Ch 1 : Construction de l'anneau des polynômes K[X]

1) Rappel sur la structure d'anneau :

Théorie des modules

Déf : On appelle anneau $(A, +, \times)$ un ensemble muni de 2 lois internes : additif noté + et multiplicatif noté × Tq

→ 1) $(A, +)$ groupe abélien (commutatif)

→ 2) La loi × est associative ~~et admet un élément neutre~~

→ 3) La loi × est distributive par rapport à +

$\forall x, y, z \in A$: $x \times (y+z) = (x \times y) + (x \times z)$

$(y+z) \times x = (y \times x) + (z \times x)$

Si de plus la loi × est commutative on dit que l'anneau est commutatif. Si A admet un élément neutre 1 pour la loi × : on dit que A est un anneau unitaire

Exp : $(\mathbb{Z}, +, \times)$ anneau commutatif unitaire

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ anneau commutatif

~~$(M_n(\mathbb{R}), +, \times)$~~ anneau unitaire non abélien

Corps : Un corps est un anneau commutatif unitaire où tout élément différent de 0 est inversible pour la loi ×

Déf : On appelle élément inversible de l'anneau $(A, +, \times)$ tout élément inversible pour la multiplication

A : x inversible $\Leftrightarrow \exists y \in A : x \times y = y \times x = 1$

Exp : 1) a est inversible dans $\mathbb{Z}/n\mathbb{Z}$ ssi $pgcd(a, n) = 1$

2) $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps $\Leftrightarrow$ n est premier

Th de Bézout : p et q premiers entre eux $\Leftrightarrow \exists m, n \in \mathbb{Z} : \; mp + nq = 1$

Déf 3 : On appelle diviseur de 0 dans un anneau $(A, +, \times)$ tout élément $a \in A$ $\exists b \neq 0 \in A$ vérifiant $a \times b = 0$

Déf 4 : On appelle sous-anneau B d'un anneau $(A, +, \times)$ tout sous-ens B de A tq les lois $+, \times$ induites sur B le munissent d'une structure d'anneau (R, *)

* $(B, +)$ groupe abélien
* La loi $\times$ est interne dans B

[~~Remarque : $1 \in B$ ou pas que~~]

Proposition : B est un sous anneau de A ssi :

* $\forall x, y \in B : \; x + (-y) \in B$
* $\forall x, y \in B : \; x \times y \in B$

$\Leftrightarrow \forall x, y, z \in B : \; x(y - z) \in B$

exp : Rq les seuls sous anneaux de $(\mathbb{Z}, +, \times)$ sont les $n\mathbb{Z}$

1) $\forall n \in \mathbb{N}$; $n\mathbb{Z}$ sous anneau de $(\mathbb{Z}, +, \times)$: évident

2) Soit B un sous-anneau de $\mathbb{Z}$; mq : $\exists n \in \mathbb{N} : \; B = n\mathbb{Z}$

On prend $B^+ = \{ a \in B : a > 0 \}$; soit $p = \min B^+$ et montrons que $\forall a \in B \; \exists b \in \mathbb{Z} : \; a = bp$ donc $B = p\mathbb{Z}$

On a $\forall a \in B : \; a = bp + r \;/\; 0 \leq r < p$

on a $p = \min B^+ \Rightarrow r = 0$ donc $\forall a \in B : \exists b \in B : \; a = bp$

$\Rightarrow \boxed{B = p\mathbb{Z}}$

A !

Entiers de Gauss : $\mathbb{Z}[i] = \{a+ib \mid a,b \in \mathbb{Z}\}$ sous anneau de $\mathbb{C}$

$(a+ib).(a'+ib') = 1 \Leftrightarrow \begin{cases} aa' - bb' = 1 \\ ab' + a'b = 0 \end{cases}$

Déf 5 : Un idéal I d'un anneau $(A,+,\times)$ est un sous anneaux de A tq : $\forall a \in I, \forall b \in A$: ($a \times b \in I$ et $(I,+)$ sous groupe)

Proposition : si $(A,+,\times)$ est un anneau unitaire et $1 \in I$ ou un élément inversible est dans I alors $\boxed{I = A}$

exp : les $n\mathbb{Z}$ sont des idéaux de $\mathbb{Z}$

Morphisme d'anneaux :

Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux, on appelle morphisme $f : A \to B$ une application vérifiant :

1) $\forall x,y \in A \quad f(x +_A y) = f(x) +_B f(y)$

2) $\forall x,y \in A : f(x \times_A y) = f(x) \times_B f(y)$

et si A et B sont unitaires : $f(1_A) = 1_B$

- **Relation d'équivalence dans un anneau en utilisant les Idéaux**

On définit la relation $\mathcal{R}$ dans A par :

$\forall x,y \in A : x \mathcal{R} y \Leftrightarrow x - y \in I$; $\dot{x} = \{x + I\}$

Théorème : Si I est un idéal de $(A,+,\times)$ alors $(A/I, \dot{+}, \dot{\times})$ un anneau. Unitaire si A est unitaire et commutatif si A est $(A,+,\times)$ commutatif.

$\forall \dot{x}, \dot{y} \in A/I$: $\dot{x} \dot{+} \dot{y} = \overset{\cdot}{x+y}$

$\dot{x} \dot{\times} \dot{y} = \overset{\cdot}{x \times y}$

Déf: On appelle anneau intègre tout anneau ne contenant pas de diviseurs de 0.

Théorème: Soit $f: A \to B$ un morphisme d'anneaux, alors $\ker f$ est un idéal de A et $A/\ker f$ est isomorphe à $\operatorname{Im} f$

Preuve: $\ker f$ idéal de A :

$\forall x, y \in \ker f$: $x - y \in \ker f$ car $f(x) - f(y) = 0_B - 0_B = 0_B$

$\forall x \in \ker f, \forall y \in A$: $x \cdot y \in \ker f$ car $f(xy) = f(x) \times f(y) = 0_B \times f(y) = 0_B$

D'où $\ker f$ est un idéal de A

$f(A)$ sous-anneau de B :

$\Leftrightarrow \forall y_1, y_2 \in f(A)$: $y_1 - y_2 \in f(A)$ car $\exists x_1, x_2 \in A$, $y_1 = f(x_1)$; $y_2 = f(x_2)$

$y_1 - y_2 = f(x_1 - x_2) \in f(A)$

$\forall y_1, y_2 \in f(A)$: $y_1 \times y_2 \in f(A)$

car $y_1 \times y_2 = f(x_1 \times x_2) \in f(A)$

D'où $f(A)$ est un sous anneau de B.

Soit $F : A/\ker f \to \operatorname{Im} f = f(A)$

$\dot{x} \mapsto F(\dot{x}) = f(x)$

$\forall \dot{x}, \dot{x}' \in A/\ker f$:

$\dot{x} = \dot{x}' \Rightarrow x - x' \in \ker f \Leftrightarrow f(x - x') = f(x) - f(x') = 0_B$

$\Rightarrow f(x) = f(x') \Rightarrow F(\dot{x}) = F(\dot{x}')$

F ne dépend pas du choix de représentant de la classe.

1) $\forall y \in f(A)$: $\exists x \in A$ · $y = f(x) = F(\dot{x}) \Rightarrow F$ surjective

2) $\ker F = \{ \dot{x} \in A/\ker f : F(\dot{x}) = \dot{0} \} \overset{?}{=} \dot{0} = \{ x : x \in \ker f \}$?

~~$F(\dot{x}) = 0$~~

$F(\dot{x}) = 0 \Rightarrow f(0) \Leftrightarrow f(x) = 0 \Rightarrow x \in \ker f \Rightarrow \dot{x} = \dot{0}$

D'où F injective

Déf: Soit $(A, +, \times)$ un anneau, E une partie de A, on appelle idéale engendré par E le plus petit idéal qui contient E, on note $Id(E)$.

Rq: si $E = \{ x_1, x_2, \dots, x_n \}$

$Id(E) = \{ A x_1 + A x_2 + \dots + A x_n \}$

Déf: On appelle idéale principal tout idéal I engendré par un seul élément de A ; $I = a \times A$

exp: $n\mathbb{Z}$ est un idéal principal de $\mathbb{Z}$; $n\mathbb{Z} = Id(\{n\})$

Déf: On appelle idéal maximal I de $(A, +, \times)$ tout idéal non contenu dans aucun autre idéal. ($I \subset I$ et $I \subset A$ only)

Théorème: I maximale ssi A/I est un corps → à démontrer

/ $(A, +, \times)$ anneau unitaire

Rq: $\mathbb{Z}/n\mathbb{Z}$ $n\mathbb{Z}$ maximal $\Leftrightarrow$ n est premier

Rq: $Id(E) = \bigcap_{\substack{E \subset I \\ I \text{ idéal}}} I$

Rq:

$f : A \longrightarrow B$

inj ↓ ↑ surj

$A/\ker f \xrightarrow{\text{isom}} \text{Im} f$

Définitions :

1) Un anneau $(A, +, \times)$ est dit principale si tout idéal I de A est engendré par un seul élt :

$\forall I$ Idéal : $\exists a \in A$: $I = \langle a \rangle$

$\mathbb{Z}$ est un anneau principale

2) Un anneau $(A, +, \times)$ est dit intègre s'il n'existe aucun diviseur de 0 dans A.

Un Idéal I est dit premier si A/I est intègre

Exp : $6\mathbb{Z}$ n'est pas premier car $\mathbb{Z}/6\mathbb{Z}$ contient des diviseurs de 0, par contre $2\mathbb{Z}$, $3\mathbb{Z}$, $5\mathbb{Z}$ sont premiers.

Proposition : $n\mathbb{Z}$ est premier dans $\mathbb{Z}$ ssi n est premier

I est premier ssi $\forall a,b \in A$, $ab \in I \Rightarrow a \in I$ ou $b \in I$

Notions de Divisibilité

Soient $a,b,c \in (A, +, \times)$, on dit que a divise b et on écrit a/b ssi $\exists c \in A$ / $b = a \times c$ ie : $\langle b \rangle \subset \langle a \rangle$

Exercice.

Soit $(A, +, \times)$ un anneau, on appelle centre de A l'ensemble $\mathcal{C} = \{a \in A : \forall x \in A : a \times x = x \times a\}$

montrer que $\mathcal{C}$ est un idéal de A et Définir $A/\mathcal{C}$

$\forall a,b \in \mathcal{C}$

$\forall x \in A$ $(a-b)x = ax - bx = xa - xb = x(a-b) \Rightarrow a-b \in \mathcal{C}$

$\forall a \in \mathcal{C}, \forall x \in A$

$\Rightarrow \forall x \in A$ $(ab)x = (ba)x = b(ax) =$

Déf: Soit $(A, +, \times)$ un anneau, on dit qu'un élt $a \in A$ est nilpotent d'ordre n ssi $a^n = 0$

Soit N = l'ens des nilpotents de A.

Mq N est un idéal de A.

Formule du binôme dans un anneaux Commutatifs $(a+b)^2 = a^2 + b^2 + 2ab$

" " " non " $(a+b)^2 = a^2 + ab + ba + b^2$

II] L'anneau des polynômes

Déf: On appelle polynôme à une indéterminée à coefficients dans un corps $\mathbb{K}$ (un anneau A) toute suite $P = (a_i)_{i \in \mathbb{N}}$ d'éléments de $\mathbb{K}$ (de A) nuls à partir d'un certain rang n appelé degré de P.

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

$x = (0, 1, 0, 0, \dots)$

$x^n = (0, 0, \dots, 1, 0, \dots)$ (1 à la place n)

alors: la schématisation formelle d'un polynôme P $(a_0, a_1, \dots)$

$P(x) = \sum_{i=0}^{n} a_i x^i$

ainsi $\mathbb{K}[x]$ est appelé anneau de polynômes à une indéterminée à coefficients dans $\mathbb{K}$

$\mathbb{K}[x]$ est une $\mathbb{K}$-algèbre (Un anneau qui possède une structure (extérieure) d'espace vectoriel)

Propriété : Soient $(a_i)_{i\in\mathbb{N}}$; $(b_i)_{i\in\mathbb{N}}$ alors :

- $P+Q = (a_i + b_i)_{i\in\mathbb{N}}$
- $\lambda P = (\lambda a_i)_{i\in\mathbb{N}}$ $\forall \lambda \in \mathbb{K}$
- $P.Q = (c_i)_{i\in\mathbb{N}}$ tq $c_i = \sum_{k=0}^{i} a_k b_{i-k}$

$(\mathbb{K}[X], +, \times)$ anneau commutatif unitaire

$P(x) = x$; $\langle P \rangle = \{ xQ(x) \ / \ Q \in \mathbb{K}[X] \}$

~~Division~~

Diviseurs de $\mathbb{K}[X]$

Theoreme : Soient $A, B \in \mathbb{K}[X]$, $B \neq 0$; il existe un unique couple $(Q, R) \in (\mathbb{K}[X])^2$: $A = BQ + R$ / $d^\circ R < d^\circ B$

Def : Si $R = 0$, on dit que B divise A : $A = BQ$

Proposition : Si $A \mid B$ et $B \mid A$ alors $\exists \lambda \in \mathbb{K}$ / $A = \lambda . B$

Preuve du Theoreme : On pose $b = d^\circ B$, et β son coefficient dominant (le coeff de x^b)

$(B(x) = a_0 + a_1 x + \dots + \beta x^b)$

1) Si B divise A : $\exists Q \in \mathbb{K}[X]$ / $A = B.Q$

alors $(Q, R=0)$ existent

2) Supposons que B ne divise pas A :

Soit $E = \{ A - BS \ / \ S \in \mathbb{K}[X] \} \neq \emptyset$

$E = \{ d^\circ(A - B.S) \ / \ S \in \mathbb{K}[X] \} \in \mathbb{N}$ non vide

On pose $\min E = r$ obtenu pour un certain polynôme Q

$A - BQ \in E$ et ~~deg Q = r~~ et $\deg(A - BQ) = r$

On pose $R = A - BQ$, $\deg R = r$

Rq : $r < b$

On suppose que $r \geq b$: alors

$$\deg\left(R - \frac{a_r}{\beta} X^{r-b} \times B\right) < r$$

$$R - \frac{a_r}{\beta} X^{r-b} \cdot B = A - BQ - \frac{a_r}{\beta} X^{r-b} \times B$$

$$= A - B \times \left(Q + \frac{a_r}{\beta} X^{r-b}\right) = A - BP \notin E$$

où $P = Q + \frac{a_r}{\beta} X^{r-b}$

On a donc :

$\deg(A - BP) < \min E$ ce qui est Absurde

D'où $\boxed{r < b}$

Unicité : par l'absurde :

On suppose qu'il $\exists (Q_1, R_1)(Q_2, R_2)$ tq

$A = BQ_1 + R_1 = BQ_2 + R_2$

$\deg(R_1) < b$

$\deg(R_2) < b$

$B(Q_1 - Q_2) = R_2 - R_1$

$Q_1 - Q_2 \neq 0 \Rightarrow \deg(B(Q_1 - Q_2)) \geq b$ et $\deg(R_2 - R_1) < b$

d'où $Q_1 - Q_2 = 0 \Rightarrow Q_1 = Q_2$ et $R_1 = R_2$

CQFD