Annales de la Faculté des Sciences de Toulouse
MATHÉMATIQUES

RODOLPHE RICHARD

Manin–Mumford topologique fort

Tome XXXIII, n° 2 (2024), p. 419–446.

https://doi.org/10.5802/afst.1776

Publication membre du centre
Mersenne pour l'édition scientifique ouverte
http://www.centre-mersenne.org/
e-ISSN : 2258-7519

Annales de la faculté des sciences de Toulouse Volume XXXIII, n° 2, 2024
pp. 419-446

Manin–Mumford topologique fort (*)

Rodolphe Richard (1)

Résumé. — Cet article fait suite à [15]. Ce dernier décrivait l'adhérence topologique d'une famille d'orbites galoisiennes de points de torsion dans une variété abélienne complexe, donnée sur un corps de type fini. Là où [15] concluait que l'adhérence est une union finie de composantes de sous-groupes de Lie réels, nous montrons que ces composantes sont des translatées de sous-variétés abéliennes. Les arguments utilisés ici, outre les conclusions de [15], utilisent les modules de Tate et se basent sur les théorèmes de Faltings concernant la conjecture de Tate.

Nous donnons aussi des conséquences concernant certains problèmes de dynamique homogène.

Abstract. — In this sequel to [15], we characterise the topological closure of a family of Galois orbits of torsion points of a complex abelian variety, with a model over a field of finite type. Where [15] proved this closure is a finite union of components of real Lie subgroups, we prove here that these components are translates of abelian subvarieties. On top of the conclusions of [15], our arguments work with Tate modules and are based on Faltings's theorems on Tate conjecture.

We also state some consequences concerning some problems in homogeneous dynamics.

Introduction

Cet article fait suite à [15]. Celui-ci présentait une nouvelle preuve de la conjecture de Manin–Mumford, au moyen du critère de Weyl, un résultat d'équidistribution de Pólya et Vinogradov et un théorème de Serre sur les homothéties des modules de Tate réalisées par l'action galoisienne. L'argumentation obtenait en outre des énoncés plus précis d'adhérence en topologie réelle de familles d'orbites galoisiennes. Nous complétons cette argumentation par un usage de la conjecture de Tate sur les endomorphismes, prouvée

(*) Reçu le 12 août 2021, accepté le 21 septembre 2022.

(1) Department of Mathematics, University College London, 25 Gordon St, WC1H 0AY London, United Kingdom — rodolphe.richard@normalesup.org

Article proposé par Laurent Clozel.

par Faltings. Il s'ensuit un énoncé plus fort, et optimal : cette adhérence en topologie réelle est Zariski-fermée. Notre premier énoncé théorème 1.1 résulte déjà d'énoncés d'équidistribution de type Szpiro–Ullmo–Zhang. Si leur travaux portent sur la conjecture de Bogomolov, plus large que la conjecture de Manin–Mumford, leur article original ne concerne que les corps de nombres. Dans ce cadre, nous le retrouvons ici par une autre preuve, peut-être plus accessible. Les démonstrations utilisées ici permettent également (voir théorème 1.2) de traiter d'orbites de groupes plus généraux[(1)] que les groupes de Galois, pour peu qu'ils satisfont les propriétés : de la conjecture de Tate ; et du résultat de Serre.

Plan de l'article

La section 1 formule et commente l'énoncé principal, le théorème 1.1. La section 1.1 donne, au delà des orbites galoisiennes, un théorème 1.2 plus général que nous obtenons. Ce théorème 1.2 est un énoncé intéressant en soi en dynamique, et le lecteur uniquement intéressé par les orbites Galoisiennes pourra passer le section 1.1.

La section 2 introduit diverses variantes de modules de Tate, et compare différentes formulations la conjecture de Tate sur les endomorphismes et de semi-simplicité, confirmée par Faltings. Le lemme 2.9 servira à notre exposé de la preuve. La proposition 2.11 adapte [1, Prop. 4.2.1, Lem. 4.2.2] à notre contexte : ici, la démonstration se simplifie. Comme dans [1], la proposition 2.11, combinée au théorème 2.10, permet la construction de sous-variété abéliennes dans l'argument central 3.1.

La section 3 finale démontre le théorème 1.1, adaptant les arguments de [1].

Remerciements

Cet article a été réalisé à la suite d'une invitation de l'auteur par l'IHÉS, bénéficié du financement RPG-2019-180 accordé par le Leverhulme Trust. Qu'ils en soit remerciés. Que soient également remerciés E. Ullmo, G. Baldi et A. Yafaev pour leur enthousiasme, et ce dernier pour ses relectures.

(1) Si on croit à la conjecture de Mumford–Tate, ils ne seront pas toujours des groupes de Galois.

1. Énoncé principal

Nous utiliserons la situation suivante dans tout cet article. Notre espace ambiant sera le groupe de Lie réel $A(\mathbf{C})$ pour une variété abélienne A sur le corps $\mathbf{C}$ des nombres complexe, et on se fixe un sous-corps K de $\mathbf{C}$ sur lequel A est définissable, et tel que K est de type fini sur $\mathbf{Q}$. On voit $A(\mathbf{C})$ comme un groupe de Lie réel, muni de la topologie correspondante, dite « topologie réelle » pour la distinguer de la topologie, plus grossière, « de Zariski ».

Nous distinguons deux sortes de sous-ensembles de $A(\mathbf{C})$.

(1) Les sous-variétés « réelles-spéciales », qui désigneront les ensembles $a+H$ pour un point de torsion a de $\mathbf{C}$ et un sous-groupe de Lie réel et connexe H de $A(\mathbf{C})$.
(2) Les sous-variétés « Zariski-spéciales », qui désigneront les ensembles $a+B(\mathbf{C})$ pour un point de torsion a de $\mathbf{C}$ et une sous-variété abélienne complexe B de A.

Un fois choisies des équations de A sur K, nous avons une action de $\mathrm{Aut}(\mathbf{C}/K)$ sur $A(\mathbf{C})$, non continue. Les points de torsion auront des orbites finies et seront dans $A(\overline{K})$ où $\overline{K}$ est la fermeture algébrique de K dans $\mathbf{C}$. Nous notons U l'image de la représentation

$$\mathrm{Aut}(\mathbf{C}/K) \twoheadrightarrow \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(A(\mathbf{C})_{tors})$$

dans le groupe des automorphismes (abstraits) du groupe $A(\mathbf{C})_{tors} \approx \mathbf{Q}^{2\dim(A)}/\mathbf{Z}^{2\dim(A)}$ des points d'ordre fini.

Théorème 1.1 (Manin–Mumford topologique fort). — *Soit E un ensemble de points de torsion de $A(\mathbf{C})$. Alors l'adhérence, pour la topologie* réelle, *$\overline{U\cdot E}$ de $U\cdot E$ est une union finie de sous-variétés* Zariski-*spéciales.*

Comparons l'énoncé à deux variations, chacune plus faible que le théorème 1.1.

- L'énoncé correspondant pour l'adhérence $\overline{U\cdot E}^{Zar}$ en topologie de Zariski est la conjecture de Manin–Mumford classique. (Voir [10] à propos de la conjecture, [13, 14] pour sa première preuve.)
- L'énoncé correspondant pour une union finie de sous-variétés *réelles*-spéciales est obtenu dans [15] par une autre preuve que celle de [25]. Il suffit à démontrer la conjecture de Manin–Mumford classique, comme le fait [15].

Nous appelons « Manin–Mumford topologique faible » ce dernier, et « Manin–Mumford topologique fort » le théorème 1.1.

Dans le cas des corps nombres, on trouve dans [25] un énoncé plus fort qui a permis aussi de démontrer la généralisation par Bogomolov de la conjecture de Manin–Mumford. Ses auteurs utilisent la géométrie d'Arakelov.

Notre preuve du théorème 1.1 procède en deux étapes.

(1) La première est de montrer que $V := \overline{U \cdot E}$ est une union finie de sous-variétés réelles-spéciales. Soit alors une écriture minimale $V = \bigcup_{i=1}^{c} a_i + H_i$.
(2) La seconde est de montrer que ces H_i sont chacun de la forme $B_i(\mathbf{C})$ pour une sous-variété abélienne complexe B_i.

La première étape a été accomplie dans [15]. C'est notre point de départ. Le présent texte comble la seconde étape.

L'article [15] utilisait l'équidistribution et peu d'information sur le groupe U : il n'utilisait que la structure réelle de $A(\mathbf{C}) \approx \mathbf{R}^{2\dim(A)}/\mathbf{Z}^{2\dim(A)}$ et un résultat de Serre précisant un autre de Bogomolov en direction d'une conjecture de Serre. Voir [15] sur le sujet.

Ici nous nous basons sur les théorèmes de Faltings sur la conjecture de Tate pour les endomorphismes. L'argumentation est parallèle à la seconde partie de [1], et indépendante des outils de [15]. Le point central est la proposition 3.1, adaptée de [1]. Les objets utilisés sont les modules de Tate, et les outils sont de l'algèbre linéaire, les groupes, les suites, l'inclusion-exclusion. (Plus un peu de mesure de Haar, et l'algèbre de Lie d'un tore réel). Combiné avec [15] cela donne une preuve accessible et relativement courte du théorème 1.1, admettant un théorème de Faltings et un autre de Serre (voir [15]).

Pour être complet, mentionnons que ce résultat de Faltings était déjà apparu dans la preuve par Serre de son résultat. Et que certains arguments repris de [1] ont d'abord germé avec pour objectif ce texte.

1.1. Orbites adéliques

Le reste de l'article ne dépend pas de ce numéro.

1.1.1.

Nos preuves utilisent des propriétés bien identifiées de l'action galoisienne : la conjecture de Tate (et dans [15] une forme partielle de celle de Lang). Cela permet d'aborder le problème, intéressant en soi, des énoncés du type du théorème 1.1 pour des sous-groupes $U \leqslant \mathrm{Aut}(A(\mathbf{C})_{tors}) \approx \mathrm{GL}(2\dim(A), \widehat{\mathbf{Z}})$ plus généraux. Le sous-groupe des homothétie $\widehat{\mathbf{Z}}^\times \simeq \mathrm{GL}(1, \widehat{\mathbf{Z}}) \leqslant \mathrm{GL}(2\dim(A), \widehat{\mathbf{Z}})$ agit sur $A(\mathbf{C})_{tors}$ par : si $a \in A_{tors}$ est d'ordre N et si $\lambda \in \widehat{\mathbf{Z}}^\times$ a image $k + N\mathbf{Z}$ dans $\mathbf{Z}/(N)^\times$, alors

$$\lambda(a) = a + \cdots + a = k \cdot a.$$

Pour $c \in \mathbf{Z}_{\geqslant 1}$ on définit, au sens de [1, 15] le « sous-groupe de Lang »

$$L(c) := \{\lambda^c \mid \lambda \in \mathbf{Z}^\times\} \leqslant \mathrm{GL}(1, \widehat{\mathbf{Z}}),$$

agissant par homothéties sur $A(\mathbf{C})_{tors}$.

Théorème 1.2. — *Soit* $U \leqslant \mathrm{Aut}(A(\mathbf{C})_{tors}) \approx \mathrm{GL}(2\dim(A), \widehat{\mathbf{Z}})$ *un sous-groupe*

- *tel qu'il existe* $c \in \mathbf{Z}_{\geqslant 1}$ *tel que* U *contient* $L(c)$ *;*
- *satisfaisant la conjecture de Tate comme dans le théorème 2.1.*

Soit $E \subseteq A(\mathbf{C})_{tors}$ *un sous-ensemble.*

Alors la conclusion du théorème 1.1 vaut : l'adhérence, pour la topologie réelle, $\overline{U \cdot E}$ *de* $U \cdot E$ *est une union finie de sous-variétés* Zariski-*spéciales.*

On peut affaiblir la premièrer hypothèse en la remplaçant, au choix,

- par une condition sur E : que $\overline{U \cdot E}$ est une union finie de sous-variétés *réelles*-spéciales.
- ou par une condition plus faible sur $L(U) := U \cap \mathrm{GL}(1, \widehat{\mathbf{Z}})$.

Si cela permet bien d'utiliser les arguments [15, §3], une condition suffisante sur $L(U)$ doit être la conjonction ces deux propriétés :

- Pour tout p, et toute suite $(\zeta_n)_{n \in \mathbf{Z}_{\geqslant 0}}$ de racines de l'unité, d'ordre respectifs (exactement) p^n,
$$L(U) \cdot \zeta_n \text{ s'équidistribue dans } U(1).$$
- Pour toute suite $(p_n)_{n \in \geqslant \mathbf{Z}_0}$ de nombres premiers distincts, et $(\zeta_n)_{n \in \mathbf{Z}_{\geqslant 0}}$ une suite de racines de l'unité, d'ordre respectifs p_n,
$$L(U) \cdot \zeta_n \text{ s'équidistribue dans } U(1).$$

Lorsque U est une image galoisienne : la première propriété équivaut au résultat de Bogomolov [7] sur la conjecture de Lang (voir encore [7] sur les conséquences pour Manin–Mumford) ; la seconde propriété est plus faible que le résultat de Serre.(2)

(2) Pour les images de l'action du groupe de Galois, Lang conjecture $\forall\, p \gg 0, \#L(U) \cdot \zeta_p = p - 1$, et Serre a démontré $\exists\, C \in \mathbf{R}_0, \forall\, p, \#L(U) \cdot \zeta_p \geqslant p/C$. Des avancées de Bourgain

1.1.2. Dynamique Homogène

Dans le théorème 1.2, on doit pouvoir remplacer $A(\mathbf{C})$ par $\mathbf{R}^d/\mathbf{Z}^d$ et $\mathrm{End}(A)$ par une sous-algèbre $N \leqslant M(n,\mathbf{Z})$ telle que $N \otimes \mathbf{Q}$ est une $\mathbf{Q}$-algèbre semi-simple. Cela donnerait l'énoncé suivant, laissé au conditionnel, que nous nous contenterons d'affirmer.

Énoncé 1.3. — *Soit* $U \leqslant \mathrm{Aut}(\mathbf{Q}^d/\mathbf{Z}^d) \approx \mathrm{GL}(n,\widehat{\mathbf{Z}})$ *un sous-groupe fermé*

- *tel qu'il existe* $c \in \mathbf{Z}_{\geqslant 1}$ *tel que* U *contient* $L(c)$ *;*
- *et vérifiant la conjecture de Tate (relativement à* N *sur* $\mathbf{Z}^d$*) au sens de la définition 2.2.*

Soit $E \subseteq \mathbf{Q}^n/\mathbf{Z}^n$ *un sous-ensemble. Alors, dans* $\mathbf{R}^n/\mathbf{Z}^n$*, on peut écrire l'adhérence*

$$\overline{U\cdot E} = (a_1 + H_1) \cup \cdots \cup (a_k + H_k)$$

avec $a_i \in \mathbf{Q}^n/\mathbf{Z}^n$ *et où* H_i *est de la forme* $H_i = Im(z_i)$ *avec* $z_i \in N$*.*

Il s'agit alors plus proprement d'un problème de dynamique homogène, et on est tenté d'appliquer les théorèmes de rigidité tels ceux de Ratner.

Concernant les variétés de Shimura, soulignons [17, 18, 20] qui, comme ici, part des théorèmes de Faltings, et les combine aux théorèmes de Ratner p-adiques via [20, 21], permettant de travailler sur des problèmes analogues, mais avec la limitation principale qu'on ne peut travailler qu'en un nombre fini de places : ici on travaillerait avec $\mathbf{Z}[1/N]^d/\mathbf{Z}^d \subseteq \mathbf{Q}^d/\mathbf{Z}^d$.

Les théorèmes [2, 3, 4, 5, 6], substantiels, de Y. Benoîst et J.-F. Quint étendent des résultats de Ratner à certains groupes plus généraux, y compris discrets. Seule la version archimédienne est utile dans cette approche, même s'ils démontrent des versions p-adiques. Des applications directes au problème ci-dessus sont donnés par ces auteurs ([6, Cor. 1.10] pour la forme finale, voir aussi [5, Cor. 1.4], [3, Th. 1.3, Cor. 1.4]). On peut réinterpréter en termes adéliques leur hypothèses en utilisant un théorème de Weisfeiler [11, 26] et Nori [12, §5] : leur résultats concernent les sous-groupes d'une forme proche de $U = M(\widehat{\mathbf{Z}}) \leqslant \mathrm{GL}(d,\widehat{\mathbf{Z}})$, et les hypothèse de Benoîst–Quint imposent à M d'être *défini sur* $\mathbf{Q}$, et *semisimple*, et de type non compact sur $\mathbf{R}$.

Notre approche est radicalement différente :

et Konyagin [8] semblent autoriser des groupes $L(U)$ considérablement plus petits, ceux soumis à $\exists\, \varepsilon > 0, \#L(U)\cdot\zeta_p \geqslant p^{\varepsilon}$.

- Nous utilisons les homothéties contenues dans U pour produire de l'équidistribution, déduite de résultats anciens. Nous n'auront jamais $U \leqslant \mathrm{SL}(d, \widehat{\mathbf{Z}})$ (sauf $d = 0$), tandis qu'ils requièrent que leur groupe M soit semi-simple. Nos hypothèses sont opposées.
- Plus radicalement, nous utilisons l'analogue de la conjecture de Tate (vite dit : « le centralisateur de U est défini sur $\mathbf{Q}$ ») qui est considérablement plus faible que leur hypothèse, l'analogue de la conjecture de Mumford–Tate (vite dit :« U est défini sur $\mathbf{Q}$ ».)

1.1.3. Manin–Mumford en famille géométrique

Nous projetons d'établir dans une suite la variante de [1] en caractéristique nulle en combinant l'équidistribution de [15] avec des idées de [16] pour travailler en famille.

2. Modules de Tate et Théorèmes de Faltings

Après avoir introduit nos notations, dans la section 2.1, pour les modules de Tate, nous énoncerons des formulations, dans la section 2.2, de théorèmes de Faltings qui nous seront commodes. Nous donnons ensuite, dans les sections 2.3 and 2.4, plusieurs conséquences des théorèmes de Faltings qui nous serviront dans notre preuve du théorème 1.1.

2.1. Modules de Tate et Images de représentations galoisiennes

Pour tout entier $N \in \mathbf{Z}_{\geqslant 1}$ on note $A(\mathbf{C})[N]$ le sous-groupe des points d'ordre divisant N. Ainsi nous retrouvons $A_{tors} = \bigcup_{N \in \mathbf{Z}_{\geqslant 1}} A(\mathbf{C})[N]$.

Pour chaque nombre premier p, on note

$$T_p \approx {\mathbf{Z}_p}^{2\dim(A)} \quad \text{et} \quad V_p = T_p \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$$

les variantes usuelles des modules de Tate p-adiques.(3)

L'action de U sur A_{tors} induit une représentation $\mathbf{Z}_p$-linéaire notée

$$\rho_p : U \longrightarrow \mathrm{GL}_{\mathbf{Z}_p}(T_p).$$

(3) On pourra utiliser comme définition $T_p = \mathrm{Hom}^{cont.}(\mathbf{Z}_p, A_{tors})$ (groupe des homomorphismes continus, c.-à-d. localement constants).

Le morphisme ρ_p est continu pour la topologie profinie de U héritée de $\mathrm{Gal}(\overline{K}/K)$ et la topologie p-adique sur $\mathrm{GL}_{\mathbf{Z}_p}(T_p)$.

La variante adélique, $\widehat{\mathbf{Z}}$-linéaire est, où p parcourt les nombres premiers, donnée par

$$\widehat{T} := \prod_p T_p \approx \widehat{\mathbf{Z}}^{2\dim(A)},$$

et est munie de la représentation $\widehat{\mathbf{Z}}$-linéaire continue $\widehat{\rho} := \prod_p \rho_p$. La représentation $\widehat{\rho}$ est fidèle, et nous identifierons U à son image notée encore

$$U \leqslant \mathrm{GL}_{\widehat{\mathbf{Z}}}(\widehat{T}). \tag{2.1}$$

Les images de U par ρ_p son notées U_p, et l'inclusion $U \leqslant \prod_p U_p$ vaut. Au sujet de l'inclusion inverse, on peut consulter [22, 24].

2.2. Formulation uniforme de la conjecture de Tate

Ce numéro discute de plusieurs formulations des conjectures de Tate de semi-simplicité et des isogénies pour les variétés abéliennes. En caractéristique nulle elles ont été démontrées par Faltings. La variante que nous utilisons, les énoncés 2.1 et 2.2, issue des mêmes résultats de Faltings, est un peu plus fine que les énoncés couramment rencontrés, dont nous discutons quelques-uns pour mettre en relief la formulation qui nous servira.

Nous notons $\mathrm{End}(A/K)$ la $\mathbf{Z}$-algèbre des endomorphismes de A qui sont défini sur K et $\mathrm{End}(A/\mathbf{C})$ celle de ceux définis sur $\mathbf{C}$. La sous-algèbre $\mathrm{End}(A/K)$ est le lieu fixe d'une action continue de $\mathrm{Gal}(\overline{K}/K)$, et quitte à passer à une extension finie, $\mathrm{End}(A/K) = \mathrm{End}(A/\mathbf{C})$. C'est la forme suivante de la conjecture de Tate sur laquelle nous reposons.

On renvoie à [19, §4.6] pour le théorème 2.1. On rappelle que K est supposé de type fini sur $\mathbf{Q}$.

Théorème 2.1 (Faltings, voir [19, Th. 4.8]). — *On suppose* $\mathrm{End}(A/K) = \mathrm{End}(A/\mathbf{C})$. *Alors, au sens de la définition 2.2, le groupe U donné par* (2.1) *satisfait la conjecture de Tate, relativement à $N = \mathrm{End}(A/K)$ agissant sur $\widehat{T} \simeq T \otimes \widehat{\mathbf{Z}}$ pour $T = H_1(A(\mathbf{C}); \mathbf{Z})$.*

On a séparé la définition pour permettre un traitement axiomatique de nos arguments. (cf. section 1.1.)

Définition 2.2. — *Soit $T \approx \mathbf{Z}^d$, soit $N \leqslant \mathrm{End}_{\mathbf{Z}}(T)$ une algèbre telle que $N \otimes \mathbf{Q}$ est semi-simple, et soit $U \leqslant \mathrm{GL}_{\widehat{\mathbf{Z}}}(T \otimes \widehat{\mathbf{Z}})$ un sous-groupe compact. On dit que U satisfait la conjecture de Tate (relativement à N sur T) si*

(T) *Pour tout $C \in \mathbf{Z}_{\geqslant 1}$, il existe $M \in \mathbf{Z}_{\geqslant 1}$ tel que pour tout sous-groupe ouvert $U' \leqslant U$ d'indice au plus C, on a, comme sous-algèbres de* $\mathrm{End}_{\widehat{\mathbf{Z}}[1/M]}\widehat{T} \otimes_{\widehat{\mathbf{Z}}[1/M]} \widehat{\mathbf{Z}}[1/M]$,

$$(\widehat{\mathbf{Z}}[1/M])\big[U'\big] \text{ est la commutante de } N \otimes \widehat{\mathbf{Z}}[1/M]. \tag{2.2}$$

La forme la plus classique de la conjecture de Tate est la suivante.

Théorème 2.3 (Faltings). — *Pour tout nombre premier p,*

- *le commutant de U_p dans* $\mathrm{End}_{\mathbf{Q}_p}(V_p)$ *est* $\mathrm{End}(A/K) \otimes \mathbf{Q}_p$.
- *et l'action de U_p est semi-simple*[(4)] *sur V_p.*

De manière équivalente[(5)], *comme sous-algèbre de* $\mathrm{End}_{\mathbf{Q}_p}(V_p)$, *l'algèbre* $\mathbf{Q}_p[U_p]$ *engendrée par U_p égale la commutante de* $\mathrm{End}(A) \otimes \mathbf{Q}_p$.

Une formulation plus forte suivante est exposée par [9] comme conséquence des énoncés de finitude de Faltings.

Théorème 2.4 (Faltings, [9, Th. 2.7]). — *Le commutant de* $\mathrm{End}(A)$ *dans* $\mathrm{End}_{\widehat{\mathbf{Z}}}(\widehat{T})$ *est commensurable à la sous-$\widehat{\mathbf{Z}}$-algèbre, que nous notons $\widehat{\mathbf{Z}}[U]$, engendrée $\widehat{\mathbf{Z}}$-linéairement par U dans* $\mathrm{End}_{\widehat{\mathbf{Z}}}(\widehat{T})$.

L'énoncé 2.4 revient au cas $C = 1$ de (2.2) : il existe M tel que (2.2) vaut pour $U' = U$. Cet énoncé 2.4 équivaut à la conjonction de 2.3 et du suivant.

Théorème 2.5 (Faltings). — *Il existe M tel que pour tout nombre premier p ne divisant pas M, et en notant $U(p)$ l'image de U dans* $\mathrm{End}_{\mathbf{F}_p}(A[p]) \simeq \mathrm{End}_{\widehat{\mathbf{Z}}}(\widehat{T}) \otimes \mathbf{F}_p$, *on a, comme sous-algèbres de* $\mathrm{End}_{\mathbf{F}_p}(A[p])$,

$$\mathbf{F}_p\big[U(p)\big] \text{ est la commutante de } \mathrm{End}(A) \otimes \mathbf{F}_p. \tag{2.3}$$

De la même manière, le théorème 2.1 se ramène à la conjonction de théorème 2.3 et de ce théorème 2.6.

Théorème 2.6 (Faltings). — *On suppose* $\mathrm{End}(A/K) = \mathrm{End}(A/\mathbf{C})$. *Pour tout entier $C \in \mathbf{Z}_{\geqslant 1}$, il existe M tel que pour tout nombre premier p ne divisant pas M, et en notant $U(p)$ l'image de U dans* $\mathrm{End}_{\mathbf{F}_p}(A[p]) \simeq \mathrm{End}_{\widehat{\mathbf{Z}}}(\widehat{T}) \otimes \mathbf{F}_p$, *on a, pour tout sous-groupe U' de $U(p)$ d'indice au plus C, comme sous-algèbres de* $\mathrm{End}_{\mathbf{F}_p}(A[p])$,

$$\mathbf{F}_p\big[U'\big] \text{ est la commutante de } \mathrm{End}(A) \otimes \mathbf{F}_p. \tag{2.4}$$

(4) C.-à-d. :Tout sous-espace U_p-invariant a un supplémentaire U_p-invariant.

(5) La semi-simplicité est cachée dans celle de $\mathrm{End}(A) \otimes \mathbf{Q}$, donc de son commutant, donc de U_p. Dans l'autre sens il faut connaître le bicommutant d'une sous-algèbre semi-simple de $\mathrm{End}_{\mathbf{Q}_p}(V_p)$. On peut passer à $\overline{\mathbf{Q}_p}$: où il s'agit d'algèbres de matrices ; voir aussi [23, I.§4,II.§6]

2.2.1. Dépendance en A

Nos preuves n'utiliseront pas ces énoncés pour la variété abélienne A elle-même, mais plutôt pour une variété abélienne quotient $A \twoheadrightarrow A'$. Lorsqu'on travaille avec l'action du groupe de Galois, les théorèmes de Faltings s'appliquent à A' tout autant qu'à A. Dans les généralisations discutées à la section 1.1, on souhaite travailler avec un groupe U plus général, soumis uniquement à la définition 2.2, et nous aurons besoin que l'action de U dans A'_{tors} satisfasse encore la définition. Les propriétés de la définition 2.2 se transmettent au passage de A à A'. Il va exister $M \in \mathbf{Z}_{\geqslant 1}$, lié au nombre de composantes du noyau de $A \to A'$, tel que $\widehat{T}(A')[1/M]$ se relève en un facteur direct et U-invariant de $\widehat{T}(A)[1/M]$.

2.3. Spectre adélique

L'artifice suivant aura l'avantage de traiter uniformément[6] les phénomènes à p fixé et ceux lorsque p varie : on remplace dans les démonstrations $\mathbf{Q}_p$ par un certain corps L du style suivant.

Pour tout morphisme d'anneau $\widehat{\mathbf{Z}} \to L$ vers un corps L, nous introduisons la notation

$$T_L = \widehat{T} \otimes_{\widehat{Z}} L \quad \text{et} \quad \rho_L = \widehat{\rho} \otimes_{\widehat{Z}} L : U \longrightarrow \mathrm{GL}_L(T_L). \tag{2.5}$$

Si on se limitait aux morphismes continus, il n'y aurait guère que les usuels

$$\widehat{\mathbf{Z}} \longrightarrow\!\!\!\!\!\rightarrow \mathbf{F}_p = L \quad \text{et} \quad \widehat{\mathbf{Z}} \longrightarrow \mathbf{Z}_p \hookrightarrow \mathbf{Q}_p$$

pour la topologie discrète sur $\mathbf{F}_p$ et ultramétrique sur $\mathbf{Q}_p$.

Nous voulons autoriser tout homomorphisme abstrait (aucune considération topologique sur L). Les corps L utilisés dans cet article viendront du lemme 2.9, et se factorisent

$$\widehat{\mathbf{Z}} \longrightarrow \prod_p \mathbf{F}_p \longrightarrow L.$$

[6] Il semble que la forme théorème 2.4 se ramène à théorème 2.3 étendu à tout T_L pour L un corps de caractéristique nulle du type discuté ici.

On peut décrire ces derniers morphismes[7], dont l'existence demande l'axiome du choix[8].

Une conséquence de (2.2) de théorème 2.4 est la suivante.

Corollaire 2.7. — *Soit* $\widehat{\mathbf{Z}} \to L$ *vers un corps* L *de caractéristique nulle.*

$$L[\rho_L(U')] \text{ est la commutante de } \operatorname{End}(A) \otimes \widehat{\mathbf{Z}} \otimes L \text{ dans } \operatorname{End}_L(T_L).$$

Démonstration. — Notons R l'anneau $\widehat{\mathbf{Z}}[1/M]$ de (2.2), et notons Z la commutante de $N = \operatorname{End}(A)$ dans $M = \operatorname{End}_{\mathbf{Z}}(H_1(A(\mathbf{C}); \mathbf{Z}))$, et Z_R celle de $\operatorname{End}(A) \otimes R$ dans $\operatorname{End}_R(T_R)$ et Z_L celle de $\operatorname{End}(A) \otimes L$ dans $\operatorname{End}_L(T_L)$.

Par (2.2), on sait que $R[U']$ est la commutante Z_R de $N \otimes R$ dans $M \otimes R$. Il va suivre que

$$L[\rho_L(U')] = R[U'] \otimes_R L = Z_R \otimes_R L.$$

On a les inclusions faciles $Z \otimes R \leqslant Z_R$ et $Z_R \otimes L \leqslant Z_L$. Plongeons $\mathbf{Z} \leqslant \mathbf{Q}$ dans L et M dans $M \otimes L \simeq \operatorname{End}_L(T_L)$. Comme N engendre linéairement N_L, on sait que Z_L est le commutant de N dans M_L. Donc

- on a $Z_L \cap M = Z$
- et Z_L est défini sur $\mathbf{Q}$.

Donc $Z_L = (Z \cap (M \otimes \mathbf{Q})) \otimes L$. Enfin $Z_{\mathbf{Q}} = Z \otimes \mathbf{Q}$ car M est un réseau de $M \otimes \mathbf{Q}$. $\square$

La conséquence suivante du corollaire 2.7 va nous servir.

Corollaire 2.8. — *Soit* $\widehat{\mathbf{Z}} \to L$ *vers un corps* L *de caractéristique nulle, et soit* $W \leqslant T_L$ *un sous-espace* U*-invariant. Alors il existe un élément de* $\operatorname{End}(A) \otimes L$ *(que l'on peut choisir idempotent) et dont l'image est* W*.*

Démonstration. — Par le corollaire 2.7, on sait que $L[\rho_L(U)]$ est la commutante Z_L de $\operatorname{End}(A) \otimes L$. Comme $\operatorname{End}(A) \otimes L$ est semi-simple, son commutant Z_L aussi. L'espace W étant $L[\rho_L(U)]$-invariant, il admettra un supplémentaire W' stable par Z_L. Il sera en particulier stable par U. Donc le

[7] Ils correspondront aux ultraproduits de corps finis, chacun attaché à un ultrafiltre $\mathfrak{U}$ de la suite des nombre premiers. Le noyau de ce morphisme se décrit comme suit. Il est décrit par les suites $(\lambda_p)_p$ qui sont nulles le long de cet ultrafiltre : il existe un élément Σ de $\mathfrak{U}$ – un tel Σ est un ensemble de nombre premiers, et dépendra de $(\lambda_p)_p$ – tel que $\lambda_p = 0$ pour les p situés dans Σ.

L'existence de ces ultrafiltres et de ces corps passe par l'axiome du choix. L'ensemble des ultrafiltres s'identifie à la compactification maximale de Stone-Čech de l'ensemble des nombres premiers, et aux spectre de $\prod_n \mathbf{F}_{p_n}$ comme espace topologique pour la topologie de Zariski.

[8] [...] qui apparaît dans le théorème des zéros de Hilbert dans la preuve du lemme.

projecteur u sur W de noyau W' est Z_L équivariant, il est dans le commutant de Z_L. Or c'est $\mathrm{End}(A)\otimes L$. $\square$

2.3.1. Caractéristique variable

On développe ici certains argument utilisés plus tard.

LEMME 2.9. — *Soit une suite de nombre premiers distincts p_n et considérons la projection correspondante*

$$\widehat{\mathbf{Z}} \longrightarrow R := \prod_n \mathbf{F}_{p_n}.$$

(1) *Choisissons pour tout $n\in\mathbf{Z}_{\geqslant 0}$ un élément $a_n\in T_{\mathbf{F}_{p_n}}\simeq A[p_n]$ non nul, et notons $a_\infty=(a_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ comme élément de T_R. Alors il existe un morphisme $R\to L$ vers un corps de caractéristique nulle, telle que l'image a_L de a_∞ dans T_L est non nulle.*

(2) *Soit un morphisme $R\to L$ vers un corps. Choisissons pour tout $n\in\mathbf{Z}_{\geqslant 0}$ un sous-espace vectoriel $V_n\leqslant T_{\mathbf{F}_{p_n}}\simeq A[p_n]$. Notons $V_R=\prod_n V_n$ comme R-module. Soit aussi une constante $C\in\mathbf{Z}_{\geqslant 1}$ telle que pour tout n, l'espace V_n est stable par un sous-groupe (ouvert) H_n d'indice au plus C de U. Alors il existe $M\in\mathbf{Z}_{\geqslant 1}$ tel que*
   - *le $R[1/M]$-module $V_R\otimes_R R[1/M]$ de $T_{R[1/M]}$ est stable par U ;*
   - *si M est inversible dans L, alors le L-espace vectoriel $V_R\otimes_R L$ dans T_L est stable par U.*

Traitons la première partie.

Démonstration. — Posons $k=2\dim(A)$. Pour chaque n on choisit un isomorphisme $A[p_n]\simeq {\mathbf{F}_{p_n}}^k$ de $\mathbf{F}_{p_n}$-modules. Il s'ensuit un isomorphisme $T_R\simeq R^k$ de R-modules et un isomorphisme $T_R\otimes\mathbf{Q}\simeq R\otimes\mathbf{Q}^k$ de $R\otimes\mathbf{Q}$-modules, et pour tout homomorphisme d'anneaux $R\to L$, un isomorphisme $T_L\simeq L^k$ de L-modules.

On note a'_n l'image de a_n dans ${\mathbf{F}_{p_n}}^k$ et a'_∞ l'image de a_∞ dans R^k. On a $a'_n\neq 0$ pour tout n.

Étudions le morphisme $R\to R\otimes\mathbf{Q}\simeq R[1/2,1/3,\ldots]$. Son noyau est formé des éléments de R annulés par au moins un entier $M\in\mathbf{Z}_{\geqslant 1}$. Donc a'_∞ est dans le noyau de $R^k\to R\otimes\mathbf{Q}^k$ si et seulement si il est annulé par au moins un entier $M\in\mathbf{Z}_{\geqslant 1}$. Comme les p_n sont distincts et en nombre infini, il existera n tel que $p_n\nmid M$. Dès lors $M\cdot a'_n\neq 0$ car a'_n est non nul et M est inversible dans $\mathbf{F}_{p_n}$. A fortiori $M\cdot a'_\infty\neq 0$. Comme c'est vrai pour tout entier $M\in\mathbf{Z}_{\geqslant 1}$ l'image, disons b_∞, de a'_∞ dans $R\otimes\mathbf{Q}^k$ est non nulle.

Étudions le morphisme $R\otimes\mathbf{Q}\to\prod_{\mathfrak{p}}\kappa(\mathfrak{p})$ où $\mathfrak{p}$ décrit l'ensemble des idéaux premiers de $R\otimes\mathbf{Q}$ et où $\kappa(\mathfrak{p})$ désigne le corps des fractions de $(R\otimes\mathbf{Q})/\mathfrak{p}$. On sait que le noyau est le nilradical $\mathfrak{N} := \sqrt{(0)} = \bigcap_{\mathfrak{p}}\mathfrak{p}$. Les $\mathbf{F}_{p_n}$ sont des corps, donc des anneaux réduits. L'anneau produit R est donc réduit. Et le localisé $R\otimes\mathbf{Q} = R[1/2, 1/3, \ldots]$ est donc réduit. Son nilradical $\mathfrak{N}$ est donc nul, et $R\otimes\mathbf{Q}\to\prod_{\mathfrak{p}}\kappa(\mathfrak{p})$ est injectif.

Par conséquent, l'application

$$(R\otimes\mathbf{Q})^k \longrightarrow \prod_{\mathfrak{p}}\kappa(\mathfrak{p})^k \tag{2.6}$$

est injective. L'image de b_∞ est donc non nulle : il existe $\mathfrak{p}_0$ tel que l'image de b_∞ par $(R\otimes\mathbf{Q})^k\to\kappa(\mathfrak{p}_0)^k$ est non nulle. Ainsi, l'image de a'_∞ par $R^k\to\kappa(\mathfrak{p}_0)^k$ est non nulle.

De manière équivalente, en vertu des isomorphismes choisi, l'image de $a_\infty\in T_R$ dans $T_{\kappa(\mathfrak{p}_0)}$ est non nulle.

Il existe des morphismes $\mathbf{Q}\to R\otimes\mathbf{Q}$ et $R\otimes\mathbf{Q}\to\kappa(\mathfrak{p}_0)$. Donc le corps $\kappa(\mathfrak{p}_0)$ est de caractéristique nulle.

Le corps $L=\kappa(\mathfrak{p}_0)$ a les propriétés demandées. □

La seconde situation va venir du théorème 2.6.

Démonstration. — Soit M l'entier donné par le théorème 2.6. Rappelons $V_R = \prod_n V_n$. Il suffit de montrer que pour tout n, le $\mathbf{F}_p\otimes R[1/M]$-module $V_n\otimes R[1/M]$ est stable par U. Si p divise M, on a $\mathbf{F}_p\otimes R[1/M]=0$ et $V_n=0$ et rien à montrer. Sinon on a $\mathbf{F}_p\otimes R[1/M]\simeq\mathbf{F}_p$ et $V_n\otimes R[1/M]\simeq V_n$. On sait que V_n est H_n invariant. Donc les éléments de $\mathbf{F}_p[H_n]$ stabilisent V_n. On sait que U commute à $\mathrm{End}(A)$ et donc U est contenu dans son centralisateur, disons Z_n, de $\mathrm{End}(A)\otimes\mathbf{F}_{p_n}$ dans $\mathrm{End}_{\mathbf{F}_{p_n}}(A[p_n])$. Par définition de M, on peut appliquer théorème 2.6 et $U\subseteq Z_n=\mathbf{F}_p[H_n]$: tout élément de U stabilise V_n. □

2.4. Modules de Tate transcendants

Mettant à profit le plongement complexe $K\leqslant\mathbf{C}$, nous pouvons définir une variante sur $\mathbf{Z}$ des modules de Tate, mais dont la construction n'est plus algébrique. La construction se généralise à tout sous-groupe de Lie réel $H\leqslant A(\mathbf{C})$, supposé connexe pour simplifier.

On note

$$H_1(H;\mathbf{Z})$$

le groupe d'« homologie de Betti entier ». On pourra utiliser l'homologie singulière ou poser $H_1(H;\mathbf{Z}) = \pi^1(H)$, le groupe fondamental pointé à l'origine. Pour tout anneau L on notera encore

$$H_1(H;L) := H_1(H;\mathbf{Z}) \otimes L.$$

On sait[9] que $H_1(H;\mathbf{R})$ s'identifie à l'algèbre de Lie de H et que l'exponentielle de groupe de Lie $\exp_H : H_1(H;\mathbf{R}) \to H$ induit la suite exacte courte

$$0 \longrightarrow H_1(H;\mathbf{Z}) \longrightarrow H_1(H;\mathbf{R}) \xrightarrow{\exp_H} H \longrightarrow 0.$$

Il suit une identification, où $H[N] := H \cap A(\mathbf{C})[N]$,

$$H_1(H;\mathbf{Z}) \otimes \mathbf{Z}/(N) \simeq \frac{1}{N} H_1(H;\mathbf{Z})/H_1(H;\mathbf{Z}) \simeq H[N].$$

Lorsque H est une variété abélienne $A(\mathbf{C})$, on en déduit une identification

$$H_1(H;\mathbf{Z}) \otimes \mathbf{Z}_p \simeq T_p \quad \text{et} \quad H_1(H;\mathbf{Z}) \otimes \widehat{\mathbf{Z}} \simeq \widehat{T}.$$

Lorsque H est un sous-groupe de Lie connexe de $A(\mathbf{C})$, la même construction induit des sous-modules que nous noterons

$$T_p(H) := H_1(H;\mathbf{Z}) \otimes \mathbf{Z}_p \leqslant T_p \quad \text{et} \quad \widehat{T}(H) := H_1(H;\mathbf{Z}) \otimes \widehat{\mathbf{Z}} \leqslant \widehat{T}.$$

En revanche ces modules n'hériteront en général pas d'une représentation de U.

2.4.1. Critère d'algébricité

La situation est éclaircie par la situation suivante, déduite du théorème de Faltings.

Théorème 2.10. — *Soit $\widehat{\mathbf{Z}} \to L$, comme en section 2.3, et supposons L de caractéristique nulle.*

Soit W un sous-espace vectoriel de T_L. Alors W est de la forme $H_1(B(\mathbf{C});\mathbf{Z}) \otimes_{\mathbf{Z}} L \simeq T_L(B)$ pour une sous-variété abélienne $B \leqslant A$ si et seulement si :

- *On peut écrire W sous la forme $W = V \otimes L$ pour un sous-espace vectoriel $V \leqslant H_1(A(\mathbf{C});\mathbf{Q})$;*
- *et l'espace W est laissé stable sous l'action ρ_L de U sur T_L.*

[9] Une 1-forme $\mathbf{R}$-différentielle fermée ω (on peut la choisir invariante) donnera la forme linéaire qui envoie une classe de lacet (choisi différentiable) $[\gamma]$ sur l'intégrale $\int_\gamma \omega$.

Les conditions sont clairement nécessaires. On démontre leur suffisance pour l'existence de B.

Démonstration. — Dans $M = \mathrm{End}(H_1(A(\mathbf{C}); \mathbf{Z}))$ soit $Z = Z_M(N)$ l'algèbre commutante de $N = \mathrm{End}(A)$ dans M. Il suit de la conjecture de Tate que W est U-invariant si et seulement il est invariant par

$$Z \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}} \otimes_{\widehat{\mathbf{Z}}} L \simeq Z \otimes L.$$

Dans notre contexte $V \otimes L$ est $Z \otimes L$-invariant et donc V est Z-invariant. Comme l'action de $\mathrm{End}(A)$ est semi-simple, celle de Z aussi. Il existe un sous-espace supplémentaire V' à V dans $H_1(A(\mathbf{C}); \mathbf{Q})$. Dès lors le projecteur $\pi \in \mathrm{End}(H_1(A(\mathbf{C}); \mathbf{Q})) \simeq M \otimes \mathbf{Q}$ d'image V et noyau V' est Z-équivariant, donc appartient au commutant de Z dans $M \otimes \mathbf{Q}$, le bicommutant de N, qui est aussi $N \otimes \mathbf{Q}$. Quitte à multiplier par l'éventuel dénominateur $d \in \mathbf{Z}_{\geqslant 1}$, on aura un endomorphisme $m = \pi \cdot d$ de A tel que $m(H_1(A(\mathbf{C}); \mathbf{Q})) = V$. Comme $A(\mathbf{C})$ est un groupe de Lie complexe et connexe, son image $H = m(A(\mathbf{C}))$ aussi. Nécessairement $H = B(\mathbf{C})$ pour une sous-variété abélienne $B \leqslant A$. On détermine H, comme sous-groupe de Lie réel connexe, par son algèbre de Lie $\mathfrak{h}$. Celle-ci se calcule dans $H_1(A(\mathbf{C}); \mathbf{R})$ et vaut $m(H_1(A(\mathbf{C}); \mathbf{R})) = m(H_1(A(\mathbf{C}); \mathbf{Q})) \otimes \mathbf{R}$. On en déduit $V = H_1(B(\mathbf{C}); \mathbf{Q})$, puis, dans T_L,

$$\begin{aligned} W = V \otimes L &= H_1(B(\mathbf{C}); \mathbf{Z}) \otimes L \\ &= H_1(B(\mathbf{C}); \mathbf{Z}) \otimes \widehat{\mathbf{Z}} \otimes_{\widehat{\mathbf{Z}}} L = \widehat{T}(B) \otimes_{\widehat{\mathbf{Z}}} L = T_L(B). \qquad \square \end{aligned}$$

On utilisera la conséquence suivante.

Proposition 2.11. — *Soit*

$$W \leqslant T_L \quad \textit{et} \quad V \leqslant H_1(A(\mathbf{C}); \mathbf{Q})$$

deux sous-espaces vectoriels, sur L resp. $\mathbf{Q}$, tels que

- *l'espace W est invariant par U,*
- *et on a l'inclusion $W \leqslant V \otimes L$.*

Alors il existe au moins une sous-variété abélienne $B \leqslant A$, et il existe un unique sous-groupe de Lie réel connexe $B(\mathbf{C}) \leqslant H \leqslant A(\mathbf{C})$ tels que

- *on a $V = H^1(H; \mathbf{Q})$,*
- *on a $W \leqslant T_L(B) \leqslant V \otimes L$.*

L'idée est de relier les sous-variétés abéliennes aux endomorphismes dans $\mathrm{End}(A)$ ou plutôt à des idempotents de $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes \mathbf{Q}$. La preuve de [1] se simplifie.

- Car on dispose d'une homologie sur $\mathbf{Q}$: pas besoin des artifices de passer par les idéaux d'algèbres semi-simples ; on travaille directement sur des sous-espaces vectoriels sur $\mathbf{Q}$;
- pas de problème de ramification de la p-torsion en caractéristique p : on s'épargne la théorie de Hodge p-adique.

Démonstration. — La première conclusion sur H est un simple rappel, seule la seconde conclusion mérite une démonstration. D'après le Théorème il suffit de trouver $X \leqslant V$ tel que $W \leqslant X \otimes L$ et $X \otimes L$ est invariant par U.

On considère l'algèbre $M = \mathrm{End}_{\mathbf{Q}}(H_1(A(\mathbf{C}); \mathbf{Q}))$ et identifions $N = \mathrm{End}^0(A)$ à une sous-algèbre de M.

Le point crucial est que le commutant $N \otimes L$ de U dans $M \otimes L$ est défini sur $\mathbf{Q}$: par Faltings, c'est $Z \otimes L$ où on note Z le commutant de N dans M (bicommutant de U). Comme, par Faltings, les actions sont semi-simples, on aura la caractérisation suivante

(A) Un sous-espace vectoriel W' de T_L est invariant par U si et seulement si il est invariant par $Z\otimes L$, et si et seulement si il est invariant par Z.

Construisons la variété algébrique $\mathcal{X}$ sur $\mathbf{Q}$ telle que pour une extension de corps $F/\mathbf{Q}$

$$\mathcal{X}(F) = \{W' \leqslant H_1(A(\mathbf{C}); \mathbf{Q}) \otimes F \mid W' = Z \cdot W' \text{ et } W' \leqslant V \otimes F\}.$$

C'est bien une variété algébrique (fermée dans l'union disjointe des grassmanniennes), et elle est définie sur $\mathbf{Q}$. Donc $\mathcal{X}(\overline{\mathbf{Q}})$ est invariant par $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

Dès lors le sous-espace vectoriel $\overline{X} = \sum_{W' \in \mathcal{X}(\overline{\mathbf{Q}})} W'$ sur $\overline{\mathbf{Q}}$ de $H_1(A(\mathbf{C}); \overline{\mathbf{Q}})$ est invariant sous $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Vu dans les grassmanniennes, c'est donc un $\overline{\mathbf{Q}}$-point définissable sur $\mathbf{Q}$. Le $\mathbf{Q}$-point sous-jacent est une espace vectoriel $X \leqslant H_1(A(\mathbf{C}); \mathbf{Q})$ tel que $X \otimes \overline{\mathbf{Q}} = \overline{X}$. (On a paraphrasé Hilbert 90).

On vérifie $X \leqslant V$: on peut passer à $\overline{\mathbf{Q}}$, et cela vient de la construction de $\overline{X}$. (On peut aussi remarquer que X est un point de $\mathcal{X}(\mathbf{Q})$).

Pareillement on voit que X est invariant par Z, et donc $X \otimes L$ par U.

La propriété algébrique suivante étant vraie sur $\overline{\mathbf{Q}}$, elle vaut pour toute extension de corps $F/\mathbf{Q}$:

(B) Dans $H_1(A(\mathbf{C}); \mathbf{Q})$, tout point de $\overline{X}(K)$ (un sous-espace Z invariant et contenu dans $V \otimes K$) est contenu dans $X \otimes K$.

D'après (A), notre W est un L-point de $\mathcal{X}$; par (B) pour $F = L$ on trouve $W \leqslant X \otimes L$. Comme voulu : on a $X \leqslant V$, l'espace $X \otimes L$ est invariant par U, et $W \leqslant X \otimes L$. □

3. Argumentation

3.1. Démonstration du résultat principal

On déduit ici le théorème 1.1, à partir de [15] et de la proposition 3.1 du numéro suivant.

Démonstration. — Par [15] on peut écrire

$$V := \overline{U\cdot E} = \bigcup_{i=1}^{c} a_i + H_i, \tag{3.1}$$

pour des points de torsion $a_i \in A(\mathbf{C})$ et $H_i \leqslant A(\mathbf{C})$ des sous-groupes de Lie réels connexes.

On peut remplacer E par $U\cdot E$, et on aura alors $U'\cdot E = U\cdot E = E$ pour tout sous-groupe $U' \leqslant U$.

On suppose l'écriture (3.1) minimale, ce qui implique que, pour $1 \leqslant i < j \leqslant c$, les ensembles a_i+H_i et a_j+H_j s'intersectent proprement dans chacun. L'intersection sera même d'intérieur vide dans $a_i + H_i$. Il suit que

$$(a_i + H_i)^* := a_i + H_i \smallsetminus \bigcup_{j\in\{1;\ldots;c\}\smallsetminus\{i\}} a_j + H_j$$

est un ouvert de V et est dense dans $a_i + H_i$. Donc $E \cap (a_i + H_i)^*$ est dense dans $(a_i + H_i)^*$, et

$$\overline{(a_i + H_i)^* \cap E} = \overline{(a_i + H_i)^*} = a_i + H_i. \tag{3.2}$$

Décomposons en union disjointe $\{1;\ldots;c\} = I \sqcup J$ suivant la dichotomie

- on a $i \in I$ si le groupe de Lie réel H_i est un groupe de Lie complexe $D_i(\mathbf{C})$;
- on a $i \in J$ sinon : le groupe de Lie réel H_i n'est un groupe de Lie complexe.

Préparation. — Une étape de préparation est de se ramener à $I = \emptyset$. Posons

$$E_{\mathbf{C}} = E \cap \bigcup_{i\in I} a_i + H_i \quad \text{et} \quad E_{\mathbf{R}} = E \smallsetminus E_{\mathbf{C}}.$$

Soit $M \in \mathbf{Z}_{\geqslant 1}$ un multiple commun des ordres des a_i et soit U' le noyau de $U \to \mathrm{Aut}(A[M])$ de sorte que les a_i sont fixés par U'.

Soit $i \in I$. Alors D_i est l'image d'un endomorphisme $A \to A$ défini sur $\mathbf{C}$, et par suite $D_i(\mathbf{C})_{tors}$ est invariant par U, car U commute à cet endomorphisme. Donc $a_i + D_i(\mathbf{C})_{tors}$ est invariant par U'. Il suit que $E_{\mathbf{C}}$ est invariant par U', et par suite $E_{\mathbf{R}}$ est invariant par U'.

Grâce à (3.2), on a en outre

$$\overline{E_{\mathbf{R}}} = \bigcup_{j\in J} a_j + H_j. \tag{3.3}$$

On peut donc remplacer U par U', l'ensemble E par $E_{\mathbf{R}}$ et l'écriture (3.1) par (3.3).

La préparation est finie. □

Si E est vide, on a terminé. On suppose donc E non vide. Par l'absurde tout revient à montrer qu'au moins l'un des H_i est complexe. On applique la proposition 3.1 et obtenons

$$\bigcup_{i=1}^{c} a_i + H_i = \overline{U\cdot E} \subseteq F + \bigcup_{i=1}^{c} D_i \quad \text{et} \quad \bigcup_{i=1}^{c} D_i \subseteq \bigcup_{i=1}^{c} H_i.$$

Soit $M \in \mathbf{Z}_{\geqslant 1}$ un multiple commun de l'ordre des $f \in F$ et des a_i. Appliquant l'isogénie $a \mapsto M \cdot a : A \to A$, qui est propre en topologie réelle, on aura

$$\bigcup_{i=1}^{c} H_i = M \cdot \bigcup_{i=1}^{c} a_i + H_i = M \cdot \overline{U\cdot E} \subseteq M \cdot \left(F + \bigcup_{i=1}^{c} D_i\right) = \bigcup_{i=1}^{c} D_i \subseteq \bigcup_{i=1}^{c} H_i.$$

Par double inclusion

$$\bigcup_{i=1}^{c} H_i = \bigcup_{i=1}^{c} D_i.$$

Argumentant comme avec (3.2) on peut reformuler ainsi : les éléments maximaux, pour l'inclusion, de $\{H_1; \ldots; H_c\}$ sont les mêmes que les éléments maximaux de $\{D_1; \ldots; D_c\}$. Ces ensembles sont non vides par l'hypothèse $E \neq \emptyset$, et sont finis. Il existe donc un des H_i qui est maximal et il sera donc de la forme D_j, autrement dit un groupe de Lie complexe : c'est la contradiction annoncée. □

3.2. Argument central

L'énoncé suivant et son argumentation sont adaptés de [1]. Les énoncés dont il dépend ont été adaptés aux sections 2.3 and 2.4.1 rappelé dans la section 3.3. Sous la forme énoncée les hypothèses sur U valent lorsque U est l'image galoisienne telle que dans le théorème 1.1.

Proposition 3.1. — *Soit U l'image de* $\mathrm{Gal}(\overline{K}/K)$ *ou un groupe pour lequel vaut le théorème 2.1 pour* $N = \mathrm{End}(A/\mathbf{C})$, *et supposons* $\mathrm{End}(A/K) = \mathrm{End}(A/\mathbf{C})$.

Soit E un ensemble de points de torsion de $A(\mathbf{C})$ et soit des sous-variétés réelles spéciales $b_1+H_1, \ldots, b_c+H_c$, notées comme en (1) *(à la p. 421), telles que*

$$U \cdot E \subseteq \bigcup_{i=1}^{c} b_i + H_i.$$

Notons D_i la plus grande sous-variété abélienne complexe *de A telle que $D_i(\mathbf{C}) \leqslant H_i$.*

Alors il existe un ensemble fini F de points de torsion tel que

$$U \cdot E \subseteq F + \bigcup_{i=1}^{c} D_i(\mathbf{C}).$$

Démonstration. — Comme $E \subseteq A(\mathbf{C})_{tors}$ est au plus dénombrable, il peut s'écrire $E = \{a_n \,|\, n \in \mathbf{Z}_{\geqslant}0\}$.

Soit M un multiple commun des ordres des b_i, de sorte que $M \cdot b_1 = \cdots = M \cdot b_c = 0$ dans A. La conclusion étant insensible au passage à l'isogénie $a \mapsto M \cdot a : A \to A$, nous pouvons, en remplaçant a_n par $M \cdot a_n$, remplacer les b_i par $M \cdot b_i$: bref, nous pouvons supposer que les b_i sont tous nuls.

Notons $\mathrm{ord}(a_n + D_i)$ l'ordre de $a_n + D_i$ comme élément de A/D_i. Quitte à agrandir F pour le mettre de la forme $A[M]$, la conclusion se récrit

$$\max_{n \geqslant 0} \min_{1 \leqslant i \leqslant c} \mathrm{ord}(a_n + D_i) \leqslant M. \tag{3.4}$$

Nous pouvons alors argumenter par l'absurde, en supposant qu'il n'existe pas de M tel que dans (3.4). On peut donc passer à une sous-suite $(a_n)_{n \in \mathbf{Z}_{\geqslant 0}}$ telle que pour chacun des D_i,

$$\lim_{n \to \infty} \mathrm{ord}(a_n + D_i) = \infty. \tag{3.5}$$

La stratégie va être de construire, pour l'un des indices i, une sous-variété abélienne D' dans A/D_i qui est :

(I) non nulle ;
(II) et telle que $D'(\mathbf{C}) \subseteq H_i/D_i(\mathbf{C})$.

La contradiction viendra alors de la composante neutre D'' du sous-groupe algébrique image inverse de D' par $A \to A/D_i$: sera une variété abélienne contenant D_i strictement et telle que $D''(\mathbf{C}) \leqslant H_i$. C'est en conflit avec la définition de D_i supposée maximale pour ces propriétés.

On va s'aider des a_n pour construire des espaces U-invariants dans des modules de Tate.

Nous trouvons d'abord un indice i convenable. Fixons n. Comme les H_i recouvrent $U \cdot a_n$, on peut estimer

$$\#U \cdot a_n = \#U \cdot a_n \cap \bigcup_i H_i = \# \bigcup_i (U \cdot a_n) \cap H_i \leqslant \sum_i \#U \cdot a_n \cap H_i.$$

Par l'absurde il va donc exister au moins un indice i tel que

$$\#(U \cdot a_n) \cap H_i \geqslant \frac{1}{c} \#U \cdot a_n, \tag{3.6}$$

car sinon $\#U \cdot a_n \leqslant \sum_i \#U \cdot a_n \cap H_i < c \cdot \frac{1}{c} \#U \cdot a_n = \#U \cdot a_n$. Nous choisissons un indice i tel que dans (3.6), et, quitte à extraire le supposerons indépendant de n. Ce sera le i recherché.

Dorénavant, posons $D = D_i$, et $H = H_i$ et $H' = H/D_i(\mathbf{C})$, et $A' = A/D$, et $a''_n = a_n + D/D$ l'image de a_n dans A/D, qui est contenue dans H', et enfin d_n l'ordre de a''_n dans A'. Comme U commute à $\mathrm{End}(A)$ il préserve le sous-groupe $D(\mathbf{C})_{tors}$, et l'action passe au quotient à $A'(\mathbf{C})_{tors}$.

Dans (3.5), quitte à extraire, l'un des deux cas se présente

(III) il existe un facteur premier p tel que p^{k_n} divise d_n avec $k_n \to \infty$;
(IV) il existe des facteurs premiers p_n tels que p_n divise d_n et $p_n \to \infty$.

Nous introduisons dans A' les multiples de a''_n suivants

$$a'_n = m \cdot a''_n \quad \text{pour } m = \frac{d_n}{p^{k_n}}, \text{ resp. } m = \frac{d_n}{p_n}.$$

L'intérêt est que a'_n est d'ordre exactement p^{k_n}, resp. p_n. Nous affirmons qu'en outre

$$\#(U \cdot a'_n) \cap H' \geqslant \frac{1}{c} \#U \cdot a'_n. \tag{3.7}$$

Démontrons l'affirmation (3.7).

Démonstration. — Nous considérons l'application

$$\pi : u \cdot a_n \longmapsto m \cdot u \cdot a_n + D.$$

Elle est équivariante donc ses fibres sont en bijection les unes avec les autre. On aura donc, pour $X \subseteq U \cdot a_n$ et $Y \supseteq \pi(X)$,

$$\frac{\#\pi(Y)}{\#U \cdot a'_n} \geqslant \frac{\#\pi(X)}{\#U \cdot a'_n} = \frac{\# \overset{-1}{\pi}(\pi(X))}{\#U \cdot a_n} \geqslant \frac{\#X}{\#U \cdot a_n}. \tag{3.8}$$

Posons $X = (U \cdot a_n) \cap H$ et $Y = (U \cdot a'_n) \cap H'$. Alors $\pi(X) \subseteq Y$. Vu (3.6) et (3.8) on obtient (3.7). $\square$

Pour le corps $L = \mathbf{Q}_p$ (resp. un corps L construit depuis la suite p_n), nous construisons à la section 3.2.1, resp. 3.2.2 un « point limite » a'_∞ dans $T_L(A')$ qui satisfait

(V) l'élement a'_∞ est non nul dans $T_L(A')$
(VI) l'élément a'_∞ appartient au sous-espace vectoriel $T_L(H')$
(VII) chacun des $u(a'_\infty) := \rho_L(u)(a'_\infty)$ appartient aussi à $T_L(H')$.

Avant ces constructions voyons d'abord comment terminer l'argumentation par l'absurde.

Dès lors le sous-L-espace vectoriel $W = \langle U \cdot a'_\infty \rangle$ engendré par $U \cdot a'_\infty$ est

- non nul il contient l'élément a'_∞ qui est non nul par (V),
- invariant par U (par construction)
- et contenu dans l'espace $T_L(H')$ par (VII).

Utilisons[10] la proposition 2.11 pour $W := W$ et $V := T(H')$ (on a $T_L(H') = T(H') \otimes L$) : il existe un espace intermédiaire

$$W \leqslant V \otimes_{\mathbf{Q}} L \leqslant T_L(H')$$

avec $V \leqslant H_1(A/D(\mathbf{C}); \mathbf{Q})$ défini sur $\mathbf{Q}$ (donné par $T_L(B)$ dans la proposition 2.11) et $V \otimes_{\mathbf{Q}} L$ invariant par U. Par le critère théorème 2.10, on a $V = H_1(D'(\mathbf{C}); \mathbf{Q})$ pour une sous-variété abélienne D' de A'.

C'est la variété abélienne recherchée : vérifions (I) et (II).

- Comme W est non nul, $V \otimes L$ aussi, donc V tout autant, et finalement la condition (I) est satisfaite.
- De $V = H_1(D'(\mathbf{C}); \mathbf{Q}) \leqslant T(H') = H_1(H/D(\mathbf{C}); \mathbf{Q})$ vient $H_1(D'(\mathbf{C}); \mathbf{R}) \leqslant H_1(H/D(\mathbf{C}); \mathbf{R})$. Comme ces derniers s'identifient aux algèbres de Lie, et que $D'(\mathbf{C})$ est un groupe de Lie réel connexe, on a bien $D'(\mathbf{C}) \leqslant H/D(\mathbf{C})$. La condition (II) est satisfaite.

Ce qui conclut le raisonnement par l'absurde. Il ne nous reste que la construction de a'_∞ et l'étude des $u(a'_\infty)$. □

À ce point il y a lieu de traiter les cas (III) et (IV) séparément.

3.2.1. Construction dans le cas p-adique

L'objectif est d'obtenir $a'_\infty \in T_p(A')$ satisfaisant (V), (VII) et (VII) pour $L = \mathbf{Q}_p$. On va construire a'_∞ comme limite p-adiques de relevés

[10] La remarque 2.2.1 intervient ici à propos des généralisations de la section 1.1.

des a'_n à $T_p(A')$, montrer l'indépendance de a'_∞ au choix des relevés, étudier la compatibilité à l'action de U, et utiliser les nombreux $u_n \cdot a'_n$ qui sont dans $U \cdot a'_n \cap H'[p^{k_n}]$ avant d'utiliser le lemme 3.3.

Nous notons $|\ |$ une valeur absolue p-adique et munissons $T_p(A') \approx \mathbf{Z}_p{}^{2\dim_{\mathbf{C}}(A')}$ d'une norme $\|\ \|$. Alors $T_p(A')$ et $T_p(A') \smallsetminus p \cdot T_p(A')$ sont compacts.

Pour tout entier $k \in \mathbf{Z}_{\geqslant 0}$ les applications suivantes sont surjectives,

$$\pi_k : T_p(A') \twoheadrightarrow T_p(A') \otimes_{\mathbf{Z}_p} \mathbf{Z}/(p^k) \simeq A'[p^k],$$

$$\text{resp.}\quad \pi'_k = \pi_k \restriction_{T_p(H')} : T_p(H') \twoheadrightarrow H'[p^k].$$

Nous pouvons donc choisir pour chaque n l'un des $\alpha_n \in T_p(A')$ tels que de $\pi_{k_n}(\alpha_n) = a'_n$.

Comme k_n diverge nous pouvons, quitte à extraire, supposer $k_n \neq 0$ pour tout n. Comme a'_n est d'ordre exactement p^{k_n}, nous aurons $a'_n \notin pA'[p^{k_n}]$ et donc α_n évolue dans le compact $T_p(A') \smallsetminus p \cdot T_p(A')$. Quitte à extraire, il y aura une limite a'_∞, non nulle.

Pour un autre choix $(\alpha'_n)_{n \in \mathbf{Z}_{\geqslant 0}}$, on aura $\alpha_n - \alpha'_n \in \ker(\pi_{k_n}) = p^{k_n} T_p$ d'où

$$\|\alpha_n - \alpha'_n\| \leqslant |p|^{k_n}. \tag{3.9}$$

Dès lors $(\alpha'_n)_{n \in \mathbf{Z}_{\geqslant 0}}$ convergera (critère de Cauchy) et aura encore limite a'_∞.

L'application π_k est $\mathrm{GL}_{\mathbf{Z}_p}(T_p(A'))$-équivariante et donc U-équivariante. Pour toute suite $(u_n)_{n \in \mathbf{Z}_{\geqslant 0}}$ dans U, convergeant vers une limite u_∞, on a

$$\pi_{k_n}(u_n \cdot \alpha_n) = u_n \cdot a_n \text{ et convergence } \lim_{n \in \mathbf{Z}_{\geqslant 1}} u_n \cdot \alpha_n = u_\infty \cdot a'_\infty. \tag{3.10}$$

Notons μ la mesure de probabilité de Haar sur U et posons $\Sigma_n = \{u \in U \mid u \cdot a'_n \in H'[p^{k_n}]\}$. (C'est un ouvert et un fermé de U.) Alors (3.7) se récrit

$$\mu(\Sigma_n) \geqslant \frac{1}{c}.$$

Quitte à extraire Σ_n va converger pour la distance de Hausdorff vers une autre partie compacte Σ_∞ de U. Rappelons que l'on aura alors $\mu(\Sigma_\infty) \geqslant 1/c$, par exemple en utilisant(11) l'énoncé [16, Lem. 4.2].

Par définition, pour tout u_∞ dans Σ_∞ il existe une suite $(u_n)_{n \in \mathbf{Z}_{\geqslant 0}} \in \prod_{n \in \mathbf{Z}_{\geqslant 0}} \Sigma_n$ telle que $u_\infty = \lim\,(u_n)_{n \in \mathbf{Z}_{\geqslant 0}}$. Comme $b_n := u_n \cdot a'_n$ est dans $H'[p^{k_n}]$ il existe un relèvement β_n dans $T_p(H')$ tel que $\pi_k(\beta_n) = b_n$.

(11) On prend $Z_i = \Sigma_i$ et μ_i la restriction à Z_i de la mesure de Haar de U. Quitte à extraire μ_i converge vers une mesure μ_∞, de masse au moins $1/c$, et on a $\mu(\Sigma_\infty) \geqslant \mu_\infty(\mathrm{Supp}(\mu_\infty)) \geqslant 1/c$.

D'après (3.10) la suite $\beta'_n = u_n \cdot \alpha_n$ converge vers $u_\infty \cdot a'_\infty$, et comme β'_n est un autre relèvement de $(b_n)_{n\in\mathbf{Z}_{\geqslant 0}}$, on aura, pareillement que dans (3.9),

$$\lim\,(\beta'_n)_{n\in\mathbf{Z}_{\geqslant 0}} = \lim\,(\beta_n)_{n\in\mathbf{Z}_{\geqslant 0}} = u_\infty \cdot a'_\infty.$$

Comme $(\beta_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ évolue dans le fermé $T_p(H')$ on a en outre

$$u_\infty \cdot a'_\infty = \lim\,(\beta_n)_{n\in\mathbf{Z}_{\geqslant 0}} \in T_p(H').$$

Bref l'élément a'_∞ est dans $T_p(H') \smallsetminus p \cdot T_p(H')$ et c'est donc un élément non nul de $V_p(H') = T_p(H') \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Par ailleurs

$$\Sigma_\infty \cdot a'_\infty \subseteq T_p(H') \subseteq V_p(H') \ \text{ avec } \ \frac{\mu(\Sigma_\infty)}{\mu(U)} \geqslant \frac{1}{c}.$$

Soit μ' la mesure de probabilité U-invariante sur $U \cdot a'_\infty$. C'est la mesure image, par l'application $u \mapsto u \cdot a'_\infty$ de μ' : on a donc $\mu'(\Sigma_\infty \cdot a') \geqslant \mu'(\Sigma_\infty) \geqslant \frac{1}{c} \cdot \mu(U) = \frac{1}{c}$. Il s'ensuit l'analogue de (3.7) suivant :

$$\frac{\mu'(U \cdot a'_\infty \cap V_p(H'))}{\mu'(U \cdot a'_\infty)} \geqslant \frac{1}{c}.$$

Par le lemme 3.3 il existera un sous-espace $W \leqslant V_p(H')$ et un sous-groupe $U' = \mathrm{Stab}_U(W) \leqslant U$, ouvert d'indice au plus $C' = 3 \cdot c^{4^{\dim(V_p(H'))}} \leqslant 3^{4^{2\cdot\dim(A)}}$ tel que

$$U \cdot a'_\infty \cap V_p(H') \neq \emptyset.$$

Soit $\alpha \in U \cdot a'_\infty \cap V_p(H')$.

Soit M tel que dans (2.2) avec $C = [U : U'] \leqslant C'$. Appliquons $- \otimes_{\widehat{\mathbf{Z}}[1/M]} \mathbf{Q}_p$ à (2.2) pour $U' = U'$, et pour $U' = U$. On déduit que le commutant de $N \otimes \mathbf{Q}_p$ s'écrit

$$\mathbf{Q}_p[U] = \mathbf{Q}_p[U, 1/M] = \mathbf{Q}_p[U', 1/M] = \mathbf{Q}_p[U'].$$

L'espace W est $U' = \mathrm{Stab}_G(W)$-invariant, et donc $\mathbf{Q}_p[U'] = \mathbf{Q}_p[U]$-stable, et donc U-invariant.

Ainsi,

$$U \cdot a'_\infty = U \cdot \alpha \subseteq W.$$

On a bien (V), (VI) et (VII).

3.2.2. Construction pour un nombre premier variable

L'objectif est d'obtenir le corps L (muni de $\widehat{\mathbf{Z}} \to L$) et $a'_\infty \in T_L(A')$ satisfaisant (V), (VI) et (VII).

Comme on a la divergence $p_n \to \infty$, quitte à extraire nous pouvons supposer que les p_n sont deux-à-deux distincts.

À $n \in \mathbf{Z}_{\geqslant 0}$ fixé, notons $\mathbf{F} = \mathbf{F}_{p_n}$, et $V = T_{\mathbf{F}}$, et G l'image de U dans $\mathrm{GL}_{\mathbf{F}_{p_n}}(T_{\mathbf{F}_{p_n}})$. D'après (3.7) nous pouvons appliquer le lemme 3.2 pour obtenir $W \leqslant T_{\mathbf{F}}$, et $C = 3 \cdot c^{4^{2\dim A}}$ et $H := \mathrm{Stab}_G(W) \leqslant G$. On choisit en outre α_n dans $U \cdot a'_n \cap W$ qui, comme a'_n, est non nul.

On choisit $R \to L$ comme dans le lemme 2.9, pour la variété abélienne A'. Notons W_n ce W et H_n l'image inverse de ce H par $U \to G$. Nous appliquons le lemme 2.9. Alors $W_L = W_R \otimes_R L$ qui est U-invariant. Comme $W_n \leqslant T_{\mathbf{F}_{p_n}}(H')$ pour tout n, on a $W_R \leqslant T_R(H')$ et par suite $W_L \leqslant T_L(H')$. Comme $(\alpha_n)_{n \in \mathbf{Z}_{\geqslant 0}}$ est dans W_R, son image α_L dans $T_L(A')$ sera dans $W_L \leqslant T_L(H')$, et par U-invariance, $u(\alpha_L) \in W_L \leqslant T_L(H')$ pour tout $u \in U$. Par le lemme 2.9 on aura $\alpha_L \neq 0$.

Choisissons $a'_\infty = \alpha_L$. On a bien (V), (VI) et (VII).

3.3. Passage combinatoire à une composante

Nous recopions le lemme suivant de [1] pour la commodité du lecteur. Nous renvoyons à [1] pour sa démonstration, qui en l'esprit est une récurrence descendante sur la dimension et basée sur les inégalités d'inclusion-exclusion.

Lemme 3.2 ([1, Prop. 4.3.2]). — *Soit F un corps, U un groupe, et $U \to \mathrm{GL}(d, F)$ une représentation F-linéaire, et $U \cdot a$ une orbite finie de U dans F^d. Nous considérons un sous-espace vectoriel V et un nombre réel $1 \leqslant C < +\infty$ satisfaisant*
$$\frac{\#U \cdot a \cap V}{\#U \cdot a} \geqslant \frac{1}{C}. \tag{3.11}$$
Alors il existe un sous-espace vectoriel $W \leqslant V$ tel que

- *l'orbite $U \cdot a$ rencontre W : on a $U \cdot a \cap W \neq \emptyset$,*
- *le stabilisateur $H = \mathrm{Stab}_U(W)$ de W dans U est d'indice majoré par*
$$[U : H] \leqslant 3 \cdot C^{4^{\dim(V)}}. \tag{3.12}$$

On peut même choisir W tel que $U \cdot a \cap W$ engendre linéairement W.

Ce qui faut retenir de ce lemme est que l'on passe du sous-espace V contenant une grande proportion de l'orbite $U \cdot a$ à un sous-espace W contenant une sous-orbite d'un grand *sous-groupe* de U. Dans les représentations galoisiennes, on passe à une extension finie du corps de base de degré borné.

Cela s'applique notamment dans une situation où, pour C donné, on a

$$U \cdot a \subseteq V_1 \cup \cdots \cup V_C.$$

En remarquant qu'au moins un des V_i doit vérifier (3.11), on peut se ramener à ce seul V_i au prix de passer à un sous-groupe d'indice fini. En outre on a le contrôle (3.12) sur cet indice. Ce qui nous importe est que cet indice est contrôlé par C et d seulement, indépendamment de F et de U. La formule précise $f(C, \dim(V)) = 3 \cdot C^{4^{\dim(V)}}$ est pour nous anecdotique.

Ce qui nous contraint à utiliser la formulation plus fine du théorème 2.1 des théorèmes de Faltings est que ce contrôle se fait sur l'indice, mais pas sur le sous-groupe H lui-même.

Ce qui nous oblige à travailler sur les ordres de points de torsion avant de passer à une seule composante, pour les mettre sous-la forme p^{k_n} ou p_n est que ce lemme ne vaut que sur des corps, tels $\mathbf{Q}_p$ ou $\mathbf{F}_{p_n}$, mais pas pour des représentations dans $\mathrm{GL}_{\mathbf{Z}/(N)}(A[N]) \simeq \mathrm{GL}(d, \mathbf{Z}/(N))$.

3.3.1. Variante p-adique

Nous utilisons aussi la variante suivante du lemme 3.2. La preuve est la même que [1, Prop. 4.3.2], après modifications indiquées plus bas.

Lemme 3.3. — *Soit p un nombre premier, soit $U \leqslant \mathrm{GL}(d, \mathbf{Q}_p)$ un groupe compact, soit $a \in {\mathbf{Q}_p}^d$ et munissons $U \cdot a$ de la mesure de probabilité U invariante μ'. Nous considérons un sous-espace vectoriel $V \leqslant {\mathbf{Q}_p}^d$ et un nombre réel $1 \leqslant C < +\infty$ satisfaisant*

$$\mu'(U \cdot a \cap V) \geqslant \frac{1}{C}. \tag{3.13}$$

Alors il existe un sous-espace vectoriel $W \leqslant V$ tel que

- *l'orbite $U \cdot a$ rencontre W : on a $U \cdot a \cap W \neq \emptyset$,*
- *le stabilisateur $H = \mathrm{Stab}_U(W)$ de W est ouvert dans U est d'indice majoré par*

$$[U : H] \leqslant 3 \cdot C^{4^{\dim(V)}}. \tag{3.14}$$

On peut même choisir W tel que $U \cdot a \cap W$ engendre linéairement W.

La démonstration de [1, §4.3.2] fonctionne, après les modifications suivantes.

(1) On définit

$$\varepsilon(S) := \mu'(S) \quad \text{et} \quad \varepsilon(W) := \varepsilon(W \cap U \cdot a) = \mu'(W).$$

(2) Pour prouver que $\varepsilon(W)$ admet un maximum, on peut supposer $0 \leqslant \dim(W) \leqslant \dim(V)$ fixé : il suffit alors que $\mu'(W)$ admette un maximum, ce que garantit le lemme 3.4.
(3) Si $[G : G(W)]$ est infini, on choisit une suite infinie de d'éléments distincts $g_1 \cdot G(W), g_2 \cdot G(W), \ldots$
(4) Comme $\mathrm{Stab}_U(W)$ est un sous-groupe fermé dans U d'indice fini, il est aussi ouvert dans U.

Lemme 3.4. — *Reprenons les notations du lemme 3.3.*

Soit $i \in \{0; \ldots; \dim(V)\}$, et soit $\mathbf{G}(i, V)$ la Grassmannienne des sous-espaces vectoriels de dimension i de V. Alors

$$Z \longmapsto \mu'(Z \cap (U \cdot a))$$

est une fonction semi-continue supérieurement sur $\mathbf{G}(i, V)$, et admet un maximum.

Démonstration. — Rappelons que toute fonction semi-continue supérieurement sur un compact admet un maximum. Or $\mathbf{G}(i, V)$ est compact. Il suffit donc d'établir la semi-continuité.

Comme $U \cdot a$ est compact, il existe $k \in \mathbf{Z}$ tel que $U \cdot a \subseteq B := p^k \cdot {\mathbf{Z}_p}^d$. On munit B de la distance usuelle et on munit l'espace $H(B)$ des parties fermées de B de la distance de Hausdorff. Nous affirmons que l'application

$$Z \longmapsto Z \cap B : \mathbf{G}(i, V) \longrightarrow H(B)$$

est une application continue.

Démonstration. — L'application $g \mapsto g \cdot {\mathbf{Z}_p}^i : \mathrm{GL}(d, \mathbf{Z}_p) \mapsto H(V)$ vérifie $d(g_1 \cdot {\mathbf{Z}_p}^i, g_2 \cdot {\mathbf{Z}_p}^i) \leqslant \|g_2 - g_1\|$. Elle est donc continue. Or : elle passe au quotient à la grassmanienne

$$\mathrm{GL}(d, \mathbf{Z}_p)/\operatorname{Stab}_{\mathrm{GL}(d,\mathbf{Z}_p)}({\mathbf{Z}_p}^i) \longrightarrow H(V); \tag{3.15}$$

et l'application quotient $\mathrm{GL}(d, \mathbf{Z}_p) \to \mathrm{GL}(d, \mathbf{Z}_p)/\operatorname{Stab}_{\mathrm{GL}(d,\mathbf{Z}_p)}({\mathbf{Z}_p}^i)$ est ouverte. Cela implique que l'application (3.15) est continue. On peut en déduire l'affirmation. □

En outre $\mu'(Z) = \mu'(Z \cap B)$. Il suffit donc de montrer que

$$K \longmapsto \mu'(K) : H(B) \longrightarrow [0; 1]$$

est une application semi-continue. C'est une conséquence directe de la régularité extérieure de la mesure μ'. (Voir le lemme 3.5). □

Lemme 3.5. — *Soit C un espace compact métrisable, et soit μ une mesure de probabilité dans C. Notons $H(C)$ l'ensemble des parties compactes de C, muni de la topologie de la distance de Hausdorff*[12].

Alors la fonction

$$K \longmapsto \mu(K) : H(C) \longrightarrow [0;1]$$

est semi-continue supérieurement.

Démonstration. — Soit $K \in H(C)$ et démontrons la semi-continuité en K. On choisit une distance $d(\ ,\ )$ sur C.

Les ouverts $U(\varepsilon) = \{c \in C \mid \min_{k\in K} d(c,k) < \varepsilon\}$, pour $\varepsilon > 0$, forment une base de voisinages ouverts dans C du sous-ensemble $K \subseteq C$.

Comme C est compact métrisable, toute mesure de probabilité, dont μ, est extérieurement régulière. Donc, pour tout $\eta > 0$, il existe $\varepsilon_\eta > 0$ tel que $\mu(U(\varepsilon_\eta)) < \mu(K) + \eta$.

Par définition de la distance de Hausdorff, pour tout $\varepsilon > 0$, l'ensemble

$$V(\varepsilon) := \{K' \in H(C) \mid K' \subseteq U(\varepsilon)\}.$$

est un voisinage de l'élément K dans $H(C)$.

Pour $K' \in V(\varepsilon_\eta)$, on a $K' \subseteq U(\varepsilon_\eta)$, et donc

$$\mu(K') \leqslant \mu(U(\varepsilon_\eta)) \leqslant \mu(K) + \eta.$$

Résumons : pour tout $\eta > 0$, il existe un voisinage, en l'occurance $V(\varepsilon_\eta)$, de K dans $H(C)$ sur lequel $\mu \leqslant \mu(K) + \eta$. Ce qu'il fallait démontrer. ☐

Bibliographie

[1] G. Baldi, R. Richard & E. Ullmo, « Manin-Mumford in arithmetic pencils », 2021, `https://arxiv.org/abs/2105.12027`.

[2] Y. Benoist & J.-F. Quint, « Mesures stationnaires et fermés invariants des espaces homogènes », *C. R. Math. Acad. Sci. Paris* **347** (2009), n° 1-2, p. 9-13.

[3] ———, « Mesures stationnaires et fermés invariants des espaces homogènes », *Ann. Math.* **174** (2011), n° 2, p. 1111-1162.

[4] ———, « Mesures stationnaires et fermés invariants des espaces homogènes II », *C. R. Math. Acad. Sci. Paris* **349** (2011), n° 5-6, p. 341-345.

[5] ———, « Stationary measures and invariant subsets of homogeneous spaces (II) », *J. Am. Math. Soc.* **26** (2013), n° 3, p. 659-734.

[12] Si $d(\ ,\ )$ est une distance sur C, c'est, la distance de Hausdorff entre deux fermés non vides $F, F' \subseteq C$ est $\max\{d(f,F') \mid f \in F\} \cup \{d(f',F) \mid f' \in F'\}\}$ où $d(a,B) = \inf\{d(a,b) \mid b \in B\}$. Le fermé vide est un point isolé de $H(C)$.

[6] ———, « Stationary measures and invariant subsets of homogeneous spaces (III) », *Ann. Math.* **178** (2013), nº 3, p. 1017-1059.
[7] F. A. Bogomolov, « Sur l'algébricité des représentations l-adiques », *C. R. Math. Acad. Sci. Paris* **290** (1980), nº 15, p. 701-703.
[8] J. Bourgain & S. V. Konyagin, « Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order », *C. R. Math. Acad. Sci. Paris* **337** (2003), nº 2, p. 75-80.
[9] P. Deligne, « Preuve des conjectures de Tate et de Shafarevitch (d'après G. Faltings) », in *Seminar Bourbaki 1983/84*, Astérisque, vol. 121-122, Société Mathématique de France, 1985, p. 25-41.
[10] S. Lang, « Division points on curves », *Ann. Mat. Pura Appl.* **70** (1965), p. 229-234.
[11] C. R. Matthews, L. N. Vaserstein & B. Weisfeiler, « Congruence properties of Zariski-dense subgroups. I », *Proc. Lond. Math. Soc.* **48** (1984), nº 3, p. 514-532.
[12] M. V. Nori, « On subgroups of $\mathrm{GL}_n(\mathbf{F}_p)$ », *Invent. Math.* **88** (1987), nº 2, p. 257-275.
[13] M. Raynaud, « Courbes sur une variété abélienne et points de torsion », *Invent. Math.* **71** (1983), p. 207-233.
[14] ———, « Sous-variétés d'une variété abélienne et points de torsion », in *Arithmetic and geometry. Papers dedicated to I. R. Shafarevich on the occasion of his sixtieth birthday. Vol. I : Arithmetic*, Progress in Mathematics, vol. 35, 1983, p. 327-352.
[15] R. Richard, « Manin-Mumford par le critère de Weyl », *J. Number Theory* **239** (2022), p. 137-150.
[16] R. Richard & E. Ullmo, « Equidistribution de sous-variétés spéciales et o-minimalité : André–Oort géométrique », with an appendix with Jiaming Chen, 2021, `https://arxiv.org/abs/2104.04439`.
[17] R. Richard & A. Yafaev, « Inner Galois Equidistribution in S-Hecke orbits », 2017, `https://arxiv.org/abs/1711.03009`.
[18] ———, « Topological and equidistributional refinement of the André–Pink–Zannier conjecture at finitely many places », *C. R. Math. Acad. Sci. Paris* **357** (2019), nº 3, p. 231-235.
[19] ———, « Generalised André-Pink-Zannier Conjecture for Shimura varieties of abelian type », 2021, `https://arxiv.org/abs/2111.11216`.
[20] R. Richard, A. Yafaev & T. Zamojski, « Homogeneous Dynamics and Unlikely Intersections », 2018, `https://arxiv.org/abs/1809.03802`.
[21] R. Richard & T. Zamojski, « Limit distribution of Translated pieces of possibly irrational leaves in S-arithmetic homogeneous spaces », 2016, `https://arxiv.org/abs/1604.08494`.
[22] J.-P. Serre, *Cours d'arithmétique*, Le Mathématicien, vol. 2, Presses Universitaires de France, 1977, deuxième édition revue et corrigée, 188 pages.
[23] ———, *Représentations linéaires des groupes finis*, revised éd., Hermann, 1978, 182 pages.
[24] ———, « Un critère d'indépendance pour une famille de représentations ℓ-adiques », *Comment. Math. Helv.* **88** (2013), nº 3, p. 541-554.
[25] L. Szpiro, E. Ullmo & S. Zhang, « Équirépartition des petits points », *Invent. Math.* **127** (1997), nº 2, p. 337-347.
[26] B. Weisfeiler, « Strong approximation for Zariski-dense subgroups of semisimple algebraic groups », *Ann. Math.* **120** (1984), nº 2, p. 271-315.