1 Fonctions polynômes

Définition 1.1

Soit $(A,+,\times)$ un anneau, et $n \in \mathbb{N}^*$. Soit $(a_i)_{i\in[\![0,n]\!]} \in A^{n+1}$. On appelle fonction polynôme l'application

$$\begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & \displaystyle\sum_{k=0}^{n} a_k x^k \end{array}$$

La fonction nulle est aussi appelée fonction polynôme.

Remarque 1 *La somme, le produit et la composée de deux fonction polynômes est une fonction polynôme.*

Définition 1.2

Soit f et g deux fontions polynômes sur A.
On dit que f et g sont (formellement) égales si $(a_i)_{i\in[\![0,n]\!]} = (b_j)_{j\in[\![0,m]\!]}$.
On dit que f et g sont numériquement égales si $\forall x \in A, f(x) = g(x)$.

Exemple Soit $f : \begin{array}{ccc} \mathbb{F}_2 & \longrightarrow & \mathbb{F}_2 \\ x & \longmapsto & 0 \end{array}$ et $g : \begin{array}{ccc} \mathbb{F}_2 & \longrightarrow & \mathbb{F}_2 \\ x & \longmapsto & x^2+x \end{array}$.
Ces deux fonctions sont numériquement égales, mais pas formellement égales.
Exemple Les polynômes d'endomorphismes ou de matrices sont des fonctions polynômes sur l'anneau des endomorphismes ou sur celui des matrices.

2 Polynômes à une indéterminée.

2.1 Définition

Définition 2.3

Soit $(A,+,\times)$ un anneau commutatif. On appelle polynôme à une indéterminée à éléments dans A toute suite presque nulle d'éléments de A.
On appelle polynôme nul la suite nulle d'éléments de A.

Notation On la note provisoirement $P = (a_i)$.

Définition 2.4

L'élément a_i est dit coefficient d'indice i du polynôme P. Le degré et la valuation sont respectivement le plus grand et le plus petit indice pour lequel le coefficient est non nul; ils existent lorsque P n'est pas le polynôme nul (celui dont tous les coefficients sont nuls).
On les note $deg(P)$ et $val(P)$.

Définition 2.5

Un polynôme dont tous les coefficients sont nuls, sauf l'un d'entre eux est appelé monôme.

Remarque 2 *Le degré d'un monôme est égal à sa valuation.*

On note temporairement $\mathcal{P}$ l'ensemble des polynômes.

2.2 L'anneau $(\mathcal{P}, +, \times)$

Théorème 2.1 (et Définition)

Soient P et Q deux polynômes de coefficients a_i et b_j. Alors les deux suites $(a_i + b_i)$ et $(\sum_{k=0}^{i} a_k b_{i-k})$ sont deux polynômes appelés respectivement somme et produit de P et Q; on les note $P + Q$ et $P.Q$.

Proposition 2.2

$(\mathcal{P}, +)$ est un sous-groupe du groupe additif $(A^{\mathbb{N}}, +)$.

Théorème 2.3

$(\mathcal{P}, +, \times)$ est un anneau commutatif.
L'élément neutre pour la multiplication est $(\delta_{0,1})$.

Remarque 3 *Attention, la multiplication des polynômes n'est pas induite par la multiplication dans $A^{\mathbb{N}}$. Il ne s'agit donc pas d'un sous-anneau.*

Proposition 2.4

Si A est un anneau intégre, $\mathcal{P}$ est aussi intègre.

2.3 La A-algèbre

Définition 2.6

Soient P un polynôme de coefficents a_i et b un élément de A.
Alors la suite (ba_i) est un polynôme, appelé produit de P par le scalaire b.
On le note $b.P$.

Théorème 2.5

$(\mathcal{P}, +, .)$ est un A-module. En particulier si A est un corps, il s'agit d'un A-espace vectoriel.
$(\mathcal{P}, +, \times, .)$ est une A-algèbre commutative.

Proposition 2.6

L'application $j : \begin{array}{ccc} A & \longrightarrow & \mathcal{P} \\ a & \longmapsto & a(\delta_{0,1}) \end{array}$ *est un morphisme injectif d'algèbre.*

2.4 Propriétés des degrés et valuations

Définition 2.7

Pour simplifier les formules qui suivent, on dit que le polynôme nul est de degré $-\infty$ et de valuation $+\infty$. Les règles de calcul dans $\overline{\mathbb{N}}$ s'appliquent.

Proposition 2.7

Soient P et Q deux polynômes, et b un scalaire non nul.

- $deg(P+Q) \leq max(deg(P); deg(Q))$;
- $val(P+Q) \geq max(val(P); val(Q))$;
- $deg(P \times Q) \leq deg(P) + deg(Q)$;
- $val(P \times Q) \geq val(P) + val(Q)$;
- $deg(bP) = deg(P)$;
- $val(bP) = val(P)$.

Si l'anneau est intègre, les lignes 3 et 4 sont des égalités.

Exercice : Dans quels cas a-t-on l'égalité pour les lignes 1 et 2 ?

Proposition 2.8

Si l'anneau est intègre, le groupe des inversibles de $\mathcal{P}$ est l'image par j de celui des inversibles de A. En particulier si A est un corps K, il s'agit de l'ensemble des monômes de degré 1.

2.5 Génération

Proposition 2.9

On note $e_i = (\delta_{ij})$. Cette famille est une partie basique du A-module.

On rappelle qu'une partie basique est une famille dont toute sous-famille est libre, et dont tout élément de $\mathcal{P}$ peut s'écrire comme une combinaison linéaire finie d'éléments de cette famille.

Remarque 4 $\forall (i,j) \in \mathbb{N}^2, e_{i+j} = e_i \times e_j$. *Donc* $\forall i \in \mathbb{N}^*, e_i = e_1^i$.
Par convention, on pose $e_0 = e_1^0$.

Définition 2.8

On appelle indéterminée le polynôme e_1, et on le note X.
L'ensemble des polynômes est alors appelé $A[X]$, et A est identifié à son image par j, ce qui implique que l'on notera a_0X^0 par a_0.

Remarquons que la notation $A[X]$ permet de savoir quel est l'indéterminée. Il ne s'agit en aucun d'une variable, et elle ne saurait prendre de valeurs.

Remarque 5 *On peut noter un polynôme de deux manières : soit selon les puissances croissantes, soit selon les puissances décroissantes.*

Définition 2.9

Le coefficient ayant pour indice le degré d'un polynôme non nul est appelé le coefficient dominant.
Un polynôme de coefficient dominant égal à 1 est appelé polynôme unitaire ou normalisé.

Théorème 2.10

Soit $\varphi : A \longrightarrow B$ un morphisme non nul d'anneaux commutatifs.
Il existe un et un seul morphisme d'anneaux $A[X]$ dans $B[Y]$ qui prolonge φ et transforme l'indéterminée X de $A[X]$ et l'indéterminée Y en $A[Y]$

2.6 Composition de polynômes

Définition 2.10

Soient P et Q deux polynômes. On appelle polynôme composé des deux polynômes P et Q, noté $P \circ Q$ le polynôme défini par :

$$P \circ Q = \sum_{n \in \mathbb{N}} a_n Q^n$$

Proposition 2.11

La composition de deux polynômes est associative, distributive à droite par rapport à l'addition, et on a $P \circ X = P$, et $X \circ P = P$, pour tout polynôme P de $A[X]$.

Remarque 6 *$P \circ X = P$ justifie la notation $P(X)$, et permet de savoir quelle est l'indéterminée.*
La composition de deux polynômes n'est pas commutative; elle n'est pas non plus distributive à gauche pour l'addition.

2.7 Fonction polynôme

Définition 2.11

Soit A un anneau commutatif, $P = \sum_{k=0}^{n} a_k X^k$ un polynôme de $A[X]$. On appelle $\tilde{P} : \begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & \sum_{k=0}^{n} a_k x^k \end{array}$.
Cette fonction est appelée fonction polynôme associée à P.

On note A^A l'algèbre des applications de A dans lui-même.

Théorème 2.12

L'application qui à un polynôme associe sa fonction polynôme est un morphisme de A-algèbre de $A[X]$ dans A^A. L'image de $A[X]$ par ce morphisme est la sous-algèbre des fonctions polynômes.

Remarque 7 *: A priori ce morphisme n'est ni injectif, ni surjectif.*

Remarque 8 *Soient B un anneau, et A un sous-anneau de B. A tout polynôme P de $A[X]$, on peut, en considérant P comme un polynôme de $B[X]$, lui associer la fonction polynôme $\tilde{P} : B \longrightarrow B$.*
En particulier, si $B = A[X]$, on trouve $\tilde{P}(Q) = P \circ Q$, ce qui justifie la notation $P(Q)$ adoptée pour $P \circ Q$.

3 Anneau euclidien

3.1 Division euclidienne de deux polynômes

Théorème 3.13 (et Définition)

Soient A un anneau commutatif, F et G deux polynômes de $A[X]$ tels que G soit non nul, et de coefficient dominant inversible dans A.
Alors il existe un unique couple Q, R de polynômes de $A[X]$ tels que

$$F = GQ + R \text{ et } deg(R) < deg(G)$$

On dit que Q et R sont respectivement le quotient et le reste dans la division euclidienne du dividende F par le diviseur G.

Remarque 9 *Il faut lire l'inéquation des degrés dans $\mathbb{N} \cup \{-\infty\}$, ou la lire dans $\mathbb{N}$, et rajouter la condition $R = 0$.*

Preuve du Théorème 3.13:
A faire !

■

Proposition 3.14

1. *Soient A un anneau commutatif, et F et G deux polynômes tels que l'on puisse effectuer la division euclidienne de F par G.*
   Soit B un sur-anneau de A, alors le quotient et le reste de la division euclidienne de F par G dans B existent et sont ceux de la division euclidienne de F par G dans A.

2. *Soit $(F_i)_{i\in[\![1,n]\!]}$ une famille de polynômes de $A[X]$, et $(\alpha_i)_{i\in[\![1,n]\!]}$ une famille d'éléments de A.*
   Soit G un polynôme non nul de coefficient inversible dans A. On note (Q_i) et (R_i) les quotients et reste des divisions euclidiennes de F_i par G. Alors

   - *le quotient et le reste de la division euclidienne de $\sum_{i=1}^{n} \alpha_i F_i$ par B sont $\sum_{i=1}^{n} \alpha_i Q_i$ et $\sum_{i=1}^{n} \alpha_i R_i$.*
   - *le reste de la division euclidienne de $\prod_{i=1}^{n} F_i$ par B est celui de la division euclidienne de $\prod_{i=1}^{n} R_i$ par B.*

3. *Si dans une division euclidienne, on multiplie (resp on divise dans la mesure du possible) le dividende et le diviseur par une même polynôme P, alors le quotient ne change pas et le reste est multiplié (resp divisé) par P.*

Définition 3.12

On dit que G <u>divise</u> F si le reste de la division euclidienne de F par G est nul.

En fait, on peut considérer $\mathcal{I}$ l'idéal engendré par G. Alors le reste de la division euclidienne de F par G est défini par les conditions $F \equiv R \mod(\mathcal{I})$ et $deg(R) < deg(G)$. Cela nous permet de travailler dans $A[X]/\mathcal{I}$.

Proposition 3.15

Soit $a \in A$. Le reste de la division euclidienne de F par $(X - a)$ est l'élément $\tilde{A}(a)$ de A.

3.2 Etude des idéaux de $K[X]$

On se place désormais dans un corps commutatif K.

Corollaire 3.16

$K[X]$ est un anneau euclidien.

Théorème 3.17

$K[X]$ est un anneau principal.
Soit I un idéal de $K[X]$, il existe un polynôme P de $K[X]$, unique au produit près par un élément de K^*, tel que I soit l'idéal engendré par P.
Si de plus I n'est pas l'idéal nul, il existe un unique polynôme unitaire P tel que $I =< P >$.

Rappel : la somme de deux idéaux est un idéal, et l'intersection de deux idéaux est encore un idéal.

Théorème 3.18 (et Définition)

Soient P et Q deux polynômes de $K[X]$. On suppose que l'un des deux est non nul.
Alors il existe un unique polynôme unitaire qui engendre $(P) + (Q)$. On le note $P \wedge Q$, et on l'appelle le PGCD de P et de Q.
Soit C un diviseur de P et de Q, alors C divise $P \wedge Q$.
De plus, si D polynôme est tel que, pour tout C diviseur commun à P et Q, C divise D, alors D est associé à $P \wedge Q$.

Définition 3.13

On définit de même le PGCD d'une famille de polynôme.

Proposition 3.19

Soit $(P_i)_{i\in I}$ une famille de polynômes.

- *Soit σ une permutation de I,*
$$\wedge_{i\in I} P_{\sigma(i)} = \wedge_{i\in I} P_i.$$
- *Si $(I_j)_{j\in J}$ est une partition de I,*
$$\wedge_{j\in J}(\wedge_{i\in I_j} P_i) = \wedge_{i\in I} P_i.$$
- *Pour tout polynôme P de $K[X]$, $(\wedge_{i\in I} P_i)P = \wedge_{i\in I} PP_i$.*
- *Soit P un polynôme divisant tous les P_i,*
$$\frac{\wedge_{i\in I} P_i}{P} = \wedge_{i\in I} \frac{P_i}{P}$$

Le calcul effectif se fait par l'algorithme d'Euclide. On rappelle le lemme essentiel

Lemme 3.20

Soient F et G deux polynômes non nuls tels que $deg(G) \leq deg(F)$. Alors si on appelle R le reste de la division euclidienne de F par G,
$$F \wedge G = G \wedge R.$$

Exercice Enoncer, et montrer l'algorithme d'Euclide.

3.3 Polynômes premiers entre eux

Définition 3.14

On dira d'une famille de polynômes que ces polynômes sont premiers entre eux si leur PGCD est 1.
On remarquera alors que l'idéal qu'ils engendrent est $K[X]$.

Théorème 3.21 (Saint Bezout)

Pour que $(P_i)_{i\in I}$ soit une famille de polynômes premiers entre eux, il faut et il suffit qu'il existe une famille presque nulle $(A_i)_{i\in I}$ telle que

$$1 = \sum_{i\in I} A_i P_i.$$

Théorème 3.22

Soit $(P_i)_{i\in I}$ une famille de polynômes non tous nuls. Pour que D soit PGCD de cette famille, il faut et il suffit que D divise chacun des P_i, et que la famille $(\frac{P_i}{D})_{i\in I}$ soit une famille de polynômes premiers entre eux, et qu'il soit unitaire.

Théorème 3.23 (Saint Gauss)

Si $A|BC$ et $A \wedge B$ alors $A|C$.

Corollaire 3.24

Soient P et $(P_i)_{i\in[\![1,n]\!]}$ des polynômes de $K[X]$.

- *Si $\forall i \in [\![1,n]\!], P \wedge P_i = 1$, alors $P \wedge \prod_{i=1}^{n} P_i = 1$;*
- *Si $P|\prod_{i=1}^{n} P_i$ et si $\forall i \in [\![1,n-1]\!], P \wedge P_i = 1$, alors $P|P_n$;*
- *Si les P_i sont premiers entre eux deux à deux, et si chaque P_i divise P, alors $\prod_{i=1}^{n} P_i|P$.*

Théorème 3.25 (Bachet-Bezout)

Soient P et Q deux polynômes de $K[X]$, non tous deux constants, et premiers entre eux. Alors il existe un couple unique (U_0, V_0) de polynômes de $K[X]$ vérifiant les conditions

$$PU_0 + QV_0 = 1, \text{ et } deg(U_0) < deg(Q), \text{ et } deg(V_0) < deg(P).$$

De plus l'ensemble des couples (U, V) vérifiant $PU + QV = 1$ est donné par :

$$U = U_0 + CQ \text{ et } V = V_0 + CP, \text{ avec } C \in K[X].$$

On retrouve le même théorème dans $\mathbb{Z}$.

3.4 Plus Petit Commun Multiple

Théorème 3.26 (et Définition)

Soit $(P_i)_{i\in I}$ une famille de polynômes de $K[X]$. Il existe un unique polynôme unitaire qui engendre l'idéal $\underset{i\in I}{\cap}(P_i)$.
Ce polynôme est appelé PPCM de la famille, et noté $\vee_{i\in I} P_i$.
Soit Q un multiple commun à tous les P_i, alors $\vee_{i\in I} P_i | Q$.
Soit M un polynôme tel que $\forall Q \in K[X]$ tel que $\forall i \in I, P_i | Q$ implique que $M|Q$, alors M est associé à $\vee_{i\in I} P_i$.

On retrouve les résultats de $\mathbb{Z}$:
Si la famille contient un polynôme nul, le PPCM est 0,
Si la famille est finie et ne contient aucun polynôme nul, le PPCM est non nul,
Il y a commutatitivité et associativité de la loi interne PPCM,
Le produit par un polynôme est distributif par rapport à la loi PPCM.

Théorème 3.27

Soient A et B deux polynômes non nuls de $K[X]$, M et D leur PPCM et leur PGCD.
Alors $\exists! k \in K$ tel que

$$AB = kMD$$

Preuve du Théorème 3.27:
Il suffit de l'écrire. ■

3.5 Polynômes irréductibles

Définition 3.15

Un polynôme est irréductible sur $K[X]$ s'il est non inversible, et si ses seuls diviseurs dans $K[X]$ sont les inversibles de $K[X]$ et ses associés.

Proposition 3.28

Les trois assertions suivantes sont équivalentes

i P *est irréductible*

ii (P) *est premier*

iii (P) *est maximal*

Preuve de la Proposition 3.28:
A vous

■

Proposition 3.29

Soit P un polynôme irréductible, et A un polynôme.
$A \wedge P = 1 \Longleftrightarrow P \not| A$.

Exercice Montrer que si P et Q sont irréductibles, non associés, $P^k \wedge Q^k = 1$, quel que soit $k \in \mathbb{N}$.

Corollaire 3.30

Soit P un polynôme irréductible dans $K[X]$. Pour que P divise un produit de polynômes, il faut et il suffit qu'il divise un des termes du produit.

3.6 Anneau factoriel

Théorème 3.31

$K[X]$ est un anneau factoriel. Tout polynôme A, non nul, de $K[X]$ se décompose de manière unique à l'ordre près en un produit d'un élément de K^* par des puissances de polynômes irréductibles.

$$A = u \prod_{i=1}^{m} P_i^{\alpha_i}, \quad \alpha_i \in \mathbb{N}^*, \ \ u \in K^* \text{ et } P_i \text{ irréductible.}$$

Preuve du Théorème 3.31:
Il n'y a pas besoin d'utiliser "principal $\Longrightarrow$ factoriel". On a juste besoin d'utiliser le lemme suivant :

Lemme 3.32

Tout polynôme non constant admet un diviseur irréductible.

Preuve du Lemme 3.32:
C'est la même preuve que dans $\mathbb{Z}$.
On considère l'ensemble des diviseurs non constants de P: il est non vide. En considérant le stasthme, on regarde l'ensemble des degrés des diviseurs non constant de P : c'est un ensemble non vide, minoré par 1, il admet donc un plus petit élément.

■

4 Lien avec l'Analyse

4.1 Division selon les puissances croissantes

On se place à nouveau dans un anneau A.

Théorème 4.33 (et Définition)

Soient p un entier naturel, A un anneau commutatif, F et G deux polynômes de $A[X]$ tels que $\tilde{B}(0) = b_0$ soit un élément inversible de A.
Alors il existe un unique couple Q, R de polynômes de $A[X]$ tels que

$$A = BQ + X^{p+1}R \quad \text{et } deg(Q) \leq p.$$

4.2 Dérivation

Définition 4.16

Soit A un anneau commutatif, et $P = \sum_{k=0}^{n} a_k X^k$ un polynôme de $A[X]$.
On appelle polynôme dérivé le polynôme $P' \in A[X]$ défini par:

$$P' = \sum_{k=0}^{n-1} a_{k+1}(k+1)X^k.$$

Proposition 4.34

Si A est intègre et de caractéristique nulle, alors

$$deg(P') = deg(P) - 1.$$

Définition 4.17

On appelle primitive de P tout polynôme dont P est le polynôme dérivé.

Remarque 10 *Si A est intègre et de caractéristique nulle, les primitives du polynôme nul sont les constantes.*

Théorème 4.35

L'application D qui à tout polynôme associe son polynôme dérivé est un endomorphisme du A-module $A[X]$.

Théorème 4.36

Soient P et Q deux polynômes de $A[X]$,

$$\begin{aligned} (P.Q)' &= P'Q + Q'P \\ (P \circ Q)' &= (P' \circ Q).Q' \end{aligned}$$

Définition 4.18

Pour tout polynôme P de $A[X]$, $D^k(P)$, que l'on note aussi $P^{(k)}$, est appelé polynôme dérivé k-ième du polynôme P.
Par convention, $D^0(P) = P^{(0)} = P$.

Exercice : Retrouver la formule de Leibnitz.

Théorème 4.37

Soient P un polynôme de $K[X]$, et a un élément de K. On a alors l'égalité des polynômes, dite Formule de Taylor :

$$P = \sum_{k=0}^{n} \frac{\tilde{P}^{(k)}(a)}{k!}(X-a)^k$$

Preuve du Théorème 4.37:
Dans la cas $a = 0$, il s'agit de la formule de Taylor-Mac-Laurin. Le calcul monter que $\tilde{P}^{(k)}(0) = k!a_k$.
Dans le cas $a \neq 0$, on s'y ramène en introduisant le polynôme $Q = P \circ (X + a)$. ■

4.3 Racines

Théorème 4.38 (et Définition)

Soient A un anneau commutatif, P un polynôme de $A[X]$, a un élément de A. Les assertions suivantes sont équivalentes :

1. $\tilde{P}(a) = 0$
2. *Le polynôme $X - a$ divise P.*

Dans le cas où ces assertions sont vraies, on dit que a est racine (ou zéro) de P.

Remarque 11

1. *Le polynôme nul admet tous les éléments de A pour racine.*
2. *Un polynôme constant non nul n'admet aucune racine.*
3. *Soit A un anneau et B un sur-anneau. Soit P un polynôme de $A[X]$, et donc de $B[X]$. Toute racine de P dans A l'est dans B, mais la réciproque est fausse.*
4. *Si A est un corps commutatif, et donc $A[X]$ un anneau factoriel, ces deux assertions sont encore équivalentes à $(X - a)$ figure dans la décomposition de P.*
5. *Tout polynôme de degré supérieur ou égal à 2 qui admet une racine n'est pas irréductible; la réciproque est fausse.*

Théorème 4.39 (et Définition)

Soient K un corps commutatif, P un polynôme de $K[X]$, a un élément de K et k un entier tel que $k \geq 1$.
Les assertions suivantes sont équivalentes :

1. *Il existe Q tel que $P = (X-a)^k Q$, et $\tilde{Q}(a) \neq 0$.*
2. *$(X-a)^k$ divise P mais pas $(X-a)^{k+1}$.*

Dans le cas où ces assertions sont vraies, on dit que k est l'ordre de multiplicité de la racine a de P.

On dit encore que a est racine d'ordre k de P.

Théorème 4.40

Soient K un corps commutatif de caractéristique nulle, P un polynôme de $K[X]$, a un élément de K, k un entier tel que $k \geq 1$.
Pour que a soit racine d'ordre k de P, il faut et il suffit que a soit racine de P et de ses $k-1$ premières dérivées, mais pas de $P^{(k)}$.

Corollaire 4.41

a est racine d'ordre k de P si et seulement si (a est racine de P et a est racine d'ordre $k-1$ de P').

4.4 Isomorphisme entre polynôme et fonctions polynômes

Théorème 4.42

Soient K un corps commutatif et P un polynôme de $K[X]$.
Etant donnés les éléments deux à deux distincts $a_1, ..., a_r$ de K et les entiers naturels $k_1, ..., k_r$ non nuls, P admet chacun des a_i comme racine d'ordre k_i si et seulement si P est divisible par $\prod_{i \in [\![1,r]\!]} (X-a_i)^{k_i}$.

Corollaire 4.43

Soit P un polynôme non nul de $K[X]$ admettant, dans K r racines deux à deux distinctes $a_1, ..., a_r$ d'ordre au moins égaux à $k_1, \ldots, k_r$, alors

$$k_1 + \ldots + k_r \leq deg(P).$$

Corollaire 4.44

Un polynôme de K de degré p admet au plus p racines deux à deux distinctes.

Corollaire 4.45

Soit $P \in K[X]$, tel que $deg(P) \leq n$ admettant r racines distinctes à des ordres au moins égaux à $k_1, \ldots, k_r$, avec $k_1 + \ldots k_r > n$. Alors P est le polynôme nul.

Corollaire 4.46

Soient P et Q deux polynômes de $K[X]$ de degré au plus n tels que leurs fonctions polynômes prennent les même valeurs en $n+1$ points deux à deux distincts de K. Alors $P = Q$.

Définition 4.19

On appelle polynôme scindé sur K tout polynôme dont la somme des ordres de multiplicité des racines est égale au degré de P.

Alors P est associé à $\prod_{i \in [\![1,r]\!]} (X - a_i)^{k_i}$. Si A est un corps infini, le morphisme qui à un polynôme associe sa fonction est donc injectif. Donc

Théorème 4.47

Si K est un corps commutatif infini, alors la K-algèbre des fonctions polynômes sur K est isomorphe à la K-algèbre $K[X]$.

Exercice : polynôme d'interpolation de Lagrange.

5 $\mathbb{C}[X], \mathbb{R}[X]$

5.1 $\mathbb{C}$ algèbriquement clos

Définition 5.20

On appelle corps algèbriquement clos tout corps commutatif tel que tout polynôme non constant admmette au moins une racine dans K.

Théorème 5.48

Soit K un corps. K est algèbriquement clos si et seulement si les seuls polynômes irréductibles sont de degré 1.

Proposition 5.49

Si K est algèbriquement clos, tout polynôme est scindé.

Corollaire 5.50

Soient P et Q deux polynômes non constants sur un corps algèbriquement clos. Q divise P si et seulement si toute racine de Q d'ordre k est racine de P d'ordre au moins k.

Corollaire 5.51

Pour que deux polynômes non constants soient associés, il faut et il suffit qu'ils aient les mêmes racines avec les mêmes ordres de multiplicité.

Théorème 5.52 (de D'Alembert)

$\mathbb{C}$ est algèbriquement clos.

Théorème 5.53

A tout polynôme non nul P de $\mathbb{C}[X]$, on peut associer un et un seul couple constitué d'un complexe $a \in \mathbb{C}$, et d'une application presque nulle $\nu : \mathbb{C} \longrightarrow \mathbb{N}$, tels que

$$P = a \prod_{x \in \mathbb{C}} (X - x)^{\nu(x)}.$$

On dit que cette décomposition est la décomposition de D'Alembert de P.

Proposition 5.54

On définit un automorphisme involutif φ de l'anneau $\mathbb{C}[X]$ en posant

$$\varphi(\sum_{n \in \mathbb{N}} a_n X^n) := \sum_{n \in \mathbb{N}} \overline{a_n} X^n.$$

Les deux polynômes P et $\varphi(P)$ sont dits conjugués : on note $\varphi(P) := \overline{P}$.

Remarque : a est racine d'ordre de k de P si et seulement si $\overline{a}$ est d'ordre k de $\overline{P}$.

5.2 $\mathbb{R}[X]$

Lemme 5.55

Tout polynôme de degré impair de $\mathbb{R}[X]$ admet au moins une racine.

On peut retrouver ce lemme avec

Lemme 5.56

Si $P \in \mathbb{R}[X]$ admet sur $\mathbb{C}$ un racine $x \in \mathbb{C}\backslash\mathbb{R}$, à l'ordre $\nu(x)$, alors P admet aussi la racine $\overline{x}$ à l'ordre $\nu(\overline{x}) = \nu(x)$.

Exercice 1 Chercher les polynômes irréductibles de degré 2. On appellera $\mathcal{P}_2$ leur ensemble.

Proposition 5.57

A tout polynôme non nul P de $\mathbb{R}[X]$, on peut associer un et un seul triplet constitué d'un élément non nul a d e $\mathbb{R}$, et de deux applications presque-nulles $\nu : \mathbb{R} \longrightarrow \mathbb{N}$, et $\mu : \mathcal{P}_2 \longrightarrow \mathbb{N}$ telles que

$$P = a \prod_{x \in \mathbb{R}} (X - x)^{\nu(x)} \prod_{P \in \mathcal{P}_2} P^{\mu(P)}.$$

Théorème 5.58

Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1, et les polynômes de degré 2 sans racine réelle.

Exercice 2 : $X^4 + X^2 + 1, X^4 + pX^2 + q$.

6 Algèbre des polynômes à plusieurs indéterminées

6.1 Polynôme à plusieurs indéterminées

On munit le semi-groupe $(\mathbb{N}^n, +)$ d'une longueur : $|(i_1, \ldots, i_n)| = i_1 + \ldots + i_n$.

Définition 6.21

Soient A un anneau commutatif et n un entier naturel non nul. On appelle polynôme à n indéterminées sur A toute famille presque nulle d'éléments de A indexées par $\mathbb{N}^n$.

Autrement dit, c'est $(a_{i=(i_1,\ldots,i_n)})_{i \in \mathbb{N}^n}$, pour lequel à partir d'un entier n_0, $\forall i \in \mathbb{N}^n, |i| \geq n_0$, $i = (0, \ldots, 0)$.
On note l'ensemble des polynômes à n indéterminées : $A[X_1, \ldots, X_n]$.

Théorème 6.59 (et Définition)

Soient $P = (a_i)_{i \in \mathbb{N}^n}$ et $Q = (b_i)_{i \in \mathbb{N}^n}$ deux polynômes de $A[X_1, \ldots, X_n]$. Alors les deux familles $(c_i)_{i \in \mathbb{N}^n}$ et $(d_i)_{i \in \mathbb{N}^n}$ d'éléments de A définies par, $\forall i \in \mathbb{N}^n$:

$$\begin{aligned} c_i &= a_i + b_i \\ d_i &= \sum_{j+k=i} a_j b_k \end{aligned}$$

sont des polynômes de $A[X_1, \ldots, X_n]$ respectivement appelés somme et produit de P et Q; on les note $P + Q$ et PQ.

Théorème 6.60

$(A[X_1, \dots X_n], +, .)$ est un anneau commutatif non nul.

Définition 6.22

Soit $P = (a_i)_{i \in \mathbb{N}^n}$ un polynôme et b un élément de A. Alors $(ba_i)_{i \in \mathbb{N}^n}$ est un polynôme appelé produit du polynôme P par le scalaire b; on le note bP.

Théorème 6.61

$(A[X_1, \dots X_n], +, .)$ est un A-module, et en particulier, c'est un espace vectoriel si A est un corps.
$(A[X_1, \dots X_n], +, ., .)$ est une A-algèbre commutative.

Proposition 6.62

L'application $j : A \longrightarrow A[X_1, \dots, X_n]$, qui à $a \in A$ fait correspondre le polynôme

$$(a_i)_{i \in \mathbb{N}^n} \text{ tel que } a_{0,\dots,0} = a \text{ et } a_i = 0 \text{ si } |i| \geq 1$$

est un morphisme injectif d'algèbre.

Définition 6.23

Dans l'algèbre $A[X_1, \dots, X_n]$, on appelle indéterminées les polynômes $X_q = (b_{q,j})_{j \in \mathbb{N}^n}, q \in [\![1, n]\!]$, définis par :

$$\begin{cases} b_{q,j} = 1 \text{ si } j = (j_1, \dots, j_n) \text{ vérifie } j_q = 1 \text{ et } j_k = 0 \text{ si } k \neq q; \\ b_{q,j} = 0 \text{ dans les autres cas.} \end{cases}$$

Théorème 6.63

Dans le $A[X_1, \dots, X_n]$ tout polynôme peut s'exprimer de manière unique comme combinaison linéaire de la famille des $X_1^{i_1} \dots X_n^{i_n}$. Les coefficients de la combinaison linéaire sont ceux du polynôme.

On peut ordonner P selon les puissances croissantes de X_n :

$$P = \sum_{k\in\mathbb{N}} \left(\sum_{(i_1,\ldots,i_{n-1},k)\in\mathbb{N}^n} a_{(i_1,\ldots,i_{n-1},k)} X_1^{i_1} \ldots X_{n-1}^{i_{n-1}} X_n^k \right)$$

Théorème 6.64

L'ordination selon les puissances croissantes de X_n est un isomorphisme d'algèbre de $A[X_1,\ldots,X_n]$ dans $A[X_1,\ldots,X_{n-1}][X_n]$.

Corollaire 6.65

Si A est un anneau intègre, $A[X_1,\ldots,X_n]$ est un anneau intègre et son groupe des unités est celui de A.

Définition 6.24

On appelle degré partiel de P relativement à X_q le degré du polynôme P considéré comme polynôme à une seule indéterminée :X_q : on le note $deg_{X_q}(P)$.
On appelle degré total de P la longueur du plus grand multiindice pour lequel a_i n'est pas nul : on le note $deg(P)$.
Si p est nul, on convient que tous ses degrés partiels et total sont $-\infty$

Proposition 6.66

$$\begin{aligned} deg(P+Q) &\leq max(deg(P), deg(Q)) \\ deg(PQ) &\leq deg(P) + deg(Q). \end{aligned}$$

6.2 Polynômes homogènes

Définition 6.25

Soit p un entier naturel. Un polynôme P est p-homogène si $|i| \neq p$ implique $a_i = 0$.

Proposition 6.67

Si P est p-homogène et Q est q-homogène, leur produit est $(p+q)$-homogène.

Théorème 6.68

$A[X_1, \ldots, X_n]$ est somme directe des sous-modules constituées des polynômes p-homogènes.

6.3 Fonction polynôme de n variables.

Définition 6.26

Soit A un anneau commutatif et P un polynôme de $A[X_1, \ldots, X_n]$. L'application $\tilde{P} : A^n \longrightarrow A$, définie par

$$(x_1, \ldots, x_n) \longmapsto \sum_{i \in \mathbb{N}^n} a_i x_1^{i_1} \ldots x_n^{i_n}$$

est appelée fonction polynôme de n variables associée au polynôme P.

Théorème 6.69

C'est un morphisme de A-algèbre. Si A est un anneau intègre infini, c'est un isomorphisme.

6.4 Substitution

C'est l'opération habituelle qui consiste à substituer n polynômes à p indeterminées $Y_1, \ldots, Y_p$ à chaque indéterminée X_i.

7 Dérivation partielle des polynômes

7.1 Polynôme dérivé partiel

Définition 7.27

Soient A un anneau commutatif, et P un polynôme de $A[X_1, \ldots, X_n]$. On appelle polynôme dérivé partiel de P par rapport à l'indéterminée X_q, noté $\frac{\partial P}{\partial X_q}$ le polynôme dérivé de P considéré comme élément de $A[X_1, \ldots, X_{q-1}, X_{q+1}, \ldots, X_n][X_q]$.

Théorème 7.70

L'application D_q qui à tout polynôme associe son polynôme dérivé partiel par rapport à l'indéterminée X_q est un endomorphisme de A-module.

Corollaire 7.71

$D_p \circ D_q = D_q \circ D_p$.

Proposition 7.72

Soit $D_1^{i_1} \circ \ldots \circ D_n^{i_n}$ une dérivation partielle d'ordre $k = |i|$ du polynôme P.

1. *Si $deg(P) < k, D_1^{i_1} \circ \ldots \circ D_n^{i_n}(P) = 0$.*
2. *Si $deg(P) \geq k, deg(D_1^{i_1} \circ \ldots \circ D_n^{i_n}(P)) \leq deg(P) - k$.*

7.2 Formule de Taylor

On se place dans un corps K de caractéristique nulle.

Définition 7.28

Soient k un entier naturel, et P un polynôme de $K[X_1, \ldots, X_n]$. On appelle puissance symbolique d'ordre k de P, on note

$$[Y_1 D_1(P) + \ldots + Y_n D_n(P)]^{[k]}$$

le polynôme

$$\sum_{|i|=k} \frac{k!}{i_1! \ldots i_n!} Y_1^{i_1} \ldots Y_n^{i_n} \frac{\partial^k}{\partial X_1^{i_1} \ldots \partial X_n^{i_n}}(P)$$

de l'anneau $K[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$.

Théorème 7.73

Soit P un polynôme de $K[X_1, \ldots, X_n]$. On a l'égalité entre les polynômes de $K[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$:

$$P(X_1 + Y_1, \ldots, X_n + Y_n) = \sum_{k \in \mathbb{N}} \frac{1}{k!} [Y_1 P'_{X_1} + \ldots + Y_n P'_{X_n}]^{[k]}$$

7.3 Dérivation des polynômes homogènes. Théorème d'Euler

Proposition 7.74

Soit P un polynôme p-homogène de $A[X_1, \ldots, X_n]$. Alors $\forall q \in [\![0, n]\!]$,

1. *Si $p = 0$, $\frac{\partial}{\partial X_q}(P) = 0$,*
2. *Si $p \geq 1$, $\frac{\partial}{\partial X_q}(P)$ est $(p-1)$-homogène (éventuellement nul)*

Théorème 7.75 (d'Euler)

Soient K un corps commutatif de caractéristique nulle, et P un polynôme de $K[X_1, \ldots, X_n]$. Les deux asssertions suivantes sont équivalentes :

1. *P est p-homogène,*
2. $\sum_{q=1}^{n} X_q P'_{X_q} = pP.$

8 Propriétés arithmétiques de $K[X_1, \ldots, X_n]$

8.1 Divisibilité dans $K[X_1, \ldots, x_n]$

Attention, pas de division euclidienne globale. Par contre, on garde une division euclidienne par rapport à la variable X_n, dès que le coefficient dominant en X_n est inversible !

Proposition 8.76

Dans $K[X_1, \ldots, X_n]$, pour que le polynôme A soit divisible par le polynôme $X_n - B$, où B est un polynôme de $K[X_1, \ldots, X_{n-1}]$, il et il suffit que le polynôme obtenu en substituant, dans A, le polynôme B à l'indéterminée X_n soit le polynôme nul.

Corollaire 8.77

Pour que le polynôme A soit divisible par la produit $\prod_{1 \leq i < j \leq n} (X_j - X_i)$, il faut et il suffit que A soit divisible par chacun des $(X_j - X_i)$.

Remarque 12 *Pour $n \geq 2$, $K[X_1, \ldots, X_n]$ n'est pas un anneau principal.*
Si A est un anneau factoriel, $A[X_1, \ldots, X_n]$ l'est aussi. Donc $K[X_1, \ldots, X_n]$ est un anneau factoriel.

9 Polynômes symétriques

9.1 Polynômes invariants par un sous-groupe G de $\mathcal{S}_n$

Proposition 9.78

Etant donné un élément σ du groupe symétrique de degré n $\mathcal{S}_n$, l'application de $A[X_1, \ldots, X_n]$ qui à tout polynôme P fait correspondre le polynôme $\sigma(P)$ défini par $\sigma(P)(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma[n)})$ est un automorphisme d'algèbre.
L'application qui à tout couple (σ, P) fait correspondre le polynôme $\sigma(P)$ est une opération du groupe $\mathcal{S}_n$ sur $A[X_1, \ldots, X_n]$. Enfin, si P est p-homogène, $\sigma(P)$ l'est aussi.

Définition 9.29

Etant donné un sous-groupe G de $\mathcal{S}_n$, un polynôme P de $A[X_1, \ldots, X_n]$ est dit invariant par G si $\forall \sigma \in G$, $\sigma(P) = P$.

C'est donc un point fixe (orbite réduite à un point). L'ensemble des polynômes invariants par G est noté $\mathcal{P}_G$: c'est une sous-algèbre de $A[X_1, \ldots, X_n]$. Nous avons en particulier deux sous-algèbres importantes : celle des polynômes alternés (invariants par le groupe alterné $\mathcal{A}_n$), et celle des polynômes symétriques.

9.2 Polynômes symétriques élémentaires

Théorème 9.79 (et Définition)

Dans $A[X_1, \ldots, X_n]$, les n polynômes Σ_p, définis par

$$\Sigma_p = \sum_{1 \leq i_1 < \ldots < i_p \leq n} X_{i_1} \ldots X_{i_p}$$

sont symétriques et portent le nom de polynômes symétriques élémentaires.

Preuve du Théorème 9.79:
Il suffit d'introduire $P = \prod_{i=1}^{n} (Y - X_i)$, et de développer avec Newton.

■

Théorème 9.80 (de Newton)

Soient $k \in \mathbb{N}$, *et* $S_k = \sum_{i=0}^{n} X_i^k$.

Alors :

1. $S_0 = n$ *et* $S_1 = \Sigma_1$,
2. *pour* $k \in [\![1, n]\!]$,

$$S_k - \Sigma_1 S_{k-1} + S_2 \Sigma_{k-2} + \ldots + (-1)^k S_k \Sigma_{n-k} + \ldots + (-1)^{k-1} S_{k-1} \Sigma_1 + (-1)^k k \Sigma_k = 0$$

3. *pour* $k \geq n$,

$$\sum_{i=0}^{n} (-1)^i S_{k-i} \Sigma_i = 0.$$

Ces relations portent le nom de relation de Newton.