# Correspondance de Jacobson

## Sommaire



On présente la correspondance de Jacobson entre sous-extensions d'une extension purement inséparable $K \hookrightarrow L$ de hauteur $\leq 1$ et sous-algèbres de Lie restreintes de l'algèbre de Lie $\mathrm{Der}_K(L)$ des $K$-dérivations de $L$. Ce résultat est apparu en premier dans l'article [2]. La preuve présentée ici est tirée de [1].

## 1 Extensions purement inséparables

**Définition 1.1.** Soient $K$ un corps de caractéristique $p > 0$ et $L$ une extension de $K$.

(i) Un élément $x \in L$ est radiciel (sur $K$) s'il existe $f \geq 0$ tel que $x^{p^f} \in K$. Le plus petit tel entier $f$ est appelé la hauteur de $x$ (sur $K$).

(ii) L'extension $L$ est dite purement inséparable (ou radicielle) si tous ses éléments sont radiciels. La hauteur de $L$ est la borne supérieure (dans $\mathbb{N} \cup \{+\infty\}$) des hauteurs des éléments de $L$.

Dit autrement, la hauteur d'une extension purement inséparable $K \hookrightarrow L$ est finie s'il existe un entier $f \geq 0$ tel que $x^{p^f} \in K$ pour tout $x \in L$, auquel cas la hauteur de $L$ est le plus petit tel entier. Sinon, la hauteur de $L$ est infinie. Dire que l'extension $K \hookrightarrow L$ est purement inséparable de hauteur $\leq f$ revient donc à dire que $x^{p^f} \in K$ pour tout $x \in L$. En particulier, $L$ est purement inséparable de hauteur $\leq 1$ si et seulement si $x^p \in K$ pour tout $x \in L$.
Un élément radiciel de hauteur $f$ est algébrique, car annulé par le polynôme $X^{p^f} - x^{p^f} \in K[X]$. En particulier, une extension purement inséparable est algébrique.

Si $K$ est un corps de caractéristique $p > 0$, on note $K^{[p]}$ l'ensemble des éléments de $K$ de la forme $x^p$ avec $x \in K$. Autrement dit, $K^{[p]}$ est l'image du morphisme de Frobenius $K \to K$.

**Lemme 1.2.** *Soient $a \in K \backslash K^{[p]}$ et $n \geq 0$. Alors le polynôme $P = X^{p^n} - a \in K[X]$ est irréductible dans $K[X]$.*

*Preuve.* Soient $\Omega$ une clôture algébrique de $K$, $b \in \Omega$ tel que $b^{p^n} = a$, $Q$ le polynôme minimal de $b$ sur $K$, $s$ son degré. Dans $\Omega[X]$, $P$ se factorise sous la forme $P = (X - b)^{p^n}$. Si $R$ est un facteur irréductible unitaire de $P$ dans $K[X]$, il est non constant et divise $P = (X - b)^{p^n}$ dans $\Omega[X]$, donc est de la forme $(X - b)^d$ avec $d \geq 1$. En particulier, $R$ annule $b$, donc est un multiple de $Q$, puis est égal à $Q$ par irréductibilité. Ainsi, $Q$ est le seul facteur irréductible unitaire de $P$ dans $K[X]$, donc la décomposition de $P$ en produit d'irréductibles dans $K[X]$ est de la forme $P = Q^r$. En identifiant les degrés, on obtient $p^n = rs$, donc $r$ divise $p^n$ et est donc de la forme $p^m$, $m \leq n$. Supposons que $m > 0$, alors, en notant $c$ le terme constant de $Q$ et en identifiant les termes constants de $P = Q^r$, on obtient $-a = c^r$, puis $a = (-c)^r = (-c)^{p^m}$ [(1)]. Cela contredit l'hypothèse selon laquelle $a \notin K^{[p]}$, donc nécessairement $m = 0$, $P = Q$, et $P$ est irréductible. □

**Proposition 1.3.** *Soient $L$ une extension de $K$, $x \in L$ un élément radiciel de hauteur $f$, $a = x^{p^f} \in K$. Alors le polynôme minimal de $x$ est $X^{p^f} - a$. Réciproquement, si $x$ est algébrique de polynôme minimal $X^{p^f} - a$ ($f \geq 0$, $a \in K$) alors $x$ est radiciel de hauteur $f$, et $x^{p^f} = a$.*

[(1)] On a $(-1)^{p^m} = -1$ : c'est clair si $p$ est impair, et c'est encore vrai si $p = 2$ car alors $-1 = 1$ dans $K$.

*Preuve.* Si $f = 0$, le résultat est immédiat, donc on suppose que $f \geq 1$. Le polynôme $X^{p^f} - a \in K[X]$ annule $x$, et pour montrer que c'est le polynôme minimal de $x$, il suffit de montrer qu'il est irréductible. En vertu du lemme 1.2, il suffit de montrer que $a \notin K^{[p]}$. S'il existait $b \in K$ tel que $a = b^p$, on aurait $(x^{p^{f-1}} - b)^p = x^{p^f} - b^p = x^{p^f} - a = 0$, donc $x^{p^{f-1}} = b \in K$, mais c'est impossible car $x$ est de hauteur $f$.
Réciproquement, si le polynôme minimal de $x \in L$ est $X^{p^f} - a$ ($a \in K$) alors $x^{p^f} = a$, donc $x$ est radiciel de hauteur $\leq f$. S'il existait $0 \leq g < f$ tel que $x^{p^g} \in K$, alors le polynôme $X^{p^g} - x^{p^g} \in K[X]$ annulerait $x$, mais c'est impossible car il est non nul, de degré $p^g < p^f$ et, par hypothèse, le polynôme minimal de $x$ sur $K$ est $X^{p^f} - a$. Donc $x$ est de hauteur $f$. □

**Proposition 1.4.** *Soient $K$ un corps de caractéristique $p > 0$ et $K \hookrightarrow L \hookrightarrow M$ des extensions. Alors $M$ est purement inséparable sur $K$ si et seulement si $M$ est purement inséparable sur $L$ et $L$ est purement inséparable sur $K$. Si c'est le cas, la hauteur de $M$ sur $K$ est inférieure ou égale à la somme de la hauteur de $M$ sur $L$ et de la hauteur de $L$ sur $K$.*

*Preuve.* Supposons que $M$ est purement inséparable sur $L$ et $L$ est purement inséparable sur $K$. Soit $x \in M$, il existe $f \geq 0$, inférieur ou égal à la hauteur de $M$ sur $L$, tel que $x^{p^f} \in L$. Il existe donc $g \geq 0$, inférieur ou égal à la hauteur de $L$ sur $K$, tel que $x^{p^{f+g}} = (x^{p^f})^{p^g} \in K$. Cela montre que $x$ est radiciel sur $K$, de hauteur inférieure ou égale à la somme des hauteurs de $M$ sur $L$ et de $L$ sur $K$.
Réciproquement, supposons $M$ purement inséparable sur $K$. Si $x \in M$, il existe $f \geq 0$ tel que $x^{p^f} \in K \subset L$, donc $M$ est purement inséparable sur $L$. De même, si $x \in L \subset M$, il existe $f \geq 0$ tel que $x^{p^f} \in K$, donc $L$ est purement inséparable sur $K$. □

**Corollaire 1.5.** *Si $K \hookrightarrow L$ est une extension purement inséparable de hauteur $\leq 1$, alors pour toute sous-extension $E$ de $L$, $L$ est une extension purement inséparable de hauteur $\leq 1$ de $E$ et $E$ est une extension purement inséparable de hauteur $\leq 1$ de $K$.*

Dans la suite de cette section, $K \hookrightarrow L$ est une extension purement inséparable de hauteur $\leq 1$.

Si $I$ est un ensemble, on note $\Lambda_I^{(p)}$ l'ensemble des multi-indices $\boldsymbol{\alpha} = (\alpha_i)_{i \in I} \in \mathbb{N}^{(I)}$ de support fini et tels que $\alpha_i < p$ pour tout $i$. Si $(x_i)_{i \in I}$ est une famille d'éléments de $L$ et $\boldsymbol{\alpha} \in \Lambda_I^{(p)}$, on note $x^{\boldsymbol{\alpha}} := \prod_{i \in I} x_i^{\alpha_i}$. Notons que si $I$ est vide, il existe un unique élément "vide" $\boldsymbol{\alpha}_0$ dans $\mathbb{N}^{(I)}$, qui par convention appartient à $\Lambda_I^{(p)}$ ; dans ce cas, si $x$ est la famille vide d'éléments de $L$ alors $x^{\boldsymbol{\alpha}_0}$ est le produit vide, donc est égal à 1.

**Définition 1.6.** Une famille $(x_i)_{i \in I}$ d'éléments de $L$ est dite $p$-libre (sur $K$) si la famille $(x^{\boldsymbol{\alpha}})_{\boldsymbol{\alpha} \in \Lambda_I^{(p)}}$ est libre sur $K$ ; on dit que $(x_i)_{i \in I}$ est une $p$-base de $L$ (sur $K$) si la famille $(x^{\boldsymbol{\alpha}})_{\boldsymbol{\alpha} \in \Lambda_I^{(p)}}$ est une base de $L$ sur $K$.

De même, on dit qu'un sous-ensemble $S \subset L$ est $p$-libre (resp. est une $p$-base) sur $K$ si la famille identité $(x)_{x \in S}$ est $p$-libre (resp. est une $p$-base) sur $K$. Une famille $(x_i)_{i \in I}$ d'éléments de $L$ est $p$-libre (resp. est une $p$-base) sur $K$ si et seulement si elle est injective et l'ensemble $\{x_i \mid i \in I\}$ est $p$-libre (resp. est une $p$-base) sur $K$.
On dira également qu'une famille d'éléments de $L$ (ou un sous-ensemble de $L$) est $p$-liée si elle n'est pas $p$-libre.

**Remarque 1.7.**

(i) La famille vide est toujours $p$-libre. Une famille à un élément $(x)$ est $p$-libre si et seulement si $x$ est de degré $p$ sur $K$, et d'après la proposition 1.3, c'est le cas si et seulement si $x$ est de hauteur 1, autrement dit si et seulement si $x \in L \backslash K$.

(ii) Si $M \subset L$ est une sous-extension et $(x_i)_{i \in I}$ est une famille de $L$ $p$-libre sur $M$, alors elle est $p$-libre sur $K$. En effet, la famille $(x^{\boldsymbol{\alpha}})_{\boldsymbol{\alpha} \in \Lambda_I^{(p)}}$ est alors libre sur $M$, donc sur $K$.

(iii) Si $(x_i)_{i \in I}$ est $p$-libre, alors pour tout sous-ensemble $J \subset I$, la famille $(x_i)_{i \in J}$ est $p$-libre, car la famille $(x^{\boldsymbol{\alpha}})_{\boldsymbol{\alpha} \in \Lambda_J^{(p)}}$ est une sous-famille de $(x^{\boldsymbol{\alpha}})_{\boldsymbol{\alpha} \in \Lambda_I^{(p)}}$. Réciproquement, si pour tout sous-ensemble fini $J \subset I$, la famille $(x_i)_{i \in J}$ est $p$-libre, alors $(x_i)_{i \in I}$ est $p$-libre. En effet, toute sous-famille finie de $(x^{\boldsymbol{\alpha}})_{\boldsymbol{\alpha} \in \Lambda_I^{(p)}}$ est contenue dans une famille $(x^{\boldsymbol{\alpha}})_{\boldsymbol{\alpha} \in \Lambda_J^{(p)}}$ pour un certain sous-ensemble fini $J \subset I$, donc est libre, ce qui implique que la famille $(x^{\boldsymbol{\alpha}})_{\boldsymbol{\alpha} \in \Lambda_I^{(p)}}$ est libre.

Si $(x_i)_{i \in I}$ est n'importe quelle famille d'éléments de $L$, le morphisme d'évaluation $\varphi : K[(X_i)_{i \in I}] \to L$ qui envoie $X_i$ sur $x_i$ a pour image la sous-algèbre $K[(x_i)_{i \in I}]$ engendrée par les $x_i$, et puisque les $x_i$ sont algébriques, celle-ci coïncide avec la sous-extension $K((x_i)_{i \in I})$ engendrée par les $x_i$. Par ailleurs, puisque les $x_i$ sont radiciels de hauteur $\leq 1$ sur $K$, on a $a_i = x_i^p \in K$ pour tout $i$. Ainsi, l'idéal $\mathcal{J}$ engendré par les polynômes $X_i^p - a_i \in K[(X_i)_{i \in I}]$ est contenu dans le noyau de $\varphi$, et $\varphi$ induit un morphisme $\overline{\varphi} : {K[(X_i)_{i \in I}]}/{\mathcal{J}} \to L$ d'image $K((x_i)_{i \in I})$.

**Proposition 1.8.** *Avec les notations ci-dessus, on a :*

*(i) La famille $(x_i)_{i\in I}$ est p-libre si et seulement si le morphisme $\overline{\varphi}$ est injectif (autrement dit, si et seulement si le noyau du morphisme $\varphi$ est égal à $\mathcal{J}$).*

*(ii) La famille $(x_i)_{i\in I}$ est une p-base si et seulement si le morphisme $\overline{\varphi}$ est un isomorphisme, si et seulement si $(x_i)_{i\in I}$ est p-libre et engendre $L$ comme extension de $K$.*

*Preuve.* Le $K$-espace vectoriel $K[(X_i)_{i\in I}]/\mathcal{J}$ admet pour base les (classes des) monômes $(X^{\boldsymbol{\alpha}})_{\boldsymbol{\alpha}\in\Lambda_I^{(p)}}$, et cette base est envoyée par $\overline{\varphi}$ sur la famille $(x^{\boldsymbol{\alpha}})_{\boldsymbol{\alpha}\in\Lambda_I^{(p)}}$. Par conséquent, $\overline{\varphi}$ est injectif (resp. bijectif) si et seulement si $(x^{\boldsymbol{\alpha}})_{\boldsymbol{\alpha}\in\Lambda_I^{(p)}}$ est libre (resp. une base) sur $K$, autrement dit si et seulement si $(x_i)_{i\in I}$ est $p$-libre (resp. une $p$-base) sur $K$. □

**Proposition 1.9.** *Soient $S,T$ deux parties de $L$. On a équivalence entre :*

*(i) $S$ est p-libre sur $K$ et $T$ est p-libre sur $K(S)$.*

*(ii) $T$ est p-libre sur $K$ et $S$ est p-libre sur $K(T)$.*

*(iii) $S\cap T=\emptyset$ et $S\cup T$ est p-libre sur $K$.*

*Preuve.* On note $\mathbf{x}$ la famille $(x)_{x\in S\cup T}$. Par symétrie, il suffit de prouver l'équivalence entre (i) et (iii).

(i) ⇒ (iii) : Puisque $T$ est $p$-libre sur $K(S)$, en particulier $T$ ne rencontre pas $K(S)$, et donc $T\cap S=\emptyset$. Soient $(\lambda_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha}\in\Lambda_{S\cup T}^{(p)}}$ des coefficients dans $K$ tels que $\sum_{\boldsymbol{\alpha}\in\Lambda_{S\cup T}^{(p)}}\lambda_{\boldsymbol{\alpha}}\mathbf{x}^{\boldsymbol{\alpha}}=0$. On peut identifier $\Lambda_{S\cup T}^{(p)}$ à $\Lambda_S^{(p)}\times\Lambda_T^{(p)}$ puisque $S\cap T=\emptyset$. On peut donc réécrire l'égalité sous la forme $\sum_{\boldsymbol{\gamma}\in\Lambda_T^{(p)}}(\sum_{\boldsymbol{\beta}\in\Lambda_S^{(p)}}\lambda_{(\boldsymbol{\beta},\boldsymbol{\gamma})}\mathbf{x}^{\boldsymbol{\beta}})\mathbf{x}^{\boldsymbol{\gamma}}=0$. On a $\sum_{\boldsymbol{\beta}\in\Lambda_S^{(p)}}\lambda_{(\boldsymbol{\beta},\boldsymbol{\gamma})}\mathbf{x}^{\boldsymbol{\beta}}\in K(S)$ pour tout $\boldsymbol{\gamma}\in\Lambda_T^{(p)}$, donc, étant donné que $T$ est $p$-libre sur $K(S)$, on obtient $\sum_{\boldsymbol{\beta}\in\Lambda_S^{(p)}}\lambda_{(\boldsymbol{\beta},\boldsymbol{\gamma})}\mathbf{x}^{\boldsymbol{\beta}}=0$ pour tout $\boldsymbol{\gamma}\in\Lambda_T^{(p)}$. En utilisant ensuite que $S$ est $p$-libre sur $K$, on obtient $\lambda_{(\boldsymbol{\beta},\boldsymbol{\gamma})}=0$ pour tout $\boldsymbol{\beta}\in\Lambda_S^{(p)}$ et tout $\boldsymbol{\gamma}\in\Lambda_T^{(p)}$, autrement dit $\lambda_{\boldsymbol{\alpha}}=0$ pour tout $\boldsymbol{\alpha}\in\Lambda_{S\cup T}^{(p)}$. Cela montre que $S\cup T$ est $p$-libre sur $K$.

(iii) ⇒ (i) : Puisque $S\cup T$ est $p$-libre sur $K$, en particulier $S\subset S\cup T$ est $p$-libre sur $K$ d'après la remarque 1.7 (iii), et donc $S$ est une $p$-base de $K(S)$. On identifie comme précédemment $\Lambda_{S\cup T}^{(p)}$ à $\Lambda_S^{(p)}\times\Lambda_T^{(p)}$ (ce qui est possible puisque $S\cap T=\emptyset$ par hypothèse). Soient $(\lambda_{\boldsymbol{\gamma}})_{\boldsymbol{\gamma}\in\Lambda_T^{(p)}}$ des coefficients dans $K(S)$ tels que $\sum_{\boldsymbol{\gamma}\in\Lambda_T^{(p)}}\lambda_{\boldsymbol{\gamma}}\mathbf{x}^{(0,\boldsymbol{\gamma})}=0$. On développe chaque $\lambda_{\boldsymbol{\gamma}}$ suivant la base $(\mathbf{x}^{(\boldsymbol{\beta},0)})_{\boldsymbol{\beta}\in\Lambda_S^{(p)}}$ de $K(S)$ : $\lambda_{\boldsymbol{\gamma}}=\sum_{\boldsymbol{\beta}\in\Lambda_S^{(p)}}\mu_{(\boldsymbol{\beta},\boldsymbol{\gamma})}\mathbf{x}^{(\boldsymbol{\beta},0)}$. On obtient donc : $\sum_{\boldsymbol{\gamma}\in\Lambda_T^{(p)}}(\sum_{\boldsymbol{\beta}\in\Lambda_S^{(p)}}\mu_{(\boldsymbol{\beta},\boldsymbol{\gamma})}\mathbf{x}^{(\boldsymbol{\beta},0)})\mathbf{x}^{(0,\boldsymbol{\gamma})}=\sum_{(\boldsymbol{\beta},\boldsymbol{\gamma})\in\Lambda_S^{(p)}\times\Lambda_T^{(p)}}\mu_{(\boldsymbol{\beta},\boldsymbol{\gamma})}\mathbf{x}^{(\boldsymbol{\beta},\boldsymbol{\gamma})}=0$. Puisque $S\cup T$ est $p$-libre sur $K$, on en conclut que $\mu_{(\boldsymbol{\beta},\boldsymbol{\gamma})}=0$ pour tout $(\boldsymbol{\beta},\boldsymbol{\gamma})\in\Lambda_S^{(p)}\times\Lambda_T^{(p)}$, puis que $\lambda_{\boldsymbol{\gamma}}=0$ pour tout $\boldsymbol{\gamma}\in\Lambda_T^{(p)}$, donc que $T$ est $p$-libre sur $K(S)$. □

**Proposition 1.10.** *Soient $S\subset T\subset L$ tels que $S$ est p-libre et $L=K(T)$. Alors il existe une p-base $B$ de $L$ sur $K$ telle que $S\subset B\subset T$.*

*Preuve.* Soit $\mathcal{B}$ l'ensemble des parties $S\subset B\subset T$ telles que $B$ soit $p$-libre sur $K$. On ordonne $\mathcal{B}$ par la relation d'inclusion ; montrons que c'est un ensemble inductif. Il contient $S$, donc est non vide. Soit $\mathcal{C}\subset\mathcal{B}$ une partie non vide totalement ordonnée. On pose $B_0=\bigcup_{B\in\mathcal{C}}B$. On a clairement $S\subset B_0\subset T$, et si l'ensemble $B_0$ n'était pas $p$-libre, il existerait une partie finie $B_1\subset B_0$ qui n'est pas $p$-libre d'après la remarque 1.7 (iii), mais c'est impossible car $B_1$ serait inclus dans un $B\in\mathcal{C}$, et devrait donc être $p$-libre. Ainsi, $B_0\in\mathcal{B}$, et $B_0$ majore l'ensemble $\mathcal{C}$, ce qui montre que $\mathcal{B}$ est inductif. D'après le lemme de Zorn, il existe un ensemble $B\in\mathcal{B}$ maximal pour l'inclusion. On a donc $S\subset B\subset T$ et $B$ est $p$-libre ; pour conclure, il suffit de montrer que $L=K(B)$. Si ce n'était pas le cas, alors puisque $L=K(T)$, il devrait exister $x\in T$ tel que $x\notin K(B)$. Mais alors $(x)$ serait $p$-libre sur $K(B)$ d'après la remarque 1.7 (i), et la proposition 1.9 impliquerait que $B\cup\{x\}\subset T$ serait $p$-libre sur $K$, ce qui contredirait la maximalité de $B$ dans $\mathcal{B}$. □

**Théorème 1.11.** *Il existe des p-bases de $L$ sur $K$. De plus, elles ont toutes le même cardinal. Plus précisément, si $(x_i)_{i\in I}$ est une p-base de $L$ sur $K$, on a :*

*(i) Si* $[L:K] < +\infty$, $[L:K] = p^{|I|}$ *et donc* $|I| = \log_p([L:K])$.

*(ii) Si* $[L:K]$ *est infini,* $|I| = [L:K]$.

*Preuve.* L'existence de $p$-bases résulte de la proposition 1.10 appliquée à $S = \emptyset$ et $T = L$. Soit $(x_i)_{i\in I}$ une $p$-base de $L$, alors $(x^{\boldsymbol{\alpha}})_{\boldsymbol{\alpha}\in\Lambda_I^{(p)}}$ est une base de $L$ sur $K$, donc $[L:K] = |\Lambda_I^{(p)}|$. Si $I$ est fini, on a clairement $|\Lambda_I^{(p)}| = p^{|I|}$. Si $I$ est infini, on a une surjection $\bigsqcup_{J\subset I,\ J \text{ fini}} \Lambda_J^{(p)} \to \Lambda_I^{(p)}$ qui envoie $(\alpha_j)_{j\in J} \in \Lambda_J^{(p)}$ sur $(\beta_i)_{i\in I} \in \Lambda_I^{(p)}$ avec $\beta_j = \alpha_j$ si $j \in J$ et $\beta_i = 0$ sinon. L'ensemble $\mathcal{P}_f(I)$ des parties finies de $I$ est équipotent à $I$ puisque $I$ est infini, et l'ensemble $\Lambda_J^{(p)}$ est fini pour tout $J \in \mathcal{P}_f(I)$, donc $|\Lambda_I^{(p)}| \leq |I|$. L'inégalité inverse $|I| \leq |\Lambda_I^{(p)}|$ est immédiate. □

On appellera le cardinal commun à toutes les $p$-bases de $L$ sur $K$ la $p$-dimension de $L$ sur $K$[2], que l'on notera $\dim_K^{(p)}(L)$. Notons que d'après le théorème, la $p$-dimension de $L$ sur $K$ est finie si et seulement si le degré de $L$ sur $K$ est fini.

# 2 Dérivations

**Définition 2.1.** Soit $A$ un anneau (commutatif). Une dérivation de $A$ est une application $D : A \to A$ qui vérifie les deux identités suivantes :

(i) $\forall x, y \in A,\ D(x+y) = D(x) + D(y)$

(ii) $\forall x, y \in A,\ D(xy) = D(x)y + xD(y)$

La condition (i) exprime que $D$ est un morphisme de groupes. L'identité (ii) est appelée identité de Leibniz. On note $\mathrm{Der}(A)$ l'ensemble des dérivations de $A$.

Soient $A$ un anneau et $D$ une dérivation de $A$. Des récurrences immédiates donnent les deux identités suivantes :

(a) $D^n(xy) = \sum_{i=0}^{n} \binom{n}{i} D^i(x) D^{n-i}(y)$

(b) $D(\prod_{i=1}^{n} x_i) = \sum_{i=1}^{n} (\prod_{j\neq i} x_j) D(x_i)$

On déduit de (ii) en prenant $x_1 = \ldots = x_n = x$ $(n \geq 1)$ :

(c) $D(x^n) = nx^{n-1}D(x)$

En particulier, on a $D(1) = D(1^2) = 2D(1)$, donc $D(1) = 0$. Si $x \in A$ est inversible, on a $0 = D(1) = D(xx^{-1}) = D(x)x^{-1} + xD(x^{-1})$, donc :

(d) $D(x^{-1}) = -x^{-2}D(x)$

et en écrivant $x^{-n} = (x^{-1})^n$, on trouve via (c) : $D(x^{-n}) = n(x^{-1})^{n-1}D(x^{-1}) = -nx^{1-n}x^{-2}D(x) = -nx^{-n-1}D(x)$. Autrement dit, la formule (c) s'étend à tout $n \in \mathbb{Z}$ si $x$ est inversible. En combinant les formules (ii) et (d), on trouve pour $x \in A,\ y \in A^\times$ :

(e) $D(xy^{-1}) = y^{-2}(D(x)y - xD(y))$

On appelle constante de $D$ tout élément $x \in A$ tel que $D(x) = 0$. Il suit immédiatement de (i) et (ii) que si $x, y$ sont des constantes de $D$ alors $x+y$ et $xy$ sont encore des constantes de $D$. Par ailleurs, on a vu que 1 est une constante de $D$, donc l'ensemble des constantes de $D$ est un sous-anneau de $A$. Il suit également de (d) que si $x \in A^\times$ est une constante de $D$, alors $x^{-1}$ est une constante de $D$. En particulier, si $A = K$ est un corps, alors l'ensemble des constantes de $D$ est un sous-corps de $K$.

L'application nulle $A \to A,\ x \mapsto 0$ est une dérivation de $A$. Si $D, D'$ sont des dérivations de $A$ et $a \in A$, il est clair que $D + D'$ et $aD$ sont encore des dérivations de $A$, autrement dit l'ensemble $\mathrm{Der}(A)$ est un sous-$A$-module du $A$-module $\mathrm{End}_{\mathrm{Ab}}(A)$ des endomorphismes de groupe de $A$.

[2] Cette terminologie n'est pas standard.

Supposons maintenant que $B$ est une $A$-algèbre (associative, unitaire, commutative). On note $f : A \to B$ le morphisme structural, de sorte que $a \cdot b = f(a)b$ pour tous $a \in A$ et $b \in B$. Si $D : B \to B$ est une dérivation de $B$, on trouve :

$$\forall a \in A,\ \forall b \in B,\ D(a \cdot b) = D(f(a)b) = D(f(a))b + f(a)D(b) = D(f(a))b + a \cdot D(b)$$

On en déduit que si $D(f(a)) = 0$ pour tout $a \in A$ alors $D$ est $A$-linéaire. Réciproquement, si $D$ est $A$-linéaire, on obtient $D(f(a)) = D(a \cdot 1) = a \cdot D(1) = 0$ pour tout $a \in A$. Ainsi, la dérivation $D$ est $A$-linéaire si et seulement si l'image du morphisme structural $f : A \to B$ est contenue dans l'ensemble des constantes de $D$, ou encore, par abus de langage (en identifiant un élément de $A$ avec son image par $f$), si et seulement si l'ensemble des constantes de $D$ contient $A$. On dit qu'une dérivation $A$-linéaire de $B$ est une $A$-dérivation, et on note $\mathrm{Der}_A(B)$ l'ensemble des $A$-dérivations de $B$. Les dérivations d'un anneau $A$ coïncident avec les $\mathbb{Z}$-dérivations de $A$, $A$ étant muni de son unique structure de $\mathbb{Z}$-algèbre. Si $D, D'$ sont des $A$-dérivations de $B$ et $b \in B$, alors $D + D'$ et $bD$ sont encore des $A$-dérivations de $B$, donc l'ensemble $\mathrm{Der}_A(B)$ est un sous-$B$-module, et a fortiori un sous-$A$-module, de $\mathrm{End}_A(B)$ (l'ensemble des applications $A$-linéaires $B \to B$). Si $D$ est une $A$-dérivation de $B$, l'ensemble des constantes de $D$ est un sous-anneau de $B$ qui contient l'image du morphisme structural $A \to B$, donc c'est une sous-algèbre de $B$ ; si $A = K$ est un corps et $B = L$ est une extension de $K$, l'ensemble des constantes de $D$ est un sous-corps de $L$ qui contient $K$, donc c'est une sous-extension de $L$.

**Remarque 2.2.**

(i) Si $D, E$ sont deux $A$-dérivations d'une $A$-algèbre $B$, il suit immédiatement de la linéarité de $D$ et $E$, de l'axiome (ii) de la définition 2.1 et de l'identité $D(1) = E(1) = 0$ que l'ensemble $\{D = E\}$ des $x \in B$ tels que $D(x) = E(x)$ est une sous-algèbre de $B$. En particulier, si $D$ et $E$ coïncident sur une partie $S$ de $B$, alors $D$ et $E$ coïncident sur la sous-algèbre $A[S]$ engendrée par $S$. Par ailleurs, la formule (d) ci-dessus montre que si $x \in \{D = E\}$ et $x$ est inversible, alors $x^{-1} \in \{D = E\}$. En particulier, si $A = K$ est un corps et $B = L$ est une extension de $K$, alors l'ensemble $\{D = E\}$ est une sous-extension de $L$ ; si $D$ et $E$ coïncident sur une partie $S$ de $L$, alors $D$ et $E$ coïncident sur la sous-extension $K(S)$ engendrée par $S$.

(ii) Si $B$ est une $A$-algèbre, $C$ est une $B$-algèbre et $D : C \to C$ est une $B$-dérivation alors $D$ est en particulier une $A$-dérivation. En effet, l'ensemble des constantes de $D$ contient l'image du morphisme structural $B \to C$ de $C$ comme $B$-algèbre, donc il contient l'image du morphisme composé $A \to B \to C$ où $A \to B$ est le morphisme structural de $B$ comme $A$-algèbre, et ce morphisme composé est le morphisme structural de $C$ comme $A$-algèbre.

(iii) Soient $L$ un corps de caractéristique $p > 0$, $D$ une dérivation de $L$ et $K$ le sous-corps des constantes de $D$. Alors $L$ est une extension purement inséparable de hauteur $\leq 1$ de $K$. En effet, si $x \in L$, on a $D(x^p) = px^{p-1}D(x) = 0$, donc $x^p \in K$. Plus généralement, si $M$ est un sous-corps de $L$ qui contient $K$, alors $L$ est une extension purement inséparable de hauteur $\leq 1$ de $M$.

**Exemple 2.3.**

(i) Si $A$ est un anneau, l'application $A[X] \to A[X],\ P \mapsto P'$ est une $A$-dérivation de $A[X]$.

(ii) Plus généralement, si $I$ est un ensemble, alors pour tout $i \in I$, l'application $D_i : A[(X_i)_{i\in I}] \to A[(X_i)_{i\in I}],\ P \mapsto \frac{\partial P}{\partial X_i}$ est une $A$-dérivation de $A[(X_i)_{i\in I}]$.

**Proposition 2.4.** *Soient $A$ un anneau, $I$ un ensemble, $(P_i)_{i\in I}$ une famille d'éléments de $A[(X_i)_{i\in I}]$. Alors il existe une unique $A$-dérivation $D$ de $A[(X_i)_{i\in I}]$ telle que $D(X_i) = P_i$ pour tout $i$. Elle est définie sur un polynôme $Q \in A[(X_i)_{i\in I}]$ par :*

$$D(Q) = \sum_{i\in I} \frac{\partial Q}{\partial X_i} P_i \tag{1}$$

*Preuve.* Puisque $Q$ ne contient qu'un nombre fini de variables, $\frac{\partial Q}{\partial X_i}$ est nul sauf pour un nombre fini de $i \in I$, donc la somme à droite de l'égalité dans (1) est bien définie. Pour tout sous-ensemble fini $J \subset I$, notons $D^{(J)}$ l'application $Q \mapsto \sum_{i\in J} \frac{\partial Q}{\partial X_i} P_i$. C'est une $A$-dérivation comme combinaison linéaire de $A$-dérivations. Les applications $D$ et $D^{(J)}$ coïncident dans $A[(X_i)_{i\in J}] \subset A[(X_i)_{i\in I}]$. Si $Q, R \in A[(X_i)_{i\in I}]$, il existe un sous-ensemble fini $J$ de $I$ tel que $Q, R \in A[(X_i)_{i\in J}]$, et on obtient donc, pour tous $a, b \in A$ :

$$D(aQ + bR) = D^{(J)}(aQ + bR) = aD^{(J)}(Q) + bD^{(J)}(R) = aD(Q) + bD(R)$$
$$D(QR) = D^{(J)}(QR) = D^{(J)}(Q)R + QD^{(J)}(R) = D(Q)R + QD(R)$$

Donc $D$ est bien une $A$-dérivation. On a clairement $D(X_i) = P_i$, et $D$ est la seule $A$-dérivation de $A[(X_i)_{i\in I}]$ qui envoie $X_i$ sur $P_i$ pour tout $i$ car les $X_i$ engendrent $A[(X_i)_{i\in I}]$ comme $A$-algèbre. □

**Lemme 2.5.** *Soient $A$ un anneau, $B$ une $A$-algèbre, $D$ une $A$-dérivation de $B$, $P \in A[(X_i)_{i\in I}]$ et $(x_i)_{i\in I}$ une famille d'éléments de $B$. Alors on a :*

$$D(P((x_i)_{i\in I})) = \sum_{i\in I} \frac{\partial P}{\partial X_i}((x_i)_{i\in I})D(x_i) \tag{2}$$

*Preuve.* Il n'existe qu'un nombre fini de $i \in I$ tels que $\frac{\partial P}{\partial X_i} \neq 0$, donc la somme à droite du signe = dans (2) est bien définie. Par $A$-linéarité de $D$ et des dérivations partielles, il suffit de vérifier (2) lorsque $P = X_{i_1}^{n_1} \dots X_{i_k}^{n_k}$ est un monôme. D'après les identités (b) et (c) du début de section, on a :

$$\begin{aligned} D(x_{i_1}^{n_1} \dots x_{i_k}^{n_k}) &= \sum_{j=1}^{k} (n_j x_{i_j}^{n_j-1} \prod_{l\neq j} x_{i_l}^{n_l}) D(x_{i_j}) \\ &= \sum_{j=1}^{k} \frac{\partial (X_{i_1}^{n_1} \dots X_{i_k}^{n_k})}{\partial X_{i_j}}((x_i)_{i\in I})D(x_{i_j}) \\ &= \sum_{j\in I} \frac{\partial (X_{i_1}^{n_1} \dots X_{i_k}^{n_k})}{\partial X_j}((x_i)_{i\in I})D(x_j) \end{aligned}$$

où, dans la dernière égalité, on utilise que $\frac{\partial (X_{i_1}^{n_1} \dots X_{i_k}^{n_k})}{\partial X_j} = 0$ si $j \notin \{i_1, \dots, i_k\}$. □

**Proposition 2.6.** *Soit $B$ une $A$-algèbre, donnée par la présentation $B = \langle (x_i)_{i\in I} | (P_j((x_i)_{i\in I}))_{j\in J} \rangle$ où les $x_i$ sont des éléments de $B$ et les $P_j$ sont des polynômes dans $A[(X_i)_{i\in I}]$. Alors :*

*(i) Si $D$ est une $A$-dérivation de $B$, et si pour tout $i \in I$ on pose $y_i = D(x_i)$, alors on a :*

$$\sum_{i\in I} \frac{\partial P_j}{\partial X_i}((x_i)_{i\in I})y_i = 0 \text{ pour tout } j \in J \tag{3}$$

*(ii) Réciproquement, si $(y_i)_{i\in I}$ est une famille d'éléments de $B$ qui satisfait (3) alors il existe une unique $A$-dérivation de $B$ qui envoie $x_i$ sur $y_i$ pour tout $i$.*

*Preuve.* (i) D'après le lemme 2.5, on a $\sum_{i\in I} \frac{\partial P_j}{\partial X_i}((x_i)_{i\in I})y_i = D(P_j((x_i)_{i\in I})) = D(0) = 0$.

(ii) Soit $\mathcal{I}$ l'idéal de $A[(X_i)_{i\in I}]$ engendré par les polynômes $P_j$, de sorte que $B \cong {}^{A[(X_i)_{i\in I}]}\!/_{\mathcal{I}}$. Soient $Q_j$, $j \in I$ des polynômes dans $A[(X_i)_{i\in I}]$ tels que $y_j = Q_j((x_i)_{i\in I})$. D'après la proposition 2.4, il existe une $A$-dérivation $E$ de $A[(X_i)_{i\in I}]$ telle que $E(X_i) = Q_i$ pour tout $i$. D'après le lemme 2.5, on a $E(P_j) = \sum_{i\in I} \frac{\partial P_j}{\partial X_i} E(X_i) = \sum_{i\in I} \frac{\partial P_j}{\partial X_i} Q_i$. En évaluant en $(x_i)_{i\in I}$ dans $B$, on obtient, compte tenu de (3), que $E(P_j)((x_i)_{i\in I}) = 0$, donc que $E(P_j) \in \mathcal{I}$. Montrons que $E$ préserve $\mathcal{I}$ : si $R \in \mathcal{I}$, il existe des polynômes $A_j$ presque tous nuls tels que $R = \sum_{j\in J} A_j P_j$. Alors $E(R) = \sum_{j\in J} E(A_j)P_j + \sum_{j\in J} A_j E(P_j) \in \mathcal{I}$ car $P_j$, $E(P_j) \in \mathcal{I}$ pour tout $j$. Ainsi, $E$ induit une application $A$-linéaire $D : B \to B$ telle que $D(P((x_i)_{i\in I})) = E(P)((x_i)_{i\in I})$ pour tout polynôme $P \in A[(X_i)_{i\in I}]$, et en particulier $D(x_i) = y_i$. Pour montrer que $D$ est une $A$-dérivation, il ne reste qu'à montrer que $D$ satisfait l'identité de Leibniz. Soient $a, b \in B$, il existe des polynômes $Q, R \in A[(X_i)_{i\in I}]$ tels que $a = Q((x_i)_{i\in I})$ et $b = R((x_i)_{i\in I})$. On obtient alors :
$D(ab) = D(QR((x_i)_{i\in I})) = E(QR)((x_i)_{i\in I}) = (E(Q)R + QE(R))((x_i)_{i\in I}) = D(a)b + aD(b)$.
Donc $D$ est bien une $A$-dérivation. Puisque les $x_i$ engendrent $B$ comme $A$-algèbre, $D$ est l'unique $A$-dérivation de $B$ qui envoie $x_i$ sur $y_i$ pour tout $i \in I$. □

**Corollaire 2.7.** *Soient $K$ un corps de caractéristique $p > 0$, $L$ une extension purement inséparable de hauteur $\leq 1$ de $K$, $(x_i)_{i\in I}$ une $p$-base de $L$ sur $K$. Pour toute famille $(y_i)_{i\in I}$ d'éléments de $L$, il existe une unique $K$-dérivation de $L$ qui envoie $x_i$ sur $y_i$ pour tout $i \in I$.*

*Preuve.* Soit $a_i = x_i^p \in K$. D'après la proposition 1.8 (ii), une présentation de $L$ comme $K$-algèbre est donnée par $L = \langle (x_i)_{i\in I} | (x_i^p - a_i)_{i\in I} \rangle$. Le corollaire suit alors immédiatement de la proposition 2.6, en remarquant que la condition (3) est automatiquement vérifiée, car $\frac{\partial (X_i^p - a_i)}{\partial X_i} = pX_i^{p-1} = 0$, et évidemment $\frac{\partial (X_j^p - a_j)}{\partial X_i} = 0$ si $j \neq i$. □

**Corollaire 2.8.** *Soient $K$ un corps de caractéristique $p > 0$ et $L$ une extension purement inséparable de hauteur $\leq 1$ de $K$. On suppose que $L$ est de degré fini sur $K$. Alors $\dim_L(Der_K(L)) = \dim_K^{(p)}(L)$.*

*Preuve.* Soit $(x_1, \dots, x_m)$ une $p$-base de $L$ sur $K$. L'application $\mathrm{Der}_K(L) \to L^m$, $D \mapsto (D(x_1), \dots, D(x_m))$ est clairement $L$-linéaire, et elle est bijective d'après le corollaire 2.7. On a donc $\dim_L(\mathrm{Der}_K(L)) = m = \dim_K^{(p)}(L)$. □

# 3 Correspondance de Jacobson

Étant donnés un corps $K$, un $K$-espace vectoriel $V$ et deux endomorphismes $D, E$ de $V$, on note $[D, E] = D \circ E - E \circ D$ le commutateur de $D$ et $E$ dans $\mathrm{End}_K(V)$.

**Proposition 3.1.** *Soit $K \hookrightarrow L$ une extension de corps. Alors :*

*(i) Si $D, E \in Der_K(L)$ alors $[D, E] \in Der_K(L)$.*

*(ii) Si $char(K) = p > 0$ et $D \in Der_K(L)$ alors $D^p \in Der_K(L)$.*

*Preuve.* Les applications $[D, E]$ et $D^p$ sont $K$-linéaires, et on a :

$$\begin{aligned}
[D,E](xy) &= D(E(xy)) - E(D(xy)) \\
&= D(E(x)y + xE(y)) - E(D(x)y + xD(y)) \\
&= D(E(x))y + E(x)D(y) + D(x)E(y) + xD(E(y)) - E(D(x))y - D(x)E(y) - E(x)D(y) - xE(D(y)) \\
&= (D(E(x)) - E(D(x)))y + x(D(E(y)) - E(D(y))) \\
&= [D,E](x)y + x[D,E](y) \\
D^p(xy) &= \sum_{i=0}^{p} \tbinom{p}{i} D^i(x) D^{p-i}(y) \\
&= D^p(x)y + xD^p(y) \qquad \text{puisque } \tbinom{p}{i} = 0 \text{ dans } K \text{ si } 1 \leq i \leq p-1 \text{ et } \mathrm{char}(K) = p
\end{aligned}$$

□

Soit $K \hookrightarrow L$ une extension purement inséparable de hauteur $\leq 1$. On dira qu'une partie $\mathfrak{D} \subset \mathrm{Der}_K(L)$ est une sous-$L$-algèbre de Lie restreinte de $\mathrm{Der}_K(L)$[3] si elle satisfait aux trois conditions suivantes : (i) $\mathfrak{D}$ est un sous-$L$-espace vectoriel de $\mathrm{Der}_K(L)$ (ii) on a $[D, E] \in \mathfrak{D}$ pour tous $D, E \in \mathfrak{D}$ (iii) on a $D^p \in \mathfrak{D}$ pour tout $D \in \mathfrak{D}$.

À toute sous-$L$-algèbre de Lie restreinte $\mathfrak{D} \subset \mathrm{Der}_K(L)$, on associe l'ensemble $\mathcal{C}(\mathfrak{D}) = \{x \in L \mid D(x) = 0 \; \forall D \in \mathfrak{D}\}$ des constantes de $\mathfrak{D}$, c'est-à-dire des éléments de $L$ qui sont des constantes pour toutes les dérivations dans $\mathfrak{D}$. Dans l'autre sens, on associe à toute sous-extension $M$ de $L$ l'ensemble $\mathcal{D}(M) = \mathrm{Der}_M(L) = \{D \in \mathrm{Der}_K(L) \mid D(x) = 0 \; \forall x \in M\}$. Les propriétés suivantes sont immédiates :

(i) Pour toute sous-$L$-algèbre de Lie restreinte $\mathfrak{D}$ de $\mathrm{Der}_K(L)$, $\mathcal{C}(\mathfrak{D})$ est une sous-extension de $L$. Pour toute sous-extension $M \subset L$, $\mathcal{D}(M)$ est une sous-$L$-algèbre de Lie restreinte de $\mathrm{Der}_K(L)$.

(ii) Les applications $\mathfrak{D} \mapsto \mathcal{C}(\mathfrak{D})$ et $M \mapsto \mathcal{D}(M)$ sont décroissantes pour l'inclusion.

(iii) Pour toute sous-$L$-algèbre de Lie restreinte $\mathfrak{D} \subset \mathrm{Der}_K(L)$, on a $\mathfrak{D} \subset \mathcal{D}(\mathcal{C}(\mathfrak{D}))$. Pour toute sous-extension $M \subset L$, on a $M \subset \mathcal{C}(\mathcal{D}(M))$.

On notera $\mathscr{M}$ l'ensemble des sous-extensions $M$ de $L$ telles que $[L : M] < +\infty$ et $\mathscr{D}$ l'ensemble des sous-$L$-algèbres de Lie restreintes de $\mathrm{Der}_K(L)$ de dimension finie sur $L$. Les ensembles $\mathscr{M}$ et $\mathscr{D}$ sont ordonnés par inclusion. Notons que si $[L : K] < +\infty$ (autrement dit si $L$ est de $p$-dimension finie sur $K$) alors $\mathscr{M}$ est l'ensemble de toutes les sous-extensions de $L$ et $\mathscr{D}$ est l'ensemble de toutes les sous-$L$-algèbres de Lie restreintes de $\mathrm{Der}_K(L)$.

**Théorème 3.2** (Correspondance de Jacobson)**.** *Avec les notations ci-dessus, les applications :*

$$\begin{array}{ccc} \mathscr{M} & \rightleftarrows & \mathscr{D} \\ M & \mapsto & \mathcal{D}(M) \\ \mathcal{C}(\mathfrak{D}) & \hookleftarrow & \mathfrak{D} \end{array}$$

*sont bien définies et sont des bijections strictement décroissantes réciproques l'une de l'autre. De plus, si $M$ et $\mathfrak{D}$ se correspondent via ces bijections, on a $\dim_M^{(p)}(L) = \dim_L(\mathfrak{D})$.*

On commence par montrer deux lemmes :

**Lemme 3.3.** *Soient $k$ un corps de caractéristique $p > 0$, $D$ une dérivation de $k$ telle que $D^p = D$ et telle qu'il existe $x \in k^\times$ pour lequel $D(x) = x$. Si $M$ est le sous-corps des constantes de $D$ alors $[k : M] = p$.*

*Preuve.* L'endomorphisme $M$-linéaire $D$ est annulé par le polynôme $X^p - X$. Or, dans $\mathbb{F}_p[X]$ (et a fortiori dans $M[X]$), ce polynôme se factorise sous la forme $X^p - X = \prod_{\lambda \in \mathbb{F}_p} (X - \lambda)$. D'après le lemme des noyaux, on a une décomposition de $k = \mathrm{Ker}(D^p - D)$ en somme directe de sous-$M$-espaces vectoriels $k = \bigoplus_{\lambda \in \mathbb{F}_p} M_\lambda$ avec

[3] Cette dénomination est abusive pour la raison suivante : $\mathrm{Der}_K(L)$ est une $K$-algèbre de Lie mais n'est pas une $L$-algèbre de Lie, car le crochet $[-, -]$ est $K$-bilinéaire mais n'est pas $L$-bilinéaire.

$M_\lambda = \mathrm{Ker}(D - \lambda \mathrm{Id}_L)$ pour tout $\lambda \in \mathbb{F}_p$. Si $y \in M_\lambda$, on a $D(xy) = D(x)y + xD(y) = xy + x(\lambda y) = (1+\lambda)xy$ donc $xy \in M_{1+\lambda}$. Ainsi, l'application $M$-linéaire $m_x : k \to k,\ y \mapsto xy$ envoie $M_\lambda$ dans $M_{\lambda+1}$ pour tout $\lambda \in \mathbb{F}_p$. Puisque $x \neq 0$, l'application $m_x$ est bijective, et étant donné que $k = \bigoplus_{\lambda \in \mathbb{F}_p} M_\lambda$, $m_x$ induit par restriction un isomorphisme de $M$-espaces vectoriels de $M_\lambda$ sur $M_{\lambda+1}$ pour tout $\lambda \in \mathbb{F}_p$. Par conséquent, tous les $M_\lambda$ ont même $M$-dimension, et puisque $M_0 = \mathrm{Ker}(D) = M$, on en déduit que $\dim_M(M_\lambda) = 1$ pour tout $\lambda$, puis que $\dim_M(k) = \dim_M(\bigoplus_{\lambda \in \mathbb{F}_p} M_\lambda) = p$. □

**Lemme 3.4.** *Soit $\mathfrak{D} \in \mathscr{D}$ i.e. $\mathfrak{D}$ est une sous-$L$-algèbre de Lie de $Der_K(L)$ de dimension finie $s$ sur $L$. Alors $[L : \mathcal{C}(\mathfrak{D})] = p^s$. En particulier, on a $\mathcal{C}(\mathfrak{D}) \in \mathscr{M}$.*

*Preuve.* Notons $M = \mathcal{C}(\mathfrak{D})$. Si $x \in L$, on note $\theta_x : \mathfrak{D} \to L$ la forme linéaire définie par $\theta_x(D) = D(x)$. Si $D \in \mathfrak{D}$ est dans l'orthogonal de l'ensemble des $\theta_x$, on a $D(x) = 0$ pour tout $x \in L$, donc $D = 0$. Ainsi, l'orthogonal de l'ensemble des $\theta_x$ est trivial, donc les $\theta_x$ engendrent le dual $\mathfrak{D}^*$ de $\mathfrak{D}$ (vu comme $L$-espace vectoriel). Par conséquent, on peut extraire une base de la famille $(\theta_x)_{x \in L}$, et cette base est nécessairement de cardinal $s = \dim_L(\mathfrak{D}) = \dim_L(\mathfrak{D}^*)$. Soient donc $x_1, \ldots, x_s \in L$ tels que $(\theta_{x_1}, \ldots, \theta_{x_s})$ est une base de $\mathfrak{D}^*$. Notons que les $x_i$ sont forcément non nuls et deux à deux distincts. Soit également $(\Delta_1, \ldots, \Delta_s) \in \mathfrak{D}^s$ la base antéduale de $(\theta_{x_1}, \ldots, \theta_{x_s})$, de sorte que $\theta_{x_i}(\Delta_j) = \Delta_j(x_i) = \delta_{i,j}$ pour tous $i, j$. On pose enfin $D_i = x_i\Delta_i \in \mathfrak{D}$, ce qui donne $D_j(x_i) = \delta_{i,j}x_j$. Puisque les $x_i$ sont non nuls, la famille $(D_1, \ldots, D_s)$ est encore une base de $\mathfrak{D}$. Pour tous $i, j$, les dérivations $D_i^p - D_i$ et $[D_i, D_j]$ appartiennent à $\mathfrak{D}$ et on vérifie immédiatement qu'elles s'annulent en $x_1, \ldots, x_s$. Puisque $(\theta_{x_1}, \ldots, \theta_{x_s})$ est une base de $\mathfrak{D}^*$, on en conclut que $D_i^p - D_i = [D_i, D_j] = 0$ pour tous $i, j$, autrement dit $D_i^p = D_i$ et $D_i, D_j$ commutent pour tous $i, j$. Cela implique que, pour tous $i, j$, le noyau de $D_i$ est stable par $D_j$, puis que $M_i = \bigcap_{l=1}^{i} \mathrm{Ker}(D_l)$ est stable par $D_j$. Notons que puisque $(D_1, \ldots D_s)$ est une base de $\mathfrak{D}$, $M_s$ est égal à l'ensemble des constantes de $\mathfrak{D}$, donc à $M$. On a une suite de sous-extensions $M = M_s \subset M_{s-1} \subset \ldots \subset M_1 \subset M_0 = L$. On remarque que pour tout $1 \leq i \leq s$, $x_i$ appartient à $M_{i-1}$ et $D_i(x_i) = x_i$. On applique le lemme 3.3 avec $k = M_{i-1}$, $D = D_{i|M_{i-1}}$ et $x = x_i$. Puisque $\mathrm{Ker}(D_{i|M_{i-1}}) = \mathrm{Ker}(D_i) \cap M_{i-1} = M_i$, on obtient $[M_{i-1} : M_i] = p$. On en conclut que $[L : M] = \prod_{i=1}^{s} [M_{i-1} : M_i] = p^s$. □

*Preuve du théorème 3.2.* Soit $M$ une sous-extension de $L$ telle que $[L : M] < +\infty$. On note $m$ la $p$-dimension de $L$ sur $M$. Il suit du corollaire 2.8 que $\mathrm{Der}_M(L)$ est de dimension finie $m$ sur $L$, donc $\mathcal{D}(M) = \mathrm{Der}_M(L)$ appartient bien à $\mathscr{D}$. D'autre part, il suit du lemme 3.4 que $[L : \mathcal{C}(\mathcal{D}(M))] = p^m$. Puisque $M \subset \mathcal{C}(\mathcal{D}(M))$ et $[L : M] = p^m$, on en conclut que $\mathcal{C}(\mathcal{D}(M)) = M$.
Soit $\mathfrak{D}$ une sous-$L$-algèbre de Lie de $\mathrm{Der}_K(L)$ de dimension finie $s$ sur $L$. Le lemme 3.4 implique que $M = \mathcal{C}(\mathfrak{D})$ appartient bien à $\mathscr{M}$ et que $[L : M] = p^s$. On en déduit que $\dim_M^{(p)}(L) = s$, et le corollaire 2.8 implique que $\dim_L(\mathcal{D}(M)) = \dim_L(\mathrm{Der}_M(L)) = s$. On a donc $\dim_L(\mathcal{D}(\mathcal{C}(\mathfrak{D}))) = \dim_L(\mathfrak{D})$. Étant donné que $\mathfrak{D} \subset \mathcal{D}(\mathcal{C}(\mathfrak{D}))$, cela implique que $\mathfrak{D} = \mathcal{D}(\mathcal{C}(\mathfrak{D}))$.
On a montré au passage que si $M$ et $\mathfrak{D}$ se correspondent, alors $\dim_M^{(p)}(L) = \dim_L(\mathfrak{D})$. Les applications $\mathfrak{D} \mapsto \mathcal{C}(\mathfrak{D})$ et $M \mapsto \mathcal{D}(M)$ étant décroissantes et bijectives, elles sont strictement décroissantes. □

# Bibliographie


[1] N. Bourbaki. *Algèbre: Chapitres 4 à 7.* Springer, 2006.

[2] Nathan Jacobson. Abstract derivation and Lie algebras. *Transactions of the American Mathematical Society*, 42(2):206–224, 1937.