Extensions de corps

Déf 1.1 Soit K un corps. Une K-algèbre est un anneau A muni d'un morphisme d'anneaux $i: K \to A$ (qui est injectif).

– Un morphisme de K-algèbres (parfois appelé K-morphisme) est un morphisme $\varphi: A \to B$ de K-algèbres $K \xrightarrow{i} A$ et $K \xrightarrow{j} B$, t.q. $\varphi \circ i = j$.

Déf 1.2 (1) Soit K un corps. Une extension de corps de K est un corps L muni d'un morphisme de corps $K \xrightarrow{\theta} L$. On écrira L/K.

– Abus de notation fréquent : $K \subseteq L$ à la place de L/K. (on identifie K à son image dans L)

(2) Une sous-extension de L/K est un corps E muni de morphismes de corps

$$\begin{tikzcd} K \arrow[r] \arrow[rr, bend right, "\theta"'] & E \arrow[r] & L \end{tikzcd}$$

. On écrira $L/E/K$, et on appelera la donnée de ces extensions une tour de corps.

Exemples : (1) $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$, $\mathbb{C}/\mathbb{R}$

(2) $\mathbb{Q}(i) \hookrightarrow \mathbb{C}$ deux $\mathbb{Q}$-morphisme, où

$\varphi_1 : i \mapsto i$

$\varphi_2 : i \mapsto -i$

$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$

(3) $\mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{C}$ deux $\mathbb{Q}$-morphismes, où

$\varphi_1 : \sqrt[3]{2} \mapsto \sqrt[3]{2}$

$\varphi_2 : \sqrt[3]{2} \mapsto j\sqrt[3]{2}$

$j^3 = 1$, $j \neq 1$ et

$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}$

(4) Pour $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, l'application

$$\begin{array}{ccc} \mathbb{F}_p(T) & \to & \mathbb{F}_p(T) \\ x & \mapsto & x^p \end{array}$$ est ~~[illegible]~~ un morphisme de

corps (donc injective), ~~[illegible]~~ pas surjective.

(5) Soit $f : \mathbb{R} \to \mathbb{R}$ un morphisme de corps. Comme $f(1)=1$
on a que $f(n)=n$ pour tout $n \in \mathbb{Z}$, et donc $f(q)=q$, $\forall q \in \mathbb{Q}$.
Remarquons que si $r \leq s$ dans $\mathbb{R}$, on a $s = r + t^2$ avec un $t \in \mathbb{R}$,
donc $f(s) = f(r) + f(t)^2$, d'où $f(r) \leq f(s)$ et donc f est croissante.
Soit $A := \{q \in \mathbb{Q} \mid r < q\}$ et $B := \{q \in \mathbb{Q} \mid q \leq r\}$. Alors

$$\forall q \in A,\ f(r) \leq f(q) = q \quad \text{et} \quad \forall q \in B,\ q = f(q) \leq f(r)$$
$$\Downarrow \qquad\qquad\qquad \Downarrow$$
$$f(r) \leq \inf(A) = r \quad \text{et} \quad f(r) \geq \sup(B) = r,$$ d'où $f = \mathrm{id}_{\mathbb{R}}$.

<u>Déf. 1.3</u> Soit I un ensemble et $S := (X_i)_{i \in I}$ une famille
d'indéterminées indexée par I. On définit :

$$K[X_i \mid i \in I] := \left\{ P(X_{i_1}, \dots, X_{i_n}) \;\middle|\; \begin{array}{l} \exists \{i_1, \dots, i_n\} \subseteq I \text{ fini t.q.} \\ P \in K[X_{i_1}, \dots, X_{i_n}] \end{array} \right\}.$$

Remarquons que $K[X_i \mid i \in I] = \bigcup_{\substack{E \subseteq I \\ \text{fini}}} K[X_i \mid i \in E]$, ce qui permet
de définir les lois internes '+' et '.' sur $K[X_i \mid i \in I]$. On construit
ainsi une structure de K-algèbre sur $K[X_i \mid i \in I]$. De plus,
$K[X_i \mid i \in I]$ est intègre.

- Soit $K(X_i \mid i \in I) := \operatorname{Frac} K[X_i \mid i \in I]$. C'est une extension de corps de K.

Exemple : Soit $I = \mathbb{N}$. Le K-morphisme

$$K[X_i \mid i \in I) \longrightarrow K(X_i \mid i \in I)$$
$$X_i \longmapsto X_{i+1}$$

est un morphisme de corps non surjectif.

Remarquons que si I est fini, ~~on a~~ et on écrit $I = \{1, 2, \dots, n\}$, on a $K[X_i \mid i \in I] = K[X_1, \dots, X_n]$ et $K(X_i \mid i \in I) = K(X_1, \dots, X_n) =$ Frac $K[X_1, \dots, X_n]$.

Rmq. Si L/K est une ext. de corps, alors L est un K-espace vectoriel : $\alpha \in K$, $v \in L$, $\alpha \cdot v \in L$.

Déf. 1.4 Le degré d'une ext. de corps L/K, noté $[L:K]$, est la dimension du K-espace vectoriel L.

On a que $[L:K] \in \mathbb{N} \cup \{\infty\}$.

- Si $[L:K] < \infty$, on dira que L/K est une ext. finie.
- Si $[L:K] = \infty$, elle sera dite infinie (et on parlera de son cardinal).

Exemples : (1) $[\mathbb{C}:\mathbb{R}] = 2 = [\mathbb{Q}(i):\mathbb{Q}]$

$[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$

(2) $[\mathbb{R}:\mathbb{Q}]$ non-dénombrable (sinon $\mathbb{R}$ serait dénombrable

(3) $[K(X):K] = \max(\mathrm{Card}(K), \mathrm{Card}(\mathbb{N}))$;

une base est donnée par $\left\{ X^j, \frac{X^i}{P(X)^n} \;\middle|\; \begin{array}{l} j \in \mathbb{N} \quad i,n \in \mathbb{N}_{>0}, i < \deg P(X) \\ P(X) - \text{unitaire irréductible} \\ \text{dans } K[X] \end{array} \right\}$

<u>Thm. 1.5</u> Soit $M/L/K$ une tour de corps. Alors

$$[M:K] = [M:L]\cdot[L:K]. \quad \dots(1)$$

En particulier, M/K est une ext. finie ssi M/L et L/K le sont

<u>Rmq.</u> La relation (1) est à lire : si $\mathcal{B}_1$ est une base de M/L et $\mathcal{B}_2$ une base de L/K, alors $\dim_K M = \mathrm{Card}(\mathcal{B}_1 \times \mathcal{B}_2)$.

<u>Preuve:</u> Soit $(e_i)_{i\in I}$ une base du L-espace vectoriel M et $(f_j)_{j\in J}$ une base du K-esp. vectoriel L. Montrons que $(e_if_j)_{(i,j)\in I\times J}$ est une base de M/K.

- Cette famille est libre: si $\sum_{i,j} a_{ij} e_i f_j = 0$ avec $a_{ij}\in K$ qui sont tous, sauf un nombre fini, nuls, alors $\sum_{i\in I} e_i\left(\sum_{j\in J} a_{ij} f_j\right) = 0$. Comme $(e_i)_{i\in I}$ est libre sur L, on a que $\forall i \in I$, $\sum_{j\in J} a_{ij} f_j = 0$. Comme $(f_j)_{j\in J}$ est libre sur K, on a $a_{ij} = 0$, $\forall j \in J$, $\forall i \in I$.
- Elle est génératrice: pour $x \in M$, $\exists (l_i)_{i\in I}$ tous sauf un nombre fini nuls dans L, t.q. $x = \sum_{i\in I} l_i e_i$. De même, pour $i \in I$, $\exists (n_{ij})_j$ presque tous nuls dans K t.q. $l_i = \sum_{j\in J} n_{ij} f_j$. On a alors

$$x = \sum_{i,j} n_{ij} e_i f_j.$$

En conclusion, $\dim_K M = \mathrm{Card}(I\times J) = \mathrm{Card}(I) \times \mathrm{Card}(J) = \dim_K L \cdot \dim_L M.$ ▨

Soit L/K une extension et $S \subseteq L$.

Déf. 1-6 (1) Le sous-anneau de L/K engendré par S, noté $K[S]$ est défini comme $\bigcap_{\substack{K \cup S \subseteq A \subseteq L \\ A\text{ - sous-anneau de } L}} A$. C'est le plus petit sous-anneau de L contenant K et S.

(2) La sous-extension de L/K engendrée par S, notée par $K(S)$ est $\bigcap_{\substack{K \cup S \subseteq E \\ E\text{ - sous-corps de } L}} E$. C'est le plus petit sous-corps de L contenant K et S.

(3) On dira que L/K est de type finie s'il $\exists S \subseteq L$ tel que $L = K(S)$.

Rmq. (1) $K[S] = \mathrm{Vect}_K(\mathcal{B})$ avec $\mathcal{B} = \{\prod_{\text{fini}} \alpha \mid \alpha \in S\}$

(2) $K(S) = \mathrm{Frac}\, K[S]$

Si $S = \{a_1, \dots, a_n\} \subseteq L$, on écrira $K[a_1, \dots, a_n]$ et $K(a_1, \dots, a_n)$, resp.
On a alors $K[a_1, \dots, a_n] = \{P(a_1, \dots, a_n) \mid P \in K[X_1, \dots, X_n]\}$.

(3) $K(S) = \bigcup_{\substack{A \subseteq S \\ \text{finie}}} K(A)$ car $\bigcup_{A\text{ finie}} K(A)$ est un corps

(4) Toute extension de corps finie est de type fini.
(toute base est un ensemble générateur)

<u>Exemples:</u> (1) $\mathbb{Q}(\mu_n)/\mathbb{Q}$ avec $\mu_n \in \mathbb{C}$ racine primitive n-ième de l'unité avec $n \geq 1$, est une extension finie

On verra que $\mathbb{Q}(\mu_n) = \mathbb{Q}[\mu_n]$. On dit que $\mathbb{Q}(\mu_n)/\mathbb{Q}$ est une <u>ext. cyclotomique.</u>

(2) $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ - finie

(3) $K(X)/K$ est de type fini, mais pas finie

(4) $K(X_n \mid n \in \mathbb{N})/K$ n'est pas de type fini

$\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$ ne le sont pas non plus

On verra cela en utilisant des <u>bases de transcendances.</u>

Extensions algébriques et transcendantes

Soit L/K une ext. de corps.

<u>Déf. 1.7</u> Un élt. $\alpha \in L$ est dit <u>algébrique</u> sur K si $\exists P(X) \in K[X]$ t.q. $P(\alpha) = 0$. Sinon, il est dit <u>transcendant</u> sur K.

L'ext. L/K est dite <u>algébrique</u> si tout élt. de L est alg. sur K

Sinon on dira qu'elle est <u>totalement transcendante.</u>

<u>Exemples:</u> (1) e, π - transcendants dans $\mathbb{C}/\mathbb{Q}$

(2) $\sqrt{2}$, $\sqrt[n]{m}$ sont alg. dans $\mathbb{C}/\mathbb{Q}$

(3) $2^{\sqrt{2}}$ est transcendant dans $\mathbb{R}/\mathbb{Q}$

(4) On ne sait pas si $e+\pi$, $e-\pi$ sont transcendants

Thm. 1.8 Soit $\alpha \in L$. Soit $E_\alpha : K[X] \longrightarrow L$, $P(X) \mapsto P(\alpha)$. C'est un K-morphisme d'anneaux. De plus,

(1) L'élt. α est transcendant dans L/K ssi E_α est injectif. Dans ce cas, il induit un isomorphisme de K-algèbres $K[X] \to K[\alpha]$ qui se prolonge en un K-isomorphisme $K(X) \to K(\alpha)$. Dans ce cas, $\dim_K K[\alpha]$ et $\dim_K K(\alpha)$ sont infinies.

(2) L'élt. α est algébrique dans L/K ssi E_α n'est pas injectif. ~~De plus~~ Dans ce cas, il existe un unique polynôme unitaire $P_\alpha(X)$ dans $K[X]$ de degré minimal t.q. $P_\alpha(\alpha) = 0$. Ce pol. est irréductible sur K. De plus, $K[\alpha] = K(\alpha) \cong K[X]/(P_\alpha(X))$ et $[K(\alpha) : K] = \deg P_\alpha$.

Déf. 1.9 Le polynôme $P_\alpha(X) \in K[X]$ du thm précédent est dit le *polynôme minimal de $\alpha \in L$ sur K.*

Preuve du thm. 1.8 (1) α - transc. $\Leftrightarrow$ E_α - injectif par définition.

Alors $E_\alpha(K[X]) \underset{\hookrightarrow K\text{-isomorphisme}}{\cong} \mathrm{Im}(E_\alpha) = K[\alpha]$. Donc E_α induit un K-isomorphisme $K[X] \to K[\alpha]$, et elle se prolonge à $K(X) \xrightarrow{\sim} K(\alpha)$.

$$\frac{P(X)}{Q(X)} \mapsto P(\alpha) \cdot Q(\alpha)^{-1}$$

Remarquons que $Q(\alpha) \neq 0$ pour tout $Q(X) \in K[X] \setminus \{0\}$ par hypothèse.

(2) α - alg. $\underset{\text{par déf.}}{\Longleftrightarrow}$ E_α non injectif $\Leftrightarrow$ $\mathrm{Ker}(E_\alpha) \neq \{0\}$.

Comme $K[X]$ est principal, $\mathrm{Ker}(E_\alpha) \neq \{0\}$ est un idéal principal, donc engendré par un élt. de degré minimal dans $\mathrm{Ker}(E_\alpha)$.

Soit $P_\alpha(X) \in \mathrm{Ker}(E_\alpha)$ le seul élt. de $\mathrm{Ker}(E_\alpha)$ unitaire et de degré minimal. Comme $\mathrm{Ker}(E_\alpha)$ est un idéal premier, on a que $P_\alpha(X)$ est irréductible.

- De plus, $(P_\alpha(X))$ est maximal, d'où $K[X]/(P_\alpha(X))$ est un corps. Remarquons que $\mathrm{Im}(E_\alpha) \overset{\leftarrow \text{Ker}}{\cong} K[X]/(P_\alpha(X))$, et comme $\mathrm{Im}(E_\alpha) = K[\alpha]$, on a que $K[\alpha]$ est un corps et $K[X]/_{(P_\alpha(X))} \xrightarrow{\sim} K[\alpha]$, $X + (P_\alpha(X)) \mapsto \alpha$ est un K-isomorphisme. En particulier, $K(\alpha) = K[\alpha]$.

- Si $m := \deg P_\alpha$, alors $\{1, \alpha, \ldots, \alpha^{m-1}\}$ est une base de $K[\alpha]/K$:

Elle est libre: sinon $\exists\, Q(X) \in K[X]$, $\deg Q(X) \leq m-1 < m$ t.q. $Q(\alpha) = 0$, d'où $Q(X) \in \mathrm{Ker}(E_\alpha)$, absurde.

Elle est génératrice: Soit $x \in K[\alpha]$. Il existe alors $T(X) \in K[X]$ t.q. $x = T(\alpha)$. Division euclidienne: $T(X) = P_\alpha(X) \cdot Q_1(X) + R(X)$ avec $Q_1(X), R(X) \in K[X]$ et $\deg R(X) < m$, d'où $T(\alpha) = R(\alpha)$ $= a_0 + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1}$, avec $a_i \in K$ pour $i = 0, 1, \ldots, m-1$.

On a donc $[K(\alpha) : K] = \dim_K K[\alpha] = \deg P_\alpha$. ▨

<u>Rmq.</u> (1) On a aussi montré que $[K[X]/_{(P_\alpha(X))} : K] = \deg P_\alpha$, et que $K[\alpha] = \{a_0 + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1} \mid a_i \in K\}$, où $\alpha \in L$ est alg. sur K et $m := \deg P_\alpha$.

(2) Si $P(X)$ est un polynôme irréductible dans $K[X]$, alors $(P(X))$ est un idéal maximal, donc $L := K[X]/(P(X))$ est un

corps, et L/K une extension. Soit $\alpha := X + (P(X)) \in L$. Alors le morphisme projection $\begin{array}{l} K[X] \longrightarrow L \\ X \mapsto \alpha \end{array}$ coïncide avec E_α. Dans ce cas, $P_\alpha(X) = \mu \cdot P(X)$, où $\mu \in K^\times$ est telle que P_α soit unitaire. On a alors que $[L:K] = \deg P$.

(3) Pour $\alpha \in L$ algébrique sur K, et $Q(X) \in K[X]$, on a que $Q(\alpha) = 0 \iff Q(X) \in \mathrm{Ker}(E_\alpha) \iff P_\alpha(X) \mid Q(X)$ dans $K[X]$.

Exemples: (1) Dans $\mathbb{C}/\mathbb{R}$ tout pol. minimale d'un élt. de $\mathbb{C}$ est de degré ≤ 2.

(2) Dans $K(X)/K$, l'élt. X est transc. sur K

(3) Dans $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, le polynôme minimal de $a+b\sqrt{2}$, $b \neq 0$ est $(X-a)^2 - 2b^2 \in \mathbb{Q}[X]$.

Proposition 1.10 Toute extension de corps finie est algébrique.

Preuve: Soit L/K une ext. de corps t.q. $n := [L:K] < \infty$. Soit $\alpha \in L$. ~~Alors ...~~ Alors $[K(\alpha):K] < \infty$, d'où α est algébrique dans L/K par le théorème précédent. Donc, L/K — alg.

Exemple:

On verra plus tard que $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha - \text{algébrique dans } \mathbb{C}/\mathbb{Q}\}$ est dénombrable. Remarquons que par définition, $\overline{\mathbb{Q}}/\mathbb{Q}$ est algébrique. De plus, on démontrera que $\overline{\mathbb{Q}}/\mathbb{Q}$ n'est pas finie, et donc elle n'est pas de type finie,

Corollaire 1.11. Soit L/K une ext. de t.f. Si L est engendrée par des élts alg., alors L/K est finie et algébrique.

Preuve: Soit $L = K(S)$ avec $S \subseteq L$ fini et consistant d'élts. alg. sur K. Raisonnons par récurrence sur $\mathrm{Card}(S)$. Si $\mathrm{Card}(S) = 0$, alors c'est clair. Sinon, soit $x \in S$ et prenons $E := K(S \setminus \{x\})$. Alors, par l'hypothèse de récurrence, E/K est alg. et finie. De plus, $L = E(x)$, et comme x est alg. sur K, il l'est aussi sur E, d'où L/E — algébrique et finie. On a que L/K est ~~algébrique~~ $\underbrace{\text{finie}}_{\text{par le Thm. 1.5}}$, $\underbrace{\text{donc alg.}}_{\text{par la prop. 1.10}}$ ∎

Corollaire 1.12 La somme et le produit de deux élts. alg. dans L/K sont algébriques. L'ensemble d'élts alg. de L/K est une sous-extension, noté $\overline{K}^L$, et appelée clôture alg. de K dans L. De plus, $\overline{K}^L/K$ est algébrique.

Preuve: Soient $x, y \in L$ alg. sur K. Alors $K(x,y)/K$ est une ext. alg. par le Cor. 1.11, donc $x-y$, xy^{-1} (si $y \neq 0$) sont dans $K(x,y)$, et donc alg. aussi. Le reste de l'énoncé est immédiat. ∎

Exemples: 1) L'extension $\mathbb{R}/\mathbb{Q}$ — non alg., ni de t.f.

2) $K(X)/K$ de t.f. mais pas alg.

3) $\mathbb{Q}(\sqrt[3]{2}, i)/\mathbb{Q}$ est alg. et finie

4) $\overline{\mathbb{Q}}$ = clôt. alg. de $\mathbb{Q}$ dans $\mathbb{C}$, est un corps

$\overline{\mathbb{Q}}/\mathbb{Q}$ n'est pas de t.f. ou finie

($\forall n \in \mathbb{N}$, $\exists P(X) \in \mathbb{Q}[X]$ — irréductible et $\deg P \geq n$)

Déf. 1.13 Si $\overline{K}^L = K$, on dit que K est algébriquement clos dans L.

Remarquons qu'alors l'extension L/K est totalement transcendante.

Corollaire 1.14 Une ext. de corps engendrée par des élts algébriques est algébrique.

Preuve: Soit L/K une ext. de corps et $S \subseteq L$ consistant d'élts. alg. t.q. $L = K(S)$. Alors $S \subseteq \overline{K}^L$, donc $L = \overline{K}^L$, et on a que L/K alg. ■

Proposition 1.15 Soit $M/L/K$ une tour de corps. Alors

M/K est algébrique $\Longleftrightarrow$ M/L et L/K le sont.

Preuve: ($\Rightarrow$) Clair.

($\Leftarrow$) Soit $\alpha \in M$. Comme α est algébrique sur L, $\exists\ P(X) = \sum_{i=0}^{m} a_i X^i \in L[X]$ t.q. $P(\alpha) = 0$. Alors α est algébrique dans $M/K(a_0, \dots, a_m)$, d'où $[K(a_0, \dots, a_m)(\alpha) : K] < \infty$ car $K(a_0, \dots, a_m)/K$ est algébrique par le corollaire précédent, et étant de type fini, on a $[K(a_0, \dots, a_m) : K] < \infty$. De plus, $[K(a_0, \dots, a_m)(\alpha) : K(a_0, \dots, a_m)] < \infty$ pour les mêmes raisons, et on conclut par le th. 1. Comme $K(a_0, a_1, \dots, a_m, \alpha)/K$ est finie, elle est algébrique, voir la prop. 1.10 d'où α est algébrique dans M/K, et donc M/K est algébrique. ■

Le degré de transcendance

Soit L/K une ext. de corps.

Déf 2.1 Une famille $(\alpha_i)_{i \in I}$ d'éléments de L est dite algébriquement indépendante sur K si le morphisme de K-algèbres

$$K[X_i \mid i \in I] \longrightarrow L \quad \text{est injectif.}$$
$$X_i \longmapsto \alpha_i$$

L'extension L/K est dite <u>transcendante pure</u> si L/K est engendrée par une famille ~~base~~ algébriquement indépendante.
- Cela arrive ssi L est K-isomorphe à $K(X_i \mid i \in I)$.

<u>Remarque</u>: (1) La famille d'élts $(\alpha_i)_{i\in I}$ de L/K est alg. indép. si et seulement si pour tout ~~...~~ $\{i_1, \dots, i_n\} \subseteq I$ fini, et pour tout $P(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$, on a $P(\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_n}) \neq 0$.

(2) Remarquons que si $(\alpha_i)_{i\in I}$ est alg. indép. dans L/K, le K-morphisme
$$K[X_i \mid i \in I] \longrightarrow L \quad \text{est injectif, et se}$$
$$X_i \longmapsto \alpha_i$$
prolonge donc à un K-morphisme de corps
$$K(X_i \mid i \in I) \xrightarrow{\varphi} L \quad \text{avec image } K(\alpha_i \mid i \in I)$$
$$\frac{P(X_{i_1}, \dots, X_{i_n})}{Q(X_{j_1}, \dots, X_{j_m})} \longmapsto \frac{P(\alpha_{i_1}, \dots, \alpha_{i_n})}{Q(\alpha_{j_1}, \dots, \alpha_{j_m})}$$

<u>Lemme 2.2</u> Soit L/K une ext. de corps et $S \subseteq L$ un ensemble alg. indépendant dans L/K. Soit $x \in L \setminus S$. Alors $S \cup \{x\}$ est alg. indép. dans L/K ssi x est transcendant dans $L/K(S)$.

<u>Preuve</u>: ($\Rightarrow$) Supposons que x est algébrique dans $L/K(S)$. Soit $P(X) \in K(S)[X] \setminus \{0\}$ tel que $P(x) = 0$. Soit
$$P(X) = \sum_{i=0}^{n} a_i X^i \quad \text{avec } a_i \in K(S).$$