(X))$$

Soient $P(X), Q(X), G(X) \in A[X]$, $G(X) = \sum_{i=0}^{n} c_i X^i$

$$\begin{aligned}
(\ P(X) + Q(X)) + G(X) &= (\sum_{i=0}^{n} (a_i + b_i) X^i) + \sum_{i=0}^{n} c_i X^i \\
&= \sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{n} b_i X^i + \sum_{i=0}^{n} c_i X^i \\
&= \sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{n} (b_i + c_i) X^i \\
&= P(X) + (Q(X) + G(X))
\end{aligned}$$

ii) La loi " + " admet un élément neutre :

$\exists E(X) = 0 = \sum_{i=0}^{n} 0_i X^i$ tel que : pour tout $P(X) \in A[X]$:

$E(X) + P(X) = P(X) + E(X) = P(X)$

iii) Existence d'un élément inverse : pour tout $P(X) \in A[X]$, il existe $P'(X) \in A[X]$ tel que :

$$\begin{aligned} P(X)+P'(X) &= \sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{n} a_i' X^i = 0 \\ &= \sum_{i=0}^{n} (a_i + a_i') X^i = 0 \\ &\Rightarrow \quad (a_i + a_i') = 0 \\ &\Rightarrow \quad a_i' = -a_i \end{aligned}$$

Donc $P'(X) = -P(X)$

iv) La loi " + " est commutatif : Soient $P(X), Q(X) \in A[X]$

$$P(X)+Q(X) = \sum_{i=0}^{n}(a_i+b_i)X^i = \sum_{i=0}^{n}(b_i+a_i)X^i \quad = Q(X)+P(X)$$

Alors $(A[X], +)$ est un groupe abélien.

2) La loi " $\times$ " est associative : pour tout $P(X), Q(X)$ et $G(X) \in A[X]$,

$P(X) = \sum_{i=0}^{n} a_i X^i$, $Q(X) = \sum_{j=0}^{m} b_j X^j$, et $G(X) = \sum_{k=0}^{l} c_k X^k$, $a_i, b_j, c_k \in A$

$$\begin{aligned} (P(X)\times Q(X))\times G(X) &= (\sum_{i=0}^{n} a_i X^i \times \sum_{j=0}^{m} b_j X^j) \times \sum_{k=0}^{l} c_k X^k \\ &= ((\sum_{i=0}^{n} a_i \times \sum_{j=0}^{m} b_j) X^{i+j}) \times \sum_{k=0}^{l} c_k X^k \\ &= \sum_{i=0}^{n} a_i \times (\sum_{j=0}^{m} b_j \times \sum_{k=0}^{l} c_k) X^i X^{j+k} \\ &= \sum_{i=0}^{n} a_i X^i \times (\sum_{j=0}^{m} b_j \times \sum_{k=0}^{l} c_k) X^{j+k} \\ &= P(X) \times (Q(X) \times G(X)) \end{aligned}$$

3)La loi " $\times$ " admet un élément neutre : Il existe $E'(X) = 1 \in A[X]$ (constant), tel que :

pour tout $P(X) \in A[X]$,

$$P(X)\times E'(X) = \sum_{i=0}^{n} a_i X^i \times 1 = 1 \times \sum_{i=0}^{n} a_i X^i = \sum_{i=0}^{n} a_i X^i = P(X)$$

4)La loi " $\times$ " est distribitif :

$$(P(X)+Q(X))\times G(X) = P(X)G(X)+Q(X)G(X)$$

Soient $P(X), Q(X), G(X) \in A[X]$,

$P(X)=\sum_{i=0}^{n} a_i X^i$, $Q(X)=\sum_{j=0}^{m} b_j X^j$, et $G(X)=\sum_{k=0}^{l} c_k X^k$, $a_i, b_j, c_k \in A$

$$\begin{aligned}(P(X)+Q(X))\times G(X) &= (\sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{m} b_j X^j) \times \sum_{i=0}^{l} c_i X^i \\ &= (\sum_{i=0}^{n} a_i X^i \times \sum_{k=0}^{l} c_k X^k) + (\sum_{i=0}^{m} b_j X^j \times \sum_{k=0}^{l} c_k X^k) \\ &= P(X)G(X)+Q(X)G(X)\end{aligned}$$

De plus, on a : Pour tout $P(X), Q(X) \in A[X]$,

$$\begin{aligned}P(X)\times Q(X) &= \sum_{i=0}^{n} a_i X^i \times \sum_{j=0}^{m} b_j X^j \\ &= (\sum_{i=0}^{n} a_i \times \sum_{j=0}^{m} b_j) X^{i+j} \\ &= (\sum_{i=0}^{n} b_j \times \sum_{j=0}^{m} a_i) X^{j+i} \\ &= \sum_{i=0}^{n} b_j X^j \times \sum_{j=0}^{m} a_i X^i \\ &= Q(X)\times P(X)\end{aligned}$$

La loi " $\times$ " est commutatif.

Donc $(A[X], +, \times)$ est un anneau commutatif unitaire . ■

Remarque 1.5.1 *$A[X]$ n'est pas un corps .*

1.5.1 Éléments inversibles dans $A[X]$

Définition 1.5.2 *dans l'anneau $A[X]$,les éléments inversibles sont les constants non nuls car :*

Si ; $P(X)$ *est inversible et son inverse* $Q(X)$*, alors* $P(X) \times Q(X) = 1$.
$\deg(P(X)) + \deg(Q(X)) = \deg(P(X) \times Q(X)) = 0$*, donc* $\deg(P(X)) = 0$.

Proposition 1.5.2 *En général, si* A *est un anneau intègre,* $F(A[X]) = F(A)(X)$ *avec* F *est le corps des fonction de* A.

1.5.2 Quelques propositions sur $A[X]$

1) Si A corps, alors $A[X]$ principal.

2) Si A corps, alors $A[X]$ euclidien.

3) Si A corps, alors $A[X]$ noétherien.

4) $A[X]$ est un anneau intégre.

5) $A[X]$ est un anneau principal.

6) Si A noétherien, alors $A[X]$ est noétherien.

7) Si A factoriel, alors $A[X]$ est factoriel.

8) $U(A) = U(A[X])$.

Preuve. 4$\Longrightarrow$) Soient $P(X)$ et $Q(X)$ deux polynômes non nuls dans $A[X]$, et $\deg(P) = m$, $\deg(Q) = n$

$$P(X) = \sum_{i=0}^{m} p_i X^i \qquad , Q(X) = \sum_{j=0}^{n} q_i X^i \qquad p_i \ \ , q_j \in A$$

et $(p_m, q_n) \neq (0, 0)$,Alors le produit $P(X) \times Q(X) \neq 0$ dont terme dominant est $p_m \times q_n$ $X^{m+n} \neq 0$. Donc $A[X]$ est intégre. De plus :

si $P(X) \times Q(X) = 0 \in A[X]$ Alors $p_m = 0$ ou $q_n = 0$. ∎

Preuve. 5$\Longrightarrow$Soit I un ideal de $A[X]$

Si $I = \{0\}$, $I = (0)$

Si $I \neq \{0\}$

Soit $P(X)$ un polynôme non nul dans I de dégre minimale, on montre que $I = (P(X))$
$Q(X) \in (P(X))$ c-à-dire : $\exists S(X) \in A[X]$ tel que: $Q(X) = P(X)S(X)$

$\subseteq$) Soit $Q(X) \in I$ un polynôme de plus petit dégre non nul
$\exists S(X), R(X) \in A[X]$ tel que :

$$Q(X) = P(X)S(X) + R(X) \qquad \text{avec} \ \ deg(R(X)) < deg(S(X))$$

Si $R(X) \neq 0$

$R(X) = Q(X) - P(X)S(X)$ $\qquad P(X)S(X) \in I$

$R(X) \in I$ $\qquad$ (comme $(I,+)$ un groupe)

contraduction

donc $\quad R(X) = 0$

$Q(X) = P(X)S(X) \quad \in (P(X\ ))$

Donc $\ I \subseteq (P(X))$

$\supseteq$) Soit $Q(X) \in (P(X\ ))$

$\exists S(X) \in A[X]$ tel que :

$Q(X) = P(X\ )S(X)$ $\qquad P(X\ ) \in I\ \ , S(X) \in A[X]$

Donc $Q(X) \in I$

Alors $\ (P(X)) \subseteq I$

Donc $\quad (P(X)) = I$

$A[X]$ est principal. ■

Preuve. 6$\Longrightarrow$) Supposons qu'il existe un idéal I de $A[X]$ non nul et de type infini.

Soit $P_1 \in I \setminus \{0\}$ de dégre minimal et $I \neq (P_1)$, P_2 est un polynôme fixé tel que : $P_2 \in I \setminus (P_1)$ de dégre minimal parmi les élément de $I \setminus (P_1)$. De proche en proche, on construit ainsi une suite $(P_n)_{n\geq 1}$ d'élément de I verifiant, pour tout $n \in \mathbb{N}^*$,$P_{n+1} \in I \setminus [(P_1) + ... + (P_n)]$.

$\deg(P_{n+1}) \leq \deg(Q)$, pour tout $Q \in I \setminus [(P_1) + ... + (P_n)]$

$\deg(P_{n+1}) \geq \deg(P_n)$, pour tout $\ n \in \mathbb{N}^*$

Notons a_n est un coefficient dominant de P_n et $\forall n \in \mathbb{N}^*$ posons : $b_n = Aa_1 + ... + Aa_n$

Alors $(b_n)_n$ une suite croissante d'ideaux de A .

Si A est noetherien, il existe $n \in \mathbb{N}^*$, $a_{n+1} \in b_n$ tel que :

$a_{n+1} = \lambda_1 a_1 + ... + \lambda_n a_n$ avec $\lambda_1, ..., \lambda_n \in A$, posons :

$Q = P_{n+1} - \sum_{i=1}^{n} \lambda_i X^{\deg(P_{n+1}) - \deg(P_i)} P_i$

on a $\deg(Q) < \deg(P_{n+1})$ et $\ Q \in I\ |[(P_1) + ... + (P_n)]$

contraduction. ■

Preuve. 7$\Longrightarrow$) On doit d'abord d´emontrer qu'on a l'existence de la d´ecomposition , Quitte à écrire $P = c(P)P_1$ et à décomposer $c(P)$ en produit d'irréductibles dans A, on se ramène à P primitif. On décompose alors P (qu'on peut supposer non constant) dans

l'anneau principal $K[X]$, soit $P = P_1...P_r$, ou encore $aP = Q_1...Q_r$ avec $Q_i \in A[X]$, $a \in A$, et Q_i irréductible dans $K[X]$. En passant aux contenus, on obtient $a = c(Q_1)...c(Q_r)(modA^*)$ et d'aprés le théorème précédent $P = u \times \prod_{i=1}^{n} \frac{Q_i}{c(Q_i)}$ (avec $u \in A^*$) est une décomposition de P en produits d'irréductibles de $A[X]$, puisque chaque $\prod_{i=1}^{n} \frac{Q_i}{c(Q_i)}$ est un polynôme primitif de $A[X]$ qui est irréductible dans $K[X]$ (il est le produit de Q_i par une constante deK^*). Si $P \in A[X]$ est irréductible, alors (P) est premier. Si $P = p$ est une constante irréductible de $A[X]$, alors p n'est pas inversible et si p divise un produit QR de deux polynômes de $A[X]$, alors il divise aussi le contenu $c(QR) = c(Q)c(R)$, donc il divise $c(Q)$ ou $c(R)$ vu que (p) est premier dans A (puisque Aest factoriel). Ainsi la constante p divise bien Q ou R dans $A[X]$ (on aurait pu aussi remarquer que $A[X]/(p)$ est isomorphe à $(A/(p))[X]$, qui est intègre vu que (p) est premier dans A). ■

Chapitre 2

Polynômes à plusieurs indéterminées

2.1 Polynômes en deux indéterminées

Définition 2.1.1 *Soit $A[X]$ un anneau commutatif unitère* ***(déf 1.5.1)*** *.*
et soit Y indéterminée sur $A[X]$, tels que :

Pour tout polynôme $F(Y) \in A[X][Y]$, on a :

$$\begin{aligned} F(Y) &= a_0(X) + a_1(X)Y + a_2(X)Y^2 + ... + a_n(X)Y^n \\ &= \sum_{j=0}^{n} a_j(X)Y^j \quad , a_j(X) \in A[X] \end{aligned}$$

définit une structure d'anneau commutatif unitaire $(A[X][Y], +, \times)$.

Remarque 2.1.1
$(A[X][Y], +, \times)$ est un anneau commutatif unitère .
1) *Pour tout polynôme $F(Y) \in A[X][Y]$ on a :*

$$\begin{aligned} F(Y) &= \sum_{j=0}^{n} a_j(X)Y^j \quad , a_j(X) \in A[X] \\ &= \sum_{j=0}^{n} (\sum_{i=0}^{n} a_i X^i)_j Y^j \\ &= \sum_{i=0}^{n} (\sum_{j=0}^{n} a_{ij} Y^j) X^i \\ &= \sum_{i=0}^{n} (\sum_{j=0}^{n} a_j Y^j)_i X^i \quad , a_i(y) \in A[Y] \\ &= \sum_{i=0}^{n} a_i(y) X^i \quad \in A[Y][X] \end{aligned}$$

Donc $A[X][Y] = A[Y][X]$.

2) *Pour tout polynôme* $G(Y) \in A[X][Y]$ *on a :*

$$\begin{aligned} G(Y) &= \sum_{j=0}^{n} a_j(X)Y^j \quad , a_j(X) \in A[X] \\ &= \sum_{j=0}^{n}(\sum_{i=0}^{n} a_i X^i)_j Y^j \\ &= \sum_{j,i\in\mathbb{N}} a_{ij}X^iY^j \qquad a_{ij} \in A \end{aligned}$$

$G(Y) \in A[X,Y]$

Donc $A[X][Y] \widetilde{\rightarrow} A[X,Y]$

Définition 2.1.2 $A[X,Y]$ *est appellée l'anneau des polynômes à deux indéterminées* X *et* Y*.*

2.2 Polynômes en plusieur indéterminées

Définition 2.2.1 *Soit* A *un anneau commutatif et* $X_1, ..., X_n$ *indéterminées sur* A*.*
On note $A[X_1, ..., X_n]$ *l'ensemble des polynômes à* $X_1, ..., X_n$ *variables et à cofficients dans* A*, avec un nombre fini de termes non nuls, écrit comme combinaisons linéaires des* $X_1^{k_1}.....X_n^{k_n}$*.*
$k_j \geq 0$ *: s'écrivent sous la forme :*

$$P = \sum_{k_1...k_n} a_{k_1...k_n} X_1^{k_1}.....X_n^{k_n} = \sum\nolimits_k a_k X_1^{k_1}.....X_n^{k_n}.$$

$A[X_1, ..., X_n]$ *est muni des opérations :*

$$(\sum\nolimits_k a_k X_1^{k_1}.....X_n^{k_n}) + (\sum\nolimits_k b_k X_1^{k_1}.....X_n^{k_n}) = \sum\nolimits_k (a_k + b_k) X_1^{k_1}.....X_n^{k_n}.$$

$$(\sum\nolimits_k a_k X_1^{k_1}.....X_n^{k_n})(\sum\nolimits_l b_l X_1^{l_1}.....X_n^{l_n}) = \sum\nolimits_t c_t X_1^{t_1}.....X_n^{t_n} \text{ avec } c_t = \sum_{t=k+l} a_k b_l.$$

$.(A[X_1, ..., X_n], +, \times)$ *est l'anneau des polynômes en plusieurs indéterminées.*

Corollaire 2.2.1 *On a un isomorphisme d'algèbres naturel* $A[X_1, ..., X_{n_{-1}}][X_n] \widetilde{\rightarrow} A[X_1, ..., X_{n_{-1}}, X_n]$.

2.2.1 Dégre d'un polynôme

Soit $P \in A[X,Y]$.

Si on considère $P \in A[X][Y]$,on peut définir son degré en tant que polynôme en$Y$.

Si on considère $P \in A[Y][X]$,on peut définir son degré en tant que polynôme en X.

le degré total d'un monôme $aX_1^{i_1}...X_s^{i_s}$ est la somme $i_1 + ... + i_s$.

le degré total d'un polynôme est le maximum des degrés tataux de ses monômes.

Exemple 2.2.1 $P = X^3Y^2 + Y^4 - XY^3 + X^2$.

$\deg_X(P) = 3$.

$\deg_Y(P) = 4$.

dégre totale de $P(X, Y)$ *est* 5.

2.2.2 Polynôme homogène

Définition 2.2.2 *Un polynôme homogène est un polynôme dont tous les monômes ont le même degré total.*

Exemple 2.2.2 $F(X, Y, Z) = 3X^4 + 5X^2YZ - 7Y^2Z^2$.

$F(X, Y, Z)$ *est un polynôme homogène de degré* 4 *de* $A[X, Y, Z]$.

Remarque 2.2.1

1) *Soit* f *un polynôme non nul dans* $A[X_1, X_2, ..., X_n]$, $n > 1$, *le monôme le plus haut, degré parmi ceux dont il est la somme, est appelé* ***le monôme directeur de*** f *; notée par* $\mathbf{MD}(f)$.

2) *A étant un domaine d'intégrité, pour deux polynômes non nuls* f *et* g *dans* $A[X_1, X_2, ..., X_n]$, $n \geq 1$, *on a :*

$$\mathbf{MD}(fg) \ = \ \mathbf{MD}(f)\mathbf{MD}(g).$$

Proposition 2.2.1 *Soit A un anneau .*

Si A est intègre, alors $A[X_1, ..., X_n]$ *est intègre.*

Théorème 2.2.1 *[Théorème de Gauss]*

Si A est un anneau factoriel, si $n \geq 1$ *est un entier, et si* $X_1, ..., X_n$ *sont des indéterminées, alors l'anneau de polynômes* $A[X_1, ..., X_n]$ *est aussi factoriel.*

Plus précisément, son groupe des unités est :

$$(A[X_1, ..., X_n])^\times = A^\times$$

et tout polynôme $P \in A[X_1, ..., X_n]$ *de degré* ≥ 1 *admet une décomposition :*
$P(X) = uP_1(X)...P_K(X)$, *avec* $u \in A^\times$ *et* $P_1, ..., P_K$ *polynômes irréductibles de degrés* ≥ 1.

Théorème 2.2.2 *(Théorème de Hilbert)*

Si A *est un anneau noethérien, alors pour tout* $n \in N^*$, *l'anneau* $A[X_1, ., X_n]$ *est noethérien.*

Preuve.

Dans A, l'idéal engendré par des éléments $x_1, x_2, ..., x_k$ sera noté $(x_1, x_2, ... , x_k)$.

1) Cas $n = 1$. Pour prouver que :

$$A \text{ noethérien} \Rightarrow A[X] \text{ noethérien}$$

démontrons la contraposée de cette implication, c'est-à-dire :

$$A[X] \text{ non noethérien} \Rightarrow A \text{ non noethérien.}$$

Si l'anneau $A[X]$ n'est pas noethérien, il contient au moins un idéal propre, non nul I, qui n'est pas de type fini.

Soit $f_1 \in I\backslash(0)$, de degré minimal ; l'hypothèse implique $I \neq (f_1)$. On en déduit qu'il existe $f_2 \in I\backslash(f_1)$, que l'on choisit de degré minimal.

Ainsi de proche en proche, pour tout entier $k \geqslant 1$, on choisit $f_{k+1} \in I\backslash(f_1, f_2, ..., f_k)$, de degré minimal.

Posons $n_k = \deg f_k$; le choix des f_k, pour $k \in N^*$, implique $1 \leq n_1 \leq n_2 \leq ... \leq n_k \leq n_{k+l} \leq .....$

D'autre part, pour tout$k \in N^*$, notons a_k le coefficient directeur. du polynôme f_k et considérons la chaîne croissante d'idéaux de A :

$(a_1) \subseteq (a_1, a_2) \subseteq ... \subseteq (a_1, ..., a_k) \subseteq (a1, ...,a_k,a_{k+1}) \subseteq .....$

Si cette chaîne était stationnaire, il existerait un entier $k > 0$ tel que :

$$(a_1, ..., a_k) = (a_1, ..., a_k, a_{k+l})$$

on pourrait donc écrire dans A,

$$a_{k+1} = \sum_{1\leq i\leq k} b_i a_i, \text{où } \ \forall i(1 \leq i \leq k), b_i \in A.$$

En posant $g = f_{k+l} - \sum_{1\leq i\leq k} biX^{n_{k+1}-n_i} f_i$. on aurait $g \in I\backslash(f_1, f_2, ..., f_k)$ et $\deg g < \deg f_{k+1}$

ce qui est contraire au choix de f_{k+1}.

2) Pour $n > 1$, on raisonne par récurrence sur n.

Supposons l'anneau $A[X_1, ..., X_{n-1}]$ noethérien, alors le résultat démontré pour $n = 1$, implique $A[X_1, ..., X_n] = A[X_1, ..., X_{n-1}]\ [X_n]$. ■

2.3 Polynôme symétrique

Définition 2.3.1 *Soit $A[X_1, ..., X_n]$ anneau des polynôme à n indéterminées. Un polynôme $P \in A[X_1, ..., X_n]$ est dite symétrique si :*

pour tout permutation $\sigma \in S_n$ (groupe des permutations de $\{1...n\}$) on a :

$P(X_{\sigma(1)}, X_{\sigma(2)}, ..., X_{\sigma(n)}) = \quad P(X_1, X_2, ..., X_n)$.

Exemple 2.3.1 *les polynômes suivant sont symétriques :*

1) $P(X) = \prod_{i=1}^{n} X_i$.

2) $P(X) = \sum_{i=1}^{n} X_i$.

3)$P(X) \ = \ XY + X + Y$.

Proposition 2.3.1 ***i)*** *Tout polynômes constant sont est un polynôme symétrique.*

ii) *Soit P, Q deux polynômes symétriques on a :*

1)$P - Q$ est un polynôme symétrique.

2) PQ est un polynôme symétrique .

3) Pour un polyôme symétrique $P \in A[X_1, X_2, ..., X_n]$, on a :

Si $\mathbf{MD}(P) = aX_1^{k_1}X_2^{k_2}...X_n^{k_n}$ *alors* $k_1 \geq k_2 \geq .... \geq k_n$.

Preuve. (ii,1)

Soient P et Q deux polynômes symétrique de $A[X_1, ..., X_n]$ et soit $\pi \in S_n$. Alors :

$$\begin{aligned}(P-Q)(X_{\pi(1)},X_{\pi(2)},.....,X_{\pi(n)}) &= P(X_{\pi(1)},X_{\pi(2)},.....,X_{\pi(n)})-Q(X_{\pi(1)},X_{\pi(2)},.....,X_{\pi(n)})\\ &= P(X_1,X_2,.....,X_n)-Q(X_1,X_2,.....,X_n)\\ &= (P-Q)(X_1,X_2,.....,X_n)\end{aligned}$$

Donc $P-Q$ est un polynôme symétrique.

(le même pour PQ) ■

2.3.1 Polynôme symétrique élémentaire

Définition 2.3.2 *Soient A un anneau, et $n \geq 0$. Pour tout entier k, le polynôme symétrique élémentaire de degré k de $A[X_1,...,X_n]$, que nous noterons σ_i , est défini par :*

$$\sigma_i = \sum_{H\subset\{1...n\},|H|=k} \prod_{i\in H} X_i.$$

$\sigma_1 = X_1 + ... + X_n$ *(n termes).*

$\sigma_2 = \sum_{1\leq i<j\leq n} X_iX_j$ *(C_n^2 termes).*

$\vdots$

$\sigma_k = \sum_{1\leq i_1<....<i_k\leq n} X_{i_1}...X_{i_k}$ *(C_n^k termes).*

$\vdots$

$\sigma_n = X_1...X_n.$

D'une façon générale, pour tout k $(l \leq k \leq n)$, on a :

$$\sum\nolimits_k = \sum\nolimits_{1\leq i_1<i_2<.....<i_k\leq n} X_{i_1}X_{i_2}X_{i_k}.$$

où $(i_1,i_2,....,i_k)$ décrit l'ensemble des C_n^k combinaisons de $\{1,2,...,n\}$ tel que :

$$1 \leq i_1 < i_2 < .... < i_k \leq n.$$

Lemme 2.3.1 *Soient $\sum_1,\sum_2,...,\sum_n$ les polynômes symétriques élémentaires en $X_1,...,X_n$: si pour tout $(I_1,I_2,...,I_n)$ dans $\mathbb{N}^n$, on pose $I=\sum_{1\leq i\leq n} I$, tel que $I \in A[X_1,...,X_n]$, on a :* $\mathbf{MD}(\sum_1^{I_1},\sum_2^{I_2},...,\sum_n^{I_n}) = X_1^I X^{I-I_1}...X_n^{I_n}$.

Définition 2.3.3 *Les hypothèses et les notations étant celles du lemme **(lemme 2.3.1)** l'entier $I_1+2I_2+....+nI_n$ est appelé le **poids** de $\sum_1^{I_1},\sum_2^{I_2},...,\sum_n^{I_n}$.*

*Pour tout polynôme $\phi(\sum_1,\sum_2,...,\sum_n)$, le **poids** de ϕ est le maximum des poids des monômes dont il est la somme.*

Théorème 2.3.1 *A étant un* ***domain intégre (D.l)****, si* $f \in A[X_1, X_2, ..., X_n]$ *est un polynôme symétrique de degré total d, alors l'unique polynôme* ϕ *tel que :*

$f(X_1, ..., X_n) = \phi(\sum_1, \sum_2, ..., \sum_n)$ *est de poids d.*

Proposition 2.3.2 *Soit* $\Bbbk = \mathbb{C}$ *un corps commutatif, Pour tout polynôme symétrique* $p \in \Bbbk[x_1, ..., x_n]$*, il existe un polynôme* $q \in \Bbbk[x_1, ..., x_n]$ *est unique tel que :* $\sigma_1, \sigma_2, ..., \sigma_n$ *étant les polynôme symétrique élémentaire de* $\Bbbk[x_1, ..., x_n]$*,*

$$p(x_1, ..., x_n) = q(\sigma_1, ..., \sigma_n).$$

2.3.2 Polynôme symétrique homogène

Degré de polynôme symétrique

Proposition 2.3.3 *Soient* $F \in A[X_1, ..., X_n]$ *un polynôme et* $P \in A[X_1, ..., X_n]$ *un monôme tel que :*

$$P = aX_1^{\alpha_1} X_2^{\alpha_2} ... X_n^{\alpha_n} \qquad (\alpha_i \in \mathbb{N})$$

$\deg P = \sum_{i=1}^{n} \alpha_i$.

le degré total de F *est le maximum des degré de ces monômes .*

Définition 2.3.4 *On dit que un polynôme est homogène si tous ces monômes ont même degré .*

Exemple 2.3.2

1) $F = X_1X_3 + X_2X_4 + X_5^2$.

le polynôme F *est un polynôme homogène de degré* 2.

2) $\sum_1^{I_1}, \sum_2^{I_2}, ..., \sum_n^{I_n}$*, considéré dans* $A[X_1, ..., X_n]$*, est un polynôme symétrique homogène de degré* $I_1 + 2I_2 + ... + nI_n$.

Remarque 2.3.1 ***1)*** *Les polynômes symétrique élémentaire sont* $\sigma_1, \sigma_2 ... \sigma_n$ *sont homogènes .*

2) *Le degré total de* σ_i *est égale l'indice i .*

D'autres polynômes symétriques homogènes vont intervenir dans la suite ce sont :

$$S_k = X_1^k + X_2^k + ... + X_n^k \quad = \sum_{i=1}^{n} X_i^k \qquad \text{pour tout } k \in \mathbb{N}.$$

Les sommes S_k sont appelées ***sommes de Newton****.*

Dans le cas $k = 0$.

$S_0 = X_1^0 + X_2^0 + ... + X_n^0 = n.$

quelle que soit $k \in \mathbb{N}$*, le degré total de* S_k *égal* k.

On les nomme ***polynômes symétriques simples .***

Proposition 2.3.4 *L'ensemble des polynômes symétriques de* $A[X_1, ..., X_n]$ *forme une sous-anneau de* $A[X_1, ..., X_n]$.

Soit P polynôme symétrique homogène de degré **d** *si :*

1) $\mathbf{d = 1}$ *; alors P est les formes linéaires.*

$$P = \sum_{i=1}^{n} a_i X_i = a_1 X_1 + a_2 X_2 + \cdots + a_n X_n.$$

2) $\mathbf{d = 2}$ *; alors P est les formes quadratiques .*

$$P = \sum_{1 \le i \le j \le n} a_{ij} X_i X_j = a_{11} X_1^2 + a_{12} X_1 X_2 + \cdots + a_{nn} X_n^2.$$

3) $\mathbf{d \geq 3}$ *alors P est le forme d'un espace vectoriel.*

2.3.3 Théorème fondamental

Théorème 2.3.2 *L'anneau A étant un* ***D.I****, pour tout polynôme symétrique* $f \in A[X_1, ..., X_n]$*, il existe un unique polynôme* Ψ *à n indéterminées sur A tel que :*

$$f(X_1, X_2, ..., X_n) = \Psi(\sum_{1}, \sum_{2}, ..., \sum_{n}).$$

où les $\sum_k$, $1 \le k \le n$, *sont les polynômes symétriques élémentaires des* Xi_i, $1 \le i \le n$.

Preuve. Soit f un polynôme symétrique dans $A[X_1, ..., X_n]$.

Existence du polynôme ϕ vérifiant **(Remarque 2.1.1).**

Si $f = 0$, il suffit de prendre $\phi = 0$: on suppose donc $f \neq 0$ et on raisonne par récurrence sur la hauteur du monôme directeur de f. Supposons :

$$\mathbf{MD}(f) = aX_1^{k_1}X_2^{k_2}.....X_n^{k_n}, \text{Où } a \in A^*.$$

Si pour tout i $(1 \leq i \leq n)$, on a $k_i = 0$, alors $\mathbf{MD}(f) = a$, donc $f = a$. Le théorème est vérifié en prenant $\phi = a$.

Si f est non constant, supposons le théorème vrai pour tout polynôme symétrique de $A[X_1, ..., X_n]$, dont le monôme directeur est moins haut que celui de f.

La relation **(Remarque 2.1.1)** implique :

$$\mathbf{MD}(f) = \mathbf{MD}(a \sum_1^{k_1-k_2} \sum_2^{k_2-k_3} .... \sum_n^{k_n}).$$

Considérons alors le polynôme $g(X_1, ..., X_n) = f(X_1, ..., X_n) - a \sum_1^{k_1-k_2} \sum_2^{k_2-k_3} .... \sum_n^{k_n}$.

On a $\mathbf{MD}(g) < \mathbf{MD}(f)$. Par suite, compte tenu de l'hypothèse de récurrence, il existe un unique polynôme Ψà n indéterminées sur A tel que :

$$g(X_1, ..., X_n) = \Psi(X_1, ..., X_n).$$

d'où, $f(X_1, ..., X_n) = \Psi(X_1, ..., X_n) + a \sum_1^{k_1-k_2} \sum_2^{k_2-k_3} .... \sum_n^{k_n}$.
En notant $\phi(\sum_1, \sum_2, ..., \sum_n)$ le second membre de l'égalité précédente, on a la relation **(Remarque 2.1.1)**.Unicité du polynôme ϕ vérifiant **(Remarque 2.1.1)**

Supposons que par une autre méthode, on ait trouvé un polynôme θ à n indéterminées sur A tel que :

$$f(X_1, ..., X_n) = \theta(X_1, ..., X_n).$$

Démontrons que $\theta = \phi$. Supposons $\theta \neq \phi$, alors :

$$\phi(\sum_1, \sum_2, ..., \sum_n) - \theta(\sum_1, \sum_2, ..., \sum_n) = \delta(\sum_1, \sum_2, ..., \sum_n).$$

où δ est un polynôme non nul dans $A[\sum_1, \sum_2, ..., \sum_n]$.

Cependant, en exprimant les $\sum_k$, $1 \leq k \leq n$, en fonction des X_i, $1 \leq i \leq n$, on obtient, compte tenu des relations **(Remarque 2.1.1)** ,

$$\delta(\sum_1, \sum_2, ..., \sum_n) = d(X_1, ..., X_n) = \ f(X_1, ..., X_n) - \ f(X_1, ..., X_n) = 0.$$

où d est donc le polynôme nul dans $A[X_1, ..., X_n]$.

Démontrons que δ est nécessairement le polynôme nul dans $A[\sum_1, \sum_2, ..., \sum_n]$.
En effet, $\delta \neq 0$ peut s'écrire comme une somme de monômes non nuls ordonnés suivant : l'ordre décroissant de leurs poids :

$$\delta = \sum_{1 \leq j \leq n} a_j \sum_1^{i_{j,1}} \sum_2^{i_{j,2}} ... \sum_n^{i_{j,n}}$$

les a_j, $1 \leq j \leq r$, étant non nuls dans A.

D'après le lemme **(2.3.2)**, dans le développement de δ en fonction des X_i, chaque monôme $a_j \sum_1^{i_{j,1}} \sum_2^{i_{j,2}} ... \sum_n^{i_{j,n}}$ donne, dans $d(X_1, ..., X_n)$, une composante homogène de degré égal à son poids : $i_{j,1} + 2i_{j,2} + ... + ni_{j,n}$ Par suite, $d = 0 \Rightarrow aj = 0$, $\forall j (1 \leq j \leq r) \Rightarrow \delta = 0$, donc $\theta = \phi$. ■

Proposition 2.3.5 *Le produit $(X - X_i)$ et relation entre coefficients et racines.*
Soit $n \geq 0$ $(n \in \mathbb{N})$. Dans l'anneau $\mathbb{Z}[X_1, ..., X_n]$ on a :

$$\prod_{1 \leq i \leq n} (X - X_i) = \sum_{0 \leq k \leq n} (-1)^k S_k X^{n-k}$$

Preuve. Montrons cette formule par réccurence sur n. Elle est vraie $n = 0, 1$

Supposons la vrai pour $n \geq 1$, notons S_k les polynômes symétriques élémentaires de $\mathbb{Z}[X_1, ..., X_n]$ et $T_k \in \mathbb{Z}[X_1, ..., X_{n+1}]$ on a :

$$\begin{aligned}\prod_{1\leq i\leq n+1}(X-X_i) &= (\prod_{1\leq i\leq n}(X-X_i))(X-X_{n+1})\\ &= (\sum_{0\leq k\leq n}(-1)^k S_k X^{n-k})(X-X_{n+1})\\ &= \sum_{0\leq k\leq n}(-1)^k S_k X^{n-k+1} - \sum_{0\leq k\leq n}(-1)^k S_k X^{n-k}X_{n+1}\\ &= X^{n+1} + \sum_{1\leq k\leq n}(-1)^k[S_k + S_{k-1}X_{n+1}]X^{n+1-k} + (-1)^{n+1}S_n X_{n+1}\end{aligned}$$

$S_n X_{n+1} = T_{n+1}$, pour $1 \leq k \leq n$ on voir, distinguant les parties à k éléments de $\{1, ..., n+1\}$ qui contiennent $n+1$ et celles qui ne le contiennent pas, que $T_k = S_k + S_{k-1}X_{n+1}$, C' est gagné. ■

Corollaire 2.3.1 *Soient $\Bbbk$ un corps, A un sous-anneau de $\Bbbk$, P dans $\Bbbk[X]$ unitaire, Ω un sur corps de $\Bbbk$ sur lequel P est scindé :*

$$P = \prod_{i=1}^{n}(X - x_i).$$

Alors, pour tout polynôme U de $A[X_1, ..., X_n]$ symétrique, on a :

$$U(x_1, ..., x_n) \in A.$$

2.3.4 Calcul des polynômes symétriques simples

Le principal problème qui se pose maintenant est de calculer les S_k au moyen des polynôme élémentaires σ_i.

Deux indéterminées

Dans le cas de deux indéterminées. On a :

$$\begin{aligned}S_1 &= \sigma_1 = x_1 + x_2\\ S_1 &= x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1x_2 = \sigma_1^2 - 2\sigma_2\end{aligned}$$

Pour l'entier $k \in \mathbb{N}$ $(k > 2)$, on considère le polynôme $p(y)$ tel que :

$$\begin{aligned} p(y) &= (y - x_1)(y - x_2) \\ &= y^2 - \sigma_1 y + \sigma_2 \end{aligned}$$

on a évidemment $p(x_1) = p(x_2) = 0$.

Pour tout entier $k > 2$, et pour tout $i \in \{1, 2\}$ on a :

$$x_i^{k-2} p(x_i) = x_i^k - \sigma_1 x_i^{k-1} + \sigma_2 x_i^{k-2} = 0.$$

et, en ajoutant membre à membre les deux égalités de ce type,

$$S_k = \sigma_1 S_{k-1} - \sigma_2 S_{k-2}. \tag{2.3.1}$$

On peut donc calculer S_3 :

$$S_3 = \sigma_1 S_2 - \sigma_2 S_1 = \sigma_1^3 - 3\sigma_1\sigma_2.$$

La formule de récurrence 2.3.1 permet le calcule successif de S_4, S_5, etc.

Trois indéterminées

Dans le cas de trois indéterminées. On a :

$$S_2 = x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_3x_1),$$

donc

$$S_2 = \sigma_1^2 - 2\sigma_2.$$

On trouve la même relation que dans le cas $n = 2$.

calculer S_k $(k > 2)$, on considère le polynôme $p(y)$ tel que :

$$\begin{aligned} p(y) &= (y - x_1)(y - x_2)(y - x_3) \\ &= y^3 - \sigma_1 y^2 + \sigma_2 y - \sigma_3 \end{aligned}$$

On a, pour tout $i \in \{1, 2, 3\}$, $p(x_i) = 0$. donc pour $k \geq 2$

$$x_i^{k-2} p(x_i) = x_i^{k+1} - \sigma_1 x_i^k + \sigma_2 x_i^{k-1} - \sigma_3 x_i^{k-2} = 0.$$

et, en ajoutant les trois relation de ce type,

$$S_{k+1} = \sigma_1 S_k - \sigma_2 S_{k-1} + \sigma_3 S_{k-2}. \tag{2.3.2}$$

On obtient ainsi, pour $k = 2$ (rappelons que $S_0 = 3$)

$$\begin{aligned} S_3 &= \sigma_1 S_2 - \sigma_2 S_1 + 3\sigma_3 \\ &= \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 \end{aligned}$$

La formule de récurrence 2.3.2 permet ensuite de calcules successivement S_4, S_5, etc. Par exemple,

$$\begin{aligned} S_4 &= \sigma_1 S_3 - \sigma_2 S_2 + \sigma_3 S_1 \\ &= \sigma_1^4 - 4\sigma_1^3\sigma_2 + 4\sigma_1\sigma_3 + 2\sigma_2^2 \end{aligned}$$

2.3.5 Calcul des polynômes symétriques doubles

Définition 2.3.5 *Soit $p \in K[x_1, x_2, ..., x_n]$ de polynôme symetrique double s'il existe deux entiers naturels h et k tels que :*

$$p = \sum x_1^h x_2^k.$$

Un tel polynôme est évidemment homogène.

Calculer p au moyen des polynômes symetriques élémentaire, et d'abord en fonction des S_k. Considérons :

$$\begin{aligned} S_h &= x_1^h + x_2^h + ... + x_n^h \\ S_k &= x_1^k + x_2^k + ... + x_n^k \end{aligned}$$

Multiplions membre à membre.

Dans le produit S_hS_k apparaissent des termes de deux type différents ;

1) Pour les termes du premier type x_1^{h+k}, leur somme est évidemment S_{h+k}.

2) Pour les termes du second type, il y a deux cas à considérer :

$$S_hS_k = \begin{cases} S_h^2 = S_{2h} + 2\sum x_1^h x_2^h & \text{si } h = k \\ S_{h+k} + \sum x_1^h x_2^k & \text{si } h \neq k \end{cases} \Longrightarrow \begin{cases} 2p = S_h^2 - S_{2h} & \text{du type } \mathrm{x_1^h x_2^h} \\ p = S_hS_k - S_{h+k} & \text{du type } \mathrm{x_1^h x_2^k} \end{cases}$$

Exemple 2.3.3 *Le polynôme $p \in K[x_1, x_2, ..., x_n]$ tel que :*

$$p = \sum x_1^3 x_2.$$

D'après le résultat précédent :

$$\begin{aligned} p &= S_3S_1 - S_4 \\ &= (\sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3)\sigma_1 - \sigma_1^4 + 4\sigma_1^2\sigma_2 - 4\sigma_3\sigma_1 - 2\sigma_2^2 + 4\sigma_4, \end{aligned}$$

donc

$$p = \sigma_1^2\sigma_2 - \sigma_1\sigma_3 - 2\sigma_2^2 + 4\sigma_4.$$

Chapitre 3

Quelques applications

Parmi les polynômes en plusieurs indéterminées sont remarquables ceux qui restent inchangés peu importe le réarrangement des indéterminées se produisent. Ainsi, toutes indéterminées apparaissent dans ces polynômes de façon symétrique. D'ou le nom des polynômes symétriques.

3.1 Discriminant d'un polynôme

Lemme 3.1.1 *Soit A un anneau commutatif. On rappelle que l'opérateur de dérivation $D : A[X] \to A[X]$ est l'application linéaire définie par $D(1) = 0$ et $D(X_n) = nX_{n-1}$, pour tout $n \geq 1$.*
Soient $P_1, ..., P_r \in A[X]$. On a $D(P_1 \cdots P_r) = \sum_{i=1}^{r} P_1 ... D(P_i) ... P_r$.

Théorème 3.1.1 ***(Discriminant du polynôme général de degré** n**)***
Soient $X_1, ..., X_n$ des indéterminées, et $\sigma_1, ..., \sigma_n$ les polynômes symétriques élémentaires en $X_1, ..., X_n$. Posons $a_i = (-1)^i \sigma_i$. Soient $T_1, ..., T_n$ d'autres indéterminées. Il existe un unique polynôme $\Delta_n \in \mathbb{Z}[X_1, ..., X_n]$ tel que :

$$\Delta_n(a_1, ..., a_n) = \prod_{1 \leq i < j \leq n} (X_j - X_i)^2$$

Ce polynôme Δ_n est appelé le discriminant du polynôme

$$P = X^n + a_1X^{n-1} + \cdots + a_n,$$

et est aussi noté discP. De plus, on a :

$$\prod_{i=1}^{n} P'(X_i) = (-1)^{\frac{n(n-1)}{2}}\Delta_n(a_1, ..., a_n) \tag{3.1.1}$$

Preuve. Posons $\Delta = \prod_{1\leq i<j\leq n} (X_j - X_i)^2$; c'est un élément de $\mathbb{Z}[X_1, ..., X_n]^{S_n}$. Donc, d'après le théorème fondamental des polynômes symétriques **2.3.3**, il existe un unique polynôme $\Delta_n^- \in \mathbb{Z}[T_1, ..., T_n]$, tel que :

$$\Delta_n(a_1, ..., a_n) = \Delta_n^-(a_1, ..., a_n) = \Delta$$

De plus, on a :

$$P = X^n + \sum_{i=1}^{n}(-1)^i\sigma_iX^{n-i} = \prod_{i=1}^{n}(X - X_i).$$

D'après le lemme précédent, on a : $P' = \sum_{i=1}^{n}\prod_{j\neq i}^{n}(X_i - X_j)$.

Alors, pour tout $i = 1, ..., n$, on a $P' = \prod_{j\neq i}^{n}(X_i - X_j)$. Par conséquent, l'on a :

$$\prod_{i=1}^{n} P'(X_i) = \prod_{j\neq i}^{n}(X_i - X_j) = (-1)^{\frac{n(n-1)}{2}}\Delta.$$

■

Corollaire 3.1.1 ***(Discriminant d'un polynôme*** $P \in k[X]$***)***

Soient k un corps et $P = X^n + \sum a_iX^{n-i}$ un polynôme unitaire de degré n à coefficients dans k. Soit L une extension de k dans laquelle P est scindé et soient $x_1, ..., x_n$ les racines

de P dans L. Alors :

$$\prod_{1\leq i<j\leq n}(X_j - X_i)^2 = \Delta_n(a_1, ..., a_n)$$

En particulier, P a une racine multiple ssi $\Delta_n(a_1, ..., a_n) = 0$.

Preuve. Soit $R = \mathbb{Z}[X_1, ..., X_n]$ un anneau et posons $V_n = \prod_{1\leq i<j\leq n}(X_j - X_i)^2$ et $A_i = (-1)^i\sigma_i$ pour $i = 1, ..., n$. D'après le théorème précédent, on a dans R l'égalité :

$$V_n^2 = \Delta_n(A_1, ..., A_n). \tag{3.1.2}$$

Soit φ l'unique morphisme d'anneaux de R dans L, défini par $\varphi(X_i) = x_i$. Pour $r = 1, ..., n$, on a :

$\varphi(A_r) = (-1)^r \sum_{i_1<...<i_r} \varphi(X_{i_1}...X_{i_r}) = (-1)^r\sigma_r(x_1, ..., x_n) = a_r$.

Par conséquent, appliquant φ à l'égalité 3.1.2, on obtient :

$$\prod_{1\leq i<j\leq n}(X_j - X_i)^2 = \Delta_n(a_1, ..., a_n)$$

La dernière assertion est alors claire. Le corollaire est démontré. ■

Proposition 3.1.1 ***(Discriminant d'un trinôme $X^n + pX + q$)***

Soient k un corps et p, $q \in k$. Le discriminant du trinôme $P = X^n + pX + q$, noté $discP$, égale :

$$(-1)^{\frac{n(n-1)}{2}}((1-n)^{n-1}p^n + n^n q^{n-1})$$

En particulier, pour

$$P = \begin{cases} X^2 + aX + b, & discP = a^2 - 4b; \\ X^3 + pX + q, & discP = -4p^3 - 27q^2. \end{cases}$$

Preuve. Soit L une extension de k dans laquelle P est scindé et soient $x_1, ..., x_n$ les racines de P dans L. D'après l'égalité 3.1.1 du théorème **3.1.1**, l'égalité à démontrer est équivalente à la suivante :

$$\prod_{i=1}^{n} P'(X_i) = (1-n)^{n-1}p^n + n^n q^{n-1}.$$

Or, $P'(X_i) = nX^{n-1} + p$. Supposons d'abord $q \neq 0$. Alors, pour $i = 1, ..., n$, l'on a $x_i \neq 0$ et

$$x_i^{n-1} = -p - \frac{q}{x_i}$$

On en déduit que $\prod_{i=1}^{n} P'(X_i)$ égale :

$$(1-n)^n p^n + \frac{(-n)^n q^n}{x_1 ... x_n} + \sum_{i=1}^{n-1} (1-n)^r p^r (-nq)^{n-r} \sigma_{n-r}(x_1^{-1}, ..., x_n^{-1}). \tag{3.1.3}$$

Or, $x_1 ... x_n = (-1)^n q$ et, d'autre part, on voit facilement que :
$\sigma_{n-r}(x_1^{-1}, ..., x_n^{-1}) = \frac{\sigma_r(x_1,...,x_n)}{x_1,...,x_n} = \begin{cases} 0 & \text{si } 1 \leq r \leq n-2; \\ \frac{-p}{q} & \text{si } r = n-1 \end{cases}$
Par conséquent, on déduit de 3.1.3 que $\prod_{i=1}^{n} P'(X_i)$ égale :

$$n^n q^{n-1} + (1-n)^{n-1} p^n (1 - n + n) = n^n q^{n-1} + (1-n)^{n-1} p^n.$$

Ceci prouve le résultat voulu, lorsque $q \neq 0$. Lorsque $q = 0$, l'argument est analogue : $x_n = 0$ est racine simple, $P_0(0) = p$, et pour les autres racines $x_1, ..., x_{n-1}$ l'on a $P_0(x_i) = (1-n)p$. On obtient ainsi que $\prod_{i=1}^{n} P'(X_i) = (1-n)^{n-1} p^n$ lorsque $q = 0$. Ceci démontre la proposition. En particulier, pour $n = 2$ ou 3, on obtient que le discriminant du trinôme $X^n + pX + q$ vaut $p^2 - 4q$, resp. $-4p^3 - 27q^2$. ■

Corollaire 3.1.2 *Soient $\Bbbk$ un corps, A un sous-anneau de $\Bbbk$, P dans $A[X]$ unitaire scindé sur $\Bbbk$. Alors :*

$$\Delta(P) \in A$$

Si P n'est pas scindé sur $\Bbbk$, on peut calculer $\Delta(P)$ en travaillant dans un sur corps Ω de $\Bbbk$ sur lequel P est scindé : l'existence de R ci-dessus montre que le résultat ne dépend pas de Ω.

Le discriminant généralise le $\ll b^2 - 4ac \gg$ de l'équation du second degré. La définition entraîne en effet le résultat suivant.

Lemme 3.1.2 *Soient $\mathbb{k}$ un corps, P dans $\mathbb{k}[X]$ unitaire. Alors P est séparable si et seulement si $\Delta(P) \neq 0$.*

Proposition 3.1.2

$$\Delta(P) = (-1)^{\frac{n(n-1)}{2}} \prod_{j=1}^{n} P'(x_j)$$

Exemple 3.1.1 ***1) Second degré.***

Si $P = aX^2 + bX + c$ *avec* $(a, b, c) \in \mathbb{k} * \times \mathbb{k} \times \mathbb{k}$,

$\Delta(P) = -(2ax_1 + b)(2ax_2 + b) = -4a^2x_1x_2 - 2ab(x_1 + x_2) - b^2 = b^2 - 4ac.$

2) Troisième degré.

Si $P = X^3 + pX + q$ *avec* $(p, q) \in \mathbb{k}^2$, *alors* $\Delta(P)$ *vaut*

$\prod_{i=1}^{3}(3x_i^2 + p) = 27(x_1x_2x_3)^2 + 9p(x_1^2x_2^2 + x_2^2x_3^2 + x_3^2x_1^2) + 3p^2(x_1^2 + x_2^2 + x_3^2) + p^3.$

On a :

$x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_3x_1) = -2p.$

En appliquant au polynôme symétrique $X_1^2X_2^2 + X_2^2X_3^2 + X_3^2X_1^2$, *on arrive à*

$$\Delta(P) = -4p^3 - 27q^2.$$

3)Binômes.

Soit a un élément du corps $\mathbb{k}$. Supposons que la caractéristique de $\mathbb{k}$ ne divise pas n, de sorte que $X^n - a$ est séparable. Soient α une racine de $X^n - a$. dans Ω. On a alors :

$$\Delta(X^n - a) = (-1)^{\frac{n(n-1)}{2}} \prod_{\omega \in U_n(\Omega)} (n\omega^{n-1}\alpha) = (-1)^{\frac{n(n-1)}{2}} n^n a.$$

Prenons $\mathbb{k} = \Omega = \mathbb{C}$, $n = p$ premier impair et $a = 1$. On déduit du calcul précédent que tout corps contenant U_p contient une racine carrée de

$$(-1)^{\frac{p(p-1)}{2}} p.$$

3.2 Applications aux équations algébriques

3.2.1 Équation du second degré

Soit $f \in \mathbb{C}[X_1, X_2]$ un polynôme symétrique à coefficients dans $\mathbb{C}$.

On consédère l'équation du second degrè suivant :

$$ax^2 + bx + c = 0 \quad (a, b, c \in \mathbb{C}; a \neq 0) \tag{3.2.1}$$

Si r_1 et r_2 sont les racines de 3.2.1,on a :

$$r_1 + r_2 = -\frac{b}{a},\ r_1 r_2 = \frac{c}{a}.$$

calculer le nombre complexe $f(r_1, r_2)$.

On sait (Proposition 2.3.3) qu'il existe un polynôme $g \in \mathbb{C}[X_1, X_2]$. unique, tel que :

$$f(r_1, r_2) = g(\sigma_1, \sigma_2).$$

par conséquent,

$$f(r_1, r_2) = g(\frac{-b}{a}, \frac{c}{a}).$$

ce qui résout le problème sans calcul effecif de r_1, r_2.

Exemple 3.2.1 ***1)*** *On consédre le polynôme symétrique* $f \in \mathbb{C}[x_1, x_2]$

$$f(x_1, x_2) = x_1^2 x_2 + x_2^2 x_1.$$

Calculer $f(r_1, r_2)$, telle que r_1, r_2 sont solutions de 3.2.1,

On a

$$\begin{aligned} f(x_1, x_2) &= x_1^2 x_2 + x_2^2 x_1 \\ &= x_1 x_2 (x_1 + x_2) \\ &= \sigma_2 \sigma_1 \end{aligned}$$

Donc

$$f(r_1, r_2) = \frac{-bc}{a^2}$$

2) On consédère l'équation

$$r^2 + \alpha r + 1 = 0 \qquad \alpha \in \mathbb{C} \tag{3.2.2}$$

t_1, t_2 sont des racines de 3.2.2 , tel que :

$$r_1 + r_2 = -\alpha,\ r_1 r_2 = 1$$

Déterminer une équation de degré 2 dont les racines sont cubes des racines de 3.2.2,

On calculer$s_1 = r_1^3 + r_2^3$ et $s_2 = r_1^3 r_2^3 = (r_1 r_2)^3 = 1$

L'équation demonde est $x^2 - s_1 x + s_2 = 0$

Ensuite, calcule le polynôme S_3 à deux indéterminée

$$S_3 = \sigma_1 - 3\sigma_1\sigma_3$$

Donc $s_1 = -\alpha + 3\alpha$.

Alors équation demandée est :

$$x^2 - (\alpha^3 - 3\alpha)x + 1 = 0$$

3.2.2 Équation de degré n

Soit $f \in \mathbb{C}[x_1, x_2, ..., x_n]$un polynôme symétrique ,considérons l'équation

$$\alpha_n t^n + \alpha_{n-1} t^{n-1} + ... + \alpha_0 = 0 \ \ (\alpha_i \in \mathbb{C} \quad \alpha_n \neq 0) \tag{3.2.3}$$

Si $r_1, ..., r_n$ sont des racines de 3.2.3, calculer le nombre complexe $f(r_1, ..., r_n)$.

Pour tout $k \in \mathbb{N}$, $k = 1...n$ on a :

$$\sum r_1...r_k = (-1)^k \frac{\alpha_k}{\alpha_n}.$$

D'aprés (Proposition 2.3.3), $g \in \mathbb{C}[x_1, x_2, .., x_n]$ tel que ;

$$f(x_1, x_2, .., x_n) = g(\sigma_1, \sigma_2, ..., \sigma_n)$$

Par conséquent :

$$f(r_1, r_2, .., r_n) = g(-\frac{\alpha_{n-1}}{\alpha_n}, \frac{\alpha_{n-2}}{\alpha_n}, ..., (-1)^n \frac{\alpha_0}{\alpha_n})$$

Exemple 3.2.2 *donne l'équation suivant :*

$$t^4 + t^2 + 1 = 0 \tag{3.2.4}$$

t_1, t_2, t_3, t_4 *sont des racines de 3.2.4,calculer le nombre* $f(r_1, r_2, r_3, r_4)$*, pour le polynôme symétrique*

$$f = \sum x_1^3 x_2$$

On a trouvé

$$f = \sigma_1^2\sigma_2 - \sigma_1\sigma_3 - 2\sigma_2^2 + 4\sigma_4$$

Pour les racines de 3.2.4, $(\sigma_1, \sigma_2, \sigma_3, \sigma_4) = (0, 1, 0, 1)$*, donc :*

$$f(r_1, r_2, r_3, r_4) = 2.$$

Conclusion

Dans ce travail, nous avons tenté de mener une étude sur anneau des polynômes à plusieurs indéterminées en expliquant les concepts de base nécessaires à cette étude.

Les polynômes à plusieurs indéterminées jouent un rôle important dans la détermination du discriminant des équations ou dans la recherche d'équations algébriques sans calculer leurs racines.

Bibliographie

[1] **A. Doneddu,** Polynômes et Algèbre linéaire, librairie Vuibert, Paris 1976.

[2] **A. Kurosh,** Higher Algebra, © English translation, Mir Publishers, 1980.

[3] **D. Guin**, Algèbre II " Anneaux, Modules et Algèbre multinéaire", EDP Sciences, 2013.

[4] **I. Assem et P.Leduc,** Cours d'algèbre " Group,anneau,modules et corps", presses internationales polytechnique, 2009.

[5] **J. Escofier,**Tout l'algèbre de la licence "cours et exercices corrigés", Dunod, Paris, 2011.

[6] **J. Calais**, Éléments de théorie des anneaux " Anneaux commutatifs, niveau $L3$ ", Ellipses édition Marketing S.A, 2006.

[7] **K. Djeghaba**, Mémoire pour l'oboration du diplome de magister "la cryptographie asymétrique sur l'anneau de polynômes à plusieurs variables, Université de m'sila, le 01/07/2019.

[8] **L. Ladjetat**,Cours Master1, Les anneaux, Université M.Boudiaf de Msila.
Année univ $2020 - 2021$.

[9] **L. Schwartz**, Algèbre 3^e année "Cours et exercices avec solutions", Dunod, Paris, 2003.

[10] **P.Tauvel,** Algèbre "cours", 2^e édition, Dunod, Paris, 2005.

[11] **P. Tauvel,** Cours D'algèbre, © Dunod, Paris, 1999.

الملخص:

في هذا العمل قمنا بإجراء دراسة على حلقة كثيرات الحدود في عدة متغيرات بمعاملات من حلقة تبديلية واحدية ثم قمنا بدراسة خاصة لكثيرات الحدود المتماثلة.

ينقسم هذ ا العمل الى ثلاثة فصول: نعطي أولا مفاهيم عامة عن الزمر، الحلقات، الحقول، كثيرات الحدود وحلقة كثيرات الحدود في عدة متغيرات. ثم نقوم بدراسة حلقة كثيرات الحدود في عدة متغيرات وحلقة كثيرات الحدود المتماثلة. أخيرا نذكر بعض التطبيقات لكثيرات الحدود المتماثلة.

الكلمات المفتاحية: الحلقة، الحقل، المثالي، حلقة كثيرات الحدود في عدة متغيرات، كثيرات الحدود المتماثلة.

Résumé :

Dans ce travail, on étudie l'anneau des polynômes en plusieurs indéterminées à coefficients dans un anneau commutatif unitaire. Ensuite, nous allons essayer de citer certaines de leurs applications. Ce travail est divisé en trois chapitres :

On donne tout d'abord des notions générales sur les groupes, les anneaux et les corps, les polynômes, l'anneau de polynômes.

Ensuite, on fait une étude sur l'anneau de polynômes à plusieurs variables et les polynômes symétriques.

Enfin, on donne quelques applications des polynômes symétriques.

Mots clés : Anneau, corps, idéal, l'anneau de polynômes à plusieurs variables, polynôme symétrique.

Abstract:

In this work, we give a study of the ring of polynomials in several indeterminate over a unitary commutative ring. This work is divided into three chapters:

First, we give general notions on groups, rings, fields, polynomials, ring of polynomials.

Next, we make a study on the ring of polynomials with several variables and the symmetric polynomial.

Finally, we are interested in some applications of symmetric polynomials.

Keywords: Ring, field, ideal, the ring of several polynomials, symmetric polynomials.