HAL
open science

Théorie des modèles des corps munis d'une dérivation de Hasse

Franck Benoist

To cite this version:

Franck Benoist. Théorie des modèles des corps munis d'une dérivation de Hasse. Mathématiques [math]. Université Paris-Diderot - Paris VII, 2005. Français. NNT : . tel-00134889

HAL Id: tel-00134889

https://theses.hal.science/tel-00134889v1

Submitted on 5 Mar 2007

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

UNIVERSITÉ PARIS 7 - DENIS DIDEROT

THÈSE DE DOCTORAT - MATHÉMATIQUES

Spécialité : logique et fondements de l'informatique

THÉORIE DES MODÈLES DES CORPS MUNIS D'UNE DÉRIVATION DE HASSE

Franck Benoist

Soutenue le 1er juillet 2005

DIRECTRICE :
Françoise Delon

RAPPORTEURS :
Thomas Scanlon
Frank Wagner

JURY :
Daniel Bertrand
Elisabeth Bouscaren
Françoise Delon
François Loeser
Thomas Scanlon
Carol Wood

Remerciements

Puisque cette thèse marque la fin de mon statut d'étudiant en mathématiques, même s'il s'agit d'un apprentissage sans fin, je saisis l'occasion pour remercier les professeurs qui ont avivé mon goût pour cette discipline, que ce soit au collège, au lycée ou en classes préparatoires. Je pense tout particulièrement à Messieurs Brossard et Weil à Lillebonne, et à Monsieur Dehon à Rouen.

Mon orientation vers le domaine de la logique doit beaucoup aux cours de Jean-Louis Krivine à l'Ecole Normale Supérieure, qui m'ont fait découvrir et apprécier cette discipline. Ceci a été conforté par les très bons cours que j'ai reçus dans le cadre du DEA de logique et fondements de l'informatique par Paul Rozière, Gabriel Sabbagh, Boban Velickovic, Ramez Labib-Sami et Elisabeth Bouscaren.

En particulier, je suis très reconnaissant à Elisabeth Bouscaren pour m'avoir orienté vers la théorie des modèles et ses applications à l'algèbre, en me mettant en contact avec ma directrice de thèse Françoise Delon pour mon mémoire de DEA. Je la remercie également pour sa présence bienveillante tout au long de ma thèse, pour les discussions, les questions, les commentaires et les corrections qui m'ont beaucoup apporté. Je suis très heureux qu'elle fasse partie du jury.

Un part essentielle de ces remerciements revient tout naturellement à Françoise Delon, qui a su m'accompagner et me guider pendant de longues années depuis 1999, lors de mon mémoire de DEA puis de ma thèse, dans le domaine mathématique et ses à-côtés. Elle m'a permis d'aborder un sujet de recherche intéressant et d'en saisir les subtilités, en particulier en ce qui concerne les corps non parfaits. Je lui suis reconnaissant d'avoir toujours montré de l'intérêt pour mon travail, même dans les moments plus difficiles, d'avoir relu patiemment cette thèse et de m'avoir signalé les nombreuses corrections nécessaires.

Je tiens à remercier les personnes qui m'ont accueilli lors de mes deux séjours à l'Université de l'Illinois à Urbana-Champaign, en particulier Anand Pillay et Margit Messmer. Ma thèse doit beaucoup aux discussions avec Anand Pillay et à ses questions stimulantes, qui sont à l'origine de mon travail concernant les D-structures. Les rencontres avec Wai Yan Pong et Piotr Kowalski m'ont également beaucoup apporté.

Je remercie Thomas Scanlon et Frank Wagner d'avoir accepté la tâche de rapporteurs et de l'avoir remplie dans de brefs délais. Je suis très honoré que

Thomas Scanlon ait accepté de faire partie du jury. A travers Frank Wagner, je tiens aussi à remercier le groupe de théorie des modèles de l'Université Lyon 1 pour m'avoir permis d'exposer mes résultats lors de son séminaire, et en particulier Thomas Blossier qui m'a aidé à éclaircir différents points concernant les corps séparablement clos.

Je suis heureux que Daniel Bertrand, François Loeser et Carol Wood aient trouvé du temps dans leurs emplois du temps chargés pour faire partie du jury.

Je remercie également l'équipe de logique de l'Université Paris 7 pour l'atmosphère de travail stimulante qu'elle offre, en particulier via le séminaire général de logique. J'ai aussi apprécié l'aide que j'ai reçue de la part de Khadija Bayoud et de Michèle Wasse, qui m'ont guidé avec patience et efficacité dans de nombreuses démarches administratives. Je salue également les thésards du bureau 5C6, les discussions mathématiques et extra-mathématiques qui s'y mènent permettent de se rendre au bureau avec plaisir.

Un grand merci enfin à ma famille et mes amis pour avoir manifesté de l'intérêt pour ce travail un peu mystérieux qu'est une thèse de mathématiques, et pour la motivation qu'ils m'ont apportée.

Table des matières

i Introduction **7**

ii Notations et conventions **13**

I Premiers éléments de D-algèbre **15**
- I.1 Dérivations de Hasse 15
- I.2 Autres éléments de D-algèbre 20
  - I.2.1 D-homomorphismes et D-idéaux 20
  - I.2.2 D-modules 22
  - I.2.3 D-algèbres 23
- I.3 L'algèbre des polynômes différentiels 23
  - I.3.1 Définition de $A\{X\}$ 23
  - I.3.2 Description des D-idéaux de $A\{X\}$ en caractéristique nulle 24
  - I.3.3 Séparabilité et clôture minimale 25

II Les théories CHC_p **29**
- II.1 Axiomatisation 29
- II.2 Élimination des quantificateurs 30
  - II.2.1 L'élimination des quantificateurs 30
  - II.2.2 Les conséquences 32
  - II.2.3 Algébricité et définissabilité 33

III Géométrie D-algébrique **35**
- III.1 Notions de base de géométrie D-algébrique 35
  - III.1.1 La D-topologie 35
  - III.1.2 Fonctions et morphismes 38
  - III.1.3 Les variétés D-algébriques 39
  - III.1.4 Les variétés algébriques vues comme variétés D-algébriques 40
- III.2 Structure supplémentaire sur les variétés algébriques 41
  - III.2.1 Les prolongations 41
  - III.2.2 Foncteurs Π_n et restriction du corps de base 46
  - III.2.3 Variétés algébriques avec D-structure 49
- III.3 Les foncteurs 55
  - III.3.1 La catégorie des groupes infiniment définissables 55
  - III.3.2 Equivalence de catégories entre les groupes D-algébriques et les groupes infiniment définissables . . . 57

III.3.3 Equivalence de catégories entre les groupes rationnellement minces et les groupes algébriques munis d'une D-structure . . . 63

IV Sous-groupes dans les groupes algébriques 67
IV.1 Utilisation des prolongations . . . 67
IV.2 Un cas particulier : le groupe multiplicatif . . . 71
IV.3 Sous-groupes minces . . . 79

V Cas de la caractéristique nulle 89
V.1 Description des D-idéaux de $k\{X\}$ . . . 89
V.2 Quelques rangs dans la théorie CHC_0 . . . 94
V.2.1 Le rang RH . . . 94
V.2.2 Le rang RD . . . 97
V.2.3 Relations entre les différents rangs . . . 99
V.2.4 Rangs et types génériques dans les groupes définissables . 100
V.2.5 Le cas des groupes de rang fini . . . 101
V.2.6 Le cas des groupes D-algébriques . . . 102
V.3 Contre-exemples de rang infini . . . 103
V.3.1 Les bijections Φ_n . . . 103
V.3.2 Un groupe connexe avec deux types de RH maximum . . 105
V.3.3 Un groupe connexe irréductible avec deux notions différentes de type générique . . . 105
V.3.4 Un groupe irréductible non-connexe . . . 106

Annexe A 107

Annexe B 111

Bibliographie 115

Chapitre i

Introduction

Le sujet de cette thèse est l'étude de la théorie des modèles des corps munis d'une dérivation de Hasse. Le choix d'aborder ces structures tire son origine principale des récentes applications de la théorie des modèles à des branches des mathématiques extérieures au domaine de la logique, en particulier à la géométrie algébrique. En effet, Ehud Hrushovski a récemment donné une preuve utilisant fortement des outils de théorie des modèles (voir [Hru96]) d'une conjecture géométrique, dite de Mordell-Lang. Il a pour cela utilisé des théories qui enrichissent le cadre "naturel" de la géométrie algébrique, celui des corps algébriquement clos : il s'agit des corps différentiellement clos en caractéristique nulle et des corps séparablement clos de degré d'imperfection fini non nul en caractéristique positive. L'étude logique de ces théories a commencé de plus longue date. La notion de corps différentiellement clos a été dégagée pour la première fois par Abraham Robinson dans les années 1950, puis étudiée par Lenore Blum entre autres, s'appuyant sur des travaux de Joseph Ritt et Ellis Kolchin en algèbre différentielle. Les premiers résultats sur la théorie des modèles des corps séparablement clos non parfaits ont été montrés par J.L. Eršov, puis leur étude s'est poursuivie avec en particulier Carol Wood, Zoé Chatzidakis, Gregory Cherlin, Shaharon Shelah, Gabriel Srour, Françoise Delon et Margit Messmer. L'étude commune de ces structures sera faite ici dans le langage des dérivations de Hasse, notamment employé par Martin Ziegler ([Zie03b]). L'objectif est d'utiliser une telle étude comparée pour mieux comprendre la théorie des modèles de chacune de ces structures, et particulièrement les objets géométriques qui y sont définis. En particulier, on définit une géométrie D-algébrique dans les corps munis d'une dérivation de Hasse, et on montre qu'elle capture la notion de groupes infiniment définissables en montrant une équivalence de catégorie entre les groupes D-algébriques et les groupes infiniment définissables dans les corps munis d'une dérivation de Hasse (avec les morphismes adéquats). On montre aussi (au travers d'une autre équivalence de catégorie) que certains "petits" sous-groupes des points rationnels $G(K)$ d'un groupe algébrique G, dits sous-groupes rationnellement minces, sont déterminés par une *D-structure* sur G, c'est-à-dire une structure de faisceau de D-algèbres sur le faisceau des fonctions régulières de G. On étudie aussi la question des sous-groupes infiniment définissables des points rationnels d'un groupe algébrique avec l'exemple du groupe multiplicatif $\mathbb{G}_m$, pour lequel on donne une description exhaustive des sous-groupes définissables de $\mathbb{G}_m(K)$ contenant les constantes $\mathbb{G}_m(C_K)$. Don-

nons quelques précisions.

Dans le **premier chapitre**, on introduit les premières définitions : une dérivation de Hasse sur un anneau commutatif A est une suite dénombrable $(D_i)_{i\in\omega}$ de fonctions additives de A dans A satisfaisant les axiomes :

- $D_0 = id_A$
- $D_n(xy) = \sum_{m+l=n} D_m(x)D_l(y)$ pour tout x, y dans A
- $D_m \circ D_n = \binom{m+n}{m} D_{m+n}$.

On donne aussi les premières propriétés d'une dérivation de Hasse, et on fait le rapprochement entre les corps munis d'une dérivation de Hasse et d'autres théories déjà connues : en caractéristique nulle, une dérivation de Hasse n'est rien d'autre qu'une dérivation "classique", les autres fonctions D_i pour $i > 1$ étant obtenues par itération ; et en caractéristique positive, les corps K avec une dérivation de Hasse non triviale qui sont *stricts* (c'est-à-dire tels que leur sous-corps de constantes C_K est le sous-corps K^p des puissances p-ièmes) sont des corps de degré d'imperfection 1, et en nommant une *p-base canonique* de K, la dérivation de Hasse est définissable dans le pur langage des corps. Le reste du chapitre relie la dérivation de Hasse à certaines notions algébriques de base (D-homomorphismes, D-idéaux, D-modules, D-algèbres), définit la D-algèbre des D-polynômes $A\{X\}$ sur un D-anneau A, qui est une notion centrale dans toute la suite, et donne quelques propriétés sur ses D-idéaux.

Le **deuxième chapitre** utilise ces préliminaires D-algébriques pour introduire les théories CHC_p. La classe des D-corps existentiellement clos est élémentaire ; à caractéristique p fixée, on rappelle une axiomatisation de leur théorie CHC_p, due à Lenore Blum pour $p = 0$ et à Margit Messmer et Carol Wood d'une part dans [MesWoo95] puis Martin Ziegler d'autre part dans [Zie03b] pour $p > 0$ (leurs deux approches coïncident dans le cas d'une seule dérivation de Hasse que l'on considère ici). On remarque que ces théories correspondent à la théorie des corps différentiellement clos en caractéristique nulle, et aux théories des corps séparablement clos de degré d'imperfection 1 en caractéristique positive. On rappelle alors que ces théories CHC_p sont complètes et admettent l'élimination des quantificateurs (voir par exemple [Poi87a] pour la caractéristique nulle, et [Del88] pour la caractéristique positive, dans un langage introduit implicitement dans [Woo79]) ; et aussi les premières conséquences modèle-théoriques pour ces théories : description des types, stabilité, élimination des imaginaires, description de l'algébricité et de la définissabilité.

Le **troisième chapitre** est consacré à l'introduction de la géométrie D-algébrique. Les résultats modèle-théoriques dégagés dans le chapitre précédent, comme l'élimination des quantificateurs, permettent des constructions assez semblables à celles de la géométrie algébrique. On montre ici en particulier un analogue du théorème des zéros de Hilbert dans les modèles K de CHC_p suffisamment saturés ; et on définit alors la *D-topologie* dont les fermés correspondent bijectivement aux D-idéaux radiciels de $K\{X\}$ (en caractéristique nulle, on retrouve la topologie utilisée par Ellis Kolchin dans les corps différentiels). On en déduit alors la construction d'une catégorie des variétés D-algébriques (et aussi des groupes D-algébriques) ; les propriétés géométriques de ces objets reflètent les propriétés des théories CHC_p, en particulier la D-topologie est noetherienne

si $p = 0$, mais ne l'est pas si $p > 0$ (dans ce cas, les D-fermés ne sont pas définissables en général mais *infiniment* définissables).
Les points rationnels des variétés algébriques sont des cas particuliers de variétés D-algébriques, mais la D-topologie leur donne d'avantage de structure. Il existe ainsi, en caractéristique positive, des variétés algébriques irréductibles qui ne sont plus irréductibles quand on les voit comme variétés D-algébriques. Toutefois, on étend ici un résultat d'irréducibilité de Kolchin valable dans les corps différentiels de caractéristique nulle (voir l'appendice C de [Mar96]) pour les variétés algébriques lisses, en caractéristique quelconque :

Théorème i.1 (III.1) *Soit V une variété algébrique lisse et irréductible, alors V est encore irréductible dans la D-topologie.*

Cette propriété particulière au cas lisse permet la construction d'un foncteur de *prolongation* sur la catégorie des variétés lisses irréductibles ; c'est une version déformée des fibrés tangents d'ordre quelconque (voir la définition III.12). Ces objets ont déjà été etudiés en caractéristique nulle (par exemple dans [Pil96a] et dans [Mar00]) ; en caractéristique quelconque, le bon comportement de ces prolongations est assuré par la proposition III.6.
Dans le cas de la caractéristique positive, il existe d'autres constructions algébriques qui permettent de comprendre la structure des points rationnels $V(K)$ de la variété V dans un corps non parfait K. L'une d'elle est une famille de foncteurs Λ_n, dont on peut trouver une construction explicite dans [BouDel01] : pour une variété affine V, $\Lambda_n V$ est la clôture de Zariski des racines p-ièmes des coordonnées des points de $V(K)$ dans une base fixée de K en tant que K^{p^n}-espace vectoriel. Une autre construction est la restriction du corps de base de K à K^{p^n} pour une variété V définie sur V ; c'est un objet universel dans la catégorie des variétés algébriques définies sur K^{p^n} envoyées dans V.
Dans la section III.2.2, on établit les relations entre ces différentes constructions ; en particulier, on montre que la restriction du corps de base de K à K^{p^n} est possible pour des variétés algébriques quelconques quand K est un modèle de CHC_p. Plus précisément, on montre les résultats suivants :

Proposition i.1 (III.8) *Pour V une variété algébrique définie sur V, $Fr^n \circ \Lambda_n V$ est une restriction du corps de base de K à K^{p^n} pour V.*

Proposition i.2 (III.9) *Pour V une variété algébrique lisse et irréductible définie sur K, $Fr^n \circ \Lambda_n V$ est isomorphe à la $(p^n - 1)$-ème prolongation de V $\Delta_{p^n-1} V$.*

La dernière construction que l'on fait ici est une généralisation de la notion de D-structure qu'Alexandru Buium avait définie dans des corps différentiels de caractéristique nulle (voir [Bui92]). Une *D-structure* sur une variété algébrique V est une structure de faisceau de D-algèbres sur son faisceau de fonctions régulières $\mathcal{O}_V$ (définition III.15). Une étude modèle-théorique de ces D-structures est aussi menée par Piotr Kowalski et Anand Pillay (dans [KowPil03] en caractéristique nulle, en cours pour la caractéristique positive). Pour les variétés lisses et irréductibles, on montre ici que la donnée d'une D-structure sur V est équivalente à la donnée d'une famille de sections pour la famille projective des prolongations $(\Delta_i V)_{i \in \omega}$. Cela nous permet d'établir des critères pour qu'une

variété algébrique V (lisse et irréductible) puisse être munie d'une D-structure ; des critères cohomologiques avaient déjà été dégagés par Alexandru Buium dans le cas de la caractéristique nulle ; pour la caractéristique positive, on donne ici une condition sur les corps de définition :

Proposition i.3 (III.13) *La variété algébrique lisse et irréductible V peut être munie d'une D-structure si et seulement si, pour tout n, il existe une variété algébrique V_n, définie sur K^{p^n}, isomorphe à V, l'isomorphisme induit entre V_n et V_{n+1} étant de plus défini sur K^{p^n}.*

Ce chapitre se termine par deux théorèmes d'équivalence de catégorie. Le premier est un analogue dans CHC_p du théorème de Weil affirmant qu'un groupe constructible dans un corps algébriquement clos n'est rien d'autre qu'un groupe algébrique ; il recouvre une équivalence de catégorie déjà montrée dans le cas de la caractéristique nulle par Anand Pillay (voir [Pil97]) et approfondit un résultat de plongement des groupes infiniments définissables dans les points rationnels d'un groupe algébrique dû à Elisabeth Bouscaren et Françoise Delon (voir [BouDel01]) :

Théorème i.2 (III.3) *La catégorie des groupes D-algébriques irréductibles, munies des p-homomorphismes, est équivalente à celle des groupes infiniment définissables connexes.*

L'autre théorème généralise lui aussi un résultat montré par Alexandru Buium dans le cas de la caractéristique nulle. Il fait intervenir une notion de minceur : on dit qu'un ensemble définissable (avec paramètres dans k) est *mince* si, pour chacun de ses points x, le corps $k(\{x\})$ engendré par x et ses dérivées successives est une extension algébrique d'une extension finiment engendrée au dessus de k, qu'il est *très mince* si $k(\{x\})$ est une extension algébrique séparable d'une extension finiment engendrée au dessus de k et *rationnellement mince* si $k(\{x\})$ est finiment engendré au dessus de k. Le résultat est le suivant :

Théorème i.3 (III.5) *La catégorie des groupes algébriques irréductibles munis d'une D-structure est équivalente à celle des groupes D-algébriques irréductibles rationnellement minces.*

Dans le **quatrième chapitre**, on utilise les outils construits précédemment pour déterminer la structure supplémentaire apportée par la dérivation de Hasse aux groupes algébriques, c'est-à-dire comprendre quels sont les sous-groupes infiniment définissables de $G(K)$ pour un groupe algébrique G et pour K un modèle suffisament saturé de CHC_p. On constate que ce problème repose surtout sur la compréhension des prolongations de G : en effet, la donnée d'un sous-groupe infiniment définissable H de G correspond à une famille $(H_n)_{n\in\omega}$, avec H_n un sous-groupe de la n-ième prolongation $\Delta_n G$, telle que les H_n vérifient des conditions de compatibilités (voir la proposition et définition IV.1). L'objet de la proposition suivante est de comprendre la structure de groupe algébrique de $\Delta_n G$:

Corollaire i.1 (IV.1) *Le groupe $\Delta_n G$ est une extension de G par un groupe unipotent.*

De plus, dans le cas de la caractéristique positive, le lemme sur les groupes algébriques démontré en annexe B permet d'avoir des renseignements sur la puissance de p qui annule le groupe unipotent en question.
On s'intéresse ensuite au cas particulier du groupe multiplicatif $\mathbb{G}_m$. Les noyaux des projections $\Delta_n\mathbb{G}_m \longrightarrow \mathbb{G}_m$ sont facilement décrits, mais ne suffisent pas pour obtenir une description des sous-groupes infiniment définissables de $\mathbb{G}_m(K)$. Toutefois, une description précise du quotient $\mathbb{G}_m(K)/\mathbb{G}_m(C_K)$ nous permet d'obtenir en section IV.2 une description exhaustive des sous-groupes infiniment définissables de $\mathbb{G}_m(K)$ contenant $\mathbb{G}_m(C_K)$:

Proposition i.4 (IV.10) *Soit $a \in \mathbb{G}_m(K) \setminus \mathbb{G}_m(C_K)$ fixé. Il existe une bijection croissante entre les sous-groupes (infiniment) définissables de $\mathbb{G}_m(K)$ contenant $\mathbb{G}_m(C_K) \cup \{a\}$ et les sous-groupes additifs (infiniment) définissables de $Ker\ D_{p-1}$.*

On exhibe en particulier un sous-groupe (infiniment) définissable de $\mathbb{G}_m(K)$ qui n'est pas définissablement isomorphe au groupe multiplicatif d'un corps (infiniment) définissable dans K.
La dernière partie de ce chapitre se concentre sur les sous-groupes minces infiniment définissables dans les groupes algébriques. L'étude de ces sous-groupes s'est avérée essentielle dans la preuve de la conjecture de Mordell-Lang par Ehud Hrushovski. En caractéristique nulle, il a été exhibé un *noyau de Manin* dans les variétés abéliennes, c'est-à-dire un sous-groupe définissable, mince (ou très mince, ou rationnellement mince, car les trois notions coïncident en caractéristique nulle), Zariski-dense et minimal avec ces propriétés. Les critères pour qu'un groupe algébrique commutatif soit muni d'une D-structure dus à Alexandru Buium ([Bui92]), et le théorème III.5 liant les groupes rationnellement minces au D-structures permettent de montrer :

Proposition i.5 (IV.14) *En caractéristique nulle, tout groupe algébrique commutatif admet un sous-groupe définissable mince et Zariski-dense.*

L'analogue du noyau de Manin en caractéristique positive est la partie divisible $p^\infty A(K)$ de la variété abélienne A. Il était déjà connu que $p^\infty A(K)$ est mince. Toutefois, un des enjeux de la compréhension de ces sous-groupes est de trouver une preuve "directe" de la conjecture de Mordell-Lang, c'est-à-dire qui ne fasse pas intervenir le résultat de dichotomie sur les géométries de Zariski invoqué dans la preuve donnée par Ehud Hrushovski. Un tel objectif a été atteint dans le cas de la caractéristique nulle par Anand Pillay ([Pil04]) ; en caractéristique positive, on connaît une preuve directe dans le cas où $p^\infty A(K)$ est très mince (voir [PilZie03]). Dans la proposition IV.17, on donne un critère pour que $p^\infty A(K)$ soit très mince, qui porte sur la séparabilité d'une factorisation du Verschiebung (l'isogénie duale du Frobenius) à travers les restrictions du corps de base de A de K aux K^{p^n}. Dans cette optique, on s'intéresse aussi à savoir si $p^\infty A(K)$ est rationnellement mince. D'après la proposition IV.18, c'est le cas si et seulement si A est isogène à une variété abélienne munie d'une D-structure. Un argument apporté par Damien Roessler permet de répondre positivement à la question de "descente au corps des constantes" :

Corollaire i.2 (IV.6) *Soit A une variété abélienne munie d'une D-structure,*

alors A est isomorphe à une variété abélienne définie sur le corps des "constantes infinies" $C_K^\infty = K^{p^\infty}$.

On en déduit alors que $p^\infty A(K)$ est rationnellement mince si et seulement si A est isogène à une variété abélienne définie sur C_K^∞ (corollaire IV.8).
On obtient aussi, en utilisant l'annexe A donnant une condition suffisante pour qu'un ensemble définissable soit très mince, le résultat suivant :

Corollaire i.3 (IV.9) *Si A est une courbe elliptique qui n'est pas isogène à une courbe elliptique définie sur C_K^∞, alors $p^\infty A(K)$ est très mince mais pas rationnellement mince.*

Enfin, le **cinquième chapitre** est consacré à la caractéristique nulle. On reprend tout d'abord la description due à Joseph Ritt ([Rit50]) des D-idéaux premiers de $k\{X\}$, qui correspondent aux types sur k. Ensuite, on généralise deux notions de rang qui étaient définis jusqu'à maintenant dans le cas de 1-types (voir [Poi78] ou [Mar96]) : il s'agit du rang RH, qui est une description de la dimension topologique des D-fermés, et du rang RD, une généralisation du degré de transcendance qui peut prendre des valeurs ordinales infinies. Enfin, on s'intéresse au rapport entre les différentes notions de rang (les rang de la stabilité RU et RM et ces rangs ad hoc RH et RD) et les notions de types génériques (c'est-à-dire de types de rang maximal) qui y sont associées. On regarde plus particulièrement ce qui se passe dans le cadre des groupes définissables. D'un côté, Anand Pillay et Wai Yan Pong ont montré dans [PilPon02] que les rangs RU et RM d'un groupe définissable dans la théorie CHC_0 sont égaux ; mais de l'autre, on donne ici des exemples qui montrent que la situation est très différente du cas des corps algébriquement clos, où l'équivalent des rangs modèle-théoriques (RU et RM), topologique (RH) et algébrique (RD) coïncident. En effet, on construit :

- un groupe connexe avec deux types de rang RH maximum
- un groupe connexe et irréductible où l'unique type générique au sens topologique est différent de l'unique type générique au sens modèle-théorique
- un groupe irréductible qui n'est pas connexe.

Cette dernière partie a été l'objet de la publication [Ben02].

Chapitre ii

Notations et conventions

Le vocabulaire de théorie des modèles que l'on utilisera vient principalement de [Poi87a] ; il peut être considéré comme standard, sauf éventuellement le fait que l'on appelle fils (respectivement père) d'un type ce que d'autres appellent plutôt extension (respectivement restriction) d'un type. Outre le vocabulaire, on recommande aussi la référence [Poi87a] pour se familiariser avec le contexte modèle-théorique de ce qui suit ; pour certains points (sur la stabilité géométrique évoquée au chapitre IV par exemple), citons aussi [Pil96b].
A partir du chapitre III, nous utiliserons aussi des notions de géométrie algébrique. Il est hors de question de citer une approche géométrique moderne comme référence, en partie parce que la manière de voir les objets de la géométrie algébrique aujourd'hui est totalement différente de ce qu'elle était il y a cinquante ans. L'approche utilisée ici est plutôt cette dernière. Elle est plus "naïve" et sans doute plus intuitive pour les non spécialistes ; les objets que l'on considère pourront être vus comme des ensembles de points, nous ne parlerons jamais de schémas. Parmi toutes les références possibles, citons [Lan58], [Har77] et [Spr98].
Les conventions diffèrent d'un ouvrage à l'autre ; mais précisons simplement que :

- un morphisme ou une fonction régulière sur une variété algébrique sera toujours pour nous partout définie, et si ce n'est pas le cas, on en donnera un ouvert de définition
- pour la notion de corps de définition d'une variété algébrique, on suit les références données ; et le corps de définition d'un morphisme sera celui de son graphe
- pour un morphisme de variétés algébriques, on rappelle que la notion de surjectivité n'a pas son sens ensembliste : on dira qu'un morphisme est surjectif s'il est séparable et si son image est dense (qu'il s'agisse de variétés irréductibles ou non).

Parmi les notations utilisées, citons :
$S(k)$ espace des types d'une théorie complète fixée sur un ensemble de paramètres k en un nombre fini de variables quelconque mais fixé
$\subset$ inclusion au sens large
$\subsetneq$ inclusion au sens strict
$\mathbb{F}_p$ corps à p éléments si p est premier, et $\mathbb{Q}$ si $p = 0$
$\mathbb{Z}$ anneau premier dans $\mathbb{F}_p$
$\binom{j}{i}$ coefficient binomial dans $\mathbb{Z}$ si $j \geq i$, et 0 sinon

$[m]x$ $\underbrace{x * \ldots * x}_{m \text{ fois}}$ dans un groupe de loi $*$

K^q sous-corps des puissances q-ièmes des éléments de K, pour un corps K de caractéristique p et q une puissance de p

K^n ou $K^{\times n}$ en cas d'ambiguïté puissance cartésienne de K

$\mathcal{O}_V$ faisceau des fonctions régulières sur une variété algébrique V

$f^{\#}$ morphisme de faisceaux $\mathcal{O}_W \longrightarrow \mathcal{O}_V$ associé au morphisme de variétés algébriques $f : V \longrightarrow W$, par la relation $f^{\#}(h) = h \circ f$

$\mathbb{G}_a$ groupe additif

$\mathbb{G}_m$ groupe multiplicatif

$\chi_a(G)$ groupe des caractères additifs du groupe algébrique G

$\chi_m(G)$ groupe des caractères multiplicatifs du groupe algébrique G

$Ext(G, H)$ groupe dont les éléments sont les groupes algébriques commutatifs qui s'écrivent comme une extension de G par H (voir [Ser59])

Chapitre I

Premiers éléments de D-algèbre

I.1 Dérivations de Hasse

Définition I.1 *On dit qu'un anneau A (commutatif) est muni d'une dérivation de Hasse s'il existe une famille $D = (D_i)_{i\in\omega}$ d'applications additives de A dans A, vérifiant les axiomes suivants :*

1. $D_0 = id_A$
2. $D_n(xy) = \sum_{m+l=n} D_m(x)D_l(y)$ *pour tous x, y dans A*
3. $D_m \circ D_n = \binom{m+n}{m} D_{m+n}$.

Le couple (A, D) sera appelé un D-anneau. S'il n'y a pas d'ambiguïté, on dira aussi que A est un D-anneau.

Exemples Tout anneau A peut être muni d'une dérivation de Hasse, dite triviale, en posant $D_0 = id_A$ et $D_i = 0$ pour $i \geq 1$.
Si A est un D-anneau, on peut munir l'algèbre de polynômes $A[t]$ (ainsi que l'algèbre des séries entières $A[[t]]$) d'une structure de D-anneau, dite standard, prolongeant celle de A, en posant $D_1(t) = 1$ et $D_i(t) = 0$ pour $i > 1$. On obtient immédiatement par l'axiome 2 que $D_i(t^j) = \binom{j}{i} t^{j-i}$ pour tous i, j.

Pour un D-anneau A, les propriétés suivantes sont obtenues facilement. On pourra consulter à ce sujet la section I.1 de [Oku63].

Proposition I.1 *Dans un D-anneau A :*

1. *D_1 est une dérivation sur A, c'est-à-dire une application linéaire de A dans A qui vérifie la règle de Leibniz : $\forall x, y,\ D_1(xy) = xD_1(y) + D_1(x)y$.*
2. $D_n(x_1 \dots x_m) = \sum_{i_1+\dots+i_m=n} D_{i_1}(x_1) \dots D_{i_m}(x_m)$.
3. $D_{i_1} \circ \dots \circ D_{i_n} = \frac{(i_1+\dots+i_n)!}{i_1!\dots i_n!} D_{i_1+\dots+i_n}$;
   en particulier $D_i^n = \frac{(ni)!}{(i!)^n} D_{in}$ (où D_i^n représente la composition de D_i n fois),

et si p est un nombre premier et $n = \sum_{i=0}^{s} c_i p^i$ la décomposition de n en base p, alors

$$D_1^{c_0} \circ \ldots \circ D_{p^s}^{c_s} = \underbrace{\frac{n!}{(p!)^{c_1} \ldots (p^s!)^{c_s}}}_{non\ divisible\ par\ p} D_n.$$

4. *La dérivation de Hasse ($D_{|\mathbb{Z}}$) est triviale.*
5. *Si A est de caractéristique p, alors $D_n(x^{p^e}) = 0$ si p^e ne divise pas n, et $D_n(x^{p^e}) = (D_m(x))^{p^e}$ si $n = mp^e$.*

Définition I.2 *On dit que k est un D-corps si c'est à la fois un corps et un D-anneau.*

On va étudier la théorie des modèles des corps munis d'une dérivation de Hasse, dans le langage du premier ordre $\mathcal{L}_H := \{0, 1, +, -, ., (D_i)_{i \geq 0}\}$.

Définition I.3 *Pour p nul ou nombre premier, on note CH_p la théorie des corps de caractéristique p muni d'une dérivation de Hasse dans le langage $\mathcal{L}_H$.*

Proposition I.2 *Soit A un D-anneau intègre. La dérivation de Hasse D se prolonge de manière unique au corps de fraction de A pour en faire un D-corps, par la formule suivante (pour $(x, y) \in A \times A^*$) :*

$$D_n(\frac{x}{y}) = \frac{D_n(x) - \sum_{m<n} D_m(\frac{x}{y}) D_{n-m}(y)}{y}.$$

Preuve La formule donnée est imposée par l'axiome 2, ce qui donne l'unicité. Le fait qu'on obtienne bien une dérivation de Hasse sur le corps de fraction de A est immédiat. □

Définition I.4 *Soit A un D-anneau. On note*

$$C_A := \{x \in A | D_1(x) = 0\}$$

et

$$C_A^\infty := \{x \in A | \forall n > 0, D_n(x) = 0\}.$$

Fait I.1 *Pour D-anneau A, C_A et C_A^∞ sont des sous-anneaux de A. Si A est un corps, ce sont de plus des sous-corps de A.*

Fait I.2 *Si le D-anneau A est de caractéristique nulle, alors $C_A = C_A^\infty$ (d'après la proposition I.1.3).*
Si A est de caractéristique $p > 0$, alors $A^p \subset C_A$ (d'après la proposition I.1.5).

Définition I.5 *Soit $p > 0$ et $k \models CH_p$. On dit que k est un D-corps strict si $C_k = k^p$.*

Exemple Soit k un corps parfait de caractéristique $p > 0$, muni de la dérivation de Hasse triviale. On munit $k(t)$ de la dérivation de Hasse standard au-dessus de k. Alors $k(t)$ est un D-corps strict. On remarque tout d'abord que pour montrer

que $C_{k(t)} = k(t)^p$, il suffit de le montrer sur $k[t]$: en effet, si $\frac{f(t)}{g(t)} \in C_{k(t)}$, où $f(t)$ et $g(t)$ sont des éléments de $k[t]$ premiers entre eux, avec $f(t)$ unitaire, alors

$$D_1\Big(\frac{f(t)}{g(t)}\Big) = \frac{D_1(f(t))g(t) - f(t)D_1(g(t))}{g(t)^2} = 0,$$

et donc soit $D_1(f(t)) = D_1(g(t)) = 0$, et on est ramené à $k[t]$, soit $\frac{f(t)}{g(t)} = \frac{D_1(f(t))}{D_1(g(t))}$, ce qui est exclu par le choix de f et g car $deg\, D_1(f(t)) < deg\, f(t)$. Maintenant, pour $h(t) = \sum_i a_i t^i \in C_{k[t]}$, on a $D_1(h(t)) = \sum_i i a_i t^{i-1} = 0$, et donc $h(t) \in k[t^p] = k[t]^p$ car k est parfait.

Fait I.3 *Si k est un D-corps strict, alors pour tout $n \geq 1$,*

$$k^{p^n} = \{x \in k | \forall 1 \leq i < p^n, D_i(x) = 0\},$$

et

$$C_k^\infty = k^{p^\infty} := \bigcap_{n \in \omega} k^{p^n}.$$

Proposition et définition I.1 *Soit $k \models CH_p$, pour $p > 0$. Il existe un plus petit D-corps strict contenant k, on le note k^{strict}. L'extension k^{strict}/k est purement inséparable. Par convention, pour $p = 0$, on note $k^{strict} := k$.*

Preuve On construit par induction une suite croissante de D-corps $(k_i)_{i \in \omega}$. Soit $k_0 = k$, et supposons k_i construit. Pour x dans C_{k_i}, on a $D_m(x) = 0$ pour tout m non divisible par p (proposition I.1.3), et il s'ensuit que $D' := (D_0, D_p, D_{2p}, \ldots)$ est une dérivation de Hasse sur C_{k_i}. On pose alors $k_{i+1} := C_{k_i}^{1/p}$, et on munit k_{i+1} de la dérivation de Hasse issue de D' par $D_n(x) = D'_n(x^p)^{1/p}$. Alors k_{i+1} est bien une D-extension de k_i (car pour $x \in k_i$, $D'_n(x^p) = D_{np}(x^p) = D_n(x)^p$ d'après la proposition I.1.5), purement inséparable car $k_{i+1}^p \subset C_{k_i}$.
Alors $k^{strict} := \cup_{i \in \omega} k_i$ est bien la plus petite D-extension stricte de k ; et c'est une extension purement inséparable de k. □

Exemple Si k est un corps de caractéristique p non nulle et de degré d'imperfection 1 (c'est-à-dire que $[k : k^p] = p$), tout élément $b \in k \setminus k^p$ forme une p-base de k : $1, b, \ldots, b^{p-1}$ est une base de k en tant que k^p-espace vectoriel. On peut définir alors une dérivation de Hasse sur k, en posant $D_1(b) = 1$ et $D_i(b) = 0$ pour $i > 1$. On obtient ainsi un D-corps strict. On va maintenant regarder la construction inverse.

Définition I.6 *Pour $p > 0$, soit $k \models CH_p$, de degré d'imperfection 1 ; et $n \geq 1$. On dit qu'un élément b de k est une p-base de k si $1, b, \ldots, b^{p-1}$ est une base de k en tant que k^p-espace vectoriel. On dit que cette p-base est n-canonique si $D_1(b) = 1$ et $D_i(b) = 0$ pour tout $1 < i < p^n$. On dit que b est une p-base canonique si c'est une p-base n-canonique pour tout n.*

Fait I.4 *Soit b une p-base d'un D-corps k de degré d'imperfection 1. Alors, pour tout entier n, $(b^i)_{0 \leq i < p^n}$ forme une base de k en tant que k^{p^n}-espace vectoriel, et les applications D_i pour $i < p^n$ sont k^{p^n}-linéaires. Si $x = \sum_{i=0}^{p^n-1} x_i b^i$ est*

la décomposition d'un élément x de k dans cette base, alors $\mathbb{F}_p(\{b\})(x_i)_{i<p^n} = \mathbb{F}_p(\{b\})(D_i(x))_{i<p^n}$. La relation entre ces deux p^n-uplets est donnée matriciellement par

$$\begin{pmatrix} D_0(x) \\ D_1(x) \\ \vdots \\ D_{p^n-1}(x) \end{pmatrix} = \begin{pmatrix} D_0(1) & D_0(b) & \dots & D_0(b^{p^n-1}) \\ D_1(1) & D_1(b) & \dots & D_1(b^{p^n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ D_{p^n-1}(1) & D_{p^n-1}(b) & \dots & D_{p^n-1}(b^{p^n-1}) \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{p^n-1} \end{pmatrix}.$$

Si de plus b est une p-base n-canonique, la matrice $D_i(b^j)_{i,j<p^n}$ est triangulaire supérieure car $D_i(b^j) = \binom{j}{i} b^{j-i}$ (conséquence de la proposition I.1.2).

Définition I.7 *Pour une p-base fixée d'un D-corps K de degré d'imperfection 1, on note $\varphi_n(x) = (x_0, \dots, x_{p^n-1})$ le p^n-uplet d'éléments de K^{p^n} tel que $x = \sum_{i=0}^{p^n-1} x_i b^i$.*

Corollaire I.1 *Soit k un D-corps de degré d'imperfection 1, admettant une p-base canonique b ; soit $l := \mathbb{F}_p(b)$. Pour tout entier n, on écrit, suivant les notations de [Del98],*

$$x = \sum_{i=0}^{p^n-1} \lambda_{i,n}(x)^{p^n} b^i$$

la décomposition d'un élément x de k dans la base $1, b, \dots, b^{p^n-1}$ de k en tant que k^{p^n}-espace vectoriel (c'est-à-dire que $\lambda_{\cdot,n}^{p^n} = \varphi_n$). Alors

$$(l(\{x\}))^{strict} = l(\lambda_{i,n}(x) | n \in \mathbb{N}, 0 \leq i \leq p^n - 1).$$

Preuve D'après le fait précédent,

$$l(\{x\}) = l(\lambda_{i,n}(x)^{p^n} | n \in \mathbb{N}, 0 \leq i \leq p^n - 1).$$

Pour tout $n \in \mathbb{N}$ et $0 \leq i \leq p^n - 1$, $\lambda_{i,n}(x)^{p^n}$ est dans k^{p^n}, donc annule $D_1, \dots, D_{p^n-1}$: $(l(\{x\}))^{strict}$ doit donc contenir $\lambda_{i,n}(x)$.
On obtient alors l'égalité voulue en montrant que $l(\lambda_{i,n}(x) | n \in \mathbb{N}, 0 \leq i \leq p^n - 1)$ est strict. Soit $y \in l(\lambda_{i,n}(x) | n \in \mathbb{N}, 0 \leq i \leq p^n - 1)$ tel que $D_1(y) = 0$. Les relations de composition des fonctions $\lambda_{i,n}$ exposées dans [Del98] montrent que $l(\lambda_{i,n}(x) | n \in \mathbb{N}, 0 \leq i \leq p^n - 1)$ est stable par ces fonctions. Or $D_1(y) = 0$ équivaut à $\lambda_{1,1}(y) = \dots = \lambda_{p-1,1}(y) = 0$, donc $y = \lambda_{0,1}(y)^p \in l(\lambda_{i,n}(x) | n \in \mathbb{N}, 0 \leq i \leq p^n - 1)^p$. □

Fait I.5 *(section 1 de [Del98]) Si un corps k de caractéristique p admet une p-base b, et si l est une extension de k, alors l'extension est séparable si et seulement si $b \notin l^p$.*

Proposition I.3 *Soit k un D-corps strict, avec une dérivation de Hasse non-triviale. Alors le degré d'imperfection de k vaut 1. De plus, pour tout entier $n \geq 1$, il existe dans k un élément b qui est une p-base n-canonique pour k.*

Preuve On montre d'abord que pour un élément b tel que $D_1(b) = 1$, b est une p-base 1-canonique. On obtient en effet, d'après la proposition I.1.3, que $D_i(b) = 0$ pour $1 < i < p$; et si $a_0 + a_1 b + \ldots + a_m b^m = 0$ est une combinaison linéaire à coefficients dans C_k, avec $m < p$, on obtient en appliquant D_m que $a_m = 0$. La famille $1, b, \ldots, b^{p-1}$ est donc libre sur C_k.
On montre alors par récurrence sur i entre 1 et p que

$$\{x \in k | D_1^i(x) = 0\} = C_k \oplus C_k b \oplus \ldots \oplus C_k b^{i-1}.$$

C'est la définition de C_k pour $i = 1$; ensuite, pour $i < p$, si $D_1^{i+1}(x) = 0$, alors, par hypothèse de récurrence, $D_1(x) = a_0 + \ldots + a_{i-1} b^{i-1}$ avec $a_j \in C_k$, et alors $D_1(x - (a_0 b + \ldots + \frac{a_{i-1}}{i} b^i)) = 0$, donc $x \in C_k \oplus \ldots \oplus C_k b^i$. Comme $D_1^p = p! D_p$ est nul sur k, on en déduit que $1, b, \ldots, b^{p-1}$ est une base de k sur $C_k = k^p$.
On construit ensuite une p-base n-canonique par récurrence sur n. Pour $n = 1$, il suffit de trouver un élément b tel que $D_1(b) = 1$. On sait qu'il existe un élément c de k et un entier $m \geq 1$ tel que $D_m(c) \neq 0$, on choisit un tel m minimum. Nécessairement, m est une puissance de p ; en effet, soit q la plus grande puissance de p inférieure à m, alors $\binom{m}{q} D_m(c) = D_{m-q} \circ D_q(c) \neq 0$ (car $\binom{m}{q}$ vaut $\lfloor \frac{m}{q} \rfloor$, qui est compris entre 1 et $p - 1$), donc $D_q(c) \neq 0$. Ensuite, par choix de q, $D_i(c) = 0$ pour tout $1 \leq i < q$, donc, comme k est strict, il existe c' tel que $c'^q = c$ d'après le fait I.3 ; on a alors $D_1(c')^q = D_q(c) \neq 0$. Enfin, puisque $D_1^p(c') = p! D_p(c') = 0$, il existe un plus petit entier l ($1 \leq l < p$) tel que $D_1^l(c') \neq 0$ et $D_1^{l+1}(c') = 0$. Posons alors $b = \frac{D_{l-1}(c')}{l D_l(c')}$, on a bien $D_1(b) = 1$.
Ensuite, en supposant connue b une p-base n-canonique, on cherche une p-base n+1-canonique sous la forme $b' = b - c^{p^n}$. En effet, un tel b' vérifie $D_i(b') = D_i(b)$ pour tout $0 < i < p^n$, donc reste une p-base n-canonique, et on cherche c tel que $D_{p^n}(b') = 0$. On a $D_{p^n}(b') = D_{p^n}(b) - D_1(c)^{p^n}$; or pour tout $1 \leq j < p^n$, $D_j(D_{p^n}(b)) = D_{p^n}(D_j(b)) = 0$ puisque $D_j(b)$ vaut 0 ou 1. Comme k est strict, il existe donc $d \in k$ tel que $D_{p^n}(b) = d^{p^n}$. Reste donc à trouver $c \in k$ tel que $D_1(c) = d$, ce qui est possible si $D_{p-1}(d) = 0$ (car d'après le premier point de cette preuve, on a alors $d \in C_k \oplus \ldots \oplus C_k b^{p-2}$, donc d est intégrable). Or $(D_{p-1}(d))^{p^n} = D_{p^{n+1}-p^n}(d^{p^n}) = D_{p^{n+1}-p^n} \circ D_{p^n}(b) = \binom{p^{n+1}}{p^n} D_{p^{n+1}}(b) = 0$, ce qui permet de trouver b' tel que $D_{p^n}(b') = 0$. On a bien trouvé une p-base $n + 1$-canonique, puisque pour $p^n \leq j < p^{n+1}$, $D_j(b') = \frac{D_{j-p^n} \circ D_{p^n}(b')}{\binom{j}{p^n}} = 0$. □

Remarque La proposition précédente est aussi montrée de manière différente dans [Zie03a].

Proposition I.4 *Soit k un D-corps strict et l une D-extension de k. Alors cette extension est séparable.*

Preuve Si D est triviale sur k, alors, puisque k est strict, $k^p = C_k = k$, donc k est parfait et toute extension de k est séparable.
Si D est non-triviale, il existe par la proposition précédente une p-base 1-canonique (b). Pour montrer que l'extension l/k est séparable, il suffit de vérifier que $b \notin l^p$; c'est évident puisque $D_1(b) \neq 0$. □

Dans le cas de la caractéristique nulle, la théorie CH_0 n'est rien d'autre que la théorie des corps différentiels, comme le montre la proposition suivante.

Proposition I.5 *Soit (k, d) un corps de caractéristique nulle, muni d'une dérivation, alors il existe une unique dérivation de Hasse D sur k telle que $D_1 = d$.*

Preuve Si D est une dérivation de Hasse telle que $D_1 = d$, la proposition I.1.3 impose que, pour $n \geq 1$,

$$D_n(x) = \frac{1}{n!} \underbrace{d \circ \ldots \circ d}_{n\, fois}(x).$$

On obtient immédiatement par récurrence que, si $D = (D_i)_{i \in \omega}$ est donnée par ces formules à partir de d, D est bien une dérivation de Hasse sur k. □

Ce qui précède n'est pas valable en caractéristique positive, puisque $n!$ peut s'annuler. D'après la proposition I.1.4, il suffit de connaître les D_q pour toutes les puissances q de p pour connaître la dérivation de Hasse sur k. La donnée de D_1 ne permet de connaître D_{p^n} que sur k^{p^n} (puisque $D_{p^n}(x^{p^n}) = (D_1(x))^{p^n}$ d'après la proposition I.1.5) ; l'utilité des dérivations de Hasse en caractéristique positive est de prolonger ces applications à k tout entier.

I.2 Autres éléments de D-algèbre

I.2.1 D-homomorphismes et D-idéaux

Définition I.8 *Soient A et B deux D-anneaux (respectivement D-corps). On dit qu'une application $\phi : A \longrightarrow B$ est un homomorphisme de D-anneaux (respectivement de D-corps) si c'est un homomorphisme d'anneaux (respectivement de corps) qui commute avec la dérivation de Hasse. On emploiera aussi le terme de D-homomorphisme.*

Définition I.9 *Soit A un D-anneau. On dit que I est un D-idéal de A si c'est un idéal de A stable par l'application de $D = (D_i)_{i \geq 0}$.*

Fait I.6 *Soit I un D-idéal d'un D-anneau A. Alors il existe une unique structure de D-anneau sur A/I telle que la projection $A \longrightarrow A/I$ soit un D-homomorphisme.*

Proposition et définition I.2 *Soit U une partie d'un D-anneau A. Il existe un plus petit D-idéal de A contenant U, c'est l'idéal engendré par la famille $(D_i(x))_{\substack{i \in \omega \\ x \in U}}$. On le note $\{U\}$.*

Définition I.10 *Soit I un idéal d'un D-anneau A. On appelle radical de I, et on note $\sqrt{I}$, l'idéal*

$$\sqrt{I} := \{x \in A | \exists n \in \mathbb{N}, x^n \in I\}.$$

On dit que I est radiciel si $I = \sqrt{I}$.

Fait I.7 *Pour tout idéal I, $\sqrt{I}$ est le plus petit idéal radiciel contenant I.*

Définition I.11 *Soit I un idéal d'un D-anneau A et S une partie multiplicative de A (c'est-à-dire $1 \in S$ et $(x, y \in S \Rightarrow xy \in S)$). Alors on note*

$$S^{-1}I = \{x \in A | \exists y \in S, xy \in I\}.$$

Proposition I.6 *Si I est un D-idéal d'un D-anneau A et S une partie multiplicative de A, alors $S^{-1}I$ est un D-idéal.*

Preuve Il est tout d'abord clair que $S^{-1}I$ est un idéal.
Pour montrer que $S^{-1}I$ est un D-idéal, considérons $a \in S^{-1}I$, et $b \in S$ tel que $ba \in I$. Alors, pour tout $i \geq 0$ et $h \geq 1$, $D_i(b^h a) \in I$. On montre par récurrence sur h que pour tout $0 \leq i \leq h$, il existe $c \in A$ tel que $D_i(b^h) = cb^{h-i}$. C'est clair si $h = 1$; supposons la propriété montrée pour un $h \geq 1$, et montrons-la pour $h+1$. Le résultat est clair si $i = h+1$; et pour $0 \leq i \leq h$, il existe $c_0, \ldots, c_i \in A$ tels que :

$$D_i(b^{h+1}) = \sum_{j=0}^{i} D_j(b^h) D_{i-j}(b)$$

$$= \sum_{j=0}^{i} c_j b^{h-j} D_{i-j}(b) = (\sum_{j=0}^{i-1} c_j b^{i-j-1} D_{i-j}(b) + c_i) b^{h+1-i}.$$

On en déduit, par récurrence sur i, que pour tout $i \geq 0$, $b^{i+1} D_i(a) \in I$. On utilise pour cela la relation suivante, où $c_1, \ldots, c_i$ sont les éléments de A que l'on vient d'exhiber :

$$\underbrace{D_i(b^{i+1}a)}_{\in I} = \sum_{j=0}^{i} D_j(b^{i+1}) D_{i-j}(a) = b^{i+1} D_i(a) + \underbrace{\sum_{j=1}^{i} c_j b^{i-j+1} D_{i-j}(a)}_{\in I}.$$

On obtient ainsi que $D_i(a) \in S^{-1}I$, donc $S^{-1}I$ est un D-idéal. □

Nous aurons besoin dans la suite de la décomposition des D-idéaux radiciels en intersection de D-idéaux premiers.

Lemme I.1 *Soit I un D-idéal d'un D-anneau A, et $ab \in I$. Alors pour tous entiers i, j, $D_i(a) D_j(b) \in \sqrt{I}$.*

Preuve La démonstration se fait par récurrence sur $n = i + j$. Pour $n = 0$, c'est l'hypothèse $ab \in I$.
Ensuite, pour i_0, j_0 fixés tels que $i_0 + j_0 = n$, on a :

$$D_{i_0}(a) D_{j_0}(b) D_n(ab) = \sum_{i+j=n} D_i(a) D_{i_0}(a) D_j(b) D_{j_0}(b) \in I.$$

Or, pour $i < i_0$, $i + j_0 < n$ donc $D_i(a) D_{j_0}(b) \in \sqrt{I}$, et pour $i > i_0$, $i_0 + j < n$ donc $D_{i_0}(a) D_j(b) \in \sqrt{I}$. Donc $(D_{i_0}(a) D_{j_0}(b))^2 \in \sqrt{I}$, et donc $D_{i_0}(a) D_{j_0}(b) \in \sqrt{I}$ puisque $\sqrt{I}$ est radiciel. □

Proposition I.7 *Soit I un D-idéal d'un D-anneau A, et S une partie multiplicative de A, disjointe de I. Alors il existe un D-idéal premier P contenant I et disjoint de S.*

Preuve L'union d'une famille bien ordonnée par l'inclusion de D-idéaux contenant I et disjoints de S est un D-idéal contenant I et disjoint de S, donc d'après le lemme de Zorn, il existe un D-idéal P contenant I et disjoint de S maximal pour ces propriétés.
On va montrer que P est premier. Supposons le contraire et fixons $a \notin P$, $b \notin P$ tels que $ab \in P$ (c'est la seule possibilité pour que P ne soit pas premier, puisque $1 \notin P$). Les D-idéaux $P' := (P, D_i(a))_{i\in\omega}$ et $P'' := (P, D_j(b))_{j\in\omega}$ contiennent strictement P, donc ils rencontrent S, c'est donc aussi le cas de $P'.P''$ puisque S est multiplicative. Or, d'après le lemme précédent,

$$P'.P'' = (P, D_i(a)D_j(b))_{i,j\in\omega} \subset \sqrt{P},$$

donc $\sqrt{P}$ rencontre S, donc P rencontre S puisque S est multiplicative ; ce qui contredit l'hypothèse sur P. □

Proposition I.8 *Soit I un D-idéal propre d'un D-anneau A. Alors*

$$\sqrt{I} = \bigcap_{P\in\mathcal{P}} P \quad , \quad \mathcal{P} \text{ l'ensemble des } D\text{-idéaux premiers contenant } I.$$

En particulier, $\sqrt{I}$ est un D-idéal.

Preuve Si P est un idéal premier contenant I, on a $\sqrt{I} \subset P$.
Pour l'inclusion inverse, si $x \notin \sqrt{I}$, alors $S := \{x^n | n \in \mathbb{N}\}$ est une partie multiplicative de A, disjointe de I, donc par la proposition précédente, il existe un D-idéal premier P contenant I et disjoint de S ; d'où $\bigcap_{P\in\mathcal{P}} P \subset \sqrt{I}$. □

Nous aurons aussi besoin du lemme technique suivant (lemme 1.14 de [Mar96]).

Lemme I.2 *Soit S et T deux parties d'un D-anneau A. Alors*

$$\sqrt{\{S\}}\sqrt{\{T\}} \subset \sqrt{\{ST\}}.$$

Preuve Soit $x \in S$. Alors $x^{-1}\sqrt{\{ST\}} := \{y \in A | xy \in \sqrt{\{ST\}}\}$ contient T, et c'est un D-idéal radiciel (c'est clairement un idéal radiciel, et c'est un D-idéal d'après le lemme I.1). Donc $\sqrt{\{T\}} \subset x^{-1}\sqrt{\{ST\}}$, ou encore $x\sqrt{\{T\}} \subset \sqrt{\{ST\}}$. Ainsi, $(\sqrt{\{T\}})^{-1}\sqrt{\{ST\}} := \{x \in A | x\sqrt{\{T\}} \subset \sqrt{\{ST\}}\}$ contient S, et c'est un D-idéal radiciel (car $(\sqrt{\{T\}})^{-1}\sqrt{\{ST\}} = \bigcap_{x\in\sqrt{\{T\}}} x^{-1}\sqrt{\{ST\}}$). Donc $\sqrt{\{S\}}\sqrt{\{T\}} \subset \sqrt{\{ST\}}$. □

I.2.2 D-modules

Définition I.12 *Soit A un D-anneau. On appelle D-module sur A, ou encore A-D-module un A-module M muni d'applications additives $(D_i)_{i\geq 0}$ de M dans M vérifiant :*

- $D_0 = id_M$
- $D_n(ax) = \sum_{m+l=n} D_m(a)D_l(x)$ *pour tout* a *dans* A *et* x *dans* M
- $D_m \circ D_n = \binom{m+n}{m} D_{m+n}$

On appelle encore dérivation de Hasse (pour un module) cette famille d'applications.
Un homomorphisme de A-D-modules est un homomorphisme de A-modules qui commute avec la dérivation de Hasse.

Fait I.8 *Si* M *et* M' *sont deux A-D-modules, on peut munir* $M \oplus M'$ *d'une structure de A-D-module en posant* $D_n(x + x') = D_n(x) + D_n(x')$ *; ainsi que* $M \otimes_A M'$ *en posant* $D_n(x \otimes x') = \sum_{m+l=n} D_m(x) \otimes D_l(x')$.

I.2.3 D-algèbres

Définition I.13 *Soit A un D-anneau. On appelle D-algèbre sur A, ou encore A-D-algèbre, un D-anneau B muni d'un D-homomorphisme de A dans B.*
Un homomorphisme de A-D-algèbres est un homomorphisme de A-algèbres qui commute avec la dérivation de Hasse.

Exemple Soit (A, D) un D-anneau. On considère la A-algèbre des séries entières $A[[t]]$, que l'on munit de la dérivation de Hasse standard au-dessus de (A, D^0) (dérivation triviale sur A), donnée par

$$D_i^{st}(\sum_{j\geq 0} a_j t^j) = \sum_{j\geq i} \binom{j}{i} a_j t^{j-i}.$$

L'homomorphisme $T : (A, D) \longrightarrow (A[[t]], D^{st})$, dit de *développement de Taylor*, donné par

$$a \mapsto T(a) := \sum_{i\geq 0} D_i(a)t^i,$$

est un D-homomorphisme ; il fait de $A[[t]]$ une A-D-algèbre.
Réciproquement, si A est un anneau, et s'il existe un homomorphisme $T : A \longrightarrow A[[t]]$ tel que $T(a) \equiv a \mod t$ pour tout $a \in A$, alors il existe une unique famille D de fonctions sur A telle que T soit l'homomorphisme de développement de Taylor. Cette famille D vérifie tous les axiomes des dérivations de Hasse, sauf éventuellement l'axiome 3 d'itérativité. Cet axiome est vérifié si et seulement si $D^{st} \circ T = T \circ D$, et T est alors un D-homomorphisme.

Fait I.9 *Si* B *et* B' *sont deux A-D-algèbres, on munit* $B \otimes_A B'$ *d'une structure de A-D-algèbre en définissant la dérivation de Hasse de la même manière que pour les A-D-modules.*

I.3 L'algèbre des polynômes différentiels

I.3.1 Définition de $A\{X\}$

Définition I.14 *Soit A un D-anneau et* $X = (X_1, \ldots, X_r)$ *une multivariable. On appelle algèbre des polynômes différentiels en X à coefficients dans A, et on note* $A\{X\}$*, l'algèbre des polynômes en une infinité dénombrable de variables* $A[d_iX]_{i\geq 0}$ *(où* d_iX *désigne la multivariable* $(d_iX_1, \ldots, d_iX_r)$*).*

La A-algèbre $A\{X\}$ peut être naturellement munie d'une structure de D-algèbre sur A en posant $D_j(d_iX) = \binom{i+j}{i} d_{i+j}X$. On veillera à ne pas confondre $D_1(P)$ et $P' = \frac{dP}{dX}$ pour les polynômes P en une variable.

Définition I.15 *Soit $P \in A\{X\}$ un polynôme différentiel non-nul et X_i ($1 \leq i \leq r$) une variable. On appelle ordre de P en X_i, et on note $ordre_{X_i}(P)$, l'indice maximum j tel que d_jX_i apparaît dans P. Par convention, on pose $ordre_{X_i}(P) = -1$ si aucun d_jX_i n'apparaît dans P.*
On notera $A\{X\}_{\leq n}$ la sous-algèbre de $A\{X\}$ formée des polynômes d'ordre en chacune des variables inférieur ou égal à n.

Définition I.16 *Soit $P \in A\{X\}$ un polynôme différentiel non-nul et X_i ($1 \leq i \leq r$) une variable telle que $j := ordre_{X_i}(P) \geq 0$. On appelle séparante de P par rapport à X_i, et on note $S_{X_i}(P)$, la dérivée partielle $\frac{\partial P}{\partial d_jX_i}$. Si m est le degré de P en d_jX_i, on appelle majeur de P par rapport à X_i, et on note $M_{X_i}(P)$, le coefficient dans P de $(d_jX_i)^m$; c'est un élément de $A\{X_1, \ldots, X_{i-1}, X_{i+1}, X_r\}\{X_i\}_{<j}$.*

Fait I.10 *Soit $P \in A\{X\}$ d'ordre j en la variable X_i. Alors, pour tout entier $h \geq 1$, il existe $Q \in A\{X\}$, avec $ordre_{X_i}Q < h + j$ tel que*

$$D_h(P) = S_{X_i}(P)\binom{h+j}{j} d_{h+j}X_i + Q.$$

I.3.2 Description des D-idéaux de $A\{X\}$ en caractéristique nulle

Dans cette section, A est un D-anneau commutatif intègre et de caractéristique nulle. Dans le chapitre V, on donnera une description assez détaillée des D-idéaux de $A\{X\}$, principalement issue de [Rit50]. Cette description ne repose pas sur ce qui sera fait par la suite, et nous donnons simplement ici les résultats (respectivement le lemme V.1, le théorème V.1, le corollaire V.1 et la proposition V.1) qui seront utiles pour les prochains chapitres. Ces résultats peuvent aussi être trouvés dans [Mar96] et dans le chapitre 6 de [Poi87a].

Lemme I.3 *Soit X une monovariable, et $P \in A\{X\} \setminus A$ un D-polynôme non-scalaire, de séparante S et de majeur M. Pour tout $Q \in A\{X\}$, il existe $Q_1 \in A\{X\}$, avec $ordre_X(Q_1) < ordre_X(P)$ ou ($ordre_X(Q_1) = ordre_X(P) = m$ et $deg_{d_mX}Q_1 < deg_{d_mX}P$), et des entiers i, j tels que $S^iM^jQ \equiv Q_1 \mod \{P\}$.*

Théorème I.1 (Ritt-Raudenbush) *Supposons que A satisfasse la condition de chaîne ascendante pour les D-idéaux radiciels, et soit X une monovariable. Alors $A\{X\}$ satisfait la condition de chaîne ascendante pour les D-idéaux radiciels.*

Corollaire I.2 *Soit $k \models CH_0$ et X une multivariable. Alors $k\{X\}$ satisfait la condition de chaîne ascendante pour les D-idéaux radiciels. Ainsi, tout D-idéal radiciel propre de $k\{X\}$ s'écrit comme intersection finie de D-idéaux premiers.*

Proposition I.9 *Soit I un D-idéal premier non nul de $k\{X\}$ pour une monovariable X. Alors il existe un D-polynôme P dans I tel que*

$$I := I_{(P)} = \{\ Q \in k\{X\} \mid \text{il existe des entiers } u, v, S_X(P)^u M_X(P)^v Q \in \{P\}\ \},$$

et réciproquement, pour tout D-polynôme irréductible P de $k\{X\}$, $I_{(P)}$ est un D-idéal premier de $k\{X\}$.
Si $Q \in I_{(P)}$ vérifie $ordre_X(Q) < ordre_X(P)$ ou ($ordre_X(Q) = ordre_X(P) = j$ et $deg_{d_jX} Q < deg_{d_jX} P$), alors $Q = 0$.
Si Q est un D-polynôme irréductible de $I_{(P)}$, de même ordre que P, alors il existe un élément $a \in k$ non nul tel que $Q = aP$; en particulier, $I_{(P)} = I_{(Q)}$.

I.3.3 Séparabilité et clôture minimale

Proposition I.10 (Satz 7 de [HasSch37]) *Soit k un D-corps, et $k(x)$ une extension algébrique séparable de k. Alors il existe une unique dérivation de Hasse sur $k(x)$ prolongeant celle de k.*

Preuve Notons $g(u) := u^n + a_1 u^{n-1} + \ldots + a_n$ le polynôme minimal (séparable) de x sur k. On reprend la construction du développement de Taylor $T : k \longrightarrow k[[t]]$ donnée dans la section I.2.3 : soit $G(u) := u^n + T(a_1)u^{n-1} + \ldots + T(a_n) \in k[u][[t]]$. On a alors dans $k(x)[[t]]$,, modulo l'idéal maximal engendré par t, $G(x) \equiv g(x) = 0$ et $\frac{dG}{du}(x) \equiv \frac{dg}{du}(x) \neq 0$ par séparabilité de g. On en déduit, d'après le lemmme de Hensel, qu'il existe $z \in k(x)[[t]]$ tel que $G(z) = 0$ et $z \equiv x \mod t$. L'homomorphisme

$$\begin{array}{ccc} k[u] & \longrightarrow & k(x)[[t]] \\ b_0 u^m + \ldots + b_m & \mapsto & T(b_0)z^m + \ldots + T(b_m) \end{array}$$

étend T et envoie g sur $G(z) = 0$; il induit donc un homomorphisme $\overline{T} : k(x) \mapsto k(x)[[t]]$, qui étend T et qui vérifie $\overline{T}(x) = z \equiv x \mod t$. D'après la section I.2.3, cet homomorphisme définit une famille $\overline{D}$ sur $k(x)$, qui est une dérivation de Hasse à l'axiome 3 près, et qui coïncide avec D sur k puisque $\overline{T}$ prolonge T. Pour montrer que $\overline{D}$ est une dérivation de Hasse, on montre que, pour tout $y \in k(x)$, $\overline{D_i} \circ \overline{D_j}(y) = \binom{i+j}{i}\overline{D_{i+j}}(y)$, par récurrence sur $i+j$. Soit f un polynôme minimal séparable de y sur k, on sait d'après le fait I.10, et sans utilisation de l'axiome 3, que

$$D_i(f) = \frac{df}{dX} d_i X + f_i(d_0 X, \ldots, d_{i-1} X) \quad \text{pour un certain } f_i \in k[X_0, \ldots, X_{i-1}],$$

$$D_j(D_i(f)) = \frac{df}{dX} D_j(d_i X) + \sum_{k=1}^{j} D_k(\frac{df}{dX}) D_{j-k}(d_i X) + D_j(f_i(d_0 X, \ldots, d_{i-1} X)),$$

$$D_{i+j}(f) = \frac{df}{dX} d_{i+j} X + f_{i+j}(d_0 X, \ldots, d_{i+j-1} X) \text{ pour un } f_{i+j} \in k[X_0, \ldots, X_{i+j-1}].$$

L'axiome 3 dans $k\{X\}$ donne que $D_j(D_i(f)) = \binom{i+j}{i} D_{i+j}(f)$, et d'autre part, dans $k(x)$, $\overline{D_j}(\overline{D_i}(f(y))) = \overline{D_{i+j}}(f(y)) = 0$. Donc si on suppose par récurrence que $\overline{D_l} \circ \overline{D_m}(y) = \binom{l+m}{l}\overline{D_{l+m}}(y)$ dès que $l + m < i + j$, on obtient

$$\sum_{k=1}^{j} \overline{D_k}(\frac{df}{dX}(y))\overline{D_{j-k}}(\overline{D_i}(y)) + \overline{D_j}(f_i(\overline{D_0}(y), \ldots, \overline{D_{i-1}}(y)))$$

$$= \binom{i+j}{i} f_{i+j}(\overline{D_0}(y), \ldots, \overline{D_{i+j-1}}(y)),$$

et donc $\overline{D_j} \circ \overline{D_i}(y) = \binom{i+j}{i}\overline{D_{i+j}}(y)$.
L'unicité vient aussi du fait I.10 : pour une dérivation de Hasse D sur $k(x)$, et $y \in k(x)$ de polynôme minimal séparable f sur k, il existe un polynôme $f_i \in k[X_0, \ldots, X_{i-1}]$ tel que

$$D_i(f(y)) = \frac{df}{dX}(y)D_i(y) + f_i(D_0(y), \ldots, D_{i-1}(y)) = 0,$$

ce qui donne l'unicité de $\overline{D}$ par induction sur i. □

Corollaire I.3 *Soit k un D-corps. La dérivation de Hasse de k s'étend de manière unique en une dérivation de Hasse sur la clôture séparable k^{sep}.*

Proposition I.11 *Soit k un D-corps strict, on prolonge la dérivation de Hasse de k à k^{sep}. Alors (k^{sep}, D) est strict.*

Preuve On fait la preuve pour $p > 0$ (si $p = 0$, il n'y a rien à montrer). Soit $a \in k^{sep}$, avec $D_1(a) = 0$. Posons $f(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_0$ le polynôme minimal séparable unitaire de a sur k. En appliquant D_1 à la relation $f(a) = 0$, on obtient

$$D_1(a_{d-1})a^{d-1} + \ldots + D_1(a_0) = 0,$$

et donc, par minimalité de f, on a, pour tout i, $D_1(a_i) = 0$ et il existe $b_i \in k$ tel que $a_i = b_i^p$. Le polynôme $g(X) := X^d + b_{d-1}X^{d-1} + \ldots + b_0$ reste séparable (car en élevant à la puissance p une éventuelle racine commune à g et à $\frac{dg}{dX}$, on obtient une racine commune à f et à $\frac{df}{dX}$) et tous les éléments b de k^{alg} tels que b^p est solution de f sont solutions de g : il existe donc $b \in k^{sep}$ tel que $b^p = a$.□

Corollaire I.4 *Soit k un D-corps. Alors $(k^{sep})^{strict} = (k^{strict})^{sep}$.*

Preuve Par construction et la proposition précédente, $(k^{strict})^{sep}$ est le plus petit D-corps strict et séparablement clos contenant k. Pour montrer qu'il en est de même de $(k^{sep})^{strict}$, il suffit de vérifier que ce corps est séparablement clos, ce qui est le cas car c'est une extension purement inséparable du corps séparablement clos k^{sep} (voir la proposition et définition I.1). □

On donne maintenant, dans le langage des corps avec dérivation de Hasse, une traduction du lemme 2.1 de [BouDel01], qui reste valable dans le cas d'une caractéristique nulle. On fixe pour cela un D-corps k de caractéristique p quelconque, et X une multivariable de taille n.

Proposition I.12 *Soit I un idéal premier séparable de $k[X]$, vu comme sous-k-algèbre de $k\{X\}$. Alors il existe un polynôme S dans $k[X] \setminus I$, et un D-idéal premier Q de $k\{X\}$ tel que Q est le plus petit D-idéal premier contenant I et pas S. C'est aussi le plus petit D-idéal premier tel que $Q \cap k[X] = I$.*

Preuve Soit k_1 le corps de fraction de $k[X]/I$, et $(x_1, \ldots, x_n)$ l'image de X par la projection naturelle. Le corps $k_1 = k(x_1, \ldots, x_n)$ est une extension séparable de k donc, quitte à réordonner les variables, on peut supposer que $(x_1, \ldots, x_r)$ est une base de transcendance séparante de k_1 sur k, pour un entier r entre 1 et n. Soit k_2 le corps de fraction de $k\{X_1, \ldots, X_r\}$, les différentes variables $(d_i X_j)_{i \geq 1, 1 \leq j \leq r}$ sont vues comme des éléments algébriquement indépendants au-dessus de k_1, et $k(x_1, \ldots, x_r)$ est vu comme un sous-corps de k_2 par l'identification $x_j = d_0 X_j$ $(1 \leq j \leq r)$. Il y a disjonction linéaire entre k_2 et k_1 au-dessus de $k(x_1, \ldots, x_r)$, et k_1 est algébrique séparable sur $k(x_1, \ldots, x_r)$, donc $k_3 := k_1 k_2 = k_2(x_{r+1}, \ldots, x_n)$ est algébrique séparable sur k_2. Comme k_2 est un D-corps, il existe par la proposition I.10 une unique structure de D-corps sur k_3 qui prolonge celle de k_2. Posons

$$Q := \{P \in k\{X\} | k_3 \models P(x_1, \ldots, x_n) = 0\},$$

on va montrer que Q convient.
Par construction, $Q \cap k[X] = I$.
Pour $r + 1 \leq i \leq n$, notons $P_i(X_1, \ldots, X_r, X_i)$ le polynôme minimal de x_i sur $k(x_1, \ldots, x_r)$, c'est un polynôme séparable en la variable X_i donc $\frac{dP_i}{dX_i}(x_1, \ldots, x_r, x_i) \neq 0$, donc $S_i := \frac{dP_i}{dX_i} \notin I$. D'autre part, on montre par récurrence sur j que $D_j(x_i) \in k\{x_1, \ldots, x_r\}_{\leq j}[x_i][S_i(x_1, \ldots, x_r, x_i)^{-1}]$; il suffit pour cela d'utiliser la relation

$$0 = D_j(P_i(x_1, \ldots, x_r, x_i)) = S_i(x_1, \ldots, x_r, x_i) D_j(x_i) + Q_{i,j}(x_1, \ldots, x_r, x_i),$$

où $Q_{i,j} \in k\{X_1, \ldots, X_r\}_{\leq j}\{x_i\}_{<j}$. Soit alors $G_{i,j} \in k\{X_1, \ldots, X_r\}_{\leq j}[X_i][S_i(X)^{-1}]$ tel que, pour un entier $m_{i,j}$ suffisamment grand,

$$S_i(X)^{m_{i,j}}(d_j X_i - G_{i,j}(X_1, \ldots, X_r, X_i, S_i(X)^{-1})) \in Q.$$

Soit R un D-idéal premier de $k\{X\}$ tel que $I \subset R$ et $S := \Pi_{i=r+1}^n S_i \notin R$; et $y := (y_1, \ldots, y_n)$ une réalisation de R.
Posons $C := k\{X_1, \ldots, X_r\}[X_{r+1}, \ldots, X_n]$; puisque k_2 est une extension purement transcendante de $k(x_1, \ldots, x_r)$, et que k_2 et k_1 sont linéairement disjoints au-dessus de $k(x_1, \ldots, x_r)$, $Q \cap C = IC \subset R \cap C$, d'où un homomorphisme de k-algèbres :

$$k\{x_1, \ldots, x_r\}[x_{r+1}, \ldots, x_n] \simeq C/(Q \cap C) \longrightarrow C/(R \cap C) \simeq k\{y_1, \ldots, y_r\}[y_{r+1}, \ldots, y_n].$$

Puisque R est premier et ne contient pas S, cet homomorphisme s'étend de manière unique en un homomorphisme :

$$k\{x_1, \ldots, x_r\}[x_{r+1}, \ldots, x_n][S_{r+1}(x)^{-1}, \ldots, S_n(x)^{-1}] \longrightarrow$$
$$k\{y_1, \ldots, y_r\}[y_{r+1}, \ldots, y_n][S_{r+1}(y)^{-1}, \ldots, S_n(y)^{-1}].$$

Puisque R est un D-idéal, il contient lui aussi les D-polynômes $S_i(X)^{m_{i,j}}(d_j X_i - G_{i,j}(X_1, \ldots, X_r, X_i, S_i(X)^{-1}))$, et donc l'homomorphisme précédent induit de manière unique un homomorphisme de k-algèbres

$$k\{x_1, \ldots, x_n\} \longrightarrow k\{y_1, \ldots, y_n\},$$

envoyant, pour tout i, j, $D_j(x_i)$ sur $D_j(y_i)$. C'est donc un homomorphisme de k-D-algèbres de $k\{X\}/Q$ dans $k\{X\}/R$, envoyant la classe de X sur la classe

de X ; et donc $Q \subset R$.
Donc Q est bien le plus petit D-idéal premier contenant I et pas S ; et par suite, c'est aussi le plus petit D-idéal premier tel que $Q \cap k[X] = I$. $\square$

Remarque Si r désigne encore le degré de transcendance de $k[X]/I$ sur k, notons que pour tout j, le degré de transcendance de $k\{X\}_{<j}$ sur k vaut jr.

Chapitre II

Les théories CHC_p

II.1 Axiomatisation

Théorème II.1 *Pour p nul ou nombre premier, la théorie CH_p admet une modèle-complétion notée CHC_p.*
Pour $p = 0$, la théorie CHC_0 est axiomatisée par :
- *les axiomes de CH_0*
- *un schéma d'axiomes affirmant : pour tout couple de D-polynômes non-nuls P, Q en une variable X, tels que $ordre_X(P) > ordre_X(Q)$, il existe une solution au système $P = 0 \wedge Q \neq 0$*

Pour $p > 0$, la théorie CHC_p est axiomatisée par :
- *les axiomes de CH_p*
- *l'axiome $\exists x D_1(x) \neq 0$ (la dérivation est non triviale)*
- *l'axiome $\forall x \exists y (D_1(x) = 0 \Rightarrow x = y^p)$ (le corps est strict)*
- *un schéma d'axiomes affirmant : pour tout polynôme P tel que $\frac{dP}{dX} \neq 0$, il existe x tel que $P(x) = 0$ (le corps est séparablement clos)*

Preuve Ces théories CHC_p sont des extensions des théories CH_p. On va montrer ici que tout modèle k de CH_p se plonge dans un modèle K de CHC_p, c'est-à-dire que les théories CH_p et CHC_p sont compagnes l'une de l'autre. La fin de la démonstration arrivera plus tard, comme corollaire du fait que les théories CHC_p admettent l'élimination des quantificateurs.

Pour $p = 0$, on reprend la démonstration que l'on peut trouver dans le chapitre 6 de [Poi87a]. On va construire une suite croissante $(k_i)_{i\in\omega}$ de D-corps, avec $k_0 = k$, tels que pour tout couple (P, Q) de D-polynômes non nuls à coefficients dans k_i, avec $ordre(P) > ordre(Q)$, il existe dans k_{i+1} une solution au système $P = 0 \wedge Q \neq 0$. Supposons k_i construit et désignons par $(P_\alpha, Q_\alpha)_{\alpha\in\beta}$ une énumération ordinale de tels couples. On construit par induction une suite croissante $(k_{i,\alpha})_{\alpha\in\beta+1}$ de D-corps, avec $k_{i,0} = k_i$ et pour tout $\alpha \in \beta + 1$, $k_{i,\alpha}$ contient une solution à tous les systèmes $P_\gamma = 0 \wedge Q_\gamma \neq 0$ pour $\gamma < \alpha$. Pour cela, on pose $k_{i,\alpha} = \cup_{\gamma<\alpha} k_{i,\gamma}$ si α est un ordinal limite. Puis, en supposant $k_{i,\alpha}$ construit, on considère T_α un facteur irréductible de P_α, de même ordre que P_α, dans $k_{i,\alpha}\{X\}$. D'après la proposition I.9, $I_{(T_\alpha)}$ est un D-idéal premier de $k_{i,\alpha}\{X\}$, qui ne contient pas Q_α. On pose alors $k_{i,\alpha+1}$ le corps de fractions du D-anneau intègre $k_{i,\alpha}\{X\}/I_{(T_\alpha)}$. L'image de la variable X dans cette D-

extension de $k_{i,\alpha}$ est bien une solution au système $P_\alpha = 0 \wedge Q_\alpha \neq 0$.
Puis, en posant $k_{i+1} := \cup_\alpha k_{i,\alpha}$ et $K := \cup_{i\in\omega} k_i$, on trouve bien que K est une D-extension de k qui est un modèle de CHC_0.

Pour $p > 0$, la démonstration qui suit est essentiellement extraite de [Zie03b].
Soit X une variable et k_1 le corps de fraction de la k-D-algèbre $k\{X\}$, k_1 est une D-extension de k avec une dérivation non triviale. En utilisant le corollaire I.3 et la proposition et définition I.1, posons $K := (k_1^{sep})^{strict}$, c'est une D-extension de k. Le D-corps K est strict et séparablement clos (d'après le corollaire I.4) et la dérivation de Hasse est non triviale sur K. Donc K est bien un modèle de CHC_p. □

Exemple En caractéristique $p > 0$, considérons $\mathbb{F}_p(t)$ muni de la D-structure standard. C'est un D-corps strict (voir l'exemple suivant la définition I.5 ; et donc, d'après le corollaire I.4, $(\mathbb{F}_p(t))^{sep}$ est un modèle de CHC_p. En caractéristique nulle, on ne connaît pas de modèle "naturel" de CHC_0.

Remarque Signalons qu'il existe d'autres axiomatisations des théories CHC_p, de nature géométrique. Elles ont été données par David Pierce et Anand Pillay dans le cas de la caractéristique nulle (voir [PiePil98]), et par Piotr Kowalski dans le cas de la caractéristique positive (voir [Kow05]). Ces axiomatisations reposent sur la notion de prolongation, qui sera développée dans la section III.2.1.

II.2 Eliminations des quantificateurs et conséquences modèle-théoriques

II.2.1 L'élimination des quantificateurs

Théorème II.2 *Soit p nul ou premier fixé. Les théories CHC_p sont complètes et admettent l'élimination des quantificateurs.*

Preuve Remarquons tout d'abord que les formules atomiques dans le langage $\mathcal{L}_H$, avec paramètres a (uplet éventuellement vide), sont équivalentes (modulo la théorie CH_p) à des équations polynomiales de la forme $P(a) = 0$, pour $P \in \mathbb{F}_p\{X\}$. Par conséquent, deux uplets a et b (éventuellement vides) de deux D-corps K et L satisfont les mêmes formules atomiques si et seulement s'ils engendrent deux sous-D-corps isomorphes, par un isomorphisme envoyant a sur b.
On doit donc montrer que, pour deux modèles $\aleph_0$-saturés K et L de CHC_p :
- K et L ont le même D-corps premier
- si a et b sont deux uplets de K et L respectivement, qui engendrent des sous-D-corps isomorphes par un isomorphisme envoyant a vers b, et si c est un élément de K, alors il existe un élément d de L tel que a, c et b, d engendrent des sous-D-corps isomorphes par un isomorphisme envoyant a, c vers b, d.

Pour le premier point, comme K et L ont même caractéristique p, ils ont même corps premier $\mathbb{F}_p$. D'après les propositions I.1.4 et I.2, la dérivation de Hasse $D_{|\mathbb{F}_p}$ est triviale, donc K et L admettent pour D-corps premier $\mathbb{F}_p$ muni de la dérivation de Hasse triviale.

Pour le deuxième point, soit k et l les deux sous-D-corps engendrés par a et b respectivement, Φ un isomorphisme de k vers l envoyant a vers b et c un élément de K.
Pour le cas $p = 0$, on reprend la démonstration du théorème 6.16 de [Poi87a]. Soit $I_{c/k} := \{R \in k\{X\} | R(c) = 0\}$ le D-idéal annulateur de c dans $k\{X\}$. Soit J l'image de $I_{c/k}$ par Φ. C'est un D-idéal premier ; d'après la proposition I.9, il est donc soit nul, soit de la forme $I_{(P)}$ pour P un D-polynôme irréductible de $l\{X\}$. Dans les deux cas, on peut trouver par $\aleph_0$-saturation de L un élément d de L tel que $I_{d/l} = J$: l'ensemble de formules $\{P(x) = 0 \wedge Q(x) \neq 0 | Q \in l\{X\}, ordre_X(Q) < ordre_X(P)\}$ (respectivement $\{Q(x) \neq 0 | Q \in l\{X\} \setminus \{0\}\}$ si $J = 0$), dont les paramètres peuvent être choisis parmi b, est en effet finiment consistant, et une réalisation d de cet ensemble de formules vérifie respectivement $I_{d/l} = I_{(P)}$ (car P est irréductible et d'ordre minimal dans le D-idéal premier $I_{d/l}$, et la dernière assertion de la proposition I.9 s'applique) ou $I_{d/l} = 0$. Ainsi, $l\{d\} \simeq l\{X\}/J$ est isomorphe à $k\{c\} \simeq k\{X\}/I$ par un isomorphisme prolongeant Φ et envoyant c sur d.

Pour le cas $p > 0$, la preuve donnée ici correspond à une traduction dans le langage $\mathcal{L}_H$ de la preuve de la proposition 27 de [Del88]. Remarquons tout d'abord que K contient une p-base canonique (car K est $\aleph_0$-saturé et contient une p-base n-canonique pour tout n) ; quitte à lui ajouter un élément de C_K^∞ transcendant sur k (ce qui est possible car k est finiment engendré comme D-corps et K est $\aleph_0$-saturé), on peut supposer que cette p-base e est transcendante sur k. On trouve de même une p-base f dans L, transcendante sur l, et ainsi l'isomorphisme Φ se prolonge en un isomorphisme de $k(e)$ vers $l(f)$, avec $\Phi(e) = f$. D'autre part, en utilisant la construction de la "clôture stricte" (proposition et définition I.1), on remarque que cet isomorphisme se prolonge de manière unique en un isomorphisme Φ de $k_1 := k(e)^{strict}$ dans $l_1 := l(f)^{strict}$; les hypothèses de $\aleph_0$-saturation pourront encore être utilisées puisque que k_1 et l_1 sont inclus dans la clôture définissable de uplets finis (respectivement a, e et b, f).
Soit $I_{c/k_1} := \{R \in k_1\{X\} | R(c) = 0\}$ le D-idéal annulateur de c dans $k_1\{X\}$, on doit trouver un élément d de L tel que I_{d/l_1} soit l'image de I_{c/k_1} par Φ. Puisque L est $\aleph_0$-saturé, il suffit pour cela de trouver, pour tout n, un élément $d \in L$ tel que $I_{d/l_1} \cap l_1\{X\}_{<p^n} = \Phi(I_{c/k_1}) \cap k_1\{X\}_{<p^n}$. Comme K est strict, il existe $(c_i)_{i<p^n}$ dans K tel que $c = \sum_{i=0}^{p^n-1} c_i^{p^n} e^i$. L'extension $k_1(c_i)_{i<p^n}/k_1$ est séparable en tant que sous-extension de la D-extension K/k_1, qui est séparable car k_1 est strict. On peut donc extraire de $(c_i)_{i<p^n}$ une base de transcendance séparante $(c_{i_j})_j$ (c'est-à-dire $k_1(c_{i_j})_j$ est purement transcendante sur k_1, et $k_1(c_i)_{i<p^n}$ est algébrique séparable sur $k_1(c_{i_j})_j$. Comme L est $\aleph_0$-saturé, on trouve dans L des éléments $(d_{i_j})_j$ algébriquement indépendants au-dessus de l_1 ; puis, comme L est séparablement clos, on trouve, pour tout $i < p^n$, $d_i \in L$ tel que $l_1(d_{i_j})_j(d_i) \simeq k_1(c_{i_j})_j(c_i)$ par un isomorphisme de corps prolongeant Φ et respectant les indices. Posons alors $d = \sum_{i=0}^{p^n-1} d_i^{p^n} f^i$, Φ se prolonge en un isomorphisme de corps

$$k_1(D_0(c), \ldots, D_{p^n-1}(c)) = k_1(c_i^{p^n})_{i<p^n} \simeq l_1(d_i^{p^n})_{i<p^n} = l_1(D_0(d), \ldots, D_{p^n-1}(d)),$$

ce qui termine la démonstration. $\square$

II.2.2 Les conséquences

Corollaire II.1 *Pour p fixé, la théorie CHC_p est la modèle-complétion de la théorie CH_p.*

Preuve En effet, les théories CH_p et CHC_p sont compagnes l'une de l'autre, et CHC_p est complète avec l'élimination des quantificateurs (voir le chapitre 5 de [Poi87a] pour la caractérisation des modèle-complétions). □

Si A est un ensemble de paramètres dans un D-corps, le D-corps k engendré par A est inclus dans la clôture définissable de A ; ainsi il est équivalent d'étudier les types sur A et les types sur k.

Corollaire II.2 *Soit k un D-corps et $n \geq 1$. L'ensemble des n-types sur k est en bijection avec l'ensemble des D-idéaux premiers de $k\{X\}$ (X multivariable de longueur n), par l'application associant à tout type t le D-idéal premier $I_t := \{P \in k\{X\} | \text{“}P(X) = 0\text{”} \in t\}$.*

Corollaire II.3 *Soit $k \subset l$ une extension de D-corps, $s \in S_n(k)$ et $t \in S_n(l)$. Alors t est un fils de s si et seulement si $I_t \cap k\{X\} = I_s$.*

Corollaire II.4 *Soit $K \models CHC_p$, et l une D-extension de K. Soit a une réalisation d'un type sur K. Alors $tp(a/l)$ ne dévie pas sur K si et seulement si l et $K(\{a\})$ sont algébriquement disjoints au-dessus de K, si et seulement si l et $K(\{a\})$ sont linéairement indépendants au-dessus de K.*

Preuve Ces caractérisations, et la démonstration, suivent la proposition 36 de [Del88]. Puisque K est un modèle, on sait (voir par exemple la proposition 3.8 de [Pil83]) que $tp(a/l)$ ne dévie pas sur K si et seulement si les mêmes formules sont représentées dans $tp(a/l)$ et dans $tp(a/K)$. D'après l'élimination des quantificateurs, cela équivaut au fait que les mêmes D-polynômes sont représentés dans $I_{a/K}$ et dans $I_{a/l}$, ce qui signifie exactement que $K(\{a\})$ et l sont algébriquement disjoints au-dessus de K. Puisque l'extension $K \subset l$ est régulière, cela équivaut aussi au fait que $K(\{a\})$ et l sont linéairement disjoints au-dessus de K (voir [Lan58]). □

Corollaire II.5 *La théorie CHC_0 est ω-stable.*
Pour $p > 0$, la théorie CHC_p est stable mais non-superstable.

Preuve Pour $p = 0$ et $k \models CH_0$, les D-idéaux premiers de $k\{X\}$ (monovariable) sont soit nuls, soit déterminés par un polynôme minimal, donc $|S_1(k)| \leq |k|$.
Pour $p > 0$, les types sont déterminés par des idéaux de $k\{X\}$, qui sont dénombrablement engendrés puisque $k\{X\}$ est une union croissante d'anneaux de polynômes noetheriens ; donc $|S_1(k)| \leq |k|^\omega$. Enfin, un modèle K de CHC_p admet une suite strictement décroissante infinie de sous-corps définissables

$$K^{p^n} = \{x \in K | \forall i < p^n, D_i(x) = 0\},$$

donc CHC_p n'est pas superstable (voir [BerLas86]). □

Corollaire II.6 *Les théories CHC_p admettent l'élimination des imaginaires.*

On utilise pour cela la proposition suivante issue de [MesWoo95] (proposition 4.8).

Proposition II.1 *Soit T une théorie de corps stable. Supposons que pour tout $n \geq 1$, il existe un ensemble (éventuellement infini) d'indéterminées $(X_i)_{i\in J}$ tel que pour tout modèle F de T, il existe une correspondance bijective entre $S_n(F)$ et un sous-ensemble des idéaux de l'anneau de polynômes $F[X_i]_{i\in J}$ telle que pour tout automorphisme σ de F, σ fixe un type si et seulement s'il fixe l'idéal correspondant. Alors T admet l'élimination des imaginaires.*

Le corollaire s'en déduit puisque la correspondance $t \mapsto I_t$ vérifie l'hypothèse exigée : si σ est un D-automorphisme de $K \models CHC_p$, et $p \in S_n(K)$, $\sigma(I_t) = I_{\sigma(t)}$.

II.2.3 Algébricité et définissabilité

Proposition II.2 *Soit t un type algébrique de CHC_p sur $k \models CH_p$, et a un élément qui réalise le type t. Alors a est algébrique sur k au sens de la théorie des corps.*

Preuve La preuve dans le cas où $p = 0$ suit celle du lemme 5.1 de [Mar96], elle utilise le lemme suivant :

Lemme II.1 *On suppose $p = 0$. Soit P un D-polynôme irréductible de $k\{X\}$, où X est une monovariable, l une D-extension de k et Q un facteur irréductible de P dans $l\{X\}$. Alors $I_{(Q)} \cap k\{X\} = I_{(P)}$.*

Preuve du lemme Notons tout d'abord, en utilisant la théorie de Galois, que tous les diviseurs de P dans $l\{X\}$ sont conjugués par k-automorphismes, ils sont donc tous de même ordre que P ; et d'autre part ce sont des facteurs simples de P.
Si $R \in I_{(P)}$, il existe des entiers u et v tels que $M(P)^u S(P)^v R \in \{P\} \subset \{Q\}$ (par définition). Si on note $P = AQ$, on obtient facilement que $S(P) \equiv AS(Q)$ mod $\{Q\}$ et que $M(P) = M(A)M(Q)$, donc $M(A)^u M(Q)^u A^v S(Q)^v R \in \{Q\}$, c'est-à-dire $M(A)^u A^v R \in I_{(Q)}$. Or $M(A)^u A^v$ est d'ordre inférieur ou égal à celui de Q, et non divisible par Q (puisque Q ne divise ni les autres facteurs irréductibles de P, ni $M(A)$ qui est d'ordre strictement inférieur à celui de Q) ; donc d'après la proposition I.9, $R \in I_{(Q)}$.
Réciproquement, si $R \in I_{(Q)} \cap k\{X\}$, on trouve par le lemme I.3 des entiers u et v tels que $M(P)^u S(P)^v R \equiv R_1 \mod \{P\}$, avec $R_1 \in k\{X\}$ vérifiant $ordre_X(R_1) < ordre_X(P)$ ou ($ordre_X(R_1) = ordre_X(P) = j$ et $deg_{d_j X} R_1 < deg_{d_j X} P$), A fortiori, $R_1 \in I_{(Q)}$, et R_1 est d'ordre inférieur ou égal à celui de Q, donc Q divise R_1 (proposition I.9). Puisque $R_1 \in k\{X\}$, tous les conjugués de Q par k-automorphismes divisent R_1, donc P divise R_1, et donc $R \in I_{(P)}$.□

Dans le cas $p = 0$, $I_t = I_{(P)}$ pour P un D-polynôme irréductible de $k\{X\}$, ou $I_t = \{0\}$. Si P est d'ordre nul, P est une équation algébrique à coefficients dans k satisfaite par a. Si ce n'est pas le cas, soit K un modèle de CHC_0 contenant k, K contient toutes les réalisations de t. On considère l'extension de t sur K donnée par le D-idéal nul si $I_t = \{0\}$, et par le D-idéal $I_{(Q)}$ si $I_t = I_{(P)}$, où Q est un facteur irréductible de P dans $K\{X\}$, de même ordre que P. Dans les

deux cas, ce type n'est pas réalisé dans K, puisque le D-idéal correspondant ne contient pas de D-polynôme d'ordre nul ; ce qui contredit que K contient toutes les réalisations de t.

Pour le cas $p > 0$, considérons tout d'abord le cas où la dérivation de Hasse est non triviale sur k. Dans ce cas, on sait que $K := (k^{sep})^{strict}$ est un modèle de CHC_p, il contient donc toutes les réalisations de t. Or K est une extension algébrique de k, donc toute réalisation a de t est algébrique sur k. Maintenant, dans le cas quelconque, considérons K un modèle de CHC_p contenant k, et donc aussi toutes les réalisations de t. Soit x un élément transcendant au dessus de K, le corps des fractions rationnelles $k(x)$, que l'on munit de la D-structure standard, est linéairement disjoint de K au dessus de k (donc aussi algébriquement disjoint, voir [Lan58]). Par disjonction linéaire, $k(x)K$ est isomorphe au corps de fraction de $k(x) \otimes_k K$, on le munit de la D-structure définie dans le fait I.9, ce qui en fait une D-extension commune de $k(x)$ et de K. D'après le cas précédent, une réalisation $a \in K$ de t est algébrique au dessus de $k(x)$. Par disjonction linéaire, a est algébrique au dessus de k. □

Proposition II.3 *Soit A un ensemble de paramètres dans un modèle K de CHC_p. La clôture définissable $dcl(A)$ de A est k^{strict}, où k est le D-corps engendré par A.*

Preuve Le fait que $k^{strict} \subset dcl(A)$ est évident, puisque k est la clôture de A par les applications D et les opérations de corps, et que tout élément de k^{strict} est dans k si $p = 0$ ou défini par une équation purement inséparable $X^{p^n} = a$ avec $a \in k$ si $p > 0$.
Réciproquement, considérons $a \in dcl(A)$, et t le type de a sur k^{strict}. D'après la proposition précédente, a est algébrique sur k^{strict}, notons P son polynôme minimal ; P est séparable car k^{strict} est strict (proposition I.4). Il vient d'après la proposition I.10 que t est isolé par l'équation $P = 0$; donc le polynôme séparable P n'admet qu'une seule racine, il est donc de degré 1, c'est-à-dire $a \in k^{strict}$.□

Chapitre III

Géométrie D-algébrique

III.1 Notions de base de géométrie D-algébrique

Par analogie avec les objets de base de la géométrie algébrique naïve, on présente ceux de la géométrie D-algébrique, qui en constitue un enrichissement. Fixons K un modèle $\aleph_1$-saturé de CHC_p. Soit n un entier supérieur ou égal à 1 ; X désignera la multivariable $(X_1, \ldots, X_n)$.

III.1.1 La D-topologie

Définition III.1 *On appelle sous-variété D-affine de K^n, et aussi variété D-affine, l'ensemble des zéros d'une partie A de $K\{X\}$, on le note*

$$\mathcal{V}(A) := \{x \in K^n | \forall P \in A, P(x) = 0\}.$$

Proposition III.1 *Si V est une sous-variété D-affine de K^n, alors*

$$\mathcal{I}(V) := \{P \in K\{X\} | \forall x \in V, P(x) = 0\}$$

est un D-idéal radiciel de $K\{X\}$.
Les applications $I \mapsto \mathcal{V}(I)$ et $V \mapsto \mathcal{I}(V)$ sont des bijections inverses l'une de l'autre entre l'ensemble des D-idéaux radiciels de $K\{X\}$ et l'ensemble des sous-variétés D-affines de K^n.

Preuve La première assertion est évidente.
Les applications $I \mapsto \mathcal{V}(I)$ et $V \mapsto \mathcal{I}(V)$ sont décroissantes, et vérifient $I \subset \mathcal{I}(\mathcal{V}(I))$ et $V \subset \mathcal{V}(\mathcal{I}(V))$. Pour montrer que ces applications sont bijectives entre les ensembles annoncés, il ne reste donc plus qu'à montrer que pour deux D-idéaux radiciels $I_1 \subsetneq I_2$, $\mathcal{V}(I_2) \subsetneq \mathcal{V}(I_1)$.
Puisque I_1 est l'intersection des D-idéaux premiers le contenant (proposition I.8), il existe un de ces D-idéaux qui ne contient pas I_2 ; quitte à remplacer I_1 par cet idéal, on peut supposer que I_1 est premier.
Soit $(P_\alpha)_{\alpha \in \beta}$ une famille d'éléments de $K\{X\}$ qui engendrent I_1 en tant que D-idéal radiciel ; on peut choisir β fini si $p = 0$, et dénombrable si $p > 0$ (section I.3.1 et théorème I.1). Soit $Q \in I_2 \setminus I_1$. Le corps de fractions L de $K\{X\}/I_1$ est une D-extension de K, la classe x de X dans L est un élément qui vérifie $P_\alpha(x) = 0$ pour tout α et $Q(x) \neq 0$. Puisque K est un D-corps existentiellement

clos, et $\aleph_1$-saturé si $p > 0$, il existe un élément $a \in K$ tel que $P_\alpha(a) = 0$ pour tout α et $Q(a) \neq 0$, c'est-à-dire $a \in \mathcal{V}(I_1) \setminus \mathcal{V}(I_2)$. □

Remarque La démonstration précédente montre que l'hypothèse selon laquelle K est $\aleph_1$-saturé est superflue quand $p = 0$. Ce n'est pas le cas pour $p > 0$.
En effet, soit $k = \mathbb{F}_p(t)^{sep}$ le modèle de CHC_p exhibé dans l'exemple de la section II.1, tel que t est une p-base canonique, et L une extension élémentaire $\aleph_1$-saturée de k. Notons $(a_i)_{i\in\omega}$ une énumération des éléments de $k^{p^\infty} = \mathbb{F}_p^{alg}$. Il existe dans L un couple (x, y) vérifiant $D_i(x) = 0$ pour tout $i \geq 1$ et $D_{p^i}(y)(x - a_i) = 1$ pour tout $i \in \omega$ (car il existe par $\aleph_1$-saturation un élément x dans $L^{p^\infty} \setminus \mathbb{F}_p^{alg}$, puis un élément y vérifiant les conditions voulues qui sont finiment consistantes : considérer l'élément $y_i = \sum_{j=0}^{i} \frac{t^{p^j}}{x-a_j}$). Soit I l'idéal annulateur de (x, y) dans $k\{X, Y\}$, alors $I \subsetneq k\{X, Y\}$ et pourtant dans k, $\mathcal{V}(I) = \mathcal{V}(k\{X, Y\}) = \emptyset$.

On munit K^n d'une topologie, appelée la D-topologie, en fixant pour fermés de K^n les sous-variétés D-affines de K^n. Toute sous-variété D-affine de K^n sera considérée munie de la topologie induite par la D-topologie de K^n, qui sera encore appelée D-toplogie.
Si k est un sous-D-corps de K, on définit la D-topologie à coefficients dans k en fixant pour fermés de K^n les sous-variétés D-affines de K^n de la forme $\mathcal{V}(A)$ pour A une partie de $k\{X\}$. C'est bien entendu une topologie plus grossière que la D-topologie.
Pour tout entier $m \geq 0$, on peut aussi définir la $D_{\leq m}$-topologie : les fermés pour cette topologie sont les zéros des D-idéaux de $K\{X\}_{\leq m}$, c'est-à-dire les intersections des D-idéaux de $K\{X\}$ avec $K\{X\}_{\leq m}$. Les $D_{\leq m}$-topologies sont clairement nœtheriennes ; en particulier, la $D_{\leq 0}$-topologie est la topologie de Zariski.
Par construction, la D-topologie est la limite des $D_{\leq m}$-topologies : un sous-ensemble F de K^n est un D-fermé si et seulement s'il s'écrit $F = \bigcap_{m\geq 0} F_m$, où chaque F_m est un $D_{\leq m}$-fermé.
Sauf mention explicite du contraire, les termes topologiques employés dans la suite se rapporteront toujours à la D-topologie.

Définition III.2 *Soit V une variété D-affine. Si, pour un sous-D-corps k de K, il existe un sous-ensemble A de $k\{X\}$ tel que $V = \mathcal{V}(A)$, on dira que V est définie avec paramètres dans k, ou encore que k est un D-corps de définition pour V.*

Remarque On réservera l'expression "être défini sur" aux variétés algébriques, avec le sens usuel de la géométrie algébrique. Il est bien connu (voir la section 2 de [Pil98] par exemple) que pour un corps k non parfait, une variété affine peut être définie avec paramètres dans k sans être définie sur k.

Proposition III.2 *Soit V une variété D-affine. Il existe un D-corps de définition pour V qui est dénombrable.*

Preuve D'après la proposition 1, $V = \mathcal{V}(\mathcal{I}(V))$; $\mathcal{I}(V)$ est un D-idéal de $K\{X\}$, et $K\{X\}$ est l'union dénombrable des anneaux nœtheriens $K\{X\}_{\leq m}$, pour $m \in \omega$. On en déduit que $\mathcal{I}(V)$ est dénombrablement engendré en tant qu'idéal ; et

on obtient le résultat voulu en notant k le D-corps dénombrable engendré par les coefficients d'une partie génératrice dénombrable de $\mathcal{I}(V)$. □

Proposition III.3 *Toute variété D-affine est compacte. Si $p = 0$, la D-topologie sur K^n est nœtherienne. La D-topologie sur K^n n'est pas nœtherienne pour $p > 0$.*

Preuve Pour $p = 0$, on sait d'après le théorème de Ritt-Raudenbusch (théorème I.1), que tout D-idéal radiciel est finiment engendré en tant que D-idéal radiciel. Par conséquent, il n'existe pas de suite strictement croissante infinie de D-idéaux radiciels, donc la D-topologie est nœtherienne, et a fortiori compacte. Pour $p > 0$, on peut exhiber une suite infinie strictement décroissante de fermés : la suite $(K^{p^m})_{m\geq 0}$. Quant à la compacité, on a vu qu'on peut écrire toute variété D-affine V sous la forme $\mathcal{V}(A)$ pour A une partie dénombrable de $K\{X\}$, de même que tout fermé de V ; en particulier, il n'existe pas de chaîne strictement décroissante de fermés de V de longueur plus que dénombrable. Donc, s'il existe une famille de fermés de V dont l'intersection est vide, on en déduit une chaîne, de longueur au plus dénombrable, de fermés de V, d'intersection vide. La conjonction dénombrable de toutes les équations D-polynomiales définissant chacun de ces fermés n'a donc pas de solution dans K, pas plus que dans les extensions élémentaires de K puisque K est $\aleph_1$-saturé. Cela implique donc d'après le théorème de compacité de la logique du premier ordre qu'une sous-famille finie de ces fermés a une intersection vide. □

Définition III.3 *On appelle variété D-affine irréductible une variété D-affine qui n'est pas recouverte par une union de deux fermés propres.*

Fait III.1 *Une variété D-affine V est irréductible si et seulement si $\mathcal{I}(V)$ est un D-idéal premier.*

Définition III.4 *Soit V une variété D-affine irréductible, et k un D-corps de définition dénombrable pour V. On appelle point générique de V au-dessus de k un élément $x \in V$ tel que, pour tout $P \in k\{X\}$, $P(x) = 0$ si et seulement si $P \in \mathcal{I}(V)$.*

Proposition III.4 *Les points génériques existent toujours dans les variétés D-affines irréductibles. Si V est une variété D-affine définie avec paramètres dans k (dénombrable), l'adhérence d'un point générique de V au-dessus de k, pour la D-topologie sur k, est V.*

Preuve Soit V une sous-variété D-affine irréductible de K^n et k un D-corps de définition dénombrable pour V. Alors $\mathcal{I}(V) \cap k\{X\}$ est un D-idéal premier de $k\{X\}$, il correspond donc à un n-type sur k (corollaire II.2). Par $\aleph_1$-saturation de K, il existe une réalisation x de ce type dans K^n, c'est un point générique de V. □

Remarque Pour $p = 0$, on sait qu'il existe un D-corps de définition finiment engendré pour les variétés D-affines ; il suffirait donc en fait de supposer que K est $\aleph_0$-saturé pour parler de point générique.

III.1.2 Fonctions et morphismes

Définition III.5 *Soit V une variété D-affine et $I = \mathcal{I}(V)$. La K-D-algèbre $K\{V\} := K\{X\}/I$ s'appelle l'anneau des D-coordonnées de V.*

Définition III.6 *Soit V une variété D-affine. On dit qu'une fonction $f : V \longrightarrow K$ est D-régulière en un point $x \in V$ s'il existe un ouvert U de V contenant x, et des D-polynômes P et Q de $K\{X\}$, tels que Q ne s'annule pas sur U et tels que $f_{|U} = \frac{P}{Q}_{|U}$.*
Si $p > 0$, on parlera de fonction p-D-régulière en x s'il existe un ouvert U de V contenant x, un entier $n \geq 0$ et des D-polynômes P et Q de $K\{X\}$, tels que Q ne s'annule pas sur U et tels que $f_{|U}^{p^n} = \frac{P}{Q}_{|U}$ (par convention, pour $p = 0$, p-D-régulier signifiera D-régulier).
Pour un ouvert U de V, on dit qu'une fonction f est D-régulière (respectivement p-D-régulière) sur U si elle l'est en chacun des points de U. On note $\mathcal{O}_V^D(U)$ la K-D-algèbre des fonctions D-régulières sur U.

Remarque Les fonctions p-D-régulières sont en particulier continues. Pour f une fonction D-régulière sur V, on notera $Z(f)$ l'ensemble fermé des zéros de f, et $D(f)$ son complémentaire l'ouvert maximal sur lequel f est inversible. Les $Z(f)$ forment une base des fermés de V : si W est un fermé de V, il s'écrit $W = \bigcap_{f \in I(W)} Z(f)$.

Proposition III.5 *Il existe un homomorphisme injectif de K-D-algèbres de $K\{V\}$ dans $\mathcal{O}_V^D(V)$.*
Si V est irréductible, ces deux K-D-algèbres sont intègres et ont le même corps de fractions ; il est noté $K\langle V\rangle$ et appelé le corps des D-fonctions de V.

Preuve L'opération de restriction à V fournit un homomorphisme de K-D-algèbres $K\{X\} \longrightarrow \mathcal{O}_V^D(V)$. Par définition, le noyau de cet homomorphisme est $\mathcal{I}(V)$, d'où l'homomorphisme injectif $K\{V\} \longrightarrow \mathcal{O}_V^D(V)$.
Si $\mathcal{I}(V)$ est premier, $K\{V\}$ est intègre par définition ; $\mathcal{O}_V^D(V)$ est aussi intègre car V est irréductible et $fg = 0$ dans $\mathcal{O}_V^D(V)$ signifie que $V = Z(f) \cup Z(g)$. $\square$

Remarque Dans le cas d'une variété algébrique affine V définie sur un corps algébriquement clos K, il est bien connu que l'homomorphisme de l'anneau de coordonnées $K[V]$ dans l'ensemble des fonctions régulières $\mathcal{O}_V(V)$ est un isomorphisme. Ce n'est pas le cas ici. Pour $p > 0$, on peut exhiber l'exemple suivant, qui ne fait pas intervenir les dérivations de Hasse mais simplement le fait que K n'est pas algébriquement clos : si $V := \mathbb{A}^1(K)$ est l'espace affine de dimension 1, et si $b \in K \setminus K^p$, alors la fonction $\frac{1}{X^p - b}$ est dans $\mathcal{O}_V^D(V)$, mais pas dans $K\{V\}$. On peut aussi exhiber un exemple valable quelque soit la caractéristique (donc même dans le cas où $p = 0$ et K est algébriquement clos) : considérons V la sous-variété D-affine de K définie par le D-idéal $(d_i X)_{i>0}$. Soit $a \notin C_K^\infty$, alors la fonction $\frac{1}{X-a}$ est dans $\mathcal{O}_V^D(V)$, mais pas dans $K\{V\}$, qui s'identifie avec $K[X]$.

Définition III.7 *Soit V une sous-variété D-affine de K^m et W une sous-variété D-affine de K^n. On appelle morphisme (respectivement p-morphisme) de variétés D-affines une application $f : V \longrightarrow W$ telle que les composantes $(f_1, \ldots, f_n)$ de f sont des fonctions D-régulières (respectivement p-D-régulières) sur V.*

III.1.3 Les variétés D-algébriques

Définition III.8 *On appelle variété D-algébrique un espace topologique V, muni d'un recouvrement ouvert fini $U_1, \ldots, U_n$, tel que :*
- *pour tout i, il existe une bijection bicontinue $f_i : U_i \longrightarrow V_i$, pour une certaine variété D-affine V_i ;*
- *pour tous i, j, si on note $V_{ij} := f_i(U_i \cap U_j) \subset V_i$ et $V_{ji} := f_j(U_i \cap U_j) \subset V_j$, l'application $f_j \circ f_i^{-1} : V_{ij} \longrightarrow V_{ji}$ est un isomorphisme de variétés D-affines.*

Définition III.9 *Soient $(V, (U_i), (f_i), (V_i))$ et $(W, (T_j), (g_j), (W_j))$ deux variétés D-algébriques. On appelle morphisme (respectivement p-morphisme) de variétés D-algébriques une application $f : V \longrightarrow W$ telle que pour tous i, j, $g_j \circ f_{|U_i} \circ f_i^{-1} : f_i(f^{-1}(T_j)) \cap V_i \longrightarrow W_j$ est un morphisme (respectivement p-morphisme) de variétés D-affines.*
En particulier, on appelle fonction D-régulière (respectivement p-D-régulière) sur une variété D-algébrique V un morphisme (respectivement un p-morphisme) de V dans K.

Fait III.2 *La composée de deux morphismes de variétés D-algébriques est un morphisme de variétés D-algébriques. La composée de deux p-morphismes est un p-morphisme.*

Définition III.10 *Soit V une variété D-algébrique. On munit V d'un faisceau $\mathcal{O}_V^D$ de K-D-algèbres en définissant, pour tout ouvert U de V, $\mathcal{O}_V^D(U)$ comme étant la K-D-algèbre des fonctions D-régulières sur U.*
Si V est un irréductible, on appelle corps des D-fonctions de V la limite inductive :

$$K\langle V\rangle := \varinjlim_{\emptyset \neq U \text{ ouvert } \subset V} \mathcal{O}_V^D(U).$$

Remarque Si V est une variété D-algébrique irréductible, la K-D-algèbre $K\langle V\rangle$ est un D-corps, et la définition est cohérente avec la précédente dans le cas où V est une variété D-affine (l'argument est exactement le même que dans le cas de la géométrie algébrique).

Fait III.3 *Si V et W sont deux variétés D-algébriques, on munit $V \times W$ d'une structure de variété D-algébrique exactement comme en géométrie algébrique. En particulier, au niveau des faisceaux de fonctions régulières, on a l'isomorphisme*

$$\mathcal{O}_{V\times W}^D \simeq \mathcal{O}_V^D \otimes_K \mathcal{O}_W^D.$$

C'est un isomorphisme de faisceaux de K-D-algèbres quand on munit $\mathcal{O}_V^D \otimes_K \mathcal{O}_W^D$ de la dérivation de Hasse donnée dans le fait I.9, à savoir celle définie par

$$D_n(f \otimes g) = \sum_{i=0}^{n} D_i(f) \otimes D_{n-i}(g).$$

Définition III.11 *On appelle groupe D-algébrique une variété D-algébrique G, munie de deux morphismes de variétés D-algébriques $m : G \times G \longrightarrow G$ et ${}^{-1} : G \longrightarrow G$, ainsi que d'un point distingué $e \in G$ tels que $(G, m, {}^{-1}, e)$ soit un groupe.*

III.1.4 Les variétés algébriques vues comme variétés D-algébriques

Soit V une variété affine définie sur K, d'idéal I dans $K[X]$; alors $\mathcal{V}(I)$ est une variété D-affine. D'autre part, une fonction régulière est un cas particulier de fonction D-régulière (car les ouverts de Zariski sont des D-ouverts). Il en résulte donc un foncteur, noté

$$V \mapsto \hat{V} \quad ; \quad \phi \mapsto \hat{\phi}$$

de la catégorie des variétés algébriques dans celle des variétés D-algébriques (respectivement de la catégorie des groupes algébriques dans celle des groupes D-algébriques).
Pour V une variété algébrique, la D-topologie sur V est plus fine que la topologie de Zariski. On a le résultat suivant :

Théorème III.1 *Soit V une variété algébrique lisse et irréductible. Alors $\hat{V}$ est irréductible.*

Remarque Pour $p = 0$, l'hypothèse selon laquelle V est lisse est superflue ; on peut en trouver la démonstration dans [Mar96], appendice C. Pour $p > 0$, cette hypothèse est au contraire indispensable. Considérons par exemple la sous-variété affine de K^3, irréductible mais non-lisse

$$V = \{(x, y, z) \in K^3 | x^p + y^p z = 0\}.$$

On sait par la proposition I.12 qu'il existe un plus petit D-idéal irréductible Q de $K\{x, y, z\}$ tel que $Q \cap K[x, y, z]$ est l'idéal de V ; en particulier $y \notin Q$ et $d_1 z \in Q$. On constate alors que $\hat{V}$ est recouvert par deux D-fermés propres, dont les D-idéaux sont respectivement Q et le D-idéal engendré par (x, y).

Preuve On montre tout d'abord le résultat dans le cas où V est une variété affine. Soit I l'idéal (dans $K[X]$) du type générique (au sens de la géométrie algébrique) de V. Puisque I est un idéal séparable, on peut considérer (proposition I.12) Q, le plus petit D-idéal irréductible (dans $K\{X\}$) tel que $Q \cap K[X] = I$. On sait qu'il existe $S \in K[X] \setminus I$ tel que Q est le plus petit D-idéal irréductible contenant I mais pas S. On doit montrer que $V = \mathcal{V}(Q)$, et on va utiliser pour cela le lemme suivant, qui correspond au lemme C.2 de [Mar96].

Lemme III.1 *Avec les notations précédentes, soit $\alpha \in V(K)$. Il existe une D-extension L de K, et $\beta \in V(L)$ tel que $S(\beta) \neq 0$ et $I_{\beta/K} \subset I_{\alpha/K}$.*

Preuve du lemme Soit $\mathcal{M}_\alpha$ l'idéal maximal de l'anneau local $\mathcal{O}_{V,\alpha}$, et d la dimension de V. Comme α est un point rationnel et simple (car V est lisse), l'espace vectoriel $\mathcal{M}_\alpha/\mathcal{M}_\alpha^2$ est de dimension d. Fixons $t_1, \ldots, t_d$ dans $\mathcal{M}_\alpha$ tels que leurs images forment une base de $\mathcal{M}_\alpha/\mathcal{M}_\alpha^2$. On obtient alors un homomorphisme injectif ϕ de $\mathcal{O}_{V,\alpha}$ dans l'anneau des séries formelles $K[[t_1, \ldots, t_d]]$, par la méthode présentée dans [Lan58], page 206 : pour $w \in \mathcal{O}_{V,\alpha}$, il existe une unique suite $(f_j)_{j\in\omega}$ telle que pour tout $m \in \omega$, f_m est un polynôme homogène de degré m à coefficients dans K en les variables $t_1, \ldots, t_d$ et $w = \sum_{j=0}^{m} f_j \mod \mathcal{M}_\alpha^{m+1}$. On pose alors $\phi(w) = \sum_{j\geq 0} f_j$. Par passage aux corps de fractions, on en déduit un plongement de $K(V)$, le corps de fonctions de V, dans le corps des séries

de Laurent $L := K((t_1, \ldots, t_d))$. On remarque que ϕ envoie $\mathcal{M}_\alpha$ vers l'idéal $(t_1, \ldots, t_d)$.
L'homomorphisme $\pi : \mathcal{O}_{V,\alpha} \longrightarrow K$ d'évaluation en α s'étend naturellement en l'homomorphisme de $K[[t_1, \ldots, t_d]]$ dans K, associant à une série de entière son terme de degré nul.
Prolongeons les dérivées de Hasse de K à $K((t_1, \ldots, t_d))$ en posant $D_i(t_j) = 0$ pour tout $i > 0$ et $1 \leq j \leq d$. En particulier, le sous-anneau $K[[t_1, \ldots, t_d]]$ est stable par D, et chacun des D_i transforme un polynôme homogène de degré j en un polynôme homogène de degré inférieur ou égal à j (éventuellement nul), obtenu en appliquant D_i à chacun des coefficients du polynôme. Alors π est un homomorphisme de K-D-algèbres entre $K[[t_1, \ldots, t_d]]$ et K, puisque :

$$D_i(\pi(\sum_{j\geq 0} f_j)) = D_i(f_0) = \pi(\sum_{j\geq 0} D_i(f_j)) = \pi(D_i(\sum_{j\geq 0} f_j)).$$

Soit $\beta = (x_1, \ldots, x_n)$ les fonctions coordonnées dans $\mathcal{O}_{V,\alpha} \subset L$ (via le plongement ϕ). On a bien entendu $\pi(\beta) = \alpha$, et alors pour tout $f \in K\{X\}$, si $f(\beta) = 0$, alors $f(\alpha) = f(\pi(\beta)) = \pi(f(\beta)) = 0$. On a donc bien $I_{\beta/K} \subset I_{\alpha/K}$, et $S(\beta) \neq 0$ puisque $S \notin I$ et β est un point générique dans $V(L)$. □
Alors, pour tout $\alpha \in V(K)$, soit $\beta \in V(L)$ déterminé comme dans le lemme. On a $I \subset I_{\beta/K}$ et $S \notin I_{\beta/K}$; donc par minimalité de Q, $Q \subset I_{\beta/K}$, donc aussi $Q \subset I_{\alpha/K}$ par construction. Ainsi, $\alpha \in \mathcal{V}(Q)$, donc $\hat{V} = \mathcal{V}(Q)$ et $\hat{V}$ est irréductible.
Maintenant, dans le cas général, soit $V = U_1 \cup \ldots \cup U_n$ un recouvrement de V par des ouverts irréductibles, et pour tout i, des applications bicontinues $f_i : U_i \longrightarrow V_i$, les V_i étant des variétés affines irréductibles et lisses. Supposons qu'il existe un recouvrement de $\hat{V}$ par deux fermés propres F et G, alors pour tout i, on a $U_i(K) \subset F$ ou $U_i(K) \subset G$, car $\hat{V}_i$ est irréductible d'après le cas particulier précédent. Puisque F et G sont des fermés propres, aucun d'eux ne peut contenir tous les $U_i(K)$; disons donc par exemple que $U_1(K) \subset F$, $U_1(K) \not\subset G$ et $U_2(K) \subset G$. On sait que $V_{12} := f_1(U_1 \cap U_2)$ est un ouvert non-vide de V_1, $V_{12}(K)$ est donc dense dans $\hat{V}_1$, qui est irréductible. On en déduit que le fermé $f_1(U_1 \cap G)(K)$, qui contient $V_{12}(K)$, est égal à $\hat{V}_1$; et donc $U_1(K) \subset G$, ce qui est une contradiction. □

III.2 Structure supplémentaire sur les objets de la géométrie algébrique

On s'intéresse ici aux objets de la géométrie algébrique naïve, c'est-à-dire obtenus par recollement de variétés affines dans K, sans considération sur les schémas. Pour comprendre quelle structure supplémentaire leur est donnée par les dérivations de Hasse, on considère les constructions (purement algébriques) suivantes.

III.2.1 Les prolongations

La première construction considérée est celle des prolongations. L'étude de ces prolongations a déjà été faite dans le cas de la caractéristique nulle (voir par exemple [Pil96a] et [Mar00], où une version de la proposition III.6 est montrée) ;

pour la caractéristique positive, signalons que Piotr Kowalski et Anand Pillay ont aussi travaillé indépendamment sur ces objets.
On définit tout d'abord les prolongations pour les sous-variétés affines de K^n ; X, $X^{(i)}$ désigneront des multivariables de taille n.
Soit $P \in K[X]$, on notera $\overline{D_j}P$ le polynôme de $K[X^{(0)}, \ldots, X^{(j)}]$ tel que, dans $K\{X\}$, $D_j(P) = \overline{D_j}P(d_0X, \ldots, d_jX)$.

Définition III.12 *Soit V une sous-variété affine de $\mathbb{A}^n$ définie sur K, et $j \geq 0$ un entier. On appelle j-ème prolongation de V la sous-variété affine de $\mathbb{A}^{(j+1)n}$, définie sur K, dont les points K-rationnels sont :*

$$\Delta_j V(K) = \{(x^{(0)}, \ldots, x^{(j)}) \in K^{(j+1)n} | \\ \forall P \in I(V), \forall 0 \leq i \leq j, \overline{D_i}P(x^{(0)}, \ldots, x^{(i)}) = 0\}.$$

Soit $i \leq j$ deux entiers. La troncature $(x^{(0)}, \ldots, x^{(j)}) \mapsto (x^{(0)}, \ldots, x^{(i)})$ définit un morphisme de $\Delta_j V$ dans $\Delta_i V$, noté $\pi_{j,i}$. On a la relation : $\pi_{k,i} = \pi_{j,i} \circ \pi_{k,j}$. Pour $x \in V$ et $P \in I(V)$, on a $D_i(P(x)) = (\overline{D_i}P)(D_0(x), \ldots, D_i(x)) = 0$, donc $(D_0(x), \ldots, D_j(x)) \in \Delta_j V(K)$. On notera δ_j l'injection $\mathcal{L}_H$-définissable de $V(K)$ dans $\Delta_j V(K)$ ainsi définie. Ces injections vérifient, pour tout $i \leq j$, $\delta_i = \pi_{j,i} \circ \delta_j$, et en particulier $\pi_{j,0} \circ \delta_j = id_V$.

Proposition III.6 *Supposons que V est une sous-variété lisse et irréductible de $\mathbb{A}^n$, de dimension d et définie sur K. Alors $\Delta_j V$ est lisse, irréductible, de dimension $(j+1)d$ et $\delta_j(V)$ est Zariski-dense dans $\Delta_j V$; et les morphismes $\pi_{j,i}$ sont surjectifs, dans le sens ensembliste et en tant que morphismes (c'est-à-dire génériquement surjectifs et séparables).*

Preuve On fixe k un corps de définition dénombrable de V, et a une réalisation du type générique de $\hat{V}$ au dessus de k, exhibé dans le théorème III.1. On va montrer par récurrence sur j que $\Delta_j V$ est lisse et de dimension $(j+1)d$; que c'est la clôture de Zariski (au dessus de k) de $\delta_j(a)$ et que le morphisme $\pi_{j,j-1}$ est surjectif au sens ensembliste et séparable. On va aussi montrer que pour tout c dans $V(K)$, $\pi_{j,0}^{-1}(c)$ est irréductible.
Pour $j = 0$, $V = \delta_0(V) = \Delta_0 V$ est de dimension d et est la clôture de Zariski de $\delta_0(a) = a$ d'après le théorème III.1.
Soit $P_1, \ldots, P_m$ un système de polynômes générateurs de $I(V)$; puisque V est lisse, la matrice jacobienne

$$J(V) = \begin{pmatrix} \frac{\partial P_1}{\partial X_1} & \cdots & \frac{\partial P_1}{\partial X_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial P_m}{\partial X_1} & \cdots & \frac{\partial P_m}{\partial X_n} \end{pmatrix}$$

est de rang $n - d$ en tout point de V.
Par définition, les polynômes $(\overline{D_i}P_h)_{0 \leq i \leq j, 1 \leq h \leq m}$ appartiennent à $I(\Delta_j V)$, et donc le rang de la matrice jacobienne en un point x de $\Delta_j V$ est supérieur à celui de la matrice

$$A(x) := \Big(\frac{\partial \overline{D_i}P_h}{\partial X_l^{(g)}}(x)\Big)_{\substack{0 \leq i \leq j, 1 \leq h \leq m \\ 0 \leq g \leq j, 1 \leq l \leq n}}.$$

Les propriétés des dérivations de Hasse donnent (voir le fait I.10) :

$$\overline{D_i}P_h = Q_{h,i}(X^{(0)}, \ldots, X^{(i-1)}) + \sum_{l=1}^{n} \frac{\partial P_h}{\partial X_l} X_l^{(i)} \quad \text{pour un polynôme } Q_{h,i}.$$

Par conséquent, la matrice $A(x)$ s'écrit par blocs ($(j+1)\times(j+1)$ blocs de taille $m \times n$) :

$$A(x) = \begin{pmatrix} J_{\pi_{j,0}(x)}(V) & 0 & \ldots & 0 \\ * & J_{\pi_{j,0}(x)}(V) & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ * & \ldots & * & J_{\pi_{j,0}(x)}(V) \end{pmatrix}.$$

En particulier, le rang de $A(x)$, et donc celui de $J_x(\Delta_j V)$, vaut au moins $(j+1)(n-d)$, donc la dimension de l'espace tangent à V en tout point x est au plus $(j+1)d$.
Notons F la composante irréductible de $\delta_j(a)$ dans $\Delta_j V$; d'après la remarque suivant la proposition I.12, la dimension de $\delta_j(a)$ au dessus de k est $(j+1)d$, et l'inégalité précédente sur les espaces tangents donne que la dimension de F vaut $(j+1)d$, que $\delta_j(a)$ est un point générique de F au dessus de k et que F est lisse, en tant que composante de $\Delta_j V$. En particulier, F est disjoint des éventuelles autres composantes irréductibles de $\Delta_j V$. D'autre part, puisque δ_j est un isomorphisme de variétés D-algébriques entre $\hat{V}$, qui est irréductible, et $\delta_j(\hat{V})$, on obtient que $\delta_j(V)$ est contenu dans F.
Montrons la surjectivité de $\pi_{j,j-1}$. Puisque V est lisse, la matrice jacobienne $J_c(V)$ est de rang $n-d$ pour tout $c \in V(K)$. Pour une suite d'indices $1 \leq i_1 < \ldots < i_{n-d} \leq n$, l'ensemble des points c de $V(K)$ tels que les colonnes d'indices $i_1, \ldots, i_{n-d}$ de $J_c(V)$ sont linéairement indépendantes forme un ouvert de V (la condition s'exprime par la non nullité de certains mineurs, dont les coefficients sont des polynômes en c). Les images réciproques de ces ouverts par $\pi_{j-1,0}$ forment un recouvrement ouvert de $\Delta_{j-1}V$; ces ouverts sont notés $O_{i_1,\ldots,i_{n-d}}$. Soit $b \in \Delta_{j-1}V(K)$ et $c = \pi_{j-1,0}(b)$, alors

$$\pi_{j,j-1}^{-1}(b) = \left\{ (b, x^{(j)}) \in K^{(j+1)n} \middle| J_c(V) \begin{pmatrix} x_1^{(j)} \\ \vdots \\ x_n^{(j)} \end{pmatrix} + \begin{pmatrix} Q_{1,j-1}(b) \\ \vdots \\ Q_{m,j-1}(b) \end{pmatrix} = 0 \right\}.$$

L'ensemble des points $b \in O_{i_1,\ldots,i_{n-d}}$ tels que $(Q_{1,j-1}(b) \ldots Q_{m,j-1}(b))$ soit dans l'image de $J_c(V)$ forment un fermé de $O_{i_1,\ldots,i_{n-d}}$ (annulation de mineurs dont les coefficients sont des polynômes en b). Or pour $\delta_{j-1}(a)$, qui est un point générique de $\Delta_{j-1}V$, le système

$$J_a(V) \begin{pmatrix} x_1^{(j)} \\ \vdots \\ x_n^{(j)} \end{pmatrix} + \begin{pmatrix} Q_{1,j-1}(\delta_{j-1}(a)) \\ \vdots \\ Q_{m,j-1}(\delta_{j-1}(a)) \end{pmatrix} = 0$$

a une solution (à savoir $D_j(a)$), donc pour tout $b \in \Delta_{j-1}V(K)$, le système

$$J_{\pi_{j-1,0}(b)}(V)\begin{pmatrix} x_1^{(j)} \\ \vdots \\ x_n^{(j)} \end{pmatrix} + \begin{pmatrix} Q_{1,j-1}(b) \\ \vdots \\ Q_{m,j-1}(b) \end{pmatrix} = 0$$

a une solution. Il existe donc $e \in \Delta_j V(K)$ tel que $\pi_{j,j-1}(e) = b$.
Pour montrer que le morphisme $\pi_{j,j-1}$ est surjectif, il suffit donc de montrer maintenant qu'il est séparable. C'est clair car un point générique e de la préimage $\pi_{j,j-1}^{-1}(b)$ est b concaténé avec une solution générique d'un système linéaire à coefficients dans $k(b)$, et donc l'extension $k(e)/k(b)$ est purement transcendante.
On montre maintenant que, pour tout $c \in V(K)$, $\pi_{j,0}^{-1}(c)$ est irréductible. C'est le cas pour $\pi_{j-1,0}^{-1}(c)$ d'après l'hypothèse de récurrence. On vient de voir que pour tout $b \in \pi_{j-1,0}^{-1}(c)$, le système

$$J_c(V)\begin{pmatrix} x_1^{(j)} \\ \vdots \\ x_n^{(j)} \end{pmatrix} + \begin{pmatrix} Q_{1,j-1}(b) \\ \vdots \\ Q_{m,j-1}(b) \end{pmatrix} = 0$$

a une solution. On peut obtenir une solution rationnelle : si on suppose par exemple que les $n-d$ premières colonnes de $J_c(V)$ sont linéairement indépendantes, il suffit de fixer $x_{n-d+1}^{(j)} = \ldots = x_n^{(j)} = 0$, et les autres variables s'obtiennent rationnellement en fonction de $Q_{1,j-1}(b), \ldots, Q_{m,j-1}(b)$. On obtient donc une application rationnelle $s : \pi_{j-1,0}^{-1}(c) \longrightarrow \pi_{j,0}^{-1}(c)$ telle que $\pi_{j,j-1} \circ s = id$. Comme $\pi_{j,j-1}^{-1}(b)$ est irréductible pour tout point b (c'est un espace affine), on en déduit que $\pi_{j,0}^{-1}(c)$ est irréductible.
On conclut maintenant en montrant que $\Delta_j V$ est irréductible. On a vu que la composante irréductible de V contenant $\delta_j(V)$, notée F, est disjointe de la réunion des autres composantes irréductibles, notée G. S'il existe b dans G, soit $c = \pi_{j,0}(b)$. Puisque $\pi_{j,0}^{-1}(c)$ est irréductible, et que F et G sont disjoints, $\pi_{j,0}^{-1}(c)$ ne peut pas rencontrer à la fois F et G ; or, $b \in G$ et $\delta_j(c) \in \delta_j(V) \subset F$ sont envoyés sur c par $\pi_{j,0}$, ce qui contredit l'existence de b.
On obtient ainsi que $\Delta_j V$ est irréductible, lisse et de dimension $(j+1)d$; et c'est la clôture de Zariski de $\delta_j(a)$. □

Soit $O = \overline{O} \setminus F$ une variété quasi-affine (c'est-à-dire un ouvert d'une sous-variété affine), lisse, irréductible et définie sur K. Le fermé F est défini par une conjonction d'équations polynomiales dans $K[X]$; en identifiant $K[X]$ à une sous-algèbre de $K[X^{(0)}, \ldots, X^{(j)}]$ (par l'injection donnée par $X \mapsto X^{(0)}$), on obtient un fermé $F(X^{(0)})$. On définit alors :

$$\Delta_j O := \Delta_j \overline{O} \setminus F(X^{(0)}).$$

On vérifie qu'on a encore une injection $\delta_j : O \longrightarrow \Delta_j O$ et que $\delta_j(O)$ est relativement Zariski-dense dans $\Delta_j O$.

Les prolongations Δ_j des morphismes
Soit O une variété quasi-affine, lisse, irréductible et définie sur K, et $f = P/Q$

une fraction rationnelle de O dans K, définie sur K (Q ne s'annule pas sur O). On définit, pour $i \leq j$, $\overline{D_i} f \in K(X^{(0)}, \ldots, X^{(j)})$ par

$$\overline{D_i} f = \frac{\overline{D_i} P - \sum_{h<i} \overline{D_h} f \overline{D_{i-h}} Q}{Q}.$$

Pour $x \in O$, on constate aisément que $\overline{D_i} f(\delta_j(x)) = D_i(f(x))$. Cette propriété caractérise la fraction rationnelle $\overline{D_i} f$, car $\delta_j(O)$ est dense dans $\Delta_j O$. En particulier, cela implique que $\overline{D_i} f$ est indépendant du choix du représentant P/Q. On note $\Delta_j f = (\overline{D_0} f, \ldots, \overline{D_j} f)$ le morphisme de variétés quasi-affines entre $\Delta_j O$ et $\Delta_j \mathbb{A}^1$.
Soient V et W deux variétés quasi-affines lisses, irréductibles et définies sur K, et $f : V \longrightarrow W$ un morphisme, défini sur K. On construit alors un morphisme $\Delta_j f : \Delta_j V \longrightarrow \Delta_j W$ en appliquant localement la construction précédente sur chacune des composantes de f. Par densité de $\delta_j(V)$ dans $\Delta_j V$, on obtient encore que $\Delta_j f$ est le seul morphisme de $\Delta_j V$ dans $\Delta_j W$ tel que $\delta_j \circ f = \Delta_j f \circ \delta_j$ sur $V(K)$.

Notons qu'on obtient ainsi des applications entre faisceaux de fonctions $\mathcal{O}_V \longrightarrow \mathcal{O}_{\Delta_j V}$. Pour $i \leq j$, et $f \in \mathcal{O}_V$, la $i+1$-ème composante $\overline{D_i} f$ de $\Delta_j f$ est un élément de $\mathcal{O}_{\Delta_j V}$. Si $h \geq j \geq i$, on peut aussi voir $\overline{D_i} f$ comme la $i+1$-ème composante de $\Delta_h V$; et cette fonction est l'image par $\pi^{\#}_{h,j}$ de la composante $\overline{D_i} f$ de $\Delta_j V$ (car $\pi_{h,j} \circ \delta_h = \delta_j$). Pour préciser le domaine de la fonction, on notera $\pi^{\#}_{j,i} \circ \overline{D_i} f \in \mathcal{O}_{\Delta_j V}$ la $i+1$-ème composante de $\Delta_j V$.
De la caractérisation $\pi^{\#}_{j,i} \circ \overline{D_i} f(\delta_j(x)) = D_i(f(x))$, on déduit aisément que les applications $\pi^{\#}_{j,i} \circ \overline{D_i} : \mathcal{O}_V \longrightarrow \mathcal{O}_{\Delta_j V}$ vérifient des propriétés semblables à celles de la dérivation de Hasse pour la somme et le produit : ce sont des applications additives, avec $\pi^{\#}_{j,0} \circ \overline{D_0} = \pi^{\#}_{j,0}$, et telles que

$$\pi^{\#}_{j,i} \circ \overline{D_i}(fg) = \sum_{h=0}^{i} (\pi^{\#}_{j,h} \circ \overline{D_h} f)(\pi^{\#}_{j,j-h} \circ \overline{D_{j-h}} g).$$

Les prolongations Δ_j comme foncteurs de la catégorie des variétés algébriques lisses et irréductibles
La construction de la famille de foncteurs $(\Delta_j)_{j \in \omega}$ sur la catégorie des variétés quasi-affines lisses, irréductibles et définies sur K s'étend à la catégorie des variétés algébriques lisses, irréductibles et définies sur K de la manière suivante. Soit V une variété algébrique lisse irréductible et définie sur K, recouverte par des ouverts (U_s), avec des homéomorphismes $f_s : U_s \longrightarrow V_s$ pour des sous-variétés affines lisses irréductibles V_s, définies sur K. Les isomorphismes $f_{st} := f_t \circ f_s^{-1}$ entre les variétés quasi-affines lisses $V_{st} := f_s^{-1}(U_s \cap U_t)$ et $V_{ts} := f_t^{-1}(U_s \cap U_t)$ induisent des isomorphismes $\Delta_j f_{st} : \Delta_j V_{st} \longrightarrow \Delta_j V_{ts}$, qui permettent le recollement des sous-variétés affines $(\Delta_j V_s)$ le long des ouverts $(\Delta_j V_{st})$. La variété algébrique lisse ainsi obtenue est notée $\Delta_j V$.
On peut étendre carte par carte la construction de l'injection $\delta_j : V(K) \longrightarrow \Delta_j V(K)$, son image est dense dans $\Delta_j V$; ainsi que la construction des morphismes surjectifs $\pi_{j,i} : \Delta_j V \longrightarrow \Delta_i V$ (pour $i \leq j$). Ces applications vérifient encore les relations : $\pi_{k,i} = \pi_{j,i} \circ \pi_{k,j}$ et $\delta_i = \pi_{j,i} \circ \delta_j$.

Les constructions des morphismes $\Delta_j f : \Delta_j V \longrightarrow \Delta_j W$ s'étendent sans difficulté pour les morphismes de variétés algébriques lisses irréductibles $f : V \longrightarrow W$, et les diagrammes suivants sont commutatifs :

$$\begin{array}{ccc} V(K) & \xrightarrow{f} & W(K) \\ \downarrow{\scriptstyle \delta_j} & & \downarrow{\scriptstyle \delta_j} \\ \Delta_j V(K) & \xrightarrow{\Delta_j f} & \Delta_j W(K) \end{array} \quad , \quad \begin{array}{ccc} \Delta_j V & \xrightarrow{\Delta_j f} & \Delta_j W \\ \downarrow{\scriptstyle \pi_{j,i}} & & \downarrow{\scriptstyle \pi_{j,i}} \\ \Delta_i V & \xrightarrow{\Delta_i f} & \Delta_i W \end{array} .$$

Soit $(G, m, ^{-1}, e)$ un groupe algébrique irréductible défini sur K. Les propriétés fonctorielles de Δ_j font de $(\Delta_j G, \Delta_j m, \Delta_j^{-1}, \delta_j(e))$ un groupe algébrique. Les Δ_j sont des foncteurs de la catégorie des groupes algébriques irréductibles. Les applications δ_j et $\pi_{j,i}$ sont des homomorphismes de groupes.
On a ainsi obtenu qu'une variété algébrique V, lisse, irréductible et définie sur K, vient avec un système projectif $(\Delta_j V, \pi_{j,i})$. On dispose de "sections" définissables $\delta_i : V(K) \longrightarrow \Delta_i V(K)$ pour ce système ; la question de l'existence de sections rationnelles sera discutée dans la section III.2.3.

III.2.2 Foncteurs Π_n et restriction du corps de base

Dans cette section, on suppose $p > 0$.
Rappelons la construction des foncteurs Π_n, composés du foncteur Frobenius à la puissance n (Fr^n) et des foncteurs Λ_n, explicitement construits dans [BouDel01], section 1.2.4. Cette construction dépend a priori du choix d'une p-base (b) et des applications coordonnées $\varphi_n : K \longrightarrow (K^{p^n})^{\times p^n}$ pour la base correspondante de K sur K^{p^n} (plus précisément, $x = \sum_{i=0}^{p^n-1} \varphi_{n,i}(x) b^i$, comme dans la définition I.7), mais l' interprétation en terme de restriction du corps de base montrera que les foncteurs Π_n obtenus sont isomorphes au-dessus de K^{p^n}.
Si $O = \overline{O} \setminus F$ est une sous-variété quasi-affine, définie sur K, de $\mathbb{A}^m$, avec $F = V(I)$, alors on définit $\Pi_n O$ comme sous-variété affine de $\mathbb{A}^{mp^n}$ par :

$$\Pi_n O(K^{p^n}) = \overline{\varphi_n(O)} \setminus V(I(\sum_{i=0}^{p^n-1} X_i b^i)),$$

où $I(\sum_{i=0}^{p^n-1} X_i b^i)$ désigne l'idéal de $K[X_0, \ldots, X_{p^n-1}]$ obtenu en remplaçant X par $\sum_{i=0}^{p^n-1} X_i b^i$ pour chaque élément de I.
L'image $\varphi_n(O)$ est relativement Zariski-dense dans $\Pi_n(O)$, et φ_n est une "section" définissable pour le morphisme

$$\begin{array}{cccc} \rho_n & : & \Pi_n O & \longrightarrow & O \\ & & (x_i)_{0 \leq i \leq p^n-1} & \mapsto & \sum_{i=0}^{p^n-1} x_i b^i \end{array} .$$

Pour un morphisme de variétés quasi-affines $f : V \longrightarrow W$, le tout étant défini sur K, on définit $\Pi_n f$ comme étant le seul morphisme de $\Pi_n V$ dans $\Pi_n W$ vérifiant $\Pi_n f(\varphi_n(x)) = \varphi_n(f(x))$ pour tout $x \in V$.
On obtient ainsi un foncteur de la catégorie des variétés quasi-affines définies sur K, on l'étend par la même méthode de recollement que dans la section précédente en un foncteur de la catégorie des variétés algébriques définies sur K, ainsi qu'en un foncteur de la catégorie des groupes algébriques définis sur K (dans ce cas, φ_n et ρ_n sont des homomorphismes de groupes).

Fait III.4 *Si une variété algébrique V est définie sur le corps K, alors $\Pi_n V$ est définie sur K^{p^n}.*

Proposition III.7 *Pour une variété algébrique V définie sur K, le morphisme $\rho_n : \Pi_n V \longrightarrow V$ est surjectif.*

Preuve Il est génériquement surjectif car K est séparablement clos et pour tout $x \in V(K)$, $x = \rho_n(\varphi_n(x))$.
Pour montrer que ρ_n est séparable, considérons une composante irréductible F de $\Pi_n V$, d'image G par ρ_n. Soit $I(G)$ l'idéal premier séparable de G dans $k[X]$ (où k désigne un D-corps de définition dénombrable contenant la p-base fixée b). D'après la proposition I.12, il existe un idéal Q de $k\{X\}$, minimal tel que $Q \cap k[X] = I(G)$. Soit $y \in G(K)$ réalisant l'idéal Q. Puisque $\Pi_n V$ est la clôture de $\varphi_n(V(K))$, il existe un point $x \in G(K)$ tel que $\varphi_n(x)$ soit générique dans F. La minimalité de Q donne que $I_{\varphi_n(y)/k} \subset I_{\varphi_n(x)/k}$ (car cet idéal a une intersection avec $k[X]$ égale à $I(G)$) ; et comme F est une composante irréductible de $\Pi_n V$, cela signifie que $I(F) = I_{\varphi_n(y)}$. Or, puisque y est une réalisation de Q, on a que $k(\{y\})$ est une extension purement transcendante de $k(y)$ (voir la proposition I.12), ce qui donne que $k(\varphi_n(y))$ est une extension purement transcendante, donc séparable, de $k(\rho_n(\varphi_n(y))) = k(y)$. □

Rappelons maintenant la notion de restriction du corps de base, développée dans [Spr98].

Définition III.13 *Soit $E \subset F$ une extension finie de corps, et V une variété algébrique définie sur F. On dit que V admet une restriction du corps de base s'il existe une variété algébrique $\Pi_{F/E} V$, définie sur E, ainsi qu'un morphisme surjectif (défini sur F) $\pi_{F/E} : \Pi_{F/E} V \longrightarrow V$, tels que :*
pour toute variété algébrique W définie sur E et tout morphisme $\phi : W \longrightarrow V$, défini sur F, il existe un unique morphisme $\psi : W \longrightarrow \Pi_{F/E} V$, défini sur E, tel que $\phi = \pi_{F/E} \circ \psi$.
Si V admet une restriction du corps de base, celle-ci est définie à unique isomorphisme défini sur E près.

Si V et W admettent des restrictions du corps de base, et si $f : V \longrightarrow W$ est un morphisme défini sur F, alors il existe un unique morphisme $\Pi_{F/E} f$, défini sur E, tel que le diagramme suivant commute :

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ \uparrow{\scriptstyle \pi_{F/E}} & & \uparrow{\scriptstyle \pi_{F/E}} \\ \Pi_{F/E} V & \xrightarrow{\Pi_{F/E} f} & \Pi_{F/E} W \end{array}$$

On obtient ainsi un foncteur (partiel) de la catégorie des variétés algébriques définies sur F dans celle des variétés algébriques définies sur E.

Remarque La définition de la restriction du corps de base donnée ici est moins restrictive que celle donnée dans les appendices 2 et 3 de [Oes84], qui fait porter la propriété universelle sur des schémas. Mais elle n'est pas constructive, en ce sens qu'elle ne permet pas de connaître directement l'idéal de $\Pi_{F/E} V$ si l'on connaît l'idéal d'une variété affine V. Dans [Spr98], l'existence de la restriction du corps de base est montrée dans les cas particuliers d'une variété lisse et

irréductible, ou d'une variété quelconque pour une extension de corps séparable, et la construction en termes d'idéaux est explicitée. Pour notre part, nous nous intéresserons uniquement aux extensions du type K/K^{p^n}, K désignant toujours un modèle de CHC_p.

On peut aussi définir la notion équivalente dans la catégorie des groupes algébriques définis sur F.

Définition III.14 *Soit G un groupe algébrique défini sur F. On dit que G admet une restriction du corps de base s'il existe un groupe algébrique $\Pi_{F/E}G$, défini sur E, ainsi qu'un homomorphisme surjectif de groupes algébriques (défini sur F) $\pi_{F/E} : \Pi_{F/E}G \longrightarrow G$, tels que :*
pour tout groupe algébrique H défini sur E et tout homomorphisme de groupes algébriques $\phi : H \longrightarrow G$, défini sur F, il existe un unique homomorphisme de groupes algébriques $\psi : H \longrightarrow \Pi_{F/E}G$, défini sur E, tel que $\phi = \pi_{F/E} \circ \psi$.
Si G admet une restriction du corps de base, celle-ci est définie à unique isomorphisme de groupes algébriques défini sur E près.

Si G et H admettent des restrictions du corps de base, et si $f : G \longrightarrow H$ est un homomorphisme de groupes algébriques défini sur F, alors il existe un unique homomorphisme de groupes algébriques $\Pi_{F/E}f$, défini sur E, tel que le diagramme suivant commute :

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \uparrow{\scriptstyle \pi_{F/E}} & & \uparrow{\scriptstyle \pi_{F/E}} \\ \Pi_{F/E}G & \xrightarrow{\Pi_{F/E}f} & \Pi_{F/E}H \end{array}$$

On établit maintenant le lien entre le foncteur Π_n et le foncteur de restriction du corps de base $\Pi_{K/K^{p^n}}$. Ce lien a aussi été établi en partie dans [Del02].

Proposition III.8 *Si V est une variété algébrique définie sur K, alors le couple $(\Pi_n V, \rho_n)$ est une restriction du corps de base de K à K^{p^n}.*
Si G est un groupe algébrique, $(\Pi_n G, \rho_n)$ est une restriction du corps de base dans la catégorie des groupes algébriques.

Preuve Par construction, $\Pi_n V$ est une variété algébrique définie sur K^{p^n} et ρ_n un morphisme de $\Pi_n V$ dans V, défini sur K, qui est surjectif d'après la proposition III.7.
On doit montrer que si W est une variété algébrique définie sur K^{p^n} et $f : W \longrightarrow V$ un morphisme défini sur K, alors il existe un unique morphisme, défini sur K^{p^n}, $g : W \longrightarrow \Pi_n V$ tel que $f = \rho_n \circ g$.
Puisque K^{p^n} est séparablement clos, il suffit, pour déterminer g, de le déterminer comme morphisme entre les points K^{p^n}-rationnels. D'autre part, on sait que ρ_n est une application bijective de $\Pi_n V(K^{p^n})$ dans $V(K)$, de bijection réciproque φ_n ; donc g vérifie nécessairement $g = \varphi_n \circ f : W(K^{p^n}) \longrightarrow \Pi_n V(K^{p^n})$.
Reste à montrer que l'on définit ainsi un morphisme de variétés algébriques, défini sur K^{p^n}. Considérons un ouvert affine U de W, sur lequel f est défini comme une fraction rationnelle P/Q. En écrivant $P(x)/Q(x) = N(x)/Q(x)^{p^n}$ et en notant $\varphi_n(N)$ le polynôme (à coefficients dans K^{p^n}) obtenu en appliquant

φ_n aux coefficients de N, on obtient, pour $x \in U(K^{p^n})$:

$$\varphi_n(f(x)) = \varphi_n\Big(\frac{N(x)}{Q(x)^{p^n}}\Big) = \frac{\varphi_n(N)(x)}{Q(x)^{p^n}}.$$

Cette fraction rationnelle remplit les conditions cherchées.
Dans le cas d'un groupe algébrique, le morphisme g ainsi construit est un homomorphisme puisque ϕ_n et f en sont. □

Remarque Pour $m \geq n$, la proposition précédente montre qu'il existe un unique morphisme, que l'on notera $\rho_{m,n}$, de $\Pi_m V$ dans $\Pi_n V$, défini sur K^{p^n} et tel que $\rho_m = \rho_n \circ \rho_{m,n}$. On remarque facilement que $(\Pi_m V, \rho_{m,n})$ est une restriction du corps de base de K^{p^n} à K^{p^m} pour $\Pi_n V$.

Proposition III.9 *Soit V une variété algébrique lisse. Alors $\Pi_n V$ est isomorphe à $\Delta_{p^n-1}V$. Si de plus V est un groupe algébrique, l'isomorphisme obtenu est un isomorphisme de groupes algébriques.*

Preuve On fixe ici une p-base n-canonique (b). Pour $1 \leq j \leq p^n - 1$, D_j s'annule sur K^{p^n}, donc, pour $x \in K$, on a les relations (y compris pour $j = 0$) :

$$D_j(x) = \sum_{i=0}^{p^n-1} \varphi_{n,i}(x) D_j(b^i).$$

Ainsi, le p^n-uplet $\delta_{p^n-1}(x)$ est l'image du p^n-uplet $\varphi_n(x)$ par la matrice (indépendante de x) $A := (D_j(b^i))_{0 \leq i,j \leq p^n-1}$.
Comme $D_j(b^i) = \binom{i}{j} b^{i-j}$ (voir l'exemple suivant la définition I.1), cette matrice est triangulaire, avec des 1 sur la diagonale, donc en particulier inversible.
On en déduit deux bijections réciproques l'une de l'autre entre $\varphi_n(V(K))$ et $\delta_{p^n-1}(V(K))$; par densité, on obtient deux isomorphismes réciproques l'un de l'autre entre $\Pi_n V$ et $\Delta_{p^n-1}V$.
Supposons maintenant que (V, m) est un groupe algébrique, et que $\Phi : \Pi_n V \longrightarrow \Delta_{p^n-1}V$ est l'isomorphisme précédemment construit. Les lois de groupes m_1 sur $\Pi_n V$ et m_2 sur $\Delta_{p^n-1}V$ sont telles que, pour tous x, y dans $V(K)$,

$$m_1(\varphi_n(x), \varphi_n(y)) = \varphi_n(m(x,y)) \text{ et } m_2(\delta_{p^n-1}(x), \delta_{p^n-1}(y)) = \delta_{p^n-1}(m(x,y)) \quad ;$$

donc $\Phi \circ m_1 = m_2 \circ (\Phi, \Phi)$ sur $\varphi_n(V)$, donc sur $\Pi_n V$ par densité. □

Fait III.5 *Pour $m \geq n$, les isomorphismes $\psi_m : \Delta_{p^m-1}V \longrightarrow \Pi_m V$ et $\psi_m : \Delta_{p^m-1}V \longrightarrow \Pi_m V$ exhibés dans la proposition précédente font commuter le diagramme :*

$$\begin{array}{ccccc} \Delta_{p^m-1}V & \xrightarrow{\pi_{p^m-1,p^n-1}} & \Delta_{p^n-1}V & \xrightarrow{\pi_{p^n-1,0}} & V \\ \downarrow \psi_m & & \downarrow \psi_n & \nearrow \rho_n & \\ \Pi_m V & \xrightarrow{\rho_{m,n}} & \Pi_n V & & \end{array} .$$

III.2.3 Variétés algébriques avec D-structure

On s'attache ici à généraliser les constructions de Buium ([Bui92]) dans le cadre de corps de Hasse de caractéristique quelconque.

Définition III.15 *Soit V une variété algébrique définie sur un D-corps K. On appelle D-structure sur V une famille $(D_i)_{i\geq 0}$ de morphismes de faisceaux de $\mathcal{O}_V$ dans $\mathcal{O}_V$, telle que pour tout ouvert U de V, $D_i(U) : \mathcal{O}_V(U) \longrightarrow \mathcal{O}_V(U)$ munisse $\mathcal{O}_V(U)$ d'une structure de K-D-algèbre.*
On notera $\mathcal{O}_V^D$ le faisceau de K-D-algèbres ainsi défini.

Fait III.6 *Par passage aux corps de fractions, une D-structure sur une variété algébrique irréductible V fait de son corps de fonctions $K(V)$ un K-D-corps.*

Définition III.16 *Soit (V, D) et (W, D) deux variétés algébriques munies d'une D-structure. Soit $f : V \longrightarrow W$ un morphisme, et $f^\# : \mathcal{O}_W \longrightarrow \mathcal{O}_V$ le morphisme de faisceaux induit. On dit que f est un morphisme de variétés algébriques avec D-structure si $f^\#$ est un morphisme de faisceaux de K-D-algèbre.*

Définition III.17 *Soit V une variété D-algébrique (respectivement une variété algébrique munie d'une D-structure), définie sur K. Soit L un K-D-corps et U un ouvert (affine) de V. On appelle D-point de V, à valeurs dans L, et localisé sur U, un morphisme de K-D-algèbre $\mathcal{O}_V^D(U) \longrightarrow L$.*
On note $V^D(L)$ l'ensemble des points de V à valeurs dans L.

Remarque Pour un ouvert affine U de V, on peut identifier un D-point de V à valeurs dans L et localisé en U avec un uple de L, en associant à un morphisme $\mathcal{O}_V^D(U) \longrightarrow L$ l'image de la multivariable X. Cette identification permet de considérer $V^D(L)$ comme une variété D-algébrique dans L :

- si W est une sous-variété D-affine de K^n, homéomorphe à un ouvert U de V, les D-points à valeurs dans L et localisés sur U sont identifiés avec la sous-variété D-affine de L^n $\{x \in L^n | \forall P \in \mathcal{I}(W), P(x) = 0\}$. En particulier, si $L = K$, on retrouve $V^D(K) = V$.
- si V est une variété algébrique munie d'une D-structure, $V^D(L)$ est un sous-ensemble des points $V(L)$ au sens de la géométrie algébrique ; si de plus V est une sous-variété affine de K^n, $V^D(L) = \{x \in V(L) | \forall i\, D_i(x) = (D_i(X))(x)\}$ est une sous-variété D-affine de L^n.

Proposition III.10 *Soit V une variété algébrique irréductible définie sur K, munie d'une D-structure. Alors $V^D(K)$ est Zariski-dense dans V.*

Preuve On se place sur un ouvert affine U de V. La structure de D-algèbre sur $\mathcal{O}_V(U)$ donne une unique structure de D-corps sur le corps de fonctions $K(U)$, le plongement $\mathcal{O}_V^D(U) \longrightarrow K(U)$ est alors par construction un morphisme de D-algèbres, donc un D-point à valeurs dans $K(U)$. Alors, si $X \in K(U)$ désigne les fonctions coordonnées, on peut trouver, par saturation de K, un point $a \in K$ tel que $tp(a/k) = tp(X/k)$, où k est un corps de définition dénombrable pour V et pour les fonctions $D_i(X)$. On obtient alors que $a \in V^D(K)$, et que a est un point générique de V, donc $V^D(K)$ est Zariski-dense dans V. □

Définition III.18 *Soit G un groupe algébrique défini sur K. On appelle D-structure sur G une D-structure sur la variété algébrique sous-jacente à G telle que e soit un D-point et que la multiplication $G \times G \longrightarrow G$ et l'inverse $G \longrightarrow G$ soient des morphismes de variétés algébriques avec D-structure (ou encore, la*

comultiplication $\mu : \mathcal{O}_G^D \longrightarrow \mathcal{O}_G^D \otimes \mathcal{O}_G^D$ *et l'antipode* $\imath : \mathcal{O}_G^D \longrightarrow \mathcal{O}_G^D$ *sont des morphismes de faisceaux de* K*-*D*-algèbres).*

Exemple Tout groupe algébrique G défini sur le corps des constantes C_K^∞ peut être muni d'une D-structure, dite triviale : pour chaque ouvert affine U, $O_G(U)$ est de la forme $C_K^\infty[U] \otimes_{C_K^\infty} K$, on lui donne une structure de K-D-algèbre en étendant la dérivation de Hasse trivialement de C_K^∞ à $C_K^\infty[U]$. L'unité, la multiplication et l'inverse sont définis sur C_K^∞, et ils respectent donc cette D-structure triviale.

Remarque Il est sous-entendu ici que $G \times G$ est muni de la D-structure déduite de G de la même manière qu'exposée dans le fait III.3 pour la dérivation de Hasse sur l'anneau des fonctions D-régulières d'un produit de variétés D-algébriques, c'est-à-dire

$$D_n(f \otimes g) = \sum_{i=0}^{n} D_i(f) D_{n-i}(g).$$

Après l'introduction des D-structures en caractéristique nulle par Alexandru Buium, cette notion a aussi été étudiée par David Marker dans [Mar00] et par Piotr Kowalski et Anand Pillay dans [KowPil03] (et ils mènent aussi une étude sur les D-structure en caractéristique positive). En particulier, il est établi le lien entre les D-structures et les sections pour les prolongations ; nous développons ici ce lien en caractéristique quelconque (les notations sont celles de la section III.2.1).

Proposition III.11 *Soit* V *une variété algébrique lisse irréductible définie sur* K*. Alors* V *admet une* D*-structure si et seulement si le système projectif* $(\Delta_j V, \pi_{j,i})$ *admet une famille de sections* $(s_j : V \longrightarrow \Delta_j V)_{j \geq 0}$*, rationnelles, définies sur* K *et compatibles, c'est-à-dire vérifiant* $s_0 = id$*,* $\pi_{j,i} \circ s_j = s_i$ *pour tous* $i \leq j$*, et* $\binom{i+j}{i} s_{i+j}^{\#} \circ \overline{D_{i+j}} = s_i^{\#} \circ \overline{D_i} \circ s_j^{\#} \circ \overline{D_j}$ *sur* $\mathcal{O}_V$ *pour tout* i, j*.*
La donnée de cette famille de sections équivaut à la donnée de la D*-structure. Une* D*-structure de groupe algébrique correspond à une famille de sections qui sont des homomorphismes de groupes algébriques.*

Preuve Etant donnée une famille (s_i) de sections vérifiant les conditions de la proposition, on définit une D-structure sur le faisceau $\mathcal{O}_V$ par :

$$D_i := s_i^{\#} \circ \overline{D_i}$$

Puisque $s_i^{\#} = s_j^{\#} \circ \pi_{j,i}^{\#}$ pour $i \leq j$, on a aussi $D_i = s_j^{\#} \circ \pi_{j,i}^{\#} \circ \overline{D_i}$. Du fait que $s_i^{\#}$ est un homomorphisme d'anneaux, D_i vérifie les mêmes propriétés que $\overline{D_i}$ pour la somme et le produit. D'autre part, la condition $D_i \circ D_j = \binom{i+j}{i} D_{i+j}$ équivaut à la condition $\binom{i+j}{i} s_{i+j}^{\#} \circ \overline{D_{i+j}} = s_i^{\#} \circ \overline{D_i} \circ s_j^{\#} \circ \overline{D_j}$; on obtient donc bien une D-structure sur $\mathcal{O}_V$.
Connaissant une D-structure (D_i) sur $\mathcal{O}_V$, on va définir les sections sur chaque ouvert affine. La cohérence de la définition sera assurée par le fait que la D-structure (D_i) respecte les restrictions dans le faisceau $\mathcal{O}_V$. Plaçons-nous donc sur une variété affine U, isomorphe à un ouvert de V, définie par un idéal I de $K[X]$. Pour $P \in K[T]$, étant donné que $\mathcal{O}_U$ est une K-D-algèbre, la définition de $\overline{D_i}$ donne formellement que, pour tout $f \in \mathcal{O}_U$,

$$D_i(P(f)) = (\overline{D_i} P)(D_0(f), \ldots, D_i(f)).$$

Si on continue à désigner par X le uplet des fonctions coordonnées dans $(\mathcal{O}_U)^m$ (pour un certain entier m), on obtient donc que la fonction $(D_0(X), \ldots, D_j(X))$ envoie U dans $\Delta_j U$. On définit alors

$$s_j := (D_0(X), \ldots, D_j(X)).$$

C'est bien un morphisme de U dans $\Delta_j U$, puisque chacune des composantes de s_j est une fonction régulière sur U. Par construction, on obtient bien que $\pi_{j,i} \circ s_j = s_i$ pour $i \leq j$. Pour vérifier que la famille (s_i) satisfait la propriété de composition des $s_i^\# \circ \overline{D_i}$, il suffit, d'après l'équivalence avec la propriété d'itérativité de la famille (D_i) que l'on a montrée précédemment, de vérifier que les applications $(s_i) \mapsto (D_i)$ et $(D_i) \mapsto (s_i)$ sont inverses l'une de l'autre.
Or, si $s_i = (D_0(X), \ldots, D_i(X))$, on a pour tout $f \in \mathcal{O}_V$,

$$(s_i^\# \circ \overline{D_i})(f) = \overline{D_i} f(D_0(X), \ldots, D_i(X)) = D_i(f(X)),$$

et si $D_i = s_j^\# \circ \pi_{j,i}^\# \circ \overline{D_i}$ pour $i \leq j$, $D_i(X) = \overline{D_i} X \circ s_j$, où $\overline{D_i} X = X^{(i)}$ représente le $i+1$-ème uplet de coordonnées dans $K[X^{(0)}, \ldots, X^{(j)}]$; et on a donc $s_j = (D_0(X), \ldots, D_j(X))$.
Dans le cas d'un groupe algébrique G, les applications (D_i) ainsi construites donnent une D-structure de groupe algébrique si et seulement si les sections (s_i) sont des homomorphismes. Pour montrer cela, considérons l'action de la comultiplication. D'après la définition fonctorielle de la loi de groupe sur $\Delta_j G$, la comultiplication μ de G et la comultaplication μ_j de $\Delta_j G$ sont reliées par le diagramme commutatif suivant :

$$\begin{array}{ccc} \mathcal{O}_G & \xrightarrow{\mu} & \mathcal{O}_{G\times G} \\ \downarrow \Delta_j & & \downarrow \Delta_j \\ \left(\mathcal{O}_{\Delta_j G}\right)^{j+1} & \xrightarrow{(\mu_j)^{\times j+1}} & \left(\mathcal{O}_{\Delta_j G \times \Delta_j G}\right)^{j+1} \end{array} .$$

Pour $i \leq j$, on obtient donc, pour la $i+1$-ème composante, en utilisant le fait III.3, que :

$$\mu_j \circ \pi_{j,i}^\# \circ \overline{D_i} = \sum_{h=0}^{i} (\pi_{j,h}^\# \circ D_h \otimes \pi_{j,i-h}^\# \circ D_{i-h}) \circ \mu.$$

Les sections (s_j) sont des homomorphismes si et seulement si $\mu \circ s_j^\# = (s_j^\# \otimes s_j^\#) \circ \mu_j$, ce qui équivaut (puisque $\mathcal{O}_{\Delta_j G}$ est engendré en tant que K-algèbre par les images de $\mathcal{O}_G$ par les $(\pi_{j,i}^\# \circ \overline{D_i})_{i \leq j}$) à :

$$\forall i \leq j \quad , \quad \mu \circ s_j^\# \circ \pi_{j,i}^\# \circ \overline{D_i} = (s_j^\# \otimes s_j^\#) \circ \mu_j \circ \pi_{j,i}^\# \circ \overline{D_i},$$

c'est-à-dire

$$\forall i \leq j \quad , \quad \mu \circ D_i = (s_j^\# \otimes s_j^\#) \circ \sum_{h=0}^{i} (\pi_{j,h}^\# \circ \overline{D_h} \otimes \pi_{j,i-h}^\# \circ \overline{D_{i-h}}) \circ \mu = \sum_{h=0}^{i} (D_h \otimes D_{i-h}) \circ \mu,$$

ce qui signifie exactement que μ est un morphisme de faisceaux de K-D-algèbres pour la D-structure donnée par les (D_i). $\square$

Fait III.7 *Soit V une variété algébrique lisse et irréductible définie sur K, L un D-corps contenant K et $(s_i)_{i\geq 0}$ une famille de sections correspondant à une D-structure sur V. Alors*

$$V^D(L) = \{x \in V(L) | \forall i \geq 0, \delta_i(x) = s_i(x)\}.$$

Si V et W admettent une D-structure, donnée respectivement par les familles (s_i) et (t_i), alors un morphisme $f : V \longrightarrow W$ est un morphisme de variétés algébriques avec D-structure si et seulement si, pour tout i, le diagramme suivant commute :

$$\begin{array}{ccc} V & \xrightarrow{s_i} & \Delta_i V \\ \downarrow f & & \downarrow \Delta_i f \\ W & \xrightarrow{t_i} & \Delta_i W \end{array}.$$

Proposition III.12 *Pour $p = 0$, la donnée d'une D-structure équivaut à celle d'une section $s_1 : V \longrightarrow \Delta_1 V$.*

Preuve La preuve précédente montre en particulier que la donnée d'une section $s_1 : V \longrightarrow \Delta_1 V$ est équivalente à la donnée d'une dérivation D_1 sur le faisceau $\mathcal{O}_V$, étendant la dérivation de K. On a vu (proposition I.5) qu'en caractéristique nulle, cela équivaut à la donnée d'un D-structure sur $\mathcal{O}_V$. □

Proposition III.13 *Pour $p > 0$, une variété algébrique V lisse irréductible et définie sur K admet une D-structure si et seulement s'il existe une famille $(V_n, \alpha_n)_{n\in\omega}$ telle que :*
- *$V_0 = V$ et $\alpha_0 = id$*
- *pour tout n, V_n est une variété algébrique définie sur K^{p^n}*
- *pour tout n, $\alpha_n : V_n \longrightarrow V$ est un isomorphisme, et l'isomorphisme $\alpha_n^{-1} \circ \alpha_{n+1} : V_{n+1} \longrightarrow V_n$ est défini sur K^{p^n}.*

Plus précisément, il existe une application A qui à une D-structure sur V associe une telle famille $(V_n, \alpha_n)_{n\in\omega}$ et une application B qui à une telle famille $(V_n, \alpha_n)_{n\in\omega}$ associe V_0 et une D-structure sur V_0. Ces applications vérifient les propriétés :
- *$B \circ A = Id$*
- *deux familles $(V_n, \alpha_n)_{n\in\omega}$ et $(W_n, \beta_n)_{n\in\omega}$ sont telles que $B((V_n, \alpha_n)) = B((W_n, \beta_n))$ si et seulement si $V_0 = W_0$ et pour tout n, $\beta_n^{-1} \circ \alpha_n$ est défini sur K^{p^n}.*

Dans le cas où la variété V considérée est un groupe algébrique, les applications A et B font correspondre les D-structures de groupe algébrique avec les familles telles que les V_n sont des groupes algébriques et les α_n des isomorphismes de groupes algébriques.

Preuve On va utiliser la proposition III.11 qui permet de décrire une D-structure sur V en termes de famille de sections $(s_j)_{j\in\omega}$, et aussi remarquer que la donnée d'une telle famille équivaut à la donnée de la famille $(\tilde{s}_n)_{n\in\omega}$, avec $\tilde{s}_n = \psi_n \circ s_{p^n-1} : V \longrightarrow \Pi_n V$ ($\psi_n : \Delta_{p^n-1} V \longrightarrow \Pi_n V$ désigne l'isomorphisme construit dans la proposition III.9) : connaissant $s_{p^n-1} = \psi_n^{-1} \circ \tilde{s}_n$, il suffira de poser $s_i = \pi_{p^n-1,i} \circ s_{p^n-1}$ pour $p^{n-1} < i < p^n$.
On va maintenant construire les applications A et B. Supposons connue une D-structure sur V, déterminée par la donnée de $\tilde{s}_n : V \longrightarrow \Pi_n V$ pour tout n. Rappelons que $\rho_n : \Pi_n V \longrightarrow V$ fournit une bijection de $\Pi_n V(K^{p^n})$ dans

$V(K)$, de bijection réciproque φ_n (voir la section III.2.2). Sur $V^D(K)$, on a alors $\varphi_n(x) = \psi_n \circ \delta_{p^n-1}(x) = \tilde{s}_n(x) \in \Pi_n V(K^{p^n})$, notons V_n la clôture de $\tilde{s}_n(V^D(K))$ de Zariski dans $\Pi_n V$. La sous-variété V_n de $\Pi_n V$ est définie sur K^{p^n} en tant que clôture d'un ensemble de points à valeurs dans K^{p^n}. On sait déjà que $\rho_n \circ \tilde{s}_n = id_V$, et sur $V^D(K)$, $\tilde{s}_n \circ \rho_n(\tilde{s}_n(x)) = \tilde{s}_n \circ \rho_n(\varphi_n(x)) = \tilde{s}_n(x)$, donc $\tilde{s}_n \circ \rho_n = id$ sur $\tilde{s}_n(V^D(K))$, donc sur V_n par densité. On en déduit que $\alpha_n := \rho_{n|V_n}$ est un isomorphisme de V_n sur son image. Cette image contient $V^D(K)$, et comme $V^D(K)$ est Zariski-dense dans V (proposition III.10), α_n est un isomorphisme de V_n sur V. Puisque $\Pi_0 V = V$ et $\tilde{s}_0 = id$, cela montre aussi que $V_0 = V$. Pour montrer que la famille vérifie bien les propriétés voulues, il ne reste donc plus qu'à montrer que $\alpha_{n+1}^{-1} \circ \alpha_n : V_n \longrightarrow V_{n+1}$ est défini sur K^{p^n}, ou encore qu'il envoie un sous-ensemble de $V_n(K^{p^n})$, dense dans V, dans $V_{n+1}(K^{p^n})$. Or, $\tilde{s}_n(V^D(K))$ est dense dans V_n par définition, à valeurs dans K^{p^n}, et pour $x \in V^D(K)$, $\alpha_{n+1}^{-1} \circ \alpha_n(\tilde{s}_n(x)) = \alpha_{n+1}^{-1}(x) = \tilde{s}_{n+1}(x) = \varphi_{n+1}(x) \in V_{n+1}(K^{p^{n+1}})$, ce qui donne le résultat voulu.
Construisons maintenant l'application B, à partir d'une famille $(V_n, \alpha_n)_{n\in\omega}$. Posons $V = V_0$. D'après la proposition III.8, on sait que pour tout n, il existe un morphisme β_n, défini sur K^{p^n}, tel que le diagramme suivant commute :

$$\begin{array}{ccc} V_n & \xrightarrow{\alpha_n} & V \\ & \searrow \beta_n \quad \nearrow \rho_n & \\ & \Pi_n V & \end{array} .$$

Posons $\tilde{s}_n := \beta_n \circ \alpha_n^{-1}$. Pour $m \geq n$, on sait que $(\Pi_m V, \rho_{m,n})$ est la restriction du corps de base de K^{p^n} à K^{p^m} pour la variété $\Pi_n V$, et on a la situation suivante :

$$\begin{array}{ccccc} V_m & \xrightarrow{\alpha_n^{-1}\circ\alpha_m} & V_n & \xrightarrow{\alpha_n} & V \\ \downarrow \beta_m & & \downarrow \beta_n & \nearrow \rho_n & \\ \Pi_m V & \xrightarrow{\rho_{m,n}} & \Pi_n V & & \end{array} .$$

Puisque $\alpha_n^{-1} \circ \alpha_m$ est défini sur K^{p^n}, l'unicité de β_n donne que $\beta_n = \rho_{m,n} \circ \beta_m \circ \alpha_m^{-1} \circ \alpha_n$, et donc que $\tilde{s}_n = \rho_{m,n} \circ \tilde{s}_m$. On revient aux sections $s_i : V \longrightarrow \Delta_i V$ en posant $s_{p^n-1} = \psi_n^{-1} \circ \tilde{s}_n$ et $s_i = \pi_{p^n-1,i} \circ s_{p^n-1}$ pour $p^{n-1} < i < p^n$; en utilisant les correspondances (pour $m \geq n$)

$$\begin{array}{ccc} \Delta_{p^m-1} V & \xrightarrow{\pi_{p^m-1,p^n-1}} & \Delta_{p^n-1} V \\ \downarrow \psi_m & & \downarrow \psi_n \\ \Pi_m V & \xrightarrow{\rho_{m,n}} & \Pi_n V \end{array} ,$$

on obtient bien que $\pi_{j,i} \circ s_j = s_i$ pour $i \leq j$.
Pour montrer qu'on a ainsi défini une D-structure sur V, il reste à vérifier la propriété de composition des $s_i^\# \circ \overline{D_i}$. Pour i et j donnés, on fixe n tel que $p^n > i + j$. Puisque V_n est défini sur K^{p^n} (qui est séparablement clos), on sait que $\alpha_n(V_n(K^{p^n}))$ est Zariski-dense dans V ; donc pour U un ouvert de V et $f \in \mathcal{O}_V(U)$, il suffit de vérifier l'égalité $\binom{i+j}{i} s_{i+j}^\# \circ \overline{D_{i+j}}(f) = s_i^\# \circ \overline{D_i} \circ s_j^\# \circ \overline{D_j}(f)$ sur cet ensemble (intersecté avec U). Or pour $x \in V_n(K^{p^n})$, $\alpha_n(x) = \rho_n \circ \beta_n(x)$, avec $\beta_n(x) \in \Pi_n V(K^{p^n})$. Comme on sait que ρ_n fournit une bijection de $\Pi_n V(K^{p^n})$ dans $V(K)$, de bijection réciproque φ_n, on obtient que $\beta_n(x) = \varphi_n \circ \alpha_n(x)$. Donc pour $y = \alpha_n(x) \in \alpha_n(V_n(K^{p^n}))$, $\varphi_n(y) = \beta_n \circ \alpha_n^{-1}(y) = \tilde{s}_n(y)$. En appliquant ψ_n^{-1}, on obtient $s_{p^n-1}(y) = \delta_{p^n-1}(y)$; et en appliquant $\pi_{p^n-1,h}$ pour $h \leq p^n - 1$,

on obtient $s_h(y) = \delta_h(y)$. On a alors $s^{\#}_{i+j} \circ \overline{D_{i+j}}(f)(y) = \overline{D_{i+j}}f(\delta_{i+j}(y)) = D_{i+j}(f(y))$, et $s^{\#}_i \circ \overline{D_i} \circ s^{\#}_j \circ \overline{D_j}(f)(y) = D_i(s^{\#}_j \circ \overline{D_j}(f)(y)) = D_i(D_j(f(y)))$, d'où l'égalité voulue.
Maintenant, dans le cas où $(V_n, \alpha_n)_{n\in\omega} = A((V, \tilde{s}_n)_{n\in\omega})$, on a par définition $V_n \subset \Pi_n V$ et $\alpha_n = \rho_{n|V_n}$, de bijection réciproque $\tilde{s}_n$. Donc la construction de $B((V_n, \alpha_n)_{n\in\omega})$ donne que β_n est l'inclusion de V_n dans $\Pi_n V$ (par unicité) et on retrouve donc bien $s_n = \beta_n \circ \alpha_n^{-1}$, c'est-à-dire $B \circ A = Id$.
Soient deux familles $(V_n, \alpha_n)_{n\in\omega}$ et $(V'_n, \alpha'_n)_{n\in\omega}$, on leur associe les factorisations

$$\begin{array}{ccc} V_n & \xrightarrow{\alpha_n} & V \\ & \searrow^{\beta_n} \quad \nearrow^{\rho_n} & \\ & \Pi_n V & \end{array} \quad \text{et} \quad \begin{array}{ccc} V'_n & \xrightarrow{\alpha'_n} & V \\ & \searrow^{\beta'_n} \quad \nearrow^{\rho_n} & \\ & \Pi_n V & \end{array} .$$

Alors $B((V_n, \alpha_n)) = B((W_n, \beta_n))$ si et seulement si pour tout n, $\tilde{s}_n = \tilde{s}'_n$ avec $\tilde{s}_n := \beta_n \circ \alpha_n^{-1}$ et $\tilde{s}'_n := \beta'_n \circ {\alpha'_n}^{-1}$. Si $\tilde{s}_n = \tilde{s}'_n$, alors β_n et β'_n ont même image V''_n dans $\Pi_n V$, définie sur K^{p^n}. Puisque β_n et β'_n sont les premiers facteurs des isomorphismes α_n et α'_n, ils induisent des isomorphismes $\gamma_n : V_n \longrightarrow V''_n$ et $\gamma'_n : V'_n \longrightarrow V''_n$, définis sur K^{p^n}. On obtient alors que ${\alpha'_n}^{-1} \circ \alpha_n = {\gamma'_n}^{-1} \circ \gamma_n$ est défini sur K^{p^n}. Réciproquement, si ${\alpha'_n}^{-1} \circ \alpha_n$ est défini sur K^{p^n}, l'unicité de β_n dans la factorisation de α_n donne que $\beta_n = \beta'_n \circ {\alpha'_n}^{-1} \circ \alpha_n$, c'est-à-dire $\tilde{s}_n = \tilde{s}'_n$. $\square$

On déduit du fait III.7 les descriptions suivantes.

Fait III.8 *Soit $(V_n, \alpha_n)_{n\in\omega}$ une famille décrivant une D-structure sur $V = V_0$. Alors*

$$V^D(K) = \bigcap_{n\geq 0} \alpha_n(V_n(K^{p^n})).$$

Si on a deux D-structures $(V_n, \alpha_n)_{n\in\omega}$ et $(W_n, \beta_n)_{n\in\omega}$ sur V et W respectivement, et un morphisme f de V dans W, alors f est un morphisme de variétés algébriques avec D-structure si et seulement si pour tout n, $\beta_n^{-1} \circ f \circ \alpha_n : V_n \longrightarrow W_n$ est défini sur K^{p^n}.

III.3 Les foncteurs

III.3.1 La catégorie des groupes infiniment définissables

On suit pour les définitions suivantes la présentation faite dans la section 5.d de [Poi87b]. Ces définitions et les résultats donnés sont généraux, ils ne supposent en fait que la stabilité (ou l'ω-stabilité pour le corollaire III.2) des théories envisagées, ici les théories CHC_p.

Définition III.19 *On appelle groupe infiniment définissable, avec paramètres dans un D-corps k, la donnée de familles, éventuellement infinies, de formules $(\gamma_j(x))$, $\mu_j(x, y, z)$ et $\iota_j(x, y)$ à paramètres dans k, où x, y, z sont des multi-variables libres de longueur n, telles que $\bigwedge_j \mu_j(K^{3n})$ et $\bigwedge_j \iota_j(K^{2n})$ sont des graphes de fonctions $m : G \times G \longrightarrow G$ et $i : G \longrightarrow G$, où $G := \bigwedge_j \gamma_j(K^n)$, qui donnent à (G, m, i) une structure de groupe.*
Si les conjonctions $\bigwedge_j \gamma_j(x)$, $\bigwedge_j \gamma_j(x) \wedge \bigwedge_j \gamma_j(y) \wedge \bigwedge_j \gamma_j(z) \wedge \bigwedge_j \mu_j(x, y, z)$ et $\bigwedge_j \gamma_j(x) \wedge \bigwedge_j \gamma_j(y) \wedge \bigwedge_j \iota_j(x, y)$ sont chacunes équivalentes à une formule, on dira que (G, m, i) est définissable.

La différence entre un groupe infiniment définissable et un groupe définissable tient uniquement dans la définition de l'ensemble sous-jacent, comme le montre le fait suivant, conséquence du théorème de compacité.

Fait III.9 (Section 5.d de [Poi87b]) *Soit (G, m, i) un groupe infiniment définissable. Il existe un ensemble définissable D contenant G, et des fonctions définissables $\tilde{m} : D \times D \longrightarrow D$ et $\tilde{i} : D \longrightarrow D$ tels que $m = \tilde{m}_{|G\times G}$ et $i = \tilde{i}_{|G}$.*

Le théorème suivant est dû à Ehud Hrushovski, on peut en trouver une preuve dans [Poi87b] (théorème 5.18). Il utilise le fait que la structure K soit stable.

Théorème III.2 (Hrushovski) *Soit (G, m, i) un groupe infiniment définissable, avec $m = \tilde{m}_{|G\times G}$ et $i = \tilde{i}_{|G}$ pour des fonctions définissables $\tilde{m}$ et $\tilde{i}$. Alors il existe un ensemble définissable $\tilde{G}$ contenant G, tel que $(\tilde{G}, \tilde{m}_{|\tilde{G}\times\tilde{G}}, \tilde{i}_{|\tilde{G}})$ soit un groupe.*

Corollaire III.1 (Théorème 5.17 de [Poi87b]) *Un groupe infiniment définissable (G, m, i) est l'intersection d'une famille de groupes définissables.*

Dans le cas où $p = 0$, K est ω-stable. Puisqu'il n'existe pas de chaîne infinie strictement décroissante de groupes définissables dans une structure ω-stable (théorème 1.6 de [Poi87b] par exemple), on en déduit le corollaire suivant.

Corollaire III.2 (Corollaire 5.19 de [Poi87b]) *Un groupe infiniment définissable dans CHC_0 est en fait définissable.*

Définition III.20 *La catégorie des groupes infiniment définissables, avec paramètres dans un D-corps k, est la catégorie dont les objets sont les groupes infiniment définissables avec paramètres dans k, et dont les morphismes $G \longrightarrow H$ sont les homomorphismes de G dans H dont le graphe est infiniment définissable (ou de manière équivalente : relativement définissable dans $G \times H$) avec paramètres dans k.*

Nous utiliserons dans ce qui suit les outils développés dans le cadre général des groupes stables (dans [Poi87b] par exemple).

Définition III.21 *Soit G un groupe infiniment définissable. On dit que G est connexe si et seulement si G n'admet pas de sous-groupe infiniment définissable d'indice fini.*

Définition III.22 *Soit G un groupe infiniment définissable et D un ensemble définissable (avec leurs paramètres dans k). On dit que D est générique s'il existe un nombre fini d'éléments $a_1, \ldots, a_h$ de G tels que $G = a_1.(D \cap G) \cup \ldots \cup a_h.(D \cap G)$.*
Soit $t \in S(k)$ un type dans G. On dit que t est un type générique dans G si et seulement si tout ensemble D défini par une formule de t est générique.

Fait III.10 (Section 5.a de [Poi87b]) *Dans un groupe infiniment définissable G, il existe un type générique.*
Le groupe G est connexe si et seulement s'il existe un unique type générique.
Le type générique d'un groupe connexe est invariant par passage à l'inverse et par translation (plus précisément, si $a \in G$ et si b est une réalisation du type générique au-dessus de a, alors b^{-1}, $a.b$ et $b.a$ sont génériques).

III.3.2 Equivalence de catégories entre les groupes D-algébriques et les groupes infiniment définissables

Théorème III.3 *La catégorie des groupes D-algébriques irréductibles, munie des p-homomorphismes de groupes D-algébriques, est équivalente à celle des groupes infiniment définissables connexes.*

Preuve
Première étape : on construit le foncteur Ψ de la catégorie des variétés D-algébriques irréductibles, avec p-morphismes, dans celle des ensembles infiniment définissables.
Soit V une variété D-algébrique (pas nécessairement irréductible pour l'instant) ; notons $V := (V, (U_i), (f_i), (V_i))_{1 \leq i \leq m}$, où les (U_i) forment un recouvrement ouvert de V, et chaque f_i est une application bicontinue de U_i dans une variété D-affine V_i. Les (V_i) seront considérées comme sous-variétés D-affines d'un même K^n pour un certain n.
Fixons $(c_i)_{i \in \omega}$ une suite de constantes distinctes dans K. Pour $1 \leq i \leq m$, $\tilde{U_i} := U_i \setminus (U_1 \cup \ldots \cup U_{i-1})$ est un fermé de U_i, donc $\tilde{V_i} := f_i(\tilde{U_i}) \times \{c_i\}$ est une sous-variété D-affine de $V_i \times \{c_i\}$, donc en particulier un ensemble infiniment définissable dans K^{n+1}. On pose alors

$$\Psi(V) := \tilde{V_1} \cup \ldots \cup \tilde{V_m},$$

c'est un sous-ensemble infiniment définissable de K^{n+1}.
Notons aussi que :

- on dispose d'une bijection $f_V : V \longrightarrow \Psi(V)$ obtenue par recollement des $f_{i|\tilde{U_i}} \times \{c_i\} : \tilde{U_i} \longrightarrow \tilde{V_i}$ (les $\tilde{U_i}$ sont deux à deux disjoints), on verra encore $\Psi(V)$ comme un espace topologique avec la topologie transportée par f_V.
- si $V = (V, V, id, V)$ est une variété D-affine avec sa présentation "naturelle", alors $\Psi(V) = V$.
- si W est un sous-espace fermé de $V := (V, (U_i), (f_i), (V_i))$, muni de la structure naturelle de variété D-algébrique $(W, (U_i \cap W), (f_{i|U_i \cap W}), (f_i(U_i \cap W)))$, alors $\Psi(W) \subset \Psi(V)$.

Soit $h : V \longrightarrow W$ un p-morphisme de variétés D-algébriques irréductibles, avec $V := (V, (U_i), (f_i), (V_i))$ et $W = (W, (X_j), (g_j), (W_j))$. On va construire une application à graphe relativement définissable $\Psi(h) : \Psi(V) \longrightarrow \Psi(W)$, telle que le diagramme suivant commute :

$$\begin{array}{ccc} V & \xrightarrow{h} & W \\ \downarrow f_V & & \downarrow f_W \\ \Psi(V) & \xrightarrow{\Psi(h)} & \Psi(W) \end{array} .$$

Pour tous i, j, la restriction $h_{i,j}$ de $g_j \circ h \circ f_i^{-1}$ à l'ouvert $A_{i,j} := V_i \cap (h \circ f_i^{-1})^{-1}(X_j)$ est par définition un p-morphisme de variétés D-affines, de $A_{i,j}$ dans W_j. Il existe donc un recouvrement fini par des ouverts non vides $A_{i,j} = \bigcup_s A_{i,j,s}$, des entiers $n_{i,j,s}$ (nuls si $p = 0$) et des D-multipolynômes $P_{i,j,s}$ et $Q_{i,j,s}$ tels que

$$h_{i,j}{}^{p^{n_{i,j,s}}}_{|A_{i,j,s}} = \frac{P_{i,j,s}}{Q_{i,j,s}}.$$

Relativement à $A_{i,j} \times W_j$, le graphe de $h_{i,j}$ est donc donné par la formule

$$\gamma_{i,j} := \bigwedge_s Q_{i,j,s}(x) y^{p^{n_{i,j,s}}} = P_{i,j,s}(x) \quad ;$$

en effet, la formule $Q_{i,j,s}(x)h(x)^{p^{n_{i,j,s}}} = P_{i,j,s}(x)$ définit un fermé de $A_{i,j}$, contenant l'ouvert non vide $A_{i,j,s}$: cette formule est donc vraie sur $A_{i,j}$ tout entier (car $A_{i,j}$, en tant qu'ouvert de l'espace irréductible V_i, est irréductible).
Si $x = (x_1, \ldots, x_{d+1}) \in \Psi(V) = \tilde{V_1} \cup \ldots \cup \tilde{V_m} \subset K^{d+1}$, la relation $x \in \tilde{V_i}$ est donnée, relativement à $\Psi(V)$, par la formule $x_{d+1} = c_i$; et de même pour $y \in \Psi(W) \subset K^{e+1}$. En restreignant le graphe des applications $h_{i,j}$ (ou plus exactement $\tilde{h}_{i,j} : A_{i,j} \times \{c_i\} \longrightarrow W_j \times \{c_j\}$) aux ensembles deux à deux disjoints $\tilde{V_i} \times (f_W \circ h \circ f_V^{-1})^{-1}(\tilde{W_j})$, on obtient donc pour $\Psi(h)$ un graphe relativement définissable dans $\Psi(V) \times \Psi(W)$ donnée par la formule :

$$\bigvee_{i,j}(x \in \tilde{V_i} \wedge y \in \tilde{W_j} \wedge \gamma_{i,j}(x_1, \ldots, x_d, y_1, \ldots, y_e)).$$

Deuxième étape : ce foncteur induit un foncteur, toujours appelé Ψ, entre les catégories annoncées. En effet, si on considère un groupe D-algébrique irréductible $(G, m, ^{-1}, e)$, il est clair que $(\Psi(G), \Psi(m), \Psi(^{-1}))$ est un groupe infiniment définissable (car le foncteur Ψ transforme une structure de groupe en une structure de groupe). Notons aussi que, par transport de topologie via la bijection f_G, $\Psi(G)$ a une structure de groupe topologique irréductible (les translations et le passage à l'inverse y sont continues) ; il reste à montrer que $\Psi(G)$ est connexe.
On va utiliser pour cela les faits suivants concernant les groupes topologiques, certains généraux (1, 3, 5) et d'autres liés à la topologie particulière de $\Psi(G)$ (2, 4).

Fait III.11

1. *Soit D un sous-ensemble relativement définissable de $\Psi(G)$, tel qu'un nombre fini de translatés de D recouvrent $\Psi(G)$, alors D est dense dans $\Psi(G)$.*
   Preuve : par continuité des translations, si $\Psi(G) = a_1.D \cup \ldots \cup a_l.D$, alors l'espace irréductible $\Psi(G)$ est recouvert par une union finie de fermés $a_i.\overline{D}$, et donc D est dense dans $\Psi(G)$.
2. *Soit D un sous-ensemble relativement définissable et dense dans $\Psi(G)$, alors D contient un ouvert non-vide de $\Psi(G)$ (on ne fait aucune hypothèse sur l'irréducibilité de G).*
   Preuve : reprenons la définition de la première étape $\Psi(G) = \tilde{G_1} \cup \ldots \cup \tilde{G_m}$; $\tilde{G_1}$ est par construction un ouvert de $\Psi(G)$ pour la topologie apportée par la bijection f_G, et la topologie induite sur $\tilde{G_1}$ est la D-topologie induite sur $\tilde{G_1}$. Alors, puisque $D \cap \tilde{G_1}$ est dense dans $\tilde{G_1}$ pour la D-topologie induite, il vient par élimination des quantificateurs que $D \cap \tilde{G_1}$ contient un ouvert non-vide de $\tilde{G_1}$. Donc D contient un ouvert non-vide de $\Psi(G)$.
3. *Soit G un groupe topologique et H un sous-groupe dense dans G contenant un ouvert non-vide de G, alors $H = G$.*
   Preuve : par continuité des translations, $a.H$ contient aussi un ouvert non-vide pour tout a dans G, ce qui donne $a.H \cap H \neq \emptyset$, et ainsi $G = H$.
4. *Soit H un sous-groupe infiniment définissable dense dans $\Psi(G)$, alors $H = \Psi(G)$ (on ne fait aucune hypothèse sur l'irréducibilité de G).*

Preuve : d'après le corollaire III.1, H est l'intersection de sous-groupes relativement définissables de $\Psi(G)$, qui sont tous denses dans $\Psi(G)$. D'après les deux points précédents, ces groupes sont égaux à $\Psi(G)$, et donc $H = \Psi(G)$.

5. *Soit G un groupe topologique et H un sous-groupe de G, alors son adhérence $\overline{H}$ est un sous-groupe de G.*
   Preuve : par continuité de l'inverse, $\overline{H}$ est invariant par l'inverse. Par continuité des translations, $\overline{H}$ est invariant par translation par les éléments de H. L'ensemble $\{a \in \overline{H}; a.\overline{H} \subset \overline{H}\} = \cap_{b\in\overline{H}} \overline{H}.b^{-1}$ contient donc H, et il est fermé, donc $\overline{H}$ est invariant par translation (à gauche, et de même à droite)

Il vient alors que, lorsque G est irréductible, $\Psi(G)$ est connexe : soit G_0 un sous-groupe infiniment définissable de $\Psi(G)$, d'indice fini ; $\Psi(G)$ est recouvert par un nombre fini de translatés de G_0, et donc G_0 est dense et contient un ouvert non-vide de $\Psi(G)$ (fait III.11.1 et III.11.2), et donc $G_0 = \Psi(G)$ (fait III.11.3).

Troisième étape : le foncteur Ψ est pleinement fidèle, c'est-à-dire que si G et H sont deux groupes D-algébriques irréductibles définis sur k, Ψ réalise une bijection de l'ensemble des p-morphismes de groupes D-algébriques de G dans H dans l'ensemble des homomorphismes relativement définissables de $\Psi(G)$ dans $\Psi(H)$.
L'injectivité vient immédiatement du fait que pour $h : G \longrightarrow H$, on a $h = f_H^{-1} \circ \Psi(h) \circ f_G$.
Pour la surjectivité, on considère ϕ un homomorphisme relativement définissable, avec paramètres dans k, de $\Psi(G)$ dans $\Psi(H)$. Considérons $a \in \Psi(G)$ un point générique de $\Psi(G)$ sur k ; $b := \phi(a)$ est dans la clôture définissable de $k \cup \{a\}$, donc par la proposition II.3, il existe des D-multipolynômes P et Q dans $(k\{X\})^m$, avec $Q(a) \neq 0$, et un entier n tels que $b^{p^n} = \frac{P(a)}{Q(a)}$. Le point a est contenu dans l'ensemble D défini par la formule $Q(x) \neq 0 \wedge Q(x)\phi(x)^{p^n} = P(x)$. Un nombre fini de translatés de D recouvre $\Psi(G)$, donc D contient un ouvert non vide U, et $\Psi(G) = a_1.U \cup \ldots \cup a_l.U$ par compacité. Sur chacun des ouverts $a_i.U$, $\phi_{|a_i.U}$ est une fonction p-D-régulière en tant que composée de fonctions p-D-régulières (fait III.2)

$$a_i.U \xrightarrow{a_i^{-1}\cdot} U \xrightarrow{\phi} \Psi(H) \xrightarrow{\phi(a_i)\cdot} \Psi(H).$$

On en déduit immédiatement que ϕ est l'image par Ψ du p-morphisme de groupes D-algébriques $f_H^{-1} \circ \phi \circ f_G$.

Quatrième étape : le foncteur Ψ est essentiellement surjectif.
Étant donné un groupe infiniment définissable connexe (Γ, μ, ι), on va trouver un groupe D-algébrique G tel que $\Psi(G)$ est isomorphe à Γ (dans la catégorie des groupes infiniment définissables). Dans le cadre des groupes constructibles dans les corps algébriquement clos, cette dernière étape est connue sous le nom de théorème de Weil ; on va l'utiliser sous la forme suivante, issue de [Wei55] :

Théorème III.4 (Weil) *Soit V une variété irréductible, définie sur un corps K_0. Soit u une fonction rationnelle (partielle) de $V \times V$ dans V, définie sur K_0, vérifiant les conditions :*

– *si x et y sont des points génériques de V, indépendants au-dessus de K_0, alors $K_0(x,y) = K_0(y, u(x,y)) = K_0(x, u(x,y))$*
– *si x, y et z sont des points génériques de V, indépendants au-dessus de K_0, alors $u(u(x,y),z) = u(x, u(y,z))$.*

Alors il existe un groupe algébrique $(G,.)$, défini sur K_0, et une application birationnelle (partielle) β de V dans G tels que, pour tous x, y génériques indépendants au-dessus de K_0, $\beta(u(x,y)) = \beta(x).\beta(y)$.

Proposition III.14 *Soit Γ un groupe connexe infiniment définissable dans K, alors il existe un plongement définissable de Γ dans $\Psi(\hat{G})$, pour un certain groupe algébrique irréductible G.*

Preuve de la proposition On va suivre la preuve donnée dans le cas d'une caractéristique $p > 0$ (et dans un langage différent) dans [BouDel01] (proposition 4.2) et dans [Mes94] (proposition 2.4). On peut aussi trouver une preuve différente (utilisant la construction d'un pro-groupe algébrique) dans le cas où $p = 0$ dans [Pil97] (proposition 3.1).
On se fixe K_1, un sous-D-corps de K $\aleph_1$-saturé et contenant les paramètres nécessaires à la définition de (Γ, μ, ι) ; en particulier $\Gamma(K_1)$ reste un groupe. On supposera K $|K_1|^+$-saturé. D'après la caractérisation de la clôture définissable (proposition I.12), et par compacité, il existe des entiers m et r (avec $r = 0$ si $p = 0$), et des fractions rationnelles $M_1, \ldots, M_k$ et $I_1, \ldots, I_k$ à coefficients dans K_1 tels que les disjonctions suivantes soient vraies pour tous a et b dans Γ :

$$\bigvee_{i=1}^{k} \big(\mu(a,b)^{p^r} = M_i(\delta_m(a), \delta_m(b))\big) \quad \text{et} \quad \bigvee_{i=1}^{k} \big(\iota(a)^{p^r} = I_i(\delta_m(a))\big).$$

Soit q le type générique de Γ sur K_1 et g une réalisation de q. On pose

$$K_1((g)) := K_1(\mu(a,g)^{p^{2r}}, \mu(g,a)^{p^{2r}}, \mu(a,\iota(g))^{p^{2r}}, \mu(\iota(g),a)^{p^{2r}})_{a\in\Gamma(K_1)}.$$

Puisque $\iota(g)^{p^r} \in K_1(\delta_m(g))$, $\delta_m(\iota(g))^{p^r} = \delta_{mp^r}(\iota(g)^{p^r}) \in K_1(\delta_{m+mp^r}(g))$, et, pour $a \in \Gamma(K_1)$, $\mu(a,\iota(g))^{p^{2r}} \in K_1(\delta_m(\iota(g)))^{p^r} \subset K_1(\delta_{m+mp^r}(g))$. Ainsi, pour $N := m + mp^r$, on voit que $K_1((g)) \subset K_1(\delta_N(g))$, et donc $K_1((g))$ est finiment engendré au-dessus de K_1 : il existe une multi-fraction rationnelle l telle que $K_1((g)) = K_1(l(\delta_N(g)))$. On obtient ainsi une fonction partielle $l \circ \delta_N$ sur Γ. Puisque $g^{p^{2r}} \in K_1((g))$, on peut supposer que la composante $x^{p^{2r}}$ apparaît dans $l \circ \delta_N$; en remplaçant les autres composantes de $l \circ \delta_N$ par 0 aux points de Γ où elles ne sont pas définies, on obtient une bijection α relativement définissable de Γ sur son image H. Par saturation de K, H est un ensemble infiniment définissable ; il devient un groupe infiniment définissable $(H, *, ^{-1})$, isomorphe à Γ dans cette catégorie, par le transport de la structure de groupe via α.
Soit $h = \alpha(g)$, h est une réalisation du type générique de H sur K_1, et on a

$$K_1(h^{-1}) = K_1(\alpha(\iota(g))) = K_1((\iota(g))) = K_1((g)) = K_1(\alpha(g)) = K_1(h),$$

donc $^{-1}$ est génériquement rationnelle dans H.
De la même manière, si $b \in H(K_1)$, c'est à dire $b = \alpha(a)$ pour $a \in \Gamma(K_1)$, $\mu(a,g)$ reste un point générique de Γ sur K_1 et donc

$$K_1(b * h) = K_1(\alpha(\mu(a,g))) = K_1((a * g)) = K_1((g)) = K_1(\alpha(g)) = K_1(h),$$

et aussi $K_1(h*b) = K_1(h)$.
Fixons K_0 un modèle de CHC_p dénombrable, inclus dans K_1, et contenant une p-base canonique et les paramètres nécessaires à la définition de Γ et α (donc à la définition de $(H, *, ^{-1})$). Soit $b = \alpha(a)$ un point générique de $H(K_1)$ au-dessus de K_0 et $h = \alpha(g)$ un point générique de H au-dessus de K_1. On a vu que $b*h \in K_1(h)$; d'autre part, puisque $*$ est définissable à paramètres dans K_0, on a $b*h \in K_0(\{b\},\{h\})^{strict} = K_0(\{b\})^{strict}K_0(\{h\})^{strict}$ (cette dernière égalité est évidente dans le cas $p = 0$; si $p > 0$, c'est la conséquence du fait que $K_0(\{a\})^{strict} = K_0(\lambda_n(a))_{n\in\omega}$, voir le corollaire I.1). Or $tp(h/K_1)$ ne dévie pas sur K_0 (en tant que type générique du groupe H, qui est défini sur K_0), donc d'après le corollaire II.4 (caractérisation de la déviation), $K_0(\{h\})^{strict}$ est linéairement disjoint de K_1 au-dessus de K_0, donc en considérant le schéma d'extensions

$$\begin{array}{ccccc} K_0(\{h\})^{strict} & \to & K_0(\{b\},\{h\})^{strict} & & \\ \uparrow & & \uparrow & & \\ K_0(h) & \to & K_0(\{b\})^{strict}K_0(h) & \to & K_1(h) \\ \uparrow & & & & \uparrow \\ K_0 & & \longrightarrow & & K_1 \end{array} ,$$

on obtient que $K_1(h)$ et $K_0(\{b\},\{h\})^{strict}$ sont linéairement disjoints au-dessus de $K_0(\{b\})^{strict}K_0(h)$, et donc $b*h \in K_1(h) \cap K_0(\{b\},\{h\})^{strict} = K_0(h)K_0(\{b\})^{strict}$. On obtient de même que $h*b \in K_0(h)K_0(\{b\})^{strict}$.
Soit alors h' et h'' deux réalisations indépendantes au-dessus de K_0 du type générique de H au-dessus de K_0. Le couple (h', h'') réalise le même type que (h, b) et que (b, h) au-dessus de K_0, donc $h'*h'' \in K_0(h')K_0(\{h''\})^{strict} \cap K_0(h'')K_0(\{h'\})^{strict}$; or $K_0(\{h'\})^{strict}$ est linéairement disjoint de $K_0(\{h''\})^{strict}$ au-dessus de K_0, donc en considérant les extensions

$$\begin{array}{ccccc} K_0(\{h'\})^{strict} & \to & K_0(h'')K_0(\{h'\})^{strict} & & \\ \uparrow & & \uparrow & & \\ K_0(h') & \to & K_0(h',h'') & \to & K_0(h')K_0(\{h''\})^{strict} \\ \uparrow & & & & \uparrow \\ K_0 & & \longrightarrow & & K_0(\{h''\})^{strict} \end{array} ,$$

on obtient que $K_0(h')K_0(\{h''\})^{strict}$ et $K_0(h'')K_0(\{h'\})^{strict}$ sont linéairement disjoints au-dessus de $K_0(h', h'')$, et donc que $h'*h'' \in K_0(h', h'')$: la multiplication $*$ est génériquement rationnelle dans H.

Soit t le type générique de H, on considère V la variété algébrique affine irréductible définie par l'idéal ordinaire $I_t \cap K_0[X]$. Soit u et v les fonctions rationnelles, à coefficients dans K_0, telles que $u(h, h') = h*h'$ et $v(h) = h^{-1}$ pour des réalisations indépendantes du type générique de H au-dessus de K_0. Les formules suivantes

$$x = u(u(x,y), v(y)) \quad , \quad y = u(v(x), u(x,y)) \quad , \quad u(x, u(y,z)) = u(u(x,y), z)$$

s'écrivent dans le langage des corps, et sont vraies pour des points (h, h', h'') génériques deux à deux indépendants dans H (car alors les couples $(h*h', h'^{-1})$, $(h^{-1}, h*h')$, $(h*h', h'')$ et $(h, h'*h'')$ sont des couples de points génériques indépendants), qui forment un point générique de $V \times V \times V$; ces formules sont

donc vraies pour tout triplet générique (au sens de la géométrie algébrique) de $V \times V \times V$.
Les hypothèses du théorème III.4 sont donc satisfaites, et on trouve un groupe algébrique connexe $(G, .)$, et une application birationnelle partielle β de V dans G, définis sur K_0 et tels que, pour tous x, y génériques indépendants dans V, $\beta(u(x, y)) = \beta(x).\beta(y)$. Puisque V est une variété affine, on a $\Psi(\hat{V}) = V$, et $\Psi(\beta)$ est une application partielle de V dans $\Psi(\hat{G})$, quitte à la restreindre, on la supposera définie uniquement sur les points génériques de V.
L'application $\Psi(\beta)$ se prolonge en un homomorphisme définissable et injectif j de H dans $\Psi(\hat{G})$: pour tout a dans H, on peut choisir un point générique h de H indépendant de a au-dessus de K_0, et on pose $j(a) = \Psi(\beta)(h).\Psi(\beta)(h^{-1} * a)$.
On montre que :

- cette définition est indépendante du choix de h ; en effet, si h et h' sont deux points génériques de H indépendants de a, on obtient, pour h'' un point générique indépendant de a, h, h',

$$\Psi(\beta)(h).\Psi(\beta)(h^{-1}*a).\Psi(\beta)(a^{-1}*h'') = \Psi(\beta)(h).\Psi(\beta)(h^{-1}*h'') = \Psi(\beta)(h''),$$

  et de même pour h', donc $\Psi(\beta)(h).\Psi(\beta)(h^{-1}*a) = \Psi(\beta)(h').\Psi(\beta)(h'^{-1}*a)$.
- l'application j est définissable : si φ est un isomorphisme de K fixant K_0 et a, $h' := \varphi(h)$ est un point générique de H indépendant de a au-dessus de K_0, et donc $\varphi(j(a)) = \Psi(\beta)(h').\Psi(\beta)(h'^{-1} * a) = j(a)$.
- l'application j prolonge $\Psi(\beta)$, car si h, h' sont des génériques indépendants, h et $h^{-1} * h'$ le sont aussi
- l'application j est un homomorphisme, car si $a, b \in H$, et si h, h' sont des points génériques indépendants de a et b et entre eux, alors

$$\begin{aligned} j(a).j(b) &= \Psi(\beta)(h).\Psi(\beta)(h^{-1} * a).\Psi(\beta)(h').\Psi(\beta)(h'^{-1} * b) \\ &= \Psi(\beta)(h).\Psi(\beta)(h^{-1} * a * h').\Psi(\beta)(h'^{-1} * b) \\ &= \Psi(\beta)(a * h').\Psi(\beta)((a * h')^{-1} * a * b) = j(a * b). \end{aligned}$$

- l'application j est injective ; en effet, si $\Psi(\beta)(h).\Psi(\beta)(h^{-1}*a) = 1_{\Psi(\hat{G})}$ pour $a \in H$ et h générique indépendant de a, alors, pour h' un point générique inépendant de a et h, on obtient $\Psi(\beta)(h'*h^{-1}) = \Psi(\beta)(h').\Psi(\beta)(h^{-1}*a) = \Psi(\beta)(h'*h^{-1}*a)$, et donc $a = 1_H$ car $\Psi(\beta)$ est bijective sur les génériques.

En composant par l'isomorphisme définissable α, on trouve bien un plongement définissable χ de Γ dans $\Psi(\hat{G})$. □
Pour terminer la démonstration, soit Γ' l'adhérence de $\chi(\Gamma)$, on a vu que Γ' est un sous-groupe de $\Psi(\hat{G})$ (fait III.11.5). On sait aussi qu'il existe une sous-variété D-algébrique G' de $\hat{G}$ telle que $\Gamma' = \Psi(G')$; précisément, $G' := f_{\hat{G}}^{-1}(\Gamma')$ est un sous-groupe fermé de $\hat{G}$, G' a donc même une structure de groupe D-algébrique. Le groupe $\chi(\Gamma)$ est infiniment définissable et dense dans $\Psi(G')$, donc $\chi(\Gamma) = \Psi(G')$ (fait III.11.4) ; on obtient donc que χ est un isomorphisme de Γ sur $\Psi(G')$.
Et on vérifie que $\Psi(G')$ est bien irréductible : si T désigne l'ensemble des réalisations du type générique de $\Psi(G')$ (qui, comme Γ, est connexe), on obtient, d'après le fait III.10 et la continuité du passage à l'inverse et des translations, que son adhérence $\overline{T}$ est un sous-groupe infiniment définissable de $\Psi(G')$. Par le corollaire III.1, $\overline{T}$ est une intersection de sous-groupes relativement définissables et génériques de $\Psi(G')$; tous ces groupes sont donc d'indice fini dans $\Psi(G')$, et

donc égaux à $\Psi(G')$. Puisque T est l'ensemble des réalisations d'un type complet, son adhérence $\Psi(G')$ est irréductible. $\square$

III.3.3 Equivalence de catégories entre les groupes rationnellement minces et les groupes algébriques munis d'une D-structure

Définition III.23 *Soit $k \models CH_p$ et a une réalisation d'un type $q \in S(k)$. On dit que le type q est :*
- *mince si le degré de transcendance de $k(\{a\})$ sur k est fini*
- *très mince s'il existe un entier m tel que $k(\{a\})$ est algébrique séparable sur $k(D_0(a), \ldots, D_m(a))$*
- *rationnellement mince si $k(\{a\})$ est finiment engendré sur k (ou de manière équivalente s'il existe un entier m tel que $k(\{a\}) = k(D_0(a), \ldots, D_m(a))$)*

Remarque Un type rationnellement mince est en particulier très mince, un type très mince est en particulier mince, et un type mince est rangé par RU (avec $RU(a/k) \leq deg.tr(k(\{a\})/k)$).
Si $p = 0$, les trois notions coïncident : en effet, si a est une réalisation d'un type mince, il existe m tel que $k(\{a\})$ soit algébrique sur $l := k(D_0(a), \ldots, D_m(a))$. Soit P le polynôme minimal de $D_{m+1}(a)$ sur l ; en appliquant, pour $i \geq 1$, D_i à la relation $P(D_{m+1}(a)) = 0$, on obtient $\binom{m+i+1}{m+1} \frac{dP}{dX}(D_{m+1}(a)) D_{m+i+1}(a) + Q(D_0(a), \ldots, D_{m+i}(a)) = 0$ (où Q est un polynôme à coefficients dans k), ce qui donne par induction que $k(\{a\}) = k(D_0(a), \ldots, D_{m+1}(a))$.
Si $p > 0$, les trois notions sont différentes ; et aucune d'elle ne dépend de la dérivation de Hasse sur K (seulement de l'imperfection de K). On donnera un exemple de type très mince mais pas rationnellement mince en IV.3. Un exemple de type mince mais pas très mince est donné dans [PilZie03] (section 6) : soit k un sous-D-corps dénombrable de K et $c \in C_K^\infty$ transcendant sur k, on sait qu'il existe dans K un élément a, transcendant sur k, tel que $D_{p^i}(a) = c^{p^{-i}}$ pour tout $i \geq 0$ (cet ensemble de conditions est finiment consistant, en prenant $a_j := \sum_{i=0}^{j} c^{p^{-j}} t^{p^j}$ pour une p-base canonique t fixée). Alors $tp(a/k)$ est mince mais pas très mince. On peut remarquer que $RU(a/k) = deg.tr.(k(\{a\})/k) = 2$. Dans [BloKru04], il est montré qu'on peut construire un type mince, non très mince de $RU = 1$ et de degré de transcendance 2. On ne peut pas obtenir de degré de transcendance inférieur, comme le montre la proposition suivante, dont la démonstration figure dans l'annexe A.

Proposition III.15 *Soit a une réalisation d'un type $q \in S(k)$, où $k \models CHC_p$. Supposons que le degré de transcendance de $k(\{a\})$ sur k vaut 1. Alors q est très mince.*

Proposition III.16 *Soit $q \in S(k)$ un type rationnellement mince. L'image de q par une application f (à paramètres dans k) D-régulière en une réalisation de q est un type rationnellement mince.*

Preuve En effet, soit b l'image d'une réalisation a de q par f ; puisque f est D-régulière en a, on a $k(\{b\}) \subset k(\{a\})$, et puisque $k(\{a\})$ est finiment engendré sur k, c'est aussi le cas de $k(\{b\})$. $\square$

La proposition précédente permet de donner un sens à la définition suivante.

Définition III.24 *Soit V une variété D-algébrique irréductible. On dit que V est rationnellement mince si son type générique est rationnellement mince.*

Théorème III.5 *On se place sur K un modèle $\aleph_1$-saturé de CHC_p. La catégorie des groupes algébriques irréductibles munis d'une D-structure est équivalente à celle des groupes D-algébriques irréductibles rationnellement minces.*

Preuve On définit le foncteur Θ de la catégorie des groupes algébriques irréductibles munis d'une D-structure dans celle des groupes D-algébriques par :
- soit (G, D) un objet de la catégorie, on définit $\Theta(G, D) = G^D(K)$
- soit $f : (G, D) \longrightarrow (H, D)$ un morphisme de la catégorie, on définit $\Theta(f) = f_{|\Theta(G,D)}$

Etant donné (G, D), on note $(s_i)_{i\geq 0}$ l'ensemble des sections associées à la D-structure sur G par la proposition III.11. Puisque δ_i et s_i sont des morphismes de groupes D-algébriques de G dans $\Delta_i G$, on a bien que $G^D(K) = \{x \in G(K) | \forall i \geq 0, s_i(x) = \delta_i(x)\}$ (par le fait III.7) est un sous-groupe fermé de G, c'est donc un groupe D-algébrique. Il est Zariski-dense dans G d'après la proposition III.10.
Notons k un D-corps (dénombrable) sur lequel G et les sections $(s_i)_{i\geq 0}$ sont définis. Pour $x \in G^D(K)$, on a, pour tout i, $\delta_i(x) = s_i(x) \in k(x)$, et donc $tp(x/k)$ est rationnellement mince.
Pour montrer que $G^D(K)$ est irréductible, on se place sur un ouvert affine U de G. Soit F un D-fermé de $U(K)$ contenant a, un D-point générique de G. Le D-fermé F est défini par une conjonction d'équations D-polynomiales $P_i(\delta_n(x)) = 0$ (les P_i sont des polynômes). On définit un fermé de Zariski $\tilde{F}$ de U par la conjonction d'équations rationnelles $P_i(s_n(x)) = 0$ (quitte à restreindre l'ouvert U, on peut supposer que s_n est défini par une fraction rationnelle qui ne s'annule pas sur l'ouvert en question) ; on a alors $F \cap U^D(K) = \tilde{F} \cap U^D(K)$. Puisque F contient a, qui est générique dans G, on a $\tilde{F} = U$, et donc $U^D(K) = F$. On en déduit facilement (voir par exemple la fin de la démonstration du théorème III.1) que $G^D(K)$ est irréductible.
Considérons $f : (G, D) \longrightarrow (H, D)$ un morphisme de groupes algébriques avec D-structure, on doit vérifier que $\Theta(f)$ est bien un morphisme de groupes D-algébriques entre $G^D(K)$ et $H^D(K)$. Puisque c'est la restriction d'un morphisme de groupes algébriques, il suffit de vérifier que si $x \in G^D(K)$, $f(x) \in H^D(K)$. Or, pour un ouvert affine U de H contenant $f(x)$, $f^\#$ est par définition un morphisme de D-algèbres entre $\mathcal{O}_H^D(U)$ et $\mathcal{O}_G^D(f^{-1}(U))$; l'image de x par f est donc le morphisme de D-algèbres composé

$$\mathcal{O}_H^D(U) \xrightarrow{f^\#} \mathcal{O}_G^D(f^{-1}(U)) \xrightarrow{x} K,$$

c'est donc un élément de $H^D(K)$.

On a donc montré que Θ est un foncteur entre les catégories annoncées, montrons qu'il est pleinement fidèle. Soit (G, D) et (H, D) deux groupes algébriques irréductibles avec D-structure, on doit montrer que

$$\Theta : Morph((G, D), (H, D)) \longrightarrow Morph(G^D(K), H^D(K))$$

est bijectif.
L'injectivité vient du fait que $G^D(K)$ est Zariski dense dans G : si f et g sont deux morphismes de groupes algébriques, tels que $f_{|G^D(K)} = g_{|G^D(K)}$, alors $f = g$.
Si $g \in Morph(G^D(K), H^D(K))$, considérons un D-point générique x de G sur k (contenant les paramètres nécessaires à la définition de G, des sections associées à sa D-structure et de g), alors $g(x) \in k(\{x\}) = k(x)$: on a donc un homomorphisme génériquement rationnel, qui se prolonge en un morphisme de groupes algébriques de G dans H, que l'on appelle encore g. Pour montrer que g préserve les D-structures, on doit montrer que $g^\#$ est un morphisme de faisceaux de D-algèbres, c'est-à-dire que pour tout ouvert U de H, pour tout $f \in \mathcal{O}_H(U)$ et pour tout i, $g^\#(D_i(f)) = D_i(g^\#(f))$. Comme d'habitude, il suffit de vérifier cette égalité sur $U^D(K)$, et on utilisera le lien avec les sections données par les formules $D_i = s_i^\# \circ \overline{D_i}$ de la proposition III.11, où $\overline{D_i}$ désigne toujours le morphisme de faisceaux entre $\mathcal{O}_G$ et $\mathcal{O}_{\Delta_i G}$, caractérisé par $\overline{D_i}(f)(\delta_i x) = D_i(f(x))$ (on utilise les mêmes notations pour H). Avec ces notations, on doit vérifier que $\overline{D_i}(f) \circ s_i \circ g = \overline{D_i}(f \circ g) \circ s_i$; or, pour $x \in U^D(K)$, $g(x) \in H^D(K)$, donc $s_i(x) = \delta_i(x)$ et $s_i(g(x)) = \delta_i(g(x))$, ce qui donne $\overline{D_i}(f) \circ s_i \circ g(x) = \overline{D_i}(f) \circ \delta_i \circ g(x) = D_i(f(g(x)))$ et $\overline{D_i}(f \circ g) \circ s_i(x) = \overline{D_i}(f \circ g) \circ \delta_i(x) = D_i(f \circ g(x))$. Donc g est un morphsime de groupes munis de D-structure.

Il reste à montrer que Θ est essentiellement surjectif. On se donne donc Γ un groupe D-algébrique irréductible et rationnellement mince (défini avec paramètres dans k). Soit x un point générique de Γ sur k et m un entier tel que $k(\{x\}) = k(\delta_m(x))$. L'application δ_m fournit un isomorphisme (dans la catégorie des groupes D-algébriques) de Γ sur son image Γ', et on a que pour un point générique y de Γ', $k(\{y\}) = k(y)$. Il vient alors directement que la multiplication et le passage à l'inverse sont génériquement rationnels dans Γ'. Comme dans la preuve de la proposition III.14, on peut alors appliquer le théorème de Weil (théorème III.4) pour trouver un groupe algébrique G connexe tel que Γ' soit un sous-groupe D-algébrique de G. Quitte à considérer l'adhérence, pour la topologie de Zariski, de Γ' dans G (qui reste un groupe algébrique irréductible car Γ' est un groupe irréductible pour la D-topologie, qui est plus fine que la topologie de Zariski), on peut supposer que Γ' est dense dans G. Soit x un point générique de Γ', il est aussi générique dans G. Puisque $k(\{x\}) = k(x)$, l'homomorphisme δ_i de G dans $\Delta_i G$ est rationnel en x, il se prolonge donc en un morphisme de groupes algébriques $s_i : G \longrightarrow \Delta_i G$. Ces homomorphismes forment une famille de sections pour le système $(\pi_{j,i})$, puisque les égalités $\pi_{j,i} \circ s_j = s_i$ sont vraies génériquement (dès que $s_j = \delta_j$ et $s_i = \delta_i$), donc partout dans G. Pour montrer que la famille (s_i) correspond à une D-structure sur G, on doit montrer, pour tout i, j, que $\binom{i+j}{i} s_{i+j}^\# \circ \overline{D_{i+j}} = s_i^\# \circ \overline{D_i} \circ s_j^\# \circ \overline{D_j}$. Puisque le point x, générique dans Γ', est aussi générique dans G, il suffit, pour montrer cette égalité, de montrer que pour tout ouvert U de G, pour tout $f \in \mathcal{O}_G(U)$, $\binom{i+j}{i} s_{i+j}^\# \circ \overline{D_{i+j}}(f)(x) = s_i^\# \circ \overline{D_i} \circ s_j^\# \circ \overline{D_j}(f)(x)$. Or, on a $\binom{i+j}{i} s_{i+j}^\# \circ \overline{D_{i+j}}(f)(x) = \binom{i+j}{i} \overline{D_{i+j}}(f)(s_{i+j}(x)) = \binom{i+j}{i} \overline{D_{i+j}}(f)(\delta_{i+j}(x)) = \binom{i+j}{i} D_{i+j}(f(x))$, et $s_i^\# \circ \overline{D_i} \circ s_j^\# \circ \overline{D_j}(f)(x) = D_i(s_j^\# \circ D_j(f))(\delta_i(x)) = D_i(D_j(f)(\delta_j(x))) = D_i \circ D_j(f(x))$, il y a donc égalité.
On a donc obtenu un groupe avec D-structure (G, D), il reste à montrer que $\Gamma' = \Theta(G, D)$. Si x un point générique de Γ', on sait (par la fin de la démonstration

du théorème III.3) que Γ' est l'adhérence de x. Par construction, un tel point x vérifie les formules $s_i(x) = \delta_i(x)$ pour tout i, donc x appartient au fermé $\Theta(G, D)$, et donc $\Gamma' \subset \Theta(G, D)$. Par ailleurs, le fermé Γ' est défini (sur chaque carte affine) par des conjonctions d'équations D-polynomiales $\bigwedge_i P_i(\delta_n(X)) = 0$; comme précédemment, on définit un fermé de Zariski $\tilde{\Gamma}$ de G par les conjonctions d'équations rationnelles $\bigwedge_i P_i(s_n(X)) = 0$ sur chaque carte affine, de telle sorte que $\Gamma' = \tilde{\Gamma} \cap \Theta(G, D)$. Comme Γ' est Zariski-dense dans G, $\tilde{\Gamma} = G$ et donc $\Gamma' = \Theta(G, D)$. $\square$

Remarque La démonstration précédente montre que l'image du foncteur Θ est la classe des sous-groupes Γ infiniment définissables dans $G(K)$, pour G un groupe algébrique défini sur K, tels que les points génériques de x de Γ au-dessus d'un corps de définition k vérifient $k(\{x\}) = k(x)$.

Chapitre IV

Sous-groupes infiniment définissables dans les groupes algébriques

IV.1 Utilisation des prolongations

Dans cette section, on désigne par G un groupe algébrique connexe défini sur K, où K est un modèle de CHC_p, $\aleph_1$-saturé si $p > 0$. D'après le théorème III.3, on considèrera librement $G(K)$ comme un ensemble (infiniment) définissable, avec une topologie qui lui vient de la topologie de $\hat{G}$. On va chercher ici à déterminer les sous-groupes infiniment définissables de $G(K)$. On utilisera pour cela les prolongations, et en particulier les résultats montrés dans la proposition III.6, qui sont valables dans le cas d'un groupe algébrique connexe.
D'après les faits III.11, les sous-groupes infiniment définissables de $G(K)$ sont fermés. On sait que les fermés, pour la D-topologie, s'écrivent comme l'intersection d'une famille $(F_n)_{n<\omega}$, où F_n désigne un fermé pour la $D_{\leq n}$-topologie. D'autre part, par définition, un fermé de $G(K)$ pour la $D_{\leq n}$-topologie correspond, via la projection $\pi_{n,0}$, à un fermé de $\Delta_n G$ pour la topologie de Zariski.

Proposition et définition IV.1 *A tout sous-groupe infiniment définissable H de $G(K)$, on associe une suite $(H_n)_{n<\omega}$, où H_n est le sous-groupe de $\Delta_n G(K)$ défini par :*

$$H_n := \overline{\delta_n(H)}^{Zariski}.$$

Les propriétés suivantes sont vérifiées :

1. *pour $m < n$, $\pi_{n,m}(H_n) = H_m$*
2. *$H = \bigcap_{n<\omega} \delta_n^{-1}(H_n)$*

En particulier, H_0 est la clôture de Zariski de H dans G. On supposera dans la suite que H est Zariski-dense dans G, c'est-à-dire que $H_0 = G$.
La clôture de H dans G pour la $D_{\leq n}$-topologie est

$$\overline{H}^n := \delta_n^{-1}(H_n).$$

Si H est en fait un sous-groupe définissable de G, alors, pour un certaine entier N, on a $H = \overline{H}^N$. On obtient alors facilement que pour tout $n > N$, $H_n = \pi_{n,N}^{-1}(H_N)$.

La compréhension des sous-groupes infiniment définissables de $G(K)$ passe donc par celle de la structure des prolongations $\Delta_n G$. Ces prolongations sont décrites en tant qu'extensions successives de groupes algébriques

$$1 \longrightarrow Ker(\pi_{n,n-1}) \longrightarrow \Delta_n G \overset{\pi_{n,n-1}}{\longrightarrow} \Delta_{n-1} G \longrightarrow 1, \qquad (*)_n$$

ou directement

$$1 \longrightarrow Ker(\pi_{n,0}) \longrightarrow \Delta_n G \overset{\pi_{n,0}}{\longrightarrow} G \longrightarrow 1. \qquad (**)_n$$

Sur les points K-rationnels de ces groupes algébriques, il existe une "section" définissable pour la suite $(**)_n$: c'est l'application δ_n. L'existence d'une section rationnelle est liée au corps de définition de G, comme le montre la proposition suivante.

Proposition IV.1 *Si le groupe algébrique G est défini sur C_K, la suite exacte $(**)_1$ est scindée.*
Si le groupe algébrique G est défini sur C_K^∞, toutes les suites $(**)_n$ sont scindées.

Preuve Supposons que G est défini C_K. Puisque ce corps est séparablement clos, on sait que $G(C_K)$ est dense dans G. Sur $G(C_K)$, la "section" définissable δ_1 est rationnelle (elle associe au uplet x le uplet $(x, 0)$, et on définit ainsi une section $s : G \longrightarrow \Delta_1 G$ qui est un morphisme de groupes algébriques.
Si G est défini sur C_K^∞, les "sections" définissables δ_n se prolongent de $G(C_K^\infty)$ en des sections $s_n : G \longrightarrow \Delta_n G$. □

Dans le cas $p > 0$, la proposition suivante permet de préciser la situation pour les corps intermédiaires entre C_K et C_K^∞, en englobant la proposition précédente.

Proposition IV.2 *On suppose $p > 0$. Si le groupe algébrique G est isomorphe à un groupe algébrique défini sur K^{p^n}, la suite exacte $(**)_{p^n-1}$ est scindée.*

Preuve On utilise ici l'isomorphisme $\psi_n : \Pi_n G \longrightarrow \Delta_{p^n-1} G$ exhibé dans la proposition III.9, et alors $\pi_{n,0}$ admet une section si et seulement si ρ_n admet une section. On rappelle que $(\Pi_n G, \rho_n)$ est une restriction du corps de base pour l'extension K/K^{p^n}.
Si G est défini sur K^{p^n}, on sait, puisque K^{p^n} est séparablement clos, que $G(K^{p^n})$ est dense dans G ; et sur $G(K^{p^n})$, la "section" définissable $\varphi_n = (id, 0, \ldots, 0)$ est rationnelle. On peut donc définir une section $s : G \longrightarrow \Pi_n G$ qui est un morphisme de groupes algébriques. □

Remarque Les réciproques des deux propositions précédentes sont fausses en général. On verra des réciproques partielles dans les cas de groupes algébriques munis d'une D-structure.

Proposition IV.3 *Si le groupe algébrique G est commutatif, il en est de même de $\Delta_n G$ pour tout n.*

Preuve C'est une conséquence directe du fait que $\delta_n(G)$ est dense dans $\Delta_n G$, et commutatif puisque δ_n est un isomorphisme. $\square$

Proposition IV.4 *Pour tout entier n, le noyau $Ker(\pi_{n,n-1})$ est un groupe algébrique vectoriel.*

Preuve La peuve donnée ici reprend les arguments donnés dans le cas de la caractéristique nulle par le lemme 4.1 de [Pil96a] (tel qu'il est énoncé, ce lemme n'est pas exact : il montre seulement que $Ker(\pi_{1,0})$ est un groupe vectoriel, et $Ker(\pi_{n,0})$ n'est qu'un groupe unipotent, qui n'est pas nécessairement un groupe vectoriel si G n'est pas commutatif).
Soit $U \subset K^m$ un ouvert affine contenant 1_G, on peut supposer que ses coordonnées sont $(0, \ldots, 0)$. Soit d la dimension de G, quitte à intervertir l'ordre des variables, on peut supposer que $(x_1, \ldots, x_d)$ forment un système de coordonnées locales au voisinage de 1_G ; on utilisera le fait que, pour $(x_1, \ldots, x_m)$ dans U, x_i est algébrique séparable sur $k(x_1, \ldots, x_d)$ pour tout i (k est un corps de définition pour G), et que les fonctions ccordonnées $x_1, \ldots, x_d$ forment une base de l'espace vectoriel $\mathcal{M}_{1_G}/\mathcal{M}_{1_G}^2$, où $\mathcal{M}_{1_G}$ désigne l'idéal maximal de l'anneau local des fonctions régulières au voisinage de 1_G, $\mathcal{O}_{G,1_G}$. On en déduit aussi que le noyau de J_{1_G}, la matrice jacobienne de G en 1_G, est l'espace vectoriel de base $(x_1, \ldots, x_d)$.
On sait, d'après la description des prolongations donnée dans la preuve de la proposition III.6, qu'il existe un uplet Q tel que

$$\Delta_n U \cap Ker(\pi_{n,n-1}) = \left\{ \overline{x} = (0, \ldots, 0, x_1^{(n)}, \ldots, x_m^{(n)}) \in K^{m(n+1)} \;\middle|\; J_{1_G} \begin{pmatrix} x_1^{(n)} \\ \vdots \\ x_m^{(n)} \end{pmatrix} = Q \right\}.$$

D'après ce qu'on a dit sur le noyau de J_{1_G}, l'application $\overline{x} \mapsto (x_1^{(n)}, \ldots, x_d^{(n)})$ fournit donc un isomorphisme de $\Delta_n U \cap Ker(\pi_{n,n-1})$ sur K^d.
Soit $\mathcal{M}_{(1_G,1_G)}$ l'idéal maximal de $\mathcal{O}_{G\times G,(1_G,1_G)} = \mathcal{O}_{G,1_G} \otimes_K \mathcal{O}_{G,1_G}$, et $\mu : \mathcal{O}_{G,1_G} \longrightarrow \mathcal{O}_{G\times G,(1_G,1_G)}$ la comultiplication dans G au voisinage de 1_G. D'après le chapitre IX de [Lan58] (page 222), on a, pour $1 \leq i \leq d$,

$$\mu(x_i) = x_i \otimes 1 + 1 \otimes x_i \mod \mathcal{M}_{(1_G,1_G)}^2.$$

Soit $\overline{D_n} : \mathcal{O}_{G,1_G} \longrightarrow \mathcal{O}_{\Delta_n G,1_{\Delta_n G}}$ l'application exhibée dans la section III.2.1, caractérisée par le fait que $\overline{D_n}(f)(\delta_n(x)) = D_n(f(x))$; en particulier, on a pour les fonctions coordonnées $\overline{D_n}(x_i) = x_i^{(n)}$. On note $\overline{\overline{D_n}}$ l'application correspondante de $\mathcal{O}_{G\times G,(1_G,1_G)}$ dans $\mathcal{O}_{\Delta_n G\times\Delta_G,(1_{\Delta_n G},1_{\Delta_n G})}$, elle vérifie $\overline{\overline{D_n}} = \sum_{i+j=n} \pi_{n,i}^{\#} \circ \overline{D_i} \otimes \pi_{n,j}^{(\#)} \circ \overline{D_j}$. Par définition de la loi de $\Delta_n G$ (voir la preuve de la proposition III.11), la comultiplication μ_n vérifie :

$$\mu_n \circ \overline{D_n} = \overline{\overline{D_n}} \circ \mu \quad ,$$

et donc, pour $1 \leq i \leq d$,

$$\mu_n(x_i^{(n)}) = x_i^{(n)} \otimes 1 + 1 \otimes x_i^{(n)} \mod \overline{\overline{D_n}}(\mathcal{M}_{(1_G,1_G)}^2).$$

Or, pour $f, g \in \mathcal{M}_{(1_G,1_G)}$,

$$\overline{\overline{D_n}}(fg) = \sum_{i+j=n} (\pi_{n,i}, \pi_{n,i})^{\#} \circ \overline{\overline{D_i}}(f).(\pi_{n,j}, \pi_{n,j})^{\#} \circ \overline{\overline{D_j}}(g) \quad ,$$

et pour $i < n$, et $z \in Ker(\pi_{n,n-1})^2 \subset Ker(\pi_{n,i})^2$, on a

$$(\pi_{n,i}, \pi_{n,i})^{\#} \circ \overline{\overline{D_i}}(f)(z) = \overline{\overline{D_i}}(f)((\pi_{n,i}, \pi_{n,i})(z)) = \overline{\overline{D_i}}(f)(0) = D_i(f(0)) = 0.$$

On obtient donc que, pour $1 \leq i \leq d$, la comultiplication est donnée, sur $Ker(\pi_{n,n-1})$, par

$$\mu_n(x_i^{(n)}) = x_i^{(n)} \otimes 1 + 1 \otimes x_i^{(n)} \quad ,$$

et donc $Ker(\pi_{n,n-1})$ est isomorphe au groupe vectoriel $\mathbb{G}_a^d$. □

Corollaire IV.1 *Pour tout $j > i$, le noyau $Ker(\pi_{j,i})$ est un groupe algébrique unipotent. Si de plus G est commutatif et $p = 0$, alors $Ker(\pi_{j,i})$ est un groupe vectoriel.*

Preuve En effet, une extension d'un groupe unipotent par un groupe unipotent reste un groupe unipotent ; et en caractéristique nulle, un groupe unipotent commutatif est un groupe vectoriel. □

On obtient alors un résultat d'unicité (déjà énoncé dans [Bui92] pour le cas $p = 0$).

Corollaire IV.2 *Si $\chi_a(G)$, le groupe des homomorphismes de groupes algébriques de G dans le groupe additif $\mathbb{G}_a$, est réduit à 0, alors, pour tout n, il existe au plus une section pour la suite exacte $(**)_n$. En particulier, un tel G admet au plus une D-structure.*

Preuve Il suffit de remarquer que la différence entre deux sections donne un homomorphisme de G dans $Ker(\pi_{n,0})$. Comme ce groupe est unipotent, cet homomorphisme est nul. □

On donnera dans la section IV.3 un exemple de D-structure non triviale sur le groupe additif.

Dans le cas de la caractéristique positive, on obtient des résultats plus précis en passant par les foncteurs Π_n.

Proposition IV.5 *Pour $p > 0$, on considère la restriction du corps de base $\Pi_n G \xrightarrow{\rho_{n,n-1}} \Pi_{n-1} G$. Alors $Ker(\rho_{n,n-1})$ est annulé par $[p]$.*

On utilisera pour cela le lemme suivant sur les groupes algébriques. Ce résultat est cité dans [Hus87] (p. 239) pour les lois de groupe formelles, on trouvera une démonstration dans l'annexe B.

Lemme IV.1 *Soit $\mathcal{O}_{G,e}$ l'anneau local des fonctions définies au voisinage de l'unité e de G et $\mathcal{M}$ son idéal maximal. Soit q une puissance de p, et f un élément de $\mathcal{M}$. Alors $f \circ [q] \in \mathcal{M}^q$.*

Preuve de la proposition On reprend les notations de la preuve de la proposition précédente : $U \subset K^m$ désigne un ouvert affine de G contenant 1_G, $\Delta_{p^n-1}U$ est un ouvert affine de $\Delta_{p^n-1}G$ contenant $1_{\Delta_{p^n-1}G}$, que l'on suppose de coordonnées $(0,\dots,0) \in K^{mp^n}$. Les éléments de $\Delta_{p^n-1}U \cap Ker(\pi_{p^n-1,p^{n-1}-1})$ sont de la forme $(0,\dots,0,(x_i^{(j)}; 1 \leq i \leq m, p^{n-1} \leq j \leq p^n-1))$.
L'application $[p]$ dans $\Delta_{p^n-1}G$ est donnée par les relations suivantes, pour $0 \leq j \leq p^n-1$:

$$[p]^{\#}_{\Delta_{p^n-1}G} \circ \pi^{\#}_{p^n-1,j} \circ \overline{D_j} = \pi^{\#}_{p^n-1,j} \circ \overline{D_j} \circ [p]^{\#}_G : \mathcal{O}_G \longrightarrow \mathcal{O}_{\Delta_{p^n-1}G}.$$

Quand on applique cette égalité à la fonction coordonnée x_i $(1 \leq i \leq m)$ de $\mathcal{O}_G$, on obtient d'après le lemme précédent :

$$[p]^{\#}_{\Delta_{p^n-1}G}(x_i^{(j)}) \in \pi^{\#}_{p^n-1,j} \circ \overline{D_j}(\mathcal{M}^p_{1_G}).$$

On montre que ceci est réduit à 0 : si $f_1,\dots,f_p$ sont dans $\mathcal{M}_{1_G}$, on a, d'après le point 2 de la proposition I.1 (qui s'applique car $\pi^{\#}_{p^n-1,j} \circ \overline{D_j}$ vérifie la règle du produit, comme mentionné dans la section III.2.1)

$$\pi^{\#}_{p^n-1,j} \circ \overline{D_j}(f_1 \dots f_p) = \sum_{i_1+\dots+i_p=j} \pi^{\#}_{p^n-1,i_1} \circ \overline{D_{i_1}}(f_1) \dots \pi^{\#}_{p^n-1,i_p} \circ \overline{D_{i_p}}(f_p).$$

Or parmi $i_1,\dots,i_p$, il y en a nécessairement un qui est strictement inférieur à p^{n-1} (car $i_1+\dots+i_p = j < p^n$) ; et pour un tel $i_h < p^{n-1}$, $\pi^{\#}_{p^n-1,i_h} \circ \overline{D_{i_h}}(f_h) = 0$ sur $Ker(\pi_{p^n-1,p^{n-1}-1})$: en effet, pour $z \in Ker(\pi_{p^n-1,p^{n-1}-1})$,

$$\pi^{\#}_{p^n-1,i_h} \circ \overline{D_{i_h}}(f_h)(z) = \overline{D_{i_h}}(f_h)(\pi_{p^n-1,i_h}(z)) = \overline{D_{i_h}}(f_h)(0) = 0.$$

On a donc bien que $Ker(\pi_{p^n-1,p^{n-1}-1})$ est annulé par $[p]$, donc $Ker(\rho_{n,n-1})$ aussi par isomorphisme. □

IV.2 Un cas particulier : le groupe multiplicatif

On considère dans cette section le groupe multiplicatif $\mathbb{G}_m$. On sait d'après la proposition IV.1 que les suites exactes $(**)_n$ sont scindées. Les formules du produit (axiome 2 de la définition I.1) donnent directement une interprétation de $\Delta_n\mathbb{G}_m$ en terme de groupe linéaire.

Proposition IV.6 *Le groupe $\Delta_n\mathbb{G}_m$ s'identifie au groupe linéaire formé des matrices*

$$M(x_0,\dots,x_n) := \begin{pmatrix} x_0 & x_1 & \dots & \dots & x_n \\ 0 & x_0 & x_1 & \dots & x_{n-1} \\ 0 & 0 & \ddots & \dots & \vdots \\ 0 & \dots & 0 & x_0 & x_1 \\ 0 & \dots & \dots & 0 & x_0 \end{pmatrix} \quad , x_0 \neq 0.$$

Le noyau $Ker(\pi_{n,0})$ est le sous-groupe formé des matrices $M(1,x_1,\dots,x_n)$.

Proposition IV.7 *Soit H un sous-groupe infiniment définissable dense de $\mathbb{G}_m(K)$ et pour $n \in \mathbb{N}$, H_n le sous-groupe de $\Delta_n \mathbb{G}_m$ correspondant par la proposition et définition IV.1. Alors H_n est de la forme $\mathbb{G}_m \times H'_n$, où H'_n est un sous-groupe de $Ker(\pi_{n,0})$.*

Preuve On sait que tout groupe linéaire commutatif est isomorphe au produit d'un produit de groupes multiplicatifs par un groupe unipotent. Puisque H_n est un sous-groupe de $\mathbb{G}_m \times Ker(\pi_{n,0})$, qui se projette surjectivement sur $\mathbb{G}_m$, il est de la forme annoncée. □

Corollaire IV.3 *Soit H un sous-groupe infiniment définissable dense dans $\mathbb{G}_m(K)$. Alors H contient $\mathbb{G}_m(C_K^\infty)$. Si $p > 0$ et si H est de plus $D_{\leq n}$-fermé, il contient $\mathbb{G}_m(K^{p^n})$.*

Preuve En effet, puisque, pour tout n, $\mathbb{G}_m \times 0 \subset H_n$, on obtient que la clôture de H pour la $D_{\leq n}$-topologie vérifie

$$\overline{H}^n = \{x \in \mathbb{G}_m(K) | \delta_n(x) \in H_n\} \supset \mathbb{G}_m(K^{p^n}),$$

ce qui donne directement le résultat voulu. □

Dans le cas où $p > 0$, on peut utiliser la proposition suivante et son corollaire, donnés dans [BouDel02], qui concerne plus largement les groupes algébriques commutatifs divisibles.

Proposition IV.8 *Si G est commutatif et divisible, alors tout sous-groupe infiniment définissable connexe de $G(K)$ rangé par le rang U est divisible.*

Preuve Pour H un tel sous-groupe, la propriété d'additivité du rang U donne, pour tout entier n,

$$RU(Ker\ [n]) + RU(nH) \leq RU(H) \leq RU(Ker\ [n]) \oplus RU(nH).$$

Puisque G est divisible, $Ker\ [n]$ est fini dans $G(K)$ et donc dans H, ce qui donne que $RU(H) = RU(nH)$. Puisque H est connexe, c'est donc que H est n-divisible. □

On en déduit :

Corollaire IV.4 *Le seul sous-groupe infiniment définissable de $\mathbb{G}_m(K)$ à la fois connexe, rangé par le rang U et dense est $\mathbb{G}_m(C_K^\infty)$.*

Preuve Soit H un groupe vérifiant ces propriétés. Puisque H est dense, $\mathbb{G}_m(C_K^\infty) \subset H$. De plus, la proposition précédente implique que H est divisible, il doit donc être contenu dans $\mathbb{G}_m(C_K^\infty)$. □

Remarque Si l'on n'exige plus que ce sous-groupe H soit connexe, on sait simplement que sa composante connexe H_0 est $\mathbb{G}_m(C_K^\infty)$. Dans ce cas, on ne peut pas avoir $[H : H_0]$ fini et non-nul ; on aurait en effet un élément $a \in H \setminus H_0$ qui serait algébrique sur C_K^∞, qui est un corps algébriquement clos. Toutefois, on connaît un exemple de groupe H tel que $[H : H_0] = \infty$:
soit $H = \bigcap_n \bigcup_{i<p^n} b^i K^{p^n}$ (où b est un élément de $K \setminus K^p$), alors $H_0 = \mathbb{G}_m(C_K^\infty)$,

et $H/H_0 \simeq \mathbb{Z}_{(p)}$.

En étudiant précisément le quotient $\mathbb{G}_m(K)/\mathbb{G}_m(C_K)$, on peut donner une description exhaustive des sous-groupes infiniment définissables de $\mathbb{G}_m(K)$ contenant $\mathbb{G}_m(C_K)$.

Proposition IV.9 *L'application* $d : x \mapsto \frac{D_1(x)}{x}$ *est un homomorphisme définissable de* $\mathbb{G}_m(K)$ *dans* $\mathbb{G}_a(K)$*, de noyau* $\mathbb{G}_m(C_K)$*.*
Si $p = 0$*, cette application est surjective.*
Si $p > 0$*, l'image de cette application est*

$$Im\ d = \{y \in \mathbb{G}_a(K) | D_{p-1}(y) = y^p\}.$$

Preuve La première assertion est une conséquence de la formule de Leibniz.
La surjectivité de d quand $p = 0$ vient de l'axiome suivant de CHC_0 :

$$\forall y \exists x D_1(x) = xy \wedge x \neq 0.$$

Dans le cas $p > 0$, on va construire, étant donné un élément $y \in K$, une suite $(u_n)_{0 \leq n \leq p-1}$ définie par $u_0 = y$ et, pour $1 \leq n \leq p-1$,

$$u_n = \frac{D_1(u_{n-1}) + yu_{n-1}}{n}.$$

On voit aisément que u_n s'exprime comme un polynôme à coefficients dans $\mathbb{F}_p$ en les variables $D_0(y), \ldots, D_n(y)$. On note, pour des entiers $i_0, \ldots, i_n$ positifs ou nuls, $c^n_{i_0,\ldots,i_n}$ le coefficient dans u_n du monôme $D_0(y)^{i_0} \ldots D_n(y)^{i_n}$. On identifiera dans la suite $c^n_{i_0,\ldots,i_n,0}$ avec $c^n_{i_0,\ldots,i_n}$, et on fixera la valeur de ces coefficients à 0 dès qu'un des entiers i_j est strictement négatif. L'expression de u_n donne alors la relation

$$c^n_{i_0,\ldots,i_n} = \frac{1}{n}\Big(c^{n-1}_{i_0-1,\ldots,i_n} + (i_0+1)c^{n-1}_{i_0+1,i_1-1,\ldots,i_n} + \ldots + n(i_{n-1}+1)c^{n-1}_{i_0,\ldots,i_{n-1}+1,i_n-1}\Big).$$

On remarque que dans cette formule, la somme $j_0 + 2j_1 + \ldots + (n+1)j_n$ est constante pour tous les coefficients $c_{j_0,\ldots,j_n}$ qui interviennent dans le membre de droite, et vaut $(i_0 + 2i_1 + \ldots + (n+1)i_n) - 1$.
On sait aussi que $c^0_1 = 1$ et que tous les autres coefficients dans u_0 sont nuls. La relation de récurrence et la remarque précédente donne alors que les coefficients $c^n_{i_0,\ldots,i_n}$ sont nuls, sauf éventuellement si $i_0 + 2i_1 + \ldots + (n+1)i_n = n+1$ On montre alors par récurrence sur n que si $i_0 + 2i_1 + \ldots + (n+1)i_n = n+1$,

$$c^n_{i_0,\ldots,i_n} = \frac{n+1}{i_0! \ldots i_n! 2^{i_1} \ldots (n+1)^{i_n}}.$$

Cette formule est vérifiée pour le coefficient c^0_1, et si elle est vraie pour les coefficients de u_{n-1}, on a

$$c^n_{i_0,\ldots,i_n} = \frac{1}{n}\Big(\frac{n}{(i_0-1)! \ldots i_n! 2^{i_1} \ldots (n+1)^{i_n}} +$$

$$(i_0+1)\frac{n}{(i_0+1)!(i_1-1)! \ldots i_n! 2^{i_1-1} \ldots (n+1)^{i_n}} + \ldots +$$

$$n(i_{n-1}+1)\frac{n}{i_0!\dots(i_{n-1}+1)!(i_n-1)!2^{i_1}\dots n^{i_{n-1}+1}(n+1)^{i_n-1}}\Big)$$

$$=\frac{1}{i_0!\dots i_n!2^{i_1}\dots(n+1)^{i_n}}\Big(i_0+2i_1+\dots+(n+1)i_n\Big)=\frac{n+1}{i_0!\dots i_n!2^{i_1}\dots(n+1)^{i_n}}.$$

En particulier, on obtient, pour $i_0+2i_1+\dots+pi_{p-1}=p$, que

$$c^{p-1}_{i_0,\dots,i_{p-1}}=\frac{p}{i_0!\dots i_{p-1}!2^{i_1}\dots p^{i_{p-1}}}.$$

Le dénominateur n'est pas divisible par p, excepté pour les suites d'indices $(p,0,\dots,0)$ et $(0,\dots,0,1)$. On obtient donc que

$$u_{p-1}=\frac{1}{(p-1)!}D_0(y)^p+D_{p-1}(y)=-y^p+D_{p-1}(y),$$

puisque $(p-1)!=-1 \mod p$ (car dans $\mathbb{F}_p$, 1 et -1 sont les seuls éléments égaux à leur inverse).
L'équation de l'image de d s'en déduit. Si $x\in\mathbb{G}_m(K)$, posons $y=d(x)$. On obtient aisément par induction que $nD_n(x)=xu_{n-1}$ pour tout $1\le n\le p$, ce qui donne $u_{p-1}=0$ et donc y vérifie $D_{p-1}(y)=y^p$.
Réciproquement, supposons que y vérifie $D_{p-1}(y)=y^p$, c'est-à-dire que la suite précédente vérifie $u_{p-1}=0$. Si $y=0$, $y=d(x)$ pour n'importe quel élément de $\mathbb{G}_m(C_K)$; sinon, il existe un entier $1\le n\le p-1$ tel que $u_{n-1}\neq 0$ et $u_n=0$. La formule de récurrence définissant cette suite donne alors que $D_1(u_{n-1})+yu_{n-1}=0$; et donc en posant $x=\frac{1}{u_{n-1}}$, on obtient $d(x)=y$. $\square$

Cet homomorphisme définissable d induit une bijection entre les sous-groupes (connexes) de $\mathbb{G}_m(K)$ contenant $\mathbb{G}_m(C_K)$ et les sous-groupes (connexes) de $Im\ d$.
On se place désormais dans le cas $p>0$. On peut utiliser la proposition suivante pour déterminer les sous-groupes de $Im\ d$.

Proposition IV.10 *Fixons $a\in\mathbb{G}_m(K)\setminus\mathbb{G}_m(C_K)$. Soit ϕ_a l'application de $Im\ d$ dans $Ker(D_{p-1})$ (en tant que sous-groupe de $\mathbb{G}_a(K)$ définie par :*

$$\phi_a(x)=x-\frac{x^p}{d(a)^{p-1}}.$$

Alors ϕ_a est une isogénie, de noyau $d(a)\mathbb{F}_p$. L'homomorphisme $\phi_a\circ d$ permet de réaliser une bijection entre les sous-groupes de $\mathbb{G}_m(K)$ contenant $\mathbb{G}_m(C_K)$ et a et les sous-groupes de $Ker(D_{p-1})$.

Preuve L'application ϕ_a est clairement un homomorphisme. Puisque K est séparablement clos, ϕ_a est surjectif de $\mathbb{G}_a(K)$ dans $\mathbb{G}_a(K)$; et comme $D_{p-1}(d(a))=d(a)^p$, on a

$$D_{p-1}(\phi_a(x))=D_{p-1}(x)-\frac{x^p}{d(a)^p}D_{p-1}(d(a))=D_{p-1}(x)-x^p\quad,$$

et donc $x\in Im\ d$ si et seulement si $\phi_a(x)\in Ker(D_{p-1})$. Le noyau de ϕ_a, défini par $x=x^p/(d(a)^{p-1})$, est un sous-groupe additif de cardinal p et contenant $d(a)$, c'est donc $d(a)\mathbb{F}_p$.

Si H est un sous-groupe de $\mathbb{G}_m(K)$ contenant a, $d(H)$ est un sous-groupe de $Im\ d$ contenant $d(a)\mathbb{F}_p$, et ϕ_a réalise une bijection entre de tels sous-groupes et les sous-groupes de $Ker(D_{p-1})$, d'où la dernière assertion. $\square$

Remarque On peut se ramener à des choses déjà étudiés dans [Blo01] et [Blo04] pour déterminer les sous-groupes de $Ker(D_{p-1})$: en utilisant la décomposition en coordonnées dans une p-base 1-canonique, ce groupe est isomorphe à $\mathbb{G}_a(C_K)^{p-1}$ (voir la preuve de la proposition I.3).

Exemple Si $p > 2$, $Ker(D_1)$ est un sous-groupe non-trivial de $Ker(D_{p-1})$, on obtient ainsi, pour tout $a \in \mathbb{G}_m(K) \setminus \mathbb{G}_m(C_K)$, un groupe H tel que $\mathbb{G}_m(C_K) \cup \{a\} \subset H \subset \mathbb{G}_m(K)$, défini par

$$H = \{x \in \mathbb{G}_m(K) | D_1\Big(\frac{D_1(x)}{x} - \frac{D_1(x)^p}{d(a)^{p-1}x^p}\Big) = 0\}.$$

Si $p = 2$, il n'existe pas de sous-groupes connexes de $Ker(D_1)$ qui sont $D_{<2}$-fermés ; mais on peut aussi définir de tels H en considérant des groupes définis à un ordre supérieur.
De tels groupes H ne peuvent pas être définissablement isomorphes à $\mathbb{G}_m(L)$ pour L un corps (infiniment) définissable dans K. D'après le théorème 3.6 et le corollaire 3.9 de [Mes94], de tels corps sont en effet définissablement isomorphes à K ou à C_K^∞. Puisque $RU(\mathbb{G}_m(C_K^\infty)) = 1$ et que H contient $\mathbb{G}_m(C_K)$ qui n'est pas rangé par le rang U, H ne peut pas être définissablement isomorphe à $\mathbb{G}_m(C_K^\infty)$, et on conclut par la proposition suivante.

Proposition IV.11 *Les seuls sous-groupes infiniment définissables de $\mathbb{G}_m(K)$ définissablement isomorphes à $\mathbb{G}_m(K)$ sont les $\mathbb{G}_m(K^{p^n})$ pour $n \geq 0$.*

Preuve Soit H un sous-groupe infiniment définissable de $\mathbb{G}_m(K)$, on suppose qu'il existe un isomorphisme définissable $\phi : H \longrightarrow \mathbb{G}_m(K)$. Le sous-groupe H est alors définissable, et d'après le corollaire IV.3, H contient $\mathbb{G}_m(K^{p^r})$ pour un certain entier $r \geq 0$. On a vu (théorème III.3) que l'isomorphisme ϕ est un p-morphisme de groupes D-algébriques, faisant intervenir les dérivées $D_0, \ldots, D_{p^s-1}$ pour un certain entier s. On en déduit que pour m plus grand que s et r, $\phi_{|\mathbb{G}_m(K^{p^m})}$ s'écrit comme un p-morphisme de groupes algébriques, de $\mathbb{G}_m(K^{p^m})$ dans $\mathbb{G}_m(K)$. Comme ce p-homomorphisme est injectif, c'est une puissance du Frobenius Fr^n, où $n \in \mathbb{Z}$ vérifie $n + m \geq 0$ (car l'image de ϕ est contenue dans $\mathbb{G}_m(K)$).
Alors, pour tout $x \in H$, on a $Fr^m(x) \in K^{p^m}$ et donc $Fr^m \circ \phi(x) = \phi(Fr^m(x)) = Fr^{m+n}(x)$, et donc $\phi(x) = Fr^n(x)$. Puisque l'image de ϕ est $\mathbb{G}_m(K)$, on doit donc avoir $H = Fr^{-n}(\mathbb{G}_m(K)) = \mathbb{G}_m(K^{p^{-n}})$. $\square$

En appliquant une puissance convenable du Frobenius, la proposition IV.10 permet aussi de décrire tous les sous-groupes infiniment définissables H de $\mathbb{G}_m(K)$ qui vérifient $\mathbb{G}_m(K^{p^{n+1}}) \subsetneq H \subset \mathbb{G}_m(K^{p^n})$. Pour exhiber des sous-groupes H qui ne vérifient pas ces inclusions, on va étudier plus précisément la structure de $Ker(\pi_{n,0})$, ou, de manière équivalente, de $Ker(\rho_{n,0})$. On utilise pour cela les résultats exposés dans [Ser59] ; on rappelle en particulier les faits suivants concernant les groupes de Witt (section VII.8 de [Ser59]).

Fait IV.1 *1. Le groupe W_n des vecteurs de Witt de longueur n est un groupe unipotent annulé par p^n. Pour $(x_1, \ldots, x_n) \in W_n$, on a $[p](x_1, \ldots, x_n) = (0, x_1^p, \ldots, x_{n-1}^p)$. Pour tout $i < n$, on a donc $dim(Ker([p^{i+1}])/Ker([p^i])) = 1$.*

2. La troncation

$$\begin{array}{cccc} T_n & : & W_n & \longrightarrow & W_{n-1} \\ & & (x_1, \ldots, x_n) & \mapsto & (x_1, \ldots, x_{n-1}) \end{array}$$

et le décalage

$$\begin{array}{cccc} S_n & : & W_n & \longrightarrow & W_{n+1} \\ & & (x_1, \ldots, x_n) & \mapsto & (0, x_1, \ldots, x_n) \end{array}$$

sont des homomorphismes.

3. Tout groupe connexe unipotent commutatif est isogène à un produit de groupes de Witt

$$\Pi_{i=1}^m W_i^{d_i}.$$

Les entiers d_i sont déterminés de manière unique par les relations

$$\begin{array}{ccc} dim(Ker([p^m])/Ker[p^{m-1}]) & = & d_m \\ dim(Ker([p^{m-1}])/Ker[p^{m-2}]) & = & d_m + d_{m-1} \\ \vdots & & \vdots \\ dim(Ker([p])) & = & d_m + d_{m-1} + \ldots + d_1 \end{array}$$

Lemme IV.2 *Soient m, n deux entiers avec $n \geq m \geq 0$. Alors $Ker(\pi_{p^n-1,p^m-1}) = Ker([p^{n-m}])$. Sa dimension est $p^n - p^m$.*

Preuve Pour $j < p^n$ et $x \in \mathbb{G}_m(K)$, on sait que $D_j(x^{p^{n-m}})$ vaut $D_{jp^{m-n}}(x)^{p^{n-m}}$ si p^{n-m} divise j (et alors $jp^{m-n} < p^m$) et est nul sinon. On en déduit que dans $\Delta_{p^n-1}\mathbb{G}_m$ l'image du uplet $(x_0, \ldots, x_{p^n-1})$ par $[p^{n-m}]$ est un uplet formé des $x_j^{p^{n-m}}$ pour $j < p^m$. Ainsi, $Ker(\pi_{p^n-1,p^m-1}) = Ker([p^{n-m}])$; la dimension vient du fait que $dim(\Delta_i\mathbb{G}_m) = i + 1$ (proposition III.6) □

Proposition IV.12 *Le noyau $Ker(\rho_{n,0})$ est isomorphe au produit*

$$\Pi_{i=0}^n W_i^{d_i} \quad ,$$

avec $d_n = p - 1$ et $d_i = (p-1)^2 p^{n-i-1}$ pour $1 \leq i \leq n-1$.

Preuve D'après la proposition V.9 page 103 de [Ser59], le groupe $Ker(\rho_{n,0})$, isomorphe au groupe des matrices $M(1, x_1, \ldots, x_{p^n-1})$ donné dans la proposition IV.6, est isomorphe à un produit de groupes de Witt. Les entiers d_i sont donnés d'après le calcul des dimensions $dim(Ker([p^{n-1}])/Ker([p^{n-i-1}])) = p^{i+1} - p^i$ dans $Ker(\rho_{n,0})$. □

Cet isomorphisme est assez difficile à expliciter dans une forme exploitable en général. Faisons le pour $p = 3$ et $n = 1$ ou $n = 2$. Cela revient, d'après l'isomorphisme entre $\Pi_n\mathbb{G}_m$ et $\Delta_{p^n-1}\mathbb{G}_m$, à étudier les noyaux $Ker(\pi_{j,0})$ (pour

$j \leq 3^2 - 1 = 8$), que l'on a décrits sous forme matricielle dans la proposition IV.6.
Les applications

$$x \mapsto \frac{D_1(x)}{x} \quad \text{et} \quad x \mapsto D_1\Big(\frac{D_1(x)}{x}\Big)$$

sont des homomorphismes de $\mathbb{G}_m(K)$ dans $\mathbb{G}_a(K)$ qui sont "$D_{\leq 2}$-constructibles", ils induisent donc des homomorphismes de $\Delta_2\mathbb{G}_m$ dans le groupe additif W_1 qui, restreints au noyau $Ker(\pi_{2,0})$, s'expriment :

$$\psi_1(x) = x_1 \quad \text{et} \quad \psi_2(x) = -x_2 - x_1^2 \quad .$$

Cela permet d'écrire l'isomorphisme

$$Ker(\pi_{2,0}) \overset{(\psi_1,\psi_2)}{\longrightarrow} W_1^2.$$

Pour $Ker(\pi_{3,0})$, le groupe W_2 intervient. On trouve une expression de la loi de W_2 (en caractéristique 3) dans [Wit37] :

$$(x_0, x_1) * (y_0, y_1) = (x_0 + y_0, x_1 + y_1 - x_0^2 y_0 - x_0 y_0^2).$$

On remarque alors que, dans $Ker(\pi_{3,0}) \cap Ker(\psi_2)$, l'application $x \mapsto (x_1, x_3)$ est un homomorphisme vers W_2. Après avoir trouvé une section à la suite exacte

$$0 \longrightarrow Ker(\pi_{3,0}) \cap Ker(\psi_2) \longrightarrow Ker(\pi_{3,0}) \xrightarrow{\Psi_2} W_1 \longrightarrow 0,$$

on trouve l'homomorphisme $(\psi_1, \psi_3) : Ker(\pi_{3,0}) \longrightarrow W_2$, avec

$$\psi_3(x) = x_3 - x_1 x_2,$$

qui permet d'écrire l'isomorphisme

$$Ker(\pi_{3,0}) \overset{((\psi_1,\psi_3),\psi_2)}{\longrightarrow} W_2 \times W_1.$$

On trouve de la même manière que ψ_1 et ψ_2 des homomorphismes de $Ker(\pi_{8,0})$ dans W_1 obtenus à partir des homomorphismes définissables

$$x \mapsto D_3\Big(\frac{D_1(x)}{x}\Big) \quad x \mapsto D_4\Big(\frac{D_1(x)}{x}\Big) \quad x \mapsto D_6\Big(\frac{D_1(x)}{x}\Big) \quad x \mapsto D_7\Big(\frac{D_1(x)}{x}\Big) \quad ,$$

ce qui donne

$$\begin{array}{rcl}
\psi_4(x) & = & x_4 - x_1^4 + x_2^2 + x_1^2 x_2 - x_1 x_3 \\
\psi_5(x) & = & -x_5 + x_1 x_4 + x_1^3 x_2 + x_1^5 - x_1 x_2^2 + x_2 x_3 - x_1^2 x_3 \\
\psi_7(x) & = & x_7 + P_7(x_1, \ldots, x_6) \\
\psi_8(x) & = & -x_8 + P_8(x_1, \ldots, x_7)
\end{array}$$

pour des polynômes P_7 et P_8 à coefficients dans $\mathbb{F}_3$.
Pour obtenir l'isomorphisme entre $Ker(\pi_{8,0})$ et $W_2^2 \times W_1^4$, il nous reste à expliciter un autre homomorphisme de $Ker(\pi_{8,0})$ dans W_2. Pour cela, on remarque que le couple (x_2, x_6) suit la loi de W_2 dans le groupe $Ker(\pi_{6,0}) \cap Ker((\psi_1, \psi_2), \psi_4, \psi_5)$. En trouvant une section à la suite exacte

$$0 \longrightarrow Ker(\pi_{6,0}) \cap Ker((\psi_1, \psi_2), \psi_4, \psi_5) \longrightarrow Ker(\pi_{6,0}) \longrightarrow W_2 \times W_1^2 \longrightarrow 0,$$

on obtient alors l'homomorphisme $(\psi_2, \psi_6) : Ker(\pi_{6,0}) \longrightarrow W_2$, avec

$$\psi_6(x) = -x_6 - x_3^2 + x_1^3 x_3 - x_1^2 x_4 + x_1 x_5 + x_1^2 x_2^2 + x_1 x_2 x_3 + x_2 x_4 + x_2^3.$$

On a alors obtenu l'isomorphisme

$$((\psi_1, \psi_3), (\psi_2, \psi_6), \psi_4, \psi_5, \psi_7, \psi_8) : Ker(\pi_{8,0}) \longrightarrow W_2^2 \times W_1^4.$$

Via ces isomorphismes $Ker(\pi_{2,0}) \simeq W_1^2$ et $Ker(\pi_{8,0}) \simeq W_2^2 \times W_1^4$, il est clair que la projection $\pi_{8,2} : Ker(\pi_{8,0}) \longrightarrow Ker(\pi_{2,0})$ correspond à l'homomorphisme de troncation qui envoie W_2 sur W_1 et W_1 sur 0. On va utiliser ces descriptions pour construire un sous-groupe de $\mathbb{G}_m(K)$ à partir de l'exemple précédent.
Pour a une p-base canonique de K, on a construit le sous-groupe $D_{\leq 2}$-fermé

$$F_2 = \Big\{ x \in \mathbb{G}_m(K) \Big| D_1\Big(\frac{D_1(x)}{x} - \frac{a^2 D_1(x)^3}{x^3}\Big) = 0 \Big\},$$

qui correspond au sous-groupe H_2 de $\Delta_2 \mathbb{G}_m$ caractérisé par

$$\begin{aligned} H_2 \cap Ker(\pi_{2,0}) &= \{(x_1, x_2) | -x_2 - x_1^2 + a x_1^3 = 0\} \\ &= \{x \in Ker(\pi_{2,0}) | \psi_2(x) + a\psi_1(x)^3 = 0\}. \end{aligned}$$

Un groupe H $D_{\leq 8}$-fermé, correspondant à un sous-groupe H_8 de $\Delta_8 \mathbb{G}_m$, vérifie $\overline{H}^2 = F_2$ si et seulement si $\pi_{8,2}(H_8) = H_2$, ce qui équivaut au fait que l'image de $H_8 \cap Ker(\pi_{8,0})$ par l'isomorphisme $((\psi_1, \psi_3), (\psi_2, \psi_6), \psi_4, \psi_5, \psi_7, \psi_8)$ soit le sous-groupe

$$\{((u_1, u_3), (u_2, u_6), u_4, u_5, u_7, u_8) \in W_2^2 \times W_1^4 | u_2 + a u_1^3 = 0\}.$$

Considérons le sous-groupe

$$\{((u_1, u_3), (u_2, u_6), u_4, u_5, u_7, u_8) \in W_2^2 \times W_1^4 | u_2 + a u_1^3 = 0 \wedge u_6 + a^3 u_3^3 = 0\},$$

il lui correspond le sous-groupe $D_{\leq 8}$-fermé

$$\begin{aligned} H \;=\; & \Big\{ x \in \mathbb{G}_m(K) | -\frac{D_2(x)}{x} - \Big(\frac{D_1(x)}{x}\Big)^2 + a\Big(\frac{D_1(x)}{x}\Big)^3 = 0 \\ & \wedge -\frac{D_6(x)}{x} - \Big(\frac{D_3(x)}{x}\Big)^2 + \Big(\frac{D_1(x)}{x}\Big)^3 \frac{D_3(x)}{x} \\ & -\Big(\frac{D_1(x)}{x}\Big)^2 \frac{D_4(x)}{x} + \frac{D_1(x) D_5(x)}{x^2} + \Big(\frac{D_1(x) D_2(x)}{x^2}\Big)^2 \\ & + \frac{D_1(x) D_2(x) D_3(x)}{x^3} + \frac{D_2(x) D_4(x)}{x^2} + \Big(\frac{D_2(x)}{x}\Big)^3 \\ & + a^3 \Big(\frac{D_3(x)}{x} - \frac{D_1(x) D_2(x)}{x^2}\Big)^3 = 0 \Big\}. \end{aligned}$$

D'après les remarques précédentes sur la projection $\pi_{8,2}$, on voit qu'on a obtenu un sous-groupe H tel que $\overline{H}^2 = F_2$, et F_2 contient strictement $\mathbb{G}_m(C_K)$ (qui est $D_{\leq 2}$-fermé), et donc $H \not\subset \mathbb{G}_m(C_K)$.
D'autre part, les formules définissant H montrent que $x^3 \in H$ si et seulement si

$$\begin{aligned} & -\frac{D_6(x^3)}{x^3} - \Big(\frac{D_3(x^3)}{x^3}\Big)^2 + a^3 \Big(\frac{D_3(x^3)}{x^3}\Big)^3 = \\ & \quad \Big(-\frac{D_2(x)}{x} - \Big(\frac{D_1(x)}{x}\Big)^2 + a\Big(\frac{D_1(x)}{x}\Big)^3\Big)^3 = 0, \end{aligned}$$

et donc $H \cap \mathbb{G}_m(C_K) = [3]F_2 \subsetneq \mathbb{G}_m(C_K)$.
On a donc exhibé, comme on le voulait, un groupe H tel que $\mathbb{G}_m(K^{p^2}) \subset H$, mais $H \not\subset \mathbb{G}_m(K^p)$ et $\mathbb{G}_m(K^p) \not\subset H$.

IV.3 Sous-groupes minces dans les groupes algébriques

Commençons par une conséquence directe du théorème III.5.

Proposition IV.13 *Soit G un groupe algébrique irréductible ; alors $G(K)$ admet un sous-groupe infiniment définissable irréductible, rationnellement mince et Zariski-dense si et seulement s'il existe un groupe algébrique irréductible $\tilde{G}$ admettant une D-structure et un homomorphisme génériquement surjectif de $\tilde{G}$ dans G.*

Preuve Pour le sens direct, on a vu dans le théorème III.5 qu'un tel Γ sous-groupe infiniment définissable de $G(K)$, irréductible et rationnellement mince est isomorphe, en tant que groupe D-algébrique, à $\tilde{G}^D(K)$ pour un certain groupe algébrique $\tilde{G}$ admettant une D-structure. Or on a sait aussi (proposition III.10) que $\tilde{G}^D(K)$ est dense dans $\tilde{G}$, et pour un point générique x de $\tilde{G}^D(K)$ au-dessus d'un D-corps de définition k, $k(\{x\}) = k(x)$; et donc l'isomorphisme $\tilde{G}^D(K) \longrightarrow \Gamma$ est rationnel et se prolonge en un homomorphisme de $\tilde{G}$ dans G. Cet homomorphisme est génériquement surjectif car Γ est Zariski-dense dans G. Pour la réciproque, il suffit de constater que l'image de $\tilde{G}^D(K)$ est irréductible et rationnellement mince car $\tilde{G}^D(K)$ l'est (voir la proposition III.16) et Zariski-dense dans G car l'homomorphisme de $\tilde{G}$ dans G est génériquement surjectif.□

Cas des groupes algébriques commutatifs en caractéristique nulle

Dans le cas où $p = 0$, les trois notions de minceurs coïncident. Dans [Bui92], Alexandru Buium a donné des critères pour déterminer les groupes qui admettent une D-structure. Dans le cas des groupes linéaires, ce critère s'exprime simplement ; cela donne un cas où la proposition IV.1 admet une réciproque (à isomorphisme près).

Théorème IV.1 (Chapitre 2 de [Bui92]) *Soit G un groupe linéaire connexe défini sur K. Alors G admet une D-structure si et seulement si G est isomorphe à un groupe linéaire défini sur C_K.*

Il est aussi donné dans le chapitre 3 de [Bui92] un critère concernant les groupes commutatifs. Ce critère fait intervenir la cohomologie de De Rahm du groupe algébrique en question. Nous ne l'expliciterons pas ici ; nous préférons revenir sur ses conséquences : en utilisant le lien fait entre la cohomologie de De Rahm d'une variété abélienne et son extension universelle par un groupe vectoriel dans [MazMe74], Alexandru Buium a montré que cette extension universelle admet une D-structure.

Il est donné dans [Mar00] une preuve plus simple du fait que $E(A)$ admet une D-structure. C'est cette méthode que nous utiliserons pour prouver la proposition IV.14. Rappelons pour cela la caractérisation de l'extension universelle.

Proposition et définition IV.2 (Proposition 11 de [Ros58]) *Soit A une variété abélienne. Il existe une extension $f : E(A) \longrightarrow A$ de A par un groupe vectoriel (de même dimension que A), dite universelle, déterminée à unique isomorphisme près par la propriété suivante :*
pour toute extension $g : G \longrightarrow A$ de A par un groupe vectoriel, il existe un unique homomorphisme $h : E(A) \longrightarrow G$ tel que $g \circ h = f$.

Proposition IV.14 *Tout groupe algébrique commutatif et irréductible admet un sous-groupe définissable irréductible, mince et Zariski-dense.*

Preuve Commençons par définir un analogue de l'extension universelle pour un groupe algébrique commutatif quelconque. On sait d'après [Ros56] (théorème 16) qu'un tel groupe G admet une décomposition en suite exacte de la forme

$$0 \longrightarrow L \longrightarrow G \xrightarrow{g} A \longrightarrow 0$$

pour L un sous groupe linéaire irréductible de G et A une variété abélienne. On dispose aussi de la suite exacte

$$0 \longrightarrow V \longrightarrow E(A) \xrightarrow{f} A \longrightarrow 0,$$

pour un groupe vectoriel V ; ce qui permet de définir

$$E(G) := E(A) \times_A G = \{(x, y) \in E(A) \times G | f(x) = g(y)\}.$$

On a ainsi obtenu une extension de $E(A)$ par $0 \times L$:

$$0 \longrightarrow 0 \times L \longrightarrow E(G) \xrightarrow{pr_1} E(A) \longrightarrow 0.$$

On va montrer que $E(G)$ admet une D-structure, ce qui va donner en utilisant la proposition IV.13 (puisque $E(G) \longrightarrow G$ est génériquement surjective) que G a un sous-groupe irréductible, mince et Zariski-dense. On montre que $E(G)$ admet une D-structure en montrant que l'extension $\pi_{1,0} : \Delta_1 E(G) \longrightarrow E(G)$ est scindée (proposition III.12). Puisqu'on sait que le noyau de $\pi_{1,0}$ est un groupe vectoriel (proposition IV.4), il suffit de montrer que pour tout groupe vectoriel W, le groupe des extensions commutatives $Ext(E(G), W)$ est réduit à 0, c'est-à-dire au produit cartésien.
On commence par montrer cette propriété pour $E(A)$: si $H \in Ext(E(A), W))$

$$0 \longrightarrow W \longrightarrow H \xrightarrow{g} E(A) \longrightarrow 0$$

alors H s'écrit comme extension de A par W'

$$0 \longrightarrow W' \longrightarrow H \xrightarrow{f \circ g} A \longrightarrow 0,$$

avec

$$0 \longrightarrow W \longrightarrow W' \xrightarrow{g} V \longrightarrow 0,$$

et donc W' est un groupe vectoriel. La propriété universelle de l'extension universelle permet alors de trouver $h : E(A) \longrightarrow H$ tel que $f \circ g \circ h = f$. Or l'unicité de l'homomorphisme $g \circ h$ dans le diagramme

$$\begin{array}{ccc} E(A) & \xrightarrow{f \circ id} & A \\ & \searrow^{g \circ h} \quad \nearrow^{f} & \\ & E(A) & \end{array}$$

donne que $g \circ h = id$, c'est-à-dire que l'extension $H \in Ext(E(A), W)$ est triviale. Maintenant, pour $E(G)$, on utilise le fait que la suite exacte

$$0 \longrightarrow L \longrightarrow E(G) \xrightarrow{pr_1} E(A) \longrightarrow 0$$

donne, d'après la proposition 2 page 166 de [Ser59], la suite exacte

$$Ext(E(A), W) \longrightarrow Ext(E(G), W) \longrightarrow Ext(L, W).$$

Or, en caractéristique nulle, les groupes linéaires commutatifs sont des produits de $\mathbb{G}_m$ et de $\mathbb{G}_a$, ce qui donne $Ext(L, W) = 0$; et comme on vient de voir que $Ext(E(A), W) = 0$, on obtient $Ext(E(G), W) = 0$. □

Remarque Dans le cas d'une variété abélienne, on sait qu'il existe un unique tel groupe irréductible, mince et Zariski-dense qui est minimal pour ces propriétés, appelé "noyau de Manin" (voir [Man66]). Ce n'est pas le cas si on suppose seulement que G est commutatif, comme le montre l'exemple suivant, signalé par Anand Pillay.
Soit $G = \mathbb{G}_m \times \mathbb{G}_a$. En tant que groupe défini sur le corps des constantes C_K, G peut-être muni de la D-structure triviale D^0, avec $G^{D^0}(K) = G(C_K)$. On peut aussi munir G d'une structure D^1, donnée par

$$G^{D^1}(K) = \{(x, y) \in G(K) | D_1(x) = xy \wedge D_1(y) = 0\}.$$

Alors $G^{D^0}(K)$ et $G^{D^1}(K)$ sont tous les deux irréductibles, minces et Zariski-dense dans G, mais $G^{D^0}(K) \cap G^{D^1}(K) = \mathbb{G}_m(C_K) \times \{0\}$, qui n'est pas Zariski-dense dans G : il n'existe donc pas de plus petit sous-groupe définissable Zariski-dense dans G. Une telle situation existe aussi dans le groupe additif, où il existe une famille de sous-groupes Zariski-denses $b\mathbb{G}_a(C_K)$ d'intersection nulle deux à deux quand b décrit $\mathbb{G}_m(K)/\mathbb{G}_m(C_K)$; toutefois, tous ces sous-groupes sont isomorphes dans ce cas. Ici, on a de plus que $G^{D^0}(K)$ et $G^{D^1}(K)$ ne sont pas isomorphes : en effet, un tel isomorphisme induirait d'après le théorème III.5 un automorphisme de G qui transporte D^0 sur D^1. Or, puisque $\chi_a(\mathbb{G}_m) = 0$ et $\chi_m(\mathbb{G}_a) = 0$, les automorphismes de G sont de la forme $\phi(x, y) = (x^m, \alpha y)$ pour $m \in \mathbb{Z}$ et $\alpha \in \mathbb{G}_m(K)$. Or si $(x, y) \in G^{D^0}(K)$ et $\phi(x, y) \in G^{D^1}(K)$, on obtient $\alpha y x^m = D_1(x^m) = 0$ et donc $y = 0$.

Cas des variétés semi-abéliennes en caractéristique positive

Dans le cas où $p > 0$, la proposition IV.14 n'est plus valide, comme le montre l'exemple suivant.
Pour $p = 2$, fixons une p-base canonique b de K, et posons

$$G = \Lambda_1 \mathbb{G}_m := Fr^{-1} \Pi_1 \mathbb{G}_m.$$

Ses points K-rationnels sont donnés par

$$G(K) = \{(x, y) \in K^{\times 2} | x^2 + by^2 \neq 0\},$$

ils sont en bijection définissable avec $\mathbb{G}_m(K)$ via l'homomorphisme $\rho : (x, y) \mapsto x^2 + by^2$. On peut noter que G est isomorphe à $\mathbb{G}_m \times \mathbb{G}_a$ via l'isomorphisme $(x, y) \mapsto (x + b^{1/2}y, \frac{y}{x+b^{1/2}y})$ de G dans $\mathbb{G}_m \times \mathbb{G}_a$ au dessus de $K^{1/2}$ mais pas au dessus de K.
On montre que $G(K)$ n'a pas de sous-groupe infiniment définissable dense, connexe et rangé par RU (donc a fortiori pas non plus mince) : un tel sous-groupe donnerait par la bijection ρ un sous-groupe dense, connexe et rangé par RU de $\mathbb{G}_m(K)$, or le seul tel groupe est $\mathbb{G}_m(C_K^\infty)$, qui correspond à

$$\rho^{-1}(\mathbb{G}_m(C_K^\infty)) = \{(x, 0) \in K^{\times 2} | x \in \mathbb{G}_m(C_K^\infty)\} \subset G(K),$$

qui n'est pas dense dans G.

Considérons plus particulièrement les variétés semi-abéliennes. Les ensembles infiniment définissables minces sont nécessairement rangés par RU (car $RU(a/K) \leq deg.tr(K\{a\}/K)$) ; citons la proposition suivante issue de [BouDel02].

Proposition IV.15 (Lemme 3.5 et proposition 3.6 de [BouDel02]) *Supposons $p > 0$ et que G est une variété semi-abélienne. Le seul sous-groupe de $G(K)$ infiniment définissable, irréductible, Zariski-dense et rangé par RU est $p^\infty G(K) := \bigcap_{n \geq 0} p^n G(K)$. Ce sous-groupe $p^\infty G(K)$ est mince, avec*

$$deg.tr(k(\{a\})/k) = dim\ G$$

pour a un point générique de $p^\infty G(K)$ et k un corps de définition de G.
Si de plus G est définie sur C_K^∞, $p^\infty G(K) = G(C_K^\infty)$.

Il est intéressant de savoir quand ce sous-groupe $p^\infty G(K)$ est "plus" que mince. Dans [PilZie03], Anand Pillay et Martin Ziegler ont montré comment obtenir une preuve directe de la conjecture de Mordell-Lang dans le cas où $p^\infty G(K)$ est très mince. La question de savoir si $p^\infty G(K)$ est très mince pour toute variété semi-abélienne G est encore ouverte aujourd'hui. Une condition suffisante pour que ce soit le cas est que G soit *ordinaire* (voir [PilZie03]) ; cette condition est purement algébrique, c'est-à-dire qu'elle ne fait pas intervenir la dérivation de Hasse.
Donnons maintenant un critère purement algébrique pour que $p^\infty G(K)$ soit très mince. Rappelons que l'isogénie "Frobenius à la puissance n" $Fr^n : G \longrightarrow Fr^n G$ admet une isogénie duale, définie sur K, appelée *Verschiebung*, $V_n : Fr^n G \longrightarrow G$. Ces isogénies vérifient $V_n \circ Fr^n = [p^n]_G$ et $Fr^n \circ V_n = [p^n]_{Fr^n G}$.

Définition IV.1 *On pose α_n l'unique homomorphisme défini sur K^{p^n} donné par la définition III.14 tel que le diagramme suivant commute*

$$\begin{array}{ccc} Fr^n G & \xrightarrow{V_n} & G \\ & \searrow \alpha_n \quad \nearrow \rho_n & \\ & \Pi_n G & \end{array}.$$

On pose G_n l'image de $Fr^n G$ dans $\Pi_n G$ par α_n.

Proposition IV.16 *Pour $n \geq m$, $\rho_{n,m}(G_n) = G_m$; et $\rho_{n,m|G_n}$ est une isogénie de G_n sur G_m.*

Preuve Pour $n \geq m$, on a la situation suivante :

$$\begin{array}{ccccc} Fr^n G & \xrightarrow{V'_{n-m}} & Fr^m G & \xrightarrow{V_m} & G \\ & & \searrow^{\alpha_m} & \nearrow_{\rho_m} & \\ & & \Pi_m G & & \end{array}$$

où V'_{n-m} est l'isogénie duale de $Fr^{n-m} : Fr^m G \longrightarrow Fr^n G$. La relation sur l'isogénie duale d'une composée d'isogénies (voir [Lan59]) donne que $V_n = V_m \circ V'_{n-m}$. On a d'autre part $V_n = \rho_n \circ \alpha_n = \rho_m \circ \rho_{n,m} \circ \alpha_n$. Cela donne deux écritures de l'homomorphisme $V_n \circ Fr^{n-m} : Fr^m G \longrightarrow G$:

$$\rho_m \circ \rho_{n,m} \circ \alpha_n \circ Fr^{n-m} = \rho_m \circ \alpha_m \circ [p^{n-m}]_{|Fr^m G}.$$

Puisque les homomorphismes $\rho_{n,m} \circ \alpha_n \circ Fr^{n-m}$ et $\alpha_m \circ [p^{n-m}]_{|Fr^m G}$ sont définis sur K^{p^m}, ils sont donc égaux par unicité de la factorisation via $\Pi_m G$. Puisque l'image de $[p^{n-m}]_{|Fr^m G}$ est dense, on a donc $\rho_{n,m} \circ \alpha_n(Fr^{n-m}(Fr^m G)) = \alpha_m(Fr^m G)$, c'est-à-dire $\rho_{n,m}(G_n) = G_m$.
Pour montrer que $\rho_{n,m|G_n}$ réalise une isogénie, il suffit donc de montrer que G_m et G_n ont même dimension. Or ce dernier point vient du fait que α_n, tout comme V_n, a un noyau fini, et donc $dim\ G_n = dim\ Fr^n G = dim\ G$, et de même pour G_m. □

Proposition IV.17 *Le sous-groupe $p^\infty G(K)$ est très mince si et seulement s'il existe un entier m tel que le morphisme $\rho_{n,m|G_n} : G_n \longrightarrow G_m$ est séparable pour tout $n \geq m$.*

Preuve Pour $b \in p^\infty G(K)$ générique, considérons $a \in G(K)$ (lui aussi générique) tel que $b = [p^n]a$, et $a_n = \alpha_n \circ Fr^n(a) \in G_n(K^{p^n})$, qui est générique dans G_n. On a $\rho_n(a_n) = V_n \circ Fr^n(a) = [p^n]a = b$; et comme ρ_n est une bijection de $\Pi_n G(K^{p^n})$ dans $G(K)$, de bijection réciproque φ_n (voir la définition I.7), on a $a_n = \varphi_n(b)$.
On suppose tout d'abord que $p^\infty G(K)$ est très mince ; et soit m tel que $k(\{b\})$ est algébrique séparable sur $k(D_0(b), \ldots, D_{p^m-1}(b)) = k(\phi_m(b))$. Pour $n \geq m$, le point a_n générique dans G_n que l'on vient de considérer vérifie $a_n = \varphi_n(b)$ et donc $\rho_{n,m}(a_n) = \varphi_m(b)$. Dans la suite d'extension

$$k(\varphi_m(b)) \subset k(\varphi_n(b)) \subset k(\{b\}),$$

on sait que $k(\{b\})$ est algébrique séparable sur $k(\varphi_m(b))$, et donc $k(\varphi_n(b))$ aussi : on a donc que $\rho_{n,m|G_n}$ est séparable.
On suppose maintenant que $\rho_{n,m|G_n} : G_n \longrightarrow G_m$ est séparable pour tout $n \geq m$. Pour $n \geq m$, fixons b, a et a_n comme précédemment ; on a $a_n = \varphi_n(b)$, et donc $\rho_{n,m}(a_n) = \varphi_m(b)$. Comme $\rho_{n,m|G_n}$ est une isogénie séparable, on obtient que $k(\varphi_n(b))$ est algébrique séparable sur $k(\phi_m(b))$. Comme c'est vrai pour tout $n \geq m$, on a donc que $k(\{b\})$ est algébrique séparable sur $k(\varphi_m(b))$, et donc que $tp(b/k)$ est très mince. □

Remarque Ce critère est clairement vérifié dans le cas où la variété semi-abélienne G est ordinaire, puisque dans ce cas les isogénies V_n sont séparables,

et donc les isogénies $\rho_{n|G_n}$ aussi.

Pour savoir si $p^\infty G(K)$ est rationnellement mince, on utilise la proposition IV.13 en la précisant.

Proposition IV.18 *Le sous-groupe $p^\infty G(K)$ est rationnellement mince si et seulement si G est isogène à une variété semi-abélienne admettant une D-structure.*

Preuve Le sens réciproque de l'équivalence est une conséquence évidente de la proposition IV.13, puisqu'une isogénie est un homomorphisme surjectif.
Pour le sens direct, la preuve est la même que pour la proposition IV.13, sauf qu'on doit en plus vérifier que le groupe algébrique $\tilde{G}$ construit dans cette preuve est une variété semi-abélienne isogène à G. Or dans la construction de $\tilde{G}$, donnée par le théorème III.5, on a vu que l'isomorphisme $\psi : p^\infty G(K) \longrightarrow \tilde{G}^D(K)$ envoie un point générique x de vers un point $\psi(x)$ générique dans $\tilde{G}$, avec $k(\psi(x)) = k(\{x\})$ (k désigne un corps de définition dénombrable de G). Cela nous donne donc, par la proposition IV.15, que

$$dim\tilde{G} = deg.tr(k(\{x\})/k) = dimG.$$

Puisque l'homomorphisme de $\tilde{G}$ dans G est génériquement surjectif, on obtient donc que c'est une isogénie, et donc que $\tilde{G}$ est une variété semi-abélienne. □

Ici, pour $p > 0$, nous ne disposons pas de critères aussi aboutis que ceux donnés par Alexandru Buium dans [Bui92] en caractéristique nulle pour savoir si un groupe algébrique admet une D-structure. Toutefois, une conséquence directe de la proposition III.13 pour les variétés semi-abéliennes est le critère suivant :

Corollaire IV.5 *Une variété semi-abélienne définie sur K admet une D-structure si et seulement si, pour tout entier n, elle est isomorphe à une variété semi-abélienne définie sur K^{p^n}.*

Preuve Par rapport au critère donné dans la proposition III.13, on a seulement omis la condition sur les corps de définition des isomorphismes. On peut le faire d'après le théorème de rigidité des variétés semi-abéliennes : si A et B deux variétés semi-abéliennes définies sur le corps séparablement clos K^{p^n} sont isomorphes, elles le sont par un isomorphisme défini sur K^{p^n} (voir le théorème 5 page 26 de [Lan59]). □

Pour les courbes elliptiques, il est facile de voir, en utilisant la notion de j-invariant(voir [Hus87] par exemple), que cette condition se réduit au fait que la courbe elliptique est isomorphe à une courbe elliptique définie sur $C_K^\infty = \bigcap K^{p^n}$.
Ce résultat se généralise pour les variétés abéliennes de dimension quelconque à l'aide d'un argument donné par Damien Roessler, et aussi discuté avec Jean-Benoît Bost, Elisabeth Bouscaren, Anand Pillay et Thomas Scanlon.
On doit utiliser pour cela la notion de "schéma de modules", pour laquelle on prend comme référence [MumFog82].

Définition IV.2 *Soit G une variété abélienne de dimension g définie sur k. Une polarisation ω est un homomorphisme de G dans sa variété abélienne duale*

$\hat{G}$, associé à un "faisceau inversible ample" sur G. Une structure de niveau n sur G, sur k, est la donnée d'une base $x_1, \ldots, x_{2g}$ de la n-torsion dans $G(k)$. Les triplets $(G, \omega, (x_1, \ldots, x_{2g}))$ sont les objets d'une catégorie dont les morphismes sont les homomorphismes de variétés abéliennes qui commutent avec les polarisations de la source et de l'image, et qui respectent la structure de niveau n de la source et de l'image.

Proposition et définition IV.3 (Théorème 7.9 de [MumFog82]) *Quels que soient les entiers $g, d \geq 1$, et n suffisamment grand, il existe un schéma de modules $A_{g,d,n}$ au-dessus de $\mathbb{F}_p$ qui représente le foncteur $\mathcal{A}_{g,d,n}$, qui à tout corps $k \supset \mathbb{F}_p$ associe l'ensemble des variétés abéliennes de dimension g définies sur k, munies d'une polarisation de degré d^2 et d'une structure de niveau n sur k, à isomorphisme près.*

En d'autres termes, pour tout corps $k \supset \mathbb{F}_p$, l'ensemble des k-points $A_{g,d,n}(k)$ correspond "naturellement" à l'ensemble des classes d'isomorphismes des triplets $(G, \omega, (x_1, \ldots, x_{2g}))$, définis sur k, où G est de dimension g et ω de degré d^2.

Corollaire IV.6 *Si une variété abélienne G, définie sur K, admet une D-structure, alors elle est isomorphe à une variété abélienne définie sur C_K^∞.*

Preuve Pour G donnée, de dimension g, il découle de la construction de la variété duale $\hat{G}$ une polarisation ω sur G (théorème 10 page 117 de [Lan59] par exemple), de degré de la forme d^2, $d \geq 1$ (proposition 6.13 de [MumFog82]). D'autre part, choisissons n assez grand pour que la proposition et définition précédente s'applique, et premier avec p. Puisque K est séparablement clos, on sait alors que la n-torsion de G est contenue dans $G(K)$, caractérisé par une base à $2g$ éléments (voir par exemple [Hin98]). On obtient une structure de niveau n sur K en fixant cette base $\mathcal{B}$.
Ensuite, pour tout m, soit G_m une variété abélienne définie sur K^{p^m} et isomorphe à G, exhibée dans le corollaire IV.5. On transporte ω et $\mathcal{B}$ sur G_m par isomorphisme ; on obtient alors ω_m, qui reste une polarisation sur G_m, et $\mathcal{B}_m$, qui est une structure de niveau n sur K^{p^m} car la n-torsion de G_m est dans $G_m(K^{p^m})$. On a ainsi un point dans $A_{g,d,n}(K^{p^m})$.
Puisque le point de $A_{g,d,n}(K)$ correspondant à $(G, \omega, \mathcal{B})$ correspond aussi à tous les $(G_m, \omega_m, \mathcal{B}_m)$, ce point est dans l'intersection $\bigcap_m A_{g,d,n}(K^{p^m}) = A_{g,d,n}(C_K^\infty)$. Il correspond à ce point une variété abélienne définie sur C_K^∞, isomorphe à G.□

Corollaire IV.7 *Toute variété abélienne définie sur K et munie d'une D-structure (G, D) est isotriviale, c'est-à-dire isomorphe à (G_0, D^0), où G_0 est une variété abélienne définie sur C_K^∞ et D^0 la D-structure triviale qui lui est attachée.*

Preuve C'est une conséquence directe du corollaire précédent et du corollaire IV.2 : soit G_0 une variété abélienne définie sur C_K^∞ isomorphe à G, en transportant la D-structure de G, on obtient une D-structure sur G^0. Cette D-structure ne peut être que triviale du fait du résultat d'unicité exprimé dans le corollaire IV.2. □

On déduit de la proposition IV.18 et du corollaire IV.6 :

Corollaire IV.8 *Soit G une variété abélienne définie sur K. Alors $p^\infty G(K)$ est rationnellement mince si et seulement si G est isogène à une variété abélienne définie sur C_K^∞.*

Comme annoncé dans la section III.3.3, on en déduit un exemple de type très mince mais pas rationnellement mince. Considérons pour cela une courbe elliptique E définie sur K, et non isogène à une courbe elliptique définie sur C_K^∞ (il suffit pour cela de choisir son j-invariant dans $K \setminus C_K^\infty$, car C_K^∞ est algébriquement clos).

Corollaire IV.9 *Pour une telle courbe elliptique E, $p^\infty E(K)$ est très mince mais pas rationnellement mince.*

Preuve D'après ce qui précède, $p^\infty E(K)$ n'est pas rationnellement mince. Puisque $deg.tr(k\{a\}/k) = 1$ pour un point générique a de $p^\infty E(K)$, $p^\infty E(K)$ est très mince d'après la proposition III.15 (ce dernier point était déjà connu en utilisant des résultats de classification des courbes elliptiques : celles-ci sont soit ordinaires, soit isomorphes à une courbe elliptique définie sur $\mathbb{F}_p^{alg} \subset C_K^\infty$. Dans le premier cas, le cas particulier signalé après la proposition IV.17 permet de conclure que $p^\infty G(K)$ est très mince. Dans le second cas, on a $p^\infty G(K) = G(C_K^\infty)$ d'après la proposition IV.15, et ceci est rationnellement mince). $\square$

Un exemple de D-structure non triviale sur le groupe additif en caractéristique positive

Quand G est un groupe algébrique (défini sur C_K^∞) tel que $\chi_a(G)$ n'est pas trivial, on trouve des sous-groupes rationnellement minces de $G(K)$ autres que ceux donnés par la D-structure triviale, à isomorphisme près. Ainsi, pour le groupe additif $\mathbb{G}_a$, on construit à partir d'un exemple donné par Thomas Blossier une D-structure D sur $\mathbb{G}_a$, telle que $(\mathbb{G}_a, D)$ n'est pas isomorphe à $(\mathbb{G}_a, D^0)$, le groupe additif muni de la D-structure triviale.
On peut tout d'abord remarquer que $(\mathbb{G}_a, D)$ est isomorphe à $(\mathbb{G}_a, D^0)$ si et seulement si $\mathbb{G}_a^D(K)$ est un espace vectoriel (de dimension 1) au dessus de C_K^∞ (c'est un sous-groupe de la forme $a\mathbb{G}_a(C_K^\infty)$).
Soit b une p-base canonique de K, et posons Γ le sous-groupe de $\mathbb{G}_a(K)$ préimage de $\mathbb{G}_a(C_K^\infty)$ par l'isogénie $x \mapsto \frac{x-x^p}{b}$. Pour $x \in \Gamma$, x s'écrit donc $x = x^p + by$ pour un certain y dans $\mathbb{G}_a(C_K^\infty)$, ce qui donne

$$D_1(x) = y = \frac{x - x^p}{b} \in \mathbb{F}_p(b)(x),$$

puis par une induction sur $n \geq 1$:

$$D_{p^n}(x) = D_{p^n}(x^p) = (D_{p^{n-1}}(x))^p \in \mathbb{F}_p(b)(x).$$

On obtient donc que $\mathbb{F}_p(b)(\{x\}) = \mathbb{F}_p(b)(x)$, ce qui donne d'après la preuve du théorème III.5 que $\Gamma = \mathbb{G}_a^D(K)$ pour une certaine D-structure D sur $\mathbb{G}_a$. Et on constate que Γ n'est pas isomorphe à $\mathbb{G}_a(C_K^\infty)$, puisqu'il n'est pas invariant par multiplication par des éléments de C_K^∞.

Toutefois, dans cet exemple, $\mathbb{G}_a^D(K)$ est encore isogène à $\mathbb{G}_a(C_K^\infty)$ (par l'isogénie $x \mapsto \frac{x-x^p}{b}$). On ne connaît pas pour l'instant de sous-groupes rationnellement

minces autres que ceux qui sont isogènes à $G(C_K^\infty)$ pour un certain groupe algébrique G défini sur C_K^∞ ; on a vu par exemple (corollaire IV.8) que dans les variétés abéliennes, les sous-groupes rationnellement minces sont nécessairement iosgène à un certain $G(C_K^\infty)$.
La question de l'existence d'autres sous-groupes rationnellement minces, et minimaux, équivaut, d'après le théorème de dichotomie sur les géométries de Zariski, à l'existence d'un sous-groupe rationnellement mince et localement modulaire : on peut associer à un type minimal q une géométrie. Si la géométrie associée au type q vérifie certaines propriétés sur la dimension (voir [Mar98] pour plus de détails), le type q est dit type de Zariski.
Dans [Hru96], Ehud Hrushovski a montré que les types minimaux minces dans la théorie CHC_p sont de Zariski, et cela a été généralisé pour les types minimaux quelconques dans CHC_p par Françoise Delon dans [Del98]. Le résultat de dichotomie sur les géométries de Zariski prouvé dans [HruZil96] se traduit dans notre contexte par le résultat suivant (voir [BouDel02]) :

Proposition IV.19 (Fait 4.8 de [BouDel02]) *Un type minimal q non trivial est soit localement modulaire, soit non orthogonal à C_K^∞.*

On en déduit :

Corollaire IV.10 (Proposition 4.7 de [BouDel02]) *Un groupe infiniment définissable minimal H est soit localement modulaire, soit isogène à $G(C_K^\infty)$ pour G un groupe algébrique de dimension 1 défini sur C_K^∞.*

Chapitre V

Cas de la caractéristique nulle : description des types, rangs et types génériques

Ce chapitre regroupe différents outils et résultats propres à la caractéristique nulle. Il reprend et complète la publication [Ben02]. Dans la théorie CHC_0, les rangs de la stabilité RU et RM, et le rang topologique RH dont on donnera une définition, ne coïncident pas nécessairement. Néanmoins, Anand Pillay et Wai Yan Pong ont montré dans [PilPon02] que les rangs RU et RM d'un groupe définissable dans CHC_0 sont égaux. Au contraire, nous allons montrer ici (section V.3) que les rangs RM et RH d'un groupe définissable peuvent être différents, et peuvent même conduire à des notions de type générique qui ne sont pas équivalentes.
Avant cela, nous commencerons par donner une description des D-idéaux de $k\{X\}$, déjà bien connue des théoriciens des modèles quand X est une monovariable (voir le chapitre 6 de [Poi87a] par exemple), et complétée pour un nombre supérieur de variable essentiellement grâce aux travaux de Joseph Ritt ; et aussi les preuves des résultats de la section I.3.2 que l'on avait utilisés dans les deux premiers chapitres.

V.1 Description des D-idéaux de $k\{X\}$

D'après le corollaire II.2, la description des n-types sur un D-corps k équivaut à celle des D-idéaux premiers de $k\{X\}$, pour X une multivariable de taille n. La plupart des outils pour cette description, dans le cas de la caractéristique nulle, se trouvent dans [Rit50].
Dans ce qui suit, A est un D-anneau commutatif intègre et de caractéristique nulle. On reprendra les notations de la section I.3.1, où l'on a défini la D-algèbre des D-polynômes $A\{X\}$.

Définition V.1 *Soit X une monovariable. On définit un préordre $\preceq_X$ sur*

$A\{X\}$ par :

- *si X apparaît effectivement dans les deux D-polynômes P et Q, $P \preceq_X Q$ si $ordre_X(P) \leq ordre_X(Q)$, et, en cas d'égalité ($ordre_X(P) = ordre_X(Q) = m$), $deg_{d_m X}(P) \leq deg_{d_m X}(Q)$*
- *si P et Q sont deux D-polynômes non-nuls, et si X n'apparaît pas dans P, $0 \prec_X P \preceq_X Q$.*

On note respectivement $\prec_X$ et $\sim_X$ le préordre strict et la relation d'équivalence associés à $\preceq_X$.

Fait V.1 *Si Q divise P, alors $Q \preceq_X P$. Si X apparaît dans P, $0 \prec_X M_X(P) \preceq_X S_X(P) \prec_X P$.*

Les deux résultats de cette section reposent sur le lemme suivant, issu de [Rit50].

Lemme V.1 *Soit X une monovariable, et $P \in A\{X\} \setminus A$ un D-polynôme non-scalaire, de séparante S et de majeur M. Pour tout $Q \in A\{X\}$, il existe $Q_1 \prec_X P$ et des entiers i, j tels que $S^i M^j Q \equiv Q_1 \mod \{P\}$.*

Preuve Soit $m := ordre_X(P)$. On montre par récurrence sur $ordre_X(Q)$ qu'il existe Q_2, avec $ordre_X(Q_2) \leq m$, et un entier i, tel que $S^i Q \equiv Q_2 \mod \{P\}$. Pour cela, on utilise que, pour tout entier $h \geq 1$, $D_h P = \binom{m+h}{m} S d_{m+h} X + R$, avec $ordre_X(R) < m + h$ (fait I.10). Donc, si $ordre_X(Q) = m + h$, et si $d = deg_{d_{m+h} X}(Q)$, on trouve un D-polynôme Q_3, avec $ordre_X(Q_3) < m + h$, tel que $S^d Q \equiv Q_3 \mod \{P\}$, ce qui fait fonctionner le raisonnement par récurrence. Ensuite, en utilisant la division euclidienne dans $B := A\{X\}_{<m}[M^{-1}][d_m X]$, on trouve $Q_4 \in B$, de degré en $d_m X$ strictement inférieur à celui de P, tel que $Q_2 \equiv Q_4 \mod (P)$. En multipliant par une certaine puissance de M, et en utilisant le fait que $deg_{d_m X}(M) = 0$, on obtient donc $Q_1 \in A\{X\}$, tel que $Q_1 \prec_X P$ et $S^i M^j Q \equiv Q_1 \mod \{P\}$. □

Le théorème suivant est attribué à Ritt et Raudenbush, la démonstration donnée suit celle de [Mar96], théorème 1.16.

Théorème V.1 (Ritt-Raudenbush) *Supposons que A satisfasse la condition de chaîne ascendante pour les D-idéaux radiciels, et soit X une monovariable. Alors $A\{X\}$ satisfait la condition de chaîne ascendante pour les D-idéaux radiciels.*

Preuve Remarquons tout d'abord qu'un D-anneau satisfait la condition de chaîne ascendante pour les idéaux radiciels si et seulement si tout D-idéal radiciel I est finiment engendré, c'est-à-dire s'il existe une partie finie J telle que $I = \sqrt{\{J\}}$.
Remarquons aussi que si le D-idéal radiciel $\sqrt{\{J\}}$ est finiment engendré pour une certaine partie J d'un D-anneau A, alors il existe un sous-ensemble fini $J_0 \subset J$ tel que $\sqrt{\{J_0\}} = \sqrt{\{J\}}$. En effet, soit $a_1, \ldots, a_m$ des éléments tel que $\sqrt{\{J\}} = \sqrt{\{a_1, \ldots, a_m\}}$. Pour $1 \leq i \leq m$, il existe un nombre fini d'éléments $(b_{i,j})$ de J, une suite presque partout nulle $(\alpha_{i,j,h})$ d'éléments de A et un entier $n_i \geq 1$ tels que :

$$a_i^{n_i} = \sum_{j,h} \alpha_{i,j,h} D_h(b_{i,j}).$$

Alors $\sqrt{\{J\}} = \sqrt{\{(b_{i,j})\}}$, puisque c'est le plus petit D-idéal radiciel contenant les $(b_{i,j})$, et donc les (a_i).
Supposons qu'il existe dans $A\{X\}$ un D-idéal radiciel qui n'est pas finiment engendré. Par le lemme de Zorn, il existe un tel D-idéal I maximal pour ces propriétés (si une union croissante de D-idéaux radiciels est finiment engendrée, cette chaîne de D-idéaux doit être stationnaire).
Montrons tout d'abord que I est premier. C'est un idéal propre, et s'il existe $a \notin I$, $b \notin I$ tels que $ab \in I$, alors $\sqrt{\{I,a\}}$ et $\sqrt{\{I,b\}}$ sont finiment engendrés ; notons I_1 et I_2 les parties finies de I telles que $\sqrt{\{I,a\}} = \sqrt{\{I_1,a\}}$ et $\sqrt{\{I,b\}} = \sqrt{\{I_2,b\}}$. Alors, par le lemme I.2, $\sqrt{\{I_1,a\}}\sqrt{\{I_2,b\}} \subset \sqrt{\{ab, aI_1, bI_2, I_1I_2\}} \subset I$; et si $x \in I$, $x^2 \in \sqrt{\{I_1,a\}}\sqrt{\{I_2,b\}} \subset \sqrt{\{ab, aI_1, bI_2, I_1I_2\}}$, donc $x \in \sqrt{\{ab, aI_1, bI_2, I_1I_2\}}$. D'où $I = \sqrt{\{ab, aI_1, bI_2, I_1I_2\}}$, ce qui contredit que I n'est pas finiment engendré. Donc I est premier.
Par hypothèse sur A, $I \cap A$ est un D-idéal radiciel finiment engendré (par un ensemble fini J_0 d'éléments de A), notons $J = \sqrt{\{J_0\}}$ dans $A\{X\}$. Puisque I n'est pas finiment engendré, il existe un élément $P \in I \setminus J$, choisissons le minimal pour $\preceq_X$ et notons M et S respectivement son majeur et sa séparante.
On a $P = M(d_nX)^d + P_0$, avec $P_0 \prec_X P$ et $M \prec_X P$; par conséquent, $M \notin I \setminus J$. De plus, si on avait $M \in J$, on aurait $P_0 \in I \setminus J$, ce qui est impossible par minimalité de P. On a donc $M \notin I$. On montre de même que $S \notin I$, puisque $P = \frac{1}{d}(d_nX)S + P_1$, avec $P_1 \prec_X P$.
Comme I est premier, $MS \notin I$; et donc, par choix de I, $\sqrt{\{I, MS\}}$ est finiment engendré : il existe une partie finie $I_0 \subset I$ telle que $\sqrt{\{I, MS\}} = \sqrt{\{I_0, MS\}}$. De plus, par le lemme V.1, pour tout $Q \in I$, il existe des entiers u, v et $Q_1 \prec_X P$ tels que $M^uS^vQ \equiv Q_1 \mod \{P\}$; on a alors $Q_1 \in I$, et par minimalité de P, $Q_1 \in J$. On a ainsi $MSI \subset \sqrt{\{J_0, P\}}$. On en déduit, puisque I est radiciel :

$$\begin{array}{rcccl} I & = & I^2 & \subset & I\sqrt{\{I, MS\}} \\ & & & \subset & \sqrt{\{I_0I, MSI\}} \\ & & & \subset & \sqrt{\{I_0, J_0, P\}} \quad \subset \quad I, \end{array}$$

et donc $I = \sqrt{\{I_0, J_0, P\}}$ est finiment engendré. □

Corollaire V.1 *Soit $k \models CH_0$ et X une multivariable. Alors $k\{X\}$ satisfait la condition de chaîne ascendante pour les D-idéaux radiciels. Ainsi, tout D-idéal radiciel propre de $k\{X\}$ s'écrit comme intersection finie de D-idéaux premiers.*

Preuve La première assertion découle immédiatement du théorème V.1 par récurrence, puisque le corps k satisfait trivialement la condition de chaîne ascendante pour les idéaux.
Pour la deuxième assertion, s'il existait un D-idéal radiciel propre de $k\{X\}$ qui ne soit pas intersection finie de D-idéaux premiers, on pourrait d'après la condition de chaîne ascendante trouver un tel D-idéal I maximal pour cette propriété. En particulier, le D-idéal propre I n'est pas premier, donc il existe $a \notin I$, $b \notin I$ tel que $ab \in I$. Les D-idéaux $\sqrt{\{I,a\}}$ et $\sqrt{\{I,b\}}$ sont donc soit égaux à $k\{X\}$, soit intersections finies de D-idéaux premiers. Or, $\sqrt{\{I,a\}}\sqrt{\{I,b\}} \subset \sqrt{\{I,ab\}} = I$ d'après le lemme I.2, et donc pour $c \in \sqrt{\{I,a\}} \cap \sqrt{\{I,b\}}$, $c^2 \in I$ et donc $c \in I$; d'où $I = \sqrt{\{I,a\}} \cap \sqrt{\{I,b\}}$. D'après les propriétés de $\sqrt{\{I,a\}}$ et $\sqrt{\{I,b\}}$,

puisque I est propre, I est une intersection finie de D-idéaux premiers. $\square$

On utilise maintenant le lemme V.1 pour donner une description des D-idéaux premiers de $k\{X\}$ (pour $k \models CH_0$ et X une multivariable de taille n). Les notions utilisées viennent de [Rit50].

Définition V.2 *Soit P un D-polynôme non-scalaire de $k\{X\}$. On appelle indice de P l'unique entier i tel que $P \in k\{X_1, \ldots, X_i\} \setminus k\{X_1, \ldots, X_{i-1}\}$.*

Définition V.3 *On dit qu'un r-uplet $(P_1, \ldots, P_r)$ (éventuellement vide) d'éléments non scalaires de $k\{X\}$, d'indices respectifs $(i_1, \ldots, i_r)$, est une chaîne si*

- $i_1 < \ldots < i_r$
- *pour $j < h$, $P_h \prec_{X_{i_j}} P_j$*

Définition V.4 *Soit $(P_1, \ldots, P_r)$ une chaîne de D-polynômes, d'indices respectifs $(i_1, \ldots, i_r)$, et S la partie multiplicative*

$$\{S_{X_{i_1}}(P_1)^{s_1} \ldots S_{X_{i_r}}(P_r)^{s_r} M_{X_{i_1}}(P_1)^{m_1} \ldots M_{X_{i_r}}(P_r)^{m_r} | s_1, \ldots, s_r, m_1, \ldots, m_r \in \mathbb{N}\}.$$

On pose

$$I_{(P_1,\ldots,P_r)} := S^{-1}\{P_1, \ldots, P_r\}.$$

Lemme V.2 *Soit $(P_1, \ldots, P_r)$ une chaîne de D-polynômes, d'indices respectifs $(i_1, \ldots, i_r)$, et S défini comme ci-dessus. Pour tout polynôme Q, il existe un D-polynôme Q_1, et $\Pi \in S$, tels que $\Pi Q \equiv Q_1 \mod \{P_1, \ldots, P_r\}$ et que, pour $1 \leq j \leq r$, $Q_1 \prec_{X_{i_j}} P_j$. Si, de plus, Q est d'indice $i > i_r$, on peut choisir $Q_1 \preceq_{X_i} Q$.*

Preuve Ce lemme consiste en une itération du lemme V.1. Notons pour cela que, si P et Q sont d'indices respectifs i et j, avec $i < j$, le D-polynôme Q_1 est obtenu, d'après l'algorithme du lemme V.1, en remplaçant dans Q les variables $d_m X_i$ par des fractions rationnelles d'indice inférieur ou égal à i, puis en faisant une division euclidienne par P, d'indice i, et dont le majeur est d'ordre en X_i strictement inférieur à celui de P. Il découle de cela que Q_1, tel que $Q_1 \prec_{X_i} P$ et qu'il existe des entiers u, v tels que $M_{X_i}(P)^u S_{X_i}(P)^v Q \equiv Q_1 \mod \{P\}$, vérifie aussi $Q_1 \preceq_{X_j} Q$.
Le résultat cherché est donc obtenu en trouvant successivement $Q_r, \ldots, Q_1$, tels que

$$\begin{array}{ccc}
M_{X_{i_r}}(P_r)^{u_r} S_{X_{i_r}}(P_r)^{v_r} Q \equiv Q_r \mod \{P_r\} & \text{et} & Q_r \prec_{X_{i_r}} P_r \\
M_{X_{i_{r-1}}}(P_{r-1})^{u_{r-1}} S_{X_{i_{r-1}}}(P_{r-1})^{v_{r-1}} Q_r \equiv Q_{r-1} \mod \{P_{r-1}\} & \text{et} & Q_{r-1} \prec_{X_{i_{r-1}}} P_{r-1} \\
\vdots & & \vdots \\
M_{X_{i_1}}(P_1)^{u_1} S_{X_{i_1}}(P_1)^{v_1} Q_2 \equiv Q_1 \mod \{P_1\} & \text{et} & Q_1 \prec_{X_{i_1}} P_1.
\end{array}$$

Le D-polynôme Q_1 vérifie alors bien la condition exigée, y compris si Q est d'indice supérieur à i_r. $\square$

Théorème V.2 *Soit I un D-idéal premier de $k\{X\}$. Il existe une chaîne de D-polynômes $(P_1, \ldots, P_r)$ de I (et une suite $(i_1, \ldots, i_r)$ d'indices associée), tels que, de manière équivalente :*

1. *I est le plus petit D-idéal premier contenant $P_1, \ldots, P_r$ et ne contenant pas $S_{X_{i_1}}(P_1), \ldots, S_{X_{i_r}}(P_r), M_{X_{i_1}}(P_1), \ldots, M_{X_{i_r}}(P_r)$.*
2. *$I = I_{(P_1,\ldots,P_r)}$*

Preuve On va construire, par récurrence à partir de la chaîne vide, une chaîne $(P_1, \ldots, P_s)$ de D-polynômes de I, d'indices $(i_1, \ldots, i_s)$, telle que, pour tout s :
- I ne contient ni $M_{X_{i_s}}(P_s)$, ni $S_{X_{i_s}}(P_s)$
- $I \cap k\{X_1, \ldots, X_{i_s}\} = I_{(P_1,\ldots,P_s)} \cap k\{X_1, \ldots, X_{i_s}\}$

Cette construction va s'arrêter quand $I_{(P_1,\ldots,P_s)} = I$.
On considère la chaîne $(P_1, \ldots, P_s)$ déjà construite, soit $J = I_{(P_1,\ldots,P_s)}$. Si $J = I$, $(P_1, \ldots, P_s)$ est la chaîne recherchée, sinon, il existe $Q \in I \setminus J$. On choisit Q d'indice i_{s+1} minimum, puis minimum pour $\prec_{X_{i_{s+1}}}$. Par le lemme V.2, on trouve Q_1 tel que $\Pi Q \equiv Q_1 \mod \{P_1, \ldots, P_s\}$ pour un produit Π de M_j et de S_j $(1 \leq j \leq s)$, et tel que $Q_1 \prec_{X_{i_j}} P_j$ pour tout $1 \leq j \leq s$ et $Q_1 \preceq_{X_{i_{s+1}}} Q$. Puisque $Q \in I \setminus J$, $Q_1 \in I \setminus J$ (en effet, $Q_1 \in J$ implique $\Pi Q \in J$, et donc $Q \in J$ par définition de J) ; par minimalité dans le choix de Q, $Q \sim_{X_{i_{s+1}}} Q_1$. Parmi les facteurs irréductibles de Q_1, il y en a un dans $I \setminus J$, notons-le P_{s+1} ; par minimalité dans le choix de Q, on doit avoir $Q \sim_{X_{i_{s+1}}} Q_1 \sim_{X_{i_{s+1}}} P_{s+1}$.
Cette construction de P_{s+1} vérifie bien :
- $(P_1, \ldots, P_{s+1})$ est une chaîne ; en effet, $i_{s+1} > i_s$ puisque $(I \setminus J) \cap k\{X_1, \ldots, X_{i_s}\} = \emptyset$, et pour tout $1 \leq j \leq s$, $P_{s+1} \preceq_{X_{i_j}} Q_1 \prec_{X_{i_j}} P_j$.
- I ne contient ni $M_{X_{i_{s+1}}}(P_{s+1})$, ni $S_{X_{i_{s+1}}}(P_{s+1})$.
  En effet, $M := M_{X_{i_{s+1}}}(P_{s+1}) \prec_{X_{i_{s+1}}} P_{s+1}$ et $T := S_{X_{i_{s+1}}}(P_{s+1}) \prec_{X_{i_{s+1}}} P_{s+1}$, donc ils n'appartiennent pas à $I \setminus J$ par minimalité de P_{s+1}. De plus, s'ils sont dans J, et si $(d_m X_{s+1})^d$ est le monôme dominant dans P_{s+1}, alors $P' := P_{s+1} - M(d_m X_{s+1})^d \in I \setminus J$, avec $P' \prec_{X_{i_{s+1}}} P_{s+1}$ (ou respectivement $P'' := P_{s+1} - T\frac{(d_m X_{s+1})}{d} \in I \setminus J$, avec $P'' \prec_{X_{i_{s+1}}} P_{s+1}$), ce qui contredit la minimalité de P_{s+1}.
- $I \cap k\{X_1, \ldots, X_{i_{s+1}}\} = I_{(P_1,\ldots,P_{s+1})} \cap k\{X_1, \ldots, X_{i_{s+1}}\}$. En effet, si R, d'indice inférieur ou égal à i_{s+1} est dans I, on trouve, par le lemme V.2, R_1 tel que $R_1 \prec_{X_{i_j}} P_j$ pour tout $1 \leq j \leq s+1$ et $\Pi R \equiv R_1 \mod \{P_1, \ldots, P_{s+1}\}$ pour un produit Π des majeurs et séparantes de $P_1, \ldots, P_{s+1}$. En particulier, $R_1 \in I$, et par minimalité de P_{s+1}, $R_1 \in I_{(P_1,\ldots,P_s)}$, et ainsi $R \in I_{(P_1,\ldots,P_{s+1})}$. Réciproquement, si $R \in I_{(P_1,\ldots,P_{s+1})}$, $R \in I$ puisque I est premier, et contient $P_1, \ldots, P_{s+1}$ mais pas leurs majeurs ni leurs séparantes.

Cette construction s'arrête nécessairement, puisque les chaînes dans $k\{X\}$ ne peuvent pas être de longueur strictement supérieure à n ; on trouve ainsi une chaîne $(P_1, \ldots, P_r)$ tel que $I = I_{(P_1,\ldots,P_r)}$.
Montrons maintenant que les caractérisations 1 et 2 sont équivalentes. Si J est un D-idéal premier contenant $P_1, \ldots, P_r$ mais pas $S_{X_{i_1}}(P_1), \ldots, S_{X_{i_r}}(P_r)$, $M_{X_{i_1}}(P_1), \ldots, M_{X_{i_r}}(P_r)$, il est clair que $I_{(P_1,\ldots,P_r)} \subset J$. Réciproquement, la chaîne $(P_1, \ldots, P_r)$ qui a été construite vérifie bien ces hypothèses. □

En particulier, dans le cas de $k\{X\}$ où X est une monovariable, les D-idéaux premiers sont soit le D-idéal nul, soit déterminés par une chaîne qui se réduit à un D-polynôme irréductible. Il est utile d'établir la caractérisation suivante pour ce D-polynôme "minimal".

Proposition V.1 *Soit I un D-idéal premier non nul de $k\{X\}$ pour une monovariable X, et (P) la chaîne déterminée dans le théorème précédent telle que $I = I_{(P)}$.*
Si $Q \in I$ et $Q \prec_X P$, alors $Q = 0$.
Si Q est un D-polynôme irréductible de I, de même ordre que P, alors il existe un élément $a \in k$ non nul tel que $Q = aP$; en particulier, $I = I_{(P)} = I_{(Q)}$.

Preuve La première assertion découle directement de la construction donnée dans la preuve précédente. Pour la deuxième assertion, on trouve en effectuant la division euclidienne de Q par P un D-polynôme $R \prec_X P$, un D-polynôme A et un entier u tels que $M_X(P)^u Q = AP + R$. Comme $R \in I$, on a $R = 0$; et comme P est irréductible et ne divise pas son majeur, P divise Q. Comme Q est irréductible, Q et P ne diffèrent que par la multiplication par un élément non nul de k. Il découle ensuite directement de la définition que $I_{(Q)} = I_{(P)}$. □

V.2 Quelques rangs dans la théorie CHC_0

Outre les rangs RU et RM que l'on peut définir dans toute théorie ω-stable, on définit les deux rangs suivants, qui se rapportent respectivement aux propriétés topologiques et algébriques des modèles de CHC_0. Les définitions et propriétés données ici ne sont que des généralisations au cas de plusieurs variables des notions de rang développées dans les corps différentiellement clos de caractéristique nulle (voir [Poi78] ou [Mar96]). Pour la définition de la notion de rang au sens de Lascar, on peut consulter le chapitre 17 de [Poi87a].

V.2.1 Le rang RH

On définit le rang RH comme un rang de profondeur sur les D-idéaux premiers. Pour cela, on utilisera la correspondance associant à un type $p \in S(k)$, pour $k \models CH_0$, le D-idéal premier I_p de $k\{X\}$ comme défini dans le corollaire II.2. Pour l'étude de ces D-idéaux, on utilisera la correspondance avec les objets de la géométrie D-algébrique décrits dans la section III.1.1. Le corollaire V.1, qui est un résultat de finitude, permet de donner des versions fortes des résultats de cette section.

Fait V.2

1. *La proposition III.1 est valable quand K est simplement un modèle de CHC_0.*
2. *Toute variété D-affine admet un D-corps de définition finiment engendré en tant que D-corps.*
3. *L'existence des points génériques dans les variétés D-affines est assurée dès que K est un modèle $\aleph_0$-saturé de CHC_0.*

Définition V.5 *On définit la relation $RH(p) \geq \alpha$ par l'induction sur l'ordinal α, simultanément pour tout $k \models CH_0$ et $p \in S(k)$:*
- *si α est un ordinal limite, $RH(p) \geq \alpha$ si et seulement si $RH(p) \geq \beta$ pour tout ordinal $\beta < \alpha$*

– *pour un ordinal successeur, $RH(p) \geq \alpha + 1$ si et seulement s'il existe un fils q de p sur un $l \models CH_0$ contenant k, et un type $r \in S(l)$ tels que $I_q \subsetneq I_r$ et $RH(r) \geq \alpha$.*

S'il existe, le plus petit ordinal β tel que $RH(p) \not\geq \beta$ est un ordinal successeur $\alpha+1$. On définit alors $RH(p) = \alpha$; dans le cas contraire, on dit que p n'est pas rangé par RH.

Proposition V.2 *Le rang RH est un rang au sens de Lascar.*

Preuve La définition de RH est évidemment préservée par isomorphisme de modèles. La propriété de filiation du rang (le rang d'un père est supérieur ou égal à celui de ses fils) découle aussi directement de la définition.
Pour les propriétés d'extension et de multiplicité bornée, on va utiliser la description de la D-topologie de la section III.1.1. Si k est inclus dans un modèle K de CHC_0, les types sur k correspondent aux variétés D-affines avec paramètres dans k, irréductibles en tant que D-fermés sur k. Il découle de la proposition III.1 que les propriétés topologiques entre les diverses variétés D-affines ne dépendent pas du modèle K considéré ; on omettra donc de le préciser, supposant seulement qu'il contient tous les ensembles de paramètres. Avec cette identification, on a la caractérisation suivante :

Lemme V.3 *Soit $p \in S(k)$ rangé par RH, et $q \in S(l)$. Alors q est un fils de p de même RH si et seulement si $\mathcal{V}(I_q)$ est une composante irréductible en tant que D-fermé sur l de $\mathcal{V}(I_p)$.*

Preuve du lemme Supposons que q est un fils de p de même RH. Puisque $I_p \subset I_q$, $\mathcal{V}(I_q) \subset \mathcal{V}(I_p)$, et $\mathcal{V}(I_q)$ est défini avec paramètres dans l par définition, et irréductible en tant que tel. Un tel $\mathcal{V}(I_q)$ est contenu dans une composante irréductible F de $\mathcal{V}(I_p)$ en tant que D-fermé sur l ; et alors $\mathcal{I}(F) \cap l\{X\}$ est un D-idéal premier de $l\{X\}$, donc c'est l'idéal I_r d'un type $r \in l\{X\}$. En intersectant les inclusions $I_p \subset I_r \subset I_q$ avec $k\{X\}$, on obtient $I_r \cap k\{X\} = I_p$ (puisque $I_q \cap k\{X\} = I_p$). Le type r est donc un fils de p et $I_r \subset I_q$; puisque $RH(p) = RH(q)$, on doit donc avoir que $I_r = I_q$: $\mathcal{V}(I_q)$ est une composante irréductible en tant que D-fermé sur l de $\mathcal{V}(I_p)$.
Réciproquement, supposons que $\mathcal{V}(I_q)$ est une composante irréductible en tant que D-fermé sur l de $\mathcal{V}(I_p)$. Les isomorphismes de K fixant k permuttent les composantes absolument irréductibles de $\mathcal{V}(I_p)$; notons F l'union des conjugués de $\mathcal{V}(I_q)$ par k-isomorphisme. Alors le fermé F est stable par k-isomorphisme, et donc, en utilisant l'élimination des imaginaires (corollaire II.6), on obtient que le plus petit D-corps de définition pour $\mathcal{I}(F)$ est inclus dans k. Puisque $\mathcal{V}(I_p)$ est k-irréductible, on obtient que $\mathcal{V}(I_p) = F$: les conjugués de $\mathcal{V}(I_q)$ par k-isomorphisme recouvrent $\mathcal{V}(I_p)$. Le fermé $\mathcal{V}(I_q \cap k\{X\})$, défini sur k, contient tous les conjugués de $\mathcal{V}(I_q)$ par k-isomorphisme, il est donc égal à $\mathcal{V}(I_p)$: on a donc $I_q \cap k\{X\} = I_p$, c'est-à-dire que q est un fils de p.
On montre maintenant par induction sur $RH(p)$ que q a même rang que p. Puisque $RH(q) \leq RH(p)$, c'est évident quand $RH(p) = 0$. Si $RH(p) = \alpha + 1$, par définition, il existe une extension k' de k, un fils p' de p sur k' et $r \in S(k')$ tel que $RH(r) = \alpha$ et $I_{p'} \subsetneq I_r$. Regardons les composantes absolument irréductibles de $\mathcal{V}(I_p)$, dans un modèle K contenant k, k' et l ; $\mathcal{V}(I_{p'})$ est une composante irréductible de $\mathcal{V}(I_p)$ en tant que D-fermé sur k' (car p' a même

rang que p par choix de p', et la première partie de l'équivalence s'applique) et $\mathcal{V}(I_q)$ est une composante irréductible de $\mathcal{V}(I_p)$ par hypothèse, donc $V(I_{p'})$ et $\mathcal{V}(I_q)$ s'écrivent tous les deux comme union finie de composantes absolument irréductible de $\mathcal{V}(I_p)$. Par hypothèse d'induction, une composante absolument irréductible de $\mathcal{V}(I_r)$ correspond à un fils de r (sur K) de même rang que r ; et elle strictement contenue dans une composante absolument irréductible de $\mathcal{V}(I_p)$. Par k-isomorphisme de K, on peut transporter cette composante dans une composante absolument irréductible de p contenue dans $\mathcal{V}(I_q)$; on trouve donc des types q' et r' sur K qui sont dans la configuration suivante : $\mathcal{V}(I_{q'})$ est une composante absolument irréductible de $\mathcal{V}(I_q)$, et donc correspond à un fils de q sur K, et elle contient strictement $V(I_{r'})$, avec $RH(r') = \alpha$ car c'est l'image par isomorphisme d'un fils équirang de r. Cela montre donc que $RH(q) = \alpha+1$. Dans le cas où $RH(p) = \alpha$ est un ordinal limite, on suppose par l'absurde que $RH(q) = \beta < \alpha$. Comme $RH(p) > \beta + 2$, il existe, dans une extension k' de k, un fils q' de p et $r \in S(k')$ tels que $I_{q'} \subsetneq I_r$ et $RH(r) \geq \beta + 1$. D'autre part, $RH(r) < \alpha$ (car sinon $RH(r) \geq \alpha + 1$), et on peut donc appliquer l'hypothèse d'induction pour r : sur un modèle K contenant k' et l, il existe une composante irréductible $\mathcal{V}(I_t)$ (avec $t \in S(K)$) de $\mathcal{V}(I_r)$, et $RH(r) = RH(t)$. Or cette composante irréductible $\mathcal{V}(I_t)$ est contenue dans une composante absolument irréductible $\mathcal{V}(I_s)$ de $\mathcal{V}(I_p)$, et on a donc $RH(s) \geq RH(t) = RH(r) \geq \beta+1$. Or toute les composantes absolument irréductibles de $\mathcal{V}(I_p)$ sont conjuguées, donc $\mathcal{V}(I_q)$ contient un des conjugués de $\mathcal{V}(I_s)$, et donc $RH(q) \geq RH(s)\beta + 1$. Cette contradiction conclut la preuve du lemme. □

La propriété d'extension vient alors directement de l'existence des composantes irréductibles. On en déduit aussi la propriété de multiplicité bornée (et même finie) : d'après le corollaire V.1, $\mathcal{V}(I_p)$ n'a qu'un nombre fini de composantes irréductibles, et donc un nombre fini de fils de même rang RH dans $S(l)$. □

Lemme V.4 *Soit $p \in S(K)$ pour $K \models CHC_0$ un modèle $\aleph_0$-saturé. Alors $RH(p) \geq \alpha+1$ si et seulement s'il existe $t \in S(K)$ tel que $I_p \subsetneq I_t$ et $RH(t) \geq \alpha$.*

Preuve Soit $q, r \in S(l)$ donnés comme dans la définition de $RH(p) \geq \alpha+1$. Soit $K' \models CHC_0$ contenant l. Les inclusions $I_p \subset I_q \subsetneq I_r$ donnent $\mathcal{V}(I_r) \subsetneq \mathcal{V}(I_p)$ dans une puissance cartésienne de K'. Soient a et b des uplets de paramètres qui engendrent des D-corps de définition de $\mathcal{V}(I_p)$ et $\mathcal{V}(I_r)$ respectivement, avec $a \in K$. Soit c une réalisation de $tp(b/a)$ dans K. Soit $\phi(x, b)$ la conjonction d'équations D-polynomiales définissant $\mathcal{V}(I_r)$, alors, dans une puissance cartésienne de K, on a :

- $\phi(K, c) \subsetneq \mathcal{V}(I_p)$ car c'est une formule de $tp(c/a)$
- $\phi(K, c)$ est irréductible car c'est une conjonction infinie de formules de $tp(c/a)$; et donc il existe un type $t \in S(K)$ tel que $\phi(K, c) = \mathcal{V}(I_t)$
- $RH(t) = RH(r) \geq \alpha$ car t est l'image de r par un isomorphisme envoyant b sur c.

Cela donne le résultat voulu. □

Proposition V.3 *Tous les types sont rangés par RH.*

Preuve Supposons le contraire : soit $p \in S(K)$ non rangé par RH ; on peut aussi supposer que l'ensemble de paramètres K est un modèle $\aleph_0$-saturé. Pour tout ordinal α, $RH(p) \geq \alpha + 1$, donc d'après le lemme précédent, il existe q_α tel

que $I_p \subsetneq I_{q_\alpha}$ et $RH(q_\alpha) \geq \alpha$. Puisqu'il ne peut pas exister dans $S(K)$ des types de RH arbitrairement grand (le nombre de variables est fixé), cela signifie qu'il existe parmi les q_α un type p_1 non rangé par RH. En répt́ant cette construction, on trouve une suite infinie dénombrable de types p_i, non rangés par RH, et tels que

$$I_p \subsetneq I_{p_1} \subsetneq \ldots \subsetneq I_{p_i} \subsetneq \ldots \quad .$$

Cela contredit la condition de chaîne ascendante pour les D-idéaux premiers (corollaire V.1). □

Remarque On voit facilement que le type p est l'unique type de RH maximum de $\mathcal{V}(I_p)$; pour tout sous-ensemble définissable A de $\mathcal{V}(I_p)$ contenant p (en particulier les ouverts relatifs à $\mathcal{V}(I_p)$), on dira que p est le type générique au sens topologique de A.

Proposition V.4 *$RM \leq RH$*

Preuve D'après la caractérisation 1 du théorème V.2, pour tout $p \in S(k)$ tel que $I_p \neq 0$, il existe des D-polynômes $P_1, \ldots, P_r, M_1, \ldots, M_r, S_1, \ldots, S_r$ tel que si $q \in S(k)$ vérifie

$$P_1 = 0 \wedge \ldots \wedge P_r = 0 \wedge M_1 \neq 0 \wedge \ldots \wedge M_r \neq 0 \wedge S_1 \neq 0 \wedge \ldots \wedge S_r \neq 0, \qquad (*)$$

alors $I_p \subset I_q$; et d'autre part la formule $(*)$ est dans p. On en déduit que la formule $(*)$ isole p des types de RH supérieur ou égal ; et donc, par une induction aisée, que $RM \leq RH$. □

V.2.2 Le rang RD

Le rang RD est une généralisation du degré de transcendance, prenant des valeurs ordinales dans le cas où celui-ci est infini. C'est surtout un outil de calcul efficace pour déterminer les autres rangs ; pour pouvoir le comparer au rang RH, on utilisera essentiellement le rang RD pour des types sur des modèles K.
Ce rang RD est lié à la notion de polynôme de Kolchin d'un uplet sur un corps différentiel ; on pourra consulter à ce propos [Pon99], [Pon00] et [Joh69].

Proposition et définition V.1 *Soit $p \in S_n(K)$. Il existe des entiers α_p et β_p tels que pour toute réalisation a de p, et pour tout entier r suffisamment grand,*

$$deg.tr(K(\{a\}_{\leq r})/K) = \alpha_p.r + \beta_p.$$

Ce polynôme $r \to \alpha_p.r + \beta_p$ est appelé polynôme de Kolchin du type p. On a toujours $\beta_p \geq \alpha_p$.

Preuve Soit a une réalisation de p. Pour $r \geq 0$, notons

$$m_r := deg.tr(K(\{a\}_{\leq r+1})/K(\{a\}_{\leq r}))$$

(m_r est indépendant du choix de la réalisation a de p). Le résultat est alors une conséquence du fait suivant : la suite $(m_r)_{r\geq 0}$ est décroissante. Pour montrer ce fait, il suffit de constater que si $D_r(a_1), \ldots, D_r(a_{m_{r-1}})$ est une base de transcendance de $K(\{a\}_{\leq r})$ sur $K(\{a\}_{\leq r-1})$ extraite du uplet $D_r(a)$ (quitte

à modifier l'ordre des variables), alors pour tout $m_r < i \leq n$, on obtient, en appliquant D_1 à l'égalité $P(D_r(a_i)) = 0$, où P est le polynôme minimal de $D_r(a_i)$ sur $K(\{a\}_{\leq r-1})(D_r(a_1), \ldots, D_r(a_{m_{r-1}}))$, une égalité donnant $D_{r+1}(a_i)$ comme élément de $K(\{a\}_{\leq r})(D_{r+1}(a_1), \ldots, D_{r+1}(a_{m_{r-1}}))$; d'où $m_r \leq m_r - 1$.□

Définition V.6 *Soit $p \in S(K)$. Si $r \to \alpha_p.r + \beta_p$ est le polynôme de Kolchin du type p, on note $RD(p) = \omega.\alpha_p + (\beta_p - \alpha_p)$.*

Remarque La fonction RD obtenue ne peut pas être à proprement parler considérée comme un rang, puisqu'elle ne porte que sur les types sur des modèles de CHC_0. Toutefois, une fois définie de manière restreinte, et après avoir montré la proposition suivante, on peut étendre la définition de RD pour $p \in S(k)$, avec $k \models CH_p$: c'est la valeur de $RD(q)$, pour q un fils non-déviant de p sur un modèle K contenant k.

Proposition V.5 *On obtient ainsi un rang au sens de Lascar.*

Preuve Les propriétés de filiation et de conservation par isomorphisme de modèles sont évidemment vérifiées. Pour montrer les propriétés d'extension et de multiplicité bornée, il suffit de montrer la caractérisation suivante :
pour deux modèles $K \subset L$ et $q \in S(L)$ une extension de $p \in S(K)$, $RD(p) = RD(q)$ si et seulement si q est un fils non déviant de p.
Supposons tout d'abord que q est un fils non déviant de p, et fixons une réalisation a de q. D'après le corollaire II.4, cela signifie que $K(\{a\})$ est algébriquement disjoint de L au dessus de K, et donc que $RD(a/K) = RD(a/L)$.
Réciproquement, si $RD(p) = RD(q)$ et si a est une réalisation de q, alors pour tout entier r suffisamment grand, $deg.tr(K(\{a\}_{\leq r})/K) = deg.tr(L(\{a\}_{\leq r})/L)$.
On montre alors que tout ensemble algébriquement indépendant au dessus de K parmi $D_0(a), \ldots, D_r(a)$ le reste au dessus de L. En effet, si on complète un tel ensemble en une base de transcendance $\mathcal{B}$ de $K(\{a\}_{\leq r})$ sur K, alors tout élément de $L(\{a\}_{\leq r})$ est algébrique sur $L(\mathcal{B})$; et comme

$$card(\mathcal{B}) = deg.tr(K(\{a\}_{\leq r})/K) = deg.tr(L(\{a\}_{\leq r})/L),$$

$\mathcal{B}$ est algébriquement indépendant au dessus de L. On en déduit que $K(\{a\})$ est algébriquement disjoint de L au dessus de K, et donc que q est un fils non déviant de p d'après le corollaire II.4. □

On note aussi que, si $RD(p)$ est fini, $RD(p) = deg.tr(K\{a\}/K)$ pour toute réalisation a de p.
D'autre part, il existe une autre détermination de α_p :

Définition V.7 *Soit $k \subseteq l$ une extension de corps différentiels, on dit qu'un sous-ensemble A de l est δ-algébriquement indépendant sur k si l'ensemble*

$$\{D_i(x); x \in A, i \in \mathbb{N}\}$$

est algébriquement indépendant sur k.
On définit, dans $\mathbb{N} \cup \{\infty\}$,

$$\delta.deg.tr(l/k) = sup\{card(A); A \subset l \text{ est } \delta\text{-algébriquement indépendant sur } k\}.$$

Remarque Dans le cas où $l = k\{a_1, \ldots, a_n\}$, on peut prendre parmi $a_1, \ldots, a_n$ un ensemble δ-algébriquement indépendant maximal de l sur k, et on a donc $\delta.deg.tr(l/k) \leq n$.

Fait V.3 *Soit $p \in S_n(K)$, alors $\alpha_p = \delta.deg.tr(K\{a\}/K)$ pour une réalisation a de p, et donc $\alpha_p \leq n$, avec égalité si et seulement si $RD(p) = \omega.n$.*

Soient deux types p et q de $S(K)$ tels que $I_p \subsetneq I_q$, alors pour tout r suffisamment grand, on a

$$I_p \cap K\{X\}_{\leq r} \subsetneq I_q \cap K\{X\}_{\leq r}$$

et donc $RD(p) > RD(q)$.
On en déduit :

Proposition V.6

- *Pour tout ensemble définissable irréductible, son type générique au sens topologique est son unique type de RD maximal*
- *Pour tout type p, $RH(p) \leq RD(p)$.*

V.2.3 Relations entre les différents rangs

On vient de voir que l'on a :

$$RU \leq RM \leq RH \leq RD.$$

De plus, si $\alpha_p = \delta.deg.tr(K\{a\}/K)$ pour une réalisation a de p, on a d'après les inégalités de Lascar et la définition de RD :

$$\omega.\alpha_p \leq RU(p) \leq RM(p) \leq RH(p) \leq RD(p) < \omega.(\alpha_p + 1).$$

En particulier, pour chaque type p, tous ces rangs sont simultanément finis, et on pourra parler sans ambiguité de type de rang fini.

L'inégalité entre RU et RM peut être stricte, ce résultat a été montré par Hrushovski et Scanlon dans [HruSca99]. Notons que l'égalité entre les rangs RU et RM dans tout groupe de rang de Morley fini (théorème V.4) ci-dessous, montré dans un cas plus général dans [Las85], page 462) montre que le type exhibé dans [HruSca99], qui est de rang fini, ne peut être inclus dans aucun groupe de rang fini.
L'inégalité entre RM et RH peut être stricte, il est montré dans [Poi78] (et aussi dans [Mar96]) que le 1-type de D-idéal associé $I_{(2Xd_2X-d_1X)}$ est de $RM = 1$ et de $RH = 2$; plus précisément $I_{(d_1X)}$ est le seul D-idéal premier de $RD = 1$ contenant $I_{(2Xd_2X-d_1X)}$.
L'inégalité entre RH et RD peut être stricte, comme le montre l'exemple de l'équation de Painlevé, étudié par Kolchin : il est prouvé dans [Mar96] que le 1-type de D-idéal associé $I_{(d_2X-3X^2-x)}$, pour $x \in K \setminus C_K$, est de $RH = 1$ et de $RD = 2$.

Puisque tous ces rangs sont différents, ils peuvent donner des notions différentes de type générique (c'est-à-dire de type de rang maximal dans un ensemble

définissable).
On a vu que, dans un ensemble définissable irréductible, les deux notions "être de RH maximal" et "être de RD maximal" coïncident. Ce n'est plus le cas si l'ensemble n'est plus irréductible, si on définit par exemple p et q dans $S_2(K)$ par $I_p = I_{(d_2X-3X^2-x, d_2Y-3Y^2-x)}$ (pour $x \in K \setminus C_K$) et $I_q = I_{(d_2X, d_1Y)}$, on voit facilement que $RD(p) = 4$, $RH(p) = 2$ et $RD(q) = RH(q) = 3$, donc p est le type de RD maximal de $D := \mathcal{V}(I_p) \cup \mathcal{V}(I_q)$, et q est le type de RH maximal de D.
Un autre exemple de différence entre les notions de type générique est donné grâce aux types p et q de $S_1(K)$ définis par $I_p = I_{(2Xd_2X-d_1X)}$ et $I_q = I_{(d_1X)}$; alors p et q sont deux types de $\mathcal{V}(I_p)$, p est l'unique type générique au sens topologique de $\mathcal{V}(I_p)$, mais $\mathcal{V}(I_p)$ a deux types de RM maximum, p et q. Dans cet exemple, le type générique au sens topologique est encore de RM maximum. On verra dans la section V.3 un fermé irréductible où les deux notions différent totalement, cet exemple sera de rang infini ; on n'en connait pas de tels de rang fini.
Ce même exemple montre que le RH, même pour des rangs finis, n'est pas conservé par bijection définissable, ce qui sera une question importante pour la suite. En effet, l'application qui à tout élément x de $D := \langle 2xD_2(x) = D_1(x) \wedge D_1(x) \neq 0 \rangle$ associe (x, y) avec $y = 1/x'$ est une bijection de D sur son image, et elle envoie p, qui est de $RH = 2$, sur le type r défini par $I_r = I_{(2Xd_2X-d_1X, Yd_1X-1)}$, et le fait que $I_{(d_1X)}$ soit le seul D-idéal premier de $RD = 1$ qui contient I_p permet de montrer que $RH(r) = 1$. On verra dans la section V.3 un autre exemple, de rang infini et plus exploitable pour construire des groupes, de bijection définissable qui ne conserve pas le RH.

V.2.4 Rangs et types génériques dans les groupes définissables

On a rappelé dans la section III.3.1 les notions de connexité et de type générique pour les groupes définissables dans une théorie stable. Dans le contexte de la théorie CHC_0, où l'on dispose des rangs précédemment évoqués, le théorème suivant, montré dans [Poi87b] pour le rang de Morley, donne une nouvelle caractérisation du type générique.

Théorème V.3 *Soit G un groupe, et R une application définie sur $S_1(G)$ à valeurs ordinales, invariante par multiplication par les éléments de G et telle que G ne contienne qu'un nombre fini de types de rang R maximum.*
Alors le groupe G est connexe (c'est-à-dire sans sous-groupe propre définissable d'indice fini) si et seulement si G ne contient qu'un type p de rang R maximum. Dans ce cas, ce type p est le type générique de G au sens des groupes.

Ce théorème s'applique en particulier quand R est le rang U ou le rang de Morley, qui sont conservés par bijection définissable, et on obtient ainsi :

Corollaire V.2 *Soit G un groupe définissable dans la théorie CHC_0. Alors G est connexe si et seulement si G ne contient qu'un type de RU (respectivement de RM) maximum. Dans ce cas, ce type est le type générique de G au sens des groupes.*

On peut aussi citer le résultat suivant, issu de [PilPon02], qui montre que les rangs RU et RM ont des comportements proches dans les groupes définissables

dans la théorie CHC_0.

Théorème V.4 *Soit G un groupe connexe défini dans la théorie CHC_0, de type générique p. Alors $RU(p) = RM(p)$.*
Si de plus G est de rang fini, alors les rangs RU et RM coïncident dans G tout entier.

V.2.5 Le cas des groupes de rang fini

Le cas des groupes de rang fini est particulier du fait de la proposition suivante :

Proposition V.7 *Soit f une bijection définissable avec paramètres dans un D-corps k, de domaine E, et soit a un élément de rang fini de E dans une extension de k. Alors $RD(a/k) = RD(f(a)/k)$.*

Preuve Il suffit de remarquer que le fait que f soit une bijection définissable implique que $k(\{a\}) = k(\{f(a)\})$ (voir la proposition II.3). On en déduit directement en considérant les degrés de transcendance que $RD(a/k) = RD(f(a)/k)$.□

Remarque Ce résultat n'est pas valable pour les types de rang infini. Considérons en effet l'application qui à un élément x associe le couple $(x, D_1(x))$, elle envoie bijectivement le 1-type générique (c'est-à-dire de D-idéal associé nul), qui est de $RD = \omega$, sur le 2-type de D-idéal associé $I_{(Y-d_1X)}$, qui est de $RD = \omega + 1$. Les exemples qui seront donnés dans la section V.3 reposent également sur une bijection qui ne conserve pas le rang RD.

D'autre part, RD range tous les types, et si D est un ensemble définissable, les types de RD maximal de D se trouvent parmi les types génériques au sens topologique de chacune des composantes irréductibles de G (puisque sur un ensemble irréductible, le type générique au sens topologique est le seul type de RD maximal), et il y en a donc un nombre fini puisque la D-topologie est nœtherienne.
Le théorème V.3 s'applique donc au rang RD, et permet d'obtenir pour des groupes irréductibles, dont le type générique au sens topologique est le seul type de RD maximal :

Proposition V.8 *Un groupe G irréductible et de rang fini est connexe, et son type générique au sens des groupes est son type générique au sens topologique.*

Remarque Comme dans les corps algébriquement clos, il existe des groupes définissables connexes et non-irréductibles : on peut transporter de manière définissable sur le fermé non-irréductible $\langle XY = 1\rangle \cup (0,0)$, la structure de groupe additif connexe de $K \models CHC_0$ en utilisant la bijection donnée par la première projection ; on obtient un exemple de rang fini en prenant la trace sur le plan des constantes $C_K \times C_K$.
Toutefois, dans cet exemple, le type générique au sens des groupes est tout de même l'unique type de RH maximal. On ne sait pas si le type générique au sens des groupes est toujours de RH maximal pour des groupes de rang fini ; on verra dans la section V.3 un contre-exemple pour un groupe de rang infini.

V.2.6 Le cas des groupes D-algébriques

Dans le théorème III.3, on a vu l'équivalence entre les groupes définissables connexes et les groupes D-algébriques irréductibles. Dans ces derniers, les translations sont continues donc préservent la topologie du groupe D-algébrique ; cela explique que l'on obtienne le théorème suivant.

Théorème V.5 *Soit G un groupe D-algébrique. Alors G est connexe si et seulement s'il est irréductible. Dans ce cas, son unique type générique au sens des groupes coïncide avec son unique type générique au sens topologique.*

Preuve La plupart des outils pour cette démonstration viennent de la preuve du théorème III.3. Ce théorème permet de voir le groupe D-algébrique G comme un groupe définissable ; on a montré en utilisant le fait III.11 que si G est irréductible, alors G est connexe en tant que groupe définissable. Si on suppose maintenant que G est connexe, de type générique p (au sens des groupes), on va montrer que G est irréductible de type générique topologique p.
Soit $G := \bigcup_{i=1}^{n} F_i$ une décomposition non redondante de G en fermés irréductibles. On va montrer qu'il n'existe qu'une de ces composantes qui contienne l'unité e, et cette composante est un sous-groupe de G. Remarquons tout d'abord que pour a dans G et F_j une des composantes irréductibles, on a, par bicontinuité de la multiplication par a, que $a.F_j$ est un fermé irréductible maximal de G, c'est donc une autre composante irréductible F_h ; de même pour F_j^{-1}. Supposons que $e \in F_1$, comme $F_1 \not\subset F_2 \cup \ldots \cup F_n$, il existe $b \in F_1 \setminus (F_2 \cup \ldots \cup F_n)$. Alors si F_j est une composante contenant e, $b.F_j$ est une composante irréductible contenant b, c'est donc F_1, et de même $b.F_1 = F_1$, donc $F_1 = F_j$: c'est donc la seule composante irréductible contenant e. Ensuite, puisque F_1^{-1} est une composante irréductible contenant e, $F_1^{-1} = F_1$; et pour tout $a \in F_1$, $a^{-1} \in F_1$, donc $a.F_1$ est une composante irréductible contenant e, c'est donc F_1. Ainsi F_1 est bien un sous-groupe de G.
On en déduit que G est irréductible. En effet, pour tout a dans G, $a.F_1$ est parmi le nombre fini de composantes irréductibles de G, donc F_1 est un sous-groupe d'indice fini de G, donc $F_1 = G$ et G est irréductible.
Montrons maintenant que p est le type générique au sens topologique de G. L'ensemble définissable $\overline{p}$ (réunion des fermés $\mathcal{V}(I_p)$ vus dans chacun des ouverts de carte) contient p donc, par définition, il exite des éléments $a_1, \ldots, a_l$ tels que $G = a_1.\overline{p} \cup \ldots \cup a_l.\overline{p}$. Or G est irréductible, et tous les $a_i.\overline{p}$ sont fermés, donc $G = a_i.\overline{p}$ pour un cerain i, c'est-à-dire $G = \overline{p}$: p est le type générique au sens topologique de G. □

On sait par le théorème III.3 que tous les groupes définissables connexes peuvent être munis d'une structure de groupe D-algébrique irréductible. Mais les renseignements donnés par le théorème précédent sur les types génériques des groupes D-algébriques ne donnent pas de renseignements sur le type générique du groupe définissable originel, avec la topologie induite par la D-topologie. En effet, quand on considère un groupe D-algébrique comme un groupe définissable, cela ne se fait qu'à isomorphisme définissable près, et ces isomorphismes "oublient" la topologie du groupe D-algébrique. Ce fait va être illustré par les exemples suivants, qui montrent qu'en prenant les images par isomorphismes définissables de groupes D-algébriques affines, ni le fait d'être irréductible, ni la notion de type générique au sens topologique ne sont conservés.

V.3 Contre-exemples pour les types génériques de rang infini

Les objets que l'on définira dans cette section garderont leur signification tout au long de celle-ci.

V.3.1 Les bijections Φ_n

Pour $n \geq 1$, on définit une application Φ_n qui associe (y_1, y_2) à (x_1, x_2) avec :

$$y_1 = x_1 D_n\Big(\frac{x_2}{x_1}\Big) \qquad y_2 = x_2 D_n\Big(\frac{x_2}{x_1}\Big).$$

Cette application est une bijection de $A_n := \{\, (x_1, x_2) \,|\, x_1 \neq 0 \wedge D_n(\frac{x_2}{x_1}) \neq 0 \,\}$ sur lui-même (car $y_2/y_1 = x_2/x_1$), la bijection réciproque étant donnée par :

$$x_1 = \frac{y_1}{D_n(y_2/y_1)} \qquad x_2 = \frac{y_2}{D_n(y_2/y_1)}.$$

Soit p le type de $S_2(K)$ défini par $I_p = I_{(d_1 X_2)}$; on remarque que pour tout entier n, $p \in A_n$, et on note $p_n := \Phi_n(p)$. On va montrer que les bijections Φ_n ne conservent ni le rang RH ni le rang RD du type p.

Rangs des types p et p_n

Si (x_1, x_2) est une réalisation de p, les éléments $x_2, x_1, D_1(x_1), \ldots, d_i(x_1), \ldots$ sont algébriquement indépendants au-dessus de K ; les inégalités de Lascar et le calcul du polynôme de Kolchin donnent :

$$\omega + 1 \leq RU(p) \leq RM(p) \leq RH(p) \leq RD(p) = \omega + 1.$$

d'où $RM(p) = RH(p) = \omega + 1$ et aussi $RM(p_n) = \omega + 1$, d'après la conservation par bijection définissable.

Proposition V.9 *Pour tout $n \geq 1$, $RH(p_n) = \omega + n + 1$.*

Preuve On cherche une chaîne minimale de polynômes pour l'idéal I_{p_n}.
Soit (y_1, y_2) une réalisation de p_n, image de (x_1, x_2). En appliquant D_1 à l'expression $y_2 = x_2 D_n(x_2/x_1)$, on obtient $D_1(y_2) = (n+1)x_2 D_{n+1}(x_2/x_1)$ (puisque $D_1(x_2) = 0$), ce qui donne une équation d'ordre $n+1$ en y_1 et en y_2 vérifiée par (y_1, y_2) :

$$\frac{D_1(y_2)}{y_2} = (n+1)\frac{D_{n+1}(y_2/y_1)}{D_n(y_2/y_1)}$$

ce qui peut s'écrire, après multiplication par les dénominateurs, sous forme d'équation D-polynomiale :

$$P(y_1, y_2) := (n+1)y_2 y_1^{n+2} D_n + 1\Big(\frac{y_2}{y_1}\Big) - D_1(y_2) y_1^{n+2} D_n\Big(\frac{y_2}{y_1}\Big) = 0.$$

Le terme de P en $d_{n+1}Y_2$ est $(n+1)Y_2 Y_1^{n+1} d_{n+1}Y_2$, et la séparante de P par rapport à Y_2 est $S_{Y_2}(P) = (n+1)Y_2 Y_1^{n+1}$. On va montrer que P constitue une

chaîne minimale de polynômes pour I_{p_n} ; pour cela, il suffit de montrer qu'il n'y a pas de relation algébrique sur K non-triviale entre $(D_i(y_1))_{i\geq 0}$ et $y_2, \ldots, D_n(y_2)$ (puisqu'alors, y_1 est générique sur K et $P(y_1, Y_2)$ est un polynôme minimal de y_2 sur $K(\{y_1\})$).
Soit, pour $r \geq 0$,

$$K_r := K(\{y_1, y_2\}_{\leq r}).$$

Le polynôme P permet d'écrire $D_{n+1}(y_2)$ comme fraction rationnelle en les variables $y_1, \ldots, D_{n+1}(y_1), y_2, \ldots, D_n(y_2)$, et on obtient donc par induction sur $r > n$, en appliquant $D_{r-(n+1)}$ à cette relation, que $D_r(y_2)$ s'écrit comme fraction rationnelle en les variables $y_1, \ldots, D_r(y_1), y_2, \ldots, D_n(y_2)$, et donc :

$$K_r = K(y_1, \ldots, D_r(y_1), y_2, \ldots, D_n(y_2)).$$

Pour montrer que $(D_i(y_1))_{i\geq 0}$ et $y_2, \ldots, D_n(y_2)$ sont algébriquement indépendants sur K, on va montrer que $deg.tr(K_r/K) = (r+1) + (n+1)$ pour tout r assez grand ; l'expression précédente de K_r montre déjà que $deg.tr(K_r/K) \leq (r+1) + (n+1)$.

Soit $r \geq 2n-1$, en appliquant D_i pour tout $i \leq r-n$ à la relation $x_1 = \frac{y_1}{D_n(y_2/y_1)}$, on obtient que $x_1, \ldots, D_{r-n}(x_1)$ sont dans K_r ; d'autre part, $x_2 = \frac{y_2}{D_n(y_2/y_1)}$ est dans K_r. De plus, on a la relation

$$y_2 = x_2 D_n\Big(\frac{x_2}{x_1}\Big) = -\frac{x_2^2}{x_1^2} D_n(x_1) + R_0(x_1, \ldots, D_{n-1}(x_1), x_2)$$

pour une certaine fraction rationnelle R_0, et comme $n-1 \leq r-n$, on vient de voir que $x_2, x_1, \ldots, D_{n-1}(x_1)$ sont dans K_r, donc $D_n(x_1)$ également. En appliquant D_i à la relation précédente pour $i \leq r$, on obtient,

$$D_i(y_2) = -\binom{n+i}{n} \frac{x_2^2}{x_1^2} D_{n+1}(x_1) + R_i(x_1, \ldots, D_{n+i-1}(x_1), x_2)$$

pour une certaine fraction rationnelle R_i, ce qui permet de montrer par récurrence que $D_n(x_1), \ldots, D_{n+r}(x_1)$ sont dans K_r. Ainsi, K_r contient $x_1, \ldots, x_1^{(n+r)}, x_2$, qui sont algébriquement indépendants par définition de p, donc $deg.tr(K_r/K) \geq r+n+2$ dès que $r \geq 2n-1$, et il y a en fait égalité :

$$deg.tr(K_r/K) = r+n+2.$$

On a donc montré que $I_{p_n} = I_{(P)}$, et aussi que

$$RH(p_n) \leq RD(p_n) = \omega + n + 1,$$

et on va trouver une chaîne de D-idéaux premiers qui prouvent que $RH(p_n) \geq \omega + n + 1$.
Pour tout entier $m \geq 0$, on note Q_m le D-polynôme $Q_m = Y_1^{m+1} D_m\Big(\frac{Y_2}{Y_1}\Big)$, et q_m le 2-type sur K défini par $I_{q_m} = I_{(Q_m)}$. Soit $m \geq 1$, on utilise le théorème 2 : puisque $Q_m \in I_{(Q_{m-1})}$ et $S_{Y_2}(Q_m) = Y_1^m \notin I_{(Q_{m-1})}$, $I_{(Q_m)} \subsetneq I_{(Q_{m-1})}$. De même $P \in I_{(Q_n)}$ et $S_{Y_2}(P) = (n+1)Y_2 Y_1^{n+1} \notin I_{(Q_n)}$, donc $I_{(P)} \subsetneq I_{(Q_n)}$, d'où la tour de D-idéaux premiers $I_{p_n} \subsetneq I_{q_n} \subsetneq I_{q_{n-1}} \subsetneq \ldots \subsetneq I_{q_0}$, avec $I_{q_0} = I_{(Y_2)}$ de $RH = \omega$. Donc $RH(p_n) \geq \omega + n + 1$.
Ceci prouve que $RH(p_n) = \omega + n + 1$. $\square$

V.3.2 Un groupe connexe avec deux types de RH maximum

On considère le sous-groupe du groupe additif

$$G := \{\, (x_1, x_2) \mid D_2(x_2) = 0 \,\},$$

et G_1 le sous-groupe de G défini par

$$G_1 := \{\, (x_1, x_2) \mid D_1(x_2) = 0 \,\}.$$

Le groupe G est connexe, et son type générique t (au sens des groupes, mais ici les différents sens coïncident) est défini par $I_t = I_{(d_2 X_2)}$; et G_1 est un groupe connexe de type générique p. Les inégalités de Lascar et le calcul du polynôme de Kolchin donnent

$$RU(t) = RM(t) = RH(t) = RD(t) = \omega + 2.$$

On va construire un groupe définissablement isomorphe à G, avec deux types de RH maximum, en envoyant le type non générique p de G vers un type de $RH = \omega + 2$.

L'ensemble définissable $A := A_1 \cap G_1$ est inclus dans G, son type de RM maximum est le type p. Le groupe G est en bijection définissable avec

$$H := \Phi_1(A) \times \{0\} \cup (G \setminus A) \times \{1\},$$

et on transporte sur H la structure de groupe (connexe) de G.
Or

$$\begin{aligned}\Phi_1(A) &\subset \langle Y_1 \neq 0 \wedge D_1\Big(\frac{Y_2}{Y_1}\Big) \neq 0 \wedge 2Y_2Y_1^3 D_2\Big(\frac{Y_2}{Y_1}\Big) = D_1(Y_2)Y_1^3 D_1\Big(\frac{Y_2}{Y_1}\Big)\rangle \\ &\subset \langle Y_2Y_1^2 \neq 0 \wedge 2Y_2Y_1^3 D_2\Big(\frac{Y_2}{Y_1}\Big) = D_1(Y_2)Y_1^3 D_1\Big(\frac{Y_2}{Y_1}\Big)\rangle \subset \mathcal{V}(I_{p_1}),\end{aligned}$$

et $p_1 = \Phi_1(p)$ est dans $\Phi_1(A)$, donc le type de RH maximum de $\Phi_1(A)$ est p_1, avec $RH(p_1) = \omega + 2$; et celui de $G \setminus A$ est t, avec $RH(t) = \omega + 2$. Donc H est un groupe connexe avec deux types de RH maximum.

Cela permet aussi de voir le phénomène suivant :
soit H_1 le sous-groupe de H image du sous-groupe G_1. Comme H_1 contient p_1, on a $RH(H_1) = RH(H) = \omega + 2$, et pourtant l'indice de H_1 dans H est infini.

V.3.3 Un groupe connexe irréductible avec deux notions différentes de type générique

On considère le fermé irréductible $\mathcal{V}(I_{p_2})$; celui-ci contient le type q_2, d'idéal associé $I_{(Y_1^3 D_2\left(\frac{Y_2}{Y_1}\right))}$. On a vu précédemment que $RU(p_2) = RM(p_2) = \omega + 1$ et $RH(p_2) = \omega + 3$, et les inégalités de Lascar et l'utilisation du rang RD montrent que $RU(q_2) = RM(q_2) = RH(q_2) = RD(q_2) = \omega + 2$, on obtient donc déjà un exemple où les notions de type générique topologique (ici p_2) et de type de RM

maximum, et aussi de RU maximum (ici q_2), d'un fermé irréductible sont totalement disjointes ; ce qui diffère du cas des variétés algébriques irréductibles (c'est-à-dire définies dans le pur langage des corps) pour lesquelles il est montré dans [Pon99] que le type générique au sens topologique est de RU maximum. On ne sait pas si ce phénomène peut exister en rang fini.

On va de plus mettre sur une partie de $\mathcal{V}(I_{p_2})$ contenant à la fois p_2 et q_2 une structure de groupe. Pour cela, on utilise toujours le groupe G, en envoyant le type t, de RM maximum dans G, sur q_2, qui est de RM maximum dans $\mathcal{V}(I_{p_2})$ mais pas de RH maximum, et le type p, non générique dans G, sur p_2, le type générique au sens topologique de $\mathcal{V}(I_{p_2})$.
On définit d'abord une injection Ψ de G dans $\mathcal{V}(I_{q_2})$, qui associe (y_1, y_2) à (x_1, x_2) comme suit :

- si $x_1 \neq 0$ et $D_2(x_2) = 0$, on pose $y_1 = x_1$ et $y_2 = x_1 x_2$, la réciproque étant donnée par $x_2 = y_2/y_1$; alors $(y_1, y_2) \in \langle Y_1 \neq 0 \wedge Y_1^3 D_2\left(\frac{Y_2}{Y_1}\right) = 0\rangle \subset \mathcal{V}(I_{q_2})$, et en particulier que $q_2 = \Psi(t)$,
- si $x_1 = 0$ et $D_2(x_2) = 0$, on pose $y_1 = 0$ et $y_2 = x_2$; et alors $(y_1, y_2) \in \mathcal{V}(I_{q_2})$ car le polynôme minimal de I_{q_2} est $Q_2 = Y_1^2 d_2 Y_2 - Y_1 d_1 Y_1 d_1 Y_2 - Y_1 d_2 Y_1 Y_2 + Y_2 (d_1 Y_1)^2$, de séparante $S_{Y_2}(Q_2) = Y_1^2$ et on remarque donc que
$$I_{(Q_2)} \subset I_{(d_1 Y_1, d_2 Y_2)} \subset I_{(Y_1, d_2 Y_2)},$$
d'où $(y_1, y_2) \in \mathcal{V}(I_{q_2})$.

Le groupe G est en bijection définissable avec
$$F := \Phi_2(G_1 \cap A_2) \cup \Psi(G \setminus (G_1 \cap A_2)),$$
ces deux ensembles étant disjoints puisque $\Phi_2(A_2) = A_2$ et $\Psi(G) \subset \mathcal{V}(I_{q_2})$.
D'autre part, $F \subset \mathcal{V}(I_{p_2})$, et F contient $p_2 = \Phi_2(p)$, donc F est irréductible, de type générique topologique p_2.

On transporte sur F, par bijection définissable, la structure de groupe connexe de G, et alors son type générique au sens des groupes est l'image de celui de G, cette image est $q_2 = \Psi(t)$ puisque $t \notin G_1$.

Donc F est un groupe irréductible et connexe, mais son type générique au sens topologique (p_2) ne coïncide pas avec son type générique au sens des groupes (q_2).

V.3.4 Un groupe irréductible non-connexe

Le groupe F précédent permet immédiatement de construire un groupe irréductible et non-connexe :
soit F_1 l'image du sous-groupe G_1 dans F ; en particulier, $p_2 \in F_1$. Soit a un élément de $F \setminus F_1$, alors $a.F_1$ est toujours inclus dans F donc dans $\mathcal{V}(I_{p_2})$.
On munit
$$F_2 := F_1 \cup a.F_1$$
d'une structure de groupe définissable isomorphe à $F_1 \times \mathbb{Z}/2\mathbb{Z}$ (en tant qu'union de deux copies de F_1) ; l'adhérence de F_2 est $\mathcal{V}(I_{p_2})$. Donc F_2 est un groupe irréductible et non-connexe.

Annexe A

Proposition A.1 *Soit $K \models CHC_p$, et q un type sur K, de rang de transcendance 1. Alors q est très mince.*

Preuve Soit a une réalisation de q. Puisque pour tout D-corps L contenant K, l'extension L/K est régulière, on sait que a est transcendant sur K. On va mener la démonstration dans le cas où q est un 1-type ; on peut toujours se ramener à cette situation en extrayant du uplet a une base de transcendance séparante.
On va montrer par récurrence sur n que $K(a)^{sep}$ est stable par $D_0, \ldots, D_n$. Pour cela, il est (nécessaire et) suffisant de montrer que $D_0(a), \ldots, D_n(a) \in K(a)^{sep}$. En effet, si c'est le cas, on a $D_i(K(a)) \subset K(a)^{sep}$ pour tout $i \leq n$; puis, si $b \in K(a)^{sep}$, et si $f(X)$ désigne son polynôme minimal (séparable) sur $K(a)$, alors on obtient par récurrence sur $i \leq n$ que $D_i(b) \in K(a)^{sep}$ puisque l'on a la relation (fait I.10)

$$0 = D_i(f(b)) = \frac{df}{dX}(b)D_i(b) + g_i,$$

avec $g_i \in K(a)^{sep}[D_0(b), \ldots, D_{i-1}(b)] \subset K(a)^{sep}$ et $\frac{df}{dX}(b) \neq 0$.
On sait aussi que si l'on a l'hypothèse de récurrence pour $n = p^{r-1}$, on l'a pour $p^r - 1$, puisque tout D_i, pour $i \leq p^r - 1$, s'écrit (à un coefficient non nul près) comme composée de $D_0, D_1, D_p, \ldots, D_{p^{r-1}}$.
Il s'agit donc de montrer que $D_{p^r}(a) \in K(a)^{sep}$, sachant que $K(a)^{sep}$ est stable par $D_0, \ldots, D_{p^r-1}$.
Supposons le contraire. Comme $D_{p^r}(a)$ est algébrique sur $K(a)$, on peut choisir n minimal tel que $D_{p^r}(a)^{p^n} \in K(a)^{sep}$, avec $n \geq 1$. On note

$$f(X) := X^d + f_{d-1}(a)X^{d-1} + \ldots + f_0(a)$$

le polynôme minimal séparable unitaire de $D_{p^r}(a)^{p^n}$ sur $K(a)$, où les f_i désignent des fractions rationnelles à coefficients dans K (et $f_d = 1$).
Appliquons D_{p^r} à $f(D_{p^r}(a)^{p^n})$, en utilisant le fait que $D_j(x^{ip^n}) = D_{j/p^n}(x^i)^{p^n}$ si p^n divise j, et 0 sinon. On obtient

$$0 = D_{p^r}(f(D_{p^r}(a)^{p^n})) = \sum_{i=0}^{d} D_{p^r}(f_i(a)D_{p^r}(a)^{ip^n}),$$

avec

$$D_{p^r}(f_i(a)D_{p^r}(a)^{ip^n}) = \sum_{j=0}^{p^{r-n}} D_{p^r-p^nj}(f_i(a))D_j(D_{p^r}(a)^i)^{p^n}. \qquad (*)$$

(si $r < n$, le seul terme est $D_{p^r}(f_i(a))D_{p^r}(a)^{ip^n}$)
Puisque $n \geq 1$, $p^{r-n} < p^r$. On va montrer que l'hypothèse de récurrence implique que $D_j(D_{p^r}(a)^i)$ s'écrit $h(D_{p^r}(a))$, où h est un polynôme à coefficients dans $K(a)^{sep}$ (de degré au plus i). L'expression

$$D_j(x^i) = \sum_{h=0}^{j} D_h(x)D_{j-h}(x^{i-1})$$

montre qu'il suffit d'obtenir le résultat pour $D_j(D_{p^r}(a))$.
D'après l'hypothèse de récurrence, pour $j < p^r$, $D_j(a)$ est algébrique séparable sur $K(a)$, et on considère u le polynôme minimal séparable de $D_j(a)$ sur $K(a)$. Puisque $K(a)^{sep}$ est stable par $D_0, \ldots, D_{p^r-1}$, on obtient

$$D_{p^r}(u(X)) = u^{D_{p^r}}(X) + \frac{du}{dX} d_{p^r} X + v(d_0 X, \ldots, d_{p^r-1} X),$$

où $u^{D_{p^r}}$ est le polynôme obtenu en appliquant D_{p^r} aux coefficients de u et v est un polynôme à coefficients dans $K(a)^{sep}$. D'autre part, on constate que pour une fraction rationnelle $t(X)$ à coefficients dans K,

$$D_{p^r}(t(a)) = \frac{dt}{dX}(a)D_{p^r}(a) + b,$$

avec $b \in K(a)^{sep}$.
On en déduit qu'il existe $\alpha, \beta \in K(a)^{sep}$ tels que

$$0 = D_{p^r}(u(D_j(a))) = \frac{du}{dX}(D_j(a))D_{p^r} \circ D_j(a) + \alpha D_{p^r}(a) + \beta.$$

Puisque $\frac{du}{dX}(D_j(a))$ est un élément non nul de $K(a)^{sep}$, on obtient l'expression voulue pour $D_j \circ D_{p^r}(a)$.
Traitons à part le terme correspondant à $j = 0$ dans l'expression $(*)$; on a le terme $D_{p^r}(f_i(a))D_{p^r}(a)^{ip^n}$, avec $D_{p^r}(f_i(a)) = \frac{df_i}{dX}(a)D_{p^r}(a)+c$, pour un élément c de $K(a)^{sep}$.
En regroupant le tout, on obtient un polynôme g à coefficient dans $K(a)^{sep}$ tel que

$$D_{p^r}(f(D_{p^r}(a)^{p^n})) = g(D_{p^r}(a)^{p^n}) + \sum_{i=0}^{d-1} \frac{df_i}{dX}(a)D_{p^r}(a)^{ip^n+1} = 0.$$

Si on considère cette expression comme un poynôme P à coefficients dans $K(a)^{sep}$, évalué en $D_{p^r}(a)$, on voit que l'on a :

$$\frac{dP}{dX}(D_{p^r}(a)) = \sum_{i=0}^{d-1} \frac{df_i}{dX}(a)D_{p^r}(a)^{ip^n}.$$

Puisque $D_{p^r}(a)$ n'est pas par hypothèse séparable sur $K(a)$, cette dernière expression doit s'annuler. Mais on obtient alors un polynôme de degré strictement inférieur à d, à coefficients dans $K(a)$, et qui s'annule en $D_{p^r}(a)^{p^n}$. D'après la minimalité du polynôme f, cela impose que $\frac{df_i}{dX}(a) = 0$ pour tout i. Puisque a est transcendant sur K, c'est donc que $\frac{df_i}{dX} = 0$, et donc $f_i(X) = g_i(X^p)$ pour

une certaine fraction rationnelle g_i à coefficients dans K.
On applique maintenant D_1 à l'expression $f(D_{p^r}(a)^{p^n}) = 0$:

$$\sum_{i=0}^{d-1} D_1(g_i(a^p))D_{p^r}(a)^{ip^n} = 0.$$

Puisque $D_1(g_i(a^p)) \in K(a)$ et que f est le polynôme minimal de $D_{p^r}(a)^{p^n}$ sur $K(a)$, on doit avoir $D_1(g_i(a^p)) = 0$ pour tout i. Or, si on écrit $g_i(X) = \frac{P_i(X)}{Q_i(X)}$, pour P_i et Q_i des polynômes premiers entre eux, et avec P_i unitaire, on a

$$D_1\Big(\frac{P_i(a^p)}{Q_i(a^p)}\Big) = \frac{P_i^{D_1}(a^p)Q_i(a^p) - P_i(a^p)Q_i^{D_1}(a^p)}{Q_i(a^p)^2} = 0,$$

et comme a^p est transcendant sur K, on a $P_i^{D_1}Q_i - P_iQ_i^{D_1} = 0$. Or, comme P_i est unitaire, le degré de $P_i^{D_1}$ est strictement inférieur à celui de P_i ; et l'irréducibilité de l'écriture $\frac{P_i}{Q_i}$ donne donc $P_i^{D_1} = Q_i^{D_1} = 0$. Comme K est strict, P_i et Q_i ont donc leurs coefficients dans K^p, et il existe donc une fraction rationnelle h_i, à coefficients dans K, telle que $g_i(a^p) = (h_i(a))^p$.
Mais on obtient alors, en prenant la racine p-ième de l'expression $f(D_{p^r}(a)^{p^n}) = 0$:

$$D_{p^r}(a)^{dp^{n-1}} + h_{d-1}(a)D_{p^r}(a)^{(d-1)p^{n-1}} + \ldots + h_0(a)D_{p^r}(a)^{p^{n-1}} = 0.$$

Donc $D_{p^r}(a)^{p^{n-1}}$ est racine d'un certain polynôme $\tilde{f}$ à coefficients dans $K(a)$; c'en est une racine simple car

$$\frac{d\tilde{f}}{dX}(D_{p^r}(a)^{p^{n-1}}) = \Big(\frac{df}{dX}(D_{p^r}(a)^{p^n})\Big)^{1/p} \neq 0.$$

Ainsi $D_{p^r}(a)^{p^{n-1}}$ est séparable sur $K(a)$, ce qui contredit la minimalité de n. $\square$

Annexe B

Soit G un groupe algébrique connexe défini sur un corps k de caractéristique p ; on notera $\mathcal{O}_{G,e}$ l'anneau local des fonctions définies au voisinage de l'unité e et $\mathcal{M}$ son idéal maximal.

Lemme B.1 *Soit q une puissance de p, et f un élément de $\mathcal{M}$. Alors $f \circ [q] \in \mathcal{M}^q$.*

Preuve On se donne un sytème de coordonnées locales $x_1, \ldots, x_d$ au voisinage de e ; en particulier, les $x_1, \ldots, x_d$ engendrent l'idéal $\mathcal{M}$ dans $\mathcal{O}_{G,e}$, et forment même une base du k-espace vectoriel $\mathcal{M}/\mathcal{M}^2$. Il suffira donc de montrer le lemme pour ces fonctions $x_1, \ldots, x_d$.
Puisque la loi $*$ de G est un morphisme de $G \times G$ dans G, il existe un ouvert V de $G \times G$ contenant (e, e) et une fonction rationnelle g telle que $x * y = g(x, y)$ pour tout (x, y) dans V. Pour tout i entre 1 et d, on peut décomposer la i-ème coordonnée de g selon les puissances de l'idéal maximal M de $\mathcal{O}_{G\times G,(e,e)}$:

$$(x * y)_i = g_i(x, y) = x_i + y_i + \sum_{n=2}^{q-1} g_i^{(n)}(x, y) \mod M^q,$$

avec $g_i^{(n)} \in M^n/M^{n+1}$, vu comme le k-espace vectoriel des polynômes homogènes de degré n en les variables $x_1, \ldots, x_d, y_1, \ldots, y_d$ (ces fonctions forment en effet un système de coordonnées locales au voisinage de (e, e) dans $G \times G$).
En regroupant correctement les différents termes, on peut écrire :

$$g_i^{(n)} = \sum_{m=1}^{n-1} g_i^{(n,m)}(\underbrace{x, \ldots, x}_{m\,termes}, \underbrace{y, \ldots, y}_{n-m\,termes}),$$

où les $g_i^{(n,m)}$ sont des fonctions n-linéaires et x, y représentent abusivement les vecteurs $x_1, \ldots, x_d$ et $y_1, \ldots, y_d$. Dans cette écriture, il n'apparaît pas de termes de la forme $g_i^{(n,n)}(x, \ldots, x)$ ou $g_i^{(n,0)}(y, \ldots, y)$ car on a $(x * e)_i = x_i$ et $(e * y)_i = y_i$.
On obtient finalement, pour $(x, y) \in V$, l'écriture (en tant que d-uplet) :

$$(x * y) = x + y + \sum_{n=2}^{q-1} \sum_{m=1}^{n-1} g^{(n,m)}(x, \ldots, x, y, \ldots, y) \mod M^q.$$

Ensuite, l'ensemble $U = \bigcap_{l=1}^{q-1} \{ x \in G \mid ([l]x, x) \in V \}$ est un ouvert contenant e, c'est donc un ouvert dense ; et pour tout $x \in U$, et l entre 1 et $q-1$, on pourra donc utiliser la fonction g pour calculer :

$$([l+1]x) = ([l]x * x) = g([l]x, x).$$

Considérons la décomposition du d-uplet :

$$[l]x = \sum_{n=1}^{q-1} ([l]x)^{(n)} \mod \mathcal{M}^q,$$

où $([l]x)^{(n)}$ est un élément de $\mathcal{M}^n/\mathcal{M}^{n+1}$ qui s'écrit comme polynôme homogène de degré n en les variables $x_1, \ldots, x_d$. Pour $n = 1$, on voit aisément que l'on a $([l]x)^{(1)} = lx$; et pour $l = 1$, on a $(x)^{(1)} = x$ et $(x)^{(n)} = 0$ pour $n > 1$.
Ensuite, l'expression de g permet de calculer par récurrence sur l et n tous les termes $([l]x)^{(n)}$; on a en effet, pour $n > 1$, la relation :

$$([l+1]x)^{(n)} = ([l]x)^{(n)} + \sum_{m=2}^{n} \sum_{j=1}^{m-1} \sum_{\substack{\alpha_1,\ldots,\alpha_j \geq 1 \\ \alpha_1+\ldots+\alpha_j = n-m+j}} g^{(m,j)}(([l]x)^{(\alpha_1)}, \ldots, ([l]x)^{(\alpha_j)}, \underbrace{x, \ldots, x}_{m-j\ termes})$$

Appelons *termes* les fonctions obtenues en composant les différents d-uplets de fonctions $g^{(n,m)}$ (en respectant l'arité des fonctions), et $T^{(n)}$ l'ensemble des *termes de degré* n, c'est-à-dire les termes qui apparaissent dans l'écriture des différents $([l]x)^{(n)}$ pour l entre 1 et q.
On a alors :

$$T^{(1)} = \{id\}$$

et la relation de récurrence suivante pour $n \geq 2$:

$$T^{(n)} = \left\{ g^{(m,j)}(t_1, \ldots, t_j, id, \ldots, id) \;\middle|\; \begin{smallmatrix} 2 \leq m \leq n; 1 \leq j \leq m-1; \alpha_1, \ldots, \alpha_j \geq 1 \\ \alpha_1 + \ldots + \alpha_j = n-m+j; t_h \in T^{(\alpha_h)} \end{smallmatrix} \right\}.$$

Si t est élément de $T^{(n)}$, il apparaît dans $([l]x)^{(n)}$ avec un coefficient $f_t(l)$. Pour montrer que le d-uplet $([q]x)$ est dans $\mathcal{M}^q$, il suffit donc de montrer que, pour tous les termes t de degré n, avec $1 \leq n \leq q-1$, p divise $f_t(q)$.
Pour calculer ces fonctions $f_t(l)$, procédons par récurrence sur le degré du terme t. Si t est un terme de degré 1, on a $t = id$ et $f_t(l) = l$. Ensuite, si $t = g^{(m,j)}(t_1, \ldots, t_j, id, \ldots, id)$ est un élément de $T^{(n)}$, avec $t_h \in T^{(\alpha_h)}$, on a, par une récurrence simple à partir de l'expression de $([l+1]x)^{(n)}$:

$$f_t(l) = \sum_{i=1}^{l-1} f_{t_1}(i) \ldots f_{t_j}(i).$$

Plus généralement, associons à tout arbre fini T une fonction de $\mathbb{N}$ dans $\mathbb{N}$ de la façon suivante :

- si T est un feuille, $f_T(l) = l$
- si T est un arbre avec j embranchements à la racine, avec pour sous-arbres correspondants $T_1, \ldots, T_j$, $f_T(l) = \sum_{i=1}^{l-1} f_{T_1}(i) \ldots f_{T_j}(i)$.

Pour tout arbre fini T, il existe un terme t, qui est nécessairement de degré au moins $n(T)$, tel que les fonctions f_t et f_T coïncident :

- si T est une feuille, le seul terme possible est $t = id$, qui est de degré $n(T) = 1$
- si T est un arbre dont les sous-arbres à la racins sont $T_1, \ldots, T_j$, les termes t possibles sont ceux de la forme $g^{(m,j)}(t_1, \ldots, t_j, id, \ldots, id)$, où les termes t_h correspondent aux arbres T_h. Le degré d'un tel terme vérifie la relation $deg(t) = deg(t_1) + \ldots + deg(t_j) + m - j$, avec la condition $j \leq m - 1$, le degré minimal possible pour t est donc $n(T) = n(T_1) + \ldots + n(T_j) + 1$; cela montre par récurrence que $n(T)$ est le nombre de noeuds de T.

On est donc ramené à montrer un résultat de type combinatoire : si $q > n(T)$, alors p divise $f_T(q)$.
On considère la famille de fonctions P_n pour $n \geq 0$ définies par $P_n(l) = \binom{l}{n}$ quand $l \geq n$ et $P_n(l) = 0$ pour $0 \leq l < n$; et on va montrer par induction sur l'arbre T que f_T est une combinaison linéaires, à coefficients entiers, des fonctions $P_1, \ldots, P_{n(T)}$, ce qui donnera le résultat puisque si q est une puissance de p telle que $1 \leq n < q$, p divise $\binom{q}{n}$.
Si T est une feuille, on a $f_T(l) = l$, c'est-à-dire $f_T = P_1$.
Si T est l'arbre dont les sous-arbres à la racine sont $T_1, \ldots, T_j$, on sait que $f_T(l) = \sum_{i=1}^{l-1} f_{T_1}(i) \ldots f_{T_j}(i)$. Par hypothèse d'induction, chaque f_{T_h} est une combinaison linéaire à coefficients entiers des fonctions $P_1, \ldots, P_{n(T_h)}$. Remarquons qu'on a la relation $P_{n+1}(l) = \sum_{i=1}^{l-1} P_n(i)$. Montrons que pour deux entiers r et s, $P_r P_s$ est une combinaison linéaire à coefficients entiers de $P_{r+s}, \ldots, P_0$ (P_0 n'apparaît que si r et s sont nuls), par récurrence sur $r + s$:

- si $r = 0$ ou $s = 0$, c'est évident puisque $P_0 = 1$
- sinon, on écrit, pour tout l :

$$P_r(l)P_s(l) = \sum_{0 \leq i,j \leq l-1} P_{r-1}(i)P_{s-1}(j)$$

$$= \sum_{i=0}^{l-1} \sum_{j=0}^{i-1} P_{r-1}(i)P_{s-1}(j) + \sum_{i=0}^{l-1} P_{r-1}(i)P_{s-1}(i) + \sum_{j=0}^{l-1} \sum_{i=0}^{j-1} P_{r-1}(i)P_{s-1}(j)$$

$$= \sum_{i=0}^{l-1} \big(P_{r-1}(i)P_s(i) + P_{r-1}(i)P_{s-1}(i) + P_r(i)P_{s-1}(i) \big).$$

D'après l'hypothèse de récurrence, il y a à l'intérieur de la parenthèse une combinaison linéaire à coefficients entiers de $P_{r+s-1}, \ldots, P_0$, évaluée en i ; ce qui donne en sommant pour i de 0 à $l - 1$ une combinaison linéaire à coefficients entiers de $P_{r+s}, \ldots, P_1$.

Ainsi on obtient que $f_T(l)$ est la somme pour i de 0 à $l - 1$ des évaluations en i d'une combinaison linéaire à coefficients entiers de $P_{n(T_1)+\ldots+n(T_j)}, \ldots, P_1$; et ainsi f_T est une combinaison linéaire à coefficients entiers de $P_{n(T)}, \ldots, P_1$, ce qui termine la démonstration. $\square$

Bibliographie

[Ben02] Franck Benoist. Rangs et types de rang maximum dans les corps différentiellement clos. *Journal of Symbolic Logic 67, 1178-1188*, 2002.

[BerLas86] Chantal Berline and Daniel Lascar. Superstable groups. *Annals of Pure and Applied Logic 30, 1-43*,1986.

[Blo01] Thomas Blossier. *Ensembles minimaux localement modulaires.* Thèse, Paris, 2001.

[Blo04] Thomas Blossier. Subgroups of the additive group of a separably closed field. *A paraître dans Annals of Pure and Applied Logic*, 2004.

[BloKru04] Thomas Blossier and Krzysztof Krupiński. A special thin type. *A paraître dans Illinois Journal of Mathematics*, 2004.

[BouDel01] Elisabeth Bouscaren and Françoise Delon. Groups definable in separably closed fields. *Transactions of the American Mathematical Society 354, 945-966*, 2001.

[BouDel02] Elisabeth Bouscaren and Françoise Delon. Minimal groups in separably closed fields. *Journal of Symbolic Logic, 67, 239-259*, 2002.

[Bui92] Alexandru Buium. *Algebraic differential groups of finite dimension.* Lecture Notes in Mathematics 1506, Springer, Berlin, 1992.

[Del88] Françoise Delon. *Idéaux et types sur les corps séparablement clos.* Supplément au bulletin de la Société Mathématique de France, Tome 116, Mémoire 33, 1988.

[Del98] Françoise Delon. *Separably closed fields.* Model theory and algebraic geometry : An introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture, Bouscaren (editor), Lecture Notes in Mathematics, Springer, Berlin, 1998.

[Del02] Françoise Delon. Le foncteur lambda des corps de degré d'imperfection fini et non nul, versus "Prolongations". *Notes*, 2002.

[Har77] Robin Hartshorne. *Algebraic geometry.* Springer-Verlag, 1977.

[HasSch37] Helmut Hasse and F.K. Schmidt. Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionkörper mit einer Unbestimmten. *Journal für die reine und angewandte Mathematik 177, 215-237*, 1937.

[Hin98] Marc Hindry. *Introduction to abelian varieties and the Mordell-Lang conjecture.* Model theory and algebraic geometry : An introduction to E. Hrushovski's proof of the geometric Mordell-Lang

conjecture, Bouscaren (editor), Lecture Notes in Mathematics, Springer, Berlin, 1998.

[Hru96] Ehud Hrushovski. The Mordell-Lang conjecture for function fields. *Journal of the American Mathematical Society 9, 667-690*, 1996.

[HruSca99] Ehud Hrushovski and Thomas Scanlon. Lascar and Morley ranks differ in differentially closed fields. *Journal of Symbolic Logic 64, 1280-1284*, 1999.

[HruZil96] Ehud Hrushovski and Boris Zil'ber. Zariski geometries. *Journal of the American Mathematical Society 9, 1-56*, 1996.

[Hus87] Dale Husemöller. *Elliptic curves.* Springer-Verlag, 1987.

[Joh69] Joseph Johnson. Differential dimension polynomials and a fundamental theorem on differential modules. *American Journal of Mathematics 91, 239-248*, 1969.

[Kow05] Piotr Kowalski. Geometric axioms for existentially closed Hasse fields. *A paraître dans Annals of Pure and Applied Logic*, 2005.

[KowPil03] Piotr Kowalski and Anand Pillay. Quantifier elimination for algebraic D-groups. *A paraître dans Transactions of the American Mathematical Society*, 2003.

[Lan58] Serge Lang. *Introduction to algebraic geometry.* Interscience Publishers, New York, 1958.

[Lan59] Serge Lang. *Abelian varieties.* Interscience Publishers, New York, 1959.

[Las85] Daniel Lascar. Les groupes ω-stables de rang fini. *Transactions of the American Mathematical Society 292, 451-462*, 1985.

[Man66] Yuri Manin. Rational points of algebraic curves over function fields. *Translations of the American Mathematical Society 59*, 1966.

[Mar96] David Marker. *Model Theory of Differential Fields.* Model Theory of Fields, Lecture Notes in Logic 5, Springer, Berlin, 1996.

[Mar98] David Marker. *Zariski geometries.* Model theory and algebraic geometry : An introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture, Bouscaren (editor), Lecture Notes in Mathematics, Springer, Berlin, 1998.

[Mar00] David Marker. *Manin kernels.* Connections between model theory and algebraic and analytic geometry, Macintyre (editor), Quaderni di Matematica 6, Seconda Università di Napoli, 2000.

[MazMe74] Barry Mazur and William Messing. *Universal Extensions and One Dimensional Crystalline Cohomology.* Lecture Notes in Mathematics 370, Springer, 1974.

[Mes94] Margit Messmer. Groups and fields interpretable in separably closed fields. *Transactions of the American Mathematical Society 344, 361-377*, 1994.

[MesWoo95] Margit Messmer and Carol Wood. Separably closed fields with higher derivations. *Journal of Symbolic Logic 60, 898-910*, 1995.

[MumFog82] David Mumford and John Fogarty. *Geometric Invariant Theory.* second enlarged edition, Springer-Verlag, Berlin Heidelberg, 1982.

[Oes84] Joseph Oesterlé. Nombres de Tamagawa et groupes unipotents en caractéristique p. *Inventiones mathematicae 78, 13-88*, 1984.

[Oku63] Kôtaro Okugawa. Basic properties of differential fields of arbitrary characteristic and the Picard-Vessiot theory. *Journal of Mathematics of Kyoto University 2, 294-322*, 1963.

[PiePil98] David Pierce and Anand Pillay. A note on the axioms of differentially closed fields of characteristic zero. *Journal of Algebra 204, 108-115*, 1998.

[Pil83] Anand Pillay. *An introduction to stability theory.* Oxford University Press, 1983.

[Pil96a] Anand Pillay. Differential algebraic groups and the number of countable differentially closed fields. *Model Theory of Fields, Lecture Notes in Logic 5, Springer, Berlin*, 1996.

[Pil96b] Anand Pillay. *Geometric Stability Theory.* Oxford University Press, 1996.

[Pil97] Anand Pillay. Some foundational questions concerning differential algebraic groups. *Pacific Journal of Mathematics 179, 179-200*, 1997.

[Pil98] Anand Pillay. *Algebraically closed fields.* Model theory and algebraic geometry : An introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture, Bouscaren (editor), Lecture Notes in Mathematics, Springer, Berlin, 1998.

[Pil04] Anand Pillay. Mordell-Lang for function fields in characteristic zero, revisited. *Compositio Mathematica 140, 64-68*, 2004.

[PilPon02] Anand Pillay and Wai Yan Pong. On Lascar rank and Morley rank of definable groups in the theory of differentially closed fields. *Journal of Symbolic Logic 67, 1189-1196*, 2002.

[PilZie03] Anand Pillay and Martin Ziegler. Jet spaces of varieties over differential and difference fields. *Selecta Mathematica, New Series, 9, 579-599*, 2003.

[Poi78] Bruno Poizat. Rangs des types dans les corps différentiels. *Théories stables. 1ère année. 1977/78. Publication de l'Institut Henri Poincaré, Paris*, 1978.

[Poi87a] Bruno Poizat. *Cours de théorie des modèles.* Nur al-Mantiq wal-Ma'rifah, 1987.

[Poi87b] Bruno Poizat. *Groupes stables.* Nur al-Mantiq wal-Ma'rifah, 1987.

[Pon99] Wai Yan Pong. *Ordinal dimensions and differential completeness.* Thèse, Chicago, 1999.

[Pon00] Wai Yan Pong. Some applications of ordinal dimensions to the theory of differentially closed fields. *Journal of Symbolic Logic 65, 347-356*, 2000.

[Rit50] Joseph Fels Ritt. *Differential algebra.* AMS, New York, 1950.

[Ros56] Maxwell Rosenlicht. Some basic theorems on algebraic groups. *American Journal of Mathematics 78, 401-443*, 1956.

[Ros58] Maxwell Rosenlicht. Extensions of vector groups by abelian varieties. *American Journal of Mathematics 80, 685-714*, 1958.

[Ser59] Jean-Pierre Serre. *Groupes algébriques et corps de classes.* Hermann, Paris, 1959.

[Spr98] Tonny Albert Springer. *Linear algebraic groups.* Birkhäuser, Boston, 1998.

[Wei55] André Weil. On algebraic groups of transformations. *American Journal of Mathematics 77, 355-391*, 1955.

[Wit37] Ernst Witt. Zyklische Körper und Algebren der Charakteristik p vom Grade p^n. *Journal für die reine und angewandte Mathematik 176, 126-140*, 1937.

[Woo79] Carol Wood. Notes on the stability of separably closed fields. *Journal of Symbolic Logic 44, 412-416*, 1979.

[Zie03a] Martin Ziegler. Canonical-p-bases. *Manuscrit*, 2003.

[Zie03b] Martin Ziegler. Separably closed fields with Hasse derivations. *Journal of Symbolic Logic 68, 311-318*, 2003.