Anneau des séries formelles. Applications.

Soient A un anneau commutatif unitaire et K un corps.

1. Définitions et généralités

1.1. définition et notations :

Déf : une série formelle à coefficients dans A est un élément de $A^{\mathbb{N}}$.
On note $A[[X]]$ l'ensemble $A^{\mathbb{N}}$.

On note X la série formelle $(0, 1, 0, 0 \dots)$,
et $\forall (a_n) \in A[[X]]$, on note $\sum_{n\geqslant 0} a_n \cdot X^n$ la série formelle (a_n).

1.2. structure d'algèbre :

Déf : on munit $A[[X]]$ de la structure de A-algèbre suivante :

* $(a_n) + (b_n) := (a_n + b_n)$.
* $(a_n)\cdot(b_n) := \left(\sum_{k=0}^{n} a_k \cdot b_{n-k}\right)$ [produit de Cauchy].
* $a\cdot(b_n) := (a\cdot b_n)$.

pour tous $(a_n), (b_n) \in A[[X]]$ et $a \in A$.

Prop : l'inclusion naturelle $A[X] \subset A[[X]]$ fait de $A[X]$ une sous-A-alg. de $A[[X]]$.

Ex : $\left(\sum_{n\geqslant 0} X^n\right)^2 = \sum_{n\geqslant 0} (n+1)\cdot X^n = \sum_{n\geqslant 1} n\cdot X^{n-1}$.

1.3. propriétés élémentaires et opérations sur $A[[X]]$:

- la dérivation $A[X] \longrightarrow A[X]$ s'étend en une dérivation

$$\begin{array}{rcl} A[[X]] & \longrightarrow & A[[X]] \\ S & \longmapsto & S' \end{array} \quad \text{définie par : si } S = \sum_{n\geqslant 0} a_n X^n, \quad S' := \sum_{n\geqslant 1} n\cdot a_n \cdot X^{n-1}.$$

Cette dérivation vérifie les mêmes règles de calcul que celle de $A[X]$.

- l'anneau $A[[X]]$ est muni d'une valuation naturelle, notée v :

si $S = \sum a_n X^n$, $v(S) := \inf\{n \geqslant 0 : a_n \neq 0\}$ (si A intègre).

$(v(0) = +\infty)$. $\begin{cases} v(x) = \infty \Leftrightarrow x = 0 \\ v(xy) = v(x) + v(y) \\ v(x+y) \geqslant \min(v(x), v(y)). \end{cases}$

- composition de séries formelles :

Soient $S, T \in A[[X]]$, $S = \sum a_n X^n$, $T = \sum b_n X^n$.
Si S est un polynôme ou si $v(T) > 0$, on peut définir $S \circ T \in A[[X]]$ par :

$$S\circ T := \sum_{n\geqslant 0} a_n \cdot T^n = \sum_{n\geqslant 0} a_n \cdot \left(\sum_{m\geqslant 0} b_m X^m\right)^n.$$

2. Propriétés algébriques et topologiques de $A[[X]]$:

2.1. Propriétés algébriques :

Prop : $A[[X]]$ est intègre $\Longleftrightarrow$ A est intègre.

Décrivons les éléments inversibles de $A[[X]]$:

Prop : $S = \sum a_n X^n$ est inversible dans $A[[X]] \Longleftrightarrow a_0 \in A^\times$.

Conseq : si A est un anneau local, d'idéal maximal $\mathfrak{m}$,
alors $A[[X]]$ est un anneau local, d'idéal maxi $(\mathfrak{m}; X) =: \mathfrak{m}'$
(i.e. $\mathfrak{m}' = \{S = \sum a_n X^n : a_0 \notin A^\times\} = A[[X]] \setminus A[[X]]^\times$).

- Anneau de Fractions :

Soit K un corps.
Alors $\mathrm{Frac}(K[[X]])$ est noté $K((X))$.
C'est l'ensemble (le corps) des séries de Laurent, dont les éléments sont les séries de la forme $\sum_{n\geqslant n_0} a_n X^n$, $n_0 \in \mathbb{Z}$ et $a_n \in K$.

- Division euclidienne :

Thm : Soit K un corps, $f = \sum a_i X^i \in K[[X]]$.
On suppose $f \neq 0$.
Pour tout $g \in K[[X]]$, $\exists!(q, r) \in K[[X]] \times K[X]$
tq $g = q\cdot f + r$ et $\deg r \leq v(f) - 1$.

Cor : l'anneau $(K[[X]], v)$ est euclidien (donc principal). C'est un anneau de valuation discrète, idéal maxi $\mathfrak{m} = (X)$.

. Généralisation : le théorème de division euclidienne se généralise à $A[[X]]$, où A est un anneau local complet.

. Exemple : si $A = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5}, \sqrt[7]{7})$, alors $A[[X]]$ n'est pas factoriel, alors que A l'est.

. Noethérianité :

Thm : si A est noethérien, alors $A[[X]]$ l'est aussi.

rq : les idéaux (X^n) sont les seuls idéaux de $K[[X]]$.

2.2. Propriétés topologiques :

Déf : on munit $K[[X]]$ de la topologie $\mathcal{T}$ produit sur $K^{\mathbb{N}}$, où K est lui-même muni de la topologie discrète.
Autrement dit, une base de voisinages de 0 ds $K[[X]]$ est donnée par les idéaux (X^n), $n \geqslant 0$.

Déf : soit $\lambda \in]0,1[$. $\forall S, T \in K[[X]]$,
on pose $d_\lambda(S,T) := \lambda^{v(S-T)}$.

Prop : $(K[[X]], d_\lambda)$ est un espace métrique complet, ultramétrique, et la topologie définie par d_λ est équivalente à la topologie $\mathcal{T}$.

On dit que $K[[X]]$ est un anneau de valuation discrète complet.

Prop : $K[[X]]$ est le complété de $K[X]$ pour la topologie précédente.
En particulier, $K[X]$ est dense dans $K[[X]]$, et $K[X]/(X^n) \xrightarrow{\simeq} K[[X]]/(X^n)$.

exemple : si $S = \sum a_n . X^n \in K[[X]]$,
la suite (S_N) où $S_N := \sum_{n=0}^{N} a_n . X^n \in K[X]$
converge vers S dans $K[[X]]$.

Prop : l'anneau topologique $K[[X]]$ est (localement) compact
$\iff$ K est un corps fini

Cor : si $\mathbb{F}$ est un corps fini, le corps $\mathbb{F}((X))$ est un corps de valuation discrète, complet, localement compact (comme les corps p-adiques).

. structure des anneaux de valuation discrète complet :

Thm : soit A un anneau de valuation discrète complet, de corps résiduel K. On suppose que A et K ont même caractéristique.
Alors $A \simeq K[[T]]$.

$\boxed{\text{Dév}^t\ 1}$: Thm : a) $K((X))$ est un corps complet.
b) si $h_n \in K((X))$, la série $\sum_{n \geqslant 0} h_n$ converge $\iff (h_n) \to 0$.
c) $K[[X]]$ est le complété de $K[X]$ (i.e. l'adhérence de $K[X]$ dans $K((X))$).

3. Applications

3.1. Séries génératrices et combinatoire :

Principe : pour étudier des nombres entiers (a_n) de nature combinatoire
par exemple $a_n := \#\{\text{arbres binaires à } n \text{ feuilles}\}$ ou
$a_n := \#\{(n_1, \dots, n_r) \in \mathbb{N}^r : n_1 + \dots + n_r = n\}$, on est souvent amené à étudier des séries formelles associées, de la forme $\sum_{n \geqslant 0} a_n . X^n$ (dans $\mathbb{Z}[[X]]$ par exemple).

Prop : si $(a_n) \in A^{\mathbb{N}}$, $\sum a_n X^n \in A[X]$
$\iff$ (a_n) vérifie une récurrence linéaire.
$[a_{n+p} = \alpha_0 . a_n + \alpha_1 . a_{n+1} + \dots + \alpha_{p-1} . a_{n+p-1}]$.

*** nombres de Fibonacci :**

$F_0 := 0, F_1 := 1, F_n := F_{n-1} + F_{n-2}$.

Alors la série génératrice $F(X) := \sum F_n . X^n$ vérifie

$$(1-X-X^2)F(X) = X \quad , \text{ i.e } F(X) = \frac{X}{1-X-X^2}.$$

En décomposant en élément simple, on trouve :

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

*** nombres de Catalan :**

plusieurs définitions équivalentes :

$C_n = \#\{$arbres binaires entiers à $n+1$ feuilles$\}$

$= \#\{$parenthésages d'une expression de $n+1$ facteurs$\}$

$= \#\{$triangulations d'un polygone convexe à $n+2$ côtés$\}$

$= \#\{$chemins monotones sous-diagonaux dans une grille $n \times n\}$.

Si $C(X) := \sum C_n . X^n$, on a :

Thm : $\left[\begin{array}{l} C(X) = \dfrac{1-\sqrt{1-4X}}{2X}, \text{ et :} \\ C_n = \dfrac{1}{n+1} . \dbinom{2n}{n}. \end{array}\right.$ $\boxed{\text{Dév}^t 2}$

*** nombre de solutions d'équations diophantiennes linéaires**

On fixe $\alpha_1, \dots, \alpha_r \in \cancel{\mathbb{N}}$, et $n \in \mathbb{N}$. On suppose $(\alpha_1, \dots, \alpha_r) = 1$.

On considère l'équation suivante :

$$(E_{\underline{\alpha}}, n) : \sum_{i=1}^{r} \alpha_i . x_i = n, \quad \text{d'inconnues } (x_i) \in \mathbb{N}^r.$$

On note $e_n := \#\{(x_i) \in \mathbb{N}^r$ solutions de $(E_{\underline{\alpha}}, n)\}$.

Thm : 1) on dispose d'une méthode permettant de calculer une formule pour e_n, valable pour tout $n \geq 0$.

$\boxed{\text{Dév}^t 3}$ 2) en outre, $e_n \underset{n\to\infty}{\sim} \dfrac{1}{\alpha_1 \cdots \alpha_r} . \dfrac{n^{r-1}}{(r-1)!}$.

Exemple : On cherche à déterminer le nombre de façons distinctes de payer n euros avec des pièces (en nombre illimité) de $\alpha_1, \alpha_2, \dots, \alpha_r$ euros $(\alpha_1 < \dots < \alpha_r)$.

On note $D(n; \alpha_1, \alpha_2 \dots \alpha_r)$ ce nombre.

i.e $D(n; \alpha_1, \dots, \alpha_r) := \#\{(x_1, \dots, x_r) \in \mathbb{N}^r : \sum \alpha_i . x_i = n\}$.

Le théorème assure que $D(n; \underline{\alpha}) \underset{n\to\infty}{\sim} \dfrac{1}{\alpha_1 \cdots \alpha_r} . \dfrac{n^{r-1}}{(r-1)!}$.

Plus précisément, on peut calculer par exemple :

$$D(n; 1, 2) = \frac{1}{4}\left(2n + 3 + (-1)^n\right) = \left[\!\left[\frac{2n+3}{4}\right]\!\right]$$

$$D(n; 1, 2, 5) = \left[\!\left[\frac{(n+4)^2}{20}\right]\!\right]. \quad \text{ex: } D(100; 1, 2, 5) = 541.$$

*** nombre de dérangements.**

On note $D_n := \#\{\sigma \in \mathfrak{S}_n$ sans point fixe$\}$.

Thm : on pose $D(T) := \sum_{n \geq 0} \frac{D_n}{n!} . T^n \in \mathbb{Q}[[T]]$.

1) $D(T) = \dfrac{e^{-T}}{1-T}$.

2) $D_n = n! . \displaystyle\sum_{k=0}^{n} \frac{(-1)^k}{k!}$

3) $\displaystyle\lim_{n\to\infty} \frac{D_n}{n!} = \frac{1}{e}$

3.2. Équations différentielles.

Pour résoudre certaines équations différentielles linéaires, on peut utiliser des séries formelles.

ex : $t^2 . y'' + (\alpha+1) t . y' + (t^2 + \frac{1}{4}) y = 0$, en cherchant $y = t^\alpha . \varphi(t)$

avec $\varphi(t)$ série formelle $\varphi(t) = \sum a_n . t^n$, $a_0 = 1$.

on trouve $a_{2n} = \dfrac{1}{\prod_{k \leq} P(\alpha + 2k)}$ et $a_{2n+1} = 0$, avec $P(X) = X(X-1) + (\alpha+1)X + \frac{1}{4}$.

3.3. Identités de Newton :

Soit $n \geq 1$, on note $S_k = X_1^k + \dots + X_n^k$ et σ_k les fonctions symétriques élémentaires.

Thm : on a $S_k - \sigma_1 S_{k-1} + \dots + (-1)^{k-1} . \sigma_{k-1} . S_1 + (-1)^k . k . \sigma_k = 0$.

Preuve : série formelle $\sum S_k . T^k = -T . P'(T) / P(T)$, où $P = \prod_{i=1}^{n} (1 - X_i T)$.