Canad. Math. Bull.Vol. **36** (3), 1993 pp. 358–367

AUTOUR DU THÉORÈME DU SOUS-GROUPE ALGÉBRIQUE

DAMIEN ROY* ET MICHEL WALDSCHMIDT

RÉSUMÉ. A known consequence of the theorem of the algebraic subgroup is a lower bound for the rank of matrices whose entries are linear combinations, with algebraic coefficients, of logarithms of algebraic numbers. We extend this kind of result to commutative algebraic groups.

Introduction. Désignons par $\bar{\mathbf{Q}}$ la clôture algébrique de $\mathbf{Q}$ dans $\mathbf{C}$ et par $\mathcal{L}$ le sous-$\bar{\mathbf{Q}}$-espace vectoriel de $\mathbf{C}$ engendré par 1 et par les logarithmes de nombres algébriques :

$$\mathcal{L} = \{\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n \,;\, n \geq 0, \beta_i \in \bar{\mathbf{Q}}, \alpha_j \in \bar{\mathbf{Q}}^*\}.$$

Si m est un entier positif et V un sous-espace vectoriel de $\mathbf{C}^m$, une condition nécessaire et suffisante pour que le $\bar{\mathbf{Q}}$-espace vectoriel $V \cap \mathcal{L}^m$ soit de dimension finie est $V \cap \bar{\mathbf{Q}}^m = 0$; dans ce cas, on a

$$\dim_{\bar{\mathbf{Q}}}(V \cap \mathcal{L}^m) \leq m \dim_{\mathbf{C}}(V).$$

Ce résultat, qui est démontré dans [R2], repose sur le théorème du sous-groupe algébrique (*cf.* théorème 4.1 de [W1] et §6 de [R1]). Nous allons le généraliser en remplaçant le groupe multiplicatif $\mathbf{G}_{\mathrm{m}}$, qui apparaît implicitement ci-dessus, par un groupe algébrique commutatif G défini sur $\bar{\mathbf{Q}}$. Nous désignons par $\exp_G : T_G(\mathbf{C}) \longrightarrow G(\mathbf{C})$ l'application exponentielle du groupe de Lie $G(\mathbf{C})$; de plus, quand K est un corps de nombres, c'est-à-dire un sous-corps de $\bar{\mathbf{Q}}$ de degré fini sur $\mathbf{Q}$, nous désignons par $\Lambda_K(G)$ le sous-K-espace vectoriel de $T_G(\mathbf{C})$ engendré par les points $u \in T_G(\mathbf{C})$ tels que $\exp_G(u) \in G(\bar{\mathbf{Q}})$, et par $\Omega_K(G)$ le sous-espace de $\Lambda_K(G)$ engendré par le noyau de $\exp_G$.

Une première question consiste à trouver une condition nécessaire et suffisante pour qu'un sous-espace V de $T_G(\mathbf{C})$ vérifie $\dim_K\big(V \cap \Lambda_K(G)\big) < \infty$. Nous donnerons une telle condition et nous montrerons que, quand la dimension est finie, elle est majorée par $2d \dim_{\mathbf{C}} V$, avec $d = \dim G$.

Nous allons résoudre une question plus générale : quand E est un $\mathbf{C}$-espace vectoriel muni d'une $\bar{\mathbf{Q}}$-structure, V un sous-espace vectoriel de E et $\Psi : T_G(\mathbf{C}) \longrightarrow E$ une application linéaire rationnelle sur $\bar{\mathbf{Q}}$, nous donnons une condition nécessaire et suffisante pour que le K-espace vectoriel $V \cap \Psi\big(\Lambda_K(G)\big)$ soit de dimension finie. En particulier une condition suffisante est que V ne contienne pas de point rationnel sur $\bar{\mathbf{Q}}$ non nul. L'énoncé précis (*cf.* §2 ci-dessous) demande que V ne contienne pas l'image par Ψ de certains

* Le travail de cet auteur a été partiellement subventionné par le CRSNG et le FCAR.
Reçu par les éditeurs le 28 février 1992.
Classification (AMS) par sujet : 11J81.

sous-espaces de $T_G(\mathbf{C})$ lorsque cette image n'est pas réduite à zéro ; quand $K = \mathbf{Q}$ ces sous-espaces obstructeurs sont les sous-algèbres de Lie algébriques de $T_G(\mathbf{C})$ (*cf.* [W2]).

Quand la dimension considérée est finie, nous verrons qu'elle est encore majorée par $2d \dim_{\mathbf{C}} V$. Pour avoir une majoration plus fine, nous introduisons quelques ingrédients supplémentaires : d'abord nous tenons compte des éventuels points rationnels sur $\bar{\mathbf{Q}}$ de E qui appartiennent à V, l'espace qu'ils engendrent sera noté W, ainsi que des éléments de $V \cap \Psi\big(\Omega_K(G)\big)$ dont la dimension sur K sera désignée par le paramètre κ ; ensuite, afin que notre estimation contienne celle que l'on connaît dans le cas d'un groupe algébrique linéaire, nous écrivons G sous la forme $\mathbf{G}_{\mathrm{a}}^{d_0} \times \mathbf{G}_{\mathrm{m}}^{d_1} \times G_2$, avec $\dim G_2 = d_2$; alors nous obtenons la majoration

$$\dim_K \Big(V \cap \Psi\big(\Lambda_K(G)\big)\Big) \leq (d_1 + 2d_2 - \kappa) \dim_{\mathbf{C}}(V/W).$$

Le théorème ci-dessous est encore plus précis : par exemple, quand G_2 est un produit de courbes elliptiques, on peut tenir compte des éventuels endomorphismes non triviaux de certains facteurs. Pour cela nous introduisons au paragraphe 1 un coefficient $\alpha_K(G)$, dépendant du corps K et du groupe algébrique G, qui est toujours majoré par $d_1 + 2d_2$; mais pour une courbe elliptique A, quand k est le corps de ses endomorphismes, on a

$$\alpha_K(A) = \begin{cases} 1 & \text{si } k \neq \mathbf{Q} \text{ et } k \subset K\,; \\ 2 & \text{si } k \cap K = \mathbf{Q}. \end{cases}$$

Le premier paragraphe contient la définition de ce coefficient $\alpha_K(G)$, ainsi que la définition de l'ensemble des sous-espaces obstructeurs $\mathcal{S}_K(G)$. Le théorème principal se trouve au paragraphe 2, avec sa démonstration. Enfin des exemples sont donnés au paragraphe 3.

1. **Préliminaires.** Étant donné un groupe algébrique commutatif G défini sur $\bar{\mathbf{Q}}$, on note $d_0(G)$ (resp. $d_1(G)$) le plus grand entier d pour lequel il existe un homomorphisme surjectif, défini sur $\bar{\mathbf{Q}}$, de G dans $\mathbf{G}_{\mathrm{a}}^d$ (resp. dans $\mathbf{G}_{\mathrm{m}}^d$). On pose

$$\alpha(G) = 2\dim(G) - 2d_0(G) - d_1(G).$$

Ce nombre $\alpha(G)$ ne change pas si on remplace G par un groupe isogène à G sur $\bar{\mathbf{Q}}$. Il vérifie donc $\alpha(G) \leq d_1 + 2d_2$ si G est isogène sur $\bar{\mathbf{Q}}$ à un produit $\mathbf{G}_{\mathrm{a}}^{d_0} \times \mathbf{G}_{\mathrm{m}}^{d_1} \times G_2$ avec G_2 de dimension d_2. En vertu du lemme 4.3 de [R1], il vérifie aussi

$$\alpha(G') + \alpha(G/G') \leq \alpha(G)$$

pour tout sous-groupe algébrique G' de G défini sur $\bar{\mathbf{Q}}$ et

$$\alpha(G_1 \times G_2) = \alpha(G_1) + \alpha(G_2)$$

pour toute paire de groupes algébriques commutatifs G_1 et G_2 définis sur $\bar{\mathbf{Q}}$.

https://doi.org/10.4153/CMB-1993-049-8 Published online by Cambridge University Press

Soient K un corps de nombres de degré n sur $\mathbf{Q}$ et $(\beta_1, \dots, \beta_n)$ une base de K sur $\mathbf{Q}$. Identifiant $T_{G^n}(\mathbf{C})$ à $T_G^n(\mathbf{C})$, on définit une application $\mathbf{C}$-linéaire surjective

$$(1) \qquad \begin{aligned} p_\beta \colon T_{G^n}(\mathbf{C}) &\longrightarrow T_G(\mathbf{C}) \\ (z_1, \dots, z_n) &\longmapsto \beta_1 z_1 + \cdots + \beta_n z_n \end{aligned}.$$

Soit $\mathcal{S}_K(G)$ l'ensemble des sous-espaces de $T_G(\mathbf{C})$ de la forme $p_\beta\big(T_{G'}(\mathbf{C})\big)$, où G' est un sous-groupe algébrique de G^n défini sur $\bar{\mathbf{Q}}$. Il est clair que cet ensemble ne dépend que de K et non du choix de la base $(\beta_1, \dots, \beta_n)$. Ainsi, si $K = \mathbf{Q}$, $\mathcal{S}_{\mathbf{Q}}(G)$ n'est autre que l'ensemble des sous-algèbres de Lie algébriques de $T_G(\mathbf{C})$ (voir [B2]). De manière générale, on notera que les éléments de $\mathcal{S}_K(G)$ sont des sous-espaces de $T_G(\mathbf{C})$ rationnels sur $\bar{\mathbf{Q}}$, puisque p_β est rationnel sur $\bar{\mathbf{Q}}$. On considère aussi le plus grand sous-groupe algébrique connexe H de G^n, défini sur $\bar{\mathbf{Q}}$, qui vérifie $p_\beta\big(T_H(\mathbf{C})\big) = 0$ et on pose :

$$\alpha_K(G) = \frac{1}{n}\alpha(G^n/H).$$

Ce nombre ne dépend pas non plus du choix de la base de K sur $\mathbf{Q}$ et on vérifie que si $K_1 \subset K_2$ sont deux corps de nombres, on a $\alpha_{K_2}(G) \leq \alpha_{K_1}(G)$; en particulier $\alpha_K(G) \leq \alpha(G)$. Montrons que l'on a

$$(2) \qquad \alpha_K(G_1 \times G_2) = \alpha_K(G_1) + \alpha_K(G_2)$$

pour toute paire de groupes algébriques commutatifs G_1 et G_2 définis sur $\bar{\mathbf{Q}}$.

On pose $G = G_1 \times G_2$. Une base $(\beta_1, \dots, \beta_n)$ de K sur $\mathbf{Q}$ étant fixée, on définit à l'image de (1) des applications linéaires

$$p_i \colon T_{G_i^n}(\mathbf{C}) \longrightarrow T_{G_i}(\mathbf{C}) \quad (i = 1, 2);$$

l'application correspondante pour G est

$$p_1 \times p_2 \colon T_{G_1^n}(\mathbf{C}) \times T_{G_2^n}(\mathbf{C}) \longrightarrow T_{G_1}(\mathbf{C}) \times T_{G_2}(\mathbf{C}).$$

Pour $i = 1, 2$, soit H_i le plus grand sous-groupe algébrique connexe de G_i^n défini sur $\bar{\mathbf{Q}}$ qui vérifie $p_i\big(T_{H_i}(\mathbf{C})\big) = 0$ et soit H le sous-groupe algébrique de G^n défini de manière analogue. Puisque

$$(p_1 \times p_2)\big(T_{H_1}(\mathbf{C}) \times T_{H_2}(\mathbf{C})\big) = 0,$$

le produit $H_1 \times H_2$ est contenu dans H. Par ailleurs, si π_i désigne la projection de G^n sur son facteur G_i^n et si $\mathrm{d}\pi_i$ désigne la projection correspondante de $T_{G^n}(\mathbf{C})$ sur $T_{G_i^n}(\mathbf{C})$, alors $\pi_i(H)$ est un sous-groupe algébrique connexe de G_i^n défini sur $\bar{\mathbf{Q}}$, dont l'algèbre de Lie est $\mathrm{d}\pi_i\big(T_H(\mathbf{C})\big)$. Comme $p_1 \times p_2$ s'annule sur $T_H(\mathbf{C})$, p_i s'annule sur $\mathrm{d}\pi_i\big(T_H(\mathbf{C})\big)$. Cela implique $\pi_i(H) \subset H_i$ $(i = 1, 2)$, c'est-à-dire $H \subset H_1 \times H_2$. On en déduit $H = H_1 \times H_2$ et

$$G^n/H \cong G_1^n/H_1 \times G_2^n/H_2.$$

La relation (2) s'ensuit.

Le lemme suivant précise la valeur de α_K pour les groupes algébriques simples.

https://doi.org/10.4153/CMB-1993-049-8 Published online by Cambridge University Press

LEMME. *Soit K un corps de nombres de degré n. On a :*

$$\alpha_K(\mathbf{G}_a) = 0 \text{ et } \alpha_K(\mathbf{G}_m) = 1.$$

D'autre part, soient A une variété abélienne simple définie sur $\bar{\mathbf{Q}}$ de dimension g, D son algèbre d'endomorphismes, Z le centre de D, et KD la sous-K-algèbre de $\mathrm{End}_{\mathbf{C}}\big(T_A(\mathbf{C})\big)$ engendrée par D (K agit par homothétie sur $T_A(\mathbf{C})$). Alors on a

$$\alpha_K(A) = 2g\frac{\dim_K(KD)}{\dim_{\mathbf{Q}}(D)}.$$

Ce nombre vérifie $g \leq \alpha_K(A) \leq 2g$. De plus,

(i) si Z est totalement réel, on a $\alpha_K(A) = 2g$;

(ii) si A est de type CM*, et si K contient tous les plongements de Z dans $\mathbf{C}$, on a : $\alpha_K(A) = g$.*

Ainsi, quand A est une courbe elliptique, le lemme donne $\alpha_K(A) = 1$ si A admet des multiplications complexes ($D \neq \mathbf{Q}$) et si K contient un sous-corps isomorphe à D ; il donne $\alpha_K(A) = 2$ sinon.

DÉMONSTRATION. Le cas $G = \mathbf{G}_a$ est banal : on a en effet $\alpha_K(\mathbf{G}_a) \leq \alpha(\mathbf{G}_a) = 0$.

Si $G = \mathbf{G}_m$, on choisit une base de $T_G(\mathbf{C})$ sur $\mathbf{C}$ de sorte que $T_G(\mathbf{C})$ s'identifie à $\mathbf{C}$ et $T_{G^n}(\mathbf{C})$ à $\mathbf{C}^n$. Alors, les algèbres de Lie des sous-groupes algébriques de G^n s'identifient aux sous-espaces de $\mathbf{C}^n$ rationnels sur $\mathbf{Q}$. L'application p_β donnée par (1) fournit par restriction un isomorphisme de $\mathbf{Q}^n$ sur K, donc $T_H(\mathbf{C}) = 0$, $H = 0$ et

$$\alpha_K(\mathbf{G}_m) = \frac{1}{n}\alpha(\mathbf{G}_m^n) = \alpha(\mathbf{G}_m) = 1.$$

Passons enfin au cas d'une variété abélienne simple A. Les inégalités

$$\alpha_K(A) \leq \alpha(A) \leq 2g$$

sont banales. On considère de nouveau l'application $\mathbf{C}$-linéaire p_β de $T_{A^n}(\mathbf{C})$ dans $T_A(\mathbf{C})$ donnée par (1) relativement à une base $(\beta_1, \ldots, \beta_n)$ de K sur $\mathbf{Q}$, et on désigne par H le plus grand sous-groupe algébrique connexe de A^n qui vérifie $p_\beta\big(T_H(\mathbf{C})\big) = 0$.

L'algèbre d'endomorphismes D de A est naturellement plongée dans $\mathrm{End}_{\mathbf{C}}\big(T_A(\mathbf{C})\big)$. On a noté KD la sous-K-algèbre de $\mathrm{End}_{\mathbf{C}}\big(T_A(\mathbf{C})\big)$ qu'elle engendre ; on considère l'application linéaire surjective de D-modules à droite $\pi_\beta : D^n \longrightarrow KD$ qui envoie $(x_1, \ldots, x_n) \in D^n$ sur $\beta_1 x_1 + \cdots + \beta_n x_n$. Le groupe algébrique H est l'image d'un morphisme algébrique de A^{n-r} dans A^n, avec $r = \dim(A^n/H)$, dont l'application tangente, de $T_{A^{n-r}}(\mathbf{C})$ dans $T_{A^n}(\mathbf{C})$, est donnée par une matrice $n \times (n-r)$ à coefficients dans D dont les colonnes forment une base de $\ker(\pi_\beta)$ comme D-module à droite (voir par exemple le §7 de [SD]). Le quotient A^n/H est donc isomorphe à A^r avec $r = \dim_D(KD)$, et on obtient :

$$\alpha_K(A) = \frac{1}{n}\alpha(A^r) = 2g\frac{r}{n} = 2g\frac{\dim_{\mathbf{Q}}(KD)}{n\dim_{\mathbf{Q}}(D)}.$$

https://doi.org/10.4153/CMB-1993-049-8 Published online by Cambridge University Press

Pour minorer $\alpha_K(A)$, il n'y a pas de restriction à supposer K suffisamment gros. On désigne par S l'ensemble des plongements de Z dans $\mathbf{C}$, et on suppose à partir de maintenant que K contient $\sigma(Z)$ pour chaque $\sigma \in S$. L'algèbre $K \otimes_{\mathbf{Q}} D$ est alors isomorphe au produit direct des algèbres simples $D_\sigma = K \otimes_{Z,\sigma} D$ où Z agit sur K via σ. On a aussi une décomposition de $T_A(\mathbf{C})$ en somme directe de sous-espaces T_σ où Z agit par multiplication scalaire via σ. Comme KD est l'image de $K \otimes_{\mathbf{Q}} D$ par l'homomorphisme de K-algèbres qui applique $\beta \otimes x$ sur βx pour tout $\beta \in K$ et tout $x \in D$, on en déduit que KD est isomorphe au produit direct des D_σ pour les éléments σ de S tels que $T_\sigma \neq 0$. Donc, si n' désigne le nombre de ces derniers, on a $\alpha_K(A) = 2g(n'/n)$. Or, la représentation rationnelle de D est isomorphe à la somme directe de la représentation complexe de D et de son conjugué (lemme 39 de [SD]). En restreignant ce résultat à Z, on en déduit :

$$\frac{2g}{[Z:\mathbf{Q}]} = \dim_{\mathbf{C}}(T_\sigma) + \dim_{\mathbf{C}}(T_{\bar\sigma})$$

pour tout $\sigma \in S$, où $\bar\sigma$ désigne la composée de σ et de la conjugaison complexe de $\mathbf{C}$. Ainsi, pour chaque $\sigma \in S$, au moins un des espaces T_σ ou $T_{\bar\sigma}$ est non nul. Cela implique $n' \geq n/2$, donc $\alpha_K(A) \geq g$. Si le corps Z est totalement réel (c'est-à-dire si A est de première espèce au sens de [SD]), on a $T_\sigma = T_{\bar\sigma}$ pour tout $\sigma \in S$, donc $n' = n$ et $\alpha_K(A) = 2g$. Enfin, si A est de type CM, c'est-à-dire si $[Z:\mathbf{Q}] = 2g$, l'égalité ci-dessus montre que, pour chaque $\sigma \in S$, un et un seul des espaces T_σ et $T_{\bar\sigma}$ est $\neq 0$. Dans ce cas, on a $n' = n/2$ et on obtient $\alpha_K(A) = g$.

REMARQUE. Si O désigne l'anneau des entiers de K, on peut identifier G^n à $G \otimes_{\mathbf{Z}} O$. Cela munit G^n d'une structure de O-module (G^n devient ainsi un groupe algébrique de type (K) au sens du §1 de [B1]). Son algèbre de Lie s'identifie alors à $T_G(\mathbf{C}) \otimes_{\mathbf{Q}} K$ et, celle de G s'identifiant à $T_G(\mathbf{C}) \otimes_K K$, l'application (1) devient simplement la projection canonique

$$p\colon T_G(\mathbf{C}) \otimes_{\mathbf{Q}} K \longrightarrow T_G(\mathbf{C}) \otimes_K K.$$

On peut vérifier que les éléments de $\mathcal{S}_K(G)$ sont les images par p des algèbres de Lie des sous-groupes algébriques de G^n définis sur $\bar{\mathbf{Q}}$ et *stables sous l'action de* O (à savoir les sous-groupes algébriques de type (K) de G^n au sens du §1 de [B1]).

2. **Le résultat principal.** Dans tout ce paragraphe, G désigne un groupe algébrique commutatif défini sur $\bar{\mathbf{Q}}$ de dimension strictement positive. On désigne par $\Omega(G)$ le noyau de l'application exponentielle de G et par $\Lambda(G)$ le $\mathbf{Q}$-espace vectoriel formé par les logarithmes des points algébriques sur G :

$$\Omega(G) = \ker(\exp_G), \quad \Lambda(G) = \exp_G^{-1}\big(G(\bar{\mathbf{Q}})\big).$$

Quand K est un sous-corps de $\mathbf{C}$, on désigne par $\Omega_K(G)$ (resp. $\Lambda_K(G)$) le sous-K-espace vectoriel de $T_G(\mathbf{C})$ engendré par $\Omega(G)$ (resp. $\Lambda(G)$).

THÉORÈME. *Soient E un $\mathbf{C}$-espace vectoriel de dimension finie muni d'une $\bar{\mathbf{Q}}$-structure, $\Psi: T_G(\mathbf{C}) \longrightarrow E$ une application linéaire rationnelle sur $\bar{\mathbf{Q}}$, V et W deux sous-espaces de E avec $W \subset V$ et W rationnel sur $\bar{\mathbf{Q}}$, et K un corps de nombres. On pose*

$$\kappa = \dim_K\Big(V \cap \Psi\big(\Omega_K(G)\big)\Big).$$

Alors les conditions suivantes sont équivalentes :

(i) le sous-espace V ne contient pas de sous-espace non nul de la forme $\Psi(S)$ avec $S \in \mathcal{S}_K(G)$;

(ii) le K-espace vectoriel $V \cap \Psi\big(\Lambda_K(G)\big)$ est de dimension finie ;

(iii) on a

$$\dim_K\Big(V \cap \Psi\big(\Lambda_K(G)\big)\Big) \leq (\alpha_K(G) - \kappa)\dim_{\mathbf{C}}(V/W).$$

REMARQUES. 1. Le moyen le plus simple de satisfaire (i) est de demander que V ne contienne pas de point rationnel sur $\bar{\mathbf{Q}}$ non nul ; mais, dans ce cas, on est contraint à prendre $W = 0$ (voir le corollaire 1).

2. Quand $K = \mathbf{Q}$ et que Ψ est l'identité, on retrouve une conséquence du théorème du sous-groupe algébrique (théorème 4.1 de [W1]) qui est connue lorsque $\dim_{\mathbf{C}}(V) = d - 1$ (théorème 1.1 de [W1]), ou lorsqu'on remplace κ par 0 (remarque (i) du §6 de [R1]), mais qui se démontre en toute généralité en raffinant les arguments du §6 de [R1] (en travaillant avec la fonction a' au lieu de a'', dans les notations de [R1]). La démonstration de notre théorème va se déduire de ce cas particulier.

3. Quand Ψ est l'identité et que le groupe G est isomorphe à une puissance de $\mathbf{G}_{\mathrm{m}}$, le théorème présent se déduit du théorème 5 de [R2]. La démonstration qui suit s'inspire du même argument.

DÉMONSTRATION DU THÉORÈME. (a) Démontrons d'abord le théorème dans le cas $K = \mathbf{Q}$ quand Ψ est l'identité.

Le fait que (iii) implique (ii) est trivial.

Démontrer l'implication (ii) $\Longrightarrow$ (i) équivaut à vérifier que, pour tout sous-groupe algébrique G' de G défini sur $\bar{\mathbf{Q}}$ de dimension strictement positive, la dimension de $\Lambda(G')$ sur $\mathbf{Q}$ est infinie ou, ce qui revient au même, que le rang de $G'(\bar{\mathbf{Q}})$ comme groupe abélien est infini. Faute de pouvoir donner une référence précise pour ce résultat, nous renvoyons le lecteur aux démonstrations que nous avons incluses en appendice.

Enfin, l'implication (i) $\Longrightarrow$ (iii) découle du théorème 4.1 de [W1] de manière purement formelle, à l'aide des catégories. En effet, si une catégorie $\mathcal{C}$ et des fonctions $a, b, c, d, r: \mathrm{Ob}(\mathcal{C}) \longrightarrow \mathbf{N}$ vérifient les hypothèses de la proposition 2.1 de [R1] et au moins un des six énoncés de cette proposition, alors ils les vérifient tous les six ; en particulier, ils vérifient l'énoncé 3, donc aussi la propriété suivante : "Si Y est un objet de $\mathcal{C}$ qui satisfait $b(X) \neq 0$ pour tout noyau $i: X \longrightarrow Y$ de $\mathcal{C}$ de but Y avec $r(X) \neq 0$, alors on a $c(Y) \leq a(Y)b(Y)$". Pour obtenir le résultat en vue, il suffit d'appliquer cette observation à la catégorie $\mathcal{G}_w$ et aux fonctions a', b, c, d, r définies au §6 de [R1].

(b) Pour traiter le cas général, on écrit $K = \mathbf{Q}\beta_1 + \cdots + \mathbf{Q}\beta_n$ avec $n = [K : \mathbf{Q}]$ et on pose

$$\Psi_\beta = \Psi \circ p_\beta : T_{G^n}(\mathbf{C}) \longrightarrow E.$$

Notons que cette application Ψ_β est rationnelle sur $\bar{\mathbf{Q}}$. Soit H le plus grand sous-groupe algébrique connexe de G^n défini sur $\bar{\mathbf{Q}}$ qui vérifie $T_H(\mathbf{C}) \subset \ker(\Psi_\beta)$, et soit $G' = G^n/H$. Par passage au quotient, on obtient une application $\mathbf{C}$-linéaire Ψ' de $T_{G'}(\mathbf{C})$ dans E. Si on note

$$V' = \Psi'^{-1}(V) \quad \text{et} \quad W' = \Psi'^{-1}(W),$$

on a

$$\dim_{\mathbf{C}}(V'/W') = \dim_{\mathbf{C}}(V/W), \tag{3}$$

et W' est rationnel sur $\bar{\mathbf{Q}}$. De plus, Ψ' applique surjectivement $V' \cap \Lambda(G')$ sur $V \cap \Psi\big(\Lambda_K(G)\big)$ et $V' \cap \Omega(G')$ sur $V \cap \Psi\big(\Omega_K(G)\big)$. Par ailleurs, comme $\ker(\Psi')$ est rationnel sur $\bar{\mathbf{Q}}$ et ne contient pas d'élément non nul de $\mathcal{S}_{\mathbf{Q}}(G')$, le cas particulier de l'implication (i) $\Longrightarrow$ (iii) démontré en (a) donne $\Lambda(G') \cap \ker(\Psi') = 0$. Donc Ψ' est injectif sur $\Lambda(G')$ et on obtient :

$$\dim_K\Big(V \cap \Psi\big(\Lambda_K(G)\big)\Big) = \frac{1}{n}\dim_{\mathbf{Q}}\big(V' \cap \Lambda(G')\big) \tag{4}$$

$$\text{et} \quad \kappa = \dim_K\Big(V \cap \Psi\big(\Omega_K(G)\big)\Big) = \frac{1}{n}\dim_{\mathbf{Q}}\big(V' \cap \Omega(G')\big).$$

Si la condition (i) n'est pas vérifiée, V' contient un élément non nul de $\mathcal{S}_{\mathbf{Q}}(G')$; alors, comme on l'a vu en (a), la dimension de $V' \cap \Lambda(G')$ sur $\mathbf{Q}$ est infinie et, en vertu de (4), la dimension de $V \cap \Psi\big(\Lambda_K(G)\big)$ sur K est elle-aussi infinie. Cela démontre (ii) $\Longrightarrow$ (i) en toute généralité.

Enfin, si la condition (i) est vérifiée, V' ne contient pas d'élément non nul de $\mathcal{S}_{\mathbf{Q}}(G')$ et le cas particulier de l'implication (i) $\Longrightarrow$ (iii) démontré en (a) donne

$$\dim_{\mathbf{Q}}\big(V' \cap \Lambda(G')\big) \leq \Big(\alpha(G') - \dim_{\mathbf{Q}}\big(V' \cap \Omega(G')\big)\Big)\dim_{\mathbf{C}}(V'/W').$$

On peut aussi majorer $\alpha(G')$ par $n\alpha_K(G)$ puisque H contient le plus grand sous-groupe algébrique connexe de G^n défini sur $\bar{\mathbf{Q}}$ dont l'algèbre de Lie est contenue dans $\ker(p_\beta)$. Alors, en tenant compte de (3) et (4), on obtient l'inégalité (iii) du théorème. Cela démontre (i) $\Longrightarrow$ (iii) dans le cas général. Le fait que (iii) implique (ii) étant trivial, la démonstration du théorème est complète.

3. **Quelques corollaires.** On conserve les notations du paragraphe précédent.

COROLLAIRE 1. *Soient m un entier ≥ 1, K un corps de nombres et $f : T_G(\mathbf{C}) \longrightarrow \mathbf{C}$ une forme linéaire rationnelle sur $\bar{\mathbf{Q}}$. On pose $\mathcal{L} = f\big(\Lambda_K(G)\big) \subset \mathbf{C}$. Alors, pour tout sous-espace vectoriel V de $\mathbf{C}^m$ satisfaisant $V \cap \bar{\mathbf{Q}}^m = \{0\}$, on a :*

$$\dim_K\big(V \cap \mathcal{L}^m\big) \leq m\alpha_K(G)\dim_{\mathbf{C}}(V).$$

DÉMONSTRATION. *Il suffit d'appliquer le théorème à* $\Psi = f^m\colon \big(T_G(\mathbf{C})\big)^m \longrightarrow \mathbf{C}^m$.

Les deux derniers corollaires concernent le sous-$\bar{\mathbf{Q}}$-espace vectoriel de $\mathbf{C}$, que l'on désigne par $\mathcal{L}_G$, engendré par 1 et par les coordonnées des éléments de $\Lambda(G)$ dans une base de $T_G(\mathbf{C})$ rationnelle sur $\bar{\mathbf{Q}}$.

COROLLAIRE 2. *Supposons que G soit un produit de groupes algébriques $G_1 \times \cdots \times G_s$ avec G_i de dimension d_i pour $i = 1, \ldots, s$. Alors, pour tout entier $m \geq 1$ et tout sous-espace vectoriel V de $\mathbf{C}^m$ satisfaisant $V \cap \bar{\mathbf{Q}}^m = \{0\}$, on a*

$$\dim_{\bar{\mathbf{Q}}}\left(V \cap \mathcal{L}_G^m\right) \leq m\Big(\sum_{i=1}^{s} d_i \alpha(G_i)\Big) \dim_{\mathbf{C}}(V).$$

DÉMONSTRATION. Comme $\alpha(\mathbf{G}_a) = 0$, quitte à remplacer G par $\mathbf{G}_a \times G$, on se ramène à la situation dans laquelle $\mathcal{L}_G$ est le $\bar{\mathbf{Q}}$-espace vectoriel engendré par les coordonnées des éléments de Λ_G.

Soit $G' = G_1^{d_1} \times \cdots \times G_s^{d_s}$. On observe d'abord qu'il existe une forme linéaire $f\colon T_{G'}(\mathbf{C}) \longrightarrow \mathbf{C}$ rationnelle sur $\bar{\mathbf{Q}}$ telle que $\mathcal{L}_G = f\big(\Lambda_{\bar{\mathbf{Q}}}(G')\big)$. Par exemple, si $s = 1$, on a $G = G_1$ et, en posant $d = d_1$, on prend

$$\begin{aligned} f\colon T_G^d(\mathbf{C}) &\longrightarrow \mathbf{C} \\ (z_1, \ldots, z_d) &\longmapsto f_1(z_1) + \cdots + f_d(z_d) \end{aligned}$$

où $(f_1, \ldots, f_d)$ désignent les fonctions coordonnées attachées à une base de $T_G(\mathbf{C})$ rationnelle sur $\bar{\mathbf{Q}}$. Ainsi, pour conclure, il suffit de démontrer l'inégalité du corollaire avec un corps de nombres K quelconque au lieu de $\bar{\mathbf{Q}}$ et $f\big(\Lambda_K(G')\big)$ au lieu de $\mathcal{L}_G$. Cette nouvelle inégalité découle du corollaire 1 puisqu'on a

$$\alpha_K(G') \leq \alpha(G') = \sum_{i=1}^{s} d_i \alpha(G_i).$$

COROLLAIRE 3. *Soient s un entier ≥ 0 et $A_1, \ldots, A_s$ des courbes elliptiques définies sur $\bar{\mathbf{Q}}$. Pour chaque i, on note k_i le corps des endomorphismes de A_i. On pose $G = \mathbf{G}_a \times \mathbf{G}_m \times A_1 \times \cdots \times A_s$. Alors, pour tout entier $m \geq 1$ et tout sous-espace vectoriel V de $\mathbf{C}^m$ satisfaisant $V \cap \bar{\mathbf{Q}}^m = \{0\}$, on a*

$$\dim_{\bar{\mathbf{Q}}}(V \cap \mathcal{L}_G^m) \leq m\left(1 + 2\sum_{i=1}^{s} \frac{1}{[k_i : \mathbf{Q}]}\right) \dim_{\mathbf{C}}(V).$$

DÉMONSTRATION. On reprend la démonstration du corollaire 2 en observant que, pour tout corps de nombres K qui contient des sous-corps isomorphes à $k_1, \ldots, k_s$, on a, en vertu du lemme,

$$\alpha_K(\mathbf{G}_a \times \mathbf{G}_m \times A_1 \times \cdots \times A_s) = 1 + \sum_{i=1}^{s} \alpha_K(A_i) = 1 + \sum_{i=1}^{s} \frac{2}{[k_i : \mathbf{Q}]}.$$

https://doi.org/10.4153/CMB-1993-049-8 Published online by Cambridge University Press

4. **Appendice.** Au cours de la démonstration du théorème, nous avons utilisé le résultat suivant :

PROPOSITION. *Soit G un groupe algébrique commutatif de dimension $d > 0$, défini sur un corps de nombres k. Alors le rang de $G(\bar{\mathbf{Q}})$ en tant que groupe abélien est infini.*

Cet énoncé est sans aucun doute bien connu, mais faute d'avoir trouvé une référence explicite dans la littérature nous en indiquons deux démonstrations. La première, qui nous a été communiquée par Martin Brown, repose sur le théorème de spécialisation de Néron (voir le corollaire 6.3 du chapitre 9 de [L]). La seconde, que nous devons à l'amabilité de Marc Hindry, utilise la quadraticité de la hauteur de Néron-Tate.

DÉMONSTRATION. On peut supposer que G est connexe et qu'il ne contient aucun sous-groupe isomorphe à $\mathbf{G}_a$ ou à $\mathbf{G}_m$, car les rangs de $\mathbf{G}_a(\bar{\mathbf{Q}})$ et de $\mathbf{G}_m(\bar{\mathbf{Q}})$ sont infinis. Un théorème de Barsotti, Chevalley et Rosenlicht montre alors que G est une variété abélienne (voir par exemple le §1a de [H]).

PREMIÈRE DÉMONSTRATION. Soit donc G une variété abélienne sur un corps de nombres k de dimension $d \geq 1$; montrons que, pour tout entier $m \geq 1$, il existe un corps de nombres k_m tel que $G(k_m)$ ait un rang $\geq m$.

Le groupe abélien $G(\mathbf{C})$, quotient de $\mathbf{C}^d$ par un réseau, a un rang infini; pour tout m entier ≥ 1, il existe un corps k'_m de type fini sur k tel que le rang de $G(k'_m)$ soit $\geq m$. Le théorème de spécialisation de Néron permet de conclure.

DEUXIÈME DÉMONSTRATION. Soit D le degré de G dans l'espace projectif $\mathbf{P}^N$ dans lequel on suppose G plongé. On note $G(k, D)$ le sous-ensemble de $G(\bar{\mathbf{Q}})$ constitué des points de G définis sur une extension de k de degré $\leq D$. On va montrer que le rang du sous-groupe de $G(\bar{\mathbf{Q}})$ engendré par $G(k, D)$ est infini.

Pour cela on emploie la hauteur logarithmique absolue de Weil

$$h\colon \mathbf{P}^N(\bar{\mathbf{Q}}) \longrightarrow [0, \infty).$$

Soit X un nombre réel ≥ 2, et soit $n(X)$ le nombre de points de $G(k, D)$ de hauteur $\leq \log X$. On observe d'une part qu'il existe une constante $c_1 > 0$ indépendante de X telle que $n(X) \geq X^{c_1}$. En effet, d'après le théorème de spécialisation de Noether, il existe une projection linéaire de $\mathbf{P}^N$ sur $\mathbf{P}^d$, qui est définie sur k et qui induit par restriction un morphisme fini de G sur $\mathbf{P}^d$. Ce morphisme est de degré $\leq D$, donc tout point P de $\mathbf{P}^d(k)$ se relève en au moins un point Q de $G(k, D)$. De plus, il existe une constante $c > 0$ telle que si la hauteur de P est $\leq c \log X$, alors celle de Q est $\leq \log X$. Comme $\mathbf{P}^d(k)$ contient au moins X^{dc} points de hauteur $\leq c \log X$, on obtient $n(X) \geq X^{c_1}$ en posant $c_1 = dc$.

D'autre part, soit α l'homomorphisme canonique de $G(\bar{\mathbf{Q}})$ dans $\mathbf{R} \otimes_{\mathbf{Z}} G(\bar{\mathbf{Q}})$, dont le noyau est le sous-groupe de torsion de $G(\bar{\mathbf{Q}})$. La décomposition de Néron-Tate donne une forme quadratique définie positive q sur $\mathbf{R} \otimes_{\mathbf{Z}} G(\bar{\mathbf{Q}})$ et une constante $c_2 > 0$ qui vérifient

$$\left| h(P)^{1/2} - q\big(\alpha(P)\big)^{1/2} \right| \leq c_2$$

https://doi.org/10.4153/CMB-1993-049-8 Published online by Cambridge University Press

pour tout $P \in G(\bar{\mathbf{Q}})$ (voir le lemme 7 de [M]). En particulier, on a $h(P) \leq c_2^2$ pour tout point de torsion P de $G(\bar{\mathbf{Q}})$. Pour chaque $P_1 \in G(k, D)$, le nombre de $P_2 \in G(k, D)$ tels que $\alpha(P_1) = \alpha(P_2)$ est majoré par le nombre de points de torsion de $G(\bar{\mathbf{Q}})$ définis sur une extension de k de degré $\leq 2D$. Comme $\mathbf{P}^N(\bar{\mathbf{Q}})$ ne contient qu'un nombre fini de points de hauteur et de degré bornés, ce nombre est fini. Pour la même raison, il existe une constante $c_3 > 0$ telle que pour tout couple de points $P_1, P_2 \in G(k, D)$ avec $\alpha(P_1) \neq \alpha(P_2)$ on ait $q\big(\alpha(P_1) - \alpha(P_2)\big) > c_3$; en d'autres termes, dans la métrique induite par q, les points de l'image de $G(k, D)$ sont distants d'au moins $\sqrt{c_3}$. Si le rang du sous-groupe H de $G(\bar{\mathbf{Q}})$ engendré par $G(k, D)$ était fini, et si m était ce rang, la dimension réelle de $\mathbf{R} \otimes_{\mathbf{Z}} H$ serait aussi égale à m et les observations précédentes impliqueraient $n(X) \leq c_4 (\log X)^{m/2}$ avec une constante c_4 indépendante de X, en contradiction avec la borne inférieure établie ci-dessus.

REMERCIEMENTS. Ce travail a été entrepris lors d'un séjour de M. Waldschmidt aux universités Laval et McGill alors que D. Roy y était chercheur post-doctoral. Tous deux remercient vivement les professeurs C. Levesque et R. Murty pour leurs invitations.

RÉFÉRENCES

[B1] D. Bertrand, *Endomorphismes de groupes algébriques; applications arithmétiques*, Approximations Diophantiennes et Nombres Transcendants, (éd. D. Bertrand et M. Waldschmidt), Proc. Conf. Luminy 1982, Progress in Math. **31**, Birkhaüser (1983), 1–45.

[B2] ———, *Lemmes de zéros et nombres transcendants*, Sém. Bourbaki 38ème année, Nov. 85, no. 82 ; Astérisque **145–146**(1987), 21–44.

[H] M. Hindry, *Autour d'une conjecture de Serge Lang*, Invent. math. **94**(1988), 575–603.

[L] S. Lang, *Fundamentals of Diophantine Geometry*, Springer Verlag, 1983.

[M] D. Masser, *Small values of the quadratic part of the Néron-Tate height on an abelian variety*, Compositio Mathematica **53**(1984), 153–170.

[R1] D. Roy, *Transcendance et questions de répartition dans les groupes algébriques*, Approximations Diophantiennes et Nombres Transcendants, (éd. P. Philippon), Proc. Conf. Luminy 1990, W. de Gruyter (1992), 249–274.

[R2] ———, *Matrices whose coefficients are linear forms in logarithms*, J. Number Theory **41**(1992), 22–47.

[SD] H. P. F. Swinnerton-Dyer, *Analytic Theory of Abelian Varieties*, London Math. Soc. Lect. Note Ser. **14**, Cambridge Univ. Press 1974.

[W1] M. Waldschmidt, *On the transcendence methods of Gel'fond and Schneider in several variables*, New Advances in Transcendence Theory, (éd. A. Baker), Cambridge Univ. Press. 1988, Chap. 24, 375–398.

[W2] ———, *Dependence of logarithms of algebraic points*, Number Theory, Vol. II, Diophantine and Algebraic, Coll. Math. Soc. J. Bolyai **51**, North Holland (1987), 1013–1035.

McGill University
Department of Mathematics
805, rue Sherbrooke Ouest
Montréal, Québec H3A 2K6

Université P. et M. Curie (Paris VI)
Problèmes Diophantiens, URA 763 du C.N.R.S.
Institut Henri Poincaré
11, rue P. et M. Curie
75231 Paris Cedex 05 France