Invent. math. 94, 575–603 (1988)

Inventiones mathematicae

Autour d'une conjecture de Serge Lang

Marc Hindry

Institut Henri Poincaré, 11 Rue Pierre et Marie Curie, F-75231 Paris Cedex 05, France

Introduction

Manin et Mumford ont posé, à peu près au même moment, la question suivante: «Une courbe de genre au moins deux possède-t-elle un nombre fini de points de torsion dans sa jacobienne?». Dans [20] (voir aussi [21]), Serge Lang a généralisé cette question en conjecturant que l'intersection d'une sous-variété algébrique d'une variété abélienne avec ses points de torsion est décrite par un nombre fini de translatés de sous-groupes algébriques; il ajoutait qu'on pouvait poser la même conjecture sur un tore linéaire et plus généralement sur une extension d'une variété abélienne par un tore.

La question de Manin et Mumford a été résolue affirmativement par Michel Raynaud [30] en utilisant notamment la réduction «mod p^2»; il a également prouvé la conjecture de Lang, pour une variété abélienne, dans [31] – les premiers résultats dans cette direction étant dus à Bogomolov [4]. Michel Laurent [24] a ensuite prouvé la conjecture pour un tore linéaire. La partie principale du présent travail consiste à établir le théorème suivant: «Soit V une sous-variété algébrique d'un groupe algébrique commutatif G défini sur $\mathbb{C}$, alors V contient un nombre fini de translatés de sous-groupes algébriques contenant tous les points de torsion de G situés sur V». Nous donnons une version quantitative et «presque» effective de ce résultat dans le cas où G est un produit d'un groupe linéaire et d'une variété abélienne ou bien quand V est une courbe et esquissons la démonstration générale – développant et étendant les résultats de [14]. Signalons que l'idée de départ est due à Lang (voir [21]) et que c'est un résultat difficile de Serre (voir lemme 12 de ce travail ou théorème 2 de [37]) sur l'image de Galois dans le groupe des homothéties qui nous a permis d'adapter l'idée originelle de Lang. A la demande du referee, insistons toutefois sur le fait que ce résultat de Serre est annoncé dans [37] et a été exposé par Serre dans son cours au collège de France de 1985–86 mais qu'aucune preuve n'en a été publiée à ce jour.

Notons que la méthode permet d'expliciter les bornes et qu'on obtient une généralisation de la question de Manin-Mumford: «Une courbe ne contient qu'un nombre fini de points de torsion dans une jacobienne généralisée (quand elle ne lui est pas égale)».

Il est connu depuis longtemps (cela résulte du théorème de Mordell-Weil) que la conjecture de Mordell – désormais théorème de Faltings [10] – est équivalente à l'énoncé suivant: «Soit C une courbe de genre au moins deux dans une variété abélienne A, soit Γ un sous-groupe de *type* fini de $A(\mathbb{C})$, alors $C \cap \Gamma$ est fini». Lang a donné un énoncé conjectural décrivant la situation pour les sous-variétés de dimension supérieure et recouvrant les résultats précédents:

Conjecture (Lang). *Soit V une sous-variété algébrique de A variété abélienne définie sur $\mathbb{C}$ et soit Δ un sous-groupe de rang fini de $A(\mathbb{C})$, alors il existe un nombre fini de translatés de sous-variétés abéliennes contenues dans V contenant tous les points de $V \cap \Delta$.*

Remarquons qu'on peut espérer que cette conjecture soit vraie pour une extension d'une variété abélienne par un tore, mais qu'il est indispensable d'exclure la présence de groupes de type $\mathbb{G}_a$: ils n'introduisent pas de nouvelle torsion et ne pertubaient pas les premiers énoncés mais il est évident par exemple qu'une variété affine peut contenir une infinité de points rationnels ou même entiers sans contenir de ligne droite. La conjecture a été prouvé par M. Laurent [24] pour un tore linéaire en utilisant le théorème du sous-espace de W. Schmidt. Raynaud dans [32] a observé que dans le cas d'une sous-variété d'une variété abélienne, si V ne contient pas de translaté de sous-variété abélienne non triviale, alors la conjecture résulterait de l'énoncé a priori plus faible obtenue en remplaçant Δ par un sous-groupe de type fini (ce qui démontre la conjecture, pour les courbes, d'après les travaux de Faltings). Nous nous proposons d'étendre le résultat de Raynaud aux sous-variétés d'un produit d'une variété abélienne par un tore, en levant la restriction géométrique. Ici nous utiliserons des résultats fins de Ribet sur la théorie de Kummer sur les variétés abéliennes (voir [33]). Nous indiquons aussi comment cette démonstration s'étend aux extensions de A par $\mathbb{G}_m^s$, dans le cas où Δ ne rencontre pas les points d'ordre infini paramétrisant l'extension.

Signalons aussi que Raynaud démontre aussi dans [32] essentiellement la conjecture de Lang «sur les corps de fonctions», toujours dans le cas où la sous-variété considérée ne contient pas de translatée de sous-variété abélienne (voir le dernier paragraphe pour un éconcé précis ainsi qu'une application de ce résultat).

Le plan de ce travail est le suivant: Les deux premiers paragraphes contiennent divers préliminaires; le premier rappelle la construction de plongements d'un groupe algébrique commutatif et rassemble des calculs de degrés projectifs. Le deuxième énonce les propriétés galoisiennes des points de torsion et de division que nous utiliserons (les théorèmes de Serre et Ribet). Le troisième paragraphe contient les idées centrales de ce papier (voir surtout la proposition 2); les deux paragraphes suivants mènent aux théorèmes principaux (théorème 1 pour le §4 et théorèmes 2 et 3 pour le §5): avec l'aide des deux outils développés dans les préliminaires (géométrie et théorie de Galois) on fait dans le troisième paragraphe une étude détaillée des sous-groupes algébriques maximaux d'une variété. Dans la quatrième section on démontre un énoncé quantitatif précis décrivant la torsion sur une sous-variété d'un produit de variété abélienne par un tore. On explique dans la cinquième partie comment modifier la démonstration pour un groupe algébrique commutatif général; bien sûr cette partie redémontre les résultats qualitatifs du §4 mais la méthode n'est pas identique et les estimations sont moins précises dans le cas

général. On y explicite toutefois le cas des courbes car la démonstration est notablement plus simple, ce qui permet d'exhiber clairement le mécanisme d'identification d'actions d'endomorphismes d'un coté et d'automorphismes de Galois de l'autre. La sixième partie contient la réduction de la conjecture de Lang à l'énoncé sur les sous-groupes de *type* fini (théorème 4). Un dernier paragraphe contient quelques remarques sur les cas où l'on peut prouver la conjecture et le lien avec les points algébriques de degré donné sur une courbe. Un premier appendice indique la réduction de ces problèmes au cas où les variétés sont définies sur un corps de nombres. Le deuxième appendice donne une démonstration de la forme raffinée de la théorie de Kummer (essentiellement due à Ribet) que nous utilisons dans le sixième paragraphe.

Table des matières

1. Plongements et calculs de degrés projectifs

Le fait qu'un groupe algébrique soit quasi-projectif a été observé il y a longtemps par Chow (on the projective embedding of homogeneous spaces; p 122–128 in symposium in honor of Lefschetz, Princeton U.P. 1957). Nous rappelons brièvement ici la construction de «bons plongements» exposée dans [36] et la notion de degré et multidegré projectif, puis nous démontrons quelques lemmes de calcul de degré dont nous ferons un usage constant.

a) construction de plongement (référence [36])

Soit G un groupe algébrique commutatif défini sur un corps k de caractéristique zéro, on sait depuis Chevalley que G possède un plus grand sous-groupe linéaire connexe L et que le quotient est une variété abélienne A. On dispose donc de la suite exacte suivante:

$$0 \to L \xrightarrow{i} G \xrightarrow{\pi} A \to 0 .$$

Suivant [36], on peut compactifier G ainsi: quitte à étendre k, on peut déployer $L = \prod_{\alpha} L_\alpha$ (avec chaque L_α isomorphe à $\mathbb{G}_a$ ou $\mathbb{G}_m$) et plonger chaque L_α dans $\mathbb{P}^1 = \bar{L}_\alpha$ de sorte que $\bar{L}_\alpha - L_\alpha$ soit égal à $\{\infty\}$ si $L_\alpha = \mathbb{G}_a$ et à $\{0, \infty\}$ si $L_\alpha = \mathbb{G}_m$. La

projection π fait de G un fibré et on définit $\bar{G}=G\times^L\bar{L}$. Sur $\bar{G}$ on dispose des diviseurs suivants:

$G_\alpha^\infty=G\times^L L_\alpha^\infty$ et $G^\infty=\sum_\alpha G_\alpha^\infty$ (où on a posé: $L_\alpha^\infty=\{\bar{L}_\alpha-L_\alpha\}\times\prod_{\beta\neq\alpha}\bar{L}_\beta$) et pour chaque diviseur D sur A, on note $\tilde{D}=\pi^*D$ (on note encore π la fibration $\bar{G}\to A$ prolongeant π). Par exemple si $G=L\times A$ alors $\bar{G}=(\mathbb{P}^1)^s\times A$ et $G_\alpha^\infty=L_\alpha^\infty\times A$ et $\tilde{D}=(\mathbb{P}^1)^s\times D$.

Lemme 1. *Soit a un entier $\geqq 3$ et b un entier $\geqq 1$, soit D un diviseur ample sur A, alors le diviseur $a\tilde{D}+bG^\infty$ est très ample sur $\bar{G}$ et le réalise comme sous-variété projectivement normale de $\mathbb{P}^N$.*

Preuve voir [36], prop. 1 et cor. 1. On supposera dans la suite qu'on a choisi au départ $D=3D'$ avec D' ample sur A de sorte que $\tilde{D}+G^\infty$ soit très ample.

On note $[d]=[d]_G$ l'isogénie multiplication par d; on voit aisément que $[d]$ se prolonge en un morphisme de $\bar{G}$ dans $\bar{G}$, qu'on note encore $[d]$. On a alors:

Lemme 2. (i) *Si $L_\alpha=\mathbb{G}_\alpha$ alors $[d]^*G_\alpha^\infty=G_\alpha^\infty$.*
(ii) *Si $L_\alpha=\mathbb{G}_m$ alors $[d]^*G_\alpha^\infty=|d|G_\alpha^\infty$.*
(iii) *Si D est symétrique sur A, alors $[d]^*(\tilde{D})\sim d^2\tilde{D}$.*

Preuve voir [36] prop. 3 ($\sim$ désigne l'équivalence linéaire de diviseurs). Ceci suggère de définir G_a^∞ comme la somme des G_α^∞ pour $L_\alpha=\mathbb{G}_a$ et G_m^∞ comme la somme des G_α^∞ pour $L_\alpha=\mathbb{G}_m$. Nous dirons que G est bien plongé dans $\mathbb{P}^N$ si la section hyperplane de $\bar{G}$ est un diviseur du type $a\tilde{D}+bG^\infty$ avec D symétrique; nous supposerons toujours dans la suite qu'on s'est donné un tel plongement, en particulier dans les deux lemmes suivants.

Lemme 3. *Soit d un entier, il existe $N+1$ polynômes homogènes de degré d^2 à coefficients dans k, sans zéros communs dans G, tels que si*

$$x=(x_0,\ldots,x_N)\in G,\quad \textit{alors:}\quad [d]_G(x)=(P_{0,d}(x),\ldots,P_{N,d}(x)).$$

Preuve. Cor. 2 de la prop. 3 de [36].

Lemme 4. *Les translations peuvent être définies par des polynômes homogènes de degré au plus deux.*

Preuve voir [23].

Remarque. Dans le cas d'un produit $G=G_1\times\ldots\times G_p$, il est souvent intéressant de plonger G dans un produit d'espaces projectifs $\mathbb{P}^{N_1}\times\ldots\times\mathbb{P}^{N_p}$. Cela se fait en choisissant un bon plongement pour chaque G_i; les lemmes 3 et 4 restent vrais dans ce contexte en remplaçant le mot homogène par multihomogène.

b) Calculs de degrés projectifs

On connait la notion de degré projectif d'une sous-variété de $\mathbb{P}^N$; si V est une sous-variété quasi-projective de $\mathbb{P}^N$, on définit son degré comme le degré de son adhérence de Zariski. Nous utiliserons l'interprétation suivante du degré utilisant la théorie de l'intersection (nous prenons comme référence [13], appendice A): si A est une variété lisse plongée dans $\mathbb{P}^N$ par un diviseur très ample H, si V est une sous-

variété de dimension m de A, alors: $\deg V = \deg_0(V.H \ldots H) = \deg_0 V.H^m$, où l'on note pour un cycle de dimension zéro $\deg_0(\Sigma n_i P_i) = \Sigma n_i$. Dans le cas de sous-variétés de $\mathbb{P}^{N_1} \times \ldots \times \mathbb{P}^{N_p}$, on a la notion de multidegré projectif (voir [29] par exemple). Si V est une sous-variété de dimension m de $A_1 \times \ldots \times A_p$, où chaque A_i est lisse et plongé dans $\mathbb{P}^{N_i}$ à l'aide du diviseur H_i', posons $H_i = H_i' \times \prod_{j \neq i} A_j$, alors on a l'interprétation suivante du multidegré pour $i_k \in \mathbb{N}$ tels que $i_1 + \ldots + i_p = m$:

$$\deg_{i_1,\ldots,i_p} V = \deg_0 V.H_1^{i_1} \ldots H_p^{i_p},$$

On introduit également le polynôme suivant qui est essentiellement la partie m-homogène du polynôme de Hilbert-Samuel (voir [29]; par exemple, si $p=1$, on a $H(V;D) = (\deg V)D^m$):

$$H(V;D_1,\ldots,D_p) = \sum_{i_1+\ldots+i_p=m} (\deg_{i_1,\ldots,i_p} V) \frac{m!}{i_1!\ldots i_p!} D_1^{i_1} \ldots D_p^{i_p}.$$

On peut alors énoncer la version suivante du théorème de Bézout:

Lemme 5 *(théorème de Bézout). Soit V une sous-variété irréductible de $\mathbb{P}^{N_1} \times \ldots \times \mathbb{P}^{N_p}$, soit $\{P_t / t \in T\}$ une famille de polynômes multihomogènes de multidegré au plus $(D_1,\ldots,D_p)$, soit S l'ensemble des composantes irréductibles de $X = V \cup \left(\bigcap_{t \in T} Z(P_t) \right)$, alors on a:*

$$\sum_{C \in S} H(C;D_1,\ldots,D_p) \leqq H(V;D_1,\ldots,D_p).$$

Preuve (voir [29] prop. 3.3.

Avant d'énoncer les lemmes suivants, donnons quelques définitions et notations. Nous dirons qu'un sous-ensemble algébrique X de V plongée dans $\mathbb{P}^{N_1} \times \ldots \times \mathbb{P}^{N_p}$ est défini incomplètement dans V par des équations de degré au plus $(D_1,\ldots,D_p)$ si X est somme de composantes irréductibles de l'intersection de V avec des hypersurfaces de degré au plus $(D_1,\ldots,D_p)$. Si V est un sous-ensemble algébrique de G groupe algébrique, si α est une isogénie de G, l'image directe de V par α et l'image réciproque sont notées respectivement $\alpha(V)$ et $\alpha^{-1}(V)$; ce sont des sous-ensembles algébriques de G. Enfin on notera G_V (resp. G_V^0) le stabilisateur de V dans G (resp. la composante neutre du stabilisateur de V).

Lemme 6. *Soit G_i un groupe algébrique bien plongé dans $\mathbb{P}^{N_i}$ par un diviseur H_i', soit α_i une isogénie de G_i telle que $\alpha_i^*(H_i') \sim n_i H_i'$, notons $[\alpha_1,\ldots,\alpha_p]$ l'isogénie produit des α_i et m_i la dimension de G_i, soit V une sous-variété de $G_1 \times \ldots \times G_p$ de dimension m, alors pour $i_1 + \ldots + i_p = m$ on a:*

(i) $\deg_{i_1,\ldots,i_p} [\alpha_1,\ldots,\alpha_p]^{-1}(V) = n_1^{m_1-i_1} \ldots n_p^{m_p-i_p} \deg_{i_1,\ldots,i_p} V$

(ii) $\deg_{i_1,\ldots,i_p} [\alpha_1,\ldots,\alpha_p](V) = \dfrac{n_1^{i_1} \ldots n_p^{i_p}}{|\mathrm{Ker}\,[\alpha_1,\ldots,\alpha_p] \cap G_V|} \deg_{i_1,\ldots,i_p} V$ *et donc:*

$$H([\alpha_1,\ldots,\alpha_p](V);D_1,\ldots,D_p) = \frac{1}{|\mathrm{Ker}\,[\alpha_1,\ldots,\alpha_p] \cap G_V|} H(V;n_1D_1,\ldots,n_pD_p).$$

(iii) *Si V est définie dans $G=G_1\times\ldots\times G_p$ par des équations de degrés au plus $(D_1,\ldots,D_p)$, alors $[\alpha_1,\ldots,\alpha_p]^{-1}(V)$ (resp. $V+t$) est défini dans G par des équations de degrés au plus $(n_1D_1,\ldots,n_pD_p)$ (resp. au plus $(2D_1,\ldots,2D_p)$).*

Remarque. Nous appliquerons ce lemme à l'isogènie multiplication par d (Cf le lemme 2), mais les hypothèses sont vérifiées pour d'autres isogénies très intéressantes comme celle qui relève en caracteristique zéro le Frobenius modulo p (voir [16] pour les détails et des applications).

Preuve de (i): Soit $H_i=H_i'\times\prod_{j\neq i}G_j$, en remarquant que nécessairement on a: $|\mathrm{Ker}\,\alpha_i|=n_i^{m_i}$ on peut écrire:

$$\begin{aligned}n_1^{m_1}\ldots n_p^{m_p}\deg_{i_1,\ldots,i_p}V&=|\mathrm{Ker}\,[\alpha_1,\ldots,\alpha_p]|\deg_0(V.H_1^{i_1}\ldots H_p^{i_p})\\&=\deg_0([\alpha_1,\ldots,\alpha_p]^*(V.H_1^{i_1}\ldots H_p^{i_p})\\&=\deg_0\{([\alpha_1,\ldots,\alpha_p]^*(V)\ldots([\alpha_1,\ldots,\alpha_p]^*(H_p))^{i_p}\}\\&=\deg_0\{[\alpha_1,\ldots,\alpha_p]^{-1}(V).(n_1H_1)^{i_1}\ldots(n_pH_p)^{i_p}\\&=n_1^{i_1}\ldots n_p^{i_p}\deg_{i_1,\ldots,i_p}[\alpha_1,\ldots,\alpha_p]^{-1}(V).\end{aligned}$$

Le démonstration de (ii) utilise le résultat suivant qui est un corollaire d'une propriété de platitude (voir [13] th. 9.9.) comme cela a été remarqué par J-C Moreau:

Lemme 7. *Soit V une sous-variété de $G=G_1\times\ldots\times G_p$ bien plongé dans $\mathbb{P}^{N_1}\times\ldots\times\mathbb{P}^{N_p}$ alors pour tout point t de G on a: $H(V+t;D_1,\ldots,D_p)=H(V;D_1,\ldots,D_p)$.*

Preuve de (ii). D'après le lemme 7 et (i), on peut écrire:

$$\begin{aligned}n_1^{m_1-i_1}\ldots n_p^{m_p-i_p}\deg_{i_1,\ldots,i_p}[\alpha_1,\ldots,\alpha_p](V)&=\deg_{i_1,\ldots,i_p}[\alpha_1,\ldots,\alpha_p]^{-1}([\alpha_1,\ldots,\alpha_p](V))\\&=\deg_{i1,\ldots,i_p}(V+\mathrm{Ker}\,[\alpha_1,\ldots,\alpha_p])\\&=\frac{|\mathrm{Ker}\,[\alpha_1,\ldots,\alpha_p]|}{|\mathrm{Ker}\,[\alpha_1,\ldots,\alpha_p]\cap G_V|}\deg_{i_1,\ldots,i_p}V.\end{aligned}$$

Preuve de (iii). Cela résulte des lemmes 3 et 4 (le lemme 3 est énoncé seulement pour $\alpha=[d]$ mais en reprenant la démonstration de [36] on voit que l'essentiel est une relation du type $\alpha^*(H)\sim nH$.

Remarque. Si l'on suppose que V est une sous-variété de dimension m de G, que $H_1,\ldots,H_m$ sont des diviseurs sur $\bar{G}$ tels que $\alpha^*(H_i)\sim n_iH_i$, alors on peut obtenir une expression simple de $\deg_0\alpha^{-1}(V).H_1\ldots H_m$ et $\deg_0\alpha(V).H_1\ldots H_m$ en fonction de $\deg_0V.H_1\ldots H_m$.

Lemme 8. *Soit $G=G_1\times\ldots\times G_p$ un groupe algébrique bien plongé dans $\mathbb{P}^{N_1}\times\ldots\times\mathbb{P}^{N_p}$, soit C une sous-variété irréductible définie incomplètement dans G par des équations de degré au plus $(D_1,\ldots,D_p)$, alors le stabilisateur de C est défini incomplètement dans G par des polynômes de degré au plus $(2D_1,\ldots,2D_p)$ et l'on a: $(G_C:G_C^0)H(G_C^0;2D_1,\ldots,2D_p)=H(G_C;2D_1,\ldots,2D_p)\leqq H(C;2D_1,\ldots,2D_p)$.*

Preuve. Par hypothèse C est composante de $X = G \cap \left\{ \bigcap_t Z(P_t) \right\}$, où les P_t sont des polynômes de degré au plus $(D_1, \ldots, D_p)$. Considérons $M = \bigcap_{x \in C} X - x$; d'après le lemme 6, M est défini par des équations de degré au plus $(2D_1, \ldots, 2D_p)$. Clairement, $G_C \subset M$ et M est homogène sous G_C; il suffit donc de prouver que G_C^0 est une composante de M. Soit Y une composante de M contenant G_C^0, *alors* $Y + C \subset X$ et donc $C \subset Y + C \subset X$ et donc comme C est une composante de X on conclut que $Y + C = C$. Ainsi $G_C^0 \subset Y \subset G_C$ et donc $Y = G_C^0$. La deuxième affirmation se déduit immédiatement du théorème de Bézout (lemme 5) en décrivant G_C comme somme de composantes de même degré de $C - x$ coupée par des hypersurfaces de degré au plus $(2D_1, \ldots, 2D_p)$.

Nous terminons ce chapitre par un énoncé qui est presque évident sur le groupe $(\mathbb{G}_m)^s$ mais contient le théorème de réductibilité de Poincaré pour une variété abélienne:

Lemme 9. *Soit G un produit d'un tore multiplicatif T par une variété abélienne A, définie sur K, plongé dans $\mathbb{P}^N \times \mathbb{P}^M$, alors:*

(i) *Il existe une extension fini de K sur laquelle tous les endomorphismes et les sous-groupes algébriques connexes de G sont définis.*

(ii) *Il existe une constante $C_G > 0$ telle que si B est un sous-groupe algébrique connexe de G, alors il existe un sous-groupe algébrique connexe B' tel que $B + B' = G$ et aussi $|B \cap B'| \leqq C_G H(B; 1, 1)$.*

(iii) *Il n'existe qu'un nombre fini de sous groupes algébriques de degré borné.*

Remarque 1. Les parties (i) et (iii) de l'énoncé restent vraies pour une extension non triviale d'une variété abélienne par un tore multiplicatif, mais sont fausses en général – par exemple sur $(\mathbb{G}_a)^2$.

Remarque 2. D. Bertrand a montré qu'en fait on peut choisir B' de sorte que $|B \cap B'|$ soit majoré par C'_G (voir [1]).

Preuve de (i). Soit K' sur laquelle T est déployé et tous les endomorphismes de A sont définis, la variété A possède une isogénie α définie sur K' disons sur $A' = A_1 \times \ldots \times A_r$ produit de variétés simples dont tous les endomorphismes sont définis sur K'. Soit α' telle que $\alpha' \circ \alpha = [\deg \alpha]$, alors toute sous-variété abélienne de A est l'image par α' d'une sous-variété abélienne de A' elle-même image par un produit d'endomorphismes d'une variété de type $A_1 \times \{0\} \times \ldots \times A_r$ et est donc définie sur K'. Les sous-groupes algébriques de T sont bien sûr tous définis sur K'.

(ii) Soit $B = B_0 \times T_0 \subset A \times T$, on peut choisir T_0' sous-tore de T tel que $|T_0 \cap T_0'| = 1$. On peut choisir B_0'' du type $A_1 \times \{0\} \times \ldots \times A_r$ de sorte que $\dim B_0'' + \dim \alpha(B) = \dim A'$ et $\alpha(B) \cap B_0''$ soit fini; posons $B_0' = \alpha'(B_0'')$ et $B' = B_0' \times T_0'$ alors comme B_0' parcourt une famille finie, $|B_0 \cap B_0'| \leqq C_A \deg B_0$ et donc $|B \cap B'| \leqq C_A \deg B_0 \leqq C_G H(B; 1, 1)$.

(iii) Ceci est bien connu et peut se déduire des résultats de [3] ou bien des lemmes 5 et 6 précédents.

Concluons ce paragraphe par deux lemmes sur la géométrie des sous-variétés de groupes algébriques:

Lemme 10. *Soit V une sous-variété d'un groupe G extension d'une variété abélienne par un tore linéaire, supposons que pour un entier $d \geqq 2$ on ait : $[d](V) = V + v_0$ alors V est un translaté de sous-groupe algébrique.*

Notons que sur un groupe algébrique quelconque, le résultat est encore vrai pour une courbe (voir lemme 16) mais devient faux pour une variété de dimension supérieure (un cone dans l'espace affine n'est pas forcément linéaire).

Preuve. On choisit une compactification et un bon plongement; alors on voit d'après les lemmes précédents que pour deux entiers tels que $i+j=m=\dim V$ on a:

$$\deg_0 [d](V) \,.\, \tilde{D}^i \,.\, (G^\infty)^j = \frac{d^{2i+j}}{|\mathrm{Ker}\,[d] \cap G_V|} \deg_0 V \,.\, \tilde{D}^i \,.\, (G^\infty)^j$$

En observant que pour k entier $\geqq 1$ on a encore $[d^k](V) = V + v_k$ on obtient:

$$\deg V = \sum_{i+j=m} (m!/i!j!) \deg_0 V \,.\, \tilde{D}^i \,.\, (G^\infty)^j = \deg(V + v_k) = \deg [d^k](V)$$

$$= \sum_{i+j=m} (m!/i!j!) \frac{d^{k(2i+j)}}{|\mathrm{Ker}\,[d^k] \cap G_V|} \deg_0 V \,.\, \tilde{D}^i \,.\, (G^\infty)^j \,.$$

G_V^0 est une extension d'une variété abélienne de dimension g par un tore linéaire de dimension t et donc $|\mathrm{Ker}\,[d^k] \cap G_V^0| = d^{k(2g+t)}$ et pour k assez grand $|\mathrm{Ker}\,[d^k] \cap G_V| / |\mathrm{Ker}\,[d^k] \cap G_V^0|$ est constant. On observe donc que pour deux entiers positifs tels que $i+j=m$ et $2i+j > 2g+t$ on a: $\deg_0 V \,.\, \tilde{D}^i \,.\, (G^\infty)^j = 0$. On conclut alors par l'argument suivant que nous énonçons pour future référence:

Lemme 11. *Supposons que V soit une sous-variété de dimension m d'un groupe G extension d'une variété abélienne par un tore linéaire et que son stabilisateur soit une extension d'une variété abélienne de dimension g par un groupe linéaire de dimension t ; si pour chaque entiers i,j tels que $i+j=m$ et $2i+j > 2g+t$ on a: $\deg_0 V \,.\, \tilde{D}^i \,.\, (G^\infty)^j = 0$, alors V est un translaté de sous-groupe algébrique.*

Preuve. Choisissons $i = \dim \pi(V)$, alors comme D est ample sur A, $\pi(V) \,.\, D^i$ est un cycle effectif non nul de A de dimension nulle. Ainsi $V \,.\, \tilde{D}^i$ est un cycle effectif non nul dimension $j = m - i$ et est concentré dans un nombre fini de fibres de $\pi : \bar{G} \to A$; comme G^∞ est relativement ample pour la fibration π (Cf la remarque dans [36] prop. 1 et cor. 1) on en déduit que $\deg_0 V \,.\, \tilde{D}^i \,.\, (G^\infty)^j > 0$. On conclut que $2g + t \geqq 2i + j = m + \dim \pi(V)$. Mais bien sûr $\pi(v_0 + G_V) \subset \pi(V)$ et donc $\dim \pi(V) \geqq g$ et ainsi $\dim G_V = g + t \geqq m = \dim V$; ce qui montre que $V = v_0 + G_V$.

2. Propriétés galoisiennes

Nous énonçons diverses propriétés sous la forme qui nous sera utile; elles affirment qu'un point de torsion ou un point de division a beaucoup de conjugués par Galois, sous des hypothèses convenables. Si K est un corps (en pratique un corps de nombres) on note $\bar{K}$ une clôture algébrique de K et $\mathrm{Gal}(\bar{K}/K)$ son groupe de Galois absolu. Si A est un groupe abélien on note A_n son groupe de n-torsion. La notation $C = C(a_1, a_2, \ldots)$ désigne une constante ne dépendant que de $a_1, a_2, \ldots$ etc.

a) Points de torsion

Lemme 12. *Considérons le produit G d'un tore T et d'une variété abélienne A, supposons G défini sur un corps de nombres K, alors:*

i) *Il existe un entier non nul $c=c(G,K)$ tel que si p est premier à n et si (ξ,x) est un point d'ordre n sur $G=T\times A$ alors il existe σ appartenant à $\mathrm{Gal}(\bar{K}/K)$ tel que: $\sigma(\xi,x)=[p^{2c},p^c](\xi,x)$.*

ii) *Il existe deux constantes positives $C_1=C_1(G,K)$ et $q=q(G)$ telles que l'orbite sous $\mathrm{Gal}(\bar{K}/K)$ d'un point d'ordre n de G ait un cardinal au moins $C_1 n^{1/q}$.*

Preuve de i). Lorsque $T=(0)$, on reconnaît l'énoncé du théorème 2 de [37]. En prenant donc $c=c(A,K)$ donnée par le théorème de Serre et en posant $d=p^c$, on voit qu'il existe $\sigma\in\mathrm{Gal}(\bar{K}/K)$ agissant par multiplication par d sur les points de n-torsion de A. Considérant l'accouplement de Weil – noté e_n – on voit que σ agit par élévation à la puissance d^2 sur les racines n-ièmes de l'unité:

$$\sigma(e_n(y,y'))=e_n(\sigma y,\sigma y')=e_n([d](y),[d](y'))=e_n(y,y')^{d^2}.$$

Preuve de ii). Cela résulte de la même propriété pour $\mathbb{G}_m$ (irréductibilité du polynôme cyclotomique) et pour une variété abélienne (ce qui peut s'obtenir par méthode de transcendance, voir [2] et [26] par exemple, ou par méthode algébrique comme dans [37]).

Remarque. Ce lemme pose un problème d'effectivité: les méthodes de transcendance donnent des versions effectives de ii), mais le calcul de la constante c de i) n'est effectif à notre connaissance que pour une variété abélienne de type CM (voir [22]) ou une puissance d'une courbe elliptique définie sur $\mathbb{Q}$ (idem pour les versions algébriques de ii) en prenant $q<1$).

On peut décrire très explicitement l'action du groupe de Galois sur les points de torsion d'une extension de variété abélienne (voir par exemple [33]); en fait nous nous servirons des faits suivants:

Lemme 13. *Soit G une extension d'une variété abélienne A par un groupe linéaire commutatif L, définie sur un corps de nombres K, alors:*

i) *Il existe un entier $c=c(G,K)$ tel que si p est premier à n, si x est un point de torsion de G dont la projection sur A est d'ordre n, alors il existe σ appartenant à $\mathrm{Gal}(\bar{K}/K)$ et η point de torsion de L tel que:*

$$\sigma(x)=[p^c](x)+\eta$$

ii) *Il existe deux constantes $C_1'=C_1'(G,K)$ et $q'=q'(G)$ telles que si K^{cyc} désigne l'extension de K par toutes les racines de l'unité, alors, si x est un point d'ordre n de A, son orbite sous $\mathrm{Gal}(\bar{K}/K^{cyc})$ a pour cardinal au moins $C_1' n^{1/q'}$.*

Preuve. i) est un corollaire immédiat du lemme 12: Considérant la suite exacte

$$0\to L\to G\xrightarrow{\pi} A\to 0$$

On choisit σ tel que $\sigma(\pi(x))=[p^c](\pi(x))$, on observe alors que $\sigma(x)-[p^c](x)$ est tué par π donc est dans L et est un point de torsion. La preuve de ii) est plus délicate et utilise des résultats fins sur les représentations l-adiques. Il suffit bien sûr de le prouver pour A simple. Il est bien connu que $K(\mu_n)\subset K(A_n)$, en fait on peut

montrer que $[K(A_n)\cap K^{cyc}:K(\mu_n)]$ est borné quand n varie. D'après [37], si A n'est pas de type CM, si x est un point d'ordre n, alors $[K(x):K]\geqq C_1 n^{2-\varepsilon}$ et donc $[K(x):K(x)\cap K^{cyc}]\geqq C_1 n^{1-\varepsilon}$; si A est de type CM on a une description explicite de l'action de Galois sur les points de torsion (voir [34], [38] et [39]) qui fournit le résultat désiré. On pourrait aussi utiliser le résultat de Ribet démontré en appendice de [18] disant que le sous-groupe de torsion de $A(K^{cyc})$ est fini.

b) Théorie de Kummer

Nous énonçons le résultat sur une variété abélienne A (définie sur un corps de nombres K), l'analogue sur le groupe multiplicatif étant bien connu. Si P est un point d'ordre infini de $A(\bar{K})$, on désigne par $\frac{1}{m}P$ un des points Q tels que $[m](Q)=P$; il n'est défini qu'à un point de m-torsion près mais l'extension $K\left(A_m, \frac{1}{m}P\right)$ est bien définie et galoisienne sur $K(A_m)$.

Lemme 14. *Soit A une variété définie sur un corps de nombres K, il existe une constante strictement positive $f_0=f_0(A,K)$ telle que si P est un point d'ordre infini de $A(K)$, non divisible dans $A(K)$ par aucun entier distinct de plus ou moins un et si m divise n, alors:*

$$\left|\mathrm{Gal}\left(K\left(A_n, \frac{1}{m}P\right)/K(A_n)\right)\right|\geqq f_0 m.$$

Ce lemme se déduit aisément de la proposition suivante et ne sera utilisé qu'au paragraphe 6. Si P est un point d'ordre infini de $A(K)$, on note G_P le plus petit sous-groupe algébrique de A contenant P et B_P sa composante connexe; nous dirons que P est indivisible dans $A(K)$ si l'égalité $\alpha(Q)=P$ avec $\alpha\in\mathrm{End}(A)$ et $Q\in A(K)$ entraine l'existence de $\beta\in\mathrm{End}(A)$ tel que $\beta(P)=Q$.

Proposition 1. *(Ribet). Soit A une variété abélienne définie sur un corps de nombres K, il existe une constante $f=f(A,K)$ telle que si P est un point d'ordre infini indivisible dans $A(K)$, si $B=B_P$ est la plus petite sous-variété abélienne contenant un multiple de P et si $(G_P:B)m$ divise n, alors le groupe de Galois $\mathrm{Gal}\left(K\left(A_n, \frac{1}{m}P\right)/K(A_n)\right)$ s'identifie à un sous-groupe de B_m d'indice borné par f (indépendamment de m et n).*

Cette formulation est prise dans [16]; pour la commodité du lecteur nous reproduisons la démonstration en appendice (n° 2): il s'agit de mettre bout à bout les résultats de Ribet [33], Faltings [10] et Serre [37]. Ribet a énoncé un résultat pour $\mathrm{Gal}\left(K\left(A_l, \frac{1}{l}P\right)/K(A_l)\right)$ sous certains axiomes qui sont devenus des théorèmes grâce à Faltings et Serre; il faut ensuite prouver qu'il n'y a pas de dégénérescence quand on translate $K\left(A_{lm}, \frac{1}{l^m}P\right)/K(A_{lm})$ en $K\left(A_{lm_n}, \frac{1}{l^m}P\right)/K(A_{lm_n})$.

Remerquons que le lemme 14 se déduit aisément de la proposition et que la minoration en $f_0 m$ est souvent améliorable (par exemple si $\mathrm{End}(A)=\mathbb{Z}$, alors on peut minorer par $f_0 m^{2\dim A}$) mais, en toute généralité, elle est optimale comme le

montre l'exemple suivant: Soit E une courbe elliptique avec multiplication complexe par O un ordre d'un corps quadratique imaginaire, soit $l=\alpha\alpha'$ un nombre premier décomposé; choisissons $P=\alpha(Q)$, où Q est un point indivisible dans $A(K)$, alors P n'est divisible par aucun entier distinct de un ou moins un mais $\mathrm{Gal}\left(K\left(A_l, \frac{1}{l}P/K(A_l)\right)\right)$ s'identifie à $\mathrm{Ker}(\alpha')$ de cardinal l.

3. Sous-groupe maximaux

Soit V une sous-variété d'un groupe algébrique commutatif G et soit x un point de V, nous dirons qu'un sous-groupe algébrique B est maximal en x relativement à V si B est connexe et maximal au sens de l'inclusion parmi les groupes algébriques connexes tels que $x+B\subset V$. Nous étudions ces sous-groupes et bornons en particulier leur degré quand ils sont en nombre fini, entamant ainsi l'étude des points de torsion sur V.

Ce paragraphe étudie les groupes produits d'un tore linéaire et d'une variété abélienne; ceux-ci sont plus «riches» en endomorphismes et donc plus faciles à traiter, mais nous étendrons au § 5 la plupart des résultats aux extensions de variétés abéliennes par des tores, au prix de quelques complications (les lemmes 10 et 11 jouant alors un role clef); Commençons par le corollaire suivant des résultats du premier paragraphe:

Lemme 15. *Si V est une sous-variété irréductible du produit d'un tore T par une variété abélienne, si d est un entier $\geqq 2$, alors si $[d^2,d](V)\subset V+t$ alors V est un translaté de sous-groupe algébrique.*

Preuve. On a donc, pour $s\geqq 1$, $[d^{2s},d^s](V)=V+t_s$. On se donne un bon plongement et on utilise le lemme 6:

$$H(V;X,Y)=H(V+t_s;X,Y)=H([d^{2s},d^s](V);X,Y)$$
$$=\frac{d^{2s\dim V}}{|\mathrm{Ker}\,[d^{2s},d^s]\cap G_V|}H(V;X,Y)$$

D'autre part, si $G_V^0=(\mathbb{G}_m)^r\times B$, alors $|\mathrm{Ker}\,[d^{2s},d^s]\cap G_V^0|=d^{2s(r+\dim B)}$ et donc $r+\dim B=\dim G_V^0=\dim V$ et ainsi $V=v_0+G_V^0$.

Remarque. Il reste vrai qu'une sous-variété irréductible d'une extension d'une variété abélienne par un tore qui est stable (à translation près) par $[d]$ est un translaté de sous-groupe algébrique d'après le lemme 10; mais bien sûr cela est faux dans $(\mathbb{G}_a)^r$ – i.e. une variété homogène n'est pas forcément linéaire. Ceci suggère d'introduire pour un entier d bien choisi les sous-ensembles algébriques suivants:

$$V_t=V_{t,d}=V\cap[d^2,d]^{-1}(V)\cap\ldots\cap[d^{2t},d^t]^{-1}(V)$$

$$V_\infty=\bigcap_{t=0}^{\infty}[d^{2t},d^t]^{-1}(V)$$

On considère maintenant une sous-variété V de dimension m d'un produit d'un tore T et d'une variété abélienne A bien plongé dans $\mathbb{P}^M\times\mathbb{P}^N$, telle que V soit définie

dans $G = T \times A$ par des polynômes bihomogènes de degré au plus (D_1, D_2) et définie sur un corps de nombres K; on démontre alors la proposition suivante:

Proposition 2. *Soit x un point de torsion de V est soit d un entier tel que $[d^2, d](x)$ soit un conjugué de x par $\mathrm{Gal}(\bar{K}/K)$ et tel que $d^2 > H(V; 2D_1, 2D_2)$; alors pour tout t supérieur à h la partie entière de $\sum_{i=1}^{m} (2m)^i/i!$ on a: $\dim_x V_\infty = \dim_x V_t$ et de plus V contient le translaté par x d'un sous-groupe algébrique B maximal de dimension celle de V_∞ en x et vérifiant: $H(B; D_1, D_2) \leqq d^{2hm} H(V; 2D_1, D_2)$.*

En appliquant la proposition à $V - b$ et $x = 0$ et $d = [H(V; 2D_1, 2D_2)^{1/2}] + 1$ on obtient (Cf Bogomolov [4] pour une variété abélienne):

Corollaire. *Soit $b \in V$, supposons $b + B$ maximal dans V alors:*

$$H(B; D_1, D_2) \leqq H(V; 2D_1, 2D_2)^{hm}.$$

En particulier il n'y a qu'un nombre fini de sous-groupes B possibles.

Preuve de la proposition. Remarquons d'abord que si $x + B \subset V$, alors: $[d^2, d](x + B) = [d^2, d]x + B = \sigma x + B = \sigma(x + B) \subset V$ (car B et V sont définis sur K et B est stable par $[d^2, d]$). On conclut que $x + B$ est contenu dans V_1 et par induction dans V_∞. Ainsi, si l'on trouve une composante de V_r de la forme $x + B$, c'est nécéssairement un sous-groupe maximal en x relativement à V. Supposons maintenant que $\dim_x V_s = \dim_x V_{s+1} = \ldots = \dim_x V_{s+k} = m'$; on va montrer que ou bien V_s contient un sous-groupe de dimension m' translaté par x ou bien k est borné. On en déduira alors, par un calcul par récurrence aisé, la proposition.

Une composante C de dimension m', contenant x, de V_s reste donc dans V_{s+k}. On en déduit: $[d^{2k}, d^k](C) \subset [d^{2k}, d^k](V_{s+k}) \subset V_s$. Mais $[d^{2k}, d^k](C)$ contient $x' = [d^{2k}; d^k]x$ qui est par hypothèse un conjugué de x (par $\mathrm{Gal}(\bar{K}/K)$); comme V_s est définie sur K, on voit aisément que $\dim_x V_s = \dim_{x'} V_s$ et donc que $[d^{2k}, d^k](C)$ est une composante irréductible de V_s. D'après les lemmes 5 et 6 on peut écrire:

$$H([d^{2k}, d^k](C); d^{2s}D_1, d^{2s}D_2) = \frac{H(C; d^{2k+2s}D_1, d^{2k+2s}D_2)}{|\mathrm{Ker}\,[d^{2k}, d^k] \cap G_C|} \leqq H(V; d^{2s}D_1, d^{2s}D_2).$$

Par ailleurs en utilisant le lemme 8 on a:

$$|\mathrm{Ker}\,[d^{2k}, d^k] \cap G_C| \leqq d^{2k \dim G_C}(G_C : G_C^0) \leqq d^{2k \dim G_C} H(C; 2d^{2s}D_1, 2d^{2s}D_2).$$

D'où l'on tire: $d^{2k(m' - \dim G_C) - 2sm} \leqq H(V; 2D_1, 2D_2)$. Comme on a supposé d^2 strictement plus grand que le nombre de droite, on en déduit que, *ou bien* $m' = \dim G_C = \dim C$ et alors $C = x + G_C$, c'est-à-dire que V_s contient un translaté de sous-groupe par x nécéssairement maximal d'après les remarques préliminaires et dont on estime le degré en utilisant encore une fois le théorème de Bézout:

$$H(C; d^{2s}D_1, d^{2s}D_2) \leqq H(V; d^{2s}D_1, d^{2s}D_2)$$

et donc

$$H(G_C, D_1, D_2) \leqq d^{2sm} H(V; 2D_1, 2D_2).$$

Il reste à voir que l'on a bien $s \leqq h$; *ou bien* $\dim G_C < \dim C = m'$ et alors on conclut:

$k \leqq sm(m' - \dim G_C)$. Par noethérianité il existe deux suites d'entiers s_i et m_i tels que:

$$m = m_1 = \dim_x V = \ldots = \dim_x V_{s_1} > \dim_x V_{s_1+1} = \ldots = \dim_x V_{s_2}$$
$$= m_2 > \ldots > \ldots = \dim_x V_{s_r} = m_r > \dim_x V_{s_r+1} = t$$

Le raisonnement précédent montre que: $s_1 \leqq m/(m-g_1)$ et $s_{i+1} - s_i \leqq (s_i+1)m/(m_i - g_i)$ où l'on note $g_i = \dim G_{C_i}$ la dimension du stabilisateur de la composante C_i intervenant au i-ème cran de la démonstration. Comme $g_i \leqq t = \dim_x V_\infty$ on a:

$$s_r \leqq \left[\frac{m(m+m_2-g_2)\ldots(m+m_{r-1}-g_{r-1})}{(m_1-g_1)(m_2-g_2)\ldots(m_{r-1}-g_{r-1})}\right] + \ldots + \frac{m}{(m_{r-1}-g_{r-1})} < \frac{(2m)^r}{r!} + \ldots + 2m,$$

d'où l'on tire la majoration cherchée: $s_{r+1} \leqq h$.

4. Points de torsion (cas d'un produit de tore et de variété abélienne)

On se propose de démontrer dans cette partie le théorème suivant (on rappelle la constante q du lemme 12 et l'entier h de la proposition 2):

Thèorème 1. *Soit G un produit d'un tore T et d'une variété abélienne A, bien plongé dans $\mathbb{P}^M \times \mathbb{P}^N$, défini sur un corps de nombres K, il existe une constante $C_0 = C_0(G, K)$ telle que si V est une K-sous-variété pure de dimension m de G, définie dans G par des équations de bidegré au plus (D_1, D_2), alors il existe $t_1, \ldots, t_r$ points de torsion de G d'ordre au plus $C_0 H(V; D_1, D_2)^{q(hm+1)}$ et des sous-groupes algébriques $B_1, \ldots, B_r$ tels que $H(B_i, D_1, D_2) \leqq H(V, 2D_1, 2D_2)^{hm}$ et tels que:*

$$V(\bar{K}) \cap G(\bar{K})_{\text{torsion}} = \bigcup_{i=1}^{r} (t_i + B_i(\bar{K})_{\text{torsion}}).$$

Remarques. a) Il est clair que le théorème fournit une méthode de détermination effective de la torsion sur une sous-variété dès que l'on sait calculer la constante C_0; malheureusement ce calcul dépend de la constante $c = c(A, K)$ du lemme 12 et n'est effectif que dans quelques cas, comme on l'a signalé.

b) On peut aisément tirer du théorème l'énoncé uniforme suivant:

Corollaire: Soit $e \geqq 1$, il existe $R = R(G, K, e)$ et un ensemble fini de sous-groupes algébriques $\{B_s / s \in S\}$ tels que:

i) *On a: $\deg B_s \leqq R$ (ceci pour tout $s \in S$).*

ii) *Si V est une K-sous-variété définie par des équations de degré au plus e, alors il existe $t_1, \ldots, t_r$ points de torsion d'ordre au plus R et $s_1, \ldots, s_r$ éléments de S tels que:*

$$V(\bar{K}) \cap G(\bar{K})_{\text{tor}} = \bigcup_{i=1}^{r} (t_i + B_{s_i}(\bar{K})_{\text{tor}}).$$

Remarquons que les résultats de Raynaud contiennent des énoncés (avec borne non explicite) pour les translatés d'une courbe par des points de $A(\bar{K})$ (et non de $A(K)$ comme nous devons le supposer); Coleman (voir [7] et [8]) a aussi obtenu des résultats très précis sur les courbes; [15] contient une discussion des diverses bornes obtenus.

Preuve du Théorème 1. Soit x un point de torsion situé sur V, d'ordre n, soit B un sous-groupe algébrique de dimension maximale en x relativement à V; le lemme 9 permet de choisir un sous-groupe algébrique B' tel que $B+B'=G$ et $|B\cap B'|\leqq C_G H(B;1,1)$. On peut d'autre part supposer que $x\in B'$ (sinon $x=b+b'$ avec $b\in B$ et $b'\in B'$ et donc $x+B=b'+B$ et on peut raisonner avec b'). On choisit alors p ne divisant pas n, l'ordre de x, tel que: $p^{2c}=d^2>H(V;2D_1,2D_2)$. Utilisant le lemme 12i) et la proposition 2, on voit que $Z=\bigcup_{\sigma\in \mathrm{Gal}(\bar{K}/K)}(\sigma x+B)$ est somme de composantes de $V_{d,h}=V_h$. D'autre part tous ces translatés ont même degré et il y en a au moins $(C_1 n^{1/q})/C_G H(B;1,1)$ d'après le lemme 12ii). En appliquant le théorème de Bézout on obtient:

$$(C_1 n^{1/q})/C_G \leqq H(Z;d^{2h}D_1,d^{2h}D_2)\leqq d^{2hm}H(V;D_1,D_2) \qquad (*)$$

Supposons que $n\geqq C_0 H(V;D_1,D_2)^{q(hm+1)}$ avec C_0 grand en fonction de A,K et $c(A,K)$. Par un argument élémentaire de théorie analytique des nombres premiers, il existe p premier avec n tel que:

$$H(V;2D_1,2D_2)^{1/2c}<p<\{C_1 n^{1/q}/C_G H(V;D_1,D_2)\}^{1/2hmc}.$$

En choisissant $d=p^c$ dans le raisonnement précédent on aboutit à une contradicition entre $(*)$ et la majoration de d; on a donc bien prouvé que $n\leqq C_0 H(V;D_1,D_2)^{q(hm+1)}$ et le théorème annoncé.

5. Point de torsion (cas général)

Let but de ce paragraphe est de démontrer le théorème suivant:

Théorème 2. *Soit G un groupe algébrique commutatif défini sur un corps de caractéristique zéro K, soit V une sous-variété algébrique de G, alors il existe un nombre fini de points de torsion $t_1,\ldots,t_r$ et de sous-groupes algébriques $G_1,\ldots,G_r$ tels que:*

$$V(\bar{K})\cap G(\bar{K})_{\mathrm{tor}}=\bigcup_{i=1}^{r}(t_i+G_i(\bar{K})_{\mathrm{tor}}).$$

Remarques. – Cet énoncé est bien sur faux en caractéristique positive (si K est fini tous les points algébriques sont de torsion).

– Par des arguments de spécialisation (voir appendice) il suffit de prouver le résultat si K est un corps de nombres, c'est ce que nous ferons.

Nous commençons par donner une démonstration directe si V est une courbe (par exemple plongée dans une jacobienne généralisée); nous réduisons ensuite l'énoncé général à un résultat dont nous démontrons ensuite une version quantitative très semblable au théorème 1, lorsque G ne contient pas de sous-groupe de type $\mathbb{G}_a$; nous terminons en traitant succintement le cas ou G contient une partie additive.

On rappelle la suite exacte canonique: $0\to L\to G\xrightarrow{\pi} A\to 0$.

α) Le cas d'une courbe

Soit donc G un groupe algébrique, on le suppose plongé par le diviseur sur $\bar{G}$ défini en § 1 : $H=\tilde{D}+G_a^\infty+G_m^\infty$ dans $\mathbb{P}^N$. On commence par l'analogue des lemmes 10 et 15 (qui serait faux pour une variété de dimension $\geqq 2$):

Lemme 16. *Soit C une courbe irréductible de G, soit d un entier $\geqq 2$, supposons que $[d](C)\subset C+t$ alors C est un translaté de sous-groupe algébrique.*

Preuve. $\deg(C+t)=\deg C=\deg_0 C\,.\,H=\deg_0 C\,.\,\tilde{D}+\deg_0 C\,.\,G_m^\infty+\deg_0 C\,.\,G_a^\infty$ et d'autre part d'après les lemmes 2 et 7 et les remarques suivant la démonstration du lemme 6 on a, en posant $C'=[d](C)$:

$$\deg[d]^{-1}(C')=\frac{|\mathrm{Ker}\,[d]|}{|\mathrm{Ker}\,[d]\cap G_C|}\deg C$$

$$=|\mathrm{Ker}\,[d]|\{\deg_0 C'\,.\,\tilde{D}/d^2+\deg_0 C'\,.\,G_m^\infty/d+\deg_0 C'\,.\,G_a^\infty\}.$$

Donc, $[d^s](C)=C+t_s$ entraine:

$$\frac{d^{2s}}{|\mathrm{Ker}\,[d^s]\cap G_C|}(\deg_0 C\,.\,\tilde{D}+\deg_0 C\,.\,G_m^\infty+\deg_0 C\,.\,G_a^\infty)$$

$$=\deg_0 C\,.\,\tilde{D}+d^s\deg_0 C\,.\,G_m^\infty+d^{2s}\deg_0 C\,.\,G_a^\infty.$$

Si G_C est fini, en faisant s très grand on voit que $\deg_0 C\,.\,\tilde{D}=0=\deg_0 C\,.\,G_m^\infty$ ce qui entraine que $C\subset(\mathbb{G}_a)^r$ et la conclusion est alors élémentaire. Si G_C n'est pas fini alors $C=c_0+G_C$.

Remarquons qu'on peut extraire de la démonstration le corollaire:

Corollaire. *Si C est une courbe dans G,* $\deg[d](C)\leqq\dfrac{d^2}{|\mathrm{Ker}\,[d]\cap G_C|}\deg C\leqq d^2\deg C.$

Preuve du théorème. Soit x un point de torsion sur C, dont la projection sur A est d'ordre n, on choisit p de l'ordre de $\log n$ ne divisant pas n, on pose $d=p^c$, alors d'après le lemme 13i) il existe un point de torsion η de L et $\sigma\in\mathrm{Gal}(\bar{K}/K)$ tels que $\sigma x=[d](x)+\eta$; donc σx ainsi que tous ses conjugués sur $K(\eta)$ appartiennent à $C\cap([d](C)+\eta)$. Donc soit $[d](C)+\eta=C$ et alors C est un translaté de sous-groupe algébrique, soit $|C\cap([d](C)+\eta)|\leqq d^2(\deg C)^2$ et alors en utilisant le lemme 13ii) on obtient: $C_1'n^{1/q'}\leqq d^2(\deg C)^2$, soit encore $n/(\log n)^{2q'}\leqq C_3(\deg C)^{2q'}$.

Soit M un majorant de n, soit $C'=[M!](C)$, alors si x est un point de torsion de C', on a $x=[M!]y$ pour $y\in C$ et donc $\pi(x)=\pi([M!]y)=[M!](\pi(y))=0$ donc $C'\cap G_{\mathrm{tor}}\subset L_{\mathrm{tor}}$ et donc est fini (Cf le théorème 1), ce qui achève la démonstration.

Note. Cette démonstration est proche de l'idée originale de Lang dans [21].

b) Réduction du théorème général (cas des extensions sans $\mathbb{G}_a$)

Voyons qu'il suffit de prouver un résultat du type: «Soit G une extension d'une variété abélienne A par un tore L, soit V une sous-variété de G, il existe une constante $M=M(G,V)$ telle que si x est un point de torsion situé sur V *ou bien* il existe un sous-groupe algébrique maximal H de dimension non nulle tel que

$x+H\subset V$ et de degré borné par M, *ou bien* l'ordre de la projection de x sur A est borné par M''. En effet considérons $V'=[M!](V)$, si $x'\in V'\cap G_{\mathrm{tor}}$, alors $x'=[M!]x$ avec $x\in V\cap G_{\mathrm{tor}}$ donc ou bien il existe H sous-groupe algébrique de dimension non nulle telle que $x+H\subset C$ ou bien $0=[M!]\pi(x)=\pi([M!]x)=\pi(x')$ et donc $x'\in V'\cap L_{\mathrm{tor}}$ que l'on sait décrire comme union finie d'ensemble du type $t+H_{\mathrm{tor}}$ avec H sous-groupe algébrique. On conclut qu'il existe $M'=M'(G,V)$ telle que ou bien l'ordre de x est borné par M' ou bien V contient le translaté par x d'un sous-groupe algébrique de dimension positive. On raisonne alors par récurrence en considérant la clôture de Zariski de l'ensemble des translatés de sous-groupes algébriques de dimension positive contenus dans V:

$$Z=\overline{\bigcup_{\substack{t+H\subset V\\ \dim H>0}}(t+H)}\,.$$

Si $\dim Z<\dim V$ alors on peut supposer le théorème démontré pour Z, et donc pour V.

Si $Z=V$ on montre que $\dim G_V>0$ et qu'on peut se ramener à une sous-variété de dimension inférieure. En effet on peut dans l'écriture de Z ne considérer que les sous-groupe maximaux (qui sont en nombre fini car de degré borné) et donc on peut écrire: $V=Z=\bigcup_{i=1}^{r}\overline{\left\{\bigcup_{\lambda\in S_i}(t_\lambda+H_i)\right\}}$, mais comme V est irréductible, il existe $H_i=H$ tel que $V=\overline{\bigcup_{\lambda}(t_\lambda+H)}$ et donc H stabilise V. On considère alors le quotient $G\xrightarrow{p}G'=G/H$. On a alors $V=p^{-1}\{p(V)\}$ et $\dim p(V)<\dim V$; par récurrence on sait qu'il existe des points de torsion $t_1',\dots,t_r'$ et des sous-groupes algébriques de G': $H_1',\dots,H_r'$ tels que $p(V)\cap G'_{\mathrm{tor}}=\bigcup_{i=1}^{r}\{t_i'+H_i'(\bar K)_{\mathrm{tor}}\}$. En posant $p(t_i)=t_i'$ et $H_i=p^{-1}(H_i')$ on obtient bien: $V\cap G(\bar K)_{\mathrm{tor}}=\bigcup_{i=1}^{r}\{t_i+H_i(\bar K)_{\mathrm{tor}}\}$.

c) Fin de la démonstration (dans le cas sans $\mathbb{G}_a$)

Le démonstration suivante bien qu'un peu plus compliquée est très semblable à celle de la proposition 2 et du théorème 1; on répète néanmoins l'argument en étant bref sur les parties totalement similaires. On suppose le groupe G bien plongé dans $\mathbb{P}^N$ comme au § 1 et que V est une sous-variété de dimension m définie par des équations de degré au plus D dans G, on prouve alors le résultat suivant où l'on rappelle les constantes C_1' et q' du lemme 13:

Théorème 3. *Soit π un point de torsion de G situé sur V, alors ou bien V contient un translaté par x d'un sous-groupe algébrique de dimension strictement positive et de degré borné en fonction de G, K et du degré des équation définissant V, ou bien l'ordre de $\pi(x)$ est majoré par $C_0'(\deg VD^m)^{q'(h'm+1)}$, où C_0' est une constante ne dépendant que de G et K, et $h'=(2m+1)^m$.*

Preuve. Soit $x\in V$ un point de torsion tel que $\pi(x)$ soit d'ordre n, soit p ne divisant pas n et tel que $p^{2c}\geqq\deg V(2D)^m$, d'après le lemme 13, si l'on pose $d=p^c$, il existe $\sigma\in\mathrm{Gal}(\bar K/K)$ et $\eta\in L_{\mathrm{tor}}$ tels que $\sigma(x)=[d](x)+\eta$. Posons:

$$\eta_s=\eta^{d^{s-1}}\sigma(\eta^{d^{s-2}})\dots\sigma^{s-2}(\eta^d)\sigma^{s-1}(\eta)\,.$$

On verifie que $\eta^{d^s}(\eta_{s+1})^{-1}=\sigma(\eta_s)^{-1}$ et $\sigma^s(x)=[d^s](x)+\eta_s$. Comme $\sigma^s(x)\in V$, on a $x\in[d^s]^{-1}(V-\eta_s)$, ce qui suggère de poser $V_{d,t}=V_t=\bigcap_{s=0}^{t}[d^s]^{-1}(V-\eta_s)$ et de même $V_\infty=\bigcap_{s=0}^{\infty}[d^s]^{-1}(V-\eta_s)$. On voit que en posant $\sigma'=\sigma^{-1}$ on a:

$\sigma'([d]V_s+\eta)\subset V_{s-1}$, en effet:

$$[d]V_s+\eta\subset V\cap[d]^{-1}(V-\eta_2+\eta^d)\cap\ldots\cap[d^{s-1}]^{-1}(V-\eta_s+\eta^{d^{s-1}})$$
$$=V\cap\ldots\cap[d^{s-1}]^{-1}(V-\sigma(\eta_{s-1}))\,,$$

d'où:

$$\sigma'([d]V_s+\eta)\subset V\cap[d]^{-1}(V-\eta_1)\cap\ldots\cap[d^{s-1}]^{-1}(V-\eta_{s-1})=V_{s-1}\,.$$

Supposons que $\dim_x V_s=\ldots=\dim_x V_{s+k}$, alors il existe une composante C de V_s et V_{s+k} de dimension $\dim_x V_s$ et contenant x. Alors $\sigma'([d]V_{s+k}+\eta)$ est une composante de V_{s+k-1} et contient x; en répétant l'opération, on obtient une composante de V_s de la forme $C'=\tau([d^k]C+\eta')$. Bien sûr dans un bon plongement $\deg C'=\deg[d^k]C$. Si $m'=\dim_x V_s$ et $m=\dim V$ alors, pour $i+j=m'$, on a d'après le lemme 2 et les remarques suivant le lemme 6:

$$\deg_0([d]C).(\tilde{D})^i.(G_m^\infty)^j=\frac{d^{2i+j}}{|\mathrm{Ker}\,[d]\cap G_C|}\deg_0 C.(\tilde{D})^i.(G_m^\infty)^j.$$

D'après le lemme 8, si G_C^0 est une extension d'une sous-variété abélienne B de dimension g par un tore T de dimension t, on a:

$$|\mathrm{Ker}\,[d^k]\cap G_C|\leqq(G_C:G_C^0)d^{k(2g+t)}\leqq d^{k(2g+t)}\deg C(2d^{2s}D)^{m'-g-t}.$$

D'autre part: $\deg C=\sum_{i+j=m'}(m'!/i!j!)\deg_0 C.(\tilde{D})^i.(G_m^\infty)^j$ et donc:

$$\deg[d^k]C=\left\{\sum_{i+j=m'}(m'!/i!j!)d^{k(2i+j)}\deg_0 C.(\tilde{D})^i.(G_m^\infty)^j\right\}/|\mathrm{Ker}\,[d^k]\cap G_C|$$

qui est minoré par:

$$\left\{\sum_{i+j=m'}(m'!/i!j!)d^{k(2i+j-2g-t)-2s(m'-g-t)}\deg_0 C.(\tilde{D})^i.(G_m^\infty)^j\right\}/(2D)^{m'-g-t}\deg C.$$

Remarquons que tous les termes de la somme sont positifs ou nuls et qu'il y a un terme d'indice disons i,j non nul et que $\deg C\leqq\deg V(d^{2s}D)^{m-m'}$, donc:

$$\deg[d^k]C\geqq d^{k(2i+j-2g-t)-2s(m'-g-t)}/\deg V(2D)^m.$$

Ou bien $2i+j\leqq 2g+t$ chaque fois que $\deg_0 C.(\tilde{D})^i.(G_m^\infty)^j>0$ et alors on conclut que $C=G_C+x$ en utilisant le lemme 11.

Ou bien on obtient par le théorème de Bézout: $d^{k-2sm'}/\deg V(2D)^m\leqq\deg V(d^{2s}D)^{m-m'}$ soit encore: $d^{(k-2sm)}<(\deg V(2D)^m)^2$. Comme nous avons supposé que $d^2>\deg V(2D)^m$, on voit aisément que $k\leqq 2sm+4$. On vérifie que, en posant $h=(2m+1)^m$ on a $\dim_x V_h=\dim_x V_\infty$. Ainsi *ou bien* il existe un sous-groupe algébrique connexe non nul H tel que $x+H\subset V$, il est nécéssairement maximal et l'on peut borner son degré de la manière suivante:

Ecrivons que $x+G_C^0$ est composante de V_h et notons $B=\pi(G_C^0)$; d'après le lemme 9 il existe B' sous-variété abélienne de A telle que $A=B+B'$ et telle que: $|B\cap B'|\leqq C_A \deg B\leqq C_A \deg G_C^0$. On peut supposer $\pi(x)\in B'$ on déduit qu'il y a au moins $C_1' n^{1/q'}/\deg G_C^0$ translatés distincts de la forme $\sigma x+G_C^0$ avec $\sigma\in \mathrm{Gal}(\bar{K}/K^{cyc})$ en invoquant le lemme 13; la somme des degrés de ces translatés (tous composantes de V_h) est bornée par $\deg V(2d^{2h}D)^m$ d'après le théorème de Bézout. On écrit d'abord $C_1' n^{1/q}\leqq \deg V(2d^{2h}D)^m$ d'où l'on tire une borne pour n en utilisant le théorème des nombres premiers comme au paragraphe 4 en choisissant convenablement d, puis on écrit $\deg G_C^0\leqq \deg V(2d^{2h}D)^m$ où maintenant d est borné puisque n l'est. Notons que cela donne une démonstration de la finitude du nombre de sous-groupes algébriques maximaux dans V comme dans le corollaire de la proposition 2 – fait que nous avons utilisé lors de la réduction du théorème 2; *ou bien* $\dim_x V_h=0$ et alors comme tous les conjugués de x sur $K(\eta)$ appartiennent à V_h on en déduit, utilisant le lemme 13ii) et le théorème de Bézout encore une fois: $C_1' n^{1/q'}\leqq \deg V(d^{2h}D)^m$ d'où il n'est pas difficile d'en tirer la borne du théorème 3 comme précedemment.

d) Démonstration lorsque G contient un $\mathbb{G}_a$

Les complications proviennent de la possible existence d'une infinité de sous-groupes algébriques de degré borné, de l'absence de corps de rationnalité de degré fini sur $\mathbb{Q}$ pour les sous-groupes connexes et de l'existence de sous-variété stable par les isogénies $[d]$ sans être un translaté de sous-groupes algébriques.

Je remercie le referee pour m'avoir demandé de clarifier cette section et avoir notamment suggéré d'énoncer le lemme suivant:

Lemme 17. *Soit G un groupe algébrique commutatif connexe, soit G' le quotient de G par sa partie additive, soit d un entier* $\geqq 2$ *et soit V une sous-variété irréductible de G telle que* $[d](V)=V+v$, *alors:*

i) *L'image de V dans G' est un translaté d'un sous-groupe algébrique H' de G'.*

ii) *L'image de* G_V *(le stabilisateur de V dans G) dans G' est égale à H'.*

Preuve de i). En notant V' l'image de V dans G' on a $[d](V')=V'+v'$ donc d'après le lemme 10 on sait que V' est un translaté de sous-groupe.

Preuve de ii). Posons $m=\dim V$ et $c_{ijk}=m!/i!j!k!$, en reprenant le raisonnement du lemme 10 on obtient (pour tout entier $s\geqq 1$):

$$\deg(V+v_s)=\deg(V)=\sum_{i+j+k=m} c_{ijk}\deg_0 V.(\tilde{D})^i.(G_m^\infty)^j.(G_a^\infty)^k$$

$$=\sum_{i+j+k=m} c_{ijk}\frac{d^{s(2i+j)}}{|\mathrm{Ker}\,[d^s]\cap G_V|}\deg_0 V.(\tilde{D})^i.(G_m^\infty)^j.(G_a^\infty)^k.$$

Notons a (resp. a') la dimension de la partie abélienne de G_V (resp. H') et t (resp. t') la dimension de la partie tore linéaire de G_V (resp. H'), alors:

$$\text{Si}\quad \deg_0 V.(\tilde{D})^i.(G_m^\infty)^j.(G_a^\infty)^k \quad \text{n'est pas nul alors}\quad 2i+j=2a+t.$$

Puisque l'image de V dans G' a pour dimension abélienne a' et dimension linéaire t' on en déduit (comme au lemme 11) que:

$$\deg_0 V.(\tilde{D})^{a'}.(G_m^\infty)^{t'}.(G_a^\infty)^{m-a'-t'}>0 \quad \text{et donc} \quad 2a'+t'=2a+t.$$

Or il est clair que l'image de G_V dans G' est contenue dans H' donc $a'\geqq a$ et $t'\geqq t$ et enfin $a'=a$ et $t'=t$, ce qui prouve le lemme.

On procède maintenant à la démonstration:

Si x est un point de torsion sur V (avec $\pi(x)$ d'ordre n) on utilise le lemme 13 pour choisir σ, d et η tels que $\sigma(x)=[d](x)+\eta$ et on forme comme précédemment la suite V_s. Si $\dim_x V_\infty=0$ on montre comme précédemment que $\dim_x V_h=0$ et un utilisant le théorème de Bézout et le lemme 13ii) on obtient: $C_1' n^{1/q'}\leqq \deg V(d^{2h}D)^m$ d'où on tire une borne pour n. L'obstruction peut provenir d'une sous-variété C contenant x, de dimension m', possédant un stabilisateur G_C dont la partie abélienne est de dimension g et la partie tore linéaire de dimension t, qui reste composante de V_s. Si $i+j+k=m'$ et si $2i+j>2g+t$, alors $\deg V.(\tilde{D})^i.(G_m^\infty)^j.(G_a^\infty)^k=0$; d'après le lemme 17, on voit que, en notant n' l'application quotient par L_a le plus grand sous-groupe additif de G, on a $\pi(C)=\pi(x+G_C)$ et $\pi'(C)=\pi'(x+G_C)$. En particulier il existe une sous-variété affine C' (contenue dans un $(\mathbb{G}_a)^b$) telle que $C=C'+G_C$; ainsi $\pi'(G_C)$ ne peut être trivial car sinon x est nul (L_a n'a pas de point de torsion non nul). Le degré de G_C est borné par $\deg C(2d^{2s}D)^{m'}$ et si on pose $B=\pi(G_C^0)$ alors par le lemme 9 on peut choisir une sous-variété abélienne B' telle que $B+B'=A$ et $|B\cap B'|\leqq C_A \deg B\leqq C_A \deg G_C$ (l'application π est une projection linéaire, voir [3]). On peut supposer que $\pi(x)\in B'$, alors les conjugués par $\mathrm{Gal}(\bar{K}/K^{cyc})$ donnent au moins $C_1' n^{1/q'}/\deg B$ translatés distincts $\sigma\pi(x)+B$ et donc V_s possède au moins ce nombre de composantes du type σC distinctes; en utilisant encore une fois le théorème de Bézout on en déduit: $(C_1'/C_A)n^{1/q'}\leqq \deg V(2d^{2s}D)^m$, ce qui donne une borne pour n. Ayant majoré l'ordre de $\pi(x)$, on conclut alors le démonstration comme précédemment.

6. Réduction de la conjecture de Lang

Considérons les deux énoncés (où G est une extension d'une variété abélienne par un tore définie sur un corps de nombres K):

(a) Soit V une sous-variété de dimension $\leqq m$ de G, soit Δ un sous-groupe de type fini de $G(\bar{K})$, il existe des points de Δ: $t_1,\ldots,t_r$ et des sous-groupes algébriques $B_1,\ldots,B_r$ tels que $t_i+B_i\subset V$ et $V\cap\Delta=\bigcup_{i=1}^{r}\{t_i+(\Delta\cap B_i)\}$.

(b) Soit V une sous-variété de dimension $\leqq m$ de G, soit $\bar{\Delta}$ un sous-groupe de rang fini de $G(\bar{K})$, il existe des points de $\bar{\Delta}$: $t_1,\ldots,t_r$ et des sous-groupes algébriques $B_1,\ldots,B_r$ tels que $V\cap\bar{\Delta}=\bigcup_{i=1}^{r}\{t_i+(\bar{\Delta}\cap B_i)\}$.

On se propose de démontrer dans ce paragraphe que: «*L'énoncé (a) entraine l'énoncé (b) dans le cas où G est isogène à un produit de tore et de variété abélienne*». Dans le cas d'une extension non scindée la méthode oblige à faire des hypothèses sur $\bar{\Delta}$; nous discutons brièvement ce point dans une remarque. Rappelons que (b) est vrai si G est un tore d'après Laurent [24] et que si G est une variété abélienne et si V

ne contient pas de translaté de sous-variété abélienne non nulle l'implication: «(a) ⇒ (b)» a été prouvée par Raynaud [32]. Il suffit bien sûr de prouver ceci pour un produit d'un tore T et d'une variété abélienne A. De plus grâce au théorème de Mordell-Weil on peut sans perte de généralité supposer $\Delta = \Gamma \times A(K)$ où Γ est un sous-groupe de type fini de $(K^x)^s$; on peut aussi supposer que $\{x \in (K^x)^s / \text{il existe } n > 0$ tel que $x^n \in \Gamma\} = \Gamma$. On considère alors le groupe divisé $\bar{\Delta} = \{x \in G(\bar{K}) / \text{il existe } n > 0$ tel que $[n]x \in \Delta\}$ et on démontre le résultat suivant:

Théorème 4. *Suppose $T \times A = G$ bien plongé dans $\mathbb{P}^{N_1} \times \mathbb{P}^{N_2}$, soit V une K-sous-variété de dimension m, définie dans G par des équations de bidegré au plus (D_1, D_2), soit Δ' le sous-groupe obtenu en divisant Δ par $M \leqq f_0^{-1} H(V; 2D_1, 2D_2)$ et $K' = K(\Delta')$, soit Δ'' le sous-groupe obtenu en ajoutant à Δ' les points de torsion d'ordre au plus $C_0(G, K') H(V; 2D_1, 2D_2)$, alors: Si $P \in V \cap \bar{\Delta}$, ou bien $P \in V \cap \Delta''$, ou bien il existe un sous-groupe algébrique H de dimension positive tel que $P + H \subset V$.*

Remarque. La constante $C_0(G, K')$ est calculable en fonction de $c(G, K')$ que l'on peut prendre égale à $[K' : K] c(G, K)$, le degré $[K' : K]$ étant aisément majorable.

Preuve. Soit $M = \inf\{n \in \mathbb{N}^x / [n]P \in \Delta + G(\bar{K})_{\text{tor}}\}$ et soit $[M]P = P_0 + t_0$ avec $P_0 \in \Delta$ et $t_0 \in G_N$ (on peut supposer bien sûr que M divise N). D'après le lemme 14 et la théorie classique de Kummer, si l'on note $J(M, N)$ l'image du groupe $\mathrm{Gal}\left(K\left(A_N, \frac{1}{M} P_0\right) / K(A_N)\right)$ dans G_N alors $|J(M, N)| \geqq f_0 M$. Notons que bien sûr $K(G_N) = K(A_N)$ lorsque A est non nulle, ce que l'on peut bien sûr supposer ici. Considérons alors l'ensemble algébrique:

$$X = \bigcap_{t \in J(M,N)} (V + t).$$

X est définie sur $K(A_N)$, est stable par translation par $J(M, N)$ et $P \in X$. Soit C une composante de dimension maximale en P de X, alors $Y = \bigcup_{t \in J(M,N)} (C + t)$ est somme de composantes de X. Si $\dim G_C > 0$ alors $P + G_C \subset V$, et si $\dim G_C = 0$ alors d'après le lemme 8 on a: $|G_C| = \deg G_C \leqq H(C; 2D_1, 2D_2)$. Par ailleurs en appliquant le théorème de Bézout et l'invariance du degré par translation on obtient:

$$f_0 M \leqq |J(M, N)| \leqq \frac{|J(M, N)|}{|J(M, N) \cap G_C|} H(C; 2D_1, 2D_2) \leqq H(V; 2D_1, 2D_2).$$

Soit donc Δ' le sous-groupe obtenu en divisant Δ par $M \leqq f_0^{-1} H(V; 2D_1, 2D_2)$ et $K' = K(\Delta')$. On vient de montrer que soit il existe un sous-groupe algébrique H de dimension positive tel que $P + H \subset V$ soit $P = \delta' + t_0$ avec $\delta' \in \Delta'$ et $t_0 \in G(\bar{K})_{\text{tor}}$. Bien sûr $t_0 \in V - \delta'$, qui est définie sur K' et est définie dans G par des équations de bidegré au plus $(2D_1, 2D_2)$ donc d'après le théorème 1 soit il existe un sous-groupe algébrique de dimension positive H tel que $t_0 + H \subset V - \delta'$, et alors $P + H \subset V$, soit l'ordre de t_0 est au plus $C_0(G, K') H(V; 2D_1, 2D_2)$.

Voyons maintenant que l'on peut démontrer simplement par récurrence que «l'énoncé (a) pour des sous-variété de dimension $\leqq m$ de $G = T \times A$ entraine l'énoncé (b) pour les mêmes sous-variétés»:

On considère comme au § 5b l'ensemble algébrique Z adhérence de Zariski de l'ensemble des translatés de sous-groupes algébriques de dimension positive con-

tenus dans V. Si $Z=V$ alors comme en § 5b on se ramène à une sous-variété de dimension plus petite en quotientant par G_V^0 qui est de dimension positive. Si $\dim Z<\dim V$ alors on sait que $Z\cap\bar{\Delta}=\bigcup_{i=1}^{r}\{t_i+(\bar{\Delta}+H_i(\bar{K}))\}$ pour des points t_i de $\bar{\Delta}$ et des sous-groupes algébriques H_i. En utilisant le théorème 4 on voit que:

$$V\cap\bar{\Delta}=\{(V-Z)\cap\Delta''\}\,U\{Z\cap\bar{\Delta}\}.$$

On conclut en observant que l'énoncé (a) dit précisément que $(V-Z)\cap\Delta''$ est fini.

Concluons ce paragraphe en signalant que l'argument de théorie de Kummer ne passe pas en général aux extensions non scindées de A par $\mathbb{G}_m$. Ribet dans [33] a tout de même démontré que $\mathrm{Gal}\left(K\left(G_{N'}\frac{1}{N}P\right)/K(G_N)\right)$ restait «gros» lorsque le point $\pi(P)$ n'était pas contenu dans le $\mathrm{End}(A)$-module engendré par les points paramétrisant l'extension G au sens de [35]. Ces points sont dans $\hat{A}$ la variété duale de A, mais en prenant leur image par une isogénie de $\hat{A}$ sur A cela a un sens de parler du module qu'ils engendre sur $\mathrm{End}(A)$. Lorsque cette hypothèse d'indépendance linéaire est vérifiée on peut continuer la démonstration comme ci-dessus.

7. Quelque remarques sur la conjecture de Mordell-Lang

On s'intéresse dans ce paragraphe aux cas où l'on sait démontrer la conjecture de Lang pour Δ de type fini (alias la conjecture de Mordell-Lang). M. Laurent [24] a prouvé le résultat pour un tore linéaire, on se restreint donc aux variétés abéliennes. On cite les résultats connus et dans un deuxième temps on établit un lien avec la recherche de points de degré donné sur une courbe algébrique que nous avons dejà exploité dans [17].

a) Un théorème-désormais célèbre – de Faltings [10] affirme que si C est une courbe de genre $\geqq 2$ alors $C(K)$ est fini. Donc si Δ est un sous-groupe de type fini et C est une courbe non translatée d'une courbe elliptique dans une variété abélienne A, alors $C\cap\Delta$ *est fini et même d'après le* § 6 *ou les résultats de Raynaud cités*, $C\cap\bar{\Delta}$ est fini.

b) Les résultats de Michel Raynaud dans [32] contiennent le théorème suivant:

Théorème *(Raynaud). Soit K un corps de type fini sur $\mathbb{Q}$, soit k la clôture algébrique de $\mathbb{Q}$ dans K, soit V une K-sous-variété d'une variété abélienne A définie sur K; on suppose que la K/k Trace de A est nulle et que V ne contient aucun translaté de sous-variété abélienne non nulle, alors $V(K)$ est fini.*

Remarque. A l'hypothèse géométrique près sur V, c'est «la conjecture de Lang sur les corps de fonctions».

c) Le résultat le plus ancien, obtenue par un remarquable argument p-adique, est dû à Chabauty [6]; on peut le traduire ainsi:

Théorème *(Chabauty* 1941*). Si V est une sous-variété de dimension m d'une variété abélienne A de dimension g et si* $\mathrm{rang}_{\mathbb{Z}}A(K)=r$, *si ε est un sous-ensemble infini de $V(K)$, alors il existe une sous-variété abélienne B de dimension $\leqq r+m-1$ contenant un sous-ensemble infini de ε.*

Remarque. Dans le cas d'une courbe, Coleman [9] en déduit une borne effective pour le nombre de points rationnels sur une courbe engendrant une variété abélienne dont le rang du groupe de Mordell-Weil est strictement inférieur au genre.

Application. i) Si A est simple et si $r \leqq g-m$ alors $V(K)$ est fini

ii) Si V engendre A et si $r \leqq \dim A - \dim V$ alors les points de $V(K)$ ne sont pas Zariski denses dans V; en particulier si V est une surface la conjecture de Lang est vrai pour $V(K)$.

Exemple. Soient $s, t \in \mathbb{N}^x$ tels que $s+t<p$ un nombre premier régulier supérieur à 5, on considère la courbe $y^p = x^s(1-x)^t$ (qui est un facteur de la courbe de Fermat $X^p+Y^p=Z^p$), d'après [12] et [19], la jacobienne que nous noterons $A_{s,t,p}$ est simple (de dimension $(p-1)/2$) sauf si $p \equiv 1 \bmod 3$ et $s, t, -s-t$ sont les racines troisièmes de l'unité mod p; de plus on a $\operatorname{rang} A_{s,t,p}(\mathbb{Q}) \leqq \frac{1}{4}(p-5)$ si $p \equiv 1 \bmod 4$ (resp. $\leqq \frac{1}{4}(p-7)$ si $p \equiv 3 \bmod 4$). Par exemple si V est une $\mathbb{Q}$-sous-variété de $A_{1,1,41}$ de dimension $\leqq 11$ alors $V(\mathbb{Q})$ est fini.

d) Un autre résultat dans cette direction est dû à Manin et Demjanenko [25]:

Théorème *(Manin-Demjanenko). Soit V lisse possédant M morphismes $\mathbb{Z}$-indépendants dans une variété abélienne A, on suppose de plus le groupe de Néron-Severi de V cyclique et* $\operatorname{rang} A(K) < M$, *alors $V(K)$ est fini.*

e) Signalons aussi des résultats démontrant la conjecture «à un ensemble de densité nulle près» pour les courbes dus à Mumford [28] et en général à Martin Brown [5].

f) Terminons cette revue par des remarques et un lemme aisés:

On peut toujours supposer que: i) $0 \in V$, ii) G_V est fini (et même nul), iii) V engendre A, (évident); on prouve alors:

Lemme 18. *Soit V sous-variété de A, supposons que A possède un quotient B non trivial avec un groupe de Mordell-Weil $B(K)$ fini, alors $V(K)$ n'est pas Zariski-dense dans V; en particulier si V une surface la conjecture est vraie pour $A(K)$ et V.*

Preuve. Considérons le quotient $A \xrightarrow{p} B$; comme V engendre A, $p(V)$ engendre B et n'est donc pas réduit à un point. L'ensemble $V(K)$ est donc contenu dans $\bigcup_{x \in B(K)} \{V \cap p^{-1}(x)\}$ qui est une union fini de sous-variétés propres de V. La seconde affirmation résulte du théorème de Faltings.

Un exemple fort intéressant dû à Mazur [27] est celui de la jacobienne d'une courbe modulaire $X_0(p)$ et de son «quotient d'Eisenstein», voir [17] pour une application ainsi que [11] pour une utilisation similaire.

g) Lien avec les points de degré donné sur une courbe

Soit C une courbe algébrique définie sur K corps de nombres et $d \geqq 2$ un entier; on se demande quand il est vrai que l'ensemble des points de C de degré au plus d (l'ensemble des points de $C(\bar{K})$ rationnels sur un corps de degré $\leqq d$ sur K) est fini. Deux exemples interviennent clairement: si C est revêtement de degré $\leqq d$ de $\mathbb{P}^1$ ou d'une courbe elliptique E avec $E(K)$ infini alors il y une infinité de points sur C de degré $\leqq d$. Identifions C dans sa jacobienne $\operatorname{Jac}(C)$ et notons $W_d = W_d(C)$

$= C + \ldots + C$ (d fois); on se propose de prouver que la conjecture de Lang pour $\mathrm{Jac}(C)(K)$ et la sous-variété W_d entraine l'énoncé suivant:

Conjecture. *Supposons que C ne soit pas revêtement de degré $\leqq d$ de la droite projective et que $W_d(C)$ ne contienne pas de translaté de sous-variété abélienne non nulle, alors C ne possède qu'un nombre fini de points de degré $\leqq d$ sur K.*

Remarque. Si $e \geqq 1 + g/2$, une courbe de genre g est revêtement de degré $\leqq e$ de la droite projective; d'autre part observons que C est revêtement de degré $\leqq d$ d'une courbe elliptique si et seulement si W_d contient une courbe elliptique translatée.

Preuve que la conjecture de Lang implique la conjecture éconcée: On considère $S^d(C)$ le produit symétrique de C et les applications:

$$C \times \ldots \times C = (C)^d \xrightarrow{\pi} S^d(C) \xrightarrow{\Phi} W_d \subset \mathrm{Jac}(C),$$

$$(x_1, \ldots, x_d) \to [(x_1, \ldots, x_d)] \to x_1 + \ldots + x_d$$

(où $[(x_1, \ldots, x_d)]$ désigne le point $(x_1, \ldots, x_d)$ modulo permutation).

Supposons $\Phi(x) = \Phi(x')$ avec $x \neq x'$, alors il existe une fonction rationnelle f de C telle que: diviseur de $f = (x_1) + \ldots + (x_d) - (x_1') - \ldots - (x_d') \neq 0$ et donc f induit un morphisme de degré $\leqq d$ sur $\mathbb{P}^1$. Ainsi sous les hypothèses, Φ est injective. Un point de degré d possède d conjugués par $\mathrm{Gal}(\bar{K}/K)$: $x_1, \ldots, x_d$ et on peut lui associer le point $\Phi([x_1, \ldots, x_d]) = x_1 + \ldots + x_d \in W_d(K)$. Réciproquement soit $z \in W_d(K)$, alors $z = x_1 + \ldots + x_d$ avec $x_i \in C$. Comme Φ est injective on voit que pour tout $\sigma \in \mathrm{Gal}(\bar{K}/K)$ on a: $\{x_1, \ldots, x_d\} = \{\sigma x_1, \ldots, \sigma x_d\}$ et un raisonnement aisé montre qu'on peut décomposer $z = z_1 + \ldots + z_r$ avec $z_j \in W_{d_j}$ et $d_1 + \ldots + d_r = d$ tels que chaque z_j provienne d'un point de degré d_j de C. La conclusion cherchée équivaut alors à dire que $W_d(K)$ est fini ce qui est le contenu de la conjecture de Lang.

Concluons en remarquant que si K est un corps de type fini sur $\mathbb{Q}$, si k est la clôture algébrique de $\mathbb{Q}$ dans K, si C est une courbe sur K telle que la K/k Trace de sa jacobienne soit nulle (disons que C est complètement non isotriviale), alors, d'après les résultats de Raynaud [32] cités en *b*) la conjecture que nous avons énoncé est vérifiée (i.e. elle est vraie sur les corps de fonctions).

Appendice 1: Arguments de spécialisation

Soit K un corps de type fini sur $\mathbb{Q}$, en choisissant une $\mathbb{Q}$-sous-algèbre R de type fini dont le corps des fractions est K, on peut considérer les homomorphismes d'anneaux de R dans $\bar{\mathbb{Q}}$ «la» clôture algébrique de $\mathbb{Q}$. On appellera spécialisation un tel homomorphisme et on notera $x \to \tilde{x}$ la spécialisation des divers objets geométriques définis sur K en des objets définis sur $\tilde{K}$ l'image de R dans $\bar{\mathbb{Q}}$ ($\tilde{K}$ est un corps de nombres). On utilisera librement l'existence de spécialisations ayant de «bonnes propriétés»; elle provient simplement de la non-vacuité d'intersection d'ouverts de Zariski ou de variantes du théorème d'irréductibilité de Hilbert (Cf [20] chapitre 9 paragraphe 6).

Cet appendice a pour but de montrer que ce procédé permet d'étendre aux variétés définies sur un corps de type fini sur $\mathbb{Q}$ (et donc aux veriétés définies sur $\mathbb{C}$) les théorèmes établis dans ce travail pour des variétés définies sur un corps de

nombres (nous nous bornons par commodité aux variétés abéliennes). Notons que ces arguments deviendrait inutiles si on démontrait l'analogue du théorème 2 de [37] (le lemme 12i de ce travail) pour K corps de type fini sur $\mathbb{Q}$, car les lemmes 12ii et 14 sont encore valables (une spécialisation ne peut que baisser le degré d'une extension) et le reste de la démonstration est purement géométrique (donc valable sur tout corps de caractéristique nulle).

Une difficulté a priori provient de la possible apparition de nouvelles sous-variétés abéliennes quand on spécialise; nous allons controler ce phénomène grâce au lemme suivant:

Lemme A. *Soit A une variété abélienne définie sur un corps de caractéristique nulle plongée dans $\mathbb{P}^N$, soit V une sous-variété de A de dimension m définie par des équations de degré au plus D, soit Z_V la clôture de Zariski de l'union des translatés de sous-variétés abéliennes non nulles contenues dans V, soit d un entier tel que $d^2 \geqq \deg V(2D)^m$ et soit h la partie entière de $\sum_{i=0}^{h} (2m)^i/i!$ alors un point x de V est situé sur Z_V si et seulement si $\sum_{s=0}^{h} [d^s]^{-1}(V-x)$ est de dimension non nulle en l'origine.*

Remarque. L'interêt est que la propriété de dimension ou son contraire se conserve génériquement par spécialisation (i.e. hors d'un fermé propre).

Preuve. C'est un corollaire immédait de la proposition 2 (§ 3). Nous allons prouver:

Proposition B. *Soit K un corps de type fini sur $\mathbb{Q}$, soit A une variété abélienne sur K, soit Γ un sous-groupe de type fini de $A(K)$, alors il existe $M = M(A, V, K)$ telle que si $\gamma \in \Gamma$ et x est un point de torsion sur $\gamma + V$ et si aucune sous-variété abélienne B non nulle ne vérifie $x + B \subset \gamma + V$, alors l'ordre de x est borné par M.*

Cette proposition entraine bien sûr le théorème général décrivant la torsion sur V (et ses translatés par $A(K)$) et permet de prouver:

Proposition C. *La conjecture de Lang pour les sous-variétés de dimension $\leqq m$ et les sous-groupes de type fini de rang $\leqq r$, définis sur un corps de nombres entraine la conjecture générale de Lang pour les sous-variétés sur $\mathbb{C}$ de dimension $\leqq m$ et les sous-groupe de $A(\mathbb{C})$ de rang fini $\leqq r$.*

Preuve de B. On ramène tout de suite le corps de définition à un corps K de type fini sur $\mathbb{Q}$ (les objets ne font intervenir qu'un nombre fini de polynômes) et on prouve cela par induction sur la dimension de V. On peut supposer $Z_V \neq V$ car sinon on prouve comme au paragraphe 5 que $\dim G_V > 0$ et en passant au quotient par G_V on est ramené à une sous-variété de dimension plus petite que celle de V. On choisit une spécialisation injective sur Γ et telle que $\tilde{Z}_V$ soit une sous-variété propre de $\tilde{V}$ (voir [20] pour la possibilité d'un tel choix, particulièrement les théorème 6.2 et corollaire 6.3). Ainsi un point x de V hors d'un fermé propre de V se spécialise hors de $Z_{\tilde{V}}$ (grâce au lemme A). Si x est un point de torsion, alors d'après le théorème «uniforme» sur les corps de nombres l'ordre de $\tilde{x}$ est borné uniformément pour les divers translatés de $\tilde{V}$ par $\tilde{\Gamma}$ (corollaire du théorème 1 § 4) – la borne ne dépend que de $\tilde{K}$, $\tilde{A}$ et du degré des équations de V. En observant qu'une spécialisation de

caractéristique zéro à caractéristique zéro est injective sur les points de torsion on a donc prouvé la proposition B sauf peut-être pour les points situés sur une sous-variété propre de V et l'on conclut par récurrence sur la dimension de V.

Preuve de la proposition C. La structure de la réduction aux sous-groupes de type fini (§6) utilisait deux arguments non purement géométriques:

Un énoncé uniforme par translation par un sous-groupe de type fini qui est ici fourni par la proposition B et le lemme galoisien 14 dont on a déjà signalé qu'il s'étendait sans difficulté.

Enfin le lemme A permet de ramener la conjecture sur les sous-groupes de type fini à des variétés définies sur un corps de nombres:

On procède encore par induction sur la dimension de V. Si $Z_V = V$ on peut se ramener à une variété de dimension plus petite que V. Si $Z_V \neq V$, on choisit une spécialisation injective sur Γ telle que $\tilde{Z}_V \neq \tilde{V}$ et d'après le lemme A on peut assurer que $Z_{\tilde{V}}$ est un fermé propre de $\tilde{V}$; par hypothèse on suppose démontré qu'alors les points de $\tilde{V} \cap \tilde{\Gamma}$ ne sont pas Zariski denses dans $\tilde{V}$, donc l'ensemble $V \cap \Gamma$ n'est pas non plus Zariski dense dans V et l'on conclut par induction sur la dimension de V.

Appendix 2: Théorie de Kummer

Nous présentons ici pour la commodité du lecteur une démonstration de la proposition 1 paragraphe 2 dont nous reprenons les notations. Rappelons qu'il s'agit d'un résultat essentiellement dû à Ribet [33].

Notations. A est une variété abélienne définie sur un corps de nombres K; on note G_K le groupe de Galois absolu de K; A_n est le groupe des points de n-torsion; $G(n)$ désigne le quotient de G_K par $H(n)$ le sous-groupe de G_K fixant A_n (en fait $G(n)$ s'identifie naturellement à $\mathrm{Gal}(K(A_n)/K)$).

On prend un point P indivisible dans $A(K)$ (en particulier d'ordre infini), c'est-à-dire tel que si il existe $\alpha \in \mathrm{End}(A)$ et $Q \in A(K)$ tels que $\alpha(Q) = P$ alors il existe aussi $\beta \in \mathrm{End}(A)$ tel que $\beta(P) = Q$. On veut alors montrer que le groupe de Galois: $\mathrm{Gal}\left(K\left(A_n, \frac{1}{m} P\right)/K(A_n)\right)$ est essentiellement B_m le groupe des points de m-torsion de B la plus petite sous-variété abélienne contenant un multiple de P (on suppose $(G_P : B)m$ divise n, où G_P est le plus petit sous-groupe algébrique contenant P).

Remarque. L'hypothèse $(G_P : B)m$ divise n permet de se ramener dans la démonstration au cas $(G_P : B) = 1$ et en particulier dans ce cas tous les groupes $G\left(K\left(A_n, \frac{1}{m} P\right)/K(A_n)\right)$ s'identifient bien à des sous-groupes de B_m.

Nous prouvons maintenant la proposition par une série de lemmes:

Lemme D *(Sah). Soit α un élément du centre de G un groupe agissant sur V un groupe abélien, alors $\alpha - 1$ tue le premier groupe de cohomologie $H^1(G, V)$. En particulier si $\alpha - 1$ est un automorphisme de V on en déduit $H^1(G, V) = \{0\}$.*

Preuve. Classique; voir par exemple [20].

On note dans la suite $l_0 = l_0(A, K)$ un nombre premier assez grand pour que les lemmes énoncés soit vrais.

Lemme E. *Si $l \geqq l_0$ et si l divise n alors $H^1(G(n), A_l) = \{0\}$.*

Soit σ une homothétie de rapport d dans $G(n)$ (i.e. agissant comme $[d]$ sur A_n), alors si d n'est pas congru à 1 modulo l, $\sigma - 1$ est un automorphisme de A_l et le lemme D permet de conclure. Voyons qu'il existe toujours un tel σ si l est assez grand. Notons J_n le sous-groupe des éléments de $(\mathbb{Z}/n\mathbb{Z})^*$ représentant l'action d'un élément de Galois sur A_n. Si J_n est contenu dans le sous-groupe des éléments de $(\mathbb{Z}/n\mathbb{Z})^*$ congrus à 1 modulo l (rappel: l divise n) alors $l-1$ divise l'exposant du groupe $(\mathbb{Z}/n\mathbb{Z})^*/J_n$; mais ce dernier est borné d'après Serre [37] théorème 2 (Cf. lemme 12), donc l est borné.

Lemme F. *Soit $\Gamma = A(K)$, alors l'application:*

$$P \to \delta(P) : \sigma \to \sigma\left(\frac{1}{n} P\right) - \frac{1}{n} P,$$

est bien définie $\left(\text{i.e. ne dépend pas du choix de } \frac{1}{n} P\right)$ *et induit une injection de $\Gamma/n\Gamma$ dans $H^1(G_K, A_n)$.*

Plutot que de vérifier à la main ce lemme classique interprétons-le ainsi: On part de la suite exacte de G_K-modules:

$$0 \to A_n \to A(\bar{K}) \xrightarrow{[n]} A(\bar{K}) \to 0.$$

On en déduit la suite longue:

$$0 \to A_n(K) \to A(K) \xrightarrow{[n]} A(k) \xrightarrow{\delta} H^1(G_K, A_n) \to H^1(G_K, A(\bar{K})) \xrightarrow{[n]} H^1(G_K, A(\bar{K}))$$

On obtient la suite exacte courte cherchée:

$$0 \to A(K)/nA(K) \xrightarrow{\delta} H^1(G_K, A_n) \to (H^1(G_K, A(\bar{K})))_n.$$

Un calcul classique montre que δ est bien l'application de l'énoncé du lemme.

Lemme G. *Si $l \geqq l_0$ et l divise n alors l'application définie par:*

$$P \to \text{Restriction à } H(n) \text{ de } \delta(P)$$

$$\Gamma/l\Gamma \to H^1(H(n), A_l),$$

que l'on note encore δ est encore injective.

C'est une conséquence immédiate de l'exactitude de la suite inflation et restriction:

$$0 \to H^1(G(n), A_l) \xrightarrow{\text{inf}} H^1(G_K, A_l) \xrightarrow{\text{res}} H^1(H(n), A_l)$$

et des lemmes E et F (observer que comme l divise n on a: $A_l^{H(n)} = A_l$).

Enoncons maintenant sous forme de lemme les résultats de Faltings relatifs à la conjecture de Tate (Cf les «axiomes» de Ribet):

On note O l'anneau des endomorphismes de A; comme un endomorphisme trival sur A_n est divisible par n, on peut considérer O/nO comme un sous-anneau de

End (A_n). Avec une identification évidente on a $G(n) \subset \mathrm{Aut}(A_n)$ et l'on sait que O/nO commute avec $G(n)$.

Lemme H *(Faltings).* a) *Pour $l \geqq l_0$, O/lO est le commutant de $G(l)$ dans* End (A_l).
b) *Pour $l \geqq l_0$, A_l est un G_K-module semi-simple.*

Preuve voir [10].

Observons maintenant les deux propriétés suivantes:

$$\forall \alpha \in O, \quad \delta(\alpha P)(\sigma) = \alpha(\delta(P)(\sigma)). \tag{*}$$

$$\forall \tau \in G_K, \quad \delta(P)(\tau\sigma\tau^{-1}) = \tau\delta(P)(\sigma). \tag{**}$$

Notons M le sous-module de A_l qui s'identifie au groupe $\mathrm{Gal}\left(K\left(A_l, \frac{1}{l}P\right)/K(A_n)\right)$ pour l divisant n; M est un G_K-sous module d'après (**).

Lemme I. *Soit P un point d'ordre infini indivisible dans $A(K)$; soit B la plus petite sous-variété abélienne contenant un multiple de P; soit $l \geqq l_0$ tel que l divise n alors:*

$$\mathrm{Gal}\left(K\left(A_n \frac{1}{l}P\right)/K(A_n)\right) \quad \textit{s'identifie avec} \quad M = B_l.$$

D'après le lemme Hb), on peut décomposer $A_l = M \oplus M'$ comme G_K-module. Soit π la projection sur M' de noyau M, c'est un élément de End (A_l) commutant avec $G(l)$; d'après le lemme Ha) π provient d'un endomorphisme $\alpha \in O$ et on a:

$$M = \{x \in A_l / \alpha(x) = 0\} = A_l \cap \mathrm{Ker}\,\alpha.$$

Si l divise α alors $M = A_l$ (et donc $= B_l$); on écarte ce cas et on déduit alors de (*) que $\delta(\alpha(P)) = 0$, donc d'après le lemme G, $\alpha(P) \in l\Gamma$; mais P est par hypothèse indivisible (et l ne divise pas α) donc en fait $\alpha(P) = 0$. Donc Ker α contient le plus petit sous-groupe algébrique contenant P ce qui achève la démonstration du lemme (cette méthode est essentiellement due à Ribet [33]).

Lemme Ibis. *Avec les mêmes notations, si l^m divise n alors:*

$$\mathrm{Gal}\left(K\left(A_n, \frac{1}{l^m}P\right)/K(A_n)\right) \quad \textit{s'identifie avec} \quad M = B_{l^m}.$$

Il est équivalent de prouver une formulation l-adique de ce lemme. La preuve résulte du classique lemme de Nakayama ou si l'on préfère de la version explicite (et élémentaire) suivante: «Un sous-module fermé de $(\mathbb{Z}_l)^s$ dont l'image en réduction modulo l est $(\mathbb{F}_l)^s$ ne peut être que l'espace $(\mathbb{Z}_l)^s$».

Lemme J. *Supposons m et m' premier entre eux et mm' divise n alors les extensions $K\left(A_n, \frac{1}{m}P\right)$ et $K\left(A_n, \frac{1}{m'}\right)$ sont linéairement disjointes sur $K(A_n)$.*

C'est évident car les degrés de ces corps sur $K(A_n)$ sont premiers entre eux. Le résultat cherché est maintenant évident à partir des lemmes I et J, à condition de traiter l'ensemble fini de premiers exclus de lemme I:

Lemme K. *Il existe* $f(l)=f(l,A,K)$ *tel que dès que* l^m *divise* n *alors le groupe* $\mathrm{Gal}\left(K\left(A_n, \frac{1}{l^m}P\right)/K(A_n)\right)$ *s'identifie à un sous-groupe de* B_{l^m} *d'indice au plus* $f(l)$.

Il suffit de démontrer des analogues partiels des lemmes précédents: ainsi $H^1(G(n), A_{l^m})$ n'est plus nécéssairement nul mais et d'ordre borné indépendamment de m. On consultera [2] pour plus de précisions.

Références

1. Bertrand, D.: Minimal heights and polarizations on abelian varieties. Preprint MSRI, Berkeley juin 87 (à paraître)
2. Bertrand, D.: Galois representations and transcendental numbers. Proceedings of Durham conference 1986. (New advances in Transcendance theory, Baler A. ed. Cambridge University Press (à paraître)
3. Bertrand D., Philippon, P.: Sous-groupes de groupes algébriques commutatifs Ill. J. Math. **32**, 263–280 (1988)
4. Bogomolov, F.: Points of finite order on an abelian variety. Math. USSR Izv. **17**, 55–72 (1981)
5. Brown, M.: Schémas en groupes et lemmes de zéros. Publ. Paris **6**, problèmes diophantiens **73**, exposé n° 3, 17 pages (1984–85)
6. Chabauty, C.: Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension. C. R. Acad. Sci. Paris, Ser. A **212** (1941) p 1022–1024
7. Coleman, R.: Torsion points on curves and p-adic abelian inegrals. Ann. Math. **121**, 111–168 (1985)
8. Coleman, R.: Ramified points on curves. Duke Math. J. **54**, 615–40 (1987)
9. Coleman, R.: Effective Chabauty. Duke Math. J. **52**, 765–770 (1985)
10. Faltings, G.: Endlichkeitssätze für abelsche Varietaten über Zahlkörpern. Invent. Math. **73**, 349–366 (1983)
11. Frey, G.: A remark about isogenies of elliptic curves over quadratic fields. Compos. Math. **58**, 133–134 (1986)
12. Gross, B., Rohrlich, D.: Some result on the Mordell-Weil group of the Jacobian of the Fermat curve. Invent. Math. **44**, 201–224 (1978)
13. Hartshorne, R.: Algebraic geometry. Berlin-Heidelberg-New York: Springer 1977
14. Hindry, M.: Points de torsion sur les sous-variétés de variétés abéliennes. C.R. Acad. Sci., Paris Ser. A–304, **12**, 311–314 (1987)
15. Hindry, M.: Points de torsion sur les sous-variétés de groupes algébriques. Séminaire de théorie des nombres de Bordeaux (1986–87) exposé n° 18
16. Hindry, M.: Thèse de doctorat. (Université Paris 6, mai 1987)
17. Hindry, M.: Points quadratiques sur les courbes. C.R. Acad. Sci. Paris, Ser. A–305, 219–221 (1987)
18. Katz, N., Lang, S.: Finiteness in geometric classfield theory. Enseignement Math. **27**, 285–319 (1981)
19. Koblitz, N., Rohrlich, D.: Simple factors in the jacobian of the Fermat curve. Can. J. Math. **XXX**, 1183–1205 (1978)
20. Lang, S.: Fundamentals of diophantine geometry. Berlin-Heidelberg-New York: Springer 1983
21. Lang, S.: Division points on curves. Ann. Mat. Pura Appl. **LXX**, 229–234 (1965)
22. Lang, S.: Complex multiplication. Berlin-Heidelberg-New York: Springer 1983
23. Lange, H.: Translations de groupes algébriques commutatifs. C.R. Acad. Sci. Paris, Ser. A, **300**, 255–258 (1985)
24. Laurent, M.: Equations diophantiennes exponentielles. Invent. Math. **78**, 299–327 (1984)
25. Manin, Y.: The p-torsion of elliptic curves is uniformly bounded. Izv. Akad Nauk. USSR **33**, 433–438 (1969) AMS Transl.
26. Masser, D.: Small values of the quadratic part of the Néron-Tate height. Compos. Math. **53**, 153–170 (1986)

27. Mazur, B.: Modular curves and the Eisenstein ideal. Publ. Math., Inst. Hautes Etud. Sci. **47**, 33–186 (1977)
28. Mumford, D.: A remark on Mordell's conjecture. Amer. J. Math. **LXXXVII**, 1007–1016 (1965)
29. Philippon, P.: Lemme de zéros dans les groupes algébriques commutatifs. Bull. Soc. Math. France **114**, 355–383 (1986)
30. Raynaud, M.: Courbe sur une variété abélienne et points de torsion. Invent. Math. **71**, 207–233 (1983)
31. Raynaud, M.: Sous-variété d'une variété abélienne et points de torsion. Arithmetic and geometry (dédié à Shafarevic)Vol. 1, pp 327–352). Boston: Birkhäuser 1983
32. Raynaud, M.: Around the Mordell conjecture for function fields and a conjecture of Serge Lang. Proceedings of algebraic geometry of Tokyo (1982). (Lect. Notes Math., Vol. 1016). Berlin-Heidelberg-New York: Springer 1983
33. Ribet, K.: Kummer theory on extension of abelian varieties by tori. Duke Math. J. **46**, 745–761 (1979)
Voir aussi: Deficient points on extension of abelian varieties by G_m. (en collaboration avec O. Jacquinot) J. Number Theory **25**, 133–151 (1987)
34. Ribet, K.: Division fields of abelian varieties with complex multiplication. Mém. Soc. Math. France **2**, 75–94 (1980)
35. Serre, J.-P.: Groupes algébriques et corps de classes. Paris: Hermann 1959
36. Serre, J.-P.: Quelques propriétés des groupes algébriques commutatifs. Appendice dans Astérisque **69–70**, 191–202 (1979)
37. Serre, J.-P.: Résumé des cours au collège de France (1985–86). Ann. Collège France (1986) 95–99
38. Shimura, G., Taniyama, Y.: Complex multiplication of abelian varieties and its applications to number theory. Publ. Math. Soc. Japan **6**, Tokyo (1961)
39. Silverberg, A.: Points de torsion des variétés abéliennes de type CM. Publ. Univ. Paris 6, n° 79 problèmes diophantiens 1985–86

Oblatum 3-II-1988