Densité des points rationnels sur un groupe algébrique

Michel Waldschmidt

À Wolfgang Schmidt pour son 60ème anniversaire

TABLE DES MATIÈRES

Partant d'une conjecture de Mazur concernant la topologie des points rationnels sur une variété algébrique, nous étudions la densité des sous-groupes de type fini du groupe des points rationnels d'un groupe algébrique commutatif sur un corps de nombres. Dans le cas particulier des groupes linéaires, le problème considéré se ramène à une conjecture bien connue sur l'indépendance algébrique de logarithmes linéairement indépendants de nombres algébriques.

Starting from a conjecture of Mazur concerning the topology of rational points on an algebraic variety, we consider the density properties of finitely generated subgroups of rational points on a commutative algebraic group over a number field. In the special case of linear algebraic groups, this problem reduces to a well known conjecture on the algebraic independence of linearly independent logarithms of algebraic numbers.

1. INTRODUCTION

Dans son article [Mazur 1992] sur la topologie des points rationnels, Mazur propose la conjecture suivante :

Conjecture 1.1 (Mazur). *Soit V une variété lisse définie sur $\mathbb{Q}$; on suppose que $V(\mathbb{Q})$ est dense dans V pour la topologie de Zariski ; alors l'adhérence de $V(\mathbb{Q})$ dans $V(\mathbb{R})$ pour la topologie réelle est ouverte (donc est réunion de composantes connexes de $V(\mathbb{R})$).*

Nous discutons ici ce type de problème quand V est un groupe algébrique commutatif ; au lieu de considérer tous les points rationnels, on en considère seulement un sous-groupe de type fini ; accessoire-

1058-6458/96 $0.50 per page

ment, on remplace le corps $\mathbb{Q}$ des rationnels par un corps de nombres K plongé dans $\mathbb{R}$ (ce sera suffisant, comme nous le verrons au paragraphe 5, pour traiter aussi le cas d'un corps de nombres plongé dans $\mathbb{C}$).

Définition 1.2. Soient K un corps de nombres plongé dans $\mathbb{R}$ et G un groupe algébrique commutatif défini sur K. On dira que G *possède la propriété de densité* si pour tout sous-groupe de type fini Γ de $G(K)$, les assertions suivantes sont équivalentes :

(i) $\Gamma \cap G(\mathbb{R})^0$ est dense dans $G(\mathbb{R})^0$;

(ii) si $\{\gamma_1, \dots, \gamma_l\}$ sont des éléments de Γ qui engendrent un sous-groupe d'indice fini de Γ et si H désigne l'adhérence de Zariski dans G^l du sous-groupe $\mathbb{Z}(\gamma_1, \dots, \gamma_l)$, alors il existe un point $(\eta_1, \dots, \eta_l)$ dans $H(\mathbb{R})$ tel que $\mathbb{Z}\eta_1 + \cdots + \mathbb{Z}\eta_l$ soit un sous-groupe dense de $G(\mathbb{R})^0$.

On a désigné par $G(\mathbb{R})^0$ la composante connexe de l'élément neutre de $G(\mathbb{R})$. L'implication (i) $\Rightarrow$ (ii) est banale : si $\Gamma \cap G(\mathbb{R})^0$ est dense dans $G(\mathbb{R})^0$, il suffit de prendre pour $(\eta_1, \dots, \eta_l)$ un multiple convenable de $(\gamma_1, \dots, \gamma_l)$. D'autre part si l'assertion (ii) est vraie pour une famille $\{\gamma_1, \dots, \gamma_l\}$ d'éléments de Γ qui engendrent un sous-groupe d'indice fini, alors elle est vraie pour toute famille. Enfin la propriété de densité est attachée au couple (G, K) plutôt qu'au groupe G tout seul, mais l'abus de notation allège le langage.

Les groupes unipotents $\mathbb{G}_{\mathrm{a}}^d$ possèdent trivialement la propriété de densité. Nous étudierons les groupes linéaires, les variétés abéliennes, certains produits, ainsi que les extensions d'une courbe elliptique par un groupe multiplicatif. Il semble raisonnable d'espérer que chacun de ces groupes algébriques possède la propriété de densité. Dans une première version de ce texte, la propriété de densité était présentée comme une conjecture pour tous les groupes algébriques commutatifs sur un corps de nombres réel ; mais D. Bertrand [1995] a montré que certaines extensions non triviales de variétés abéliennes par un groupe multiplicatif ne possèdent pas cette propriété.

Pour une variété abélienne simple A définie sur un corps de nombres réel K, dont le groupe de Mordell–Weil $A(K)$ est de rang ≥ 1, la propriété de densité, si elle est vérifiée, implique que tout point de $A(K) \cap A(\mathbb{R})^0$ d'ordre infini engendre un sous-groupe dense de $A(\mathbb{R})^0$; la conjecture de Mazur n'entraîne un tel résultat que quand $K = \mathbb{Q}$ et quand le rang de $A(\mathbb{Q})$ est égal à 1.

Un autre exemple intéressant consiste à prendre comme groupe algébrique G sur $K = \mathbb{Q}$ la restriction des scalaires, d'un corps de nombres k à $\mathbb{Q}$, du groupe multiplicatif $\mathbb{G}_{\mathrm{m}}$ (voir § 4). Pour ce groupe G, la conjecture de Mazur se déduit du théorème d'approximation faible :

> *quand k est un corps de nombres, l'image de $k^\times$ dans $(k \otimes_{\mathbb{Q}} \mathbb{R})^\times$ est dense,*

tandis que la propriété de densité permettrait de préciser l'énoncé suivant de D. Roy [1992b], qui répond à une question de Sansuc [1982] :

> *si r_1 est le nombre de plongements réels de k et $2r_2$ le nombre de plongements complexes non réels, il existe un sous-groupe de type fini de $k^\times$, de rang $r_1 + r_2 + 1$, dont l'image dans $(k \otimes_{\mathbb{Q}} \mathbb{R})^\times$ est dense.*

Plan de l'article

Nous ferons intervenir quatre types d'ingrédients :

- des conjectures de transcendance sur la fonction exponentielle usuelle équivalent à la propriété de densité pour les groupes linéaires ;
- des théorèmes de transcendance fournissent des réponses partielles ;
- un théorème de Kronecker sert à relier un énoncé de densité avec un résultat de transcendance ;
- enfin on utilise un lemme topologique de D. Roy.

Ces quatre outils sont présentés dans le paragraphe 2, qui termine par un exemple illustrant la méthode. Le théorème principal fait l'objet du paragraphe 3, où il est énoncé et démontré ; des conséquences de ce théorème principal en liaison avec la propriété de densité sont données aux paragraphes 4 et 5.

Notations

On note $\bar{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$. Quand G est un groupe algébrique commutatif défini sur un sous-corps K de $\bar{\mathbb{Q}}$, on désigne par T_G l'espace tangent à l'origine de G, par

$$\exp_G : T_G(\mathbb{C}) \to G(\mathbb{C})$$

l'exponentielle du groupe de Lie $G(\mathbb{C})$, par $\Omega_G = \ker \exp_G \subset T_G(\mathbb{C})$ son noyau et par

$$\mathcal{L}_K(G) = \exp_G^{-1} G(K) \subset T_G(\mathbb{C})$$

le $\mathbb{Z}$-module des logarithmes de points de $G(K)$.

Pour alléger l'écriture, on désignera par $\mathcal{L}$ le $\mathbb{Q}$-espace vectoriel $\mathcal{L}_{\bar{\mathbb{Q}}}(\mathbb{G}_{\mathrm{m}})$:

$$\mathcal{L} = \exp^{-1}(\bar{\mathbb{Q}}^\times) = \{z \in \mathbb{C};\, e^z \in \bar{\mathbb{Q}}^\times\}.$$

Les éléments de $\mathcal{L}$ sont les logarithmes (usuels) de nombres complexes algébriques non nuls. Pour $G = \mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}$, par exemple, on a $\mathcal{L}_{\bar{\mathbb{Q}}}(G) = \bar{\mathbb{Q}}^{d_0} \times \mathcal{L}^{d_1}$.

Quand G est un groupe algébrique commutatif défini sur $\bar{\mathbb{Q}}$ de dimension d, on désigne par d_0 et par d_1 les plus grands entiers ≥ 0 tels que G possède un facteur isomorphe sur $\bar{\mathbb{Q}}$ à $\mathbb{G}_{\mathrm{a}}^{d_0}$ et à $\mathbb{G}_{\mathrm{m}}^{d_1}$, respectivement. On pose $d_2 = d - d_0 - d_1$. Ainsi on peut écrire $G = \mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1} \times G_2$, où le groupe algébrique G_2 est défini sur $\bar{\mathbb{Q}}$, est de dimension d_2 et n'a pas de facteur linéaire non trivial. On définit alors, comme dans [Roy 1990b],

$$\alpha(G) = d_1 + 2d_2.$$

Pour un groupe algébrique de dimension d, on a $\alpha(G) \leq 2d$; si G est linéaire, $\alpha(G) \leq d$, avec égalité pour un tore.

Nous utiliserons la notation suivante, inspirée par [Roy 1992b] : si H est un groupe topologique, le nombre $m(H)$ désignera le plus petit rang d'un sous-groupe de type fini de H dense dans H ; ainsi, quand H est un groupe fini, on a $m(H) = 0$, tandis que pour $(d_0, d_1) \neq (0, 0)$, on a

$$m\big(\mathbb{R}^{d_0} \times (\mathbb{R}^\times)^{d_1}\big) = d_0 + d_1 + 1,$$
$$m\big(\mathbb{C}^{d_0} \times (\mathbb{C}^\times)^{d_1}\big) = 2d_0 + d_1 + 1.$$

Quand G est un groupe algébrique commutatif défini sur $\mathbb{C}$, nous écrirons $m_{\mathbb{C}}(G)$ au lieu de $m\big(G(\mathbb{C})\big)$. D'après un théorème de Barsotti [Serre 1979], le groupe algébrique G a un plus grand sous-groupe linéaire L et le quotient G/L est une variété abélienne A ; à son tour L se décompose en produit d'un facteur unipotent $\mathbb{G}_{\mathrm{a}}^u$ par un facteur de type multiplicatif (tore) $\mathbb{G}_{\mathrm{m}}^t$; alors $m_{\mathbb{C}}(G) = 2u + t + 1$. Si on désigne par $\kappa_{\mathbb{C}}(G)$ le rang de Ω_G, on a $\kappa_{\mathbb{C}}(G) = t + 2g$, où g est la dimension de A ; ces formules sont bien compatibles avec la relation $m_{\mathbb{C}}(G) + \kappa_{\mathbb{C}}(G) = 2d + 1$, où $d = u + t + g$ est la dimension de G.

Soit maintenant G un groupe algébrique commutatif défini sur $\mathbb{R}$; nous posons $m_{\mathbb{R}}(G) = m\big(G(\mathbb{R})\big)$. L'application exponentielle du groupe de Lie connexe $G(\mathbb{R})^0$ est la restriction à $T_G(\mathbb{R})$ de $\exp_G$; si on désigne par $\kappa_{\mathbb{R}}(G) = \operatorname{rang}\big(\Omega_G \cap T_G(\mathbb{R})\big)$ le rang de son noyau, on a

$$m_{\mathbb{R}}(G) + \kappa_{\mathbb{R}}(G) = d + 1,$$

avec $d = \dim(G)$.

Pour une variété abélienne A de dimension d, on a $\kappa_{\mathbb{R}}(A) = d$ et $m_{\mathbb{R}}(A) = 1$, tandis que pour un groupe linéaire déployé $L = \mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}$ on a $\kappa_{\mathbb{R}}(L) = 0$ et $m_{\mathbb{R}}(L) = d + 1$, avec $d = d_0 + d_1$.

2. TRANSCENDANCE ET APPROXIMATION DIOPHANTIENNE

2a. Conjectures de transcendance sur la fonction exponentielle

Voici la principale conjecture concernant les logarithmes de nombres algébriques :

Conjecture 2.1 (d'indépendance algébrique). *Si des éléments $\lambda_1, \ldots, \lambda_n$ de $\mathcal{L}$ sont $\mathbb{Q}$-linéairement indépendants, alors ces éléments sont algébriquement indépendants.*

On ne sait pas encore démontrer qu'il existe deux éléments de $\mathcal{L}$ qui sont algébriquement indépendants ! Nous utiliserons plusieurs fois le cas particulier suivant de la conjecture d'indépendance algébrique :

Conjecture 2.2 (d'indépendance algébrique homogène réelle). *Soient $\alpha_1, \dots, \alpha_n$ des nombres algébriques réels positifs multiplicativement indépendants. Si $P \in \mathbb{Z}[X_1, \dots, X_n]$ est un polynôme* homogène *non nul, alors le nombre $P(\log \alpha_1, \dots, \log \alpha_n)$ n'est pas nul.*

Un autre cas particulier bien connu de la conjecture d'indépendance algébrique a été proposé notamment par Schneider, Lang et Ramachandra :

Conjecture 2.3 (des quatre exponentielles). *Soit M une matrice 2×2 à coefficients logarithmes de nombres algébriques ; on suppose que les deux colonnes de M sont linéairement indépendantes sur $\mathbb{Q}$ et aussi que les deux lignes de M sont linéairement indépendantes sur $\mathbb{Q}$; alors la matrice M est inversible.*

La conjecture d'indépendance algébrique équivaut, d'après [Roy 1989], à une description conjecturale du rang des matrices à coefficients dans le $\mathbb{Q}$-espace vectoriel engendré par 1 et $\mathcal{L}$. Le point essentiel est l'énoncé suivant ([Roy 1989, proposition 3] ; c'est le seul énoncé de cette sous-section qui ne soit pas conjectural !) :

Proposition 2.4 (critère d'indépendance algébrique). *Soient $t_1, \dots, t_n$ des nombres complexes algébriquement indépendants, et $x_1, \dots, x_n$ des nombres complexes quelconques. Pour que $x_1, \dots, x_n$ soient algébriquement indépendants sur $\mathbb{Q}$, il faut et il suffit que pour toute matrice M à coefficients dans $\mathbb{Q} + \mathbb{Q}t_1 + \dots + \mathbb{Q}t_n$, le rang de M soit égal au rang de la matrice M' à coefficients dans le $\mathbb{Q}$-espace vectoriel $\mathbb{Q} + \mathbb{Q}x_1 + \dots + \mathbb{Q}x_n$ obtenue en spécialisant t_i en x_i pour $1 \le i \le n$.*

Pour obtenir ce critère, D. Roy démontre que si A est un anneau (commutatif unitaire) et $R = A[T_1, \dots, T_n]$ est l'anneau des polynômes à coefficients dans A, tout élément de R est le déterminant d'une matrice à coefficients dans le A-module $A + AT_1 + \dots + AT_n$ (voir aussi [Roy 1995, proposition 3.3]).

Ce critère d'indépendance algébrique nous permettra de voir au paragraphe 3 (lemmes 3.4 et 3.5) que la conjecture d'indépendance algébrique homogène réelle est équivalente à la propriété de densité pour un groupe linéaire déployé $\mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}$ et qu'elle est aussi équivalente à la propriété de densité pour un tore déployé $\mathbb{G}_{\mathrm{m}}^{d}$.

2b. Théorèmes de transcendance

Les réponses partielles que nous obtiendrons dépendent du Théorème du sous-groupe algébrique ([Waldschmidt 1988, théorème 1.1] ; il nous suffit ici d'un cas particulier [Waldschmidt 1987, théorème 4.1 ; Roy 1990b, p. 270, remarque 1], que nous appelons quand même "Théorème du sous-groupe algébrique").

Théorème 2.5 (du sous-groupe algébrique). *Soient G un groupe algébrique commutatif défini sur un sous-corps K de $\bar{\mathbb{Q}}$ et $\mathcal{V}$ un sous-espace vectoriel de $T_G(\mathbb{C})$; on suppose que, si G' est un sous-groupe algébrique de G défini sur K de dimension > 0, $\mathcal{V}$ ne contient pas $T_{G'}(\mathbb{C})$. On définit $\kappa = \mathrm{rang}_{\mathbb{Z}}(\mathcal{V} \cap \Omega_G)$. Alors le $\mathbb{Z}$-module $\mathcal{V} \cap \mathcal{L}_K(G)$ est de rang fini majoré par*

$$\mathrm{rang}_{\mathbb{Z}}\big(\mathcal{V} \cap \mathcal{L}_K(G)\big) \le \big(\alpha(G) - \kappa\big)(d-1).$$

Pour un tore déployé $G = \mathbb{G}_{\mathrm{m}}^{d}$ (voir aussi [Waldschmidt 1981 ; Emsalem 1987, théorèmes 1 et 2 ; Waldschmidt 1987, théorème 1.1]), on en déduit :

Théorème 2.6 (du sous-groupe linéaire). *Soient d un entier positif et $\mathcal{V}$ un sous-espace vectoriel de $\mathbb{C}^d$ tel que $\mathcal{V} \cap \mathbb{Q}^d = \{0\}$. Alors le $\mathbb{Q}$-espace vectoriel $\mathcal{V} \cap \mathcal{L}^d$ est de dimension finie $\le d(d-1)$.*

L'exemple le plus simple a été démontré dans [Lang 1966, chap. II, théorème 1] et [Ramachandra 1968, p. 67] :

Théorème 2.7 (des six exponentielles). *Soit M une matrice $d \times l$ à coefficients logarithmes de nombres algébriques ; on suppose que les d colonnes de M sont linéairement indépendantes sur $\mathbb{Q}$ et aussi que les l lignes de M sont linéairement indépendantes sur $\mathbb{Q}$; si $dl > d + l$, le rang de M est ≥ 2.*

2c. Le théorème de Kronecker

Nous rappelons ici un résultat d'approximation diophantienne bien connu qui joue un rôle central dans la suite : il s'agit d'un théorème de Kronecker sur la densité de sous-groupes de type fini d'un $\mathbb{R}$-espace vectoriel de dimension finie (voir par exemple [Cassels 1957]).

Théorème 2.8 (Kronecker). *Soient E un $\mathbb{R}$-espace vectoriel de dimension finie et Y un sous-groupe de type fini de E. Les conditions suivantes sont équivalentes :*

(i) *Y est dense dans E ;*

(ii) *pour tout sous-espace vectoriel V de E, $V \neq E$, on a*
$$\operatorname{rang}_{\mathbb{Z}}\bigl(Y/Y\cap V\bigr) > \dim_{\mathbb{R}}\bigl(E/V\bigr) ;$$

(iii) *pour toute forme linéaire non nulle $\varphi : E \to \mathbb{R}$, on a $\varphi(Y) \not\subset \mathbb{Z}$.*

Choisissons une base $(e_1, \dots, e_d)$ de E sur $\mathbb{R}$, des générateurs $y_1, \dots, y_l$ de Y (ou d'un sous-groupe d'indice fini de Y) sur $\mathbb{Z}$ et écrivons les coordonnées des y_j dans la base choisie :
$$y_j = y_{1j}e_1 + \cdots + y_{dj}e_d,$$
où $1 \le j \le l$. Alors la condition (iii) s'écrit

(iv) *pour tout $(s_1, \dots, s_l) \neq (0, \dots, 0)$ dans $\mathbb{Z}^l$, la matrice*
$$\begin{pmatrix} y_{11} & \cdots & y_{1l} \\ \vdots & \ddots & \vdots \\ y_{d1} & \cdots & y_{dl} \\ s_1 & \cdots & s_l \end{pmatrix}$$
est de rang $d+1$.

2d. Lemme topologique de D. Roy

Lemme 2.9 [Roy 1992b, lemme 3.3]. *Soient E un $\mathbb{R}$-espace vectoriel de dimension finie d, Y_0 un sous-groupe discret de E, Y un sous-groupe de type fini de E contenant Y_0 ; on suppose que tout sous-groupe de Y contenant Y_0 et de rang $\ge \operatorname{rang} Y - d + 1$ est dense dans E ; alors il existe un sous-groupe de Y, de rang $d+1$, dense dans E et qui contient Y_0.*

2e. Illustration de la méthode avec $\mathbb{G}_{\mathrm{m}}^2$

Voici, sur l'exemple du groupe algébrique $\mathbb{G}_{\mathrm{m}}^2$, comment interviennent les différents instruments que nous venons d'introduire.

1. Densité de sous-groupes de type fini de $(\mathbb{R}_+^\times)^2$

Considérons des éléments $\gamma_1, \dots, \gamma_l \in (\mathbb{R}_+^\times)^2$, multiplicativement indépendants, et écrivons
$$\gamma_j = (\alpha_j, \beta_j)$$
pour $j = 1, \dots, l$. D'après le théorème de Kronecker, le sous-groupe Γ engendré par $\gamma_1, \dots, \gamma_l$ est dense dans $(\mathbb{R}_+^\times)^2$ si et seulement si, pour tout $s \in \mathbb{Z}^l \setminus \{0\}$, la matrice à trois lignes et l colonnes
$$\begin{pmatrix} \log\alpha_1 & \cdots & \log\alpha_l \\ \log\beta_1 & \cdots & \log\beta_l \\ s_1 & \cdots & s_l \end{pmatrix}$$
est de rang 3. Une condition évidemment nécessaire est que pour tout $(a, b) \in \mathbb{Z}^2 \setminus \{0\}$, deux au moins des l nombres
$$a\log\alpha_1 + b\log\beta_1,\ \dots,\ a\log\alpha_l + b\log\beta_l$$
soient $\mathbb{Q}$-linéairement indépendants. Cette condition signifie que pour tout sous-groupe algébrique G' de $G = \mathbb{G}_{\mathrm{m}}^2$ de dimension 1, la projection de Γ sur $(G/G')(\mathbb{R})$ est dense (ce qui veut dire ici qu'elle a un rang > 1).

On suppose maintenant que cette condition est vérifiée, et aussi que les $2l$ nombres α_j et β_j sont algébriques.

(a) Si on admet la conjecture des quatre exponentielles et si $l \ge 3$, alors Γ est dense dans $(\mathbb{R}_+^\times)^2$. Ainsi les seules contraintes sont :
$$\operatorname{rang}_{\mathbb{Z}}\bigl(\Gamma/\Gamma \cap G'(\mathbb{R})\bigr) > \dim(G/G')$$
pour tout sous-groupe algébrique G' de G distinct de G. Ces contraintes nous permettent de vérifier la condition (ii) du théorème de Kronecker pour les sous-espaces vectoriels de $\mathbb{R}^2$ rationnels sur $\mathbb{Q}$, tandis que la conjecture des quatre exponentielles permet de traiter les sous-espaces vectoriels de $\mathbb{R}^2$ qui ne sont pas rationnels sur $\mathbb{Q}$.

(b) D'après le théorème des six exponentielles, si $l \geq 4$, alors Γ est dense dans $(\mathbb{R}_+^\times)^2$.

Par exemple pour $l = 4$, si les huit nombres α_j, β_j sont multiplicativement indépendants, le groupe Γ de rang 4 est dense dans $(\mathbb{R}_+^\times)^2$.

Pour $l = 5$, on voit en utilisant le lemme topologique 2.9 de D. Roy que si les dix nombres α_j, β_j sont multiplicativement indépendants, le groupe Γ contient un sous-groupe de rang 3 dense dans $(\mathbb{R}_+^\times)^2$.

Exemple 2.10. Prenons le corps quadratique $\mathbb{Q}(\sqrt{2})$, et choisissons l éléments $\gamma_1, \dots, \gamma_l$ dans ce corps tels que, si γ_j^σ désigne le conjugué de γ_j (avec $\sqrt{2}^\sigma = -\sqrt{2}$), les $2l$ nombres γ_j et γ_j^σ, où $1 \leq j \leq l$, soient multiplicativement indépendants. On prend aussi $\gamma_1 > 0$, $\gamma_1^\sigma < 0$, $\gamma_2 < 0$ et $\gamma_2^\sigma < 0$ de telle sorte que les couples (γ, γ^σ), pour $\gamma \in \{\gamma_1, \gamma_2, \gamma_1^2, \gamma_1\gamma_2\}$, soient dans chacune des quatre composantes connexes de $(\mathbb{R}^\times)^2$. Par exemple on peut prendre

$$\begin{aligned} \gamma_1 &= 2\sqrt{2} - 1, & \gamma_2 &= -3\sqrt{2} - 1, \\ \gamma_3 &= 4\sqrt{2} - 1, & \gamma_4 &= 6\sqrt{2} - 1, \\ \gamma_5 &= 7\sqrt{2} - 1. \end{aligned}$$

Du théorème des six exponentielles, on déduit que le sous-groupe de $(\mathbb{R}^\times)^2$, de rang 4, engendré par les images des nombres $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ via le plongement canonique du corps quadratique réel $\mathbb{Q}(\sqrt{2})$ est dense dans $(\mathbb{R}^\times)^2$. De plus le sous-groupe de $\mathbb{Q}(\sqrt{2})^\times$ engendré par les 5 nombres $\gamma_1, \dots, \gamma_5$ contient un sous-groupe de rang 3 dont l'image par le plongement canonique est dense dans $(\mathbb{R}^\times)^2$. Cependant la démonstration de Roy ne permet pas de préciser ce sous-groupe de rang 3 ; si la conjecture des quatre exponentielles est vraie, le sous-groupe de rang 3 engendré par $\gamma_1, \gamma_2, \gamma_3$ a une image dense.

2. Densité de sous-groupes de type fini de $\mathbb{C}^\times$

Soient $\gamma_1, \dots, \gamma_l$ des nombres complexes non nuls multiplicativement indépendants ; le théorème de Kronecker montre que le sous-groupe Γ de $\mathbb{C}^\times$ engendré par $\gamma_1, \dots, \gamma_l$ est dense si et seulement si, pour tout $s \in \mathbb{Z}^{l+1} \setminus \{0\}$, la matrice à trois lignes et $l+1$ colonnes

$$\begin{pmatrix} 0 & \log|\gamma_1| & \cdots & \log|\gamma_l| \\ 2i\pi & \log(\gamma_1/\bar{\gamma}_1) & \cdots & \log(\gamma_l/\bar{\gamma}_l) \\ s_0 & s_1 & \cdots & s_l \end{pmatrix}$$

est de rang 3 ; cette condition ne dépend évidemment pas du choix des logarithmes complexes

$$\log(\gamma_j/\bar{\gamma}_j).$$

Une première condition nécessaire pour que Γ soit dense dans $\mathbb{C}^\times$ est que deux au moins des l nombres réels $|\gamma_1|, \dots, |\gamma_l|$ soient multiplicativement indépendants : cela signifie que l' image de Γ par la surjection $z \mapsto |z|$ est dense dans $\mathbb{R}_+^\times$. Une deuxième condition nécessaire est que l'un au moins des l nombres $\gamma_j/|\gamma_j|$, où $1 \leq j \leq l$, ne soit pas racine de l'unité : cela revient à dire que Γ a une image dense dans $\mathbb{R}/\mathbb{Z}$ par la projection que l'on déduit de l'isomorphisme entre $\mathbb{C}^\times$ et $\mathbb{R} \times (\mathbb{R}/\mathbb{Z})$.

Supposons maintenant que les l nombres complexes γ_j sont algébriques.

(a) Si on admet la conjecture des quatre exponentielles, alors ces conditions sont aussi suffisantes pour que Γ soit dense dans $\mathbb{C}^\times$.

(b) Supposons que trois au moins des nombres $|\gamma_1|, \dots, |\gamma_l|$ sont multiplicativement indépendants ; on déduit alors du théorème des six exponentielles que Γ est dense dans $\mathbb{C}^\times$. Enfin, si quatre au moins des nombres $|\gamma_1|, \dots, |\gamma_l|$ sont multiplicativement indépendants, et si deux au moins des nombres $\gamma_j/|\gamma_j|$, où $1 \leq j \leq l$, sont multiplicativement indépendants, alors tout sous-groupe de Γ de rang $l-1$ est dense dans $\mathbb{C}^\times$, et par conséquent Γ contient un sous-groupe de rang 2 dense dans $\mathbb{C}^\times$.

Exemple 2.11. Considérons le corps $\mathbb{Q}(i)$, et choisissons dans $\mathbb{Q}(i)^\times$ des éléments $\gamma_1, \dots, \gamma_l$ tels que les $2l$ nombres complexes γ_j et $\bar{\gamma}_j$ soient multiplicativement indépendants (pour simplifier) ; par exemple

$$\gamma_1 = 2+i, \quad \gamma_2 = 2+3i, \quad \gamma_3 = 4+i, \quad \gamma_4 = 5+2i.$$

Le sous-groupe de $\mathbb{C}^\times$, de rang 3, engendré par $\gamma_1, \gamma_2, \gamma_3$ est dense dans $\mathbb{C}^\times$, et le sous-groupe de

$\mathbb{Q}(i)^\times$, de rang 4, engendré par $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ contient un sous-groupe de rang 2 dense dans $\mathbb{C}^\times$. Si la conjecture des quatre exponentielles est vraie, alors le sous-groupe de rang 2 engendré par γ_1, γ_2 est dense dans $\mathbb{C}^\times$; pour le démontrer inconditionnellement, il faudrait prouver que pour tout $(\lambda, \mu) \in \mathbb{Q}^2$, le déterminant

$$\det\begin{pmatrix} \log|\gamma_1| & \log|\gamma_2| \\ \log(\gamma_1/\bar\gamma_1) + 2\lambda i\pi & \log(\gamma_2/\bar\gamma_2) + 2\mu i\pi \end{pmatrix}$$

n'est pas nul.

3. LE THÉORÈME PRINCIPAL

3a. Plongement réel d'un sous-groupe de type fini

Soit K un corps de nombres plongé dans $\mathbb{R}$, soit G un groupe algébrique commutatif défini sur K et soit Γ un sous-groupe de type fini de $G(K)$; on demande à quelle condition l'image de Γ dans $G(\mathbb{R})$ est dense (pour la topologie réelle) dans la composante neutre de l'origine. Il est évidemment nécessaire (comme dans la conjecture de Mazur) de supposer que Γ est Zariski-dense dans G ; comme l'adhérence de Zariski d'un sous-groupe de $G(K)$ est un sous-groupe algébrique de G défini sur K, la condition de densité pour la topologie de Zariski se traduit ainsi : *pour tout sous-groupe algébrique G' de G défini sur K avec* $\dim G' < \dim G$, *le sous-groupe* $\Gamma/\Gamma \cap G'(K)$ *a un rang* ≥ 1.

Cette condition n'est pas suffisante en général : si l'image de Γ dans $G(\mathbb{R})$ est dense, pour tout sous-groupe algébrique G' de G défini sur K, avec $G' \neq G$, l'image de Γ dans le quotient $G(\mathbb{R})/G'(\mathbb{R})$ est encore dense ; cela impose une contrainte sur le rang de $\Gamma/\Gamma \cap G'(K)$ que nous allons expliciter. Nous verrons ensuite que cette contrainte n'est pas encore suffisante ; cela nous conduira à justifier la définition de la propriété de densité.

Nous expliciterons enfin les liens entre la propriété de densité pour les groupes linéaires déployés d'une part et la conjecture d'indépendance algébrique homogène de logarithmes de nombres algébriques d'autre part.

Rappelons la notation $m_\mathbb{R}(G)$ qui a été introduite dans le premier paragraphe. La contrainte dont nous venons de parler s'écrit :

Lemme 3.1. *Soient K un sous-corps de $\mathbb{R}$, G un groupe algébrique commutatif défini sur K de dimension ≥ 1, Γ un sous-groupe de type fini de $G(K)$. Supposons que l'adhérence réelle de Γ dans $G(\mathbb{R})$ contienne la composante neutre $G(\mathbb{R})^0$. On a alors, pour tout sous-groupe algébrique G' de G défini sur K,*

$$\operatorname{rang}_\mathbb{Z}\bigl(\Gamma/\Gamma \cap G'(K)\bigr) \geq m_\mathbb{R}(G/G').$$

Dans le cas $G = \mathbb{G}_\mathrm{a}^d$, le théorème de Kronecker montre que la réciproque est vraie. Dans le cas général, en supposant que K est un corps de nombres, une réciproque partielle peut-être obtenue en remplaçant $m_\mathbb{R}(G)$ par un nombre $m'_\mathbb{R}(G)$ (qui, pour un groupe différent de $\mathbb{G}_\mathrm{a}^d$, est au moins égal à $m_\mathbb{R}(G)$), défini par $m'_\mathbb{R}(G) = \alpha(G)(d-1) + 2$ si $\kappa_\mathbb{R}(G) = 0$ et

$$m'_\mathbb{R}(G) = \bigl(\alpha(G) - \kappa_\mathbb{R}(G) + 1\bigr)(d-1) + 2 - \kappa_\mathbb{R}(G)$$

si $\kappa_\mathbb{R}(G) \geq 1$. Ainsi on a toujours

$$m'_\mathbb{R}(G) \leq \alpha(G)(d-1) + 2\,;$$

de plus, $m'_\mathbb{R}(G) = d^2 - d + 1$ si G est une variété abélienne.

3b. Le théorème principal : énoncé et démonstration

Théorème 3.2. *Soit G un groupe algébrique commutatif de dimension d défini sur un corps de nombres réel K. Soit Γ un sous-groupe de type fini de $G(K)$.*

a) *On suppose, pour tout sous-groupe algébrique G' de G défini sur K avec $\dim G' < \dim G$, qu'on a $\operatorname{rang}_\mathbb{Z}\bigl(\Gamma/\Gamma \cap G'(K)\bigr) \geq m'_\mathbb{R}(G/G')$. Alors l'adhérence de Γ dans le groupe topologique $G(\mathbb{R})$ contient la composante neutre $G(\mathbb{R})^0$.*
b) *On suppose, pour tout sous-groupe algébrique G' de G défini sur K avec $\dim G' < \dim G$,*

$$\operatorname{rang}_\mathbb{Z}\bigl(\Gamma/\Gamma \cap G'(K)\bigr) \geq m'_\mathbb{R}(G/G') + d - 1.$$

Alors Γ contient un sous-groupe de rang $m_\mathbb{R}(G)$ dense (pour la topologie réelle) dans $G(\mathbb{R})^0$.

Démonstration. Soient G un groupe algébrique commutatif défini sur un corps de nombres réels K et Γ un sous-groupe de type fini de $G(K)$ et de rang l ; on définit

$$Y = \big(\exp_G^{-1}(\Gamma)\big) \cap T_G(\mathbb{R})\,;$$

c'est un sous-groupe de type fini de $T_G(\mathbb{R})$ de rang $l + \kappa_{\mathbb{R}}(G)$, dont l'image par $\exp_G$ est $\Gamma \cap G(\mathbb{R})^0$. Dire que $\Gamma \cap G(\mathbb{R})^0$ est dense dans $G(\mathbb{R})^0$ équivaut à dire que Y est dense dans $T_G(\mathbb{R})$, donc que pour tout hyperplan réel V de $T_G(\mathbb{R})$,

$$\operatorname{rang}_{\mathbb{Z}}\big(Y/Y \cap V\big) \geq 2.$$

Comme Y contient $\Omega_G \cap T_G(\mathbb{R})$, cette inégalité est banale si on a déjà

$$\operatorname{rang}_{\mathbb{Z}}\big(\Omega_G \cap T_G(\mathbb{R})/\Omega_G \cap V\big) \geq 2\,;$$

par conséquent il n'y a pas de restriction à supposer

$$\operatorname{rang}_{\mathbb{Z}}(\Omega_G \cap V) \geq \max\big\{\kappa_{\mathbb{R}}(G) - 1,\, 0\big\}.$$

On commence par établir le résultat suivant :

Lemme 3.3. *Supposons $l \geq m'_{\mathbb{R}}(G)$; supposons aussi que V ne contient pas de sous-espace vectoriel de $T_G(\mathbb{R})$ de la forme $T_{G'}(\mathbb{R})$, avec G' sous-groupe algébrique de G de dimension ≥ 1 défini sur K ; alors l'inégalité désirée $\operatorname{rang}_{\mathbb{Z}}\big(Y/Y \cap V\big) \geq 2$ est bien vérifiée.*

Démonstration. On utilise le théorème 2.5 du sous-groupe algébrique ; on écrit une équation de l'hyperplan réel V dans $T_G(\mathbb{R})$ et on considère l'hyperplan complexe $\mathcal{V}$ de $T_G(\mathbb{C})$ défini par la même équation, de sorte que $V = \mathcal{V} \cap T_G(\mathbb{R})$. Si G' est un sous-groupe algébrique de G défini sur K de dimension ≥ 1, $T_{G'}(\mathbb{C})$ est un sous-espace vectoriel de $T_G(\mathbb{C})$ qui s'écrit comme intersection d'hyperplans définis sur K, donc sur $\mathbb{R}$, et

$$T_{G'}(\mathbb{R}) = T_{G'}(\mathbb{C}) \cap T_G(\mathbb{R})\,;$$

l'hypothèse que V ne contient pas $T_{G'}(\mathbb{R})$ implique que $\mathcal{V}$ ne contient pas non plus $T_{G'}(\mathbb{C})$. Comme $\mathcal{V} \cap \Omega_G$ contient $V \cap \Omega_G$, on a

$$\operatorname{rang}_{\mathbb{Z}}(\mathcal{V} \cap \Omega_G) \geq \max\{\kappa_{\mathbb{R}}(G) - 1,\, 0\}.$$

Enfin, puisque $Y \cap V$ est contenu dans $\mathcal{L}_K(G) \cap \mathcal{V}$, on peut conclure

$$\operatorname{rang}_{\mathbb{Z}}(Y \cap V) \leq \big(\alpha(G) - \max\{\kappa_{\mathbb{R}}(G) - 1,\, 0\}\big)(d-1).$$

Le lemme maintenant résulte de la définition de $m'_{\mathbb{R}}(G)$. □

On ne fait plus d'hypothèse sur l'hyperplan réel V, mais on suppose

$$\operatorname{rang}_{\mathbb{Z}}\big(\Gamma/\Gamma \cap G'(K)\big) \geq m'_{\mathbb{R}}(G/G')$$

pour tout sous-groupe algébrique G' de G défini sur K avec $\dim G' < \dim G$. On prend pour G' le plus grand sous-groupe algébrique connexe de G, défini sur K, tel que $T_{G'}(\mathbb{R})$ soit contenu dans V et on applique le lemme 3.3 au sous-groupe de $T_{G/G'}(\mathbb{R})$ donné par $Y/Y \cap T_{G'}(\mathbb{R})$, dont l'image par $\exp_{G/G'}$ dans $(G/G')(\mathbb{R})$ est $\Gamma/\Gamma \cap G'(K)$:

$$\begin{array}{ccccc}
Y \subset T_G(\mathbb{R}) & \xrightarrow{\exp_G} & G(\mathbb{R}) & \supset G(K) \supset \Gamma & \\
\downarrow & & \downarrow & & \\
T_{G/G'}(\mathbb{R}) & \xrightarrow{\exp_{G/G'}} & (G/G')(\mathbb{R}) & \supset (G/G')(K) & \\
\cup & & & \cup & \\
Y/Y \cap T_{G'}(\mathbb{R}) & & \xrightarrow{\exp_{G/G'}} & \Gamma/\Gamma \cap G'(K). &
\end{array}$$

La deuxième partie du théorème principal résulte maintenant de la première partie et du lemme topologique 2.9 de D. Roy, avec $E = T_G(\mathbb{R})$ et $Y_0 = \Omega_G \cap T_G(\mathbb{R})$. □

3c. Motivations pour la propriété de densité

Le théorème principal pourrait laisser penser que la réciproque du lemme 3.1 est vraie ; en fait, cela voudrait dire qu'un sous-groupe de type fini de $G(K)$ (où G est un groupe algébrique commutatif sur un corps de nombres réel K), de rang $\geq m_{\mathbb{R}}(G)$, dont la projection sur tout quotient $(G/G')(K)$ (avec G' sous-groupe algébrique de G défini sur K, de dimension positive et $< \dim G$) a une image dense dans $(G/G')(\mathbb{R})^0$, est alors dense dans $G(\mathbb{R})^0$.

Nous allons donner un contre-exemple pour un tore ; la construction est inspirée par une remarque de M. Langevin (voir [Waldschmidt 1987, p. 1014], ainsi que [Roy 1992a, théorème 6]), concernant les matrices antisymétriques

$$\begin{pmatrix} 0 & -\log\alpha_3 & \log\alpha_2 \\ \log\alpha_3 & 0 & -\log\alpha_1 \\ -\log\alpha_2 & \log\alpha_1 & 0 \end{pmatrix}.$$

En supposant que les trois nombres $\log\alpha_1$, $\log\alpha_2$, $\log\alpha_3$ sont linéairement indépendants sur $\mathbb{Q}$, on vérifie que si Y désigne le sous-$\mathbb{Z}$-module engendré par les trois vecteurs colonnes de cette matrice dans $\mathbb{C}^3$, pour tout sous-espace $\mathcal{V}$ de $\mathbb{C}^3$ rationnel sur $\mathbb{Q}$ et distinct de $\{0\}$ et de $\mathbb{C}^3$,

$$\operatorname{rang}_{\mathbb{Z}}\big(\mathcal{V}\cap Y\big) = \dim_{\mathbb{C}}\mathcal{V} - 1.$$

Le fait que le rang de la matrice soit seulement 2 est dû à des raisons “structurelles” indépendantes du fait que les α_j peuvent être algébriques ; il ne se voit pas en regardant les sous-groupes algébriques de $\mathbb{G}_{\mathrm{m}}^3$ et les images par l'exponentielle des vecteurs colonnes ; il se voit en regardant les sous-groupes algébriques de $\mathbb{G}_{\mathrm{m}}^9$ et l'image par l'exponentielle du point correspondant aux 9 coefficients de la matrice.

Prenons $2d$ nombres réels positifs multiplicativement indépendants $\alpha_1,\dots,\alpha_d$ et $\beta_1,\dots,\beta_d$, avec $d\ge 3$; par exemple, on peut les prendre algébriques. Considérons le sous-groupe Γ de $(\mathbb{R}_+^\times)^d$ engendré par les $\frac12 d(d-1)+1$ points

$$\begin{aligned}\gamma_{ij} &= \big(\alpha_j^{\delta_{hi}}\alpha_i^{-\delta_{hj}}\big)_{1\le h\le d}\\ &= (1,\dots,1,\alpha_j,1,\dots,1,\alpha_i^{-1},1,\dots,1),\end{aligned}$$

où $1\le i<j\le d$, et

$$\gamma_0 = (\beta_1,\dots,\beta_d).$$

On peut écrire $\Gamma=\exp(Y)$, où $\exp(x_1,\dots,x_d) = \big(e^{x_1},\dots,e^{x_d}\big)$, tandis que

$$Y = \sum_{1\le i<j\le d}\mathbb{Z}y_{ij} + \mathbb{Z}y_0$$

est le sous-groupe de $\mathbb{R}^d$ engendré par

$$y_{ij} = \big(\delta_{hi}\log\alpha_j - \delta_{hj}\log\alpha_i\big)_{1\le h\le d},$$

où $1\le i<j\le d$, et

$$y_0 = (\log\beta_1,\,\dots,\,\log\beta_d).$$

Si H est l'hyperplan de $\mathbb{R}^d$ defini par $x_1\log\alpha_1+\dots+x_d\log\alpha_d=0$, une base de $\mathcal{L}^d\cap H$ sur $\mathbb{Q}$ est précisément $\{y_{ij}\}$, où $1\le i<j\le d$. On a

$$\operatorname{rang}_{\mathbb{Z}}\Gamma = \operatorname{rang}_{\mathbb{Z}} Y = \tfrac12 d(d-1)+1 \ge d+1\,;$$

pourtant, comme la forme linéaire $(x_1,\dots,x_d)\mapsto x_1\log\alpha_1+\dots+x_d\log\alpha_d$ sur $\mathbb{R}^d$ envoie Y sur un sous-groupe de rang ≤ 1, Y n'est pas dense dans $\mathbb{R}^d$, d'où il résulte que l'adhérence réelle de Γ dans $G(\mathbb{R})=(\mathbb{R}^*)^d$ ne contient pas $G(\mathbb{R})^0=(\mathbb{R}_+^\times)^d$.

Soit maintenant G' un sous-groupe algébrique de $\mathbb{G}_{\mathrm{m}}^d$ de codimension $\delta>0$; on va montrer

$$\operatorname{rang}_{\mathbb{Z}}(\Gamma/\Gamma\cap G') \ge m_{\mathbb{R}}(G/G'),$$

c'est-à-dire

$$\operatorname{rang}_{\mathbb{Z}}\big(Y/Y\cap T_{G'}(\mathbb{R})\big) \ge \delta+1.$$

Quitte à appliquer à G un automorphisme, ce qui a pour effet de remplacer $\alpha_1,\dots,\alpha_d$ par une autre base du sous-groupe de $\mathbb{R}_+^\times$ qu'ils engendrent et de même pour $\beta_1,\dots,\beta_d$, on peut supposer que $T_{G'}(\mathbb{R})$ est défini par $x_1=\dots=x_\delta=0$ (l'utilisation des automorphismes de G, suggérée par D. Roy, simplifie la démonstration).

Quand s_{ij}, où $1\le i<j\le d$, sont des entiers rationnels, pour que $\sum_{1\le i<j\le d}s_{ij}y_{ij}$ appartienne à $T_{G'}(\mathbb{R})$, il faut et il suffit que les $d\delta-\frac12\delta(\delta+1)$ conditions linéaires indépendantes $s_{ij}=0$, pour $1\le i<j\le\delta$ et pour $1\le i\le\delta<j\le d$, soient satisfaites. On en déduit

$$\operatorname{rang}_{\mathbb{Z}}\big(\Gamma/\Gamma\cap G'(\mathbb{R})\big) = \delta d+1-\tfrac12\delta(\delta+1).$$

Pour $d\ge 3$ et $1\le\delta\le d$, on a $\delta d\ge\delta+\frac12\delta(\delta+1)$, donc

$$\delta d+1-\tfrac12\delta(\delta+1) \ge \delta+1 = m_{\mathbb{R}}(G/G').$$

Par conséquent la réciproque du lemme 3.1 n'est pas vraie. En prenant un sous-groupe algébrique de dimension maximale G' de G, $\dim G'<\dim G$, tel que $\tilde\Gamma=\Gamma/\Gamma\cap G'(\mathbb{R})$ ne soit pas dense dans

$\widetilde{G}(\mathbb{R})$, où $\widetilde{G}$ désigne le quotient G/G', on obtient le contre-exemple annoncé : $\mathrm{rang}_{\mathbb{Z}}(\widetilde{\Gamma}) \geq m_{\mathbb{R}}(\widetilde{G})$, et les projections de $\widetilde{\Gamma}$ sur les quotients de $\widetilde{G}$ (distincts de $\{0\}$ et de $\widetilde{G}$) sont denses dans les points réels.

Étant donné que, pour $1 \leq \delta \leq d$, on a

$$\delta d - \tfrac{1}{2}\delta(\delta+1) \geq \tfrac{1}{2}\delta(\delta-1),$$

le groupe Γ que nous venons de construire satisfait

$$\mathrm{rang}_{\mathbb{Z}}\big(\Gamma/\Gamma\cap G'(\mathbb{R})\big) \geq \tfrac{1}{2}\delta(\delta-1)+1\,;$$

le théorème 2.6, du sous-groupe linéaire, montre qu'il n'y a pas d'exemple où le coefficient $\frac{1}{2}$ soit remplacé par 1 : si un sous-groupe Γ de $\big(\bar{\mathbb{Q}}\cap\mathbb{R}_+^\times\big)^d$ vérifie

$$\mathrm{rang}_{\mathbb{Z}}\big(\Gamma/\Gamma\cap G'(\mathbb{R})\big) \geq \delta(\delta-1)+1$$

pour tout G' sous-groupe algébrique de $\mathbb{G}_{\mathrm{m}}^d$ de codimension $\delta \geq 1$, alors Γ est dense dans $(\mathbb{R}_+^\times)^d$. D'après [Roy 1990a, p. 278, corollaire 2], la conjecture d'indépendance algébrique réelle entraîne la même conclusion sous l'hypothèse

$$\mathrm{rang}_{\mathbb{Z}}\big(\Gamma/\Gamma\cap G'(\mathbb{R})\big) > \tfrac{1}{2}\big(\delta(\delta-1)+2\big).$$

Quand elle est vérifiée pour un groupe algébrique G commutatif défini sur un corps de nombres réel K, la propriété de densité (définition 1.2) donne description des sous-groupes de type fini Γ de $G(K)$ qui sont denses dans $G(\mathbb{R})$. Nous nous sommes inspiré du point de vue de [Roy 1989] et de son critère d'indépendance algébrique. Pour un tore $\mathbb{G}_{\mathrm{m}}^d$, on choisit une base $\gamma_1,\ldots,\gamma_l$ sur $\mathbb{Z}$ de $\Gamma\cap(\mathbb{R}_+^\times)^d$ (prendre un sous-groupe d'indice fini ne change rien) ; on écrit les dl nombres algébriques γ_{ij} sur une base du $\mathbb{Z}$-module (sous-groupe multiplicatif de $\mathbb{R}_+^\times$) qu'ils engendrent et on remplace les éléments de la base par des indéterminées, ce qui donne un sous-groupe "générique" de $(\mathbb{R}_+^\times)^d$ associé à Γ ; la condition cherchée est que ce sous-groupe générique soit dense.

Quand on veut adapter ce raisonnement à un groupe algébrique commutatif non linéaire, on modifie légèrement la présentation de cet argument : considérer le sous-groupe multiplicatif de $\mathbb{R}_+^\times$ engendré par les dl nombres γ_{ij} revient à prendre le sous-groupe de $(\mathbb{R}_+^\times)^{dl}$ engendré par le point $(\gamma_1, \ldots,\gamma_l)$ [Waldschmidt 1983b, § 3e].

Explicitons la situation dans le cas d'un groupe linéaire déployé $\mathbb{G}_{\mathrm{a}}^{d_0}\times\mathbb{G}_{\mathrm{m}}^{d_1}$.

Soient l, d_0 et d_1 des entiers ≥ 0 avec $l>0$ et $d=d_0+d_1>0$. Soient aussi α_{ij} et β_{hj}, où $1\leq h\leq d_0$, $1\leq i\leq d_1$ et $1\leq j\leq l$, des nombres algébriques réels avec $\alpha_{ij}>0$ pour tout (i,j). On définit $\gamma_1,\ldots,\gamma_l$ dans $(\bar{\mathbb{Q}}\cap\mathbb{R})^{d_0}\times(\bar{\mathbb{Q}}^\times\cap\mathbb{R}_+^\times)^d$ par

$$\gamma_j = (\beta_{1j},\ldots,\beta_{d_0j};\alpha_{1j},\ldots,\alpha_{d_1j}),$$

où $1\leq j\leq l$, et on note Γ le sous-groupe de $\mathbb{R}^{d_0}\times(\mathbb{R}_+^\times)^{d_1}$ qu'ils engendrent :

$$\Gamma = \big\{(s_1\beta_{h1}+\cdots+s_l\beta_{hl}\,;\,\alpha_{i1}^{s_1}\cdots\alpha_{il}^{s_l})_{1\leq h\leq d_0;1\leq i\leq d_1}\,;\; s=(s_1,\ldots,s_l)\in\mathbb{Z}^l\big\}.$$

On choisit une base $(\theta_1,\ldots,\theta_r)$ dans $\bar{\mathbb{Q}}^\times\cap\mathbb{R}_+^\times$ du sous-groupe multiplicatif engendré par les d_1l nombres α_{ij} et on écrit

$$\alpha_{ij} = \prod_{\rho=1}^{r}\theta_\rho^{b_{ij\rho}},$$

où $1\leq i\leq d_1$, $1\leq j\leq l$, et les $b_{ij\rho}$ sont des entiers.

Passons aux logarithmes : on définit encore un sous-groupe $Y=\mathbb{Z}y_1+\cdots+\mathbb{Z}y_l$ de $\mathbb{R}^d$ par

$$y_j = (\beta_{1j},\ldots,\beta_{d_0j};\log\alpha_{1j},\,\ldots,\,\log\alpha_{d_1j}),$$

où $1\leq j\leq l$.

Lemme 3.4. *Si la conjecture 2.2 sur l'indépendance algébrique homogène réelle de logarithmes est vraie, les conditions suivantes sont équivalentes :*

(i) *le sous-groupe Γ est dense dans $\mathbb{R}^{d_0}\times(\mathbb{R}_+^\times)^{d_1}$;*
(ii) *le sous-groupe Y est dense dans $\mathbb{R}^d$;*
(iii) *il existe $(x_1,\ldots,x_r)$ dans $(\mathbb{R}_+^\times)^r$ tel que le sous-groupe de $\mathbb{R}^{d_0}\times(\mathbb{R}_+^\times)^{d_1}$ engendré par $\eta_1,\ldots,\eta_l$, avec*

$$\eta_j = \Big(\beta_{1j},\ldots,\beta_{d_0j};\prod_{\rho=1}^{r}x_\rho^{b_{1j\rho}},\ldots,\prod_{\rho=1}^{r}x_\rho^{b_{d_1j\rho}}\Big)$$

où $1\leq j\leq l$, soit dense dans $\mathbb{R}^{d_0}\times(\mathbb{R}_+^\times)^{d_1}$;

(iv) *il existe* $(\xi_1,\ldots,\xi_r)$ *dans* $\mathbb{R}^r$ *tel que le sous-groupe de* $\mathbb{R}^d$ *engendré par*

$$\left(\beta_{1j},\ldots,\beta_{d_0j};\sum_{\rho=1}^r b_{1j\rho}\xi_\rho,\ldots,\sum_{\rho=1}^r b_{d_1j\rho}\xi_\rho\right)$$

où $1\le j\le l$, *soit dense dans* $\mathbb{R}^d$.

Démonstration. L'équivalence entre (i) et (ii) d'une part, (iii) et (iv) d'autre part, provient du fait que l'application exponentielle attachée au groupe algébrique $\mathbb{G}_\mathrm{a}^{d_0}\times\mathbb{G}_\mathrm{m}^{d_1}$ sur $\mathbb{R}$:

$$(u_1,\ldots,u_{d_0};v_1,\ldots,v_{d_1})\mapsto(u_1,\ldots,u_{d_0};e^{v_1},\ldots,e^{v_{d_1}})$$

établit un isomorphisme de groupes topologiques entre $\mathbb{R}^d$ et $\mathbb{R}^{d_0}\times(\mathbb{R}_+^\times)^{d_1}$. Les implications (i) $\Rightarrow$ (iii) et (ii) $\Rightarrow$ (iv) sont banales : la première se prouve en prenant $x_\varrho=\theta_\varrho$ pour $1\le\varrho\le r$, la deuxième en prenant $\xi_\varrho=\log\theta_\varrho$. C'est seulement pour établir l'implication (iv) $\Rightarrow$ (ii) que la conjecture d'indépendance algébrique homogène réelle va être utile.

Supposons que le sous-groupe Y de $\mathbb{R}^d$ n'est pas dense : il existe une forme linéaire non nulle $\varphi:\mathbb{R}^d\to\mathbb{R}$ telle que $\varphi(Y)\subset\mathbb{Z}$. On choisit une base $z_1,\ldots,z_s$ de $Y\cap\ker\varphi$:

$$z_\sigma=(z_{\sigma1},\cdots,z_{\sigma d})=\sum_{j=1}^l s_j^{(\sigma)}y_j$$

où $1\le\sigma\le s$, avec des $s_j^{(\sigma)}$ dans $\mathbb{Z}$. Comme $\varphi(z_\sigma)=0$, la matrice

$$(z_{\sigma i})_{1\le\sigma\le s;1\le i\le d}$$

a un rang $<d$. On écrit les coefficients de cette matrice : pour $1\le\sigma\le s$ et $1\le i\le d$,

$$z_{\sigma i}=\begin{cases}\sum_{j=1}^l s_j^{(\sigma)}\beta_{ij} & \text{pour } 1\le i\le d_0,\\ \sum_{j=1}^l s_j^{(\sigma)}\sum_{\varrho=1}^r b_{i-d_0,j,\varrho}\log\theta_\varrho & \text{pour } d_0<i\le d.\end{cases}$$

Etant donné que les nombres $\log\theta_1,\ldots,\log\theta_r$ ne vérifient pas de relation algébrique homogène non triviale (grâce à la conjecture que l'on admet), si $\xi_1,\ldots,\xi_r$ sont des nombres réels et si on pose

$$\zeta_{\sigma i}=\begin{cases}\sum_{j=1}^l s_j^{(\sigma)}\beta_{ij} & \text{pour } 1\le i\le d_0,\\ \sum_{j=1}^l s_j^{(\sigma)}\sum_{\varrho=1}^r b_{i-d_0,j,\varrho}\xi_\varrho & \text{pour } d_0<i\le d,\end{cases}$$

la matrice $(\zeta_{\sigma i})_{1\le\sigma\le s;1\le i\le d}$ a encore un rang $<d$. En renversant l'argument, on déduit que le sous-groupe de $\mathbb{R}^d$ engendré par

$$\left(\beta_{1j},\ldots,\beta_{d_0j};\sum_{\rho=1}^r b_{1j\rho}\xi_\rho,\cdots,\sum_{\rho=1}^r b_{d_1j\rho}\xi_\rho\right),$$

où $1\le j\le l$, n'est pas dense et l'assertion (iv) n'est pas satisfaite. $\square$

Le lemme 3.4 montre que la propriété de densité pour les groupes $\mathbb{G}_\mathrm{a}^{d_0}\times\mathbb{G}_\mathrm{m}^{d_1}$ résulte de la conjecture d'indépendance algébrique homogène réelle : l'adhérence de Zariski H du sous-groupe de

$$(\mathbb{G}_\mathrm{a}^{d_0}\times\mathbb{G}_\mathrm{m}^{d_1})^l$$

engendré par le point $(\gamma_1,\ldots,\gamma_l)$ vérifie

$$H(\mathbb{R})\supset\left\{\left(x_0\beta_{hj};\prod_{\rho=1}^r x_\rho^{b_{ij\rho}}\right)_{1\le h\le d_0,1\le i\le d_1,1\le j\le l};\ (x_0;x_1,\ldots,x_r)\in\mathbb{R}\times(\mathbb{R}^\times)^r\right\}\subset\mathbb{R}^{d_0l}\times(\mathbb{R}^\times)^{d_1l},$$

et la composante connexe de l'origine de $H(\mathbb{R})$ est

$$H(\mathbb{R})^0=\left\{\left(x_0\beta_{hj};\prod_{\rho=1}^r x_\rho^{b_{ij\rho}}\right)_{1\le h\le d_0,1\le i\le d_1,1\le j\le l};\ (x_0;x_1,\ldots,x_r)\in\mathbb{R}\times(\mathbb{R}_+^\times)^r\right\}\subset\mathbb{R}^{d_0l}\times(\mathbb{R}_+^\times)^{d_1l}.$$

On peut aussi procéder dans l'autre sens et déduire la conjecture d'indépendance algébrique homogène réelle du cas particulier de la propriété de densité pour les groupes $\mathbb{G}_\mathrm{m}^d$.

Lemme 3.5. *On suppose que les groupes algébriques* $\mathbb{G}_\mathrm{m}^d$, *où* $d\ge1$, *possèdent la propriété de densité.*

Alors la conjecture 2.2 *d'indépendance algébrique homogène réelle est vraie.*

Démonstration. On suppose que la conjecture d'indépendance algébrique homogène réelle n'est pas vraie ; en utilisant le critère d'indépendance algébrique de D. Roy (proposition 2.4), on voit qu'il y a des nombres algébriques réels positifs multiplicativement indépendants $\theta_1, \ldots, \theta_r$ et des rationnels $b_{ij\varrho} \in \mathbb{Q}$, où $1 \le i \le d$, $1 \le j \le l$, $1 \le \varrho \le r$, tels que la matrice

$$\left(\sum_{\varrho=1}^{r} b_{ij\varrho} \log \theta_\varrho \right)_{1 \le i \le d; 1 \le j \le l}$$

soit de rang $< d$ et la matrice

$$\left(\sum_{\varrho=1}^{r} b_{ij\varrho} X_\varrho \right)_{1 \le i \le d; 1 \le j \le l}$$

soit de rang d. On choisit des nombres algébriques réels positifs $\alpha_1, \ldots, \alpha_d$ tels que les $d + r$ nombres $\alpha_1, \ldots, \alpha_d$, $\theta_1, \ldots, \theta_r$ soient multiplicativement indépendants et on définit des éléments de $(\bar{\mathbb{Q}}^\times \cap \mathbb{R}_+^\times)^d$ par $\gamma_0 = (\alpha_1, \ldots, \alpha_d)$ et

$$\gamma_j = \left(\prod_{\varrho=1}^{r} \theta_\varrho^{b_{ij\varrho}} \right)_{1 \le i \le d}$$

pour $1 \le j \le l$. Le sous-groupe de $(\mathbb{R}_+^\times)^d$ engendré par $\gamma_0, \ldots, \gamma_l$ n'est pas dense, mais si $x_1, \ldots, x_r$, $\xi_1, \ldots, \xi_\varrho$ sont des nombres réels positifs dont les logarithmes sont algébriquement indépendants, le sous-groupe engendré par $\eta_0, \eta_1, \ldots, \eta_l$, avec $\eta_0 = (\xi_1, \ldots, \xi_d)$ et

$$\eta_j = \left(\prod_{\varrho=1}^{r} x_\varrho^{b_{ij\varrho}} \right)_{1 \le i \le d}$$

pour $1 \le j \le l$, est dense dans $(\mathbb{R}_+^\times)^d$. $\square$

Noter qu'en combinant les lemmes 3.4 et 3.5, on constate qu'il suffit de connaître la propriété de densité pour les tores déployés $\mathbb{G}_{\mathrm{m}}^d$ si on la veut pour les groupes linéaires $\mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}$. Ainsi la situation conjecturale contraste avec ce que l'on sait démontrer : dans le théorème principal, les facteurs unipotents recèlent des informations non redondantes (voir la section 4b).

4. CONSÉQUENCES

Nous donnons plusieurs conséquences d'une part du théorème principal énoncé au paragraphe 3, et d'autre part de la propriété de densité du paragraphe 1. Nous étudions dans cette section le problème de densité dans le cas réel pour des variétés abéliennes simples, puis pour des groupes linéaires ; nous considérons aussi les extensions d'une courbe elliptique par un groupe multiplicatif. Dans la section suivante nous considérerons le problème complexe.

4a. Variétés abéliennes

La propriété de densité est triviale non seulement pour une courbe elliptique E définie sur le corps $\bar{\mathbb{Q}} \cap \mathbb{R}$, mais aussi pour une puissance E^n d'une telle courbe : un point

$$(\gamma_1, \ldots, \gamma_n) \in E^n(\mathbb{R})^0$$

engendre un sous-groupe dense de $E^n(\mathbb{R})^0$ si et seulement si $\gamma_1, \ldots, \gamma_n$ sont linéairement indépendants sur $\mathbb{Z}$ dans $E(\mathbb{R})$.

Prenons maintenant une variété abélienne simple. Étant donné que, pour une variété abélienne A de dimension d, on a $m_{\mathbb{R}}(A) = 1$ et $m'_{\mathbb{R}}(A) = d^2 - d + 1$, on déduit immédiatement du théorème principal :

Corollaire 4.1. *Soient K un corps de nombres plongé dans $\mathbb{R}$, A une variété abélienne simple définie sur K de dimension $d \ge 1$ et Γ un sous-groupe de $A(K)$.*

a) *Si le rang de Γ est $\ge d^2 - d + 1$, alors $\Gamma \cap A(\mathbb{R})^0$ est dense dans $A(\mathbb{R})^0$ pour la topologie réelle.*
b) *Si le rang de Γ est $\ge d^2$, il existe un point de Γ dont les multiples engendrent un sous-groupe dense de $A(\mathbb{R})^0$.*
c) *Si la variété abélienne A possède la propriété de densité, le groupe $\Gamma \cap A(\mathbb{R})^0$ est dense dans $A(\mathbb{R})^0$ si et seulement si* $\operatorname{rang}_{\mathbb{Z}} \Gamma \ge 1$.

Pour une variété abélienne simple A sur un sous-corps K de $\bar{\mathbb{Q}} \cap \mathbb{R}$ possédant la propriété de densité, tout point d'ordre infini $\gamma \in A(K) \cap A(\mathbb{R})^0$ engendre un sous-groupe dense de $A(\mathbb{R})^0$. On peut écrire cette affirmation de la manière suivante :

Si A est une variété abélienne simple, définie sur un corps de nombres plongé dans $\mathbb{R}$, possédant la propriété de densité, et si $\omega_1, \ldots, \omega_{d-1}$ sont $d-1$ périodes réelles linéairement indépendantes de $\exp_A$, alors

$$\big(\mathbb{R}\omega_1 + \cdots + \mathbb{R}\omega_{d-1}\big) \cap \mathcal{L}_K(A) \subset \mathbb{Q}\omega_1 + \cdots + \mathbb{Q}\omega_{d-1}.$$

Quand on examine la situation conjecturale, il n'y a pas de raison, a priori, pour se limiter au cas réel, ni même à des périodes : cet énoncé suggère une extension aux variétés abéliennes de la conjecture des quatre exponentielles :

Conjecture 4.2 (pour une variété abélienne simple). *Soient K un sous-corps de $\bar{\mathbb{Q}}$, A une variété abélienne simple sur K de dimension $d \geq 1$ et $u_1, \ldots, u_d$ des éléments $\mathbb{Q}$-linéairement indépendants de $\mathcal{L}_K(A)$. Alors $u_1, \ldots, u_d$ sont linéairement indépendants sur $\mathbb{C}$.*

Cet énoncé est banal pour $d = 1$ et facile pour $d = 2$. Pour $d \geq 3$, même le cas où tous les u_i sont des périodes est ouvert (et intéressant) ; d'un autre côté, d'après ce que nous venons de voir, afin de résoudre la conjecture de Mazur pour les variétés abéliennes simples ([Mazur 1992, conjecture 5] ; voir [Waldschmidt 1993]), il suffit de considérer le cas où $u_1, \ldots, u_{d-1}$ sont $d-1$ périodes de l'exponentielle de A, tandis que u_d n'appartient pas au $\mathbb{Q}$-espace vectoriel engendré par le réseau des périodes (c'est-à-dire que u_d est un logarithme abélien d'un point d'ordre infini de $A(K)$). Enfin la conjecture pour une variété abélienne simple contient l'énoncé suivant :

? *Si A est une variété abélienne simple sur un corps de nombres K, de dimension d et si Γ est un sous-groupe de $A(K)$ de rang l contenu dans l'image d'un sous-groupe à n paramètres de $A(\mathbb{C})$, alors $n \geq \min\{d, l\}$.*

Ce dernier énoncé a déjà été conjecturé par S. Lang dans le cas particulier $l = 2$ [Lang 1971, p. 648]. A cette époque le seul résultat connu [Lang 1966, chap. II, § 4, th. 4] était :

pour $l \geq 7$ et $d \geq 2$ on a $n \geq 2$.

On sait maintenant que l'on a $ld \leq n(l+2d)$ [Waldschmidt 1983a, corollaire 1.2].

4b. Groupes linéaires déployés

Nous avons déjà dit que la propriété de densité était banale pour un groupe unipotent $\mathbb{G}_a^d$. Nous l'étudions ici pour un groupe linéaire déployé $\mathbb{G}_a^{d_0} \times \mathbb{G}_m^{d_1}$.

Corollaire 4.3. *Soient K le corps $\bar{\mathbb{Q}} \cap \mathbb{R}$, $d_0 \geq 0$, $d_1 \geq 1$ et $l \geq 1$ des entiers, α_{ij} pour $1 \leq i \leq d_1$ et $1 \leq j \leq l$ des nombres algébriques réels positifs multiplicativement indépendants, et β_{hj} pour $1 \leq h \leq d_0$ et $1 \leq j \leq l$ des nombres algébriques réels. On définit $\gamma_1, \ldots, \gamma_l$ dans $K^{d_0} \times (K^\times)^{d_1}$ par*

$$\gamma_j = (\beta_{1j}, \ldots, \beta_{d_0 j}; \alpha_{1j}, \ldots, \alpha_{d_1 j})$$

pour $1 \leq j \leq l$, et on désigne par Γ le sous-groupe de $K^{d_0} \times (K^\times)^{d_1}$ engendré par ces l éléments. On désigne aussi par Γ_0 la projection de Γ sur K^{d_0} : c'est le sous-groupe additif de K^{d_0} engendré par $\beta_1, \ldots, \beta_l$, avec

$$\beta_j = (\beta_{1j}, \ldots, \beta_{d_0 j})$$

pour $1 \leq j \leq l$. Enfin on pose $d = d_0 + d_1$.

a) *On suppose que Γ_0 est dense dans $\mathbb{R}^{d_0}$. Si $l \geq d_1(d-1)+2$, alors Γ est dense dans $\mathbb{R}^{d_0} \times (\mathbb{R}_+^\times)^{d_1}$.*
b) *On suppose, pour tout sous-espace vectoriel V de $\mathbb{R}^{d_0}$ rationnel sur K avec $V \neq \mathbb{R}^{d_0}$,*

$$\operatorname{rang}_{\mathbb{Z}}\big(\Gamma_0/\Gamma_0 \cap V\big) \geq d+1.$$

Si $l \geq d_1(d-1)+d+1$, alors Γ contient un sous-groupe de rang $d+1$ dense dans $\mathbb{R}^{d_0} \times (\mathbb{R}_+^\times)^{d_1}$.

c) *Si les groupes linéaires possèdent la propriété de densité, pour que Γ soit dense dans $\mathbb{R}^{d_0} \times (\mathbb{R}_+^\times)^{d_1}$, il faut et il suffit que l'on ait $l \geq d+1$ et que Γ_0 soit dense dans $\mathbb{R}^{d_0}$.*

Avant de prouver ce corollaire, on remarque qu'on peut en déduire le cas particulier suivant du théorème des six exponentielles :

Corollaire 4.4. *Si* α_{ij}, *pour* $i = 1, 2$ *et* $j = 1, 2, 3$, *sont des nombres algébriques réels positifs multiplicativement indépendants*, *la matrice*

$$\begin{pmatrix} \log \alpha_{11} & \log \alpha_{12} & \log \alpha_{13} \\ \log \alpha_{21} & \log \alpha_{22} & \log \alpha_{23} \end{pmatrix}$$

est de rang 2.

Démonstration. On choisit deux autres nombres algébriques réels positifs β_1 et β_2 tels que $\alpha_{11}, \alpha_{12}, \alpha_{13}, \alpha_{21}, \alpha_{22}, \alpha_{23}, \beta_1, \beta_2$ soient multiplicativement indépendants, et on utilise le corollaire 4.3 avec $d_0 = 0$, $d = d_1 = 2$, $l = 4$: le sous-groupe de $(\mathbb{R}_+^\times)^2$ engendré par $(\alpha_{11}, \alpha_{21})$, $(\alpha_{12}, \alpha_{22})$, $(\alpha_{13}, \alpha_{23})$ et (β_1, β_2) est dense, donc la matrice 2×3 considérée est de rang 2. □

On déduit aussi du corollaire 4.3 le cas réel homogène du théorème de Baker sur l'indépendance linéaire de logarithmes, c'est-à-dire l'énoncé suivant :

Corollaire 4.5. *Si* $\alpha_1, \ldots, \alpha_n$ *sont des nombres algébriques réels positifs multiplicativement indépendants*, *les* n *nombres* $\log \alpha_1, \ldots, \log \alpha_n$ *sont linéairement indépendants sur* $\bar{\mathbb{Q}}$.

Démonstration. On considère une éventuelle relation de dépendance linéaire de longueur minimale ; il s'agit donc de vérifier que, si $\alpha_1, \ldots, \alpha_{n+1}$ sont des nombres algébriques positifs et multiplicativement indépendants et si $\beta_1, \ldots, \beta_n$ sont des nombres algébriques réels tels que les nombres $1, \beta_1, \ldots, \beta_n$ soient linéairement indépendants sur $\mathbb{Q}$, alors

$$\beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n \neq \log \alpha_{n+1}.$$

On choisit alors un nombre algébrique positif α_0 tel que les $n+2$ nombres $\alpha_0, \ldots, \alpha_{n+1}$ soient multiplicativement indépendants et on applique le corollaire 4.3 avec $d_0 = n$, $d_1 = 1$, $l = n+2$ au sous-groupe de $\mathbb{R}^n \times \mathbb{R}_+^\times$ engendré par les $n+2$ points $(0, \ldots, 0, \log \alpha_0)$, $(\beta_1, \ldots, \beta_n, \log \alpha_{n+1})$, et

$$(\delta_{1j}, \ldots, \delta_{nj}, \log \alpha_j)$$

où $1 \leq j \leq n$. □

Démonstration du corollaire 4.3. On définit $G_0 = \mathbb{G}_{\mathrm{a}}^{d_0}$ et $G_1 = \mathbb{G}_{\mathrm{m}}^{d_1}$; on va appliquer le théorème principal 3.2 au groupe $G = G_0 \times G_1$, avec $m'_{\mathbb{R}}(G) = d_1(d-1) + 2$. L'hypothèse que les $d_1 l$ nombres α_{ij} sont multiplicativement indépendants assure que les sous-groupes algébriques G' de G pour lesquels $\Gamma \cap G'(K) \neq \{0\}$ sont de la forme $G' = G'_0 \times G_1$, avec G'_0 sous-groupe algébrique de G_0 ; pour un tel sous-groupe G',

$$\operatorname{rang}_{\mathbb{Z}}\bigl(\Gamma / \Gamma \cap G'(K)\bigr) = \operatorname{rang}_{\mathbb{Z}}\bigl(\Gamma_0 / \Gamma_0 \cap G'_0(K)\bigr).$$

Pour démontrer la partie (a) de l'énoncé, on utilise l'hypothèse que Γ_0 est dense dans $\mathbb{R}^{d_0}$: quand G'_0 est un sous-groupe de G_0 de dimension $< d_0$ (ce qui ne concerne que le cas $d_0 \geq 1$), on a

$$\operatorname{rang}_{\mathbb{Z}}\bigl(\Gamma_0 / \Gamma_0 \cap G'_0(K)\bigr) \geq m_{\mathbb{R}}(G_0 / G'_0) \,;$$

mais G_0/G'_0 est un groupe unipotent de la forme $\mathbb{G}_{\mathrm{a}}^{\delta}$ avec $\delta \geq 1$, donc $m_{\mathbb{R}}(G_0/G'_0) = \delta + 1 \geq 2$, tandis que $m'_{\mathbb{R}}(G_0/G'_0) = 2$; l'inégalité

$$\operatorname{rang}_{\mathbb{Z}}\bigl(\Gamma / \Gamma \cap G'(K)\bigr) \geq m'_{\mathbb{R}}(G/G')$$

est donc bien vérifiée pour tous les sous-groupes G' de G avec $\dim G' < \dim G$ pour lesquels

$$\Gamma \cap G'(K) \neq \{0\} \,;$$

pour les autres, c'est-à-dire quand $\Gamma \cap G'(K) = \{0\}$,

$$\begin{aligned} \operatorname{rang}_{\mathbb{Z}}\bigl(\Gamma / \Gamma \cap G'(K)\bigr) &= \operatorname{rang}_{\mathbb{Z}}(\Gamma) \geq m'_{\mathbb{R}}(G) \\ &\geq m'_{\mathbb{R}}(G/G'). \end{aligned}$$

Pour démontrer la partie (b), on utilise l'hypothèse

$$\operatorname{rang}_{\mathbb{Z}}\bigl(\Gamma_0 / \Gamma_0 \cap V\bigr) \geq d + 1$$

pour tout sous-espace vectoriel V de $\mathbb{R}^{d_0}$ rationnel sur K avec $V \neq \mathbb{R}^{d_0}$; on en déduit

$$\operatorname{rang}_{\mathbb{Z}}\bigl(\Gamma / \Gamma \cap G'(K)\bigr) \geq d + 1 = m'_{\mathbb{R}}(G/G') + d - 1$$

pour tout sous-groupe G' de G défini sur K avec $\dim G' < \dim G$ et $\Gamma \cap G'(K) \neq \{0\}$; si G' est un sous-groupe algébrique de G défini sur K tel que $\dim G' < \dim G$ et $\Gamma \cap G'(K) = \{0\}$,

$$\begin{aligned}\operatorname{rang}_{\mathbb{Z}}\bigl(\Gamma/\Gamma \cap G'(K)\bigr) = \operatorname{rang}_{\mathbb{Z}}(\Gamma) &\geq m'_{\mathbb{R}}(G) + d - 1\\ &\geq m'_{\mathbb{R}}(G/G') + d - 1,\end{aligned}$$

donc on peut appliquer la partie (b) du théorème principal.

Pour la partie (c), une implication est banale : si Γ est dense dans $\mathbb{R}^{d_0} \times (\mathbb{R}_+^\times)^{d_1}$, alors d'une part la projection Γ_0 de Γ sur le facteur $\mathbb{R}^{d_0}$ est dense et d'autre part on a $l = \operatorname{rang}_{\mathbb{Z}}(\Gamma) \geq m_{\mathbb{R}}(G) = d + 1$. Pour la réciproque, on utilise la propriété de densité : le fait que les $d_1 l$ nombres α_{ij} soient multiplicativement indépendants assure que l'adhérence de Zariski H du sous-groupe de $G^l = \mathbb{G}_{\mathrm{a}}^{d_0 l} \times \mathbb{G}_{\mathrm{m}}^{d_1 l}$ engendré par le point $(\beta_{hj}; \alpha_{ij})_{1\leq h\leq d_0, 1\leq i\leq d_1, 1\leq j\leq l}$ vérifie

$$\begin{aligned}H(\mathbb{R})^0 = \bigl\{&(x_0\beta_{hj}; x_{ij})_{1\leq h\leq d_0, 1\leq i\leq d_1, 1\leq j\leq l};\\ &(x_0, x_{ij}) \in \mathbb{R} \times (\mathbb{R}_+^\times)^{d_1 l}\bigr\}.\end{aligned}$$

Il reste à montrer qu'il existe $(x_{ij})_{1\leq i\leq d_1, 1\leq j\leq l} \in (\mathbb{R}_+^\times)^{d_1 l}$ tel que le sous-groupe $\mathbb{Z}\eta_1 + \cdots + \mathbb{Z}\eta_l$ de $\mathbb{R}^{d_0} \times (\mathbb{R}_+^\times)^{d_1}$ engendré par

$$\eta_j = (\beta_{1j}, \ldots, \beta_{d_0 j}; x_{1j}, \ldots, x_{d_1 j}),$$

où $1 \leq j \leq l$, soit dense dans $G(\mathbb{R})^0 = \mathbb{R}^{d_0} \times (\mathbb{R}_+^\times)^{d_1}$. On utilise pour cela les hypothèses : Γ_0 est dense dans $\mathbb{R}^{d_0}$ et $l \geq d+1$; on prend des nombres réels t_{ij}, où $1 \leq i \leq d_1$ et $1 \leq j \leq l$, qui sont algébriquement indépendants (sur $\mathbb{Q}$, donc sur K) et on pose $x_{ij} = e^{t_{ij}}$, où $1 \leq i \leq d_1$ et $1 \leq j \leq l$; on vérifie que pour tout $(s_1, \ldots, s_l) \in \mathbb{Z}^l \setminus \{0\}$, la matrice

$$\begin{pmatrix} \beta_{11} & \cdots & \beta_{1j} & \cdots & \beta_{1l}\\ \vdots & \ddots & \vdots & \ddots & \vdots\\ \beta_{d_0 1} & \cdots & \beta_{d_0 j} & \cdots & \beta_{d_0 l}\\ t_{11} & \cdots & t_{1j} & \cdots & t_{1l}\\ \vdots & \ddots & \vdots & \ddots & \vdots\\ t_{d_1 1} & \cdots & t_{d_1 j} & \cdots & t_{d_1 l}\\ s_1 & \cdots & s_j & \cdots & s_l \end{pmatrix}$$

(qui, malgré les apparences, a plus de lignes que de colonnes) est de rang $d+1$ et on applique le théorème de Kronecker. □

4c. Les questions de Colliot-Thélène, Coray et Sansuc

Une autre application concernant un groupe linéaire (tore non déployé) provient d'une question posée dans [Colliot-Thélène et al. 1980] et [Sansuc 1982] et résolue dans [Roy 1992b].

Corollaire 4.6. *Soient k un corps de nombres de degré $d = r_1 + 2r_2$; on note $\sigma_1, \ldots, \sigma_d$ les plongements de k dans $\mathbb{C}$ (avec $\sigma_1, \ldots, \sigma_{r_1}$ réels et $\sigma_{r_1+r_2+i} = \bar\sigma_{r_1+i}$ pour $1 \leq i \leq r_2$). Soient $\gamma_1, \ldots, \gamma_l$ des éléments de $k^\times$; on suppose que les nombres $\sigma_i\gamma_j$, pour $1 \leq i \leq d$ et $1 \leq j \leq l$, sont multiplicativement indépendants. On désigne par Γ le sous-groupe multiplicatif de $k^\times$ engendré par $\gamma_1, \ldots, \gamma_l$ et par $\sigma(\Gamma)$ son image dans $(\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$.*

a) *On suppose*

$$l \geq \begin{cases} d^2 - d + 2 & \text{si } r_2 = 0,\\ d^2 - dr_2 + 1 & \text{si } r_2 \geq 1\,; \end{cases}$$

alors l'adhérence de $\sigma(\Gamma)$ dans le groupe topologique $(\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$ contient $(\mathbb{R}_+^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$.

b) *On suppose*

$$l \geq \begin{cases} d^2 + 1 & \text{si } r_2 = 0,\\ d^2 - dr_2 + d & \text{si } r_2 \geq 1\,; \end{cases}$$

alors il existe un sous-groupe de $\sigma(\Gamma)$, de rang $r_1 + r_2 + 1$, dense dans $(\mathbb{R}_+^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$.

c) *Si les tores possèdent la propriété de densité, pour que l'adhérence de $\sigma(\Gamma)$ dans*

$$(\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$$

soit réunion de composantes connexes, il faut et il suffit que l'on ait $l \geq r_1 + r_2 + 1$.

On retrouve les exemples 2.10 et 2.11 en prenant $d = 2$. Si le corps quadratique k est réel ($r_1 = 2$, $r_2 = 0$), alors

- le théorème des six exponentielles montre que pour $l \geq 4$, l'adhérence de l'image de Γ dans $(\mathbb{R}^\times)^2$ contient $(\mathbb{R}_+^\times)^2$; de plus, pour $l \geq 5$, le

groupe Γ contient un sous-groupe de rang 3 dont l'image est dense dans $(\mathbb{R}_+^\times)^2$;
- la conjecture des quatre exponentielles implique que pour $l \geq 3$, l'adhérence de l'image de Γ dans $(\mathbb{R}^\times)^2$ est ouverte.

Si k est imaginaire ($r_1 = 0$, $r_2 = 1$), alors

- le théorème des six exponentielles montre que pour $l \geq 3$, $\sigma(\Gamma)$ est dense dans $\mathbb{C}^\times$ et pour $l \geq 4$, Γ contient un sous-groupe de rang 2 dont l'image est dense dans $\mathbb{C}^\times$;
- la conjecture des quatre exponentielles entraîne que pour $l \geq 2$, le sous-groupe Γ de $k^\times$ a une image dense dans $\mathbb{C}^\times$.

Démonstration du corollaire 4.6. On applique le théorème principal au groupe algébrique

$$G = \operatorname{Res}_{k/\mathbb{Q}} \mathbb{G}_{\mathrm{m}}$$

(restriction des scalaires de k à $\mathbb{Q}$ du groupe multiplicatif $\mathbb{G}_{\mathrm{m}}$; voir [Weil 1982]). Ce groupe algébrique G est défini sur $\mathbb{Q}$, de dimension $d = r_1 + 2r_2$ et $G(\mathbb{Q}) \simeq k^\times$, tandis que $G(\mathbb{R}) \simeq (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$. Sur $\bar{\mathbb{Q}}$, on a $G = \mathbb{G}_{\mathrm{m}}^d$. Par conséquent on a $\alpha(G) = d$, $\kappa_{\mathbb{R}}(G) = r_2$ et

$$m'_{\mathbb{R}}(G) = \bigl(d - \max\{r_2 - 1, 0\}\bigr)(d-1) + 2 - r_2.$$

Enfin, si G' est un sous-groupe algébrique de G de dimension $< d$, on a $\Gamma \cap G'(\mathbb{R}) = \{1\}$, grâce à l'hypothèse d'indépendance multiplicative des $\sigma_i(\gamma_j)$. □

Remarque. Dans le cas $r_2 \geq 2$, on peut raffiner le corollaire 4.6 en remplaçant l'hypothèse de (a) par

$$l \geq (r_1 + r_2)(r_1 + r_2 + 1) + 1$$

et celle de (b) par $l \geq (r_1 + r_2 + 1)^2 + 1$.

4d. Produit d'un groupe multiplicatif par une courbe elliptique

L'énoncé suivant est encore une variante elliptique de la conjecture des quatre exponentielles et aussi un cas particulier d'une conjecture de Ramachandra [1968, p. 87] :

? *Soit E une courbe elliptique définie sur un corps de nombres réels K. Soient ω une période réelle non nulle de $\exp_E$, $u \in \mathbb{R}$ un logarithme elliptique d'un point d'ordre infini de $E(K)$ et α_1, α_2 deux nombres algébriques réels positifs multiplicativement indépendants. Alors les trois nombres*

$$\frac{\log \alpha_1}{\log \alpha_2},\ \frac{u}{\omega},\ 1$$

sont linéairement indépendants sur $\mathbb{Q}$.

Cela signifie en effet que le sous-groupe de $\mathbb{R}_+^\times \times E(\mathbb{R})^0$ engendré par les deux points $(\alpha_1, \exp_E u)$ et $(\alpha_2, 0)$ est dense pour la topologie réelle et cette condition s'écrit encore : pour tout $(\lambda, \mu) \in \mathbb{Q}^2$,

$$\det\begin{pmatrix} \log\alpha_1 & \log\alpha_2 \\ u + \lambda\omega & \mu\omega \end{pmatrix} \neq 0.$$

Ce que l'on sait sur cette question se déduit d'un analogue elliptique du théorème des six exponentielles [Ramachandra 1968 ; Waldschmidt 1979, chap. 4] :

Corollaire 4.7. *Soient $\alpha_1, \dots, \alpha_l$ des nombres algébriques réels positifs qui engendrent un groupe multiplicatif de rang l_1. Soient E une courbe elliptique sur le corps $K = \bar{\mathbb{Q}} \cap \mathbb{R}$ et soient $\gamma_1, \dots, \gamma_l$ des éléments de $E(K) \cap E(\mathbb{R})^0$ qui engendrent un sous-groupe de rang l_2. On désigne par Γ le sous-groupe de $\mathbb{R}_+^\times \times E(\mathbb{R})^0$ engendré par les points (α_j, γ_j), où $1 \leq j \leq l$, et on suppose que Γ est de rang l.*

a) *On suppose $l \geq 4$, $l_1 \geq 2$ et $l_2 \geq 1$. Alors Γ est dense dans $\mathbb{R}_+^\times \times E(\mathbb{R})^0$.*
b) *On suppose $l \geq 5$, $l_1 \geq 3$ et $l_2 \geq 2$. Alors Γ contient un sous-groupe de rang 2 dense dans $\mathbb{R}_+^\times \times E(\mathbb{R})^0$.*
c) *Si le groupe algébrique $\mathbb{G}_{\mathrm{m}} \times E$ possède la propriété de densité, Γ est dense dans $\mathbb{R}_+^\times \times E(\mathbb{R})^0$ si et seulement si on a $l_1 \geq 2$ et $l_2 \geq 1$.*

Remarque. Voici l'énoncé analogue pour le produit du groupe additif et d'une courbe elliptique :

Soient E une courbe elliptique sur le corps $K = \bar{\mathbb{Q}} \cap \mathbb{R}$, β_1, β_2 des éléments $\mathbb{Q}$-linéairement indépendants de K, γ_1, γ_2 des points de

$$E(K) \cap E(\mathbb{R})^0$$

qui ne sont pas tous deux de torsion. Alors le sous-groupe de $K \times E(K)$ engendré par les deux points (β_1, γ_1) et (β_2, γ_2) est dense dans $\mathbb{R} \times E(\mathbb{R})^0$.

Cela résulte de la transcendance du nombre u/ω quand ω est une période non nulle de $\exp_E$ et u est un logarithme elliptique d'un point rationnel sur $\bar{\mathbb{Q}}$ d'ordre infini (résultat dû à Th. Schneider ; voir par exemple [Waldschmidt 1979, corollaire 3.2.3]). Le théorème principal ne contient donc pas tout ce que l'on peut dire sur ce type de question (voir la remarque finale au paragraphe 6).

4e. Extension d'une courbe elliptique par un groupe multiplicatif

Après avoir considéré un produit d'une courbe elliptique par un groupe multiplicatif, il est naturel, comme me l'a suggéré B. Mazur, d'étudier le cas d'une extension non triviale.

Prenons par exemple une courbe elliptique E définie sur $\mathbb{Q}$ avec $E(\mathbb{Q})$ de rang positif. Comme E est sa propre duale, à chaque point $\gamma \in E(\mathbb{Q})$ correspond une extension G_γ de E par $\mathbb{G}_{\mathrm{m}}$, définie sur $\mathbb{Q}$, et $G_\gamma(\mathbb{Q})$ se projette sur $E(\mathbb{Q})$. Supposons γ d'ordre infini dans $G(\mathbb{Q})$; alors l'extension G_γ n'est pas isotriviale, et le groupe algébrique G_γ, de dimension 2, possède exactement trois sous-groupes algébriques : les deux sous-groupes triviaux $\{1\}$ et G_γ lui-même, et un sous-groupe algébrique de dimension 1 isomorphe à $\mathbb{G}_{\mathrm{m}}$, que l'on notera simplement $\mathbb{G}_{\mathrm{m}}$.

Dans ce cas, *l'adhérence réelle de $G_\gamma(\mathbb{Q})$ dans $G_\gamma(\mathbb{R})$ contient $G_\gamma(\mathbb{R})^0$*. En effet, comme $G_\gamma(\mathbb{Q})$ contient $\mathbb{G}_{\mathrm{m}}(\mathbb{Q}) \simeq \mathbb{Q}^*$, si η est un point de $G_\gamma(\mathbb{Q})$ dont la projection sur $E(\mathbb{Q})$ est γ, alors le sous-groupe de $G_\gamma(\mathbb{Q})$ engendré par 2, 3 et η est dense dans $G_\gamma(\mathbb{R})^0$.

Nous allons voir qu'un sous-groupe de rang suffisamment élevé, dont la projection sur la courbe elliptique est dense, est alors dense, et contient même un sous-groupe de rang 2 qui est dense.

Corollaire 4.8. *Soient K un corps de nombres réel, E une courbe elliptique définie sur K, γ un point d'ordre infini de $E(K)$, et G_γ l'extension de E par le groupe multiplicatif $\mathbb{G}_{\mathrm{m}}$ attachée à γ.*

a) *Tout sous-groupe de type fini de $G_\gamma(K)$, de rang ≥ 5, dont la projection sur $E(K)$ est infinie, est dense.*
b) *Tout sous-groupe de type fini de $G_\gamma(K)$, de rang ≥ 6, dense dans $G_\gamma(\mathbb{R})^0$, contient un sous-groupe de rang 2 qui est encore dense.*
c) *Si le groupe algébrique G_γ possède la propriété de densité, alors pour tout sous-groupe de type fini Γ de $G_\gamma(K)$, les deux conditions suivantes sont équivalentes :*
   (i) *l'adhérence réelle de Γ dans $G_\gamma(\mathbb{R})$ contient $G_\gamma(\mathbb{R})^0$;*
   (ii) *on a $\mathrm{rang}_{\mathbb{Z}} \Gamma \geq 2$ et*

$$\mathrm{rang}_{\mathbb{Z}}\big(\Gamma/\Gamma \cap \mathbb{G}_{\mathrm{m}}(K)\big) \geq 1.$$

Démonstration. Si Γ est un sous-groupe de type fini de $G_\gamma(K)$ vérifiant $\mathrm{rang}_{\mathbb{Z}} \Gamma \geq 5$ et

$$\mathrm{rang}_{\mathbb{Z}}\big(\Gamma/\Gamma \cap \mathbb{G}_{\mathrm{m}}(K)\big) \geq 1,$$

alors les hypothèses de la partie (a) du théorème principal sont vérifiées, avec $d = d_2 = 2$, $d_0 = d_1 = 0$, $\alpha(G) = 4$, $\kappa_{\mathbb{R}}(G) = 1$ et $m'_{\mathbb{R}}(G_\gamma) = 5$. Donc $\Gamma \cap G_\gamma(\mathbb{R})^0$ est dense dans $G_\gamma(\mathbb{R})^0$.

De même, si $\mathrm{rang}_{\mathbb{Z}} \Gamma \geq 6$, les hypothèses de la partie (b) du théorème principal sont vérifiées, et $\Gamma \cap G_\gamma(\mathbb{R})^0$ contient un sous-groupe de rang 2 qui est encore dense dans $G_\gamma(\mathbb{R})^0$.

Dans l'assertion (c), l'implication (i) $\Rightarrow$ (ii) résulte des égalités $m_{\mathbb{R}}(G_\gamma) = 2$ et $m_{\mathbb{R}}(E) = 1$. Dans l'autre sens, on désigne par $(\eta, \omega) \in \mathbb{R}^2$ un générateur du noyau de $\exp_{G_\gamma} : \mathbb{R}^2 \to G_\gamma(\mathbb{R})$. Comme $\omega \neq 0$, il existe des triplets $(x, y, z) \in \mathbb{R}^3$ tels que le sous-groupe de $\mathbb{R}^2$ engendré par les trois points $(x, 0)$, (y, z) et (η, ω) soit dense dans $\mathbb{R}^2$. Ainsi dans le sous-groupe $(\mathbb{G}_{\mathrm{m}} \times G_\gamma)(\mathbb{R})$ de $(G_\gamma \times G_\gamma)(\mathbb{R})$, il existe un point (u_1, u_2) tel que $\mathbb{Z}u_1 + \mathbb{Z}u_2$ engendre un sous-groupe dense de $G_\gamma(\mathbb{R})^0$. Or l'hypothèse (ii) signifie qu'il existe γ_1 et γ_2 dans Γ tels que l'adhérence de Zariski dans $G_\gamma \times G_\gamma$ du sous-groupe $\mathbb{Z}(\gamma_1, \gamma_2)$ contienne $\mathbb{G}_{\mathrm{m}} \times G_\gamma$. On peut donc utiliser la propriété de densité. □

4f. Plusieurs plongements

Un autre exemple d'application du théorème 3.2 (théorème principal) provient d'une question posée par A. Ogg au MSRI de Berkeley en Mai 1992 : soit A une variété abélienne définie sur un corps de nombres K et soient $\sigma_1, \dots, \sigma_r$ des plongements distincts de K dans $\mathbb{R}$; pour $1 \le i \le r$, on a une variété abélienne A_i définie sur $\mathbb{R}$ et un plongement φ_i de $A(K)$ dans $A_i(\mathbb{R})$ associé à σ_i ; on définit $B = A_1 \times \cdots \times A_r$. A quelle condition l'adhérence de l'image d'un sous-groupe Γ de $A(K)$ dans $B(\mathbb{R})$ par $\varphi = (\varphi_1, \dots, \varphi_r)$ est-elle ouverte?

Si la variété abélienne B possède la propriété de densité, une condition nécessaire et suffisante est encore que $\varphi(\Gamma)$ soit Zariski-dense dans B. Pour le vérifier, on utilise la remarque suivante, dont la démonstration repose sur le fait qu'une réunion finie de sous-groupes de $\mathbb{Z}^l$ distincts de $\mathbb{Z}^l$ est encore distincte de $\mathbb{Z}^l$:

si B est une variété abélienne sur un corps K, et si Γ est un sous-groupe de $B(K)$ Zariski dense dans B, il existe $\gamma \in \Gamma$ qui engendre un sous-groupe $\mathbb{Z}\gamma$ Zariski dense dans B.

Nous traitons maintenant un exemple qui préfigure ce qui va se passer avec un plongement complexe (où il faudra considérer au même temps le plongement complexe conjugué).

Corollaire 4.9. *Soient K un sous-corps de $\mathbb{R} \cap \bar{\mathbb{Q}}$, σ un automorphisme du corps K et A une variété abélienne simple sur K de dimension d. On désigne par A^σ la variété abélienne déduite de A en faisant agir σ, par $\gamma \mapsto \gamma^\sigma$ l'isomorphisme de groupes naturel de $A(K)$ sur $A^\sigma(K)$, par B la variété abélienne $A \times A^\sigma$ définie sur K, et par $\varphi : A(K) \to B(K)$ l'homomorphisme de groupes qui envoie γ sur (γ, γ^σ). Soit finalement Γ un sous-groupe de $A(K)$ de rang l.*

a) *On suppose $l \ge 4d^2 - 2d + 1$. On suppose de plus, pour toute sous-variété abélienne B' de B, définie sur K, de dimension d,*
$$\operatorname{rang}_{\mathbb{Z}}\bigl(\varphi(\Gamma)/\varphi(\Gamma) \cap B'(K)\bigr) \ge d^2 - d + 1.$$
Alors $\varphi(\Gamma) \cap B(\mathbb{R})^0$ est dense dans $B(\mathbb{R})^0$.

b) *On suppose $l \ge 4d^2$. On suppose de plus, pour toute sous-variété abélienne B' de B, définie sur K, de dimension d,*
$$\operatorname{rang}_{\mathbb{Z}}\bigl(\varphi(\Gamma)/\varphi(\Gamma) \cap B'(K)\bigr) \ge d^2 + d.$$
Alors il existe $\gamma \in \Gamma$ tel que $\mathbb{Z}\varphi(\gamma)$ soit un sous-groupe dense de $B(\mathbb{R})^0$.

c) *Si les variétés abéliennes possèdent la propriété de densité, une condition nécessaire et suffisante pour que l'adhérence pour la topologie réelle de $\varphi(\Gamma)$ dans $B(\mathbb{R})$ soit ouverte est que l'on ait*
$$\operatorname{rang}_{\mathbb{Z}}\bigl(\varphi(\Gamma)/\varphi(\Gamma) \cap B'(K)\bigr) \ge 1$$
pour toute sous-variété abélienne B' de B, définie sur K, de dimension d.

La condition faisant intervenir les sous-variétés abéliennes B' s'explique facilement : il faut éviter, par exemple, que A soit définie sur le sous-corps
$$\{x \in K \,;\, x^\sigma = x\}$$
et que les éléments de Γ soient tous rationnels sur ce sous-corps.

5. PLONGEMENT COMPLEXE D'UN SOUS-GROUPE DE TYPE FINI

5a. Retour sur Kronecker

Le problème de la densité complexe se ramène à une question diophantienne grâce au lemme suivant :

Théorème 5.1 (Kronecker, variante complexe). *Soient V et $\bar{V}$ deux espaces vectoriels sur $\mathbb{C}$ et $\tau : V \to \bar{V}$ un anti-isomorphisme :*
$$\tau(\lambda z) = \bar{\lambda}\tau(z) \qquad \text{pour } \lambda \in \mathbb{C} \text{ et } z \in V,$$

où $\bar\lambda$ est le complexe conjugué de λ. On désigne par φ l'application $\mathbb{R}$-linéaire de V dans $V \times \bar V$ qui envoie z sur $\bigl(z, \tau(z)\bigr)$. Soit Y un sous-groupe de type fini de V ; on définit $\widetilde Y = \varphi(Y)$:

$$\widetilde Y = \bigl\{\bigl(y, \tau(y)\bigr)\,;\, y \in Y\bigr\} \subset V \times \bar V.$$

Les trois conditions suivantes sont équivalentes :

(i) *Y est dense dans V ;*

(ii) *pour tout hyperplan complexe H de $V \times \bar V$,*

$$\mathrm{rang}_{\mathbb{Z}}\bigl(\widetilde Y/\widetilde Y \cap H\bigr) \ge 2\,;$$

(iii) *$\widetilde Y$ est dense dans $\varphi(V)$.*

Choisissons une base $(e_1, \ldots, e_d)$ de V sur $\mathbb{C}$, des générateurs $y_1, \ldots, y_l$ (d'un sous-groupe d'indice fini) de Y sur $\mathbb{Z}$ et écrivons les coordonnées des y_j dans la base choisie :

$$y_j = y_{1j}e_1 + \cdots + y_{dj}e_d,$$

pour $1 \le j \le l$. Alors $\tau(e_1), \ldots, \tau(e_d)$ est une base de $\bar V$, les coordonnées de $\tau(y_j)$ dans cette base sont les $\bar y_{ij}$, et la condition (iii) s'écrit

(iv) *pour tout $(s_1, \ldots, s_l) \neq (0, \ldots, 0)$ dans $\mathbb{Z}^l$, la matrice*

$$\begin{pmatrix} y_{11} & \cdots & y_{1l} \\ \bar y_{11} & \cdots & \bar y_{1l} \\ \vdots & \ddots & \vdots \\ y_{d1} & \cdots & y_{dl} \\ \bar y_{d1} & \cdots & \bar y_{dl} \\ s_1 & \cdots & s_l \end{pmatrix}$$

a pour rang $2d + 1$.

5b. Le problème de densité complexe

Soient K un corps de nombres plongé dans $\mathbb{C}$ et G un groupe algébrique commutatif défini sur K. On définit un groupe algébrique $\widetilde G$ sur $\mathbb{R}$ par restriction des scalaires de $\mathbb{C}$ à $\mathbb{R}$ [Weil 1982, chap. 1, § 3] : on a une application $p : \widetilde G \to G$ définie sur $\mathbb{C}$ qui donne un isomorphisme $(p, \bar p) : \widetilde G \to G \times \bar G$ sur $\mathbb{C}$; le groupe des points réels $\widetilde G(\mathbb{R})$ est isomorphe au groupe $G(\mathbb{C})$.

La conjugaison complexe permet de définir un sous-corps $\bar K$ de $\mathbb{C}$, conjugué complexe de K, puis un groupe algébrique $\bar G$ défini sur $\bar K$, un isomorphisme de groupes $\gamma \mapsto \bar\gamma$ de $G(\mathbb{C})$ sur $\bar G(\mathbb{C})$ puis un homomorphisme de groupes φ de $G(\mathbb{C})$ dans $G(\mathbb{C}) \times \bar G(\mathbb{C})$ qui envoie γ sur $(\gamma, \bar\gamma)$, et enfin un $\mathbb{C}$–isomorphisme θ de $\widetilde G(\mathbb{C})$ sur $G(\mathbb{C}) \times \bar G(\mathbb{C})$. Si $s : \bar G(\mathbb{C}) \times G(\mathbb{C}) \to G(\mathbb{C}) \times \bar G(\mathbb{C})$ envoie (z, w) sur (w, z), on a $s \circ \bar\theta = \theta$:

$$\begin{tikzcd} \widetilde G(\mathbb{C}) \arrow[r, "\theta"] \arrow[d, "\bar\theta"'] & G(\mathbb{C}) \times \bar G(\mathbb{C}) \\ \bar G(\mathbb{C}) \times G(\mathbb{C}) \arrow[ur, "s"'] & \end{tikzcd}$$

de sorte que θ identifie $\widetilde G(\mathbb{R})$ avec l'image de φ :

$$\begin{aligned} \theta\bigl(\widetilde G(\mathbb{R})\bigr) &= \bigl\{(\gamma, \bar\gamma)\,;\, \gamma \in G(\mathbb{C})\bigr\} \\ &= \varphi\bigl(G(\mathbb{C})\bigr) \subset G(\mathbb{C}) \times \bar G(\mathbb{C}). \end{aligned}$$

Sur l'espace tangent du groupe de Lie $\widetilde G(\mathbb{C})$, le $\mathbb{R}$-espace vectoriel

$$\begin{aligned} T_{\widetilde G}(\mathbb{R}) &= \bigl\{(z, \bar z)\,;\, z \in T_G(\mathbb{C})\bigr\} \\ &\subset T_{\widetilde G}(\mathbb{C}) = T_G(\mathbb{C}) \times T_{\bar G}(\mathbb{C}) \end{aligned}$$

définit une $\mathbb{R}$-structure.

Le groupe $\widetilde G$ est défini sur le corps $\widetilde K$, intersection (dans $\mathbb{C}$) de $\mathbb{R}$ avec le compositum de K et $\bar K$; quitte à remplacer K par son compositum avec $\bar K$, on peut supposer $K = \bar K$ (la seule modification qu'apporte une extension finie, ou même algébrique, concerne l'hypothèse de simplicité pour une variété abélienne). Quand K est stable sous la conjugaison complexe,

- si $K \subset \mathbb{R}$, on a $\widetilde K = K$ (et alors, si $\dim G > 0$, $G(\mathbb{R})$ n'est pas dense dans $G(\mathbb{C})$) ;
- sinon, $\widetilde K = K \cap \mathbb{R}$ avec $[K : \widetilde K] = 2$ et alors $\widetilde G = \mathrm{Res}_{K/\widetilde K}\, G$.

Quand Γ est un sous-groupe de $G(\mathbb{C})$, $\widetilde\Gamma = \varphi(\Gamma)$ est un sous-groupe de $\widetilde G(\mathbb{R})$; si $\Gamma \subset G(K)$, alors $\widetilde\Gamma \subset \widetilde G(\widetilde K)$. Enfin Γ est dense dans $G(\mathbb{C})$ si et seulement si $\widetilde{\Gamma}$ est dense dans $\widetilde{G}(\mathbb{R})$ (la variante complexe ci-dessus du théorème de Kronecker correspond à la situation où G est un groupe unipotent). Grâce à cela, on obtient l'énoncé suivant :

Corollaire 5.2. *Si le groupe algébrique $\widetilde{G}$ possède la propriété de densité* (*définition* 1.2), *alors pour tout sous-groupe Γ de type fini de $G(K)$, les deux assertions suivantes sont équivalentes*:

(i) *Γ est dense dans $G(\mathbb{C})$;*

(ii) *si $\gamma_1, \dots, \gamma_l$ engendrent un sous-groupe d'indice fini de Γ et si H désigne l'adhérence de Zariski dans $\widetilde{G}^l$ du sous-groupe $\mathbb{Z}\bigl(\varphi(\gamma_1), \dots, \varphi(\gamma_l)\bigr)$, il existe un élément $(\eta_1, \dots, \eta_l)$ de $H(\mathbb{R})$ tel que le sous-groupe $\mathbb{Z}\eta_1 + \cdots + \mathbb{Z}\eta_l$ soit dense dans $\widetilde{G}(\mathbb{R})$.*

5c. Application du théorème principal

Voici un résultat de densité pour un plongement complexe, qui résulte immédiatement du théorème principal combiné avec la version complexe du théorème de Kronecker.

Corollaire 5.3. *Soit G un groupe algébrique commutatif connexe de dimension d défini sur un corps de nombres K plongé dans $\mathbb{C}$. Soit Γ un sous-groupe de type fini de $G(K)$.*

a) *On suppose, pour tout sous-groupe algébrique G' de $\widetilde{G}$ défini sur $\widetilde{K}$ avec* $\dim G' < \dim \widetilde{G}$,

$$\operatorname{rang}_{\mathbb{Z}}\bigl(\widetilde{\Gamma}/\widetilde{\Gamma} \cap G'(\widetilde{K})\bigr) \geq m'_{\mathbb{R}}(\widetilde{G}/G').$$

Alors Γ est dense dans le groupe topologique $G(\mathbb{C})$.

b) *On suppose, pour tout sous-groupe algébrique G' de $\widetilde{G}$ défini sur $\widetilde{K}$ avec* $\dim G' < \dim \widetilde{G}$,

$$\operatorname{rang}_{\mathbb{Z}}\bigl(\widetilde{\Gamma}/\widetilde{\Gamma} \cap G'(\widetilde{K})\bigr) \geq m'_{\mathbb{R}}(\widetilde{G}/G') + 2d - 1.$$

Alors il y a un sous-groupe de Γ de rang $m_{\mathbb{C}}(G)$ qui est dense (*pour la topologie complexe*) *dans $G(\mathbb{C})$.*

Ce corollaire permet de montrer que pour tout groupe algébrique commutatif G défini sur $\overline{\mathbb{Q}}$, il existe un corps de nombres K tel que $G(K)$ contienne un sous-groupe de rang $m_{\mathbb{C}}(G)$ qui soit dense dans $G(\mathbb{C})$.

Remarque. On a $\dim \widetilde{G} = 2 \dim G$, $\alpha(\widetilde{G}) = 2\alpha(G)$ et $\kappa_{\mathbb{R}}(\widetilde{G}) \geq \kappa_{\mathbb{C}}(G)$. La condition qui correspond au sous-groupe trivial $G' = \{0\}$ suggère d'introduire la notation suivante. Quand G est un groupe algébrique commutatif défini sur $\mathbb{C}$, on pose $m'_{\mathbb{C}}(G) = 2$ si $\kappa_{\mathbb{C}}(G) = 0$, et

$$m'_{\mathbb{C}}(G) = \bigl(2\alpha(G) - \kappa_{\mathbb{C}}(G) + 1\bigr)(2d-1) + 2 - \kappa_{\mathbb{C}}(G)$$

si $\kappa_{\mathbb{C}}(G) \geq 1$. La condition $\kappa_{\mathbb{C}}(G) = 0$ signifie que G est unipotent, ce qui s'écrit aussi $\alpha(G) = 0$.

De cette définition on va déduire que

$$m'_{\mathbb{C}}(G) \leq 2(d-1)\alpha(G) + 2d + 1$$

si G est un groupe linéaire,

$$m'_{\mathbb{C}}(G) \leq 4d^2 - 2d + 1$$

si G est une variété abélienne, et

$$m'_{\mathbb{C}}(G) \leq (3d-2)\alpha(G) + 2d + 1$$

dans le cas général. Seule la dernière majoration mérite une explication : si G est extension d'une variété abélienne A de dimension g par un groupe linéaire $\mathbb{G}_{\mathrm{a}}^u \times \mathbb{G}_{\mathrm{m}}^t$ et si G n'a pas de facteur $\mathbb{G}_{\mathrm{a}}$, alors $u \leq g$; on en déduit $\alpha(G) \leq 2\kappa_{\mathbb{C}}(G)$.

Avec cette notation, on a $m'_{\mathbb{R}}(\widetilde{G}) \leq m'_{\mathbb{C}}(G)$, donc pour vérifier l'hypothèse (a) du corollaire 5.3 pour le sous-groupe trivial $\{0\}$, il suffit d'imposer

$$\operatorname{rang}_{\mathbb{Z}} \Gamma \geq m'_{\mathbb{C}}(G).$$

Pour vérifier (b), il suffit d'imposer

$$\operatorname{rang}_{\mathbb{Z}} \Gamma \geq m'_{\mathbb{C}}(G) + 2d - 1.$$

5d. Variétés abéliennes simples

Soit A une variété abélienne simple sur $\mathbb{C}$, de dimension d, et soit γ un point de $A(\mathbb{C})$; une condition nécessaire et suffisante pour que le sous-groupe engendré par γ ne soit pas dense dans $A(\mathbb{C})$ est qu'il existe $2d-1$ périodes $\omega_1, \dots, \omega_{2d-1}$ de $\exp_A$

et un entier $n \geq 1$, tels que $n\gamma$ appartienne au sous-groupe à $2d-1$ paramètres

$$\exp_A(\mathbb{R}\omega_1 + \cdots + \mathbb{R}\omega_{2d-1}).$$

Il s'agit de voir quand cela peut arriver avec un point γ rationnel sur $\bar{\mathbb{Q}}$.

Soit K un sous-corps de $\bar{\mathbb{Q}}$ et soit A une variété abélienne simple sur K de dimension d. On note $\bar{A}$ la variété abélienne déduite de A par action de la conjugaison complexe et on pose $\widetilde{A} = \operatorname{Res}_{\mathbb{C}/\mathbb{R}} A$. Pour appliquer le corollaire 5.3 on est amené à décrire les sous-variétés abéliennes de $\widetilde{A}$ définies sur $\mathbb{R}$. Comme $\widetilde{A}(\mathbb{C})$ est le produit des deux variétés abéliennes simples $A(\mathbb{C})$ et $\bar{A}(\mathbb{C})$, les éventuelles sous-variétés de $\widetilde{A}$ définies sur $\mathbb{R}$ et distinctes de $\{0\}$ et de $\widetilde{A}$ ont pour dimension d. On choisit une base de $T_A(\mathbb{C})$ sur $\mathbb{C}$ de manière à identifier $T_A(\mathbb{C})$ à $\mathbb{C}^d$, $T_{\widetilde{A}}(\mathbb{C})$ à $\mathbb{C}^{2d}$, Ω_A à un réseau Ω de $\mathbb{C}^d$ et $\Omega_{\bar{A}}$ au réseau conjugué $\bar{\Omega}$.

On désigne par $\mathcal{E}(A)$ l'ensemble (éventuellement vide) des éléments $\theta \in \mathrm{GL}_d(\mathbb{C})$ tels que $\theta\Omega \cap \overline{\theta\Omega}$ soit un sous-groupe d'indice fini de $\theta\Omega$.

Pour chaque $\theta \in \mathcal{E}(A)$,

$$\big\{(z_1, z_2) \in T_{\widetilde{A}}(\mathbb{C})\,;\ \theta z_1 = \bar{\theta} z_2\big\}$$

est l'espace tangent sur $\mathbb{C}$ d'une sous-variété abélienne A_θ de $\widetilde{A}$ définie sur $\mathbb{R}$ de dimension d et on les obtient toutes ainsi.

Corollaire 5.4. *Soient K un sous-corps de $\bar{\mathbb{Q}}$, A une variété abélienne simple sur K de dimension d et Γ un sous-groupe de $A(K)$ de rang l.*

a) *On suppose $l \geq 4d^2-2d+1$. On suppose de plus, pour tout $\theta \in \mathcal{E}(A)$,*

$$\operatorname{rang}_{\mathbb{Z}}\big(\widetilde{\Gamma}/\widetilde{\Gamma} \cap A_\theta(\mathbb{R})\big) \geq d^2 - d + 1.$$

Alors Γ est dense dans $A(\mathbb{C})$.

b) *On suppose $l \geq 4d^2$. On suppose de plus, pour tout $\theta \in \mathcal{E}(A)$,*

$$\operatorname{rang}_{\mathbb{Z}}\big(\widetilde{\Gamma}/\widetilde{\Gamma} \cap A_\theta(\mathbb{R})\big) \geq d^2 + d.$$

Alors Γ contient un sous-groupe de rang 1 dense dans $A(\mathbb{C})$.

c) *Si les variétés abéliennes possèdent la propriété de densité, une condition nécessaire et suffisante pour que Γ soit dense dans $A(\mathbb{C})$ est*

$$\operatorname{rang}_{\mathbb{Z}}\big(\widetilde{\Gamma}/\widetilde{\Gamma} \cap A_\theta(\mathbb{R})\big) \geq 1$$

pour tout $\theta \in \mathcal{E}(A)$.

Exemple 5.5. Soit E une courbe elliptique sur $\bar{\mathbb{Q}}$; on choisit un modèle de Weierstrass

$$E(\mathbb{C}) = \big\{(x{:}y{:}t) \in \mathbb{P}_2(\mathbb{C})\,;\ y^2t = 4x^3 - g_2xt^2 - g_3t^3\big\}.$$

Soit $\wp$ la fonction elliptique de Weierstrass d'invariants g_2 et g_3 :

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3.$$

On identifie $T_E(\mathbb{C})$ à $\mathbb{C}$ par

$$\exp_E(z) = \begin{cases} \big(\wp(z){:}\wp'(z){:}1\big) & \text{si } u \notin \Omega, \\ \big(0{:}1{:}0\big) & \text{si } u \in \Omega, \end{cases}$$

où $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ désigne le réseau des périodes de $\wp$. On désigne ensuite par $\bar{\Omega} = \mathbb{Z}\bar{\omega}_1 + \mathbb{Z}\bar{\omega}_2$ le réseau conjugué complexe de Ω, par $\bar{\wp}$ la fonction elliptique de Weierstrass d'invariants $\overline{g_2}$, $\overline{g_3}$ et de réseau de périodes $\bar{\Omega}$, et par $\bar{E}$ la courbe elliptique de Weierstrass associée.

La courbe E admet un modèle défini sur $\mathbb{R}$ si et seulement s'il existe $\theta \in \mathbb{C}^\times$ tel que $\theta\Omega = \overline{\theta\Omega}$. On vérifie aussi facilement (comparer à [Huisman 1992, lemme 5.2]) que les conditions suivantes sont équivalentes :

(i) la variété abélienne $\widetilde{E} = \operatorname{Res}_{\mathbb{C}/R} E$ n'est pas simple sur $\mathbb{R}$;

(ii) l'ensemble

$$\mathcal{E}(E) = \big\{\theta \in \mathbb{C}^\times\,;\ \operatorname{rang}_{\mathbb{Z}}\big(\theta\Omega \cap \overline{\theta\Omega}\big) = 2\big\}$$

n'est pas vide ;

(iii) il existe trois nombres entiers a, b, c dans $\mathbb{Z}$ tels que a^2+bc soit un carré non nul et que le nombre $\tau = \omega_2/\omega_1$ vérifie

$$b|\tau|^2 + a(\tau + \bar{\tau}) - c = 0.$$

Si ces conditions sont vérifiées, les deux courbes E et $\bar{E}$ sont isogènes.

Supposons dans un premier temps $\mathcal{E}(E) = \varnothing$; alors

- si Γ est un sous-groupe de $E(\bar{\mathbb{Q}})$ de rang ≥ 3, le corollaire 5.2 montre que Γ est dense dans le groupe topologique $E(\mathbb{C})$;
- si $\Gamma \subset E(\bar{\mathbb{Q}})$ a un rang ≥ 4, il existe $\gamma \in \Gamma$ qui engendre un sous-groupe dense de $E(\mathbb{C})$;
- si la propriété de densité vaut pour les surfaces abéliennes, tout point d'ordre infini de $E(\bar{\mathbb{Q}})$ engendre un sous-groupe dense pour la topologie complexe de $E(\mathbb{C})$.

Quand $\mathcal{E}(E) \neq \varnothing$, il faut travailler un peu plus. Soit $\theta \in \mathcal{E}(E)$; le quotient E_θ du $\mathbb{C}$-espace vectoriel

$$T_{E_\theta}(\mathbb{C}) = \bigl\{(z_1, z_2) \in \mathbb{C}^2 \,;\, \theta z_1 = \bar{\theta} z_2\bigr\}$$

par le réseau

$$\Omega_\theta = \bigl\{(\omega, \overline{\omega'}) \,;\, \theta\omega = \overline{\theta\omega'}\bigr\} \subset \Omega \times \bar{\Omega}$$

est une courbe elliptique, que l'on peut aussi écrire comme le quotient de $\mathbb{C}$ par le réseau

$$\bigl\{\omega \in \Omega \,;\, \theta\omega \in \overline{\theta\Omega}\bigr\} \subset \Omega.$$

Le quotient E'_θ de la variété abélienne

$$\widetilde{E} = \mathrm{Res}_{\mathbb{C}/R}\, E$$

par E_θ s'écrit aussi $\mathbb{C}/\Omega'_\theta$, avec

$$\Omega'_\theta = \bigl\{\theta\omega - \overline{\theta\omega'} \,;\, (\omega, \omega') \in \Omega \times \Omega\bigr\} \subset \mathbb{C}.$$

Ainsi on déduit du corollaire 5.4 :

Corollaire 5.6. *Soient $u_1, \dots, u_l$ des éléments de $\mathbb{C}$ tels que les points $\gamma_j = \exp_E(u_j)$, pour $1 \leq j \leq l$, engendrent un sous-groupe Γ de $E(\bar{\mathbb{Q}})$ de rang l. On pose $Y = \mathbb{Z}u_1 + \dots + \mathbb{Z}u_l + \Omega$. Pour $\theta \in \mathbb{C}^\times$, on définit*

$$Y_\theta = \bigl\{\theta y - \overline{\theta y} \,;\, y \in Y\bigr\}.$$

1. *S'il existe $\theta \in \mathcal{E}(E)$ tel que $Y_\theta \cap \Omega'_\theta$ soit un sous-groupe d'indice fini de Y_θ, alors Γ n'est pas dense dans $E(\mathbb{C})$.*
2. *Supposons que pour tout $\theta \in \mathcal{E}(E)$, $Y_\theta \cap \Omega'_\theta$ n'est pas un sous-groupe d'indice fini de Y_θ. Alors :*
   a) *Si $l \geq 3$, le sous-groupe Γ est dense dans $E(\mathbb{C})$.*
   b) *Si $l \geq 4$, et si*
   $$\mathrm{rang}_{\mathbb{Z}}\bigl(Y_\theta / Y_\theta \cap \Omega'_\theta\bigr) \geq 2$$
   pour tout $\theta \in \mathcal{E}(E)$, alors il existe $\gamma \in \Gamma$ qui engendre un sous-groupe dense dans $E(\mathbb{C})$.
   c) *Si la propriété de densité est vraie pour un produit de deux courbes elliptiques, alors Γ est dense dans $E(\mathbb{C})$.*

5e. Groupes linéaires

Voici une dernière conséquence du corollaire 5.3.

Corollaire 5.7. *Soient $d_0 \geq 0$, $d_1 \geq 1$ et $l \geq 1$ des entiers. Soient α_{ij}, pour $1 \leq i \leq d_1$ et $1 \leq j \leq l$, des nombres algébriques non nuls, et β_{hj}, pour $1 \leq h \leq d_0$ et $1 \leq j \leq l$, des nombres algébriques. On suppose que les $2d_1 l$ nombres α_{ij} et $\bar{\alpha}_{ij}$ sont multiplicativement indépendants. On définit $\gamma_1, \dots, \gamma_l$ dans $\bar{\mathbb{Q}}^{d_0} \times (\bar{\mathbb{Q}}^\times)^{d_1}$ par*

$$\gamma_j = (\beta_{1j}, \dots, \beta_{d_0 j}; \alpha_{1j}, \dots, \alpha_{d_1 j}),$$

où $1 \leq j \leq l$, et on désigne par Γ le sous-groupe de $\bar{\mathbb{Q}}^{d_0} \times (\bar{\mathbb{Q}}^\times)^{d_1}$ engendré par ces l éléments. On désigne ensuite par Γ_0 la projection de Γ sur $\bar{\mathbb{Q}}^{d_0}$: c'est le sous-groupe additif de $\bar{\mathbb{Q}}^{d_0}$ engendré par $\beta_1, \dots, \beta_l$, avec

$$\beta_j = (\beta_{1j}, \dots, \beta_{d_0 j})$$

pour $1 \leq j \leq l$. On désigne aussi par $\widetilde{\Gamma}_0$ le sous-groupe de $\bar{\mathbb{Q}}^{2d_0}$ engendré par $(\beta_1, \bar{\beta}_1), \dots, (\beta_l, \bar{\beta}_l)$. Enfin on pose $d = d_0 + d_1$.

a) *On suppose que Γ_0 est dense dans $\mathbb{C}^{d_0}$. Si*
$$l \geq 2d_1(d-1) + 2d + 1,$$
alors Γ est dense dans $\mathbb{C}^{d_0} \times (\mathbb{C}^\times)^{d_1}$.

b) *On suppose, pour tout sous-espace vectoriel $\mathcal{V}$ de $\mathbb{C}^{2d_0}$ rationnel sur $\bar{\mathbb{Q}}$ avec $\mathcal{V} \neq \mathbb{C}^{2d_0}$,*
$$\mathrm{rang}_{\mathbb{Z}}\bigl(\widetilde{\Gamma}_0 / \widetilde{\Gamma}_0 \cap \mathcal{V}\bigr) \geq 2d + 1.$$

Si $l \geq 2d_1(d-1)+4d$, *alors* Γ *contient un sous-groupe de rang* $2d_0+d_1+1$ *dense dans* $\mathbb{C}^{d_0} \times (\mathbb{C}^\times)^{d_1}$.

c) *Supposons que la propriété de densité soit vraie pour les groupes linéaires. Alors, pour que* Γ *soit dense dans* $\mathbb{C}^{d_0} \times (\mathbb{C}^\times)^{d_1}$, *il faut et il suffit que l'on ait* $l \geq 2d_0+d_1+1$ *et que* Γ_0 *soit dense dans* $\mathbb{C}^{d_0}$.

On pourra comparer le cas $d_0 = 0$, $d = d_1 = 1$ avec l'exemple 2.11.

6. LA SUITE DE L'HISTOIRE

Pour terminer, mentionnons la possibilité de développer cette étude dans (au moins) deux directions :

- nous nous sommes limité dans cet travail à des considérations homogènes (d'indépendance linéaire ou algébrique) ; on peut aussi faire intervenir des formes linéaires non homogènes, ou encore des polynômes non homogènes ;
- on peut donner des énoncés quantitatifs (mesures de densité).

Ces thèmes seront développés ailleurs.

REMERCIEMENTS

L'auteur remercie cordialement Daniel Bertrand, Barry Mazur, Damien Roy et Federico Pellarin, pour leurs remarques pertinentes sur une version préliminaire de ce texte.

BIBLIOGRAPHIE

[Bertrand 1995] D. Bertrand, "Points rationnels sur les sous-groupes compacts des groupes algébriques", à paraître dans *Experimental Mathematics*.

[Cassels 1957] J. W. S. Cassels, *An Introduction to Diophantine Approximation*, Cambridge Univ. Press, Cambridge, 1957.

[Colliot-Thélène et al. 1980] J-L. Colliot-Thélène, D. Coray et J-J. Sansuc, "Descente et principe de Hasse pour certaines variétés rationnelles", *J. reine angew. Math.* **320** (1980), 150–191.

[Emsalem 1987] M. Emsalem, "Sur les idéaux dont l'image par l'application d'Artin dans une $\mathbb{Z}_p$-extension est triviale", *J. reine angew. Math.* **382** (1987), 181–198.

[Huisman 1992] J. Huisman, "The underlying real algebraic structure of complex elliptic curves", *Math. Ann.* **294** (1992), 19–35.

[Lang 1966] S. Lang, *Introduction to Transcendental Numbers*, Addison-Wesley, Reading, MA, 1966.

[Lang 1971] S. Lang, "Transcendental numbers and diophantine approximations", *Bull. Amer. Math. Soc.* **77** (1971), 635–677.

[Mazur 1992] B. Mazur, "The topology of rational points", *Experimental Mathematics* **1** (1992), 35–45.

[Ramachandra 1968] K. Ramachandra, "Contributions to the theory of transcendental numbers I–II" *Acta Arith.* **14** (1968), 65–88.

[Roy 1989] D. Roy, "Sur la conjecture de Schanuel pour les logarithmes de nombres algébriques", *Publ. Math. Univ. Pierre et Marie Curie* (Paris VI) **90** (1989), n° 6, 12 p.

[Roy 1990a] D. Roy, "Matrices dont les coefficients sont des formes linéaires", p. 273–281 dans le *Séminaire de théorie de nombres*, 1987–88, Paris (édité par C. Goldstein), Prog. in Math. **81**, Birkhäuser, Berlin, 1990.

[Roy 1990b] D. Roy, "Transcendance et questions de répartition dans les groupes algébriques", p. 249–274 dans *Approximations Diophantiennes et Nombres Transcendants, Luminy* 1990 (édité par P. Philippon), de Gruyter, Berlin, 1992.

[Roy 1992a] D. Roy, "Matrices whose coefficients are linear forms in logarithms", *J. Number Theory* **41** (1992), 22–47.

[Roy 1992b] Roy 1992b D. Roy, "Simultaneous approximations in number fields", *Invent. Math.* **109** (1992), 547–556.

[Roy 1995] D. Roy, "Points whose coordinates are logarithms of algebraic numbers on algebraic varieties", à paraître dans *Acta Math.*

[Sansuc 1982] J-J. Sansuc, "Descente et principe de Hasse pour certaines variétés rationnelles", p. 253–271 dans le *Séminaire de Théorie de Nombres, Paris*

1980–81 (édité par M.-J. Bertin), Prog. in Math. **22**, Birkhäuser, Berlin, 1982.

[Serre 1979] J-P. Serre, "Quelques propriétés des groupes algébriques commutatifs", appendice 2 de [Waldschmidt 1979].

[Waldschmidt 1979] M. Waldschmidt, "Nombres transcendants et groupes algébriques", *Astérisque* **69/70** (1979).

[Waldschmidt 1981] M. Waldschmidt, "Transcendance et exponentielles en plusieurs variables", *Invent Math.* **63** (1981), 97–127.

[Waldschmidt 1983a] M. Waldschmidt, "Sous-groupes analytiques de groupes algébriques", *Annals of Math.* **117** (1983), 627–657.

[Waldschmidt 1983b] M. Waldschmidt, "Dépendance de logarithmes dans les groupes algébriques", p. 289–328 dans *Approximations diophantiennes et nombres transcendants, Luminy* 1982 (édité par D. Bertrand et M. Waldschmidt), Prog. in Math. **31**, Birkhäuser, Berlin, 1983.

[Waldschmidt 1987] M. Waldschmidt, "Dependence of logarithms of algebraic points", *Coll. Math. Soc. János Bolyai* **51** (1987), 1013–1035.

[Waldschmidt 1988] M. Waldschmidt, "On the transcendence methods of Gel'fond and Schneider in several variables", p. 375–398 dans *New Advances in Transcendence Theory, Durham* 1986 (édité par A. Baker), Cambridge Univ. Press, Cambridge, 1988.

[Waldschmidt 1993] M. Waldschmidt, "Transcendental numbers and functions of several variables", p. 67–80 *Advances in Number Theory, Kingston* 1991 (édité par F. Q. Gouvêa et N. Yui), Oxford Univ. Press, New York, 1993.

[Weil 1982] A. Weil, *Adèles and algebraic groups*, Prog. in Math. **23**, Birkhäuser, Berlin, 1982.

Michel Waldschmidt, Université Pierre et Marie Curie (Paris VI), Mathématiques, T. 45–46, 5ème étage, 4, Place Jussieu, F–75252 Paris, France (miw@mathp6.jussieu.fr)

Received September 21, 1994; accepted in revised form 4 February 1995