4. A-algèbres de polynômes

1. Elément algébrique, élément transcendant
2. Construction de $A[X]$
3. Propriété universelle de $(A[X], j)$
4. Polynômes à plusieurs indéterminées
5. Division euclidienne dans $A[X]$
6. Racine d'un polynôme $P \in A[X]$

Soit un anneau $(A, +, 0, *, e)$ commutatif.

1. Elément algébrique, élément transcendant

Soit $A \hookrightarrow B$ une extension d'anneau.

Définitions (algébrique, transcendant sur A)

Soit $b \in B$. On dit que b est transcendant sur A si

$$(\forall n \in \mathbb{N})\left(\forall (a_k \in A)_{k\in[\![0,n]\!]}\right) \qquad \sum_{k=0}^{n} a_k b^k = 0 \implies \forall k \in [\![0,n]\!], \quad a_k = 0$$

Sinon, on dit que b est algébrique sur A.

Exemples :

1. Tout $x = \frac{a}{b} \in \mathbb{Q}$ est algébrique sur $\mathbb{Z}$ car $-a + bx = 0$.
2. $\sqrt{2} \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$ car $-2 + (\sqrt{2})^2 = 0$.
3. $e \in \mathbb{R}$ est transcendant sur $\mathbb{Q}$ (Hermite, 1873).
4. $\pi \in \mathbb{R}$ est transcendant sur $\mathbb{Q}$ (Lindemann, 1882).

Problème : Etant donné A, trouver $A \hookrightarrow B$, une extension d'anneau contenant un élément transcendant sur A.

2. Construction de $A[X]$

Soit un anneau $(A, +, 0, *, e)$ commutatif.

• Considérons l'ensemble des suites finies d'éléments de A :

$$B \overset{\text{déf}}{=} \left\{ b = (b_k)_{k\in\mathbb{N}} \in A^{\mathbb{N}} \ : \exists n \in \mathbb{N},\ \forall k \leq n, \quad b_k = 0 \right\}$$

On va munir B d'une structure de A-algèbre.

• Définissons d'abord une addition

$$\begin{array}{rcl} + : B \times B & \longrightarrow & B \\ \left((b_k)_{k\in\mathbb{N}}, (b'_k)_{k\in\mathbb{N}}\right) & \longmapsto & (b_k + b'_k)_{k\in\mathbb{N}} \end{array}$$

Désignons encore par 0 la suite nulle.

Exercice : $(B, +, 0)$ est un groupe abélien.

Construction de $A[X]$ (2)

- Définissons une multiplication par des éléments de A :

$$\begin{array}{rcl} \cdot : A \times B & \longrightarrow & B \\ (a, (b_k)_{k\in\mathbb{N}}) & \longmapsto & (a * b_k)_{k\in\mathbb{N}} \end{array}$$

de sorte que $(B, +, 0, \cdot)$ soit maintenant un A-module :

Définition (structure de A-module)

Soit $(A, +, 0, *, e)$ un anneau. On dit que $(M, +, 0, \cdot)$ est un A-module si $(M, +, 0)$ est un groupe abélien et si

$$(\forall a, a' \in A)(\forall m, m' \in M) \qquad \begin{array}{rcl} (a + a') \cdot m & = & a \cdot m + a' \cdot m \\ a \cdot (m + m') & = & a \cdot m + a \cdot m' \\ a \cdot (a' \cdot m) & = & (a * a') \cdot m \\ e \cdot m & = & m \end{array}$$

Si A est un corps, on parle de A-espace vectoriel.

Construction de $A[X]$ (3)

- Pour tout $n \in \mathbb{N}$, considérons la suite finie $\delta_n \in B$ définie par

$$\begin{array}{rcl} \delta_n : \mathbb{N} & \longrightarrow & A \\ k & \longmapsto & \delta_n(k) = \left| \begin{array}{lll} e & \text{si} & k = n \\ 0 & \text{si} & k \neq n \end{array} \right. \end{array}$$

Exercice : Tout élément $b \in B$ s'écrit de manière unique comme une somme finie (dire pourquoi) :

$$b = \sum_{n \in \mathbb{N}} b_n \cdot \delta_n$$

On dit que la famille $\{\delta_n \ : n \in \mathbb{N}\}$ forme une base de B.

- Définissons enfin une multiplication

$$\begin{array}{rcl} * : B \times B & \longrightarrow & B \\ \left((b_k)_{k \in \mathbb{N}}, (b'_k)_{k \in \mathbb{N}}\right) & \longmapsto & \left(\sum_{l=0}^{k} b_l * b'_{k-l}\right)_{k \in \mathbb{N}} \end{array}$$

Construction de $A[X]$ (4)

Exercices :

1. $(\forall b \in B) \qquad b * \delta_0 = \delta_0 * b = b.$
2. $(\forall n, n' \in \mathbb{N}) \qquad \delta_n * \delta_{n'} = \delta_{n+n'}.$
3. $(B, +, 0, *, \delta_0)$ est un anneau commutatif.
4.

$$\begin{array}{rcl} j : A & \longrightarrow & B \\ a & \longmapsto & a \cdot \delta_0 \end{array}$$

est un morphisme d'anneau injectif.

Convention : On identifiera A à $j(A)$, en notant encore a l'élément $a \cdot \delta_0$, de sorte que A est considéré comme un sous-anneau de B.

Définition de $A[X]$

On note

$$\begin{aligned} 1 &\overset{\text{notation}}{=} \delta_0 \\ X &\overset{\text{notation}}{=} \delta_1 \\ X^n &\overset{\text{notation}}{=} \delta_n, \quad \forall n \in \mathbb{N},\ n \geq 2 \end{aligned}$$

Définition (l'algèbre des polynômes en l'indéterminée X)

La A-algèbre $(B, +, 0, *, \delta_0)$ précédemment construite est notée $(A[X], +, 0, \cdot, 1)$ et s'appelle l'algèbre des polynômes en l'indéterminée X à cœfficients dans A.

Un élément de $A[X]$ s'appelle un polynôme à cœfficients dans A et se note $P = \sum_k a_k X^k$.

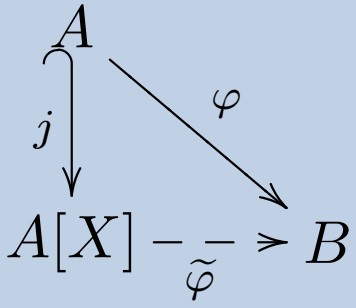
Exercice : Vérifier que $X \in A[X]$ est bien transcendant sur A.

3. Propriété universelle de $(A[X], j)$

Soit un anneau $(A, +, 0, \cdot, 1)$ commutatif.

Propriété universelle de l'algèbre des polynômes $(A[X], j)$

(PU) Pour tout triplet (B, φ, b) où (B, φ) est une $A-$algèbre et $b \in B$,
$\exists!\ \widetilde{\varphi} : A[X] \to B$ morphisme de $A-$algèbre tel que $\boxed{\widetilde{\varphi}(X) = b}$.



Démonstration : On doit avoir $(\forall a \in A) \quad \widetilde{\varphi}(a) = \varphi(a)$ et aussi :

$$\left(\forall P = \sum_k a_k X^k \in A[X]\right) \qquad \widetilde{\varphi}(P) = \sum_k \varphi(a_k) b^k$$

Vérifier que $\widetilde{\varphi} : A[X] \to B$ ainsi défini est un morphisme de A-algèbre (exercice). □

Propriété universelle de $(A[X], j)$ (suite)

Si de plus (B, φ) est une extension d'anneau, on identifie A à $\varphi(A)$, sous-anneau de B. Ainsi le morphisme de A-algèbre $\widetilde{\varphi}$ s'appelle l'évaluation en b :

$$\begin{array}{rcl} \widetilde{\varphi} : A[X] & \longrightarrow & B \\ P = \sum_k a_k X^k & \longmapsto & P(b) = \sum_k a_k b^k \end{array}$$

$\boxed{\mathrm{Im}(\widetilde{\varphi}) = A[b]}$, sous-anneau de B engendré par $A \cup \{b\}$ et on a :

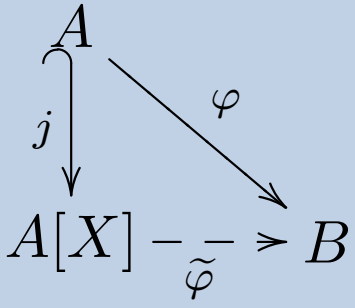
$$b \text{ transcendant sur } A \iff \mathrm{Ker}(\widetilde{\varphi}) = \{0\}$$

b est transcendant sur A si et seulement si $\widetilde{\varphi} : A[X] \to A[b]$ est un isomorphisme de A-algèbre.

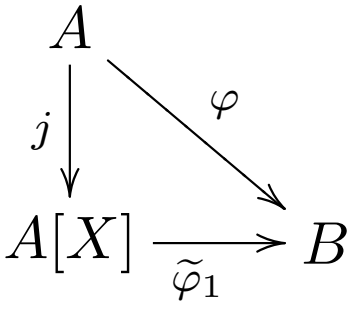
Unicité à isomorphisme (unique) de $(A[X], j)$

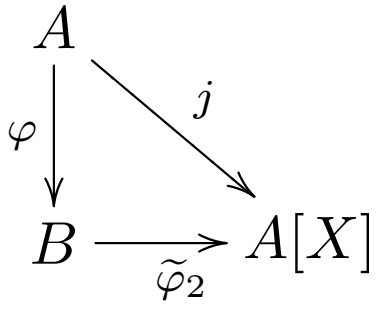
Théorème (unicité à isomorphisme (unique) près de $(A[X], j)$)

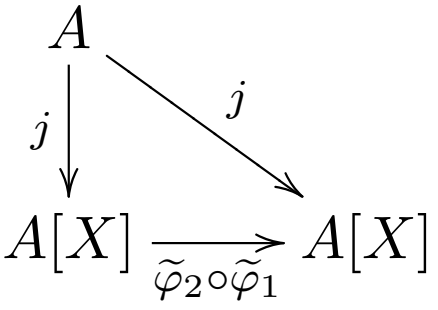
Si (B, φ, b), où (B, φ) est une A-algèbre et $b \in B$, vérifie aussi la propriété universelle, alors il existe un unique isomorphisme de A-algèbre $\widetilde{\varphi} : A[X] \to B$ tel que $\widetilde{\varphi}(X) = b$:

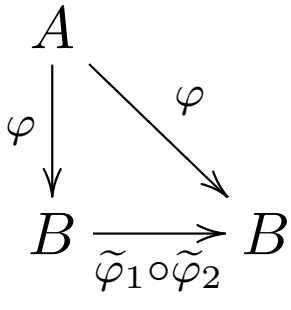


Démonstration :









□

4. Polynômes à plusieurs indéterminées

Soit un anneau $(A, +, 0, \cdot, 1)$ commutatif.

Théorème (algèbre des polynômes à m indéterminées)

Soit $m \in \mathbb{N} \setminus \{0\}$. Il existe un triplet $(\mathbb{A}, j, \alpha)$, où $(\mathbb{A}, j)$ est une A-algèbre et $\alpha : [\![1, m]\!] \to \mathbb{A}$ une application, ayant la propriété universelle :

$$(PU) \begin{cases} Pour\ tout\ triplet\ (B, \varphi, \beta)\ où\ (B, \varphi)\ est\ une\ A-algèbre\ et \\ \alpha : [\![1, m]\!] \to B\ une\ application, \\ \exists!\ \widetilde{\varphi} : \mathbb{A} \to B\ morphisme\ de\ A-algèbre\ tel\ que\ \boxed{\widetilde{\varphi} \circ \alpha = \beta}. \end{cases}$$

Un tel triplet $(\mathbb{A}, j, \alpha)$ est unique à isomorphisme unique près.

Notation : $(\forall k \in [\![1, m]\!]) \quad X_k \overset{\text{notation}}{=} \alpha(k)$

$$\mathbb{A} \overset{\text{notation}}{=} A[X_1, \ldots, X_m]$$

s'appelle l'algèbre des polynômes en les m indéterminées $X_1, \ldots, X_m$ à cœfficients dans A.

Polynômes à plusieurs indéterminées (suite)

Démonstration : existence par récurrence sur m.

• pour $m = 1$: le triplet $(A[X], j, \alpha)$, où $(A[X], j)$ est l'algèbre des polynômes en l'indéterminée X et $\alpha(1) = X$, satisfait (PU).

• pour $m > 1$: on construit $A[X_1, \ldots, X_m]$ par la relation de récurrence :

$$A[X_1, \ldots, X_m] = A[X_1, \ldots, X_{m-1}][X_m]$$

Un élément $P \in A[X_1, \ldots, X_m]$ s'écrit :

$$P = \sum_{k_m} \underbrace{\left(\sum_{k_1, \ldots, k_{m-1}} a_{k_1, \ldots, k_m} X_1^{k_1} \cdots X_{m-1}^{k_{m-1}} \right)}_{\in A[X_1, \ldots, X_{m-1}]} X_m^{k_m}$$

$$\overset{\text{notation}}{=} \sum_{k_1, \ldots, k_m} a_{k_1, \ldots, k_m} X_1^{k_1} \cdots X_m^{k_m}$$

Exercice : Vérifier la (PU), et en déduire l'unicité à isomorphisme près, comme d'habitude ...

□

5. Division euclidienne dans $A[X]$

Pour tout polynôme $P = \sum_n a_n X^n \ \in A[X]$, on définit :

Définitions (degré, cœfficient directeur, unitaire)

Si $P \neq 0$,

$$\deg(P) \overset{\text{déf}}{=} \max\{n \in \mathbb{N} \ : \quad a_n \neq 0\} \qquad \in \mathbb{N}$$

$a_{\deg(P)}$ s'appelle le cœfficient directeur (ou dominant) du polynôme P.
On dit que le polynôme P est unitaire si $a_{\deg(P)} \in A^*$.

Remarque : on a toujours $a_{\deg(P)} \neq 0$.

Lemme (du degré)

Pour tous polynômes non nuls $B = \sum b_n X^n$ et $C = \sum c_n X^n$, on a :

$$b_{\deg(B)} c_{\deg(C)} \neq 0 \implies \deg(BC) = \deg(B) + \deg(C)$$

Division euclidienne dans $A[X]$ (suite)

Corollaire

$$A \text{ intègre} \implies A[X] \text{ intègre et } A[X]^* = A^*$$

Exercice : démontrer le lemme et son corollaire.

Théorème (division euclidienne dans $A[X]$)

Soient $P, B \in A[X]$ avec B unitaire. Alors il existe un unique couple de polynômes (Q, R) vérifiant :

$$P = BQ + R \quad et \quad (R = 0 \ ou \ \deg(R) < \deg(B))$$

Si $R = 0$, on dit que B divise P et on note $B|P$.

Division euclidienne dans $A[X]$ (suite)

Démonstration : Soient $P = \sum a_n X^n$ et $B = \sum b_n X^n$ unitaire.

1. existence par récurrence sur $\deg(P)$.
   - si $P = 0$: $(Q, R) = (0, 0)$ convient.
   - si $\deg(P) < \deg(B)$: $(Q, R) = (0, P)$ convient.
   - si $\deg(B) \leq \deg(P)$: on applique l'hypothèse de récurrence au polynôme :
   $$P - a_{\deg(P)} b_{\deg(B)}^{-1} X^{\deg(P)-\deg(B)} B$$
2. unicité en exercice.

□

6. Racine d'un polynôme $P \in A[X]$

Soit un anneau $(A, +, 0, \cdot, 1)$ commutatif.
Exercice : Munir l'ensemble A^A des applications $f : A \to A$ d'une structure de A-algèbre de sorte que

$$\begin{array}{rcl} \Psi : A[X] & \longrightarrow & A^A \\ P & \longmapsto & \begin{array}{rcl} \Psi(P) : A & \longrightarrow & A \\ a & \longmapsto & P(a) \end{array} \end{array}$$

soit un morphisme de A-algèbre.

Définition (fonction polynôme)

$\Psi(P)$ s'appelle la fonction polynôme associée à P.

On la note plus simplement $\widetilde{P}$, ou même encore P, mais ce n'est pas sans danger car :
Attention : en général, Ψ n'est pas injectif (ex : $A = \mathbb{Z}/2\mathbb{Z}$ et vérifier qu'alors $P = X^2 + X \in \mathrm{Ker}(\Psi)$)

Racine d'un polynôme $P \in A[X]$

Lemme

Soient $P \in A[X]$ *et* $a \in A$.

$$P(a) = 0 \iff X - a | P$$

Démonstration : Le polynôme $X - a$ étant unitaire, la division euclidienne permet de conclure (exercice). □

Définition (racine d'ordre n d'un polynôme)

On dit que $a \in A$ est une racine d'ordre n (ou de multiplicité n) d'un polynôme $P \in A[X]$ si

$$(X - a)^n | P \quad \text{et} \quad (X - a)^{n+1} \not| P$$

polynôme dérivé et exercices

Soit un polynôme non nul $P = \sum_{n=0}^{\deg(P)} a_n X^n$.

Si $\deg(P) = 0$, on pose $P' = 0$, sinon

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

P' s'appelle le polynôme dérivé de P.

Exercices :

1. $a \in A$ est racine simple ($=$ d'ordre 1) de P si et seulement si a est racine de P mais pas de P'.
2. Si A est un anneau intègre, un polynôme de degré n a au plus n racines (comptées avec multiplicité). Contre-exemple pour $A = \mathbb{Z}/9\mathbb{Z}$.
3. Si A est un anneau intègre et $\mathrm{car}(A) = 0$, alors $a \in A$ est racine d'ordre n de P si et seulement si

$$P(a) = P'(a) = \cdots = P^{(n-1)}(a) = 0 \quad \text{et} \quad P^{(n)}(a) \neq 0$$