



HAL
open science

Questions de corps de définition pour les variétés abéliennes en caractéristique positive

Franck Benoist, Françoise Delon

► **To cite this version:**

Franck Benoist, Françoise Delon. Questions de corps de définition pour les variétés abéliennes en caractéristique positive. 2007. hal-00137362v1

HAL Id: hal-00137362

<https://hal.science/hal-00137362v1>

Preprint submitted on 19 Mar 2007 (v1), last revised 8 Jan 2008 (v2)

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.

Questions de corps de définition pour les variétés abéliennes en caractéristique positive

Franck Benoist Françoise Delon

14 février 2007

Résumé

Dichotomies in various conjectures from algebraic geometry are in fact occurrences of the dichotomy among Zariski structures. This is what Hrushovski showed and which enabled him to solve, positively, the geometric Mordell Lang conjecture in positive characteristic. Are we able now to avoid this use of Zariski structures ? Pillay and Ziegler have given a direct proof that works for abelian varieties they called “very thin”, which include the ordinary abelian varieties. But it does not apply in all generality : We describe here an abelian variety which is not very thin. More generally, we consider from a model-theoretical point of view several questions about the fields of definition of semi-abelian varieties.

Résumé

La dichotomie apparaissant dans plusieurs conjectures géométriques est une occurrence de la dichotomie des structures de Zariski, introduites par Hrushovski et Zilber en théorie des modèles. C'est ce qu'a compris Hrushovski et qui lui a permis de résoudre, par l'affirmative, la conjecture géométrique de Mordell-Lang en caractéristique positive. Ce recours aux structures de Zariski peut-il être évité ? Pillay et Ziegler ont donné une preuve directe qui s'applique aux variétés semi-abéliennes qu'ils appellent « très minces », en particulier aux variétés ordinaires. Mais elle ne s'applique pas en toute généralité : il y a des variétés qui ne sont pas très minces, nous en donnons ici un exemple. Le présent article traite plus généralement de questions de corps de définition des variétés abéliennes en caractéristique positive, dont les questions de descente, considérées sous l'angle de la théorie des modèles.

1 Introduction

Dans [Hr96], Hrushovski a donné une démonstration d'une conjecture de géométrie algébrique, dite conjecture de Mordell-Lang. On peut donner plusieurs énoncés de ce résultat (voir [Bo98] par exemple) ; en voici un énoncé très général en caractéristique positive :

Théorème 1 (Hrushovski) *Soit K une extension d'un corps algébriquement clos k de caractéristique p ; A une variété semi-abélienne, et X une sous-variété algébrique de A , toutes deux définies sur K ; Γ un sous-groupe de $A(K)$ de p -rang fini, c'est-à-dire tel que $\Gamma \otimes \mathbb{Z}_{(p)}$ soit finiment engendré en tant que $\mathbb{Z}_{(p)}$ -module.*

On suppose que $\Gamma \cap X(K)$ est Zariski-dense dans X , que le stabilisateur de X est réduit à l'unité et que la sous-variété semi-abélienne engendrée par X est A . Alors il existe une variété semi-abélienne B et une sous-variété algébrique Y de B , définies sur k , et une isogénie de B dans A qui envoie Y sur un translaté de X .

En voici un énoncé un peu différent où une certaine dichotomie apparaît plus clairement :

Théorème 2 Soit k et K comme précédemment, A une variété abélienne et X une sous-variété de A définies sur K , et Γ un sous-groupe de $A(K)$ de p -rang fini. Alors, ou bien il existe une image non nulle de A qui soit définie sur k , ou bien il existe un nombre fini de sous-variétés abéliennes B_i de A telles que $X(K) \cap \Gamma$ soit union finie de translatés de $B_i(K) \cap \Gamma$.

La preuve de Hrushovski utilise de façon centrale les géométries de Zariski et leur dichotomie « modularité locale/définition d'un corps » (voir [HrZi96]). Un de nos buts est d'aborder ces questions de descente pour une extension de corps K/k par des moyens beaucoup plus légers de théorie des modèles des corps différentiels.

L'extension de corps K/k est étudiée au moyen d'un langage dans lequel k est infiniment définissable, et où l'on pourra réduire l'énoncé pour le groupe Γ au même énoncé pour le groupe infiniment définissable $p^\infty A(K) := \bigcap_{n \geq 0} p^n A(K)$ (auquel on s'intéressera dans la suite). La théorie utilisée dans la preuve de Hrushovski est celle des corps séparablement clos de degré d'imperfection fini et non nul, dans le langage décrit dans [De98]. Nous adopterons ici principalement le langage d'une dérivation de Hasse, introduit sous cette forme par Ziegler dans [Zi03].

La partie 2 sera consacrée aux préliminaires sur les dérivations de Hasse et sur les corps séparablement clos. Dans la partie 3, nous donnerons une description du sous-groupe $p^\infty A(K)$ qui utilise les prolongations de la variété semi-abélienne A , pour lesquelles on montrera un résultat d'isomorphisme avec les restrictions de Weil pour les extensions de corps K/K^{p^n} . On s'intéressera ensuite aux propriétés de *minceur* de $p^\infty A(K)$, que l'on peut voir comme des notions plus ou moins fortes de dimension finie, dans un contexte où chaque point vient avec la suite infinie de ses dérivées itérées. Dans la partie 4, on montre qu'une variété abélienne A est isogène à une variété abélienne définie sur $K^{p^\infty} := \bigcap_{n \geq 0} K^{p^n}$ si et seulement si $p^\infty A(K)$ est *rationnellement mince*. Dans la partie 5, on répond par la négative à la question de savoir si, pour toute variété abélienne simple A , $p^\infty A(K)$ est *séparablement mince*; une telle propriété aurait fourni une preuve « directe », c'est-à-dire algébrique, de la conjecture de Mordell-Lang, d'après des résultats de Pillay et Ziegler dans [PiZi03]. La construction de ce contre-exemple utilise la description détaillée que Frans Oort a faite de la stratification des espaces de modules des variétés principalement polarisées. Un exemple de même nature a été construit dans le groupe additif, voir [BKr05].

Que François Mestre, Richard Pink, et surtout Frans Oort, soient ici remerciés de nous avoir aidés à comprendre certaines subtilités des variétés abéliennes.

2 Préliminaires

Définition 1 Une dérivation de Hasse sur un anneau A (commutatif avec unité) est une suite d'applications $(D_i)_{i \in \mathbb{N}}$ additives de A dans A , qui vérifient :

- $D_0 = id$
- une règle de Leibniz généralisée : $D_i(xy) = \sum_{m+n=i} D_m(x)D_n(y)$
- une règle d'itération : $D_i \circ D_j = \binom{i+j}{i} D_{i+j}$

On s'intéressera désormais aux corps de caractéristique $p > 0$ munis d'une dérivation de Hasse, dans le langage du premier ordre $\mathcal{L} := (0, 1, +, -, \cdot, (D_i)_{i \in \mathbb{N}})$; leur théorie sera notée HF_p .

Donnons quelques notions utiles dans un tel corps K .

- L'ensemble

$$C_K := \{x \in K; D_1(x) = 0\}$$

est un sous-corps définissable de K , appelé *corps des constantes de K* .

- L'ensemble

$$C_K^\infty := \{x \in K; \forall i \geq 1, D_i(x) = 0\}$$

est un sous-corps infiniment définissable de K , appelé *corps des constantes absolues de K* .

- Le sous-corps des puissances p -ièmes dans K , noté K^p , est toujours contenu dans C_K . On dira que K est *strict* si $C_K = K^p$. Dans ce cas, on aura aussi

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

$$\text{et } C_K^\infty = \bigcap_{n \geq 0} K^{p^n} =: K^{p^\infty}.$$

- Pour $X = (X_1, \dots, X_m)$ un m -uplet de variables, on note $K\{X\}$ l'*algèbre des D -polynômes en X* , c'est-à-dire :

$$K\{X\} := K[d_i X]_{i \in \mathbb{N}},$$

où $d_i X := (d_i X_1, \dots, d_i X_m)$ et où les $d_i X_j$, pour $i \in \mathbb{N}$ et $j = 1, \dots, m$, sont des indéterminés indépendantes. On la munit d'une extension de la dérivation de Hasse sur K en posant

$$D_j(d_i X) = \binom{i+j}{i} d_{i+j} X.$$

La théorie que l'on utilisera a été exhibée par Ziegler (et précédemment par Messmer et Wood, dans un langage un peu différent, voir [MeWo95]) :

Théorème 3 ([Zi03]) La classe des corps de caractéristique p , munis d'une dérivation de Hasse et existentiellement clos, est axiomatisable par une théorie notée CHF_p .

Une liste d'axiomes est donnée par :

- les axiomes HF_p pour un corps commutatif de caractéristique p muni d'une dérivation de Hasse
- un axiome exprimant que la dérivation de Hasse est non triviale (c'est-à-dire $\exists x D_1(x) \neq 0$)

- un axiome exprimant que le corps est strict : $\forall x \exists y (D_1(x) = 0 \rightarrow x = y^p)$
- un schéma d'axiomes exprimant que le corps est séparablement clos.

La théorie CHF_p est complète et admet l'élimination des quantificateurs; par conséquent, pour un ensemble de paramètres $k \models HF_p$, il y a une bijection entre l'ensemble des n -types sur k et les D -idéaux premiers de $k\{X\}$, donnée par :

$$tp(a/k) \mapsto \{P \in k\{X\}; P(a) = 0\}.$$

Exemples

1. Considérons $\mathbb{F}_p(t)$, que l'on munit d'une dérivation de Hasse en posant $D_1(t) = 1$, $D_i(t) = 0$ pour $i > 1$ (et d'autre part la dérivation de Hasse est nécessairement triviale sur \mathbb{F}_p). Cette dérivation de Hasse s'étend de manière unique à la clôture séparable $\mathbb{F}_p(t)^{sep}$ (voir [HaSc37]). Montrons que $K := (\mathbb{F}_p(t)^{sep}, D)$ est un modèle de CHF_p , avec $C_K^\infty = \mathbb{F}_p^{alg}$.

Assertion K est strict.

Preuve Plus généralement, si C est un corps parfait (et donc muni de la dérivation de Hasse triviale), nous allons montrer que $C(t)$ est strict (pour la dérivation précédemment définie sur t). Supposons que

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

pour des polynômes $f(t)$ et $g(t)$ de $C[t]$ premiers entre eux, avec $f(t)$ unitaire. Puisque le cas où $\frac{f(t)}{g(t)} = \frac{D_1(f(t))}{D_1(g(t))}$ est exclu par minimalité du choix de f et g (car le degré de $D_1(f(t))$ est inférieur à celui de $f(t)$), on a $D_1(f(t)) = D_1(g(t)) = 0$, et on est donc ramené à montrer que $C[t]$ est strict. Or, si $h(t) = \sum_i a_i t^i$ est annulé par D_1 , on obtient que pour tout i , $ia_i = 0$, et donc $h(t) \in C[t^p] = (C[t])^p$ puisque C est parfait. Puis, pour passer de $C(t)$ à $C(t)^{sep}$, considérons $x \in C(t)^{sep}$, de polynôme minimal séparable unitaire $f(X) = \sum_{i=0}^d a_i X^i$ sur $C(t)$, tel que $D_1(x) = 0$. Alors en écrivant

$$D_1(f(x)) = \sum_{i=0}^{d-1} D_1(a_i) x^i = 0,$$

on doit avoir d'après la minimalité de f que $D_1(a_i) = 0$ pour tout i , et donc qu'il existe $b_i \in C(t)$ tel que $a_i = b_i^p$. Considérons le polynôme $g(X) = X^d + b_{d-1}X^{d-1} + \dots + b_0$; c'est encore un polynôme séparable (car en élevant à la puissance p une éventuelle racine commune à g et à dg/dX , on obtient une racine commune pour f et df/dX). Or, si $y \in C(t)^{alg}$ est tel que y^p est solution de f , alors y est solution de g , et donc dans $C(t)^{sep}$: x a donc une racine p -ième dans $C(t)^{sep}$. \square

Puisque K est strict, on obtient aussi que $C_K^\infty = K^{p^\infty} = \mathbb{F}_p^{alg}$.

2. Pour un corps algébriquement clos k , il existe une extension K de $k(t_1, \dots, t_n)^{sep}$ et une dérivation de Hasse sur K telles que $C_K^\infty = k$.

Preuve L'exemple précédent permet de construire une dérivation de Hasse sur $k(t_1)^{sep}$, de corps de constantes absolues k . Puis, en ajoutant (t_2, \dots, t_n) une réalisation du $(n-1)$ -type générique au-dessus de $k(t_1)^{sep}$ (ce type

correspondant à l'idéal nul de $k(t_1)^{sep}\{T_2, \dots, T_n\}$, on construit un modèle de CHF_p qui contient $k(t_1, \dots, t_n)$ et dont le corps des constantes absolues reste inchangé égal à k (car le type générique est orthogonal aux constantes absolues, voir la proposition 50 de [De88] pour une preuve dans un langage différent, exposé ci-dessous). \square

Le langage des p -composantes

Après avoir remarqué (lemme 2.1 de [Zi03]) qu'un modèle de CHF_p est un corps séparablement clos de degré d'imperfection 1, on utilisera parfois le langage donné dans [De98] :

pour $K \models CHF_p$, on fixe une p -base $\{b\}$ de K . Par définition, pour tout n , $\{1, b, \dots, b^{p^n-1}\}$ est une base de K en tant que K^{p^n} -espace vectoriel. On notera $\lambda_n = (\lambda_{n,i})_{0 \leq i < p^n}$ les fonctions de K dans K , définissables dans le pur langage des corps avec paramètre b , telles que tout $x \in K$ s'écrive

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

Il suit du fait que les applications D_i sont nulles sur K^{p^n} pour $0 < i < p^n$ que

$$\begin{pmatrix} D_0(x) \\ D_1(x) \\ \vdots \\ D_{p^n-1}(x) \end{pmatrix} = \begin{pmatrix} D_0(1) & D_0(b) & \dots & D_0(b^{p^n-1}) \\ D_1(1) & D_1(b) & \dots & D_1(b^{p^n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ D_{p^n-1}(1) & D_{p^n-1}(b) & \dots & D_{p^n-1}(b^{p^n-1}) \end{pmatrix} \begin{pmatrix} \lambda_{n,0}(x)^{p^n} \\ \lambda_{n,1}(x)^{p^n} \\ \vdots \\ \lambda_{n,p^n-1}(x)^{p^n} \end{pmatrix}.$$

Assertion $(D_i(b^j))_{0 \leq i, j < p^n}$ est inversible.

Preuve On montre plus généralement que des éléments x_0, \dots, x_{p^n-1} de K sont linéairement dépendants au-dessus de K^{p^n} si et seulement si le Wronskien

$$\begin{vmatrix} D_0(x_0) & \dots & D_0(x_{p^n-1}) \\ \vdots & \ddots & \vdots \\ D_{p^n-1}(x_0) & \dots & D_{p^n-1}(x_{p^n-1}) \end{vmatrix}$$

est nul.

S'il existe une relation de dépendance linéaire entre les x_i à coefficients dans K^{p^n} , il est clair que le Wronskien est nul car les applications D_j sont K^{p^n} -linéaires pour $j < p^n$.

Réciproquement, supposons que le Wronskien est nul, c'est-à-dire qu'il existe des coefficients μ_i dans K , non tous nuls, tels que, pour tout $j < p^n$,

$$\sum_{i=0}^{p^n-1} \mu_i D_j(x_i) = 0.$$

Montrons alors que, pour tout $h, j < p^n$,

$$\sum_{i=0}^{p^n-1} D_h(\mu_i) D_j(x_i) = 0 \quad .$$

Pour $h = 0$, c'est l'égalité précédente. Ensuite, on procède par induction sur h :

$$\begin{aligned}
0 &= D_h \left(\sum_{i=0}^{p^n-1} \mu_i D_j(x_i) \right) = \sum_{l=0}^h \sum_{i=0}^{p^n-1} D_l(\mu_i) D_{h-l} \circ D_j(x_i) \\
&= \sum_{i=0}^{p^n-1} D_h(\mu_i) D_j(x_i) + \underbrace{\sum_{l=0}^{h-1} \binom{h-l+j}{j} \sum_{i=0}^{p^n-1} D_l(\mu_i) D_{h-l+j}(x_i)}_{=0, \text{ par induction si } h-l+j < p^n, \text{ et, dans le cas contraire, parce que le coefficient binomial est nul}}.
\end{aligned}$$

Considérons $0 \leq h < p^n$ maximum tel que les $D_h(\mu_i)$ ne sont pas tous nuls. On a alors, pour tous $0 \leq i < p^n$ et $1 \leq j < p^n$, $D_j(D_h(\mu_i)) = \binom{j+h}{h} D_{j+h}(\mu_i) = 0$, d'après le choix de h si $j+h < p^n$, et parce que le coefficient binomial est nul sinon. Puisque K est strict, il en résulte que les $D_h(\mu_i)$ sont dans K^{p^n} . On a ainsi des coefficients non tous nuls $D_h(\mu_i)$ dans K^{p^n} , qui témoignent du fait que les x_i ne sont pas linéairement indépendants au-dessus de K^{p^n} . \square

En d'autres termes, puisque la matrice $(D_i(b^j))_{0 \leq i, j \leq p^n-1}$ est inversible, les p^n -uplets $(D_i(x))_{i < p^n}$ et $\lambda_n(x)^{p^n}$ sont birationnellement équivalents au-dessus de $\mathbb{F}_p(\{b\}) := \mathbb{F}_p(D_i(b))_{i \in \mathbb{N}}$.

3 Points rationnels des variétés abéliennes

Etant donnée une variété algébrique V définie sur un corps K , l'ensemble des points K -rationnels de V s'écrit naturellement comme un ensemble définissable dans $(K, 0, 1, +, -, \cdot)$: si V est une variété affine, dont l'idéal dans $K[X]$ est engendré par P_1, \dots, P_r , on a simplement

$$V(K) = \{x \in K^n; \forall i, P_i(x) = 0\}.$$

Dans le cas d'une variété algébrique générale, il suffit par exemple de recouvrir V par des ouverts affines V_1, \dots, V_m , et d'identifier $V(K)$ avec l'union

$$V_1(K) \cup (V_2 \setminus V_1)(K) \cup \dots \cup (V_m \setminus (V_1 \cup \dots \cup V_{m-1}))(K).$$

Pour un modèle (K, D) de CHF_p , notons que $V(K)$ est Zariski-dense dans V , puisque K est séparablement clos. Les sous-ensembles (infiniment) définissables de $V(K)$ ne proviennent pas simplement de combinaisons booléennes de sous-variétés algébriques de V .

On appellera dans la suite *sous-variété D-algébrique de V* un sous-ensemble de $V(K)$ qui s'écrit, dans chaque ouvert affine, comme la collection des zéros d'une famille de D-polynômes de $K\{X\}$ (c'est-à-dire fermé pour la *D-topologie*). On peut décrire ces sous-variétés D-algébriques en utilisant les *prolongations* de V , comme suit.

Pour V une variété algébrique lisse et irréductible, on peut construire un système projectif de prolongations, avec $\Delta_0 V = V$:

$$(\pi_{j,i} : \Delta_j V \longrightarrow \Delta_i V)_{j \geq i \geq 0}.$$

Il existe des applications définissables, d'image dense :

$$\begin{array}{ccc} \delta_j : V(K) & \longrightarrow & \Delta_j V(K) \\ x & \longmapsto & (D_0(x), \dots, D_j(x)) \end{array} \quad .$$

Dans le cas d'un groupe algébrique, les prolongations forment un système projectif de groupes algébriques.

Une sous-variété D -algébrique W de V est déterminée par un système projectif de sous-variétés algébriques $W_i \subseteq \Delta_i V$, compatible avec les projections :

$$W(K) = \{x \in V(K); \forall i \geq 0, \delta_i(x) \in W_i(K)\}.$$

Dans le cas qui nous intéresse d'une caractéristique $p > 0$, nous disposons d'une description alternative des prolongations.

Plaçons-nous au-dessus d'un modèle K de CHF_p , fixons une p -base $\{b\}$ de K et les fonctions λ_n correspondantes (voir la section 1). Dans [BoDe01], il est défini un foncteur Λ_n , de la catégorie des variétés algébriques définies sur K dans elle-même. On dispose en outre de projections régulières $\rho_{m,n} : \Lambda_m V \longrightarrow \Lambda_n V$ pour $m \geq n$, et d'applications définissables $\lambda_n : V(K) \longrightarrow (\Lambda_n V)(K)$ qui coïncident localement avec les fonctions λ_n déjà définies sur l'espace affine, et telles que $\rho_{n,0}$ et λ_n sont des bijections réciproques entre $V(K)$ et $(\Lambda_n V)(K)$.

On utilise la notion de restriction de Weil pour caractériser le foncteur Λ_n :

Définition 2 Soit V une variété algébrique définie sur K . On appelle $\tilde{\rho}_n : \Pi_n V \longrightarrow V$ une restriction de Weil pour V de K à K^{p^n} si :

- $\Pi_n V$ est définie sur K^{p^n} et $\tilde{\rho}_n$ est un morphisme surjectif défini sur K
- pour toute variété algébrique W définie sur K^{p^n} et tout morphisme $f : W \longrightarrow V$ défini sur K , il existe un unique morphisme g défini sur K^{p^n} tel que le diagramme suivant commute :

$$\begin{array}{ccc} W & \xrightarrow{f} & V \\ g \searrow & & \nearrow \tilde{\rho}_n \\ & \Pi_n V & \end{array} \quad .$$

Nous noterons, pour tout entier n , $Fr^n : A \longrightarrow Fr^n A$ l'isogénie Frobenius à la puissance n .

Proposition 1 Soit V une variété algébrique définie sur K . Alors $((Fr^n \circ \Lambda_n)V, \rho_{n,0} \circ Fr^{-n})$ est une restriction de Weil pour V de K à K^{p^n} .

Preuve Voir la proposition III.8 de [Be05]. □

On notera désormais $(\Pi_n V, \tilde{\rho}_n)$ pour $((Fr^n \circ \Lambda_n)V, \rho_{n,0} \circ Fr^{-n})$.

Proposition 2 Si V est une variété algébrique lisse et irréductible définie sur K , alors

$$\pi_{p^n-1,0} : \Delta_{p^n-1} V \longrightarrow V \text{ et } \tilde{\rho}_n : \Pi_n V \longrightarrow V$$

sont isomorphes au-dessus de V .

Preuve Tout d'abord, on a vu dans la partie 2 qu'il existe une matrice inversible B à coefficients dans $\mathbb{F}_p(\{b\})$ telle que, pour tout $x \in V(K)$,

$$\begin{pmatrix} D_0(x) \\ D_1(x) \\ \vdots \\ D_{p^n-1}(x) \end{pmatrix} = B \begin{pmatrix} \lambda_{n,0}(x)^{p^n} \\ \lambda_{n,1}(x)^{p^n} \\ \vdots \\ \lambda_{n,p^n-1}(x)^{p^n} \end{pmatrix}.$$

On en déduit deux bijections réciproques l'une de l'autre entre $\delta_{p^n-1}(V(K))$ et $\lambda_n^{p^n}(V(K))$. Ces applications sont polynômiales, donc se prolongent, d'après la densité de ces deux ensembles dans les variétés algébriques voulues, en des morphismes de variétés algébriques

$$\Phi : \Delta_{p^n-1}V \longrightarrow \Pi_n V \quad \text{et} \quad \Psi : \Pi_n V \longrightarrow \Delta_{p^n-1}V \quad .$$

Les identités $\Phi \circ \Psi = id$ et $\Psi \circ \Phi = id$, qui sont vraies respectivement sur $\lambda_n^{p^n}(V(K))$, dense dans $\Pi_n V$, et sur $\delta_{p^n-1}(V(K))$, dense dans $\Delta_{p^n-1}V$, sont donc vraies respectivement sur $\Pi_n V$ et sur $\Delta_{p^n-1}V$: Φ et Ψ sont les isomorphismes recherchés.

Pour la même raison de densité, ils vérifient $\tilde{\rho}_n \circ \Phi = \pi_{p^n-1,0}$. \square

Le cas particulier important auquel on s'intéressera désormais est celui d'une variété semi-abélienne A définie au-dessus d'un modèle K de CHF_p . Dans ce cas, on sait que $A(K)$ est un groupe n -divisible pour tout n premier à p (car K est séparablement clos), mais qu'il n'est pas p -divisible (car K n'est pas parfait). On pose :

$$p^\infty A(K) := \bigcap_{n \geq 0} p^n A(K).$$

C'est le plus grand sous-groupe divisible de $A(K)$. C'est un sous-groupe infiniment définissable, fermé pour la D-topologie, de $A(K)$, c'est-à-dire un sous-groupe D-algébrique de $A(K)$. Il est aussi connexe et Zariski-dense dans A (voir [BoDe02]). Décrivons-le par l'intermédiaire du système projectif des $\Pi_n A$.

Pour tout n , l'isogénie Frobenius à la puissance n , $F r^n : A \longrightarrow F r^n A$, admet une isogénie duale, appelée *Verschiebung*, et notée $V_n : F r^n A \longrightarrow A$. Elle vérifie $V_n \circ F r^n = [p^n]_A$ et $F r^n \circ V_n = [p^n]_{F r^n A}$ (où, pour un entier m , $[m]$ désigne la multiplication par m dans le groupe algébrique considéré). Puisque $F r^n A$ est définie sur K^{p^n} , on déduit de la propriété universelle des restrictions de Weil un morphisme α_n , défini sur K^{p^n} , tel que le diagramme suivant commute :

$$\begin{array}{ccc} F r^n A & \xrightarrow{V_n} & A \\ \alpha_n \searrow & & \nearrow \tilde{\rho}_n \\ & \Pi_n A & \end{array} \quad .$$

Par functorialité du Frobenius et de la restriction de Weil, α_n est un homomorphisme de groupes algébriques. Notons A_n l'image de l'homomorphisme

α_n . C'est un sous-groupe algébrique de $\Pi_n A$, défini sur K^{p^n} . Les A_n décrivent alors $p^\infty A(K)$, plus précisément :

Lemme 1

$$p^\infty A(K) = \bigcap_{n \geq 0} \tilde{\rho}_n(A_n(K^{p^n})) = \{x \in A(K); \forall n \geq 0, \lambda_n(x)^{p^n} \in A_n(K)\}.$$

Preuve Tout d'abord, la deuxième égalité est une conséquence du fait que $\tilde{\rho}_n$ et $\lambda_n^{p^n}$ sont des bijections réciproques l'une de l'autre entre $(\Pi_n A)(K^{p^n})$ et $A(K)$. Ensuite, si $x \in p^\infty A(K)$, on trouve pour tout n un élément x_n dans $A(K)$ tel que

$$x = [p^n]x_n = V_n(Fr^n(x_n)) = \tilde{\rho}_n(\alpha_n(Fr^n(x_n))).$$

Comme $\alpha_n(Fr^n(x_n)) \in A_n(K^{p^n})$, on a bien $x \in \tilde{\rho}_n(A_n(K^{p^n}))$. Réciproquement, si pour $x \in A(K)$, $\lambda_n(x)^{p^n} \in A_n(K) \cap (\Pi_n A)(K^{p^n}) = A_n(K^{p^n})$, il existe $y_n \in (Fr^n A)(K^{p^n})$ tel que $\alpha_n(y_n) = \lambda_n(x)^{p^n}$ (car $\alpha_n : Fr^n A \rightarrow A_n$ est par définition un homomorphisme de groupes algébriques, dominant et défini sur K^{p^n} , et donc surjectif au niveau des points K^{p^n} -rationnels), et par suite $x_n \in A(K)$ tel que $Fr^n(x_n) = y_n$. On en déduit que $[p^n](x_n) = V_n \circ Fr^n(x_n) = \tilde{\rho}_n \circ \alpha_n(y_n) = \tilde{\rho}_n(\lambda_n(x)^{p^n}) = x$, donc $x \in p^n A(K)$. \square

Définition 3 On dit que le type de a au-dessus d'un modèle k de CHF_p est mince si le D -corps engendré par a au-dessus de k , $k(\{a\}) := k(D_i(a))_{i \in \mathbb{N}}$, est de degré de transcendance fini au-dessus de k .

La caractérisation précédente de $p^\infty A(K)$ permet de montrer facilement le lemme suivant (qui est le lemme 2.15 de [Hr96]).

Lemme 2 Soit k un D -corps de définition de A contenant la p -base fixée pour K . Alors, pour tout $a \in p^\infty A(K)$, le type de a au-dessus de k est mince.

Preuve Tout d'abord, on a vu que $k(\{a\}) = k(\lambda_n(a)^{p^n})_{n \geq 0}$. Ensuite, pour tout $n \geq 0$, on trouve $a_n \in A(K)$ tel que $a = [p^n]a_n = V_n \circ Fr^n(a_n)$. Comme V_n est une isogénie, $k(Fr^n(a_n))$ est une extension algébrique de $k(a)$. Or, $\alpha_n(Fr^n(a_n)) \in k(Fr^n(a_n))$, et on a vu que $\tilde{\rho}_n \circ \alpha_n \circ Fr^n(a_n) = [p^n]a_n = a$ implique que $\alpha_n \circ Fr^n(a_n) = \lambda_n(a)^{p^n}$: on a donc que $\lambda_n(a)^{p^n}$ est algébrique sur $k(a)$. \square

Dans la suite, on s'intéressera à des conditions, portant sur les isogénies V_n , qui permettent de renforcer cette propriété de minceur, ainsi qu'à leur rapport avec la conjecture de Mordell-Lang.

4 La minceur rationnelle

On considère une notion de minceur plus forte que la notion précédente, la minceur rationnelle.

Définition 4 On dit que le type de a au-dessus d'un modèle k de CHF_p est rationnellement mince si le D -corps engendré par a au-dessus de k , $k(\{a\}) := k(D_i(a))_{i \in \mathbb{N}}$, est finiment engendré en tant que corps au-dessus de k .

On dit qu'un groupe infiniment définissable connexe, défini au-dessus de k est rationnellement mince si son type générique l'est.

Dans [Bu92], Alexandru Buium étudie la notion de *D-structure* sur une variété algébrique en caractéristique nulle, c'est-à-dire d'extension de la dérivation au faisceau des fonctions régulières, et montre l'équivalence entre la catégorie des groupes algébriques munis d'une D-structure et celle des groupes « δ -algébriques » de dimension finie. Dans [Be05], il est montré comment généraliser cette notion à la caractéristique positive, et aussi l'équivalence entre la catégorie des groupes algébriques connexes munis d'une D-structure et celle des groupes infiniment définissables connexes rationnellement minces. Ici, on ne va s'intéresser et montrer qu'une conséquence de ce résultat : si $p^\infty A(K)$ est rationnellement mince, on peut, quitte à remplacer A par une variété semi-abélienne qui lui est isogène, trouver une suite de sections pour les projections $\pi_{i,0} : \Delta_i A \rightarrow A$.

Dans la suite, A désigne une variété semi-abélienne définie sur un modèle k de CHF_p , et K un modèle $|k|^+$ -saturé contenant k .

Proposition 3 *Si $p^\infty A(K)$ est rationnellement mince, il existe une isogénie de variétés semi-abéliennes au-dessus de k , $B \rightarrow A$, telle que, si b désigne un point générique de $p^\infty B(K)$, alors $k(\{b\}) = k(b)$.*

Preuve Considérons un point générique a de $p^\infty A(K)$ au-dessus de k ; par définition, il existe un entier i tel que $k(\{a\}) = k(D_0(a), \dots, D_i(a))$, nous avons aussi montré, dans le lemme 2, que ce corps est une extension algébrique de $k(a)$. Nous noterons $\delta_i := (D_0, \dots, D_i)$, et Γ l'image par δ_i de $p^\infty A(K)$, munie de la structure de groupe induite par celle de $p^\infty A(K)$.

Si a et a' sont des points génériques de $p^\infty A(K)$ indépendants au-dessus de k , il vient d'après les axiomes d'une dérivation de Hasse que $k(\delta_i(a * a')) \subseteq k(\delta_i(a), \delta_i(a'))$ et $k(\delta_i(a^{-1})) \subseteq k(\delta_i(a))$ (où $*$ et $^{-1}$ représentent les opérations de groupe de $A(K)$). Les lois de groupe sur Γ sont donc génériquement rationnelles, ce qui nous permet de définir un groupe algébrique B , défini sur k , dans lequel Γ est un sous-groupe dense (on utilise pour cela un théorème de Weil, voir [We55]). D'autre part, l'homomorphisme (rationnel) « restriction », $(x_0, \dots, x_i) \mapsto x_0$, de Γ dans $p^\infty A(K)$, s'étend en un homomorphisme de groupes algébriques de B dans A (voir le théorème 3 de [Ro56]), qui est une isogénie car $k(\delta_i(a))$ est algébrique au-dessus de $k(a)$, pour $\delta_i(a)$ un point générique dans Γ , et donc dans B . On en déduit donc que B est, comme A , une variété semi-abélienne. On déduit du fait que δ_i est un isomorphisme (définissable) de $p^\infty A(K)$ sur Γ , que $\Gamma = p^\infty B(K)$, et, par construction, pour un point générique $b = \delta_i(a)$ de Γ , on a $k(\{b\}) = k(\{a\}) = k(b)$. \square

Proposition 4 *Supposons que le point générique a de $p^\infty A(K)$ vérifie $k(\{a\}) = k(a)$. Alors, pour tout $i \geq 0$, il existe une section s_i à la projection $\pi_{i,0} : \Delta_i A \rightarrow A$, qui coïncide avec $\delta_i := (D_0, \dots, D_i)$ sur $p^\infty A(K)$.*

Preuve Soit a le point générique de $p^\infty A(K)$. Par hypothèse, il existe une fraction rationnelle s_i , à coefficients dans k , telle que

$$\delta_i(a) := (D_0(a), \dots, D_i(a)) = s_i(a).$$

Les fonctions s_i sont donc des fonctions rationnelles partielles, de $p^\infty A(K)$ dans $\Delta_i A(K)$, qui sont des homomorphismes par définition de la loi de groupe de

$\Delta_i A$, et qui vérifient $\pi_{i,0} \circ s_i = id$ sur $p^\infty A(K)$. En prolongeant les fonctions s_i en des homomorphismes de groupes algébriques de A dans $\Delta_i A$ (par le même argument de densité que précédemment), on obtient les sections recherchées. \square

En utilisant les isomorphismes exhibés dans la proposition 2 entre les prolongations et les restrictions de Weil, on peut prouver le résultat de descente suivant. L'argument pour le passage des différents k^{p^m} au corps des constantes absolues k^{p^∞} nous a été donné lors de discussions avec Jean-Benoît Bost, Elisabeth Bouscaren, Anand Pillay, Damien Roessler et Thomas Scanlon. Il utilise une paramétrisation des *variétés abéliennes polarisées avec une structure de niveau n* par un *espace de modules* approprié ; on pourra trouver les propriétés de cet objet dans [MuFo82].

Théorème 4 *Supposons que A est une variété abélienne définie au-dessus de k , telle que $p^\infty A(K)$ soit rationnellement mince. Alors A est isogène à une variété abélienne B définie sur C_k^∞ .*

Preuve En utilisant la proposition 3, on trouve tout d'abord une variété abélienne B , isogène à A , telle que $k(\{b\}) = k(b)$ pour tout point générique b de $p^\infty B(K)$ au-dessus de k . La proposition 4 nous donne alors, pour tout i , des sections $s_i : B \rightarrow \Delta_i B$, que l'on va utiliser pour montrer que, pour tout entier m , B est isomorphe à une variété abélienne définie sur k^{p^m} .

D'après la proposition 2, on obtient une famille $t_m : B \rightarrow \Pi_m B$ de sections pour les projections $\tilde{\rho}_m$. Puisque les sections s_i coïncident avec les sections définissables δ_i sur $p^\infty B(K)$, on obtient aussi que $t_m(x) = \lambda_m(x)^{p^m}$ pour $x \in p^\infty B(K)$. Dans la partie 3, on a donné la caractérisation suivante :

$$p^\infty B(K) = \{x \in B(K); \forall m \geq 0, \lambda_m(x)^{p^m} \in B_m(K^{p^m})\},$$

où, pour tout m , B_m est un sous-groupe algébrique de $\Pi_m B$ défini sur K^{p^m} . On montre alors que B est isomorphe à B_m : on sait déjà que $\tilde{\rho}_m \circ t_m = id_B$, et, pour $x \in p^\infty B(K)$, $t_m \circ \tilde{\rho}_m(t_m(x)) = t_m \circ \tilde{\rho}_m(\lambda_m(x)^{p^m}) = t_m(x)$, donc $t_m \circ \tilde{\rho}_m = id$ sur l'image de $p^\infty B(K)$ par t_m , et donc sur $t_m(B)$ par densité. Or $t_m(B) = B_m$ (car pour $x \in p^\infty B(K)$ et $x_m \in B(K)$ tels que $[p^m]x_m = x$, on a vu dans la preuve de la proposition 2 que $t_m(x) = \lambda_m(x)^{p^m} = \alpha_m(Fr^m(x_m))$, et donc $t_m(p^\infty B(K))$ est dense dans l'image de $Fr^m B$ par α_m , c'est-à-dire B_m), et on a donc obtenu un isomorphisme de B sur B_m .

Pour en déduire que B est isomorphe à une variété abélienne définie sur k^{p^∞} , on utilise l'espace de modules $\mathcal{A}_{g,d^2,n}$ des variétés abéliennes de dimension $g = \dim(B)$, munie d'une polarisation de degré d^2 et d'une structure de niveau n , pour un n premier à p et suffisamment grand pour que cet espace de modules existe (voir [MuFo82]).

Fixons une polarisation ω sur B et notons d^2 son degré. Fixons aussi dans $B(k)$ une structure de niveau n , c'est-à-dire une base (x_1, \dots, x_{2g}) de la n -torsion dans $G(k)$ (ce qui est possible car n est premier à p et k est séparablement clos, de sorte que la n -torsion dans $B(k)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^{2g}$). Alors, pour tout $m \geq 0$, l'isomorphisme t_m transporte cette polarisation sur une polarisation de B_m , de même degré et définie sur k^{p^m} , et la structure de niveau n sur une structure de niveau n dans $B_m(k^{p^m})$. On a donc que la variété abélienne $(B, \omega, (x_1, \dots, x_{2g}))$ correspond à un point dans $\mathcal{A}_{g,d,n}(k^{p^m})$, pour tout $m \geq 0$, et donc à un point dans l'intersection $\mathcal{A}_{g,d,n}(k^{p^\infty})$.

On en déduit que B est isomorphe à une variété abélienne définie sur C_k^∞ , or A est isogène à B . \square

Remarque La réciproque du théorème précédent est vraie. En effet, si B est définie sur C_k^∞ , alors $p^\infty B(K) = B(C_K^\infty)$ (voir par exemple [BoDe02]), qui est rationnellement mince puisque tous les points ont leurs dérivées nulles. Et l'image d'un point rationnellement mince est rationnellement mince, puisqu'un sous-corps d'un corps finiment engendré au-dessus de k est finiment engendré au-dessus de k .

Ce théorème permet de reformuler la conclusion de la conjecture de Mordell-Lang pour les variétés abéliennes : sous les hypothèses du théorème 1, on doit essentiellement montrer que $p^\infty A(K)$ est rationnellement mince. Malheureusement, on ne sait pas encore exploiter ce fait pour donner une preuve différentielle algébrique de la conjecture.

5 La minceur séparable

Une notion intermédiaire entre la minceur et la minceur rationnelle a été dégagée dans [PiZi03] ; il s'agit de la notion de point très mince. Nous utiliserons ici l'expression "séparablement mince", qui est plus explicite et qui a un meilleur comportement grammatical.

Définition 5 *On dit que le type de a au-dessus d'un modèle k de CHF_p est séparablement mince si le D -corps engendré par a au-dessus de k , $k(\{a\}) := k(D_i(a))_{i \in \mathbb{N}}$, est une extension algébrique séparable d'un corps finiment engendré au-dessus de k .*

On dit qu'un groupe infiniment définissable connexe, défini au-dessus de k , est séparablement mince si son type générique l'est.

Dans [PiZi03], Pillay et Ziegler donnent une preuve directe de la conjecture de Mordell-Lang dans le cas où $p^\infty A(K)$ est séparablement mince. On connaît des conditions suffisantes pour que $p^\infty A(K)$ soit séparablement mince, par exemple que A soit une variété abélienne *ordinaire* ; mais on ne savait pas jusqu'à présent si $p^\infty A(K)$ pouvait ne pas être séparablement mince. Avant d'exhiber un contre-exemple, donnons la caractérisation suivante.

Fait 1 *Soit A une variété semi-abélienne définie sur k . Avec les notations de la section précédente, on considère pour $m \geq n$, l'homomorphisme $\tilde{\rho}_{m,n} := Fr^m \circ \rho_{m,n} \circ Fr^{-n}$ de $\Pi_m A$ dans $\Pi_n A$. Alors $\tilde{\rho}_{m,n}|_{A_m}$ est une isogénie de A_m dans A_n .*

Preuve Voir la proposition IV.16 de [Be05]. \square

Proposition 5 *Le groupe $p^\infty A(K)$ est séparablement mince si et seulement s'il existe $n \geq 0$ tel que $\tilde{\rho}_{m,n}|_{A_m}$ est séparable pour tout $m \geq n$.*

Preuve Tout d'abord, comme dans la section 3, pour a générique dans $p^\infty A(K)$, et a_m , lui aussi générique dans $p^\infty A(K)$, tel que $[p^m]a_m = a$, on a $b_m := \lambda_m(a)^{p^m} = \alpha_m \circ Fr^m(a_m)$ qui est générique dans A_m , et $\tilde{\rho}_{m,n}|_{A_m}(b_m) = b_n$

pour $m \geq n$.

Supposons que $p^\infty A(K)$ est très mince, et considérons l'entier n tel que $k(\{a\}) = k(\lambda_m(a)^{p^m})_{m \geq 0}$ est algébrique séparable sur $k(\lambda_n(a)^{p^n})$. On a alors que pour tout $m \geq n$, $k(b_m)$ est algébrique séparable sur $k(b_n)$, donc $\tilde{\rho}_{m,n|A_m}$ est séparable.

Réciproquement, supposons qu'il existe $n \geq 0$ tel que $\tilde{\rho}_{m,n|A_m}$ est séparable pour tout $m \geq n$. Pour a, b_m et b_n comme précédemment, on a que $k(b_m)$ est algébrique séparable sur $k(b_n)$ pour $m \geq n$, ce qui implique que $k(\{a\}) = k(b_m)_{m \geq 0}$ est algébrique séparable sur $k(\lambda_n(a)^{p^n})$. \square

Nous cherchons maintenant à construire une variété abélienne simple A au-dessus de K qui n'est pas séparablement mince, ce qui signifie pour nous par définition que $p^\infty A(K)$ n'est pas séparablement mince.

On ne peut pas trouver une telle variété abélienne de dimension 1 : le fait qu'une courbe elliptique soit toujours séparablement mince a été remarqué par plusieurs auteurs, avec des arguments variés. Il est montré par exemple dans l'annexe A de [Be05] que le type d'un point a au-dessus de k est séparablement mince dès que $k(\{a\})$ est de degré de transcendance 1 au-dessus de k . Donnons un autre argument portant sur la multiplication par p dans les courbes elliptiques, qui nous aidera à présenter celui des variétés abéliennes générales.

Pour simplifier, supposons la caractéristique différente de 2 et 3. Dans ce cas, modulo un changement de variables, l'équation (affine) d'une courbe elliptique peut être écrite sous la « forme normale » $y^2 = x^3 + px + q$. A un facteur multiplicatif entier près le discriminant d'une telle équation est $\Delta := 4p^3 + 27q^2$, son j -invariant est $j := \frac{p^3}{\Delta}$. La courbe est lisse ssi Δ n'est pas nul, son complété projectif porte alors une structure de groupe algébrique, et une seule dès qu'on a choisi un élément neutre (la loi est celle qu'on connaît, construite à partir du 3ème point d'intersection d'une sécante avec la courbe). Tout j est le j -invariant d'une courbe elliptique et deux courbes sont isomorphes (en tant que variétés projectives et, donc, en tant que groupes algébriques) si et seulement si elles ont même j -invariant.

Sur une courbe elliptique E , la multiplication par m , notée $[m]$, est, en tant qu'application rationnelle, de degré m^2 , c'est-à-dire que si x est un point générique de E , l'extension $k([m]x) \subseteq k(x)$ est de degré m^2 . En particulier la multiplication par p est de degré p^2 , avec un degré d'inséparabilité au moins p d'après la factorisation déjà citée de $[p]$ par le Frobenius, $[p] = V_1 \circ Fr$. Ou bien le degré d'inséparabilité est effectivement p et dans ce cas la Verschiebung V_1 est séparable (ainsi que tous les V_n , d'après l'écriture $V_n = Fr^{n-1}(V_1) \circ \dots \circ Fr(V_1) \circ V_1$), d'où l'on obtient que E est séparablement mince d'après la proposition 5. Ou bien le degré d'imperfection est p^2 et $[p]$ est purement inséparable, ce qui se traduit par une liaison algébrique imposant $j \in \mathbb{F}_{p^2}$ (il y a plusieurs valeurs possibles), la courbe est donc définie sur un corps fini, et $p^\infty E(K) = E(K^{p^\infty})$ est rationnellement mince, et a fortiori séparablement mince. Ainsi une courbe elliptique est toujours séparablement mince.

Dans ce qu'on vient de voir, le j -invariant est un paramètre décrivant la courbe à isomorphisme près. Ce principe du paramétrage des courbes elliptiques par un paramètre du corps ne s'étend pas directement en dimension supérieure. Le paramétrage des variétés abéliennes « nues » de dimension fixée ne se comporte pas bien, d'où l'adjonction d'une structure supplémentaire. On a déjà vu l'adjonction d'une polarisation et d'une structure de niveau n , c'est un enrichissement différent que nous considérons maintenant, avec l'adjonction d'une « polarisation principale » qui est un isomorphisme de la variété vers sa variété duale. Une variété abélienne de dimension ≥ 2 n'est en général pas isomorphe à sa variété duale mais elle est isogène à une variété abélienne qui l'est et qui porte donc une polarisation principale. Nous allons dans ce qui suit identifier une variété abélienne principalement polarisée de dimension d et le point de l'espace des modules (de dimension $\frac{d(d+1)}{2}$), qui la paramètre à isomorphisme près.

La torsion d'ordre p d'une variété de dimension d est, en tant que groupe, isomorphe à une puissance $(\mathbb{Z}/p\mathbb{Z})^n$ pour un certain entier $n \leq d$ appelé le p -rang de la variété. Ce n , s'il est strictement inférieur à d , peut être raffiné : il suffit pour cela de considérer la torsion d'ordre supérieur p^r et de la considérer non plus du point de vue naïf mais schématique. Ainsi dans le cas d'une courbe elliptique, la torsion p qui, considérée comme ensemble de points dans la clôture algébrique, était ou bien $\mathbb{Z}/p\mathbb{Z}$ ou bien 0 , est maintenant un objet, toujours de torsion p , mais de rang p^2 , en fait ou bien une extension de $(\mathbb{Z}/p\mathbb{Z})$ par μ_p (où μ_p est le noyau de la multiplication par p , $[p] : \mathbb{G}_m \mapsto \mathbb{G}_m$, donc en fait $[p]$ est ici le Frobenius) ou bien une extension de α_p par α_p (où α_p est le noyau du Frobenius sur le groupe additif cette fois, $F_r : \mathbb{G}_a \mapsto \mathbb{G}_a$). La classification par la torsion schématique n'est dans ce cas pas plus fine que la classification naïve. Elle le devient en dimension supérieure. Précisons.

Pour une variété abélienne A définie sur un corps quelconque k et un entier m , soit $A[m] := \{x \in k^{alg}; m.a = 0\}$, et pour un nombre premier q , $A[q^\infty] := \varprojlim A[q^r]$, qui porte naturellement une structure de \mathbb{Z}_q -module, c'est le *module de Tate q -adique* de la variété. Pour q différent de p , si d est la dimension de A , $A[q^\infty]$ est isomorphe à \mathbb{Z}_q^{2d} . La situation est plus compliquée pour $q = p$: l'action de \mathbb{Z}_p sur $A[p^\infty]$ peut être enrichie, en particulier de l'action du groupe de Galois absolu, et la description de ce « module de Dieudonné » sur un anneau maintenant plus gros que \mathbb{Z}_p est une des motivations de la cohomologie cristalline. A isogénie près, $A[p^\infty]$ se décompose en une somme directe de modules irréductibles, ou encore, graphiquement, est associé à $A[p^\infty]$ un « polygone de Newton », ayant les propriétés suivantes :

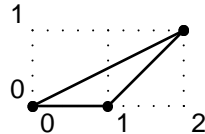
- dans le plan cartésien, c'est une ligne convexe de segments de droite à sommets entiers, commençant en $(0, 0)$ et finissant en $(2d, d)$,
 - à pentes positives ou nulles, au plus égales à 1 ,
 - avec une dualité imposant que si on a la pente c , on a également la pente $1 - c$.
- L'absence du couple pente 0 /pente 1 équivaut à un p -rang nul, la présence maximale de ce couple à une variété « ordinaire », c'est-à-dire de p -rang maximal, ou encore à un module de Tate p -adique de dimension d . Un unique segment à pente $1/2$, ou encore d fois un segment dont les projections sont à longueurs entières $(2, 1)$, correspond à une variété abélienne dite « supersingulière », c'est-à-dire

isogène à un produit de courbes elliptiques supersingulières, donc définies, ainsi que leur produit, sur \mathbb{F}_p^{alg} .

L'ensemble des polygones de Newton est partiellement ordonné par leurs positions dans le plan cartésien réel : $P \geq Q$ si tout point de P est au-dessus de Q , au sens large, P et Q peuvent avoir des sommets ou des segments communs. Chaque polygone de Newton P définit alors un fermé dans l'espace des modules, au sens suivant : les variétés abéliennes principalement polarisées ayant un polygone de Newton situé au-dessus de P , forment un fermé. Ce fermé n'est pas nécessairement irréductible mais toutes ses composantes irréductibles ont même dimension, disons $d(P)$, et $P > Q$ implique $d(P) < d(Q)$. Nous utiliserons dans la suite un moyen combinatoire simple de calculer $d(P)$, que l'on peut trouver dans [Oo01].

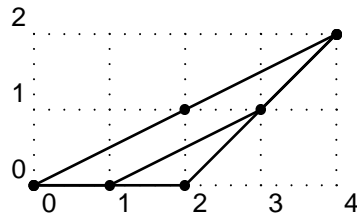
Notre but est de trouver une variété abélienne simple, de p -rang nul, qui n'est pas isogène à une variété abélienne définie sur \mathbb{F}_p^{alg} .

Regardons le cas des courbes elliptiques :



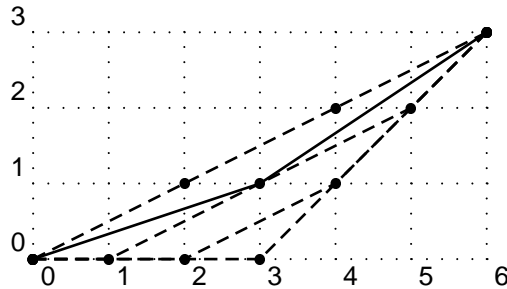
On trouve deux polygones de Newton possibles, celui du bas correspond à des courbes ordinaires, l'autre à des courbes supersingulières définies sur \mathbb{F}_p^{alg} ; ces dernières correspondent à des spécialisations (algébriques) du paramètre général.

En dimension 2, nous trouvons trois dessins possibles :



Les deux polygones de Newton du bas correspondent à des variétés ayant une torsion p non nulle (présence d'un segment horizontal), et le troisième à des variétés définies sur \mathbb{F}_p^{alg} , à isogénie près.

En dimension 3, on trouve 5 dessins possibles (par convexité et dualité) :



Le polygone de Newton P_0 , marqué en trait plein, est le seul qui correspond à des variétés de p -rang nul et non supersingulières, il pourrait donc éventuellement nous convenir. Nous convient-il vraiment ? C'est-à-dire P_0 est-il le polygone de Newton d'une variété non séparablement mince, simple de surcroît ?

Prenons un point a de dimension maximale (c'est ici 3) dans le fermé de l'espace de modules associé à ce polygone. Il a exactement P_0 pour polygone de Newton, qui n'est lui-même pas décomposable : P_0 ne contient que deux segments à sommets entiers, qui ne sont pas dissociables à cause du principe de dualité. Les variétés abéliennes principalement polarisées correspondantes sont donc simples. Par construction une variété abélienne principalement polarisée A paramétrée par a n'est pas isomorphe à une variété définie sur un corps fini (son corps de définition est de degré de transcendance 3 au-dessus de \mathbb{F}_p). De plus, une variété abélienne isogène à A doit avoir un corps de définition de degré de transcendance au moins 2 : la dimension d'une « feuille » déterminée par une classe d'isogénie à l'intérieur du fermé correspondant au polygone P_0 est 1 (voir [Oo04] pour le calcul de la dimension de ces feuilles : celle-ci est toujours strictement inférieure à la dimension du fermé défini par un polygone de Newton dès que celui-ci n'est pas de pente constante égale à $1/2$). On obtient donc que A ne peut pas être isogène à une variété abélienne définie sur un corps fini. Dorénavant, nous fixerons k un modèle de CHF_p contenant ce corps de définition, muni d'une dérivation de Hasse telle que $C_k^\infty = \mathbb{F}_p^{alg}$ (voir l'exemple 2 de la partie 2) ; de sorte que « être défini sur un corps fini » est équivalent à « être défini sur k^{p^∞} ».

Assertion A n'est pas séparablement mince.

Preuve Puisque le p -rang de A est nul, la multiplication par p^n dans A , $[p^n] = V_n \circ Fr^n$, est purement inséparable pour tout n (le noyau est trivial dans $A(k^{alg})$). Les isogénies V_n sont donc elles aussi purement inséparables. Supposons que A est séparablement mince. D'après la caractérisation de la proposition 5, il existe donc $n \geq 0$ tel que l'isogénie $\tilde{\rho}_{m,n|A_m}$ est séparable pour tout $m \geq n$. Or, pour $m \geq n$, on peut décomposer l'isogénie purement inséparable V_m à l'aide des isogénies :

$$\Pi_m A \xrightarrow{\alpha_m} A_m \xrightarrow{\tilde{\rho}_{m,n|A_m}} A_n \xrightarrow{\rho_n|A_n} A.$$

Il faut donc que $\tilde{\rho}_{m,n|A_m}$ soit également purement inséparable, et c'est donc un isomorphisme. Cela prouve que pour tout $m \geq n$, A_n est isomorphe à A_m , qui est définie au-dessus de k^{p^m} ; et comme dans le théorème 4, on en déduit que A_n est isomorphe à une variété abélienne définie sur k^{p^∞} . Comme $\rho_n|A_n$ est une isogénie de A_n sur A , A est isogène à une variété abélienne définie sur un corps fini, ce qui est impossible. \square

Références

- [Be05] Franck Benoist. *Théorie des modèles des corps munis d'une dérivation de Hasse*. Thèse, Paris, 2005.

- [BlKr05] Thomas Blossier and Krzysztof Krupiński. A special thin type. *Illinois Journal of Mathematics* 49, 281–290, 2005.
- [Bo98] Elisabeth Bouscaren (editor). *Model theory and algebraic geometry : An introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture*. Lecture Notes in Mathematics 1696, Springer, Berlin, 1998.
- [BoDe01] Elisabeth Bouscaren and Françoise Delon. Groups definable in separably closed fields. *Transactions of the American Mathematical Society* 354, 945-966, 2001.
- [BoDe02] Elisabeth Bouscaren and Françoise Delon. Minimal groups in separably closed fields. *Journal of Symbolic Logic*, 67, 239-259, 2002.
- [Bu92] Alexandru Buium. *Algebraic differential groups of finite dimension*. Lecture Notes in Mathematics 1506, Springer, Berlin, 1992.
- [De88] Françoise Delon. *Idéaux et types sur les corps séparablement clos*. Supplément au bulletin de la Société Mathématique de France, Tome 116, Mémoire 33, 1988.
- [De98] Françoise Delon. Separably closed fields. In *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.
- [HaSc37] 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.
- [Hr96] Ehud Hrushovski. The Mordell-Lang conjecture for function fields. *Journal of the American Mathematical Society* 9, 667-690, 1996.
- [HrZi96] Ehud Hrushovski and Boris Zil'ber. Zariski geometries. *Journal of the American Mathematical Society* 9, 1-56, 1996.
- [MuFo82] David Mumford and John Fogarty. *Geometric Invariant Theory*. Second enlarged edition, Springer-Verlag, Berlin Heidelberg, 1982.
- [MeWo95] Margit Messmer and Carol Wood. Separably closed fields with higher derivations. *Journal of Symbolic Logic* 60, 898-910, 1995.
- [Oo01] Frans Oort. Newton polygon strata in the moduli space of abelian varieties. In *Moduli of abelian varieties*. Editors C. Faber, G. van der Geer, F. Oort. Progress Mathematics 195, Birkhäuser Verlag, 2001.
- [Oo04] Frans Oort. Foliations in moduli spaces of abelian varieties. *Journal of American Mathematical Society* 17, 267-296, 2004.
- [PiZi03] Anand Pillay and Martin Ziegler. Jet spaces of varieties over differential and difference fields. *Selecta Mathematica, New Series*, 9, 579-599, 2003.
- [Ro56] Maxwell Rosenlicht. Some basic theorems on algebraic groups. *American Journal of Mathematics* 78, 401-443, 1956.
- [We55] André Weil. On algebraic groups of transformations. *American Journal of Mathematics* 77, 355-391, 1955.
- [Zi03] Martin Ziegler. Separably closed fields with Hasse derivations. *Journal of Symbolic Logic* 68, 311-318, 2003.