Conjecture de Schanuel et Algèbre différentielle

Killian Le Milbeau , Thibault Brasseur

ENS Rennes

14/04/2023

Table des matières

Définitions - Extensions de corps

Définition

Soit $\mathbb{K}$ un corps. On dit que que $\mathbb{L}/\mathbb{K}$ est une **extension du corps** $\mathbb{K}$ si $\mathbb{L}$ est un corps et que $\mathbb{K} \subset \mathbb{L}$.
Une extension de corps $\mathbb{L}/\mathbb{K}$ est dites **algébrique** si tous les éléments de $\mathbb{L}$ sont algébriques dans $\mathbb{K}$.

Par exemple, $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ sont des extensions de corps.

Définition

Le **degré d'une extension de corps** $\mathbb{L}/\mathbb{K}$ est la dimension de $\mathbb{L}$ en tant que $\mathbb{K}$-espavce vectoriel. On la note $[\mathbb{L} : \mathbb{K}]$.

Par exemple, comme $\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$, le degré de l'extension $\mathbb{C}/\mathbb{R}$ est $[\mathbb{C} : \mathbb{R}] = 2$. En particulier, $\mathbb{C}/\mathbb{R}$ est une extension algébrique.

Définition

La **fermeture algébrique** de $\mathbb{K}$ dans $\mathbb{L}$ est l'ensemble des élements de $\mathbb{L}$ algébrique dans $\mathbb{K}$.

Base et dégré de transcendance

Définition

On dit que $x_1, \cdots, x_n \in \mathbb{L}$ sont **algébriquement indépendant** sur $\mathbb{K}$ si pour tout polynôme $P \in \mathbb{K}[t_1, \cdots, t_n]$, on a $P(x_1, \cdots, x_n) \neq 0$.

Définition

On dit que $x_1, \cdots, x_n \in \mathbb{L}$ est une **base de transcendance** si les éléments sont algébriquements indépendant et $\mathbb{K}(x_1, \cdots, x_n) = \mathbb{L}$. On note $\dim_{\mathbb{K}} \mathbb{L} = n$ sont **degré de transcendance**.

Le degré est indépendant de la base choisie. Prenons un exemple : $\dim_{\mathbb{Q}} \mathbb{Q}(\pi, \pi\sqrt{2}) = 1$.

Définitions - Module sur un anneau

Définition

Soit A un anneau (unitaire). Un A-**module** $(M, +, .)$ est la donnée d'un ensemble M, d'une loi de composition interne $+$ sur M faisant de $(M, +)$ un groupe abélien et d'une loi de composition externe . telle que :

(i) $\forall a \in A,\ \forall (x, y) \in M,\ a.(x + y) = a.x + a.y,$

(ii) $\forall (a, b) \in A,\ \forall x \in M,\ (a + b).x = a.x + b.y,$

(iii) $\forall x \in M,\ 1.x = x.$

Un module est à un anneau ce qu'un espace vectoriel est à un corps. Par exemple, $\mathbb{Z}[i]$ est un $\mathbb{Z}$-module. Plus généralement, tout groupe abélien est un Z-module.

Définitions - Algèbre différentielle (1)

Définition

∂ est une **dérivée** de $\mathbb{L}$ dans un $\mathbb{L}$-espace vectoriel Ω si :

$$\forall x, y \in \mathbb{L},\ \partial(x+y) = \partial(x) + \partial(y) \text{ et } \partial(xy) = x\partial(y) + y\partial(x)$$

Si $\mathbb{K} \subset \mathbb{L}$, on dit que c'est une $\mathbb{K}$-**dérivée** si pour $\lambda \in \mathbb{K}$, $\partial(\lambda x) = \lambda \partial(x)$.

On note $\mathrm{Der}(A, B)$ l'ensemble des dérivations de A dans B et $\mathrm{Der}_{\mathbb{K}}(A, B)$ l'ensemble des $\mathbb{K}$-dérivations de A dans B.

Définition

Soit $s, t \in \mathbb{L}$ avec s non nul. On dit que,

(i) t est un **logarithme** si $dt = ds/s$.

(ii) s est une **exponentielle** si $ds = s \cdot dt$.

Si $\mathcal{L} = \{x \in \mathbb{L}, dx/x\}$ est un $\mathbb{Z}$-module.

Définitions - Algébre différentielle (2)

Définition

Soit A est une $\mathbb{K}$-algèbre, B un A-module. Il existe un A-module $\Omega_{A/\mathbb{K}}$ et une dérivée $\partial \in \mathrm{Der}_{\mathbb{K}}(A, \Omega_{A/\mathbb{K}})$ tel que pour tout $d \in \mathrm{Der}_{\mathbb{K}}(A, B)$, il existe une unique application A-linéaire de f tel que $f \circ \partial = d$.

La plus part du temps $B = A$.

Définition

Si $d \in \mathrm{Der}_{\mathbb{K}} A$, alors on considère l'unique application $\mathbb{K}$-linéaire dans $(\Omega_{\mathbb{L}/\mathbb{K}}, \partial)$ tel que pour tout $x, y \in \mathbb{L}$:

$$d(x\partial y) = dx\partial y + x\partial(dy)$$

appelée la **dérivée étendue**.

Ceci n'est pas une dérivée !

Conjecture de Schanuel et transcendance

Tous les corps sont considérés de caractéristique 0.

Conjecture (de Schanuel, (S))

Soient $y_1, \ldots, y_n \in \mathbb{C}$, $\mathbb{Q}$-linéairement indépendants sur . Alors,

$$\dim_{\mathbb{Q}} \mathbb{Q}(y_1, \ldots, y_n, e^{y_1}, \ldots, e^{y_n}) \geq n$$

Variantes formelles de la conjecture

(S) Soit $y_1, \ldots, y_n \in \mathbb{C}$ linéairement indépendants sur $\mathbb{Q}$. Alors,

$$\dim_{\mathbb{Q}} \mathbb{Q}(y_1, \ldots, y_n, e^{y_1}, \ldots, e^{y_n}) \geq n$$

(SF) Soit $y_1, \ldots, y_n \in \mathbb{C}[[X]]$ sans termes constants et linéairement indépendantes sur $\mathbb{Q}$. Alors,

$$\dim_{\mathbb{C}(t)} \mathbb{C}(t)(y_1, \ldots, y_n, e^{y_1}, \ldots, e^{y_n}) \geq n$$

(Σ)(Ax) Soit $y_1, \ldots, y_n \in \mathbb{C}[[t_1, \ldots, t_m]]$. Si les y_i sont linéairements indépendants sur $\mathbb{Q}$, alors

$$\dim_{\mathbb{Q}} \mathbb{Q}(y_1, \ldots, y_n, e^{y_1}, \ldots, e^{y_n}) \geq n + \operatorname{rg}\left(\frac{\partial y_i}{\partial t_j}\right)_{1\leq i\leq n, 1\leq j\leq m}$$

Théorèmes de Ax - Théorème I

Théorème (I)

Soit $\mathbb{K} \supseteq C \supseteq \mathbb{Q}$ une suite d'extension de corps et Δ un ensemble de dérivée sur $\mathbb{K}$ vérifiant $\bigcap_{D\in\Delta} \mathrm{Ker}(D) = C$.

*Soient $y_1, ..., y_n, z_1, ..., z_n \in \mathbb{K}^*$. si les propriétés **(a)** et **(b)** ou **(a)** et **(b')** sont vérifiées avec:*

(a) $\forall D \in \Delta, \forall i \in \{1, ..., n\}, D(y_i) = D(z_i)/z_i$

(b) *Aucun produit non trivial de puissance de $(z_i)_{1\leq i\leq n}$ n'est dans C*

(b') *Les $(y_i)_{1\leq i\leq n}$ sont $\mathbb{Q}$ linéairement indépendant modulo C.*

Alors,

$$\dim_C C(y_1, ..., y_n, z_1, ..., z_n) \geq n + \mathrm{rg}(D(y_i))_{1\leq i\leq n, D\in\Delta}$$

Théorèmes de Ax - Théorème II et III

Théorème (II)

La conjecture ***(Σ)(Ax)*** *est vraie si les* (y_i) *sont sans termes constants. C'est-à-dire, si les* $(y_i - y_i(0))$ *sont linéairement indépendants sur* $\mathbb{Q}$.

Théorème (III)

(S) $\Longleftrightarrow$ ***(Σ)(Ax)***.

Ce dernier théorème est le centre de cette lecture.

Plan de la démonstration

Lemme I $+$ Lemme II $+$ Lemme III $\Rightarrow$ Théorème I.
Théorème I $\Rightarrow$ Théorème II et Théorème III.

Lemme I - énoncé

Lemme (I)

$C \subset \mathbb{K} \subset \mathbb{L}$ une suite d'extension de corps, $(\Omega_{\mathbb{L}/C}, \partial)$ le $\mathbb{L}$-espace vectoriel défini en amont. On note $F = \mathrm{Vect}_{\mathbb{L}} \partial \mathbb{K}$. Alors on a:

$$\dim_C \mathbb{K} \textit{ (degré de transcendance) } = \dim_{\mathbb{L}} F \textit{ (dimension)}$$

Lemme I - Preuve

Demonstration :

Si $x_1, \cdots, x_n \in \mathbb{L}$ algébriquement dépendant sur C. Alors il existe $P \in C[t_1, \cdots, t_n]$ tel que $P(x_1, \cdots, x_n) = 0$. Alors

$$\sum_{i=1}^{n} \frac{\partial P}{\partial t_i}(x_1, \cdots, x_n)\partial x_i = 0$$

Avec $\frac{\partial P}{\partial t_i}(x_1, \cdots, x_n) \neq 0$.

Si $x_1, \cdots, x_m$ base de trascendance. On pose $D_i \in \mathrm{Der}_{\mathbb{K}}\mathbb{L}$ tel que $D_i(x_j) = \delta_{ij}$. Alors, avec $\sum_{j=1}^{m} \lambda_j \partial x_j = 0$, on a

$$\sum_{j=1}^{m} \lambda_j f_i(\partial x_j) = \sum_{i=1}^{m} \lambda_i D_i(x_j) = \lambda_i = 0$$

Lemme II

Lemme (II)

Soient $C \subset \mathbb{K} \subset \mathbb{L}$ une suite d'extension de corps et $\Delta \subset \mathrm{Der}(\mathbb{L})$ avec $\bigcap_{D\in\Delta} \mathrm{Ker} D = C$ et pour $D \in \Delta$ on a $D(\mathbb{K}) \subseteq \mathbb{K}$.
On note $\overline{\Delta}$ l'ensemble des dérivées prolongées sur $\Omega_{\mathbb{L}/\mathbb{K}}$ et $\overline{C} = \bigcap_{\overline{D}\in\overline{\Delta}} \mathrm{Ker}\overline{D} \subseteq \Omega_{\mathbb{L}/\mathbb{K}}$. On constate que $\overline{C}$ est un C-espace vectoriel. Posons l'application bilinéaire

$$\begin{array}{cccc} b & : & \mathbb{L} \times \overline{C} & \to & \Omega_{\mathbb{L}/\mathbb{K}} \\ & & (x,\omega) & \mapsto & b(x,\omega) = x\omega \end{array}$$

Alors on peut associé b à l'application $\beta : \mathbb{L} \otimes_C \overline{C} \to \Omega_{\mathbb{L}/\mathbb{K}}$ par propriété universelle du tenseur.
Le lemme affirme que alors β est injective.

Dans le cadre de cette présentation, on admettra ce résultat.
Pour le démontrer, raisonner par l'absurde.

Lemme III - énoncé

Lemme (III)

Soient $\mathbb{Q} \subset \mathbb{K} \subset \mathbb{L}$ une suite d'extension de corps
On considère $\partial \in \mathrm{Der}_{\mathbb{K}}(\mathbb{L}, \Omega_{\mathbb{L}/\mathbb{K}})$, $\partial\mathbb{L}/\mathbb{L}$ le $\mathbb{Z}$-module $\{\partial x/x, x \in \mathbb{L}^{\times}\}$, l'application bilinaire produit de $\mathbb{K} \times \partial\mathbb{L}/\mathbb{L}$ dans $\Omega_{\mathbb{L}/\mathbb{K}}$ et $\partial\mathbb{L}$ le $\mathbb{K}$-sous-espace vectoriel de $\Omega_{\mathbb{L}/\mathbb{K}}$. On pose alors l'application

$$\gamma \ : \ \mathbb{K} \otimes_{\mathbb{Z}} \partial\mathbb{L}/\mathbb{L} \ \to \ \Omega_{\mathbb{L}/\mathbb{K}}/_{\partial\mathbb{L}}$$

Le lemme affirme que γ est injective.

Lemme III - Preuve (I)

Proposition

$\mathbb{K} \subsetneq \mathbb{L}$ avec $\mathbb{K}$ algébriquement fermé dans $\mathbb{L}$ et $W = \{C \subset \mathbb{L}$ sous-corps algébriquement fermé dans $\mathbb{L}$ $|\mathbb{K} \subset C, \dim_C(\mathbb{L}) = 1\}$. Alors :

$$\bigcap_{C \in W} C = \mathbb{K}$$

__Demonstration :__

On suppose $\mathbb{K}$ algébriquement fermé et $x_1, \cdots, x_n \in \mathbb{K}$ $\mathbb{Q}$-linéairement indépendant. On vérifie selon le degré de transcendance m. Si $m = 0$, c'est trivial. Si $m = 1$, on identifie $\mathbb{L} \simeq \mathbb{K}(t)$ et on pose ν_p et μ_p respectivement l'ordre en $p \in \mathbb{K}$ d'un polynôme et son résidu en p pour se servir de l'hypothèse sur les $x_1, \cdots, x_n$ et conclure. Dans le cas général, on utilise la proposition pour se ramener au cas précédent.

Théorème I - Rappel

Théorème (I)

Soit $\mathbb{L} \supseteq C \supseteq \mathbb{Q}$ une suite d'extension de corps et Δ un ensemble de dérivée sur $\mathbb{L}$ vérifiant $\bigcap_{D \in \Delta} \mathrm{Ker}(D) = C$.

*Soient $y_1, ..., y_n, z_1, ..., z_n \in \mathbb{L}^*$. si les propriétés **(a)** et **(b)** ou **(a)** et **(b')** sont vérifiées avec:*

(a) $\forall D \in \Delta, \forall i \in \{1, ..., n\}, D(y_i) = D(z_i)/z_i$

(b) *Aucun produit non trivial de puissance de $(z_i)_{1 \leq i \leq n}$ n'est dans C*

(b') *Les $(y_i)_{1 \leq i \leq n}$ sont $\mathbb{Q}$ linéairement indépendant modulo C.*

Alors,

$$\dim_C C(y_1, ..., y_n, z_1, ..., z_n) \geq n + \mathrm{rg}(D(y_i))_{1 \leq i \leq n, D \in \Delta}$$

On rappele l'énoncée.

Théorème I - Preuve

Killian Le Milbeau , Thibault Brasseur

Proposition

Si $\omega = \partial y - \partial z/z \in \Omega_{\mathbb{L}/C}$, *alors* $\overline{d}\omega = \partial(dy - dz/z)$.

<u>Demonstration :</u>

On a $\overline{d}(\partial z/z) = -(dz/z^2)\partial z + (1/z)\partial(dz)$.

Et $\partial(dz/z) = -(\partial z/z^2)dz + (1/z)\partial(dz)$.

Proposition

Avec $r = \mathrm{rg}(Dy_i)_{1\leq i\leq n, D\in\Delta}$, *on peut ramener* Δ *à* $\{D_1, \cdots, D_r\} \cup \tilde{\Delta}$, *tel que pour* $y_1, \ldots, y_r$, *on ait* $D_i(y_j) = \delta_{ij}$ *et pour* $D \in \tilde{D}$, $D(y_i) = 0$.

Théorème I - Preuve

Demonstration :

On suppose $m = \dim_C \overbrace{C(y_1, \cdots, y_n, z_1, \cdots, z_n)}^{\mathbb{K}} < n + r$, alors par **lemme 1** $dim_{\mathbb{L}} \partial\mathbb{K} < n + r$.
On pose $\omega_i = \partial y_i - \partial z_i / z_i$ avec $i = 1, \cdots, n$. Alors $\omega_1, \cdots, \omega_n, \partial y_1, \cdots, \partial y_r$ lié et pour (α_k) et (λ_l) non tous nuls :

$$\sum_{k=1}^{n} \alpha_k \omega_k + \sum_{l=1}^{r} \lambda_l y_l = 0$$

On a $\overline{D}\omega_k = \overline{D}y_l = 0$; par le **lemme 2**, on peut prendre α_k et λ_l dans C
si $\alpha_k \neq 0$, alors on quotiente dans $\partial\mathbb{L}$ et on a

$$\sum_{k=1}^{n} \alpha_k \partial z_k / z_k = \overline{0}$$

Donc $\partial z_k / z_k$ liée dans $\mathbb{Z}$ par **lemme 3** ce qui contredit l'hypothèse **(b)**.

Théorème I - Preuve

Il reste

$$\sum_{l=1}^{r} \lambda_l y_l = 0$$

Si on pose f_i l'application linéaire associée à D_i, on obtient $\lambda_i = 0$ ce qui conclut tous les coefficients nuls, ce qui est absurde.

Supposons **(a)** et **(b')**. Par l'absurde, supposons **(b)** faux. Alors $z = \prod_{k=1}^{n} {z_k}^{N_k} \in C$. Ainsi pour $D \in \Delta$:

$$0 = Dz/z = \sum_{k=1}^{n} N_k Dz_k/z_k = D\Big(\sum_{k=1}^{n} N_k y_k\Big)$$

Ce qui contredit **(b')**.

Théorème II - Preuve

Demonstration :

Ici, $C = \mathbb{C}$, $\mathbb{L} = \mathrm{Frac}(\mathbb{C}[[t_1, \cdots, t_m]])$, $\Delta = (\frac{\partial}{\partial t_i})_{1 \leq i \leq n}$ et $z_i = \exp y_i$. Par hypothèse les $(y_i - y_i(0))$ sont $\mathbb{Q}$-linéairement indépendant donc (y_i) le sont modulo $\mathbb{C}$. On a **(a)** et **(b')** donc on applique le **Théorème I**.

$$\begin{aligned} \dim_{\mathbb{Q}} \mathbb{Q}(y_1, \dots, y_n, e^{y_1}, \dots, e^{y_n}) &\geq \dim_{\mathbb{C}} \mathbb{C}(y_1, \dots, y_n, e^{y_1}, \dots, e^{y_n}) \\ &\geq n + \mathrm{rg}\left(\frac{\partial y_i}{\partial t_j}\right)_{1 \leq i \leq n, 1 \leq j \leq m} \end{aligned}$$

Théorème III - Preuve

Demonstration :

On suppose **(S)** vrai. On pose alors $y_1 - y_1(0), \cdots, y_p - y_p(0)$ base de $\mathrm{Vect}_{\mathbb{Q}}(y_1 - y_1(0), \cdots, y_n - y_n(0))$.

On note $y_j - y_j(0) = \sum_{k=1}^{p} a_{j,k}(y_i - y_i(0))$.

On effectue un changement entre $i = p+1, \cdots, n$ avec $y_i := y_i - \sum_{k=1}^{p} a_{j,k} y_i$, de sorte à ce que $y_i \in \mathbb{C}$.

On a $y_1, \cdots, y_p$ $\mathbb{Q}$-linéairement indépendant modulo $\mathbb{C}$.

Par **Théorème II**

$$\dim_{\mathbb{Q}} \mathbb{Q}(y_1, ..., y_n, e^{y_1}, ..., e^{y_n}) \geq n + \mathrm{rg}\left(\frac{\partial y_i}{\partial t_j}\right)_{1 \leq i \leq n, 1 \leq j \leq m}$$

On a $y_{p+1}, \cdots y_n$ $\mathbb{Q}$-linéairement indépendant.

Et par hypothèse, $\dim_{\mathbb{Q}} \mathbb{Q}(y_{p+1}, ..., y_n, e^{y_{p+1}}, ..., e^{y_n}) \geq n - p$

ce qui conclut.

FIN