Journal of the Inst. of Math. Jussieu (2008) **7**(4), 623–639 © Cambridge University Press 623
doi:10.1017/S1474748008000145 Printed in the United Kingdom

QUESTIONS DE CORPS DE DÉFINITION POUR LES VARIÉTÉS ABÉLIENNES EN CARACTÉRISTIQUE POSITIVE

FRANCK BENOIST[1]* AND FRANÇOISE DELON[2]

[1]*Abteilung für mathemaische Logik, Universität Freiburg, Eckerstrasse 1, Freiburg D-79104, Germany* (benoist@logique.jussieu.fr)
[2]*Equipe de Logique, UFR de Mathématiques—Case 7012, Université Paris 7—Denis Diderot, 2, place Jussieu, 75251 Paris cedex 05, France* (delon@logique.jussieu.fr)

(Reçu le 10 février 2007 ; révisé le 7 septembre 2007 ; accepté le 5 décembre 2007)

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 semi-abéliennes en caractéristique positive, dont les questions de descente, considérées sous l'angle de la théorie des modèles.

Abstract 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 semi-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.

Mots clés : variété abélienne ; très mince ; dérivation de Hasse ; corps de définition ; points rationnels

Keywords: abelian variety; very thin; Hasse derivation; field of definition; rational points

AMS 2000 *Mathematics subject classification:* Primary 03C45; 03C60; 12H05; 14L99

1. Introduction

Dans [**11**], 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 [**3**] par exemple) ; en voici un énoncé très général en caractéristique positive.

* Present address: School of Mathematics, University of Leeds, Leeds LS2 9JT, UK.

Théorème 1.1 (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.

Dans l'énoncé suivant, une certaine dichotomie apparaît plus clairement.

Théorème 1.2. *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 [**12**]). 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 $p^\infty A(K) := \bigcap_{n\geqslant 0} p^n A(K)$ (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 [**8**]. Nous adopterons ici principalement le langage d'une dérivation de Hasse, introduit sous cette forme par Ziegler dans [**23**].

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 « foncteurs lambda » de [**4**], que l'on caractérisera au moyen des 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 successives. Dans la partie 4, on montre qu'une variété abélienne A est isogène à une variété abélienne définie sur $K^{p^\infty} := \bigcap_{n\geqslant 0} K^{p^n}$ 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 [**20**]. 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 [**2**].

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 2.1. 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 les axiomes suivants.

- $D_0 = \mathrm{id}$.
- 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
$$C_K^\infty := \{x \in K;\ \forall i \geqslant 1,\ D_i(x) = 0\}$$
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
$$\{x \in K; \forall i < p^n,\ D_i(x) = 0\} = K^{p^n}$$
et
$$C_K^\infty = \bigcap_{n\geqslant 0} K^{p^n} =: K^{p^\infty}.$$
- Pour $X = (X_1, \ldots, X_m)$ un m-uplet de variables, on note $K\{X\}$ *l'algèbre des D-polynômes en* X, c'est-à-dire :
$$K\{X\} := K[d_iX]_{i\in\mathbb{N}},$$
où $d_iX := (d_iX_1, \ldots, d_iX_m)$ et où les d_iX_j, pour $i \in \mathbb{N}$ et $j = 1, \ldots, m$, sont des indéterminées indépendantes. On la munit d'une extension de la dérivation de Hasse sur K en posant
$$D_j(d_iX) = \binom{i+j}{i} d_{i+j}X.$$

https://doi.org/10.1017/S1474748008000145 Published online by Cambridge University Press

La théorie que l'on utilisera a été exhibée par Ziegler (et précédemment par Messmer et Wood, dans un langage un peu différent, voir [**15**]).

Théorème 2.2 (Ziegler [23]). *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, c'est-à-dire $\forall x \exists y (D_1(x) = 0 \to x = y^p)$;*
- *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 $k \models \mathrm{HF}_p$, 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.

- 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 $\mathbb{F}_p(t)^{\mathrm{sep}}$ (voir [**10**]). Alors $K := (\mathbb{F}_p(t)^{\mathrm{sep}}, D)$ est un modèle de CHF_p, avec $C_K^\infty = \mathbb{F}_p^{\mathrm{alg}}$: plus généralement, il est bien connu que $C(t)$ est strict dès que C est un corps parfait et que la dérivation de Hasse est définie comme précédemment sur t, ainsi que $C(t)^{\mathrm{sep}}$. Et on obtient alors que $C_K^\infty = K^{p^\infty} = \mathbb{F}_p^{\mathrm{alg}}$.

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

  Démonstration. L'exemple précédent permet de construire une dérivation de Hasse sur $k(t_1)^{\mathrm{sep}}$, de corps de constantes absolues k. Puis, en ajoutant $(t_2, \dots, t_n)$ une réalisation du $(n-1)$-type générique au-dessus de $k(t_1)^{\mathrm{sep}}$ (ce type correspondant à l'idéal nul de $k(t_1)^{\mathrm{sep}}\{T_2, \dots, T_n\}$), 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 [**7**] pour une preuve dans un langage différent, exposé ci-dessous). □

Le langage des p-composantes

Après avoir remarqué (lemme 2.1 de [**23**]) qu'un modèle de CHF_p est un corps séparablement clos de degré d'imperfection 1, on utilisera parfois le langage donné dans [**8**], que l'on rappelle ici.

Pour $K \models \mathrm{CHF}_p$, 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 $\lambda_n = (\lambda_{n,i})_{0 \leqslant i < p^n}$ la suite de fonctions de K dans K, définissables dans le pur langage des corps avec paramètre b, telles que tout $x \in K$ s'écrive

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

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

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

Or la matrice $(D_i(b^j))_{0 \leqslant i,j < p^n}$ est inversible, du fait du lemme suivant (voir le théorème 1 de [**9**]).

Lemme 2.3. *Des éléments $x_0, \dots, x_{p^n-1}$ de K sont linéairement indépendants au-dessus de K^{p^n} si et seulement si le Wronskien*

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

est non-nul.

En d'autres termes, 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 semi-abéliennes

Etant donnée une variété algébrique V définie sur un corps K, on peut écrire naturellement l'ensemble des points K-rationnels de V 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

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

https://doi.org/10.1017/S1474748008000145 Published online by Cambridge University Press

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 se place désormais dans un modèle K de CHF_p, avec une p-base $\{b\}$ de K fixée et les fonctions λ_n correspondantes (voir la partie 2).

Il est classique de décrire les sous-variétés D-algébriques de V par l'intermédiaire d'objets purement algébriques. Dans le cas d'une caractéristique $p > 0$, on peut utiliser pour cela un système projectif de variétés algébriques

$$(\rho_{m,n} : \Lambda_m V \to \Lambda_n V)_{m \geqslant n \geqslant 0}$$

construit dans [**4**], avec $\Lambda_0 V = V$ et $\rho_{0,0} = \mathrm{id}_V$, et des applications définissables $\lambda_n : V(K) \to (\Lambda_n V)(K)$, bijectives, de réciproque $\rho_{n,0}|_{(\Lambda_n V)(K)}$. Ces applications λ_n coïncident localement avec les fonctions λ_n déjà définies sur l'espace affine.

Il est montré (voir [**4**, Proposition 1.4]) que Λ_n est un foncteur de la catégorie des variétés algébriques définies sur K dans elle-même ; ce foncteur induit un foncteur sur la catégorie des groupes algébriques définis sur K, et les applications $\rho_{m,n}$, λ_n sont alors des homomorphismes.

Une sous-variété D-algébrique W de V est alors déterminée par la suite

$$W_n(K) := \{x \in (\Lambda_n V)(K);\ \rho_{n,0}(x) \in W(K)\}, \quad n \geqslant 0,$$

avec la caractérisation

$$W(K) = \{x \in V(K) \mid \forall n \geqslant 0,\ \lambda_n(x) \in W_n(K)\}.$$

Nous donnons ci-dessous une autre caractérisation de ces foncteurs Λ_n, en utilisant la notion de restriction de Weil.

Définition 3.1. Soit V une variété algébrique définie sur K. On appelle $\tilde{\rho}_n : \Pi_n V \to V$ 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 $f : W \to V$ défini sur K, il existe un unique morphisme g défini sur K^{p^n} tel que le diagramme suivant commute

$$\begin{tikzcd} W \arrow[rr, "f"] \arrow[dr, "g"'] & & V \\ & \Pi_n V \arrow[ur, "\tilde{\rho}_n"'] & \end{tikzcd}$$

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

https://doi.org/10.1017/S1474748008000145 Published online by Cambridge University Press

Proposition 3.2 (Benoist [1, Proposition III.8]). *Soit V une variété algébrique définie sur K. Alors $((\mathrm{Fr}^n \circ \Lambda_n)V, \rho_{n,0} \circ \mathrm{Fr}^{-n})$ est une restriction de Weil pour V de K à K^{p^n}.*

Démonstration. Tout d'abord, $\Pi_n V := (\mathrm{Fr}^n \circ \Lambda_n)V$ est bien définie sur K^{p^n} puisque $\Lambda_n V$ est définie sur K, et nous devons aussi montrer que l'application $\tilde{\rho}_n := \rho_{n,0} \circ \mathrm{Fr}^{-n}$ est rationnelle, surjective et définie sur K. Rappelons pour cela (voir [**4**]) que cette application est donnée localement par

$$(x_{i,j})_{\substack{1\leqslant i\leqslant d\\ 0\leqslant j<p^n}} \mapsto \left(\sum_{j=0}^{p^n-1} x_{i,j} b^j\right)_{1\leqslant i\leqslant d}.$$

Elle est clairement définie sur K, et génériquement surjective puisque $\tilde{\rho}_n$ réalise une bijection entre $(\Pi_n V)(K^{p^n})$ et $V(K)$, K étant séparablement clos.

On doit encore montrer que $\tilde{\rho}_n$ est séparable. Considérons une composante irréductible F d'un ouvert affine de $\Pi_n V$, et G son image par $\tilde{\rho}_n$. Soit $I(G)$ l'idéal premier séparable de G dans $K[X_1, \ldots, X_d]$. D'après le lemme 2.1 de [**4**], il existe un *idéal de type Q* de $K[X_{1\infty}, \ldots, X_{d\infty}]$ (l'algèbre de polynômes décrivant les relations algébriques entre les λ-composantes), minimal tel que $Q \cap K[X_1, \ldots, X_d] = I(G)$. Considérons, pour une extension élémentaire assez saturée L de K, un point $y \in G(L)$ réalisant le type associé à Q. D'autre part, puisque $\lambda_n^{p^n}(V(K))$ est Zariski dense dans $\Pi_n V$, on peut considérer $x \in G(L)$ tel que $\lambda_n^{p^n}(x)$ soit générique dans F au-dessus de K. L'idéal $I_{x/K}$ (correspondant au type de x sur K dans $K[X_{1\infty}, \ldots, X_{d\infty}]$) a alors $I(G)$ pour intersection avec $K[X_1, \ldots, X_d]$, il contient donc Q. En particulier, on a, dans $K[X_{i,j};\ 1 \leqslant i \leqslant d,\ 0 \leqslant j < p^n]$, $I(\lambda_n(y)/K) \subseteq I(\lambda_n(x)/K)$, et ainsi $I(\lambda_n^{p^n}(y)) = I(F)$, l'idéal de la composante irréductible F. Or, d'après la construction de Q (voir la preuve du lemme 2.1 de [**4**]), si $y_1, \ldots, y_r$ désigne une base de transcendance séparante de $y = (y_1, \ldots, y_n)$ sur K, alors les $\lambda_n(y_i)$ sont algébriquement indépendants au-dessus de $K(y)$, pour $i = 1, \ldots, r$; et pour $i = r+1, \ldots, n$, $\lambda_n^{p^n}(y_i) \in K(\lambda_n^{p^n}(y_1), \ldots, \lambda_n^{p^n}(y_r), y_{r+1}, \ldots, y_n)$. On a donc que $K(\lambda_n^{p^n}(y))$ est une extension purement transcendante, donc séparable, de $K(y)$; comme $\lambda_n^{p^n}(y)$ est générique dans F et que $\tilde{\rho}_n(\lambda_n^{p^n}(y)) = y$, cela signifie que $\tilde{\rho}_n$ est séparable, donc surjective.

Montrons finalement que $(\Pi_n V, \tilde{\rho}_n)$ satisfait la propriété universelle considérée. On se donne pour cela un morphisme $f : W \to V$, défini sur K, pour une variété algébrique W définie sur K^{p^n}. Puisque K^{p^n} est séparablement clos, il suffira, pour déterminer le morphisme g recherché, de le considérer sur les points K^{p^n}-rationnels. Or, puisque $\tilde{\rho}_n|_{(\Pi_n V)(K^{p^n})}$ est bijective, g est nécessairement donné par

$$g = \lambda_n^{p^n} \circ f : W(K^{p^n}) \to (\Pi_n V)(K^{p^n}).$$

Il 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 donné par une fraction rationnelle P/Q à coefficients dans K. Ecrivons $P(x)/Q(x) = N(x)/Q(x)^{p^n}$ et notons

https://doi.org/10.1017/S1474748008000145 Published online by Cambridge University Press

$\lambda_{n,i}^{p^n}(N)$ le polynôme à coefficients dans K^{p^n} obtenu en appliquant $\lambda_{n,i}^{p^n}$ aux coefficients de N. On a alors, pour $x \in U(K^{p^n})$,

$$\lambda_{n,i}^{p^n}(f(x)) = \frac{\lambda_{n,i}^{p^n}(N)(x)}{Q(x)^{p^n}},$$

c'est-à-dire que g est donné localement par une fraction rationnelle à coefficients dans K^{p^n}. $\square$

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

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 :

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

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 [**5**]). Décrivons-le par l'intermédiaire du système projectif des $\Pi_n A$.

Pour tout n, l'isogénie Frobenius à la puissance n, $\mathrm{Fr}^n : A \to \mathrm{Fr}^n A$, admet une isogénie duale, appelée *Verschiebung*, et notée $V_n : \mathrm{Fr}^n A \to A$. Elle vérifie $V_n \circ \mathrm{Fr}^n = [p^n]_A$ et $\mathrm{Fr}^n \circ V_n = [p^n]_{\mathrm{Fr}^n A}$ (où, pour un entier m, $[m]$ désigne la multiplication par m dans le groupe algébrique considéré). Puisque $\mathrm{Fr}^n A$ 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 :

$$\begin{tikzcd} \mathrm{Fr}^n A \arrow[rr, "V_n"] \arrow[dr, "\alpha_n"'] & & A \\ & \Pi_n A \arrow[ur, "\tilde{\rho}_n"'] & \end{tikzcd}$$

Par fonctorialité du Frobenius et de la restriction de Weil, α_n est un homomorphisme de groupes algébriques. Notons A_n l'image de l'homomomorphisme α_n. C'est un sous-groupe algébrique de $\Pi_n A$, défini sur K^{p^n}. Les A_n décrivent alors $p^\infty A(K)$, comme le montre le lemme suivant.

Lemme 3.3.

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

Démonstration. 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

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

Comme $\alpha_n(\mathrm{Fr}^n(x_n)) \in A_n(K^{p^n})$, on a bien $x \in \tilde{\rho}_n(A_n(K^{p^n}))$.

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

Définition 3.4. 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 [**11**]).

Lemme 3.5. *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.*

Démonstration. Tout d'abord, on a vu que $k(\{a\}) = k(\lambda_n(a)^{p^n})_{n \geqslant 0}$. Ensuite, pour tout $n \geqslant 0$, on trouve $a_n \in A(K)$ tel que $a = [p^n]a_n = V_n \circ \mathrm{Fr}^n(a_n)$. Comme V_n est une isogénie, $k(\mathrm{Fr}^n(a_n))$ est une extension algébrique de $k(a)$. Or, $\alpha_n(\mathrm{Fr}^n(a_n)) \in k(\mathrm{Fr}^n(a_n))$, et on a vu que $\tilde{\rho}_n \circ \alpha_n \circ \mathrm{Fr}^n(a_n) = [p^n]a_n = a$ implique que $\alpha_n \circ \mathrm{Fr}^n(a_n) = \lambda_n(a)^{p^n}$: 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 4.1. 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 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 [**6**], 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 [**1**], il est montré comment généraliser cette notion à la caractéristique positive, et l'équivalence entre la catégorie des groupes algébriques connexes munis d'une D-structure et celle des groupes infiniment définissables connexes rationnellement minces est établie. Nous allons ici reprouver la partie de ce résultat qui nous intéresse.

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

Démonstration. 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 3.5, 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 classique de Weil, voir [**22**]). 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 [**21**]), 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 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 $k(\{b\}) = k(\{a\}) = k(b)$. □

Proposition 4.3. *Supposons que le point générique a de $p^\infty A(K)$ vérifie $k(\{a\}) = k(a)$. Alors, pour tout $n \geqslant 0$, il existe une section s_n à la projection $\tilde{\rho}_n : \Pi_n A \to A$, qui coïncide avec $\lambda_n^{p^n}$ sur $p^\infty A(K)$.*

Démonstration. Soit a le point générique de $p^\infty A(K)$. Par hypothèse, et en utilisant les résultats de la partie 2, il existe une fraction rationnelle s_n, à coefficients dans k, telle que

$$\lambda_n^{p^n}(a) = s_n(a).$$

Les fonctions s_n sont donc des fonctions rationnelles partielles, de $p^\infty A(K)$ dans $\Pi_n A(K)$, qui sont des homomorphismes par définition de la loi de groupe de $\Pi_n A$, et qui vérifient $\tilde{\rho}_n \circ s_n = \mathrm{id}$ sur $p^\infty A(K)$. En prolongeant les fonctions s_n en des homomorphismes de groupes algébriques de A dans $\Pi_n A$ (par le même argument de densité que précédemment), on obtient les sections recherchées. □

On peut maintenant prouver le résultat de descente suivant. L'argument pour le passage des différents k^{p^n} 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 m* par un *espace de modules* approprié ; on pourra trouver les propriétés de cet objet dans [**16**].

Théorème 4.4. *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^∞.*

Démonstration. En utilisant la proposition 4.2, 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 4.3 nous donne alors, pour tout n, une section $s_n : B \to \Pi_n B$, que l'on va utiliser pour montrer que B est isomorphe à une variété abélienne définie sur k^{p^n}.

Dans la partie 3, on a donné la caractérisation suivante :

$$p^\infty B(K) = \{x \in B(K);\ \forall n \geqslant 0,\ \lambda_n(x)^{p^n} \in B_n(K^{p^n})\},$$

où, pour tout n, B_n est un sous-groupe algébrique de $\Pi_n B$ défini sur K^{p^n}. On montre alors que B est isomorphe à B_n : on sait déjà que $\tilde{\rho}_n \circ s_n = \mathrm{id}_B$, et, pour $x \in p^\infty B(K)$, $s_n \circ \tilde{\rho}_n(s_n(x)) = s_n \circ \tilde{\rho}_n(\lambda_n(x)^{p^n}) = s_n(x)$, donc $s_n \circ \tilde{\rho}_n = \mathrm{id}$ sur l'image de $p^\infty B(K)$ par s_n, et donc sur $s_n(B)$ par densité. Or $s_n(B) = B_n$ (car pour $x \in p^\infty B(K)$ et $x_n \in B(K)$ tels que $[p^n]x_n = x$, on a vu dans la preuve du lemme 3.5 que $s_n(x) = \lambda_n(x)^{p^n} = \alpha_n(\mathrm{Fr}^n(x_n))$, et donc $s_n(p^\infty B(K))$ est dense dans l'image de $\mathrm{Fr}^n B$ par α_n, c'est-à-dire B_n), et on a donc obtenu un isomorphisme de B sur B_n.

Pour en déduire que B est isomorphe à une variété abélienne définie sur k^{p^∞}, on utilise l'espace de modules $\mathcal{A}_{g,d,m}$ des variétés abéliennes de dimension $g = \dim(B)$, munie d'une polarisation de degré d^2 et d'une structure de niveau m, pour un m premier à p et suffisamment grand pour que cet espace de modules existe (voir [**16**]).

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

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 [**5**]), 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 1.1, 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 [**20**] ; 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 5.1. 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 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 [**20**], 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.

Lemme 5.2 (Benoist [1, Proposition IV.16]). *Soit A une variété semi-abélienne définie sur k. Avec les notations de la partie 3, on considère, pour $m \geqslant n$, l'homomorphisme $\tilde\rho_{m,n} := \mathrm{Fr}^n \circ \rho_{m,n} \circ \mathrm{Fr}^{-m}$ de $\varPi_m A$ dans $\varPi_n A$. Alors $\tilde\rho_{m,n|_{A_m}}$ est une isogénie de A_m dans A_n.*

Démonstration. Comme dans les parties 3 et 4, α_n désigne l'homomorphisme obtenu dans la factorisation de V_n. On a alors la situation suivante

$$\begin{tikzcd}
\mathrm{Fr}^m A \arrow[r, "V'_{m-n}"] & \mathrm{Fr}^n A \arrow[rr, "V_n"] \arrow[dr, "\alpha_n"'] & & A \\
& & \varPi_n A \arrow[ur, "\tilde\rho_n"'] &
\end{tikzcd}$$

où V'_{m-n} désigne l'isogénie duale de $\mathrm{Fr}^{m-n} : \mathrm{Fr}^n A \to \mathrm{Fr}^m A$. On sait (voir [**13**] par exemple) que $V_m = V_n \circ V'_{m-n}$, et d'autre part $V_m = \tilde\rho_m \circ \alpha_m = \tilde\rho_n \circ \tilde\rho_{m,n} \circ \alpha_m$. Cela donne deux écritures de l'homomorphisme $V_m \circ \mathrm{Fr}^{m-n} : \mathrm{Fr}^n A \to A$:

$$\tilde\rho_n \circ \tilde\rho_{m,n} \circ \alpha_m \circ \mathrm{Fr}^{m-n} = \tilde\rho_n \circ \alpha_n \circ [p^{m-n}]_{|\mathrm{Fr}^n A}.$$

Puisque les homomorphismes $\tilde\rho_{m,n} \circ \alpha_m \circ \mathrm{Fr}^{m-n}$ et $\alpha_n \circ [p^{m-n}]_{|\mathrm{Fr}^n A}$ sont définis sur k^{p^n}, ils sont égaux d'après l'unicité de la factorisation via $\varPi_n A$. Et puisque l'image de $[p^{m-n}]_{|\mathrm{Fr}^n A}$ est dense, on obtient que $\tilde\rho_{m,n} \circ \alpha_m \circ \mathrm{Fr}^{m-n}(\mathrm{Fr}^n A) = \alpha_n(\mathrm{Fr}^n A)$, c'est-à-dire $\tilde\rho_{m,n}(A_m) = A_n$.

Il suffit donc maintenant de prouver que A_m et A_n ont même dimension pour prouver que $\tilde\rho_{m,n}$ réalise une isogénie. Or on sait que α_n, comme V_n, a un noyau fini et donc $\dim(A_n) = \dim(\mathrm{Fr}^n A) = \dim(A)$, et de même pour A_m. □

https://doi.org/10.1017/S1474748008000145 Published online by Cambridge University Press

Proposition 5.3. *Le groupe* $p^\infty A(K)$ *est séparablement mince si et seulement s'il existe* $n \geqslant 0$ *tel que* $\tilde\rho_{m,n|_{A_m}}$ *est séparable pour tout* $m \geqslant n$.

Démonstration. Tout d'abord, comme dans les parties 3 et 4, 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 $b_m := \lambda_m(a)^{p^m} = \alpha_m \circ \mathrm{Fr}^m(a_m)$ qui est générique dans A_m, et $\tilde\rho_{m,n|_{A_m}}(b_m) = b_n$ pour $m \geqslant n$.

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

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

Nous cherchons maintenant à construire une variété abélienne simple A au-dessus de K qui ne soit pas séparablement mince, ce qui siginifie pour nous par définition que $p^\infty A(K)$ n'est pas séparablement mince. Le principe du paramétrage des courbes elliptiques par leur j-invariant (deux courbes sont isomorphes si et seulement si elles ont même invariant) ne s'étend pas directement en dimension supérieure, au sens où il n'y a pas de structure de variété raisonnable sur l'ensemble des paramètres décrivant les variétés abéliennes « nues » de dimension fixée, quotienté par la relation d'équivalence correspondant à l'isomorphisme entre variétés, voir [**16**, Chapitre 5, § 1]. On sait, d'après [**16**, Chapitre 7], qu'il s'étend si l'on considère les variétés abéliennes (de dimension fixée g), munie d'une structure additionnelle, polarisation de degré fixée d^2 et structure de niveau fixé n. Dans la preuve du théorème 4.4, nous avons utilisé l'existence de l'espace de modules correspondant, $\mathcal{A}_{g,d,n}$ et son uniformité par rapport aux corps $k, k^p, k^{p^2}, \dots$ lorsque n est assez grand [**16**, 7.9]. Nous allons maintenant utiliser l'espace de modules $\mathcal{A}_{g,1} := \mathcal{A}_{g,1,1}$ des variétés principalement polarisées, c'est à dire munies d'un isomorphisme vers leur variété duale. Cette paramétrisation n'existe qu'au-dessus d'un corps algébriquement clos [**16**, 7.10] mais cela nous suffira car il s'agit ici de construire un exemple particulier. Nous identifions par la suite une variété abélienne principalement polarisée de dimension g et le point de $\mathcal{A}_{g,1}$ qui la représente.

Pour une variété abélienne A définie sur un corps quelconque k et un entier m, soit $A[m] := \{x \in k^{\mathrm{alg}} \mid m \cdot a = 0\}$, et pour un nombre premier q, la limite projective $t_q(A)$ des $A[q^r]$, 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 g est la dimension de A, $t_q(A)$ est isomorphe à $\mathbb{Z}_q^{2g}$. Il est bien connu que la situation est plus compliquée pour $q = p$: la torsion d'ordre p est de la forme $(\mathbb{Z}/p\mathbb{Z})^n$ pour un certain entier $n \leqslant g$, appelé le p-rang de la variété. Lorsqu'il est strictement inférieur à g, cet entier n peut être raffiné de la façon suivante. D'une part l'action du Frobenius permet d'enrichir la structure de $\mathbb{Z}_p$-module de $t_p(A)$ en un module sur un anneau plus gros. D'autre part on considère au lieu de la torsion naïve la torsion schématique, en particulier la p-torsion redevient ainsi un objet de rang $2g$. Cela permet d'associer à la variété un « module de Dieudonné », de rang $2g$, qui, à isogénie près, se décompose en une somme directe de modules indécomposables [**14**, Chapitre II]. Ou

https://doi.org/10.1017/S1474748008000145 Published online by Cambridge University Press

encore, graphiquement, est associé à A un « polygone de Newton », ayant les propriétés suivantes [**17**] :

- dans le plan cartésien réel, c'est une ligne convexe de segments de droite à sommets entiers, commençant en $(0,0)$ et finissant en $(2g,g)$;
- 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'ensemble des polygones de Newton est partiellement ordonné par leurs positions dans le plan : $P \geqslant Q$ si tout point de P est au-dessus de Q, au sens large, P et Q peuvent avoir des sommets ou des segments communs.

Il y a pour cet ordre un polygone maximal, composé d'un segment de pente $\frac{1}{2}$. C'est le polygone de Newton des variétés abéliennes dites *supersingulières*, c'est à dire isogènes sur k^{alg} à un produit de courbes elliptiques supersingulières. Une courbe elliptique supersingulière est elle-même par définition une courbe sur laquelle la multiplication $[p]$ est de degré d'inséparabilité maximal, p^2. Une courbe supersingulière est définie sur $\mathbb{F}_p^{\mathrm{alg}}$, un produit de telles courbes également (à isomorphisme près) et est donc rationnellement mince.

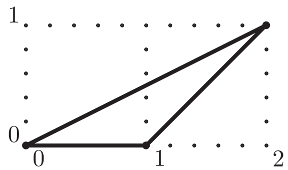
Il y a un polygone minimal, composé d'un segment $(g,0)$ et d'un segment (g,g), qui correspond à des variétés *ordinaires*, c'est à dire de p-rang maximal, g. Dans ce cas la multiplication par $[p]$ est de degré d'inséparabilité minimal p^g, la Verschiebung V_1 est séparable, ainsi que toutes les V_n, et la proposition 5.3 s'applique : une variété ordinaire est toujours séparablement mince [**20**, 6.4].

Vont nous intéresser particulièrement les variétés dont le polygone de Newton ne contient aucun segment horizontal, ce sont les variétés de p-rang nul, ou encore celles où $[p]$ est de degré d'inséparabilité maximal p^{2g}, c'est à dire purement inséparable.

Dans l'espace des modules $\mathcal{A}_{g,1}$ des variétés abéliennes principalement polarisées, la situation est particulièrement simple, voir [**18**]. Chaque polygone de Newton P définit un fermé dans l'espace des modules, au sens suivant : les variétés ayant un polygone de Newton situé au-dessus de P, forment un fermé $V_P(\mathcal{A}_{g,1})$. Ce fermé n'est pas nécéssairement irréductible mais toutes ses composantes irréductibles ont même dimension, calculable par un moyen combinatoire simple. L'ensemble des variétés ayant exactement P pour polygone de Newton sera désigné par $V_P^{\mathrm{o}}(\mathcal{A}_{g,1})$.

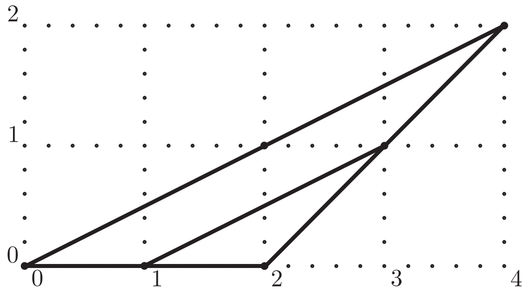
Notre but est de trouver une variété abélienne simple, de p-rang nul, qui n'est pas isogène à une variété abélienne définie sur $\mathbb{F}_p^{\mathrm{alg}}$.

Regardons le cas des courbes elliptiques :



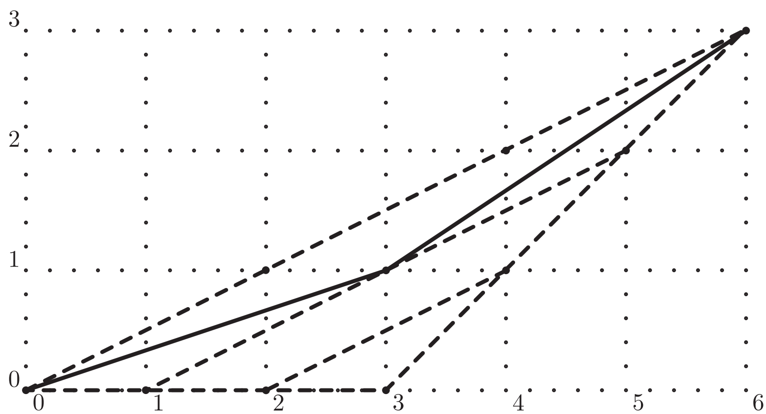
On trouve deux polygones de Newton possibles, celui du bas correspond à des courbes ordinaires, l'autre à des courbes supersingulières définies sur $\mathbb{F}_p^{\mathrm{alg}}$.

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 $\mathbb{F}_p^{\mathrm{alg}}$, à isogénie près.

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



Le polygone de Newton P_0, marqué en trait plein, est le seul qui corresponde 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 $\mathbb{F}_p$). Elle n'est pas non plus isogène à une telle variété. En effet, si une variété définie sur un corps fini contient dans sa « feuille d'isogénie » un point générique d'une composante irréductible de $V_{P_0}^{\circ}(\mathcal{A}_{3,1})$, elle les contient tous, ce qui impose à cette feuille une dimension

https://doi.org/10.1017/S1474748008000145 Published online by Cambridge University Press

supérieure ou égale à 3. Or la dimension d'une feuille d'isogénie de $V_Q^\circ(\mathcal{A}_{g,1})$ est inférieure à la dimension de $V_Q(\mathcal{A}_{g,1})$ dès que Q n'est pas le polygone de pente constante $\frac{1}{2}$ [**19**, 5.7 et 5.12].

Fixons maintenant un modèle k de CHF_p contenant a, muni d'une dérivation de Hasse telle que $C_k^\infty = \mathbb{F}_p^{\mathrm{alg}}$ (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^∞} ».

Proposition 5.4. *Pour tout point a de dimension maximale dans $V_{P_0}^\circ(\mathcal{A}_{3,1})(k)$, la variété abélienne A sur k paramétrée par a n'est pas séparablement mince.*

Démonstration. Puisque le p-rang de A est nul, la multiplication par p^n dans A, $[p^n] = V_n \circ \mathrm{Fr}^n$, est purement inséparable pour tout n (son noyau est trivial dans $A(k^{\mathrm{alg}})$). Les isogénies V_n sont donc elles aussi purement inséparables.

Supposons A séparablement mince. D'après la caractérisation de la proposition 5.3, il existe alors $n \geqslant 0$ tel que l'isogénie $\tilde{\rho}_{m,n|A_m}$ soit séparable pour tout $m \geqslant n$. Or, pour $m \geqslant n$, on peut décomposer l'isogénie purement inséparable V_m en les isogénies suivantes :

$$\mathrm{Fr}^m A \xrightarrow{\alpha_m} A_m \xrightarrow{\tilde{\rho}_{m,n|A_m}} A_n \xrightarrow{\rho_{n|A_n}} A.$$

Il en résulte que $\tilde{\rho}_{m,n|A_m}$ est également purement inséparable, c'est donc un isomorphisme. Cela prouve que, pour tout $m \geqslant n$, A_n est isomorphe à A_m, qui est définie au-dessus de k^{p^m} ; on en déduit de la même façon que dans la preuve du théorème 4.4 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. $\square$

Remerciements. Franck Benoist est financé par une bourse post-doctorale Modnet (MRTN-CT-2004-512234).

Références

1. F. Benoist, Théorie des modèles des corps munis d'une dérivation de Hasse, Thèse, Paris (2005).
2. T. Blossier and K. Krupiński, A special thin type, *Illinois J. Math.* **49** (2005), 281–290.
3. E. Bouscaren (ed.), *Model theory and algebraic geometry: an introduction to E. Hrushovski's proof of the geometric Mordell–Lang conjecture*, Lecture Notes in Mathematics, Volume 1696 (Springer, 1998).
4. E. Bouscaren and F. Delon, Groups definable in separably closed fields, *Trans. Am. Math. Soc.* **354** (2001), 945–966.
5. E. Bouscaren and F. Delon, Minimal groups in separably closed fields, *J. Symb. Logic* **67** (2002), 239–259.
6. A. Buium, *Algebraic differential groups of finite dimension*, Lecture Notes in Mathematics, Volume 1506 (Springer, 1992).
7. F. Delon, *Idéaux et types sur les corps séparablement clos*, Supplément au *Bulletin de la Société Mathématique de France*, Tome 116, Mémoire 33 (1988).

8. F. Delon, Separably closed fields, in *Model theory and algebraic geometry: an introduction to E. Hrushovski's proof of the geometric Mordell–Lang conjecture* (ed. E. Bouscaren), Lecture Notes in Mathematics, Volume 1696 (Springer, 1998).
9. A. García and J. F. Voloch, Wronskians and linear independence in fields of prime characteristic, *Manuscr. Math.* **59** (1987), 457–469.
10. H. Hasse and F. K. Schmidt, Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionkörper mit einer Unbestimmten, *J. Reine Angew. Math.* **177** (1937), 215–237.
11. E. Hrushovski, The Mordell–Lang conjecture for function fields, *J. Am. Math. Soc.* **9** (1996), 667–690.
12. E. Hrushovski and B. Zil'ber, Zariski geometries, *J. Am. Math. Soc.* **9** (1996), 1–56.
13. S. Lang, *Abelian varieties* (Interscience, New York, 1959).
14. Y. I. Manin, The theory of commutative formal groups over fields of finite characteristic, *Russ. Math. Surv.* **18** (1963), 1–83.
15. M. Messmer and C. Wood, Separably closed fields with higher derivations, *J. Symb. Logic* **60** (1995), 898–910.
16. D. Mumford and J. Fogarty, *Geometric Invariant Theory*, 2nd enlarged edn (Springer, 1982).
17. F. Oort, Newton polygons and formal groups: conjectures by Manin and Grotendieck, *Annals Math.* **152** (2000), 183–206.
18. F. Oort, Newton polygon strata in the moduli space of abelian varieties, in *Moduli of abelian varieties* (ed. C. Faber, G. van der Geer and F. Oort), Progress in Mathematics, Volume 195 (Birkhäuser, 2001).
19. F. Oort, Foliations in moduli spaces of abelian varieties, *J. Am. Math. Soc.* **17** (2004), 267–296.
20. A. Pillay and M. Ziegler, Jet spaces of varieties over differential and difference fields, *Selecta Math.* **9** (2003), 579–599.
21. M. Rosenlicht, Some basic theorems on algebraic groups, *Am. J. Math.* **78** (1956), 401–443.
22. A. Weil, On algebraic groups of transformations, *Am. J. Math.* **77** (1955), 355–391.
23. M. Ziegler, Separably closed fields with Hasse derivations, *J. Symb. Logic* **68** (2003), 311–318.

https://doi.org/10.1017/S1474748008000145 Published online by Cambridge University Press