Astérisque

ÉLISABETH BOUSCAREN

Théorie des modèles et conjecture de Manin-Mumford

Astérisque, tome 276 (2002), Séminaire Bourbaki,
exp. n° 870, p. 137-159

<http://www.numdam.org/item?id=SB_1999-2000__42__137_0>

© Société mathématique de France, 2002, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI
52e année, 1999-2000, nO 870, p. 137 à 159

Mars 2000

THÉORIE DES MODÈLES ET CONJECTURE DE MANIN-MUMFORD [d'après Ehud Hrushovski]

par **Élisabeth BOUSCAREN**

1. INTRODUCTION

Je vais présenter ici l'une des applications récentes de la théorie des modèles à la géométrie diophantienne, la nouvelle démonstration, due à E. Hrushovski ([Hr2]), de la conjecture de Manin-Mumford (généralisée) qui est basée sur l'étude, du point de vue de la théorie des modèles, des corps algébriquement clos munis d'un automorphisme.

THÉORÈME 1.1 (Conjecture de Manin-Mumford). — *Soit G un groupe algébrique commutatif connexe défini sur un corps de nombres k et X une sous-variété de G. Alors il y a un nombre fini de points de torsion de G, $a_1, \ldots, a_M$, et de sous-groupes algébriques de G, $G_1, \ldots, G_M$ tels que pour chaque i, $a_i + G_i$ est contenu dans X et*

$$X(k^{alg}) \cap Tor(G) = \bigcup_{i=1}^{M} a_i + Tor(G_i).$$

De plus on peut borner de façon effective le nombre M de translatés : il existe c, e deux constantes ne dépendant que d'invariants liés à G (et non à X) et du choix de deux premiers de bonne réduction pour G, tels que $M \leq c \deg(X)^e$.

En utilisant des méthodes de calcul assez grossières, on obtient que les constantes c et e sont doublement exponentielles.

La démonstration de Hrushovski passe par une première étape où il prend un premier de bonne réduction pour G, de caractéristique résiduelle p, et montre le résultat pour la torsion première à p, c'est-à-dire pour le sous-groupe $Tor_{p'}(G)$ des éléments de torsion de G dont l'ordre n'est pas divisible par p. On obtient dans ce cas que

$$X(k^{alg}) \cap Tor_{p'}(G) = \bigcup_{i=1}^{N} a_i + Tor_{p'}(G_i),$$

où il est facile de montrer directement que $N \leq a \deg(X)^b$, avec a doublement exponentiel (en la dimension de A, le degré de l'addition dans A et la cardinalité du corps résiduel) et b exponentiel en la dimension de A.

Le but de cet exposé, en présentant la démonstration de Hrushovski, est d'essayer d'expliquer pourquoi la théorie des modèles a quelque chose à dire sur ce type de questions et aussi de donner une idée des résultats qu'on montre et des outils qu'on développe en théorie des modèles.

Nous passerons donc rapidement sur les parties purement « géométrie algébrique » de la démonstration.

De même, la très brève présentation historique et bibliographique qui suit n'a, cela sera visible tout de suite, aucune prétention d'exhaustivité.

1.1. Petit historique et conjecture de Lang

La conjecture de Manin-Mumford originelle porte sur l'intersection d'une courbe avec les points de torsion d'une variété abélienne. Elle a été tout d'abord démontrée par M. Raynaud ([Ra1]), puis R. Coleman ([Col]) en a donné une autre démonstration par des méthodes très différentes ; Raynaud a ensuite ([Ra2]) démontré le résultat pour une sous-variété quelconque, puis M. Hindry ([Hi1]), en s'inspirant d'une idée de S. Lang ([La1]) pour le cas des courbes, a démontré le résultat général pour un groupe algébrique commutatif.

On trouve une autre approche de ces questions dans les travaux sur la conjecture de Bogomolov, on se contentera ici de renvoyer à l'exposé de A. Abbes sur le sujet dans le cadre de ce séminaire ([Ab]) et aux travaux récents de S. David et P. Philippon ([DaPh]).

En revanche, nous allons dire quelques mots de la conjecture de Lang (dite aussi conjecture de Mordell-Lang), énoncée par Lang dans [La1] et qui regroupe dans un cadre général la conjecture de Manin-Mumford et la conjecture de Mordell (voir aussi par exemple [La2]).

Nous l'énonçons ici pour la caractéristique zéro :

CONJECTURE DE LANG (ABSOLUE). — *Soient K un corps algébriquement clos de caractéristique zéro, A une variété abélienne définie sur K, X une sous-variété de A définie sur K et Γ un sous-groupe de $A(K)$ de rang fini. Alors il existe $\gamma_1, \ldots, \gamma_n \in \Gamma$ et $B_1, \ldots, B_n$ sous-variétés abéliennes de A tels que $\gamma_i + B_i \subset X$ et*

$$X(K) \cap \Gamma = \cup_{i=1}^{n} \gamma_i + (B_i(K) \cap \Gamma).$$

Cette conjecture a finalement été démontrée par G. Faltings ([Fa]) après de nombreux travaux entre autres de Manin, Vojta, Laurent, Hindry et Faltings lui-même. On peut trouver des bibliographies récentes, commentées et complètes, dans [Hi2] ou [Maz]. L'extension au cas des variétés semi-abéliennes est due à Vojta([Voj]) et McQuillan ([McQ]).

Si on veut étendre cette conjecture au cas de caractéristique non nulle, il faut se contenter d'une version relative, dite aussi conjecture de Lang pour les corps de fonctions. En voici un énoncé un peu simplifié :

CONJECTURE DE LANG POUR LES CORPS DE FONCTIONS. — *Soient $K_0 < K$ deux corps algébriquement clos, A une variété abélienne définie sur K de K/K_0-trace zéro, et X une sous-variété de A définie sur K. Soit Γ un sous-groupe de rang fini de $A(K)$. Alors il existe $\gamma_1, \ldots, \gamma_n \in \Gamma$ et $B_1, \ldots, B_n$ sous-variétés abéliennes de A tels que $\gamma_i + B_i \subseteq X$ et*

$$X(K) \cap \Gamma = \cup_{i=1}^{n} \gamma_i + (B_i(K) \cap \Gamma).$$

On rappelle que Γ est de *rang fini* si il existe un groupe Γ_0 finiment engendré tel que, pour chaque $\gamma \in \Gamma$, il y a un entier $n \geq 1$ tel que $n\gamma \in \Gamma_0$. Si on est en caractéristique $p > 0$, on demande que l'entier n ne soit pas divisible par p. Dire que A est de K/K_0-trace zéro est équivalent à dire que A n'a aucune sous-variété abélienne homomorphe à une variété abélienne définie sur K_0.

Dans [Hr1], Hrushovski a donné une démonstration modèle-théorique de la conjecture de Lang pour les corps de fonctions en toute caractéristique (on peut trouver une présentation de ces résultats dans l'exposé [Go] de ce séminaire, ou dans [Pi3], et une exposition plus détaillée dans le livre [Bo]). Pour la caractéristique $p > 0$, il s'agissait de la première démonstration du cas général, les résultats précédents (voir [AbrVo]) nécessitant des hypothèses supplémentaires. Un peu auparavant, A. Buium ([Bu]) avait donné une nouvelle démonstration du cas de caractéristique zéro, dont l'idée de départ était de passer à un corps différentiellement clos et de remplacer le groupe Γ par un groupe Δ-fermé (ou différentiellement algébrique) de dimension finie. C'est cette idée qui est l'inspiration des démonstrations de Hrushovski, pour les deux résultats, Lang pour les corps de fonctions et Manin-Mumford.

1.2. Le rapport avec la théorie des modèles

L'idée qui est à la base de ces deux démonstrations est donc la suivante : on veut remplacer le sous-groupe Γ ($Tor(G)$ dans notre cas) par un sous-groupe « fermé » ou « algébrique », pour lequel on montrera le résultat. On ne peut pas le faire sans, d'une manière ou d'une autre, rajouter des « fermés » supplémentaires (c'est-à-dire de la structure supplémentaire), puisque, quand G par exemple est une variété abélienne, la torsion est dense dans G. C'est exactement ce que fait Buium dans [Bu], quand il passe dans un corps différentiellement clos, remplace le groupe Γ par un groupe Δ-fermé de dimension finie et utilise ensuite l'arsenal des outils développés dans ce cadre. Or c'est là une méthode qui rentre tout à fait dans la problématique développée en théorie des modèles et pour laquelle nous disposons d'un cadre systématique, d'outils et de résultats déjà existants. En effet, puisant son inspiration dans la géométrie algébrique et les géométries combinatoires, la théorie des modèles développe dans un cadre abstrait des notions d'indépendance, de dimension et de géométrie. Cela a

permis d'isoler une notion qui va se retrouver au centre de toutes ces applications récentes : la notion de *modularité* qui caractérise, à partir du comportement de la relation d'indépendance, les groupes dans lesquels les seuls sous-ensembles qu'on peut définir sont les (combinaisons booléennes finies de) translatés de sous-groupes. Montrer que le groupe $Tor(G)$ satisfait l'énoncé de Manin-Mumford, c'est exactement, une fois qu'on s'est placé dans le bon cadre, montrer que c'est un groupe modulaire, nous le verrons dans les sections 2.2 et 2.3 ; et l'on a des outils pour cela.

1.3. Le cadre dans lequel on travaille

On a donc un groupe algébrique, G, défini sur un corps de nombres k. On va considérer un automorphisme σ dans $Gal(k^{alg}/k)$, judicieusement choisi, de manière à ce que la torsion soit contenue dans le sous-groupe S_σ des solutions, dans $G(k^{alg})$, d'une équation faisant intervenir σ (ce qu'on appelle traditionnellement une équation de différence) qu'on peut explicitement calculer. On plonge alors (k^{alg}, σ) dans un gros corps K sur lequel σ se prolonge et qui est clos en ce sens qu'il contient déjà des solutions pour toute équation de différence qui a une solution dans une extension. C'est ce qu'on appellera un corps de différence générique. Et, de même qu'on a la topologie de Zariski sur un corps algébriquement clos ou la Δ-topologie sur un corps différentiellement clos, on définit une σ-topologie sur K. La théorie des modèles permet d'analyser la structure de K avec ces nouveaux ensembles géométriques. Cette analyse a été faite par Z. Chatzidakis et E. Hrushovski dans [ChHr] qui montrent qu'on peut y définir une bonne notion d'indépendance et de dimension. En particulier, ils démontrent en caractéristique zéro un théorème de dichotomie, qui dit à peu près que les seuls ensembles de dimension finie qui ne sont pas « modulaires » se trouvent dans le corps fixé par σ. À partir de cette analyse et de ce théorème de dichotomie, Hrushovski trouve un critère « effectif » pour distinguer, parmi les sous-groupes de $G(K)$ définis par des équations de différence, ceux qui sont modulaires. Il ne reste plus qu'à vérifier que le sous-groupe S_σ judicieusement choisi plus haut est du bon type, puis à borner le nombre de translatés qui vont intervenir par des calculs simples à partir de l'équation qui définit S_σ.

C'est exactement comme cela que cela se passe dans le cas de la torsion première à p. Pour la torsion totale, c'est un peu plus compliqué, car, s'il est facile, en travaillant à partir de deux premiers de bonne réduction distincts, de montrer qu'il existe une σ-équation qui s'annule sur la torsion toute entière et est du bon type, on ne sait pas le faire de manière effective. Donc, si on veut garder des bornes sur le nombre de translatés, il faut travailler un peu plus, en gardant deux équations distinctes, l'une pour la torsion première à p, l'autre pour la p-torsion puis combiner les deux.

Dans une première partie, nous allons présenter le cadre modèle théorique, c'est-à-dire les corps de différence génériques et les groupes que l'on peut y définir avec des équations de différence (section 2). Ensuite nous expliquerons comment utiliser les résultats ainsi obtenus pour démontrer la conjecture de Manin-Mumford (section

3). En fait, nous traiterons le cas de la torsion première à p et ne dirons que quelques mots sur le passage à la torsion totale. Enfin nous terminerons en mentionnant d'autres applications de la même méthode (section 4).

Merci à celles et ceux qui ont bien voulu relire tout ou partie de ce texte, ou répondre aux nombreuses questions auxquelles je ne pouvais manquer d'être confrontée, puisqu'il me faut parler ici non seulement de théorie des modèles mais aussi de géométrie algébrique, domaine qui n'est pas le mien. En particulier, merci à Z. Chatzidakis, F. Delon, D. Bertrand, M. Hindry et aussi à E. Hrushovski. Je suis évidemment seule responsable des erreurs qui se seraient ici glissées dans un énoncé de théorème ou dans une esquisse de preuve, à la suite d'une tentative indue de simplification.

2. LES CORPS DE DIFFÉRENCE GÉNÉRIQUES

2.1. Définition et existence

Nous appellerons *corps de différence* un corps K muni d'un automorphisme distingué σ. On peut par exemple considérer $K = k^{alg}$, la clôture algébrique d'un corps k, muni d'un automorphisme $\sigma \in Gal(k^{alg}/k)$ ou encore, si K est un corps parfait de caractéristique $p > 0$ et $n \geq 1$, K muni de l'automorphisme de Frobenius $x \mapsto x^{p^n}$.

Les corps de différence ont été à l'origine étudiés par Ritt dans les années 30 ; on peut trouver tous les résultats algébriques de base dans le livre de R. Cohn [Coh] (dans ce livre, un corps de différence est un corps avec un monomorphisme distingué ; quand il s'agit d'un automorphisme, le corps est appelé corps de différence inversif).

Il était naturel pour des théoriciens des modèles de s'intéresser à la classe des corps de différence *existentiellement clos* c'est-à-dire tels que tout système fini d'équations de différence ayant une solution dans une extension du corps en a déjà une dans le corps. C'est l'analogue, pour les corps de différence, des corps algébriquement clos pour les corps, des corps différentiellement clos pour les corps différentiels, ou bien encore des corps réels clos pour les corps ordonnés. Les premières propriétés (axiomatisation, décidabilité etc) ont été étudiées par A. Macintyre, L. van den Dries et C. Wood (voir [Ma1]). Ensuite, une étude plus complète de la structure de ces corps du point de vue de la théorie des modèles a été faite par Z. Chatzidakis et E. Hrushovski dans un premier temps ([ChHr]), puis par les mêmes avec un troisième auteur, K. Peterzil ([ChHrPe]). C'est dans le premier de ces deux articles que se trouvent les résultats qui sont utilisés pour la démonstration de Manin-Mumford, notamment le résultat de dichotomie en caractéristique zéro qui est crucial. Enfin, dans l'article où il donne sa démonstration de la conjecture de Manin-Mumford ([Hr2]), Hrushovski commence par pousser plus loin l'étude des groupes commutatifs définissables dans ces corps de différence. Dès la prochaine section, pour simplifier les énoncés, nous nous limiterons à la caractéristique zéro et aux résultats ayant un rapport direct avec les applications

dont nous voulons parler. Pour en savoir plus sans se plonger dans les articles eux-mêmes, on pourra consulter [Ch2].

Commençons par décrire ces corps, que nous appellerons ici pour simplifier *corps de différence génériques* (au départ, dans [ChHr], ils apparaissent comme modèles d'une théorie appelée ACFA, « algebraically closed fields with an automorphism » ; on les appelle aussi souvent corps algébriquement clos avec un automorphisme générique).

Convention et notation. — Nous utiliserons le terme de variété uniquement dans le cas irréductible. Si X est une variété affine définie sur K, X^σ est la variété affine définie en appliquant σ aux coefficients des équations qui définissent X.

DÉFINITION 2.1. — *Soit (K,σ) un corps de différence. On dit que (K,σ) est un* corps de différence générique *si K est un corps algébriquement clos vérifiant la propriété :*

(*) *Soient X une variété affine définie sur K et Y une sous-variété de $X \times X^\sigma$ définie sur K, dont les projections sur les facteurs X et X^σ sont denses. Alors il existe $a \in X(K)$ tel que $(a, \sigma(a)) \in Y(K)$.*

Les corps algébriquement clos satisfaisant (*) sont bien exactement les corps de différence existentiellement clos et tout corps de différence se plonge dans un corps de différence générique.

Ces corps, comme on va le voir dans la suite, sont munis d'une structure plus riche que celle induite uniquement par la topologie de Zariski mais que l'on sait quand même analyser !

Commençons par quelques propriétés élémentaires :

Premières propriétés. — Soit (K,σ) un corps de différence générique. Le corps K est de degré de transcendance infini sur le corps premier. Le corps fixé par σ dans K, $Fix(\sigma)$, est un corps pseudo-fini. Le seul invariant nécessaire pour obtenir les complétions (au sens de la théorie des modèles) de la théorie des corps algébriquement clos est la caractéristique ; pour les corps de différence génériques, il faut préciser en plus la classe de conjugaison de σ dans le groupe des automorphismes de la clôture algébrique du corps premier.

Enfin, mentionnons un résultat frappant qui vient confirmer l'importance de cette classe de corps. Cela faisait plusieurs années que se posait la question de ce que pouvait bien être la théorie d'un « Frobenius non-standard », par exemple la limite des corps de différence $(\mathbb{F}_p^{alg}, x \mapsto x^p)$, pour p tendant vers l'infini. Il s'agit de l'analogue, pour les automorphismes de Frobenius, de la question résolue par Ax quand il a montré que la théorie élémentaire des corps finis était exactement la théorie des corps pseudo-finis [Ax]. La question précise ici était de savoir s'il s'agissait des corps de différence génériques. Une réponse positive a été indépendamment donnée par Hrushovski ([Hr3]) et Macintyre ([Ma2]) : la théorie des corps de différence génériques est exactement la théorie de tous les ultraproduits non principaux de $({\mathbb{F}_q}^{alg}, x \mapsto x^q)$, quand q varie sur l'ensemble des puissances de nombre premiers.

2.2. Ensembles définissables, indépendance

À partir de maintenant, (K, σ) sera un corps de différence générique de caractéristique zéro. Les résultats des sections 2.2 et 2.3 ont été démontrés dans [ChHr].

Comme d'habitude en Théorie des modèles (voir par exemple le chapitre d'introduction de [Bo]), on considère un corps de différence générique (K, σ) comme une structure du premier ordre. Cela veut dire que l'on étudie les ensembles que l'on peut définir à partir des opérations et des fonctions de base, dans ce cas $\{+, -, \cdot, 0, 1, \sigma\}$, en prenant la clôture par intersection et réunion finies, par complémentaire et par projection.

Dans un « pur » corps algébriquement clos K, il est naturel de commencer par considérer les sous-ensembles de K^n définis par des équations polynomiales, les fermés de Zariski. Ici il est naturel de considérer les σ- polynômes : $K[X_1, \ldots, X_n]_\sigma$, *l'anneau des polynômes de différence* (ou σ- polynômes) est l'anneau des polynômes sur K en une infinité de variables, $X_1, \ldots, X_n, \sigma(X_1), \ldots, \sigma(X_n), \sigma^2(X_1), \ldots, \sigma^2(X_n), \ldots$ Un *σ-fermé* de K^n est l'ensemble des zéros d'un nombre fini de σ- polynômes de $K[X_1, \ldots, X_n]_\sigma$. Un *$\sigma$-idéal* I de $K[X_1, \ldots, X_n]_\sigma$ est un idéal clos par σ et on dit que I est *parfait* si chaque fois que $a^j \sigma^i(a) \in I$, $i, j \in \mathbb{N}$, alors a appartient à I. Les σ-fermés correspondent exactement aux σ-idéaux parfaits et comme on a la condition de chaîne ascendante sur les σ-idéaux parfaits (voir [Coh]), on définit ainsi une topologie noetherienne contenant strictement la topologie de Zariski.

On peut alors considérer les *σ-constructibles*, les combinaisons booléennes finies de σ-fermés. Mais là, contrairement à ce qui se passe avec la topologie de Zariski sur un corps algébriquement clos ou bien avec la Δ-topologie sur un corps différentiellement clos, la classe des σ-constructibles n'est pas close par projection. On clôt donc aussi par projection et on obtient ce qu'on appelle la classe des ensembles *σ- définissables.* Si V est une variété affine définie sur K, l'ensemble $V(K)$ des points K-rationnels de V est un σ-fermé dans un produit K^n. Pour une variété V définie sur K et donnée par un recouvrement fini de cartes affines, $V(K)$ est un ensemble σ-définissable. Le corps $Fix(\sigma)$ (défini par l'équation $\sigma(x) = x$) est un exemple de σ-fermé qui n'est pas de la forme $V(K)$. Nous dirons qu'une application est σ-définissable si son graphe est σ-définissable.

Bien que cela ne soit pas évident a priori, la classe des σ-définissables est également close, à bijection σ- définissable près, par quotient. Cela veut dire précisément que si $F \subseteq K^n$ est σ-définissable et que $R \subseteq K^n \times K^n$ est une relation d'équivalence σ-définissable sur K^n, alors il existe une bijection σ-définissable entre l'ensemble quotient F/R et un sous-ensemble σ-définissable de K^m pour un certain m. On dit des structures qui ont cette propriété qu'elles *éliminent les imaginaires.*

On sera amené à s'intéresser à la *structure induite* par (K, σ) sur les sous-ensembles σ- définissables : si $D \subset K^n$ est σ-définissable, la structure induite sur D est D, muni,

pour tout $m > 0$, de la trace sur D^m de tous les sous-ensembles σ-définissables de K^{nm}.

On montre que la structure induite sur le corps $Fix(\sigma)$ se réduit (une fois qu'on a fixé un certain nombre de constantes dans $Fix(\sigma)$) à la pure structure de corps : si D est un sous-ensemble σ-définissable de K^n, alors $D \cap Fix(\sigma)^n$ est un sous-ensemble de $Fix(\sigma)^n$ définissable dans le pur langage des corps (c'est-à-dire constructible au sens habituel du terme, combinaison booléenne de fermés de Zariski).

Il est classique maintenant en théorie des modèles de regarder s'il est possible de définir une bonne notion d'indépendance dans les structures qu'on étudie, du type de l'indépendance algébrique dans les corps algébriquement clos. C'est bien le cas ici :

DÉFINITION 2.2. — *1. Si A est un sous-ensemble de K, la* σ-clôture algébrique de *A, $acl_\sigma(A)$, est égale à la clôture algébrique (au sens habituel des corps) du sous-corps de différence de (K, σ) engendré par A, c'est-à-dire à la clôture algébrique de $\mathbb{Q}(\{\sigma^i(a); a \in A, i \in \mathbb{Z}\})$.*

2. Si $A, B, C \subset K$, on dit que A et B sont indépendants *au-dessus de C si $acl_\sigma(AC)$ et $acl_\sigma(BC)$ sont linéairement disjoints au-dessus de $acl_\sigma(C)$.*

3. Si E est un sous-corps de différence de K et si a est une suite finie d'éléments de K, on définit le σ-degré *de a au-dessus de E, $d_\sigma(a/E)$ comme étant le degré de transcendance de $E(a)_\sigma$, le corps de différence engendré par $E(a)$, au-dessus de E. Si $D \subset K^n$ est un sous-ensemble σ-définissable, on définit le σ-degré de D comme étant le maximum des degrés des éléments de D.*

Le corps $Fix(\sigma)$ est de σ-degré égal à un ; en revanche si V est une variété (de dimension positive) définie sur K, $V(K)$ est de σ-degré infini. Quand il est fini, le σ-degré est une bonne notion de dimension, en particulier il est clair que si $E = acl_\sigma(E)$ et si $d_\sigma(a/E)$ est fini, alors a et b sont σ-indépendants au-dessus de E si et seulement si $d_\sigma(a/E) = d_\sigma(a/acl_\sigma(E(b))$. Il est possible (et indispensable) de définir d'autres notions de dimension ou de rang dans (K, σ) pouvant prendre des valeurs ordinales non finies, mais nous n'en parlerons pas ici. Ce qui est important pour nous. c'est que pour un a donné, ces différentes dimensions sont simultanément finies.

2.3. Modularité, le théorème de dichotomie

Comme nous l'avons dit dans l'introduction, cela fait plusieurs années que la pertinence de la notion abstraite d'ensemble « modulaire » (cette notion apparaît hélas dans la littérature sous plusieurs noms : localement modulaire, un-basé (one-based) etc.) s'est imposée à travers les conclusions très précises que l'on peut déduire sur les propriétés algébriques des structures modulaires.

Nous allons donner les définitions et les résultats sous une forme adaptée à notre contexte précis. Mais il s'agit de cas particuliers ou d'adaptations de résultats valables dans un contexte beaucoup plus général.

Si $E = acl_\sigma(E) \subset K$ et si a, a' sont deux éléments de K^n, on dit que a et a' *ont même type (d'isomorphisme)* au-dessus de E si il existe un isomorphisme ϕ : $acl_\sigma(E, a)) \mapsto acl_\sigma(E, a')$ qui fixe E, envoie a sur a' et commute avec σ.

DÉFINITION 2.3. — *Un sous-ensemble σ-définissable D de K^n est*

- stable *si, pour tout $E = acl_\sigma(E) \subset K$, pour toutes suites finies a, a' d'éléments de D ayant même type au-dessus de E, pour tout $F = acl_\sigma(F), E \subset F \subset K$, si a et F sont indépendants au-dessus de E et si a' et F sont indépendants au-dessus de E, alors a et a' ont aussi même type au-dessus de F ;*

- modulaire *si pour tout $E = acl_\sigma(E) \subset K$, pour toutes suites finies a, b d'éléments de D, $acl_\sigma(Ea)$ et $acl_\sigma(Eb)$ sont indépendants au-dessus de $acl_\sigma(Ea) \cap acl_\sigma(Eb)$.*

La stabilité veut donc dire que, si $E \subset K$ est σ-algébriquement clos, et si $a, b \in K$ alors il n'y a (à isomorphisme près) qu'une seule façon pour a et b d'être indépendants au-dessus de E.

Il y a des corps stables : les (purs) corps algébriquement clos, les corps séparablement clos ou encore les corps différentiellement clos. Mais les corps pseudo-finis ([Du]), donc en particulier $Fix(\sigma)$, ne sont pas stables. On le voit ici facilement : on peut trouver $E = acl_\sigma(E) \subset K$ et $a, b, c \in Fix(\sigma) \setminus E$, tels que a et c d'une part, b et c d'autre part sont indépendants au-dessus de E, mais tels que $\sqrt{a - c} \in Fix(\sigma)$ et $\sqrt{b - c} \notin Fix(\sigma)$.

Le corps $Fix(\sigma)$ n'est pas modulaire : on prend trois éléments de $Fix(\sigma)$, a, b, c transcendants sur $\mathbb{Q}$ et algébriquement indépendants. Alors $acl_\sigma(a, b) = \mathbb{Q}(a, b)^{alg}$ et $acl_\sigma(c, ac + b) = \mathbb{Q}(c, ac + b)^{alg}$ s'intersectent en $\mathbb{Q}^{alg}$, et pourtant ils ne sont pas algébriquement indépendants au-dessus de $\mathbb{Q}^{alg}$. En fait, la non-modularité est la traduction « abstraite », dans le cas d'un ensemble de dimension un, de l'existence d'une famille de courbes planes (ici la famille des courbes $y = ax + b$) de dimension deux. En particulier, si un ensemble D est modulaire, alors cela entraîne que *dans la structure induite par (K, σ) sur D*, on ne peut pas définir de corps infini. On va voir un peu plus loin (2.6) qu'avec l'hypothèse de stabilité, cela entraîne beaucoup plus.

Mais ce qui est particulièrement intéressant dans le cas des corps de différence génériques, c'est que toute la non-modularité et la non-stabilité sont concentrées dans le corps fixé. C'est ce que nous dit le théorème de dichotomie en caractéristique zéro.

On dit que deux ensembles σ-définissables D et F de (K, σ) sont *orthogonaux* si pour toute suite finie d d'éléments de D, pour toute suite finie b d'éléments de F, pour tout sous-corps $E = acl_\sigma(E)$ de K, d et b sont indépendantes au-dessus de E.

THÉORÈME 2.4. — Théorème de dichotomie : *Soit $D \subseteq K^n$ un sous-ensemble σ-définissable de σ-degré fini, alors D est stable et modulaire si et seulement si D et le corps fixé $Fix(\sigma)$ sont orthogonaux.*

La démonstration de ce théorème passe par une analyse des ensembles de dimension finie en termes de sous-ensembles de dimension un. Le même type de résultat avait été montré précédemment pour les corps différentiellement clos (avec le sous-corps des constantes, [HrSo]) et pour les corps séparablement clos de caractéristique $p > 0$ (avec le sous-corps des éléments infiniment p-divisibles, [Hr1]) mais par des méthodes différentes. Dans ces deux autre cas, la preuve utilise la théorie des géométries de Zariski, version abstraite de la topologie de Zariski introduite par Hrushovski et Zil'ber ([HrZi], voir aussi [Mr]).

De façon générale, la dichotomie modulaire/non-modulaire est particulièrement utile dans le cas des groupes. En effet la modularité caractérise les structures de groupes stables de manière très précise. À nouveau nous énonçons dans 2.6 un résultat qui est vrai dans un contexte beaucoup plus général.

DÉFINITION 2.5. — *Soit $G \subseteq K^n$ un groupe σ-définissable. On dit que G est* de type abélien *si pour tout m et pour tout sous-ensemble σ-définissable X de K^{nm}, $X \cap G^m$ est une combinaison booléenne finie de translatés de sous-groupes connexes (σ-définissables) de G^m.*

Il s'ensuit que le groupe G a un sous-groupe (σ-définissable) abélien d'indice fini et donc en fait que la structure induite par (K, σ) sur G se réduit à une structure de type « module généralisé ».

PROPOSITION 2.6 ([HrPi1]). — *Soit $G \subset K^n$ un groupe σ-définissable stable. Alors G est modulaire si et seulement si G est de type abélien*

On voit maintenant le rapport entre la modularité et les questions de type conjecture de Manin-Mumford ou plus généralement conjecture de Lang. On a d'ailleurs bien une équivalence formelle de la conjecture de Manin-Mumford avec l'énoncé de théorie des modèles suivant : pour tout groupe algébrique commutatif connexe G défini sur $\mathbb{Q}^{alg}$, la structure $(\mathbb{Q}^{alg}, Tor(G))$, dans le langage des anneaux avec un prédicat pour le groupe $Tor(G)$, est stable et le groupe $Tor(G)$ (qui est maintenant définissable dans cette structure) est modulaire (voir [Pi1]). Mais savoir cela ne nous donne pas pour autant une méthode pour montrer que cela est vrai. L'intérêt de passer par les corps de différence génériques c'est que là, on a un vrai critère utilisable pour reconnaître quand un groupe est modulaire grâce à la dichotomie.

2.4. Les sous-groupes σ-définissables des variétés abéliennes

Nous résumons ici les conséquences de l'étude des groupes commutatifs σ-définissables et en particulier des sous-groupes σ-définissables des points K-rationnels des variétés abéliennes faite par Hrushovski dans [Hr2]. On peut aussi en trouver une exposition détaillée dans [Ch1].

L'une des étapes essentielles de cette étude est l'analyse de l'anneau des *endomorphismes σ-définissables* de $A(K)$ pour A une variété abélienne définie sur K.

DÉFINITION 2.7. — *Soit G un groupe algébrique défini sur K. Un* endomorphisme σ-définissable *de $G(K)$ est une application σ-définissable de $G(K)$ dans $G(K)$ qui est un homomorphisme du groupe $G(K)$.*

Les endomorphismes du groupe algébrique G qui sont définis sur K induisent des endomorphismes de $G(K)$ au sens de la définition ci-dessus. Il y en a en général beaucoup d'autres mais Hrushovski montre par exemple :

PROPOSITION 2.8. — *Soient A une variété abélienne simple définie sur K, $End_\sigma(A(K))$ l'anneau des endomorphismes σ-définissables de $A(K)$ et $End_{alg}(A(K))$ le sous-anneau des endomorphismes qui sont induits par les endomorphismes (algébriques) de la variété abélienne A.*

(1) *Si A n'est pas isogène à A^{σ^n}, alors*

$$\mathbb{Q} \otimes End_\sigma(A(K)) = \mathbb{Q} \otimes End_{alg}(A(K)).$$

(2) *Sinon, $\mathbb{Q} \otimes End_\sigma(A(K))$ est isomorphe à un anneau de polynômes tordu au-dessus de $\mathbb{Q} \otimes End_{alg}(A(K))$ (que nous ne décrirons pas ici précisément). Il s'ensuit en particulier que $End_\sigma(A(K))$ est dénombrable, comme $End_{alg}(A(K))$.*

(3) *Pour chaque sous-groupe σ-définissable G de $A(K)$, il existe $f \in End_\sigma(A(K))$ tel que G est un sous-groupe d'indice fini de $Ker(f)$. Il s'ensuit qu'il n'y a qu'un nombre dénombrable de sous-groupes σ-définissables de $A(K)$.*

Des résultats similaires sont montrés pour $A = \mathbb{G}_m$, le groupe multiplicatif. On a alors $\mathbb{Q} \otimes End_\sigma(\mathbb{G}_m(K)) \simeq \mathbb{Q}[\sigma, \sigma^{-1}]$.

Soit A une variété semi-abélienne définie sur $Fix(\sigma)$ et $F[T] \in \mathbb{Z}[T]$ un polynôme à coefficients entiers. Alors $F(\sigma)$ induit naturellement un endomorphisme (σ-définissable) de $A(K)$: si $F[T] = \sum_{i=0}^{r} m_i T^i$, alors $F(\sigma)(a) = m_0 a + m_1 \sigma(a) + \cdots + m_r \sigma^r(a)$, où $+$ est l'addition dans A et $ma = [m]a$ la multiplication par l'entier m dans A.

DÉFINITION 2.9. — *Les groupes B et C sont* commensurables *si $B \cap C$ est d'indice fini dans B et dans C. Un groupe σ-définissable B est* c-minimal *si tout sous-groupe σ-définissable infini de B est d'indice fini dans B.*

PROPOSITION 2.10. — *Supposons que A est une variété abélienne simple définie sur $Fix(\sigma)$ ou bien que A est le groupe multiplicatif $\mathbb{G}_m$. Soit B un sous-groupe σ-définissable de $A(K)$ de σ-degré fini et c-minimal. Alors B n'est pas de type abélien si et seulement si il existe n tel que $B \subseteq Ker(\sigma^n - 1)$.*

Esquisse de démonstration de 2.10. — C'est bien sûr le Théorème de dichotomie (2.4) et l'équivalence (2.6) entre groupe stable modulaire et groupe de type abélien que nous allons utiliser.

Si B est inclus dans $Ker(\sigma^n - 1)$, c'est-à-dire $B \subseteq A(Fix(\sigma^n))$, alors comme $Fix(\sigma^n)$ est une extension finie de $Fix(\sigma)$, il existe une application σ-définissable à fibres finies de $Fix(\sigma)^n$ sur B, qui n'est donc pas orthogonal à $Fix(\sigma)$ et n'est donc pas de type abélien.

Réciproquement, supposons que B n'est pas de type abélien. Par 2.6 et 2.4, B et $Fix(\sigma)$ ne sont pas orthogonaux.

FAIT 2.11. — *Soit B un sous-groupe σ-définissable de σ-degré fini de $H(K)$, où H est un groupe algébrique défini sur K. Si B n'est pas orthogonal à $Fix(\sigma)$, alors il existe un sous-groupe normal D σ- définissable d'indice infini dans B, un entier $m \geq 1$ et une surjection σ-définissable (du produit cartésien) $(Fix(\sigma))^m$ sur B/D.*

Dans notre cas, la c-minimalité de B entraîne que D est fini. On en déduit l'existence d'une application injective σ-définissable h de B/D dans un produit de $Fix(\sigma)$. On transporte la loi de groupe de B/D par h sur $C = h(B/D)$. Le groupe C est alors σ-définissable, mais on sait que tout sous-ensemble σ-définissable dans $Fix(\sigma)$ est définissable dans le pur langage des corps. On peut donc utiliser des résultats antérieurs sur les groupes définissables dans les corps pseudo-finis ([HrPi2]) qui permettent de conclure qu'il existe un homomorphisme σ-définissable, de noyau fini, de C sur un sous-groupe d'indice fini de $G(Fix(\sigma))$, pour G un groupe algébrique défini sur $Fix(\sigma)$. On en déduit l'existence d'un homomorphisme σ-définissable g de B sur un sous-groupe d'indice fini de $G(Fix(\sigma))$, g de noyau fini contenant D. On peut supposer (en remplaçant B par un sous-groupe d'indice fini) que G est connexe, que $g(B) = G(Fix(\sigma))$ et donc que G est un groupe algébrique commutatif simple. Le graphe de g, qui est un sous-groupe σ-définissable de $(H \times G)(K)$ est commensurable avec le noyau d'un endomorphisme σ-définissable (par 2.8). Il n'y a qu'un nombre dénombrable de tels endomorphismes, et il suit que g est défini sur une extension finie k_1 de $Fix(\sigma)$. On peut donc bien trouver un n tel que σ^n fixe B point par point.

On peut maintenant en déduire le corollaire qui va être au centre de la démonstration de la conjecture de Manin-Mumford, en utilisant les lemmes suivants qui permettent en particulier de se ramener au cas d'une variété abélienne simple ou du groupe multiplicatif :

LEMME 2.12. — *a) Si on a une suite exacte d'homomorphismes de groupe σ-définissables*

$$0 \to A_1 \to A_2 \to A_3 \to 0,$$

où A_1, A_2, A_3 sont des groupes σ-définissables, alors A_2 est stable modulaire si et seulement si A_1 et A_2 sont stables modulaires.

b) Si A est une variété abélienne simple définie sur K et si H est un sous-groupe σ-définissable de $A(K)$, alors H est c-minimal si et seulement si il existe $f \in End_\sigma A(K)$, f irréductible dans $\mathbb{Q} \otimes End_\sigma A(K)$, tel que H et $Ker(f)$ sont commensurables.

c) Si B est un sous-groupe σ-définissable de $A(K)$, pour A une variété abélienne définie sur K, et si B est commensurable avec $Ker(f_1 \cdots f_m)$ pour $f_1, \ldots, f_m \in End_\sigma(A(K))$, alors B est stable modulaire si et seulement si tous les $Ker(f_i)$ sont stables modulaires.

Si $F[T] \in \mathbb{Z}[T]$ est un polynôme dont aucune racine n'est racine de l'unité, nous dirons que $F(T)$ est un polynôme sans facteur cyclotomique.

COROLLAIRE 2.13. — *Soit A une variété semi-abélienne définie sur $Fix(\sigma)$ et $F(T) \in \mathbb{Z}[T]$. Soit $H_\sigma = Ker(F(\sigma)) = \{a \in A(K); \sum_{i=0}^{r} m_i \sigma^i(a) = 0\}$. Alors le groupe H_σ est de type abélien si et seulement si $F(T)$ est sans facteur cyclotomique.*

Esquisse de démonstration de 2.13. — Tout d'abord H_σ est bien de σ-degré fini. Ensuite, en utilisant 2.12, on peut se ramener aux deux cas où A est une variété abélienne simple ou bien où $A = \mathbb{G}_m$, le groupe multiplicatif.

Si pour un $N > 0$ $(T^N - 1)$ et $F(T)$ ont un facteur commun $P(T)$, alors $B = Ker(P(\sigma)) \subseteq Ker(\sigma^N - 1)$ n'est pas modulaire. Mais $B \subseteq H_\sigma$ qui n'est donc pas modulaire non plus.

Supposons maintenant que H_σ n'est pas de type abélien et, pour simplifier (en fait il faut utiliser b) et c) du Lemme 2.12), qu'il est c-minimal et que $F(\sigma) = f$ est un élément irréductible de $\mathbb{Q} \otimes End_\sigma(A)$. Par 2.10 à nouveau, il existe un N tel que $Ker(f) \subseteq C = Ker(\sigma^N - 1)$. Mais en choisissant N suffisamment grand on peut supposer que f agit sur C et $F(T)$ étant sans facteur cyclotomique, f devrait être inversible sur C.

3. APPLICATION À LA CONJECTURE DE MANIN-MUMFORD

Nous sommes maintenant en mesure d' expliquer comment appliquer le théorème de dichotomie et son corollaire sur les groupes définis à partir d'un polynôme sans facteur cyclotomique (2.13) pour obtenir une nouvelle démonstration de la conjecture de Manin-Mumford. En fait, comme nous l'avons déjà dit dans l'introduction, nous n'allons vraiment traiter précisément que le cas de la torsion première à p, cas dans lequel l'application de 2.13 donne immédiatement le résultat et qui permet de comprendre pourquoi ce type de preuve fournit naturellement des bornes.

3.1. Préliminaires sans théorie des modèles

Comme on l'a déjà expliqué, la théorie des modèles va nous permettre de montrer que les ensembles qui nous intéressent sont des combinaisons booléennes finies de translatés de sous-groupes et l'on voudra en conclure qu'en fait ce sont des réunions finies de translatés. Remarquons donc tout de suite une fois pour toutes l'équivalence des différentes versions que nous pourrons rencontrer :

LEMME 3.1. — *Soit G un groupe algébrique commutatif connexe défini sur un corps algébriquement clos L, X une sous-variété de G également définie sur L et Γ un sous-groupe de $G(L)$. Les énoncés suivants sont équivalents :*

(i) $X \cap \Gamma$ est une combinaison booléenne finie de translatés de sous-groupes de Γ,

(ii) la clôture de Zariski de $X \cap \Gamma$ est une réunion finie de translatés de sous-groupes algébriques connexes de G,

(iii) $X \cap \Gamma$ est contenu dans une réunion finie de translatés $C_1, \ldots, C_n$ de sous-groupes algébriques connexes de G, chaque C_i étant contenu dans X,

(iv) $X \cap \Gamma$ est une réunion finie de translatés de sous-groupes de Γ.

Maintenant voici le principal fait « algébrique » que l'on va utiliser et sur lesquels nous ne nous étendrons pas ici.

Soit A une variété abélienne de dimension d définie sur un corps de nombres k et $\mathfrak{p}$ un premier de l'anneau $\mathfrak{R}$ des entiers de k, de corps résiduel $k_\mathfrak{p}$ de cardinalité q et de caractéristique p. On suppose que $\mathfrak{p}$ est un *premier de bonne réduction pour A*. On a donc que $A_\mathfrak{p}$, la réduction de A modulo $\mathfrak{p}$, est une variété abélienne (définie sur $k_\mathfrak{p}$) de même dimension que A. On rappelle que $Tor_{p'}(A) = \{a \in Tor(A);\ p \text{ ne divise pas l'ordre de } a\}$ et que $Tor_p(A) = \{a \in Tor(A); p^n a = 0 \text{ pour un } n \geq 1\}$.

FAIT 3.2. — *Il existe un automorphisme $\sigma \in Gal(\mathbb{Q}^{alg}/k)$ et un polynôme à coefficients entiers, $F[T] \in \mathbb{Z}[T]$, sans facteur cyclotomique, tel que l'endomorphisme $F(\sigma)$ de $A(\mathbb{Q}^{alg})$ s'annule sur $Tor_{p'}(A)$. De plus le degré de $F(T)$ est inférieur ou égal à $2d$ et la somme des valeurs absolues de ses coefficients est bornée par $(1 + q^{1/2})^{2d}$.*

Des résultats classiques de Weil (voir [We]) sur les endomorphismes des variétés abéliennes définies sur les corps finis et le polynôme caractéristique de l'automorphisme de Frobenius entraînent l'existence d'un tel polynôme $F[T] \in \mathbb{Z}[T]$ tel que $F(\Phi_q)$ s'annule sur $A_\mathfrak{p}(k^{alg})$, où Φ_q est l'automorphisme de Frobenius $\Phi_q : x \mapsto x^q$.

On peut alors relever cette équation fonctionnelle de la façon suivante : on prend pour σ un relèvement de Φ_q et, $\mathfrak{p}$ étant un premier de bonne réduction, on déduit du lemme de Hensel que la réduction modulo $\mathfrak{p}$ induit un isomorphisme de $Tor_{p'}(A)$ sur $Tor_{p'}(A_\mathfrak{p})$ et donc que $F(\sigma)$ s'annule sur $Tor_{p'}(A)$.

Remarque. — Il est possible de faire un peu mieux en travaillant à partir des facteurs simples de A et en ne comptant qu'une seule fois les facteurs isogènes. On peut ainsi borner le degré du polynôme $F[T]$ et la valeur absolue de ses coefficients en remplaçant d, la dimension de A, par un invariant de A, $d_r(A)$ qui est inférieur ou égal à la dimension de A et tel que, pour tout $n \geq 1$, $d_r(A) = d_r(A^n)$.

3.2. La torsion première à p

Nous allons donner la démonstration dans le cas des variétés abéliennes. Le cas des variétés semi-abéliennes est identique, il suffit de vérifier qu'on peut généraliser sans peine l'existence du polynôme adéquat sans facteur cyclotomique (3.2). En revanche, il faut encore travailler et utiliser de la théorie des modèles pour passer au cas d'un groupe commutatif arbitraire, nous l'expliquerons dans la section 3.2.2.

3.2.1. Les variétés abéliennes. — Soient A une variété abélienne de dimension d définie sur un corps de nombres k et X une sous-variété de A. On fixe un plongement de A dans un espace projectif $\mathbb{P}_n$ et on peut ainsi considérer le degré de A et de ses sous-ensembles algébriques.

On fixe un premier $\mathfrak{p}$ de bonne réduction pour A dont le corps résiduel est de cardinalité q et de caractéristique p.

PROPOSITION 3.3. — *Alors*

$$X \cap Tor_{p'}(A) = \bigcup_{i=1}^{M} a_i + Tor_{p'}(B_i),$$

où chaque B_i est une sous-variété abélienne de A et

$$M \leq c\ (\deg(X)^{(2d+1)(2^{d\dim(X)})})$$

où la constante c ne dépend que d'invariants liés à A (et non à X et à son corps de définition) et de q, et est deux fois exponentielle en d.

Démonstration. —

1. Pour obtenir la réunion finie. — On considère l'automorphisme σ de $Gal(\mathbb{Q}^{alg}/k)$ et le polynôme $F(T) \in \mathbb{Z}[T]$, $F(T) = \sum_{i=0}^{2d} c_i T^i$, donnés par 3.2. Soit (K, σ) un corps de différence générique extension du corps de différence $(\mathbb{Q}^{alg}, \sigma)$. Alors

$$H_\sigma := Ker(F(\sigma) \restriction_{A(K)}) = \{a \in A(K); \sum_{i=0}^{2d} c_i \sigma^i(a) = 0\}$$

est un sous-groupe de $A(K)$ défini par une σ-équation.

Puisque le polynôme $F(T)$ est sans facteur cyclotomique, 2.13 nous assure que H_σ est un sous-groupe de type abélien et donc que tous ses sous-ensembles σ-définissables sont des combinaisons booléennes finies de translatés de sous-groupes σ-définissables. C'est donc le cas en particulier pour $X \cap H_\sigma$ qui lui-même contient $X \cap Tor_{p'}(A)$.

Comme nous l'avons remarqué plus haut, cela entraîne que la clôture de Zariski de $X \cap H_\sigma$, que nous appellerons Z, est réunion finie de translatées de sous-variétés abéliennes de A, chacune contenue dans X, $Z = \bigcup_{i=1}^{M} b_i + B_i$.

On en déduit que $X \cap Tor_{p'}(A)$ est réunion d'au plus M translatés de la forme $a + Tor_{p'}(B)$ avec B sous-variété abélienne de A.

2. Pour borner le nombre M de translatées. — On va en fait borner le nombre de composantes irréductibles de Z, la clôture de Zariski de $X \cap H_\sigma$, en utilisant la définition explicite de H_σ à partir du polynôme $F[T]$.

On considère

$$S = \{(a_0, \ldots, a_{2d}) \in A^{2d+1}; \sum_{i=0}^{2d} c_i a_i = 0\}.$$

Donc $H_\sigma = \{a \in A(K); (a, \sigma(a), \ldots, \sigma^{2d}(a)) \in S\}$. Soit $U = S \cap (X \times X^\sigma \times \cdots \times X^{\sigma^{2d}})$ (chaque X^{σ^i} est une sous-variété de $A^{\sigma^i} = A$), alors

$$X \cap H_\sigma = \{a \in A(L); (a, \sigma(a), \ldots, \sigma^{2d}(a)) \in U\}.$$

Pour faire le calcul, on va utiliser une définition un peu modifiée du degré pour les sous-variétés de $(\mathbb{P}_n)^m$, pour $m > 1$, voir [Fu], exemple 8.4.4. On définit aussi le degré d'un fermé non irréductible comme la somme des degrés de (toutes) ses composantes irréductibles. Ce qui est important pour nous ici, c'est que le degré borne bien le nombre de composantes irréductibles.

Les propriétés du degré entraînent que

$$\deg(U) \leq \deg(S)(\deg(X)^{2d+1}) \leq \deg(S)(\deg(A)^{2d+1})$$

et on a que $\dim(U) \leq min\{\dim(S), (2d+1)\dim(X)\} \leq d(2d+1)$.

En utilisant le fait que le corps (K, σ) est un corps de différence générique, et donc satisfait la condition (*) de 2.1, on montre que :

LEMME 3.4. — *Soit $r > 0$, E un sous-ensemble algébrique de $\mathbb{P}_n^{r+1}$,*

$$E_\sigma := \{a \in \mathbb{P}_n(K); (a, \sigma(a), \ldots, \sigma^r(a)) \in E\}$$

et V la clôture de Zariski de E_σ. Alors $\deg(V) \leq (\deg(E))^{2^{\dim(E)}}$.

Dans notre cas on obtient donc que $M \leq \deg(Z) \leq \deg(U)^{2^{\dim(U)}}$, ce qui donne bien une borne du type annoncé, une fois qu'on a calculé le degré de S.

3.2.2. Groupes algébriques commutatifs. — Il n'est pas très difficile de généraliser à tous les groupes algébriques commutatifs le Fait 3.2 et donc l'existence du polynôme $F(T)$ sans facteur cyclotomique et de l'automorphisme σ de $\mathbb{Q}^{alg}$ adéquats. On considère comme plus haut un corps de différence générique (K, σ) étendant $(\mathbb{Q}^{alg}, \sigma)$.

La généralisation de la Proposition 3.3 aux variétés semi-abéliennes est alors immédiate puisque le corollaire central de la dichotomie (2.13) est vrai pour les variétés semi-abéliennes.

Mais dans le cas d'un groupe commutatif arbitraire 2.13 n'est plus vrai. En effet, si V est un sous-groupe vectoriel du groupe algébrique G, alors $KerF(\sigma) \cap V(K)$ ne peut pas être de type abélien : tout sous-groupe σ-définissable de degré fini de $V(K)$ est un espace vectoriel σ-définissable de dimension finie sur le corps $Fix(\sigma)$ et ne lui est donc pas orthogonal.

Mais on peut séparer la partie de type abélien et la partie espace vectoriel sur $Fix(\sigma)$ et cette dernière n'intervient pas dans le cas de la torsion. Plus précisément :

DÉFINITION 3.5. — *Soient G un groupe algébrique commutatif connexe défini sur $Fix(\sigma)$ et V le sous-groupe vectoriel maximal de G. Un sous-ensemble σ-définissable D de $G(K)$ est* spécial *s'il est de la forme $D = C + W$, avec C un translaté d'un sous-groupe σ-définissable de $G(K)$ et W un sous-ensemble σ-définissable de $V(K)$.*

PROPOSITION 3.6. — *Soient G un groupe algébrique commutatif connexe défini sur $Fix(\sigma)$ et $H_\sigma = \{g \in G(K); F(\sigma)(g) = 0\}$ pour un polynôme sans facteur cyclotomique $F(T) \in \mathbb{Z}[T]$. Alors tout sous-ensemble σ-définissable de H_σ est une combinaison booléenne finie de sous-ensembles spéciaux de $G(K)$.*

Les ingrédients de la démonstration de 3.6. — On considère la suite exacte $0 \to V \to G \to B \to 0$, où V est le sous-groupe vectoriel maximal de G et B est donc une variété semi-abélienne. Maintenant par 2.13, $H_B := H_\sigma / V(K) \cap H_\sigma$ est de type abélien mais $H_V := V(K) \cap H_\sigma$ est, lui, un espace vectoriel sur $Fix(\sigma)$. Le théorème de dichotomie (2.4) entraîne que, dans la structure (K, σ), un groupe de type abélien de σ-degré fini et un groupe vectoriel σ- définissable ne peuvent qu'être orthogonaux. Il n'y a donc aucune relation possible entre éléments de H_B et de H_V. On peut alors montrer que tout sous-ensemble σ-définissable de $H_B \times H_V$ est une réunion finie de rectangles $B_i \times V_i$ avec $B_i \subseteq H_B$ et $V_i \subseteq H_V$ et dans notre situation particulière, en déduire que tout sous-ensemble σ-définissable de H_σ est une combinaison booléenne finie de sous-ensembles σ-définissables spéciaux de la forme : $B + W$, où B est un translaté d'un sous-groupe σ-définissable de $G(K)$ et W est un sous-ensemble σ-définissable de $V(K)$.

COROLLAIRE 3.7. — *Soient G un groupe algébrique commutatif connexe défini sur $Fix(\sigma)$ et X une sous-variété de G. Alors la clôture de Zariski de $X \cap T_{p'}(G)$ est une réunion finie de translatés de sous-groupes algébriques de G.*

Démonstration de 3.7. — On considère $H_\sigma = \{g \in G(K); F(\sigma)(g) = 0\}$ pour le polynôme $F(T) \in \mathbb{Z}[T]$ donné par 3.2 (généralisé aux groupes commutatifs arbitraires). Par 3.6 $X \cap H_\sigma$ est combinaison booléenne de sous-ensembles spéciaux. Par passage à la clôture de Zariski, on obtient une réunion finie de sous-variétés spéciales de G, c'est-à-dire de sous-variétés de la forme $B + W$ où B est un translaté d'un sous-groupe algébrique connexe de G et W est une sous-variété de V, le sous-groupe vectoriel maximal de G. Il suffit maintenant de montrer que, si $C = B + W$ est une sous-variété spéciale de G d'intersection non vide avec $Tor_{p'}(G)$, alors la clôture de Zariski de $Tor_{p'}(G) \cap C$ est un translaté d'un sous-groupe algébrique de G. Par hypothèse, $B = g + E$ où E est un sous-groupe algébrique connexe de G. On peut se ramener au cas où $E \cap V = 0$ et on vérifie alors que $Tor_{p'}(G) \cap C$ est un translaté de $Tor_{p'}(E)$.

3.3. La torsion totale

3.3.1. Le cas des variétés semi-abéliennes. — On a vu dans la section précédente comment, pour une variété semi-abélienne, utiliser un premier de bonne réduction $\mathfrak{p}$ et puis un corps de différence générique $(L_\mathfrak{p}, \sigma_\mathfrak{p})$ pour « enfermer » le groupe des éléments de torsion première à p dans un groupe de type abélien en obtenant des bornes raisonnables. Puisque $Tor(A) = Tor_{p'}(A) \oplus Tor_p(A)$, l'idée est d'utiliser un second premier de bonne réduction $\mathfrak{t}$, de caractéristique résiduelle t différente de p, pour « enfermer » la torsion première à t et donc en particulier la p-torsion. C'est effectivement ce que fait Hrushovski, mais le problème va être de garder des bornes effectives. Si on cherche seulement le résultat qualitatif, il y a plusieurs preuves rapides utilisant cette méthode que l'on peut trouver par exemple dans [Pi2], [Ch2] ou [Hr2]. Nous allons en indiquer une dans la section suivante où l'on se trouve confronté à la question du calcul de $[L : k]$ où $L = k(Tor_{p'}(A)) \cap k(Tor_p(A))$.

Pour maîtriser les bornes, Hrushovski met en évidence des familles algébriques de composantes irréductibles, pour lesquelles il faut montrer une version uniforme de 3.4. Nous n'allons pas le faire ici. On peut trouver des énoncés et des calculs précis dans [Hr2] bien sûr mais aussi dans [Ch2]. On peut également en trouver une version « uniforme mais sans les calculs de bornes » dans [Pi2].

Il est important de signaler que, même si c'est moins frappant dans ce cas que dans le cas de la torsion première à p, l'existence de ces bornes effectives découle encore naturellement de la nature même de la démonstration. L'ordre de grandeur indiqué est ici aussi obtenu en effectuant les calculs avec des méthodes assez grossières.

3.3.2. Le cas des groupes commutatifs. — Pour ce qui est du passage à un groupe commutatif arbitraire, on commence par remarquer que, une fois le résultat « qualitatif » connu, pour ce qui concerne le calcul des bornes, le cas général se réduit au cas des variétés semi-abéliennes : soient G un groupe algébrique commutatif défini sur un corps de nombres k et X une sous-variété de G. Soient V le sous-groupe vectoriel maximal de V, $A := G/V$ la variété semi-abélienne correspondante et Y l'image de

X dans A. Alors le nombre de composantes irréductibles de la clôture de Zariski de $X \cap Tor(G)$ est borné par le nombre de composantes irréductibles de la clôture de Zariski de $Y \cap Tor(A)$. En effet, la projection de Y sur A est injective sur la torsion de G et induit donc une bijection entre les composantes irréductibles de la clôture de Zariski de $X \cap Tor(G)$ (dont on sait que ce sont des translatés de sous-groupes) et celles de $Y \cap Tor(A)$, (dont on sait aussi que ce sont des translatés de sous-groupes).

Il suffit donc de montrer, sans avoir à se préoccuper des bornes, que pour un groupe commutatif arbitraire il est bien vrai que l'intersection de X avec la torsion est réunion finie de translatés de sous-groupes algébriques. Comme nous l'avons dit plus haut, il y a plusieurs démonstrations possibles utilisant deux premiers de bonne réduction distincts.

Nous allons en donner une ici qui, en admettant un résultat de Jean-Pierre Serre sur l'indépendance des groupes de Galois l-adiques des variétés semi-abéliennes, permet de conclure très rapidement (voir [Se], pages 33-34 et 56-59 pour le cas des variétés abéliennes, merci à Jean-Pierre Serre de m'avoir confirmé la généralisation au cas des variétés semi-abéliennes). On a donc un groupe algébrique connexe commutatif défini sur un corps de nombres k et X une sous-variété de G. On se donne deux premiers de bonne réduction $\mathfrak{p}$ et $\mathfrak{t}$, de caractéristiques résiduelles distinctes p et t, les polynômes $F_p(T)$ et $F_t(T)$ et les automorphismes $\sigma_p, \sigma_t \in Gal(\mathbb{Q}^{alg}/k)$ correspondants donnés par 3.2. Le résultat de Serre entraîne que $L = k(Tor_{p'}(G)) \cap k(Tor_p(G))$ est une extension galoisienne finie de k, au-dessus de laquelle $k(Tor_{p'}(G))$ et $k(Tor_p(G))$ sont linéairement disjoints. Donc si $m = [L : k]$, il existe $\tau \in Gal(\mathbb{Q}^{alg}/L)$ qui étend σ_p^m sur la torsion première à p et qui étend σ_t^m sur la p-torsion. Si $f_1, \ldots, f_{2d}$ sont les racines de $F_p(T)$ et $g_1, \ldots, g_{2d}$ sont les racines de $F_t(T)$, on pose $J(T) = \prod_{i=1}^{2d}(T - f_i^m)(T - g_i^m)$. Alors $J(\tau)$ s'annule sur la torsion de G. On se place dans un corps de différence générique (K, τ) qui étend $(\mathbb{Q}^{alg}, \tau)$; par 3.6, $X \cap Ker(J(\tau))$ est une combinaison booléenne finie de sous-ensembles spéciaux de $G(K)$. La même démonstration que pour 3.7 montre qu'alors la clôture de Zariski de $X \cap Tor(G)$ est bien une réunion finie de translatés de sous-groupes algébriques de G. Mais, pour ce qui concerne le calcul du nombre de translatés, la définition explicite de $J(T)$ en fonction des deux polynômes F_p et F_t dépend de $[L : k]$.

4. AUTRES APPLICATIONS

Nous terminons en mentionnant deux autres applications des critères de modularité dans les corps de différence génériques. La première est due à Hrushovski pour un premier cas, puis à T. Scanlon, et la seconde, qui elle utilise des résultats en caractéristique p démontrés dans [ChHrPe], à T. Scanlon.

4.1. La conjecture de Tate-Voloch

J. Tate et J.F. Voloch ont conjecturé l'existence d'une borne pour la distance des points de torsion d'une variété semi-abélienne à une sous-variété ([TaVo]) :

CONJECTURE 4.1. — *Soit A une variété semi-abélienne définie sur $\mathbb{C}_p$ et soit X une sous-variété de A. Il existe une constante c telle que si $a \in Tor(G)$, et que la distance p-adique de a à X est inférieure à c, alors $a \in X(\mathbb{C}_p)$.*

$\mathbb{C}_p$ est la complétion de $\mathbb{Q}_p^{alg}$ pour la norme p-adique, qu'on note $|-|_p$. Si X est une sous-variété de l'espace affine $\mathbb{A}^n$ définie sur $\mathbb{C}_p$, on choisit un système générateur $\{f_1, \ldots, f_n\}$ de l'idéal de définition de X et on définit alors la distance p-adique d'un point a de $\mathbb{A}^n(\mathbb{C}_p)$ à X, $d_p(a, X)$ comme étant le maximum des $|f_i(a)|_p$.

Dans [TaVo] la conjecture est montrée dans le cas des tores.

E. Hrushovski, dans un premier temps, a utilisé la même méthode que pour Manin-Mumford pour établir le résultat pour A définie sur $\mathbb{Q}_p^{alg}$ et pour la torsion première à p, avec l'hypothèse que p est de bonne réduction pour A (communication à Voloch). Cela a ensuite été généralisé par T. Scanlon, toujours par les mêmes méthodes, qui montre la conjecture pour toutes les variétés semi-abéliennes définies sur $\mathbb{Q}_p^{alg}$ dans [Sc1] et [Sc2].

Nous allons indiquer ici brièvement comment on peut déduire du corollaire 2.13 le résultat dans le cas d'une variété semi-abélienne A définie sur $\mathbb{Q}_p$, avec la condition que p est de bonne réduction pour A.

Par 3.2 on a un automorphisme σ tel que la torsion première à p, $Tor_{p'}(A)$ est contenu dans $\{a \in A(\mathbb{Q}_p^{alg}); F(\sigma(a)) = 0\}$, pour $F[T] \in \mathbb{Z}[T]$ sans facteur cyclotomique.

Considérons une suite $(a_i)_{i\in\mathbb{N}}$ d'éléments de $Tor_{p'}(A)$ tels que $d_p(a_i, X)$ tend vers zéro. On va montrer que, pour presque tout i, $a_i \in X$.

Sinon il existe un ultrafiltre (non principal) $\mathfrak{U}$ sur $\mathbb{N}$ tel que $\{i \in \mathbb{N}; a_i \in X\} \notin \mathfrak{U}$. Soit R l'anneau des suites de norme p-adique bornée dans $\mathbb{C}_p$, et l'idéal I de R défini comme l'intersection des I_n, où $I_n = \{r \in R; \{i \in \mathbb{N}; |r(i)|_p \leq p^{-n}\} \in \mathfrak{U}\}$. Alors on peut montrer que $D = R/I$ est un corps, on a un plongement (diagonal) naturel $j : \mathbb{C}_p \mapsto D$ et σ induit un automorphisme de D qu'on appellera aussi σ. Soit a^* l'image de la suite $(a_0, \ldots, a_m, \ldots)$ dans D ; on voit que $a^* \in A(D)$, que $F(\sigma))(a^*) = 0$ et que $a^* \in X(D)$.

On passe dans un gros corps de différence générique (L, σ) étendant (D, σ). Le corollaire 2.13 et le lemme 3.1 nous disent que $X(L) \cap Ker(F(\sigma))$ est contenu dans une réunion finie de translatées de sous-variétés semi-abéliennes de A, chaque translatée étant incluse dans X. En particulier $a^* \in c + B \subset X$, B sous-variété semi-abélienne de A. Soit $\pi : A \mapsto A/B$. Alors la suite des $\pi(a_i)$ doit se rapprocher de $\pi(a^*)$. On a donc que, pour presque tout i, les $\pi(a_i)$ ont même image dans le corps résiduel. Par hypothèse de bonne réduction (appliquée à A/B), on a que la réduction est injective

sur la p'-torsion de A/B. Donc la suite des $\pi(a_i)$ devient constante et égale à $\pi(a^*)$. Cela veut dire que pour presque tout i, $a_i \in c + B$, c'est-à-dire que pour presque tout i, $a_i \in X$.

4.2. Modules de Drinfeld

Enfin, plus récemment, T. Scanlon, en utilisant l'analyse modèle-théorique des corps de différence génériques de caractéristique p et le théorème de dichotomie (du type de 2.4) qui est montré dans [ChHrPe], a démontré l'équivalent de la conjecture de Manin-Mumford pour les modules de Drinfeld ([Sc3]).

RÉFÉRENCES

[Ab] A. ABBES – *Hauteurs et discrétude [d'après L. Szpiro, E. Ullmo et S. Zhang]*, Sém. Bourbaki, vol. 1996/97, exp. n° 825, *Astérisque* **245** (1997), 141-166.

[AbrVo] D. ABRAMOVICH and F. VOLOCH – *Towards a proof of the Mordell-Lang conjecture in characteristic p*, Intern. Math. Research Notices (IMRN) No.2 (1992), 103-115.

[Ax] J. AX – *The elementary theory of finite fields*, Annals of Math. 88 (1968), 239-271.

[Bo] É. BOUSCAREN ed. – *Model Theory and Algebraic Geometry*, Lecture Notes in Mathematics 1696, Springer 1998.

[Bu] A. BUIUM – *Intersections in jet spaces and a conjecture of Serge Lang*, Annals of Math. 136 (1992), 583-593.

[Ch1] Z. CHATZIDAKIS – *Groups definable in ACFA*, in Algebraic Model Theory, B. Hart, A. Lachlan and M. Valeriote eds., NATO ASI Series, Kluwer Academic Publishers 1997.

[Ch2] Z. CHATZIDAKIS – *A survey on the model theory of difference fields*, in Model Theory, Algebra and Geometry, D. Haskell and C. Steinhorn ed., MSRI Publications 2000, 65-96.

[ChHr] Z. CHATZIDAKIS and E. HRUSHOVSKI – *The model theory of difference fields*, Transactions of the A.M.S, Vol. 351 (1999), 2997-3071.

[ChHrPe] Z. CHATZIDAKIS, E. HRUSHOVSKI and Y. PETERZIL – *The model theory of difference fields II*, preprint 1999.

[Coh] R.M. COHN – *Difference algebra*, Tracts in Mathematics 17, Interscience Pub. 1965.

[Col] R. COLEMAN – *p-adic integrals and torsion points on curves*, Annals of Math. 121 (1985), 111-168.

[DaPh] S. DAVID ET P. PHILIPPON – *Minorations des hauteurs normalisées des sous-variétés de variétés abéliennes*, in International Conference On Discrete Mathematics and Number Theory (Tiruchiparelli, 1996), K. Murty and M. Waldschmidt eds., Contemp. Math., 1998, 3-17.

[Du] J.L. DURET – *Les corps faiblement algébriquement clos non séparablement clos ont la propriété d'indépendance*, in Model Theory of Algebra and Arithmetic, L. Pacholski et al. ed., Lecture Notes in mathematics 834, Springer 1980, 135-157.

[Fa] G. FALTINGS – *The general case of Lang's conjecture*, in Symposium in Algebraic Geometry, V. Christante and W. Messing eds., Perspectives in Math. 15, Academic Press , 1994, 175-182.

[Fu] W. FULTON – *Intersection Theory*, Ergebnisse 2, Springer 1984.

[Go] J.B. GOODE – *H.L.M. (Hrushovski-Lang-Mordell)*, Sém. Bourbaki, vol. 1995/96, exp. n° 811, *Astérisque* **241** (1997), 179-194.

[Hi1] M. HINDRY – *Autour d'une conjecture de Serge Lang*, Invent. Math. 94 (1988), 575-603.

[Hi2] M. HINDRY – *Introduction to abelian varieties and the Mordell-Lang conjecture*, in Model Theory and Algebraic Geometry, E. Bouscaren ed., Lecture Notes in Mathematics 1696, Springer 1998.

[Hr1] E. HRUSHOVSKI – *The Mordell-Lang conjecture for function fields*, Journal of the AMS 9 (1996), 667-690.

[Hr2] E. HRUSHOVSKI – *The Manin-Mumford conjecture and the model theory of difference fields*, preprint 1995, à paraître dans Annals of Pure and Applied Logic.

[Hr3] E. HRUSHOVSKI – *The first-order theory of the Frobenius*, preprint 1995.

[HrPi1] E. HRUSHOVSKI and A. PILLAY – *Weakly normal groups*, in Logic Colloquium '85, North Holland 1987, 233-244.

[HrPi2] E. HRUSHOVSKI and A. PILLAY – *Groups definable in local fields and pseudo-finite fields*, Israel J. Math. 85 (1994), 203-262.

[HrSo] E. HRUSHOVSKI and Ž. SOKOLOVIĆ – *Minimal subsets of differentially closed fields*, à paraître dans les Transactions of the AMS.

[HrZi] E. HRUSHOVSKI and B. ZIL'BER – *Zariski Geometries*, Journal of the A.M.S. 9 (1996), 1-56.

[La1] S. LANG – *Division points on curves*, Ann. Mat. Pura Appl. (4) 70 (1965), 229-234.

[La2] S. LANG – *Number Theory III, Diophantine Geometry*, volume 60, Encyclopaedia of Mathematical Sciences, Springer 1991.

[Ma1] A. MACINTYRE – *Generic automorphisms of fields*, Annals of Pure and Applied Logic 88, vol.2-3 (1997), 165-180.

[Ma2] A. MACINTYRE – *Non-standard Frobenius*, en préparation.

[Maz] B. MAZUR – *Abelian varieties and the Mordell-Lang Conjecture*, in Model Theory, Algebra and Geometry, D. Haskell and C. Steinhorn ed., MSRI Publications 2000.

[McQ] M. MCQUILLAN – *Division points on semi-abelian varieties*, Invent. Math. 120 (1995), 143-159.

[Mr] D. MARKER – *Zariski geometries*, in Model Theory and Algebraic Geometry, É. Bouscaren ed., Lecture Notes in Mathematics 1696, Springer 1998.

[Mu] D. MUMFORD – *Abelian varieties*, Oxford University Press, Oxford 1985.

[Pi1] A. PILLAY – *The model-theoretic content of Lang's conjecture* in Model Theory and Algebraic Geometry, É. Bouscaren ed., Lecture Notes in Mathematics 1696, Springer 1998.

[Pi2] A. PILLAY – *ACFA and the Manin-Mumford conjecture*, in Algebraic Model Theory, B. Hart, A. Lachlan and M. Valeriote eds., NATO ASI Series, Kluwer Academic Publishers 1997.

[Pi3] A. PILLAY – *Model Theory and diophantine geometry*, Bull. Am. Math. Soc. 34 (1997), 405-422.

[Ra1] M. RAYNAUD – *Courbes sur une variété abélienne et points de torsion*, Invent. Math. 71 (1983), 207-233.

[Ra2] M. RAYNAUD – *Sous-variétés d'une variété abélienne et points de torsion*, in Arithmetic and Geometry, vol.I, M. Artin and J. Tate eds., Birkhäuser 1983, 327-352.

[Sc1] T. SCANLON – *p-adic distance from torsion points of semi-abelian varieties*, Journal für dir Reine und Angewandte Mathematik 499 (1998), 225-236.

[Sc2] T. SCANLON – *The conjecture of Tate and Voloch on p-adic proximity to torsion*, Intern. Math. Research Notices (IMRN) No. 17 (1999), 909-914.

[Sc3] T. SCANLON – *Diophantine geometry of the torsion of a Drinfeld module*, preprint 1999.

[Se] J.-P. SERRE – *Oeuvres, Collected papers, Volume IV, 1985-1998*, Springer 2000.

[TaVo] J. TATE and J.F. VOLOCH – *Linear forms in p-adic roots of unity*, International Mathematics Research Notices (IMRN) No.12 (1996), 589-601.

[Voj] P. VOJTA – *Integral points on subvarieties of semi-abelian varieties*, Invent. Math. 126 (1996), 133-181.

[We] A. WEIL – *Courbes algébriques et variétés abéliennes*, Hermann 1971.

Élisabeth BOUSCAREN

Université Denis-Diderot Paris 7
Équipe de Logique Mathématique
UFR de Mathématiques (case 7012)
2 place Jussieu
F-75251 Paris Cedex 05
E-mail : elibou@logique.jussieu.fr