Polynomes sur un corps

"Trois anneaux pour les rois Elfes sous le ciel,

$\mathrm{B}_{\mathrm{crys}}$, B_{st}, B_{dR},

Sept pour les Seigneurs Nains dans leurs demeures de pierre,

$E_{\mathbb{Q}_p}$, $A_{\mathbb{Q}_p}$, $B_{\mathbb{Q}_p}$, E, A, B, $\tilde{A}$

Neuf pour les Hommes Mortels destinés au trépas,

$\mathbb{Q}_p$, $\mathbb{Z}_p$, $\mathbb{F}_p$, $\overline{\mathbb{Q}_p}$, $\overline{\mathbb{F}_p}$, $\mathbb{C}_p$, $\mathcal{O}_{\mathbb{C}_p}$, $\mathbb{Q}_p^{nr}$, B_{HT}

Un pour le Seigneur Ténébreux sur son sombre trône

$\mathrm{A}_{\mathrm{inf}}$"

Fonctions Polynomiales

$K = \mathbb{R}$ $\quad P(X) = a_0 + a_1 X + \dots + a_d X^d$ $\quad a_i \in \mathbb{R}$

est défini comme la fct $P : \mathbb{R} \longrightarrow \mathbb{R}$

$$P : x \in \mathbb{R} \longrightarrow a_0 + a_1 x + a_2 x^2 + \dots + a_d x^d \in \mathbb{R}$$

$a_d \neq 0$ $\qquad \deg P = d.$

$\mathbb{R}[X]$ comme l'ensemble des fcts polynomiales

$\mathbb{R}[X]$ est un anneau (et une $\mathbb{R}$-algèbre)

$\lambda \in \mathbb{R}$ $\quad P, Q \in \mathbb{R}[X]$

$\lambda P + Q \in \mathbb{R}[X]$

$P.Q : x \longrightarrow P(x).Q(x) \quad \in \mathbb{R}[X]$

$P(X) = a_0 + a_1 X + \dots + a_d X^d$

$Q(X) = a'_0 + a'_1 X + \dots + a'_d X^d$

$$(\lambda P + Q)(X) = (\lambda a_0 + a'_0) + (\lambda a_1 + a'_1)X + \dots + (\lambda a_d + a'_d)X^d$$

$$P.Q(X) = \sum_{k=0}^{2d} c_k X^k$$

$$c_k = \sum_{i=0}^{k} a_i a'_{k-i} .$$

A anneau commutatif

$A[X]$ "=" l'ensemble de fct polynomiales de A vers A

$$= \left\{ P : x \in A \longrightarrow a_0 + a_1 x + a_2 x^2 + \dots + a_d x^d \;\; a_0, a_1, \dots, a_d \in A \right\}$$

$x^d = \underbrace{x \cdot x \cdot x \dots x}_{d \text{ fois}}$ multiplication ds A

$A[X]$ forme un anneau commutatif

⚠ les coefficient de fct polynomiale ne sont pas uniquement definis en general.

$A = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ p premier

$\forall x \in \mathbb{F}_p$ on a $x^p = x$

la fct $x \in \mathbb{F}_p \longrightarrow x^p - x = 0_{\mathbb{F}_p}$

est nulle : $X^p - X = 0$.

$\mathbb{F}_p$ est fini. si on remplace $\mathbb{F}_p$ par $\mathbb{F}_{p^2} \supset \mathbb{F}_p$

le polynome $x \longrightarrow x^p - x$ n'est pas identiquement 0

par contre le polynome

$$X^{p^2} - X \text{ est identiquement nul sur } \mathbb{F}_{p^2}$$

- $\mathbb{F}_{p^2}^\times = \mathbb{F}_{p^2} - \{0\}$ est un gpe pour la multiplication d'ordre p^2-1 et par Lagrange

$$\forall x \in \mathbb{F}_{p^2}^\times \quad x^{p^2-1} = 1_{\mathbb{F}_{p^2}}$$

et $\quad x^{p^2} = x \Longrightarrow \forall x \in \mathbb{F}_{p^2} \; X^{p^2} - X = 0_{\mathbb{F}_{p^2}}$

Polynomes comme suites

A : Anneau commutatif

$A^{\mathbb{N}}$ = l'ensemble des suites à valeurs ds A

$$= \{ a = (a_n)_{n \geq 0} \quad a_n \in A \}$$

$$= \left\{ a : \begin{array}{l} \mathbb{N} \longrightarrow A \\ n \longrightarrow a_n \end{array} \right\}$$

$A^{\mathbb{N}}$ a une structure de A-module

- $a+b : n \longrightarrow (a+b)_n = a_n + b_n$

$\lambda \in A$ $\lambda a : n \longrightarrow \lambda . a_n$

$$A_f^{\mathbb{N}} = \left\{ a = (a_n)_{n \geq 0} \text{ tq } a_n = 0_A \text{ des } n \text{ et assez grand} \right\}$$

: a est tq $\exists\, n_0(a)$ tq si $n \geq n_0$ $a_n = 0_A$

$a \in A^{\mathbb{N}}$ $\quad \mathrm{supp}(a) = \{ n \in \mathbb{N} \text{ tq } a_n \neq 0_A \} \subset \mathbb{N}$

$a \in A_f^{\mathbb{N}}$ ssi $\mathrm{supp}(a) \subset \mathbb{N}$ est fini

$A_f^{\mathbb{N}}$ est un ssmodule de $A^{\mathbb{N}}$

si (a_n) et (b_n) s'annulent pour n assez grand $(a_n + b_n)$ s'annule pour n assez grand. ainsi que $(\lambda a_n)_{n \geq 0}$

$A^{\mathbb{N}}_{f}$ = Suites de support fini

$=: A[X] :=$ les polynomes a coefs dans A

soit $P = (a_n)_{n\geq 0} \in A[X]$ on definit

$\deg P = \sup\{ n \geq 0 \text{ tq } a_n \neq 0 \} < \infty$

si $P \neq \underline{0}$ et $P = \underline{0}$ $\deg P = -\infty$

$$\begin{aligned} \deg : A[x] &\longrightarrow \mathbb{N} \cup \{-\infty\} \\ P &\longrightarrow \deg P. \end{aligned}$$

si $P = (a_n)_{n \geq 0}$ les a_i s'appellent les coefficients de P (a_i = ième coefficient)

On pose pour $m \geq 0$

$$X^m = \left(\delta_{n=m}\right)_{n \geq 0}$$

$$\delta_{n=m} = \begin{cases} 1 & \text{si } n = m \\ 0 & \text{sinon} \end{cases}$$

$$X^0 = (1, 0, 0, \ldots 0, \ldots) \qquad X^1 = (0, 1, 0, \ldots, 0, \ldots)$$

$$X^2 = (0, 0, 1, 0, \ldots 0) \qquad X^m = (0, 0, \underset{\substack{\uparrow \\ m}}{1}, 0, \ldots, 0)$$

$P = (a_n)_{n \geq 0}$ $\deg P = d$ $(a_n = 0 \text{ si } n > d)$

$P = a_0 X^0 + a_1 X^1 + \dots + a_d X^d + 0 X^{d+1} + 0 X^{d+2} + \dots$

$= (a_0, a_1, a_2, \dots \quad a_d, 0, 0, 0, \dots)$

la famille des polynômes $\{X^n \quad n \geq 0\}$ s'appelle la famille de monomes unitaires

$\{X^m \quad m \geq 0\}$ forme une base du A-module $A[X]$

$\forall P \in A[X]$ il existe $d \geq 0$ et $a_0, \ldots, a_d \in A$

tq $P = a_0 . X^0 + a_1 . X^1 + \ldots + a_d X^d$

et c'etta ecriture est unique aux zeros pres $\left(0 X^{d+1} = \underline{0} \right)$

- $A[X]_{\leq d} = \{ P \in A[X] \ \deg P \leq d \}$

$= \{ (a_n)_{n \geq 0} \text{ tq } a_n = 0 \text{ si } n \geq d+1 \}$

$= \{ P = a_0 X^0 + a_1 X^1 + \dots + a_d X^d \ \ a_0, a_1, \dots, a_d \in A \}$

$\simeq \{ (a_0, a_1, \dots, a_d) \in A^{d+1} \} \simeq A^{d+1}$

$A[X]_{\leq d}$ est un sous-A module $A[X]$.

$A[X]$ comme anneau :

si $P \in A[X]$ $\quad P = a_0 X^0 + a_1 X^1 + \dots + a_d X^d$

on lui associe une fct polynomiale

$$P : x \longrightarrow \underset{\substack{\parallel \\ 1_A}}{a_0 x^0} + a_1 x + \dots + a_d \cdot x^d$$

$$a_0 + a_1 x + \dots + a_d x^d = P(x)$$

On a un morphisme de A-modules

$$f_{Pol} : A[X] \longrightarrow Pol(A,A) \subset \mathcal{F}(A,A)$$
$$P \longrightarrow P : x \longrightarrow P(x)$$

⚠ n'est pas injectif en general : $A = \mathbb{F}_p$

$X^p - X$ est ds le noyau.

Si P et Q sont 2 fct polynomiale

$$P : x \longrightarrow a_0 + a_1 x + \dots + a_d x^d$$

$$Q : x \longrightarrow a'_0 + a'_1 x + \dots + a'_d x^d$$

alors $P.Q : x \longrightarrow (a_0 + a_1 x + \dots + a_d x^d) \times (a'_0 + a'_1 x + \dots + a'_d x^d)$

$$= a_0 a'_0 + (a_0 a'_1 + a'_0 a_1) x + \dots + c_{2d} x^{2d}$$

avec pour $k \leq 2d$

$$c_k = a_0 a'_k + a_1 a'_{k-1} + \dots + a_k a'_0$$

$$= \sum_{i=0}^{k} a_i a'_{k-i}$$

P.Q et une fct polynomiale associée au polynome

$$c_0 X^0 + c_1 X^1 + \dots + c_{2d} X^{2d}$$

$$c_k = a_0 a'_k + a_1 a'_{k-1} + \dots + a_k a'_0$$

$$= \sum_{i=0}^{k} a_i a'_{k-i}$$

On defini sur $A[X]$ un produit

en posant pour $P = (a_n)_{n \geq 0}$ $Q = (a'_n)_{n \geq 0}$

$$P.Q = (c_n)_{n \geq 0} \in A[X].$$

$$c_n = a_0 a'_n + \dots + a'_0 a_n = \sum_{i=0}^{n} a_i a'_{n-i}$$

Rmq : si $n > \deg P + \deg Q$ $c_n = 0$.

Théorème 5.2. *La loi de multiplication interne* $\bullet.\bullet$ *sur* $A[X]$ *est associative, commutative et distributive par rapport a l'addition et fait de* $(A[X], +, .)$ *un anneau commutatif dont l'element unite est le monome unitaire de degre* 0,

$$X^0 = (1_A, 0, \cdots).$$

Par ailleurs $A[X]$ *muni de la multiplication externe* $(a, P) \mapsto a.P$ *fait de* $A[X]$ *une* A*-algebre.*

Preuve: Verifier.

PROPOSITION 5.6. *Soit $\mathcal{F}(A;A)$ l'espace des fonctions de A a valeurs dans A: L'application "fonction polynomiale"*

$$P \in A[X] \mapsto P(\bullet) \in \mathcal{F}(A;A)$$

qui a un polynome associe sa fonction polynomiale est un morphisme d'anneaux.

En particulier si $P = a_0X^0$ est un polynome de degree 0 ou $-\infty <$ la fonction correspondante est la fonction constante egale a $a_0 \in A$

$$a_0X^0(\bullet) = \underline{a_0} : x \mapsto a_0.$$

⚠ $P \to P(\bullet)$ n'est pas injective en general

<u>Notations</u> :

$$\begin{aligned} A &\hookrightarrow A[X] \\ a &\mapsto (a, 0, 0, \dots) = aX^0 \end{aligned}$$

est injective et on identifie A au sous anneau $A.X^0$ et du coup on écrira simplement "a" à la place de $a.X^0$

- on écrira X pour X^1.

$$X = X^1 = (0, 1, 0, \dots)$$

Propriete du deg: $\deg P = \deg (a_n)_{n\geq 0} = \sup\{n, a_n \neq 0\}$

P et Q deux polynomes

$\deg(P+Q) \leq \max(\deg P, \deg Q)$

$\deg(P.Q) \leq \deg P + \deg Q$

"=" il faut que A soit integre.

Rmq: reste valable si P ou $Q = \underline{0}$ $\deg 0 = -\infty$

$\deg(P.Q) \leq \deg P + \deg Q$ avec "=" ssi A est intègre.

$P.Q = (c_n)_{n \geq 0}$ $\quad c_n = \sum_{i=0}^{n} a_i a'_{n-i}$

$c_n = 0$ si $n > \deg P + \deg Q$

$c_{\deg P + \deg Q} = a_{\deg P} \cdot a'_{\deg Q}$ $\quad a_{\deg P} \neq 0_A$, $a'_{\deg Q} \neq 0_A$

si A est intègre alors

$$a_{\deg P} \cdot a'_{\deg Q} \neq 0_A \Rightarrow \deg P.Q = \deg P + \deg Q$$

- si A n'est pas intègre il existe $a, a' \neq 0$ tq

$a.a' = 0_A$ et on prend

$P = aX^{\deg P} + a_{d-1}X^{d-1} + \dots\dots$

$Q = a'X^{\deg Q} + a'_{d'-1}X^{d'-1} + \dots\dots$

$P.Q = a.a'X^{d+d'} + \dots\dots$

Derivation

$A \subset \mathbb{R}$ $\quad P$ une fct polynomiale sur $\mathbb{R}$

$$P(X) = a_0 + a_1 X + \dots + a_d X^d$$

$$P'(x) = \lim_{h \to 0} \frac{P(x+h) - P(x)}{h}$$

$$= a_1 + 2a_2 x + \dots + (d-1) a_{d-1} x^{d-2} + d a_d x^{d-1}$$

Définition 5.6. *Soit*

$$P(X) = a_d.X^d + \cdots + a_1.X + a_0 \in A[X]$$

un polynome a coefficient dans un anneau commutatif A; son polynome derive est le polynome

$$P'(X) = a_d.(d-1).X^{d-1} + \cdots + a_k.k.X^{k-1} + \cdots + a_1 \in A[X].$$

Ici on a note

$$a_2.2 = a_2.2_A = a_2 + a_2 \ (2 \text{ fois}), \ \ a_d.d = a_d.d_A = a_d + \cdots + a_d \ (d \text{ fois})$$

ou

$$d_A = 1_A + \cdots + 1_A \ (d \text{ fois})$$

est l'image de d par le morphisme canonique de $\mathbb{Z}$ vers A.

THÉORÈME 5.3. *La derivation*

$$\bullet' : P \in A[X] \mapsto P' \in A[X]$$

– *est lineaire:*

$$\forall a \in A,\ \ P, Q \in A[X],\ \ (a.P + Q)' = a.P' + Q'$$

et son noyau contient les polynomes constants.

– *verifie la regle de Leibnitz:*

$$\forall P, Q \in A[X],\ \ (P.Q)' = P'.Q + P.Q'.$$

⚠ degré: $(X^d)' = d_A . X^{d-1}$

il se peut que $d_A = 0_A$ (si $d \in \ker \mathrm{Car}_A$)

par exemple si $A = \mathbb{F}_p$ $(X^p)' = pX^{p-1} = 0$

Fonction polynomiale associée dans une A-algèbre

$\mathcal{A}$ une A-algebre $(A = K \; \mathcal{A} = M_d(K))$

$$P(X) = a_0 X^0 + a_1 X + \dots\dots + a_d X^d$$

$$M \in \mathcal{A} \quad P(M) = a_0 1_{\mathcal{A}} + a_1 M + a_2 M^2 + \dots\dots + a_d M^d$$

$$P(\cdot) : \begin{array}{ccc} \mathcal{A} & \longrightarrow & \mathcal{A} \\ M & \longrightarrow & P(M) \end{array}$$

On a les propriétés suivantes

$$(P+Q)(M) = P(M) + Q(M)$$
$$(P.Q)(M) = P(M).Q(M)$$

- $P \in A[X] \longrightarrow P(\bullet) \in \mathcal{F}(\mathcal{A}, \mathcal{A})$

est un morphisme de A-algèbre

$M \in \mathcal{A}$.

$$ev_M : P \in A[X] \longrightarrow P(M) \in \mathcal{A}$$

ev_M est un morphisme d'anneau et de $\mathcal{A}$ algèbres.

Rmq : $A[X]$ est commutative mais $\mathcal{A}$ n'est pas beaucoup d'être commutative.

Integralité

PROPOSITION 5.7. *L'anneau $A[X]$ est integre ssi A est integre et on a alors pour tout $P, Q \in A[X]$,*

$$\deg(P.Q) = \deg P + \deg Q.$$

Preuve: $P = a_d X^d + \text{Pol de } d^\circ \leq d-1 \quad a_d \neq 0$

$Q = a'_{d'} X^{d'} + \text{Pol de } d^\circ \leq d'-1 \quad a'_{d'} \neq 0$

$$PQ = a_d a'_{d'} X^{d+d'} + \text{Pol de } d^\circ \leq d+d'-1$$

si A est integre $a_d . a'_{d'} \neq 0 \quad \deg PQ = d+d' = \deg P + \deg Q$

Anneau des Polynômes sur un corps

$A = K$ = Corps.

Divisibilité : $P \mid Q$ si $Q = PS$ $S \in K[X]$

$\forall P$ $\underline{1} \mid P$ et $P \mid \underline{0}$

THÉORÈME 5.4. *Soit $Q \in K[X] - \{0\}$ un polynome non-nul. Pour tout $P \in K[X]$ il existe des polynomes $S, R \in K[X]$ uniques verifiant*

$$\deg R < \deg Q \text{ et tels que } P = Q.S + R.$$

DÉFINITION 5.7. *Les polynomes R et S sont appeles respectivement "reste" et "quotient" de la division euclidienne de P par Q.*

De plus $R = 0$ si et seulement si $Q|P$.

Preuve : $q = \deg Q$ $\quad Q = b_q X^q + \dots + b_1 X + b_0 \quad b_q \neq 0$

$P = a_d X^d + \dots + a_1 X + a_0 \quad a_d \neq 0$

- Si $d < q$ on prend $S = 0$ $R = P$ on a fini

$P = 0 . Q + P$

On fait une recurrence sur $d^\circ P = d$

$$P_1 := P - \frac{a_d}{b_q} Q . X^{d-q}$$

$$P_1 = a_d X^d + \text{Pol } d^\circ \leq d-1 - \frac{a_d}{b_q} b_q X^q X^{d-q} + \text{Pol } d^\circ \leq d-1$$

$$= a_d X^d - \frac{a_d}{b_q} b_q X^d + \text{Pol } d^\circ \leq d-1$$

$$= \text{Pol } d^\circ \leq d-1$$

Il existe R_1, S_1 tq

$$P_1 = Q \cdot S_1 + R_1 \quad d^\circ R_1 < q$$

$$P = Q S_1 + R_1 + \frac{a_d}{b_q} Q X^{d-q}$$

$$P = \underbrace{Q\left(S_1 + \frac{a_d}{b_q} X^{d-q}\right)}_{S} + \underbrace{R_1}_{R}$$

Unicite

$$P = QS + R = QS' + R'$$

$$d^\circ R, d^\circ R' < \deg Q$$

$$Q(S-S') = R'-R$$

$$q + \deg(S-S') \qquad d^\circ \leq \max(\deg R', \deg R) < q$$

il faut que $\deg(S-S') = -\infty$. $S = S'$

$\square$

<u>Application aux racines</u>

Définition 5.8. *Soit*

$$P(X) = a_d.X^d + a_{d-1}.X^{d-1} + \cdots + a_1.X + a_0$$

un polynome a coefficient dans K. L'ensemble des racines de P dans K, $\mathrm{Rac}_P(K)$ est l'ensemble des solution dans K de l'equation $P(z) = 0$:

$$\mathrm{Rac}_P(K) = \{z \in K,\ P(z) = 0_K\}.$$

Proposition 5.9. *Soit K un corps et P un polynome et $z \in K$, les deux enonces suivants sont equivalents:*

(1) *$P(z) = 0$ (ie. z est une racine de P).*
(2) *Le polynome $X - z$ divise $P(X)$.*

<u>Preuve</u> : Si $P \neq 0$ $\deg P \geqslant 1$

$P = (X-z)S + R$ avec $\deg R < \deg X-z = 1$

R est constant : ou bien $R = 0$ ou bien $R = a \in K^\times$

$$P(x) = (x-z)S(x) + a$$

$$P(z) = 0 = (z-z)S(z) + a$$
$$= 0 + a$$

$$a = 0 \quad R = 0$$

$$P(x) = (x-z)S(x)$$

$$x - z \mid P.$$

$\square$

Théorème 5.6. *Soit $P \in K[X]$ un polynome non nul alors P est divisible par le produit*

$$\prod_{z \in \mathrm{Rac}_P(K)} (X - z).$$

En particulier

$$|\mathrm{Rac}_P(K)| = \deg \prod_{z \in \mathrm{Rac}_P(K)} (X - z) \leqslant \deg P.$$

Preuve : par recurrence sur $\deg P$.

si $\deg P = 0$ on a fini

- cas $\deg P \geq 1$. Soit $z \in \mathrm{Rac}_P(K)$ (sinon on a fini) par la proposition precedente

$$P(X) = (X - z) S(X)$$

si z' est une autre racine de P $(z' \neq z)$

$$P(z') = (z' - z) S(z') \qquad z' - z \neq 0$$

$$S(z') = 0 \qquad z' \in Rac_S(K)$$

$$Rac_P(K) = \{z\} \cup Rac_S(K)$$

par recurrence ($\deg S = \deg P - 1$)

S est divisible par $\displaystyle\prod_{\substack{z' \in Rac_P(K) \\ z' \neq z}} (X - z')$

$$S(X) = \prod_{\substack{z' \in Rac_P(K) \\ z' \neq z}} (X - z') \cdot S'(X)$$

$$P(X) = (X - z) \prod_{\substack{z' \in Rac_P(K) \\ z' \neq z}} (X - z') \, S'(X)$$

$$\deg P = \deg S' + \sum_{z \in Rac_P(K)} \deg(X-z)$$

$$= \deg S' + |Rac_P(K)|$$

$$|Rac_P(K)| \leq \deg P.$$

pas vrai si on l'applique à la fct polynomiale $P \in K[X]$ dans une K-algèbre générale.

Corollaire 5.2. *Soit K un corps et $|K|$ son cardinal (eventuellement infini) alors l'application lineaire*

$$P(X) \in K[X]_{\deg P<|K|} \mapsto P(\bullet) \in \mathscr{F}(K;K)$$

est injective (tout polynome de degre $<|K|$ peut etre identifie avec une unique fonction polynomiale). En particulier si $\mathrm{car} K = 0$ *alors* $|K| \geqslant |\mathbb{Q}| = \infty$ *l'application*

$$P(X) \in K[X] \mapsto P(\bullet) \in \mathscr{F}(K;K)$$

est injective.

Preuve : Soit $P \in \ker(\text{fct. Pol})$

si $P \neq 0$ alors $\forall z \in K \quad P(z) = 0$

et $\mathrm{rac}_P(K) = K$

$|K| = |\mathrm{rac}_P(K)| \leqslant \deg P < |K|$.

$K = \mathbb{F}_p \qquad \forall x \in \mathbb{F}_p \qquad x^p - x = 0$

$$\mathrm{rac}_{X^p - X}(\mathbb{F}_p) = \mathbb{F}_p .$$

Application aux Ideaux de $K[X]$

- $K[X]$ $\quad I$ un idéal de $K[X]$

$I \subset K[X] \quad \forall P \in K[X] \quad P.I \subset I$

I est un sous gpe de $(K[X], +)$

- <u>Idéaux principaux :</u>

$Q \in K[X] \quad (Q) = Q.K[X] = K[X].Q$

l'ensemble des multiples de Q = l'idéal (principal) engendré par Q.

Théorème 5.7. *Soit $I \subset K[X]$ un ideal alors il existe $Q \in K[X]$ tel que*
$$I = (Q) = \{S.Q,\ S \in K[X]\}$$
est l'ensemble des multiples de Q. De plus si on suppose Q unitaire alors Q est unique.

Définition 5.9. *Soit $I \subset K[X]$ un ideal non-nul alors l'unique polynome unitaire Q_I tel que*
$$I = (Q_I) = Q_I.K[X]$$
est appelle polynome minimal de I. Si $I = \{0_K\}$ est l'ideal nul on posera
$$Q_I = 0_K.$$

Preuve: $I \subset K[X]$ principal $I \neq \{0_K\}$ et soit $Q \subset I$ un polynome $\neq 0$ de degre minimum. (Si $I = \{0_K\}$ on a fini)

Ops Q est unitaire : si

$$Q = a_q X^q + a_{q-1} X^{q-1} + \dots + a_0 \quad a_q \neq 0$$

$$\frac{1}{a_q} \cdot Q = X^q + \frac{a_{q-1}}{a_q} X^{q-1} + \dots + \frac{a_0}{a_q}$$

est unitaire et ds I.

On va mq $Q \cdot K[X] = I$

Si $P \in I$ on a une division euclidienne

$$P = QS + R \quad \text{avec } d^\circ R < d^\circ Q$$

$$R = \underset{\substack{\cap \\ I}}{P} - \underset{\substack{\cap \\ I}}{Q}S \in I$$

Comme R est de $d^\circ < d^\circ Q$ et Q est de d° minimal parmi les Poly $\neq 0$ de $I \Rightarrow R = 0$

$P = QS$ / $P \in (Q)$ $I = (Q)$ $\square$

Q unitaire et unique tel que

$$(Q) = I$$

Si Q_1 unitaire et qui engendre $I = (Q)$

$$Q_1 \in \underset{\cap}{I} \qquad Q_1 = Q.S \quad d^\circ Q_1 \geq \deg Q$$

$$Q \in (Q_1) \qquad Q = Q_1.S_1 \quad d^\circ Q \geq \deg Q_1$$

$$Q - Q_1 = X^q + \text{Pol de } d^\circ \leq q-1 - X^q - \text{Poly de } d^\circ \leq q-1$$

$$= \text{Pol de } d^\circ \leq q-1 \qquad Q - Q_1 = 0 \quad \square$$

Proposition 5.10. *Soient*

$$I = (P) = P.K[X] \text{ et } J = (Q) = Q.K[X]$$

des ideaux de $K[X]$ *engendres par des polynomes* P *et* Q *alors on a*

$$I \subset J \Longleftrightarrow Q|P.$$

$J = K[X].Q$ et si $I \subset J \Rightarrow P \subset QK[X]$

Si $P = QS$ et $P_1 \in (P)$

$P_1 = P.S_1 = Q.S.S_1 \in J.$

Corollaire 5.3. *Soit B un anneau et $\varphi : K[X] \mapsto B$ un morphisme d'anneaux. Alors il existe $Q_\varphi \in K[X]$ unitaire (ou nul) tel que*

$$\ker(\varphi) = Q_\varphi . K[X].$$

Le polynome Q_φ s'appelle le polynome minimal de φ.

Factorisation en Irreductibles

Définition 5.11. *Un polynome $P(X) \in K[X]$ non constant est irreductible (ou premier) si les seuls diviseurs de P sont les multiples de 1 ou de P:*

$$Q|P \Longrightarrow Q = \lambda \text{ ou } Q = \lambda.P, \ \lambda \in K^{\times}.$$

De maniere equivalente: P est irreductible si et seulement si

$$Q|P \Longleftrightarrow \deg Q = 0 \text{ ou } \deg P$$

On notera $\mathscr{P} \subset K[X]$ l'ensemble de tous les polynomes irreductibles et $\mathscr{P}_u \subset \mathscr{P}$ l'ensemble de ceux qui sont unitaires.

Proposition 5.11. *(Lemme de Gauss) Soit P irreductible, si $P|Q_1.Q_2$ alors $P|Q_1$ ou $P|Q_2$.*

<u>Rmq</u>: Si P n'est pas irreductible c'est faux

$P = P_1.P_2 \quad d^\circ P_1, d^\circ P_2 \geq 1$

$P \mid P_1 P_2$ mais $P \nmid P_1 \quad P \nmid P_2$

<u>Preuve</u>:

$P \mid Q_1 Q_2$ supposons $P \nmid Q_1$

Soit $I = K[X]P + K[X]Q_1 \subset K[X]$

Comme $P \nmid Q_1$ $I \neq K[X]P$ (on va mq $I = K[X]$)

$I = D(X).K[X] = (D) \supset K[X]P$

$\Rightarrow$ $D \mid P$ mais comme P est irreductible

ou bien $D = C^{st}$ ou bien $D = \lambda P$ $\lambda \neq 0$

On n'a pas que $D = \lambda P$

$(D) = (P)$ et on a vu que $(D) \neq (P)$

$D = Cst \neq 0$ cqs $D = 1$ $(D) = K[X]$.

en particulier $K[X]P + K[X]Q_1 \ni 1$

$\exists$ $A(X)$ $B(X)$ tq

$$1 = A.P + B.Q_1$$

$\times Q_2 \qquad 1 = A.P + B.Q_1$

$$Q_2 = AP.Q_2 + BQ_1Q_2$$

on sait que $Q_1Q_2 = P.S$

$$Q_2 = (AQ_2 + BS)P$$

$\Rightarrow P \mid Q_2 \qquad \square$

Théorème 5.8. *Soient Q un polynome non constant alors Q se factorise de maniere unique sous la forme*

$$Q = \lambda.P_1.\cdots.P_s$$

ou les P_i sont des polynomes irreductibles unitaires et $\lambda \in K^\times$. De plus cette factorisation est unique: Si on a deux telles factorisation en irreductibles (unitaires)

$$Q = \lambda.P_1.\cdots.P_s = \mu.R_1.\cdots.R_r$$

alors $s = r$, $\lambda = \mu$ et il existe une permutation $\sigma : \{1, \cdots r\} \mapsto \{1, \cdots s = r\}$ telle que

$$R_i = P_{\sigma(i)}.$$

$$X^2 - 2X + 1 = (X-1)(X-1)$$

Rmq: $X - z$ et toujours irreductible.

<u>Preuve</u> : $Q \neq Cst$ par recurrence sur $d^\circ Q$

- Si $d^\circ Q = 1$ Q et irreductible

$$Q = aX + b = a\left(X + \frac{b}{a}\right) \quad a \neq 0$$

- $d^\circ Q = q+1$ (on suppose la factorisation pour tout polynome de $d^\circ \leq q$)

Q si Q est irreductible on a fini

$$Q = a_{q+1} X^{q+1} + \text{Pol de}^\circ \leq q$$

$$Q = a_q \underbrace{\left(X^{q+1} + \text{Pol de } d^\circ \leq q \right)}_{\text{et irred unitaire.}}$$

- Sinon il existe Q_1, Q_2 $d^\circ Q_i \geq 1$ $i=1,2$

tq $Q = Q_1 . Q_2$ $d^\circ Q_i \leq q$ $i=1,2$

par recurrence

$$Q_1 = \lambda_1 P_1 \ldots\ldots P_{s_1} \quad Q_2 = \lambda_2 R_1 \ldots R_{s_2}$$

P_i, R_j irred unitaires

$$Q = Q_1 Q_2 = \lambda_1 \lambda_2 P_1 \dots P_{s_1} . R_1 \dots R_{s_2}$$

Unicité :

$$Q = \lambda P_1 \dots P_s = \mu R_1 \dots R_r$$

$P_s \mid R_1 \dots R_r$ et par Gauß

P_s divise l'un de R_i (par exemple R_r)

$P_s \mid R_r$ R_r est irred

$$P_s = \eta R_r \quad \eta \neq 0 \Rightarrow \text{même } d^\circ$$

$$P_s = X^n + \text{pol de } d^\circ \leq n-1 = \eta(X^n + \text{pol de } d^\circ \leq n-1)$$

$$\Rightarrow \quad 1 = \eta \Rightarrow P_s = R_s$$

$$Q = \lambda P_1 \dots P_s = \mu R_1 \dots P_s$$

$$Q_1 = \lambda P_1 \dots P_{s-1} = \mu R_1 \dots R_{r-1}$$

$\deg Q_1 < \deg Q$ on finit par récurrence sur $d^\circ Q_1$. $\square$

<u>Valuation</u> : Soit $Q \neq Cst$ $\deg Q = q \geq 1$

$$Q = a_q \prod_{P \in \mathcal{P}_U} P^{v_P(Q)}$$

- P parcourt l'ensemble (infini) de poly irred unitaire
- $v_P(Q) \in \mathbb{N}$ $v_P(Q) = 0$ pour tout $P \in \mathcal{P}_U$ sauf un nb fini. ($P^0 = 1$)

$v_P(Q)$ est la + grde puissance $v \geq 0$ tq

$P^v \mid Q$. $\quad P^{v_P(Q)} \mid Q \quad P^{v_P(Q)+1} \nmid Q$

Def : $v_P(Q)$ = la valuation P-adique de Q

la valuation de Q en P

On pose $v_P(0) = +\infty$

Propriete fetionnelles de la valuation

$$v_p(QR) = v_p(Q) + v_p(R)$$

- $Q.R = a_q b_r \prod_{P \in \mathcal{P}_U} P^{v_p(Q)+v_p(R)}$
- On a $Q \mid R$ ssi $\forall P \in \mathcal{P}_U \quad v_p(Q) \leq v_p(R)$
- $v_p(Q+R) \geq \min(v_p(Q), v_p(R))$ avec $=$ si $v_p(Q) \neq v_p(R)$

PGCD & PPCM : $P, Q \in K[X] - \{0\}$

$$(P) = K[X].P \quad (Q) = K[X].Q$$

$$(P) \cap (Q) \subset (P),(Q) \subset (P) + (Q) = \langle P, Q \rangle$$

Le PGCD = generateur unitaire de l'ideal

$$(P) + (Q) = R.K[X] \quad R \text{ unitaire}$$

$$R = PGCD(P, Q) = (P, Q)$$

Comme $(P),(Q) \subset (R)$

$\Rightarrow R \mid P$ et $R \mid Q$ et si S divise P et Q

alors $S \mid R$

$S \mid P$ et $S \mid Q$ $\quad (P),(Q) \subset (S)$

et $\Rightarrow (P)+(Q) = (R) \subset (S)$

$S \mid R$. $\qquad R = (P,Q)$

Proposition 5.12. *(Bezout) Soient P, Q des polynomes. Il existe $A, B \in K[X]$ tels que*

$$(P, Q) = A.P + B.Q.$$

En particulier, deux polynomes P et Q sont premiers entre eux ssi il existe $A, B \in K[X]$ tels que

$$1 = A.P + B.Q.$$

$$(P,Q).K[X] = (P) + (Q) = K[X].P + K[X].Q$$

$$(P,Q) = AP + BQ.$$

Algorithme d'Euclide

P et Q but : calculer (P,Q)

si $d^\circ P \geq d^\circ Q$ on fait la division de P par Q

$$P = SQ + R \quad d^\circ R < d^\circ Q$$

- si $R = 0$ $P = SQ$ $Q \mid P$ $(P,Q) = Q$ fini

si $R \neq 0$ on applique la procedure a Q et R

$d^\circ Q > d^\circ R$

......

Si $P = QS + R$

$$(P,Q)K[x] = (P) + (Q) = K[x]P + K[x]Q$$
$$= K[x]S.Q + RK[x] + K[x]Q$$
$$= (K[x]S + K[x]).Q + K[x]R$$
$$= (Q) + (R) = (Q,R)K[x]$$

$$(P,Q) = (Q,R)$$

PPCM : $(P) \cap (Q) = \underbrace{[P,Q].K[X]}$

Proposition 5.13. *(Formule du produit) Soient $P, Q \in K[X] - \{0\}$ et unitaires. On a*

$$P.Q = [P, Q](P, Q).$$

Théorème 5.10. *Soient Q, R des polynomes non-nuls de degres q et r et*

$$Q = a_q. \prod_{P \in \mathscr{P}_u} P^{v_P(Q)}, \quad R = b_r. \prod_{P \in \mathscr{P}_u} P^{v_P(R)}$$

eur decompositions en polynomes irreductible unitaires alors

$$(Q, R) = \prod_{P \in \mathscr{P}_u} P^{\min(v_P(Q), v_P(R))}, \quad [Q, R] = \prod_{P \in \mathscr{P}_u} P^{\max(v_P(Q), v_P(R))}.$$

THÉORÈME 5.10. *Soient Q, R des polynomes non-nuls de degres q et r et*

$$Q = a_q . \prod_{P \in \mathscr{P}_u} P^{v_P(Q)}, \; R = b_r . \prod_{P \in \mathscr{P}_u} P^{v_P(R)}$$

leur decompositions en polynomes irreductible unitaires alors

$$(Q, R) = \prod_{P \in \mathscr{P}_u} P^{\min(v_P(Q), v_P(R))}, \; [Q, R] = \prod_{P \in \mathscr{P}_u} P^{\max(v_P(Q), v_P(R))}.$$