Algèbre Cours 10

Polynômes – Anneau de fraction

27 novembre 2009

Algèbre

Définition – Algèbre. Soit R un anneau commutatif. Une R-algèbre associative unitaire est un couple (A, ρ) où A est un anneau et $\rho : R \to A$ un morphisme d'anneaux tel que $\rho(R) \subset ZA$. On dit que ρ est le *morphisme structurel*.

Soit (A, ρ) et (B, ρ') deux R-algèbres. Un morphisme de R-algèbres de A dans B est un morphisme d'anneaux $f : A \to B$ vérifiant en plus $f\rho = \rho'$.

Exercice – $\mathbb{Z}$-algèbre et k-algèbre. Un anneau a-t-il beaucoup de structures de $\mathbb{Z}$-algèbre ? Qu'est-ce qu'un morphisme de $\mathbb{Z}$-algèbres ?
Soit k un corps. Montrer que le morphisme structurel est injectif (ce qui permet d'identifier k à un sous-anneau de ρ). Montrer qu'on peut munir la k-algèbre d'une structure de k-espace vectoriel. Comparer alors avec la définition vu en prépa. Montrer qu'un morphisme de k-algèbres est toujours k-linéaire pour les structures précédentes.

Séries Formelles

Définition – Série formelle. Soit A un anneau commutatif et $n \in \mathbb{N}$. On définit la A-algèbre des séries formelles à n indéterminées à coefficients dans A et notée $A[[X_1, \ldots, X_n]]$. L'ensemble sous-jacent à $A[[X_1, \ldots, X_n]]$ est l'ensemble des fonctions de $\mathbb{N}^n$ dans A ou encore l'ensemble des familles d'éléments de A indexés par $\mathbb{N}^n$: un élément typique de $A[[X_1, \ldots, X_n]]$ est de la forme $a = (a_{i_1,\ldots,i_n})_{(i_1,\ldots,i_n)\in\mathbb{N}^n}$ où $a_{i_1,\ldots,i_n} \in A$.
La somme de $a = (a_{i_1,\ldots,i_n})_{(i_1,\ldots,i_n)\in\mathbb{N}^n}$ et $b = (b_{i_1,\ldots,i_n})_{(i_1,\ldots,i_n)\in\mathbb{N}^n}$ est définie terme à terme par $c = a + b$ où $c_{i_1,\ldots,i_n} = a_{i_1,\ldots,i_n} + b_{i_1,\ldots,i_n}$ pour tout $(i_1, \ldots, i_n) \in \mathbb{N}^n$.
Le produit (qui est évidemment commutatif) de a et b est défini par $c = ab$ où

$$c_{i_1,\ldots,i_n} = \sum_{(j_1,\ldots,j_n)+(k_1,\ldots,k_n)=(i_1,\ldots,i_n)} a_{j_1,\ldots,j_n} b_{k_1,\ldots,k_n}$$

Le morphisme de A dans $A[[X_1, \ldots, X_n]]$ est donné par $a \mapsto i(a)$ où $i(a)_{0,\ldots,0} = a$ et $i(a)_{i_1,\ldots,i_n} = 0$ sinon.

Notation

Définition Pour $i \in \{1, 2, \ldots, n\}$, on définit $X_i \in A[[X_1, \ldots, X_n]]$ par $(X_i)_{0,\ldots,1,\ldots,0} = 1$ et $(X_i)_{i_1,\ldots,i_n} = 0$ sinon.

Exercice Que vaut X_i^j ? et ${X_1}^{i_1} \cdots {X_n}^{i_n}$? et $a{X_1}^{i_1} \cdots {X_n}^{i_n}$ pour $a \in A$?
« Justifier » alors la **notation** d'un élément de $A[[X_1, \ldots, X_n]]$ sous la forme

$$a = \sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{i_1,\ldots,i_n} {X_1}^{i_1} \cdots {X_n}^{i_n} .$$

Exercice Montrer que si A est intègre alors $A[[X_1, \ldots, X_n]]$ l'est aussi (on pourra introduire un ordre total compatible avec l'addition sur $\mathbb{N}^n$ (par exemple l'ordre lexicographique) et considérer les coefficients de plus bas degré).

Exercice Montrer que
$A[[X_1, \ldots, X_n]] = A[[X_1, \ldots, X_k]][[X_{k+1}, \ldots, X_n]]$.
Déterminer les inversibles de $A[[X_1, \ldots, X_n]]$.

Polynômes

Définition – Polynômes. L'ensemble des séries formelles dont le nombre de coefficients non nuls est fini est une sous-A-algèbre de $A[[X_1, \ldots, X_n]]$. notée $A[X_1, \ldots, X_n]$ et appelée l'algèbre des polynômes à n indéterminées à coefficients dans A.

Définition – Graduation. On dit que $P \in A[X_1, \ldots, X_n]$ est un polynôme homogène de degré m si $a_{i_1,\ldots,i_n} = 0$ dès que $i_1 + \cdots + i_n \neq m$.
Tout polynôme $P \in A[X_1, \ldots, X_n]$ se décompose de façon unique en $P = P_0 + P_1 + \cdots + P_m$ où P_i est homogène de degré i, $P_m \neq 0$. On dit que m est le degré total de P.

Exercice Montrer que
$A[X_1, \ldots, X_n] = A[X_1, \ldots, X_k][X_{k+1}, \ldots, X_n]$.
Déterminer les éléments inversibles, les diviseurs de 0, les éléments nilpotents de $A[X_1, \ldots, X_n]$.

PU des polynômes

Proposition – Propriété universelle des polynômes. Soit (B, ρ) une A-algèbre commutative et $b_1, \ldots, b_n \in B$. Il existe un unique morphisme φ de A-algèbres de $A[X_1, \ldots, X_n]$ dans B tel que $\varphi(X_i) = b_i$.
Il est donné par

$$\varphi\left(\sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{i_1,\ldots,i_n} {X_1}^{i_1} \cdots {X_n}^{i_n}\right) = \sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{i_1,\ldots,i_n} {b_1}^{i_1} \cdots {b_n}^{i_n}$$

φ est appelé le morphisme d'évaluation en les b_i.

Exercice Que se passe-t-il si on ne suppose plus B commutative ?

Exercice Énoncer et démontrer une propriété « d'unicité » des polynômes.

Exercice Montrer qu'il n'existe pas d'éléments U, V, W de l'anneau $\mathbb{Z}[X_1, X_2, X_3, Y_1, Y_2, Y_3]$ vérifiant

$$U^2 + V^2 + W^2 = ({X_1}^2 + {X_2}^2 + {X_3}^2)({Y_1}^2 + {Y_2}^2 + {Y_3}^2)$$

Division euclidienne

Proposition – Division euclidienne. Soit $U, V \in A[X]$. On suppose que le coefficient dominant de V est inversible dans A. Alors il existe un unique couple $(Q, R) \in A[X]$ tel que $U = VQ + R$ et $\deg R < \deg V$.

Corollaire – Racine. Soit $P \in A[X]$ et $a \in A$. On a les équivalences

1. $P \mid X - a$
2. $P(a) = 0$

Si elles sont vérifiées, on dit que a est une racine de P.

Définition – Multiplicité. Soit $P \in A[X]$ et $a \in A$. Il existe un unique entier $h \in \mathbb{N}$ tel que $(X - a)^h$ divise P et $(X - a)^{h+1}$ ne divise pas P. Cet entier s'appelle la multiplicité de a dans P.

Le cas intègre

Proposition Soit A est un anneau intègre (par exemple si $A = k$ est un corps), la somme des multiplicités des racines de P est inférieure ou égale à $\deg P$. En particulier, on a au plus $\deg P$ racines.
De façon précise, si $a_1, \ldots, a_k$ sont des racines de P de multiplicité respective $h_1, \ldots, h_k$, on peut écrire
$P = (X - a_1)^{h_1} \cdots (X - a_k)^{h_k} Q$ avec $Q(a_i) \neq 0$ pour tout i.

Corollaire Soit A un anneau intègre infini (par exemple un corps infini). Le morphisme de A-algèbres

$$\begin{cases} A[X_1, \ldots, X_n] \longrightarrow \mathscr{F}(A^n, A) \\ \qquad P \qquad\quad \longmapsto ((a_1, \ldots, a_n) \mapsto P(a_1, \ldots, a_n)) \end{cases}$$

est injectif.

Un réservoir d'identité

Application Soit A un anneau commutatif et $U, V \in \mathrm{M}_n(A)$. On a $\det(UV) = \det(U)\det(V)$ et aussi $\mathrm{com}(U)\mathrm{com}(V) = \mathrm{com}(UV)$ et encore $\chi_U(U) = 0$.

Polynôme symétrique

Définition – Polynôme symétrique. Soit A un anneau. Pour tout $\sigma \in \mathfrak{S}_n$, il existe un unique automorphisme φ_σ de A-algèbres de $A[X_1, \ldots, X_n]$ tel que $\varphi_\sigma(X_i) = X_{\sigma(i)}$. Un polynôme $P \in A[X_1, \ldots, X_n]$ est dit symétrique si $\varphi_\sigma(P) = P$ pour tout $\sigma \in \mathfrak{S}_n$. On note $A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ la sous-algèbre de $A[X_1, \ldots, X_n]$ formée des polynômes symétriques.

Définition – Polynôme symétrique élémentaires. On définit $\Sigma_k(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ comme le coefficient en Y^{n-k} dans $(Y + X_1) \cdots (Y + X_n)$. On a

$$\Sigma_k(X_1, \ldots, X_n) = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} X_{i_1} \cdots X_{i_k}.$$

Théorème Le morphisme d'évaluation en les Σ_k

$$\begin{cases} A[Y_1, \ldots, Y_n] \longrightarrow A[X_1, \ldots, X_n] \\ \qquad Q \qquad\quad \longmapsto Q(\Sigma_1, \ldots, \Sigma_n)\,. \end{cases}$$

est un morphisme injectif dont l'image est $A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$.

Partie multiplicative

Définition – Partie multiplicative. Soit A un anneau commutatif. Une partie multiplicative S de A est un sous-monoïde de $(A, *)$: $1 \in S$ et si $s, s' \in S$ alors $ss' \in S$.
Par exemple, pour $x \in A$, l'ensemble $\{x^n, n \in \mathbb{N}\}$ est une partie multiplicative de A. Si A est un anneau intègre alors $A \setminus \{0\}$ est une partie multiplicative de A. Plus généralement, l'ensemble des éléments réguliers est une partie multiplicative.

Exercice – Relation d'équivalence. On considère sur $A \times S$, la relation $\mathscr{R}$

$$(a, s)\mathscr{R}(a', s') \quad \Longleftrightarrow \quad \exists\, t \in S,\ t(as' - a's)$$

Montrer que c'est une relation d'équivalence sur $A \times S$. On note $S^{-1}A$ l'ensemble quotient $(A \times S)/\mathscr{R}$ et a/s la classe d'équivalence de (a, s).

Anneau de fractions

Proposition – Structure d'anneau. On définit sur $S^{-1}A$ les lois $+$ et $*$ par

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + s'a}{ss'} \qquad \text{et} \qquad \frac{a}{s} * \frac{a'}{s'} = \frac{aa'}{ss'}\,.$$

Les lois sont bien définies et $(S^{-1}A, +, *)$ est un anneau. De plus l'application $i : a \mapsto a/1$ muni $S^{-1}A$ d'une structure de A-algèbre (calculer le noyau de ce morphisme). De plus, $i(s)$ est inversible dans $S^{-1}A$ pour tout $s \in S$.

Proposition – Propriété universelle. Soit B un anneau commutatif et $f : A \to B$ un morphisme d'anneaux tel que $f(s)$ soit inversible dans B pour tout $s \in S$. Il existe un unique morphisme d'anneau $\varphi : S^{-1}A \to B$ tel que $\varphi \circ i = f$. Le morphisme φ est donné par $\varphi(a/s) = f(a)f(s)^{-1}$.

Exercice Que se passe-t-il si $0 \in S$?

Corps de fraction

Définition – Corps de fraction. Soit A un anneau intègre et $S = A \setminus \{0\}$ alors $S^{-1}A$ est un corps et le morphisme canonique $i : A \to S^{-1}A$ est injectif. On dit que $S^{-1}A$ est le corps de fraction de A et noté $\mathrm{Frac}(A)$.

Exemple Quel est le corps de fraction de $\mathbb{Z}$? et celui de $k[T]$? Plus généralement celui de $A[T]$ où A est un anneau intègre ? Si k est un corps, le corps de fraction de $k[X_1, \ldots, X_n]$ est noté $k(X_1, \ldots, X_n)$ et est appelé le corps des fractions rationnelles à n indéterminées à coefficient dans k.

Proposition – Propriété universelle. Soit A un anneau intègre, K un corps et $f : A \to K$ un morphisme injectif d'anneaux. Il existe un unique morphisme d'anneaux φ de $\mathrm{Frac}(A)$ dans K qui prolonge f (c'est-à-dire tel que $\varphi \circ i = f$).