Dérivations de Hasse sur des corps séparablement clos

Adriane Kaïchouh

Nous allons nous intéresser à une certaine classe de corps : les corps *séparablement clos*, sur lesquels nous aurons définis une famille de fonctions que nous appellerons des *dérivations de Hasse* en raisons de leurs ressemblances avec les dérivations usuelles. Ainsi munis d'une structure différentielle, ces corps ont des propriétés très intéressantes du point de vue de la théorie des modèles.

1 Dérivations de Hasse

Pour définir ces fameuses dérivations, nous partons des dérivations usuelles.

Définition 1. Soit A un anneau commutatif.
Une **dérivation** de A est une fonction $D : A \to A$ telle que $\forall x, y \in A$:

$$\begin{aligned} D(x+y) &= D(x) + D(y) \\ D(x \cdot y) &= x \cdot D(y) + D(x) \cdot y \end{aligned}$$

Proposition-définition 2. *Soit A un anneau commutatif muni d'une dérivation D.*
Soit $A_0 = \{a \in A | D(a) = 0\}$.
*A_0 est un sous-anneau de A appelé l'**anneau des constantes** de A.*

Nous allons présenter maintenant une propriété des dérivations qui va nous être utile par la suite.

Proposition 3. *Soit A un anneau de caractéristique p première.*
Supposons qu'il existe $x \in A$ et $D : A \to A$ une dérivation de A tels que $D(x) = 1$ et $D^p = 0$.
Soit A_0 l'anneau des constantes de (A, D).
Alors A est un A_0-module libre et admet pour A_0-base $(1, x, ..., x^{p-1})$.

Démonstration. Comme A_0 est un sous-anneau de A, A est un A_0-module.

Montrons que la famille $(1, x, .., x^{p-1})$ est libre sur A_0.
Supposons qu'il existe $i < p$ et $\alpha_k \in A_0, k \in \{0, ..., i\}$ tels que $\sum_{k=0}^{i} \alpha_k \cdot x^k = 0$.
Calculons $D(x^k)$:

$$\begin{aligned} D(x^k) &= x \cdot D(x^{k-1}) + x^{k-1} \cdot \underbrace{D(x)}_{=1} \\ &= x \cdot D(x^{k-1}) + x^{k-1} \\ &= x^2 \cdot D(x^{k-2}) + x^{k-1} \cdot D(x) + x^{k-1} \\ &= ... \\ &= k \cdot x^{k-1} \end{aligned}$$

Et $D^i(x^k) = k \cdot (k-1) \cdot ... \cdot (k-i+1) \cdot x^{k-i}$.
On applique D^i à l'égalité $\sum_{k=0}^{i} \alpha_k \cdot x^k = 0$:

$$\begin{aligned}
\sum_{k=0}^{i} D^i(\alpha_k \cdot x^k) &= \sum_{k=0}^{i} D^{i-1}(\alpha_k \cdot D(x^k) + \underbrace{D(\alpha_k)}_{=0} \cdot x^k \\
&= \sum_{k=0}^{i} D^{i-1}(\alpha_k \cdot D(x^k) \\
&= \sum_{k=0}^{i} \alpha_k \cdot D^i(x^k) \\
&= i! \cdot \alpha_i \\
&= 0
\end{aligned}$$

Comme $i < p$, $p \not| i!$ et donc $i!$ est inversible, par Bezout.
Donc $\alpha_i = 0$.
Par une récurrence descendante, on obtient que $\forall j \leq i, \alpha_j = 0$.

Montrons que la famille $(1, x, ..., x^{p-1})$ est génératrice de A sur A_0.
Comme $D^p = 0$, $\forall a \in A, \exists i, 0 \leq i < p, D^{i+1}(a) = 0$.
SI $i = 0$, alors $D(a) = 0$ et $a \in A_0$.
Sinon,

$$\begin{aligned}
D^i\left(a - \frac{x^i \cdot D^i(a)}{i!}\right) &= D^i(a) - D^i\left(\frac{x^i \cdot D^i(a)}{i!}\right) \\
&= D^i(a) - \frac{D^i(x^i \cdot D^i(a))}{i!} \\
&= D^i(a) - \frac{1}{i!} \cdot D^{i-1}(D(x^i) \cdot D^i(a) + x^i \cdot \underbrace{D^{i+1}(a)}_{=0}) \\
&= ... \\
&= D^i(a) - \frac{1}{i!} \cdot \underbrace{D^i(x^i)}_{i!} \cdot D^i(a) \\
&= 0
\end{aligned}$$

Montrons par récurrence sur i que si $D^{i+1}(a) = 0$, alors $a \in A_0 + A_0 \cdot x + ... + A_0 \cdot x^i$.
Pour $i = 0$, $D(a) = 0 \Rightarrow a \in A_0$.
Supposons que $D^i(b) \Rightarrow b \in A_0 + A_0 \cdot x + ... + A_0 \cdot x^{i-1}$.
Soit alors $a \in A$ tel que $D^{i+1}(a) = 0$.
On a $D^i\left(a - \frac{x^i \cdot D^i(a)}{i!}\right) = 0$ d'après ce qui précède.
Donc $a - \frac{D^i(a)}{i!} \cdot x^i \in A_0 + A_0 \cdot x + ... + A_0 \cdot x^{i-1}$.
Or $D\left(\frac{D^i(a)}{i!}\right) = \frac{D^{i+1}}{i!} = 0$ donc $\frac{D^i(a)}{i!} \in A_0$.
Donc $a \in A_0 + A_0 \cdot x + ... + A_0 \cdot x^i$.
En appliquant ce résultat à $i = p-1$, on obtient que, comme $D^p = 0$, $A = A_0 + A_0 \cdot x + ... + A_0 \cdot x^{p-1}$.
□

A partir d'une dérivation, nous allons donner un ensemble de relations permettant de construire des "dérivations d'ordre supérieur", d'une manière un peu différente de celle que l'on connaît, qui formeront une dérivation de Hasse.

Définition 4. Soit A un anneau commutatif.
Une **dérivation de Hasse** sur A est une famille $D = (D_0, D_1, ...)$ de fonctions $D_n : A \to A$, $\forall n \in \mathbb{N}$, telles que, $\forall x, y \in A$, $\forall n, m \in \mathbb{N}$:

$$\begin{aligned} D_0(x) &= x \\ D_n(x+y) &= D_n(x) + D_n(y) \\ D_n(x \cdot y) &= \sum_{a+b=n} D_a(x) \cdot D_b(y) \\ D_m \circ D_n &= \binom{m+n}{m} D_{m+n} \end{aligned}$$

Remarques. *D_1 est une dérivation.*
En caractéristique nulle, toutes les D_n sont déterminées par D_1.

Définition 5. On dit que deux dérivations de Hasse D et E **commutent** si $\forall m, n \in \mathbb{N}$, $D_m \circ E_n = E_n \circ D_m$.

Dans toute la suite, on fixe un entier $e \in \mathbb{N}$ et un nombre premier p.

Définition 6. Un **D-corps** est un couple (K, D) où K est un corps de caractéristique p et $D = (D_1, ..., D_e)$ est une famille de e dérivations de Hasse sur K qui commutent.
Son **corps des constantes** C est l'ensemble des éléments de K sur lesquels toutes les dérivations $D_{i,1}$, $\forall i \in \{1, ..., e\}$, s'annulent.

Proposition 7. *Soient (K, D) un D-corps et C son corps des constantes. Alors :*
- *$K^p = \{x \in K | \exists y \in K, x = y^p\}$ est un sous-corps de K.*
- *$K^p \subseteq C$.*
- *C est un bien un sous-corps de K.*

Nous allons maintenant introduire une propriété remarquable des D-corps : la strictitude. Celle-ci sera essentielle pour montrer les propriétés modèles-théoriques de notre classe de corps.

Définition 8. Soient (K, D) un D-corps et C son corps des constantes.
On dit que (K, D) est **strict** si $C = K^p$.

Nous allons maintenant présenter quelques résultats de base concernant les dérivations de Hasse et les D-corps.

Lemme 9. *Soient K un corps de caractéristique p et D une dérivation de Hasse sur K.*
Alors $\forall x \in K$, $\forall n \in \mathbb{N}$, on a :

$$D_n(x^p) = \begin{cases} D_{\frac{n}{p}}(x)^p & \text{si } p|n \\ 0 & \text{sinon.} \end{cases}$$

Corollaire 10. *Soit K un corps muni d'une dérivation de Hasse D.*
Alors $\forall x, b \in K$, $\forall n \in \mathbb{N}$, $\forall r < p$:

$$D_{p \cdot n + r}(x^p \cdot b) = \sum_{m \leq n} D_m(x)^p \cdot D_{p \cdot (n-m)+r}(b)$$

On peut aussi définir l'analogue des dérivations de Hasse sur les modules.

Définition 11. Soit (K, D^K) un D-corps.
Un **D-module** sur K est un K-espace vectoriel V muni d'une famille $D = \{D_{i,n} | i \in \{1, ..., e\}, n \in \mathbb{N}\}$ de fonctions additives $D_{i,n} : V \to V$ qui commutent et telles que, $\forall i \in \{1, ..., e\}$, $\forall n \in \mathbb{N}$, $\forall \lambda \in K$, $\forall v \in V$:

$$\begin{aligned} D_{i,0}(v) &= v \\ D_{i,n}(\lambda \cdot v) &= \sum_{a+b=n} D_{i,a}^K(\lambda) \cdot D_{i,b}(v) \\ D_{i,m} \circ D_{i,n} &= \begin{pmatrix} m+n \\ m \end{pmatrix} D_{i,m+n} \end{aligned}$$

Définition 12. Soit (K, D) un D-corps.
Une **D-algèbre** sur K est une K-algèbre commutative R est un D-module sur K tel que les D_i soient des dérivations de Hasse sur R.

Proposition 13. *Soit (K, D^K) un D-corps.*
Soient (V, D) et (W, D') deux D-modules sur K.
Alors leur produit tensoriel $V \otimes_K W$ est aussi un D-module sur K, sur lequel les dérivations sont définies par :

$$\begin{aligned} D_{i,0}^* &= Id \\ D_{i,n}^*(v \otimes w) &= \sum_{a+b=n} D_{i,a}(v) \otimes D'_{i,b}(w) \end{aligned}$$

Proposition 14. *Soit (K, D^K) un D-corps.*
Soient R et S deux D-algèbres sur K.

- *Alors leur produit tensoriel $R \otimes_K S$ est aussi une D-algèbre sur K.*
- *Si de plus R et S ont des éléments unités, R et S sont des sous-anneaux de $R \otimes_K S$ et la D-structure sur $R \otimes_K S$ est la seule qui prolonge celles de R et de S.*

Proposition 15. *Soient A un anneau intègre muni d'une dérivation de Hasse D et K son corps des fractions.*
Alors D se prolonge de manière unique en une dérivation de Hasse sur K par la formule de récurrence suivante, $\forall n \in \mathbb{N}^*$, $\forall (x, y) \in A \times A^*$:

$$\begin{aligned} D_0 &= Id_K \\ D_n\left(\frac{x}{y}\right) &= \frac{D_n(x) - \sum_{m<n} D_m\left(\frac{x}{y}\right) \cdot D_{n-m}(y)}{y} \end{aligned}$$

Démonstration. Si un tel prolongement existe, alors il vérifie, pour tout (x, y) dans $A \times A^*$:

$$\begin{aligned} D_n(x) &= D_n\left(\frac{x}{y} \cdot y\right) \\ &= \sum_{m \leq n} D_m\left(\frac{x}{y}\right) \cdot D_{n-m}(y) \\ &= y \cdot D_n\left(\frac{x}{y}\right) + \sum_{m<n} D_m\left(\frac{x}{y}\right) \cdot D_{n-m}(y) \end{aligned}$$

On a donc l'unicité.

Les fonctions D_n vérifient $D_n(x \cdot y) = \sum_{a+b=n} D_a(x) \cdot D_b(y)$, $\forall x, y \in K$.

Montrons que D est bien définie sur K.

Soient $(x, y) \in A \times A^*$ et $\lambda \in A^*$.

$$\begin{aligned} D_n\left(\frac{\lambda \cdot x}{\lambda \cdot y}\right) &= \sum_{a+b=n} D_a\left(\frac{\lambda}{\lambda}\right) \cdot D_b\left(\frac{x}{y}\right) \text{ d'après ce qui précède} \\ &= \sum_{a+b=n} D_a(1) \cdot D_b\left(\frac{x}{y}\right) \\ &= D_n\left(\frac{x}{y}\right) \text{ car } \forall a \geq 1, D_a(1) = 0 \end{aligned}$$

Montrons par récurrence sur $a + b$ que $\forall a, b \in \mathbb{N}$, $D_a \circ D_b = \binom{a+b}{a} D_{a+b}$.

Soient $a, b \in \mathbb{N}$. Supposons le résultat vrai pour tous a', b' tels que $a' + b' < a + b$.

Posons $d = D_a \circ D_b - \binom{a+b}{a}$.

Un calcul direct montre que d est une dérivation sur K.

Or le corps des constantes de d contient A car D est une dérivation de Hasse sur A, donc il contient aussi son corps des fractions.

Donc D définit bien une dérivation de Hasse sur K.

□

Remarque. *Pour étendre une séquence de dérivations de Hasse sur A qui commutent à son corps des fractions, on montre que* $\forall i, j \in \{1, ..., e\}$, $\forall m, n \in \mathbb{N}$, $D_{i,m} \circ D_{j,n} - D_{j,n} \circ D_{i,m}$ *est une dérivation dont le corps des constantes contient A.*

Passons maintenant à l'étude de la notion de séparabilité, pour pouvoir ensuite parler de corps séparablement clos.

2 Séparabilité

2.1 Extensions séparables

Donnons tout d'abord quelques définitions.

Soit K un corps de caractéristique p. Soit K^a la clôture algébrique de K.

Définition 16. Soit $P \in K[X]$.

On dit que P est **séparable** sur K s'il n'existe pas de polynôme $Q \in K[X]$ tel que $P(X) = Q(X^p)$.

Soit A une K-algèbre. Soit $x \in A$ algébrique sur K.

On dit que x est **séparable** sur K si son polynôme minimal sur K est séparable sur K.

Proposition-définition 17. *Soit* $K^s = \{x \in K^a | x$ *est algébrique séparable sur* $K\}$.
K^s *est un sous-corps de* K^a *appelé la* ***clôture séparable*** *de* K.
On dit que K *est* ***séparablement clos*** *si* $K = K^s$.

Remarques. – *En caractéristique nulle, séparablement clos équivaut à algébriquement clos.*

– *K est séparablement clos*
$\iff$ *K n'admet pas d'extension propre algébrique séparable*
$\iff$ *Tout polynôme séparable de $K[X]$ admet une racine dans K*
$\iff$ *Tout polynôme irréductible de degré strictement plus grand que 1 de $K[X]$ est de la forme $Q(x^p)$, $Q \in K[X]$.*

Définition 18. Soit L une extension de K. Soit $x \in L$.
On dit que x est **radiciel** sur K s'il existe $r \in \mathbb{N}$ tel que $x^{p^r} \in K$.
On dit que L est **purement inséparable** ou **radicielle** si tout élément de L est radiciel sur K.

Proposition-définition 19. *Soit $K^{p^{-n}} = \{x \in K^a | x^{p^n} \in K\}$.*
Soit $K^{p^{-\infty}} = \bigcup_{n\in\mathbb{N}} K^{p^{-n}}$.
*$K^{p^{-\infty}}$ est un sous-corps de K^a appelé la **clôture parfaite** de K.*
*On dit que K est **parfait** si $K = K^{p^{-\infty}}$.*

Nous allons introduire la notion d'*indépendance linéaire* de deux extensions d'un corps, qui permettra de définir de manière concise la séparabilité.

Proposition-définition 20. *Soient F et L deux extensions de K contenues dans un même corps. On dit que F et L sont **linéairement disjointes** sur K si toute famille d'éléments de F linéairement indépendants sur K reste libre sur L.*
La définition est symétrique en F et L.

Proposition 21. *Soient F, L et E des extensions de K telles que $E \subseteq L$.*
Alors F et L sont linéairement disjointes sur K si et seulement si F et E sont linéairement disjointes sur K et FE et L sont linéairement disjointes sur E.

Démonstration. $\Rightarrow$] Supposons que F et E soient linéairement disjointes sur K et que FE et L soient linéairement disjointes sur E.
Soient (β) une K-base de F, (α) une K-base de E et (λ) une E-base de L. Alors $(\alpha\lambda)$ est une K-base de L.
Si F et L ne sont pas linéairement dijointes sur K, alors $\exists c_{\beta\lambda\alpha} \in K$ non tous nuls tels que :

$$\sum_{\lambda,\alpha} \left(\sum_{\beta} c_{\beta\lambda\alpha} \cdot \beta \right) \alpha\lambda = 0$$

donc

$$\sum_{\lambda} \left(\sum_{\beta,\alpha} c_{\beta\lambda\alpha} \cdot \beta\alpha \right) \lambda = 0$$

Or comme F et E sont linéairement disjoints sur K, $(\beta\alpha)$ est une K-base de FE.
Donc cette relation contredit l'indépendance linéaire de L et de FE sur E.
$\Leftarrow$] Raisonnement analogue. □

Proposition 22. *K^s et $K^{p^{-\infty}}$ sont linéairement disjoints sur K.*

Remarque. *On a $K^a = K^s \cdot K^{p^{-\infty}}$.*

Proposition 23. *Soit L une extension purement inséparable de K^s.*
Alors L est séparablement clos.

Pour étendre la notion de séparabilité à des extensions non algébriques, nous allons demander que l'extension et la clôture parfaite soient linéairement disjointes, et cette propriété est équivalente à un certain nombre de résultats qui utilisent la notion de p-base.

Définition 24. Soient $A, B \subseteq K$. Soit $x \in K$. On dit que x est **p-indépendant** sur A dans K si $x \notin K^p(A)$.
On dit que B est **p-libre** sur A dans K si $\forall b \in B$, b est **p-indépendant** sur $A \cup (B \setminus \{b\})$ dans K.
Si $A = \emptyset$, on dit simplement que B est **p-indépendant** ou **p-libre** dans K.
On dit que B **p-génère** K si $K \subseteq K^p(B)$.
On dit que B est une **p-base** de K si B est p-libre et p-génératrice.

Définition 25. Comme K^p est un sous-corps de K, K est un K^p-espace vectoriel, dont la dimension est une puissance de p.
On dit que K est de **degré d'imperfection** d si $[K : K^p] = p^d$.

Proposition 26. *Toutes les p-bases de K ont pour cardinal le degré d'imperfection de K.*

Proposition-définition 27. *Soit L une extension non nécessairement algébrique de K.*
Les conditions suivantes sont équivalentes :
- *$K^{p^{-1}}$ et L sont linéairement disjointes sur K.*
- *$K^{p^{-\infty}}$ et L sont linéairement disjointes sur K.*
- *Toute partie p-libre de K est p-libre dans L.*
- *Il existe une p-base de K qui est p-libre dans L.*

*Si ces conditions sont vérifiées, on dit que L est **séparable** sur K.*

Définition 28. Soit L une extension de K.
On appelle **base de transcendance** de L sur K une partie S de L algébriquement libre sur K et maximale pour l'inclusion.

Proposition-définition 29. *Soit L une extension de K de type fini.*
*Alors L est séparable sur K si et seulement s'il existe une base de transcendance (t) de L sur K telle que L soit séparable algébrique sur $K(t)$. Une telle base (t) est appelée **base de transcendance séparante** de L sur K.*

2.2 Places

Nous aurons besoin de parler de places et d'anneaux de valuation pour prouver quelques propriétés sur la régularité dans la prochaine section.

Définition 30. Un anneau commutatif est dit **local** s'il admet un unique idéal maximal.

Définition 31. Soit K un corps. Soit B un sous-anneau de K.
On dit que B est un **anneau de valuation** de $K \setminus \{0\}$ si $\forall x \in K$, $x \in B$ ou $x^{-1} \in B$.

Proposition 32. *Soit K un corps. Soit B un anneau de valuation de K.*
Alors B est un anneau local.

Définition 33. Soit F un corps.
On définit le symbole ∞ par les relations usuelles.

Définition 34. Soient K et F deux corps.
Une **place** φ de K à valeurs dans F est une application $\varphi : K \to F \cup \{\infty\}$ telle que :

$$\begin{aligned} \varphi(1) &= 1 \\ \varphi(a+b) &= \varphi(a) + \varphi(b) \\ \varphi(a \cdot b) &= \varphi(a) \cdot \varphi(b) \end{aligned}$$

dès que les expressions de droite sont définies.
On dit que φ est une **place F-valuée** de K.
Les éléments de K dont l'image par φ est ∞ sont dits **infinis** et les autres **finis**.

Proposition-définition 35. *Soit K un corps. Soit φ une place F-valuée de K.*
Soit $O = \{x \in K | \varphi(x) \neq \infty\}$.
Alors O est un anneau de valuation de K appelé l' ***anneau de valuation de*** *φ.*
Son idéal maximal est $I = \{x \in O | \varphi(x) = 0\}$.

Définition 36. Soient K, F_1 et F_2 des corps.
Soient $\varphi_1 : K \to F_1 \cup \{\infty\}$ et $\varphi_2 : K \to F_2 \cup \{\infty\}$ des places.
Quitte à considérer leurs restrictions sur leurs images, on peut les supposer surjectives.
On dit que φ_1 et φ_2 sont **équivalentes** s'il existe un isomorphisme $\lambda : F_1 \to F_2$ tel que $\varphi_2 = \lambda \circ \varphi_1$ avec la convention que $\lambda(\infty) = \infty$.

Proposition 37. *Soient K, F_1 et F_2 des corps.*
Soient $\varphi_1 : K \to F_1 \cup \{\infty\}$ et $\varphi_2 : K \to F_2 \cup \{\infty\}$ des places.
Alors φ_1 et φ_2 sont équivalentes si et seulement si elles ont le même anneau de valuation O, donc les mêmes éléments finis.

Voici une petite propriété des places qui sera bien pratique dans les preuves de la section suivante.

Proposition 38. *Soient K et L des corps.*
Soit $\varphi : K \to L \cup \{\ \infty\}$ une place L-valuée de K.
Soient $x_1, ..., x_n \in K \setminus \{\ 0\}$.
Alors il existe $j \in \{1, ..., n\}$ tel que $\forall i \in \{1, ..., n\ \}, \frac{x_i}{x_j}$ soit fini.

Démonstration. Soit O l'anneau de valuation de φ.
$\forall i, j \in \{1, .., n\ \}$, on a $\frac{x_i}{x_j} \in O$ ou $\frac{x_j}{x_i} \in O$.
On définit alors le préordre suivant sur $\{x_1, .., x_n\ \} : x_i \leq x_j$ si et seulement si $\frac{x_i}{x_j} \in O$.
On a donc, $\forall i, j \in \{1, ..., n\}$, $x_i \leq x_j$ ou $x_j \leq x_i$.
On peut donc "ordonner" ces éléments.
Soit x_j le plus grand élément pour l'ordre choisi. Alors j est l'indice cherché. □

Donnons maintenant une condition suffisante pour qu'une place soit un isomorphisme.

Remarque. *Soient K un corps et L une extension de K.*
Soit $x \in L$.
Soit φ une place de L.
Si x est algébrique (ou de manière équivalente, entier) sur K, et si φ est finie sur K, alors φ est finie sur $K(x)$.

En effet, soit $x^n + a_{n-1} \cdot x^{n-1} + ... + a_0 = 0$ la relation de dépendance intégrale de x sur K.
Alors $\varphi(x^n + a_{n-1} \cdot x^{n-1} + ... + a_0) = 0$ et $\varphi(x \cdot (x^{n-1} + a_{n-1} \cdot x^{n-2} + ... + a_1)) + \varphi(a_0) = 0$.
Si $\varphi(x^{n-1} + a_{n-1} \cdot x^{n-2} + ... + a_1) = 0$, alors on recommence sur cette expression.
Sinon, on a $\varphi(x) \cdot \varphi(x^{n-1} + a_{n-1} \cdot x^{n-2} + ... + a_1) + \varphi(a_0) = 0$ donc $\varphi(x)$ est fini.
De plus, si $x \neq 0$, on a $a_0 \neq 0$ et donc $\varphi(x) \neq 0$ d'après l'équation.
Donc φ est un isomorphisme de $K(x)$ sur son image.

2.3 Extensions régulières

Parler de séparabilité nous amène naturellement à parler de régularité, une propriété très puissante dont nous nous servirons dans la suite.

Définition 39. Soient k un corps et K une extension de k.
On dit que k est **algébriquement fermé** dans K si tout élément de K algébrique sur k est dans k.
On dit que K est une extension **régulière** de k si K est séparable sur k et k est algébriquement fermé dans K.

Présentons une caractérisation équivalente de la régularité :

Proposition 40. *Soient k un corps et K une extension de k.*
Soit k^a la clôture algébrique de k.
Si K et k^a sont linéairement disjointes sur k, alors K est une extension régulière de k.

Démonstration. K est linéairement disjointe de k^a donc en particulier de $k^{p^{-\infty}}$. Donc K est séparable sur k.

Soit $x \in K$ algébrique sur k.
$x \in k^a$.
Or $K \cap k^a = k$ donc $x \in k$. Donc k est algébriquement fermé dans K.

□

Lemme 41. *Soient k un corps et K une extension de k telle que k soit algébriquement fermé dans K.*
Soit L une extension de K.
Soit $x \in L$ algébrique sur k. Alors K et $k(x)$ sont linéairement disjointes sur k.

Démonstration. Soit μ le polynôme minimal de x sur k. μ est irréductible sur k.
Dans k^a, $\mu(X) = \prod_{y \in Rac(\mu)} (X - y)^{m_y}$.
Chaque $y \in Rac(\mu)$ est algébrique sur k par définition.
Supposons que μ soit réductible sur K. Alors les coefficients des facteurs sont algébriques sur k, donc dans k, ce qui est absurde.
Donc μ est aussi irréductible sur K donc est aussi le polynôme minimal de x sur K.

Soit r le degré de μ.
Alors $(1, x, ..., x^{r-1})$ forme une base de $k(x)$ sur k, et aussi une base de $K(x)$ sur K.
Donc $[K(x) : K] = [k(x) : k]$.

Soient $x_1, ..., x_n$ des éléments de $k(x)$ linéairement indépendants sur k. Supposons qu'ils soient liés sur K : $\exists (a_1, ..., a_n) \in K^n \setminus \{0\}$ tels que $\sum_{i=1}^n a_i \cdot x_i = 0$.
Or $x_i \in k(x)$ donc $\exists \alpha_{ij} \in k$ tq $x_i = \sum_{j=0}^{r-1} \alpha_{ij} \cdot x^j$.

Donc $\sum_{i=1}^{n}\sum_{j=0}^{r-1} a_i \cdot \alpha_{ij} \cdot x^j = 0$ ie $\sum_{j=0}^{r-1}(\underbrace{\sum_{i=1}^{n} a_i \cdot \alpha_{ij}}_{\in K})x^j = 0$.

Donc $(1, x, ..., x^{r-1})$ est liée sur K. Widerspruch ! Donc K et $k(x)$ sont linéairement disjointes sur k.

□

Proposition 42. *Soient k un corps et K une extension régulière de k.*
Alors K et k^a sont linéairement disjointes sur k.

Démonstration. Par le théorème de compacité, on peut supposer que K est de type fini sur k, et il suffit de montrer que K est linéairement disjointe de toute extension algébrique finie L de k.

Traitons d'abord le cas où L est séparable sur k.
Par le théorème de l'élément primitif, L est engendrée par un élément x algébrique sur k.
Alors d'après le lemme 41, K et $L = k(x)$ sont linéairement disjointes sur k.

Revenons au cas général.
Soit $E \subseteq L$ la sous-extension séparable maximale de k dans L. D'après le cas séparable, K et E sont linéairement disjointes sur sur k.
D'après la proposition 21, il suffit de montrer que KE et L sont linéairement disjointes sur E.
Soit (t) une base de transcendance séparante de K sur k. Alors (t) est aussi une base de transcendance de KE sur E. En effet, comme K et E sont linéairement disjointes sur k, elles sont aussi algébriquement disjointes et donc (t) reste algébriquement libre sur E. De plus, KE est algébrique sur $E(t)$ par construction, et $K \subseteq (k(t))^s$ donc $KE \subseteq (k(t))^s E \subseteq (E(t))^s$, donc KE est séparable algébrique sur $E(t)$. Donc KE est séparable sur E par la proposition 29. Or par définition de E, L est inséparable sur E. Comme les les clôtures séparables et inséparables de E sont linéairement disjointes sur E , d'après la proposition 22, KE et L sont bine linéairement disjointes sur E.

□

Montrons enfin une propriété très intéressante, qui est l'équivalence des notions d'indépendances linéaire et algébrique de deux extensions dont l'une est régulière.

Proposition 43. *Soient k un corps et K une extension régulière de k.*
Soit L une extension de k.
Supposons que K et L soient contenues dans un même corps.
Si K et L sont algébriquement disjointes sur k, alors elles sont linéairement disjointes sur k.

Démonstration. D'après le théorème de compacité, on peut supposer que K est de type fini sur k.
Soient $x_1, ..., x_n$ des éléments de K linéairement indépendants sur k. Supposons qu'ils soient liés sur L : $\exists y_1, ..., y_n \in L$ tq $x_1 \cdot y_1 + ... + x_n \cdot y_n = 0$.

Soit $\varphi : L \to k^a \cup \{\infty\}$ une place k^a-valuée de L, k-linéaire.
Soit (t) une base de transcendance de K sur k.
Comme K et L sont algébriquement indépendants sur k, (t) reste algébriquement libre sur L.
On peut donc étendre φ à KL en définissant φ sur (t) :
posons $\varphi_{|k(t)} = Id_{|k(t)}$.
Pour avoir les valeurs de φ sur tout K, on prend un élément $x \in K \setminus k(t)$: par définition, il est algébrique sur $k(t)$. $\exists a_0, ..., a_m \in k(t)$ tq $a_m \cdot x^m + ... + a_0 = 0$.
On veut $a_m \cdot \varphi(x)^m + ... + a_0 = 0$ et on choisit dans K^a un $\varphi(x)$ qui convient.

K est une extension algébrique de $k(t)$ sur lequel φ est finie.
Donc d'après la remarque précédente, $\varphi_{|K}$ doit être un isomorphisme de K sur son image.

Soit $\lambda = (\varphi_{|K})^{-1}$.
Posons $\tilde{\lambda} : K^a \cup \{\infty\} \to K^a \cup \{\infty\}$ telle que $\tilde{\lambda} = \lambda$ sur $\varphi_{|K}(K)$ et $\tilde{\lambda} = Id$ ailleurs.
Soit $\psi = \tilde{\lambda} \circ \varphi_{|K}$.
Alors $\psi_{|K} = Id_K$.
ψ reste une place K^a-valuée de L, et comme $\tilde{\lambda}$ est un isomorphisme, ψ est équivalente à φ.

D'après la proposition 38, quitte à renuméroter les y_i, on peut supposer que $\forall i \in \{1, ..., n\}$, $\psi(\frac{y_i}{y_n})$ est fini.
En divisant par y_n la relation de dépendance linéaire des x_i sur L, puis en appliquant ψ, on obtient : $\sum_{i=1}^{n} \underbrace{\psi(x_i)}_{=x_i \ car \ x_i \in K} \cdot \psi(\frac{y_i}{y_n}) = 0$ et donc $\sum_{i=1}^{n} x_i \cdot \underbrace{\psi(\frac{y_i}{y_n})}_{\in k^a} = 0$.
Cette relation contredit l'indépendance linéaire de K et de k^a.
Donc finalement K et L sont linéairement disjointes sur k.

□

Exposons maintenant quelques-uns des outils de base de la théorie des modèles.

3 Modèles

La notion de morphisme permet de comparer les structures associées à un langage, de définir une relation d'ordre entre les modèles d'une théorie.

Définition 44. Soient $\mathcal{L}$ un langage, $\mathcal{M}$ et $\mathcal{N}$ deux $\mathcal{L}$-structures.
Un **$\mathcal{L}$-morphisme** de $\mathcal{M}$ dans $\mathcal{N}$ est une fonction $s : M \to N$ telle que :
- Pour tout symbole de relation R de $\mathcal{L}$, pour tout $\overline{a} \in M^{n(R)}$, si $\overline{a} \in R^{\mathcal{M}}$ alors $s(\overline{a}) \in R^{\mathcal{N}}$.
- pour tout symbole de fonction f, pour tout $\overline{b} \in M^{n(f)}$, $s(f(\overline{b})) = f(s(\overline{b}))$.

Un $\mathcal{L}$-morphisme $s : \mathcal{M} \to \mathcal{N}$ est un **$\mathcal{L}$-plongement** s'il est injectif et qui vérifie pour tout $R \in \mathcal{L}$ et pour tout $\overline{a} \in M^{n(R)}$, $\overline{a} \in R^{\mathcal{M}} \iff s(\overline{a}) \in R^{\mathcal{N}}$.

Définition 45. Soient $\mathcal{L}$ un langage, $\mathcal{M}$ et $\mathcal{N}$ deux $\mathcal{L}$-structures.
Un $\mathcal{L}$-plongement $j : \mathcal{M} \to \mathcal{N}$ est appelé un **$\mathcal{L}$-plongement élémentaire** si pour toutes les formules $\varphi(x_1, ..., x_n)$ de $\mathcal{L}$, et pour tous les $a_1, ..., a_n \in M$, on a :

$$\mathcal{M} \vDash \varphi(a_1, ..., a_n) \iff \mathcal{N} \vDash \varphi(j(a_1), ..., j(a_n))$$

Si $\mathcal{M}$ est une sous-structure de $\mathcal{N}$, on dit que $\mathcal{N}$ est une **extension élémentaire** de $\mathcal{M}$ si l'inclusion est un $\mathcal{L}$-plongement élémentaire. On note alors $\mathcal{M} \preccurlyeq \mathcal{N}$.

On peut prendre le contrepied de ce qu'on vient de faire, et s'intéresser aux formules satisfaites dans une structure donnée.

Définition 46. Soient $\mathcal{L}$ un langage et $\mathcal{M}$ une $\mathcal{L}$-structure.
Soit $\mathcal{L}_M = \mathcal{L} \cup \{m | m \in M\}$.
Soit $(\mathcal{M}, m)_{m \in M}$ la $\mathcal{L}_M$-structure obtenue à partir de $\mathcal{M}$ en interprétant les éléments de M de manière naturelle. Le **diagramme élémentaire** de $\mathcal{M}$ est :

$$Diag_{el}(\mathcal{M}) = \{\varphi(m_1, ..., m_n) | (\mathcal{M}, m)_{m \in M} \vDash \varphi(m_1, ..., m_n), \varphi \ une \ \mathcal{L}_M\text{-}formule\}$$

Définition 47. Soient $\mathcal{L}$ un langage et $\mathcal{M}$ une $\mathcal{L}$-structure.
Soit $A \subseteq M$.
Soit $\mathcal{L}_A = \mathcal{L} \cup \{a | a \in A\}$.
$(\mathcal{M}, a)_{a \in A}$ est une $\mathcal{L}_A$-structure.
Soit $Th_A(\mathcal{M}) = \{\varphi | \varphi \text{ une formule close sur } \mathcal{L}_A \text{ et } (\mathcal{M}, a)_{a \in A} \vDash \varphi\}$.
On a $Th_A(\mathcal{M}) \subseteq Diag_{el}(\mathcal{M})$.
Soit P un ensemble de formules sur $\mathcal{L}_A$ de variables libres $v_1, ..., v_n$.
On dit que P est un **n-type** si $P \cup Th_A(\mathcal{M})$ est satisfiable.

La proposition suivante assure l'existence , pour un type donné, d'un modèle qui réalise ce type.

Proposition 48. *Soient $\mathcal{L}$ un langage et $\mathcal{M}$ une $\mathcal{L}$-structure.*
Soit $A \subseteq M$.
Soit P un n-type sur A.
Alors il existe une extension élémentaire $\mathcal{N}$ de $\mathcal{M}$ qui réalise P.

Démonstration. Soit $\Gamma = P \cup Diag_{el}(\mathcal{M})$.
Montrons que Γ est satisfiable.
Par le théorème de compacité, il suffit de montrer que tout ensemble fini Δ de formules de Γ est satisfiable.
On peut supposer que Δ est de la forme :

$$\{\varphi(v_1, ..., v_n, a_1, ..., a_m) \wedge \psi(a_1, ..., a_m, b_1, ..., b_l)\}$$

où $a_1, ..., a_m \in A$, $b_1, ..., b_l \in M \setminus A$, $\varphi(\overline{v}, \overline{a}) \in P$ et $\mathcal{M} \vDash \psi(\overline{a}, \overline{b})$.

Comme P est un n-type, $P \cup Th_A(\mathcal{M})$ est satisfiable par une $\mathcal{L}_A$-structure $\mathcal{N}_0$.
La formule $\exists \overline{w}, \psi(\overline{a}, \overline{w}) \in Th_A(\mathcal{M})$ car $\mathcal{M} \vDash \psi(\overline{a}, \overline{b})$.
Donc $\mathcal{N}_0 \vDash \varphi(\overline{v}, \overline{a}) \wedge \exists \overline{w}, \psi(\overline{a}, \overline{w})$.
Alors $\mathcal{N}_0 \vDash \Delta$.

Γ est donc satisfiable.
Soit $\mathcal{N}$ telle que $\mathcal{N} \vDash \Gamma$.
En particulier, on a $\mathcal{N} \vDash Diag_{el}(\mathcal{M})$.
Soit $\begin{array}{ccccc} j & : & M & \to & N \\ & & m & \mapsto & m^{\mathcal{N}} \end{array}$.
j est un $\mathcal{L}$-plongement.
Si $\mathcal{M} \vDash \varphi(a_1, ..., a_n)$, alors $\mathcal{N} \vDash \varphi(j(a_1), ..., j(a_n))$, $\forall a_1, ..., a_n \in M$.
Et si $\mathcal{M} \nvDash \varphi(a_1, ..., a_n)$, alors $\mathcal{M} \vDash \neg\varphi(a_1, ..., a_n)$, donc $\mathcal{N} \vDash \neg\varphi(j(a_1), ..., j(a_n))$ et $\mathcal{N} \nvDash \varphi(j(a_1), ..., j(a_n))$, $\forall a_1, ..., a_n \in M$.
Donc j est un plongement élémentaire.
$\mathcal{N}$ est donc une extension élémentaire de $\mathcal{M}$ qui réalise P.

□

Une propriété qui revient très souvent en théorie des modèles et dont nous avons besoin pour continuer notre étude des extensions séparables est la saturation d'un modèle relativement à un cardinal. Avec les mains, un modèle est saturé relativement à un cardinal donné s'il réalise tout ensemble de formules dont le cardinal est inférieur à notre cardinal de départ. Plus précisément :

Définition 49. Soient $\mathcal{L}$ un langage et T une $\mathcal{L}$-théorie.
Soit $\mathcal{M}$ un modèle de T.

Soit α un cardinal.
On dit que $\mathcal{M}$ est α-**saturé** si, pour tout $A \subseteq M$, si $|A| < \alpha$, et si P est un n-type sur A, alors $\mathcal{M}$ réalise P.

On peut toujours toujours trouver un tel modèle, pourvu qu'on ait déjà un modèle de cardinal inférieur.

Proposition 50. *Soient $\mathcal{L}$ un langage et T une $\mathcal{L}$-théorie.*
Soit $\mathcal{M}$ un modèle de T de cardinal α.
Alors il existe une extension élémentaire $\mathcal{N}$ de $\mathcal{M}$ qui est α^+-saturée.

Démonstration. Construisons une chaîne d'extensions élémentaires de $\mathcal{M}$ ainsi :
- $\mathcal{N}_0 = \mathcal{M}$
- $\forall \beta < 2^\alpha$, prenons, par la proposition 48, $\mathcal{N}_{\beta+1} \succcurlyeq \mathcal{N}_\beta$ telle que $(\mathcal{N}_{\beta+1}, a)_{a\in X}$ réalise tous les types sur $(\mathcal{N}_\beta, a)_{a\in X}$ pour $X \subseteq N_\beta$ de cardinal α.
- Si β est un ordinal limite, $\mathcal{N}_\beta = \bigcup_{\gamma<\beta} \mathcal{N}_\gamma$.

Posons $\mathcal{N} = \bigcup_{\beta<2^\alpha}$.
$\mathcal{N}$ est une extension élémentaire de $\mathcal{M}$ par transitivité de $\preccurlyeq$. Et par construction, $\mathcal{N}$ est α^+-saturé. □

Appliquons enfin ces outils de théorie des modèles aux extensions séparables en exposant un résultat qui stipule l'existence d'un plongement d'une extension séparable dans une extension élémentaire, relativement à la théorie des corps séparablement clos de caractéristique p et de degré d'imperfection e.

Proposition 51. *Soit K un corps de caractéristique p et de degré d'imperfection e.*
Soit L une extension séparable de K.
Alors il existe un K-plongement de L dans une extension élémentaire de K.

Démonstration. D'après le théorème de compacité, il suffit de montrer le résultat pour L finiment engendrée sur K.

Soit $(l_1, ..., l_n)$ une base de transcendance séparante de L sur K.

Soit K^* une extension élémentaire $|K|^+$-saturée de K.
On peut traduire l'existence d'un élément transcendant sur K par un type sur le langage $\mathcal{L}_K = \{0, 1, +, -, \cdot\} \cup \{a | a \in K\}$.
Comme K^* est $|K|^+$-saturée, elle réalise ce type.
Soit x_0 un élément de K^* transcendant sur K.
On exprime l'existence d'un élément transcendant sur $K(x_0)$ par un type sur $\mathcal{L}_K \cup \{x_0\}$. On obtient ainsi x_1. Et ainsi de suite.
On obtient ainsi une suite $(x_n)_{n\in\mathbb{N}}$ algébriquement libre sur K.
Donc K^* a un degré de transcendance infini sur K.

On a un K-isomorphisme entre les algèbres de polynômes $K(l_1, ..., l_n)$ et $K(x_1, ..., x_n)$ donc $K(l_1, ..., l_n) \simeq_K K(x_1, ..., x_n) \subseteq K^*$. Donc $K(l_1, ..., l_n) \hookrightarrow_K K^*$.

Or K^* est séparablement clos donc $(K^*)^s = K^*$.
Donc $K(l_1, ..., l_n)^s \hookrightarrow_K (K^*)^s = K^*$.
Et comme $L \subseteq K(l_1, ..., l_n)^s$ par définition, $L \hookrightarrow_K K^*$.

□

4 Amalgamation

L'objectif de cette partie est de montrer que les D-corps ont la propriété d'amalgamation :

Propriété d'amalgamation. *Soit (K, D) un D-corps.*
Deux D-extensions quelconques de (K, D) peuvent être D-plongées dans une même troisième D-extension de K.

Nous allons pour cela montrer une série de lemmes nous serviront dans la preuve et plus loin.Commençons par présenter un résultat d'indépendance linéaire.

Lemme 52. *Soit (K, D) un D-corps de corps des constantes C.*
Soit (K', D') une D-extension de (K, D) de corps des constantes C'. Alors :

- $[K : C] \leq p^e$.
- *K et C' sont linéairement dijointes sur C.*

Démonstration. Pour tout $i \in \{1, ..., e\}$, posons $d_i = D_{i,1}$ et $C_i = \{ x \in K | d_i(x) = 0 \}$.
On a $C = \bigcap_{i=1}^{e} C_i$.
Quitte à réordonner les dérivations, on peut supposer que $C = \bigcap_{i=1}^{f} C_i$, avec $f \leq e$.
Posons $B_i = \bigcap_{k=1}^{i} C_k$ et $B_0 = K$.
On a $B_{i+1} \subseteq B_i$ et $C = B_f \subseteq ... \subseteq B_0 = K$.
Soit $i \in \{1, ..., e\}$.
On a $d_i^2 = D_{i,1} \circ D_{i,1} = 2 \cdot D_{i,2}$ donc $d_i^p = p! \cdot D_{i,p} = 0$.
Soient $i \in \{1, ..., e\}$, $x \in B_{i-1}$ et $k \in \{ 1, ..., i-1\}$.
Alors

$$\begin{aligned} d_k(d_i(x)) &= d_i(d_k(x)) \text{ car les } d_j \text{ commutent} \\ &= d_i(0) \text{ car } x \in B_{i-1} \subseteq C_k \\ &= 0 \end{aligned}$$

Donc $d_i(x) \in C_k$.
Donc $d_i(B_{i-1}) \subseteq B_{i-1}$.
On cherche $x_i \in B_{i-1}$ tel que $d_i(x_i) = 1$.
Si tous les d_i sont nuls, alors $C = K$ et la proposition est évidente.
Sinon, on peut supposer que $\forall i \leq f$, $d_i \not\equiv 0$.
$\exists x \in K, d_i(x) \neq 0$.
Soit $m \in \mathbb{N}$ le plus petit entier tel que $d_i^m(x) = 0$.
Posons $x_i = d_i^{m-2}(x) \cdot (d_i^{m-1}(x))^{-1}$.

$$d_i(x_i) = \underbrace{d_i^{m-1}(x) \cdot (d_i^{m-1}(x))^{-1}}_{=1} + d_i^{m-2}(x) \cdot d_i((d_i^{m-1}(x))^{-1})$$

Or

$$\begin{aligned} d_i((d_i^{m-1}(x))^{-1} \cdot d_i^{m-1}(x)) &= d(1) \\ &= 0 \\ &= d_i((d_i^{m-1}(x))^{-1}) \cdot d_i^{m-1}(x) + \underbrace{d_i^m(x) \cdot (d_i^{m-1}(x))^{-1}}_{=0} \end{aligned}$$

Donc $d_i((d_i^{m-1}(x))^{-1}) = 0$.
Alors $d_i(x_i) = 1$.

On peut appliquer le proposition 3 à $A = B_{i-1}$ muni de d_i qui est une dérivation sur A.
On a $A_0 = B_i$.
Alors $(1, x_i, ..., x_i^{p-1})$ est une B_i-base de B_{i-1}.
D'où $[K : C] \leq p^f \leq p^e$.

Une base de K sur C est donc $\{x_1^{e_1} \cdot ... \cdot x_f^{e_f} | e_i < p\}$.
On peut faire la même chose sur $K' : C' \subseteq B'_f \subseteq ... \subseteq B'_0 = K'$.
Comme les d'_i prolongent les d_i, on a $B_i \subseteq B'_i$.
On peut donc choisir les mêmes x_i tels que $d'_i(x_i) = d_i(x_i) = 1$.
Alors $\{x_1^{e_1} \cdot ... \cdot x_f^{e_f} | e_i < p\}$ forme une base de K' sur B'_f.
Comme $C' \subseteq B'_f$, les $x_1^{e_1} \cdot ... \cdot x_f^{e_f}$ sont linéairement indépendants sur C'.
Alors K et C' sont linéairement disjointes sur C.

□

Appliquons ce résultat à des D-corps stricts :

Corollaire 53. *Soient (K, D) un D-corps strict et (F, D') une D-extension de (K, D).*
Alors F est une extension séparable de K.
De plus, si $[K : K^p] = p^e$, alors (F, D') est strict si et seulement si K et F ont une p-base commune.

Démonstration. Soit C le corps des constantes de F.
D'après le lemme 52, C et K sont linéairement disjointes sur K^p, le corps des constantes de K (K est strict).
Comme $F^p \subseteq C$, K et F^p sont linéairement disjointes sur K^p.

Montrons que $K^{p^{-1}}$ et F sont linéairement disjointes sur K : soient $a_1, ..., a_n$ des éléments de $K^{p^{-1}}$ linéairement indépendants sur K.
S'il existe $\alpha_i \in F$ tels que $\sum_{i=1}^n \alpha_i \cdot a_i = 0$, alors Frobenius donne $\sum_{i=1}^n \alpha_i^p \cdot a_i^p = 0$.
Or les a_i^p sont linéairement indépendants sur K^p donc sur F^p d'après ce qui précède. Donc $\forall i, \alpha_i^p = 0$ et $\alpha_i = 0$ car F est intègre.
Alors $K^{p^{-1}}$ et F sont linéairement disjointes sur K, et donc F est une extension séparable de K.

D'après le lemme 52, on a $[F : C] \leq p^e$.
De plus, soit B une base de K sur K^p.
Comme K et C sont linéairement disjointes sur K^p, B est libre dans C et donc $card(B) \leq [F : C]$.
Alors $[K : K^p] \leq [F : C] \leq p^e$.

Si $[K : K^p] = p^e$, alors $[F : C] = p^e$.
Alors (F, D') est strict si et seulement si $C = F^p$, si et seulement si $[F : F^p] = p^e$.

Comme F est séparable sur K, il existe une p-base B de K qui est p-libre dans F.
On a $[K : K^p] = p^{|B|} = p^e$ et $[F : F^p] = p^{\textit{cardinal d'une p-base de } F}$. (F, D') est strict si et seulement si B est une famille p-libre de cardinal maximal, c'est-à-dire si B est une p-base de F.

□

Essayons maintenant d'étendre la structure différentielle d'un D-corps à une de ses extensions de corps :

Lemme 54. *Soient (K, D) un D-corps et F une extension de corps de K.*
On suppose que K et F ont une p-base commune.
Alors D s'étend de manière unique en une famille de dérivations de Hasse sur F qui commutent.

Démonstration. Traitons tout d'abord le cas d'un corps muni d'une seule dérivation de Hasse D.

Posons $E_0 = Id_F$.
Soit B une p-base commune à K et F.
Soit $x \in F$. x s'écrit de manière unique comme : $x = \sum_{i=1}^{m} x_i^p \cdot m_i$, avec $m_i = \prod_{j=1}^{n_i} b_j^{e_i(j)}$, $b_j \in B$ et $x_i \in F$.
Si on a construit $(E_0, ..., E_n)$, construisons E_{n+1} : $n+1 = p \cdot q + r$, $r < p$.
Si E_{n+1} existe, d'après le corollaire 10, E_{n+1} vérifie nécessairement :

$$\begin{aligned} E_{n+1}(x) &= \sum_{i=1}^{m} E_{n+1}(x^p \cdot m_i) \\ &= \sum_{i=1}^{m} E_{p\cdot q+r}(x^p \cdot m_i) \\ &= \sum_{i=1}^{m} \sum_{k \leq q} E_k(x_i)^p \cdot E_{p\cdot(q-k)+r}(m_i) \\ &= \sum_{i=1}^{m} \sum_{k \leq q} E_k(x_i)^p \cdot D_{p\cdot(q-k)+r}(m_i) \end{aligned}$$

Comme E_k est bien définie, on peut définir E_{n+1} par cette dernière égalité.
Donc on a bien construit le seul prolongement possible de D.

Revenons au cas général : $D = (D_1, ..., D_e)$.
Chaque D_i s'étend de manière unique à F en E_i. Pour montrer que $E = (E_1, ..., E_e)$ est bien une extension de D, il suffit de montrer que les E_i commutent. On va montrer que E_1 et E_2 commutent, ie que $E_{1,i} \circ E_{2,j} = E_{2,j} \circ E_{1,i}$, par récurrence sur $i+j$. Supposons qu'on ait $E_{1,i} \circ E_{2,j} = E_{2,j} \circ E_{1,i}$ pour tous i, j tels que $i + j < m + n$.

Montrons que $d = E_{1,m} \circ E_{2,n} - E_{2,n} \circ E_{1,m}$ est une dérivation.
Elle est linéaire. De plus, soient $x, y \in F$. Alors :

$$\begin{aligned} d(x \cdot y) &= E_{1,m} \circ E_{2,n}(x \cdot y) - E_{2,n} \circ E_{1,m}(x \cdot y) \\ &= E_{1,m}\Big(\sum_{a+b=n} E_{2,a}(x) \cdot E_{2,b}(y)\Big) - E_{2,n}\Big(\sum_{c+d=m} E_{1,c}(x) \cdot E_{1,d}(y)\Big) \\ &= \sum_{a+b=n} E_{1,m}(E_{2,a}(x) \cdot E_{2,b}(y)) - \sum_{c+d=m} E_{2,n}(E_{1,c}(x) \cdot E_{1,d}(y)) \\ &= \sum_{a+b=n} \sum_{c+d=m} E_{1,c}(E_{2,a}(x)) \cdot E_{1,d}(E_{2,b}(y)) - \sum_{c+d=m} \sum_{a+b=n} E_{2,a}(E_{1,c}(x)) \cdot E_{2,b}(E_{1,d}(y)) \\ &= d(x) \cdot y + x \cdot d(y) \text{ } \textit{par hypothèse de récurrence} \end{aligned}$$

Sur K, d est nulle puisque les $E_{i,j}$ prolongent les $D_{i,j}$ qui commutent.
Soit $C_d = \{x \in F | d(x) = 0\}$ le corps des constantes de d.
On a $K \subseteq C_d$.

Soit B une p-base commune à K et F.
Comme $B \subseteq K \subseteq C_d$, $F^p \subseteq C_d$ et $F \subseteq F^p(B)$, et que C_d est un corps, on a $F \subseteq C_d$, c'est-à-dire que les dérivations de Hasse commutent.

□

Montrons que chaque D-corps admet une extension stricte.

Lemme 55. *Soit (K, D^K) un D-corps.*
Alors (K, D^K) admet une plus petite extension stricte $(K^{stricte}, D^{stricte})$, qui est une extension purement inséparable de K.

Démonstration. Soit D une dérivation de Hasse quelconque sur un corps K'. Pour tout entier n, posons $D'_n = D_{p \cdot n}$.
Montrons que $D' = (D'_0, D'_1, ...)$ est une dérivation de Hasse sur le corps C des constantes de (K', D).
Soient $x, y \in C$.

$$\begin{aligned} D'_n(x \cdot y) &= D_{p \cdot n}(x \cdot y) \\ &= \sum_{a+b=p \cdot n} D_a(x) \cdot D_b(y) \\ &= \sum_{a+b=n} D_{p \cdot a}(x) \cdot D_{p \cdot b}(y) \text{ car si l'un des indices n'est pas divisible par p, le terme est nul} \\ &= \sum_{a+b=n} D'_a(x) \cdot D'_b(y) \end{aligned}$$

Et $D'_a \circ D'_b = \begin{pmatrix} p \cdot (a+b) \\ p \cdot a \end{pmatrix} D_{p \cdot (a+b)} = \begin{pmatrix} a+b \\ a \end{pmatrix} D'_{a+b}$.

On construit par récurrence une suite $(K_i)_{i \in \mathbb{N}}$ croissante de D-corps.
Posons tout d'abord $K_0 = K$, puis supposons qu'on ait construit (K_i, D), de corps de constantes C.
Comme les D_k commutent, tous les $D_{k,n}$ envoient C dans lui-même.
Posons $D' = (D'_1, ..., D'_e)$. Ce sont des dérivations de Hasse d'après ce qui précède. Elles commutent puisque $D_1, ..., D_e$ commutent.
Posons $K_{i+1} = C^{\frac{1}{p}}$.
Comme $K_i^p \subseteq C$, on a bien $K_i \subseteq C^{\frac{1}{p}} = K_{i+1}$.

Pour $x \in K_{i+1}$, posons $D^*_{k,n}(x) = (D'_{k,n}(x^p))^{\frac{1}{p}}$.
Si $x \in K_i$, alors $D^*_{k,n}(x) = (D_{k,p \cdot n}(x^p))^{\frac{1}{p}} = ((D_{k,n}(x))^p)^{\frac{1}{p}} = D_{k,n}(x)$.
Donc D^* est bien une dérivation de Hasse qui prolonge D.

Posons maintenant $K^{stricte} = \bigcup_{i \in \mathbb{N}} K_i$.
Chaque extension $K_i \subseteq K_{i+1}$ est purement inséparable par définition. Donc $K^{stricte}$ est une extension purement inséparable de K.

Soit $C^{stricte} = \bigcup_{i \in \mathbb{N}} C_i$ le corps des constantes de $K^{stricte}$ et $x \in C^{stricte}$.Il existe n tel que $x \in C_n$. Soit $y = x^{\frac{1}{p}}$.
Alors $y \in C_n^{\frac{1}{p}} = K_{n+1} \subseteq K^{stricte}$.
Donc $x = y^p \in (K^{stricte})^p$.
D'où $C^{stricte} \subseteq (K^{stricte})^p$. Comme on a déjà $(K^{stricte})^p \subseteq C^{stricte}$, on obtient que $K^{stricte}$ est un D-corps strict.

Soit F une extension stricte de K.
Soit C le corps des constantes de K.
Alors $C \subseteq F^p$ donc $C^{\frac{1}{p}} \subseteq (F^p)^{\frac{1}{p}} = F$.

En réitérant ce processus, on obtient $K^{stricte} \subseteq F$.
Donc $K^{stricte}$ est bien la plus petite extension stricte de K.

□

Trouvons maintenant une manière d'étendre les D-structures de deux extensions linéairement disjointes d'un même corps.

Lemme 56. *Soit (K, D^K) un D-corps.*
Soient (F, D) et (L, D') des D-extensions de (K, D^K).
Supposons que dans une extension commune, F et L soient linéairement disjointes sur K.
Alors FL a une unique D-structure qui étend celles de F et de L.

Démonstration. FL est isomorphe au corps des fractions de $F \otimes_K L$. Donc, d'après la proposition 14, on peut munir FL d'une D-structure qui prolonge celles de F et de L. □

Armés de ces lemmes puissants, nous pouvons enfin nous attaquer à la preuve de la propriété d'amalgamation des D-corps.

Démonstration. (**de la propriété d'amalgamation**) Soit (K, D) un D-corps.
Soient (F, D_F) et (L, D_L) des D-extensions de (K, D).

Considérons F^s la clôture séparable de F.
Soit B une p-base de F.
On a $F(F^s)^p \subseteq F^s$ et $F(F^s)^p = (F^s)^p[F] = (F^s)^p[F^p[B]] = (F^s)^p[B]$.
Donc $(F^s)^p[B] \subseteq F^s$.
De plus, l'extension $F(F^s)^p[B] \subseteq F^s$ est purement inséparable car $(F(F^s)^p)^{\frac{1}{p}} = F^{\frac{1}{p}}F^s \supseteq F^s$.
Or l'extension $F \subseteq F^s$ est séparable donc l'extension $F(F^s)^p \subseteq F^s$ est séparable aussi.
Alors $F^s = F(F^s)^p = (F^s)^p[B]$.
Donc F et F^s ont une p-base commune B.
D'après le lemme 54, on peut étendre D_F à F^s.
On fait de même pour L.

Considérons l'extension $F^s \subseteq (F^s)^{stricte}$.
D'après le lemme 55, on peut étendre D_{F^s} à $(F^s)^{stricte}$.
Comme l'extension $F^s \subseteq (F^s)^{stricte}$ est purement inséparable, d'après 55, $(F^s)^{stricte}$ reste séparablement clos.
On fait de même pour L.

K^s est la plus petite extension séparable de K.
On a donc

$$(F^s)^{stricte} \quad (L^s)^{stricte}$$

$$K^s$$

$$K$$

D'après le lemme 54, on peut étendre D à K^s, et (K^s, D_{K^s}) est un D-sous-corps de $(F^s)^{stricte}$ et de $(L^s)^{stricte}$.

De même, d'après le lemme 55, on peut étendre D_{K^s} à $(K^s)^{stricte}$, avec $((K^s)^{stricte}, D_{(K^s)^{stricte}})$ qui est un D-sous-corps de $(F^s)^{stricte}$ et de $(L^s)^{stricte}$.

$$(F^s)^{stricte} \quad (L^s)^{stricte}$$

$$(K^s)^{stricte}$$

Soit E une extension de corps de K, de base de transcendance (t) sur K.
Alors E est K-isomorphe à $Frac(K(t))$.
Donc tout autre extension de K de même degré de transcendance sur K est K-isomorphe à E.
A K-isomorphisme près, pour tout cardinal α, il existe une unique extension de K de degré de transcencdance α sur K. Ce corps contient toutes les extensions de K de degré de transcendance $< \alpha$.
On peut donc supposer que $(F^s)^{stricte}$ et $(L^s)^{stricte}$ sont contenues dans un même corps.

On écrit que $(F^s)^{stricte} = (K^s)^{stricte}(t)$ et que $(L^s)^{stricte} = (K^s)^{stricte}(t')$.
Quitte à renommer (t) et (t'), on peut supposer que $(F^s)^{stricte}$ et $(L^s)^{stricte}$ sont algébriquement indépendantes sur $(K^s)^{stricte}$.

D'après le corollaire 53, comme $((K^s)^{stricte}, D_{(K^s)^{stricte}})$ est strict, $(F^s)^{stricte}$ est une extension séparable de $(K^s)^{stricte}$.

Soit $x \in (F^s)^{stricte}$ algébrique sur $(K^s)^{stricte}$.
Alors x est séparable sur $(K^s)^{stricte}$ qui est séparablement clos. Donc $x \in (K^s)^{stricte}$.
Donc $(K^s)^{stricte}$ est algébriquement fermé dans $(F^s)^{stricte}$.
Alors $(F^s)^{stricte}$ est une extension régulière de $(K^s)^{stricte}$.

Comme on a supposé $(F^s)^{stricte}$ et $(L^s)^{stricte}$ algébriquement disjointes sur $(K^s)^{stricte}$, d'après la proposition 43, $(F^s)^{stricte}$ et $(L^s)^{stricte}$ sont linéairement disjointes sur $(K^s)^{stricte}$.

D'après le lemme 56, on peut alors étendre (de manière unique) les dérivations de $(F^s)^{stricte}$ et de $(L^s)^{stricte}$ à $(F^s)^{stricte}(L^s)^{stricte}$.

$$(F^s)^{stricte}(L^s)^{stricte}$$

$$(F^s)^{stricte} \qquad\qquad (L^s)^{stricte}$$

$$F^s \qquad\qquad L^s$$

$$F \qquad\qquad L$$

$$(K^s)^{stricte}$$

$$K^s$$

$$K$$

□

5 La théorie $SCH_{p,e}$

Soit $\mathcal{L}_e = \{0, 1, +, -, \cdot\} \cup \{D_{i,n} | i \in \{1, ..., e\}, n \in \mathbb{N}\}$.
On note $\mathbf{SCH_{p,e}}$ la $\mathcal{L}_e$-théorie des D-corps stricts séparablement clos de degré d'imperfection e.
C'est à cette théorie que nous allons nous intéresser et trouver des propriétés remarquables dont l'élimination des quantificateurs et la complétude.

5.1 Consistance

Tout d'abord, avant de parler de complétude ou d'élimination des quantificateurs, il est essentiel de s'assurer que la théorie que l'on considère est bien *consistante*, c'est-à-dire qu'elle n'est pas contradictoire, ou de manière équivalente, qu'elle admet un modèle.

Théorème 57. *La théorie $SCH_{p,e}$ est consistante.*
Plus précisément, tout corps séparablement clos de caractéristique p et de degré d'imperfection e peut être étendu en un modèle de $SCH_{p,e}$.

Démonstration. Soit F un corps séparablement clos de caractéristique p et de degré d'imperfection e.
On a $[F : F^p] = e$ donc toute p-base de F a e éléments.
Soit $(b_1, ..., b_e)$ une p-base de F.
Par définition, les b_i sont algébriquement indépendants sur F^p et donc en particulier sur $\mathbb{F}_p$.

Posons $K = \mathbb{F}_p(b_1, ..., b_e)$.
On a $\mathbb{F}_p \subseteq K^p$ donc $K \subseteq K^p(b_1, ..., b_e)$.
Donc $(b_1, ..., b_e)$ forme une p-base de K.
Tout élément de K s'écrit donc comme somme de termes de la forme $b_1^{k_1} \cdot ... \cdot b_e^{k_e}$.

Définissons ainsi sur K les fonctions additives $D_{i,n}, i \in \{1, ..., e\}$ suivantes :

$$D_{i,n}(b_1^{k_1} \cdot ... \cdot b_e^{k_e}) = \begin{pmatrix} k_i \\ n \end{pmatrix} b_1^{k_1} \cdot ... \cdot b_i^{k_i - n} \cdot ... \cdot b_e^{k_e}$$

Ce sont des dérivations de Hasse sur K qui commutent.

Montrons que (K, D) est un D-corps strict.
Si $D_{i,1}(b_1^{k_1} \cdot ... \cdot b_e^{k_e}) = 0$,
alors $\begin{pmatrix} k_i \\ 1 \end{pmatrix} b_1^{k_1} \cdot ... \cdot b_i^{k_i - 1} \cdot ... \cdot b_e^{k_e} = 0$
ie $k_i \cdot \underbrace{b_1^{k_1} \cdot ... \cdot b_i^{k_i - 1} \cdot ... \cdot b_e^{k_e}}_{\neq 0} = 0$
donc $k_i = 0$ c'est-à-dire $p | k_i$.
Soit C le corps des constantes de (K, D).
Alors $C \subseteq \langle b_1^{k_1} \cdot ... \cdot b_e^{k_e} | \forall i \in \{1, ..., e\}, p | k_i \rangle = K^p$.
Donc (K, D) est strict.

$K \subseteq F$.
K et F ont une p-base commune : $(b_1, ..., b_e)$.
D'après le lemme 54, D s'étend (de manière unique) à F.

On a $[F : F^p] = e$.
De plus, (K, D) est strict.
Comme K et F ont une p-base commune, on a $[K : K^p] = e$ aussi.
D'après le corollaire 53, (F, D_F) est strict.

Finalement, (F, D_F) est un modèle de $SCH_{p,e}$ qui est donc consistante. □

5.2 Elimination des quantificateurs

Passons maintenant à une propriété très puissante : l'élimination des quantificateurs, qui stipule, grossièrement, que la satisfiabilité d'une formule dans une structure ne dépend pas de l'ensemble de base de la structure.

Définition 58. Soient $\mathcal{L}$ un langage et T une $\mathcal{L}$-théorie.
On dit que T **élimine les quantificateurs** si pour toute formule $\varphi(\overline{x})$ sur $\mathcal{L}$, il existe une formule $\psi(\overline{x})$ sans quantificateur telle que :

$$T \vDash \forall \overline{x}(\varphi(\overline{x}) \leftrightarrow \psi(\overline{x}))$$

Théorème 59. *La théorie $SCH_{p,e}$ élimine les quantificateurs.*

Démonstration. Pour montrer que $SCH_{p,e}$ élimine les quantificateurs, il suffit de montrer que si F et L en sont des modèles qui ont en commun (à isomorphisme près) une sous-structure R, on peut R-plonger F dans une extension élémentaire de L.

$$\begin{array}{ccc} & & L' \\ F & & L \\ R & \simeq & R' \end{array}$$

En effet, par l'absurde :
si $SCH_{p,e}$ n'éliminait pas les quantificateurs, il existerait un n-uplet $\overline{a} = (a_1, ..., a_n) \in R^n$ et une formule $\varphi(x_1, ..., x_n)$ tels que $F \vDash \varphi(\overline{a})$ et $L \nvDash \varphi(\overline{a})$.
Alors on ne pourrait certainement pas plonger F dans une extension de L.

Soient donc (F, D) et (L, D') des modèles de $SCH_{p,e}$ et $R \simeq R'$ des sous-structures de F et L.
Soient K et K' les corps de fractions respectifs de R et R'.
Pour $r, s \in R$, on a $D_{i,n}\left(\frac{r}{s}\right) = \frac{D_{i,n}(r) - \sum_{m<n} D_{i,m}\left(\frac{r}{s}\right) \cdot D_{i,n-m}(s)}{s}$.
De même pour R' et K'.
Donc K et K' sont isomorphes en tant que D-corps.
Ce sont des D-sous-corps de (F, D) et de (L, D').

$$\begin{array}{ccc} F & & L \\ K & \simeq & K' \\ R & \simeq & R' \end{array}$$

D'après la propriété d'amalgamation, il existe un D-corps $(F', D_{F'})$ qui étend les structures de (F, D) et de (L, D').
De plus, $(F', D_{F'})$ admet une plus petite extension stricte $(F'^{stricte}, D_{F'^{stricte}})$.

$$
\begin{array}{ccc}
 & F'^{stricte} & \\
 & F' & \\
F & & L \\
K & \simeq & K' \\
R & \simeq & R'
\end{array}
$$

L est un modèle de $SCH_{p,e}$, donc L est stricte.
D'après le corollaire 53, $F'^{stricte}$ est une extension séparable de L.

D'après la proposition 51, comme L est séparablement clos, on peut L-plonger $F'^{stricte}$ dans une extension élémentaire L' de L : il existe un L-isomorphisme qui envoie $F'^{stricte}$ sur $F'' \subseteq L'$.

$$
\begin{array}{ccc}
 & & L' \\
 & & F'' \\
 & \simeq & \\
 & F'^{stricte} & \\
 & F' & \\
F & & L \\
K & \simeq & K' \\
R & \simeq & R'
\end{array}
$$

Il reste à montrer que F'' est un D-sous-corps de L' qui est isomorphe à $F'^{stricte}$.
Comme L et $F'stricte$ sont stricts, d'après le corollaire 53, L et $F'^{stricte}$ ont une p-base commune.
D'après le lemme 54, la D-structure de L s'étend de manière unique à $F'^{stricte}$ et F'', ainsi qu'à L'.

On a donc l'élimination des quantificateurs. □

Remarque. *Dans la preuve, on n'a pas utilisé le fait que F soit un modèle de $SCH_{p,e}$.*

5.3 Complétude

Nous allons maintenant montrer que notre théorie est aussi complète, c'est-à-dire que chaque formule est soit prouvable, soit fausse dans la théorie, mais qu'il n'y a pas de formule pour laquelle la théorie ne décide pas si elle est "vraie " ou "fausse".

Définition 60. Soient $\mathcal{L}$ un langage et T une $\mathcal{L}$-théorie.
On dit que T est **complète** si elle est consistante, et si pour toute formule φ close sur $\mathcal{L}$, on a $T \vDash \varphi$ ou $T \vDash \neg\varphi$.

Lemme 61. *Soit (K, D) un modèle de $SCH_{p,e}$.*
Alors (K, D) contient $\mathbb{F}_p$ muni de la dérivation de Hasse triviale D^0.

Théorème 62. *La théorie $SCH_{p,e}$ est complète.*

Démonstration. Soit φ une formule close sur $\mathcal{L}_e$.

Comme $SCH_{p,e}$ élimine les quantificateurs, φ est équivalente dans $SCH_{p,e}$ à une formule sans quantificateur, encore close, donc sans variable.
Donc, d'après le lemme 61, si (K, D) est un modèle de $SCH_{p,e}$, alors :

$$(K, D) \vDash \varphi \iff \varphi \textit{ est vraie dans } (\mathbb{F}_p, D^0)$$

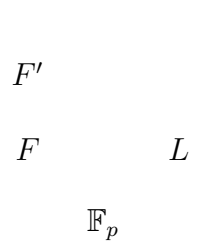
Si $SCH_{p,e} \nvDash \varphi$, alors il existe un modèle (K, D) de $SCH_{p,e}$ tel que $(K, D) \nvDash \varphi$ c'est-à-dire tel que $(K, D) \vDash \neg\varphi$ puisque φ est équivalente à une formule sans variable.
Or $(K, D) \vDash \neg\varphi \iff (\mathbb{F}_p, D^0) \vDash \neg\varphi$.
Donc, comme, par le lemme 61, tout modèle de $SCH_{p,e}$ contient $(\mathbb{F}_p, D^0)$, pour tout modèle (F, D') de $SCH_{p,e}$, on a $(F, D') \vDash \neg\varphi$.
Donc $SCH_{p,e} \vDash \neg\varphi$, et $SCH_{p,e}$ est complète.

□

5.4 Tout D-corps est inclus dans un modèle

Pour finir, montrons encore un petit résultat sur notre théorie : à partir de chaque D-corps, on peut trouver un modèle de la théorie qui le contienne.

Soit (F, D_F) un D-corps.
Soit (L, D_L) un modèle de $SCH_{p,e}$.
(F, D_F) et (L, D_L) sont des D-extensions de $(\mathbb{F}_p, D^0)$.
On peut reprendre la preuve de l'élimination des quantificateurs, puisqu'on ne s'est pas servi du fait que F était séparablement clos, strict ou de degré d'imperfection e.
Alors F se plonge dans une extension élémentaire de L, c'est-à-dire que F se plonge dans un modèle de $SCH_{p,e}$.



Références

[Cha01] Zoé Chatzidakis. Introduction to model theory. *Notes for Luminy*, 2001.

[CK90] C.C.Chang and H.Jerome Keisler. *Model Theory*, volume Studies in Logic. Elsevier Science Publishers, 1990.

[DD05] Adrien Douady and Régine Douady. *Algèbre et théories galoisiennes*. Cassini, 2005.

[Del98] Françoise Delon. *Separably closed fields*. Springer, 1998.

[Lan04] Serge Lang. *Algèbre*. Dunod, 2004.

[Mar02] David Marker. *Model Theory : An Introduction*. Springer, 2002.

[Mat86] Hideyuki Matsumura. *Commutative ring theory*. Cambridge University Press, 1986.

[MW95] Margit Messmer and Carol Wood. Seperably closed fields with higher derivations. *The Journal of Symbolic Logic*, 60, September 1995.

[Zie02] Martin Ziegler. Separably closed fields with hasse derivations. *Journal of symbolic logic*, 2002.