Cours de Troisième Cycle 1994/95 Université P. et M. Curie (Paris VI)

Topologie des Points Rationnels

par

Michel WALDSCHMIDT

TOPOLOGIE DES POINTS RATIONNELS

Sommaire

Préface

Le texte qui suit est la rédaction d'un cours de troisième cycle donné à l'Université P. et M. Curie (Paris VI) en 1994/95 dans le cadre du D.E.A. (Diplome d'Études Approfondies) *Algèbre et Géométrie de Mathématiques Pures.*

Depuis trois ans que ces notes ont été rédigées, d'importants progrès ont été réalisés. En particulier un contre exemple à la conjecture initiale de Mazur (qui est le thème central de ce cours) a été construit par J.L. Colliot-Thélène, A.N. Skorobogatov et H.P.F. Swinnerton-Dyer. Néanmoins le cas particulier de cette conjecture qui concerne les variétés abéliennes (et plus généralement les groupes algébriques commutatifs) reste plausible.

Merci à tous ceux dont les remarques m'ont permis d'améliorer le texte initial, notamment Valérie Callendreau, Vincent Bosser, Jean-Louis Colliot-Thélène, Damien Roy, Joost van Hamel et beaucoup d'autres.

Paris, Février 1998.

Michel WALDSCHMIDT.

World Wide Web `http ://www.mathp6.jussieu.fr/~miw/TPR.html`

Notations

$\mathbb{Z}$ anneau des entiers rationnels, $\mathbb{Q}$ corps des nombres rationnels

$\overline{\mathbb{Q}}$ corps des nombres algébriques (clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$)

$\mathbb{R}$ corps des nombres réels, $\mathbb{C}$ corps des nombres complexes

$\mathbb{U}$ groupe multiplicatif des nombres complexes de module 1 (cf. p. 17)

μ_n groupe des racines de l'unité d'ordre divisant n

$K^\times$ groupe multiplicatif des éléments non nuls d'un corps K

$\Re\mathrm{e}\, z$ et $\Im\mathrm{m}\, z$ parties réelles et imaginaires d'un nombre complexe z (cf. p. 34)

$\mathbb{P}_n$ et $\mathbb{A}_n$ espaces projectifs et affines de dimension n (cf. pp. 1 et 2)

$\mathbb{G}_{\mathrm{a}}$, $\mathbb{G}_{\mathrm{m}}$ groupes additifs et multiplicatifs (cf. p. 2)

$\wp$, ζ, σ fonctions de Weierstraß (cf. pp. 3, 123 et 126)

T_G, $\exp_G$, $G(\mathbb{C})$, $G(\mathbb{R})$, $G(\mathbb{R})^0$ (cf. pp. 4, 44 et 106)

G^* (sous-groupe associé, réseau dual) (cf. pp. 28–31)

$\mathrm{Mat}_{n\times m}(K)$ (espace de matrices de format $n \times m$ à coefficients dans K) (cf. p. 33)

$\widetilde{G}$ (cf. pp. 34, 89, 129)

$\mathrm{m}(G)$, $\mathrm{m}_{\mathbb{R}}(G)$, $\mathrm{m}'_{\mathbb{R}}(G)$ (cf. pp. 39, 70, 108 et 110)

$\mathcal{L}$, $\mathcal{L}(G)$, $\mathcal{L}_K(G)$, $\exp_{G,\mathbb{R}}$ (cf. pp. 45 et 108)

$\mathcal{T}_A$, χ_a (cf. p. 60–61)

$T_{K/k}$, $\mathrm{Res}_{K/k}$ (cf. pp. 91 et 130)

$\mathcal{G}_A$, $\widetilde{\Omega}_{\mathbb{R}}$, $\mathrm{m}_{\mathbb{C}}(\widetilde{G})$ (cf. pp. 91–92)

Ω_G, $\kappa_{\mathbb{C}}(G)$, $G(\mathbb{C})^0$, $\mathrm{m}_{\mathbb{C}}(G)$ (cf. p. 106)

$\alpha(G)$, $\Omega_{G,\mathbb{R}}$, $\kappa_{\mathbb{R}}(G)$ (cf. p. 107)

$G(K)_{\mathrm{tors}}$ (cf. p. 123)

$\eta_V(H)$, $\Psi_V(H)$, h (hauteur de Néron-Tate) (cf. pp. 137–138)

I. – Introduction à la lecture de l'article de Mazur

Dans ce premier chapitre, nous présentons les grandes lignes de l'article de Mazur [Maz 1992]. Pour énoncer la conjecture principale, nous commençons par quelques préliminaires de géométrie algébrique. Pour Mazur, une variété est un "schéma réduit de type fini sur un corps (en général $\mathbb{Q}$)". Pour nous, ce sera plus simplement une "variété quasi-projective". Nous en donnons la définition dans le premier paragraphe. On trouvera tous les détails dans le chapitre I de [H 1977].

§1. Variétés quasi-projectives

Soient k un corps et $n \geq 1$ un entier. L'*espace projectif* $\mathbb{P}_n(k)$ est l'espace des droites vectorielles de k^{n+1} ; un point $(x_0, \dots, x_n) \in k^{n+1}$, distinct de $(0, \dots, 0)$, définit une droite

$$\{(tx_0, \dots, tx_n);\ t \in k\} = (x_0 : \dots : x_n).$$

Quand $P \in k[X_0, \dots, X_n]$ est un polynôme homogène de degré d, on a

$$P(tx_0, \dots, tx_n) = t^d P(x_0, \dots, x_n),$$

et pour $(x_0, \dots, x_n) \in k^{n+1}$, la condition $P(x_0, \dots, x_n) = 0$ ne dépend que de la classe $(x_0 : \dots : x_n)$ de $(x_0, \dots, x_n)$ dans $\mathbb{P}_n(k)$; on dira que $(x_0 : \dots : x_n)$ *est un zéro de* P.

Un sous-ensemble de $\mathbb{P}_n(k)$ est un *ensemble algébrique* si c'est l'ensemble des zéros d'un idéal *homogène* de $k[X_0, \dots, X_n]$ (c'est-à-dire un idéal engendré par des polynômes homogènes). On définit une topologie sur $\mathbb{P}_n(k)$ en prenant comme fermés les ensembles algébriques : c'est la *topologie de Zariski.*

Un espace topologique Y est dit *irréductible* s'il est non vide et s'il n'est pas réunion de deux fermés propres.

Une *variété projective sur* k est un sous-ensemble algébrique irréductible de $\mathbb{P}_n(k)$. Une variété *quasi-projective* est un ouvert d'une variété projective.

Pour énoncer la conjecture de Mazur on a besoin de la notion de *variété lisse* : cela signifie que tous les points (géométriques, c'est-à-dire sur un corps algébriquement clos) de la variété V sont *non singuliers* : l'*anneau local* de V en ce point est un *anneau régulier.* Voici les définitions de ces termes (cf. [H 1977]).

Les fonctions *régulières* sur une variété V forment un anneau $\mathcal{O}(V)$; l'*anneau local* d'un point $P \in V(k)$ en V est l'anneau $\mathcal{O}_P$ des germes de fonctions régulières au voisinage

de P dans V ; son idéal maximal $\mathcal{M}_P$ consiste des germes de fonctions qui s'annulent au point P. L'anneau local $\mathcal{O}_P$ est *régulier* si sa *dimension* (de Krull : c'est le plus grand entier n tel qu'il existe une suite $\mathcal{P}_0 \subset \mathcal{P}_1 \subset \dots \subset \mathcal{P}_n$ d'idéaux premiers) est égale à la dimension du $\mathcal{O}_P/\mathcal{M}_P$-espace vectoriel $\mathcal{M}_P/\mathcal{M}_P^2$.

Exercice. Vérifier que la courbe d'équation affine $y^5 = x^3 + 6x^2y + 2xy^2$ *n'est pas régulière au point* $(0,0)$*. Tracer le graphe de cette courbe.*

Exemples.
1. L'espace projectif $\mathbb{P}_n(k)$ est une variété projective.
2. L'espace affine $\mathbb{A}_n$ est une sous-variété quasi-projective de $\mathbb{P}_n$:

$$\mathbb{A}_n(k) = \{(1 : x_1 : \dots : x_n);\ (x_1 : \dots : x_n) \in k^n\} \subset \mathbb{P}_n(k);$$

c'est le complémentaire du lieu des zéros du polynôme $X_0 \in k[X_0, \dots, X_n]$.
3. Si $P \in k[X_0, \dots, X_n]$ est un polynôme homogène non nul, l'ensemble $Z(P)$ de ses zéros dans $\mathbb{P}_n(k)$ est un ensemble algébrique, appelé *hypersurface de* $\mathbb{P}_n$. Si P est irréductible (ou même seulement une puissance d'un polynôme irréductible), alors $Z(P)$ est irréductible : c'est une variété algébrique.
4. Pour $k = \mathbb{Q}$ et $P(X_0, \dots, X_n) = X_0^2 + \dots + X_n^2$, on a $Z(P) = \emptyset$ dans $\mathbb{P}_n(\mathbb{Q})$. On est amené naturellement pour étudier la *géométrie* d'une variété à supposer le corps k algébriquement clos : par exemple $k = \mathbb{C}$, ou bien $k = \overline{\mathbb{Q}}$ (clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$: c'est le *corps des nombres algébriques*). Mais d'un autre côté on voudrait aussi étudier les points de la variété qui sont rationnels sur $\mathbb{Q}$ ou sur un corps de nombres, ou encore sur le corps $\mathbb{R}$ des nombres réels. On sera ainsi amené à considérer pour une même variété V (c'est-à dire pour un système d'équations données) les points de V dans différents corps k ; ceux-ci seront notés $V(k)$. Une propriété *géométrique* de V est une propriété des points de V rationnels sur un corps algébriquement clos. Une variété sur un corps k est dite *absolument irréductible* si elle est irréductible sur une clôture algébrique de k.
5. Le complémentaire de 0 dans $\mathbb{A}_1$ est une variété quasi-projective dont les points sur un corps k forment l'ensemble $k^\times = k \setminus \{0\}$; on peut aussi représenter le groupe multiplicatif $k^\times$ du corps k comme l'ensemble des points rationnels sur k de l'hypersurface affine H d'équation $X_1X_2 = 1$ dans $\mathbb{A}_2(k)$, grâce à l'isomorphisme

$$\begin{array}{ccc} k^\times & \to & H(k) \\ x & \mapsto & (x, 1/x) \end{array}$$

Sur k aussi bien que sur $k^\times$ on a une structure de groupe (additif dans le premier cas, multiplicatif dans le second). Le graphe de la loi de groupe est encore une variété :

$$\{(x, y, x+y);\ (x,y) \in k \times k\} \subset \mathbb{A}_3(k),$$

$$\{(x, y, xy);\ (x,y) \in k^\times \times k^\times\} \subset \mathbb{A}_3(k)$$

respectivement.

On obtient ainsi deux *groupes algébriques* notés $\mathbb{G}_\mathrm{a}$ et $\mathbb{G}_\mathrm{m}$ respectivement, avec $\mathbb{G}_\mathrm{a}(k) = k$ et $\mathbb{G}_\mathrm{m}(k) = k^\times$.

Définition. Un *groupe algébrique* sur un corps k est une variété quasi-projective, définie sur k, munie d'une structure de groupe, telle que le graphe de la loi de groupe soit une variété quasi-projective définie sur k.

Un autre exemple de groupe algébrique est donné par le groupe linéaire général GL_n. On définit de manière naturelle la notion de *sous-groupe algébrique* (qui est à la fois un sous-groupe et une sous-variété), et on dit qu'un groupe algébrique est *linéaire* s'il est isomorphe (comme groupe algébrique) à un sous-groupe fermé d'un groupe GL_n. Par exemple $\mathbb{G}_{\mathrm{a}}$ et $\mathbb{G}_{\mathrm{m}}$ sont deux groupes linéaires — pour le premier considérer le sous-groupe de GL_2 formé des matrices

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$

Tout produit de groupes algébriques linéaires en est encore un (car $\mathrm{GL}_n \times \mathrm{GL}_d$ est isomorphe à un sous-groupe algébrique de GL_{n+d}) ; en particulier un produit de copies de $\mathbb{G}_{\mathrm{a}}$ et de $\mathbb{G}_{\mathrm{m}}$ est un groupe linéaire.

Nous nous intéresserons principalement aux groupes algébriques commutatifs. On vérifie que tout groupe algébrique linéaire commutatif sur un corps algébriquement clos est isomorphe à un produit de copies de de $\mathbb{G}_{\mathrm{a}}$ et de copies de $\mathbb{G}_{\mathrm{m}}$:

$$\mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}.$$

Il existe des groupes algébriques commutatifs qui ne sont pas linéaires. L'exemple le plus simple est fourni par les *courbes elliptiques* (voir par exemple [Sil 1986]). On les étudiera sous la forme de Weierstraß :

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

où g_2 et g_3 sont deux éléments de k tels que le discriminant $\Delta = g_2^3 - 27g_3^2$ ne soit pas nul. Cette condition sur le discriminant signifie que la variété est lisse ; on le vérifie en utilisant le *critère jacobien* : si $f(T,X,Y) \in k[T,X,Y]$ désigne le polynôme $Y^2T - (4X^3 - g_2XT^2 - g_3T^3)$, alors la condition $\Delta \neq 0$ équivaut à dire que le système d'équations

$$f(t,x,y) = (\partial/\partial t)f(t,x,y) = (\partial/\partial x)f(t,x,y) = (\partial/\partial y)f(t,x,y) = 0$$

n'a pas de solution $(t : x : y) \in \mathbb{P}_2$.

Le corps k sera toujours de caractéristique nulle : ce sera souvent un corps de nombres. Alors le groupe $E(k)$, appelé *groupe de Mordell-Weil de E sur k*, est un $\mathbb{Z}$-module de type fini, donc isomorphe à $\mathbb{Z}^r \times E(k)_{\mathrm{tors}}$, avec $E(k)_{\mathrm{tors}}$ groupe fini. Le nombre r est le *rang* du groupe de Mordell-Weil de E sur k. Dire que $E(k)$ est infini revient à dire que son rang est ≥ 1.

On étudiera aussi les points réels ou complexes (si le corps k est plongé dans $\mathbb{R}$ ou $\mathbb{C}$ respectivement) de E. Quand $k = \mathbb{C}$, on définit une fonction méromorphe $\wp$ dans $\mathbb{C}$ telle que

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

qui admet pour groupe de périodes un réseau $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ de $\mathbb{C}$; les éléments de Ω sont aussi les pôles de $\wp$. Pour z_1 et z_2 dans $\mathbb{C}$, on a $\wp(z_1) = \wp(z_2)$ si et seulement si $z_1 - z_2 \in \Omega$. Ainsi l'application

$$\begin{array}{ccc} \mathbb{C} & \to & E(\mathbb{C}) \\ z & \mapsto & \big(1 : \wp(z) : \wp'(z)\big) \end{array}$$

qui envoie Ω sur $(0 : 0 : 1)$ induit un isomorphisme analytique entre le quotient $\mathbb{C}/\Omega$ et $E(\mathbb{C})$. On peut donc transporter la loi de groupe additif de $\mathbb{C}/\Omega$ en une loi de groupe sur $E(\mathbb{C})$ et on démontre que cette loi donne à E une structure de groupe algébrique commutatif défini sur le corps $k = \mathbb{Q}(g_2, g_3)$: la fonction $\wp$ vérifie un théorème d'addition algébrique dont nous reparlerons. Cette loi de groupe a une description géométrique simple : la courbe E est une cubique (définie par un polynôme de degré 3), et une droite de $\mathbb{P}_2(\mathbb{C})$ coupe la courbe en trois points ; alors trois éléments de $E(\mathbb{C})$ ont une somme nulle dans le groupe si et seulement s'ils sont alignés. Quand deux des points sont dans $E(k)$, le troisième l'est aussi car l'équation à résoudre pour trouver ses coordonnées est de degré 1. On retrouve le procédé de la corde et de la tangente décrit par Bachet de Méziriac qui a fournit à Fermat la traduction de certains travaux de Diophante d'Alexandrie.

Plus généralement, on définit une *variété abélienne* comme un groupe algébrique dont la variété sous-jacente est projective (un tel groupe algébrique est alors commutatif). Une variété abélienne est isomorphe au quotient de $\mathbb{C}^n$ (où n est la dimension de la variété) par un réseau (sous-groupe discret de rang $2n$).

Enfin il existe encore des groupes algébriques commutatifs qui ne sont pas des produits de copies de $\mathbb{G}_{\mathrm{a}}$, $\mathbb{G}_{\mathrm{m}}$ et de variétés abéliennes ; mais (théorème de Barsotti-Chevalley) on les obtient tous en prenant des extensions

$$0 \to \mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1} \to G \to A \to 0.$$

Les points complexes d'un groupe algébrique G commutatif sur $\mathbb{C}$ forment un *groupe de Lie complexe* ; *l'algèbre de Lie* de $G(\mathbb{C})$ est l'espace tangent à l'origine $T_G(\mathbb{C})$ de G sur $\mathbb{C}$; si d est la dimension de G, c'est un espace vectoriel sur $\mathbb{C}$ de dimension d ; on associe à $G(\mathbb{C})$ une *application exponentielle* qui est un homomorphisme analytique :

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

dont l'image est la composante neutre de l'origine $G(\mathbb{C})^0$ (donc $\exp_G$ est surjectif quand G est connexe). Le noyau de cette application est un sous-groupe discret de $T_G(\mathbb{C})$. Pour $G = \mathbb{G}_{\mathrm{a}}$, l'application exponentielle est l'identité $\mathbb{C} \to \mathbb{C}$; pour $\mathbb{G}_{\mathrm{m}}$, c'est l'application exponentielle usuelle $z \mapsto e^z$ de $\mathbb{C}$ sur $\mathbb{C}^\times$; pour une courbe elliptique E, l'application exponentielle $\mathbb{C} \to E(\mathbb{C})$ est donnée par $(1 : \wp : \wp')$.

Quand le groupe algébrique G est défini sur $\mathbb{R}$, ses points réels forment un groupe de Lie réel $G(\mathbb{R})$, l'algèbre de Lie $T_G(\mathbb{R})$ est un sous-$\mathbb{R}$-espace vectoriel de $T_G(\mathbb{C})$ de dimension $\dim G$, et $\exp_G : T_G(\mathbb{R}) \to G(\mathbb{R})$ est un homorphisme analytique de noyau $\Omega \cap T_G(\mathbb{R})$ et d'image la composante connexe de l'élément neutre $G(\mathbb{R})^0$ de $G(\mathbb{R})$.

Cette application exponentielle permettra de linéariser certains problèmes : pour étudier la densité de sous-groupes de $G(\mathbb{C})$ (ou de $G(\mathbb{R})$), on pourra se ramener à étudier la densité de certains sous-groupes de $\mathbb{C}^d$ (ou de $\mathbb{R}^d$).

§2. La conjecture de Mazur

Voici la conjecture 1 de [Maz 1992] :

Conjecture de Mazur. – *Soit V une variété lisse sur $\mathbb{Q}$ telle que $V(\mathbb{Q})$ soit Zariski dense dans V. Alors l'adhérence pour la topologie réelle de $V(\mathbb{Q})$ dans $V(\mathbb{R})$ est une réunion finie de composantes connexes de $V(\mathbb{R})$.*

L'hypothèse de lissité est nécessaire : pour le voir, on prend une variété V lisse sur $\mathbb{Q}$ telle que $V(\mathbb{R})$ ait deux composantes connexes, l'une sur laquelle les points rationnels sont denses, l'autre qui ne contient aucun point rationnel. On fait subir à cette variété une transformation birationnelle sur $\mathbb{Q}$ — qui conserve les points rationnels — de telle manière que l'image ne soit pas lisse. On peut s'arranger pour que la variété singulière ainsi construite ne vérifie pas la conclusion.

Un exemple explicite est le suivant : la variété de départ est la courbe elliptique sur $\mathbb{Q}$ d'équation $y^2 = x^3 + 6x^2 + 2x$; le lieu des points réels $E(\mathbb{R})$ a deux composantes connexes, l'une qui n'est pas bornée et sur laquelle les points rationnels sont denses (le point $(1,3)$ est d'ordre infini), l'autre bornée qui ne contient pas de point rationnel (cet exemple, dû à A. Bremner, m'a été signalé par D. Masser ; voir [NZM 1991] p. 294, fin du §5.7). On pose ensuite $X = xy$, $Y = y$; on obtient une courbe singulière $\mathcal{C}$ sur $\mathbb{Q}$, avec $\mathcal{C}(\mathbb{R})$ connexe, mais l'adhérence dans $\mathcal{C}(\mathbb{R})$ des points rationnels n'est pas $\mathcal{C}(\mathbb{R})$. En revanche, si on considère le complémentaire de $(0,0)$ dans $\mathcal{C}(\mathbb{R})$, on trouve 4 composantes connexes, et les points rationnels sont denses dans deux d'entre elles : ce n'est pas un contre exemple à la conjecture ! Une construction légèrement différente est proposée dans [Maz 1995] à partir de la surface de Swinnerton-Dyer :

$$x^2 + y^2 = (4\lambda - 7)(\lambda^2 - 2)$$

que l'on "pince" pour identifier les deux points $(x, y, \lambda) = (\pm\sqrt{2}, 1, 1)$. On obtient une surface singulière dont les points réels ont deux composantes connexes, l'une lisse où les points rationnels sont denses, l'autre ayant un seul point rationnel (singulier).

L'hypothèse suivante dans la conjecture de Mazur est que $V(\mathbb{Q})$ est Zariski dense dans V. Cela signifie que si un polynôme s'annule sur tous les points rationnels de V, alors il s'annule sur V tout entier. Quand V est une courbe, cette hypothèse signifie simplement que l'ensemble $V(\mathbb{Q})$ est infini. En dimension supérieure, on demande que $V(\mathbb{Q})$ ne soit pas contenu dans un sous-ensemble algébrique W de V distinct de V ; si c'était le cas, pour étudier la situation il suffirait d'appliquer la conjecture à chacune des composantes irréductibles de W (ou plus exactement au *lieu lisse* de chacune de ces composantes).

On considère ensuite l'adhérence de $V(\mathbb{Q})$ dans $V(\mathbb{R})$ pour la topologie réelle de $V(\mathbb{R})$ (qui est homéomorphe localement à un ouvert de $\mathbb{R}^d$, avec $d = \dim V$). La conclusion de la conjecture est que cette adhérence, qui est fermée par définition pour la topologie réelle, est aussi ouverte, donc est réunion de composantes connexes réelles.

Si $V(\mathbb{R})$ est connexe, la conclusion signifie que $V(\mathbb{Q})$ est dense pour la topologie réelle dans $V(\mathbb{R})$. Quand $V(\mathbb{R})$ n'est pas connexe, les points rationnels peuvent se trouver seulement dans certaines composantes, comme dans l'exemple ci-dessus de la courbe elliptique $y^2 = x^3 + 6x^2 + 2x$.

D'après la conjecture de Mazur, dès que $V(\mathbb{Q})$ est Zariski dense, quand $\mathcal{C}$ est une composante connexe de $V(\mathbb{R})$, alors $\mathcal{C} \cap V(\mathbb{Q})$ est soit vide, soit dense dans $\mathcal{C}$. C'est en ce sens que les points réels sont *contagieux* dans les composantes connexes.

La motivation initiale de cette conjecture est l'analogue du 10-ème problème de Hilbert (résolu par Matijasevic en 1972) pour des solutions rationnelles à des systèmes d'équations diophantiennes. Voir à ce sujet [Mat 1995].

Dixième problème de Hilbert. – *Décider si une équation diophantienne est résoluble. Etant donnée une équation diophantienne en un nombre quelconque d'inconnues avec des coefficients numériques entiers rationnels, décrire un procédé permettant de déterminer en un nombre fini d'opérations si l'équation est résoluble en entiers rationnels.*

Le lien avec ce qui précède se fait par l'intermédiaire de la conséquence suivante de la conjecture de Mazur : *si W est une variété définie sur $\mathbb{Q}$, l'adhérence pour la topologie réelle de $W(\mathbb{Q})$ dans $W(\mathbb{R})$ n'a qu'un nombre fini de composantes connexes.*

Ce dernier énoncé permettrait de démontrer que $\mathbb{Z}$ n'est pas "diophantien" au sens suivant : il n'existe pas de polynôme $P(T, X_1, \ldots, X_n) \in \mathbb{Q}[T, X_1, \ldots, X_n]$ tel que, pour $t \in \mathbb{R}$, on ait : *t est entier si et seulement s'il existe $(x_1, \ldots, x_n) \in \mathbb{Q}^n$ tel que* $P(t, x_1, \ldots, x_n) = 0$.

En effet, si un tel polynôme P existait, il définirait une hypersurface $W = Z(P)$ dans $\mathbb{A}_{n+1}$ dont la projection par le morphisme $\pi : \mathbb{A}_{n+1} \to \mathbb{A}_1$, qui envoie $(t, x_1, \ldots, x_n)$ sur t vérifierait

$$\pi\big(W(\mathbb{Q})\big) = \mathbb{Z} \subset \mathbb{Q} = \mathbb{A}_1(\mathbb{Q}),$$

et l'adhérence réelle $\overline{W}$ de $W(\mathbb{Q})$ dans $W(\mathbb{R})$ vérifierait $\pi(\overline{W}) = \mathbb{Z}$; donc $\overline{W}$ aurait une infinité de composantes connexes.

Pour plus de détails, voir [Maz 1995].

§3. Théorèmes d'approximation

Le *théorème d'approximation faible* d'Artin–Whaples (voir par exemple Bourbaki, *Algèbre commutative*, Chap. 6 §7, ou bien S. Lang [L 1993], Chap. 12 §1 th.1.2 p. 467) dit que si $|\cdot|_1, \ldots, |\cdot|_s$ sont des valeurs absolues non triviales sur un corps k, qui sont deux-à-deux indépendantes, l'image de k par le plongement diagonal dans $\prod_{1 \le i \le s}(k, |\cdot|_i)$ est partout dense : *pour tout $\epsilon > 0$ et tout $(x_1, \ldots, x_s) \in k^s$ il existe $x \in k$ tel que*

$$|x - x_i|_i < \epsilon \qquad \textit{pour } 1 \le i \le s.$$

Le qualificatif "faible" est donné en comparaison avec l'énoncé suivant (cité seulement pour mémoire : nous ne l'utiliserons pas), appelé *théorème d'approximation forte* (voir Cassels et Fröhlich, *Algebraic Number Theory*, Chap. 2, §15 p.67, et O.T. O'Meara, *Introduction to Quadratic Forms*, §36 G) :

Soit k un corps de nombres ; soit S un ensemble fini de places de k, et soit $v_0 \notin S$ une autre place de k. Pour chaque $v \in S$, soit x_v un élément du complété de k en v. Enfin soit $\epsilon > 0$. Alors il existe $\alpha \in k^\times$ tel que

$$|\alpha - x_v|_v < \epsilon \qquad \textit{pour tout } v \in S$$

et

$$|\alpha|_v \le 1 \qquad \textit{pour tout } v \notin S,\ v \neq v_0.$$

Exercice. Soient x un nombre réel, $p_1, \dots, p_m$ des nombres premiers deux-à-deux distincts, $s_1, \dots, s_m$ des entiers positifs, $a_1, \dots, a_m$ des entiers rationnels, et ϵ un nombre réel positif.
a) Montrer qu'il existe deux nombres entiers non nuls u et v, premiers entre eux, tels que

$$\left| x - \frac{u}{v} \right| < \epsilon \qquad \textit{et} \qquad u \equiv a_i v \pmod{p_i^{s_i}} \quad \textit{pour } 1 \le i \le m.$$

b) Montrer qu'il existe deux entiers $n \ge 0$ et u tels que

$$\left| x - \frac{u}{p_1^n} \right| < \epsilon \qquad \textit{et} \qquad u \equiv a_i p_1^n \pmod{p_i^{s_i}} \quad \textit{pour } 2 \le i \le m.$$

Les définitions suivantes concernent une variété X lisse sur un corps de nombres k.

Définitions.

1. On dit que X *possède la propriété d'approximation faible* sur k si le plongement diagonal

$$X(k) \to \prod_v X(k_v)$$

a une image dense (dans le produit, v décrit toutes les places de k).

Par exemple, si X est une variété affine plongée dans $\mathbb{A}_n$, et si, pour $u = (u_1, \dots, u_n) \in k_v^n$, on note $|u|_v = \max_{1 \le i \le n} |u_i|_v$, alors, par définition de la topologie sur $\prod_v X(k_v)$, dire que X possède la propriété d'approximation faible sur k signifie que pour tout ensemble *fini* S de places de k, pour toute famille $(x_v)_{v \in S}$ avec $x_v \in X(k_v)$ pour tout $v \in S$, et pour tout $\epsilon > 0$, il existe $x \in X(k)$ tel que

$$|x - x_v|_v < \epsilon \qquad \text{pour tout } v \in S.$$

Ainsi la droite affine possède la propriété d'approximation faible, d'après le théorème d'Artin–Whapples.

2. La variété X *possède la propriété d'approximation très faible* sur k s'il existe un ensemble fini T de places de k tel que, pour tout ensemble fini S de places de k avec $S \cap T = \emptyset$, l'image du plongement diagonal

$$X(k) \to \prod_{v \in S} X(k_v)$$

est dense.

Il est clair que si une variété lisse X sur k possède la propriété d'approximation faible, alors X possède la propriété d'approximation très faible (prendre $T = \emptyset$).

3. Soit S un ensemble fini de places de k. On dit que *la variété X est S-ouverte* si l'adhérence de l'image de $X(k) \to \prod_{v \in S} X(k_v)$ est un ouvert de $\prod_{v \in S} X(k_v)$.

Si une variété lisse X sur k possède la propriété d'approximation faible, alors X est S-ouverte pour tout ensemble fini non vide S disjoint de T.

Quand on prend $k = \mathbb{Q}$ et que S ne contient que la place archimédienne de $\mathbb{Q}$, la condition que la variété X est S-ouverte signifie que $X(\mathbb{Q})$ est ouvert dans $X(\mathbb{R})$: c'est la conclusion de la conjecture de Mazur.

Ces propriétés d'approximation sont étroitement liées au "principe de Hasse" : une k-variété X *satisfait le principe de Hasse* si l'existence d'un point de X rationnel sur chaque complété k_v de k implique l'existence d'un point de X rationnel sur k (voir à ce sujet [CT 1992]).

§4. Exemples

Voici quelques-uns des exemples proposés par Mazur dans [Maz 1992].

a) *Courbes.*

La conjecture de Mazur est vraie pour les courbes lisses sur $\mathbb{Q}$. Pour le démontrer, on distingue trois cas :

1. La courbe est de genre 0. Si la courbe n'a pas de points rationnels, la question ne se pose pas : les hypothèses de la conjecture de Mazur ne sont pas vérifiées. S'il y a point rationnel, le fait que le genre soit nul permet de se ramener à la droite projective $\mathbb{P}_1$ par une transformation birationnelle (une courbe de genre zéro est une courbe *rationelle*, encore appelée *unicursale*, i.e. que l'on peut "paramétrer" par des fractions rationnelles), et la densité est alors évidente.

2. Le genre de la courbe est 1. Si la courbe n'a pas de point rationnel, l'hypothèse de la conjecture n'est pas vérifiée. Si elle a un point rationnel, grâce au théorème de Riemann-Roch on montre que le choix d'un tel point permet de lui donner une structure de courbe elliptique. L'application exponentielle complexe induit un isomorphisme entre les points complexes $E(\mathbb{C})$ d'une courbe elliptique E et un tore $\mathbb{C}/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2)$; on en déduit un isomorphisme entre $E(\mathbb{R})$ et un tore $\mathbb{R}/\mathbb{Z}\omega$, qui est un groupe de Lie réel compact de dimension 1. On utilise alors un théorème d'approximation (Tchebychef-Kronecker) pour conclure. Les détails seront donnés dans le cours.

Il ne faudrait pas croire d'ailleurs que cela répond à toutes les questions que soulève le problème de la densité de $E(\mathbb{Q})$ dans $E(\mathbb{R})$. On s'interrogera sur l'approximation d'un élément de $E(\mathbb{R})$ par un élément de $E(\mathbb{Q})$, en utilisant des mesures de transcendance pour le quotient d'intégrales elliptiques (on rapprochera cette question de la discussion dans la section "Heights, measures and dynamics" de [Maz 1995]). On étudiera aussi l'adhérence de $E(k)$ dans $E(\mathbb{C})$ quand k est un corps de nombres plongé dans $\mathbb{C}$.

3. Sur une courbe de genre ≥ 2, un théorème de Faltings (anciennement *conjecture de Mordell* – voir par exemple [L 1991]) dit qu'il n'y a qu'un nombre fini de points rationnels sur $\mathbb{Q}$. Les hypothèses ne sont alors pas vérifiées.

b) *Fibrés en coniques sur* $\mathbb{P}_1$

On considère ici des "familles" de courbes paramétrées par une variable $\lambda \in \mathbb{P}_1(\mathbb{Q})$. Pour chaque λ, la courbe d'indice λ est une conique, et la variation en λ est polynomiale. Nous avons déjà mentionné l'exemple de Swinnerton-Dyer (1962) :

$$x^2 + y^2 = (4\lambda - 7)(\lambda^2 - 2);$$

le lieu réel a deux composantes connexes, et les points rationnels sont tous situés sur une de ces composantes, où ils sont denses.

Un exemple plus récent est celui de L. Wang : la surface

$$x^2 + y^2 = (4\lambda - 7)(\lambda^2 - 2)(2\lambda^2 - 3)$$

a trois composantes connexes réelles, une seule contient des points rationnels.

Les travaux de Colliot-Thélène, Salberger, Sansuc, Skorobogatov, Swinnerton-Dyer... permettent d'établir la conjecture de Mazur pour de telles surfaces ayant ≤ 5 fibres dégénérées (i.e. au plus 5 "mauvaises" valeurs de λ), ainsi que pour les surfaces cubiques lisses qui contiennent une droite rationnelle sur $\mathbb{Q}$, et aussi pour les intersections lisses de deux quadriques dans $\mathbb{P}_4$.

Colliot-Thélène et Sansuc ont fait intervenir dans ce contexte l'hypothèse (H) de Schinzel en liaison avec les variétés définies par des équations de la forme

$$Q_i(X_{i1}, \ldots, X_{in_i}) = P_i(\lambda_1, \ldots, \lambda_n), \qquad (1 \leq i \leq r),$$

où $Q_1, \ldots, Q_r$ sont des formes quadratiques en $n_1 + \cdots + n_r$ variables, chacune de rang ≥ 2, et les P_i appartiennent à $\mathbb{Q}(\lambda_1, \ldots, \lambda_n)$.

Hypothèse (H). – *Soient $f_1, \ldots, f_s$ (avec $s \geq 1$) des polynômes irréductibles de $\mathbb{Z}[X]$ dont le coefficient du terme de plus haut degré est > 0. On suppose qu'il n'existe pas d'entier $n > 1$ qui divise tous les nombres*

$$f_1(k) \cdots f_s(k), \qquad (k \in \mathbb{Z}).$$

Alors il existe $m \in \mathbb{N}$ tel que les s nombres $f_1(m), \ldots, f_s(m)$ soient premiers.

Si cette hypothèse (H) est vraie, alors sous les mêmes hypothèses il existe *une infinité* d'entiers $m \in \mathbb{N}$ tel que les s nombres $f_1(m), \ldots, f_s(m)$ soient premiers (remplacer X par $X + m + 1$). Voir à ce sujet [S-S 1958].

Dans leur article, Schinzel et Sierpinski démontrent que l'hypothèse (H) implique l'existence d'une infinité de nombres pseudo-premiers de Carmichael(*), et aussi que, pour tout $a \in \mathbb{Z}$, $|a| > 1$ sans facteurs carrés, il existe une infinité de nombres premiers p tels que a soit racine primitive modulo p (la classe de a modulo p est un générateur du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^\times$). De nombreuses autres conséquences de cette hypothèse (H) sont connues.

(*) Un entier $n > 1$ est appelé *pseudo-premier*, ou encore *nombre de Carmichael*, si pour tout entier a premier à n on a $a^{n-1} \equiv 1 \pmod{n}$; c'est seulement en 1992 que Alford, Granville et Pomerance ont montré qu'il existait une infinité de tels entiers qui ne sont pas premiers ; voir [Ri 1994].

c) *Hypersurfaces cubiques lisses*

Swinnerton-Dyer a montré qu'une hypersurface cubique X dans $\mathbb{P}_N$ avec $N \geq 3$ (c'est le lieu des zéros d'un polynôme homogène de degré 3), supposée lisse, est S-ouverte pour tout ensemble fini S de places de k ; en particulier elle vérifie la conjecture de Mazur. Un schéma de démonstration est donné dans [Maz 1992].

d) *Intersection complète de deux quadriques*

D'après Colliot-Thélène et Sansuc, si P_1 et P_2 sont deux polynômes homogènes de degré 2 en $N \geq 6$ variables à coefficients dans $\mathbb{Q}$, et si $X = Z(P_1) \cap Z(P_2)$ est une *intersection complète* (l'idéal (P_1, P_2) est de codimension 2 dans $\mathbb{Q}[X_0, \ldots, X_N]$), pure, géométriquement intègre et non conique, qui possède un point rationnel non singulier, alors X possède la propriété d'approximation faible, donc vérifie aussi la conjecture de Mazur.

e) *Surfaces elliptiques*

L'exemple suivant qu'étudie Mazur est celui d'une famille $(E_t)_{t \in \mathbb{P}_1(\mathbb{Q})}$ de courbes elliptiques : pour tout $t \in \mathbb{P}_1(\mathbb{C})$ sauf au plus un nombre fini, E_t est une courbe elliptique. Par exemple si g_2 et g_3 sont deux éléments de $\mathbb{Q}(t)$ tels que la fraction rationnelle $g_2^3 - 27g_3^2$ ne soit pas identiquement nulle, alors

$$y^2 = 4x^3 - g_2(t)x - g_3(t)$$

définit une courbe elliptique E_t pour tout t qui n'est ni pôle de g_2 ou g_3, ni zéro de $g_2^3 - 27g_3^2$. L'équation écrite est celle de la partie affine de E_t : on devrait écrire g_2 et g_3 comme quotients de deux polynômes homogènes G_2/D et G_3/D respectivement, et écrire dans $\mathbb{P}_4$

$$y^2 D(t) z^{a+1} = 4x^3 D(t) z^a - G_2(t) x z^b - G_3(t) z^c$$

avec a, b, c choisis pour que l'équation soit homogène ($a + \deg D + 3 = b + \deg G_2 + 1 = c + \deg G_3$).

Considérons par exemple la famille de courbes elliptiques

$$(E_t) \qquad y^2 = x^3 + tx.$$

Pour $t = 0$ la courbe E_0 n'est pas lisse ; pour toutes les autres valeurs de t c'est une courbe elliptique, ayant une composante connexe si $t < 0$, deux si $t > 0$. Pour $t = 7$ ou encore $t = -1$, le groupe $E_t(\mathbb{Q})$ est fini, tandis que pour $t = 877$ par exemple, $E(\mathbb{Q})$ est dense dans $E(\mathbb{R})$.

Définition. Une *surface elliptique* ou *fibration elliptique* S sur $\mathbb{Q}$ est une variété de dimension 2 sur $\mathbb{Q}$, munie d'un morphisme $\varphi : S \to \mathbb{P}_1$ sur $\mathbb{Q}$, tel que, pour tout $t \in \mathbb{P}_1(\mathbb{C})$ en dehors d'un ensemble fini, la *fibre* $E_t = \varphi^{-1}(t)$ soit une courbe elliptique définie sur $\mathbb{Q}(t)$.

Chacune des courbes elliptiques E_t possède une origine $\mathcal{O}_t \in E_t$, et on a évidemment $\varphi(\mathcal{O}_t) = t$ pour t dans l'ouvert de Zariski où E_t est une courbe elliptique. On définit une application rationnelle $\pi : \mathbb{P}_1 \to S$ par $\pi(t) = \mathcal{O}_t$ qui est une *section* de φ, c'est-à-dire vérifie $\varphi \circ \pi = I$.

Une fibration sur $\mathbb{Q}$ est *triviale* si toutes les courbes E_t sont isomorphes sur $\mathbb{Q}$.

Soit S une surface elliptique sur $\mathbb{Q}$. Désignons par $\mathcal{T}$ l'ensemble des $t \in \mathbb{P}_1(\mathbb{Q})$ tels que $E_t = \varphi^{-1}(t)$ soit une courbe elliptique et que le groupe $E_t(\mathbb{Q})$ soit infini (c'est-à-dire tels que le rang du groupe de Mordell-Weil de E_t sur $\mathbb{Q}$ soit ≥ 1).

Lemme. *–Soit S une surface elliptique sur $\mathbb{Q}$. Si l'ensemble $\mathcal{T}$ est fini, alors $S(\mathbb{Q})$ n'est pas Zariski-dense dans S.*

Démonstration. On suppose S plongée comme sous-variété quasi-projective de $\mathbb{P}_N$. Si $E_t(\mathbb{Q})$ est un ensemble fini en dehors de $\{t_1, \ldots, t_n\}$, on veut montrer que $S(\mathbb{Q})$ n'est pas dense. On utilise pour cela un théorème de Mazur [Maz 1978] : *un point de torsion d'une courbe elliptique sur $\mathbb{Q}$ est d'ordre ≤ 16* (*). Alors il existe un polynôme $P \in \mathbb{Q}[T, X_0, \ldots, X_N]$, tel que $P(t, X)$ s'annule sur $E_t(\mathbb{Q})$ pour $t \notin \{t_1, \ldots, t_n\}$. En multipliant par $(T-t_1)\cdots(T-t_n)$ on obtient un polynôme $Q \in \mathbb{Q}[T, X_0, \ldots, X_N]$, tel que $Q(\varphi(X), X)$ s'annule sur $S(\mathbb{Q})$ mais pas sur S. □

Proposition. *– Si la conjecture de Mazur est vraie pour la surface elliptique lisse S sur $\mathbb{Q}$, alors l'ensemble $\mathcal{T}$ est soit fini, soit dense dans $\mathbb{R}$.*

Démonstration. Supposons que $\mathcal{T}$ soit infini. Soit X l'adhérence réelle de $S(\mathbb{Q})$. D'après la conjecture de Mazur, X est une réunion de composantes de $S(\mathbb{R})$. Soit $S(\mathbb{R})^0$ la composante connexe qui contient l'image $\{\mathcal{O}_t;\ t \in \mathbb{P}_1\}$ de la section π considérée plus haut. Pour tout $t \in \mathbb{P}_1(\mathbb{R})$ en dehors d'un ensemble fini, $\mathcal{O}_t \in S(\mathbb{R})^0$. Comme X contient ces $\mathcal{O}_t$, X contient $S(\mathbb{R})^0$. Alors les points rationnels de S sont denses dans $S(\mathbb{R})^0$, et par conséquent ils se projettent sur un ensemble dense de $\mathbb{P}_1(\mathbb{R})$. □

On ne connait pas d'exemple de fibration non triviale où l'ensemble $\mathcal{T}$ soit fini. D'autre part Tate et Silverman ont montré que le rang de $E_t(\mathbb{Q})$ ne peut chuter qu'en un nombre fini de $t \in \mathbb{P}_1(\mathbb{Q})$.

Un cas particulier a été spécialement étudié : on fixe un polynôme $g \in \mathbb{Q}[X]$ de degré 3 et de discriminant non nul (i.e. ayant trois racines distinctes dans $\mathbb{C}$), et on considère la surface

$$(E_t) \qquad y^2 D(t) = g(x);$$

la courbe E_t est appelée “tordue quadratique” (“quadratic twist”) de la courbe $y^2 = g(x)$. Pour plus de renseignements sur ce sujet, voir [Ro 1993], [K-W 1993] et [Maz 1995].

(*) Une généralisation de cet énoncé aux corps de nombres a été obtenue par Loïc Merel : Bornes pour la torsion des courbes elliptiques sur les corps de nombres. Invent. Math. **124** (1996), no. 1-3, 437–449. `Zbl 960.24063` `MR 96i:11057`

f) *Variétés abéliennes*

L'étude de la conjecture de Mazur pour les variétés abéliennes sera le thème central de ce cours. Plus généralement nous considérerons un groupe algébrique G commutatif défini sur un corps de nombres k. Au lieu de prendre le groupe de tous les points rationnels $G(k)$, nous en prendrons un sous-groupe de type fini (pour une variété abélienne A, le groupe $A(k)$ est de type fini d'après le théorème de Mordell-Weil). Nous étudierons en premier lieu les groupes linéaires, en liaison avec la conjecture d'indépendance algébrique de logarithmes de nombres algébriques, puis les courbes elliptiques, ensuite les variétés abéliennes, enfin le cas général. Nous admettrons les théorèmes de transcendance qui seront nécessaires, mais nous montrons précisément comment ils s'appliquent. Les méthodes transcendantes nécessitent “beaucoup” de points rationnels : on demande que le rang du groupe de Mordell-Weil de $A(k)$ soit $\geq d^2 - d + 1$, où d est la dimension de A. La question reste ouverte pour les petits rangs. Un exemple de surface abélienne ($d = 2$) ayant un groupe de Mordell-Weil de rang 1 est la *Jacobienne* de la courbe

$$y^2 = x(x-1)(x-2)(x-5)(x-6);$$

cf [G-G 1993]. D'autres exemples de “petits” rangs ($0 < r < d$) dus à W. McCallum, concernent les jacobiennes des courbes

$$y^\ell = x^s(x-1);$$

voir [Maz 1995]. La conjecture de Mazur pour les variétés abéliennes a aussi été étudiée par L. Wang dans [Wa 1995].

g) *Surfaces de Kummer et surfaces $K3$*

La fin de l'article [Maz 1992] décrit d'autres surfaces pour lesquelles des réponses partielles sont connues. Il est intéressant de noter que ces surfaces ont “beaucoup” d'automorphismes.

Voici un exemple de surface de Kummer. On part de deux courbes elliptiques

$$(E_1) : \qquad y^2 = x^3 + ax + b \qquad \text{et} \qquad (E_2) : \qquad y^2 = x^3 + cx + d.$$

On considère ensuite la surface X d'équation

$$(t^3 + ct + d)y^2 = x^3 + ax + b.$$

L'application $\big((x_1, y_1); (x_2, y_2)\big) \mapsto (x_1, y_1/y_2, x_2)$ définit un morphisme surjectif de $E_1 \times E_2$ sur X : tout $(x, y, t) \in X$ a deux antécédents ; si l'un est $\big((x_1, y_1); (x_2, y_2)\big)$, l'autre est $\big((x_1, -y_1); (x_2, -y_2)\big)$. Le changement de signe de y sur une courbe elliptique est l'opposé pour la loi d'addition, correspondant au morphisme $-I$ (où I est l'identité). C'est pourquoi on écrit que X est le quotient de $E_1 \times E_2$ par $\{\pm I\}$.

La conjecture de Mazur pour ces surfaces a fait l'objet de plusieurs études, notamment par Masato Kuwata et L. Wang [K-W 1993], [Wa 1994].

En 1997, Colliot-Thélène, Skorobogatov et Swinnerton-Dyer [CSS 1997] ont construit un contre-exemple à la conjecture initiale de Mazur, et en ont proposé des modifications, notamment la suivante : *Soit V une variété lisse sur $\mathbb{Q}$ et soit U une composante connexe de $V(\mathbb{R})$. On suppose que $V(\mathbb{Q}) \cap U$ est Zariski dense dans V. Alors $V(\mathbb{Q}) \cap U$ est dense dans U pour la topologie réelle.*

§5. Une conjecture de Pierre Dèbes.

La fin de ce chapitre est rédigée par Pierre Dèbes.

UNE CONJECTURE GÉNÉRALISANT CELLE DE MAZUR.

On note $G(\mathbb{Q}) = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ le groupe de Galois absolu de $\mathbb{Q}$.

CONJECTURE :

DONNÉES : Soit $f : V \to W$ un morphisme étale défini sur $\mathbb{Q}$ entre deux variétés lisses et irréductibles. Soit $d \geq 1$ un entier.

NOTATION : (1) L'ensemble des points $w \in W(\mathbb{Q})$ tels que $f^{-1}(w)$ contient un ensemble de cardinal d invariant sous $G(\mathbb{Q})$ est noté A_d.

(2) L'ensemble des points $w \in W(\mathbb{R})$ tels que $f^{-1}(w)$ contient au moins d points réels est noté B_d.

HYPOTHÈSE : On suppose que A_d est Zariski dense dans W.

CONCLUSION : Soit $\mathcal{C}$ une composante connexe de B_d. Alors l'ensemble des points $w \in \mathcal{C} \cap W(\mathbb{Q})$ tels que la fibre $f^{-1}(w)$ contient un ensemble de cardinal d, constitué de points réels et invariant sous $G(\mathbb{Q})$ (et donc constitué de points totalement réels de degré $\leq d$), est, soit vide, soit dense dans $\mathcal{C}$ (pour la topologie réelle).

Remarques : (1) Cet énoncé contient la conjecture de Mazur : prendre $V = W$, $f = Id$ et $d = 1$.

(2) Cet énoncé est vrai pour $d = deg(f)$ si la variété W vérifie la conjecture de Mazur, en particulier si $W(\mathbb{Q})$ est dense dans toute composante connexe de $W(\mathbb{R})$ (*e.g.* W rationnelle).

Preuve. Pour $d = deg(f)$, on a $A_d = W(\mathbb{Q})$ et B_d est l'ensemble des points $w \in W(\mathbb{R})$ dont tous les points de la fibre sont réels. Soit $\mathcal{C}$ une composante connexe de B_d. Par hypothèse, $A_d = W(\mathbb{Q})$ est Zariski-dense. Donc d'après la conjecture de Mazur, $\mathcal{C}$ est contenu dans l'adhérence (réelle) de $W(\mathbb{Q})$. Mais comme B_d est ouvert, tout point w de $W(\mathbb{Q})$ suffisamment proche d'un point de $\mathcal{C}$ est automatiquement dans $\mathcal{C}$. La fibre au dessus d'un tel w est constituée de points réels et est invariante sous $G(\mathbb{Q})$.

(3) On peut voir un lien entre la conjecture de Mazur (et sa généralisation) et le théorème de Florian Pop([1]) qui affirme que "les points totalement réels d'une variété lisse et irréductible définie sur $\mathbb{Q}$ sont denses dans les points réels". L'argument est essentiellement le suivant.

([1]) Pop, Florian. – Fields of totally Σ-adic numbers, preprint, Heidelberg, 1992 ; voir aussi : B. Green, F. Pop and P. Roquette, On Rumely's local-global principle, Jahresber. Deutsch. Math.-Verein. **97** (1995), no. 2, 43–74. `Zbl 857.11033` `MR 96g:11065`

Soit $\mathcal{C}$ une courbe (il y a un argument qui permet de se ramener à ce cas) définie sur $\mathbb{Q}$ et U un ouvert non vide de $\mathcal{C}(\mathbb{R})$. On se donne aussi un diviseur $\mathbb{Q}$-rationnel D_∞ de la courbe. La premère étape consiste à construire une fonction $f \in \mathbb{R}(\mathcal{C})$ telle que

$$(*) \qquad \begin{cases} (f)_\infty \text{ soit un multiple } kD_\infty \text{ de } D_\infty \\ (f)_0 \text{ ne consiste qu'en des points réels contenus dans } U \end{cases}$$

Notons $\{u_1, \ldots, u_m\}$ une base de $L_{\mathbb{Q}}(kD_\infty)$. La fonction f s'écrit

$$f = \sum_{i=1}^{m} \alpha_i u_i \qquad (\alpha_1, \ldots, \alpha_m \in \mathbb{R})$$

Ensuite, d'après un "lemme de continuité des racines", il existe un voisinage $\mathcal{O}$ de $(\alpha_1, \ldots, \alpha_m)$ dans $\mathbb{R}^m$ tel que si $\mathbf{a} = (a_1, \ldots, a_m) \in \mathcal{O}$ alors la fonction

$$f_{\mathbf{a}} = \sum_{i=1}^{m} a_i u_i$$

vérifie aussi les conditions (*). Si on choisit $\mathbf{a} \in \mathbb{Q}^m$, la fonction $f_{\mathbf{a}}$ est définie sur $\mathbb{Q}$. Ses zéros sont réels et permutés par $G(\mathbb{Q})$ et donc sont totalement réels.

En gros, l'idée est la même que dans la remarque (2) : déformer légèrement une fonction qui n'a que des zéros réels de façon à ce qu'elle soit définie sur $\mathbb{Q}$.

(4) Le résultat de Pop nous a permis([2]), à M.Fried et moi, de démontrer le problème inverse de Galois sur $\mathbb{Q}^{tr}(T)$

[et aussi sur $\mathbb{Q}^{tp}(T)$ ($\mathbb{Q}^{tp}$ désigne le corps des totalement p-adiques) car le résultat de Pop est vrai aussi en p-adiques.]

Mon but ensuite était de montrer que tout groupe est groupe de Galois d'un revêtement de $\mathbb{P}^1$ défini sur $\mathbb{Q}^{tr}$, avec la condition supplémentaire que les points de ramification soient rationnels (globalement). Cela se ramène en gros à trouver des points totalement réels sur une variété V avec la condition supplémentaire que l'image de ces points par un certain morphisme $f : V \to W$ doit être $\mathbb{Q}$-rationnelle sur W. C'est le sens la conjecture que je fais ici, qui est aussi assez similaire à une conjecture que j'avais énoncée précédemment dans une note au CRAS([3]) dans le cadre plus restreint des espaces de Hurwitz.

([2]) Dèbes, Pierre ; Fried, Michael D. – Nonrigid constructions in Galois theory. Pacific J. Math. **163** (1994), no. 1, 81–122. `Zbl 788.12001` `MR 95c:12008.`

([3]) Dèbes, Pierre. – Critères de descente pour le corps de définition des G-revêtements de $\mathbb{P}^1$. C. R. Acad. Sci. Paris Sér. **I** Math. **315** (1992), no. 8, 863–868. `Zbl 761.12001` `MR 93m:12003.`

II. – Sous-groupes de $\mathbb{R}^n$

Le but de ce chapitre est de donner des critères pour qu'un sous-groupe d'un groupe de Lie réel ou complexe soit dense. Le cas fondamental est celui d'un sous-groupe de $\mathbb{R}^n$, où la réponse est obtenue grâce à un théorème de Kronecker (théorème 4.1).

Voici quelques indications bibliographiques concernant ce chapitre. Pour l'aspect qualitatif, voir [Bo 1974] Chap. 7. Une autre référence de base est [H-W 1979] (en particulier le chapitre XXIII pour le théorème de Kronecker, mais aussi le chapitre III pour les suites de Farey, ainsi que le chapitre XI pour l'approximation de nombres irrationnels par des nombres rationnels ; il faut noter cependant que certains arguments peuvent être simplifiés en utilisant un minimum de langage algébrique). Deux autres références fondamentales pour tout ce qui concerne les approximations diophantiennes sont [Ca 1957]et [Sc 1980].

Dans la rédaction qui suit, nous ne donnons des démonstrations que pour les énoncés qui seront utilisés dans la suite du cours.

On utilisera la notion de *groupe topologique* (voir [D 1972], t.1, Chap. 12 §8). D'autre part on utilisera plusieurs notions de rang. Le *rang d'un groupe abélien* est le nombre minimal d'éléments d'un système générateur de ce groupe. Le *rang rationnel d'un $\mathbb{Z}$-module* G, appelé encore *rang de* G *sur* $\mathbb{Z}$ ou *sur* $\mathbb{Q}$, est le nombre maximal d'éléments de G linéairement indépendants sur $\mathbb{Q}$; on le notera $\mathrm{rang}_{\mathbb{Z}} G$. Rappelons le théorème de structure des $\mathbb{Z}$-modules de type fini : si G est un $\mathbb{Z}$-module de type fini, le sous-groupe de torsion G_{tors} de G est un groupe fini, le quotient G/G_{tors} est un $\mathbb{Z}$-module libre, isomorphe à $\mathbb{Z}^r$, où r est le rang de G sur $\mathbb{Z}$, et G est isomorphe au produit direct $G_{\mathrm{tors}} \times \mathbb{Z}^r$. En particulier pour un $\mathbb{Z}$-module libre (i.e. sans torsion) le rang comme groupe abélien coïncide avec le rang comme $\mathbb{Z}$-module.

On va travailler avec des sous-groupes de $\mathbb{R}^n$. La dimension de l'espace vectoriel sur $\mathbb{R}$ engendré par un tel sous-groupe G sera appelée le *rang réel de* G ; noter que la dimension de l'espace vectoriel sur $\mathbb{Q}$ engendré par un tel sous-groupe G n'est autre que le rang rationnel du $\mathbb{Z}$-module G.

Remarquons enfin que quand G et H sont deux sous-groupes de $\mathbb{R}^n$ avec H d'indice fini dans G, alors G est dense dans $\mathbb{R}^n$ si et seulement si H est dense dans $\mathbb{R}^n$.

§1. Sous-groupes de $\mathbb{R}$

Comme le groupe $\mathbb{R}$ est sans torsion, tout sous-groupe G de type fini de $\mathbb{R}^n$ est libre : il admet une base $g_1, \dots, g_\ell$:

$$G = \mathbb{Z}g_1 + \cdots + \mathbb{Z}g_\ell,$$

où $g_1, \dots, g_\ell$ sont des éléments de G linéairement indépendants sur $\mathbb{Z}$. Il s'agit de déterminer si un tel sous-groupe est dense dans $\mathbb{R}^n$. Dans cette section nous nous restreignons au cas $n = 1$.

Soient $g_1, \dots, g_\ell$ des nombres réels linéairement indépendants sur $\mathbb{Z}$. Il est clair que, si $\ell = 1$, le sous groupe G qu'ils engendrent est discret dans $\mathbb{R}$. Nous allons voir inversement que si $\ell > 1$, alors G est dense dans $\mathbb{R}$. En prenant g_1 comme base de $\mathbb{R}$ et en posant $\theta = g_2/g_1$, le résultat que nous nous proposons d'établir s'énonce de la manière suivante (voir [H-W 1979] Th. 438 ; [Bo 1974] Chap. 5 §1 n°1 prop. 1) :

Théorème 1.1 (Tchebychef). – *Soit θ un nombre réel irrationnel. Alors le sous-groupe $\mathbb{Z} + \mathbb{Z}\theta$ de $\mathbb{R}$ est dense dans $\mathbb{R}$.*

Ainsi un sous-groupe de type fini de $\mathbb{R}$ est dense dans $\mathbb{R}$ si et seulement si son rang sur $\mathbb{Z}$ est ≥ 2. L'hypothèse que le groupe est de type fini est évidemment nécessaire : $\mathbb{Q}$ est dense dans $\mathbb{R}$, et de rang 1 sur $\mathbb{Z}$ (mais de rang infini comme groupe abélien). Cela donne une classification simple des sous-groupes de type fini de $\mathbb{R}$: ou bien ils sont discrets de la forme $\mathbb{Z}x$, pour un x dans $\mathbb{R}$, ou bien ils sont partout denses dans $\mathbb{R}$. Cependant ce critère n'est pas toujours "effectif" ; par exemple on ne sait pas si le sous-groupe $\mathbb{Z} + \mathbb{Z}\gamma$ (où γ est la constante d'Euler) est dense ou non dans $\mathbb{R}$. Il en est de même pour $\mathbb{Z}e + \mathbb{Z}\pi$. Dans le même ordre d'idées, le sous-groupe de $\mathbb{R}$ engendré par 1, $e + \pi$ et $e\pi$ est dense dans $\mathbb{R}$, donc il contient un sous-groupe de rang 2 sur $\mathbb{Z}$ qui est encore dense, mais on ne sait pas en expliciter un !

Pour démontrer le théorème 1.1 on établit deux lemmes préliminaires.

Lemme 1.2. – *Un sous-groupe non discret de $\mathbb{R}$ est partout dense dans $\mathbb{R}$.*

Démonstration. Si G est un sous-groupe de $\mathbb{R}$ qui n'est pas discret, il existe une suite x_n d'éléments de G, deux-à-deux distincts, qui a une limite dans $\mathbb{R}$. Soit $\epsilon > 0$; il existe un élément non nul x de G (de la forme $x_n - x_m$) dans l'intervalle $[-\epsilon, \epsilon]$. L'ensemble des éléments nx, $(n \in \mathbb{Z})$ de G a une intersection non vide avec tout intervalle de $\mathbb{R}$ de longueur $> \epsilon$. Donc G est partout dense dans $\mathbb{R}$. $\square$

Lemme 1.3. – *Les seuls sous-groupes fermés de $\mathbb{R}$, distincts de $\mathbb{R}$, sont les sous-groupes discrets, engendrés par un élément.*

Démonstration. Les sous-groupes $\{0\}$, $\mathbb{R}$ et $\mathbb{Z}x$, pour $x > 0$, sont des sous-groupes fermés de $\mathbb{R}$. Il s'agit de montrer qu'il n'y en a pas d'autre. Soit G un sous-groupe fermé de $\mathbb{R}$ distinct de $\mathbb{R}$. Le lemme 1.2 montre qu'il est discret. S'il n'est pas réduit à $\{0\}$, il contient un élément non nul ainsi que son opposé, donc il contient un élément $y > 0$. L'intervalle $[0, y]$ est compact, donc l'intersection avec G est finie. Ceci montre que G possède un plus petit élément $x > 0$. Soit maintenant $g \in G$; on pose $m = [g/x]$, de sorte que m est l'entier rationnel tel que $mx \leq g < (m+1)x$; comme $g - mx$ est un élément de G vérifiant $0 \leq g - mx < x$, on peut conclure $g = mx$ et $G = \mathbb{Z}x$. □

Démonstration du théorème 1.1. Le fait que θ soit irrationnel assure que l'adhérence $\overline{G}$ du groupe $G = \mathbb{Z} + \mathbb{Z}\theta$ n'est pas de la forme $\mathbb{Z}x$ pour $x \in \mathbb{R}$, donc $\overline{G}$ n'est pas discret (lemme 1.3), et par conséquent G est partout dense (lemme 1.2). □

Le théorème 1.1 dit qu'un sous-groupe de type fini de $\mathbb{R}/\mathbb{Z}$ est soit fini (c'est-à-dire est un groupe de torsion), soit dense dans $\mathbb{R}/\mathbb{Z}$ (cf. [H-W 1979], Th. 439).

L'application exponentielle $x \mapsto e^{2i\pi x}$ du groupe additif $\mathbb{R}$ dans le groupe multiplicatif $\mathbb{C}^\times$ a pour image le groupe multiplicatif $\mathbb{U} = \{z \in \mathbb{C}^\times;\ |z| = 1\}$ des nombres complexes de module 1 et pour noyau $\mathbb{Z}$. Le groupe topologique $\mathbb{R}/\mathbb{Z}$ est donc isomorphe au cercle unité $\mathbb{U}$. On appellera *intervalle de* $\mathbb{R}/\mathbb{Z}$ l'image d'une partie connexe de $\mathbb{U}$. Tout nombre réel x se décompose en somme de sa partie entière $[x] \in \mathbb{Z}$ et de sa partie fractionnaire $\{x\} \in [0,1)$:

$$x = [x] + \{x\}, \quad [x] \in \mathbb{Z}, \quad \{x\} \in [0,1).$$

Exercice. Vérifier les propriétés suivantes :

$$\{-x\} = \begin{cases} 1 - \{x\} & si\ x \notin \mathbb{Z}, \\ 0 & si\ x \in \mathbb{Z}. \end{cases}$$

$$\{x_1 + x_2\} = \begin{cases} \{x_1\} + \{x_2\} & si\ \{x_1\} + \{x_2\} < 1, \\ \{x_1\} + \{x_2\} - 1 & si\ \{x_1\} + \{x_2\} \geq 1. \end{cases}$$

$$\{x_1 - x_2\} = \begin{cases} \{x_1\} - \{x_2\} & si\ \{x_1\} - \{x_2\} \geq 0, \\ 1 + \{x_1\} - \{x_2\} & si\ \{x_1\} - \{x_2\} < 0. \end{cases}$$

On trouvera d'autres démonstrations du théorème 1.1 dans le chapitre XXIII de [H-W 1979]. Un argument simple utilise la compacité du quotient $\mathbb{R}/\mathbb{Z}$: s'il existe un intervalle de $\mathbb{R}/\mathbb{Z}$ de longueur positive ayant une intersection vide avec l'ensemble S des $\{n\theta\}$, $(n \in \mathbb{Z})$, on montre qu'il existe un tel intervalle I de longueur maximale, et on remarque que pour tout $n \in \mathbb{Z}$, le translaté $I + n\theta$ est encore une intersection vide avec S ; le choix de I de longueur maximale garantit que les intervalles $I + n\theta$ ainsi obtenus sont deux-à-deux disjoints ; mais on ne peut pas trouver une infinité d'intervalles disjoints de $\mathbb{R}/\mathbb{Z}$, de même longueur > 0. □

Une autre démonstration du théorème 1.1 (en dimension quelconque), attribuée à Bohr par [H-W 1979], §23.9, utilise la fonction $e^{2i\pi x}$. Cet argument analytique est à la base du critère de Weyl (cf. [Rau 1976], Chap.1, §2.3) qui permet de montrer que les points $\{n\theta\}$, $(n \in \mathbb{Z})$, sont, pour θ irrationnel, "équirépartis" sur le cercle unité (voir aussi [H-W 1979], §23.10, Th. 445).

Exercice. Soit R un rectangle dans le plan euclidien ; on considère une partition de R en petits rectangles dont les côtés sont parallèles à ceux de R. On suppose que chacun des petits rectangles a au moins un côté de longueur entière. Montrer que la longueur d'un au moins des côtés de R est un nombre entier.

En utilisant encore l'application exponentielle, on déduit du théorème 1.1 un critère pour qu'un sous-groupe de type fini de $\mathbb{R}^\times$ soit dense dans $\mathbb{R}^\times$:

Corollaire 1.4. – *Soit Γ un sous-groupe de type fini de $\mathbb{R}^\times$. Les deux conditions suivantes sont équivalentes :*
(i) Γ est dense dans $\mathbb{R}^\times$.
(ii) Γ est de rang ≥ 2 sur $\mathbb{Z}$, et Γ contient un nombre réel < 0.

Démonstration. Comme l'application exponentielle $\exp : \mathbb{R} \longrightarrow \mathbb{R}_+^\times$ est un isomorphisme de groupes topologiques, $\Gamma \cap \mathbb{R}_+^\times$ est dense dans $\mathbb{R}_+^\times$ si et seulement si $G = \exp^{-1}(\Gamma)$ est un sous-groupe dense de $\mathbb{R}$, et le rang de G sur $\mathbb{Z}$ est le même que celui de $\Gamma \cap \mathbb{R}_+^\times$. On déduit du théorème 1.1 que $\Gamma \cap \mathbb{R}_+^\times$ est dense dans $\mathbb{R}_+^\times$ si et seulement si G est de rang ≥ 2 sur $\mathbb{Z}$. Enfin un sous-groupe fermé de $\mathbb{R}^\times$ contenant $\mathbb{R}_+^\times$ est soit égal à $\mathbb{R}_+^\times$, soit égal à $\mathbb{R}^\times$. □

Exemple Le sous-groupe de $\mathbb{R}_+^\times$ engendré par 2 et 3

$$\{2^a 3^b;\ (a,b) \in \mathbb{Z} \times \mathbb{Z}\}$$

est dense dans $\mathbb{R}_+^\times$; le sous-groupe de $\mathbb{R}^\times$ engendré par -2 et 3

$$\{(-2)^a 3^b;\ (a,b) \in \mathbb{Z} \times \mathbb{Z}\}$$

est dense dans $\mathbb{R}^\times$. Cela résulte de l'indépendance linéaire sur $\mathbb{Z}$ de $\log 2$ et $\log 3$.

Nous appliquerons le théorème 1.1 de façon tout-à-fait analogue plus tard pour une courbe elliptique (l'application exponentielle sera remplacée par la fonction $\wp$ de Weierstrass).

Le théorème 1.1 est de nature qualitative. Kronecker en a donné une version quantitative (voir [H-W 1979], Th. 440) :

Théorème 1.5. – *Soit θ un nombre réel irrationnel. Pour tout $x \in \mathbb{R}$ et tout N entier positif, il existe deux entiers $n > N$ et k tels que*

$$|x - k - n\theta| < 3/n.$$

Un énoncé bien plus fort existe pour l'approximation de 0 par des points de $\mathbb{Z} + \mathbb{Z}\theta$ (c'est un problème homogène, alors que le théorème 1.5 est inhomogène).

Théorème 1.6 (Dirichlet). – *Soient θ et Q deux nombres réels, avec $Q > 1$. Il existe deux entiers p et q avec $1 \leq q < Q$ et*

$$|q\theta - p| \leq 1/Q.$$

Démonstration. (Voir [Ca 1957], ChapI, Th.I, ainsi que [Sc 1980], Chap. 1, Th. 1A). On déduit le théorème 1.6 du théorème 4.2 (qui sera démontré ci-dessous) grâce à la remarque suivante : dans le théorème 1.6, il n'y a pas de restriction à supposer Q entier. En effet, si Q n'est pas entier, on le remplace par $[Q] + 1$, et on remarque que pour un entier $q \in \mathbb{Z}$, les conditions $q < Q$ et $q < [Q] + 1$ sont équivalentes. □

Le théorème de Dirichlet fournit un critère d'irrationalité :

Corollaire 1.7. – *Soit θ un nombre réel. Les conditions suivantes sont équivalentes :*
(i) θ est irrationnel.
(ii) Il existe une infinité de $p/q \in \mathbb{Q}$ avec $q > 0$ tels que

$$\left|\theta - \frac{p}{q}\right| < \frac{1}{q^2}.$$

(iii) Pour tout $\epsilon > 0$ il existe $p/q \in \mathbb{Q}$ tel que

$$0 < |q\theta - p| < \epsilon.$$

Exercice.
1) Déduire le corollaire 1.7 du théorème 1.6.
2) Utiliser le corollaire 1.7 pour démontrer l'irrationalité du nombre

$$e = 1 + \frac{1}{1} + \frac{1}{2} + \frac{1}{6} + \cdots + \frac{1}{n!} + \cdots$$

Remarque. Cette démonstration de l'irrationailté de e remonte à Fourier (1815) ; l'irrationalité des nombres e et e^2 avait été démontrée dès 1737 par Euler, utilisant les fractions continues. C'est seulement en 1873 que Hermite a démontré la transcendance de e

Compléments. On peut aussi démontrer le corollaire 1.7 en étudiant les suites de Farey (voir [H-W 1979], Chapitre III, et Schmidt, Chapitre I), ou encore à l'aide des fractions continues (voir [H-W 1979], Chapitre XI, et Schmidt, Chapitre I). Le "spectre de Markoff" apporte des précisions sur la condition *(ii)* du corollaire 1.7.

On trouvera aussi dans [H-W 1979], §23.3, une application du théorème de Kronecker à un problème de billard (ou de miroir) ; (voir aussi [Rau 1976], Chap.1, §6.2).

Nous reviendrons bientôt sur ce sujet (voir le théorème 4.2 ci-dessous, ainsi que le chapitre V).

§2. Sous-groupes discrets de $\mathbb{R}^n$

Si $x_1, \ldots, x_\ell$ sont des éléments $\mathbb{R}$-linéairement indépendants de $\mathbb{R}^n$, le sous-groupe G qu'ils engendrent est de rang réel ℓ, de rang sur $\mathbb{Q}$ aussi égal à ℓ, et G est un sous-groupe discret de $\mathbb{R}^n$. Nous allons voir que tout sous-groupe discret de $\mathbb{R}^n$ est de cette forme.

Théorème 2.1. – *Tout sous-groupe discret G de $\mathbb{R}^n$ est de la forme $\mathbb{Z}g_1 + \cdots + \mathbb{Z}g_\ell$, où $g_1, \ldots, g_\ell$ sont des éléments de $\mathbb{R}^n$ linéairement indépendants sur $\mathbb{R}$.*

La démonstration va reposer sur le lemme suivant.

Lemme 2.2. – *Soit G un sous-groupe discret de rang réel r de $\mathbb{R}^n$. Soient $e_1, \ldots, e_r$ des éléments de G linéairement indépendants sur $\mathbb{R}$. Soit*

$$P = \{x_1e_1 + \cdots + x_re_r;\ -1 \le x_i \le 1\};$$

Alors $G \cap P$ est un ensemble fini, qui engendre G comme $\mathbb{Z}$-module. Tout élément de G est combinaison linéaire à coefficients rationnels de $e_1, \ldots, e_r$.

Démonstration. Comme $G \cap P$ est compact et discret, cet ensemble est fini. Soit $x \in G$; on peut écrire $x = t_1e_1 + \cdots + t_re_r$, avec des t_i réels. Pour chaque entier $m > 0$, on pose

$$z_m = mx - \sum_{i=1}^{r}[mt_i]e_i = \sum_{i=1}^{r}(mt_i - [mt_i])e_i \in G.$$

Comme $0 \le mt_i - [mt_i] < 1$, on a $z_m \in P$. En particulier

$$x = z_1 + \sum_{i=1}^{r}[t_i]e_i,$$

avec $z_1 \in G \cap P$ et $e_i \in G \cap P$, ce qui montre que $G \cap P$ engendre G comme $\mathbb{Z}$-module.

D'autre part $G \cap P$ est fini et contient tous les z_m, $(m \ge 1)$; par conséquent (principe des tiroirs !) il existe deux entiers positifs $h \ne k$ tels que $z_h = z_k$. En écrivant

$$hx - \sum_{i=1}^{r}[ht_i]e_i = kx - \sum_{i=1}^{r}[kt_i]e_i$$

et en tenant compte du fait que les e_i sont linéairement indépendants sur $\mathbb{R}$, on conclut $(h-k)t_i = [ht_i] - [kt_i]$, ce qui montre que chacun des t_i est rationnel. □

Démonstration du théorème 2.1.
Première étape. On commence par montrer qu'un sous-groupe discret G de $\mathbb{R}^n$ de rang réel ℓ est contenu dans un sous-groupe discret de la forme $\mathbb{Z}y_1 + \cdots + \mathbb{Z}y_\ell$. Pour cela on choisit ℓ éléments $e_1, \ldots, e_\ell$ dans G linéairement indépendants sur $\mathbb{R}$. Tout élément de G est, d'après le lemme 2.2, de la forme $t_1e_1 + \cdots + t_\ell e_\ell$, avec des t_i rationnels. On écrit ces coordonnées pour chacun des éléments de l'ensemble fini $G \cap P$ (qui engendre G comme $\mathbb{Z}$-module), et on désigne par $d > 0$ un dénominateur commun des t_i ; enfin on pose $y_i = e_i/d$, et on trouve $G \subset \mathbb{Z}y_1 + \cdots + \mathbb{Z}y_\ell$.
Deuxième étape. Pour terminer la démonstration du théorème 2.1, on utilise le théorème de structure des modules sur un anneau principal ("facteurs invariants") : le groupe $G_0 = \mathbb{Z}y_1 + \cdots + \mathbb{Z}y_\ell$ est abélien libre de type fini, et G en est un sous-groupe. Alors il existe une base de G_0 de la forme $(x_1, \ldots, x_\ell)$ (ce qui signifie que les x_i sont des combinaisons linéaires des y_j à coefficients dans $\mathbb{Z}$, et la matrice de passage a pour déterminant ± 1), et il existe des entiers positifs $a_1, \ldots, a_\ell$, où a_i divise a_{i+1} pour $1 \le i < \ell$, tels que $(a_1x_1, \ldots, a_\ell x_\ell)$ soit une base du $\mathbb{Z}$-module G. On pose enfin $g_i = a_ix_i$, $(1 \le i \le \ell)$. □

Corollaire 2.3. – *Soient* $e_1, \dots, e_r$ *des éléments* $\mathbb{R}$*-linéairement indépendants de* $\mathbb{R}^n$ *et* $t_1, \dots, t_r$ *des nombres réels ; on pose* $\theta = t_1 e_1 + \dots + t_r e_r$. *Alors le sous-groupe* $\mathbb{Z}e_1 + \dots + \mathbb{Z}e_r + \mathbb{Z}\theta$ *de* $\mathbb{R}^n$ *est discret dans* $\mathbb{R}^n$ *si et seulement si les nombres* $t_1, \dots, t_r$ *sont tous rationnels.*

Démonstration. Si $\mathbb{Z}e_1 + \dots + \mathbb{Z}e_r + \mathbb{Z}\theta$ est discret dans $\mathbb{R}^n$, le lemme 2.2 affirme que θ est combinaison linéaire à coefficients rationnels de $e_1, \dots, e_r$, donc $(t_1, \dots, t_r) \in \mathbb{Q}^r$. Inversement, si $(t_1, \dots, t_r) \in \mathbb{Q}^r$, on prend un dénominateur commun $d > 0$ de $t_1, \dots, t_r$, et alors G est un sous-groupe du groupe discret $\mathbb{Z}(e_1/d) + \dots + \mathbb{Z}(e_r/d)$. ∎

En particulier pour un sous-groupe discret de $\mathbb{R}^n$, le rang réel coïncide avec le rang rationnel : une famille d'éléments d'un sous-groupe discret de $\mathbb{R}^n$ est libre sur $\mathbb{R}$ si et seulement si elle est libre sur $\mathbb{Q}$ (ou sur $\mathbb{Z}$, cela revient évidemment au même).

Quand on applique le corollaire 2.3 à la base canonique de $\mathbb{R}^n$, on trouve un résultat dû à Kronecker (mais qui n'est pas “le” théorème de Kronecker dont il est question dans l'introduction).

Corollaire 2.4. – *Soient* $\theta_1, \dots, \theta_n$ *des nombres réels. Les conditions suivantes sont équivalentes.*
(i) Pour tout $\epsilon > 0$ *il existe des entiers* $p_1, \dots, p_n$, q, *avec* $q > 0$, *tels que*

$$0 < \max_{1 \le i \le n} |q\theta_i - p_i| < \epsilon.$$

(ii) L'un au moins des n *nombres* $\theta_1, \dots, \theta_n$ *est irrationnel.*

Terminons cette section par une définition : un *réseau* de $\mathbb{R}^n$ est un sous-groupe discret de rang n.

§3. Sous-groupes fermés de $\mathbb{R}^n$

Voici le résultat principal donnant la classification des sous-groupes fermés de $\mathbb{R}^n$.

Théorème 3.1. – *Soit* G *un sous-groupe fermé de* $\mathbb{R}^n$, *de rang réel* r. *Il existe un plus grand sous-espace vectoriel* V *contenu dans* G ; *si* W *est un sous-espace vectoriel de* $\mathbb{R}^n$ *supplémentaire de* V, *alors* $W \cap G$ *est un sous-groupe discret de* $\mathbb{R}^n$, *et* G *est somme directe de* V *et de* $W \cap G$.

Une étape importante de la démonstration du théorème 3.1 est fournie par le lemme suivant :

Lemme 3.2. – *Un sous groupe fermé non discret de* $\mathbb{R}^n$ *contient une droite vectorielle.*

Démonstration. On choisit une norme $\|\cdot\|$ sur $\mathbb{R}^n$. Soit G un sous-groupe fermé non discret de $\mathbb{R}^n$. Il existe un point g dans G, limite d'une suite d'éléments g_n de G, avec $g_n \neq g$. Alors $x_n = g - g_n$ est une suite d'éléments non nuls de G de limite 0. Soit M la borne supérieure des $\|x_n\|$. Pour chaque $n \ge 1$, soit k_n l'entier ≥ 0 défini par

$$\|k_n x_n\| \le M < \|(k_n + 1)x_n\|.$$

La suite $z_n = k_n x_n$ a une valeur d'adhérence $z \in \mathbb{R}^n$. Comme $\|z_n\| \le M$, on a $\|z\| \le M$; mais on a aussi

$$\|z_n\| > M - \|x_n\| \quad \text{avec} \quad \lim_{n\to\infty} \|x_n\| = 0,$$

donc $\|z\| = M$. Enfin soit $t \in \mathbb{R}$; on a

$$tz = \lim_{n\to\infty} [tk_n]x_n \quad \text{et} \quad [tk_n]x_n \in G,$$

et G est fermé, donc la droite $\{tz;\ t \in \mathbb{R}\}$ est contenue dans G. ∎

Démonstration du théorème 3.1. Soit V la réunion des droites vectorielles contenues dans G. Pour $x \in V$, $y \in V$ et $\lambda \in \mathbb{R}$, on a $\lambda x \in G$ et $\lambda y \in G$ donc $\lambda x + \lambda y \in G$; ceci étant vrai pour tout $\lambda \in \mathbb{R}$, par définition de V on obtient $\lambda x + \lambda y \in V$, ce qui montre que V est un sous-espace vectoriel de $\mathbb{R}^n$ sur $\mathbb{R}$; ainsi V est le plus grand sous-espace de $\mathbb{R}^n$ contenu dans G. Soit W un supplémentaire de V dans $\mathbb{R}^n$; tout $g \in G$ s'écrit $g = v + w$ avec $v \in V$ et $w \in W$, donc $w = g - v \in G \cap W$ et

$$G \subset V + G \cap W \subset G.$$

De plus $V \cap (G \cap W) \subset V \cap W = 0$, donc la somme $V + G \cap W$ est directe. Enfin $W \cap G$ ne contient pas de droite vectorielle de $\mathbb{R}^n$, donc (lemme 3.2) est discret dans $\mathbb{R}^n$. ∎

Le théorème 3.1 montre que si G est un sous-groupe fermé de $\mathbb{R}^n$, il existe une base $(e_1, \dots, e_n)$ de $\mathbb{R}^n$ telle que G soit l'ensemble des

$$t_1 e_1 + \dots + t_r e_r + n_{r+1} e_{r+1} + \dots + n_\ell e_\ell,$$

où $(t_1, \dots, t_r)$ décrit $\mathbb{R}^r$, tandis que $(n_{r+1}, \dots, n_\ell)$ décrit $\mathbb{Z}^{\ell - r}$. Alors G est isomorphe à $\mathbb{R}^r \times \mathbb{Z}^{\ell - r}$, où ℓ est le rang réel de G, et r la dimension du plus-grand sous-espace de $\mathbb{R}^n$ sur $\mathbb{R}$ contenu dans G.

§4. Sous-groupes denses de $\mathbb{R}^n$

Nous déduisons du théorème 3.1 un résultat d'approximation 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.

Exercice. Soient R *un groupe topologique commutatif,* V *un sous-groupe fermé de* R, G *un sous-groupe de* R.
a) On suppose que G *est dense dans* R ; *montrer que* $G/G \cap V$ *est dense dans* R/V.
b) On suppose que $G \cap V$ *est dense dans* V *et que* $G/G \cap V$ *est dense dans* R/V. *Montrer que* G *est dense dans* R.
c) Donner un exemple où G *est dense dans* R *mais* $G \cap V$ *n'est pas dense dans* V.

Exercice. Soient R_1 *et* R_2 *deux groupes topologiques commutatifs et soit* R *le produit* $R_1 \times R_2$.
a) Si G_1 *est un sous-groupe dense de* R_1 *et* G_2 *un sous-groupe dense de* R_2, *montrer que*

$G_1 \times G_2$ est dense dans R.
b) Soit G un sous-groupe de R tel que $\{x \in R_1;\, (x,0) \in G\}$ soit dense dans R_1 et $\{y \in R_2;\, (0,y) \in G\}$ soit dense dans R_2. Montrer que G est dense dans R.
c) Donner un exemple d'un sous-groupe de type fini de $\mathbb{R}^2$ dont la projection sur chacun des facteurs $\mathbb{R} \times \{0\}$ et $\{0\} \times \mathbb{R}$ est dense, mais qui n'est pas dense dans $\mathbb{R}^2$.

Soit G un sous-groupe de type fini de $\mathbb{R}^n$; si G est dense dans $\mathbb{R}^n$, alors évidemment G contient une base de $\mathbb{R}^n$ sur $\mathbb{R}$; cela ne suffit pas : il faut au moins un point supplémentaire, donc le rang de G sur $\mathbb{Z}$ est au moins $n+1$. Dans un premier temps supposons G de rang $n+1$; soit $(e_1, \dots, e_n)$ une base de $\mathbb{R}^n$ sur $\mathbb{R}$ appartenant à G, et soit $e_{n+1} \in G$ tel que le sous-groupe $\mathbb{Z}e_1 + \cdots + \mathbb{Z}e_{n+1}$ soit d'indice fini dans G. Ecrivons e_{n+1} dans la base $(e_1, \dots, e_n)$:

$$e_{n+1} = \theta_1 e_1 + \cdots + \theta_n e_n;$$

alors le théorème de Kronecker (voir par exemple [Ca 1957], [H-W 1979], Th. 442 ; [Bo 1974] Chap. 7 §1 N°3 corollaire 2 de la proposition 7)) affirme que *G est dense dans $\mathbb{R}^n$ si et seulement si les nombres $1, \theta_1, \dots, \theta_n$ sont linéairement indépendants sur $\mathbb{Q}$.*

Théorème 4.1 (Kronecker). – *Soient $\theta_1, \dots, \theta_n$ des nombres réels. Pour que le sous-groupe*

$$\mathbb{Z}^n + \mathbb{Z}(\theta_1, \dots, \theta_n) = \big\{(s_1 + s_0\theta_1, \dots, s_n + s_0\theta_n);\; (s_0, s_1, \dots, s_n) \in \mathbb{Z}^{n+1}\big\} \subset \mathbb{R}^n$$

soit dense dans $\mathbb{R}^n$, il faut et il suffit que les $n+1$ nombres $1, \theta_1, \dots, \theta_n$ soient linéairement indépendants sur $\mathbb{Q}$.

Démonstration. Supposons dans un premier temps que les nombres $1, \theta_1, \dots, \theta_n$ sont linéairement dépendants sur $\mathbb{Q}$:

$$a_1\theta_1 + \cdots + a_n\theta_n = a_0,$$

avec $(a_0, a_1, \dots, a_n) \in \mathbb{Z}^n$, $(a_0, a_1, \dots, a_n) \neq 0$. Alors $\mathbb{Z}^n + \mathbb{Z}(\theta_1, \dots, \theta_n)$ est contenu dans

$$\big\{(x_1, \dots, x_n) \in \mathbb{R}^n;\; a_1x_1 + \cdots + a_nx_n \in \mathbb{Z}\big\},$$

qui n'est pas dense dans $\mathbb{R}^n$: si H désigne l'hyperplan d'équation $a_1x_1 + \cdots + a_nx_n = 0$, la projection sur $\mathbb{R}^n/H$ est discrète.

Inversement, si G est un sous-groupe de $\mathbb{R}^n$ qui n'est pas dense, alors il existe un hyperplan V de $\mathbb{R}^n$ et un sous-groupe discret D de $\mathbb{R}^n$ isomorphe à $\mathbb{Z}$ tels que

$$G \subset V \oplus D.$$

On écrit une équation de l'hyperplan V :

$$a_1x_1 + \cdots + a_nx_n = 0,$$

avec $(a_1, \dots, a_n) \in \mathbb{R}^n$, $(a_1, \dots, a_n) \neq 0$; une telle équation n'est définie qu'à une constante multiplicative près (en fait $(a_1, \dots, a_n)$ est bien défini dans l'espace projectif). La forme

linéaire $(x_1, \dots, x_n) \mapsto a_1x_1 + \cdots + a_nx_n$ sur $\mathbb{R}^n$ a pour noyau V, et l'image de $V \oplus D$ est un sous-groupe discret de $\mathbb{R}$ (isomorphe à D). On peut donc choisir une équation de V telle sorte que

$$V \oplus D \subset \big\{(x_1, \dots, x_n) \in \mathbb{R}^n;\; a_1x_1 + \cdots + a_nx_n \in \mathbb{Z}\big\}.$$

Appliquons ceci au cas où $G = \mathbb{Z}^n + \mathbb{Z}(\theta_1, \dots, \theta_n)$. Si G n'est pas dense dans $\mathbb{R}^n$, il existe des nombres réels $a_1, \dots, a_n$ tels que tout élément $(x_1, \dots, x_n) \in G$ vérifie $a_1x_1 + \cdots + a_nx_n \in \mathbb{Z}$. On écrit d'abord que la base canonique de $\mathbb{R}^n$ appartient à G : on trouve $a_i \in \mathbb{Z}$ pour $1 \le i \le n$. On écrit enfin que $(\theta_1, \dots, \theta_n)$ appartient à G : on obtient $a_1\theta_1 + \cdots + a_n\theta_n \in \mathbb{Z}$. Donc $1, \theta_1, \dots, \theta_n$ sont linéairement dépendants sur $\mathbb{Q}$. □

Exercice. *Soit $G = \mathbb{Z}g_1 + \cdots + \mathbb{Z}g_{n+1}$ un sous-groupe de type fini de $\mathbb{R}^n$ engendré par $n+1$ éléments $g_1, \dots, g_{n+1}$ de $\mathbb{R}^n$. Ecrivons les g_j dans la base canonique de $\mathbb{R}^n$:*

$$g_j = (g_{1j}, \dots, g_{nj}), \qquad (1 \le j \le n+1).$$

Montrer que les conditions suivantes sont équivalentes :
(i) G est dense dans $\mathbb{R}^n$.
(ii) Les $n+1$ nombres réels

$$\Delta_h = \det\Big(g_{ij}\Big)_{\substack{1 \le i \le n \\ 1 \le j \le n+1,\; j \neq h}}, \qquad (1 \le h \le n+1)$$

sont linéairement indépendants sur $\mathbb{Q}$.
(iii) Pour tout $(s_1, \dots, s_{n+1})$ dans $\mathbb{Z}^{n+1}$ distinct de $(0, \dots, 0)$, le nombre

$$\det\begin{pmatrix} g_{11} & \cdots & g_{1,n+1} \\ \vdots & \ddots & \vdots \\ g_{n1} & \cdots & g_{n,n+1} \\ s_1 & \cdots & s_{n+1} \end{pmatrix}$$

n'est pas nul.

Le théorème de Kronecker peut être précisé de manière quantitative. D'une part on peut montrer (voir par exemple [Rau 1976] Chap.1, §6) que les points $(\{s\theta_1\}, \dots, \{s\theta_n\})$, $(s \ge 1)$ sont équirépartis dans $(\mathbb{R}/\mathbb{Z})^n$. D'autre part on peut préciser comment se fait l'approximation de 0 par des éléments d'un sous-groupe dense de la forme $\mathbb{Z}^n + \mathbb{Z}(\theta_1, \dots, \theta_n)$ de la manière suivante :

Théorème 4.2 (Dirichlet). – *Soient n et m deux nombres entiers positifs, Q un nombre réel > 1 et θ_{ji}, $(1 \le j \le n,\ 1 \le i \le m)$ nm nombres réels. Il existe des entiers $p_1, \dots, p_n$, $q_1, \dots, q_m$ avec*

$$0 < \max\{|q_1|, \dots, |q_m|\} < Q$$

et

$$\max_{1 \le j \le n} |q_1\theta_{j1} + \cdots + q_m\theta_{jm} - p_j| \le Q^{-m/n}.$$

Démonstration. Cet énoncé est démontré en appliquant un théorème de Minkowski sur les formes linéaires, par exemple dans [Ca 1957], Ch.I, Th. VI, ou encore dans [Sc 1980], Chap. 2, Th. 3A (voir la remarque p.37 – en fait un énoncé un peu plus précis y est démontré). Nous allons donner une démonstration plus simple, mais qui suppose que le nombre $N = Q^{m/n}$ est entier (d'après [Sc 1980], Chap. 2, Th. 1E).
Pour chaque $(t_1,\dots,t_m) \in \mathbb{Z}^m$ vérifiant $0 \le t_i < Q$, $(1 \le i \le m)$, on considère le point

$$\Big(\{t_1\vartheta_{11} + \cdots + t_m\vartheta_{1m}\},\dots,\{t_1\vartheta_{n1} + \cdots + t_m\vartheta_{nm}\}\Big)$$

dans le cube n-dimensionnel $[0,1]^n$; en comptant aussi le point $(1,\dots,1)$ qui est dans ce cube, on obtient au moins $Q^m + 1 = N^n + 1$ éléments de $[0,1]^n$ (qui ne sont pas nécessairement deux-à-deux distincts). On divise $[0,1]^n$ en N^n cubes disjoints de côté $1/N$; deux des $N^n + 1$ points considérés appartiennent au même petit cube : cela signifie qu'il existe des entiers rationnels $t_1,\dots,t_m$, $s_1,\dots,s_n$, $t'_1,\dots,t'_m$, $s'_1,\dots,s'_n$, avec $(t_1,\dots,t_m) \neq (t'_1,\dots,t'_m)$, tels que la différence $(x_1,\dots,x_n)$ entre les deux points

$$\big(t_1\vartheta_{11} + \cdots + t_m\vartheta_{1m} - s_1,\dots,t_1\vartheta_{n1} + \cdots + t_m\vartheta_{nm} - s_n\big)$$

et

$$\big(t'_1\vartheta_{11} + \cdots + t'_m\vartheta_{1m} - s'_1,\dots,t'_1\vartheta_{n1} + \cdots + t'_m\vartheta_{nm} - s'_n\big)$$

vérifie

$$\max_{1\le j\le n} |x_j| \le 1/N.$$

Le résultat annoncé s'obtient en posant $q_i = t_i - t'_i$, $(1 \le i \le m)$ et $p_j = s_j - s'_j$, $(1 \le j \le n)$. $\square$

Exercice. On désigne par $\|\cdot\|$ la distance à l'entier le plus proche : pour $x \in \mathbb{Z}$,

$$\|x\| = \min_{a\in\mathbb{Z}} |x - a|.$$

Soient n un entier positif et $\theta_1,\dots,\theta_n$ des nombres réels.
a) Montrer que les trois conditions suivantes sont équivalentes :
(i) $\quad(\theta_1,\dots,\theta_n) \notin \mathbb{Q}^n$.
(ii) Il existe une infinité d'entiers $q > 0$ tels que

$$0 < \max_{1\le j\le n} \|q\theta_j\| < q^{-1/n}.$$

(iii) Pour tout $\epsilon > 0$, il existe un entier $q > 0$ tel que

$$0 < \max_{1\le j\le n} \|q\theta_j\| < \epsilon.$$

(L'équivalence entre (i) et (iii) est le corollaire 2.4. D'autre part le cas $n = 1$ de cet exercice

est le corollaire 1.7.)
b) Montrer qu'il existe une infinité de $(q_1,\dots,q_n) \in \mathbb{Z}^n$ avec

$$\|q_1\theta_1 + \cdots + q_n\theta_n\| < \big(\max_{1\le j\le n} |q_j|\big)^{-n}.$$

c) Montrer que les deux conditions suivantes sont équivalentes :
(i) Les nombres $1,\theta_1,\dots,\theta_n$ sont linéairement indépendants sur $\mathbb{Q}$.
(ii) Pour tout $\epsilon > 0$, il existe une matrice carrée $(q_{ji})_{1\le j,i\le n}$, à coefficients dans $\mathbb{Z}$ et de déterminant non nul, telle que

$$0 < \max_{1\le i\le n} \|q_{1i}\theta_1 + \cdots + q_{ni}\theta_n\| < \epsilon.$$

Afin de donner des conditions nécessaires et suffisantes pour qu'un sous-groupe G de type fini de $\mathbb{R}^n$ soit dense dans $\mathbb{R}^n$, on introduit la définition suivante : on appelle *caractère* de $\mathbb{R}^n$ tout homomorphisme continu de $\mathbb{R}^n$ dans $\mathbb{U}$ (ou dans $\mathbb{R}/\mathbb{Z}$, cela revient évidemment au même).

Exercice.
a) Vérifier que tout homomorphisme continu du groupe additif $\mathbb{R}$ dans lui-même est une application $\mathbb{R}$-linéaire, c'est-à-dire de la forme $x \mapsto \lambda x$, pour un $\lambda \in \mathbb{R}$. En déduire d'abord que tout homomorphisme continu du groupe additif $\mathbb{R}$ dans le groupe multiplicatif $\mathbb{R}^\times$ est de la forme $x \mapsto e^{\lambda x}$, ensuite que tout homomorphisme continu du groupe additif $\mathbb{R}$ dans le groupe multiplicatif $\mathbb{U}$ est de la forme $x \mapsto e^{i\lambda x}$. En déduire que tout homomorphisme continu $\chi : \mathbb{R} \to \mathbb{R}/\mathbb{Z}$ se factorise en $\chi = s \circ h$:

$$\begin{tikzcd} \mathbb{R} \arrow[r, "h"] \arrow[dr, "\chi"'] & \mathbb{R} \arrow[d, "s"] \\ & \mathbb{R}/\mathbb{Z} \end{tikzcd}$$

où $s : \mathbb{R} \to \mathbb{R}/\mathbb{Z}$ est la surjection canonique et $h : \mathbb{R} \to \mathbb{R}$ est une application linéaire.
b) Quand u est un élément de $\mathbb{R}^n$, l'application ψ_u de $\mathbb{R}^n$ dans $\mathbb{U}$ donnée par $x \mapsto e^{2i\pi u\cdot x}$ (où $u \cdot x$ est le produit scalaire standard dans $\mathbb{R}^n$) est un caractère de $\mathbb{R}^n$. Vérifier qu'on les obtient tous ainsi. Le noyau de ψ_u est $\{x \in \mathbb{R}^n;\ u \cdot x \in \mathbb{Z}\}$.
c) En déduire que l'application de $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n,\mathbb{R})$ dans le groupe des caractères de $\mathbb{R}^n$ qui, à une forme linéaire φ, associe $\chi_\varphi : x \mapsto e^{2i\pi\varphi(x)}$, est un isomorphisme de groupes. Le noyau de χ_φ est $\varphi^{-1}(\mathbb{Z})$.

Proposition 4.3. *Soit G un sous-groupe de type fini de $\mathbb{R}^n$. Les conditions suivantes sont équivalentes.*
(i) G est dense dans $\mathbb{R}^n$.
(ii) Pour tout sous-espace vectoriel V de $\mathbb{R}^n$ distinct de $\mathbb{R}^n$, on a

$$\mathrm{rang}_{\mathbb{Z}}(G/G\cap V) > \dim_{\mathbb{R}}(\mathbb{R}^n/V).$$

(iii) Pour tout hyperplan H de $\mathbb{R}^n$, on a $\mathrm{rang}_{\mathbb{Z}}(G/G\cap H) \geq 2$.
(iv) Pour toute forme linéaire non nulle $\varphi : \mathbb{R}^n \longrightarrow \mathbb{R}$ on a $\varphi(G) \not\subset \mathbb{Z}$.
(v) Pour tout caractère non trivial χ de $\mathbb{R}^n$, on a $\chi(G) \neq \{1\}$.
(vi) Choisissons des générateurs $g_1, \ldots, g_\ell$ de G sur $\mathbb{Z}$ et écrivons les coordonnées des g_j dans la base canonique de $\mathbb{R}^n$:

$$g_j = (g_{1j}, \ldots, g_{nj}), \qquad (1 \leq j \leq \ell);$$

pour tout $(s_1, \ldots, s_\ell)$ dans $\mathbb{Z}^\ell$ distinct de $(0, \ldots, 0)$, la matrice

$$\begin{pmatrix} g_{11} & \cdots & g_{1\ell} \\ \vdots & \ddots & \vdots \\ g_{n1} & \cdots & g_{n\ell} \\ s_1 & \cdots & s_\ell \end{pmatrix}$$

est de rang $n+1$.

On peut remarquer que le cas $n = 1$ ne donne rien de nouveau par rapport au théorème 1.1.

Démonstration.
Notons déjà que l'implication $(ii) \Rightarrow (iii)$ est triviale.
$(i) \Rightarrow (ii)$. Soient G un sous-groupe de type fini dense dans $\mathbb{R}^n$, V un sous-espace de $\mathbb{R}^n$ distinct de $\mathbb{R}^n$ et $s : \mathbb{R}^n \to \mathbb{R}^n/V$ la surjection canonique. Comme s est continue et que G est dense dans $\mathbb{R}^n$, $s(G) = G/G\cap V$ est dense dans $\mathbb{R}^n/V$, donc $\mathrm{rang}_{\mathbb{Z}}(G/G\cap V) > \dim_{\mathbb{R}}(\mathbb{R}^n/V)$.

$(iii) \Rightarrow (i)$. Soit G un sous-groupe de $\mathbb{R}^n$ qui n'est pas dense. Montrons qu'il existe un hyperplan H de $\mathbb{R}^n$ tel que $\mathrm{rang}_{\mathbb{Z}}(G/G\cap H) \leq 1$. Désignons par $\overline{G}$ l'adhérence de G dans $\mathbb{R}^n$. Soit V le sous-espace vectoriel maximal de $\mathbb{R}^n$ contenu dans $\overline{G}$. Etant donné que G n'est pas dense dans $\mathbb{R}^n$, on a $V \neq \mathbb{R}^n$. De plus (théorème 3.1) $G/G\cap V$ est discret dans $\mathbb{R}^n/V$. Soit H un hyperplan de $\mathbb{R}^n$ contenant V. Alors $G/G\cap H$ est discret dans $\mathbb{R}^n/H$, donc de rang ≤ 1 sur $\mathbb{Z}$.

$(iii) \Leftrightarrow (iv)$ L'application de $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R}) \setminus \{0\}$ dans l'ensemble des hyperplans H de $\mathbb{R}^n$ (qui, à une forme linéaire non nulle, associe son noyau) est surjective, et deux éléments φ_1, φ_2 ont la même image si et seulement s'il existe $x \in \mathbb{R}^\times$ tel que $\varphi_2 = x\varphi_1$.

L'équivalence $(iv) \Leftrightarrow (v)$ résulte immédiatement de l'exercice ci-dessus qui établit un isomorphisme $\varphi \mapsto \chi_\varphi$ entre $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$ et le groupe des caractères de $\mathbb{R}^n$.

$(iv) \Leftrightarrow (vi)$ Dire que le rang de la matrice donnée dans la condition (v) est strictement inférieur à $n+1$ revient à dire qu'il existe des nombres réels $c_0, c_1, \ldots, c_n$, non tous nuls, tels que

$$c_1 g_{1j} + \cdots + c_n g_{nj} = c_0 s_j \qquad \text{pour} \quad 1 \leq j \leq \ell.$$

Quand $(s_1, \ldots, s_\ell) \neq (0, \ldots, 0)$, on a $(c_1, \ldots, c_n) \neq (0, \ldots, 0)$. L'existence de $(c_1, \ldots, c_n)$ équivaut donc à celle d'une forme linéaire non nulle $\varphi(x) = c_1x_1 + \cdots + c_nx_n$ telle que $\mathrm{rang}_{\mathbb{Z}}\varphi(G) \leq 1$. $\square$

Exercice. *Soit G un sous-groupe de type fini de $\mathbb{R}^n$ qui contient $\mathbb{Z}^n$. Montrer que G est dense dans $\mathbb{R}^n$ si et seulement si, pour tout hyperplan H de $\mathbb{R}^n$ rationnel sur $\mathbb{Q}$, la projection $G/G\cap H$ de G sur $\mathbb{R}^n/H$ a une image dense.*

Exercice. *Soit G un sous-groupe de $\mathbb{R}^n$. Montrer que les conditions suivantes sont équivalentes.*
(i) G contient un sous-groupe de type fini qui est dense dans $\mathbb{R}^n$.
(ii) Pour tout hyperplan H de $\mathbb{R}^n$, on a $\mathrm{rang}_{\mathbb{Z}}(G/G\cap H) \geq 2$.
(iii) Pour tout sous-espace vectoriel V de $\mathbb{R}^n$ distinct de $\mathbb{R}^n$, on a $\mathrm{rang}_{\mathbb{Z}}(G/G\cap V) > \dim_{\mathbb{R}}(\mathbb{R}^n/V)$.
(iv) Pour toute forme linéaire non nulle $\varphi : \mathbb{R}^n \longrightarrow \mathbb{R}$ on a $\varphi(G) \not\subset \mathbb{Q}$.
`Indication.` Voir M. Waldschmidt, *Quelques aspects transcendants de la théorie des nombres algébriques,* Cours de troisième cycle 1986/87, Publ. Math. Univ. P. et M. Curie (Paris VI), **89**, lemme 3.12.

Exercice. *Soient m et n deux entiers positifs, et soient ϑ_{ji}, $(1 \leq j \leq n,\ 1 \leq i \leq m)$ des nombres réels ; on pose*

$$\gamma_i = (\vartheta_{1i}, \ldots, \vartheta_{ni}) \in \mathbb{R}^n, \qquad (1 \leq i \leq m)$$

et

$$\delta_j = (\vartheta_{j1}, \ldots, \vartheta_{jm}) \in \mathbb{R}^m, \qquad (1 \leq j \leq n).$$

Ainsi

$$\Gamma = \mathbb{Z}^n + \mathbb{Z}\gamma_1 + \cdots + \mathbb{Z}\gamma_m \subset \mathbb{R}^n \qquad et \qquad \Delta = \mathbb{Z}^m + \mathbb{Z}\delta_1 + \cdots + \mathbb{Z}\delta_n \subset \mathbb{R}^m$$

sont les sous-groupes engendrés par les vecteurs colonnes des matrices

$$\begin{pmatrix} 1 & \cdots & 0 & \vartheta_{11} & \cdots & \vartheta_{1m} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & \vartheta_{n1} & \cdots & \vartheta_{nm} \end{pmatrix} \quad et \quad \begin{pmatrix} 1 & \cdots & 0 & \vartheta_{11} & \cdots & \vartheta_{n1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & \vartheta_{1m} & \cdots & \vartheta_{nm} \end{pmatrix}.$$

Montrer que le sous-groupe Γ est dense dans $\mathbb{R}^n$ si et seulement si le sous-groupe Δ est de rang $n+m$ sur $\mathbb{Z}$.

La fin de cette section va être consacrée à une autre démonstration de l'équivalence $(iv) \Leftrightarrow (i)$ de la proposition 4.3. On utilisera la notion de "sous-groupe associé" (voir [Bo 1974] Chap. 7 §1 n°3) qui sera encore utile au §5.

Cette équivalence signifie qu'un sous-groupe de type fini G de $\mathbb{R}^n$ est dense dans $\mathbb{R}^n$ si et seulement si la seule forme linéaire $\varphi : \mathbb{R}^n \to \mathbb{R}$ qui envoie G dans $\mathbb{Z}$ est $\varphi = 0$. Noter que, tant qu'il s'agit de groupes de type fini, il revient au même de demander $\varphi(G) \subset \mathbb{Z}$ ou $\varphi(G) \subset \mathbb{Q}$.

De manière générale, quand G est un sous-groupe (pas nécessairement de type fini) de $\mathbb{R}^n$, on définit *le sous-groupe G^* de* $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$ *associé à G* par

$$G^* = \{\varphi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R});\ \varphi(G) \subset \mathbb{Z}\}.$$

Proposition 4.4. – *Soit G un sous-groupe de $\mathbb{R}^n$; l'adhérence $\overline{G}$ de G dans $\mathbb{R}^n$ est*

$$(G^*)^* = \{x \in \mathbb{R}^n;\ \varphi(x) \in \mathbb{Z} \ \ pour\ tout\ \ \varphi \in G^*\}.$$

Afin de démontrer la proposition 4.4 on établit deux lemmes.

Lemme 4.5. – *Si G est un sous-groupe de $\mathbb{R}^n$, alors G^* est un sous-groupe fermé de* $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$ *et* $(\overline{G})^* = G^*$.

Démonstration. Pour u et x dans $\mathbb{R}^n$, notons (comme dans l'exercice précédent la proposition 4.3) $u \cdot x \in \mathbb{R}$ le produit scalaire standard. L'application de $\mathbb{R}^n$ dans $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$ qui envoie u sur $x \mapsto u \cdot x$ est un isomorphisme de groupes topologiques ; notons θ l'isomorphisme inverse. Alors

$$\theta(G^*) = \{u \in \mathbb{R}^n;\ u \cdot g \in \mathbb{Z} \ \text{ pour tout } \ g \in G\} \subset \mathbb{R}^n$$

est intersection des fermés $\{u \in \mathbb{R}^n;\ u \cdot g \in \mathbb{Z}\}$, pour g décrivant G, donc est fermé dans $\mathbb{R}^n$.

Pour $\varphi \in G^*$, on a $\varphi(G) \subset \mathbb{Z}$, et comme $\mathbb{Z}$ est discret dans $\mathbb{R}$ et φ continu, on a encore $\varphi(\overline{G}) \subset \mathbb{Z}$, ce qui montre l'inclusion $G^* \subset (\overline{G})^*$. L'autre inclusion est banale : si G_1 est un sous-groupe de G_2, alors G_2^* est un sous-groupe de G_1^*. □

Lemme 4.6. – *Soit G un sous-groupe fermé de $\mathbb{R}^n$. Choisissons une base $(e_1, \dots, e_n)$ de $\mathbb{R}^n$ telle que*

$$G = \mathbb{R}e_1 + \cdots + \mathbb{R}e_r + \mathbb{Z}e_{r+1} + \cdots + \mathbb{Z}e_\ell.$$

Désignons par $(f_1, \dots, f_n)$ la base duale de $(e_1, \dots, e_n)$:

$$f_i(e_j) = \delta_{ij}, \qquad (1 \le i, j \le n).$$

Alors

$$G^* = \mathbb{Z}f_{r+1} + \cdots + \mathbb{Z}f_\ell + \mathbb{R}f_{\ell+1} + \cdots + \mathbb{R}f_n.$$

Démonstration. Toute forme linéaire sur $\mathbb{R}^n$ s'écrit de manière unique $t_1 f_1 + \cdots + t_n f_n$, avec $(t_1, \dots, t_n) \in \mathbb{R}^n$, et une telle forme linéaire envoie G dans $\mathbb{Z}$ si et seulement si on a $t_i = 0$ pour $1 \le i \le r$ et $t_i \in \mathbb{Z}$ pour $r < i \le \ell$. □

Démonstration de la proposition 4.4. Si G est fermé, le lemme 4.6 donne facilement $(G^*)^* = G$. Dans le cas général, on a $G^* = (\overline{G})^*$ d'après le lemme 4.5, donc

$$(G^*)^* = \big((\overline{G})^*\big)^* = \overline{G}.$$

□

On déduit de la proposition 4.4 que G est dense dans $\mathbb{R}^n$ si et seulement si $G^* = \{0\}$. En effet, si $G^* = \{0\}$, alors $\overline{G} = (G^*)^* = \mathbb{R}^n$ et G est dense dans $\mathbb{R}^n$. Inversement, si $\overline{G} = \mathbb{R}^n$, alors $(\overline{G})^* = \{0\}$, et en utilisant le lemme 4.5 on peut conclure $G^* = \{0\}$.

Exercice.
1) Soient G_1 et G_2 des sous-groupes fermés de $\mathbb{R}^n$. Vérifier

$$(G_1 + G_2)^* = G_1^* \cap G_2^* \qquad \text{et} \qquad (G_1 \cap G_2)^* = \overline{G_1^* + G_2^*}.$$

2) Soit G un réseau de $\mathbb{R}^n$. Vérifier que G^* est un réseau de $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$ *(on dit que le*

réseau G^* est dual *de G). Quel est le réseau dual de G^* ?*
3) Soient G_1 et G_2 deux réseaux de $\mathbb{R}^n$, avec $G_2 \subset G_1$. Vérifier que les deux groupes finis G_1/G_2 et G_2^*/G_1^* sont isomorphes.

Exercice. Soit G un sous-groupe de $\mathbb{R}^n$.
a) On suppose que pour tout hyperplan H de $\mathbb{R}^n$, $G/G \cap H$ est dense dans $\mathbb{R}^n/H$. Alors G est dense dans $\mathbb{R}^n$.
b) En déduire l'énoncé suivant : si $G/G \cap D$ est dense dans $\mathbb{R}^n/D$ pour toute droite D de $\mathbb{R}^n$, alors G est dense dans $\mathbb{R}^n$.

§5. Sous-groupes minimaux de $\mathbb{R}^n$

Dans [R 1990a] et [R 1990b], D. Roy introduit et étudie la notion de sous-groupe minimal dense de $\mathbb{R}^n$: un sous-groupe de type fini G de $\mathbb{R}^n$ est dit *minimal dense* s'il est dense dans $\mathbb{R}^n$, et si aucun sous-groupe de G de rang strictement inférieur au rang de G n'est dense dans $\mathbb{R}^n$. Par exemple un sous-groupe de la forme $\mathbb{Z}^n + \mathbb{Z}(\theta_1, \dots, \theta_n)$ avec $1, \theta_1, \dots, \theta_n$ linéairement indépendants sur $\mathbb{Q}$ est minimal dense. Un autre exemple de sous-groupe minimal dense, de rang $2n$, est donné par $(\mathbb{Z} + \mathbb{Z}\alpha)^n$, où α est un nombre réel algébrique de degré 2 (quadratique). Si G est un sous-groupe minimal dense de $\mathbb{R}^n$ de rang $2n$, alors Roy montre qu'il existe une base $u_1, \dots, u_n$ de $\mathbb{R}^n$, et un corps quadratique réel k, tels que $\mathbb{Q}G = ku_1 + \cdots + ku_n$. De plus, tout sous-groupe minimal dense de $\mathbb{R}^n$ a un rang $\le 2n$. Ceci est démontré dans [R 1990a], prop. 4.5.

Nous démontrons dans cette section les résultats de D. Roy qui nous seront utiles dans la suite. Nous nous limitons au cas des deux corps $\mathbb{Q} \subset \mathbb{R}$ qui interviennent pour la densité, mais dans toute cette section on peut remplacer $\mathbb{Q}$ et $\mathbb{R}$ par deux corps $k \subset K$.

Exercice. Soit α un nombre réel. Le sous-groupe $G = (\mathbb{Z} + \mathbb{Z}\alpha)^2$ de $\mathbb{R}^2$ est minimal dense si et seulement si α est irrationnel quadratique.
`Indication.` *Considérer les trois éléments $(\alpha, 0)$, $(0, 1)$ et $(1, \alpha)$ de G.*

Nous utiliserons un résultat de D. Roy démontré dans [R 1992b], lemme 3.3, selon lequel, si G est un sous-groupe de type fini de $\mathbb{R}^n$ tel que tout sous-groupe de G de rang $\ge \mathrm{rang}_{\mathbb{Z}} G - n + 1$ soit dense dans $\mathbb{R}^n$, alors il existe un sous-groupe de G de rang $n+1$ qui est dense dans $\mathbb{R}^n$. Le résultat est un peu plus précis : on peut imposer aux sous-groupes considérés de contenir un réseau G_0 donné dans G. Ceci est d'ailleurs développé dans les travaux de Roy sous le nom de *sous-groupe minimal relatif.*

Théorème 5.1 (Roy). – *Soient G un sous-groupe de type fini de $\mathbb{R}^n$ et G_0 un sous-groupe de G discret dans $\mathbb{R}^n$; on suppose qu'aucun sous-groupe de G, contenant G_0, et de rang $n+1$ sur $\mathbb{Z}$, n'est dense dans $\mathbb{R}^n$. Alors il existe un sous-groupe de G, contenant G_0, de rang $\ge \mathrm{rang}_{\mathbb{Z}} G - n + 1$, qui n'est pas dense dans $\mathbb{R}^n$.*

Par exemple le sous-groupe $(\mathbb{Z} + \mathbb{Z}\sqrt{2})^n$ de $\mathbb{R}^n$ est de rang $2n$, il est dense dans $\mathbb{R}^n$, et il ne contient aucun sous-groupe de rang $< 2n$ qui soit dense dans $\mathbb{R}^n$.

Démonstration. On peut supposer que G est dense dans $\mathbb{R}^n$, sinon la conclusion est banale. Il n'y a pas de restriction à supposer que G_0 est un réseau de $\mathbb{R}^n$ (tout sous-groupe discret de G est contenu dans un réseau inclus dans G). Par hypothèse, pour tout g dans G, le sous-groupe $G_0 + \mathbb{Z}g$ de G n'est pas dense dans $\mathbb{R}^n$; la proposition 4.3 montre qu'il existe une forme linéaire non nulle ϕ sur $\mathbb{R}^n$ telle que $\phi(G_0) \subset \mathbb{Z}$ et $\phi(g) \in \mathbb{Z}$. On introduit le *réseau dual* G_0^* de G_0 :

$$G_0^* = \{\phi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R});\ \phi(G_0) \subset \mathbb{Z}\};$$

(voir la fin de la section 4). Ainsi pour tout g dans G,

$$X(g) = \{\phi \in G_0^*;\ \phi(g) \in \mathbb{Z}\}$$

est un sous-$\mathbb{Z}$-module non nul de G_0^*. On choisit d'abord $g_1 \in G$ tel que $X(g_1)$ soit de rang minimal sur $\mathbb{Z}$, puis $\phi_1 \in X(g_1)$, $\phi_1 \neq 0$, et on pose

$$G_1 = \{g \in G;\ \phi_1(g) \in \mathbb{Z}\}.$$

Ainsi G_1 est sous-groupe de G contenant G_0, et la forme linéaire non nulle ϕ_1 vérifie $\phi_1(G_1) \subset \mathbb{Z}$, donc (proposition 4.3) G_1 n'est pas dense dans $\mathbb{R}^n$. Il ne reste plus qu'à vérifier que G_1 a un rang sur $\mathbb{Z}$ au moins égal à $\mathrm{rang}_{\mathbb{Z}} G - n + 1$.

Il est plus commode de travailler avec des $\mathbb{Q}$-espaces vectoriels qu'avec des $\mathbb{Z}$-modules : on désigne par $\mathbb{Q}G$ le $\mathbb{Q}$-espace vectoriel engendré par G dans $\mathbb{R}^n$:

$$\mathbb{Q}G = \{x \in \mathbb{R}^n;\ \text{il existe } d \in \mathbb{Z},\ d > 0, \text{ tel que } dx \in G\}.$$

On définit de même $\mathbb{Q}G_0^* \subset \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$. Pour chaque $g \in \mathbb{Q}G$, on définit une application $\mathbb{Q}$-linéaire $\theta(g)$ de $\mathbb{Q}G_0^*$ dans $\mathbb{R}/\mathbb{Q}$ qui envoie ϕ sur la classe de $\phi(g)$ modulo $\mathbb{Q}$. Le noyau de $\theta(g)$ est $\mathbb{Q}X(g)$. On obtient un homomorphisme

$$\begin{array}{rccc} \theta: & \mathbb{Q}G & \longrightarrow & \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}G_0^*, \mathbb{R}/\mathbb{Q}) \\ & g & \longmapsto & \theta(g) : \phi \mapsto \phi(g) + \mathbb{Q}. \end{array}$$

Le choix qui a été fait de $g_1 \in G$ avec $X(g_1)$ de rang minimal signifie que l'application linéaire $\theta(g_1)$ est de rang maximal. Comme $0 \neq \phi_1 \in \mathrm{Ker}\ \theta(g_1)$, $\theta(g_1)$ n'est pas injective et la dimension sur $\mathbb{Q}$ de l'image de $\theta(g_1)$ est $< n$. Le lemme suivant, encore dû à D. Roy, donne, pour tout $g \in \mathbb{Q}G$,

$$\phi_1(g) + \mathbb{Q} = \theta(g)(\phi_1) \in \mathrm{Im}\ \theta(g_1).$$

Alors l'application

$$\begin{array}{rccc} \theta_1: & \mathbb{Q}G & \longrightarrow & \mathbb{R}/\mathbb{Q} \\ & g & \longmapsto & \phi_1(g) + \mathbb{Q} \end{array}$$

a une image contenue dans celle de $\theta(g_1)$. En particulier l'image de θ_1 est un $\mathbb{Q}$-espace vectoriel de dimension $\leq n-1$. Des égalités

$$\dim_{\mathbb{Q}} \mathrm{Ker}\ \theta_1 + \dim_{\mathbb{Q}} \mathrm{Im}\ \theta_1 = \dim_{\mathbb{Q}} \mathbb{Q}G = \mathrm{rang}_{\mathbb{Z}} G,$$

on déduit

$$\dim_{\mathbb{Q}} \mathrm{Ker}\ \theta_1 \geq \mathrm{rang}_{\mathbb{Z}} G - n + 1.$$

Enfin $\mathrm{Ker}\ \theta_1 \subset \mathbb{Q}G_1$, donc $\mathrm{rang}_{\mathbb{Z}} G_1 = \dim_{\mathbb{Q}} \mathbb{Q}G_1 \geq \mathrm{rang}_{\mathbb{Z}} G - n + 1$. $\square$

Il reste encore à établir le lemme suivant qui vient d'être utilisé (voir [R 1990a], lemme 3.4) :

Lemme 5.2. – *Soient E_1 et E_2 deux $\mathbb{Q}$-espaces vectoriels et F un sous-espace vectoriel de $\mathrm{Hom}_{\mathbb{Q}}(E_1, E_2)$. On suppose que E_1 et F sont de dimension finie. Soit S un élément de F de rang maximal. Alors pour tout $T \in F$ on a*

$$T(\mathrm{Ker}\ S) \subset \mathrm{Im}\ S.$$

Dans la démonstration du théorème 5.1, on avait

$$E_1 = \mathbb{Q}G_0^*, \quad E_2 = \mathbb{R}/\mathbb{Q}, \quad F = \theta(\mathbb{Q}G), \quad S = \theta(g_1), \quad T = \theta(g).$$

Comme $\phi_1 \in \mathrm{Ker}\ S$, on obtient

$$\phi_1(g) + \mathbb{Q} = \theta(g)(\phi_1) \in \mathrm{Im}\ S = \mathrm{Im}\ \theta(g_1).$$

Démonstration. Soient u un élément de $\mathrm{Ker}\ S$ et $(u_1, \ldots, u_r)$ une base d'un supplémentaire de $\mathrm{Ker}\ S$ dans E_1. L'image de S est le $\mathbb{Q}$-espace vectoriel engendré par $S(u_1), \ldots, S(u_r)$. On veut montrer que $T(u)$ appartient à ce sous-espace, c'est-à-dire que les $r+1$ éléments

$$S(u_1), \ldots, S(u_r), T(u)$$

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

Pour tout $x \in \mathbb{Q}$, le rang de $S + Tx$ est $\leq r$, et par conséquent les $r+1$ éléments

$$(S + xT)(u_1), \ldots, (S + xT)(u_r), (S + xT)(u)$$

sont linéairement dépendants sur $\mathbb{Q}$. Comme $S(u) = 0$, on en déduit que pour tout $x \in \mathbb{Q}$,

$$(S + xT)(u_1), \ldots, (S + xT)(u_r), xT(u)$$

sont linéairement dépendants sur $\mathbb{Q}$. Pour $x \neq 0$, cela veut dire que

$$(S + xT)(u_1), \ldots, (S + xT)(u_r), T(u)$$

sont linéairement dépendants sur $\mathbb{Q}$. Ceci est encore vrai pour $x = 0$: en effet, ces conditions s'expriment par l'annulation des mineurs $(r+1) \times (r+1)$ d'une matrice à coefficients dans $\mathbb{Q}$; ces mineurs sont des polynômes en x, et le fait que le coefficient de x soit nul signifie que $S(u_1), \ldots, S(u_r), T(u)$ sont linéairement dépendants sur $\mathbb{Q}$. $\square$

Remarque. L'ensemble des $S \in F$ de rang maximal forme un ouvert de Zariski *de F.* (L'espace vectoriel F est de dimension finie sur $\mathbb{Q}$; un choix de base l'identifie à $\mathbb{Q}^n$, et la topologie de Zariski sur F est induite par celle sur l'espace affine de dimension n sur $\mathbb{Q}$). En effet, si $(T_1, \ldots, T_n)$ est une base de F sur $\mathbb{Q}$, un choix de bases de E_1 et E_2 permet d'associer à T_i une matrice M_i ; pour chaque entier $m \geq 0$, soit I_m l'idéal de $\mathbb{Q}[X_1, \ldots, X_n]$ engendré par les mineurs $m \times m$ de la matrice $X_1 M_1 + \cdots + X_n M_n$; soit enfin r le plus grand entier tel que l'idéal I_r ne soit pas nul. Alors tout élément de F a un rang $\leq r$, et les éléments de F de rang $< r$ sont ceux de la forme $a_1T_1 + \cdots + a_nT_n$ où $(a_1,\dots,a_n) \in \mathbb{Q}^n$ est un zéro de I_r ; ils forment donc un fermé de Zariski.

Exercice. Soient n et s des entiers positifs et $M_1,\dots,M_s$ des matrices carrées $n\times n$ à coefficients rationnels. On désigne par

$$F = \{M_1x_1 + \cdots + M_sx_s\,;\,(x_1,\dots,x_s) \in \mathbb{Q}^s\}$$

le sous-espace vectoriel de $\mathrm{Mat}_{n\times n}(\mathbb{Q})$ engendré par $M_1,\dots,M_s$. On suppose que tout élément de F a un déterminant nul. On suppose aussi qu'il existe un élément S de F de rang $n-1$. Soient u et v deux éléments de $\mathbb{Q}^n$ tels que $Su = 0$ et $vS = 0$. Montrer que pour tout $T \in F$, on a $vTu = 0$.

N.B. Les relations $Su = 0$, $vS = 0$ et $vTu = 0$ s'écrivent respectivement

$$S\begin{pmatrix} u_1\\ \vdots\\ u_n\end{pmatrix} = \begin{pmatrix} 0\\ \vdots\\ 0\end{pmatrix}, \qquad (\,v_1 \quad \cdots \quad v_n\,)\,S = (\,0 \quad \cdots \quad 0\,)$$

et

$$(\,v_1 \quad \cdots \quad v_n\,)\,T\begin{pmatrix} u_1\\ \vdots\\ u_n\end{pmatrix} = (\,0\,)\,.$$

Mode d'emploi des résultats des sections 4 et 5. On veut montrer que certains sous-groupes G de $\mathbb{R}^n$ sont denses ; par exemple on s'intéressera aux sous-groupes engendrés par des points dont les coordonnées sont des logarithmes de nombres algébriques. Pour utiliser la condition *(iii)* de la proposition 4.3, on est amené à rechercher une majoration du rang de $G\cap H$, quand H est un hyperplan de $\mathbb{R}^n$, à savoir $\mathrm{rang}_{\mathbb{Z}} G\cap H \le \mathrm{rang}_{\mathbb{Z}} G - 2$. Pour certaines classes de groupes G, on obtiendra une majoration de $\mathrm{rang}_{\mathbb{Z}} G\cap H$ indépendante du rang de G ; alors il suffira de prendre un groupe G dans une telle classe de rang suffisamment élevé pour conclure à la densité. De même, en appliquant le théorème 5.1, on pourra conclure que G contient un sous-groupe de rang $n+1$ dense dans $\mathbb{R}^n$.

Corollaire 5.3. – *Soient n, ℓ et k trois entiers positifs et G un sous-groupe de type fini de $\mathbb{R}^n$ de rang ℓ sur $\mathbb{Z}$. On suppose que pour tout hyperplan H de $\mathbb{R}^n$, on a $\mathrm{rang}_{\mathbb{Z}} G\cap H \le k$.*
(i) Si $\ell \ge k+2$, alors G est dense dans $\mathbb{R}^n$.
(ii) Si $\ell \ge k+n+1$, alors G contient un sous-groupe de rang $n+1$ qui est dense dans $\mathbb{R}^n$.

Démonstration. La propriété *(i)* résulte de l'équivalence *(i)* $\Leftrightarrow$ *(iii)* dans la proposition 4.3 : si $\mathrm{rang}_{\mathbb{Z}} G\cap H \le \ell - 2$ pour tout hyperplan H de $\mathbb{R}^n$, alors $\mathrm{rang}_{\mathbb{Z}} G/G\cap H \ge 2$ et G est dense dans $\mathbb{R}^n$.

Supposons maintenant $\mathrm{rang}_{\mathbb{Z}} G\cap H \le \ell - n - 1$ pour tout hyperplan H de $\mathbb{R}^n$. Soit G' un sous-groupe de G de rang $\ge \ell - n + 1$. On a

$$\mathrm{rang}_{\mathbb{Z}} G'\cap H \le \mathrm{rang}_{\mathbb{Z}} G\cap H \le \ell - n - 1,$$

donc $\mathrm{rang}_{\mathbb{Z}} G'/G'\cap H \ge 2$ pour tout hyperplan H de $\mathbb{R}^n$, ce qui montre que tout sous-groupe de G de rang $\ge \ell - n + 1$ est dense dans $\mathbb{R}^n$. Le théorème 5.1 permet de conclure. $\square$

§6. Sous-groupes de $\mathbb{C}^n$

Le théorème de Kronecker permet aussi de donner un critère pour qu'un sous-groupe de type fini $\mathbb{C}^n$ soit dense. On identifie $\mathbb{C}$ avec $\mathbb{R}^2$ (et donc $\mathbb{C}^n$ avec $\mathbb{R}^{2n}$) en prenant la partie réelle et la partie imaginaire : pour $z \in \mathbb{C}$ on écrit $z = \Re\mathrm{e}\, z + i\Im\mathrm{m}\, z$. On travaillera plutôt avec le complexe conjugué (on désignera par $\overline{z} = \Re\mathrm{e}\, z - i\Im\mathrm{m}\, z$ le complexe conjugué de $z \in \mathbb{C}$), ce qui revient fondamentalement au même, puisque

$$\begin{pmatrix} z_1 & \cdots & z_n\\ \overline{z}_1 & \cdots & \overline{z}_n\end{pmatrix} = \begin{pmatrix} 1 & i\\ 1 & -i\end{pmatrix}\begin{pmatrix} \Re\mathrm{e}\, z_1 & \cdots & \Re\mathrm{e}\, z_n\\ \Im\mathrm{m}\, z_1 & \cdots & \Im\mathrm{m}\, z_n\end{pmatrix}.$$

Quand V et $\overline{V}$ sont deux espaces vectoriels sur $\mathbb{C}$, un anti-isomorphisme est un isomorphisme de $\mathbb{R}$-espaces vectoriels $\tau : V \longrightarrow \overline{V}$ qui vérifie

$$\tau(\lambda z) = \overline{\lambda}\tau(z) \qquad \text{pour } \lambda \in \mathbb{C} \text{ et } z \in V.$$

L'application $\mathbb{R}$-linéaire φ de V dans $V\times\overline{V}$, qui envoie z sur $\bigl(z,\tau(z)\bigr)$, a pour image

$$\varphi(V) = \bigl\{\bigl(z,\tau(z)\bigr);\ z \in V\bigr\} \subset V\times\overline{V},$$

qui n'est pas un sous-$\mathbb{C}$-espace vectoriel de $V\times\overline{V}$, mais qui est isomorphe à V comme $\mathbb{R}$-espace vectoriel.

Si $(e_1,\dots,e_n)$ est une base de V sur $\mathbb{C}$, alors $(e_1,\dots,e_n,ie_1,\dots,ie_n)$ est une base de V sur $\mathbb{R}$, et $\bigl(\tau(e_1),\dots,\tau(e_n)\bigr)$ est une base de $\overline{V}$ sur $\mathbb{C}$. Pour $z = z_1e_1 + \cdots + z_ne_n \in V$ avec $(z_1,\dots,z_n) \in \mathbb{C}^n$, on a $\tau(z) = \overline{z}_1\tau(e_1) + \cdots + \overline{z}_n\tau(e_n) \in \overline{V}$ et

$$\varphi(z) = \sum_{\nu=1}^{n}\bigl((\Re\mathrm{e}\, z_\nu)\varphi(e_\nu) + (\Im\mathrm{m}\, z_\nu)\varphi(ie_\nu)\bigr).$$

Ainsi $\bigl(\varphi(e_1),\dots,\varphi(e_n),\varphi(ie_1),\dots,\varphi(ie_n)\bigr)$ est une base de $\varphi(V)$ sur $\mathbb{R}$.

Voici le lemme qui nous permettra de ramener le problème de la densité complexe à une question diophantienne.

Proposition 6.1. – *Soient V et $\overline{V}$ deux espaces vectoriels sur $\mathbb{C}$, $\tau : V \longrightarrow \overline{V}$ un anti-isomorphisme et φ l'application $\mathbb{R}$-linéaire de V dans $V\times\overline{V}$ qui envoie z sur $\bigl(z,\tau(z)\bigr)$. Soit G un sous-groupe de type fini de V ; on définit $\widetilde{G} = \varphi(G)$:*

$$\widetilde{G} = \bigl\{\bigl(g,\tau(g)\bigr);\ g \in G\bigr\} \subset V\times\overline{V}.$$

Alors les quatre conditions suivantes sont équivalentes :
(i) G est dense dans V.
(ii) $\widetilde{G}$ est dense dans $\varphi(V)$.
(iii) Pour tout hyperplan complexe H de $V\times\overline{V}$ on a

$$\mathrm{rang}_{\mathbb{Z}}\bigl(\widetilde{G}/\widetilde{G}\cap H\bigr) \ge 2.$$

(iv) Choisissons une base $(e_1, \dots, e_n)$ *de* V *sur* $\mathbb{C}$ *et des générateurs* $g_1, \dots, g_\ell$ *de* G *sur* $\mathbb{Z}$ *; écrivons les coordonnées des* g_j *dans la base* $(e_1, \dots, e_n)$ *:*

$$g_j = g_{1j}e_1 + \cdots + g_{nj}e_n, \qquad (1 \le j \le \ell);$$

pour tout $(s_1, \dots, s_\ell)$ *dans* $\mathbb{Z}^\ell$ *distinct de* $(0, \dots, 0)$*, la matrice*

$$\begin{pmatrix} g_{11} & \cdots & g_{1\ell} \\ \vdots & \ddots & \vdots \\ g_{n1} & \cdots & g_{n\ell} \\ \overline{g}_{11} & \cdots & \overline{g}_{1\ell} \\ \vdots & \ddots & \vdots \\ \overline{g}_{n1} & \cdots & \overline{g}_{n\ell} \\ s_1 & \cdots & s_\ell \end{pmatrix}$$

est de rang $2n+1$.

Remarque. La condition (iii) s'exprime aussi de la manière suivante : pour tout forme linéaire complexe non nulle $\varphi : V \times \overline{V} \to \mathbb{C}$*, on a* $\mathrm{rang}_\mathbb{Z} \varphi(\widetilde{G}) \ge 2$.

Démonstration. L'équivalence entre *(i)* et *(ii)* est claire : l'application linéaire φ est injective, elle induit un isomorphisme de V sur $\varphi(V)$, et on a posé $\widetilde{G} = \varphi(G)$.

L'équivalence entre *(iii)* et *(iv)* est aussi facile : dire qu'il existe des entiers rationnels non tous nuls $s_1, \dots, s_\ell$ tels que la matrice de la condition *(iv)* ne soit pas de rang $2n+1$ revient à dire qu'il existe des nombres complexes $\vartheta_1, \dots, \vartheta_n, \kappa_1, \dots, \kappa_n$, non tous nuls, tels que, pour tout $(z_1, \dots, z_n)$ dans G, on ait

$$\sum_{j=1}^n \vartheta_j z_j + \sum_{j=1}^n \kappa_j \overline{z}_j \in \mathbb{Z};$$

ceci signifie donc que l'hyperplan d'équation $\sum_{j=1}^n \vartheta_j z_j + \sum_{j=1}^n \kappa_j \overline{z}_j = 0$ dans $V \times \overline{V}$ ne vérifie pas la condition (iii).

Pour vérifier l'équivalence entre les condition *(ii)* et *(iv)*, on utilise l'équivalence *(i)* $\Leftrightarrow$ *(vi)* des conditions de la proposition 4.3, en prenant $\big(\varphi(e_1), \dots, \varphi(e_n), \varphi(ie_1), \dots, \varphi(ie_n)\big)$ pour base de $\varphi(V)$, et on remarque que la matrice de la condition *(iv)* a le même rang que la matrice à coefficients réels

$$\begin{pmatrix} \Re\mathrm{e}\, g_{11} & \cdots & \Re\mathrm{e}\, g_{1\ell} \\ \vdots & \ddots & \vdots \\ \Re\mathrm{e}\, g_{n1} & \cdots & \Re\mathrm{e}\, g_{n\ell} \\ \Im\mathrm{m}\, g_{11} & \cdots & \Im\mathrm{m}\, g_{1\ell} \\ \vdots & \ddots & \vdots \\ \Im\mathrm{m}\, g_{n1} & \cdots & \Im\mathrm{m}\, g_{n\ell} \\ s_1 & \cdots & s_\ell \end{pmatrix}$$

$\square$

Remarque. On sait par la proposition 4.3 que la condition *(i)* équivaut à la suivante :
(v) Pour tout hyperplan réel L *de* V*, on a*

$$\mathrm{rang}_\mathbb{Z}\big(G/G \cap L\big) \ge 2.$$

Choisissons une base $(e_1, \dots, e_n)$ de V sur $\mathbb{C}$. Pour chaque $\vartheta = (\vartheta_1, \dots, \vartheta_n) \in \mathbb{C}^n$ avec $\vartheta \ne 0$, on définit un hyperplan (complexe) H_ϑ de $V \times \overline{V}$ par

$$H_\vartheta = \left\{ \left(\sum_{j=1}^n z_j e_j, \sum_{j=1}^n w_j \tau(e_j) \right) ;\ \sum_{j=1}^n \vartheta_j z_j + \sum_{j=1}^n \overline{\vartheta}_j w_j = 0 \right\}.$$

On va vérifier que la condition *(v)* est encore équivalente à :
(vi) Pour tout $\vartheta \in \mathbb{C}^n$*,* $\vartheta \ne 0$*, on a*

$$\mathrm{rang}_\mathbb{Z}\big(\widetilde{G}/\widetilde{G} \cap H_\vartheta\big) \ge 2.$$

Ecrivons pour cela une équation de L :

$$L = L_{\lambda,\mu} = \left\{ \sum_{j=1}^n (x_j + iy_j) e_j;\ \sum_{j=1}^n \lambda_j x_j + \sum_{j=1}^n \mu_j y_j = 0 \right\},$$

avec $(\lambda, \mu) = (\lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_n) \in \mathbb{R}^{2n} \setminus \{0\}$. On établit une bijection entre l'ensemble des hyperplans complexes de $V \times \overline{V}$ de la forme H_ϑ, et l'ensemble de tous les hyperplans réels de V, en faisant correspondre à H_ϑ l'hyperplan $L_{\lambda,\mu}$ avec $\vartheta_j = \lambda_j - i\mu_j$, $(1 \le j \le n)$. Dans ces conditions, pour $z \in V$, on a $z \in L_{\lambda,\mu}$ si et seulement si $\varphi(z) \in H_\vartheta$. Donc

$$\mathrm{rang}_\mathbb{Z}\big(G/G \cap L_{\lambda,\mu}\big) = \mathrm{rang}_\mathbb{Z}\big(\widetilde{G}/\widetilde{G} \cap H_\vartheta\big).$$

Ceci montre que les conditions *(i)*, *(v)* et *(vi)* sont équivalentes.

Remarque. Le fait que *(vi)* est conséquence de *(iii)* est évident. D'autre part, on peut déduire directement *(iii)* de *(vi)* de la manière suivante. Supposons qu'il existe un hyperplan H de $V \times \overline{V}$ tel que

$$\mathrm{rang}_\mathbb{Z}\big(\widetilde{G}/\widetilde{G} \cap H\big) \le 1.$$

On choisit une équation de H de la forme

$$H = \left\{ \left(\sum_{j=1}^n z_j e_j, \sum_{j=1}^n w_j \tau(e_j) \right) ;\ \sum_{j=1}^n \vartheta_j z_j + \sum_{j=1}^n \kappa_j w_j = 0 \right\},$$

(avec $\vartheta_1, \dots, \vartheta_n, \kappa_1, \dots, \kappa_n$ nombres complexes non tous nuls), de sorte que, pour tout $z_1 e_1 + \cdots + z_n e_n$ dans G, on ait

$$\sum_{j=1}^n \vartheta_j z_j + \sum_{j=1}^n \kappa_j \overline{z}_j \in \mathbb{Z}.$$

On a alors aussi, en conjugant,

$$\sum_{j=1}^{n} \overline{\kappa}_j z_j + \sum_{j=1}^{n} \overline{\vartheta}_j \overline{z}_j \in \mathbb{Z},$$

donc

$$\sum_{j=1}^{n} (\vartheta_j + \overline{\kappa}_j) z_j + \sum_{j=1}^{n} (\kappa_j + \overline{\vartheta}_j) \overline{z}_j \in \mathbb{Z}.$$

Si $(\vartheta_1, \ldots, \vartheta_n) \neq -(\overline{\kappa}_1, \ldots, \overline{\kappa}_n)$, on pose $\vartheta'_j = \vartheta_j + \overline{\kappa}_j$, $(1 \leq j \leq n)$; sinon, on pose $\vartheta'_j = i\vartheta_j$. Dans les deux cas on voit que l'hyperplan $H_{\vartheta'}$ de $V \times \overline{V}$ vérifie

$$\operatorname{rang}_{\mathbb{Z}}\big(\widetilde{G}/\widetilde{G} \cap H_{\vartheta'}\big) \leq 1.$$

On va appliquer la proposition 6.1 en prenant pour V et $\overline{V}$ l'espace $\mathbb{C}^n$ et pour τ l'anti-isomorphisme donné par la conjugaison complexe sur chacune des n composantes ; on le notera encore $z \to \overline{z}$.

Corollaire 6.2. – *Soient n, ℓ et k trois entiers positifs et G un sous-groupe de type fini de $\mathbb{C}^n$ de rang ℓ sur $\mathbb{Z}$. On pose encore $\widetilde{G} = \{(g, \overline{g});\ g \in G\}$, et on suppose que pour tout hyperplan complexe H de $\mathbb{C}^{2n}$, on a $\operatorname{rang}_{\mathbb{Z}} \widetilde{G} \cap H \leq k$.*
(i) Si $\ell \geq k + 2$, alors G est dense dans $\mathbb{C}^n$.
(ii) Si $\ell \geq k + 2n + 1$, alors G contient un sous-groupe de rang $2n+1$ qui est dense dans $\mathbb{C}^n$.

Démonstration. La première affirmation résulte de l'équivalence entre les condition *(i)* et *(iii)* dans la proposition 6.1. Pour montrer la seconde, on suppose $\operatorname{rang}_{\mathbb{Z}} \widetilde{G} \cap H \leq \ell - 2n - 1$ pour tout hyperplan complexe H de $\mathbb{C}^{2n}$. Soit G' un sous-groupe de G de rang $\geq \ell - 2n + 1$. On a

$$\operatorname{rang}_{\mathbb{Z}} \widetilde{G'} \cap H \leq \operatorname{rang}_{\mathbb{Z}} \widetilde{G} \cap H \leq \ell - 2n - 1,$$

donc $\operatorname{rang}_{\mathbb{Z}} \widetilde{G'}/\widetilde{G'} \cap H \geq 2$ pour tout hyperplan complexe H de $\mathbb{C}^{2n}$, ce qui montre (grâce à la proposition 6.1) que tout sous-groupe de G de rang $\geq \ell - 2n + 1$ est dense dans $\mathbb{C}^n$. Le théorème 5.1 (avec n remplacé par $2n$) permet de conclure. □

§7. Sous-groupes de type fini d'un groupe de Lie réel ou complexe

Dans cette section on utilise les considérations précédentes pour étendre les résultats aux groupes de Lie commutatifs de dimension $n \geq 0$. Les notions dont nous avons besoin sur les groupe de Lie sont exposées par exemple dans [D 1972], t.3, Chap. 16, §9 et t.4, Chap. 19.

Un *groupe de Lie réel* est un groupe G muni d'une structure de variété différentiable telle que les applications $(x, y) \mapsto xy$ et $x \mapsto x^{-1}$ soient de classe C^∞. Un *groupe de Lie complexe* est un groupe G muni d'une structure de variété analytique complexe telle que les applications $(x, y) \mapsto xy$ et $x \mapsto x^{-1}$ soient holomorphes.

Dans un premier temps on suppose que R (groupe de Lie réel commutatif) est connexe : alors (par exemple d'après (19.7.9.2) dans [D 1972]) R est isomorphe à un produit $\mathbb{R}^p \times (\mathbb{R}/\mathbb{Z})^q$, où p et q sont deux entiers ≥ 0, et $p + q = n$ est la dimension de R (on peut prendre cela comme définition de R). Cela veut dire qu'il existe un homomorphisme de groupes de Lie surjectif $h : \mathbb{R}^n \to R$, dont le noyau est un sous-groupe discret H de $\mathbb{R}^n$, avec $\operatorname{rang}_{\mathbb{Z}} H = q$. Soit $\mathbb{R}H$ (resp. $\mathbb{Q}H$) le sous-espace de $\mathbb{R}^n$ sur $\mathbb{R}$ (resp. sur $\mathbb{Q}$) engendré par H. Alors H est un réseau de $\mathbb{R}H$, $h(\mathbb{R}H)$ est le sous-groupe compact maximal de R, isomorphe à $(\mathbb{R}/\mathbb{Z})^q$, tandis que $h(\mathbb{Q}H)$ est le sous-groupe de torsion de R, isomorphe à $(\mathbb{Q}/\mathbb{Z})^q$.

Quelques exemples. Le groupe multiplicatif $\mathbb{R}_+^\times$ est un groupe de Lie réel connexe isomorphe à $\mathbb{R}$. Le groupe multiplicatif $\mathbb{R}^\times$ est un groupe de Lie réel non connexe isomorphe à $\mathbb{R} \times (\mathbb{Z}/2\mathbb{Z})$. Un groupe de Lie complexe a une structure naturelle de groupe de Lie réel. L'application exponentielle $\exp : \mathbb{C} \to \mathbb{C}^\times$ dont le noyau est $2i\pi\mathbb{Z}$, induit un isomorphisme entre $\mathbb{C}^\times$ et $\mathbb{C}/2i\pi\mathbb{Z}$. Quand on compose avec l'isomorphisme $\mathbb{R}^2 \to \mathbb{C}$ qui envoie $(x, y) \in \mathbb{R}^2$ sur $x + iy \in \mathbb{C}$, on obtient un morphisme surjectif $h : (x, y) \mapsto e^{x+iy}$ de $\mathbb{R}^2$ sur $\mathbb{C}^\times$ de noyau $\{0\} \times 2\pi\mathbb{Z}$, qui donne un isomorphisme de groupes de Lie réels entre $\mathbb{R} \times (\mathbb{R}/\mathbb{Z})$ et $\mathbb{C}^\times$. L'image par cet isomorphisme du tore $\mathbb{R}/\mathbb{Z}$ est le sous-groupe compact maximal $\mathbb{U}$ de $\mathbb{C}^\times$.

R	n	p	q	h	H
$\mathbb{R}^d$	d	d	0	$h(x) = x$	$\{0\}$
$(\mathbb{R}_+^\times)^d$	d	d	0	$h(x) = \exp x$	$\{0\}$
$\mathbb{C}^d$	$2d$	$2d$	0	$h(x, y) = x + iy$	$\{0\}$
$(\mathbb{C}^\times)^d$	$2d$	d	d	$h(x, y) = \exp(x + iy)$	$(\{0\} \times 2\pi\mathbb{Z})^d$

Les *caractères* d'un groupe de Lie réel commutatif R sont les homomorphismes continus de R dans $\mathbb{R}/\mathbb{Z}$. Supposons de nouveau R connexe. Soit $\pi : \mathbb{R} \to \mathbb{R}/\mathbb{Z}$ la projection canonique. Pour chaque caractère χ de R, $\chi \circ h$ est un caractère du groupe additif $\mathbb{R}^n$, donc il existe une forme linéaire $\phi : \mathbb{R}^n \to \mathbb{R}$ telle que $\chi \circ h = \pi \circ \phi$:

$$\begin{array}{ccc} \mathbb{R}^n & \xrightarrow{h} & R \\ {\scriptstyle \phi}\downarrow & & \downarrow{\scriptstyle \chi} \\ \mathbb{R} & \xrightarrow[\pi]{} & \mathbb{R}/\mathbb{Z} \end{array}$$

Cela détermine un isomorphisme entre le groupe des caractères de R et le groupe additif des formes linéaires sur $\mathbb{R}^n$ qui appliquent H dans $\mathbb{Z}$.

Lemme 7.1. – *Soient R un groupe de Lie réel commutatif connexe et Γ un sous-groupe de type fini de R. Les assertions suivantes sont équivalentes.*

(i) Γ *est dense dans* R.
(ii) Si χ *est un caractère non trivial de* R*, alors le noyau de* χ *ne contient pas* Γ.

Démonstration. Posons $G = h^{-1}(\Gamma)$; alors G est un sous-groupe de $\mathbb{R}^n$ qui contient H, et Γ est dense dans R si et seulement si G est dense dans $\mathbb{R}^n$. La proposition 4.3 montre qu'une condition nécessaire et suffisante pour qu'il en soit ainsi est que G ne soit contenu dans aucun noyau d'un caractère non trivial de $\mathbb{R}^n$. $\square$

Exercice. Vérifier qu'un sous-groupe Γ *de* R *contient un sous-groupe de type fini dense dans* R *si et seulement si aucun caractère non trivial de* R *n'envoie* Γ *dans* $\mathbb{Q}/\mathbb{Z}$.

Dans le §2 de [R 1992b] est démontré le résultat suivant : *le rang d'un sous-groupe minimal dense de* $\mathbb{R}^p \times (\mathbb{R}/\mathbb{Z})^q$ *est* $\le 2p+q$ (on a déjà vu le cas $q=0$). La démonstration nécessite l'étude des sous-groupes denses de $\mathbb{R}^n$ *minimaux relativement à un sous-groupe discret* H *de* $\mathbb{R}^n$.

Nous utiliserons la notation suivante [R 1992b] : si G est un groupe topologique commutatif, le nombre $\mathrm{m}(G)$ désignera le plus petit rang (comme groupe abélien) d'un sous-groupe de G dense dans G. Ainsi, quand G est un groupe abélien fini muni de la topologie discrète, le nombre $\mathrm{m}(G)$ est le rang de G. Si p et q sont des entiers ≥ 0 avec $p+q>0$, on a

$$\mathrm{m}\big(\mathbb{R}^p \times (\mathbb{R}/\mathbb{Z})^q\big) = p+1.$$

Exercice. Soient a, b, c, d *des entiers* ≥ 0 *avec* $a+b+c+d>0$. *Vérifier que le groupe de Lie réel*

$$G = \mathbb{R}^a \times (\mathbb{R}^\times)^b \times \mathbb{C}^c \times (\mathbb{C}^\times)^d$$

est isomorphe à

$$\mathbb{R}^p \times (\mathbb{R}/\mathbb{Z})^d \times (\mathbb{Z}/2\mathbb{Z})^b$$

avec $p = a+b+2c+d$. *En déduire* $\mathrm{m}(G) = a+b+2c+d+1$.
`Indication.` On notera que G possède 2^b composantes connexes ; si G^0 est la composante connexe de l'élément neutre, le groupe quotient G/G^0 est de rang – comme groupe abélien – égal à b ; on utilisera l'inégalité $p+1 \ge b$.

Théorème 7.2 (Roy). – *Soient* R *un groupe de Lie réel commutatif connexe de dimension* n *et* Γ *un sous-groupe de type fini de* R*, de rang* ℓ *sur* $\mathbb{Z}$. *On suppose que tout sous-groupe de* Γ *de rang* $\ge \ell-n+1$ *sur* $\mathbb{Z}$ *est dense dans* R. *Alors il existe un sous-groupe de* Γ*, de rang* $\mathrm{m}(R)$ *sur* $\mathbb{Z}$*, qui est dense dans* R.

Démonstration. Désignons par q le rang du noyau H de h, et par $G = h^{-1}(\Gamma)$ l'image inverse de Γ dans $\mathbb{R}^n$; alors G est un sous-groupe de $\mathbb{R}^n$ de rang $\ell+q$ qui contient H, et tout sous-groupe de G de rang $\ge \ell+q-n+1$ qui contient H est dense dans $\mathbb{R}^n$. D'après le théorème 5.1 de Roy, il existe un sous-groupe de G de rang $n+1$ qui contient H et qui est dense dans $\mathbb{R}^n$; son image par h est un sous-groupe de Γ, de rang $n+1-q = \mathrm{m}(R)$, qui est dense dans R. $\square$

Exercice. Inversement, déduire le théorème 5.1 du théorème 7.2.

Exemple 1. Sous-groupes de type fini de $(\mathbb{R}^\times)^n$.

On déduit du lemme 1.5 un critère de densité pour un sous-groupe multiplicatif Γ de type fini de $(\mathbb{R}^\times)^n$ de la manière suivante.

Commençons par considérer la composante connexe $(\mathbb{R}_+^\times)^n$ de l'élément neutre dans $(\mathbb{R}^\times)^n$. Soit Γ_0 un sous-groupe de $(\mathbb{R}_+^\times)^n$; on désigne par Y l'image inverse de Γ_0 dans $\mathbb{R}^n$ par l'application exponentielle :

$$Y = \{y \in \mathbb{R}^n;\ \exp(y) \in \Gamma_0\} \subset \mathbb{R}^n;$$

comme l'application exponentielle établit un isomorphisme continu entre $\mathbb{R}^n$ et $(\mathbb{R}_+^\times)^n$, il en résulte que Γ_0 est dense dans $(\mathbb{R}_+^\times)^n$ si et seulement si Y est dense dans $\mathbb{R}^n$. Choisissons des générateurs $\gamma_1, \ldots, \gamma_\ell$ du $\mathbb{Z}$-module Γ_0 et écrivons les coordonnées des γ_j dans la base canonique de $\mathbb{R}^n$:

$$\gamma_j = (\gamma_{1j}, \ldots, \gamma_{nj}), \qquad \text{avec } \gamma_{\nu j} > 0 \text{ pour } 1 \le \nu \le n,\ 1 \le j \le \ell,$$

de sorte que

$$\Gamma_0 = \Big\{ \big(\gamma_{\nu 1}^{s_1} \cdots \gamma_{\nu \ell}^{s_\ell}\big)_{1 \le \nu \le n};\ (s_1, \ldots, s_\ell) \in \mathbb{Z}^\ell \Big\}.$$

D'après la proposition 4.3, Γ_0 est dense dans $(\mathbb{R}_+^\times)^n$ si et seulement si, pour tout $(s_1, \ldots, s_\ell)$ dans $\mathbb{Z}^\ell$ distinct de $(0, \ldots, 0)$, la matrice

$$\begin{pmatrix} \log \gamma_{11} & \cdots & \log \gamma_{1\ell} \\ \vdots & \ddots & \vdots \\ \log \gamma_{n1} & \cdots & \log \gamma_{n\ell} \\ s_1 & \cdots & s_\ell \end{pmatrix}$$

est de rang $n+1$.

Une fois qu'un sous-groupe Γ de $(\mathbb{R}^\times)^n$ a une intersection $\Gamma_0 = \Gamma \cap (\mathbb{R}_+^\times)^n$ avec $(\mathbb{R}_+^\times)^n$ qui est dense, l'adhérence de Γ est une réunion de composantes connexes de $(\mathbb{R}^\times)^n$; en particulier un tel sous-groupe Γ est dense dans $(\mathbb{R}^\times)^n$ si et seulement s'il a un point dans chacune des 2^n composantes. Il suffit en fait de vérifier que l'intersection de Γ avec les n composantes connexes

$$C_\nu = \big\{(x_1, \ldots, x_n) \in (\mathbb{R}^\times)^n;\ x_\nu < 0,\ x_\mu > 0, (1 \le \mu \le n, \mu \ne \nu)\big\}, \qquad (1 \le \nu \le n)$$

n'est pas vide :

Lemme 7.3. – *Soit* Γ *un sous-groupe de type fini de* $(\mathbb{R}^\times)^n$ *dont l'intersection* $\Gamma \cap (\mathbb{R}_+^\times)^n$ *avec* $(\mathbb{R}_+^\times)^n$ *est dense dans* $(\mathbb{R}_+^\times)^n$. *Les conditions suivantes sont équivalentes :*
(i) Γ *est dense dans* $(\mathbb{R}^\times)^n$.
(ii) Pour $1 \le \nu \le n$, $\Gamma \cap C_\nu \ne \emptyset$.

Démonstration. Les images de $C_1, \ldots, C_n$ par la surjection $(\mathbb{R}^\times)^n \to (\mathbb{Z}/2\mathbb{Z})^n$ forment un système générateur du groupe $(\mathbb{Z}/2\mathbb{Z})^n$. $\square$

Exercice. Soit G est un sous-groupe de $(\mathbb{R}_+^\times)^n$, dense et de type fini. Montrer qu'il existe un sous-groupe Γ de $(\mathbb{R}^\times)^n$, dense et de type fini, tel que G soit contenu dans Γ et d'indice 2^n dans Γ.

Exercice. En utilisant le théorème 7.2, donner une condition suffisante pour qu'un sous-groupe de type fini de $(\mathbb{R}^\times)^n$ contienne un sous-groupe de rang $n+1$ qui soit dense dans $(\mathbb{R}^\times)^n$.

Exemple 2. Sous-groupes de type fini de $(\mathbb{C}^\times)^n$.

On a vu que $\mathbb{C}^\times$ était isomorphe, comme groupe de Lie réel, à $\mathbb{R}\times(\mathbb{R}/\mathbb{Z})$; de plus $\mathbb{C}^\times$ est connexe et $\mathrm{m}(\mathbb{C}^\times)^n = n+1$.

Soient $\gamma_1,\dots,\gamma_\ell$ des éléments multiplicativement indépendants de $(\mathbb{C}^\times)^n$; on veut savoir si le sous-groupe Γ qu'ils engendrent est dense dans $(\mathbb{C}^\times)^n$. Ecrivons les coordonnées des γ_j dans la base canonique :

$$\gamma_j = (\gamma_{1j},\dots,\gamma_{nj}), \qquad (1\le j\le \ell).$$

On choisit ensuite des logarithmes $g_1,\dots,g_\ell$ de $\gamma_1,\dots,\gamma_\ell$ respectivement :

$$g_j = (g_{1j},\dots,g_{nj}), \qquad (1\le j\le \ell).$$

Ainsi $g_{\nu j}$ est un nombre complexe vérifiant $e^{g_{\nu j}} = \gamma_{\nu j}$, $(1\le\nu\le n,\ 1\le j\le\ell)$; ce nombre complexe n'est déterminé que modulo $2i\pi\mathbb{Z}$; mais le sous-groupe

$$G = \mathbb{Z}g_1+\dots+\mathbb{Z}g_\ell + (2i\pi\mathbb{Z})^n \subset \mathbb{C}^n$$

ne dépend pas des choix de ces logarithmes : si $\exp : \mathbb{C}^n \to (\mathbb{C}^\times)^n$ désigne encore l'application exponentielle, on a $G = \exp^{-1}(\Gamma)$. Par abus de notation on posera $g_{\nu j} = \log\gamma_{\nu j}$ et on écrira $\log(\gamma_{\nu j}/\overline{\gamma}_{\nu j})$ au lieu de $g_{\nu j} - \overline{g}_{\nu j}$ (où $\overline{z}$ désigne toujours le nombre complexe conjugué de z).

On en déduit que le sous-groupe Γ est dense dans $(\mathbb{C}^\times)^n$ si et seulement si, pour tout $(s_1,\dots,s_\ell,t_1,\dots,t_n)\in\mathbb{Z}^{\ell+n}$ différent de $(0,\dots,0)$, la matrice suivante a pour rang $2n+1$:

$$\begin{pmatrix}
\log|\gamma_{11}| & \cdots & \log|\gamma_{1\ell}| & 0 & \cdots & 0\\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\
\log|\gamma_{n1}| & \cdots & \log|\gamma_{n\ell}| & 0 & \cdots & 0\\
\log(\gamma_{11}/\overline{\gamma}_{11}) & \cdots & \log(\gamma_{1\ell}/\overline{\gamma}_{1\ell}) & 2i\pi & \cdots & 0\\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\
\log(\gamma_{n1}/\overline{\gamma}_{n1}) & \cdots & \log(\gamma_{n\ell}/\overline{\gamma}_{n\ell}) & 0 & \cdots & 2i\pi\\
s_1 & \cdots & s_\ell & t_1 & \cdots & t_n
\end{pmatrix}$$

Par combinaisons linéaires des lignes, on voit que cette condition équivaut à dire que, pour tout $(s_1,\dots,s_\ell,t_1,\dots,t_n)\in\mathbb{Z}^{\ell+n}$ différent de $(0,\dots,0)$, les ℓ éléments suivants de $\mathbb{R}^{n+1}$ engendrent $\mathbb{R}^{n+1}$:

$$\Big(\log|\gamma_{1j}|,\dots,\log|\gamma_{nj}|, 2i\pi s_j + t_1\log(\gamma_{1j}/\overline{\gamma}_{1j})+\dots+t_n\log(\gamma_{nj}/\overline{\gamma}_{nj})\Big) \quad (1\le j\le\ell).$$

Quand on se restreint aux $(s_1,\dots,s_\ell,t_1,\dots,t_n)\in\mathbb{Z}^{\ell+n}$ pour lesquels $t_1=\dots=t_n=0$, la condition que l'on trouve exprime que la projection de Γ sur $\mathbb{R}^n$ (c'est-à-dire la projection de Γ sur le quotient de $(\mathbb{C}^\times)^n$ par le sous-groupe compact maximal) est dense dans $\mathbb{R}^n$.

Exercice. Soit Γ un sous-groupe de $(\mathbb{C}^\times)^n$ de rang $n+1$ et soient $\gamma_1,\dots,\gamma_{n+1}$ des éléments multiplicativement indépendants de Γ. Choisissons des éléments x_j et y_j dans $\mathbb{R}^n$ avec

$$\gamma_j = \exp(x_j+iy_j), \qquad (1\le j\le n+1).$$

On définit des nombres réels

$$\Delta_h = \det\Big(x_{\nu j}\Big)_{\substack{1\le\nu\le n\\ 1\le j\le n+1,\ j\ne h}}, \qquad (1\le h\le n+1)$$

et

$$\delta_k = \det\begin{pmatrix} x_{11} & \cdots & x_{1,n+1}\\ \vdots & \ddots & \vdots\\ x_{n1} & \cdots & x_{n,n+1}\\ y_{k1} & \cdots & y_{k,n+1}\end{pmatrix}, \qquad (1\le k\le n).$$

Vérifier que les conditions suivantes sont équivalentes :
(i) Le sous-groupe Γ est dense dans $(\mathbb{C}^\times)^n$.
(ii) Les $2n+1$ nombres réels

$$\Delta_1,\dots,\Delta_{n+1},\ \frac{1}{\pi}\delta_1,\dots,\frac{1}{\pi}\delta_n,$$

sont linéairement indépendants sur $\mathbb{Q}$.
(iii) Pour $s_1,\dots,s_{n+1}$, $t_1,\dots,t_n$ dans $\mathbb{Z}$ non tous nuls, le déterminant des $n+1$ vecteurs

$$(x_{1j},\dots,x_{nj}, t_1y_{1j}+\dots+t_ny_{nj}+s_j\pi), \qquad (1\le j\le n+1)$$

n'est pas nul.

`Exemple` $(n=1)$. Soient $\gamma_1 = e^{x_1+iy_1}$ et $\gamma_2 = e^{x_2+iy_2}$ deux nombres complexes. Les conditions suivantes sont équivalentes :
(i) Le sous-groupe
$$\Gamma = \{\gamma_1^{s_1}\gamma_2^{s_2};\ (s_1,s_2)\in\mathbb{Z}^2\}$$
est dense dans $\mathbb{C}^\times$.
(ii) Les 3 nombres réels
$$x_1,\quad x_2,\quad \frac{1}{\pi}(x_1y_2-x_2y_1)$$
sont linéairement indépendants sur $\mathbb{Q}$.
(iii) Pour s_1, s_2, t entiers rationnels non tous trois nuls, le déterminant

$$\det\begin{pmatrix} x_1 & x_2\\ ty_1+s_1\pi & ty_2+s_2\pi\end{pmatrix}$$

n'est pas nul.

Exercice. En utilisant le théorème 7.2, donner une condition suffisante pour qu'un sous-groupe de type fini de $(\mathbb{C}^\times)^n$ *contienne un sous-groupe de rang* $n+1$ *qui soit dense dans* $(\mathbb{C}^\times)^n$.

Exemple 3. Un cas mixte : plongement canonique d'un corps de nombres.

Pour donner une colloration arithmétique à ce chapitre, nous allons terminer par un exemple dans lequel on considère un sous-groupe engendré par des éléments *algébriques* (aucun des autres énoncés ne faisait intervenir une telle hypothèse).

Soit k un corps de nombres de degré n sur $\mathbb{Q}$: il existe un élément α de k tel que k soit égal à $\mathbb{Q}(\alpha)$. Désignons par $f \in \mathbb{Q}[X]$ le polynôme irréductible de α sur $\mathbb{Q}$; le degré de f est égal à n. On désigne par $\alpha_1, \dots, \alpha_n$ les n racines (deux-à-deux distinctes, car f est irréductible) de f dans $\mathbb{C}$:

$$f(X) = \prod_{j=1}^{n} (X - \alpha_j).$$

On choisit une numérotation de ces racines de telle sorte que les nombres $\alpha_1, \dots, \alpha_{r_1}$ soient réels, tandis que, pour $r_1 < j \le r_1 + r_2$, les deux nombres complexes α_j et α_{r_2+j} sont conjugués ; les entiers r_1 et r_2 ainsi déterminés ne dépendent pas du choix du générateur α de k ; ils satisfont $0 \le r_1 \le n$, $0 \le r_2 \le n$ et $r_1 + 2r_2 = n$. Le couple (r_1, r_2) est la *signature* du corps de nombres k.

Pour chaque indice j dans l'intervalle $1 \le j \le n$, il existe un unique homomorphisme de corps de k dans $\mathbb{C}$ qui envoie α sur α_j ; on le note σ_j. L'image de σ_j est $\mathbb{Q}(\alpha_j)$. Pour $1 \le j \le r_1$, le plongement σ_j est réel, tandis que pour $r_1 < j \le r_1+r_2$, les deux plongements complexes σ_j et σ_{r_2+j} sont conjugués.

Le *plongement canonique* du corps de nombres k est l'application σ de k dans $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ qui envoie $\gamma \in k$ sur $\bigl(\sigma_j(\gamma)\bigr)_{1 \le j \le r_1+r_2}$.

Le *théorème d'approximation faible* d'Artin–Whapples affirme que l'image de k par σ est dense dans $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. L'image par σ du groupe multiplicatif $k^\times$ est aussi dense dans $(\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$. Une des motivations de D. Roy dans [R 1990a], [R 1990b] et [R 1992b] était la question suivante, soulevée par Colliot-Thélène et Sansuc : *existe-t-il un sous-groupe de type fini de* $k^\times$ *dont l'image soit dense dans* $(\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$? Avec la question subsidiaire de Sansuc : *si oui, quel est le rang minimal d'un tel sous-groupe ?*

Le résultat final dans [R 1992b] est le suivant : *il existe un sous-groupe de type fini de* $k^\times$*, engendré par* $r_1 + r_2 + 1$ *éléments sur* $\mathbb{Z}$*, dont l'image par* σ *est dense dans* $(\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$*, et il n'en existe pas de rang plus petit.*

Comme le groupe topologique $G = (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$ est isomorphe au produit direct $(\mathbb{Z}/2\mathbb{Z})^{r_1} \times \mathbb{R}^{r_1+r_2} \times (\mathbb{R}/\mathbb{Z})^{r_2}$, on a $\mathrm{m}(G) = r_1 + r_2 + 1$; c'est pourquoi la borne de Roy est optimale.

III. – Le problème de densité pour les groupes algébriques linéaires

Soient d_0 et d_1 deux entiers ≥ 0 avec $d = d_0+d_1 > 0$. On considère le groupe algébrique linéaire $G = \mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}$. Soient k un corps de nombres, Γ un sous-groupe de type fini de $G(k) = k^{d_0} \times (k^\times)^{d_1}$ et v une place archimédienne de k. On désigne par k_v le complété de k en v (ce corps est $\mathbb{R}$ ou $\mathbb{C}$ suivant que la place v est réelle ou complexe). Notre but est de donner des conditions suffisantes pour assurer que l'image de Γ dans $G(k_v) = k_v^{d_0} \times (k_v^\times)^{d_1}$ est dense. Nous commençons par quelques exemples simples. D'abord quand le groupe de Lie réel $G(k_v)$ est de dimension 1, alors $k_v = \mathbb{R}$, et G est soit le groupe additif, soit le groupe multiplicatif ; dans chacun des deux cas le problème de transcendance que nous étudions est complétement résolu par le théorème 1.1 du chapitre II : *un sous-groupe de type fini* Γ *de* $\mathbb{R}$ *(resp.* $\mathbb{R}_+^\times$*) est dense si et seulement si son rang sur* $\mathbb{Z}$ *est* ≥ 2. En particulier l'arithmétique n'intervient pas : on ne gagne rien à supposer que Γ est contenu dans le groupe des points dont les coordonnées sont des nombres algébriques.

Dans la première section nous supposons que le groupe de Lie réel $G(k_v)$ est de dimension 2. Il n'y a que trois groupes à envisager : $(\mathbb{G}_{\mathrm{a}} \times \mathbb{G}_{\mathrm{m}})(\mathbb{R}) = \mathbb{R} \times \mathbb{R}^\times$, $\mathbb{G}_{\mathrm{m}}^2(\mathbb{R}) = (\mathbb{R}^\times)^2$ et $\mathbb{G}_{\mathrm{m}}(\mathbb{C}) = \mathbb{C}^\times$. Dans le premier cas, le théorème de Gel'fond-Schneider nous permettra de résoudre complètement le problème. Dans chacun des deux autres, on ramène la question de densité à un problème de transcendance qui n'est pas encore résolu : le *problème des quatre exponentielles* ; un énoncé partiel en direction de cette conjecture, le *théorème des six exponentielles*, permettra de donner des éléments de réponse.

Pour étudier la densité, dans le groupe des points réels, de points rationnels sur des groupes linéaires commutatifs $\mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}$, il faut disposer de généralisations en plusieurs variables des deux énoncés de transcendance auxquels on vient de faire allusion. L'extension correspondante du théorème des six exponentielles est le *théorème du sous-groupe linéaire.* Le théorème principal de ce chapitre est le théorème 2.10 qui donne des conditions suffisantes pour qu'un sous-groupe de type fini de $G(\overline{\mathbb{Q}} \cap \mathbb{R})$, où $G = \mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}$, soit dense dans $G(\mathbb{R}) = \mathbb{R}^{d_0} \times (\mathbb{R}^\times)^{d_1}$. Pour la partie conjecturale, on fera appel à la *conjecture d'indépendance algébrique de logarithmes* (le cas *homogène* suffira).

Les points complexes du groupe algébrique linéaire $G = \mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}$ forment le groupe de Lie complexe $G(\mathbb{C}) = \mathbb{C}^{d_0} \times (\mathbb{C}^\times)^{d_1}$, dont l'application exponentielle est

$$\begin{array}{rccc} \exp_G : & \mathbb{C}^d & \longrightarrow & \mathbb{C}^{d_0} \times (\mathbb{C}^\times)^{d_1} \\ & (z_1, \dots, z_d) & \longmapsto & (z_1, \dots, z_{d_0}; e^{z_{d_0+1}}, \dots, e^{z_d}) \end{array}$$

Le noyau de cette application est $\{0\}^{d_0} \times (2i\pi\mathbb{Z})^{d_1}$. L'image inverse par $\exp_G$ du groupe

$G(\overline{\mathbb{Q}}) = \overline{\mathbb{Q}}^{d_0} \times (\overline{\mathbb{Q}}^\times)^{d_1}$ est $\mathcal{L}(G) = \overline{\mathbb{Q}}^{d_0} \times \mathcal{L}^{d_1}$, où $\mathcal{L}$ désigne le $\mathbb{Q}$-espace vectoriel formé par les logarithmes de nombres algébriques non nuls :

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

Ainsi

$$\mathcal{L}(G) = \{(\beta_1, \dots, \beta_{d_0}; \lambda_1, \dots; \lambda_{d_1})\ ;\ \beta_h \in \overline{\mathbb{Q}},\ (1 \le h \le d_0),\ e^{\lambda_i} \in \overline{\mathbb{Q}}^\times,\ (1 \le i \le d_1)\}.$$

Nous travaillerons souvent aussi avec le groupe des points réels de G, qui est un groupe de Lie réel $G(\mathbb{R}) = \mathbb{R}^{d_0} \times (\mathbb{R}^\times)^{d_1}$ de dimension d ayant 2^{d_1} composantes connexes ; celle de l'élément neutre est $\mathbb{R}^{d_0} \times (\mathbb{R}_+^\times)^{d_1}$ et l'application exponentielle, qui est la restriction de $\exp_G$ à $\mathbb{R}^d$, est un isomorphisme de groupes de Lie

$$\begin{array}{cccc} \exp_{G,\mathbb{R}} : & \mathbb{R}^d & \to & \mathbb{R}^{d_0} \times (\mathbb{R}_+^\times)^{d_1} \\ & (x_1, \dots, x_d) & \mapsto & (x_1, \dots, x_{d_0}; e^{x_{d_0+1}}, \dots, e^{x_d}) \end{array}$$

Les résultats de transcendance dont nous aurons besoin (théorème de Gelfond-Schneider 1.3*, théorème des six exponentielles 1.7*, théorème du sous-groupe linéaire 2.6*, théorème de Baker 2.8*) seront formulés sans démonstration ; c'est pourquoi on leur affecte un *.

§1. Groupes de Lie réels de dimension 2

Dans cette section nous considérons le problème mentionné dans l'introduction pour les groupes de Lie de dimension 2. Pour chacun des deux groupes additifs $\mathbb{G}_a^2(\mathbb{R}) = \mathbb{R}^2$ et $\mathbb{G}_a(\mathbb{C}) = \mathbb{C}$, le théorème de Kronecker résout le problème, sans faire intervenir de condition arithmétique.

Exercice. Soient n un entier positif, k un sous-corps de $\mathbb{R}$ et Γ un sous-groupe de type fini de k^n. Montrer que Γ est dense dans $\mathbb{R}^n$ si et seulement si pour tout hyperplan H de $\mathbb{R}^n$ rationnel sur k *on a* $\mathrm{rang}_{\mathbb{Z}}(\Gamma/\Gamma \cap H) \ge 2$.

Rappel. Quand K est un corps et k un sous-corps de K, un sous-espace vectoriel V de K^n est *rationnel sur* k s'il vérifie les propriétés équivalentes suivantes :
(i) V possède une base formée d'éléments de k^n.
(ii) V est intersection d'hyperplans définis par des équations (linéaires homogènes) à coefficients dans k.

a) *Sous-groupes de $\mathbb{R} \times \mathbb{R}_+^\times$: le théorème de Gel'fond-Schneider*

Soit G le groupe algébrique $\mathbb{G}_a \times \mathbb{G}_m$. Ses points réels forment le groupe $G(\mathbb{R}) = \mathbb{R} \times \mathbb{R}^\times$ dont on va étudier la composante connexe neutre $G(\mathbb{R})^0 = \mathbb{R} \times \mathbb{R}_+^\times$. On désignera par p_a la projection $\mathbb{R} \times \mathbb{R}_+^\times \to \mathbb{R}$ sur le facteur additif, et par p_m la projection $\mathbb{R} \times \mathbb{R}_+^\times \to \mathbb{R}_+^\times$ sur le facteur multiplicatif. Etant donné que $\mathrm{m}(G(\mathbb{R})^0) = 3$ et $\mathrm{m}(\mathbb{R}) = \mathrm{m}(\mathbb{R}_+^\times) = 2$, on a :

Lemme 1.1. – *Si Γ est un sous-groupe dense de $\mathbb{R} \times \mathbb{R}_+^\times$, alors $p_a(\Gamma)$ est un sous-groupe dense de $\mathbb{R}$ et $p_m(\Gamma)$ est un sous-groupe dense de $\mathbb{R}^\times$. De plus, si Γ est de type fini, alors*

$$\mathrm{rang}_{\mathbb{Z}}\Gamma \ge 3, \qquad \mathrm{rang}_{\mathbb{Z}} p_a(\Gamma) \ge 2 \quad et \quad \mathrm{rang}_{\mathbb{Z}} p_m(\Gamma) \ge 2.$$

Ces conditions nécessaires ne sont évidemment pas suffisantes en général : si x_1, x_2, x_3 sont trois nombres réels linéairement indépendants sur $\mathbb{Q}$, le sous-groupe engendré par les trois points (x_j, e^{x_j}), $(j = 1, 2, 3)$ dans $\mathbb{R} \times \mathbb{R}_+^\times$ a pour adhérence la courbe $\{(x, e^x);\ x \in \mathbb{R}\}$.

Nous allons montrer que ces conditions sont suffisantes si Γ est un sous-groupe de type fini dont les points ont des coordonnées algébriques.

On désigne par K le corps $\overline{\mathbb{Q}} \cap \mathbb{R}$ des nombres algébriques réels (le corps $\overline{\mathbb{Q}}$ des nombres algébriques est $K(i)$). On notera $K_+^\times$ le groupe multiplicatif $\overline{\mathbb{Q}} \cap \mathbb{R}_+^\times$.

Proposition 1.2. – *Soit Γ un sous-groupe de type fini de $K \times K_+^\times$. Les deux conditions suivantes sont équivalentes :*
(i) Γ est dense dans $\mathbb{R} \times \mathbb{R}_+^\times$.
(ii) On a $\mathrm{rang}_{\mathbb{Z}}\Gamma \ge 3$, $\mathrm{rang}_{\mathbb{Z}} p_a(\Gamma) \ge 2$ *et* $\mathrm{rang}_{\mathbb{Z}} p_m(\Gamma) \ge 2$.

Quand Γ est un sous-groupe de type fini de $K \times K_+^\times$, on peut choisir un système générateur $(\gamma_1, \dots, \gamma_\ell)$; chacun des γ_j s'écrit (β_j, α_j), avec β_j nombre algébrique réel et α_j nombre algébrique réel positif, et on peut écrire

$$\Gamma = \{(s_1\beta_1 + \cdots + s_\ell\beta_\ell, \alpha_1^{s_1} \cdots \alpha_\ell^{s_\ell});\ (s_1, \dots, s_\ell) \in \mathbb{Z}^\ell\}.$$

Alors $p_a(\Gamma) = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_\ell \subset \mathbb{R}$, et de même $p_m(\Gamma)$ est le sous-groupe de $\mathbb{R}_+^\times$ engendré par $\alpha_1, \dots, \alpha_\ell$. L'application exponentielle de $G(\mathbb{R})$ est un isomorphisme de $\mathbb{R}^2$ sur la composante connexe de l'élément neutre de $G(\mathbb{R})$:

$$\begin{array}{cccc} \exp_{G,\mathbb{R}} : & \mathbb{R}^2 & \to & \mathbb{R} \times \mathbb{R}_+^\times \\ & (x, y) & \mapsto & (x, e^y) \end{array}$$

Pour $1 \le j \le \ell$, on définit $y_j \in \mathbb{R}^2$ par $y_j = (\beta_j, \log\alpha_j)$ (où log est le logarithme usuel $\mathbb{R}_+^\times \to \mathbb{R}$). On désigne par Y le sous-groupe de $\mathbb{R}^2$ engendré par $\{y_1, \dots, y_\ell\}$. Alors $Y = \exp_{G,\mathbb{R}}^{-1}(\Gamma)$, donc Γ est dense dans $\mathbb{R} \times \mathbb{R}_+^\times$ si et seulement si Y est dense dans $\mathbb{R}^2$. On ramène ainsi le problème de densité dans $\mathbb{R} \times \mathbb{R}_+^\times$ d'un sous-groupe Γ de $K \times K_+^\times$ à un problème de densité dans $\mathbb{R}^2$ d'un sous-groupe Y de $K \times (\mathcal{L} \cap \mathbb{R})$.

La démonstration de la proposition 1.2 va utiliser un résultat de transcendance : le théorème de Gel'fond-Schneider, qui résolvait (en 1934) le septième problème de Hilbert (voir par exemple [G 1952], Chap. III, §2 ; [Sch 1957], Chap. II, Th. 14 ; [L 1966], Chap. III, §1, Cor. 2 ; [L 1993], Appendice, Cor. 2 ; [W 1974], Chap. 2, Th. 2.1.1). Plus précisément nous montrerons que la proposition 1.2 est *équivalente* au cas réel du théorème de Gel'fond-Schneider.

Nous énonçons ce théorème sous plusieurs formes équivalentes. Nous démontrons l'équivalence entre les différents énoncés, mais nous ne démontrons pas les énoncés eux-mêmes. Voici pour commencer l'énoncé complexe.

Théorème 1.3* (Gel'fond-Schneider). –
$\boxed{1}$ *Soient ℓ_1 et ℓ_2 deux éléments de $\mathcal{L}$ qui sont linéairement indépendants sur $\mathbb{Q}$. Alors ℓ_1 et ℓ_2 sont linéairement indépendants sur $\overline{\mathbb{Q}}$.*
$\boxed{2}$ *Si α est un nombre algébrique non nul, $\log\alpha$ une détermination non nulle du logarithme complexe de α, et β un nombre algébrique irrationnel, alors le nombre α^β, qui est défini par $\exp(\beta\log\alpha)$, est transcendant sur $\mathbb{Q}$.*
$\boxed{3}$ *Soient ℓ_1, ℓ_2 et β trois nombres complexes, avec $(\ell_1,\ell_2)\neq(0,0)$, β irrationnel et $\ell_2=\beta\ell_1$. Alors l'un au moins des trois nombres e^{ℓ_1}, e^{ℓ_2}, β est transcendant.*
$\boxed{4}$ *Soient $\beta_1,\ldots,\ldots,\beta_n$ des nombres algébriques non tous nuls et $\ell_1,\ldots,\ell_n$ des éléments de $\mathcal{L}$ non tous nuls. On suppose que les vecteurs colonnes de la matrice*

$$\begin{pmatrix}\beta_1 & \cdots & \beta_n\\ \ell_1 & \cdots & \ell_n\end{pmatrix}$$

engendrent dans $\mathbb{C}^2$ un espace vectoriel sur $\mathbb{Q}$ de dimension ≥ 2. Alors cette matrice est de rang 2.
$\boxed{5}$ *Si D est une droite de $\mathbb{C}^2$, $D\neq\mathbb{C}\times\{0\}$, $D\neq\{0\}\times\mathbb{C}$, alors la dimension sur $\mathbb{Q}$ de l'espace vectoriel $D\cap(\overline{\mathbb{Q}}\times\mathcal{L})$ est ≤ 1.*

De cet énoncé on déduit la transcendance de nombres tels que $(\log 2)/(\log 3)$, $2^{\sqrt{2}}$, e^π.

Remarque. On déduit aussi du théorème de Gel'fond-Schneider que si β_1 et β_2 sont deux nombres algébriques linéairement indépendants, alors l'un au moins des deux nombres e^{β_1}, e^{β_2} est transcendant. Le *théorème de Hermite-Lindemann* affirme que chacun de ces deux nombres est transcendants. En revanche le théorème de Gel'fond-Schneider n'est pas limité à la base e pour l'exponentielle : il affirme en effet que *pour tout nombre complexe non nul t, l'un au moins des deux nombres $e^{t\beta_1}, e^{t\beta_2}$ est transcendant.*

Exercice.
a) Montrer que le groupe additif $K/\mathbb{Z}$ est isomorphe au groupe multiplicatif $\overline{\mathbb{Q}}^\times\cap\mathbb{U}$. Soit $f:K\to\mathbb{C}^\times$ un homomorphisme de noyau $\mathbb{Z}$ et d'image contenue dans $\overline{\mathbb{Q}}^\times\cap\mathbb{U}$. Montrer que f n'est pas continu en 0.
b) Montrer que le groupe additif $K=\overline{\mathbb{Q}}\cap\mathbb{R}$ est isomorphe au groupe multiplicatif $K_+^\times=\overline{\mathbb{Q}}^\times\cap\mathbb{R}_+^\times$. Soit $g:K\to\mathbb{R}_+^\times$ un homomorphisme injectif d'image contenue dans $K_+^\times$. Montrer que g n'est pas continu au point 0.
(`Indication` : Voir J. Dieudonné, *Algèbre linéaire et géométrie élémentaire*, Hermann, Coll. Enseignement des Sciences, 1964, Annexe I p. 163–164.)

Démonstration des équivalences $\boxed{1}\Leftrightarrow\boxed{2}\Leftrightarrow\boxed{3}\Leftrightarrow\boxed{4}\Leftrightarrow\boxed{5}$
$\boxed{1}\Rightarrow\boxed{2}$. On pose $\ell_1=\log\alpha$ et $\ell_2=\beta\log\alpha$; alors $\ell_1\in\mathcal{L}$, ℓ_1 et ℓ_2 sont $\mathbb{Q}$-linéairement indépendants, mais $\overline{\mathbb{Q}}$-linéairement dépendants. Donc $\ell_2\notin\mathcal{L}$ et le nombre $e^{\ell_2}=\alpha^\beta$ est transcendant.

$\boxed{2}\Rightarrow\boxed{3}$. On pose $\alpha=e^{\ell_1}$ et $\log\alpha=\ell_1$. Comme $\ell_2=\beta\ell_1$, les nombres α, β et $e^{\ell_2}=\alpha^\beta$ ne peuvent être tous trois algébriques.

$\boxed{3}\Rightarrow\boxed{4}$. L'un des β_i est non nul ; on peut supposer $\beta_1\neq 0$. Si $\ell_1=0$, comme l'un des ℓ_j n'est pas nul, la conclusion est triviale. Supposons $\ell_1\neq 0$; il existe un indice j, $2\leq j\leq\ell$, tel que la colonne $\begin{pmatrix}\beta_j\\ \ell_j\end{pmatrix}$ soit linéairement indépendante de $\begin{pmatrix}\beta_1\\ \ell_1\end{pmatrix}$ sur $\mathbb{Q}$. On a $\ell_1\in\mathcal{L}$, $\ell_j\in\mathcal{L}$, $\ell_1\neq 0$ et $\beta_j/\beta_1\in\overline{\mathbb{Q}}$. Grâce à $\boxed{3}$ et à l'indépendance linéaire sur $\mathbb{Q}$ des deux colonnes, on déduit $\ell_j\neq(\beta_j/\beta_1)\ell_1$.

$\boxed{4}\Rightarrow\boxed{5}$. Soit D une droite de $\mathbb{C}^2$. Supposons que (β_1,ℓ_1) et (β_2,ℓ_2) soient deux éléments $\mathbb{Q}$-linéairement indépendants de $D\cap(\overline{\mathbb{Q}}\times\mathcal{L})$. La matrice

$$\begin{pmatrix}\beta_1 & \beta_2\\ \ell_1 & \ell_2\end{pmatrix}$$

est de rang 1, et ses colonnes sont linéairement indépendantes sur $\mathbb{Q}$. Alors ou bien $\beta_1=\beta_2=0$, auquel cas $D=\{0\}\times\mathbb{C}$, ou bien $\ell_1=\ell_2=0$ et alors $D=\mathbb{C}\times\{0\}$.
$\boxed{5}\Rightarrow\boxed{1}$. On pose $\beta=\ell_2/\ell_1$ et on prend pour D la droite d'équation $y=\ell_1 x$. Elle est distincte de $\mathbb{C}\times\{0\}$ et de $\{0\}\times\mathbb{C}$, et contient les points $(1,\ell_1)$ et (β,ℓ_2). On a même $(1,\ell_1)\in D\cap(\overline{\mathbb{Q}}\times\mathcal{L})$. Comme β est irrationnel, il résulte de $\boxed{5}$ que $D\cap(\overline{\mathbb{Q}}\times\mathcal{L})$ ne contient pas (β,ℓ_2), donc le nombre β est transcendant. □

Nous appellerons *cas réel du théorème de Gel'fond-Schneider* les énoncés équivalents suivant :
$\boxed{1_\mathbb{R}}$ *Soient α_1 et α_2 deux nombres algébriques positifs multiplicativement indépendants. Alors le nombre $\log\alpha_1/\log\alpha_2$ est transcendant.*
$\boxed{2_\mathbb{R}}$ *Si α est un nombre algébrique réel positif différent de 1 et β un nombre algébrique réel irrationnel, alors le nombre $\alpha^\beta=\exp(\beta\log\alpha)$, est transcendant sur $\mathbb{Q}$.*
$\boxed{3_\mathbb{R}}$ *Soient ℓ_1, ℓ_2 et β trois nombres réels, avec $(\ell_1,\ell_2)\neq(0,0)$, $\beta\notin\mathbb{Q}$ et $\ell_2=\beta\ell_1$. Alors l'un au moins des trois nombres e^{ℓ_1}, e^{ℓ_2}, β est transcendant.*
$\boxed{4_\mathbb{R}}$ *Soient $\beta_1,\ldots,\ldots,\beta_n$ des nombres algébriques réels non tous nuls et $\alpha_1,\ldots,\alpha_n$ des nombres réels algébriques positifs non tous égaux à 1. On suppose que les vecteurs colonnes de la matrice*

$$\begin{pmatrix}\beta_1 & \cdots & \beta_n\\ \log\alpha_1 & \cdots & \log\alpha_n\end{pmatrix}$$

engendrent dans $\mathbb{R}^2$ un espace vectoriel sur $\mathbb{Q}$ de dimension ≥ 2. Alors cette matrice est de rang 2.
$\boxed{5_\mathbb{R}}$ *Si D est une droite de $\mathbb{R}^2$, $D\neq\mathbb{R}\times\{0\}$, $D\neq\{0\}\times\mathbb{R}$, alors le $\mathbb{Q}$-espace vectoriel $D\cap\big(K\times\mathcal{L}\big)$ est de dimension ≤ 1.*

Démonstration de l'implication $\boxed{5_\mathbb{R}}\Rightarrow$ Proposition 1.2.
On sait déjà (lemme 1.1) que la condition *(i)* de la proposition 1.2 implique *(ii)*. Supposons maintenant que *(ii)* est vérifiée. On définit $Y=\exp_{G,\mathbb{R}}^{-1}(\Gamma)\subset K\times(\mathcal{L}\cap\mathbb{R})$. Alors Y est isomorphe à Γ, et en particulier est de rang ≥ 3. Soit φ une forme linéaire non nulle sur $\mathbb{R}^2$. S'il existe $\lambda\in\mathbb{R}^\times$ tel que $\varphi(x,y)=\lambda x$, alors $\mathrm{rang}_\mathbb{Z}\varphi(Y)=\mathrm{rang}_\mathbb{Z}p_\mathrm{a}(\Gamma)\geq 2$. De même s'il existe $\mu\in\mathbb{R}^\times$ tel que $\varphi(x,y)=\mu y$, alors $\mathrm{rang}_\mathbb{Z}\varphi(Y)=\mathrm{rang}_\mathbb{Z}p_\mathrm{m}(\Gamma)\geq 2$. Dans les autres cas on peut écrire $\varphi(x,y)=\lambda x+\mu y$ avec $\lambda\neq 0$ et $\mu\neq 0$. La droite $D=\mathrm{Ker}\,\varphi$ n'est pas un des axes de coordonnées et on déduit de $\boxed{5_\mathbb{R}}$ la majoration $\mathrm{rang}_\mathbb{Z}(Y\cap D)\leq 1$. Comme le rang de Y est ≥ 3, on peut conclure $\mathrm{rang}_\mathbb{Z}\varphi(Y)=\mathrm{rang}_\mathbb{Z}(Y/Y\cap D)\geq 2$. Ainsi (proposition 4.3 du chapitre II) Y est dense dans $\mathbb{R}^2$.

Démonstration de l'implication Proposition 1.2 ⇒ $\boxed{3_{\mathbb{R}}}$.
On considère le sous-groupe Γ de $\mathbb{R}\times\mathbb{R}^\times$ engendré par les trois éléments $(1,e^{\ell_1})$, (β,e^{ℓ_2}) et $(1,e^{\ell_2})$. Son rang sur $\mathbb{Z}$ est 3, on a $\mathrm{rang}_{\mathbb{Z}} p_{\mathrm{a}}(\Gamma)=2$, $\mathrm{rang}_{\mathbb{Z}} p_{\mathrm{m}}(\Gamma)=2$, et Γ n'est pas dense dans $\mathbb{R}\times\mathbb{R}^\times$. Donc Γ n'est pas contenu dans $K\times K_+^\times$, et l'un au moins des trois nombres β, e^{ℓ_1}, e^{ℓ_2} est transcendant. □

Remarque. Pour démontrer que le sous-groupe Y de $\mathbb{R}^2$ est dense, il faut vérifier que le rang de $Y/Y\cap D$ est ≥ 2 pour tout hyperplan D de $\mathbb{R}^2$. Ici, grâce à l'hypothèse que Y est contenu dans $K\times(\mathcal{L}\cap\mathbb{R})$, on a pu utiliser un théorème de transcendance ; il suffit alors d'imposer cette condition pour les deux hyperplans $\mathbb{R}\times\{0\}$ et $\{0\}\times\mathbb{R}$. Dans $\mathbb{R}^2$, ces deux droites sont les images inverses, par l'application exponentielle $\exp_{G,\mathbb{R}}:(x,y)\to(x,e^y)$, des deux sous-groupes $\mathbb{R}\times\{1\}$ et $\{0\}\times\mathbb{R}^\times$. Or $\mathbb{G}_{\mathrm{a}}\times\{1\}$ et $\{0\}\times\mathbb{G}_{\mathrm{m}}$ sont, avec $\{0\}\times\{1\}$ et $\mathbb{G}_{\mathrm{a}}\times\mathbb{G}_{\mathrm{m}}$, les seuls sous-groupes algébriques connexes de $\mathbb{G}_{\mathrm{a}}\times\mathbb{G}_{\mathrm{m}}$ (cf. lemme 2.4 ci-dessous). Ainsi le résultat de transcendance permet de vérifier la condition $\mathrm{rang}_{\mathbb{Z}}(Y/Y\cap D)\geq 2$ chaque fois que l'hyperplan D n'est pas l'image inverse (par l'exponentielle) d'un sous-groupe algébrique de G. Nous allons retrouver ce phénomène dans l'exemple suivant, qui est sensiblement différent car $\mathbb{G}_{\mathrm{m}}^2$ possède beaucoup plus de sous-groupes algébriques que $\mathbb{G}_{\mathrm{a}}\times\mathbb{G}_{\mathrm{m}}$.

b1) *Sous-groupes de* $(\mathbb{R}_+^\times)^2$ *: la conjecture des quatre exponentielles*

Soit G le groupe algébrique $\mathbb{G}_{\mathrm{m}}^2$. Ses points réels forment le groupe $G(\mathbb{R})=(\mathbb{R}^\times)^2$ dont la composante neutre est $G(\mathbb{R})^0=(\mathbb{R}_+^\times)^2$. Pour chaque couple $(a,b)\in\mathbb{Z}\times\mathbb{Z}$, $(a,b)\neq 0$, on désigne par $\phi_{(a,b)}$ l'homomorphisme surjectif de groupes algébriques de G sur $\mathbb{G}_{\mathrm{m}}$ qui envoie (u,v) sur u^av^b. Le noyau de $\phi_{(a,b)}$ est le sous-groupe algébrique $H_{(a,b)}$ de G, intersection de G avec l'hypersurface $\big\{(u,v);u^av^b=1\big\}$.

Etant donné que $\mathrm{m}\big(G(\mathbb{R})^0\big)=3$ et $\mathrm{m}(\mathbb{R}_+^\times)=2$, on a :

Lemme 1.4. – *Si* Γ *est un sous-groupe dense de* $(\mathbb{R}_+^\times)^2$*, alors pour tout* $(a,b)\in\mathbb{Z}\times\mathbb{Z}$, $(a,b)\neq 0$*, l'image* $\phi_{(a,b)}(\Gamma)$ *est un sous-groupe dense de* $\mathbb{R}_+^\times$*. De plus, si* Γ *est de type fini, alors* $\mathrm{rang}_{\mathbb{Z}}\Gamma\geq 3$ *et*

$$\mathrm{rang}_{\mathbb{Z}}\phi_{(a,b)}(\Gamma)\geq 2 \qquad \textit{pour tout } (a,b)\in\mathbb{Z}\times\mathbb{Z},\ (a,b)\neq 0.$$

Supposons Γ de type fini ; soit ℓ son rang sur $\mathbb{Z}$, et soient $\gamma_1,\ldots,\gamma_\ell$ des éléments de Γ, multiplicativement indépendants ; écrivons

$$\gamma_j=(\alpha_j,\beta_j),\qquad (j=1,\ldots,\ell).$$

Pour $(a,b)\in\mathbb{Z}^2\setminus\{(0,0)\}$, la condition $\mathrm{rang}_{\mathbb{Z}}\phi_{(a,b)}(\Gamma)\geq 2$ signifie que deux au moins des ℓ nombres

$$\alpha_1^a\beta_1^b,\ldots,\alpha_\ell^a\beta_\ell^b$$

sont multiplicativement indépendants, ce qui revient à dire que deux au moins des ℓ nombres

$$a\log\alpha_1+b\log\beta_1,\ldots,a\log\alpha_\ell+b\log\beta_\ell$$

sont $\mathbb{Q}$-linéairement indépendants. Ces conditions nécessaires à la densité ne sont évidemment pas suffisantes en général : si t est un nombre irrationnel et x_1,x_2,x_3 trois nombres entiers positifs tels que les six nombres $x_1,x_2,x_3,x_1^t,x_2^t,x_3^t$ soient multiplicativement indépendants, le sous-groupe

$$\big\{(x_1^{s_1}x_2^{s_2}x_3^{s_3},x_1^{ts_1}x_2^{ts_2}x_3^{ts_3});\ (s_1,s_2,s_3)\in\mathbb{Z}^3\big\}\subset(\mathbb{R}_+^\times)^2$$

n'est pas dense dans $(\mathbb{R}_+^\times)^2$, puisque son adhérence est la courbe analytique $\big\{(x,x^t);\ x\in\mathbb{R}_+^\times\big\}$, et pourtant, pour tout $(a,b)\neq(0,0)$, sa projection par $\phi_{(a,b)}$ a pour image un sous-groupe dense de $\mathbb{R}_+^\times$.

On *conjecture* que ces conditions sont suffisantes si on suppose que les coordonnées des points de Γ sont des nombres algébriques. Cette conjecture est l'une des formes équivalentes de la *conjecture des quatre exponentielles réelles*. Nous formulons d'abord l'énoncé dans le cas complexe — plus général, et qui sera bientôt utile — (voir [Sch 1957], Chap. V §4 Problème 1 ; [L 1966], Chap. II, §1 ; [Ra 1968], p. 67 ; [W 1974], §2.3 ; [B 1979], Chap. 12 §1).

Conjecture 1.5$^?$ (conjecture des quatre exponentielles). –
$\boxed{1^?}$ *Soient* x_1,x_2 *deux nombres complexes linéairement indépendants sur* $\mathbb{Q}$*, et soient* y_1,y_2 *deux nombres complexes linéairement indépendants sur* $\mathbb{Q}$*. Alors l'un au moins des quatre nombres*

$$e^{x_1y_1},e^{x_1y_2},e^{x_2y_1},e^{x_2y_2}$$

est transcendant.
$\boxed{2^?}$ *Soit*

$$M=\begin{pmatrix}\lambda_{11}&\cdots&\lambda_{1\ell}\\ \vdots&\ddots&\vdots\\ \lambda_{d1}&\cdots&\lambda_{d\ell}\end{pmatrix}$$

une matrice $d\times\ell$ *à coefficients logarithmes de nombres algébriques ; on suppose que deux au moins des* ℓ *colonnes de* M *sont linéairement indépendantes sur* $\mathbb{Q}$ *et aussi que deux au moins des* d *lignes de* M *sont linéairement indépendantes sur* $\mathbb{Q}$*. Alors le rang de la matrice* M *est* ≥ 2.
$\boxed{3^?}$ *Soit* D *un hyperplan de* $\mathbb{C}^2$ *; on suppose* $D\cap\mathbb{Q}^2=\{(0,0)\}$*. Alors le* $\mathbb{Q}$*-espace vectoriel* $D\cap\mathcal{L}^2$ *est de dimension finie, et cette dimension est* ≤ 1.

A propos de la condition $\boxed{3^?}$, noter que si un hyperplan D de $\mathbb{C}^2$ (c'est-à-dire une droite vectorielle complexe) vérifie $D\cap\mathbb{Q}^2\neq\{(0,0)\}$, alors le $\mathbb{Q}$-espace vectoriel $D\cap\mathcal{L}^2$ est de dimension infinie, puisqu'il contient tous les $(a\lambda,b\lambda)$, pour $\lambda\in\mathcal{L}$ et $(a,b)\in D\cap\mathbb{Q}^2$.

Démonstration des équivalences $\boxed{1^?}\Leftrightarrow\boxed{2^?}\Leftrightarrow\boxed{3^?}$

$\boxed{1^?}\Rightarrow\boxed{2^?}$. Une matrice $d\times\ell$ est de rang ≤ 1 si et seulement s'il existe des nombres complexes $x_1,\ldots,x_d$, $y_1,\ldots,y_\ell$ telle que

$$M=(x_iy_j)_{\substack{1\leq i\leq d\\1\leq j\leq\ell}}=\begin{pmatrix}x_1\\ \vdots\\ x_d\end{pmatrix}\begin{pmatrix}y_1&\cdots&y_\ell\end{pmatrix}.$$

Si la matrice considérée dans $\boxed{2^?}$ était de rang ≤ 1, on pourrait écrire $\lambda_{ij} = x_i y_j$, avec $\mathbb{Z}x_1 + \ldots + \mathbb{Z}x_d$ sous-groupe de $\mathbb{C}$ de rang ≥ 2, et de même $\mathbb{Z}y_1 + \ldots + \mathbb{Z}y_\ell$ sous-groupe de $\mathbb{C}$ de rang ≥ 2. En prenant deux x_i linéairement indépendants et deux y_j aussi, on déduit de $\boxed{1^?}$ que les nombres $e^{\lambda_{ij}}$, $(1 \leq i \leq d,\ 1 \leq j \leq \ell)$ ne peuvent pas tous être algébriques.

$\boxed{2^?} \Rightarrow \boxed{3^?}$. Supposons qu'il existe deux éléments (ℓ_1, ℓ_1') et (ℓ_2, ℓ_2') $\mathbb{Q}$-linéairement indépendants dans $D \cap \mathcal{L}^2$; comme D est une droite, le déterminant de la matrice

$$\begin{pmatrix} \ell_1 & \ell_2 \\ \ell_1' & \ell_2' \end{pmatrix}$$

est nul. Les vecteurs colonnes de cette matrice sont $\mathbb{Q}$-linéairement indépendants ; d'après $\boxed{2^?}$, les deux lignes doivent être linéairement dépendantes sur $\mathbb{Q}$, ce qui signifie que D contient un élément non nul de $\mathbb{Q}^2$.

$\boxed{3^?} \Rightarrow \boxed{1^?}$. La droite $D = \big\{(u,v) \in \mathbb{C}^2;\ x_1 v = x_2 u\big\}$ a une intersection nulle avec $\mathbb{Q}^2$, car x_1 et x_2 sont $\mathbb{Q}$-linéairement indépendants. Elle contient les deux points (x_1y_1, x_2y_1) et (x_1y_2, x_2y_2) de $\mathbb{C}^2$, qui sont linéairement indépendants sur $\mathbb{Q}$, car y_1 et y_2 le sont. Utilisant $\boxed{3^?}$, on déduit que ces points ne sont pas tous deux dans $\mathcal{L}^2$. $\square$

Remarque. Sous les hypothèses de la conjecture des quatre exponentielles sous la forme $\boxed{2^?}$*, on sait démontrer que la conclusion est vraie si on ajoute l'hypothèse que le corps obtenu en adjoignant à* $\mathbb{Q}$ *les* ℓd *coefficients* λ_{ij} *de la matrice a pour degré de transcendance 1 sur* $\mathbb{Q}$*. On conjecture (cf. §3 ci-dessous) que cette hypothèse supplémentaire ne peut jamais être satisfaite, mais on sait tellement peu de choses sur l'indépendance algébrique de logarithmes que cet énoncé a quand même quelques conséquences intéressantes.*

La *conjecture des quatre exponentielles réelles* est l'un des énoncés équivalents suivants :

$\boxed{1^?_{\mathbb{R}}}$ *Soient* x_1, x_2 *deux nombres réels linéairement indépendants sur* $\mathbb{Q}$*, et soient* y_1, y_2 *deux nombres réels linéairement indépendants sur* $\mathbb{Q}$*. Alors l'un au moins des quatre nombres*

$$e^{x_1y_1}, e^{x_1y_2}, e^{x_2y_1}, e^{x_2y_2}$$

est transcendant.

$\boxed{2^?_{\mathbb{R}}}$ *Soient* α_{ij}, $(1 \leq i \leq d,\ 1 \leq j \leq \ell)$ *des nombres algébriques positifs. On considère la matrice* $d \times \ell$

$$M = \begin{pmatrix} \log\alpha_{11} & \cdots & \log\alpha_{1\ell} \\ \vdots & \ddots & \vdots \\ \log\alpha_{d1} & \cdots & \log\alpha_{d\ell} \end{pmatrix}$$

on suppose que deux au moins des ℓ *colonnes de* M *sont linéairement indépendantes sur* $\mathbb{Q}$ *et aussi que deux au moins des* d *lignes de* M *sont linéairement indépendantes sur* $\mathbb{Q}$ *; alors le rang de* M *est* ≥ 2.

$\boxed{3^?_{\mathbb{R}}}$ *Soit* D *un hyperplan de* $\mathbb{R}^2$ *; on suppose* $D \cap \mathbb{Q}^2 = \{(0,0)\}$*. Alors le* $\mathbb{Q}$*-espace vectoriel* $D \cap \mathcal{L}^2$ *est de dimension finie* ≤ 1.

On montre maintenant la conjecture des quatre exponentielles réelles est encore équivalente à l'énoncé suivant :

$\boxed{4^?_{\mathbb{R}}}$ *Si* Γ *est un sous-groupe de type fini de* $(K_+^\times)^2$*, de rang* ≥ 3 *sur* $\mathbb{Z}$*, tel que, pour tout* $(a,b) \in \mathbb{Z} \times \mathbb{Z}$, $(a,b) \neq 0$, $\mathrm{rang}_{\mathbb{Z}}\phi_{(a,b)}(\Gamma) \geq 2$*. Alors* Γ *est dense dans* $(\mathbb{R}_+^\times)^2$.

Démonstration de l'équivalence entre $\boxed{3^?_{\mathbb{R}}}$ *et* $\boxed{4^?_{\mathbb{R}}}$

$\boxed{3^?_{\mathbb{R}}} \Rightarrow \boxed{4^?_{\mathbb{R}}}$

On pose $Y = \exp_{G,\mathbb{R}}^{-1}(\Gamma) \subset \mathcal{L}^2 \cap \mathbb{R}^2$. Il s'agit de vérifier que Y est dense dans $\mathbb{R}^2$, ce qui revient à dire, d'après la proposition 4.3 du chapitre II, que pour toute forme linéaire non nulle φ sur $\mathbb{R}^2$, on a $\mathrm{rang}_{\mathbb{Z}}\varphi(Y) \geq 2$. Si la droite $\mathrm{Ker}\ \varphi$ est rationnelle sur $\mathbb{Q}$, c'est-à-dire si $\varphi(x,y) = \lambda(ax+by)$ avec $\lambda \in \mathbb{R}^\times$ et $(a,b) \in \mathbb{Z}^2$, $(a,b) \neq (0,0)$, alors $\mathrm{rang}_{\mathbb{Z}}\varphi(Y) = \mathrm{rang}_{\mathbb{Z}}\phi_{(a,b)}(\Gamma) \geq 2$. Si au contraire $D = \mathrm{Ker}\ \varphi$ n'est pas une droite rationnelle, c'est-à-dire si $D \cap \mathbb{Q}^2 = \{(0,0)\}$, alors on peut appliquer $\boxed{3^?_{\mathbb{R}}}$:

$$\mathrm{rang}_{\mathbb{Z}}(Y \cap \mathrm{Ker}\ \varphi) \leq \dim_{\mathbb{Q}}(\mathcal{L}^2 \cap D) \leq 1.$$

Comme Y est de rang ≥ 3 sur $\mathbb{Z}$, on trouve $\mathrm{rang}_{\mathbb{Z}}\varphi(Y) \geq 2$.

$\boxed{4^?_{\mathbb{R}}} \Rightarrow \boxed{3^?_{\mathbb{R}}}$

On admet $\boxed{4^?_{\mathbb{R}}}$, on considère une droite D de $\mathbb{R}^2$ telle que $D \cap \mathcal{L}^2$ a un rang ≥ 2 sur $\mathbb{Z}$, et il s'agit de vérifier $D \cap \mathbb{Q}^2 \neq \{(0,0)\}$. On dispose de deux points (λ_1, λ_1') et (λ_2, λ_2') sur $D \cap \mathcal{L}^2$; on choisit (λ_3, λ_3') dans $\mathcal{L}^2 \cap \mathbb{R}^2$ de la manière suivante : λ_3 n'appartient pas au $\mathbb{Q}$-espace vectoriel engendré par $\lambda_1, \lambda_1', \lambda_2, \lambda_2'$, tandis que λ_3' n'appartient pas au $\mathbb{Q}$-espace vectoriel engendré par $\lambda_1, \lambda_1', \lambda_2, \lambda_2', \lambda_3$. On pose encore $\alpha_j = e^{\lambda_j}$, $\alpha_j' = e^{\lambda_j'}$, $\gamma_j = (\alpha_j, \alpha_j')$, $(j = 1,2,3)$, et on considère le sous-groupe Γ engendré par $\gamma_1, \gamma_2, \gamma_3$ dans $(K_+^\times)^2$. Alors Γ est de rang 3, et il n'est pas dense dans $(\mathbb{R}_+^\times)^2$, car $Y = \exp_{G,\mathbb{R}}^{-1}(\Gamma) = \mathbb{Z}(\lambda_1, \lambda_1') + \mathbb{Z}(\lambda_2, \lambda_2') + \mathbb{Z}(\lambda_3, \lambda_3')$ vérifie $\mathrm{rang}_{\mathbb{Z}}(D \cap Y) = 2$ et $\mathrm{rang}_{\mathbb{Z}}(Y/D \cap Y) = 1$. D'après $\boxed{4^?_{\mathbb{R}}}$ il existe $(a,b) \neq (0,0)$ tel que $\mathrm{rang}_{\mathbb{Z}}\phi_{(a,b)}(\Gamma) \leq 1$. Grâce au choix de λ_3 et λ_3' on trouve d'abord $a\lambda_3 + b\lambda_3' \neq 0$, puis $a\lambda_1 + b\lambda_1' = a\lambda_2 + b\lambda_2' = 0$. Cela permet de conclure $(-b, a) \in D \cap \mathbb{Q}^2$. $\square$

Remarque. Les hypothèses $\mathrm{rang}_{\mathbb{Z}}\phi_{(a,b)}(\Gamma) \geq 2$ pour tout $(a,b) \neq (0,0)$ permettent de vérifier la condition *(iv)* de la proposition 4.3 du chapitre II 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 $\mathbb{Q}$.

Exemple : plongement canonique du corps quadratique réel $\mathbb{Q}(\sqrt{2})$.

On désigne par $\alpha \mapsto \alpha^\sigma$ le plongement de $\mathbb{Q}(\sqrt{2})$ qui n'est pas l'identité : $\sqrt{2}^\sigma = -\sqrt{2}$. Le plongement canonique de $\mathbb{Q}(\sqrt{2})$ est donné par

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \to & \mathbb{R}^2 \\ \alpha & \mapsto & (\alpha, \alpha^\sigma) \end{array}$$

On s'intéresse à l'image du groupe multiplicatif $\mathbb{Q}(\sqrt{2})^\times$ dans $(\mathbb{R}^\times)^2$: on cherche un sous-groupe de type fini de $\mathbb{Q}(\sqrt{2})^\times$ dont l'image soit dense dans $(\mathbb{R}^\times)^2$.

Un nombre premier p congru à ± 1 modulo 8 est décomposé dans le corps $\mathbb{Q}(\sqrt{2})$ (cf. [H-W 1979], Th. 256) : il existe $\alpha \in \mathbb{Z}(\sqrt{2})$ tel que $\alpha\alpha^\sigma = \pm p$. Quand p est donné il y a quatre valeurs de α vérifiant cette propriété (on peut choisir le signe $\pm$, et on peut permuter α et α^σ), et ces quatre valeurs se répartissent dans les quatre composantes connexes (quadrants) de $(\mathbb{R}^\times)^2$.

Soient $p_1, \dots, p_\ell$ (avec $\ell \geq 2$) des nombres premiers congrus à ± 1 modulo 8. Pour $1 \leq j \leq \ell$, choisissons $\alpha_j \in \mathbb{Q}(\sqrt{2})$ tels que $\alpha_j \alpha_j^\sigma = \pm p_j$, $(1 \leq j \leq \ell)$ avec

$$\alpha_1 < 0, \quad \alpha_1^\sigma > 0, \qquad \alpha_2 > 0, \quad \alpha_2^\sigma < 0;$$

ce choix est fait pour que les quatre couples (α, α^σ), pour $\alpha \in \{\alpha_1, \alpha_2, \alpha_1^2, \alpha_1\alpha_2\}$, soient dans chacune des quatre composantes connexes de $(\mathbb{R}^\times)^2$:

$$\begin{array}{c|cl} & \alpha^\sigma & \\ \alpha_1 & \alpha_1^2 & \alpha \\ \hline \alpha_1\alpha_2 & \alpha_2 & \end{array}$$

Ce choix assure que le sous-groupe de $(\mathbb{R}^\times)^2$ engendré par $(\alpha_j, \alpha_j^\sigma)$, $(1 \leq j \leq \ell)$, a une intersection non nulle avec chacune des composantes connexes ; pour qu'il soit dense, il faut et il suffit que le sous-groupe de $(\mathbb{R}_+^\times)^2$ engendré par $\gamma_j = (|\alpha_j|, |\alpha_j^\sigma|)$, $(1 \leq j \leq \ell)$ soit dense dans $(\mathbb{R}_+^\times)^2$. Par exemple on peut prendre $p_1 = 7$, $p_2 = 17$, $p_3 = 23$, $p_4 = 31$, $p_5 = 41 \dots$ et

$$\alpha_1 = 1 - 2\sqrt{2}, \quad \alpha_2 = -1 + 3\sqrt{2}, \quad \alpha_3 = 5 - \sqrt{2} \quad \alpha_4 = -1 + 4\sqrt{2} \quad \alpha_5 = 7 - 2\sqrt{2}, \ \dots$$

Les nombres $|\alpha_1|, |\alpha_1^\sigma|, |\alpha_2|, |\alpha_2^\sigma|, \dots$ sont alors multiplicativement indépendants.

Par conséquent, si la conjecture des quatre exponentielles est vraie, alors

$$\left\{\left(\alpha_1^{s_1}\alpha_2^{s_2}\alpha_3^{s_3}, (\alpha_1^\sigma)^{s_1}(\alpha_2^\sigma)^{s_2}(\alpha_3^\sigma)^{s_3}\right);\ (s_1, s_2, s_3) \in \mathbb{Z}^3\right\},$$

sous-groupe de $(\mathbb{R}^\times)^2$ de rang 3, engendré par les images des nombres $\alpha_1, \alpha_2, \alpha_3$ via le plongement canonique du corps quadratique réel $\mathbb{Q}(\sqrt{2})$, est dense dans $(\mathbb{R}^\times)^2$.

b2) *Sous-groupes de $(\mathbb{R}_+^\times)^2$: le théorème des six exponentielles*

On peut démontrer une version partielle de l'affirmation $\boxed{4^?}$ ci-dessus : il suffit de supposer que Γ a un rang ≥ 4.

Proposition 1.6. – *Soit Γ un sous-groupe de type fini de $(K_+^\times)^2$.*
a) On suppose $\mathrm{rang}_\mathbb{Z}\Gamma \geq 4$ *et* $\mathrm{rang}_\mathbb{Z}\phi_{(a,b)}(\Gamma) \geq 2$ *pour tout* $(a,b) \in \mathbb{Z}\times\mathbb{Z}$, $(a,b) \neq 0$. *Alors Γ est dense dans $(\mathbb{R}_+^\times)^2$.*
b) On suppose $\mathrm{rang}_\mathbb{Z}\Gamma \geq 5$ *et* $\mathrm{rang}_\mathbb{Z}\phi_{(a,b)}(\Gamma) \geq 3$ *pour tout* $(a,b) \in \mathbb{Z}\times\mathbb{Z}$, $(a,b) \neq 0$. *Alors Γ contient un sous-groupe de rang 3 qui est dense dans $(\mathbb{R}_+^\times)^2$.*

L'énoncé a) est équivalent au cas réel du *théorème des six exponentielles* dont nous allons parler maintenant. L'énoncé complexe est le suivant (voir [L 1966], Chap. II, §1, Th. 1 ; [Ra 1968], p. 67 ; [W 1974], Chap.2 Cor. 2.2.3 ; [B 1979], Chap. 12 Th. 12.3).

Théorème 1.7* (théorème des six exponentielles). –
$\boxed{1}$ *Soient $x_1, \dots, x_d$ des nombres complexes linéairement indépendants sur $\mathbb{Q}$, et soient $y_1, \dots, y_\ell$ des nombres complexes linéairement indépendants sur $\mathbb{Q}$. On suppose $\ell d > \ell + d$. Alors l'un au moins des nombres*

$$e^{x_i y_j}, \qquad (1 \leq i \leq d,\ 1 \leq j \leq \ell)$$

est transcendant.
$\boxed{2}$ *Soit M une matrice $d \times \ell$ à coefficients logarithmes de nombres algébriques ; on suppose que les d lignes de M sont linéairement indépendantes sur $\mathbb{Q}$ et aussi que les ℓ colonnes de M sont linéairement indépendantes sur $\mathbb{Q}$; si $d\ell > d + \ell$, alors le rang de M est ≥ 2.*
$\boxed{3}$ *Soit D un hyperplan de $\mathbb{C}^2$; on suppose $D \cap \mathbb{Q}^2 = \{(0,0)\}$. Alors le $\mathbb{Q}$-espace vectoriel $D \cap \mathcal{L}^2$ est de dimension finie, et cette dimension est ≤ 2.*

Exercice. On munit le groupe multiplicatif $K_+^\times$ de la relation d'ordre induite par celle de $\mathbb{R}$. Montrer que le seul automorphisme de ce groupe qui préserve la relation d'ordre est l'identité.
(`Indication.` Montrer que si A et B sont deux sous-groupes non triviaux de $\mathbb{R}$ et ϕ un homomorphisme de groupes de A dans B qui préserve l'ordre, alors il existe $r \in \mathbb{R}$ tel que ϕ soit l'homothétie $x \mapsto rx$. Voir A.M.W. Glass and P. Ribenboim, Automorphisms of the ordered multiplicative group of positive rational numbers ; Proc. Amer. Math. Soc., **122** (1994), 15–18.)

On laisse en exercice la formulation du théorème des six exponentielles réelles, et sa déduction de la proposition 1.6. On se contentera ici de déduire la proposition 1.6 du théorème 1.7.

Démonstration de la proposition 1.6 comme conséquence de $\boxed{3}$.
a) Soit Γ un sous-groupe de type fini de $(K_+^\times)^2$ et de rang ≥ 4 tel que $\mathrm{rang}_\mathbb{Z}\phi_{(a,b)}(\Gamma) \geq 2$ pour tout $(a,b) \in \mathbb{Z}\times\mathbb{Z}$, $(a,b) \neq 0$. Soit φ une forme linéaire non nulle sur $\mathbb{R}^2$. Pour montrer que Γ est dense dans $(\mathbb{R}_+^\times)^2$, il suffit de vérifier $\mathrm{rang}_\mathbb{Z}\varphi(Y) \geq 2$ (où $Y = \exp_{G,\mathbb{R}}^{-1}(\Gamma)$). Si la droite $D = \mathrm{Ker}\ \varphi$ est rationnelle sur $\mathbb{Q}$, on choisit $(0,0) \neq (-b,a) \in \mathbb{Q}^2 \cap D$ de sorte que $\mathrm{rang}_\mathbb{Z}\varphi(Y) = \mathrm{rang}_\mathbb{Z}\phi_{(a,b)}(\Gamma)$; on peut alors utiliser l'hypothèse de la proposition 1.6. Sinon, on a $\mathbb{Q}^2 \cap D = \{(0,0)\}$ et on utilise $\boxed{3}$ qui donne $\mathrm{rang}_\mathbb{Z}\varphi(Y) = \mathrm{rang}_\mathbb{Z}(Y/Y\cap D) \geq 2$.
b) Grâce à la partie a) et au lemme 1.8 ci-dessous, les hypothèses faites sur Γ assurent que tout sous-groupe Γ' de Γ, de rang $\geq \ell - 1$, est dense dans $(\mathbb{R}_+^\times)^2$. On utilise alors le théorème 7.2 du chapitre II avec $R = (\mathbb{R}_+^\times)^2$, $n = 2$, $\mathrm{m}(R) = 3$ pour conclure. □

Lemme 1.8. – *Soient G un groupe commutatif, H un sous-groupe, Γ un sous-groupe de type fini de G de rang ℓ et Γ' un sous-groupe de Γ de rang ℓ'. Alors*

$$\mathrm{rang}_\mathbb{Z}(\Gamma'/\Gamma'\cap H) \geq \mathrm{rang}_\mathbb{Z}(\Gamma/\Gamma\cap H) - \ell + \ell'.$$

Démonstration. La démonstration tient en une ligne :

$$\ell' - \mathrm{rang}_\mathbb{Z}(\Gamma'/\Gamma'\cap H) = \mathrm{rang}_\mathbb{Z}(\Gamma'\cap H) \leq \mathrm{rang}_\mathbb{Z}(\Gamma\cap H) = \ell - \mathrm{rang}_\mathbb{Z}(\Gamma/\Gamma\cap H).$$

□

Exemple. Soit Γ un sous-groupe de $(\mathbb{R}_+^\times)^2$ engendré par ℓ éléments (α_j,β_j), où les 2ℓ nombres réels positifs α_j, β_j sont algébriques et multiplicativement indépendants. Si $\ell \geq 4$, alors Γ est dense dans $(\mathbb{R}_+^\times)^2$. Si $\ell \geq 5$, alors Γ contient un sous-groupe de rang 3 qui est dense dans $(\mathbb{R}_+^\times)^2$.

Exemple : le corps $\mathbb{Q}(\sqrt{2})$.

Considérons de nouveau les éléments

$$\alpha_1 = 1-2\sqrt{2},\quad \alpha_2=-1+3\sqrt{2},\quad \alpha_3=5-\sqrt{2}\quad \alpha_4=-1+4\sqrt{2}\quad \alpha_5=7-2\sqrt{2}$$

du corps $\mathbb{Q}(\sqrt{2})$. Le sous-groupe de $(\mathbb{R}^\times)^2$ de rang 4, engendré par les images des nombres $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ 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 $\alpha_1,\dots,\alpha_5$, contient un sous-groupe de rang 3 dont l'image par le plongement canonique est dense dans $(\mathbb{R}^\times)^2$. Cependant la démonstration ne permet pas de préciser un tel sous-groupe de rang 3.

Exercice. Soient $\alpha_0,\alpha_1,\alpha_2$, β_0,β_1,β_2 des nombres algébriques réels positifs. On suppose
- *α_0 et β_0 sont multiplicativement indépendants ;*
- *deux au moins des trois nombres $\alpha_0,\alpha_1,\alpha_2$ sont multiplicativement indépendants ;*
- *deux au moins des trois nombres β_0,β_1,β_2 sont multiplicativement indépendants ;*
- *le sous-groupe*

$$\Gamma = \left\{ (\alpha_0^{s_1}\alpha_1^{t_1}\alpha_2^{t_2}, \beta_0^{s_2}\beta_1^{t_1}\beta_2^{t_2})\,;\,(s_1,s_2,t_1,t_2)\in\mathbb{Z}^4 \right\}$$

de $(\mathbb{R}_+^\times)^2$ est de rang 4.
Montrer que Γ est dense dans $(\mathbb{R}_+^\times)^2$.

c) *Sous-groupes de $\mathbb{C}^\times$*

On désigne ici par G le groupe algébrique $\mathbb{G}_{\mathrm{m}}$, et on considère ses points complexes $\mathbb{G}_{\mathrm{m}}(\mathbb{C}) = \mathbb{C}^\times$. L'application de $\mathbb{R}^2$ dans $\mathbb{C}^\times$ qui envoie (x,y) sur $e^{x+2i\pi y}$ induit un isomorphisme de $\mathbb{R}\times\mathbb{R}/\mathbb{Z}$ sur $\mathbb{C}^\times$; on note $(s,p) : \mathbb{C}^\times \to \mathbb{R}\times\mathbb{R}/\mathbb{Z}$ l'isomorphisme inverse :

$$\begin{array}{cccc} s: & \mathbb{C}^\times & \to & \mathbb{R} \\ & z & \mapsto & \log|z| \end{array} \quad \text{et} \quad \begin{array}{cccc} p: & \mathbb{C}^\times & \to & \mathbb{R}/\mathbb{Z} \\ & z & \mapsto & \frac{1}{2i\pi}\log(z/|z|) \end{array}$$

Pour $z\in\mathbb{C}^\times$, le nombre $2\pi p(z)$ est "l'argument" de z vu comme classe d'un nombre réel modulo 2π.

Etant donné que $\mathrm{m}(\mathbb{R}) = 2$, on a :

Lemme 1.9. – *Si Γ est un sous-groupe dense de $\mathbb{C}^\times$, alors $s(\Gamma)$ est un sous-groupe dense de $\mathbb{R}$ et $p(\Gamma)$ est un sous-groupe dense de $\mathbb{R}/\mathbb{Z}$. Par conséquent, si Γ est de type fini, alors*

$$\mathrm{rang}_{\mathbb{Z}} s(\Gamma) \geq 2 \quad \textit{et} \quad \mathrm{rang}_{\mathbb{Z}} p(\Gamma) \geq 1.$$

Quand Γ est de type fini, si ℓ est son rang sur $\mathbb{Z}$ et si $\gamma_1,\dots,\gamma_\ell$ sont des éléments de Γ multiplicativement indépendants, alors la condition que $s(\Gamma)$ est dense dans $\mathbb{R}_+^\times$ signifie que deux au moins des ℓ nombres réels $|\gamma_1|,\dots,|\gamma_\ell|$ sont multiplicativement indépendants. La condition que $p(\Gamma)$ est dense dans $\mathbb{R}/\mathbb{Z}$ revient à dire que l'un au moins des ℓ nombres $\gamma_j/|\gamma_j|$, $(1\leq j\leq \ell)$ n'est pas une racine de l'unité.

Voyons maintenant ce qui se passe quand les coordonnées des éléments de Γ sont des nombres algébriques.

Théorème 1.10. – *Soit Γ un sous-groupe de type fini de $\overline{\mathbb{Q}}^\times$. On suppose $\mathrm{rang}_{\mathbb{Z}} p(\Gamma)\geq 1$.*
a) Si la conjecture des quatre exponentielles est vraie, alors Γ est dense dans $\mathbb{C}^\times$ si et seulement si $\mathrm{rang}_{\mathbb{Z}} s(\Gamma)\geq 2$.
b) Si $\mathrm{rang}_{\mathbb{Z}} s(\Gamma)\geq 3$, alors Γ est dense dans $\mathbb{C}^\times$.
c) Si $\mathrm{rang}_{\mathbb{Z}} s(\Gamma)\geq 4$ et $\mathrm{rang}_{\mathbb{Z}} p(\Gamma)\geq 2$, alors Γ contient un sous-groupe de rang 2 qui est dense dans $\mathbb{C}^\times$.

Démonstration. Soit ℓ le rang de Γ et soient $\gamma_1,\dots,\gamma_\ell$ des éléments multiplicativement indépendants de Γ ; grâce à la proposition 6.1 du chapitre II (voir le §7 du chapitre II), on sait que Γ est dense dans $\mathbb{C}^\times$ si et seulement si, pour tout $s\in\mathbb{Z}^{\ell+1}\setminus\{0\}$, la matrice à trois lignes et $\ell+1$ colonnes

$$\begin{pmatrix} 0 & \log|\gamma_1| & \cdots & \log|\gamma_\ell| \\ 2i\pi & \log(\gamma_1/|\gamma_1|) & \cdots & \log(\gamma_\ell/|\gamma_\ell|) \\ s_0 & s_1 & \cdots & s_\ell \end{pmatrix}$$

est de rang 3 ; cette condition ne dépend évidemment pas du choix des logarithmes complexes $\log(\gamma_j/|\gamma_j|)$ (et on peut remplacer tous les $\log(\gamma/|\gamma|)$ par $\log(\gamma/\overline{\gamma})$ si on le désire). La condition que deux au moins des ℓ nombres réels $|\gamma_1|,\dots,|\gamma_\ell|$ soient multiplicativement indépendants garantit le rang 3 pour la matrice quand $s_0=0$. On considère maintenant le cas $s_0\neq 0$; il s'agit alors de vérifier que la matrice

$$M = \begin{pmatrix} \log|\gamma_1| & \cdots & \log|\gamma_\ell| \\ s_0\log(\gamma_1/|\gamma_1|)-2i\pi s_1 & \cdots & s_0\log(\gamma_\ell/|\gamma_\ell|)-2i\pi s_\ell \end{pmatrix}$$

est de rang 2.
a) On admet la conjecture des quatre exponentielles. Les ℓ colonnes de la matrice M sont $\mathbb{Q}$-linéairement indépendantes (car les ℓ éléments de la première ligne le sont). Les deux lignes de M sont aussi $\mathbb{Q}$-linéairement indépendantes, car d'une part la seconde ligne n'est pas identiquement nulle (les quotients $\gamma_j/|\gamma_j|$ ne sont pas tous racines de l'unité), et d'autre part les éléments de la seconde ligne de M sont imaginaires purs alors que ceux de la première sont réels. D'après l'énoncé $\boxed{2^?}$ dans la conjecture $1.5^?$, la matrice M est de rang 2 dès que $\ell\geq 2$.
b) Supposons que trois au moins des nombres $|\gamma_1|,\dots,|\gamma_\ell|$ sont multiplicativement indépendants ; alors de la même manière on déduit de l'énoncé $\boxed{2}$ dans le théorème des six exponentielles que Γ est dense dans $\mathbb{C}^\times$.
c) Enfin, si quatre au moins des nombres $|\gamma_1|,\dots,|\gamma_\ell|$ sont multiplicativement indépendants, et si deux au moins des nombres $\gamma_j/|\gamma_j|$, $(1\leq j\leq\ell)$ sont multiplicativement indépendants, alors tout sous-groupe de Γ de rang $\ell-1$ est dense dans $\mathbb{C}^\times$ (d'après b) et le lemme 1.8), et par conséquent Γ contient un sous-groupe de rang 2 dense dans $\mathbb{C}^\times$.

Exemple : le corps $\mathbb{Q}(i)$.

On choisit ℓ nombres premiers distincts congrus à 1 modulo 4, par exemple $5,13,17,29,\ldots$. Cela permet de trouver ℓ éléments $\gamma_1,\dots,\gamma_\ell$ de $\mathbb{Q}(i)^\times$ tels que les 2ℓ nombres complexes γ_j, $\overline{\gamma}_j$, $(1\leq j\leq\ell)$ soient multiplicativement indépendants ; par exemple

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

Le sous-groupe de $\mathbb{Q}(i)^\times$, 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

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

n'est pas nul.

Exercice. Construire un sous-groupe A de $\mathbb{C}^\times$ (remplaçant le groupe multiplicatif $\overline{\mathbb{Q}}^\times$) qui vérifie :
a) Si Γ est un sous-groupe de type fini de A, alors Γ est dense dans $\mathbb{C}^\times$ si et seulement si $\mathrm{rang}_{\mathbb{Z}} p(\Gamma) \geq 1$ *et* $\mathrm{rang}_{\mathbb{Z}} s(\Gamma) \geq 2$.
b) Soit $L = \exp^{-1}(A)$; il existe une matrice 2×2 de rang 1 à coefficients dans L dont les lignes sont $\mathbb{Q}$-linéairement indépendantes et dont les colonnes sont $\mathbb{Q}$-linéairement indépendantes.
`Indication.` On peut construire des exemples triviaux avec $A \subset \mathbb{R}_+^\times$ se sorte que $\mathrm{rang}_{\mathbb{Z}}(L/L \cap \mathbb{R}) \leq 1$. Un exemple non-trivial est obtenu en prenant pour A le sous-groupe de $\mathbb{C}^\times$ engendré par e^{x_1}, e^{x_2} et $e^{i\sqrt{x_1 x_2}}$ où x_1 et x_2 sont deux nombres réels positifs avec π, x_1, x_2 algébriquement indépendants.

Remarque. Dans les deux exemples précédents (à savoir $\mathbb{R} \times \mathbb{R}_+^\times$ et $(\mathbb{R}_+^\times)^2$) nous avons vu que, grâce à un énoncé de transcendance, la seule hypothèse nécessaire pour assurer la densité d'un sous-groupe formé de points algébriques faisait intervenir les sous-groupes algébriques de $\mathbb{G}_{\mathrm{a}} \times \mathbb{G}_{\mathrm{m}}$ et $\mathbb{G}_{\mathrm{m}}^2$ respectivement. Dans le dernier exemple $\mathbb{C}^\times$, le sous-groupe algébrique sous-jacent est $\mathbb{G}_{\mathrm{m}}$ dont les seuls sous-groupes algébriques sont $\mathbb{G}_{\mathrm{m}}$ lui-même et les sous-groupes finis. Pour comprendre ce qui se passe il faut regarder la proposition 6.1 du chapitre II : on considère l'application φ de $\mathbb{C}^\times$ dans $(\mathbb{C}^\times)^2$ qui envoie z sur $(z, \overline{z})$. Ce sont les intersections de $\varphi(\mathbb{C}^\times)$ avec les sous-groupes algébriques de $\mathbb{G}_{\mathrm{m}}^2$ qui controlent la situation.

Lemme 1.11. – *Les sous-groupes de $\mathbb{C}^\times$ de la forme*

$$H = \varphi^{-1}\bigl(G'(\mathbb{C})\bigr) = \bigl\{z \in \mathbb{C}^\times ;\ (z, \overline{z}) \in G'(\mathbb{C})\bigr\},$$

où G' est un sous-groupe algébrique de $\mathbb{G}_{\mathrm{m}}^2$, sont les suivants :

$$\mathbb{C}^\times, \qquad \mathbb{U} = \{z \in \mathbb{C}^\times ;\ |z| = 1\}, \qquad \{x\zeta ;\ x \in \mathbb{R}_+^\times,\ \zeta \in \mu_{2n}\}, \qquad \mu_n,$$

où n est un entier ≥ 1, et μ_n désigne le groupe cyclique formé de racines n-ièmes de l'unité dans $\mathbb{C}^\times$.

Démonstration. Chacun des groupes indiqués est clairement de la forme $H = \varphi^{-1}\bigl(G'(\mathbb{C})\bigr)$ pour un sous-groupe algébrique convenable G' de $\mathbb{G}_{\mathrm{m}}^2$. Il reste à vérifier qu'il n'y en a pas d'autre.

D'après le lemme 2.2 ci-dessous, le sous-groupe algébrique G' est défini par des équations monomiales $z_1^{a_i} z_2^{b_i} = 1$, $(1 \leq i \leq m)$, avec $(a_i, b_i) \in \mathbb{Z}^2$. On distingue plusieurs cas.
a) Si $a_i = b_i = 0$ pour tout $i = 1, \ldots, m$, alors $G' = \mathbb{G}_{\mathrm{m}}^2$ et $H = \mathbb{C}^\times$. On suppose maintenant (ce n'est pas restrictif) $(a_i, b_i) \neq (0,0)$ pour tout $i = 1, \ldots, m$.
b) Si $a_i = b_i$ pour tout i, alors H est l'ensemble des $z \in \mathbb{C}^\times$ vérifiant $|z|^{2a_i} = 1$, $(1 \leq i \leq m)$, et alors $H = \mathbb{U}$.
c) Si $a_i = -b_i$ pour tout $i = 1, \ldots, m$, les équations de H s'écrivent $(z/\overline{z})^{a_i} = 1$; pour $z \in H$ on a $(z/|z|)^{2a_i} = (z/\overline{z})^{a_i} = 1$, donc $H \cap \mathbb{U}$ est le groupe des racines de l'unité $\zeta \in \mathbb{U}$ vérifiant $\zeta^{2a_i} = 1$, et on a $H = \{x\zeta ;\ x \in \mathbb{R}_+^\times,\ \zeta \in \mu_{2a_i},\ (1 \leq i \leq m)\}$. Par exemple on trouve le sous-groupe $\mathbb{R}^\times$ en prenant $F = \{1, -1\}$, alors que $\mathbb{R}_+^\times$ n'est pas de la forme $\varphi^{-1}\bigl(G'(\mathbb{C})\bigr)$ (si une demi-droite $\{x\zeta ;\ x \in \mathbb{R}_+^\times\}$ est contenue dans H, alors la demi-droite opposée $\{-x\zeta ;\ x \in \mathbb{R}_+^\times\}$ est aussi contenue dans H).
d) Si $a_i \neq \pm b_i$ pour un i, alors pour $z \in H$ on a d'une part $|z|^{a_i + b_i} = 1$, donc $|z| = 1$ et $\overline{z} = 1/z$, d'autre part $z^{a_i - b_i} = 1$, donc z est une racine de l'unité et H est fini. Enfin tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique. $\square$

Remarque. On s'intéresse au rang de l'image de Γ dans $\mathbb{C}^\times/H$; si H^0 désigne la composante connexe de l'élément neutre de H, on a

$$\mathrm{rang}_{\mathbb{Z}}(\Gamma/\Gamma \cap H) = \mathrm{rang}_{\mathbb{Z}}(\Gamma/\Gamma \cap H^0).$$

La liste des sous-groupes H^0 de $\mathbb{C}^\times$ qui apparaissent comme composantes connexes d'un $\varphi^{-1}\bigl(G'(\mathbb{C})\bigr)$, avec G' sous-groupe algébrique de G, est : $\mathbb{C}^\times$, $\mathbb{U}$, $\mathbb{R}_+^\times$ et $\{1\}$.

§2. Le théorème du sous-groupe linéaire

Soient d_0 et d_1 deux entiers ≥ 0 avec $d = d_0 + d_1 > 0$. Soit Γ un sous-groupe de type fini de $\mathbb{R}^{d_0} \times (\mathbb{R}^\times)^{d_1}$. Pour étudier la densité de Γ, on va, dans un premier temps, faire intervenir les sous-groupes algébriques de $G = \mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}$: si Γ est dense dans $G(\mathbb{R})$, alors pour tout sous-groupe algébrique G' de G, $G' \neq G$, l'image de Γ dans le quotient de $G(\mathbb{R})$ par $G'(\mathbb{R})$ est encore dense. On commence donc par étudier les sous-groupes algébriques et les quotients de G. Ensuite on énonce le *théorème du sous-groupe linéaire* qui permet de majorer le rang de $Y/Y \cap V$ quand $Y = \exp_G^{-1}(\Gamma)$ et V est un hyperplan de $\mathbb{R}^d$. Une telle estimation ne peut pas être valable pour tous les hyperplans V : il faut supposer que V ne contient pas d'espace tangent à un sous-groupe algébrique G' de dimension positive. On appliquera ensuite ce théorème de transcendance au problème de densité pour donner une réponse partielle (qui étend à tous les groupes algébriques linéaires commutatifs ce que nous avons fait au §1 dans le cas où le groupe de Lie réel est de dimension 2).

a) *Sous-groupes algébriques de $G = \mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}$*

Soit K un corps algébriquement clos de caractéristique nulle. Nous allons déterminer tous les sous-groupes algébriques de $G = G_0 \times G_1$ où $G_0 = \mathbb{G}_{\mathrm{a}}^{d_0}$ et $G_1 = \mathbb{G}_{\mathrm{m}}^{d_1}$. Si G' est un sous-groupe algébrique connexe de G alors $G'(\mathbb{C})$ est un sous-groupe de $G(\mathbb{C})$, l'image inverse de $G'(\mathbb{C})$ par l'application exponentielle de G est un sous-espace vectoriel de $\mathbb{C}^d$ que l'on notera $T_{G'}(\mathbb{C})$, la restriction de $\exp_G$ à ce sous-espace est l'application exponentielle de $G'(\mathbb{C})$, et enfin le groupe quotient $G(\mathbb{C})/G'(\mathbb{C})$ est le groupe des points complexes d'un groupe algébrique linéaire commutatif G/G'.

a$_1$) *Sous-groupes algébriques de* $G_0 = \mathbb{G}_{\mathrm{a}}^{d_0}$

Commençons par montrer que les sous-groupes algébriques de G_0 sont les sous-espaces vectoriels de $G_0(K) = K^{d_0}$. Il y a un sens facile : si H_0 est un sous-espace vectoriel de K^{d_0}, comme H_0 est intersection d'hyperplans, il est défini par des équations polynomiales (de degré 1), donc H_0 est le groupe (additif) des points rationnels sur K d'un sous-groupe algébrique G_0' de G_0. La dimension δ_0 du groupe algébrique G_0' est égale à la dimension du K-espace vectoriel H_0. Le quotient K^{d_0}/H_0 est aussi le groupe additif des points rationnels sur K d'un groupe algébrique, G_0/G_0', isomorphe à $\mathbb{G}_{\mathrm{a}}^{d_0-\delta_0}$. Enfin si k est un sous-corps de K et si le K-espace vectoriel H_0 est rationnel (*) sur k, alors le groupe algébrique G_0' est *défini sur* k (c'est-à-dire peut être défini par des équations polynomiales à coefficients dans k).

Voici la réciproque :

Lemme 2.1. – *Soit G_0' un sous-groupe algébrique de G_0. Alors $G_0'(K)$ est un sous-espace vectoriel de $G_0(K) = K^{d_0}$.*

Démonstration. Comme $G_0'(K)$ est un déjà un sous-groupe additif de $G_0(K)$, pour montrer que c'est un sous-espace vectoriel il reste à vérifier qu'il est stable par multiplication par un élément de K. Soit $x \in G_0'(K)$ et soit $\lambda \in K$. Soit $P \in K[X_1, \dots, X_{d_0}]$ un élément de l'idéal des polynômes qui s'annulent sur le sous-groupe algébrique G_0'. Il s'agit de montrer que $P(\lambda x)$ est nul. Or on a $nx \in G_0'(K)$ pour tout $n \in \mathbb{Z}$, ce qui montre que le polynôme $P(tx) \in K[t]$ a une infinité de zéros, donc est identiquement nul. $\square$

Exercice. Sous les hypothèses du lemme 2.1, si k est un sous-corps de K sur lequel G_0' est défini, alors le K-espace vectoriel $G_0'(K)$ est rationnel sur k.

Remarque. On a supposé que le corps K était de caractéristique nulle ; cette hypothèse est intervenue pour dire que le polynôme $P(tx) \in K[t]$, nul sur $\mathbb{Z}$, a une infinité de zéros dans K. Sur un corps de caractéristique finie il existe des sous-groupes algébriques de $\mathbb{G}_{\mathrm{a}}^{d_0}$ qui ne sont pas des sous-espaces vectoriels, à cause des Frobenius $z \mapsto z^q$. Cela donne lieu à la théorie des modules de Carlitz et Drinfeld, où la transcendance fait aussi l'objet de nombreuses études.

Prenons maintenant $K = \mathbb{C}$; comme l'application exponentielle de $G_0(\mathbb{C})$ est l'identité, si G_0' est un sous-groupe algébrique de G_0, alors l'application exponentielle de $G_0'(\mathbb{C})$ est encore l'identité du $\mathbb{C}$-espace $G_0'(\mathbb{C})$ dans lui-même. On notera alors $T_{G_0'}(\mathbb{C}) = G_0'(\mathbb{C})$. Si G_0' est défini sur $\mathbb{R}$, alors $T_{G_0'}(\mathbb{R}) = G_0'(\mathbb{R})$ et $\exp_{G_0',\mathbb{R}} : T_{G_0'}(\mathbb{R}) \to G_0'(\mathbb{R})$ est encore l'identité.

(*) Voir le rappel au début du paragraphe 1, p.45.

a$_2$) *Sous-groupes algébriques de* $G_1 = \mathbb{G}_{\mathrm{m}}^{d_1}$

Considérons maintenant le cas $d_0 = 0$: il s'agit d'étudier les sous-groupes algébriques de G_1. Si $a^{(i)} = \left(a_1^{(i)}, \dots, a_{d_1}^{(i)}\right)$, $(1 \le i \le n)$ sont des éléments de $\mathbb{Z}^{d_1}$, le sous-groupe multiplicatif de $(K^\times)^{d_1}$ défini par

$$H_1 = \left\{(x_1, \dots, x_{d_1}) \in (K^\times)^{d_1};\ x_1^{a_1^{(i)}} \cdots x_{d_1}^{a_{d_1}^{(i)}} = 1,\ (1 \le i \le n)\right\}$$

est le groupe des points rationnels sur K d'un sous-groupe algébrique G_1' de G_1. On définit un groupe algébrique quotient G_1/G_1' dont les points rationnels sur K sont donnés par l'image de l'application $(K^\times)^{d_1} \to (K^\times)^n$:

$$(x_1, \dots, x_{d_1}) \to \left(x_1^{a_1^{(i)}} \cdots x_{d_1}^{a_{d_1}^{(i)}}\right)_{1 \le i \le n}$$

Exercice. Vérifier que si le rang du $\mathbb{Z}$-module engendré par $a^{(1)}, \dots, a^{(n)}$ dans $\mathbb{Z}^{d_1}$ est $d_1 - \delta_1$, alors la dimension du sous-groupe algébrique G_1' est δ_1, et G_1' est isomorphe à un produit de $\mathbb{G}_{\mathrm{m}}^{\delta_1}$ par un groupe fini (G_1' n'est pas nécessairement connexe).
Vérifier ensuite que le quotient G_1/G_1' est isomorphe à $\mathbb{G}_{\mathrm{m}}^{d_1-\delta_1}$.

Pour montrer que tout sous-groupe algébrique de G_1 est de cette forme, nous introduisons la notation suivante : quand A est un sous-groupe de $\mathbb{Z}^{d_1}$, on pose

$$\mathcal{T}_A(K) = \left\{(y_1, \dots, y_{d_1}) \in (K^\times)^{d_1} ;\ y_1^{a_1} \cdots y_{d_1}^{a_{d_1}} = 1 \ \text{ pour tout } \ (a_1, \dots, a_{d_1}) \in A\right\}$$

Cela définit, comme nous venons de le voir, un sous-groupe algébrique $\mathcal{T}_A$ de G_1.

Lemme 2.2. – *L'application $A \mapsto \mathcal{T}_A$ est une bijection entre les sous-groupes A de $\mathbb{Z}^{d_1}$ et les sous-groupes algébriques $\mathcal{T}_A$ de G_1.*

Remarque. Soient k un corps de caractéristique nulle et $\gamma_1, \dots, \gamma_d$ des éléments non nuls de k. Alors *le sous-groupe multiplicatif Γ de $k^\times$ engendré par $\gamma_1, \dots, \gamma_d$ a pour rang sur $\mathbb{Z}$ la dimension du plus petit sous-groupe algébrique G' de $\mathbb{G}_{\mathrm{m}}^d$ tel que $(\gamma_1, \dots, \gamma_d) \in G'(k)$.* En effet, si A désigne le noyau de l'application $\mathbb{Z}^d \to \Gamma$ qui envoie $(a_1, \dots, a_d)$ sur $\gamma_1^{a_1} \cdots \gamma_d^{a_d}$, on a $d - \mathrm{rang}_{\mathbb{Z}} A = \mathrm{rang}_{\mathbb{Z}} \Gamma$ et $G' = \mathcal{T}_A$. L'exercice suivant montre que $G'(k)$ est l'adhérence de Zariski du sous-groupe engendré par $(\gamma_1, \dots, \gamma_d)$ dans $\mathbb{G}_{\mathrm{m}}^d(k) = (k^\times)^d$.

Exercice. Montrer que si G est un groupe algébrique sur un corps k de caractéristique nulle et Γ un sous-groupe de $G(k)$, alors l'adhérence de Zariski de Γ dans $G(k)$ est le groupe des points rationnels sur k d'un sous-groupe algébrique de G.

Pour démontrer le lemme 2.2 nous utiliserons le théorème d'indépendance linéaire des caractères d'Artin (voir par exemple [L 1993], Chap.VI, Theorem 4.1) que voici :

Lemme 2.3. – *Soient G un groupe commutatif, K un corps et $\chi_1, \dots, \chi_n$ des homomorphismes deux-à-deux distincts de G dans $K^\times$. Alors $\chi_1, \dots, \chi_n$ sont linéairement indépendants sur K.*

Démonstration. Soient $\lambda_1, \dots, \lambda_n$ des éléments de K non tous nuls tels que $\lambda_1\chi_1 + \cdots + \lambda_n\chi_n = 0$. Parmi toutes les relations de cette forme, choisissons-en une pour laquelle le nombre d'indices i, $(1 \le i \le n)$ avec $\lambda_i \neq 0$ est minimal. Sans perte de généralité on peut supposer que c'est la relation que nous avons écrite. Dans ce cas on a $n \ge 2$ et $\lambda_i \neq 0$ pour tout $i = 1, \dots, n$. Soit $x_0 \in G$; pour tout $x \in G$ on a

$$\sum_{i=1}^n \lambda_i \chi_i(x) = 0 \qquad \text{et} \qquad \sum_{i=1}^n \lambda_i \chi_i(x_0 x) = 0;$$

comme $\chi_i(x_0x) = \chi_i(x_0)\chi_i(x)$ par combinaison linéaire on peut écrire

$$\sum_{i=1}^n \lambda_i\bigl(\chi_n(x_0) - \chi_i(x_0)\bigr)\chi_i(x) = 0$$

pour tout $x \in G$. Le coefficient de $\chi_n(x)$ étant nul, cette relation est "plus courte" que celle dont nous étions parti. Donc $\lambda_i\bigl(\chi_n(x_0) - \chi_i(x_0)\bigr) = 0$ pour $1 \le i \le n-1$. Comme $\lambda_i \neq 0$ pour tout i, on a $\chi_n(x_0) = \chi_i(x_0)$ pour tout $i = 1, \dots, n-1$, et ceci pour tout $x_0 \in G$. Or les caractères χ_i sont deux-à-deux distincts. $\square$

Démonstration du lemme 2.2.
Pour chaque $a = (a_1, \dots, a_{d_1}) \in \mathbb{Z}^{d_1}$ on définit un caractère $\chi_a \colon (K^\times)^{d_1} \to K^\times$ par

$$\chi_a(y_1, \dots, y_{d_1}) = y_1^{a_1} \cdots y_{d_1}^{a_{d_1}} \qquad \text{pour tout } (y_1, \dots, y_{d_1}) \in (K^\times)^{d_1}.$$

On associe aussi à chaque sous-groupe algébrique G_1' de G_1 un sous-groupe $\Phi(G_1')$ de $\mathbb{Z}^{d_1}$:

$$\Phi(G_1') = \{a \in \mathbb{Z}^{d_1} ;\ G_1' \subset \operatorname{Ker} \chi_a\}.$$

Nous allons vérifier que l'application qui associe à un sous-groupe A de $\mathbb{Z}^{d_1}$ le sous-groupe algébrique $\mathcal{T}_A$ de G_1, et l'application qui associe au sous-groupe algébrique G_1' de G_1 le sous-groupe $\Phi(G_1')$ de $\mathbb{Z}^{d_1}$ sont des bijections réciproques. Les inclusions $G_1' \subset \mathcal{T}_{\Phi(G_1')}$ et $A \subset \Phi(\mathcal{T}_A)$ sont évidentes. Il reste à montrer que ce sont des égalités.

Soit G_1' un sous-groupe algébrique de G_1 et soit $G_1'' = \mathcal{T}_{\Phi(G_1')}$. Par construction, si a et b sont des éléments de $\mathbb{Z}^{d_1}$, alors χ_a et χ_b donnent par restriction à $G_1'(K)$ le même caractère dans $K^\times$ si et seulement si $a - b \in \Phi(G_1') \subset \mathbb{Z}^{d_1}$, et dans ce cas ils donnent par restriction le même caractère de $G_1''(K)$. Nous allons vérifier l'égalité $G_1' = G_1''$ en montrant que tout polynôme $P(\underline{Y}) \in K[\underline{Y}]$ qui s'annule sur $G_1'(K)$ s'annule aussi sur $G_1''(K)$. En fait la fonction $f \colon (K^\times)^{d_1} \to K$ induite par un polynôme peut-être écrite comme une combinaison linéaire

$$f = \sum_{a \in R} p_a \chi_a$$

où R est un sous-ensemble fini de $\mathbb{N}^{d_1}$ et $(p_a)_{a\in R}$ est une famille d'éléments de K. Soit $\overline{R}$ l'image de R par l'application canonique de $\mathbb{Z}^{d_1}$ sur $\mathbb{Z}^{d_1}/\Phi(G_1')$. Pour chaque $\overline{a} \in \overline{R}$, on désigne par $R_{\overline{a}}$ l'image inverse de $\overline{a}$ dans R et par $\chi_{\overline{a}}$ et $\chi'_{\overline{a}}$ les caractères de $G_1'(K)$ et $G_1''(K)$ respectivement, à valeurs dans $K^\times$, induits par la restriction de χ_a pour $a \in \overline{a}$: ces caractères ne dépendent pas du choix de a. Alors la restriction de f à $G_1'(K)$ et $G_1''(K)$ s'écrit respectivement

$$\sum_{\overline{a}\in\overline{R}} \Bigl(\sum_{a\in R_{\overline{a}}} p_a\Bigr)\chi_{\overline{a}} \quad \text{et} \quad \sum_{\overline{a}\in\overline{R}} \Bigl(\sum_{a\in R_{\overline{a}}} p_a\Bigr)\chi'_{\overline{a}}.$$

Si f s'annule sur $G_1'(K)$, alors la somme à gauche est nulle, et comme les $\chi_{\overline{a}}$ pour $\overline{a} \in \overline{R}$ sont des caractères distincts de $G_1'(K)$ à valeurs dans $K^\times$, le lemme implique qu'ils sont linéairement indépendants sur K. On a donc

$$\sum_{a\in R_{\overline{a}}} p_a = 0 \quad \text{pour tout } \overline{a} \in \overline{R},$$

ce qui montre que la restriction de f à $G_1''(K)$ est aussi nulle.

Considérons maintenant un sous-groupe A de $\mathbb{Z}^{d_1}$; posons $A' = \Phi(\mathcal{T}_A)$. On a $A \subset A'$ et $\mathcal{T}_A = \mathcal{T}_{A'}$. Si $A \neq A'$, alors (voir exercice ci-dessous), puisque K est algébriquement clos, il existe un caractère non trivial sur A' qui est trivial sur A, et ce caractère s'étend en un caractère $c \colon \mathbb{Z}^{d_1} \to K^*$ donné par

$$c(a_1, \dots, a_{d_1}) = y_1^{a_1} \cdots y_{d_1}^{a_{d_1}}$$

pour un élément $y = (y_1, \dots, y_{d_1})$ de $(K^*)^{d_1}$. Par construction, on a $y \in \mathcal{T}_A$ et $y \notin \mathcal{T}_{A'}$. Cette contradiction montre que l'on doit avoir $A = A'$. $\square$

Exercice.
a) Si A est un groupe abélien de type fini non réduit à l'élément neutre, il existe un caractère non trivial sur A à valeur dans $K^\times$.
(Utiliser le théorème de structure des groupes abéliens de type fini, avec le fait que K est algébriquement clos.)
b) Si B est un groupe abélien de type fini et $A \subset B$ un sous-groupe avec $A \neq B$, il existe un caractère non trivial sur B mais trivial sur A.
(Appliquer a) à B/A.)
c) Si A est un sous-groupe de $\mathbb{Z}^d$ et χ un caractère de A, il existe $y = (y_1, \dots, y_d) \in (K^*)^d$ tel que, pour $(a_1, \dots, a_d) \in A$, on ait

$$\chi(a_1, \dots, a_d) = y_1^{a_1} \cdots y_d^{a_d}.$$

(Utiliser le théorème des diviseurs élémentaires : il existe une base $(e_1, \dots, e_d)$ de $\mathbb{Z}^d$, et des entiers r, $\delta_1, \dots, \delta_r$, tels que $(\delta_1 e_1, \dots, \delta_r e_r)$ soit une base de A.)

Quand $K = \mathbb{C}$, si A est un sous-groupe de $\mathbb{Z}^{d_1}$ de rang $d_1 - \delta_1$ et $G_1' = \mathcal{T}_A$, l'application exponentielle de $G_1'(\mathbb{C})$ est définie comme la restriction de $\exp_{G_1}$ au $\mathbb{C}$-espace vectoriel

$$T_{G_1'}(\mathbb{C}) = \Big\{(z_1, \ldots, z_{d_1}) \in \mathbb{C}^{d_1}\, ;\ \sum_{i=1}^{d_1} a_i z_i = 0 \quad \text{pour tout } a \in A\Big\}.$$

Ce $\mathbb{C}$-espace vectoriel est de dimension δ_1 et rationnel sur $\mathbb{Q}$; inversement, *tout sous-espace W de $\mathbb{C}^{d_1}$, rationnel sur $\mathbb{Q}$, est de la forme $T_{G_1'}(\mathbb{C})$ pour un sous-groupe algébrique G_1' de* G_1 : il suffit de définir G_1' par $G_1'(\mathbb{C}) = \exp_{G_1}(W)$ (ce qui donne même un sous-groupe algébrique connexe).

Comme G_1' est défini sur $\mathbb{Q}$, donc sur $\mathbb{R}$, l'application $\exp_{G_1',\mathbb{R}}$ est toujours définie :

$$\begin{array}{rccc} \exp_{G_1',\mathbb{R}} : & T_{G_1'}(\mathbb{R}) & \longrightarrow & G_1'(\mathbb{R})^0 \\ & (x_1, \ldots, x_{d_1}) & \longmapsto & (e^{x_1}, \ldots, e^{x_{d_1}}) \end{array}$$

où

$$T_{G_1'}(\mathbb{R}) = \Big\{(x_1, \ldots, x_{d_1}) \in \mathbb{R}^{d_1}\, ;\ \sum_{i=1}^{d_1} a_i x_i = 0 \quad \text{pour tout } a \in A\Big\}.$$

Exercice. Soient $\theta_1, \ldots, \theta_r$ des nombres réels positifs multiplicativement indépendants et $b_{i\varrho}$, $(1 \le i \le d$, $1 \le \varrho \le r)$ des entiers rationnels. On définit $(\alpha_1, \ldots, \alpha_d) \in (\mathbb{R}_+^\times)^d$ par

$$\alpha_i = \prod_{\varrho=1}^{r} \theta_\varrho^{b_{i\varrho}}, \qquad (1 \le i \le d).$$

On désigne par $H(\mathbb{R})$ l'adhérence de Zariski dans $\mathbb{G}_{\mathrm{m}}(\mathbb{R})^d$ du sous-groupe

$$\big\{(\alpha_1^s, \ldots, \alpha_d^s)\, ;\ s \in \mathbb{Z}\big\}$$

engendré par l'élément $(\alpha_1, \ldots, \alpha_d)$. Montrer que la composante connexe de l'élément neutre de $H(\mathbb{R})$ est

$$H(\mathbb{R})^0 = H(\mathbb{R}) \cap (\mathbb{R}_+^\times)^d = \Big\{\Big(\prod_{\varrho=1}^{r} x_\varrho^{b_{1\varrho}}, \ldots, \prod_{\varrho=1}^{r} x_\varrho^{b_{d\varrho}}\Big)\, ;\ (x_1, \ldots, x_r) \in (\mathbb{R}_+^\times)^r\Big\}.$$

a$_3$) *Sous-groupes algébriques de $G_0 \times G_1$*

Après avoir étudié les sous-groupes algébriques de chacun des deux facteurs $G_0 = \mathbb{G}_{\mathrm{a}}^{d_0}$ et $G_1 = \mathbb{G}_{\mathrm{m}}^{d_1}$, nous pouvons maintenant décrire les sous-groupes du produit $G = G_0 \times G_1$. Chaque fois que G_0' est un sous-groupe algébrique de G_0 et G_1' un sous-groupe algébrique de G_1, le produit $G' = G_0' \times G_1'$ est un sous-groupe algébrique de G, de dimension $\dim G_0' + \dim G_1'$, et le quotient $G/G' = (G_0/G_0') \times (G_1/G_1')$ est encore un groupe algébrique linéaire. Nous allons voir que ces produits $G_0' \times G_1'$ épuisent la liste des sous-groupes algébriques de G

Lemme 2.4. – *Soit G' un sous-groupe algébrique de $G = G_0 \times G_1$. Alors il existe un sous-groupe algébrique G_0' de G_0 et un sous-groupe algébrique G_1' de G_1 tels que $G' = G_0' \times G_1'$.*

La démonstration va utiliser un lemme sur les polynômes exponentiels.

Lemme 2.5. – *Soient K un corps de caractéristique nulle, $\alpha_1, \ldots, \alpha_n$ des éléments de $K^\times$ deux-à-deux distincts, et $a_1, \ldots, a_n$ des polynômes non nuls de $K[X]$. On désigne par d_i le degré de a_i, $(1 \le i \le n)$. Alors la fonction*

$$\begin{array}{rccc} F : & \mathbb{Z} & \longrightarrow & K \\ & m & \longmapsto & \sum_{i=1}^n a_i(m)\alpha_i^m \end{array}$$

ne peut pas s'annuler sur un ensemble de $d_1 + \cdots + d_n + n$ entiers consécutifs.

Démonstration. La démonstration se fait par récurrence sur l'entier $d_1 + \cdots + d_n + n$. Notons déjà que le résultat est banal si $n = 1$. On définit, pour $m \in \mathbb{Z}$,

$$\Phi(m) = \alpha_n^{-m} F(m) = \sum_{i=1}^{n} a_i(m)\beta_i^m,$$

avec $\beta_i = \alpha_i/\alpha_n$, de sorte que $\beta_1, \ldots, \beta_n$ sont encore des éléments de $K^\times$ deux-à-deux distincts, et $\beta_n = 1$. On écrit ensuite

$$\Phi(m+1) - \Phi(m) = \sum_{i=1}^{n} b_i(m)\beta_i^m,$$

avec $b_i(X) = \beta_i a_i(X+1) - a_i(X)$, $(1 \le i \le n)$. Pour $1 \le i \le n-1$ le polynôme $b_i \in K[X]$ est de degré d_i, tandis que b_n est soit nul, soit de degré $< d_n$. Dans tous les cas on peut appliquer l'hypothèse de récurrence pour conclure que l'application $m \mapsto \Phi(m+1) - \Phi(m)$ ne peut pas s'annuler sur un ensemble de $d_1 + \cdots + d_n + n - 1$ entiers consécutifs. ☐

Exercice.
a) Vérifier que l'estimation donnée dans le lemme 2.5 est optimale : étant donnés un corps K de caractéristique nulle, des éléments $\alpha_1, \ldots, \alpha_n$ de $K^\times$ deux-à-deux distincts, des entiers $d_1, \ldots, d_n$ tous ≥ 0, et un ensemble E de $d_1 + \cdots + d_n + n - 1$ entiers consécutifs, montrer qu'il existe des polynômes non nuls $a_1, \ldots, a_n$ de $K[X]$, avec a_i de degré d_i, $(1 \le i \le n)$, tels que la fonction

$$\begin{array}{rccc} F : & \mathbb{Z} & \longrightarrow & K \\ & m & \longmapsto & \sum_{i=1}^n a_i(m)\alpha_i^m \end{array}$$

s'annule sur E.
b) Montrer que le lemme 2.5 peut s'énoncer de manière équivalente sous la forme suivante : Soient K un corps de caractéristique nulle, $\alpha_1, \ldots, \alpha_n$ des éléments de $K^\times$ deux-à-deux distincts, $d_1, \ldots, d_n$ des entiers tous ≥ 0 et M un nombre entier. On ordonne l'ensemble des $d_1 + \cdots + d_n + n$ couples (i, j) d'entiers vérifiant $0 \le j \le d_i$, $1 \le i \le n$, et on forme la matrice

$$M = \Big(m^j \alpha_i^m\Big)_{\substack{0 \le j \le d_i,\ 1 \le i \le n \\ M+1 \le m \le M+d_1+\cdots+d_n+n}}.$$

Alors le déterminant Δ de M n'est pas nul.
c) Calculer explicitement le déterminant Δ.
`Indication.` Voir U. Rausch, On a theorem of Dobrowolski about the product of conjugate numbers, Colloquium Math. **50** (1985), 137–142.

Démonstration du lemme 2.4. On pose

$$G'_0 = \{x \in G_0;\ (x,1) \in G'\} \qquad \text{et} \qquad G'_1 = \{y \in G_1;\ (0,y) \in G'\}.$$

On a évidemment $G'_0 \times G'_1 \subset G'$. Pour montrer l'inclusion dans l'autre sens, on choisit d'abord un élément (x,y) dans G', puis un polynôme P nul sur G', et on pose, pour $(m,n) \in \mathbb{Z}^2$,

$$f(m,n) = P(mx, y^n).$$

Pour $m \in \mathbb{Z}$ on a $(mx, y^m) \in G'$, donc $f(m,m) = 0$. Le lemme 2.5 implique alors $f(m,n) = 0$ pour tout $(m,n) \in \mathbb{Z}^2$, donc $f(1,0) = f(0,1) = 0$. Ceci montre que $(x,1)$ et $(0,y)$ appartiennent à G'. $\square$

Dans le cas $K = \mathbb{C}$, on a $T_{G'}(\mathbb{C}) = T_{G'_0}(\mathbb{C}) \times T_{G'_1}(\mathbb{C}) \subset \mathbb{C}^d$ et l'application exponentielle de $G'(\mathbb{C}) = G'_0(\mathbb{C}) \times G'_1(\mathbb{C})$ est la restriction à ce sous-espace de l'application exponentielle de G :

$$\begin{array}{rccc} \exp_{G'} : & T_{G'}(\mathbb{C}) & \to & G'(\mathbb{C}) \\ & (z_1,\dots,z_d) & \mapsto & (z_1,\dots,z_{d_0}; e^{z_{d_0+1}},\dots,e^{z_d}) \end{array}$$

Dans $\mathbb{C}^d$, les espaces tangents aux sous-groupes algébriques de G définis sur un sous-corps k de $\mathbb{C}$ sont donc les produits $V_0 \times V_1$, où V_0 est un sous-espace vectoriel de $\mathbb{C}^{d_0}$ défini sur k, et V_1 est un sous-espace vectoriel de $\mathbb{C}^{d_1}$ défini sur $\mathbb{Q}$.

Si G'_0 est défini sur $\mathbb{R}$, alors $T_{G'}(\mathbb{R}) = T_{G'_0}(\mathbb{R}) \times T_{G'_1}(\mathbb{R}) \subset \mathbb{R}^d$ et

$$\begin{array}{rccc} \exp_{G',\mathbb{R}} : & T_{G'}(\mathbb{R}) & \to & G'(\mathbb{R}) \\ & (x_1,\dots,x_d) & \mapsto & (x_1,\dots,x_{d_0}; e^{x_{d_0+1}},\dots,e^{x_d}) \end{array}$$

b) *Le théorème du sous-groupe linéaire*

Soit $\mathcal{V}$ un sous-espace vectoriel de $\mathbb{C}^d$ sur $\mathbb{Q}$. On s'intéresse au $\mathbb{Q}$-espace vectoriel $\mathcal{V} \cap \mathcal{L}(G)$, où, rappelons-le, $G = G_0 \times G_1$, $G_0 = \mathbb{G}_\mathrm{a}^{d_0}$, $G_1 = \mathbb{G}_\mathrm{m}^{d_1}$ et

$$\mathcal{L}(G) = \exp_G^{-1}\big(G(\overline{\mathbb{Q}})\big) = \overline{\mathbb{Q}}^{d_0} \times \mathcal{L}^{d_1}.$$

Si $\mathcal{V} \cap \big(\overline{\mathbb{Q}}^{d_0} \times \{0\}^{d_1}\big) \neq \{0\}$, alors $\mathcal{V} \cap \mathcal{L}(G)$ est de dimension infinie sur $\mathbb{Q}$ car il contient $\mathcal{V} \cap \big(\overline{\mathbb{Q}}^{d_0} \times \{0\}^{d_1}\big)$ qui est un $\overline{\mathbb{Q}}$-espace vectoriel de dimension > 0. De même, si $\mathcal{V} \cap \big(\{0\}^{d_0} \times \mathbb{Q}^{d_1}\big) \neq \{0\}$, alors $\mathcal{V} \cap \mathcal{L}(G)$ contient λx pour tout $\lambda \in \mathcal{L}$ et tout $x \in \mathcal{V} \cap \big(\{0\}^{d_0} \times \mathbb{Q}^{d_1}\big)$, donc le $\mathbb{Q}$-espace vectoriel $\mathcal{V} \cap \mathcal{L}(G)$ est encore de dimension infinie.

Théorème 2.6* (théorème du sous-groupe linéaire). – *Soient d_0 et d_1 deux entiers ≥ 0 avec $d = d_0 + d_1$. Soit $\mathcal{V}$ un sous-espace vectoriel de $\mathbb{C}^d$ tel que*

$$\mathcal{V} \cap \big(\overline{\mathbb{Q}}^{d_0} \times \{0\}^{d_1}\big) = \{0\} \qquad \textit{et} \qquad \mathcal{V} \cap \big(\{0\}^{d_0} \times \mathbb{Q}^{d_1}\big) = \{0\}.$$

Alors le $\mathbb{Q}$-espace vectoriel $\mathcal{V} \cap \mathcal{L}(G)$ est de dimension finie majorée par

$$\dim_{\mathbb{Q}}\big(\mathcal{V} \cap \mathcal{L}(G)\big) \leq d_1(d-1).$$

Il est important de remarquer que *les conditions $\mathcal{V} \cap \big(\overline{\mathbb{Q}}^{d_0} \times \{0\}^{d_1}\big) = \{0\}$ et $\mathcal{V} \cap \big(\{0\}^{d_0} \times \mathbb{Q}^{d_1}\big) = \{0\}$ signifient que si G' est un sous-groupe algébrique de G défini sur $\overline{\mathbb{Q}}$ et de dimension > 0, alors le $\mathbb{C}$-espace vectoriel $T_{G'}(\mathbb{C})$ n'est pas contenu dans $\mathcal{V}$.* En effet, comme nous venons de le voir, un sous-espace vectoriel de $\mathbb{C}^d$ de la forme $T_{G'}(\mathbb{C})$ (avec G' sous-groupe algébrique de G défini sur $\overline{\mathbb{Q}}$) s'écrit $T_{G'_0}(\mathbb{C}) \times T_{G'_1}(\mathbb{C})$, avec $T_{G'_0}(\mathbb{C}) = W$ sous-espace vectoriel de $\mathbb{C}^{d_0}$ rationnel sur $\overline{\mathbb{Q}}$ et $G'_1 = \mathcal{T}_A$ pour un sous-groupe A de $\mathbb{Z}^{d_1}$. Si G' est de dimension positive, alors ou bien $W \neq \{0\}$, ou bien $A \neq \mathbb{Z}^{d_1}$. Dans le premier cas W contient un élément non nul de $\overline{\mathbb{Q}}^{d_0}$, et $T_{G'}(\mathbb{C})$ contient un élément non nul de $\overline{\mathbb{Q}}^{d_0} \times \{0\}^{d_1}$; dans le second cas $T_{G'_1}(\mathbb{C})$ contient un élément non nul de $\mathbb{Q}^{d_1}$, et $T_{G'}(\mathbb{C})$ contient un élément non nul de $\{0\}^{d_0} \times \mathbb{Q}^{d_1}$.

Fixons d nombres complexes $u_1,\dots,u_{d_0}, v_1,\dots,v_{d_1}$, non tous nuls. On s'intéresse aux solutions de l'équation

$$\beta_1 u_1 + \cdots + \beta_{d_0} u_{d_0} + \lambda_1 v_1 + \cdots + \lambda_{d_1} v_{d_1} = 0$$

où les inconnues sont $(\beta_1,\dots,\beta_{d_0};\lambda_1,\dots,\lambda_{d_1}) \in \mathbb{C}^d$ avec $\beta_h \in \overline{\mathbb{Q}}$, $(1 \leq h \leq d_0)$, et $e^{\lambda_i} \in \overline{\mathbb{Q}}^\times$ $(1 \leq i \leq d_1)$. Le théorème 2.6* dit que, *sauf cas triviaux*, l'espace des solutions est de dimension finie sur $\mathbb{Q}$. Les deux cas triviaux sont les suivants.

- S'il existe une solution non triviale pour laquelle $\lambda_1 = \cdots = \lambda_{d_1} = 0$:

$$\beta_1 u_1 + \cdots + \beta_{d_0} u_{d_0} = 0$$

  avec $0 \neq (\beta_1,\dots,\beta_{d_0}) \in \overline{\mathbb{Q}}^{d_0}$, alors pour tout $\beta \in \overline{\mathbb{Q}}$, $(\beta\beta_1,\dots,\beta\beta_{d_0};0,\dots,0)$ est une solution.
- S'il existe $0 \neq (b_1,\dots,b_{d_1}) \in \mathbb{Q}^{d_1}$ vérifiant

$$b_1 v_1 + \cdots + b_{d_1} v_{d_1} = 0,$$

  alors pour tout $\lambda \in \mathcal{L}$, $(0,\dots,0;\lambda b_1,\dots,\lambda b_{d_1})$ est une solution.

Exercice. Montrer que si $\mathcal{V}$ un sous-espace vectoriel de $\mathbb{C}^d$ tel que

$$\mathcal{V} \cap \big(\overline{\mathbb{Q}}^{d_0} \times \{0\}^{d_1}\big) = \{0\} \qquad \textit{et} \qquad \mathcal{V} \cap \big(\{0\}^{d_0} \times \mathbb{Q}^{d_1}\big) = \{0\},$$

alors il existe un hyperplan H de $\mathbb{C}^d$ contenant $\mathcal{V}$ tel que

$$H \cap \left(\overline{\mathbb{Q}}^{d_0} \times \{0\}^{d_1}\right) = \{0\} \qquad \text{et} \qquad H \cap \left(\{0\}^{d_0} \times \mathbb{Q}^{d_1}\right) = \{0\}.$$

En déduire que, dans le théorème 2.6, il n'y a pas de restriction à supposer que $\mathcal{V}$ est un hyperplan de $\mathbb{C}^d$.*

On déduit de ce théorème 2.6* de nombreux corollaires. Pour commencer, le théorème de Gelfond-Schneider est équivalent au cas particulier $d_0 = d_1 = 1$, $d = 2$ (c'est la forme $\boxed{5}$ du théorème 1.3*). Ensuite le théorème des six exponentielles équivaut au cas particulier $d_0 = 0$, $d_1 = d = 2$ (c'est la forme $\boxed{3}$ du théorème 1.7*). On peut aussi donner un corollaire du théorème 2.6* (correspondant au cas particulier $d_0 = 0$, $d_1 = d$) qui généralise la forme $\boxed{2}$ du théorème 1.7* :

Corollaire 2.7*. – *Soit M une matrice $d \times \ell$ à coefficients dans $\mathcal{L}$, avec $\ell > d(d-1)$. On suppose que les ℓ vecteurs colonnes de M sont linéairement indépendants sur $\mathbb{Q}$. Alors le $\mathbb{C}$-espace vectoriel engendré par les vecteurs colonnes de M dans $\mathbb{C}^d$ contient un élément non nul de $\mathbb{Q}^d$.*

Dans ce corollaire 2.7*, on ne peut pas remplacer l'hypothèse $\ell > d(d-1)$ par $\ell \geq d(d-1)/2$. Voici en effet un exemple d'hyperplan $\mathcal{V}$ dans $\mathbb{C}^d$ qui vérifie $\mathcal{V} \cap \mathbb{Q}^d = \{0\}$ et $\dim_{\mathbb{Q}}(\mathcal{V} \cap \mathcal{L}^d) \geq d(d-1)/2$: on choisit d éléments $\lambda_1, \ldots, \lambda_d$ dans $\mathcal{L}$, linéairement indépendants sur $\mathbb{Q}$, et on considère l'hyperplan d'équation

$$z_1\lambda_1 + \cdots + z_d\lambda_d = 0.$$

Comme $\lambda_1, \ldots, \lambda_d$ sont $\mathbb{Q}$-linéairement indépendants, on a $\mathcal{V} \cap \mathbb{Q}^d = \{0\}$. Pour $1 \leq i \leq d$ et $1 \leq j \leq d$ avec $i < j$, le point de coordonnées $(z_1, \ldots, z_d)$ avec

$$z_h = 0 \quad \text{pour } 1 \leq h \leq d,\ h \notin \{i,j\}, \qquad z_i = \lambda_j, \qquad z_j = -\lambda_i$$

appartient à cet hyperplan et aussi à $\mathcal{L}^d$; les $d(d-1)/2$ points ainsi obtenus sont linéairement indépendants sur $\mathbb{Q}$.

Noter que, pour minorer le rang d'une matrice à coefficients dans $\mathcal{L}$ par un entier ≥ 3, il n'est pas suffisant de supposer les lignes linéairement indépendantes sur $\mathbb{Q}$ et les colonnes linéairement indépendantes sur $\mathbb{Q}$: considérer par exemple les matrices de la forme

$$\begin{pmatrix} 0 & \lambda_2 & \ldots & \lambda_\ell \\ \lambda'_2 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \lambda'_d & 0 & \ldots & 0 \end{pmatrix}$$

qui sont de rang 2.

D'autres minorations de rangs de matrices à coefficients dans $\mathcal{L}$ sont connues ; voir en particulier [W 1983b], [W 1988], [R 1988b], [R 1992a].

Voici un autre cas particulier du théorème du sous-groupe linéaire.

Corollaire 2.8* (théorème de Baker homogène). – *Soient $\lambda_1, \ldots, \lambda_n$ des éléments de $\mathcal{L}$ qui sont linéairement indépendants sur le corps $\mathbb{Q}$ des nombres rationnels ; alors ces éléments sont linéairement indépendants sur le corps $\overline{\mathbb{Q}}$ des nombres algébriques.*

Démonstration du corollaire 2.8 comme conséquence du théorème 2.6*.*
On démontre 2.8* par récurrence sur n. Pour $n = 1$ le résultat est banal. Pour $n = 2$ il est équivalent au théorème de Gel'fond-Schneider (énoncé $\boxed{1}$ du théorème 1.3*), et nous avons vu que le théorème 1.3* était équivalent au cas $d_0 = d_1 = 1$, $d = 2$ du théorème 2.6*.

On suppose donc que $\lambda_1, \ldots, \lambda_{n+1}$ sont des éléments de $\mathcal{L}$ qui sont $\overline{\mathbb{Q}}$-linéairement dépendants. On suppose aussi, comme nous le permet l'hypothèse de récurrence, que $\lambda_1, \ldots, \lambda_n$ sont $\overline{\mathbb{Q}}$-linéairement indépendants. Il existe alors une unique relation de dépendance linéaire de la forme

$$\beta_1\lambda_1 + \cdots + \beta_n\lambda_n = \lambda_{n+1},$$

avec des nombres algébriques $\beta_1, \ldots, \beta_n$. On va utiliser le théorème 2.6* avec $d_0 = n$, $d_1 = 1$, $d = n+1$. Soit $\mathcal{V}$ l'hyperplan de $\mathbb{C}^{n+1}$ d'équation $z_{n+1} = \lambda_1 z_1 + \cdots + \lambda_n z_n$. Comme $\lambda_1, \ldots, \lambda_n$ sont $\overline{\mathbb{Q}}$-linéairement indépendants, on a $\mathcal{V} \cap (\overline{\mathbb{Q}}^n \times \{0\}) = \{0\}$. On a aussi trivialement $\mathcal{V} \cap (\{0\} \times \mathbb{Q}) = \{0\}$. Enfin $\mathcal{V}$ contient les $n+1$ vecteurs colonnes de la matrice

$$\begin{pmatrix} 1 & \cdots & 0 & \beta_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & \beta_n \\ \lambda_1 & \cdots & \lambda_n & \lambda_{n+1} \end{pmatrix}$$

Comme $d_1(d-1) = n$, le théorème 2.6* montre que ces vecteurs colonnes sont linéairement dépendants sur $\mathbb{Q}$, donc $\lambda_1, \ldots, \lambda_{n+1}$ sont linéairement dépendants sur $\mathbb{Q}$ et $\beta_1, \ldots, \beta_n$ sont tous rationnels. □

Remarque. L'énoncé 2.8* possède une version *non-homogène* :

Si des éléments $\lambda_1, \ldots, \lambda_n$ de $\mathcal{L}$ sont $\mathbb{Q}$-linéairement indépendants, alors les nombres $1, \lambda_1, \ldots, \lambda_n$ sont linéairement indépendants sur $\overline{\mathbb{Q}}$.

Ce théorème, dû à Baker, est une conséquence d'une version plus précise du théorème 2.6* :

Sous les hypothèses du théorème 2.6, si W est un sous-espace de $\mathbb{C}^d$, rationnel sur $\overline{\mathbb{Q}}$, de dimension t, contenu dans $\mathcal{V}$, alors*

$$\dim_{\mathbb{Q}}\bigl(\mathcal{V} \cap \mathcal{L}(G)\bigr) \leq d_1(d-t-1).$$

L'existence de W n'est pas une hypothèse restrictive : on retrouve le théorème 2.6* en prenant $W = 0$.

Démonstrations du théorème de Baker non homogène en utilisant la borne

$$\dim_{\mathbb{Q}}\bigl(\mathcal{V} \cap \mathcal{L}(G)\bigr) \leq d_1(d-t-1).$$

Première démonstration. On écrit une relation

$$\beta_1\lambda_1 + \cdots + \beta_n\lambda_n = \beta_{n+1},$$

avec des nombres algébriques $\beta_1, \ldots, \beta_{n+1}$ et des éléments $\lambda_1, \ldots, \lambda_n$ de $\mathcal{L}$ qui sont linéairement indépendants sur $\mathbb{Q}$ (donc sur $\overline{\mathbb{Q}}$, d'après le théorème homogène). On va utiliser le théorème 2.6* avec $d_0 = n$, $d_1 = 1$, $d = n+1$. Soit $\mathcal{V}$ l'hyperplan de $\mathbb{C}^{n+1}$ d'équation $z_{n+1} = \lambda_1 z_1 + \cdots + \lambda_n z_n$. On vérifie, exactement comme dans la démonstration du cas homogène, que l'on a $\mathcal{V} \cap (\overline{\mathbb{Q}}^n \times \{0\}) = \{0\}$ et $\mathcal{V} \cap (\{0\} \times \mathbb{Q}) = \{0\}$, et que $\mathcal{V}$ contient les n vecteurs colonnes de la matrice

$$\begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \\ \lambda_1 & \cdots & \lambda_n \end{pmatrix}$$

qui sont clairement linéairement indépendants sur $\mathbb{Q}$ (et même sur $\mathbb{C}$). Comme $d_1 = 1$ et $d = n+1$, le théorème 2.6* entraîne $t = 0$, c'est-à-dire $\mathcal{V} \cap \overline{\mathbb{Q}}^{n+1} = \{0\}$; or $(\beta_1, \ldots, \beta_{n+1})$ appartient à $\mathcal{V} \cap \overline{\mathbb{Q}}^{n+1}$. Donc $\beta_1 = \cdots = \beta_{n+1} = 0$.
Deuxième démonstration. On écrit une relation

$$\beta_0 + \beta_1\lambda_1 + \cdots + \beta_{n-1}\lambda_{n-1} = \lambda_n,$$

avec des nombres algébriques $\beta_0, \beta_1, \ldots, \beta_{n-1}$ et des éléments $\lambda_1, \ldots, \lambda_n$ de $\mathcal{L}$. Par récurrence sur n on peut supposer que les nombres $1, \beta_1, \ldots, \beta_{n-1}$ sont $\mathbb{Q}$-linéairement indépendants. On va utiliser le théorème 2.6* avec $d_0 = 1$, $d_1 = n$, $d = n+1$. Soit $\mathcal{V}$ l'hyperplan de $\mathbb{C}^{n+1}$ d'équation $z_n = z_0 + \beta_1 z_1 + \cdots + \beta_{n-1} z_{n-1}$. Comme les nombres β_i sont algébriques, on peut prendre $W = \mathcal{V}$ et $t = n$. On a trivialement $\mathcal{V} \cap (\overline{\mathbb{Q}} \times \{0\}) = \{0\}$; d'autre part, comme les nombres $1, \beta_1, \ldots, \beta_{n-1}$ sont linéairement indépendants sur $\mathbb{Q}$, on vérifie $\mathcal{V} \cap (\{0\} \times \mathbb{Q}^n) = \{0\}$. Le théorème 2.6* entraîne $\mathcal{V} \cap (\overline{\mathbb{Q}} \times \mathcal{L}^n) = \{0\}$; or $(\beta_0, \lambda_1 \ldots, \lambda_n)$ appartient à $\mathcal{V} \cap (\overline{\mathbb{Q}} \times \mathcal{L}^n)$. Donc $\beta_0 = \lambda_1 = \cdots = \lambda_n = 0$. □

Les énoncés de transcendance que nous venons de citer ne sont pas les plus généraux connus, même pour la fonction exponentielle usuelle : on sait minorer le rang de matrices de la forme

$$\begin{array}{cl} \begin{pmatrix} B_0 & B_1 \\ B_2 & M \end{pmatrix} & \begin{array}{l} \} \; d_0 \\ \} \; d_1 \end{array} \end{array},$$

où B_0, B_1, B_2 ont des coefficients algébriques, tandis que M a ses coefficients dans $\mathcal{L}$. Les vecteurs colonnes de $\begin{pmatrix} B_0 \\ B_2 \end{pmatrix}$ engendrent sur $\mathbb{C}$ un sous-espace vectoriel de $\mathbb{C}^d$ rationnel sur $\overline{\mathbb{Q}}$, tandis que les vecteurs colonnes de $\begin{pmatrix} B_1 \\ M \end{pmatrix}$ engendrent sur $\mathbb{Q}$ un sous-espace vectoriel de $\mathcal{L}(G)$. Quand le rang de la matrice est $< d$, tous ces vecteurs colonnes se trouvent dans un hyperplan de $\mathbb{C}^d$.

On trouvera dans les articles de Roy cités dans la bibliographie des résultats encore plus généraux concernant le rang de matrices dont les coefficients sont des combinaisons linéaires de logarithmes de nombres algébriques.

c) *Application au problème de densité*

On conserve les notations $G = \mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}$ et $K = \overline{\mathbb{Q}} \cap \mathbb{R}$. De plus on pose

$$\mathrm{m}_{\mathbb{R}}(G) = d+1 \qquad \text{et} \qquad \mathrm{m}'_{\mathbb{R}}(G) = d_1(d-1)+2.$$

Ainsi, avec la notation du chapitre II, §7, on a $\mathrm{m}_{\mathbb{R}}(G) = \mathrm{m}\big(G(\mathbb{R})\big)$. Le premier coefficient $\mathrm{m}_{\mathbb{R}}(G)$ nous sert à énoncer une condition nécessaire de densité, alors que le second donnera une condition suffisante.

Maintenant si Γ est dense dans $G(\mathbb{R})$, alors pour tout sous-groupe algébrique G' de G, $\Gamma/\Gamma \cap G'(\mathbb{R})$, qui est l'image de Γ dans le groupe des points réels du quotient G/G', est dense pour la topologie réelle dans $G(\mathbb{R})/G'(\mathbb{R})$.

Lemme 2.9. – *Soit Γ un sous-groupe dense de $G(\mathbb{R})^0 = \mathbb{R}^{d_0} \times (\mathbb{R}_+^\times)^{d_1}$. Soit G' un sous-groupe algébrique de $G = \mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}$ de dimension $< \dim G$. Alors $\Gamma/\Gamma \cap G'(\mathbb{R})$ est dense dans $\big((G/G')(\mathbb{R})\big)^0$. En particulier si Γ est de type fini, on a*

$$\mathrm{rang}_{\mathbb{Z}}(\Gamma/\Gamma \cap G'(\mathbb{R})) \geq \mathrm{m}_{\mathbb{R}}(G/G').$$

Noter que la condition écrite dans la conclusion entraîne, comme il se doit, $\mathrm{rang}_{\mathbb{Z}}\Gamma \geq \mathrm{m}_{\mathbb{R}}(G)$ (prendre $G' = \{0\}$).

Théorème 2.10. – *Soit Γ un sous-groupe de type fini de $G(\mathbb{R})^0 \cap G(K)$.*
a) Si

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

pour tout sous-groupe algébrique G' de G, défini sur K, de dimension $< \dim G$, alors $\Gamma \cap G(\mathbb{R})^0$ est dense dans $G(\mathbb{R})^0$.
b) Si

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

pour tout sous-groupe algébrique G' de G, défini sur K, de dimension $< \dim G$, alors Γ contient un sous-groupe de rang $\mathrm{m}_{\mathbb{R}}(G)$ qui est dense dans $G(\mathbb{R})^0$.

Démonstration. Soit ℓ le rang de Γ sur $\mathbb{Z}$; on définit

$$Y = \exp_{G,\mathbb{R}}^{-1}(\Gamma) \subset \mathbb{R}^d;$$

c'est un sous-groupe de type fini de $\mathbb{R}^d$ de rang ℓ, 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 $\mathbb{R}^d$, donc (proposition 4.3 du chapitre II) que pour tout hyperplan réel V de $\mathbb{R}^d$,

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

1) On commence par établir le résultat suivant :
supposons $\ell \geq \mathrm{m}'_{\mathbb{R}}(G)$; supposons aussi

$$V \cap \big(K^{d_0} \times \{0\}^{d_1}\big) = \{0\} \quad \textit{et} \quad V \cap \big(\{0\}^{d_0} \times \mathbb{Q}^{d_1}\big) = \{0\};$$

alors l'inégalité désirée $\operatorname{rang}_{\mathbb{Z}}\big(Y/Y\cap V\big)\geq 2$ *est bien vérifiée.*
On démontre cela en utilisant le théorème 2.6* ; on écrit une équation de l'hyperplan réel V dans $\mathbb{R}^d$ et on considère l'hyperplan complexe $\mathcal{V}$ de $\mathbb{C}^d$ défini par la même équation, de sorte que $V=\mathcal{V}\cap\mathbb{R}^d$. Les hypothèses sur V impliquent

$$\mathcal{V}\cap\big(\overline{\mathbb{Q}}^{d_0}\times\{0\}^{d_1}\big)=\{0\}\quad\text{et}\quad\mathcal{V}\cap\big(\{0\}^{d_0}\times\mathbb{Q}^{d_1}\big)=\{0\}.$$

Enfin, puisque $Y\cap V$ est contenu dans $\mathcal{L}(G)\cap\mathcal{V}$, on peut utiliser le théorème 2.6* :

$$\operatorname{rang}_{\mathbb{Z}}(Y\cap V)\leq\dim_{\mathbb{Q}}\big(\mathcal{V}\cap\mathcal{L}(G)\big)\leq d_1(d-1)=\mathrm{m}'_{\mathbb{R}}(G)-2;$$

on en déduit l'inégalité annoncée : $\operatorname{rang}_{\mathbb{Z}}\big(Y/Y\cap V\big)\geq 2$.
2) L'hypothèse que nous avons faite (dans la première partie de la démonstration) sur l'hyperplan réel V s'écrit : *il n'y a pas de sous-groupe algébrique de G, défini sur K, de dimension positive, dont l'espace tangent soit contenu dans V.* On ne fait plus cette hypothèse, mais on suppose

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

pour tout sous-groupe algébrique G' de G défini sur K avec $\dim G'<\dim G$. On considère le plus grand sous-groupe algébrique connexe G' de G, défini sur K, tel que $T_{G'}(\mathbb{R})$ soit contenu dans V. Il est défini de la manière suivante : $G'=G'_0\times G'_1$, où $G'_0(\mathbb{R})$ est le sous-espace vectoriel de $G_0(\mathbb{R})$ engendré par la projection sur $G_0(\mathbb{R})$ de $V\cap\big(K^{d_0}\times\{0\}^{d_1}\big)$, tandis que $G'_1(\mathbb{R})=\exp\big(T_{G'_1}(\mathbb{R})\big)$, où $T_{G'_1}(\mathbb{R})$ est le sous-espace vectoriel de $T_{G_1}(\mathbb{R})$ engendré par la projection sur $T_{G_1}(\mathbb{R})$ de $V\cap\big(\{0\}^{d_0}\times\mathbb{Q}^{d_1}\big)$. On vérifie que, dans l'espace tangent $T_{\widetilde{G}}(\mathbb{R})=T_{G/G'}(\mathbb{R})$ de $\widetilde{G}(\mathbb{R})=G(\mathbb{R})/G'(\mathbb{R})$, l'hyperplan $\widetilde{V}=V/T_{G'}(\mathbb{R})$ vérifie la condition suivante : *il n'y a pas de sous-groupe algébrique de $\widetilde{G}=G/G'$, défini sur K, de dimension positive, dont l'espace tangent soit contenu dans $\widetilde{V}$.*

On applique le résultat démontré en 1) au sous-groupe $\widetilde{Y}=Y/Y\cap T_{G'}(\mathbb{R})$ de $T_{\widetilde{G}}(\mathbb{R})$, dont l'image par $\exp_{\widetilde{G}}$ dans $\widetilde{G}(\mathbb{R})$ est $\widetilde{\Gamma}=\Gamma/\Gamma\cap G'(K)$:

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

On peut donc conclure :

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

3) Grâce au lemme 1.8, la partie *b)* du théorème 2.10 résulte maintenant de la partie *a)* et du théorème de Roy (théorème 7.2 du chapitre II) avec $R=G(\mathbb{R})^0$, $n=d$ et $\mathrm{m}(R)=\mathrm{m}_{\mathbb{R}}(G)$. □

Exercice. On considère un sous-espace vectoriel $\mathbb{L}$ de $\mathbb{R}$ sur $\mathbb{Q}$ et on note $\mathcal{Q}$ son image par l'application exponentielle :

$$\mathcal{Q}=\exp\mathbb{L}=\big\{e^{\lambda};\ \lambda\in\mathbb{L}\big\}\subset\mathbb{R}_+^\times.$$

Soit $\theta:\mathbb{N}\to\mathbb{N}$ une application. On suppose que pour tout entier $d\geq 1$ et pour tout hyperplan V de $\mathbb{R}^d$ satisfaisant $V\cap\mathbb{Q}^d=\{0\}$, on a

$$\dim_{\mathbb{Q}}(V\cap\mathbb{L}^d)\leq\theta(d).$$

Soient d un entier positif, G le groupe algébrique $\mathbb{G}_{\mathrm{m}}^d$, et Γ un sous-groupe de type fini de $\mathcal{Q}^d$.
a) On suppose que, pour tout sous-groupe algébrique G' de G de dimension $<d$, on a

$$\operatorname{rang}_{\mathbb{Z}}\big(\Gamma/\Gamma\cap G'(\mathbb{R})\big)\geq\theta(\delta)+2,$$

où δ est la dimension de G/G'. Alors Γ est dense dans $(\mathbb{R}_+^\times)^d$.
b) On suppose que, pour tout sous-groupe algébrique G' de G de dimension $<d$, on a

$$\operatorname{rang}_{\mathbb{Z}}\big(\Gamma/\Gamma\cap G'(\mathbb{R})\big)\geq\theta(\delta)+d+1,$$

où δ est la dimension de G/G'. Alors Γ contient un sous-groupe de rang $d+1$ qui est dense dans $(\mathbb{R}_+^\times)^d$.

Corollaire 2.11. – *Soient $d_0\geq 0$, $d_1\geq 1$ et $\ell\geq 1$ des entiers, α_{ij}, $(1\leq i\leq d_1,\ 1\leq j\leq\ell)$ des nombres algébriques réels positifs multiplicativement indépendants et β_{hj}, $(1\leq h\leq d_0,\ 1\leq j\leq\ell)$ des nombres algébriques réels. On définit $\gamma_1,\dots,\gamma_\ell$ dans $K^{d_0}\times(K_+^\times)^{d_1}$ par*

$$\gamma_j=(\beta_{1j},\dots,\beta_{d_0j};\alpha_{1j},\dots,\alpha_{d_1j}),\qquad(1\leq j\leq\ell),$$

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 $\beta_1,\dots,\beta_\ell$, avec

$$\beta_j=(\beta_{1j},\dots,\beta_{d_0j}),\qquad(1\leq j\leq\ell).$$

Enfin on pose $d=d_0+d_1$.
a) On suppose que Γ_0 est dense dans $\mathbb{R}^{d_0}$. Si $\ell\geq d_1(d-1)+2$, 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 $\ell\geq d_1(d-1)+d+1$, alors Γ contient un sous-groupe de rang $d+1$ dense dans $\mathbb{R}^{d_0}\times(\mathbb{R}_+^\times)^{d_1}$.

Démonstration du corollaire 2.11. L'hypothèse que les $d_1\ell$ 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',

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

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

$$\operatorname{rang}_{\mathbb{Z}}\big(\Gamma_0/\Gamma_0 \cap G'_0(K)\big) \geq \mathrm{m}_{\mathbb{R}}(G_0/G'_0);$$

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

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

est donc bien vérifiée pour tous les sous-groupes algébriques G' de G avec $\dim G' < \dim G$ pour lesquels $\Gamma \cap G'(K) \neq \{0\}$; pour les autres, c'est-à-dire quand $\Gamma \cap G'(K) = \{0\}$, on a

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

Pour démontrer la partie *b)* du corollaire 2.11, on utilise l'hypothèse

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

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

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

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

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

donc on peut appliquer la partie *b)* du théorème 2.10.

Remarque. On déduit aussi du corollaire 2.11 le cas *réel* du théorème de Baker homogène, c'est-à-dire l'énoncé suivant :

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 $\overline{\mathbb{Q}}$.

Pour déduire cet énoncé du corollaire 2.11, on considère une éventuelle relation de dépendance linéaire de longueur minimale ; il s'agit de vérifier :

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 2.11 avec $d_0 = n$, $d_1 = 1$, $\ell = n + 2$, au sous-groupe de $\mathbb{R}^n \times \mathbb{R}_+^{\times}$ engendré par les $n+2$ points

$$(\delta_{1j}, \ldots, \delta_{nj}; \log \alpha_j), \qquad (1 \leq j \leq n),$$

$$(\beta_1, \ldots, \beta_n; \log \alpha_{n+1}) \quad \text{et} \quad (0, \ldots, 0; \log \alpha_0).$$

§3. Indépendance algébrique de logarithmes et densité

Nous poursuivons l'étude, commencée dans le paragraphe 2, de la densité dans $G(\mathbb{R}) = \mathbb{R}^{d_0} \times (\mathbb{R}^{\times})^{d_1}$ d'un sous-groupe de type fini de $G(K) = K^{d_0} \times (K^{\times})^{d_1}$, où $K = \overline{\mathbb{Q}} \cap \mathbb{R}$ est le corps des nombres algébriques réels. Nous étudions maintenant la situation d'un point de vue conjectural.

Les cas particuliers étudiés au paragraphe 1 pourraient laisser espérer que le coefficient $\mathrm{m}'_{\mathbb{R}}$ dans le théorème 2.10 pourrait être remplacé par $\mathrm{m}_{\mathbb{R}}$. Nous montrons pour commencer qu'il n'en est rien. Nous énonçons ensuite la principale conjecture concernant les logarithmes de nombres algébriques, puis nous montrons comment elle permet de donner une réponse complète (mais conjecturale !) au problème de densité pour les groupes algébriques linéaires.

a) *Un contre-exemple*

`Question :` *Un sous-groupe de type fini Γ de $G(K) \cap G(\mathbb{R})^0$, dont la projection sur tout quotient $(G/G')(K)$, avec G' sous-groupe algébrique de G défini sur K de dimension $< \dim G$, vérifie*

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

est-il alors dense dans $G(\mathbb{R})^0$?

Cela voudrait dire qu'un sous-groupe de type fini Γ de $G(K) \cap G(\mathbb{R})^0$ de rang $\geq \mathrm{m}_{\mathbb{R}}(G)$, est dense dans $G(\mathbb{R})^0$ si et seulement si pour tout sous-groupe algébrique G' de G, défini sur K, vérifiant $0 < \dim G' < \dim G$, $\Gamma/\Gamma \cap G'(K)$ est dense dans $(G/G')(\mathbb{R})^0$.

La réponse est positive pour $d_1 = 0$, d'après la proposition 4.3 du chapitre II. L'étude que nous avons faite au paragraphe 1 montre que, si la conjecture des quatre exponentielles est vraie, alors la réponse est encore positive pour $d = 2$.

Exercice. En utilisant le théorème 2.10, montrer que la réponse est positive quand $d_1 = 1$, $d_0 \geq 0$.

Nous allons montrer que la réponse est négative pour $\mathbb{G}_{\mathrm{m}}^3$. Nous indiquerons ensuite comment étendre ce contre-exemple aux groupes $\mathbb{G}_{\mathrm{m}}^d$, $d \geq 3$.

Le point de départ est la remarque suivante (déjà faite après l'énoncé du corollaire 2.7*) : quand $\alpha_1, \alpha_2, \alpha_3$ désignent trois nombres algébriques réels positifs multiplicativement indépendants, l'hyperplan de $\mathbb{R}^3$ d'équation

$$x_1 \log \alpha_1 + x_2 \log \alpha_2 + x_3 \log \alpha_3 = 0$$

contient trois éléments de $\mathcal{L}^3$ linéairement indépendants sur $\mathbb{Q}$, à savoir les trois vecteurs colonnes de la matrice antisymétrique

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

(voir à ce propos la remarque de M. Langevin citée dans [W 1983b], p. 1014 ; comparer aussi avec le théorème 6 de [R 1992a]).

Considérons maintenant six nombres réels algébriques positifs multiplicativement indépendants $\alpha_1, \alpha_2, \alpha_3,\ \beta_1, \beta_2, \beta_3$, et posons

$$\gamma_0 = (\beta_1, \beta_2, \beta_3), \quad \gamma_1 = (1, \alpha_3, 1/\alpha_2), \quad \gamma_2 = (1/\alpha_3, 1, \alpha_1), \quad \gamma_3 = (\alpha_2, 1/\alpha_1, 1).$$

Soit Γ le sous-groupe de $(K_+^\times)^3$ de rang 4 engendré par $\gamma_0, \gamma_1, \gamma_2, \gamma_3$. Nous allons montrer : *Γ n'est pas dense dans $(\mathbb{R}_+^\times)^3$, mais pour tout sous-groupe algébrique G' de G de dimension 1 ou 2, $\Gamma/\Gamma \cap G'(K)$ est dense dans $(G/G')(\mathbb{R})^0$.* En particulier cela implique que, pour tout sous-groupe algébrique G' de G tel que $\dim G' < \dim G$, on a

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

Passons aux logarithmes : on définit un sous-groupe $Y = \mathbb{Z}y_0 + \mathbb{Z}y_1 + \mathbb{Z}y_2 + \mathbb{Z}y_3 = \exp_G^{-1}(\Gamma)$ en posant

$$y_0 = (\log\beta_1, \log\beta_2, \log\beta_3), \quad y_1 = (0, \log\alpha_3, -\log\alpha_2),$$

$$y_2 = (-\log\alpha_3, 0, \log\alpha_1), \quad y_3 = (\log\alpha_2, -\log\alpha_1, 0).$$

Il s'agit de vérifier : *Y n'est pas dense dans $\mathbb{R}^3$, mais pour tout sous-espace vectoriel V de $\mathbb{R}^3$, rationnel sur $\mathbb{Q}$, de dimension 1 ou 2, $Y/Y \cap V$ est dense dans $\mathbb{R}^3/V$.*

Le fait que Y n'est pas dense dans $\mathbb{R}^3$ est facile : la forme linéaire $\varphi : \mathbb{R}^3 \to \mathbb{R}$ qui envoie (x_1, x_2, x_3) sur $x_1\log\alpha_1 + x_2\log\alpha_2 + x_3\log\alpha_3$ n'est pas nulle, et $\varphi(Y) \subset \mathbb{Z}\varphi(y_0)$.

Nous allons maintenant vérifier que, pour tout hyperplan V de $\mathbb{R}^3$, rationnel sur $\mathbb{Q}$, on a

$$\operatorname{rang}_{\mathbb{Z}}(Y \cap V) = 1.$$

En effet, si $b_1z_1 + b_2z_2 + b_3z_3 = 0$ est une équation de V avec $(b_1, b_2, b_3) \in \mathbb{Q}^3 \setminus \{0\}$, alors un élément $s_0y_0 + s_1y_1 + s_2y_2 + s_3y_3$ de Y, avec $(s_0, s_1, s_2, s_3) \in \mathbb{Z}^4$, appartient à l'hyperplan V si et seulement si

$$b_1\bigl(s_0\log\beta_1 - s_2\log\alpha_3 + s_3\log\alpha_2\bigr) + b_2\bigl(s_0\log\beta_2 - s_3\log\alpha_1 + s_1\log\alpha_3\bigr) + b_3\bigl(s_0\log\beta_3 - s_1\log\alpha_2 + s_2\log\alpha_1\bigr) = 0.$$

De l'indépendance linéaire des six nombres $\log\alpha_1, \log\alpha_2, \log\alpha_3,\ \log\beta_1, \log\beta_2, \log\beta_3$ on déduit $s_0 = 0$ et

$$\begin{pmatrix} 0 & -b_3 & b_2 \\ b_3 & 0 & -b_1 \\ -b_2 & b_1 & 0 \end{pmatrix}\begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Comme la matrice $\begin{pmatrix} 0 & -b_3 & b_2 \\ b_3 & 0 & -b_1 \\ -b_2 & b_1 & 0 \end{pmatrix}$ est de rang 2, l'espace des solutions $(s_0, s_1, s_2, s_3) \in \mathbb{Q}^4$ du système d'équations est de dimension 1 sur $\mathbb{Q}$, engendré par $(0, b_1, b_2, b_3)$, ce qui démontre bien $\operatorname{rang}_{\mathbb{Z}}(Y \cap V) = 1$ quand V est un hyperplan rationnel sur $\mathbb{Q}$ dans $\mathbb{R}^3$. De plus on obtient aussi $Y \cap D = \{0\}$ quand D est une droite de $\mathbb{R}^3$ rationnelle sur $\mathbb{Q}$ (écrire D comme intersection de deux hyperplans rationnels sur $\mathbb{Q}$).

On a donc $\operatorname{rang}_{\mathbb{Z}}(Y/Y \cap V) = 3$ pour tout hyperplan de $\mathbb{R}^3$ rationnel sur $\mathbb{Q}$, et par conséquent $Y/Y \cap V$ est dense dans $\mathbb{R}^3/V$ (qui est isomorphe à $\mathbb{R}$). D'autre part si D est une droite de $\mathbb{R}^3$ rationnelle sur $\mathbb{Q}$, alors $Y/Y \cap D$ est de rang 4 dans $\mathbb{R}^3/D$ (qui est isomorphe à $\mathbb{R}^2$) ; un hyperplan de $\mathbb{R}^3/D$, rationnel sur $\mathbb{Q}$, s'écrit V/D, où V est un hyperplan de $\mathbb{R}^3$, rationnel sur $\mathbb{Q}$, qui contient D ; alors la projection de $Y/Y \cap D$ sur $(\mathbb{R}^3/D)/(V/D) = \mathbb{R}^3/V$ n'est autre que $Y/Y \cap V$, qui est de rang 3. On peut donc appliquer la partie a) de la proposition 1.6 pour conclure que $Y/Y \cap D$ est dense dans $\mathbb{R}^3/D$.

Cette construction se généralise à $\mathbb{R}^d$ de la manière suivante. Prenons $2d$ nombres algébriques réels positifs multiplicativement indépendants $\alpha_1, \ldots, \alpha_d, \beta_1, \ldots, \beta_d$, et considérons le sous-groupe Γ de $(\mathbb{R}_+^\times)^d$ engendré par les $d(d-1)/2 + 1$ points

$$\gamma_{ij} = \bigl(\alpha_j^{\delta_{hi}}\alpha_i^{-\delta_{hj}}\bigr)_{1 \leq h \leq d} = (1, \ldots, 1, \alpha_j, 1, \ldots, 1, \alpha_i^{-1}, 1, \ldots, 1), \qquad (1 \leq i < j \leq d),$$

et

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

Lemme 3.1. — *Pour tout sous-groupe algébrique G' de $\mathbb{G}_{\mathrm{m}}^d$ de codimension $\delta > 0$, on a*

$$\operatorname{rang}_{\mathbb{Z}}\bigl(\Gamma/\Gamma \cap G'(\mathbb{R})\bigr) \geq \delta d + 1 - \frac{1}{2}\delta(\delta+1);$$

mais Γ n'est pas dense dans $(\mathbb{R}_+^\times)^d$.

Ainsi, pour $1 \leq \delta \leq d$, le sous-groupe G' de G défini par les équations $z_1 = \cdots = z_\delta = 1$ est de codimension δ, et il contient γ_{ij} pour $\delta < i < j \leq d$, donc

$$\operatorname{rang}_{\mathbb{Z}}\bigl(\Gamma \cap G'(\mathbb{R})\bigr) \geq \frac{1}{2}(d-\delta)(d-\delta-1)$$

et

$$\operatorname{rang}_{\mathbb{Z}}\bigl(\Gamma/\Gamma \cap G'(\mathbb{R})\bigr) \leq \frac{1}{2}d(d-1) + 1 - \frac{1}{2}(d-\delta)(d-\delta-1) = \delta d + 1 - \frac{1}{2}\delta(\delta+1).$$

Démonstration. L'espace tangent à l'origine $T_{G'}(\mathbb{R})$ de G' est un sous-espace de $T_G(\mathbb{R}) = \mathbb{R}^d$ rationnel sur $\mathbb{Q}$, de codimension δ ; on écrit des équations de ce sous-espace :

$$\sum_{h=1}^d b_h^{(k)} z_h = 0, \qquad (1 \leq k \leq \delta),$$

avec $b^{(1)}, \dots, b^{(\delta)}$ linéairement indépendants dans $\mathbb{Z}^d$,

$$b^{(k)} = \big(b_1^{(k)}, \dots, b_d^{(k)}\big) \in \mathbb{Z}^d, \qquad (1 \le k \le \delta).$$

Soit

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

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

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

et

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

On a

$$\operatorname{rang}_{\mathbb{Z}}\big(\Gamma/\Gamma \cap G'(\mathbb{R})\big) = \operatorname{rang}_{\mathbb{Z}}\big(Y/Y \cap T_{G'}(\mathbb{R})\big).$$

Un élément

$$\sum_{1 \le i < j \le d} s_{ij} y_{ij} + s_0 y_0$$

de Y appartient à $T_{G'}(\mathbb{R})$ si et seulement si l'élément $s = (s_{ij}, s_0)$ de $\mathbb{Z}^{d(d-1)/2+1}$ vérifie

$$\sum_{h=1}^{d} b_h^{(k)} \left(\sum_{1 \le i < j \le d} s_{ij} (\delta_{hi} \log \alpha_j - \delta_{hj} \log \alpha_i) + s_0 \log \beta_h \right) = 0 \qquad \text{pour} \quad 1 \le k \le \delta.$$

L'hypothèse d'indépendance linéaire des nombres $\log \alpha_1, \dots, \log \alpha_d$, $\log \beta_1, \dots, \log \beta_d$ permet d'écrire ces conditions

$$s_0 = 0 \quad \text{et} \quad \sum_{i=1}^{h-1} s_{ih} b_i^{(k)} - \sum_{j=h+1}^{d} s_{hj} b_j^{(k)} = 0 \qquad \text{pour } 1 \le h \le d \text{ et } 1 \le k \le \delta.$$

Par conséquent le rang sur $\mathbb{Z}$ de $Y/Y \cap T_{G'}(\mathbb{R})$ est égal au rang du système de $\delta d + 1$ formes linéaires

$$L_0 = X_0, \quad L_{hk} = \sum_{i=1}^{h-1} X_{ih} b_i^{(k)} - \sum_{j=h+1}^{d} X_{hj} b_j^{(k)}, \qquad (1 \le h \le d,\ 1 \le k \le \delta)$$

en les indéterminées X_0, X_{ij}, $(1 \le i < j \le d)$.

Pour h et k entiers vérifiant $1 \le h \le d$ et $1 \le k \le \delta$, et pour i et j entiers vérifiant $1 \le i < j \le d$, le coefficient $c_{ij}^{(hk)}$ de X_{ij} dans $L_{h,k}$ est

$$c_{ij}^{(hk)} = \begin{cases} -b_j^{(k)} & \text{si } h = i \\ b_i^{(k)} & \text{si } h = j \\ 0 & \text{sinon.} \end{cases}$$

On a supposé que les éléments $b^{(1)}, \dots, b^{(\delta)}$ étaient linéairement indépendants. Quitte à changer de système générateur du $\mathbb{Z}$-module engendré par $b^{(1)}, \dots, b^{(\delta)}$, on peut se ramener au cas où

$$b_i^{(k)} = 0 \quad \text{pour } 1 \le i < k \le \delta \text{ et } b_k^{(k)} \ne 0 \quad \text{pour } 1 \le k \le \delta.$$

Alors $c_{ij}^{(hk)}$ est nul pour $1 \le i < k < h$, tandis que pour $1 \le i = k < h$, il vaut $b_k^{(k)} \delta_{hj}$. La matrice des $c_{ij}^{(hk)}$ avec $1 \le k < h \le d$ et $k \le \delta$ d'une part, $1 \le i < j \le d$ et $i \le \delta$ d'autre part, est triangulaire, avec pour diagonale

$$\big(b_1^{(1)}, \dots, b_1^{(1)}, \dots, b_\delta^{(\delta)}, \dots, b_\delta^{(\delta)}\big);$$

cette matrice est donc inversible, de rang

$$(d-1) + (d-2) + \cdots + (d-\delta) = d\delta - \frac{\delta(\delta+1)}{2}.$$

Il reste à vérifier que Γ n'est pas dense dans $(\mathbb{R}_+^\times)^d$, ce qui revient à dire que Y n'est pas dense dans $\mathbb{R}^d$; il suffit d'exhiber une forme linéaire non nulle $\varphi : \mathbb{R}^d \to \mathbb{R}$ telle que $\operatorname{rang}_{\mathbb{Z}} \varphi(Y) \le 1$. On prend pour cela

$$\varphi(x_1, \dots, x_d) = x_1 \log \alpha_1 + \cdots + x_d \log \alpha_d,$$

de sorte que $\varphi(Y) \subset \mathbb{Z}\varphi(y_0)$. $\square$

On remarquera que, pour $d \ge 3$ et $1 \le \delta \le d$, on a $d\delta \ge \delta + (1/2)\delta(\delta+1)$, donc

$$\delta d + 1 - \frac{1}{2}\delta(\delta+1) \ge \delta + 1 = \mathrm{m}_{\mathbb{R}}(G/G').$$

Par conséquent pour chaque entier $d \ge 3$ on trouve un contre-exemple à la réciproque du lemme 2.9 pour $\mathbb{G}_{\mathrm{m}}^d$.

Exercice. Soit d un entier ≥ 3 et soit $G = \mathbb{G}_{\mathrm{m}}^d$. Montrer qu'il existe un sous-groupe de type fini de $G(K) = (K_+^\times)^d$, de rang $\ge \mathrm{m}_{\mathbb{R}}(G)$, dont la projection sur tout quotient $(G/G')(K)$, avec G' sous-groupe algébrique de G vérifiant $0 < \dim G' < \dim G$, a une image dense dans $(G/G')(\mathbb{R})^0$, mais qui n'est pas dense dans $G(\mathbb{R})^0$.

`Indication.` Avec les notations du lemme 3.1, prendre un sous-groupe algébrique de dimension maximale G' de G, $\dim G' < \dim G$, tel que $\widetilde{\Gamma} = \Gamma/\Gamma \cap G'(\mathbb{R})$ ne soit pas dense dans $\widetilde{G}(\mathbb{R})$, où $\widetilde{G}$ désigne le quotient G/G'. Vérifier $\operatorname{rang}_{\mathbb{Z}}(\widetilde{\Gamma}) \ge \mathrm{m}_{\mathbb{R}}(\widetilde{G})$, et montrer que les projections de $\widetilde{\Gamma}$ sur les quotients de $\widetilde{G}$ (distincts de $\{0\}$ et de $\widetilde{G}$) sont denses dans les points réels.

Etant donné que, pour $1 \le \delta \le d$, on a

$$\delta d - \frac{1}{2}\delta(\delta+1) \ge \frac{1}{2}\delta(\delta-1),$$

le groupe Γ que nous venons de construire satisfait

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

le théorème 2.10 montre qu'il n'y a pas d'exemple où le coefficient 1/2 soit remplacé par 1 : *si un sous-groupe Γ de $(K_+^\times)^d$ vérifie*

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

pour tout sous-groupe algébrique G' de $\mathbb{G}_{\mathrm{m}}^d$ de codimension $\delta\geq 1$, alors Γ est dense dans $(\mathbb{R}_+^\times)^d$.

Exercice. Montrer que la conjecture $3.3^?$ ci-dessous entraîne la même conclusion sous l'hypothèse

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

`Indication.` Voir le corollaire 2 p.278 de [R 1988b].

b) *La conjecture d'indépendance algébrique*

La principale conjecture dans ce domaine est la suivante (voir [Si 1949], p.84, fin du chapitre III ; [G 1952], p.177, fin du chapitre III ; [L 1966], p.31, fin du chapitre III) :

Conjecture $3.2^?$ (conjecture d'indépendance algébrique). – *Soient $\lambda_1,\ldots,\lambda_n$ des éléments de $\mathcal{L}$ qui 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 !

Exercice. La conjecture $3.2^?$ implique trivialement les deux résultats suivants :
a) Si $\lambda_1,\lambda_2,\lambda_3,\lambda_4$ sont quatre éléments de $\mathcal{L}$ linéairement indépendants sur $\mathbb{Q}$, alors $\lambda_1\lambda_2\neq\lambda_3\lambda_4$.
b) Si $\lambda_1,\lambda_2,\lambda_3$ sont trois éléments de $\mathcal{L}$ linéairement indépendants sur $\mathbb{Q}$, alors $\lambda_1\lambda_2\neq\lambda_3^2$.
Vérifier que ces deux énoncés a) et b) sont aussi conséquences de la conjecture des quatre exponentielles $1.5^?$. Démontrer ensuite la réciproque : les deux énoncés a) et b) impliquent la conjecture des quatre exponentielles $1.5^?$.
`Indication.` On pourra utiliser l'identité

$$(aX+bY+cZ)X-YZ=(a+bc)X^2-(Y-cX)(Z-bX).$$

Exercice. `(D'après D. Roy).` *Montrer que la conjecture $3.2^?$ est équivalente à l'énoncé suivant :*
Soient n un entier positif, X une sous-variété algébrique affine de $\mathbb{C}^n$ définie sur $\overline{\mathbb{Q}}$, P un point de X dont les coordonnnées sont dans $\mathcal{L}$ et V le plus petit sous-espace vectoriel de $\mathbb{C}^n$ rationnel sur $\mathbb{Q}$ qui contient P. Alors V est contenu dans X.

Nous utiliserons le cas particulier suivant de la conjecture d'indépendance algébrique :

Conjecture $3.3^?$ (conjecture d'indépendance algébrique homogène réelle). – *Soient $\alpha_1,\ldots,\alpha_n$ des nombres algébriques réels positifs multiplicativement indépendants. Si $P\in\mathbb{Z}[X_1,\ldots,X_n]$ est un polynôme* homogène *non nul, alors le nombre $P(\log\alpha_1,\ldots,\log\alpha_n)$ n'est pas nul.*

c) *Application au problème de densité*

Soient ℓ, d_0 et d_1 des entiers ≥ 0 avec $\ell>0$ et $d=d_0+d_1>0$, α_{ij} et β_{hj} des nombres algébriques réels, $(1\leq h\leq d_0,\ 1\leq i\leq d_1,\ 1\leq j\leq\ell)$, avec $\alpha_{ij}>0$ pour tout (i,j) ; on définit $\gamma_1,\ldots,\gamma_\ell$ dans $K^{d_0}\times(K_+^\times)^d$ par

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

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

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

On choisit une base $(\theta_1,\ldots,\theta_r)$ dans $K_+^\times$ du sous-groupe multiplicatif engendré par les $d_1\ell$ nombres α_{ij} et on écrit

$$\alpha_{ij}=\prod_{\rho=1}^r\theta_\rho^{b_{ij\rho}},\qquad(1\leq i\leq d_1,\quad 1\leq j\leq\ell),$$

avec des $b_{ij\rho}$ dans $\mathbb{Z}$.

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

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

Lemme 3.4. – *Si la conjecture $3.3^?$ 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 $\eta_1,\ldots,\eta_\ell$, avec

$$\eta_j=\left(\beta_{1j},\ldots,\beta_{d_0j};\prod_{\rho=1}^r x_\rho^{b_{1j\rho}},\cdots,\prod_{\rho=1}^r x_\rho^{b_{d_1j\rho}}\right),\qquad(1\leq j\leq\ell),$$

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

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

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 $G = \mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}$ sur $\mathbb{R}$:

$$\exp_{G,\mathbb{R}} : (u_1, \ldots, u_{d_0}; v_1, \ldots, v_{d_1}) \longmapsto (u_1, \ldots, u_{d_0}; e^{v_1}, \ldots, e^{v_{d_1}})$$

établit un isomorphisme de groupes topologiques entre $\mathbb{R}^d$ et $\mathbb{R}^{d_0} \times (\mathbb{R}_+^\times)^{d_1}$. L'implication (i) $\Rightarrow$ (iii) (resp. $(ii) \Rightarrow (iv)$) est banale : on prend $x_\varrho = \theta_\varrho$ (resp. $\xi_\varrho = \log\theta_\varrho$) pour $1 \le \varrho \le r$. 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 $z_1, \ldots, z_t$ de $Y \cap \operatorname{Ker} \varphi$:

$$z_\tau = (z_{\tau 1}, \cdots, z_{\tau d}) = \sum_{j=1}^{\ell} s_j^{(\tau)} y_j, \qquad (1 \le \tau \le t),$$

avec des $s_j^{(\tau)}$ dans $\mathbb{Z}$, et

$$t = \operatorname{rang}_{\mathbb{Z}}(Y \cap \operatorname{Ker} \varphi) = \operatorname{rang}_{\mathbb{Z}} Y - \operatorname{rang}_{\mathbb{Z}} \varphi(Y) \ge \operatorname{rang}_{\mathbb{Z}} Y - 1.$$

Comme $\varphi(z_\tau) = 0$, la matrice $\bigl(z_{\tau i}\bigr)_{1 \le \tau \le t; 1 \le i \le d}$ a un rang $< d$. On écrit les coefficients de cette matrice : pour $1 \le \tau \le t$ et $1 \le i \le d$,

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

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 $3.3^?$ que l'on admet), si $\xi_1, \ldots, \xi_r$ sont des nombres réels et si on pose

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

la matrice $\bigl(\zeta_{\tau i}\bigr)_{1 \le \tau \le t; 1 \le i \le d}$ a encore un rang $< d$. En renversant l'argument, on déduit que le sous-groupe de $\mathbb{R}^d$ engendré par

$$\left(\beta_{1j}, \ldots, \beta_{d_0 j}; \sum_{\rho=1}^{r} b_{1j\rho}\xi_\rho, \cdots, \sum_{\rho=1}^{r} b_{d_1 j\rho}\xi_\rho\right), \qquad (1 \le j \le \ell),$$

n'est pas dense et l'assertion (iv) n'est pas satisfaite. □

Exercice. On admet la conjecture $3.3^?$. Soient α_0, α_1, β_0, β_1 des nombres algébriques réels positifs. On pose

$$\Gamma = \bigl\{(\alpha_0^k \alpha_1^m, \beta_0^\ell \beta_1^m)\,;\,(k, \ell, m) \in \mathbb{Z}^3\bigr\} \subset (\mathbb{R}_+^\times)^2.$$

a) On suppose que α_0 et β_0 sont multiplicativement dépendants. Montrer que Γ est dense dans $(\mathbb{R}_+^\times)^2$ si et seulement si les trois nombres $\alpha_0, \alpha_1, \beta_1$ sont multiplicativement indépendants.
b) On suppose que α_0 et β_0 sont multiplicativement indépendants. Montrer que les deux conditions suivantes sont équivalentes
(i) Γ est dense dans $(\mathbb{R}_+^\times)^2$.
(ii) Les deux nombres α_0, α_1 sont multiplicativement indépendants, et les deux nombres β_0, β_1 sont multiplicativement indépendants.

Le lemme 3.4 suggère une condition nécessaire et suffisante (conjecturale) pour qu'un sous-groupe de type fini de $G(K) \cap G(\mathbb{R})^0 = K^{d_0} \times (K_+^\times)^{d_1}$ soit dense dans $G(\mathbb{R})^0 = \mathbb{R}^{d_0} \times (\mathbb{R}_+^\times)^{d_1}$.

Conjecture $3.5^?$ (conjecture de densité pour les groupes algébriques linéaires commutatifs). – *Soient Γ un sous-groupe de type fini de $G(K) \cap G(\mathbb{R})^0$ de rang ℓ ; soient $\gamma_1, \ldots, \gamma_\ell$ des éléments de Γ linéairement indépendants sur $\mathbb{Z}$. On désigne par H l'adhérence de Zariski de $\mathbb{Z}(\gamma_1, \ldots, \gamma_\ell)$ dans G^ℓ. Alors Γ est dense dans $G(\mathbb{R})^0$ si et seulement s'il existe $(\eta_1, \ldots, \eta_\ell) \in H(\mathbb{R})$ tel que le sous-groupe $\mathbb{Z}\eta_1 + \cdots + \mathbb{Z}\eta_\ell$ soit dense dans $G(\mathbb{R})^0$.*

Du lemme 3.4 nous allons déduire :

Lemme 3.6. – *La conjecture $3.5^?$ est équivalente à la conjecture $3.3^?$.*

Démonstration.
Conjecture $3.3^?$ $\Rightarrow$ Conjecture $3.5^?$
Si H est l'adhérence de Zariski du sous-groupe $\mathbb{Z}(\gamma_1, \ldots, \gamma_\ell)$ de $(\mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1})^\ell$, engendré par le point $(\gamma_1, \ldots, \gamma_\ell)$, alors la composante connexe de l'origine de $H(\mathbb{R})$ est

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

(voir l'exercice à la fin de la section a_2) du paragraphe 2). Il suffit donc d'appliquer le lemme 3.4.

Conjecture $3.5^?$ $\Rightarrow$ Conjecture $3.3^?$
Nous n'utiliserons la conjecture $3.5^?$ que pour les groupes $\mathbb{G}_{\mathrm{m}}^d$, avec $d \ge 2$. On suppose que la conjecture d'indépendance algébrique homogène réelle n'est pas vraie : il existe des nombres algébriques réels positifs multiplicativement indépendants, $\theta_1, \ldots, \theta_r$, tels que les nombres $\log\theta_1, \ldots, \log\theta_r$ vérifient une relation de dépendance algébrique homogène non triviale. Soit $P \in \mathbb{Q}[X_1, \ldots, X_r]$ un polynôme homogène non nul tel que $P(\log\theta_1, \ldots, \log\theta_r) = 0$. Le lemme 3.7 ci-dessous affirme qu'il existe des nombres rationnels

$$b_{ij\varrho} \in \mathbb{Q}, \qquad (1 \le i \le d,\ 1 \le j \le d,\ 1 \le \varrho \le r),$$

tels que la matrice carrée

$$M(X_1,\dots,X_r)=\left(\sum_{\varrho=1}^{r} b_{ij\varrho}X_\varrho\right)_{1\le i,j\le d},$$

à coefficients dans $\mathbb{Q}X_1+\cdots+\mathbb{Q}X_r$, ait pour déterminant $X_1^{d-\deg P}P$. Ainsi la matrice M est de rang d, mais le rang de la matrice

$$M(\log\theta_1,\dots,\log\theta_r)=\left(\sum_{\varrho=1}^{r} b_{ij\varrho}\log\theta_\varrho\right)_{1\le i,j\le d}$$

est $< d$.

On choisit des nombres algébriques réels positifs $\alpha_1,\dots,\alpha_d$ tels que les $d+r$ nombres $\alpha_1,\dots,\alpha_d$, $\theta_1,\dots,\theta_r$ soient multiplicativement indépendants et on définit des éléments de $(K_+^\times)^d$ par

$$\gamma_0=(\alpha_1,\dots,\alpha_d),\qquad \gamma_j=\left(\prod_{\varrho=1}^{r}\theta_\varrho^{b_{ij\varrho}}\right)_{1\le i\le d},\qquad 1\le j\le d.$$

Le sous-groupe de $(\mathbb{R}_+^\times)^d$ engendré par $\gamma_0,\dots,\gamma_d$ n'est pas dense, car les vecteurs colonnes de $M(\log\theta_1,\dots,\log\theta_r)$ appartiennent à un même hyperplan.

Soient $x_1,\dots,x_r$, $\xi_1,\dots,\xi_d$ des nombres réels positifs dont les logarithmes sont algébriquement indépendants. On pose

$$\eta_0=(\xi_1,\dots,\xi_d),\qquad \eta_j=\left(\prod_{\varrho=1}^{r}x_\varrho^{b_{ij\varrho}}\right)_{1\le i\le d},\qquad 1\le j\le d.$$

Pour montrer que le sous-groupe engendré par $\eta_0,\eta_1,\dots,\eta_d$ est dense dans $(\mathbb{R}_+^\times)^d$, on utilise la proposition 4.3 du chapitre II : il s'agit de vérifier que pour tout $(s_0,\dots,s_d)\in\mathbb{Z}^{d+1}\setminus\{0\}$, le déterminant de la matrice

$$M'=\begin{pmatrix} & & & \log\xi_1\\ & M(\log x_1,\dots,\log x_r) & & \vdots\\ & & & \log\xi_d\\ s_1 & \cdots & s_d & s_0\end{pmatrix}$$

n'est pas nul. Ce déterminant est un polynôme en $\log\xi_1,\dots,\log\xi_d$, dont le terme constant est $s_0\det M(\log x_1,\dots,\log x_r)$. Si $s_0\neq 0$, alors $\det M'\neq 0$. Si $s_0=0$, alors on a $(s_1,\dots,s_d)\neq(0,\dots,0)$. On complète le vecteur $(s_1,\dots,s_d)$ en une base de $\mathbb{R}^d$ avec $d-1$ vecteurs lignes de la matrice $M(\log x_1,\dots,\log x_r)$; si i est l'indice du vecteur ligne de cette matrice qui n'a pas été utilisé, le coefficient de $\log\xi_i$ dans le déterminant de M' n'est pas nul. On obtient ainsi un contre exemple à la conjecture $3.5^?$ pour le groupe $\mathbb{G}_{\mathrm{m}}^d$. $\square$

La démonstration du lemme 3.6 a utilisé le résultat suivant, dû à D.Roy [R 1988a], Prop. 3 (voir aussi [R 1990b], Prop. 3.3) :

Lemme 3.7. – *Soient A un anneau commutatif unitaire et n un entier.*
a) Tout polynôme de l'anneau $A[T_1,\dots,T_n]$ est le déterminant d'une matrice carrée à coefficients dans le A-module $A+AT_1+\cdots+AT_n$.
b) Pour tout polynôme homogène f de $A[T_0,\dots,T_n]$, il existe une matrice carrée de format $d\times d$ à coefficients dans le A-module $AT_0+\cdots+AT_n$ dont le déterminant est $T_0^{d-\deg f}f$.

Démonstration.
a) On désigne par $R=A[T_1,\dots,T_n]$ l'anneau des polynômes à coefficients dans A en n indéterminées. Pour chaque entier $d\ge 1$, on note R_d le sous-A-module de R formé des polynômes de degré total $\le d$. Ainsi $R_1=A+AT_1+\cdots+AT_n$, tandis que R_d est engendré comme A-module par les monomes $T_1^{a_1}\cdots T_n^{a_n}$ avec $a_1+\cdots+a_n\le d$. Quand E et F sont deux sous-A-modules de R, on désigne par EF le sous-module de R engendré par les produits xy, $(x\in E,\ y\in F)$. Donc $R_d=R_1R_{d-1}$ pour tout $d\ge 2$.

On remarque déjà que si une matrice M a ses coefficients dans EF où E et F sont deux sous-A-modules de R, alors il existe une matrice P dont les coefficients sont dans E, et une matrice Q dont les coefficients sont dans F, telles que $M=PQ$. En effet on peut écrire $M=M_1y_1+\cdots+M_ty_t$, avec $y_1,\dots,y_t$ dans F, et les matrices $M_1,\dots,M_t$ ont toutes le même format que M, et sont à coefficients dans E. Si M est de format $d\times\ell$, on peut prendre par exemple P de format $d\times(t\ell)$ et Q de format $(t\ell)\times\ell$:

$$P=\begin{pmatrix}M_1 & \cdots & M_t\end{pmatrix},\qquad Q=\begin{pmatrix}y_1I_\ell\\ \vdots\\ y_tI_\ell\end{pmatrix},$$

où I_ℓ est la matrice identité $\ell\times\ell$.

On remarque ensuite que si P est une matrice $p\times q$ et Q une matrice $q\times p$, alors

$$\det(PQ)=\det\begin{pmatrix}I_q & Q\\ -P & 0\end{pmatrix}.$$

Pour le voir il suffit de multiplier cette dernière matrice à gauche par la matrice $\begin{pmatrix}I_q & 0\\ P & I_p\end{pmatrix}$ dont le déterminant est 1 ; le produit est $\begin{pmatrix}I_q & Q\\ 0 & PQ\end{pmatrix}$ dont le déterminant est égal à celui de PQ.

Ces deux remarques montrent que toute matrice carrée M à coefficients dans R_d, avec $d\ge 2$, a le même déterminant qu'une certaine matrice carrée à coefficients dans R_{d-1}. Par récurrence on déduit qu'il existe une matrice à coefficients dans R_1 ayant le même déterminant que M.

b) Soit $f\in A[T_0,\dots,T_n]$ un polynôme homogène. D'après a), il existe une matrice carrée M à coefficients dans $A+AT_1+\cdots+AT_n$ telle que $f(1,T_1,\dots,T_n)=\det M$. On remplace dans M chaque coefficient de la forme $a_0+a_1T_1+\cdots+a_nT_n$ par $a_0T_0+a_1T_1+\cdots+a_nT_n$. $\square$

Exercice. Soit P un polynôme de degré D en n variables ; montrer qu'il existe une matrice carrée, de format $d\times d$, avec $d\le(n+1)^{D-1}$, à coefficients dans $A+AT_1+\cdots+AT_n$,

dont le déterminant est P.
`Indication.` *Reprendre la démonstration, mais en utilisant la relation suivante, pour des matrices carrées $M_0, M_1, \ldots, M_n$ de même format $k \times k$:*

$$\det(M_0 + M_1X_1 + \cdots + M_nX_n) = \det \begin{pmatrix} & & & -X_1I_k \\ & I_{nk} & & \vdots \\ & & & -X_nI_k \\ M_1 & \cdots & M_n & M_0 \end{pmatrix}.$$

Exercice. Soit S l'anneau $A[X_1^{(1)}, \ldots, X_n^{(m)}]$ des polynômes en mn inconnues $X_i^{(j)}$, ($1 \le i \le n$, $1 \le j \le m$). Montrer que tout élément de S est le determinant d'une matrice M de la forme

$$M = \begin{pmatrix} M_{00} & M_{01} \\ M_{10} & M_{11} \\ \vdots & \vdots \\ M_{m0} & M_{m1} \end{pmatrix}$$

où M_{ji} a ses coefficients dans A si i ou j s'annule, tandis que, pour $j = 1, \ldots, m$, M_{j1} a ses coefficients dans le sous-A-module L_j de S engendré par $X_1^{(j)}, \ldots, X_n^{(j)}$.
Exemple : tout polynôme dans l'anneau $A[X_1, \ldots, X_n, Y_1, \ldots, Y_k]$ peut être écrit sous la forme

$$\det \begin{pmatrix} M_0 & M_0' \\ M_1 & M_1' \\ M_2 & M_2' \end{pmatrix}$$

où les matrices M_0, M_1, M_2, M_0' ont leurs coefficients dans A, la matrice M_1' a ses coefficients dans $AX_1 + \cdots + AX_n$ et M_2' a ses coefficients dans $AY_1 + \cdots + AY_k$.
`Indication (d'après D. Roy).` Soit $P \in S$. D'après le lemme 3.7, $P = \det N$ où N est une matrice à coefficients dans

$$A \oplus L_1 \oplus \cdots \oplus L_m.$$

Donc on peut écrire N sous la forme

$$N = N_0 + N_1 + \cdots + N_m = \begin{pmatrix} N_0 & N_1 & \ldots & N_m \end{pmatrix} \begin{pmatrix} I \\ I \\ \vdots \\ I \end{pmatrix},$$

où N_0 a ses coefficients dans A tandis que N_j a ses coefficients dans L_j pour $j = 1, \ldots, m$. On désigne par I la matrice identité de même taille que N. On a

$$\det \begin{pmatrix} I & I & \ldots & I & 0 \\ I & 0 & \ldots & 0 & N_0 \\ 0 & I & \ldots & 0 & N_1 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \ldots & I & N_m \end{pmatrix} = \det \begin{pmatrix} 0 & 0 & \ldots & 0 & -N \\ I & 0 & \ldots & 0 & N_0 \\ 0 & I & \ldots & 0 & N_1 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \ldots & I & N_m \end{pmatrix} = \pm \det N.$$

Nous avons vu (dans la démonstration du lemme 3.6) que le cas particulier $d_0 = 0$ de la conjecture $3.5^?$ suffisait pour impliquer la conjecture $3.3^?$, qui à son tour implique la conjecture $3.5^?$. Par conséquent les deux assertions suivantes sont équivalentes :

(i) Pour tout entier $d_1 > 0$, le groupe algébrique $\mathbb{G}_{\mathrm{m}}^{d_1}$ possède la propriété de densité.
(ii) Pour tout d_0 et d_1 entiers ≥ 0 avec $d = d_0 + d_1 > 0$, le groupe algébrique $\mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}$ possède la propriété de densité.

Ainsi la situation conjecturale contraste avec ce que l'on sait démontrer : dans le théorème 2.10, les facteurs $\mathbb{G}_{\mathrm{a}}$ recèlent des informations non redondantes.

Lemme 3.8. – *La conjecture $3.5^?$ est vraie dans le cas particulier $d_1 = 0$.*

Démonstration. Quand $d_1 = 0$ et $d_0 = d$, le groupe $G(\mathbb{R})$ des points réels du groupe algébrique $G = \mathbb{G}_{\mathrm{a}}^d$ est le $\mathbb{R}$-espace vectoriel $\mathbb{R}^d$. Soit Γ un sous-groupe de type fini de $\mathbb{R}^d$, de rang ℓ, et soit $(\gamma_1, \ldots, \gamma_\ell)$ un système générateur de Γ comme $\mathbb{Z}$-module. Si H est l'adhérence de Zariski dans $\mathbb{G}_{\mathrm{a}}^{d\ell}$ du sous-groupe $\mathbb{Z}(\gamma_1, \ldots, \gamma_\ell)$, alors $H(\mathbb{R})$ est le sous-espace vectoriel de $\mathbb{R}^{d\ell}$ engendré par ce point :

$$H(\mathbb{R}) = \{(\gamma_1 x, \ldots, \gamma_\ell x)\,;\, x \in \mathbb{R}\}.$$

Alors $\mathbb{Z}\gamma_1 + \cdots + \mathbb{Z}\gamma_\ell$ est dense dans $\mathbb{R}^d$ si et seulement s'il existe $x \in \mathbb{R}$ tel que $\mathbb{Z}\gamma_1 x + \cdots + \mathbb{Z}\gamma_\ell x$ soit dense dans $\mathbb{R}^d$. □

Voici un exemple pour terminer cette section :

Corollaire 3.9. – *Sous les hypothèses du corollaire 2.11, si on admet la conjecture $3.3^?$, alors 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 $\ell \ge d + 1$ et que Γ_0 soit dense dans $\mathbb{R}^{d_0}$.*

Démonstration. 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 $\ell = \mathrm{rang}_{\mathbb{Z}}(\Gamma) \ge \mathrm{m}_{\mathbb{R}}(G) = d + 1$. Pour la réciproque, on utilise la conjecture $3.5^?$: le fait que les $d_1\ell$ nombres α_{ij} soient multiplicativement indépendants assure que l'adhérence de Zariski H du sous-groupe de $G^\ell = \mathbb{G}_{\mathrm{a}}^{d_0\ell} \times \mathbb{G}_{\mathrm{m}}^{d_1\ell}$ engendré par le point $(\beta_{hj}; \alpha_{ij})_{1 \le h \le d_0, 1 \le i \le d_1, 1 \le j \le \ell}$ vérifie $H(\mathbb{R})^0 = \{(x_0\beta_{hj}; x_{ij})_{1 \le h \le d_0, 1 \le i \le d_1, 1 \le j \le \ell};\ (x_0, x_{ij}) \in \mathbb{R} \times (\mathbb{R}_+^\times)^{d_1\ell}\}$. Il reste à montrer qu'il existe $(x_{ij})_{1 \le i \le d_1, 1 \le j \le \ell} \in (\mathbb{R}_+^\times)^{d_1\ell}$ tel que le sous-groupe $\mathbb{Z}\eta_1 + \cdots + \mathbb{Z}\eta_\ell$ de $\mathbb{R}^{d_0} \times (\mathbb{R}_+^\times)^{d_1}$ engendré par

$$\eta_j = (\beta_{1j}, \ldots, \beta_{d_0j}; x_{1j}, \ldots, x_{d_1j}), \qquad (1 \le j \le \ell)$$

soit dense dans $G(\mathbb{R})^0 = \mathbb{R}^{d_0} \times (\mathbb{R}_+^\times)^{d_1}$. On prend des nombres réels t_{ij}, ($1 \le i \le d_1$, $1 \le j \le \ell$), qui sont algébriquement indépendants (sur $\mathbb{Q}$, donc sur K) et on pose $x_{ij} = e^{t_{ij}}$, ($1 \le i \le d_1$, $1 \le j \le \ell$). Il s'agit de vérifier que pour tout $(s_1, \ldots, s_\ell) \in \mathbb{Z}^\ell \setminus \{0\}$, la matrice

$$M = \begin{pmatrix} \beta_{11} & \cdots & \beta_{1j} & \cdots & \beta_{1\ell} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \beta_{d_01} & \cdots & \beta_{d_0j} & \cdots & \beta_{d_0\ell} \\ t_{11} & \cdots & t_{1j} & \cdots & t_{1\ell} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ t_{d_11} & \cdots & t_{d_1j} & \cdots & t_{d_1\ell} \\ s_1 & \cdots & s_j & \cdots & s_\ell \end{pmatrix}$$

est de rang $d+1$. Comme Γ_0 est dense dans $\mathbb{R}^{d_0}$, la matrice obtenue en ne conservant que les d_0 premières lignes et la dernière est de rang d_0+1 (c'est la proposition 4.3 du chapitre II qui le dit). On considère un mineur non nul de M de format $(d_0+1)\times(d_0+1)$. Les d_0+1 colonnes correspondantes de M sont linéairement indépendantes sur $\mathbb{R}$. Comme les nombres t_{ij} sont algébriquement indépendants sur K et que $\ell \geq d+1$, tout système de $d+1$ colonnes de M contenant les d_0+1 colonnes choisies est encore libre sur $\mathbb{R}$. On applique encore une fois la proposition 4.3 du chapitre II pour conclure. □

Exercice. On considère un sous-espace vectoriel $\mathbb{L}$ de $\mathbb{R}$ sur $\mathbb{Q}$ et on note $\mathcal{Q}$ son image par l'application exponentielle :

$$\mathcal{Q} = \exp \mathbb{L} = \{e^\lambda;\ \lambda \in \mathbb{L}\} \subset \mathbb{R}_+^\times.$$

1. On fait l'hypothèse suivante :

toute famille $\mathbb{Q}$-linéairement indépendante d'éléments de $\mathbb{L}$ est algébriquement libre sur $\mathbb{Q}$.

Soient d un entier >0, G le groupe algébrique $\mathbb{G}_{\mathrm{m}}^d$, et Γ un sous-groupe de type fini de $\mathcal{Q}^d$ de rang ℓ ; soient $\gamma_1,\dots,\gamma_\ell$ des éléments multiplicativement indépendants de Γ. On désigne par H l'adhérence de Zariski de $\mathbb{Z}(\gamma_1,\dots,\gamma_\ell)$ dans G^ℓ. Alors Γ est dense dans $(\mathbb{R}_+^\times)^d$ si et seulement s'il existe $(\eta_1,\dots,\eta_\ell)\in H(\mathbb{R})$ tel que le sous-groupe $\mathbb{Z}\eta_1+\cdots+\mathbb{Z}\eta_\ell$ soit dense dans $(\mathbb{R}_+^\times)^d$.

2. Réciproquement, on suppose :

si d est un entier >0, G le groupe algébrique $\mathbb{G}_{\mathrm{m}}^d$, Γ un sous-groupe de type fini de $\mathcal{Q}^d$ de rang ℓ, $\gamma_1,\dots,\gamma_\ell$ des éléments multiplicativement indépendants de Γ, si H désigne l'adhérence de Zariski de $\mathbb{Z}(\gamma_1,\dots,\gamma_\ell)$ dans G^ℓ et s'il existe $(\eta_1,\dots,\eta_\ell)\in H(\mathbb{R})$ tel que le sous-groupe $\mathbb{Z}\eta_1+\cdots+\mathbb{Z}\eta_\ell$ soit dense dans $(\mathbb{R}_+^\times)^d$, alors Γ est dense dans $(\mathbb{R}_+^\times)^d$.

Soient $\lambda_1,\dots,\lambda_m$ des éléments $\mathbb{Q}$-linéairement indépendants de $\mathbb{L}$ et $P\in\mathbb{Q}[X_1,\dots,X_m]$ un polynôme homogène non nul. Vérifier $P(\lambda_1,\dots,\lambda_m)\neq 0$.

§4. Groupes algébriques linéaires sur $\mathbb{C}$

Soit Γ un sous-groupe de type fini de $\overline{\mathbb{Q}}^{d_0}\times(\overline{\mathbb{Q}}^\times)^{d_1}$. On veut savoir si Γ est dense dans $\mathbb{C}^{d_0}\times(\mathbb{C}^\times)^{d_1}$. Au groupe algébrique $G=\mathbb{G}_{\mathrm{a}}^{d_0}\times\mathbb{G}_{\mathrm{m}}^{d_1}$ on associe un groupe algébrique $\widetilde{G}$ défini sur $\mathbb{R}$, dont le groupe des points réels est isomorphe à $G(\mathbb{C})$. La réponse à la question de densité fera intervenir les sous-groupes algébriques de $\widetilde{G}$.

Le cas $d_1=0$, $G=\mathbb{G}_{\mathrm{a}}^d$ est facile, grâce à la proposition 6.1 du chapitre II. On reprendra l'étude des sous-groupes de $\mathbb{C}^\times$, $(G=\mathbb{G}_{\mathrm{m}})$ qui a été commencée dans la section c) du paragraphe 1 ; on l'étendra ensuite aux sous groupes de type fini de $(\mathbb{C}^\times)^d$, $(G=\mathbb{G}_{\mathrm{m}}^d)$ avant de considérer le cas général.

a) *Sous-groupes de $\mathbb{C}^d$*

Le problème de la densité de sous-groupes de type fini de $\mathbb{C}^d$ a fait l'objet de la proposition 6.1 du chapitre II. On définit une application $\varphi:\mathbb{C}^d\to\mathbb{C}^{2d}$ par

$$\varphi(z_1,\dots,z_d)=(z_1,\dots,z_d;\overline{z}_1,\dots,\overline{z}_d).$$

Quand Γ est un sous-groupe de type fini de $\mathbb{C}^d$, on pose $\widetilde{\Gamma}=\varphi(\Gamma)$;

$$\widetilde{\Gamma}=\{(\gamma,\overline{\gamma})\,;\ \gamma\in\Gamma\}\subset\mathbb{C}^{2d}.$$

Alors les conditions suivantes sont équivalentes :

(i) Γ *est dense dans* $\mathbb{C}^d$.

(ii) *Pour tout hyperplan complexe H de $\mathbb{C}^{2d}$, on a*

$$\mathrm{rang}_{\mathbb{Z}}\big(\widetilde{\Gamma}/\widetilde{\Gamma}\cap H\big)\geq 2.$$

Choisissons une base $(\gamma_1,\dots,\gamma_\ell)$ du $\mathbb{Z}$-module Γ et posons $\widetilde{\gamma}_j=\varphi(\gamma_j)$, $(1\leq j\leq\ell)$, de sorte que $\widetilde{\Gamma}=\mathbb{Z}\widetilde{\gamma}_1+\cdots+\mathbb{Z}\widetilde{\gamma}_\ell$. L'adhérence de Zariski Z de $\mathbb{Z}(\widetilde{\gamma}_1,\dots,\widetilde{\gamma}_\ell)$ dans $(\mathbb{C}^{2d})^\ell=\mathbb{G}_a^{2d\ell}(\mathbb{C})$ est le plus petit sous-espace vectoriel sur $\mathbb{C}$ de $\mathbb{C}^{2d\ell}$ contenant le point $\big(\varphi(\gamma_1),\dots,\varphi(\gamma_\ell)\big)$: si on écrit $\gamma_j=(\beta_{ij})_{1\leq i\leq d}$, $(1\leq j\leq\ell)$, alors

$$Z=\{(z\beta_{ij},z\overline{\beta}_{ij})_{1\leq i\leq d,1\leq j\leq\ell}\,;\ z\in\mathbb{C}\}.$$

L'intersection de Z avec l'image diagonale de φ est le plus petit sous-espace vectoriel sur $\mathbb{R}$ de $\mathbb{C}^{2d\ell}$ contenant le point $\big(\varphi(\gamma_1),\dots,\varphi(\gamma_\ell)\big)$:

$$Z\cap\big(\varphi(\mathbb{C}^d)\big)^\ell=\{(x\beta_{ij},x\overline{\beta}_{ij})_{1\leq i\leq d,1\leq j\leq\ell}\,;\ x\in\mathbb{R}\}.$$

Quand Γ est contenu dans $G(\overline{\mathbb{Q}})=\overline{\mathbb{Q}}^d$, ce sous-espace est rationnel sur $K=\overline{\mathbb{Q}}\cap\mathbb{R}$. On notera enfin que les conditions (i) et (ii) précédentes sont encore équivalentes à la suivante :

(iii) *Il existe $x\in\mathbb{R}$ tel que $\mathbb{Z}x\gamma_1+\cdots+\mathbb{Z}x\gamma_\ell$ soit dense dans $G(\mathbb{C})=\mathbb{C}^d$.*

b) *Sous-groupes de $\mathbb{C}^\times$*

On a vu (dans le paragraphe 1, section c)) que l'étude de la densité dans $\mathbb{C}^\times$ d'un sous-groupe de type fini Γ faisait intervenir le sous-groupe $\widetilde{\Gamma}\subset(\mathbb{C}^\times)^2$ défini par

$$\widetilde{\Gamma}=\{(\gamma,\overline{\gamma})\,;\ \gamma\in\Gamma\}.$$

On pose

$$\begin{array}{rccc} \varphi: & \mathbb{C} & \to & \mathbb{C}^2 \\ & z & \mapsto & (z,\overline{z}) \end{array} \qquad \text{et} \qquad \begin{array}{rccc} \phi: & \mathbb{C}^\times & \to & (\mathbb{C}^\times)^2. \\ & t & \mapsto & (t,\overline{t}) \end{array}$$

Le groupe algébrique $\mathbb{G}_{\mathrm{m}}^2$ est linéaire ; on le plonge habituellement dans GL_2 de façon diagonale, mais il y a d'autres plongements. Considérons l'application

$$\begin{array}{rccc} \theta: & (\mathbb{C}^\times)^2 & \to & \mathrm{GL}_2(\mathbb{C}) \\ & (t_1,t_2) & \mapsto & \begin{pmatrix} \frac{1}{2}(t_1+t_2) & \frac{1}{2i}(t_1-t_2) \\ -\frac{1}{2i}(t_1-t_2) & \frac{1}{2}(t_1+t_2) \end{pmatrix}. \end{array}$$

Le déterminant de la matrice est

$$\frac{1}{4}(t_1+t_2)^2 - \frac{1}{4}(t_1-t_2)^2 = t_1 t_2.$$

L'image de θ est un sous-groupe de $\mathrm{GL}_2(\mathbb{C})$:

$$\theta\big((\mathbb{C}^\times)^2\big) = \left\{ \begin{pmatrix} u & v \\ -v & u \end{pmatrix} ;\, (u,v) \in \mathbb{C}^2,\, u^2+v^2 \neq 0 \right\} \subset \mathrm{GL}_2(\mathbb{C}).$$

On définit une sous-variété algébrique $\widetilde{G}$ de GL_2 de la manière suivante : on écrit GL_2 comme l'hypersurface d'équation $(X_1X_4 - X_2X_3)X_5 = 1$ dans l'espace affine $\mathbb{A}_5$ et $\widetilde{G}$ est la sous-variété d'équations $X_1 = X_4$, $X_2 = -X_3$. On peut donc voir aussi $\widetilde{G}$ comme l'hypersurface algébrique d'équation $T_3(T_1^2+T_2^2) = 1$ dans $\mathbb{A}_3$. Le groupe des points complexes du groupe algébrique $\widetilde{G}$ est

$$\widetilde{G}(\mathbb{C}) = \theta\big((\mathbb{C}^\times)^2\big).$$

Le groupe algébrique $\widetilde{G}$ est isomorphe *sur* $\mathbb{C}$ au groupe $\mathbb{G}_{\mathrm{m}}^2$, mais il n'y a pas d'isomorphisme sur $\mathbb{R}$ entre ces deux groupes algébriques. La variété $\widetilde{G}$ est définie sur $\mathbb{R}$ (et même sur $\mathbb{Q}$), et ses points réels forment le sous-groupe

$$\widetilde{G}(\mathbb{R}) = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} ;\, (x,y) \in \mathbb{R}^2,\, (x,y) \neq \{0,0\} \right\} \subset \widetilde{G}(\mathbb{C})$$

qui est isomorphe à $\mathbb{C}^\times$ par $\theta\circ\phi$: pour $x+iy \in \mathbb{C}^\times$ on a

$$\theta\circ\phi(x+iy) = \theta(x+iy, x-iy) = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}.$$

Plus généralement, si K est un sous-corps de $\mathbb{C}$, l'application

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \longmapsto \begin{cases} a+ib & \text{si } i=\sqrt{-1} \notin K, \\ (a+ib, a-ib) & \text{si } i \in K \end{cases}$$

donne un isomorphisme

$$\widetilde{G}(K) \simeq \begin{cases} K(i)^\times & \text{si } i \notin K, \\ K^\times \times K^\times & \text{si } i \in K. \end{cases}$$

On obtient l'application exponentielle $\exp_{\widetilde{G}}$ de $\widetilde{G}(\mathbb{C})$ en composant avec θ l'application exponentielle de $(\mathbb{C}^\times)^2$:

$$\exp_{\mathbb{G}_{\mathrm{m}}^2} : \begin{array}{ccc} \mathbb{C}^2 & \to & (\mathbb{C}^\times)^2 \\ (z_1,z_2) & \mapsto & (e^{z_1}, e^{z_2}) \end{array}$$

et

$$\exp_{\widetilde{G}} = \theta\circ\exp_{\mathbb{G}_{\mathrm{m}}^2} : \begin{array}{ccc} T_{\widetilde{G}}(\mathbb{C}) = \mathbb{C}^2 & \longrightarrow & \widetilde{G}(\mathbb{C}) \\ (z_1,z_2) & \longmapsto & \begin{pmatrix} \frac{1}{2}(e^{z_1}+e^{z_2}) & \frac{1}{2i}(e^{z_1}-e^{z_2}) \\ -\frac{1}{2i}(e^{z_1}-e^{z_2}) & \frac{1}{2}(e^{z_1}+e^{z_2}) \end{pmatrix}. \end{array}$$

Comme θ est un isomorphisme, les noyaux de $\exp_{\widetilde{G}}$ et de $\exp_{\mathbb{G}_{\mathrm{m}}^2}$ sont les mêmes, à savoir $(2i\pi\mathbb{Z})^2$:

$$\begin{tikzcd} \mathbb{C}^2 \arrow[r, "\exp_{\mathbb{G}_{\mathrm{m}}^2}"] \arrow[dr, "\exp_{\widetilde{G}}"'] & (\mathbb{C}^\times)^2 \arrow[d, "\theta"] \\ & \widetilde{G}(\mathbb{C}). \end{tikzcd}$$

La restriction de $\exp_{\widetilde{G}}$ au sous-espace $\varphi(\mathbb{C})$ est l'application exponentielle de $\widetilde{G}(\mathbb{R})$. On écrira donc $T_{\widetilde{G}}(\mathbb{R}) = \varphi(\mathbb{C})$ (qui est un $\mathbb{R}$-espace vectoriel de dimension 2). Le $\mathbb{C}$-espace vectoriel $\mathbb{C}^2$ admet comme base $(1,1)$ et $(i,-i)$; on définit une $\mathbb{R}$-structure sur $\mathbb{C}^2$ en considérant le $\mathbb{R}$-sous-espace vectoriel engendré par ces deux éléments :

$$\begin{array}{cl} \mathbb{C}^2 & = \big\{(z_1+iz_2, z_1-iz_2) ;\, (z_1,z_2) \in \mathbb{C}^2\big\} \\ \bigcup & \\ \varphi(\mathbb{C}) & = \big\{(x+iy, x-iy) ;\, (x,y) \in \mathbb{R}^2\big\}. \end{array}$$

On a le diagramme commutatif (où $\exp_{\mathbb{G}_{\mathrm{m}}}$ est l'application exponentielle usuelle $z \mapsto e^z$) :

$$\begin{tikzcd} \mathbb{C} \arrow[r, "\exp_{\mathbb{G}_{\mathrm{m}}}"] \arrow[d, "\varphi"'] & \mathbb{C}^\times \arrow[d, "\theta\circ\phi"] \\ T_{\widetilde{G}}(\mathbb{R}) \arrow[r, "\exp_{\widetilde{G},\mathbb{R}}"] \arrow[d, phantom, "\bigcap"] & \widetilde{G}(\mathbb{R}) \arrow[d, phantom, "\bigcap"] \\ T_{\widetilde{G}}(\mathbb{C}) \arrow[r, "\exp_{\widetilde{G}}"] & \widetilde{G}(\mathbb{C}). \end{tikzcd}$$

Le noyau de $\exp_{\widetilde{G},\mathbb{R}}$ est $\varphi(2i\pi\mathbb{Z})$, sous-groupe de rang 1 de $T_{\widetilde{G}}(\mathbb{R})$.

D'après le lemme 1.11, si G' est un sous-groupe algébrique de $\widetilde{G}$, l'intersection $G'(\mathbb{R})$ de $G'(\mathbb{C})$ avec $\widetilde{G}(\mathbb{R})$ est l'image par l'isomorphisme $\theta\circ\phi$ de l'un des sous-groupes suivants :

$$\mathbb{C}^\times, \quad \mathbb{U}, \quad \mathbb{R}_+^\times \times \mu_{2n}, \quad \mu_n,$$

avec n entier ≥ 1.

Remarque. La construction qui vient d'être faite est un cas particulier de la *restriction des scalaires.* Quand k est un corps de caractéristique nulle et A une k-algèbre commutative unitaire, ayant une base finie $e_1,\ldots,e_d$ comme k-espace vectoriel, on peut définir une loi interne sur l'espace affine de dimension d de la manière suivante :

$$(x_1,\ldots,x_d)(y_1,\ldots,y_d) = \big(f_1(x,y),\ldots,f_d(x,y)\big),$$

où les polynômes $f_1, \ldots, f_d$ dans $k[X_1, \ldots, X_d, Y_1, \ldots, Y_d]$ sont définis par :

$$(x_1e_1 + \cdots + x_de_d)(y_1e_1 + \cdots + y_de_d) = f_1(x,y)e_1 + \cdots + f_d(x,y)e_d.$$

En écrivant $1 = u_1e_1 + \cdots + u_de_d$, on obtient un élément unité $u = (u_1, \ldots, u_d)$. On montre qu'il existe un polynôme $D \in k[X_1, \ldots, X_d]$ ayant la propriété suivante : *si B est une k-algèbre commutative, pour $(x_1, \ldots, x_d) \in B^d$, le système d'équations*

$$f_i(x,y) = u_i, \qquad (1 \leq i \leq d)$$

a une solution $(y_1, \ldots, y_d) \in B^d$ si et seulement si $D(x) \in B^\times$. On note T_A le groupe algébrique défini sur k, ouvert de Zariski de $\mathbb{A}_d$ défini par $D(x) \neq 0$. Pour toute k-algèbre B, $T_A(B)$ est un groupe, et $T_A(k) = A^\times$ est le groupe des unités de A.

Par exemple si on prend pour A un corps K extension finie de k, le groupe algébrique ainsi obtenu, noté $T_{K/k}$, est le *tore associé à l'extension K/k*. Le groupe $T_{K/k}(k)$ est $K^\times$, alors que $T_{K/k}(K)$ est $(K^\times)^d$. On dit aussi que $T_{K/k}$ est *le tore obtenu par restriction des scalaires de $\mathbb{G}_{\mathrm{m}}$ de K à k* ; on note encore $T_{K/k} = \mathrm{Res}_{K/k}(\mathbb{G}_{\mathrm{m}})$. Nous reviendrons sur cette question dans le chapitre suivant.

c) *Densité dans $(\mathbb{C}^\times)^d$ de sous-groupes de $(\overline{\mathbb{Q}}^\times)^d$*
Soit d un entier ≥ 1. On conservera la notation $\theta : (\mathbb{C}^\times)^2 \to \mathrm{GL}_2(\mathbb{C})$ pour l'application qui a été introduite ci-dessus, mais maintenant φ et ϕ désigneront les applications

$$\begin{array}{rccc} \varphi : & \mathbb{C}^d & \to & \mathbb{C}^{2d} \\ & z & \mapsto & (z, \overline{z}) \end{array} \qquad \text{et} \qquad \begin{array}{rccc} \phi : & (\mathbb{C}^\times)^d & \to & (\mathbb{C}^\times)^{2d} \\ & t & \mapsto & (t, \overline{t}) \end{array}$$

On pose

$$\begin{array}{rccc} \theta^d : & (\mathbb{C}^\times)^{2d} & \longrightarrow & \mathrm{GL}_{2d}(\mathbb{C}) \\ & (t_1, \ldots, t_d; t'_1, \ldots, t'_d) & \longmapsto & \mathrm{diag}\big(\theta(t_1, t'_1), \ldots, \theta(t_d, t'_d)\big) \end{array}$$

L'image, qui est évidemment isomorphe à $(\mathbb{C}^\times)^{2d}$, est le groupe $\widetilde{G}(\mathbb{C})$ des points complexes d'un sous-groupe algébrique $\widetilde{G}$ de GL_{2d}, de dimension $2d$, défini sur $\mathbb{Q}$. Ce sous-groupe algébrique est isomorphe *sur* $\mathbb{C}$ au groupe algébrique $\mathbb{G}_{\mathrm{m}}^{2d}$. L'application $\theta^d \circ \phi$ donne un isomorphisme de $(\mathbb{C}^\times)^d$ sur le groupe $\widetilde{G}(\mathbb{R})$ des points réels de la variété algébrique $\widetilde{G}$. On définit $T_{\tilde{G}}(\mathbb{R}) = \varphi(\mathbb{C}^d)$, qui est un $\mathbb{R}$-espace vectoriel de dimension $2d$, isomorphe à $\mathbb{C}^d$ par φ, contenu dans $T_{\tilde{G}}(\mathbb{C}) = \mathbb{C}^{2d}$, et on a encore un diagramme commutatif

$$\begin{tikzcd} \mathbb{C}^d \arrow[r, "\exp_{\mathbb{G}_{\mathrm{m}}^d}"] \arrow[d, "\varphi"'] & (\mathbb{C}^\times)^d \arrow[d, "\theta^d \circ \phi"] \\ T_{\tilde{G}}(\mathbb{R}) \arrow[r, "\exp_{\tilde{G},\mathbb{R}}"] \arrow[d, phantom, "\bigcap"] & \widetilde{G}(\mathbb{R}) \arrow[d, phantom, "\bigcap"] \\ T_{\tilde{G}}(\mathbb{C}) \arrow[r, "\exp_{\tilde{G}}"] & \widetilde{G}(\mathbb{C}). \end{tikzcd}$$

Le noyau $\widetilde{\Omega}$ de $\exp_{\tilde{G}}$ est $(2i\pi\mathbb{Z})^{2d}$, tandis que celui de $\exp_{\tilde{G},\mathbb{R}}$ est le sous-groupe suivant de rang d de $T_{\tilde{G}}(\mathbb{R})$:

$$\widetilde{\Omega}_{\mathbb{R}} = \varphi\big((2i\pi\mathbb{Z})^d\big) = \mathbb{Z}2i\pi\widetilde{\epsilon_1} + \cdots + \mathbb{Z}2i\pi\widetilde{\epsilon_d},$$

où $\epsilon_1, \ldots, \epsilon_d$ désigne la base canonique de $\mathbb{C}^d$ et $\widetilde{\epsilon_j} = (\epsilon_j, -\epsilon_j)$, $(1 \leq j \leq d)$.

Comme groupe topologique, $\widetilde{G}(\mathbb{C})$ est isomorphe à $(\mathbb{C}^\times)^{2d}$ et $\widetilde{G}(\mathbb{R})$ à $(\mathbb{C}^\times)^d$, ce qui donne

$$\mathrm{m}\big(\widetilde{G}(\mathbb{C})\big) = 2d + 1 \quad \text{et} \quad \mathrm{m}\big(\widetilde{G}(\mathbb{R})\big) = d + 1.$$

On pose $\mathrm{m}_{\mathbb{C}}\big(\widetilde{G}\big) = \mathrm{m}\big(\widetilde{G}(\mathbb{C})\big)$ et $\mathrm{m}_{\mathbb{R}}\big(\widetilde{G}\big) = \mathrm{m}\big(\widetilde{G}(\mathbb{R})\big)$.

Les sous-groupes algébriques de $\widetilde{G}$ sont obtenus en prenant les images par θ^d des sous-groupes algébriques de $\mathbb{G}_{\mathrm{m}}^{2d}$; ils sont donc indexés par les sous-groupes A de $\mathbb{Z}^{2d}$: l'image par θ^d du sous-groupe $\mathcal{T}_A(\mathbb{C})$ sera notée $\mathcal{G}_A(\mathbb{C})$:

$$\mathcal{G}_A = \big\{(t_1, \ldots, t_d; t'_1, \ldots, t'_d) \in \widetilde{G}\,;\, t_1^{a_1} \cdots t_d^{a_d} t'^{a'_1}_1 \cdots t'^{a'_d}_d = 1 \quad \text{pour tout} \quad (a, a') \in A\big\}.$$

Le groupe des points réels de $\mathcal{G}_A$ est $\mathcal{G}_A(\mathbb{R}) = \mathcal{G}_A(\mathbb{C}) \cap \widetilde{G}(\mathbb{R})$:

$$\begin{aligned} \mathcal{G}_A(\mathbb{R}) = \big\{(t_1, \ldots, t_d; \bar{t}_1, \ldots, \bar{t}_d)\,;\, &(t_1, \ldots, t_d) \in (\mathbb{C}^\times)^d, \\ &t_1^{a_1} \cdots t_d^{a_d} \bar{t}_1^{a'_1} \cdots \bar{t}_d^{a'_d} = 1 \quad \text{pour tout} \quad (a, a') \in A\big\}. \end{aligned}$$

L'espace tangent à l'origine de $\mathcal{G}_A(\mathbb{C})$ est le plus grand sous-espace vectoriel contenu dans $\exp_{\tilde{G}}^{-1}\big(\mathcal{G}_A(\mathbb{C})\big)$:

$$T_{\mathcal{G}_A}(\mathbb{C}) = \left\{(z, z') \in \mathbb{C}^{2d}\,;\, \sum_{i=1}^d \big(a_iz_i + a'_iz'_i\big) = 0 \ \text{ pour tout } \ (a, a') \in A\right\}.$$

C'est un sous-espace vectoriel de $\mathbb{C}^{2d}$ rationnel sur $\mathbb{Q}$, et

$$T_{\mathcal{G}_A}(\mathbb{R}) = \left\{(z, \overline{z})\,;\, z \in \mathbb{C}^d,\ \sum_{i=1}^d \big(a_iz_i + a'_i\overline{z}_i\big) = 0 \ \text{ pour tout } \ (a, a') \in A\right\}.$$

Le noyau de l'application exponentielle de $\mathcal{G}_A(\mathbb{R})$ est

$$\begin{aligned} \mathrm{Ker}\ \exp_{\mathcal{G}_A,\mathbb{R}} = \Big\{(2i\pi n, -2i\pi n)\,;\, &n = (n_1, \ldots, n_d) \in \mathbb{Z}^d, \\ &\sum_{i=1}^d \big(a_i - a'_i\big)n_i = 0 \ \text{ pour tout } \ (a, a') \in A\Big\} \subset T_{\mathcal{G}_A}(\mathbb{R}). \end{aligned}$$

Si κ est son rang, alors $d - \kappa$ est le rang de l'image de A dans $\mathbb{Z}^d$ par l'application $(a, a') \mapsto a - a'$.

Soit G' un sous-groupe algébrique de $\widetilde{G}$ de codimension δ ; désignons par κ le rang sur $\mathbb{Z}$ du noyau de $\exp_{G',\mathbb{R}}$. La composante connexe de l'élément neutre de $G'(\mathbb{R})$ est isomorphe au quotient de $\mathbb{R}^{2d-\delta}$ par un sous-groupe de rang κ, donc

$$\mathrm{m}_{\mathbb{R}}(G') = \mathrm{m}\big(G'(\mathbb{R})\big) = \dim G' - \mathrm{rang}_{\mathbb{Z}}\mathrm{Ker}\ \exp_{G',\mathbb{R}} + 1 = 2d - \delta - \kappa + 1;$$

de même

$$\mathrm{m}_{\mathbb{R}}(\widetilde{G}/G') = \mathrm{m}\big(\widetilde{G}(\mathbb{R})/G'(\mathbb{R})\big) = \dim(\widetilde{G}/G') - \mathrm{rang}_{\mathbb{Z}}\big(\mathrm{Ker}\ \exp_{\widetilde{G}/G',\mathbb{R}}\big) + 1 = \delta - (d-\kappa) + 1.$$

Quand Γ est un sous-groupe de type fini de $(\mathbb{C}^\times)^d$, on définit $\widetilde{\Gamma} = \theta^d \circ \phi(\Gamma)$; c'est un sous-groupe de $\widetilde{G}(\mathbb{R})$, et Γ est dense dans $(\mathbb{C}^\times)^d$ si et seulement si $\widetilde{\Gamma}$ est dense dans $\widetilde{G}(\mathbb{R})$. Si Γ est dense, alors pour tout sous-groupe algébrique G' de $\widetilde{G}$, l'image de $\widetilde{\Gamma}$ dans le quotient $\widetilde{G}(\mathbb{R})/G'(\mathbb{R})$ est encore dense, donc

$$\mathrm{rang}_{\mathbb{Z}}\big(\widetilde{\Gamma}/\widetilde{\Gamma}\cap G'(\mathbb{R})\big) \geq \mathrm{m}_{\mathbb{R}}(\widetilde{G}/G').$$

Soient $\gamma_1,\dots,\gamma_\ell$ des éléments de $(\overline{\mathbb{Q}}^\times)^d$ multiplicativement indépendants, et soit Γ le sous-groupe multiplicatif (de rang ℓ) qu'ils engendrent. On veut donner des conditions suffisantes qui entraînent que Γ est dense dans $(\mathbb{C}^\times)^d$.

Exercice. En s'inspirant des démonstrations des corollaires 2.11 et 3.9, établir le résultat suivant. Soient α_{ij} $(1 \leq i \leq d,\ 1 \leq j \leq \ell)$ des nombres complexes algébriques non nuls, tels que les $2d\ell$ nombres α_{ij}, $\overline{\alpha}_{ij}$ soient multiplicativement indépendants. On désigne par $\gamma_j \in (\overline{\mathbb{Q}}^\times)^d$ le point de coordonnées $(\alpha_{1j},\dots,\alpha_{dj})$, $(1 \leq j \leq \ell)$, et par Γ le sous-groupe de $(\overline{\mathbb{Q}}^\times)^d$ qu'ils engendrent.
a) Si $\ell \geq 2d(2d-1)+2$, alors Γ est dense dans $(\mathbb{C}^\times)^d$.
b) On admet la conjecture $3.5^?$. Si $\ell \geq d+1$, alors Γ est dense dans $(\mathbb{C}^\times)^d$.

Nous allons donner un résultat plus précis que celui proposé dans l'exercice précédent. On définit

$$Y = \exp^{-1}_{\mathbb{G}_{\mathrm{m}}^d}(\Gamma) = \mathbb{Z}y_1 + \cdots + \mathbb{Z}y_\ell + \mathbb{Z}2i\pi\epsilon_1 + \cdots + \mathbb{Z}2i\pi\epsilon_d \subset \mathbb{C}^d.$$

On pose encore $\widetilde{Y} = \varphi(Y)$; il s'agit de vérifier que pour tout hyperplan complexe H de $\mathbb{C}^{2d}$, on a $\mathrm{rang}_{\mathbb{Z}}(\widetilde{Y}/\widetilde{Y}\cap H) \geq 2$. Rappelons la notation

$$\widetilde{\Omega}_{\mathbb{R}} = \mathrm{Ker}\ \exp_{\widetilde{G},\mathbb{R}} = \varphi\big((2i\pi\mathbb{Z})^d\big) = \mathbb{Z}2i\pi\widetilde{\epsilon}_1 + \cdots + \mathbb{Z}2i\pi\widetilde{\epsilon}_d.$$

On remarque que $\widetilde{Y}$ contient $\widetilde{\Omega}_{\mathbb{R}}$; si $\mathrm{rang}_{\mathbb{Z}}(\widetilde{\Omega}_{\mathbb{R}}/\widetilde{\Omega}_{\mathbb{R}}\cap H) \geq 2$, alors l'inégalité à démontrer est claire. On peut donc supposer que le nombre $\eta = \mathrm{rang}_{\mathbb{Z}}(\widetilde{\Omega}_{\mathbb{R}}/\widetilde{\Omega}_{\mathbb{R}}\cap H)$ est égal à 0 ou 1.

On considère le sous-espace de $\mathbb{C}^{2d}$ engendré par $\mathbb{Q}^{2d}\cap H$: c'est le plus grand sous-espace de $\mathbb{C}^{2d}$ rationnel sur $\mathbb{Q}$ contenu dans H, donc c'est le plus grand sous-espace de la forme $T_{G'}(\mathbb{C})$ qui soit contenu dans H, avec G' sous-groupe algébrique de $\widetilde{G}$. De la définition de $T_{G'}$ on déduit que $\widetilde{\Omega}_{\mathbb{R}}\cap H$ est contenu dans $T_{G'}(\mathbb{R})$: plus précisément

$$T_{G'}(\mathbb{R})\cap\widetilde{\Omega}_{\mathbb{R}} = H\cap\widetilde{\Omega}_{\mathbb{R}}.$$

En particulier la dimension de G' est $\geq d-\eta$.

On pose $\mathcal{V} = H/T_{G'}(\mathbb{C})$; c'est un hyperplan de $T_{\widetilde{G}/G'}(\mathbb{C})$, qui ne contient pas de sous-espace de $T_{\widetilde{G}/G'}(\mathbb{C})$ rationnel sur $\mathbb{Q}$ de dimension > 0 (il ne contient pas de sous-espace de la forme $T_{G''/G'}(\mathbb{C})$, avec G'' sous-groupe algébrique de $\widetilde{G}$ contenant G' et de dimension $> \dim G'$). On pose encore $Y' = \widetilde{Y}/\widetilde{Y}\cap T_{G'}(\mathbb{R})$. C'est un sous-groupe de type fini de $T_{\widetilde{G}/G'}(\mathbb{R})$ dont l'image par l'application exponentielle de $\widetilde{G}/G'$ est contenue dans $\big(\widetilde{G}/G'\big)(\overline{\mathbb{Q}}) \simeq (\overline{\mathbb{Q}}^\times)^\delta$, avec $\delta = \dim\widetilde{G} - \dim G'$. On est donc dans les conditions d'applications du théorème 2.6 :

$$\mathrm{rang}_{\mathbb{Z}}(Y'\cap\mathcal{V}) \leq \dim_{\mathbb{Q}}(\mathcal{L}^\delta\cap\mathcal{V}) \leq \delta(\delta-1).$$

Comme $Y'/Y'\cap\mathcal{V}$ et $\widetilde{Y}/\widetilde{Y}\cap H$ sont isomorphes, pour conclure à la densité de Γ dans $(\mathbb{C}^\times)^d$ il ne reste plus qu'à vérifier la condition

$$\mathrm{rang}_{\mathbb{Z}}Y' \geq \delta(\delta-1)+2 \quad \text{où} \quad Y' = \widetilde{Y}/\widetilde{Y}\cap T_{G'}(\mathbb{R}) \quad \text{et} \quad \dim G' = 2d-\delta.$$

On imposera cette condition pour tous les sous-groupes algébriques G' de $\widetilde{G}$ pour lesquels

$$\mathrm{rang}_{\mathbb{Z}}\big(T_{G'}(\mathbb{R})\cap\widetilde{\Omega}_{\mathbb{R}}\big) = d-\eta \quad \text{avec } \eta = 0 \text{ ou } 1 \text{ et } \delta \leq d+\eta.$$

Remarque a) : le cas $\eta = 0$. Un hyperplan H de $\mathbb{C}^{2d}$ qui vérifie $\mathrm{rang}_{\mathbb{Z}}\big(H\cap\widetilde{\Omega}_{\mathbb{R}}\big) = d$ contient $\widetilde{\Omega}_{\mathbb{R}}$, donc contient $\widetilde{\epsilon}_1,\dots,\widetilde{\epsilon}_d$ (*). Par conséquent il a une équation de la forme

$$\sum_{k=1}^d \vartheta_k(z_k + z_k') = 0,$$

avec $(\vartheta_1,\dots,\vartheta_d) \in \mathbb{C}^d\setminus\{0\}$. L'intersection d'un tel hyperplan H avec $\varphi(\mathbb{C}^d)$ est l'image par φ de

$$\left\{z\in\mathbb{C}^d\ ;\ \sum_{k=1}^d \vartheta_k \Re\mathrm{e}\ z_k = 0\right\}.$$

La condition

$$\mathrm{rang}_{\mathbb{Z}}\big(\widetilde{Y}/\widetilde{Y}\cap T_{G'}(\mathbb{R})\big) \geq \delta(\delta-1)+2$$

dans le cas $\widetilde{\Omega}_{\mathbb{R}} \subset T_{G'}(\mathbb{R})$ n'est autre que l'hypothèse qui est nécessaire pour pouvoir appliquer le théorème 2.6* et garantir la densité du sous-groupe de $(\mathbb{R}_+^\times)^d$ engendré par les éléments

$$(|\alpha_{1j}|,\dots,|\alpha_{dj}|), \qquad (1 \leq j \leq \ell).$$

(*) Noter qu'un tel hyperplan H ne contient pas $\varphi(\mathbb{C}^d)$, bien qu'il contienne l'image par φ d'une base de $\mathbb{C}^d$; mais φ n'est pas $\mathbb{C}$-linéaire !

Remarque b) : le cas $\eta = 1$. L'hypothèse que nécessite le théorème 2.6* pour garantir la densité du sous-groupe de $\mathbb{U}^d$ engendré par les éléments

$$(\alpha_{1j}/\overline{\alpha}_{1j}, \dots, \alpha_{dj}/\overline{\alpha}_{dj}), \qquad (1 \le j \le \ell)$$

provient des hyperplans ayant une équation de la forme

$$\sum_{k=1}^{d} \vartheta_k (z_k - z'_k) = 0,$$

avec $(\vartheta_1, \dots, \vartheta_d) \in \mathbb{C}^d \setminus \{0\}$ et $\eta = 1$.

Voici un exemple :

Proposition 4.1. *– Soient α_{ij}, $(1 \le i \le d,\ 1 \le j \le \ell)$ des nombres algébriques complexes non nuls. On suppose que si $s_1, \dots, s_\ell$, $a_1, \dots, a_d$, $a'_1, \dots, a'_d$ sont des nombres entiers tels que*

$$\prod_{i=1}^{d} \prod_{j=1}^{\ell} \alpha_{ij}^{a_i s_j} \overline{\alpha}_{ij}^{a'_i s_j} = 1,$$

alors ou bien $s_1 = \cdots = s_\ell = 0$, ou bien $a_1 = \cdots = a_d = a'_1 = \cdots = a'_d = 0$. On définit $\gamma_j = (\alpha_{1j}, \dots, \alpha_{dj}) \in (\overline{\mathbb{Q}}^\times)^d$, $(1 \le j \le \ell)$ et on désigne par Γ le sous-groupe de $(\overline{\mathbb{Q}}^\times)^d$ engendré par $\gamma_1, \dots, \gamma_\ell$.
a) Si Γ est dense dans $(\mathbb{C}^\times)^d$, alors $\ell \ge d+1$.
b) Si $\ell \ge d^2 + d + 1$, alors Γ est dense dans $(\mathbb{C}^\times)^d$.
c) Si $\ell \ge d^2 + 3d$, alors Γ contient un sous-groupe de rang $d+1$ qui est dense dans $(\mathbb{C}^\times)^d$.

Démonstration. La partie a) de l'énoncé résulte de l'égalité $\mathrm{m}\big((\mathbb{C}^\times)^d\big) = d+1$. Pour la partie b), on remarque que si G' est un sous-groupe algébrique de $\widetilde{G}$ tel que $\dim G' < \dim \widetilde{G}$, alors

$$\widetilde{Y} \cap T_{G'}(\mathbb{R}) = \widetilde{\Omega}_{\mathbb{R}} \cap T_{G'}(\mathbb{R}).$$

Pour le vérifier, on écrit qu'un élément

$$y = \sum_{j=1}^{\ell} s_j \varphi(y_j) + \sum_{k=1}^{d} t_k \varphi(2i\pi\epsilon_k)$$

de $\widetilde{Y}$ appartient à un sous-espace de $\mathbb{C}^{2d}$ rationnel sur $\mathbb{Q}$:

$$\sum_{\nu=1}^{d} (a_\nu z_\nu + a'_\nu z'_\nu) = 0,$$

avec $(a, a') \ne (0,0)$; on déduit de l'hypothèse d'indépendance multiplicative :

$$s_1 = \cdots = s_\ell = 0 \quad \text{et} \quad \sum_{\nu=1}^{d} (a_\nu - a'_\nu) t_\nu = 0,$$

ce qui donne $y \in \varphi\big((2i\pi\mathbb{Z})^d\big) = \widetilde{\Omega}_{\mathbb{R}}$.

Ainsi $Y' = \widetilde{Y}/\widetilde{Y} \cap T_{G'}(\mathbb{R})$ a pour rang

$$\mathrm{rang}_{\mathbb{Z}} Y' = \mathrm{rang}_{\mathbb{Z}} \widetilde{Y} - \mathrm{rang}_{\mathbb{Z}} \widetilde{\Omega}_{\mathbb{R}} \cap T_{G'}(\mathbb{R}) = \ell + \eta.$$

Enfin, comme $\eta \le 1$ et $\delta \le d + \eta$, l'hypothèse $\ell \ge d^2 + d + 1$ entraîne $\ell + \eta \ge \delta(\delta - 1) + 2$.

Pour démontrer la partie c) de la proposition 4.1, on utilise le théorème 7.2 du chapitre II pour $R = (\mathbb{C}^\times)^d$ avec $n = 2d$. Il s'agit de vérifier, si $\ell \ge d(d+3)$, que tout sous-groupe Γ_1 de Γ de rang $\ell_1 = \ell - 2d + 1$ est dense dans $(\mathbb{C}^\times)^d$. Soient $\gamma'_1, \dots, \gamma'_{\ell_1}$ des éléments $\mathbb{Q}$-linéairement indépendants de Γ :

$$\gamma'_\lambda = (\alpha'_{1\lambda}, \dots, \alpha'_{d\lambda}), \qquad \alpha'_{i\lambda} = \prod_{j=1}^{\ell} \alpha_{ij}^{m_{j\lambda}}, \qquad (1 \le \lambda \le \ell_1,\ 1 \le i \le d),$$

où la matrice entière $\big(m_{j\lambda}\big)_{1 \le j \le \ell, 1 \le \lambda \le \ell_1}$ est de rang ℓ_1. Alors pour $a_1, \dots, a_d$, $a'_1, \dots, a'_d$, $t_1, \dots, t_{\ell_1}$ dans $\mathbb{Z}$, la relation

$$\prod_{i=1}^{d} \prod_{\lambda=1}^{\ell_1} (\alpha'_{i\lambda})^{a_i t_\lambda} (\overline{\alpha}'_{i\lambda})^{a'_i t_\lambda} = 1$$

s'écrit

$$\prod_{i=1}^{d} \prod_{j=1}^{\ell} \alpha_{ij}^{a_i s_j} \overline{\alpha}_{ij}^{a'_i s_j} = 1,$$

avec

$$s_j = \sum_{\lambda=1}^{\ell_1} m_{j\lambda} t_\lambda, \qquad (1 \le j \le \ell).$$

Comme les conditions $s_1 = \cdots = s_\ell = 0$ et $t_1 = \cdots = t_{\ell_1} = 0$ sont équivalentes, on peut utiliser b) pour conclure que Γ_1 est dense dans $(\mathbb{C}^\times)^d$. $\square$

Problème. Sous les hypothèses de la proposition 4.1, et en admettant la conjecture 3.3?, peut-on déduire que Γ est dense dans $(\mathbb{C}^\times)^d$ dès que $\ell \ge d+1$?

Exercice. Soit Γ un sous-groupe de $(\overline{\mathbb{Q}}^\times)^2$ de rang 3. On suppose que Γ n'est pas dense dans $(\mathbb{C}^\times)^2$, mais que ses images par les applications $(z_1, z_2) \mapsto (z_1/|z_1|, z_2/|z_2|)$ et $(z_1, z_2) \mapsto (|z_1|, |z_2|)$ sont denses dans $\mathbb{U}^2$ et $(\mathbb{R}_+^\times)^2$ respectivement. Montrer qu'il existe une matrice carrée 3×3, à coefficients dans $\mathcal{L}$, de déterminant nul, dont les lignes sont linéairement indépendantes sur $\mathbb{Q}$, dont les colonnes sont aussi linéairement indépendantes sur $\mathbb{Q}$, et qui n'est pas de la forme PMQ avec P et Q dans $\mathrm{GL}_3(\mathbb{Q})$ et M antisymétrique.

Exercice. Soient $\alpha_1, \alpha_2, \alpha_3$ des nombres réels positifs et $\beta_1, \beta_2, \beta_3$ des nombres complexes non nuls. On suppose que les six nombres $\alpha_1, \alpha_2, \alpha_3$, $|\beta_1|, |\beta_2|, |\beta_3|$ sont multiplicativement *indépendants, et que les trois nombres $\beta_1/|\beta_1|$, $\beta_2/|\beta_2|$, $\beta_3|\beta_3|$ sont aussi multiplicativement indépendants. Montrer que le sous-groupe de $(\mathbb{C}^\times)^3$ de rang 4 engendré par*

$$\begin{pmatrix}1\\ \alpha_3\\ \alpha_2^{-1}\end{pmatrix},\quad \begin{pmatrix}\alpha_3^{-1}\\ 1\\ \alpha_1\end{pmatrix},\quad \begin{pmatrix}\alpha_2\\ \alpha_1^{-1}\\ 1\end{pmatrix},\quad \begin{pmatrix}\beta_1\\ \beta_2\\ \beta_3\end{pmatrix}$$

n'est pas dense dans $(\mathbb{C}^\times)^3$, mais que ses images par les deux projections $(z_1,z_2,z_3)\mapsto(z_1/|z_1|,z_2/|z_2|,z_3/|z_3|)$ et $(z_1,z_2,z_3)\mapsto(|z_1|,|z_2|,|z_3|)$ sont denses dans $\mathbb{U}^3$ et $(\mathbb{R}_+^\times)^3$ respectivement.

d) *Densité dans $\mathbb{C}^{d_0}\times(\mathbb{C}^\times)^{d_1}$ de sous-groupes de $\overline{\mathbb{Q}}^{d_0}\times(\overline{\mathbb{Q}}^\times)^{d_1}$*

On considère enfin le cas général où G est le groupe algébrique $\mathbb{G}_{\mathrm{a}}^{d_0}\times\mathbb{G}_{\mathrm{m}}^{d_1}$, de dimension $d=d_0+d_1$. En combinant les situations examinées dans les sous-sections a) et c), on introduit un groupe algébrique linéaire commutatif $\widetilde{G}$, défini sur $\mathbb{R}$, dont le groupe des points complexes $\widetilde{G}(\mathbb{C})$ est isomorphe à $G(\mathbb{C})\times G(\mathbb{C})$, dont le groupe des points réels $\widetilde{G}(\mathbb{R})$ est isomorphe à $G(\mathbb{C})$. On désigne par ϕ l'application de $G(\mathbb{C})$ dans $\widetilde{G}(\mathbb{C})$ qui envoie $t\in G(\mathbb{C})$ sur $\phi(t)=(t,\bar t)\in\widetilde{G}(\mathbb{C})$, de sorte que $\widetilde{G}(\mathbb{R})=\phi\bigl(G(\mathbb{C})\bigr)$. Pour Γ sous-groupe de $G(\mathbb{C})$, $\widetilde{\Gamma}=\phi(\Gamma)$ sera l'image de Γ dans $\widetilde{G}(\mathbb{R})$.

On note ensuite $\varphi:\mathbb{C}^d\to\mathbb{C}^{2d}$ l'application qui envoie $z\in T_G(\mathbb{C})$ sur $(z,\overline{z})\in T_{\widetilde{G}}(\mathbb{C})$. L'image de φ est l'espace tangent à l'origine $T_{\widetilde{G}}(\mathbb{R})$ de $\widetilde{G}(\mathbb{R})$. Enfin $\exp_{\widetilde{G},\mathbb{R}}$ sera la restriction à $T_{\widetilde{G}}(\mathbb{R})$ de l'application exponentielle de $\widetilde{G}$. Quand on sépare la partie additive de la partie multiplicative, on écrit

$$\widetilde{G}(\mathbb{C})=\bigl\{(u,v;u',v')\,;\,(u,u')\in(\mathbb{C}^{d_0})^2,\ (v,v')\in\bigl((\mathbb{C}^\times)^{d_1}\bigr)^2\bigr\},$$

$$T_{\widetilde{G}}(\mathbb{C})=\bigl\{(z_0,z_1;z_0',z_1')\,;\,(z_0,z_0')\in(\mathbb{C}^{d_0})^2,\ (z_1,z_1')\in(\mathbb{C}^{d_1})^2\bigr\},$$

et

$$\widetilde{G}(\mathbb{R})=\bigl\{(u,v;\overline{u},\overline{v})\,;\,u\in\mathbb{C}^{d_0},\ v\in(\mathbb{C}^\times)^{d_1}\bigr\},$$

$$T_{\widetilde{G}}(\mathbb{R})=\bigl\{(z_0,z_1;\overline{z}_0,\overline{z}_1)\,;\,z_0\in\mathbb{C}^{d_0},\ z_1\in\mathbb{C}^{d_1}\bigr\}.$$

Le noyau de

$$\begin{array}{rccc}\exp_{\widetilde{G}}: & T_{\widetilde{G}}(\mathbb{C}) & \longrightarrow & \widetilde{G}(\mathbb{C})\\ & (z_0,z_1;z_0',z_1') & \longmapsto & \bigl(z_0,\exp(z_1);z_0',\exp(z_1')\bigr)\end{array}$$

est $\widetilde{\Omega}_{\mathbb{C}}=\bigl(\{0\}^{d_0}\times(2i\pi\mathbb{Z})^{d_1}\bigr)^2$, sous-groupe discret de $\mathbb{C}^{2d}$ de rang $2d_1$ tandis que celui de

$$\begin{array}{rccc}\exp_{\widetilde{G},\mathbb{R}}: & T_{\widetilde{G}}(\mathbb{R}) & \longrightarrow & \widetilde{G}(\mathbb{R})\\ & (z_0,z_1;\overline{z}_0,\overline{z}_1) & \longmapsto & \bigl(z_0,\exp(z_1);\overline{z}_0,\exp(\overline{z}_1)\bigr)\end{array}$$

est $\widetilde{\Omega}_{\mathbb{R}}=\{0\}^{d_0}\times(2i\pi\mathbb{Z})^{d_1}$, sous-groupe discret de $\mathbb{C}^d$ de rang d_1. On en déduit

$$\mathrm{m}_{\mathbb{C}}(\widetilde{G})=\mathrm{m}\bigl(\widetilde{G}(\mathbb{C})\bigr)=4d_0+2d_1+1,\qquad \mathrm{m}_{\mathbb{R}}(\widetilde{G})=\mathrm{m}\bigl(\widetilde{G}(\mathbb{R})\bigr)=2d_0+d_1+1.$$

Noter aussi que l'on a $\mathrm{m}_{\mathbb{C}}(G)=\mathrm{m}\bigl(G(\mathbb{C})\bigr)=\mathrm{m}_{\mathbb{R}}(\widetilde{G})=2d_0+d_1+1$.

Si G' est un sous-groupe algébrique de $\widetilde{G}$, le quotient $\widetilde{G}/G'$ est un produit $\mathbb{G}_a^{\delta_0}\times\mathbb{G}_m^{\delta_1}$, où $\delta=\delta_0+\delta_1$ est la codimension de G' dans $\widetilde{G}$. Enfin on a

$$\mathrm{m}_{\mathbb{R}}(\widetilde{G}/G')=\dim(\widetilde{G}/G')-\mathrm{rang}_{\mathbb{Z}}\bigl(\mathrm{Ker}\ \exp_{\widetilde{G}/G',\mathbb{R}}\bigr)+1.$$

On pose encore

$$\mathrm{m}'_{\mathbb{R}}(\widetilde{G}/G')=\begin{cases}\delta_1(\delta-1)+2 & \text{si } \mathrm{rang}_{\mathbb{Z}}\bigl(\widetilde{\Omega}_{\mathbb{R}}\cap T_{G'}(\mathbb{R})\bigr)\ge d_1-1,\\ 0 & \text{si } \mathrm{rang}_{\mathbb{Z}}\bigl(\widetilde{\Omega}_{\mathbb{R}}\cap T_{G'}(\mathbb{R})\bigr)< d_1-1.\end{cases}$$

Soit Γ un sous-groupe de type fini de $G(\mathbb{C})$ et soit $Y=\exp_G^{-1}(\Gamma)\subset\mathbb{C}^d$ l'image inverse de Γ par $\exp_G$; alors $\varphi(Y)=\widetilde{Y}=\exp_{\widetilde{G}}^{-1}(\widetilde{\Gamma})\subset T_{\widetilde{G}}(\mathbb{R})$ est l'image inverse de $\widetilde{\Gamma}$ par $\exp_{\widetilde{G},\mathbb{R}}$, et on a équivalence entre les assertions

(i) Γ est dense dans $G(\mathbb{C})$.
(ii) Y est dense dans $\mathbb{C}^d$.
(iii) $\widetilde{Y}$ est dense dans $T_{\widetilde{G}}(\mathbb{R})$.
(iv) $\widetilde{\Gamma}$ est dense dans $\widetilde{G}(\mathbb{R})$.

Noter que Γ et $\widetilde{\Gamma}$ ont le même rang, disons ℓ, tandis que Y et $\widetilde{Y}$ sont de rang $\ell+d_1$.

Proposition 4.2. – *Soit Γ un sous-groupe de type fini de $G(\overline{\mathbb{Q}})$.*
a) Si Γ est dense (pour la topologie complexe) dans $G(\mathbb{C})$, alors pour tout sous-groupe algébrique de $\widetilde{G}$ défini sur $K=\overline{\mathbb{Q}}\cap\mathbb{R}$ vérifiant $\dim G'<\dim\widetilde{G}$, on a

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

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

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

Alors Γ est dense dans le groupe topologique $G(\mathbb{C})$.
c) On suppose, pour tout sous-groupe algébrique G' de $\widetilde{G}$ défini sur K avec $\dim G'<\dim\widetilde{G}$,

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

Alors il existe un sous-groupe de Γ de rang $\mathrm{m}_{\mathbb{C}}(G)$ qui est dense dans $G(\mathbb{C})$.
d) Supposons que la conjecture 3.3? est vraie ; soient $\gamma_1,\dots,\gamma_\ell$ des éléments de Γ linéairement indépendants sur $\mathbb{Z}$ avec $\ell=\mathrm{rang}_{\mathbb{Z}}\Gamma$; désignons par H l'adhérence de Zariski dans $\widetilde{G}^\ell$ du sous-groupe $\mathbb{Z}(\gamma_1,\dots,\gamma_\ell,\overline{\gamma}_1,\dots,\overline{\gamma}_\ell)$. Alors Γ est dense dans $G(\mathbb{C})$ si et seulement s'il existe $(\eta_1,\dots,\eta_\ell,\overline{\eta}_1,\dots,\overline{\eta}_\ell)\in H(\mathbb{R})$ tel que $\mathbb{Z}\eta_1+\dots+\mathbb{Z}\eta_\ell$ soit dense dans $G(\mathbb{C})$.

Exemple. Prenons $d_0 = 0$, $d_1 = 1$; pour un sous-groupe algébrique G' de $\widetilde{G}$ défini sur $\mathbb{R}$ de dimension 1 (et de codimension $\delta = \delta_1 = 1$), on a

$$\mathrm{m}_{\mathbb{R}}(\widetilde{G}/G') = \begin{cases} 1 & \text{si } G'(\mathbb{R})^0 \simeq \mathbb{R}_+^\times, \\ 2 & \text{si } G'(\mathbb{R}) \simeq \mathbb{U}, \end{cases} \qquad \mathrm{m}'_{\mathbb{R}}(\widetilde{G}/G') = 2,$$

tandis que pour un sous-groupe algébrique G' de $\widetilde{G}$ de dimension 0 (et de codimension $\delta = \delta_1 = 2$), on a

$$\mathrm{m}_{\mathbb{R}}(\widetilde{G}/G') = 3, \qquad \mathrm{m}'_{\mathbb{R}}(\widetilde{G}/G') = 4.$$

Le lemme 1.11 permet alors de déduire les parties b) et c) du théorème 1.10 de la proposition 4.2.

Exercice. Soit Γ un sous-groupe de type fini de $G(\overline{\mathbb{Q}})$. On suppose qu'il existe des éléments $\gamma_1, \dots, \gamma_{\ell'}$, (avec $\ell' \geq \ell = \mathrm{rang}_{\mathbb{Z}}\Gamma$), qui engendrent un sous-groupe d'indice fini de Γ, et qui vérifient la propriété suivante :

il existe $(\eta_1, \dots, \eta_{\ell'}, \overline{\eta}_1, \dots, \overline{\eta}_{\ell'}) \in H(\mathbb{R})$, où H désigne l'adhérence de Zariski dans $\widetilde{G}^{\ell'}$ du sous-groupe $\mathbb{Z}(\gamma_1, \dots, \gamma_\ell, \overline{\gamma}_1, \dots, \overline{\gamma}_{\ell'})$, tel que $\mathbb{Z}\eta_1 + \cdots + \mathbb{Z}\eta_{\ell'}$ soit dense dans $G(\mathbb{C})$.

Montrer que toute famille $\gamma_1, \dots, \gamma_{\ell'}$ d'éléments de Γ qui engendre un sous-groupe d'indice fini vérifie la même propriété.

Démonstration de la proposition 4.2. On désigne par $Y \subset T_G(\mathbb{R})$ l'image inverse de Γ par $\exp_G$. Si Γ est de rang ℓ, alors Y est de rang $\ell + d_1$, car le noyau de $\exp_G$, qui est $\widetilde{\Omega}_{\mathbb{R}} = \{0\}^{d_0} \times (2i\pi\mathbb{Z})^{d_1}$, est de rang d_1 sur $\mathbb{Z}$. Posons, pour $1 \leq k \leq d_1$,

$$\epsilon_k = (0, \dots, 0, \delta_{1k}, \dots, \delta_{d_1 k}) \in \{0\}^{d_0} \times \mathbb{Z}^{d_1}.$$

Alors l'image inverse dans $T_{\tilde{G}}(\mathbb{R})$ de Γ par $\exp_{\tilde{G},\mathbb{R}}$ est

$$Y = \mathbb{Z}y_1 + \cdots + \mathbb{Z}y_\ell + \mathbb{Z}2i\pi\epsilon_1 + \cdots + \mathbb{Z}2i\pi\epsilon_{d_1} = \mathbb{Z}y_1 + \cdots + \mathbb{Z}y_\ell + \widetilde{\Omega}_{\mathbb{R}}.$$

b) Pour vérifier que $\widetilde{Y}$ est dense dans $T_{\tilde{G}}(\mathbb{R})$ on utilise la proposition 6.2 du chapitre II : il s'agit de vérifier que, pour tout hyperplan complexe de $T_{\tilde{G}}(\mathbb{C})$, le rang de $\widetilde{Y}/\widetilde{Y} \cap H$ est ≥ 2. Comme $\widetilde{Y}$ contient $\widetilde{\Omega}_{\mathbb{R}}$, on peut supposer que $\widetilde{\Omega}_{\mathbb{R}}/\widetilde{\Omega}_{\mathbb{R}} \cap H$ est lui-même de rang ≤ 1, c'est-à-dire que $\widetilde{\Omega}_{\mathbb{R}} \cap H$ est de rang $\geq d_1 - 1$. Dans ce cas soit G' le plus grand sous-groupe algébrique connexe de $\widetilde{G}$, défini sur K, tel que $T_{G'}(\mathbb{C})$ soit contenu dans H. Alors $T_{G'}(\mathbb{R})$ contient $\widetilde{\Omega}_{\mathbb{R}} \cap H$, et

$$\mathrm{rang}_{\mathbb{Z}}\big(\widetilde{\Omega}_{\mathbb{R}} \cap T_{G'}(\mathbb{R})\big) \geq d_1 - 1.$$

Par hypothèse le rang du sous-groupe $\Gamma' = \widetilde{\Gamma}/\widetilde{\Gamma} \cap G'(K)$ de $\widetilde{G}(K)/G'(K)$ est $\geq \delta_1(\delta - 1) + 2$. Or Γ' est l'image, par l'exponentielle de $(\widetilde{G}/G')(\mathbb{R})$, de $Y' = \widetilde{Y}/\widetilde{Y} \cap T_{G'}(\mathbb{R})$. Par conséquent on a

$$\mathrm{rang}_{\mathbb{Z}} Y' \geq \delta_1(\delta - 1) + 2.$$

On applique maintenant le théorème 2.6 à $\mathcal{V} = H/T_{G'}(\mathbb{C})$:

$$\mathrm{rang}_{\mathbb{Z}}\big(Y' \cap \mathcal{V}\big) \leq \dim_{\mathbb{Q}}\big(\mathcal{V} \cap \mathcal{L}(G)\big) \leq \delta_1(\delta - 1).$$

Ainsi on peut conclure

$$\mathrm{rang}_{\mathbb{Z}}\big(\widetilde{Y}/\widetilde{Y} \cap H\big) = \mathrm{rang}_{\mathbb{Z}}\big(Y'/Y' \cap \mathcal{V}\big) \geq 2$$

c) La partie c) de la proposition 4.2 résulte de b), grâce au théorème 7.2 du chapitre II.
d) Si Γ est dense dans $G(\mathbb{C})$, il suffit de prendre $(\eta_1, \dots, \eta_\ell) = (\gamma_1, \dots, \gamma_\ell)$ pour vérifier la condition énoncée. Supposons inversement que Γ n'est pas dense dans $G(\mathbb{C})$. D'après la proposition 6.1 du chapitre II, il existe des entiers $(s_1, \dots, s_\ell; t_1, \dots, t_{d_1})$, non tous nuls, tels que la matrice suivante soit de rang $\leq 2d$:

$$\begin{pmatrix} y_1 & \cdots & y_\ell & 2i\pi\epsilon_1 & \cdots & 2i\pi\epsilon_{d_1} \\ \overline{y}_1 & \cdots & \overline{y}_\ell & -2i\pi\epsilon_1 & \cdots & -2i\pi\epsilon_{d_1} \\ s_1 & \cdots & s_\ell & t_1 & \cdots & t_{d_1} \end{pmatrix}$$

On a noté, pour alléger l'écriture, y_j pour le vecteur colonne de composantes

$$(\beta_{1j}, \dots, \beta_{d_0 j}, \log\alpha_{1j}, \dots, \log\alpha_{d_1 j}),$$

$\overline{y}_j$ a pour composantes les conjugués des coordonnées de y_j, et $2i\pi\epsilon_k$ est le vecteur colonne dont les composantes sont les coordonnées de $2i\pi\epsilon_k$.

Maintenant on choisit une base $\theta_1, \dots, \theta_{r+1}$ du $\mathbb{Q}$-espace vectoriel engendré par $2i\pi$ et les $d_1\ell$ nombres $\log\alpha_{kj}$, $(1 \leq k \leq d_1,\ 1 \leq j \leq \ell)$, avec $\theta_{r+1} = 2i\pi$. On écrit chaque $\log\alpha_{kj}$ comme combinaison linéaire de $\theta_1, \dots, \theta_{r+1}$ à coefficients rationnels :

$$\log\alpha_{kj} = \sum_{\varrho=1}^{r+1} b_{kj\varrho}\theta_\varrho.$$

Pour chaque $x = (x_0, x_1, \dots, x_r) \in \mathbb{C}^{r+1}$, on définit $\xi_j(x) \in \mathbb{C}^d$ par

$$\xi_j(x) = \Big(x_0\beta_{1j}, \dots, x_0\beta_{d_0 j}, \sum_{\varrho=1}^{r+1} b_{1j\varrho}x_\varrho, \dots, \sum_{\varrho=1}^{r+1} b_{d_1 j\varrho}x_\varrho\Big)$$

avec $x_{r+1} = 2i\pi$. La composante connexe $H(\mathbb{R})^0$ du groupe des points réels de l'adhérence de Zariski H à laquelle il est fait allusion dans d) est l'image par $\exp_{\tilde{G}^\ell,\mathbb{R}}$ du sous-groupe

$$\Big\{\big(\xi_j(x), \overline{\xi}_j(x)\big)_{1 \leq j \leq \ell}\,;\ x \in \mathbb{C}^{r+1}\Big\} \subset T_{\tilde{G}}(\mathbb{R})^\ell.$$

La proposition 4.2 se déduit facilement de ces arguments. $\square$

Exercice. Déduire la proposition 4.1 de la proposition 4.2.
`Indication.` *Soit $G = \mathbb{G}_{\mathrm{m}}^d$. Vérifier que pour tout sous-groupe algébrique G' de $\widetilde{G}$ défini sur $\mathbb{R}$, on a*

$$\mathrm{m}'_{\mathbb{R}}(\widetilde{G}/G') \leq d^2 + d + 2;$$

de plus, si $T_{G'}(\mathbb{R})$ contient $\widetilde{\Omega}_{\mathbb{R}}$, alors

$$\mathrm{m}'_{\mathbb{R}}(\widetilde{G}/G') \leq d^2 - d + 2.$$

§5. Le plongement canonique d'un corps de nombres

Une autre application concernant encore un groupe linéaire (tore non déployé) provient de questions posées par Colliot-Thélène, Coray et Sansuc, et dont la solution a été donnée par D. Roy dans [R 1992b].

Proposition 5.1. – *Soient k un corps de nombres, $\sigma_1, \ldots, \sigma_{r_1}$ des plongements distincts de k dans $\mathbb{R}$ et $\sigma_{r_1+1}, \ldots, \sigma_{r_1+2r_2}$ des plongements distincts de k dans $\mathbb{C}$ avec $\sigma_{r_1+r_2+i} = \overline{\sigma}_{r_1+i}$ pour $1 \le i \le r_2$. On pose*

$$\sigma = (\sigma_1, \ldots, \sigma_{r_1+r_2}) : k^\times \to (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}.$$

Soient $\gamma_1, \ldots, \gamma_\ell$ des éléments de $k^\times$; on suppose que les $(r_1 + 2r_2)\ell$ nombres

$$\sigma_i\gamma_j, \qquad (1 \le i \le r_1 + 2r_2,\ 1 \le j \le \ell)$$

sont multiplicativement indépendants. On désigne par Γ le sous-groupe multiplicatif de $k^\times$ engendré par $\gamma_1, \ldots, \gamma_\ell$ et par $\sigma(\Gamma)$ son image dans $(\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$.
a) On suppose

$$\ell \ge \begin{cases} r_1(r_1-1)+2 & \text{si } r_2 = 0, \\ (r_1+r_2)(r_1+r_2+1)+1 & \text{si } r_2 \ge 1\,; \end{cases}$$

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 (*)

$$\ell \ge \begin{cases} r_1^2+1 & \text{si } r_2 = 0, \\ (r_1+r_2+1)^2+r_2-1 & \text{si } r_2 \ge 1\,; \end{cases}$$

alors il existe un sous-groupe de $\sigma(\Gamma)$, de rang r_1+r_2+1, dont l'image par σ est dense dans $(\mathbb{R}_+^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$.
c) Si la conjecture 3.3? est vraie, 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 $\ell \ge r_1+r_2+1$.

On a toujours $r_1 + 2r_2 \le [k:\mathbb{Q}]$, avec égalité quand on prend tous les plongements de k dans $\mathbb{C}$ (alors σ est le *plongement canonique*). On retrouve les exemples considérés dans le paragraphe 1 en prenant $r_1 + 2r_2 = [k:\mathbb{Q}] = 2$:

∗ si le corps quadratique k est réel ($r_1 = 2$, $r_2 = 0$), alors
– le théorème des six exponentielles montre que pour $\ell \ge 4$, l'adhérence de l'image de Γ dans $(\mathbb{R}^\times)^2$ contient $(\mathbb{R}_+^\times)^2$; de plus, pour $\ell \ge 5$, 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 $\ell \ge 3$, 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 $\ell \ge 3$, $\sigma(\Gamma)$ est dense dans $\mathbb{C}^\times$ et pour $\ell \ge 4$, 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 $\ell \ge 2$, le sous-groupe Γ de $k^\times$ a une image dense dans $\mathbb{C}^\times$.

(*) Ceci corrige la remarque à la fin de la section 4c de [W 1994]. où $(r_1+r_2+1)^2+r_2-1$ a été malencontreusement remplacé par $(r_1+r_2+1)^2+1$ – voir [W 1995].

Démonstration de la proposition 5.1. On peut commencer par remarquer que le cas $r_2 = 0$ résulte du corollaire 2.11 avec $d_0 = 0$, $d_1 = d$, tandis que le cas $r_1 = 0$ est une conséquence de la proposition 4.1.

Passons au cas général. On pose $\widetilde{G} = \mathbb{G}_m^{r_1} \times \widetilde{\mathbb{G}_m^{r_2}}$, où $\widetilde{\mathbb{G}_m^{r_2}}$ a été défini dans le paragraphe 4 :

$$\widetilde{\mathbb{G}_m^{r_2}}(\mathbb{C}) \simeq (\mathbb{C}^\times)^{2r_2}, \quad \widetilde{\mathbb{G}_m^{r_2}}(\mathbb{R}) \simeq (\mathbb{C}^\times)^{r_2}.$$

Ainsi

$$\widetilde{G}(\mathbb{C}) \simeq (\mathbb{C}^\times)^{r_1+2r_2}, \quad \widetilde{G}(\mathbb{R}) \simeq (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}.$$

On a encore

$$T_{\widetilde{G}(\mathbb{C})} = \mathbb{C}^{r_1+2r_2} \supset T_{\widetilde{G}(\mathbb{R})} \simeq \mathbb{R}^{r_1+2r_2}.$$

Le noyau de $\exp_{\widetilde{G}}$ est $(2i\pi\mathbb{Z})^{r_1+2r_2}$, celui de sa restriction $\exp_{\widetilde{G},\mathbb{R}}$ à $T_{\widetilde{G}(\mathbb{R})}$ est isomorphe à $(2i\pi\mathbb{Z})^{r_2}$; on notera ce dernier $\widetilde{\Omega}_\mathbb{R}$.

On désigne par Y le sous-groupe de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ de rang $\ell + r_2$ qui est l'image inverse par l'application exponentielle de $\sigma(\Gamma)$. On définit ensuite $\widetilde{Y} \subset \mathbb{R}^{r_1+2r_2}$ et on considère un hyperplan H de $\mathbb{R}^{r_1+2r_2}$ d'équation

$$t_1x_1 + \cdots + t_{r_1}x_{r_1} + u_1y_1 + \cdots + u_{r_2}y_{r_2} + u'_1y'_1 + \cdots + u'_{r_2}y'_{r_2} = 0.$$

Il s'agit de vérifier $\mathrm{rang}_\mathbb{Z}(\widetilde{Y}/\widetilde{Y} \cap H) \ge 2$. On définit G' comme le sous-groupe algébrique connexe de dimension maximale de $\widetilde{G}$ tel que $T_{G'}(\mathbb{C})$ soit contenu dans H. Le rang de $H \cap \widetilde{\Omega}_\mathbb{R}$ sera noté $r_2 - \eta$. On peut supposer $\eta = 0$ ou 1, sinon le résultat est banal, puisque $\widetilde{\Omega}_\mathbb{R} \subset \widetilde{Y}$. De plus, si $r_2 = 0$, alors $\eta = 0$. Comme $T_{G'}(\mathbb{R})$ contient $H \cap \widetilde{\Omega}_\mathbb{R}$, la dimension de G' est au moins $r_2 - \eta$. Les hypothèses faites sur l'indépendance multiplicative des nombres $\sigma_i(\gamma_j)$ permettent de vérifier

$$\widetilde{Y} \cap T_{G'}(\mathbb{R}) = \widetilde{\Omega}_\mathbb{R} \cap T_{G'}(\mathbb{R}).$$

Alors le rang de $Y' = \widetilde{Y}/\widetilde{Y} \cap T_{G'}(\mathbb{R})$ est $\ell + \eta$. Soit δ la codimension de G' dans $\widetilde{G}$: on a $\widetilde{G}/G' \simeq \mathbb{G}_m^\delta$ avec $\delta \le r_1 + r_2 + \eta$. On pose encore $\mathcal{V} = H/T_{G'}(\mathbb{C})$. Le théorème du sous-groupe linéaire assure

$$\mathrm{rang}_\mathbb{Z}(Y' \cap \mathcal{V}) \le \delta(\delta - 1).$$

Mais d'une part on a

$$\mathrm{rang}_\mathbb{Z}\bigl(\widetilde{Y}/\widetilde{Y} \cap H\bigr) = \mathrm{rang}_\mathbb{Z}(Y'/Y' \cap \mathcal{V}),$$

et d'autre part on déduit de l'hypothèse sur ℓ et de la majoration $\delta \le r_1 + r_2 + \eta$ avec $\eta = 0$ ou 1 que l'on a $\ell + \eta \ge \delta(\delta-1)+2$. On peut donc conclure $\mathrm{rang}_\mathbb{Z}\bigl(\widetilde{Y}/\widetilde{Y} \cap H\bigr) \ge 2$. □

Remarques. Cela n'épuise pas le sujet. Il serait bon d'étudier le cas des groupes algébriques linéaires plus en détail : d'une part voir ce qui se passe dans le cas des groupes commutatifs non déployés, d'auéaires non commutatifs. Enfin nous reviendrons au chapitre V sur l'aspect quantitatif et les mesures de densité effectives.

IV. – Le problème de densité pour les groupes algébriques

Dans ce chapitre on étend la discussion faite pour les groupes linéaires dans le chapitre précédent à tous les groupes algébriques commutatifs. On commence par le cas facile des courbes elliptiques sur $\mathbb{R}$. On continue avec le cas général (sur $\mathbb{R}$), et on étudie ensuite plus en détail la situation pour les variétés abéliennes. La fin du chapitre est consacrée au problème de densité complexe.

On utilisera encore un résultat de la théorie des nombres transcendants — le théorème 2.3* (théorème du sous-groupe algébrique) — pour démontrer le théorème principal de ce chapitre, le théorème 2.2. La situation conjecturale est moins facile que pour les groupes algébriques linéaires (cf. [Be 1995]).

§1. Courbes elliptiques sur un corps de nombres réel

Soit E une courbe elliptique sur $\mathbb{Q}$. Le groupe de Mordell-Weil $E(\mathbb{Q})$ est soit fini (i.e. de rang nul), soit infini (de rang ≥ 1). Le groupe $E(\mathbb{R})$ est soit connexe, soit composé de deux composantes connexes ; quand la courbe est écrite sous forme de Weierstraß $y^2 = 4x^3 - g_2x - g_3$, il y a deux composantes connexes si et seulement si le polynôme $4x^3 - g_2x - g_3$ a trois racines réelles, ce qui revient encore à dire que le discriminant $\Delta = g_2^3 - 27g_3^2$ est > 0. La composante connexe de l'élément neutre $E(\mathbb{R})^0$ n'est pas bornée. Les points rationnels de la courbe peuvent être en nombre fini, ou bien denses dans $E(\mathbb{R})$, ou encore, quand il y a deux composantes connexes, être denses sur une seulement de ces deux composantes (et absents sur l'autre). Voici un exemple explicite de chacune de ces situations.

- Pour p premier congru à 7 ou à 11 modulo 16, la courbe $y^2 = x^3 + px$ a une seule composante connexe, et un nombre fini de points rationnels (cf. [Sil 1986], Chap.10 §6, p.314).
- La courbe elliptique d'équation $y^2 = x^3 - x$ a un groupe de Mordell-Weil sur $\mathbb{Q}$ isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, et possède deux composantes connexes réelles ; les points rationnels ne sont denses dans aucune des deux composantes.
- La courbe elliptique $y^2 = x^3 + 877x$ a une seule composante connexe réelle, dans laquelle les points rationnels sont denses ; cet exemple a été étudié par Bremner et Cassels ; le groupe de Mordell-Weil $E(\mathbb{Q})$ est de rang 1 ; un générateur explicite est reproduit dans [Sil 1986], Chap.8 §10, p.235.
- La courbe elliptique $y^2 = x(x-2)(x-10)$ a deux composantes connexes réelles, et les points rationnels sont denses dans chacune des deux composantes [Sil 1986], Chap.10

§1, exemple 1.5. Un autre exemple semblable est celui de la courbe $y^2 = x(x-3)(x+32)$ illustré dans [R-H 1994].

- Il reste à donner un exemple d'une courbe elliptique sur $\mathbb{Q}$ ayant deux composantes connexes, où les points rationnels sont denses seulement dans l'une d'elles. En réponse à une question de N. A'Campo, D.W. Masser m'a indiqué la référence [NZM 1991]dans laquelle on trouve (à la fin du §5.7, p.294) l'exemple attribué à A. Bremner de la courbe $y^2 = x^3 + 6x^2 + 2x$ qui a deux composantes connexes réelles, dont l'une, bornée, ne contient pas de point rationnel, tandis que les multiples du point $(x = 1, y = 3)$ sont denses sur l'autre. Un autre exemple similaire m'a été indiqué par J-L. Colliot-Thélène : sur la courbe $y^2 = (x-14)(x^2-128)$, le point $(x = 16, y = 16)$ est d'ordre infini, mais la composante connexe bornée ne contient pas de point rationnel.

Le tableau suivant résume certains de ces exemples ; dans la deuxième colonne, le nombre N représente le nombre de composantes connexes de $E(\mathbb{R})$, qui est l'indice de $E(\mathbb{R})^0$ dans $E(\mathbb{R})$.

E	N	$E(\mathbb{Q})$
$y^2 = x^3 + 7x$	1	fini
$y^2 = x^3 - x$	2	fini
$y^2 = x^3 + 877x$	1	dense dans $E(\mathbb{R})$
$y^2 = x(x-2)(x-10)$	2	dense dans $E(\mathbb{R})$
$y^2 = x^3 + 6x^2 + 2x$	2	dense dans $E(\mathbb{R})^0$

Le problème de Mazur est facilement résolu pour une courbe elliptique ; en fait l'arithmétique n'intervient pas (on utilise le théorème 1.1 du chapitre II, mais il n'est pas nécessaire de supposer que les points sont rationnels sur $\mathbb{Q}$) :

Proposition 1.1. – *Soient E une courbe elliptique sur $\mathbb{R}$, γ un point d'ordre infini sur $E(\mathbb{R})$ et $\Gamma = \mathbb{Z}\gamma$ le sous-groupe qu'il engendre. Alors l'adhérence de Γ dans $E(\mathbb{R})$ pour la topologie réelle est une réunion de composantes (donc soit $E(\mathbb{R})$, soit $E(\mathbb{R})^0$).*

En particulier, si k est un corps de nombres, alors $E(k)$ est un groupe abélien de type fini, donc $E(k)$ est infini si et seulement s'il contient un élément d'ordre infini ; on peut alors appliquer la proposition 1.1 : si $E(k)$ est infini, c'est-à-dire si le groupe de Mordell-Weil $E(k)$ est de rang ≥ 1, son adhérence dans $E(\mathbb{R})$ est soit $E(\mathbb{R})$, soit $E(\mathbb{R})^0$.

Démonstration. Comme $E(\mathbb{R})^0$ est un sous-groupe d'indice 1 ou 2 de $E(\mathbb{R})$, l'hypothèse que Γ est infini montre que $\Gamma_0 = \Gamma \cap E(\mathbb{R})^0$ est aussi infini. Commençons par montrer que Γ_0 est dense dans $E(\mathbb{R})^0$.

On utilise la paramétrisation des points complexes de E par la fonction $\wp$ de Weierstrass. Comme g_2 et g_3 sont réels, l'intersection du réseau $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ de $\mathbb{C}$

avec $\mathbb{R}$ est un $\mathbb{Z}$-module de rang 1 ; on note ω le générateur positif. La restriction de l'exponentielle complexe $(1:\wp:\wp')$ à $\mathbb{R}$ induit un isomorphisme de groupes de Lie entre $\mathbb{R}/\mathbb{Z}\omega$ et $E(\mathbb{R})^0$. L'image inverse de Γ_0 est un sous-groupe G de $\mathbb{R}/\mathbb{Z}$ engendré par un élément d'ordre infini ; il résulte alors immédiatement du théorème 1.1 du chapitre II que G est dense dans $\mathbb{R}/\mathbb{Z}$, donc que Γ_0 est dense dans $E(\mathbb{R})^0$.

Si $E(\mathbb{R})$ est connexe, alors $\Gamma=\Gamma_0$ est dense dans $E(\mathbb{R})=E(\mathbb{R})^0$. Si $E(\mathbb{R})$ n'est pas connexe et que Γ possède un point dans $E(\mathbb{R})\setminus E(\mathbb{R})^0$ (c'est la composante connexe de $E(\mathbb{R})$ qui ne contient pas l'élément neutre), alors de nouveau Γ est dense dans $E(\mathbb{R})$. Enfin si $E(\mathbb{R})$ n'est pas connexe et que Γ ne possède pas de point dans $E(\mathbb{R})\setminus E(\mathbb{R})^0$, alors l'adhérence réelle de $\Gamma=\Gamma_0$ est $E(\mathbb{R})^0$. □

Les deux exemples suivants, empruntés au livre de J.E. Cremona : *Algorithms for modular elliptic curves,* Cambridge Univ. Press., 1992, sont cités par L. Wang [Wa 1995] :

- *Si E est la courbe elliptique d'équation $y^2=x^3-50x-125$ et K le corps quadratique réel $\mathbb{Q}(\sqrt{10})$, alors les groupes de Mordell-Weil $E(K)$ et $E(\mathbb{Q})$ ont tous deux pour rang* 1.
- *Soit E la courbe elliptique d'équation $y^2=x^3-8x+8$ et soit K le corps quadratique imaginaire $\mathbb{Q}(i)$. Alors les groupes de Mordell-Weil $E(K)$ et $E(\mathbb{Q})$ ont tous deux pour rang* 1.

Ces exemples montrent que la conjecture de Mazur ne s'étend pas sans précaution aux corps de nombres. Le deuxième exemple montre que $E(K)$ peut être dense pour la topologie de Zariski dans $E(\mathbb{C})$ sans être dense pour la topologie complexe.

La conjecture de Mazur est triviale non seulement pour une courbe elliptique, mais aussi pour une puissance d'une courbe elliptique :

Proposition 1.2. – *Soient E une courbe elliptique définie sur $\mathbb{R}$ et d un entier positif. On désigne par A la variété abélienne E^d.*
a) Si Γ est un sous-groupe de type fini de $A(\mathbb{R})$, alors $\Gamma\cap A(\mathbb{R})^0$ est dense dans $A(\mathbb{R})^0$ si et seulement si la projection de Γ sur tout quotient $(A/A')(\mathbb{R})$, A' sous-variété abélienne de A de dimension $d-1$, est dense dans $(A/A')(\mathbb{R})^0$.
b) Un point $(\delta_1,\dots,\delta_d)$ de $A(\mathbb{R})^0$ engendre un sous-groupe dense de $A(\mathbb{R})^0$ si et seulement si $\delta_1,\dots,\delta_d$ sont linéairement indépendants sur $\mathbb{Z}$ dans $E(\mathbb{R})$.

Démonstration. Soit $\exp_{E,\mathbb{R}}:\mathbb{R}\to E(\mathbb{R})^0$ l'application exponentielle de $E(\mathbb{R})$, et soit $\omega\in\mathbb{R}^\times$ un générateur du $\mathbb{Z}$-module $\mathrm{Ker}\ \exp_{E,\mathbb{R}}$.
a) Soient $\gamma_1,\dots,\gamma_\ell$ des générateurs du $\mathbb{Z}$-module $\Gamma\cap A(\mathbb{R})^0$. Pour $1\le j\le\ell$, choisissons $y_j\in\mathbb{R}^d$ vérifiant $\exp_{A,\mathbb{R}}(y_j)=\gamma_j$, de telle sorte que l'image inverse par $\exp_{A,\mathbb{R}}$ du sous-groupe $\Gamma\cap A(\mathbb{R})^0$ de $A(\mathbb{R})^0$ soit le sous-groupe $Y=\mathbb{Z}^d\omega+\mathbb{Z}y_1+\cdots+\mathbb{Z}y_\ell$ de $\mathbb{R}^d$. Ainsi $\Gamma\cap A(\mathbb{R})^0$ est dense dans $A(\mathbb{R})^0$ si et seulement si Y est dense dans $\mathbb{R}^d$. D'après la proposition 4.3 du chapitre II, cette condition s'écrit encore : pour tout hyperplan H de $\mathbb{R}^d$, on a $\mathrm{rang}_\mathbb{Z}\big(Y/Y\cap H\big)\ge 2$. Comme $Y/Y\cap H$ contient $\mathbb{Z}^d\omega/\mathbb{Z}^d\omega\cap H$, on peut se restreindre aux hyperplans H pour lesquels $\mathrm{rang}_\mathbb{Z}\big(\mathbb{Z}^d\omega\cap H\big)=d-1$, c'est à-dire aux hyperplans H qui sont rationnels sur $\mathbb{Q}$; un tel hyperplan s'écrit $T_{A'}(\mathbb{R})$, où A' est une sous-variété abélienne de A de dimension $d-1$, et on a

$$\mathrm{rang}_\mathbb{Z}\big(Y/Y\cap H\big)=\mathrm{rang}_\mathbb{Z}\big(\Gamma/\Gamma\cap A'(\mathbb{R})\big).$$

b) Pour $1\le i\le d$, soit $u_i\in\mathbb{R}$ vérifiant $\exp_{E,\mathbb{R}}(u_i)=\delta_i$. On pose encore $\gamma=(\delta_1,\dots,\delta_d)\in\mathbb{R}^d$ et $y=(u_1,\dots,u_d)\in\mathbb{R}^d$, de sorte que $\gamma=\exp_{A,\mathbb{R}}(y)$. Alors $\Gamma=\mathbb{Z}\gamma$ est dense dans $A(\mathbb{R})^0$ si et seulement si $Y=\exp^{-1}(\Gamma)=\mathbb{Z}^d\omega+\mathbb{Z}y$ est dense dans $\mathbb{R}^d$. D'après le théorème de Kronecker, cette condition s'écrit encore : les nombres $\omega,u_1,\dots,u_d$ sont linéairement indépendants sur $\mathbb{Q}$. Cela signifie aussi que les points $\delta_1,\dots,\delta_d$ sont $\mathbb{Z}$-linéairement indépendants dans $E(\mathbb{R})$. □

Nous reviendrons sur le cas elliptique dans la section 6 pour étudier la situation complexe, et dans le chapitre V quand nous nous intéresserons à l'aspect quantitatif.

§2. Groupes algébriques commutatifs sur $\mathbb{R}$

a) Notations

Soit G un groupe algébrique commutatif de dimension d défini sur $\mathbb{C}$. Les points de G dans le corps des nombres complexes forment un groupe de Lie commutatif complexe $G(\mathbb{C})$, l'espace tangent à l'origine de $G(\mathbb{C})$ est un $\mathbb{C}$-espace vectoriel $T_G(\mathbb{C})$ de dimension d, et l'application exponentielle $\exp_G:T_G(\mathbb{C})\to G(\mathbb{C})$ de $G(\mathbb{C})$ est un morphisme analytique, dont l'image est la composante connexe de l'élément neutre de $G(\mathbb{C})$, et dont le noyau $\Omega_G=\mathrm{Ker}\ \exp_G$ est un sous-groupe discret de $T_G(\mathbb{C})$. On notera $\kappa_\mathbb{C}(G)$ son rang sur $\mathbb{Z}$.

Nous avons déjà vu ce qui se passait dans le cas d'un groupe linéaire $\mathbb{G}_\mathrm{a}^{d_0}\times\mathbb{G}_\mathrm{m}^{d_1}$, où le noyau est engendré par d_1 éléments linéairement indépendants sur $\mathbb{C}$. Un autre exemple important est celui d'une variété abélienne, qui correspond au cas où le noyau Ω_G est un réseau de $T_G(\mathbb{C})$ (sous-groupe discret de rang $2d$).

D'après un théorème de Barsotti (voir [Se 1979]), un groupe algébrique commutatif G possède un plus grand sous-groupe linéaire L et le groupe quotient G/L peut être muni d'une structure de variété projective qui en fait une variété abélienne A. Sur $\mathbb{C}$, le groupe linéaire L se décompose en produit d'un facteur unipotent $\mathbb{G}_\mathrm{a}^u$ par un facteur de type multiplicatif (*tore*) $\mathbb{G}_\mathrm{m}^t$. On a alors un diagramme commutatif

$$\begin{array}{ccccccccc}
0 & \longrightarrow & T_L(\mathbb{C}) & \longrightarrow & T_G(\mathbb{C}) & \longrightarrow & T_A(\mathbb{C}) & \longrightarrow & 0\\
 & & \Big\downarrow{\scriptstyle \exp_L} & & \Big\downarrow{\scriptstyle \exp_G} & & \Big\downarrow{\scriptstyle \exp_A} & & \\
0 & \longrightarrow & L(\mathbb{C}) & \longrightarrow & G(\mathbb{C}) & \longrightarrow & A(\mathbb{C}) & \longrightarrow & 0,
\end{array}$$

avec $T_L(\mathbb{C})=\mathbb{C}^{u+t}$, $T_G(\mathbb{C})=\mathbb{C}^d$, $T_A(\mathbb{C})=\mathbb{C}^g$ et $L(\mathbb{C})=\mathbb{C}^u\times(\mathbb{C}^\times)^t$. Le noyau de $\exp_L$ est $\{0\}^u\times(2i\pi\mathbb{Z})^t$, celui de $\exp_A$ est un réseau Ω_A de $\mathbb{C}^g$ de rang $2g$, donc celui de $\exp_G$ est de rang

$$\kappa_\mathbb{C}(G)=t+2g.$$

Comme groupe topologique, $G(\mathbb{C})^0$ est isomorphe au quotient de $\mathbb{C}^d\simeq\mathbb{R}^{2d}$ par un sous-groupe de rang $\kappa_\mathbb{C}(G)$, donc le nombre $\mathrm{m}_\mathbb{C}(G)=\mathrm{m}\big(G(\mathbb{C})\big)$ vérifie

$$\mathrm{m}_\mathbb{C}(G)=2d+1-\kappa_\mathbb{C}(G)=2u+t+1.$$

On ne sait malheureusement pas encore faire intervenir, dans les énoncés de transcendance, les entiers u, t et g, correspondant aux dimensions du plus grand sous-groupe unipotent de G, du plus grand tore linéaire contenu dans G, et de la variété abélienne quotient. Mais on sait faire intervenir la dimension des plus grands quotients correspondants de G. On notera d_0 (resp. d_1) le plus grand entier ≥ 0 tel que G possède un facteur isomorphe à $\mathbb{G}_{\mathrm{a}}^{d_0}$ (resp. à $\mathbb{G}_{\mathrm{m}}^{d_1}$) et 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 de dimension d_2 et n'a pas de facteur linéaire non trivial. On définit alors, comme dans [R 1991],

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

Noter que l'on a $d_0 \leq u$ et $d_1 \leq t$. Pour un groupe algébrique de dimension d, $\alpha(G) \leq 2d$; si G est linéaire, $\alpha(G) \leq d$, avec égalité pour une puissance de $\mathbb{G}_{\mathrm{m}}$. Dans la suite, quand le groupe algébrique G sera défini sur le corps $\overline{\mathbb{Q}}$ des nombres algébriques, on demandera que les facteurs $\mathbb{G}_{\mathrm{a}}^{d_0}$, $\mathbb{G}_{\mathrm{m}}^{d_1}$ et G_2 le soient aussi.

Nous utiliserons (sans les démontrer) plusieurs faits relatifs aux sous-groupes algébriques. Soit G un groupe algébrique commutatif défini sur $\mathbb{C}$, et soit G' un sous-groupe algébrique. L'espace tangent à l'origine $T_{G'}(\mathbb{C})$ de $G'(\mathbb{C})$ est le plus grand sous-espace vectoriel sur $\mathbb{C}$ de $T_G(\mathbb{C})$ qui soit contenu dans $\exp^{-1}\big(G'(\mathbb{C})\big)$. Si G et G' sont définis sur un sous-corps K de $\mathbb{C}$, alors $T_G(\mathbb{C})$ possède une K-structure, et $T_{G'}(\mathbb{C})$ est rationnel sur K. Le groupe quotient $G(\mathbb{C})/G'(\mathbb{C})$ est le groupe des points complexes d'un groupe algébrique G/G', et son espace tangent à l'origine s'identifie au quotient $T_G(\mathbb{C})/T_{G'}(\mathbb{C})$.

Quand le groupe algébrique G est un produit $L \times A$ d'un groupe linéaire L par une variété abélienne A, alors tout sous-groupe algébrique connexe de G est un produit $L' \times A'$, avec L' sous-groupe algébrique de L et A' sous-variété abélienne de A. Une des démonstrations de cet énoncé consiste à montrer qu'il n'y a pas de morphisme de groupes algébriques non trivial entre une variété linéaire et une variété abélienne, puis à utiliser le *lemme de Goursat* (voir par exemple [L 1993], 3rd Ed., Chap. I, §12, ex. 5).

On a déjà vu dans le chapitre précédent (chap.3, §2) que les sous-groupes algébriques de $\mathbb{G}_{\mathrm{a}}^d$ correspondaient, via l'exponentielle, aux sous-espaces vectoriels de l'espace tangent ; on a vu aussi que les sous-groupes algébriques de $\mathbb{G}_{\mathrm{m}}^d$ correspondaient, dans l'espace tangent, aux sous-espaces vectoriels rationnels sur $\mathbb{Q}$.

Pour une puissance E^d d'une courbe elliptique E, les sous-groupes algébriques correspondent, dans l'espace tangent, aux sous-espaces vectoriels rationnels sur le corps des endomorphismes de la courbe elliptique (qui est soit $\mathbb{Q}$, soit un corps imaginaire quadratique). Plus généralement si A est une variété abélienne simple et r, s deux entiers, tout morphisme de groupes algébriques $A^s \to A^r$ est donné par

$$(x_1, \ldots, x_s) \longmapsto \Big(\sum_{i=1}^{s} \ell_{ij}(x_i)\Big)_{1 \leq j \leq r}$$

où ℓ_{ij} sont des endomorphismes de A (voir par exemple [SwD 1974], Chap. III §7, ou [LB 1992], Chap. V, Cor. 3.8).

Soit maintenant G un groupe algébrique commutatif défini sur $\mathbb{R}$. L'application exponentielle du groupe de Lie connexe $G(\mathbb{R})^0$ est la restriction à $T_G(\mathbb{R})$ de $\exp_G$; son noyau est donc $\Omega_{G,\mathbb{R}} = \Omega_G \cap T_G(\mathbb{R})$. On désigne par $\kappa_{\mathbb{R}}(G)$ le rang de ce sous-groupe

discret de $T_G(\mathbb{R})$. Si G est une variété abélienne, alors $\Omega_{G,\mathbb{R}}$ est un réseau de $\mathbb{R}$, tandis que pour un groupe linéaire déployé $\mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}$, le noyau est réduit à $\{0\}$. Mais nous avons vu un exemple d'un groupe linéaire non déployé (le groupe $\widetilde{G}$ du chapitre III, §4) pour lequel le noyau $\Omega_{G,\mathbb{R}}$ n'est pas trivial.

Le groupe de Lie réel $G(\mathbb{R})^0$ est encore un quotient d'un espace vectoriel de dimension $d = \dim G$, à savoir $T_G(\mathbb{R})$, par un sous-groupe discret de rang $\kappa_{\mathbb{R}}(G)$. En posant $\mathrm{m}_{\mathbb{R}}(G) = \mathrm{m}\big(G(\mathbb{R})\big)$, nous avons

$$\mathrm{m}_{\mathbb{R}}(G) = d + 1 - \kappa_{\mathbb{R}}(G).$$

Pour une variété abélienne A de dimension d, $\kappa_{\mathbb{R}}(A) = d$ et $\mathrm{m}_{\mathbb{R}}(A) = 1$, 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 $\mathrm{m}_{\mathbb{R}}(L) = d+1$, avec $d = d_0 + d_1$.

Soit G un groupe algébrique commutatif défini sur un sous-corps K de $\mathbb{C}$ de dimension d ; on désigne par

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

le $\mathbb{Z}$-module des logarithmes de points de $G(K)$. Quand K est le corps $\overline{\mathbb{Q}}$ des nombres algébriques, on omettra l'indice $\overline{\mathbb{Q}}$: ainsi, comme dans le chapitre III, $\mathcal{L}(G)$ désignera le $\mathbb{Q}$-espace vectoriel des logarithmes de points de $G(\overline{\mathbb{Q}})$. Par exemple quand G est un produit $\mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1} \times A$ où A est une variété abélienne définie sur $\overline{\mathbb{Q}}$, on a

$$\mathcal{L}(G) = \overline{\mathbb{Q}}^{d_0} \times \mathcal{L}^{d_1} \times \mathcal{L}(A);$$

si K est le corps $\overline{\mathbb{Q}} \cap \mathbb{R}$ des nombres algébriques réels, on a

$$\mathcal{L}_K(G) = K^{d_0} \times (\mathcal{L} \cap \mathbb{R})^{d_1} \times \mathcal{L}_K(A).$$

Les nombres complexes que l'on considère ainsi sont des valeurs *d'intégrales abéliennes*. Les plus simples s'expriment comme combinaisons linéaires à coefficients algébriques d'éléments de $\mathcal{L}$, comme

$$\int_0^1 \frac{dx}{1+x^3} = \frac{1}{3}\Big(\log 2 + \frac{\pi}{\sqrt{3}}\Big).$$

On trouve ensuite des intégrales elliptiques de première espèce : la longueur de la lemniscate $(x^2+y^2)^2 = 2(x^2-y^2)$ est $\Gamma(1/4)^2/\sqrt{\pi} = 2\sqrt{2}\omega$, où $(\omega, i\omega)$ est une base du réseau des périodes de la courbe elliptique $y^2 = 4x^3 - 4x$, avec

$$\begin{aligned}\omega = 2\int_1^\infty \frac{dx}{\sqrt{4x^3-4x}} &= \frac{1}{2}\int_0^1 u^{-3/4}(1-u)^{-1/2}du\\ &= \frac{1}{2}B(1/4,1/2) = \frac{\Gamma(1/4)\Gamma(1/2)}{2\Gamma(3/4)} = \frac{\Gamma(1/4)^2}{2\sqrt{2\pi}}.\end{aligned}$$

(Voir à ce sujet [Si 1949]). Un autre exemple d'intégrale elliptique de première espèce est la période réelle de la courbe $y^2 = 4x^3 - 4$:

$$\omega = 2\int_1^\infty \frac{dx}{\sqrt{4x^3-4}} = \frac{1}{3}B(1/6,1/2) = \frac{\Gamma(1/3)^3}{2\sqrt[3]{2}\,\pi}.$$

Parmi les intégrales abéliennes plus générales, on trouve les intégrales Eulériennes qui donnent les fonctions Beta et Gamma :

$$B(a,b) = \int_0^1 t^{a-1}(1-t)^{b-1}dt = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}.$$

b) 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.

Exercice. Vérifier que l'adhérence de Zariski d'un sous-groupe Γ de $G(K)$ est un sous-groupe algébrique de G défini sur K
`Indication.` L'idéal des polynômes nuls sur Γ est le même que celui des polynômes nuls sur l'adhérence de Zariski $\overline{\Gamma}$. Soit P un élément de cet idéal ; pour $x \in G(K)$, on notera $P(x+X)$ la fonction sur $G(K)$ obtenue en composant l'application polynomiale P sur $G(K)$ et la translation : $g \mapsto x+g$. Vérifier que pour $x \in \Gamma$, la fonction $P(x+X)$ est nulle sur Γ ; en déduire qu'elle est aussi nulle sur $\overline{\Gamma}$. Montrer ensuite que, pour $y \in \overline{\Gamma}$, $P(y+X)$ est nulle sur Γ ; en déduire qu'elle est aussi nulle sur $\overline{\Gamma}$. Conclure.

La condition de densité pour la topologie de Zariski se traduit donc 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.* La conjecture de Mazur restreinte aux groupes algébriques commutatifs s'énonce donc de la manière suivante :

$\boxed{?}$ *Si G est un groupe algébrique commutatif défini sur le corps $\mathbb{Q}$ des nombres rationnels, et si $G(\mathbb{Q})$ n'est pas contenu dans $G'(\mathbb{Q})$ quand G' est un sous-groupe algébrique de G distinct de G, alors $G(\mathbb{Q}) \cap G(\mathbb{R})^0$ est dense pour la topologie réelle dans $G(\mathbb{R})^0$.*

On peut ramener cette question au cas particulier des variétés abéliennes simples :

$\boxed{?}$ *Si A est une variété abélienne simple sur $\mathbb{Q}$ et si $A(\mathbb{Q})$ est infini, alors $A(\mathbb{Q}) \cap A(\mathbb{R})^0$ est dense pour la topologie réelle dans $A(\mathbb{R})^0$.*

Nous allons considérer, plus généralement, un corps de nombres (à la place de $\mathbb{Q}$), et un sous-groupe Γ de $G(K)$ (à la place de $G(K)$ tout entier). La condition de densité pour la topologie de Zariski n'est pas suffisante dans ce cadre plus 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, la conjecture d'indépendance algébrique homogène de logarithmes de nombres algébriques d'autre part.

Voici déjà la condition nécessaire annoncée pour qu'un sous-groupe de type fini de $G(K) \cap G(\mathbb{R})^0$ soit dense dans $G(\mathbb{R})^0$.

Lemme 2.1. – *Soient K un sous-corps de $\mathbb{R}$, G un groupe algébrique commutatif défini sur K de dimension ≥ 1 et Γ un sous-groupe de type fini de $G(K)$. On suppose que l'adhérence réelle de Γ dans $G(\mathbb{R})$ contient la composante neutre $G(\mathbb{R})^0$. Alors, pour tout sous-groupe algébrique G' de G défini sur K,*

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

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 $\mathrm{m}_{\mathbb{R}}(G)$ par le nombre $\mathrm{m}'_{\mathbb{R}}(G)$ (qui, pour un groupe différent de $\mathbb{G}_{\mathrm{a}}^d$, est au moins égal à $\mathrm{m}_{\mathbb{R}}(G)$), défini de la manière suivante :

$$\mathrm{m}'_{\mathbb{R}}(G) = \begin{cases} \alpha(G)(d-1)+2 & \text{si } \kappa_{\mathbb{R}}(G) = 0, \\ \big(\alpha(G) - \kappa_{\mathbb{R}}(G) + 1\big)(d-1) + 2 - \kappa_{\mathbb{R}}(G) & \text{si } \kappa_{\mathbb{R}}(G) \geq 1. \end{cases}$$

Ainsi on a toujours $\mathrm{m}'_{\mathbb{R}}(G) \leq \alpha(G)(d-1)+2$; de plus

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

Théorème 2.2 (théorème de densité). – *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 que, pour tout sous-groupe algébrique G' de G défini sur K avec $\dim G' < \dim G$, on a $\mathrm{rang}_{\mathbb{Z}}\big(\Gamma/\Gamma \cap G'(K)\big) \geq \mathrm{m}'_{\mathbb{R}}(G/G')$. 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 $\dim G' < \dim G$,

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

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

c) Le théorème du sous-groupe algébrique
La démonstration du théorème 2.2 repose sur le Théorème du sous-groupe algébrique ([W 1988], Théorème 1.1 ; il nous suffit ici d'un cas particulier [W 1987], Théorème 4.1, [R 1991], Remarque 1 p. 270, que nous appelons quand même "Théorème du sous-groupe algébrique").

Théorème 2.3* (théorème du sous-groupe algébrique). – *Soient G un groupe algébrique commutatif défini sur $\overline{\mathbb{Q}}$ 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 $\overline{\mathbb{Q}}$ 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 $\mathbb{Q}$-espace vectoriel $\mathcal{V} \cap \mathcal{L}(G)$ est de dimension finie majoré par*

$$\dim_{\mathbb{Q}}\big(\mathcal{V} \cap \mathcal{L}(G)\big) \leq \big(\alpha(G) - \kappa\big)(d-1).$$

On déduit de cet énoncé le théorème du sous-groupe linéaire (théorème 2.10 du chapitre III). Pour cela on prend simplement $G = \mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}$.

Nous allons déduire du théorème 2.3 quelques corollaires concernant les produits de deux groupes algébriques de dimension 1. Pour $\mathbb{G}_{\mathrm{a}} \times \mathbb{G}_{\mathrm{m}}$ (resp. $\mathbb{G}_{\mathrm{m}}^2$), on sait déjà (via le théorème du sous-groupe linéaire) que l'on obtient le théorème de Gel'fond-Schneider (resp. le théorème des six exponentielles). Il nous reste à regarder les groupes algébriques $\mathbb{G}_{\mathrm{a}} \times E$, $\mathbb{G}_{\mathrm{m}} \times E$ et $E \times E^*$, quand E et E^* sont deux courbes elliptiques.

Corollaire 2.4. — *Soient E une courbe elliptique définie sur le corps $\overline{\mathbb{Q}}$ des nombres algébriques, $\alpha_1, \alpha_2, \alpha_3$ des nombres algébriques non tous nuls et u_1, u_2, u_3 des éléments de $\mathcal{L}(E)$ non tous nuls. On suppose que les trois colonnes de la matrice*

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ u_1 & u_2 & u_3 \end{pmatrix}$$

sont linéairement indépendantes sur $\mathbb{Q}$. Alors cette matrice est de rang 2.

Démonstration. Soit G le groupe algébrique $\mathbb{G}_a \times E$. Les sous-groupes algébriques G' de G sont de la forme $\{(0,0)\}$, $\mathbb{G}_a \times F$, $\{0\} \times F$, $\{0\} \times E$ et G, où F est un groupe fini. Grâce à la fonction $\wp$, on identifie l'espace tangent à l'origine de $G(\mathbb{C}) = \mathbb{C} \times E(\mathbb{C})$ à $\mathbb{C}^2$. Une droite $\mathcal{V}$ de $\mathbb{C}^2$, qui n'est pas l'un des axes $\{0\} \times \mathbb{C}$ ou $\mathbb{C} \times \{0\}$, ne contient pas de sous-espace non nul de la forme $T_{G'}(\mathbb{C})$. Comme $\alpha(G) = 2$ on déduit du théorème 2.3 la majoration $\dim\bigl(\mathcal{V} \cap \mathcal{L}(G)\bigr) \leq 2$. Le corollaire 2.4 en résulte. $\square$

Remarque. Supposons que la courbe elliptique E admette des endomorphismes non triviaux : il existe $\lambda \in \mathbb{C} \setminus \mathbb{Q}$ tel que, si $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ désigne le réseau des périodes de $\wp$, on ait $\lambda\Omega \subset \Omega$ (on dit que la courbe elliptique *admet des multiplications complexes*, ou encore *est de type C.M.*). Dans ce cas le quotient $\tau = \omega_2/\omega_1$ est un nombre algébrique (de degré 2 sur $\mathbb{Q}$: il est imaginaire quadratique). La matrice

$$\begin{pmatrix} 1 & \tau \\ \omega_1 & \omega_2 \end{pmatrix}$$

a ses deux colonnes $\mathbb{Q}$-linéairement indépendantes ; la première ligne a ses composantes algébriques, la seconde a ses composantes dans $\mathcal{L}(E)$, et le déterminant s'annule. On ne peut donc pas remplacer 3 par 2 dans le corollaire 2.4.

On peut cependant améliorer le corollaire 2.4 dans le cas où la courbe elliptique E n'a pas d'endomorphismes non triviaux. Plus précisément, on peut démontrer le résultat suivant :

Soient E une courbe elliptique définie sur $\overline{\mathbb{Q}}$, α_1, α_2 des nombres algébriques non tous deux nuls et u_1, u_2 des éléments de $\mathcal{L}(E)$ linéairement indépendants sur l'anneau des endomorphismes de E. Alors le déterminant de la matrice

$$\begin{pmatrix} \alpha_1 & \alpha_2 \\ u_1 & u_2 \end{pmatrix}$$

n'est pas nul.

Dans le cas C.M., cela se déduit du corollaire 2.4. Dans le cas non C.M., on utilise un autre résultat de transcendance, l'analogue elliptique du septième problème de Hilbert, dû à Th. Schneider (voir [W 1979], corollaire 3.2.3) :

Soient E une courbe elliptique définie sur $\overline{\mathbb{Q}}$ et u_1, u_2 des éléments de $\mathcal{L}(E)$ linéairement indépendants sur l'anneau des endomorphismes de E. Alors u_1, u_2 sont linéairement indépendants sur $\overline{\mathbb{Q}}$.

Une conséquence remarquable de cet énoncé porte sur la fonction modulaire $j(\tau)$, qui est définie dans le demi-plan supérieur $\Im m\, \tau > 0$ par la condition suivante : si $\tau = \omega_2/\omega_1$ et si $\wp$ est la fonction elliptique de Weierstrass de réseau de périodes $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, alors $j(\tau) = 1728 g_2^3/\Delta$, où g_2 et g_3 sont les invariants de $\wp$ et $\Delta = g_2^3 - 27 g_3^2$.

Soient $\tau \in \overline{\mathbb{Q}}$ satisfaisant $\Im m\, \tau > 0$. Alors $j(\tau)$ est algébrique si et seulement si τ est quadratique.

Le résultat de Schneider sur l'indépendance de deux logarithmes elliptiques a été généralisé par D. Bertrand et D.W. Masser [BeM 1980] : c'est l'analogue elliptique du théorème de Baker :

Soient E une courbe elliptique définie sur $\overline{\mathbb{Q}}$ et $u_1, \ldots, u_n$ des éléments de $\mathcal{L}(E)$ linéairement indépendants sur l'anneau des endomorphismes de E. Alors $1, u_1, \ldots, u_n$ sont linéairement indépendants sur $\overline{\mathbb{Q}}$.

Exercice. Dans le cas CM, déduire du théorème 2.3 l'indépendance linéaire sur $\overline{\mathbb{Q}}$ des nombres $u_1, \ldots, u_n$. Dans le cas non C.M., déduire du théorème 2.3 que le $\overline{\mathbb{Q}}$ espace vectoriel engendré par ces nombres a une dimension $\geq n/2$.

Remarque. On peut déduire ce résultat de Bertrand-Masser d'un raffinement [W 1987] du théorème 2.3 : *sous les hypothèses du théorème 2.3, si $\mathcal{V}$ contient un sous-espace vectoriel W de $T_G(\mathbb{C})$ qui est rationnel sur $\overline{\mathbb{Q}}$ et de dimension t, alors*

$$\dim_{\mathbb{Q}}\bigl(\mathcal{V} \cap \mathcal{L}(G)\bigr) \leq \bigl(\alpha(G) - \kappa\bigr)(d - t - 1).$$

Le cas particulier où $\mathcal{V} = W$ est dû à Wüstholz [Wü 1989] : sous les hypothèses du théorème 2.3, si $\mathcal{V}$ est rationnel sur $\overline{\mathbb{Q}}$, alors $\mathcal{V} \cap \mathcal{L}(G) = \{0\}$.

Exercice. En utilisant ce résultat de Wüstholz, démontrer l'énoncé suivant : Soient $\lambda_1, \ldots, \lambda_m$ des éléments $\mathbb{Q}$-linéairement indépendants de $\mathcal{L}$. Soient E une courbe elliptique définie sur $\overline{\mathbb{Q}}$ et $u_1, \ldots, u_n$ des éléments de $\mathcal{L}(E)$ linéairement indépendants sur l'anneau des endomorphismes de E. Alors les nombres $1, \lambda_1, \ldots, \lambda_m, u_1, \ldots, u_n$ sont linéairement indépendants sur $\overline{\mathbb{Q}}$.

Passons maintenant au produit du groupe multiplicatif par une courbe elliptique.

Corollaire 2.5. – *Soient $\lambda_1, \ldots, \lambda_\ell$ des éléments $\mathbb{Q}$-linéairement indépendants de $\mathcal{L}$. Soit E une courbe elliptique définie sur $\overline{\mathbb{Q}}$, et soient $u_1, \ldots, u_\ell$ des éléments non tous nuls de $\mathcal{L}(E)$.*
a) Si $\ell \geq 4$, alors la matrice à deux lignes et ℓ colonnes

$$\begin{pmatrix} \lambda_1 & \ldots & \lambda_\ell \\ u_1 & \ldots & u_\ell \end{pmatrix}$$

est de rang 2.
b) Si λ_1 est un multiple rationnel de $2\pi i$, et u_1 une période de $\exp_E$, alors la conclusion est encore vraie pour $\ell = 3$.

De la partie b) du corollaire 2.5, Ramachandra déduit (voir [Ra 1968], p. 87) :

Si a et b sont des nombres algébriques réels positifs différents de 1, avec $\log a/\log b$ irrationnel et $a < b < a^{-1}$, alors un au moins des deux nombres

$$x = \left(\frac{1}{240} + \sum_{n=1}^{\infty} \frac{n^3 a^n}{1-a^n}\right) \prod_{n=1}^{\infty} (1-a^n)^{-8},$$

$$y = \left\{\frac{6}{(b^{1/2}-b^{-1/2})^4} - \frac{1}{(b^{1/2}-b^{-1/2})^2} - \sum_{n=1}^{\infty} \frac{n^3 a^n (b^n + b^{-n})}{1-a^n}\right\} \prod_{n=1}^{\infty} (1-a^n)^{-8},$$

est transcendant.

Ramachandra a conjecturé dans [Ra 1968] que la conclusion du corollaire 2.5 était encore vraie sous l'hypothèse plus faible $\ell \geq 2$. Cela signifierait qu'une matrice de la forme

$$\begin{pmatrix} \log\alpha & \log\beta \\ u & v \end{pmatrix}$$

a un déterminant non nul. C'est un analogue de la conjecture des quatre exponentielles (voir [D 1997]). Le seul cas particulier connu est celui où u et v sont des périodes de $\wp$, et $\log\alpha = i\pi$: le résultat en question s'énonce :

Si $\wp$ est une fonction elliptique de Weierstrass d'invariants g_2 et g_3 algébriques et si ω_1 et ω_2 sont deux périodes $\mathbb{Q}$-linéairement indépendantes de $\wp$, alors le nombre $e^{2i\pi\omega_2/\omega_1}$ est transcendant.

En posant $\tau = \omega_2/\omega_1$, $q = e^{2i\pi\tau}$, $J(q) = j(\tau) = 1728 g_2^3/\Delta$, on voit en effet qu'une formulation équivalente de cet énoncé est le théorème de K. Barré-Sirieix, G. Diaz, F. Gramain et G. Philibert [BDGP 1995] :

Si q est un nombre complexe algébrique avec $0 < |q| < 1$, alors le nombre

$$J(q) = \frac{1}{q} + 744 + 196884q + \cdots$$

est transcendant.

Nous terminons cette série de corollaires en considérant un produit de deux courbes elliptiques.

Corollaire 2.6. – *Soient E et E^* deux courbes elliptiques définies sur $\overline{\mathbb{Q}}$, attachées à des fonctions elliptiques de Weierstrass $\wp$ et $\wp^*$ respectivement. Soient $u_1, \dots, u_\ell$ des éléments $\mathbb{Q}$-linéairement indépendants de $\mathcal{L}(E)$, et $u_1^*, \dots, u_\ell^*$ des éléments $\mathbb{Q}$-linéairement indépendants de $\mathcal{L}(E^*)$. On suppose que les deux fonctions $\wp(u_1 z)$ et $\wp^*(u_1^* z)$ sont algébriquement indépendantes.*
a) Si $\ell \geq 5$, alors la matrice

$$\begin{pmatrix} u_1 & \dots & u_\ell \\ u_1^* & \dots & u_\ell^* \end{pmatrix}$$

est de rang 2.
b) Si u_1 est une période de $\wp$ et u_1^* une période de $\wp^*$, alors le rang de la matrice est encore 2 pour $\ell = 4$.

Ramachandra conjecture que la conclusion est encore vraie dès que $\ell \geq 2$. C'est de nouveau un analogue elliptique de la conjecture des quatre exponentielles.

d) Démonstration du Théorème 2.2
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

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

c'est un sous-groupe de type fini de $T_G(\mathbb{R})$ de rang $\ell + \kappa_{\mathbb{R}}(G)$, 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 $T_G(\mathbb{R})$,

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

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

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

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

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

1) On commence par établir le résultat suivant :

supposons $\ell \geq \mathrm{m}'_{\mathbb{R}}(G)$; 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 $\operatorname{rang}_{\mathbb{Z}}\left(Y/Y \cap V\right) \geq 2$ est bien vérifiée.

On démontre cela en utilisant le théorème 2.3* ; 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 $\mathcal{L}(G) \cap \mathcal{V}$, on peut conclure

$$\operatorname{rang}_{\mathbb{Z}}(Y \cap V) \leq \dim_{\mathbb{Q}}\left(\mathcal{L}(G) \cap \mathcal{V}\right) \leq \left(\alpha(G) - \max\{\kappa_{\mathbb{R}}(G) - 1, 0\}\right)(d-1).$$

Le résultat annoncé résulte de la définition de $\mathrm{m}'_{\mathbb{R}}(G)$.

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

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

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 résultat démontré en 1) au sous-groupe $Y/Y\cap T_{G'}(\mathbb{R})$ de $T_{G/G'}(\mathbb{R})$, dont l'image par $\exp_{G/G'}$ dans $(G/G')(\mathbb{R})$ est $\Gamma/\Gamma\cap G'(K)$:

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

3) La partie *b)* du théorème 2.2 résulte maintenant de la partie *a)* et du théorème de D. Roy (chapitre II théorème 7.2 avec $R = G(\mathbb{R})^0$). □

e) La propriété de densité

Il nous reste à décrire la situation d'un point de vue conjectural. Nous savons déjà (Chap. III, §3) qu'il existe des exemples de couples (G,Γ), où G est un groupe algébrique commutatif défini sur $\overline{\mathbb{Q}}$ et Γ un sous-groupe de type fini de $G(\mathbb{Q})$, dont la projection sur tout quotient G/G', G' sous-groupe algébrique de G de dimension > 0, vérifie $\mathrm{rang}_{\mathbb{Z}}\bigl(\Gamma/\Gamma\cap G'(\overline{\mathbb{Q}})\bigr) \geq \mathrm{m}_{\mathbb{R}}(G/G')$, et pourtant $\Gamma\cap G(\mathbb{R})^0$ n'est pas dense dans $G(\mathbb{R})^0$.

Une première approche est fournie par la définition suivante.

Définition : propriété de densité. – *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 $\{\gamma_1,\ldots,\gamma_\ell\}$ 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 $\mathbb{Z}(\gamma_1,\ldots,\gamma_\ell)$, alors il existe un point $(\eta_1,\ldots,\eta_\ell)$ dans $H(\mathbb{R})$ tel que $\mathbb{Z}\eta_1+\cdots+\mathbb{Z}\eta_\ell$ soit un sous-groupe dense de $G(\mathbb{R})^0$.*

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 $(\eta_1,\ldots,\eta_\ell)$ un multiple convenable de $(\gamma_1,\ldots,\gamma_\ell)$. D'autre part si l'assertion (ii) est vraie pour *une* famille $\{\gamma_1,\ldots,\gamma_\ell\}$ 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.

Exercice. Soient G un groupe algébrique commutatif connexe sur $\mathbb{R}$, $\gamma_1,\ldots,\gamma_\ell$, $\gamma'_1,\ldots,\gamma'_{\ell'}$ des éléments de $G(\mathbb{R})$. On désigne par Γ le sous-groupe de $G(\mathbb{R})$ engendré par $\gamma_1,\ldots,\gamma_\ell$, et on pose de même $\Gamma' = \mathbb{Z}\gamma'_1+\cdots+\mathbb{Z}\gamma'_{\ell'}$. On suppose que $\Gamma\cap\Gamma'$ est un sous-groupe d'indice fini dans Γ et aussi dans Γ'. On désigne enfin par H l'adhérence de Zariski dans G^ℓ du sous-groupe $\mathbb{Z}(\gamma_1,\ldots,\gamma_\ell)$ et par H' l'adhérence de Zariski dans $G^{\ell'}$ du sous-groupe $\mathbb{Z}(\gamma'_1,\ldots,\gamma'_{\ell'})$. Les propriétés suivantes sont équivalentes :

(i) Il existe un point $(\eta_1,\ldots,\eta_\ell)$ dans $H(\mathbb{R})$ tel que $\mathbb{Z}\eta_1+\cdots+\mathbb{Z}\eta_\ell$ soit un sous-groupe dense de $G(\mathbb{R})^0$.

(ii) Il existe un point $(\eta'_1,\ldots,\eta'_{\ell'})$ dans $H'(\mathbb{R})$ tel que $\mathbb{Z}\eta'_1+\cdots+\mathbb{Z}\eta'_{\ell'}$ soit un sous-groupe dense de $G(\mathbb{R})^0$.

Il est clair que la conjecture 3.5? du chapitre III peut s'énoncer : *tout groupe algébrique linéaire $\mathbb{G}_{\mathrm{a}}^{d_0}\times\mathbb{G}_{\mathrm{m}}^{d_1}$ possède la propriété de densité.* Un exemple de groupe algébrique qui ne vérifie pas la propriété de densité est donné dans [Be 1995] (voir la fin du §5 ci-dessous).

Exercice. Soient G un groupe algébrique défini sur $\overline{\mathbb{Q}}$ et Y un sous-groupe de type fini de l'espace tangent $T_G(\mathbb{C})$ tel que $\exp_G(Y)\subset G(\overline{\mathbb{Q}})$. On définit $r(Y,G)$ comme la dimension du sous-espace de $T_G(\mathbb{C})$ sur $\mathbb{C}$ engendré par Y. On définit un autre nombre $r_{\mathrm{str}}(Y,G)$ de la manière suivante : soient ℓ le rang de Y, et soit $y_1,\ldots,y_\ell$ des éléments de Y qui engendrent un sous-groupe d'indice fini dans Y. Soit $T_{\mathcal{H}}(\mathbb{C})$ le plus petit sous-espace tangent d'un sous-groupe algébrique $\mathcal{H}$ de G^ℓ, défini sur $\overline{\mathbb{Q}}$, tel que $(y_1,\ldots,y_\ell)\in T_{\mathcal{H}}(\mathbb{C})$. On pose

$$r_{\mathrm{str}}(Y,G) = \max\dim_{\mathbb{C}}\bigl\{\mathbb{C}z_1+\cdots+\mathbb{C}z_\ell;\ (z_1,\ldots,z_\ell)\in T_{\mathcal{H}}(\mathbb{C})\bigr\}.$$

On dira que le groupe algébrique G vérifie la propriété (A.I.) *si, pour tout sous-groupe de type fini Y de $\mathcal{L}(G)$, on a $r_{\mathrm{str}}(Y,G)=r(Y,G)$.*

a) Montrer que le nombre $r_{\mathrm{str}}(Y,G)$ ne dépend pas du choix de $y_1,\ldots,y_\ell$.

b) Vérifier que les deux assertions suivantes sont équivalentes :

(i) Des éléments de $\mathcal{L}=\exp^{-1}(\overline{\mathbb{Q}}^\times)$ linéairement indépendants sur $\mathbb{Q}$ sont algébriquement indépendants sur $\mathbb{Q}$.

(ii) Pour tout entier $d\geq 1$, le groupe algébrique $\mathbb{G}_{\mathrm{m}}^d$ vérifie la propriété (A.I.).

c) Soient $\wp$ une fonction elliptique de Weierstraß d'invariants g_2 et g_3 algébriques, E la courbe elliptique associée à $\wp$ et $\mathcal{O}$ l'anneau des endomorphismes de E. Montrer que les assertions suivantes sont équivalentes :

(i) Pour tout entier positif d, le groupe algébrique E^d vérifie la propriété (A.I.).

(ii) Si $u_1,\ldots,u_m$ des éléments de $\mathcal{L}(E)$ linéairement indépendants sur $\mathcal{O}$, alors les nombres $u_1,\ldots,u_m$ sont algébriquement indépendants sur $\mathbb{Q}$.

d) Montrer que si un groupe algébrique G défini sur $\overline{\mathbb{Q}}\cap\mathbb{R}$ vérifie la propriété (A.I.)*, alors il possède la propriété de densité.*

`(Pour de plus amples informations, voir` [W 1996]`)`

§3. Produits de deux groupes algébriques de dimension 1

Dans cette section nous appliquons le théorème de densité (théorème 2.2) aux groupes algébriques de dimension 2 qui sont produits de deux groupes algébriques de dimension 1. Nous avons déjà étudié en détail (au chapitre III) les groupes linéaires $\mathbb{G}_{\mathrm{a}}^2$, $\mathbb{G}_{\mathrm{a}}\times\mathbb{G}_{\mathrm{m}}$ et $\mathbb{G}_{\mathrm{m}}^2$. Il nous reste donc à considérer les produits $\mathbb{G}_{\mathrm{a}}\times E$, $\mathbb{G}_{\mathrm{m}}\times E$ et $E\times E^*$, quand E et E^* sont deux courbes elliptiques.

a) Produit d'un groupe additif par une courbe elliptique

Les produits $\mathbb{G}_{\mathrm{a}}\times E$ font partie des rares groupes algébriques pour lesquels on connaît un énoncé de densité optimal.

Proposition 3.1. – *Soient E une courbe elliptique sur le corps $K = \overline{\mathbb{Q}} \cap \mathbb{R}$, G le groupe algébrique $\mathbb{G}_{\mathrm{a}} \times E$ et Γ un sous-groupe de type fini de $G(K) \cap G(\mathbb{R})^0$. Alors Γ est dense dans $G(\mathbb{R})^0 = \mathbb{R} \times E(\mathbb{R})^0$ si et seulement si les deux projections de Γ sur $\mathbb{R}$ et sur $E(\mathbb{R})^0$ sont denses.*

Par exemple si β_1, β_2 sont des éléments $\mathbb{Q}$-linéairement indépendants de K et 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 $\mathbb{R} \times E(\mathbb{R})^0$.

La proposition 3.1 se déduit de l'analogue elliptique du septième problème de Hilbert – théorème de Schneider cité plus haut (après le corollaire 2.4).

b) Produit d'un groupe multiplicatif par une courbe elliptique

Le théorème 2.2 (ou bien le corollaire 2.5) permet de donner un résultat partiel sur la densité dans $\mathbb{R}_+^\times \times E(\mathbb{R})^0$ de sous-groupes de type fini de $K^\times \times E(K)$, quand E est une courbe elliptique définie sur $K = \overline{\mathbb{Q}} \cap \mathbb{R}$.

Proposition 3.2. – *Soient ℓ, ℓ_1, ℓ_2 des entiers positifs, $\alpha_1, \ldots, \alpha_\ell$ des nombres algébriques réels positifs, qui engendrent un groupe multiplicatif de rang ℓ_1, E une courbe elliptique sur le corps $K = \overline{\mathbb{Q}} \cap \mathbb{R}$ et $\gamma_1, \ldots, \gamma_\ell$ 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 ℓ points (α_j, γ_j), $(1 \le j \le \ell)$ et on suppose que Γ est de rang ℓ.*
a) On suppose $\ell \ge 4$, $\ell_1 \ge 2$ et $\ell_2 \ge 1$. Alors Γ est dense dans $\mathbb{R}_+^\times \times E(\mathbb{R})^0$.
b) On suppose $\ell \ge 5$, $\ell_1 \ge 3$ et $\ell_2 \ge 2$. 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 $\ell_1 \ge 2$ et $\ell_2 \ge 1$.

Pour apporter une réponse complète à la question, il faudrait démontrer l'énoncé suivant, qui est encore une variante elliptique de la conjecture des quatre exponentielles et aussi un cas particulier d'une conjecture de Ramachandra ([Ra 1968], p. 87) citée plus haut :

$\boxed{?}$ *Soient E une courbe elliptique définie sur un corps de nombres réels K, 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 $\mathbb{Q}$.

Cet énoncé signifie 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 $(\lambda, \mu) \in \mathbb{Q}^2$,

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

c) Produit de deux courbes elliptiques

Voici ce que l'on connait sur le problème de densité pour un produit de deux courbes elliptiques. Pour simplifier on traite le cas où les deux courbes ne sont pas isogènes ; cela signifie que si $\wp$ et $\wp^*$ sont les fonctions elliptiques de Weierstraß associées, pour tout $t \in \mathbb{C}^\times$ les deux fonctions $\wp(tz)$ et $\wp^*(z)$ sont algébriquement indépendantes.

Proposition 3.3. – *Soient E et E^* deux courbes elliptiques définies sur $K = \overline{\mathbb{Q}} \cap \mathbb{R}$ et non isogènes. Soient ℓ un entier positif et $\gamma_1, \ldots, \gamma_\ell$ (resp. $\gamma_1^*, \ldots, \gamma_\ell^*$) des éléments de $E(\mathbb{R})^0 \cap E(\overline{\mathbb{Q}})$ (resp. de $E^*(\mathbb{R})^0 \cap E^*(\overline{\mathbb{Q}})$) vérifiant*
a) $\gamma_1, \ldots, \gamma_\ell$ ne sont pas tous des points de torsion dans $E(\overline{\mathbb{Q}})$;
b) $\gamma_1^*, \ldots, \gamma_\ell^*$ ne sont pas tous des points de torsion dans $E^*(\overline{\mathbb{Q}})$;
c) le sous-groupe Γ de $E(\overline{\mathbb{Q}}) \times E^*(\overline{\mathbb{Q}})$ engendré par les ℓ points (γ_j, γ_j^*), $(1 \le j \le \ell)$ est de rang ℓ.
Alors
1) si $\ell \ge 3$, Γ est dense dans $E(\mathbb{R})^0 \times E^*(\mathbb{R})^0$.
2) si $E \times E^*$ possède la propriété de densité, alors la même conclusion est vraie dès que $\ell \ge 1$.

Exercice. Démontrer la partie 1) de la proposition 3.3 :
a) à partir du thèorème 2.2 ;
b) à partir du corollaire 2.6.
Démontrer ensuite une variante de la proposition 3.3 correspondant au cas $E = E^*$.

La conjecture de densité pour le produit $E \times E^*$ implique l'énoncé suivant, conjecturé par Ramachandra :

$\boxed{?}$ *Soient $\wp$ (resp. $\wp^*$) une fonction elliptique de Weierstraß d'invariants g_2, g_3 (resp. g_2^*, g_3^*) algébriques ; soit ω (resp. ω^*) une période non-nulle de $\wp$ (resp. de $\wp^*$), et soit $u \in \mathcal{L}(E)$ (resp. $u^* \in \mathcal{L}(E^*)$) , avec u/ω et u^*/ω^* irrationnels ; on suppose que les deux fonctions $\wp(\omega z)$ et $\wp^*(\omega^* z)$ sont algébriquement indépendantes. Alors les trois nombres*

$$1, \ \frac{u}{\omega}, \ \frac{u^*}{\omega^*}$$

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

En d'autres termes, selon cette conjecture, si s_0, s_0^*, s sont des entiers rationnels, le déterminant

$$\det \begin{pmatrix} \omega & 0 & u \\ 0 & \omega^* & u^* \\ s_0 & s_0^* & s \end{pmatrix}$$

ne peut s'annuler que si $s_0 = s_0^* = s = 0$.

§4. Variétés abéliennes sur $\mathbb{R}$

Nous appliquons le théorème de densité aux variétés abéliennes simples sur un corps de nombres réel. Nous étudions ensuite la propriété de densité pour des produits de courbes elliptiques. Nous terminons en considérant plusieurs plongements réels d'un corps de nombres sur lequel une variété abélienne simple est définie.

a) Variétés abéliennes simples

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 (cf. §2, section e), 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.

Etant donné que, pour une variété abélienne A de dimension d, on a $\mathrm{m}_{\mathbb{R}}(A) = 1$ et $\mathrm{m}'_{\mathbb{R}}(A) = d^2 - d + 1$, on déduit immédiatement du théorème 2.2 :

Proposition 4.1. – *Soient K un corps de nombres plongé dans $\mathbb{R}$, A une variété abélienne simple définie sur K de dimension $d \geq 1$ et Γ un sous-groupe de $A(K)$.*
a) Si le rang de Γ est $\geq d^2 - d + 1$, 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 $\geq d^2$, 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 $\mathrm{rang}_{\mathbb{Z}}\Gamma \geq 1$.

Soit A une variété abélienne sur $\mathbb{R}$; le noyau $\Omega_{A,\mathbb{R}}$ de $\exp_{A,\mathbb{R}}$ contient une base $(e_1, \ldots, e_d)$ de l'espace tangent $T_A(\mathbb{R})$ de $A(\mathbb{R})^0$. Pour $u = x_1 e_1 + \cdots + x_d e_d \in T_A(\mathbb{R})$, une condition nécessaire et suffisante pour que $\gamma = \exp_{A,\mathbb{R}}(u)$ engendre un sous-groupe dense de $A(\mathbb{R})^0$ est que les nombres réels $1, x_1, \ldots, x_d$ soient linéairement indépendants sur $\mathbb{Q}$. En posant $Y = \Omega_{A,\mathbb{R}} + \mathbb{Z}u$, cela s'écrit encore $\mathrm{rang}_{\mathbb{Z}}(Y/Y \cap V) \geq 2$ pour tout hyperplan V de $T_A(\mathbb{R})$. Il suffit évidemment de vérifier cette condition quand $\mathrm{rang}_{\mathbb{Z}}(\Omega_{A,\mathbb{R}}/\Omega_{A,\mathbb{R}} \cap V) \leq 1$, c'est-à-dire quand l'hyperplan V est engendré par des éléments de $\Omega_{A,\mathbb{R}}$. Ainsi $\mathbb{Z}\gamma$ est dense dans $A(\mathbb{R})^0$ si et seulement si, pour toute famille $\omega_1, \ldots, \omega_{d-1}$ d'éléments de $\Omega_{A,\mathbb{R}}$ linéairement indépendants sur $\mathbb{Q}$ (ou sur $\mathbb{R}$, cela revient au même), on a

$$\bigl(\mathbb{R}\omega_1 + \cdots + \mathbb{R}\omega_{d-1}\bigr) \cap \bigl(\mathbb{Z}u + \Omega_{A,\mathbb{R}}\bigr) \subset \mathbb{Q}\omega_1 + \cdots + \mathbb{Q}\omega_{d-1},$$

ce qui s'écrit : pour tout entier $n \geq 1$ et tout $\omega \in \Omega_{A,\mathbb{R}}$, les éléments $nu + \omega, \omega_1, \ldots, \omega_{d-1}$ sont linéairement indépendants sur $\mathbb{R}$(*).

La partie c) de la proposition 4.1 signifie que, pour une variété abélienne simple A sur un sous-corps K de $\overline{\mathbb{Q}} \cap \mathbb{R}$ 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 donc écrire cette assertion de la manière suivante :

(*) Joost van Hamel m'a fait remarquer qu'on ne peut pas se restreindre à $n = 1$ et $\omega = 0$, comme le montre l'exemple $d = 2$, $u = (1/2)\omega_1 + \sqrt{2}\omega_2$.

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

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

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$^?$. – *Soient K un sous-corps de $\overline{\mathbb{Q}}$, 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 $\mathcal{L}(A)$. Alors $u_1, \ldots, u_d$ sont linéairement indépendants sur $\mathbb{C}$.*

Cet énoncé est banal pour $d = 1$. Pour $d = 2$, c'est un analogue abélien de la conjecture des quatre exponentielles (*). 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 (conjecture 5 de [Maz 1992]— voir [W 1994]), il suffirait 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 de la conjecture 4.2$^?$ on déduit :

Conjecture 4.3$^?$. – *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 un sous-groupe à n paramètres de $A(\mathbb{C})$, alors $n \geq \min\{d, \ell\}$.*

Un *sous-groupe à n paramètres* de $A(\mathbb{C})$ est l'image par l'application exponentielle d'un sous-espace vectoriel de dimension n de l'espace tangent.

Cette conjecture 4.3$^?$ a déjà été proposée par S. Lang dans le cas particulier $\ell = 2$ (voir [L 1971], p. 648). A cette époque le seul résultat connu ([L 1966], Chap. II, § 4, Th. 4) était :

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

On sait maintenant que l'on a $\ell d \leq n(\ell + 2d)$ (voir [W 1983b], Corollaire 1.2).

b) Produits de courbes elliptiques

Nous considérons dans cette sous-section une variété abélienne sur le corps $K = \overline{\mathbb{Q}} \cap \mathbb{R}$ qui se décompose en un produit de courbes elliptiques.

Exercice. Montrer que la propriété de densité est vraie pour une puissance d'une courbe elliptique.
`Indication :` utiliser la proposition 1.2.

(*) Dans [W 1994], il est dit que la conjecture 4.2 est facile quand $d = 2$; mais c'est seulement quand $d = 2$ et que u_1 et u_2 sont des périodes, que le résultat est banal – voir [W 1995].

Proposition 4.4. — *Soient $E_1, \dots, E_k$ des courbes elliptiques sur K deux-à-deux non isogènes. Soient $n_1, \dots, n_k$ des entiers positifs. On suppose que le groupe algébrique $G = E_1^{n_1} \times \cdots \times E_k^{n_k}$ possède la propriété de densité. Enfin soit $\gamma \in G(K) \cap G(\mathbb{R})^0$. Alors $\mathbb{Z}\gamma$ est dense dans $G(\mathbb{R})^0$ si et seulement si, pour $1 \le i \le k$, la projection de $\mathbb{Z}\gamma$ est dense dans $E_i^{n_i}(\mathbb{R})^0$.*

Démonstration. Soit H l'adhérence de Zariski de $\mathbb{Z}\gamma$ dans G ; comme les courbes elliptiques E_i sont deux-à-deux non isogènes, H est un produit $H_1 \times \cdots \times H_k$, où H_i est un sous-groupe algébrique de $E_i^{n_i}$. Comme la projection de $\mathbb{Z}\gamma$ est dense dans $E_i^{n_i}(\mathbb{R})^0$, on a $H_i = E_i^{n_i}$ pour $1 \le i \le k$, donc $H = G$. Enfin $m_{\mathbb{R}}(G) = 1$, ce qui permet d'appliquer la propriété de densité. ∎

Exercice. Etendre la proposition 4.4 à un produit de variétés abéliennes deux-à-deux non isogènes. Remplacer aussi le sous-groupe $\mathbb{Z}\gamma$ de rang 1 par un sous-groupe de rang > 0 quelconque.

Remarque. Soit $G = G_1 \times G_2$ un produit de deux groupes algébriques ; on suppose que G n'admet pas d'autre sous-groupe algébrique connexe que les produits $H_1 \times H_2$; soit Γ un sous-groupe de type fini de $G(\mathbb{R})$; même si G possède la propriété de densité, il ne suffit pas que les projections de Γ sur chaque facteur soient denses pour assurer que Γ est dense : par exemple le fait que les projections soient denses n'implique pas $\mathrm{rang}_{\mathbb{Z}}\Gamma \ge m_{\mathbb{R}}(G)$.

c) Plusieurs plongements

Un autre exemple d'application du théorème 2.2 provient d'une question posée par A. Ogg au M.S.R.I. 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 ?*

Dans le cas où les variétés abéliennes $A_1, \dots, A_r$ sont deux-à-deux non isogènes(*), en supposant que la variété abélienne B possède la propriété de densité, une condition nécessaire et suffisante est encore que $\varphi(\Gamma)$ soit Zariski dense dans B. Cela résulte de la remarque suivante

> *si une variété abélienne B sur un corps K est produit de variétés abéliennes simples deux-à-deux non isogènes, 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.*

Démonstration. On écrit B comme produit de variétés abéliennes simples $A_1, \dots, A_r$ deux-à-deux non isogènes : un sous-groupe algébrique connexe B' de B est un produit

(*) Cette hypothèse a été omise dans [W 1994], mais elle est évidemment nécessaire : si $B = A^2$ est le carré d'une variété abélienne A, et si η est un point d'ordre infini de $A(K)$, alors $\Gamma = \mathbb{Z}(\eta, 0) + \mathbb{Z}(0, \eta) \subset A(K)^2$ est un sous-groupe de $B(K)$ Zariski dense dans B, mais il n'existe pas de $\gamma \in \Gamma$ qui engendre un sous-groupe $\mathbb{Z}\gamma$ Zariski dense dans B – voir [W 1995].

$B_1' \times \cdots \times B_r'$ où chaque B_i' est soit A_i, soit $\{0\}$. Un sous-groupe de type fini de $B(K)$ est Zariski dense dans B si et seulement si pour tout $i = 1, \dots, r$, son image par la projection $\pi_i : B(K) \to A_i(K)$ n'est pas contenue dans $A_i(K)_{\mathrm{tors}}$. On choisit ℓ éléments $\gamma_1, \dots, \gamma_\ell$ de Γ, linéairement indépendants sur $\mathbb{Z}$, avec $\ell = \mathrm{rang}_{\mathbb{Z}}\Gamma$. Pour $1 \le i \le r$, désignons par M_i le sous-$\mathbb{Z}$-module de $\mathbb{Z}^\ell$ formé des $s \in \mathbb{Z}^\ell$ tels que $\gamma_s = s_1\gamma_1 + \cdots + s_\ell\gamma_\ell$ vérifie $\pi_i(\gamma_s) \in A_i(K)_{\mathrm{tors}}$; comme Γ est Zariski dense dans B, M_i est un sous-groupe de $\mathbb{Z}^\ell$ de rang $\le \ell - 1$. Le nombre d'éléments de M_i dont les composantes sont majorées par N est $O(N^{\ell-1})$ quand $N \to \infty$. Il en résulte (*) que la réunion $M_1 \cup \cdots \cup M_r$ est distincte de $\mathbb{Z}^\ell$: soit $s \in \mathbb{Z}^\ell$ en dehors de cette réunion. Alors $\mathbb{Z}\gamma_s$ est Zariski dense dans B. ∎

Noter que le sous-groupe $\Gamma = \mathbb{Z}(\gamma, 0) + \mathbb{Z}(0, \gamma)$ de $A(K)^2$ est Zariski dense dans A^2 si γ est un point d'ordre infini de $A(K)$, mais aucun sous-groupe de Γ de rang 1 n'est Zariski dense dans A^2.

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

Corollaire 4.5. – *Soient K un sous-corps de $\mathbb{R} \cap \overline{\mathbb{Q}}$, 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 Γ un sous-groupe de $A(K)$ de rang ℓ.*

a) On suppose $\ell \ge 4d^2 - 2d + 1$. On suppose de plus, pour toute sous-variété abélienne B' de B, définie sur K, de dimension d,

$$\mathrm{rang}_{\mathbb{Z}}\bigl(\varphi(\Gamma)/\varphi(\Gamma) \cap B'(K)\bigr) \ge d^2 - d + 1.$$

Alors $\varphi(\Gamma) \cap B(\mathbb{R})^0$ est dense dans $B(\mathbb{R})^0$.

b) On suppose $\ell \ge 4d^2$. On suppose de plus, pour toute sous-variété abélienne B' de B, définie sur K, de dimension d,

$$\mathrm{rang}_{\mathbb{Z}}\bigl(\varphi(\Gamma)/\varphi(\Gamma) \cap B'(K)\bigr) \ge d^2 + d.$$

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

$$\mathrm{rang}_{\mathbb{Z}}\bigl(\varphi(\Gamma)/\varphi(\Gamma) \cap B'(K)\bigr) \ge 1$$

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

(*) Dans la section 4f de [W 1994], p. 346, est écrit : *une réunion finie de sous-groupes de $\mathbb{Z}^\ell$ distincte de $\mathbb{Z}^\ell$ est encore distincte de $\mathbb{Z}^\ell$*. Comme me l'a fait remarquer J-P. Serre, $\mathbb{Z}^2$ est réunion de trois sous-groupes d'indice 2, par exemple $(2\mathbb{Z})\times\mathbb{Z}$, $\mathbb{Z}\times(2\mathbb{Z})$ et $\mathbb{Z}(1,1)+\mathbb{Z}(1,-1)$. Mais *une réunion finie de sous-groupes de $\mathbb{Z}^\ell$ de rang $\le \ell - 1$ est distincte de $\mathbb{Z}^\ell$* – voir [W 1995].

éléments de Γ soient tous rationnels sur ce sous-corps. Un exemple concret – cité au §1 – est donné par la courbe elliptique $y^2 = x^3 - 50x - 125$ avec le corps $\mathbb{Q}(\sqrt{10})$.

§5. Extensions

Nous étudions d'abord les extensions d'une courbe elliptique par $\mathbb{G}_{\mathrm{a}}$, puis les extensions par $\mathbb{G}_{\mathrm{m}}$, et enfin les extensions d'une variété abélienne par $\mathbb{G}_{\mathrm{m}}$.

a) Extension d'une courbe elliptique par le groupe additif
(Voir [W 1979], Chap. 3, §2c).

Soit G un groupe algébrique commutatif connexe de dimension 2, extension non triviale d'une courbe elliptique E par le groupe additif $\mathbb{G}_{\mathrm{a}}$. Le groupe algébrique G possède trois sous-groupes algébriques connexes, à savoir $\{0\}$, G, et un sous-groupe isomorphe à $\mathbb{G}_{\mathrm{a}}$. Soit $\wp$ la fonction elliptique de Weierstrass associée à $E(\mathbb{C})$; on peut choisir une base de l'espace tangent de $G(\mathbb{C})$ et un plongement de $G(\mathbb{C})$ comme sous-variété quasi-projective d'un espace projectif tels que l'application exponentielle de $G(\mathbb{C})$ soit paramétrée par des fonctions complexes de deux variables (z_1, z_2), parmi lesquelles se trouvent $z_2 - \zeta(z_1)$ et $\wp(z_1)$, où ζ est la primitive impaire de $\wp$. Comme $\wp$ est périodique, ζ est quasi-périodique : si $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ désigne le réseau des périodes de $\wp$, il existe deux nombres complexes η_1 et η_2 tels que

$$\zeta(z + \omega_i) = \zeta(z) + \eta_i, \qquad (i = 1, 2).$$

Ces nombres complexes sont reliés par la *relation de Legendre* :

$$\omega_1\eta_2 - \omega_2\eta_1 = \pm 2i\pi$$

(le signe dépend du signe de la partie imaginaire de ω_2/ω_1 ; voir par exemple [Sil 1986], Chap.6, ex. 6.4). Si G est défini sur un sous-corps K de $\mathbb{C}$, alors les invariants g_2 et g_3 de $\wp$ sont dans K, et $\mathcal{L}_K(G)$ est la réunion de Ker $\exp_G = \mathbb{Z}(\omega_1, \eta_1) + \mathbb{Z}(\omega_2, \eta_2)$, et de

$$\bigl\{(z_1, z_2) \in \mathbb{C}^2\ ;\ z_1 \notin \Omega,\ z_2 - \zeta(z_1) \in K,\ \wp(z_1) \in K\bigr\}.$$

Si le groupe G est défini sur $\mathbb{R}$, alors le noyau de $\exp_{G,\mathbb{R}}$ est un sous-groupe de rang 1 de $\mathbb{R}^2$ engendré par un élément de la forme (ω, η), avec $\omega = m_1\omega_1 + m_2\omega_2$ et $\eta = m_1\eta_1 + m_2\eta_2$, $((m_1, m_2) \in \mathbb{Z}^2)$. Le *sous-groupe compact maximal* G^c de $G(\mathbb{R})^0$ est l'image par $\exp_G$ de la droite vectorielle $\mathbb{R}(\omega, \eta)$ engendrée par le noyau, et le quotient $G(\mathbb{R})^0/G^c$ est isomorphe à $\mathbb{R}$. En particulier on a $\mathrm{m}_{\mathbb{R}}(G) = \mathrm{m}\bigl(G(\mathbb{R})\bigr) = 2$. Le sous-groupe de torsion de $G(\mathbb{R})$ est

$$G(\mathbb{R})_{\mathrm{tors}} = \exp_{G,\mathbb{R}}\bigl(\mathbb{Q}(\omega, \eta)\bigr) \subset G^c.$$

Les parties a) et b) du théorème 5.1 ci-dessous proviennent de [Be 1995]. Elles utilisent le résultat de transcendance suivant :

Soient E une courbe elliptique définie sur $\overline{\mathbb{Q}}$, $\omega \in \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ une période non nulle de la fonction de Weierstraß $\wp$ associée à $E(\mathbb{C})$, η la quasi-période correspondante

de la fonction ζ et $u \in \mathcal{L}(E)$ un logarithme elliptique qui n'est pas de torsion : $u \notin \mathbb{Q}\omega_1 + \mathbb{Q}\omega_2$. On pose $\lambda_u(\omega) = \omega\zeta(u) - \eta u$. Alors les trois nombres

$$\lambda_u(\omega),\ \omega,\ u$$

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

Il s'agit d'un analogue du théorème de Baker, dû à Wüstholz [Wü 1989], et que l'on peut déduire de la version raffinée du théorème du sous-groupe algébrique (voir la remarque avant le corollaire 2.5) appliquée à une extension non triviale d'une courbe elliptique par le groupe multiplicatif $\mathbb{G}_{\mathrm{m}}$.

Théorème 5.1. – *Soit G un groupe algébrique commutatif connexe de dimension 2 défini sur un corps de nombres réel K. On suppose que G est extension d'une courbe elliptique E par le groupe additif $\mathbb{G}_{\mathrm{a}}$, et n'est pas isogène au produit $\mathbb{G}_{\mathrm{a}} \times E$. On note $\pi : G(K) \to E(K)$ la projection de noyau $\mathbb{G}_{\mathrm{a}}(K) \simeq K$.*
a) Tout point de $G(K) \cap G^c$ est d'ordre fini.
b) Si Γ est un sous-groupe de type fini de $G(K) \cap G(\mathbb{R})^0$ vérifiant

$$\mathrm{rang}_{\mathbb{Z}}\pi(\Gamma) \geq 1 \qquad \textit{et} \qquad \mathrm{rang}_{\mathbb{Z}}\bigl(\Gamma \cap \mathbb{G}_{\mathrm{a}}(K)\bigr) \geq 1,$$

alors Γ est dense dans $G(\mathbb{R})^0$.
c) Si Γ vérifie

$$\mathrm{rang}_{\mathbb{Z}}\pi(\Gamma) \geq 1 \qquad \textit{et} \qquad \mathrm{rang}_{\mathbb{Z}}\Gamma \geq 5,$$

alors Γ est dense dans $G(\mathbb{R})^0$.
d) Si G possède la propriété de densité, et si Γ vérifie

$$\mathrm{rang}_{\mathbb{Z}}\pi(\Gamma) \geq 1 \qquad \textit{et} \qquad \mathrm{rang}_{\mathbb{Z}}\Gamma \geq 2,$$

alors Γ est dense dans $G(\mathbb{R})^0$.

Démonstration.
a) Soit $\gamma \in G(K) \cap G^c$; on écrit $\gamma = \exp_G(u, v)$; l'hypothèse $\gamma \in G(K)$ s'écrit $u \in \mathcal{L}_K(E)$ et $\alpha = -v + \zeta(u) \in K$. Le fait que γ appartienne au sous-groupe compact maximal G^c de $G(\mathbb{R})^0$ signifie que (u, v) se trouve sur la droite $\mathbb{R}(\omega, \eta)$. Alors $\lambda_u(\omega) = \omega\zeta(u) - \eta u = \alpha\omega$, et le résultat de transcendance cité plus haut entraîne que u appartient à $\mathbb{Q}\omega_1 + \mathbb{Q}\omega_2$. La relation de Legendre donne alors $u \in \mathbb{Q}\omega$, donc γ est un point de torsion de $G(K)$.
b) Si Γ contient un point non nul γ_0 dans $\mathbb{G}_{\mathrm{a}}(K)$ et un point γ tel que $\pi(\gamma)$ ne soit pas de torsion dans $E(K)$, alors $Y = \exp_G^{-1}(\Gamma)$ est un sous-groupe de type fini de $\mathbb{R}^2$ qui contient trois éléments de la forme $(0, \beta)$, $(u, \zeta(u) - \alpha)$ et (ω, η), avec $u \in \mathcal{L}_K(E)$ et α, β dans K, $\beta \neq 0$. Les coordonnées de $(u, \zeta(u) - \alpha)$ dans la base $\bigl((0, \beta),\ (\omega, \eta)\bigr)$ de $\mathbb{R}^2$ sont u/ω et $\bigl(\zeta(u) - \alpha - (u/\omega)\eta\bigr)/\beta$, et les trois nombres

$$\beta\omega,\ \beta u,\ \omega\zeta(u) - \alpha\omega - \eta u$$

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

c) La partie c) du théorème 5.1 résulte du théorème de densité 2.2, compte tenu de l'égalité $\mathrm{m}'_{\mathbb{R}}(G) = 5$.
d) Grâce à b), on peut se limiter au cas où $\Gamma \cap \mathbb{G}_{\mathrm{a}}(K) = \{0\}$. Soient γ_1 et γ_2 deux éléments de Γ linéairement indépendants sur $\mathbb{Z}$. Les hypothèses faites impliquent que tout sous-groupe algébrique de $G \times G$ contenant le point (γ_1, γ_2) se projette surjectivement sur $E \times E$. Par conséquent l'adhérence de Zariski de $\mathbb{Z}(\gamma_1, \gamma_2)$ dans $G \times G$ est $G \times G$. Il ne reste plus qu'à utiliser l'égalité $\mathrm{m}_{\mathbb{R}}(G) = 2$. □

Exercice (Un analogue elliptique du problème des quatre exponentielles, d'après [Be 1995], question 3.)
Montrer que le groupe algébrique G considéré dans le théorème 5.1 possède la propriété de densité si et seulement si l'assertion suivante est vraie :
$\boxed{?}$ *Soient α et β deux nombres algébriques réels, et u, v deux nombres réels dans $\mathcal{L}(E)$, avec u, v, ω linéairement indépendants sur $\mathbb{Q}$. Alors*

$$\frac{\lambda_u(\omega) - \alpha\omega}{u} \neq \frac{\lambda_v(\omega) - \beta\omega}{v}.$$

`Indication.` Montrer déjà que la propriété de densité pour G est équivalente à l'assertion suivante :
$\boxed{?}$ *Soient u et v des éléments de $\mathcal{L}(E) \cap \mathbb{R}$ avec ω, u, v linéairement indépendants sur $\mathbb{Q}$, et soient α et β deux nombres algébriques. On pose*

$$\theta_u = \lambda_u(\omega) + \alpha u, \quad \theta_v = \lambda_v(\omega) + \beta v.$$

Alors les trois nombres $\omega\theta_u$, $\omega\theta_v$, $u\theta_v - v\theta_u$ sont linéairement indépendants sur $\mathbb{Q}$.

En particulier on devrait avoir $u\theta_v \neq v\theta_u$, ce qui est la condition annoncée. Dans l'autre sens, poser $u' = au + c\omega$ et $v' = av - b\omega$, et utiliser le fait que la fonction $\zeta(az) - a\zeta(z)$ est elliptique, donc le nombre $\zeta(au) - a\zeta(u)$ est algébrique.

Exercice. Soit G un groupe algébrique commutatif connexe sur $\overline{\mathbb{Q}}$, extension non triviale d'une courbe elliptique E définie sur $\overline{\mathbb{Q}}$ par $\mathbb{G}_{\mathrm{a}}$. Soient ℓ un entier et (u_j, v_j) $(1 \le j \le \ell)$ des éléments de $\mathcal{L}(G)$ linéairement indépendants sur $\mathbb{Q}$, avec $u_j \in \mathcal{L}(E)$. On suppose que $u_1, \dots, u_\ell$ ne sont pas tous dans $\mathbb{Q}\omega_1 + \mathbb{Q}\omega_2$.
1) On suppose $\ell \ge 5$; montrer que la matrice

$$\begin{pmatrix} u_1 & \cdots & u_\ell \\ v_1 & \cdots & v_\ell \end{pmatrix}$$

est de rang 2.
2) On suppose $\ell = 4$ et $(u_1, v_1) \in \mathrm{Ker}\ \exp_G$; montrer que la matrice

$$\begin{pmatrix} u_1 & u_2 & u_3 & u_4 \\ v_1 & v_2 & v_3 & v_4 \end{pmatrix}$$

est de rang 2.

b) Extension d'une courbe elliptique par le groupe multiplicatif
(Voir [W 1979], Chap. 3, §2e).

Soit G un groupe algébrique commutatif connexe de dimension 2, qui est une extension d'une courbe elliptique E par le groupe additif $\mathbb{G}_{\mathrm{m}}$, et qui n'est pas isogène au produit $\mathbb{G}_{\mathrm{m}} \times E$. Le groupe algébrique G possède trois sous-groupes algébriques connexes, à savoir $\{0\}$, G, et un sous-groupe isomorphe à $\mathbb{G}_{\mathrm{m}}$. Soient $\wp$ la fonction elliptique de Weierstraß associée à $E(\mathbb{C})$, $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ le réseau des périodes de $\wp$ et σ le produit canonique de Weierstrass associé à Ω (cf. [Sil 1986], Chap. 6 §3). On peut choisir une base de l'espace tangent de $G(\mathbb{C})$ et un plongement de $G(\mathbb{C})$ comme sous-variété quasi-projective d'un espace projectif, tels que l'application exponentielle de $G(\mathbb{C})$ soit paramétrée par des fonctions complexes de deux variables (z_1, z_2), parmi lesquelles se trouvent $\wp(z_1)$, et une fonction

$$F_u(z_1, z_2) = \frac{\sigma(z_1 - u)}{\sigma(z_1)\sigma(u)} e^{z_1\zeta(u) - z_2},$$

où $u \in \mathbb{C}$. L'hypothèse que G n'est pas isogène au produit $\mathbb{G}_{\mathrm{m}} \times E$ se traduit par le fait que le point $\gamma = \exp_E(u) \in E(\mathbb{C})$ n'est pas de torsion, c'est-à-dire $u \notin \mathbb{Q}\omega_1 + \mathbb{Q}\omega_2$.

Quand le groupe algébrique G est défini sur $\mathbb{R}$, le noyau de $\exp_{G,\mathbb{R}}$ est un sous-groupe de rang 1 de $\mathbb{R}^2$; la droite réelle engendrée a pour image par l'exponentielle le sous-groupe compact maximal G^c de $G(\mathbb{R})^0$ et $G(\mathbb{R})^0/G^c$ est isomorphe à $\mathbb{R}$.

Si la courbe elliptique E est définie sur un corps de nombres K plongé dans $\mathbb{R}$ et que le groupe de Mordell-Weil $E(K)$ a un rang positif, alors à chaque point $\gamma \in E(K)$ correspond une extension G_γ de E par $\mathbb{G}_{\mathrm{m}}$, définie sur K, et $G_\gamma(K)$ se projette sur $E(K)$. Quand γ est d'ordre infini dans $E(K)$, *l'adhérence réelle de $G_\gamma(K)$ dans $G_\gamma(\mathbb{R})$ contient $G_\gamma(\mathbb{R})^0$*. En effet, comme $G_\gamma(K)$ contient $\mathbb{G}_{\mathrm{m}}(K) \simeq K^*$, si η est un point de $G_\gamma(K)$ dont la projection sur $E(K)$ est γ, alors le sous-groupe de $G_\gamma(K)$ 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.

Proposition 5.2. – *Soient K un corps de nombres réel, E une courbe elliptique définie sur K, γ un point d'ordre infini de $E(K)$, G_γ l'extension de E par le groupe multiplicatif $\mathbb{G}_{\mathrm{m}}$ attachée à γ, $\pi : G_\gamma(K) \to E(K)$ la projection de noyau $\mathbb{G}_{\mathrm{m}}(K) \simeq K^\times$, et Γ un sous-groupe de type fini de $G_\gamma(K) \cap G_\gamma(\mathbb{R})^0$, de rang ℓ. On note ℓ_1 le rang sur $\mathbb{Z}$ de $\pi(\Gamma)$.*
a) Si $\ell - \ell_1 \ge 2$ et $\ell_1 \ge 1$, alors Γ est dense dans $G_\gamma(\mathbb{R})^0$.
b) Si $\ell \ge 5$ et $\ell_1 \ge 1$, alors Γ est dense dans $G_\gamma(\mathbb{R})^0$.
c) Si $\ell \ge 6$ et $\ell_1 \ge 1$, alors Γ contient un sous-groupe de rang 2 qui est encore dense dans $G_\gamma(\mathbb{R})^0$.
d) Si le groupe algébrique G_γ possède la propriété de densité, alors les deux conditions suivantes sont équivalentes :
(i) Γ est dense dans $G_\gamma(\mathbb{R})^0$;
(ii) on a $\ell \ge 2$ et $\ell_1 \ge 1$.

Démonstration.
a) Le rang de $\Gamma_1 = \Gamma \cap \mathbb{G}_{\mathrm{m}}(K)$ est $\ell - \ell_1$. Soit $Y = \exp_{G_\gamma}^{-1}(\Gamma)$ et soit H un hyperplan de $\mathbb{R}^2$. Si $H = \{0\} \times \mathbb{R}$, on utilise l'hypothèse $\ell_1 \geq 1$ pour en déduire $\mathrm{rang}_{\mathbb{Z}}\big(Y/Y \cap H\big) \geq \ell_1 + 1 \geq 2$. Si au contraire $H \neq \{0\} \times \mathbb{R}$, alors en posant $Y_1 = Y \cap \big(\{0\} \times K\big)$ on a $Y \supset Y_1$ et

$$\mathrm{rang}_{\mathbb{Z}}\big(Y/Y \cap H\big) \geq \mathrm{rang}_{\mathbb{Z}} Y_1 = \mathrm{rang}_{\mathbb{Z}} \Gamma_1 = \ell - \ell_1 \geq 2.$$

b) Si $\ell \geq 5$ et $\ell_1 \geq 1$, alors les hypothèses de la partie *a)* du théorème 2.2 sont vérifiées, avec

$$d = d_2 = 2, \quad d_0 = d_1 = 0, \quad \alpha(G_\gamma) = 4, \quad \kappa_{\mathbb{R}}(G_\gamma) = 1, \quad m'_{\mathbb{R}}(G_\gamma) = 5,$$

donc Γ est dense dans $G_\gamma(\mathbb{R})^0$.
c) Si $\ell \geq 6$, les hypothèses de la partie *b)* du théorème 2.2 sont vérifiées, et Γ contient un sous-groupe de rang 2 qui est encore dense dans $G_\gamma(\mathbb{R})^0$.
d) L'implication $(i) \Rightarrow (ii)$ résulte des égalités $\mathrm{m}_{\mathbb{R}}(G_\gamma) = 2$ et $\mathrm{m}_{\mathbb{R}}(E) = 1$. Dans l'autre sens, on désigne par $(\omega, \vartheta) \in \mathbb{R}^2$ 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

$$(0, x), \qquad (y, z) \quad \text{et} \quad (\omega, \vartheta)$$

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. $\square$

Remarque. La propriété de densité pour le groupe G_γ de la proposition 5.2 s'énonce de la manière suivante :
Pour le cas $\mathrm{rang}_{\mathbb{Z}}\big(\Gamma \cap \mathbb{G}_{\mathrm{m}}(K)\big) \geq 1$ *:*

$\boxed{?}$ *Si α est un nombre algébrique positif $\neq 1$, si u et u_0 sont deux éléments de $\mathcal{L}(E) \cap \mathbb{R}$ qui n'appartiennent pas à $\mathbb{Q}\omega$, et si $v \in \mathbb{R}$ est tel que le nombre*

$$\frac{\sigma(u - u_0)}{\sigma(u)\sigma(u_0)} e^{u\zeta(u_0) - v}$$

est algébrique, alors les trois nombres

$$u \log \alpha, \ \omega \log \alpha, \ u\vartheta - v\omega$$

sont linéairement indépendants sur $\mathbb{Q}$.
Pour le cas $\mathrm{rang}_{\mathbb{Z}}\big(\Gamma \cap \mathbb{G}_{\mathrm{m}}(K)\big) = 0$ *:*

$\boxed{?}$ *Soient u_0, u_1, u_2 des éléments de $\mathcal{L}(E) \cap \mathbb{R}$ avec $u_0 \notin \mathbb{Q}\omega$ et ω, u_1, u_2 linéairement indépendants sur $\mathbb{Q}$; soient v_1 et v_2 deux nombres réels tels que les nombres*

$$\frac{\sigma(u_i - u_0)}{\sigma(u_i)\sigma(u_0)} e^{u_i\zeta(u_0) - v_i} \qquad (i = 1, 2)$$

soient algébriques, alors les trois nombres

$$u_1v_2 - u_2v_1, \ u_1\vartheta - v_1\omega, \ u_2\vartheta - v_2\omega$$

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

Exercice. Soit G un groupe algébrique commutatif connexe sur $\overline{\mathbb{Q}}$, extension d'une courbe elliptique E définie sur $\overline{\mathbb{Q}}$ par $\mathbb{G}_{\mathrm{m}}$, qui n'est pas isogène au produit $\mathbb{G}_{\mathrm{m}} \times E$. Soient ℓ un entier et (u_j, v_j) $(1 \leq j \leq \ell)$ des éléments de $\mathcal{L}(G)$ linéairement indépendants sur $\mathbb{Q}$, avec $u_j \in \mathcal{L}(E)$. On suppose que $u_1, \ldots, u_\ell$ ne sont pas tous dans $\mathbb{Q}\omega_1 + \mathbb{Q}\omega_2$.
1) On suppose $\ell \geq 5$; montrer que la matrice

$$\begin{pmatrix} u_1 & \cdots & u_\ell \\ v_1 & \cdots & v_\ell \end{pmatrix}$$

est de rang 2.
2) On suppose $\ell = 4$ et $(u_1, v_1) \in$ Ker $\exp_G$; montrer que la matrice

$$\begin{pmatrix} u_1 & u_2 & u_3 & u_4 \\ v_1 & v_2 & v_3 & v_4 \end{pmatrix}$$

est de rang 2.

c) Extension d'une variété abélienne par un groupe multiplicatif
(Voir [Be 1995])

Soit A une variété abélienne simple de dimension g sur un corps de nombres réel K, et soit L le groupe $\mathbb{G}_{\mathrm{a}}$ ou bien $\mathbb{G}_{\mathrm{m}}$. On considère un groupe algébrique commutatif connexe G, défini sur K, de dimension $d = g + 1$, extension de A par L, non isogène au produit $L \times A$. Les applications exponentielles font commuter le diagramme suivant :

$$\begin{array}{ccccccccc}
0 & \to & T_L(\mathbb{R}) & \to & T_G(\mathbb{R}) & \to & T_A(\mathbb{R}) & \to & 0 \\
 & & \downarrow{\scriptstyle \exp_{L,\mathbb{R}}} & & \downarrow{\scriptstyle \exp_{G,\mathbb{R}}} & & \downarrow{\scriptstyle \exp_{A,\mathbb{R}}} & & \\
0 & \to & L(\mathbb{R})^0 & \to & G(\mathbb{R})^0 & \to & A(\mathbb{R})^0 & \to & 0
\end{array}$$

Comme $\Omega_{A,\mathbb{R}} = \mathrm{Ker}\ \exp_{A,\mathbb{R}}$ est un réseau de $T_A(\mathbb{R}) \simeq \mathbb{R}^g$ et que $\exp_{L,\mathbb{R}}$ est injective, le noyau $\Omega_{G,\mathbb{R}}$ de $\exp_{G,\mathbb{R}}$ est un sous-groupe discret de $T_G(\mathbb{R}) \simeq \mathbb{R}^d$ de rang $g = d - 1$. L'hyperplan réel $\mathbb{R}\Omega_{G,\mathbb{R}}$ de $T_G(\mathbb{R})$ a pour image par $\exp_{G,\mathbb{R}}$ le sous-groupe compact maximal G^c de $G(\mathbb{R})^0$. En tant que groupe de Lie réel, G^c est isomorphe à $\mathbb{R}^g/\Omega_{A,\mathbb{R}}$, donc à $A(\mathbb{R})$, mais G^c n'est pas un sous-groupe algébrique de $G(\mathbb{R})$: les seuls sous-groupes algébriques connexes de G sont $\{0\}$, L et G.

Proposition 5.3. [Be 1995]– *Si G vérifie la propriété de densité, tout point de $G(K) \cap G^c$ est d'ordre fini.*

Démonstration. Supposons qu'il existe un point $\gamma \in G(K) \cap G^c$ n'appartenant pas à $G(K)_{\mathrm{tors}}$. On choisit un point γ_0 dans $L(K) \cap L(\mathbb{R})^0$ d'ordre infini. Le sous-groupe

$\Gamma = \mathbb{Z}\gamma_0 + \mathbb{Z}\gamma$ de $G(K)$ est de rang 2, sa projection sur $A(K)$ est de rang 1. L'image inverse Y de Γ par $\exp_{G,\mathbb{R}}$ est le sous-groupe de $T_G(\mathbb{R})$ engendré par $\Omega_{G,\mathbb{R}}$ et $\mathbb{Z}u_0 + \mathbb{Z}u$, quand u_0 et u sont deux éléments de $T_G(\mathbb{R})$ satisfaisant $\exp_{G,\mathbb{R}}(u_0) = \gamma_0$ et $\exp_{G,\mathbb{R}}(u) = \gamma$. Mais $\gamma \in G^c$, donc $u \in \mathbb{R}\Omega_{G,\mathbb{R}}$, et la projection de Y sur $T_G(\mathbb{R})/\mathbb{R}\Omega_{G,\mathbb{R}}$ a un rang ≤ 1. Ceci montre que Y n'est pas dense dans $T_G(\mathbb{R})$, ce qui veut dire que Γ n'est pas dense dans $G(\mathbb{R})^0$.

Soit H l'adhérence de Zariski du sous-groupe $\mathbb{Z}(\gamma_0, \gamma)$ dans $G \times G$. Comme γ_0 appartient à $L(K)$, que la projection de γ dans $A(K)$ est d'ordre infini, et que l'extension G de A par L n'est pas isotriviale, on a $H = L \times G$. On en déduit qu'il existe (η_1, η_2) dans $H(\mathbb{R})$ tel que $\mathbb{Z}\eta_1 + \mathbb{Z}\eta_2$ soit dense dans $G(\mathbb{R})^0$: il suffit de prendre $n+1$ nombres réels, ou plutôt deux éléments x, z de $T_L(\mathbb{R}) \simeq \mathbb{R}$ et un élément $y \in T_A(\mathbb{R}) \simeq \mathbb{R}^g$, tels que le sous-groupe de $T_G(\mathbb{R}) \simeq T_A(\mathbb{R}) \times T_L(\mathbb{R})$ engendré par $(0, x)$, (y, z) et $\Omega_{G,\mathbb{R}}$ soit dense dans $T_G(\mathbb{R})$. Par conséquent si $G(K) \cap G^c \not\subset G(K)_{\mathrm{tors}}$, alors G ne vérifie pas la propriété de densité. $\square$

Remarque. Dans [Be 1995], D. Bertrand construit une surface abélienne (variété abélienne de dimension 2, quotient de la Jacobienne de la courbe modulaire $X_1(29)$), définie sur un corps de nombres totalement réel K de degré 4 sur $\mathbb{Q}$, et une extension non isotriviale G de A par $\mathbb{G}_{\mathrm{m}}$, telles que $G(K) \cap G^c$ contienne des points d'ordre infini. Ce groupe algébrique G, de dimension 3, ne vérifie donc pas la propriété de densité.

§6. Groupes algébriques commutatifs sur $\mathbb{C}$

a) Restriction des scalaires

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 $\mathbb{R}$ (cf. [We 1982], Chap. 1 §3, [Gr 1960], et la thèse de Johan Huisman [Hu 1992] pour la restriction relative à une extension galoisienne finie) : on a une application $p : \widetilde{G} \to G$ définie sur $\mathbb{C}$ qui donne un isomorphisme $(p, \overline{p}) : \widetilde{G} \to G \times \overline{G}$ 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 $\overline{K}$ de $\mathbb{C}$, conjugué complexe de K, puis un groupe algébrique $\overline{G}$ défini sur $\overline{K}$, un isomorphisme de groupes $\gamma \longmapsto \overline{\gamma}$ de $G(\mathbb{C})$ sur $\overline{G}(\mathbb{C})$ puis un homomorphisme de groupes φ de $G(\mathbb{C})$ dans $G(\mathbb{C}) \times \overline{G}(\mathbb{C})$ qui envoie γ sur $(\gamma, \overline{\gamma})$, et enfin un $\mathbb{C}$–isomorphisme θ de $\widetilde{G}(\mathbb{C})$ sur $G(\mathbb{C}) \times \overline{G}(\mathbb{C})$. Si $s : \overline{G}(\mathbb{C}) \times G(\mathbb{C}) \to G(\mathbb{C}) \times \overline{G}(\mathbb{C})$ envoie (z, w) sur (w, z), on a $s \circ \overline{\theta} = \theta$:

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

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

$$\theta\big(\widetilde{G}(\mathbb{R})\big) = \big\{(\gamma, \overline{\gamma}) \; ; \; \gamma \in G(\mathbb{C})\big\} = \varphi\big(G(\mathbb{C})\big) \subset G(\mathbb{C}) \times \overline{G}(\mathbb{C}).$$

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

$$T_{\widetilde{G}}(\mathbb{R}) = \big\{(z, \overline{z}) \; ; \; z \in T_G(\mathbb{C})\big\} \subset T_{\widetilde{G}}(\mathbb{C}) = T_G(\mathbb{C}) \times T_{\overline{G}}(\mathbb{C})$$

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 $\overline{K}$; quitte à remplacer K par son compositum avec $\overline{K}$, on peut supposer $K = \overline{K}$ (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 $\widetilde{G} = \mathrm{Res}_{K/\widetilde{K}} G$.

b) Application à la densité

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 :

Si le groupe algébrique $\widetilde{G}$ possède la propriété de densité, 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 $\gamma_1, \ldots, \gamma_\ell$ engendrent un sous-groupe d'indice fini de Γ et si H désigne l'adhérence de Zariski dans $\widetilde{G}^\ell$ du sous-groupe $\mathbb{Z}\big(\varphi(\gamma_1), \ldots, \varphi(\gamma_\ell)\big)$, il existe un élément $(\eta_1, \ldots, \eta_\ell)$ de $H(\mathbb{R})$ tel que le sous-groupe $\mathbb{Z}\eta_1 + \cdots + \mathbb{Z}\eta_\ell$ soit dense dans $\widetilde{G}(\mathbb{R})$.

Voici un résultat de densité pour un plongement complexe, qui résulte immédiatement du théorème 2.2 combiné avec la version complexe du théorème de Kronecker.

Proposition 6.1. – *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 $\dim G' < \dim \widetilde{G}$,

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

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 $\dim G' < \dim \widetilde{G}$,

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

Alors il existe un sous-groupe de Γ de rang $\mathrm{m}_{\mathbb{C}}(G)$ qui est dense (pour la topologie complexe) dans $G(\mathbb{C})$.

La proposition 6.1 permet de montrer que pour tout groupe algébrique commutatif connexe G défini sur $\overline{\mathbb{Q}}$, il existe un corps de nombres K tel que $G(K)$ contienne un sous-groupe de rang $\mathrm{m}_{\mathbb{C}}(G)$ 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 connexe défini sur $\mathbb{C}$, on pose

$$\mathrm{m}'_{\mathbb{C}}(G) = \begin{cases} 2 & \text{si } \kappa_{\mathbb{C}}(G) = 0, \\ \big(2\alpha(G) - \kappa_{\mathbb{C}}(G) + 1\big)(2d-1) + 2 - \kappa_{\mathbb{C}}(G) & \text{si } \kappa_{\mathbb{C}}(G) \geq 1. \end{cases}$$

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

De la définition de $\mathrm{m}'_{\mathbb{C}}(G)$ on va déduire :

$$\mathrm{m}'_{\mathbb{C}}(G) \leq \begin{cases} 2(d-1)\alpha(G) + 2d + 1 & \text{si } G \text{ est un groupe linéaire,} \\ 4d^2 - 2d + 1 & \text{si } G \text{ est une variété abélienne,} \\ (3d-2)\alpha(G) + 2d + 1 & \text{dans le cas général.} \end{cases}$$

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 $\mathrm{m}'_{\mathbb{R}}(\widetilde{G}) \leq \mathrm{m}'_{\mathbb{C}}(G)$, donc pour vérifier l'hypothèse *a)* (resp. *b)*) de la proposition 6.1 pour le sous-groupe trivial $\{0\}$, il suffit d'imposer

$$\mathrm{rang}_{\mathbb{Z}}\Gamma \geq \mathrm{m}'_{\mathbb{C}}(G) \qquad (\text{resp.} \quad \mathrm{rang}_{\mathbb{Z}}\Gamma \geq \mathrm{m}'_{\mathbb{C}}(G) + 2d - 1\ ).$$

c) 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 $\omega_1, \ldots, \omega_{2d-1}$ 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 $\overline{\mathbb{Q}}$.

Soit K un sous-corps de $\overline{\mathbb{Q}}$ et soit A une variété abélienne simple sur K de dimension d. On note $\overline{A}$ la variété abélienne déduite de A par action de la conjugaison complexe et on pose $\widetilde{A} = \mathrm{Res}_{\mathbb{C}/\mathbb{R}}A$. Pour appliquer la proposition 6.1 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 $\overline{A}(\mathbb{C})$, 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 $\Omega_{\overline{A}}$ au réseau conjugué $\overline{\Omega}$.

Soit A' une sous-variété abélienne de $\widetilde{A}$ définie sur $\mathbb{R}$ de dimension strictement positive et inférieure à $2d$. Alors $\widetilde{A}$ n'est pas simple, donc A et $\overline{A}$ sont isogènes, et A' est aussi isogène à A ; en particulier la dimension de A' est d, et il existe deux applications linéaires $\varphi : T_A(\mathbb{C}) \to \mathbb{C}^d$ et $\psi : T_{\bar{A}}(\mathbb{C}) \to \mathbb{C}^d$ telles que

$$T_{A'}(\mathbb{C}) = \big\{(z_1, z_2) \in T_A(\mathbb{C}) \times T_{\bar{A}}(\mathbb{C})\ ;\ \varphi(z_1) = \psi(z_2)\big\} \subset T_{\widetilde{A}}(\mathbb{C})$$

et

$$T_{A'}(\mathbb{R}) = \big\{(z, \overline{z}) \in T_A(\mathbb{C}) \times T_{\bar{A}}(\mathbb{C})\ ;\ \varphi(z) = \psi(\overline{z})\big\} \subset T_{\widetilde{A}}(\mathbb{R}).$$

Le noyau de $\exp_{A'} : T_{A'}(\mathbb{C}) \to A'(\mathbb{C})$ est $T_{A'}(\mathbb{C}) \cap \Omega_{\widetilde{A}}$ — réseau de $T_{A'}(\mathbb{C})$ (de rang $2d$), tandis que le noyau de $\exp_{A',\mathbb{R}} : T_{A'}(\mathbb{R}) \to A'(\mathbb{R})$ est $T_{A'}(\mathbb{R}) \cap \Omega_{\widetilde{A}}$ — réseau de rang d dans $T_{A'}(\mathbb{R})$. Soient $\omega_1, \ldots, \omega_d$ des éléments de Ω_A avec $(\omega_i, \overline{\omega_i}) \in T_{A'}(\mathbb{R})$ linéairement indépendants sur $\mathbb{R}$, $(1 \leq i \leq d)$, et soit $W \in \mathrm{GL}_d(\mathbb{C})$ la matrice de $(\omega_1, \ldots, \omega_d)$ dans la base choisie de $T_A(\mathbb{C})$. On pose encore $\theta = W^{-1} \in \mathrm{GL}_d(\mathbb{C})$; ainsi

$$\varphi \circ \theta^{-1} = \varphi \circ W = \psi \circ \overline{W} = \psi \circ \overline{\theta}^{-1}.$$

Si $(z_1, z_2) \in T_{\widetilde{A}}(\mathbb{C})$ vérifie $\theta z_1 = \overline{\theta} z_2$, alors

$$\varphi(z_1) = \varphi \circ \theta^{-1} \circ \theta(z_1) = \psi \circ \overline{\theta}^{-1} \circ \overline{\theta}(z_2) = \psi(z_2).$$

Comme $\theta z_1 = \overline{\theta} z_2$ définit un sous-espace de dimension d dans $T_{\widetilde{A}}(\mathbb{C})$, on en déduit

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

De plus, compte tenu de

$$\Omega_{\widetilde{A}} = \big\{(\omega, \overline{\omega'})\ ;\ \omega \in \Omega_A, \omega' \in \Omega_A\big\} \subset T_{\widetilde{A}}(\mathbb{C}),$$

on a

$$\mathrm{Ker}\ \exp_{A'} = T_{A'}(\mathbb{C}) \cap \Omega_{\widetilde{A}} = \big\{(\omega, \overline{\omega'})\ ;\ \omega \in \Omega_A, \omega' \in \Omega_A;\ \theta\omega = \overline{\theta\omega'}\big\},$$

ce qui montre que

$$\theta\Omega \cap \overline{\theta\Omega} = \big\{\theta\omega\ ;\ \omega \in \Omega;\ \text{il existe } \omega' \in \Omega \text{ tel que } \theta\omega = \overline{\theta\omega'}\big\}$$

est un sous-groupe d'indice fini de $\theta\Omega$.

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

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

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 6.2. – *Soient K un sous-corps de $\overline{\mathbb{Q}}$, A une variété abélienne simple sur K de dimension d et Γ un sous-groupe de $A(K)$ de rang ℓ.*
a) On suppose $\ell \geq 4d^2 - 2d + 1$. On suppose de plus, pour tout $\theta \in \mathcal{E}(A)$,

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

Alors Γ est dense dans $A(\mathbb{C})$.
b) On suppose $\ell \geq 4d^2$. On suppose de plus, pour tout $\theta \in \mathcal{E}(A)$,

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

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*

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

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

d) Exemple : courbes elliptiques.
Soit E une courbe elliptique sur $\mathbb{C}$ et soit $\gamma \in E(\mathbb{C})$. On choisit une base (ω_1, ω_2) de $\Omega_E = \operatorname{Ker} \exp_E$ sur $\mathbb{Z}$, ce qui fournit une base de l'espace tangent $T_E(\mathbb{C})$ sur $\mathbb{R}$, et on choisit un logarithme elliptique $u = \theta_1\omega_1 + \theta_2\omega_2$ de γ : on a $\exp_E(u) = \gamma$ et $(\theta_1, \theta_2) \in \mathbb{R}^2$. Les conditions suivantes sont équivalentes :

(*i*) $\mathbb{Z}\gamma$ est dense dans $E(\mathbb{C})$.
(*ii*) $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \mathbb{Z}u$ est dense dans $\mathbb{C}$.
(*iii*) Les nombres réels $1, \theta_1, \theta_2$ sont linéairement indépendants sur $\mathbb{Q}$.
(*iv*) Pour tout $\omega \in \Omega_E$ et pour tout entier $n \geq 1$, on a $n\gamma \notin \exp_E(\mathbb{R}\omega)$.

On remarquera que pour tout $\omega \in \Omega_E$, $\omega \neq 0$, $\exp(\mathbb{R}\omega)$ est un sous-groupe fermé, isomorphe à $\mathbb{R}/\mathbb{Z}$, du tore $\mathbb{C}/\Omega_E \simeq E(\mathbb{C})$: c'est un sous-groupe à un paramètre réel. Tout sous-groupe fermé infini de $E(\mathbb{C})$ différent de $E(\mathbb{C})$ est de cette forme.

Les conditions (*i*), (*ii*), (*iii*), (*iv*) ci-dessus *impliquent* les conditions équivalentes suivantes :

(*a*) $\gamma \notin E(\mathbb{C})_{\text{tors}}$.
(*b*) Les nombres complexes u, ω_1, ω_2 sont linéairement indépendants sur $\mathbb{Q}$.
(*c*) $(\theta_1, \theta_2) \notin \mathbb{Q}^2$.

Les conditions (*a*), (*b*), (*c*) sont plus faibles que (*i*), (*ii*), (*iii*), (*iv*) : par exemple pour $u = \sqrt{2}\omega_1$, le sous-groupe $\mathbb{Z}\gamma$ n'est pas dense dans $E(\mathbb{C})$. On peut même donner un exemple avec une courbe elliptique E définie sur le corps des nombres algébriques, et $\gamma \in E(\overline{\mathbb{Q}})$: si γ est un point d'ordre infini de E rationnel sur un corps de nombres réel, alors les conditions (*a*), (*b*), (*c*) sont vérifiées, mais pas les conditions (*i*), (*ii*), (*iii*), (*iv*).

Soit E une courbe elliptique sur $\overline{\mathbb{Q}}$; on choisit un modèle de Weierstraß

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

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

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

où $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ désigne le réseau des périodes de $\wp$. On désigne ensuite par $\overline{\Omega} = \mathbb{Z}\overline{\omega_1} + \mathbb{Z}\overline{\omega_2}$ le réseau conjugué complexe de Ω, par $\overline{\wp}$ la fonction elliptique de Weierstraß d'invariants $\overline{g_2}, \overline{g_3}$ et de réseau de périodes $\overline{\Omega}$, et par $\overline{E}$ 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 $\theta\Omega = \overline{\theta\Omega}$. Nous allons vérifier (comparer au lemme 5.2 de [Hu 1992]) que les conditions suivantes sont équivalentes :

(*i*) *la surface abélienne* $\widetilde{E} = \operatorname{Res}_{\mathbb{C}/R}E$ *n'est pas simple sur* $\mathbb{R}$.
(*ii*) *l'ensemble*

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

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*

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

Démonstration. Nous avons déjà établi l'équivalence entre (*i*) et (*ii*) dans le cadre plus général des variétés abéliennes. Montrons que (*ii*) implique (*iii*). De (*ii*) on déduit qu'il existe des entiers m, a, b, c, d avec $m > 0$ satisfaisant

$$m\theta\omega_1 = a\overline{\theta\omega_1} + b\overline{\theta\omega_2},$$
$$m\theta\omega_2 = c\overline{\theta\omega_1} + d\overline{\theta\omega_2}.$$

Alors

$$c + d\overline{\tau} = m\frac{\theta\omega_2}{\overline{\theta\omega_1}} = \tau(a + b\overline{\tau})$$

et

$$\frac{m}{a + b\tau} = \frac{\theta\omega_1}{\overline{\theta\omega_1}} = \frac{a + b\overline{\tau}}{m}.$$

Comme τ n'est pas réel, de la relation $b|\tau|^2 + a(\tau + \overline{\tau}) - c - (a+d)\overline{\tau} = 0$ on déduit $a + d = 0$ et $b|\tau|^2 + a(\tau + \overline{\tau}) - c = 0$. Ce qui précède entraîne $m^2 = a^2 + bc + b(a+d)\overline{\tau} = a^2 + bc$.

Enfin, supposons la propriété (*iii*) vérifiée : $a^2 + bc = m^2$ avec $\tau(a + b\overline{\tau}) = c - a\overline{\tau}$. Alors le nombre $\alpha = (a + b\overline{\tau})/m$ vérifie

$$m^2\alpha\overline{\alpha} = (a + b\tau)(a + b\overline{\tau}) = a^2 + bc = m^2,$$

donc $|\alpha| = 1$, et il existe $\theta \in \mathbb{C}^\times$ tel que $\alpha\overline{\omega_1}/\omega_1 = \theta/\overline{\theta}$. On vérifie alors

$$m\theta\omega_1 = m\alpha\overline{\theta\omega_1} = a\overline{\theta\omega_1} + b\overline{\theta\omega_2}$$

et

$$m\theta\omega_2 = \tau m\theta\omega_1 = \tau\overline{\theta\omega_1}(a + b\overline{\tau}) = c\overline{\theta\omega_1} - a\overline{\theta\omega_2},$$

d'où on déduit (*ii*). $\square$

Remarque. Si les conditions sont vérifiées, les deux courbes E et $\overline{E}$ sont isogènes : en effet, si on pose $\alpha = \theta/\overline{\theta}$, alors $\alpha\Omega \cap \overline{\Omega}$ est de rang 2 ; il existe donc une isogénie de module 1. Si $\tau + \overline{\tau}$ est rationnel, on peut choisir $\alpha = 1$. Si $\tau + \overline{\tau}$ n'est pas rationnel, la relation $b|\tau|^2 + a(\tau + \overline{\tau}) - c = 0$ est unique (à un coefficient multiplicatif près). Il ne suffit pas qu'il existe une isogénie entre E et $\overline{E}$ pour que les conditions (i), (ii) et (iii) soient satisfaites. Par exemple si $|\tau| = 2$ et $\tau + \overline{\tau} \notin \mathbb{Q}$, alors $\alpha = \overline{\tau}$ vérifie $\alpha\Omega \subset \overline{\Omega}$, mais aucun α de module 1 ne possède cette propriété.

Exercice. Soient $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ un réseau de $\mathbb{C}$ et soit $x \in \mathbb{R}$, $x > 0$. On pose $\tau = \omega_2/\omega_1$. Vérifier que les propriétés suivantes sont équivalentes :
(a) Il existe $\alpha \in \mathbb{C}$, $|\alpha| = x$, tel que $\alpha\Omega \cap \overline{\Omega}$ soit un $\mathbb{Z}$-module de rang 2.
(b) Il existe des entiers a, b, c, d et m avec $m > 0$ tels que

$$m^2x^2 = a^2 + bc \qquad \text{et} \qquad b|\tau|^2 + a(\tau + \overline{\tau}) - c = 0.$$

Revenons au problème de densité. Supposons dans un premier temps $\mathcal{E}(E) = \emptyset$; alors
– si Γ est un sous-groupe de $E(\overline{\mathbb{Q}})$ de rang ≥ 3, le corollaire 6.2 montre que Γ est dense dans le groupe topologique $E(\mathbb{C})$;
– si $\Gamma \subset E(\overline{\mathbb{Q}})$ a un rang ≥ 4, il existe $\gamma \in \Gamma$ qui engendre un sous-groupe dense de $E(\mathbb{C})$;
– d'après la propriété de densité, tout point d'ordre infini de $E(\overline{\mathbb{Q}})$ engendre un sous-groupe dense pour la topologie complexe de $E(\mathbb{C})$.

Corollaire 6.3. *– Soit E un courbe elliptique définie sur le corps des nombres algébriques. On suppose que E n'est pas isogène à sa conjuguée complexe $\overline{E}$. Soit Γ un sous-groupe de type fini de $E(\overline{\mathbb{Q}})$ de rang ℓ. Si $\ell \geq 3$, alors Γ est dense dans $E(\mathbb{C})$. Si $\ell \geq 4$, alors il existe $\gamma \in \Gamma$ tel que $\mathbb{Z}\gamma$ soit dense dans $E(\mathbb{C})$. Si $E \times \overline{E}$ possède la propriété de densité, alors tout sous groupe infini de rang fini de $E(\overline{\mathbb{Q}})$ est dense dans $E(\mathbb{C})$.*

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

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

par le réseau

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

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

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

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

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

Ainsi on déduit du corollaire 6.2 :

Corollaire 6.4. *– Soient $u_1, \ldots, u_\ell$ des éléments de $\mathbb{C}$ tels que les points $\gamma_j = \exp_E(u_j)$, $(1 \leq j \leq \ell)$, engendrent un sous-groupe Γ de $E(\overline{\mathbb{Q}})$ de rang ℓ. On pose $Y = \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_\ell + \Omega$. Pour $\theta \in \mathbb{C}^\times$, on définit*

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

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 $\ell \geq 3$, le sous-groupe Γ est dense dans $E(\mathbb{C})$.
b) Si $\ell \geq 4$, et si

$$\mathrm{rang}_{\mathbb{Z}}(Y_\theta / Y_\theta \cap \Omega'_\theta) \geq 2$$

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 les variétés abéliennes, alors Γ est dense dans $E(\mathbb{C})$.

Exercice. On admet la conjecture suivante de Ramachandra [Ra 1968] *:*

> *Soient $\wp$ et $\wp^*$ deux fonctions elliptiques de Weierstraß d'invariants g_2, g_3 et g_2^*, g_3^* algébriques, E et E^* les courbes elliptiques associées, ω une période non nulle de $\wp$ et ω^* une période non nulle de $\wp^*$. On suppose que les deux fonctions $\wp(\omega z)$ et $\wp^*(\omega^* z)$ sont algébriquement indépendantes ; si $u \in \mathbb{C}$ est tel que $\omega u \in \mathcal{L}(E)$ et $\omega^* u \in \mathcal{L}(E^*)$, alors u est rationnel.*

Sous les hypothèses de la partie 2) du corollaire 6.4, montrer que Γ est dense dans $E(\mathbb{C})$.

Exercice.
a) Donner un exemple de quatre nombres réels $\theta_1, \theta_2, \theta'_1, \theta'_2$, tels que les cinq nombres $1, \theta_1, \theta_2, \theta'_1, \theta'_2$ soient linéairement dépendants sur $\mathbb{Q}$, mais que, pour tout $(s, s') \in \mathbb{Z}^2$, $(s, s') \neq (0, 0)$, les trois nombres $1, s\theta_1 + s'\theta'_1, s\theta_2 + s'\theta'_2$ soient linéairement indépendants sur $\mathbb{Q}$
b) Soit E une courbe elliptique définie sur $\mathbb{C}$ et sans multiplication complexe. On désigne par $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset \mathbb{C}$ le noyau de $\exp_E$, et par A la surface abélienne E^2. On pose

$$\gamma = \big(\exp_E(\theta_1\omega_1 + \theta_2\omega_2), \exp_E(\theta'_1\omega_1 + \theta'_2\omega_2)\big) \in A(\mathbb{C}),$$

où $\theta_1, \theta_2, \theta'_1, \theta'_2$ satisfont la condition énoncée en a). Montrer que $\mathbb{Z}\gamma$ n'est pas dense dans $A(\mathbb{C})$, mais que sa projection sur tout quotient $(A/A')(\mathbb{C})$, A' sous-variété abélienne de A de dimension 1, est dense dans $(A/A')(\mathbb{C})$.

V. – Approximation simultanée dans les groupes algébriques

Soit G un groupe algébrique commutatif défini sur un corps de nombres K plongé dans $\mathbb{R}$, et soit Γ un sous-groupe de type fini de $G(K)$ qui est dense dans $G(\mathbb{R})^0$; on étudie l'approximation des éléments de $G(\mathbb{R})^0$ par des éléments de Γ. Nous savons déjà que Γ est dense dans $G(\mathbb{R})^0$ si et seulement si $Y = \exp^{-1}(\Gamma)$ est dense dans $T_G(\mathbb{R})$. Par le théorème de Kronecker, cette condition se traduit de la manière suivante : pour toute forme linéaire non nulle $\varphi : T_G(\mathbb{R}) \to \mathbb{R}$, on a $\varphi(Y) \not\subset \mathbb{Q}$. Il s'agit donc d'un problème d'irrationalité, sur lequel le théorème du sous-groupe algébrique nous a permis d'obtenir des réponses partielles : *si le noyau de φ ne contient pas de sous-espace non nul de la forme $T_{G'}(\mathbb{C})$, avec G' sous-groupe algébrique de G défini sur K, et si Y est un sous-groupe de $\mathcal{L}_K(G) = \exp^{-1}\big(G(K)\big)$, alors on peut minorer le rang de $\varphi(Y)$ en fonction du rang de Y*. En particulier si on obtient la conclusion $\mathrm{rang}_{\mathbb{Z}}\varphi(Y) \geq 2$, alors on peut déduire l'irrationalité de l'un des nombres $\varphi(y)$, $(y \in Y)$, donc la densité de Γ.

Pour obtenir des énoncés effectifs, nous seront amenés à rechercher des *mesures d'irrationalité* : si Y est engendré par des éléments $y_1, \ldots, y_m$ comme $\mathbb{Z}$-module, il s'agit d'étudier l'approximation simultanée des nombres réels $\varphi(y_1), \ldots, \varphi(y_m)$ par des nombres entiers. Nous verrons que cette question est liée à un problème de transcendance : *quand $\varphi : T_G(\mathbb{R}) \to \mathbb{R}$ est une forme linéaire non nulle, montrer $\varphi(Y) \not\subset \overline{\mathbb{Q}}$*. Là encore, le théorème du sous-groupe algébrique va nous permettre de donner des résultats partiels, sous des hypothèses convenables concernant Y (qui doit en particulier être de rang suffisamment grand), et c'est essentiellement quand ces hypothèses seront satisfaites que nous pourrons donner des réponses relativement satisfaisantes au problème de densité effective.

§1. Introduction

Soit K un corps de nombres admettant un plongement réel ; on considère K comme un sous-corps de $\mathbb{R}$; soit V une variété lisse définie sur K, et soit Z l'adhérence (pour la topologie réelle) de $V(K)$ dans $V(\mathbb{R})$. Dans son article [Maz 1992] sur la topologie des points rationnels, Mazur suppose $K = \mathbb{Q}$ et $V(\mathbb{Q})$ Zariski dense ; il suggère alors que Z est réunion de composantes connexes de $V(\mathbb{R})$).

Nous proposons ici une version quantitative de cette conjecture. Supposons V plongée, comme variété quasi-projective, dans un espace projectif $\mathbb{P}_N$ sur K ; désignons par h la hauteur logarithmique absolue de Weil sur $\mathbb{P}_N(K)$, et choisissons une métrique sur $\mathbb{P}_N$. Pour chaque nombre réel $H \geq 1$, on définit $\eta_V(H)$ comme la borne inférieure des $\epsilon > 0$

tels que tout point de Z soit à une distance $\leq \epsilon$ d'un point de $V(K)$ de hauteur $\leq \log H$:

$$\eta_V(H) = \inf\big\{\epsilon > 0 \;; \quad \text{pour tout } P \in Z, \text{ il existe } Q \in V(K) \text{ avec } \mathrm{h}(Q) \leq \log H \text{ et } \mathrm{dist}(P,Q) \leq \epsilon\big\}.$$

Dire que $V(K)$ est dense dans Z s'écrit

$$\lim_{H\to\infty} \eta_V(H) = 0.$$

Majorer $\eta_V(H)$, c'est montrer que les points rationnels sont “bien répartis” sur la variété. Dans ce contexte, on pourrait aussi chercher à minorer la distance de deux points rationnels distincts sur la variété, si possible en améliorant l'inégalité de type Liouville que voici : *il existe une constante $C(V) > 0$ telle que, pour tout Q_1 et Q_2 dans $V(K)$, on ait*

$$\mathrm{dist}(Q_1, Q_2) > \exp\big(-C \max\{\mathrm{h}(Q_1), \mathrm{h}(Q_2), 1\}\big);$$

une amélioration de cette inégalité signifierait que les points rationnels sur une variété, qui devraient être “contagieux” d'après Mazur, restent néanmoins éloignés les uns des autres. Cependant il ne semble pas que la recherche de telles minorations sur l'éloignement mutuel de points rationnels soit une méthode efficace pour majorer $\eta_V(H)$: une minoration, même fine, de la distance mutuelle entre points rationnels, n'empêcherait pas ces points rationnels d'être concentrés dans une région de l'espace ; elle ne donnerait qu'une information locale, alors que η_V est une donnée globale.

D'un autre côté, si $\psi_V(H)$ désigne le nombre de points de $V(K)$ de hauteur $\leq \log H$, on a

$$\liminf_{H\to\infty} \psi_V(H)\eta_V(H)^{\dim V} > 0.$$

Noter que l'inégalité $\psi_V(H) \leq CH^{\dim V + 1}$ est toujours vraie, avec une constante C ne dépendant pas de H, donc on a toujours

$$\liminf_{H\to\infty} \eta_V(H) \cdot H^{1+(1/\dim V)} > 0.$$

Dans certains cas une estimation plus précise est connue ; ainsi, quand V est une variété abélienne A, on a

$$\psi_A(H) \leq C(\log H)^{\ell/2},$$

où ℓ est le rang du groupe de Mordell-Weil $A(K)$, tandis que C est une (nouvelle) constante indépendante de H. La démonstration de cette inégalité repose sur la quadraticité de la hauteur de Néron-Tate (voir par exemple [L 1978], Chap. IV ou [Sil 1986], Chap. VIII §6 et §9 pour les courbes elliptiques, et [L 1983], Chap. V §6, [Se 1989], §3.3 [L 1991], Chap. III §3, [Hu 1993], §3 pour les variétés abéliennes) :

> *Soient A une variété abélienne sur un corps de nombres K et $\gamma_1, \ldots, \gamma_\ell$ des éléments de $A(K)$. Il existe une constante $C > 0$ ayant la propriété suivante : si $t_1, \ldots, t_\ell$ sont des entiers rationnels, et si T est un nombre réel satisfaisant $T \geq \max\{1, |t_1|, \ldots, |t_\ell|\}$, alors*
>
> $$\mathrm{h}(t_1\gamma_1 + \cdots + t_\ell\gamma_\ell) \leq CT^2.$$

Dans le cas d'une variété abélienne A de dimension g, on ne peut donc pas majorer $\eta_A(H)$ mieux que par une puissance (négative) de $\log H$.

Conjecture 1.1$^?$. — *Soit A une variété abélienne simple de dimension g définie sur un corps de nombres K plongé dans $\mathbb{R}$; désignons par ℓ le rang sur $\mathbb{Z}$ du groupe de Mordell-Weil $A(K)$. Pour tout $\epsilon > 0$, il existe un nombre $H_0 > 0$ (ne dépendant que de la variété abélienne A, du corps de nombres K et de ϵ) tel que, pour $H \geq H_0$, on ait*

$$\eta_A(H) \leq (\log H)^{-(\ell/2g)+\epsilon}.$$

Cela signifie que tout point de $A(\mathbb{R})^0$ devrait être à une distance $\leq (\log H)^{-(\ell/2g)+\epsilon}$ d'un point de $A(K)$ de hauteur logarithmique $\leq \log H$. Nous verrons que cette conjecture $1.1^?$ équivaut à un résultat d'approximation diophantienne, pour lequel nous donnerons des résultats partiels.

Nous étudions d'abord le cas d'une courbe elliptique ; nous obtenons une mesure de densité du sous-groupe des points rationnels en utilisant une minoration, due à N. Hirata, pour l'approximation simultanée de logarithmes elliptiques. Nous considérons ensuite le cas plus général d'une variété abélienne ayant suffisamment de points rationnels. Les démonstrations utilisent d'une part un lemme de transfert, d'autre part un résultat de transcendance (version effective du théorème du sous-groupe algébrique).

§2. Mesure de la densité des points rationnels sur une courbe elliptique

Considérons la conjecture $1.1^?$ dans le cas de dimension 1 : soit E une courbe elliptique définie sur un corps de nombres réel K, soit $\omega \in \mathbb{R}$ une période réelle de la fonction de Weierstraß $\wp$ associée à $E(\mathbb{C})$, et soient $y_1, \ldots, y_\ell$ des nombres réels, avec $\omega, y_1, \ldots, y_\ell$ linéairement indépendants sur $\mathbb{Q}$, et $\wp(y_j) \in K$, $(1 \leq j \leq \ell)$. On désigne par $\gamma_j \in E(K)$ l'image de y_j par l'application exponentielle de $E(\mathbb{C})$. Rechercher une mesure de densité pour le sous-groupe $\mathbb{Z}\gamma_1 + \cdots + \mathbb{Z}\gamma_\ell$ dans $E(\mathbb{R})^0$ revient à rechercher une mesure de densité pour le sous-groupe $\mathbb{Z}\omega + \mathbb{Z}y_1 + \cdots + \mathbb{Z}y_\ell$ de $\mathbb{R}$. Par conséquent la conjecture $1.1^?$, dans le cas des courbes elliptiques, est conséquence de la suivante (où on n'a pas supposé que $\gamma_1, \ldots, \gamma_\ell$ engendre tout le groupe de Mordell-Weil $E(K)$) :

$\boxed{?}$ *pour tout $\epsilon > 0$ il existe une constante $T_0 > 0$, ne dépendant que de $E, K, \omega, y_1, \cdots, y_\ell$, ayant la propriété suivante : pour tout entier $T \geq T_0$ et pour tout $\zeta \in \mathbb{R}$, il existe des entiers $t_0, t_1, \ldots, t_\ell$ dans $\mathbb{Z}$ vérifiant*

$$\max_{1\leq j\leq \ell} |t_j| \leq T \quad \textit{et} \quad \bigl|\zeta - t_0\omega - t_1 y_1 - \cdots - t_\ell y_\ell\bigr| \leq T^{-\ell+\epsilon}.$$

L'exposant ℓ est évidemment optimal (comme il résulte de la discussion précédant l'énoncé de la conjecture $1.1^?$, ou bien du théorème 4.2 du chapitre II) ; c'est "l'exposant de Dirichlet" de [W 1979], p.36. Un lemme de transfert (voir §4 ci-dessous) permet de formuler cette question de façon équivalente en termes d'approximation simultanée de nombres réels (transcendants) par des nombres rationnels :

$\boxed{?}$ *pour tout $\epsilon > 0$ il existe une constante $Q > 0$, ne dépendant que de ϵ, E, K, ω, $y_1, \cdots, y_\ell$, ayant la propriété suivante : pour tout $q, p_1, \ldots, p_\ell$ entiers rationnels avec $q \geq Q$, on a*

$$\max_{1\leq j\leq \ell} \left|\frac{y_j}{\omega} - \frac{p_j}{q}\right| > q^{-(1/\ell)-1-\epsilon}.$$

Ce dernier énoncé devrait être vrai pour une courbe elliptique sur un corps de nombres K quelconque, sans supposer que K est plongé dans $\mathbb{R}$. La meilleure mesure d'approximation simultanée connue pour les nombres y_i/ω est due à N. Hirata-Kohno (cf. [HK 1993]) :

Proposition 2.1* (Hirata-Kohno). — *Soit E une courbe elliptique définie sur un corps de nombres K, soit $\omega \in \mathbb{C}$ une période non nulle $\exp_E$, et soient $y_1, \ldots, y_\ell$ des nombres complexes tels que $\exp_E(y_j) \in E(K)$ pour $1 \leq j \leq \ell$. On suppose que les nombres $\omega, y_1, \ldots, y_\ell$ sont linéairement indépendants sur $\mathbb{Q}$. Alors il existe deux constantes c et q_0, ne dépendant que de E, K, ω, $y_1, \cdots, y_\ell$, telles que, pour tout $(q, p_1, \ldots, p_\ell) \in \mathbb{Z}^{\ell+1}$ avec $q \geq q_0$, on ait*

$$\max_{1\leq j\leq \ell} \left|\frac{y_j}{\omega} - \frac{p_j}{q}\right| \geq \exp\{-c(\log q)(\log\log q)^{1+(2/\ell)}\}.$$

Remarque. – On peut prendre $q_0 = 3$, quitte à remplacer c par une constante plus grande.

Quand le corps de nombres K est réel, on en déduira (au §5) une mesure de densité des points rationnels sur K dans $E(\mathbb{R})^0$:

Corollaire 2.2. —*Pour une courbe elliptique E définie sur un corps de nombres K plongé dans $\mathbb{R}$, il existe deux constantes $C > 0$ et $H_0 > 0$ (ne dépendant que de E et K) telles que, pour tout $H \geq H_0$, on ait*

$$\eta_E(H) \leq \exp\bigl\{-C(\log\log H)(\log\log\log H)^{-1-(2/\ell)}\bigr\}.$$

Compte tenu de la définition de la fonction η_E, cela signifie que pour tout $H \geq H_0$ et tout point P dans la composante neutre $E(\mathbb{R})^0$ de $E(\mathbb{R})$, il existe $Q \in E(K)$ avec

$$\mathrm{h}(Q) \leq \log H \quad \text{et} \quad \mathrm{dist}(P, Q) \leq \exp\bigl\{-C(\log\log H)(\log\log\log H)^{-1-(2/\ell)}\bigr\}.$$

La fonction η_E est définie à partir du modèle de Weierstraß de E ; elle dépend aussi du choix d'une métrique sur le plan projectif ; donc C et H_0 en dépendent tout autant.

Si on en croit la conjecture $1.1^?$, le facteur $C(\log\log\log H)^{-1-(2/\ell)}$ dans la conclusion du corollaire 2.2 devrait pouvoir être remplacé par $(\ell/2) - \epsilon$ pour $H > H_0(\epsilon)$.

§3. Répartition des points rationnels sur un groupe algébrique

Nous donnerons deux exemples d'énoncés qui précisent de façon quantitative la densité de certains sous-groupes de points rationnels. Le premier va concerner les variétés abéliennes simples et la question de Mazur, le second portera sur le plongement canonique d'un corps de nombres et les questions de Colliot-Thélène et Sansuc.

Voici déjà une minoration de $\eta_A(H)$ pour une variété abélienne simple A sur K, de dimension g, ayant suffisamment de points rationnels. Par translation, il suffit de considérer la composante connexe $A(\mathbb{R})^0$ de l'origine.

Théorème 3.1. — *Soit A une variété abélienne simple sur un corps de nombres $K \subset \mathbb{R}$, de dimension g, plongée dans un espace projectif $\mathbb{P}_N$ sur K. On choisit une métrique sur $\mathbb{P}_N$. On suppose que le groupe de Mordell-Weil $A(K)$ a un rang $> (2g-1)g$. Il existe alors trois constantes H_0, C et θ positives ayant la propriété suivante : pour tout $H \geq H_0$ et tout point P dans la composante neutre $A(\mathbb{R})^0$ de $A(\mathbb{R})$, il existe $Q \in A(K)$ avec*

$$\mathrm{h}(Q) \leq \log H \quad \textit{et} \quad \mathrm{dist}(P,Q) \leq \exp\{-C(\log\log H)^{\theta}\}.$$

Nous obtiendrons ce résultat avec $\theta = 1 - \big(2g^2/(\ell+g)\big)$. En particulier quand ℓ est grand, θ est proche de la valeur conjecturale 1. Il est vraisemblable que l'on a une estimation de la forme

$$\eta_A(H) \leq \exp\{-C(\log\log H)^{\theta}\}$$

dès que $\ell \geq g^2 - g + 1$ (qui est la valeur à partir de laquelle on sait conclure à la densité – voir le chapitre IV, proposition 4.1), mais cela semble difficile à établir avec les méthodes actuelles. En revanche il ne devrait pas être difficile d'obtenir cette estimation sous l'hypothèse $\ell \geq g^2 + 1$. Pour les valeurs de ℓ satisfaisant $g^2 - g + 1 \leq \ell \leq g^2$, les méthodes actuelles permettent seulement d'espérer une estimation plus faible :

$$\eta_A(H) \leq C(\log\log H)^{-\theta}.$$

En tout cas nous verrons que cette dernière estimation est valable au moins pour $\ell \geq 2g^2 - 3g + 2$, avec

$$\theta = \frac{1}{g} - \frac{2g}{\ell + 3g - 1}.$$

Dans le cas particulier $d = 1$, nous avons vu que le théorème 3.1 se ramène à une mesure de transcendance de u/ω, quand ω est une période d'une fonction elliptique de Weierstraß d'invariants g_2, g_3 algébriques, et u est un logarithme elliptique d'un point algébrique d'ordre infini. Dans le cas général $d \geq 2$, il faut établir un nouveau type d'estimation (théorème 6.1* ci-dessous).

Le deuxième énoncé de cette section fournit un résultat effectif de densité concernant un groupe multiplicatif formé de points à coordonnées algébriques.

Théorème 3.2. – *Soient r_1 et r_2 des entiers ≥ 0 avec $n = r_1 + r_2 > 0$. On pose aussi $d = r_1 + 2r_2$. Soit Γ un sous-groupe de $(\mathbb{R}_+^{\times})^{r_1} \times (\mathbb{C}^{\times})^{r_2}$, engendré par des éléments $(\gamma_{ij})_{1\leq i\leq n}$, $(j = 1\dots,\ell)$, où les $d\ell$ nombres*

$$\gamma_{ij}, \quad (i = 1,\dots,n,\ j = 1\dots,\ell) \quad \textit{et} \quad \overline{\gamma}_{ij}, \quad (i = r_1+1,\dots,n,\ j = 1\dots,\ell)$$

sont multiplicativement indépendants. On suppose $\ell > d^2$. Il existe des constantes positives c_1 et c_2 possédant la propriété suivante : pour tout $\zeta = (\zeta_1,\dots,\zeta_n) \in (\mathbb{R}_+^{\times})^{r_1} \times (\mathbb{C}^{\times})^{r_2}$, et pour tout $T \geq c_1 \log \max_{1\leq i\leq n}\{2 + |\zeta_i|\}$, il existe $(t_1,\dots,t_\ell) \in \mathbb{Z}^\ell$ tel que

$$\max_{1\leq j\leq \ell} |t_j| \leq T \quad \textit{et} \quad \max_{1\leq i\leq n} \big|\zeta_i - \gamma_{i1}^{t_1}\cdots\gamma_{i\ell}^{t_\ell}\big| \leq \exp\big\{-c_2(\log T)^{1-(d^2/\ell)}\big\}.$$

On peut donner des estimations qui sont moins précises en fonction de T, mais qui sont valables pour des valeurs plus petites de ℓ. Par exemple on démontrera le même énoncé avec la borne

$$\max_{1\leq i\leq n} \big|\zeta_i - \gamma_{i1}^{t_1}\cdots\gamma_{i\ell}^{t_\ell}\big| \leq c_3(\log\log T)^{-\theta}\}$$

où

$$\theta = \frac{1}{d} - \frac{d}{\ell + d - 1},$$

ce qui donne un résultat non trivial dès que $\ell \geq d^2 - d + 2$.

On *conjecture* que la conclusion du théorème 3.2 peut être remplacée par

$$(?) \qquad \max_{1\leq i\leq n} \big|\zeta_i - \gamma_{i1}^{t_1}\cdots\gamma_{i\ell}^{t_\ell}\big| \leq c(\epsilon)T^{1-(\ell/d)+\epsilon}.$$

Un tel énoncé serait optimal.

§4. Lemme de transfert

a) Une version quantitative du théorème de Kronecker

On va utiliser une version quantitative d'un théorème de Kronecker. Rappelons déjà la version qualitative (Chap. II, §4 ; voir aussi [Ca 1957], ainsi que les travaux de D.Roy ([R 1990a] et [R 1990b]) sur les sous-groupes minimaux). Soient m et n deux entiers positifs, et soient ϑ_{ji}, $(1 \leq j \leq n,\ 1 \leq i \leq m)$ des nombres réels ; on pose

$$\gamma_i = (\vartheta_{1i},\dots,\vartheta_{ni}) \in \mathbb{R}^n, \qquad (1 \leq i \leq m)$$

et

$$\delta_j = (\vartheta_{j1},\dots,\vartheta_{jm}) \in \mathbb{R}^m, \qquad (1 \leq j \leq n).$$

Ainsi

$$\Gamma = \mathbb{Z}^n + \mathbb{Z}\gamma_1 + \cdots + \mathbb{Z}\gamma_m \subset \mathbb{R}^n \quad \text{et} \quad \Delta = \mathbb{Z}^m + \mathbb{Z}\delta_1 + \cdots + \mathbb{Z}\delta_n \subset \mathbb{R}^m$$

sont les sous-groupes engendrés par les vecteurs colonnes des matrices

$$\begin{pmatrix} 1 & \cdots & 0 & \vartheta_{11} & \cdots & \vartheta_{1m} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & \vartheta_{n1} & \cdots & \vartheta_{nm} \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & \cdots & 0 & \vartheta_{11} & \cdots & \vartheta_{n1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & \vartheta_{1m} & \cdots & \vartheta_{nm} \end{pmatrix}.$$

D'après la proposition 4.3 du chapitre II (voir l'exercice avant la proposition 4.4), Γ est dense dans $\mathbb{R}^n$ si et seulement si Δ est de rang $n + m$ sur $\mathbb{Z}$. Un lemme de transfert de Khinchine permet de préciser ce résultat de la manière suivante.

Lemme 4.1. *Soient ϑ_{ji}, $(1 \le j \le n,\ 1 \le i \le m)$ des nombres réels, T et S des nombres réels positifs.*
(i) On pose $\eta = 2^{-n-m}\big((n+m)!\big)^2$ et on suppose que pour tout $(s_1,\dots,s_n) \in \mathbb{Z}^n \setminus \{0\}$ vérifiant

$$\max_{1\le j\le n} |s_j| \le S,$$

on a

$$\|s_1\delta_1 + \dots + s_n\delta_n\| \ge \eta T^{-1},$$

Alors pour tout $\zeta \in \mathbb{R}^n$, il existe $(t_1,\dots,t_m) \in \mathbb{Z}^m$ vérifiant

$$\max_{1\le i\le m} |t_i| \le T,$$

et tel que

$$\|\zeta - t_1\gamma_1 - \dots - t_m\gamma_m\| \le \eta S^{-1}.$$

(ii) On suppose que pour tout $\zeta \in \mathbb{R}^n$, il existe $(t_1,\dots,t_m) \in \mathbb{Z}^m$ vérifiant

$$\max_{1\le i\le m} |t_i| \le T,$$

et

$$\|\zeta - t_1\gamma_1 - \dots - t_m\gamma_m\| \le \frac{1}{2(n+m)S}.$$

Alors pour tout $(s_1,\dots,s_n) \in \mathbb{Z}^n \setminus \{0\}$ vérifiant

$$\max_{1\le j\le n} |s_j| \le S,$$

on a

$$\|s_1\delta_1 + \dots + s_n\delta_n\| \ge \frac{1}{2(n+m)T}.$$

On a noté $\|\cdot\|$:

- la distance à $\mathbb{Z}^m$ dans l'hypothèse de *(i)* et dans la conclusion de *(ii)*,
- la distance à $\mathbb{Z}^n$ dans l'hypothèse de *(ii)* et dans la conclusion de *(i)*.

C'est surtout la partie *(i)* qui nous sera utile : elle ramène la question de densité effective à un problème d'approximation diophantienne homogène. La partie *(ii)* montre qu'il y a en fait équivalence entre les deux questions.

Démonstration. On utilise un lemme de transfert de Khinchine (théorème XVII du chapitre V §8 de [Ca 1957]), pour les formes linéaires $L_1,\dots,L_n$, $M_1,\dots,M_m$ définies par

$$L_j(x) = \sum_{i=1}^m \vartheta_{ji}x_i, \quad (1\le j\le n) \quad \text{et} \quad M_i(u) = \sum_{j=1}^n \vartheta_{ji}u_j, \quad (1 \le i \le m).$$

Pour montrer *(i)⇒(ii)*, on utilise la partie B du lemme de transfert, avec $C = \eta S^{-1}$ et $X = T$. Soit $\zeta \in \mathbb{R}^n$. Il suffit de vérifier, pour tout $s = (s_1,\dots,s_n) \in \mathbb{Z}^n$,

$$\|s\zeta\| \le \frac{1}{2\eta}\max\{X \max_{1\le i\le m}\|M_i(s)\|\,;\, C\max_{1\le j\le n}|s_j|\}.$$

Cette inégalité est vraie pour $s = 0$. Comme $\|s\zeta\| \le 1/2$, elle est aussi trivialement vérifiée pour les $s \in \mathbb{Z}^n$ tels que $\max_{1\le j\le n}|s_j| > S$. Il ne reste plus qu'à considérer les $s \in \mathbb{Z}^n$ pour lesquels $0 \ne \max_{1\le j\le n}|s_j| \le S$, et pour ceux-là on applique l'hypothèse *(i)* qui donne :

$$\max_{1\le i\le m}\|M_i(s)\| \ge \frac{\eta}{X}.$$

Pour montrer *(ii)⇒(i)*, on procède par l'absurde : supposons qu'il existe $(s_1,\dots,s_n) \in \mathbb{Z}^n$ vérifiant $0 < \max_{1\le j\le n}|s_j| \le S$ et

$$\|s_1\delta_1 + \dots + s_n\delta_n\| < \frac{1}{2(n+m)T}.$$

On choisit $\zeta \in \mathbb{R}^n$ tel que $\|s\zeta\| = 1/2$, et on utilise la partie A du lemme de Khinchine, avec $C = \big(2(n+m)S\big)^{-1}$ et $X = T$: il n'existe pas de $(t_1,\dots,t_m) \in \mathbb{Z}^m$ vérifiant $\max_{1\le i\le m}|t_i| \le T$ et

$$\max_{1\le j\le n}\|L_j(t) - \zeta_j\| \le C.$$

□

Remarque. Le théorème de Dirichlet (théorème 4.2 du chapitre II) montre que pour tout S réel > 1, il existe $(s_1,\dots,s_n) \in \mathbb{Z}^n$ vérifiant

$$0 < \max_{1\le i\le n}|s_i| \le S,$$

et

$$\|s_1\delta_1 + \dots + s_n\delta_n\| \le S^{-n/m}.$$

On en déduit que l'hypothèse de l'assertion *(i)* du lemme 4.1 ne peut pas être vérifiée avec un nombre T inférieur à $\eta S^{n/m}$. De même l'argument qui nous a permis de minorer η_V en fonction de Ψ_V au paragraphe 1 montre que pout tout entier $T \ge 1$, il existe $\zeta \in \mathbb{R}^n$ tel que, pour tout $(t_1,\dots,t_m) \in \mathbb{Z}^m$ vérifiant

$$\max_{1\le j\le m}|t_j| \le T,$$

on ait

$$\|\zeta - t_1\gamma_1 - \dots - t_m\gamma_m\| \ge \frac{1}{2}(2T+1)^{-m/n}.$$

Par conséquent, si l'hypothèse de la condition *(ii)* du lemme 4.1 est vérifiée, alors

$$S \le \frac{1}{(n+m)}(2T+1)^{m/n}$$

Exercice.
a) Soient ϑ_{ji}, $(1 \le j \le n,\ 1 \le i \le m)$ *des nombres réels. Montrer que les deux assertions suivantes sont équivalentes*
(i) Pour tout $\epsilon > 0$, *il existe un nombre réel* $S_0(\epsilon) > 0$ *tel que, pour tout* $S \ge S_0(\epsilon)$ *et pour tout* $(s_1, \dots, s_n) \in \mathbb{Z}^n$ *vérifiant*

$$0 < \max_{1 \le j \le n} |s_j| \le S,$$

on a

$$\|s_1\delta_1 + \cdots + s_n\delta_n\| \ge S^{-(n/m)-\epsilon}.$$

(ii) Pour tout $\epsilon > 0$, *il existe un nombre réel* $T_0(\epsilon) > 0$ *tel que, pour tout* $T \ge T_0(\epsilon)$ *et pour tout* $\zeta \in \mathbb{R}^n$, *il existe* $(t_1, \dots, t_m) \in \mathbb{Z}^m$ *vérifiant*

$$\max_{1 \le i \le m} |t_i| \le T,$$

et tel que

$$\|\zeta - t_1\gamma_1 - \cdots - t_m\gamma_m\| \le T^{-(m/n)+\epsilon}.$$

b) Soient $\vartheta_1, \dots, \vartheta_m$, *des nombres réels. Montrer que les deux assertions suivantes sont équivalentes*
(i) Pour tout $\epsilon > 0$, *il existe un nombre réel* $Q_0(\epsilon) > 0$ *tel que, pour tout* $(p_1, \dots, p_m, q) \in \mathbb{Z}^{m+1}$ *vérifiant* $q \ge Q_0(\epsilon)$, *on a*

$$\max_{1 \le i \le m} \left|\vartheta_i - \frac{p_i}{q}\right| \ge q^{-(1/m)-1-\epsilon}.$$

(ii) Pour tout $\epsilon > 0$, *il existe un nombre réel* $T_0(\epsilon) > 0$ *tel que, pour tout* $T \ge T_0(\epsilon)$ *et pour tout* $\zeta \in \mathbb{R}$, *il existe* $(t_0, \dots, t_m) \in \mathbb{Z}^{m+1}$ *vérifiant*

$$\max_{1 \le i \le m} |t_i| \le T,$$

et

$$|\zeta - t_0 - t_1\vartheta_1 - \cdots - t_m\vartheta_m| \le T^{-m+\epsilon}.$$

c) Soient $\vartheta_1, \dots, \vartheta_n$, *des nombres réels. Montrer que les deux assertions suivantes sont équivalentes*
(i) Pour tout $\epsilon > 0$, *il existe un nombre réel* $S_0(\epsilon) > 0$ *tel que, pour tout* $S \ge S_0(\epsilon)$ *et pour tout* $(s_0, \dots, s_n) \in \mathbb{Z}^{n+1}$ *vérifiant*

$$0 < \max_{1 \le j \le n} |s_j| \le S,$$

on a

$$|s_0 + s_1\vartheta_1 + \cdots + s_n\vartheta_n| \ge S^{-n-\epsilon}.$$

(ii) Pour tout $\epsilon > 0$, *il existe un nombre réel* $T_0(\epsilon) > 0$ *tel que, pour tout* $T \ge T_0(\epsilon)$ *et pour tout* $\zeta \in \mathbb{R}^n$, *il existe* $(t_0, \dots, t_n) \in \mathbb{Z}^{n+1}$ *vérifiant* $|t_0| \le T$ *et*

$$\max_{1 \le j \le n} |\zeta_j - t_0\vartheta_j - t_j| \le T^{-(1/n)+\epsilon}.$$

Soient E un $\mathbb{R}$-espace vectoriel normé de dimension n et soit Ω un réseau de E. On note $E^* = \mathrm{Hom}(E, \mathbb{R})$ l'espace vectoriel dual de E, et Ω^* le réseau dual de Ω (cf. Chap. II §4). Il résulte de la proposition 4.3 du chapitre III qu'un sous-groupe de type fini Y de E contenant Ω est dense dans E si et seulement si, pour tout $\varphi \in \Omega^*$ non nul, on a $\varphi(Y) \not\subset \mathbb{Z}$. Nous allons donner une version quantitative de cet énoncé. On fixe un entier $m \ge 1$ et on pose encore $\eta = 2^{-n-m}\big((n+m)!\big)^2$.

L'énoncé qui suit fait intervenir une fonction réelle de variable réelle $F : [S_0, \infty) \to \mathbb{R}_+$, définie sur un intervalle $[S_0, \infty)$ de $\mathbb{R}^+$, et à valeurs positives. On suppose F strictement croissante et non bornée : $\lim_{S \to \infty} F(S) = \infty$; on désigne par F^{-1} la bijection réciproque de F, on pose $T_0 = \eta F(S_0)$ et on définit une fonction G, croissante sur l'intervalle $[T_0, \infty)$ et à valeurs réelles positives, par

$$G(T) = \frac{F^{-1}(T/\eta)}{\eta \sum_{j=1}^n |\omega_j|}.$$

Lemme 4.2. – *Soient* $\omega_1, \dots, \omega_n$ *des éléments de* Ω *linéairement indépendants (sur* $\mathbb{Z}$ *ou sur* $\mathbb{R}$*, c'est équivalent), et soient* $y_1, \dots, y_m$ *des éléments de* E. *Soit* $F : [S_0, \infty) \to \mathbb{R}_+$ *une fonction strictement croissante. On suppose que pour tout* $\varphi \in \Omega^*$ *non nul, si on pose*

$$S = \max\{|\varphi(\omega_1)|, \dots, |\varphi(\omega_n)|; S_0\},$$

on a

$$\max_{1 \le i \le m} \|\varphi(y_i)\| \ge 1/F(S).$$

Alors pour tout $x \in E$ *et pour tout entier* $T \ge T_0$, *il existe* $\omega \in \Omega$ *et* $(t_1, \dots, t_m) \in \mathbb{Z}^m$ *vérifiant*

$$\max\{|t_1|, \dots, |t_m|\} \le T \quad \text{et} \quad \big|x - \omega - t_1y_1 - \cdots - t_my_m\big| \le 1/G(T).$$

On peut écrire la conclusion sous la forme suivante : *il existe* $\epsilon_0 > 0$ *tel que, pour tout* $x \in E$ *et pour tout* ϵ *dans l'intervalle* $0 < \epsilon < \epsilon_0$, *il existe* $\omega \in \Omega$ *et* $(t_1, \dots, t_m) \in \mathbb{Z}^m$ *vérifiant*

$$\big|x - \omega - t_1y_1 - \cdots - t_my_m\big| \le \epsilon$$

avec

$$\max\{|t_1|, \dots, |t_m|\} \le \eta F(S), \quad \text{où} \quad S = \epsilon^{-1}\eta\sum_{j=1}^n |\omega_j|.$$

Démonstration. Pour démontrer le lemme 4.2, on écrit $y_1,\ldots,y_m$ dans la base $\omega_1,\ldots,\omega_n$ de E :

$$y_i=\sum_{j=1}^n \vartheta_{ji}\omega_j,\qquad (1\le i\le m).$$

On va utiliser la partie *(i)* du lemme 4.1. Soit S un nombre réel $\ge S_0$ et soit $s\in\mathbb{Z}^n$ vérifiant $0<\max_{1\le j\le n}|s_j|\le S$. On définit $\varphi\in\Omega^*$ par $\varphi(\omega_j)=s_j$, $(1\le j\le n)$. Alors

$$\varphi(y_i)=\sum_{j=1}^n \vartheta_{ji}s_j,\qquad (1\le i\le m).$$

On a par hypothèse

$$\max_{1\le i\le m}\left\|\sum_{j=1}^n \vartheta_{ji}s_j\right\|\ge 1/F(S),$$

ce qui permet d'appliquer le lemme 4.1. Soit $x\in E$, soit T un nombre réel $\ge T_0$, et soit S le nombre réel défini par $F(S)=T/\eta$. On écrit $x=\zeta_1\omega_1+\cdots+\zeta_n\omega_n$ avec $(\zeta_1,\ldots,\zeta_n)\in\mathbb{R}^n$. Alors il existe $t\in\mathbb{Z}^m$ vérifiant $\max_{1\le i\le m}|t_i|\le T$ et

$$\max_{1\le j\le n}\left\|\zeta_j-\sum_{i=1}^m \vartheta_{ji}t_i\right\|\le \eta/S.$$

Autrement dit il existe $a=(a_1,\ldots,a_n)\in\mathbb{Z}^n$ tel que

$$\max_{1\le j\le n}\left|\zeta_j-a_j-\sum_{i=1}^m t_i\vartheta_{ji}\right|\le \eta/S.$$

On pose alors $\omega=a_1\omega_1+\cdots+a_n\omega_n$ et on utilise la relation

$$G(T)=\frac{S}{\eta\sum_{j=1}^n|\omega_j|}.$$

□

Remarque. Notons déjà que si l'hypothèse du lemme 4.2 est vraie pour une fonction F, alors elle est encore vraie pour toute fonction qui majore F. Il est quelquefois plus simple d'énoncer la conclusion non pas pour la fonction G elle même, mais pour une fonction minorant G. Plusieurs types de fonctions F interviendront.

- Le cas le plus favorable est celui où l'hypothèse est vraie avec $F(S)=cS^\kappa$ pour $S\ge S_0$ (où S_0, c et κ sont trois constantes) ; l'exposant κ est alors nécessairement $\ge n/m$. Dans ce cas on a $G(T)=c'T^\theta$ pour $T\ge T_0$ avec $\theta=1/\kappa$ et deux autres constantes T_0 et c'. En particulier on a $\theta\le m/n$. Dans ces circonstances, le nombre $\theta+1$ est le coefficient de densité de [W 1979], Chap. I §3 ; il est majoré par ℓ/n, où ℓ est le rang de $\Omega+Y$ sur $\mathbb{Z}$. Le lemme 1.3.7 de [W 1979] donne une majoration de ce coefficient introduisant des conditions algébriques, et non diophantiennes, sur la répartition de $\Omega+Y$ dans $\mathbb{R}^n$.
- Le cas le plus fréquent est celui où $F(S)=\exp\{c(\log S)^\kappa\}$, avec $\kappa\ge1$. Alors la conclusion est vraie pour une fonction G de la forme $G(T)=\exp\{c'(\log T)^\theta\}$ pour $T\ge T_0$, avec $\theta=1/\kappa$.
- Enfin dans les cas moins favorables on aura seulement $F(S)=\exp\{cS^\kappa\}$, avec $\kappa>0$, donc $G(T)=c'(\log T)^\theta$ avec $\theta=1/\kappa$.

Exercice. En utilisant le lemme 4.1, établir la réciproque du lemme 4.2.

b) Exemple : variétés abéliennes

Soit A une variété abélienne définie sur $\mathbb{R}$ de dimension g. On prend $E=T_A(\mathbb{R})$ et $\Omega=\operatorname{Ker}\exp_A$. On considère un sous-groupe Γ de $A(\mathbb{R})^0$, et on désigne par Y l'image inverse de Γ par $\exp_A$. Si ℓ est le rang de Γ, on peut écrire $Y=\Omega+\mathbb{Z}y_1+\cdots+\mathbb{Z}y_\ell$, où $y_1,\ldots,y_\ell$ sont des éléments de $T_A(\mathbb{R})$ linéairement indépendants modulo Ω. Pour avoir un énoncé de densité effectif de Γ dans $A(\mathbb{R})^0$, on est amené à rechercher des minorations de

$$\max_{1\le j\le\ell}\|\varphi(y_j)\|$$

pour $\varphi\in\Omega^*$, $\varphi\ne0$.

Supposons A définie sur un corps de nombres K plongé dans $\mathbb{R}$; soient $\omega_1,\ldots,\omega_g$ des périodes linéairement indépendantes de $\exp_A$ dans $T_A(\mathbb{R})$. La conjecture $4.2^?$ du chapitre IV, qui précise la conjecture de Mazur (conjecture 5 de [Maz 1992], correspondant au cas $K=\mathbb{Q}$ et $A(\mathbb{Q})$ de rang 1), contient l'énoncé suivant :

(?) *si $u\in T_A(\mathbb{R})$ est un logarithme d'un point d'ordre infini de $A(K)$, quand on écrit*

$$u=\vartheta_1\omega_1+\cdots+\vartheta_g\omega_g,$$

avec $\vartheta_i\in\mathbb{R}$, les nombres $1,\vartheta_1,\ldots,\vartheta_g$ sont linéairement indépendants sur $\mathbb{Q}$.

Le lemme 4.1 montre que la conjecture $1.1^?$ est équivalente à la suivante : soient $y_1,\ldots,y_\ell$ des logarithmes dans $T_A(\mathbb{C})$ d'une base du groupe de Mordell-Weil de $A(K)$. Ecrivons

$$y_j=\vartheta_{j1}\omega_1+\cdots+\vartheta_{jg}\omega_g,\qquad (1\le j\le\ell).$$

Conjecture $4.3^?$. – *Pour tout $\epsilon>0$ il existe une constante $C(\epsilon)>0$ ayant la propriété suivante : si $\varphi: T_A(\mathbb{R})\longrightarrow\mathbb{R}$ est une forme linéaire non nulle qui envoie tous les ω_i dans $\mathbb{Z}$, alors*

$$\max_{1\le j\le\ell}\|\varphi(y_j)\|\ge C(\epsilon)S^{-(g/\ell)-\epsilon}\qquad \text{où}\qquad S=\max_{1\le i\le g}|\varphi(\omega_i)|.$$

Le fait que la conjecture $4.3^?$ équivaut à l'inégalité proposée dans la conjecture $1.1^?$ sur la fonction η_A se voit en appliquant le lemme 4.1 avec

$$n=g,\qquad m=\ell,\qquad F(S)=C(\epsilon)S^{(g/\ell)+\epsilon},\qquad G(T)=C'(\epsilon')T^{(\ell/g)-\epsilon'}.$$

La hauteur de $\exp_A(t_1y_1+\cdots+t_\ell y_\ell)$ dans $A(K)$ est $\le CT^2=\log H$.

Pour démontrer le théorème 3.1, il suffit de vérifier, sous les hypothèses de la conjecture 4.3?,

$$\max_{1\le j\le \ell} \|\varphi(y_j)\| > \exp\{-c(\log S)^\kappa\}.$$

On aura alors la conclusion avec $\kappa = 1/\theta$. Si on obtient seulement

$$\max_{1\le j\le \ell} \|\varphi(y_j)\| > \exp\{-cS^\kappa\},$$

on trouvera

$$\eta_A(H) \le C(\log\log H)^{-\theta}$$

avec $\theta = 1/\kappa$.

Démonstration du corollaire 2.2. On utilise la proposition 2.1* pour vérifier l'hypothèse du lemme 4.2. Un élément φ de Ω^* est déterminé par l'entier $\varphi(\omega) = q$. Alors $\varphi(y_j) = qy_j/\omega$, et la proposition 2.1* montre que toute fonction F croissante vérifiant

$$F(S) \ge S^{-1}\exp\bigl\{c(\log S)(\log\log S)^{1+(2/\ell)}\bigr\}$$

pour $S \ge S_0$ satisfait l'hypothèse du lemme 4.2. On en déduit que la conclusion est vraie avec

$$G(T) = \exp\bigl\{c'(\log T)(\log\log T)^{-1-(2/\ell)}\bigr\}$$

pourvu que l'on prenne $c' < 1/c$. Enfin la quadraticité de la hauteur de Néron-Tate sur les courbes elliptiques montre que T est minoré par une constante fois $(\log H)^{1/2}$, ce qui donne le corollaire 2.2 à condition de prendre $C < 1/2c$. □

c) Variante réelle du lemme de transfert

Le lemme 4.2 est bien adapté au cas où l'espace réel ambiant contient un réseau apparaissant de façon naturelle, comme l'espace tangent d'une variété abélienne sur $\mathbb{R}$ avec le réseau des périodes. Quand il n'y a pas de réseau naturel, on peut appliquer la variante suivante. Nous allons donner d'abord un énoncé réel, puis nous l'utiliserons pour un sous-groupe d'un produit de copies de $\mathbb{R}$ et de $\mathbb{C}$. On désignera par $|\cdot|$ la norme $|x| = \max_{1\le i\le n}|x_i|$ sur $\mathbb{R}^n$ ou sur $\mathbb{C}^n$.

Lemme 4.4. – *Soient $y_1,\dots,y_\ell$ des éléments de $\mathbb{R}^n$ et $F : [S_0,\infty) \to \mathbb{R}_+$ une fonction réelle de variable réelle, croissante et non bornée. On suppose que pour tout $\sigma = (\sigma_1,\dots,\sigma_n) \in \mathbb{R}^n\setminus\{0\}$, si on pose*

$$\varphi(x) = \sigma_1x_1+\cdots+\sigma_nx_n \quad et \quad S = \max\bigl\{|\sigma_1|,\dots,|\sigma_n|; S_0\bigr\},$$

on a

$$\max_{1\le j\le \ell}\|\varphi(y_j)\| \ge 1/F(S).$$

Dans ces conditions il existe des constantes T_0, C_1 et C_2 positives telles que, si on pose $G(T) = C_1F^{-1}(C_2T)$ pour $T \ge T_0$, alors pour tout $x \in \mathbb{R}^n$ et tout $T \ge T_0(1+|x|)$, il existe $t \in \mathbb{Z}^\ell$ avec

$$\max_{1\le j\le \ell}|t_j| \le T \quad et \quad \bigl|x - t_1y_1 - \cdots - t_\ell y_\ell\bigr| \le 1/G(T).$$

Démonstration. Le sous-groupe $Y = \mathbb{Z}y_1+\cdots+\mathbb{Z}y_\ell$ est dense dans $\mathbb{R}^n$: en effet, l'hypothèse implique que pour tout $\varphi \in \mathrm{Hom}_\mathbb{R}(\mathbb{R}^n,\mathbb{R})$, $\varphi \ne 0$, on a $\varphi(Y) \not\subset \mathbb{Z}$. En particulier $\{y_1,\dots,y_\ell\}$ contient une base de $\mathbb{R}^n$. Il n'y a donc pas de restriction à supposer que $y_{\ell-n+1},\dots,y_\ell$ sont linéairement indépendants sur $\mathbb{R}$. On pose $m = \ell - n$, $\omega_i = y_{m+i}$, $(1 \le i \le n)$ et $\Omega = \mathbb{Z}\omega_1+\cdots+\mathbb{Z}\omega_n$. On va utiliser le lemme 4.2. Pour en vérifier l'hypothèse, on considère un élément non nul φ de Ω^*, et on pose $S_1 = \max_{1\le i\le n}|\varphi(\omega_i)|$. On peut aussi écrire $\varphi(x) = \sigma_1x_1+\cdots+\sigma_nx_n$ avec $\sigma_i = \varphi(e_i)$, $(1\le i\le n)$, où $(e_1,\dots,e_n)$ est la base canonique de $\mathbb{R}^n$. Alors le nombre $S = \max_{1\le i\le n}|\varphi(e_i)|$ vérifie $S_1 \le c_1S$, avec une constante c_1 qui ne dépend que de $y_1,\dots,y_\ell$. On définit une fonction F_1 par $F_1(S_1) = F(c_1S_1)$, de sorte que

$$\max_{1\le j\le \ell}\|\varphi(y_j)\| \ge 1/F_1(S_1).$$

Les hypothèses du lemme 4.2 sont donc vérifiées pour la fonction F_1. Par conséquent il existe une constante $c_2 \ge 1$ telle que, pour tout $T_1 \ge c_2$ et tout $x \in \mathbb{R}^n$, il existe $t \in \mathbb{Z}^\ell$ avec

$$\max_{1\le j\le m}|t_j| \le T_1 \quad \text{et} \quad \bigl|x - t_1y_1 - \cdots - t_\ell y_\ell\bigr| \le 1/G_1(T_1),$$

avec une fonction G_1 de la forme

$$G_1(T_1) = c_3F^{-1}(c_4T_1).$$

On majore $\max_{m+1\le j\le \ell}|t_j|$ par $c_5(T_1+|x|)$ et on pose $T_0 = 2c_2c_5$. Pour $T \ge T_0(1+|x|)$, on peut appliquer ce qui vient d'être démontré avec $T_1 = T/2c_5$. □

Exercice. Soient $y_1,\dots,y_\ell$ des éléments de $\mathbb{R}^n$ avec $\ell > n$. Vérifier que les deux conditions suivantes sont équivalentes.
(i) Pour tout $\epsilon > 0$, il existe une constante S_0 telle que, pour tout nombre réel $S \ge S_0$ et pour toute forme linéaire non nulle $\varphi : \mathbb{R}^n \to \mathbb{R}$ s'écrivant $\varphi(x) = \sigma_1x_1+\cdots+\sigma_nx_n$ avec des nombres réels $\sigma_1,\dots,\sigma_n$ vérifiant $\max\bigl\{|\sigma_1|,\dots,|\sigma_n|\bigr\} \le S$, *on a*

$$\max_{1\le j\le \ell}\|\varphi(y_j)\| \ge S^{-(n+\epsilon)/(\ell-n)}.$$

(ii)Pour tout $\epsilon > 0$, il existe une constante T_0 telle que, pour tout $x \in \mathbb{R}^n$ et tout nombre réel $T \ge T_0(1+|x|)$, il existe $t = (t_1,\dots,t_\ell) \in \mathbb{Z}^\ell$ vérifiant

$$\max_{1\le j\le \ell}|t_j| \le T \quad et \quad \bigl|x - t_1y_1 - \cdots - t_\ell y_\ell\bigr| \le T^{1-(\ell/n)+\epsilon}.$$

Remarque. L'hypothèse du lemme 4.4 fait intervenir tous les $\varphi \in \mathrm{Hom}_\mathbb{R}(\mathbb{R}^n,\mathbb{R})$, $\varphi \ne 0$, tandis que celle du lemme 4.2 se restreint aux éléments non nuls φ de Ω^*. En fait ce n'est pas différent : si on désigne par $|\cdot|$ la norme sur $\mathbb{R}^n$ définie par

$$|x_1\omega_1+\cdots+x_n\omega_n| = \max_{1\le i\le n}|x_i|,$$

alors pour tout $\varphi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$ il existe $\psi \in \Omega^*$ tel que

$$\|\psi(x) - \varphi(x)\| \le |x| \sum_{i=1}^{n} \|\varphi(\omega_i)\| \qquad \text{pour tout } x \in \mathbb{R}^n.$$

Exercice. Soient $\alpha_0, \dots, \alpha_n$ des nombres réels positifs multiplicativement indépendants. On suppose qu'il existe une constante $\kappa > 0$ telle que, pour tout nombre réel $S \ge 2$ et pour tout $(s_0, \dots, s_n) \in \mathbb{Z}^{n+1}$ satisfaisant $0 < \max_{0 \le i \le n} |s_i| \le S$, on ait

$$\left|\alpha_0^{s_0} - \alpha_1^{s_1} \cdots \alpha_n^{s_n}\right| \ge S^{-\kappa}.$$

Alors il existe une constante $C > 0$ telle que, pour tout $x = (x_1, \dots, x_n) \in \mathbb{R}^{n+1}$ et pour tout nombre réel $T \ge \max\{2, |x|\}$, il existe $(t_0, \dots, t_n) \in \mathbb{Z}^{n+1}$ satisfaisant $\max_{0 \le i \le n} |t_i| \le T$ et

$$\max_{1 \le i \le n} \left|x_i - \alpha_0^{t_i} \alpha_i^{t_0}\right| \le C T^{-1/\kappa}.$$

`Remarque.` D'après un théorème de N.I. Fel'dman (1968), l'hypothèse de cet exercice est satisfaite si les nombres $\alpha_0, \dots, \alpha_n$ sont algébriques ; voir par exemple [B 1979], Th. 3.1. Cette hypothèse est aussi vérifiée pour presque tout $n+1$-uplet $(\alpha_0, \dots, \alpha_n)$ de $\mathbb{R}^{n+1}$ (pour la mesure de Lebesgue) ; voir par exemple [Sc 1980], Chap. III Th. 3A.

d) Variante complexe du lemme de transfert

Soient r_1 et r_2 des entiers ≥ 0 avec $(r_1, r_2) \ne (0, 0)$. On pose $n = r_1 + r_2$ et $d = r_1 + 2r_2$. Pour $\xi \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ on pose $|\xi| = \max_{1 \le i \le n} |\xi_i|$.

Lemme 4.5. – *Soient $y_1, \dots, y_\ell$ des éléments de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ et $F : [S_0, \infty) \to \mathbb{R}_+$ une fonction réelle de variable réelle, croissante et non bornée. On suppose que pour tout $\sigma = (\sigma_1, \dots, \sigma_n) \in (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}) \setminus \{0\}$, si on définit $\varphi : \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \to \mathbb{R}$ par*

$$\varphi(\xi) = \sigma_1\xi_1 + \cdots + \sigma_n\xi_n + \overline{\sigma}_{r_1+1}\overline{\xi}_{r_1+1} + \cdots + \overline{\sigma}_n\overline{\xi}_n$$

et si on pose

$$S = \max\bigl\{|\sigma_1|, \dots, |\sigma_n|; S_0\bigr\},$$

on a

$$\max_{1 \le j \le \ell} \|\varphi(y_j)\| \ge 1/F(S).$$

Il existe des constantes T_0, C_1 et C_2 positives telles que, si on pose $G(T) = C_1 F^{-1}(C_2 T)$ pour $T \ge T_0$, alors pour tout $\xi \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ et tout $T \ge T_0(1 + |\xi|)$, il existe $t \in \mathbb{Z}^\ell$ avec

$$\max_{1 \le j \le \ell} |t_j| \le T \quad \textit{et} \quad \left|\xi - t_1 y_1 - \cdots - t_\ell y_\ell\right| \le 1/G(T).$$

Remarque. Dans le cas $r_2 = 0$, $n = d = r_1$, on retrouve le lemme 4.4.

Démonstration. On désigne par E l'espace vectoriel réel normé $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ et on définit $\theta : E \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$ par $\theta(x, z) = (x, z, \overline{z})$ et $\psi : E \longrightarrow \mathbb{R}^d$ par $\psi(x, z) = \bigl(x, \Re\mathrm{e}\,(z), \Im\mathrm{m}\,(z)\bigr)$.

On définit encore $y'_j = \psi(y_j)$, $(1 \le j \le \ell)$. On va vérifier l'hypothèse du lemme 4.4 pour le sous-groupe de $\mathbb{R}^d$ engendré par $y'_1, \dots, y'_\ell$. Pour cela, soit $\sigma' = (\sigma'_1, \dots, \sigma'_d) \in \mathbb{R}^d \setminus \{0\}$; on définit $\sigma = (\sigma_1, \dots, \sigma_n) \in E$ par

$$\sigma_\nu = \begin{cases} \sigma'_\nu & \text{pour } 1 \le \nu \le r_1, \\ \frac{1}{2}\bigl(\sigma'_{r_1+\nu} - i\sigma'_{n+\nu}\bigr) & \text{pour } r_1 < \nu \le n, \\ \\ \frac{1}{2}\bigl(\sigma'_{r_1+\nu} + i\sigma'_{n+\nu}\bigr) & \text{pour } n < \nu \le d, \end{cases}$$

de sorte que, si on définit $\varphi' : \mathbb{R}^d \to \mathbb{R}$ par $\varphi'(x_1, \dots, x_d) = \sigma'_1 x_1 + \cdots + \sigma'_d x_d$, on ait $\varphi = \varphi' \circ \psi$. L'hypothèse du lemme 4.5 concernant $\max_{1 \le j \le \ell} \|\varphi(y_j)\|$ permet donc de vérifier l'hypothèse corresponsante du lemme 4.4 portant sur $\max_{1 \le j \le \ell} \|\varphi'(y'_j)\|$. On en déduit que pour tout $\xi \in E$, si on pose $x = \psi(\xi)$, alors pour tout $T \ge T_0(1 + |x|)$ il existe $t \in \mathbb{Z}^\ell$ avec

$$\max_{1 \le j \le \ell} |t_j| \le T \quad \text{et} \quad \left|x - t_1 y'_1 - \cdots - t_\ell y'_\ell\right| \le 1/G(T).$$

On peut conclure

$$\left|\xi - t_1 y_1 - \cdots - t_\ell y_\ell\right| \le \sqrt{2}/G(T).$$

Remarque. Pour appliquer le lemme 4.5, on vérifiera une hypothèse apparemment plus forte :

pour tout $\sigma = (\sigma_1, \dots, \sigma_d) \in \mathbb{C}^d \setminus \{0\}$, si on définit $\varphi : \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \to \mathbb{C}$ par

$$\varphi(\xi) = \sigma_1\xi_1 + \cdots + \sigma_n\xi_n + \sigma_{n+1}\overline{\xi}_{r_1+1} + \cdots + \sigma_d\overline{\xi}_n$$

et si on pose

$$S = \max\bigl\{|\sigma_1|, \dots, |\sigma_d|; S_0\bigr\},$$

on a

$$\max_{1 \le j \le \ell} \|\varphi(y_j)\| \ge 1/F(S).$$

En fait, malgré les apparences, cette condition n'est pas plus restrictive que celle qui intervient dans l'hypothèse du lemme 4.5 (comparer avec la proposition 6.1 du chapitre II). En effet, partons de $\sigma \in \mathbb{C}^d$ et définissons, pour $1 \le j \le \ell$, $\epsilon_j = \|\varphi(y_j)\|$ et $s_j = \varphi(y_j) - \epsilon_j \in \mathbb{Z}$. Soit M la matrice de format $(d+1) \times \ell$ à coefficients complexes dont la j-ème colonne $(1 \le j \le \ell)$ a pour composantes les coordonnées de

$$\bigl(\theta(y_j), s_j + \epsilon_j\bigr) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \times \mathbb{C}.$$

Comme $\varphi(\xi) = \sigma_1\xi_1 + \cdots + \sigma_n\xi_n + \sigma_{n+1}\overline{\xi}_{r_1+1} + \cdots + \sigma_d\overline{\xi}_n$, la dernière ligne de M est combinaison linéaire des d précédentes (avec les coefficients complexes $\sigma_1, \dots, \sigma_d$). Alors la matrice M' de format $(d+1) \times \ell$ à coefficients réels, dont la j-ème colonne $(1 \le j \le \ell)$ a pour composantes les coordonnées de

$$\bigl(\psi(y_j), s_j + \Re\mathrm{e}\,(\epsilon_j)\bigr) \in \mathbb{R}^{d+1},$$

a aussi un déterminant nul. On en déduit qu'il existe $(\sigma'_1, \dots, \sigma'_n) \in \mathbb{R}^n$ tel que, si on pose

$$\varphi'(\xi) = \sigma'_1\xi_1 + \cdots + \sigma'_n\xi_n + \overline{\sigma}'_{r_1+1}\overline{\xi}_{r_1+1} + \cdots + \overline{\sigma}'_n\overline{\xi}_n,$$

on ait $\varphi'(y_j) = s_j + \Re\mathrm{e}\,(\epsilon_j)$, $(1 \le j \le \ell)$. Finalement, on utilise la majoration $|\Re\mathrm{e}\,(\epsilon_j)| \le |\epsilon_j|$.

§5. Irrationalité et transcendance

Soient G un groupe algébrique commutatif de dimension d défini sur le corps $\overline{\mathbb{Q}}$, Y un sous-groupe de $\mathcal{L}_{\overline{\mathbb{Q}}}(G)$ et $\varphi : T_G(\mathbb{C}) \to \mathbb{C}$ une forme linéaire. On étudie d'abord un problème d'irrationalité : *a-t-on* $\varphi(Y) \subset \mathbb{Q}$? Pour répondre à cette question on étudiera le $\mathbb{Z}$-module $\varphi^{-1}(\mathbb{Q}) \cap \mathcal{L}_{\overline{\mathbb{Q}}}(G)$. Un problème un peu plus général (par lequel on commencera) consiste à rechercher une minoration du rang sur $\mathbb{Z}$ de $\varphi(Y)$; si on trouve que ce rang est ≥ 2, on en déduit que $\varphi(Y)$ n'est pas contenu dans $\mathbb{Q}$. C'est précisément une telle information que fournit le théorème du sous-groupe algébrique. Une autre généralisation du problème d'irrationalité est une question de transcendance : *a-t-on* $\varphi(Y) \subset \overline{\mathbb{Q}}$? Cette fois-ci, c'est l'étude du $\mathbb{Q}$-espace vectoriel $\varphi^{-1}(\overline{\mathbb{Q}}) \cap \mathcal{L}_{\overline{\mathbb{Q}}}(G)$ qui permet d'obtenir une réponse. Nous verrons que le théorème du sous-groupe algébrique s'applique encore, mais nécessite des hypothèses un peu plus contraignantes que pour la question d'irrationalité, ce qui est bien naturel.

a) Minoration du rang sur $\mathbb{Z}$ de $\varphi(Y)$ pour $Y \subset \mathcal{L}_{\overline{\mathbb{Q}}}(G)$.

Si le noyau de φ contient un sous-espace vectoriel de $T_G(\mathbb{C})$ de la forme $T_{G'}(\mathbb{C})$, où G' est un sous-groupe algébrique de G défini sur $\overline{\mathbb{Q}}$ de dimension ≥ 1, on ne peut pas, en général, minorer le rang sur $\mathbb{Z}$ de $\varphi(Y)$ en fonction du rang de Y, mais il faut faire intervenir le rang de $Y/Y \cap T_{G'}(\mathbb{C})$. Quitte à remplacer G par G/G', on se ramène à la situation suivante :

($*$) *On suppose que le noyau de φ ne contient aucun sous-espace de $T_G(\mathbb{C})$ de la forme $T_{G'}(\mathbb{C})$, G' sous-groupe algébrique de G défini sur $\overline{\mathbb{Q}}$ de dimension ≥ 1.*

On rappelle la notation $\alpha(G) = d_1 + 2d_2$ introduite au chapitre IV. On pose aussi

$$\kappa = \mathrm{rang}_{\mathbb{Z}}\big(\Omega_G \cap \mathrm{Ker}\ \varphi\big),$$

où Ω_G est le noyau de l'exponentielle de $G(\mathbb{C})$. D'après le théorème du sous-groupe algébrique, sous l'hypothèse ($*$) on a

$$\mathrm{rang}_{\mathbb{Z}}\big(Y \cap \mathrm{Ker}\ \varphi\big) \leq \big(\alpha(G) - \kappa\big)(d-1),$$

ce qui implique

$$\mathrm{rang}_{\mathbb{Z}}\varphi(Y) \geq \mathrm{rang}_{\mathbb{Z}}Y - \big(\alpha(G) - \kappa\big)(d-1). \tag{5.1}$$

Par exemple si $G = A$ est une variété abélienne simple de dimension g, il suffit de demander que φ soit non nulle pour assurer que son noyau ne contient pas de sous-espace de la forme $T_{G'}(\mathbb{C})$ de dimension > 0, et alors

$$\mathrm{rang}_{\mathbb{Z}}\varphi(Y) \geq \mathrm{rang}_{\mathbb{Z}}Y - (2g - \kappa)(g-1).$$

Dans ce cas, le nombre $\kappa = \mathrm{rang}_{\mathbb{Z}}\big(\Omega_A \cap \mathrm{Ker}\ \varphi\big)$ vérifie $0 \leq \kappa \leq g-1$, donc si on pose $m = \mathrm{rang}_{\mathbb{Z}}Y$, on a toujours

$$\mathrm{rang}_{\mathbb{Z}}\varphi(Y) \geq m - 2g^2 + 2g,$$

tandis que pour $\kappa = g-1$, on a

$$\mathrm{rang}_{\mathbb{Z}}\varphi(Y) \geq m - g^2 + 1.$$

La condition $\kappa = g-1$ est vérifiée quand il existe g périodes $\omega_1, \ldots, \omega_g$ de $\Omega_A = \mathrm{Ker}\ \exp_A$, linéairement indépendantes, dont les images par φ sont rationnelles : $\varphi(\omega_i) \in \mathbb{Q}$ pour $1 \leq i \leq g$.

b) Irrationalité.

En appliquant la majoration (5.1) au sous-groupe $Y = \varphi^{-1}(\mathbb{Q}) \cap \mathcal{L}_{\overline{\mathbb{Q}}}(G)$ de $T_G(\mathbb{C})$, on déduit l'énoncé suivant :

Proposition 5.2. – *Soient G un groupe algébrique commutatif de dimension d défini sur le corps $\overline{\mathbb{Q}}$ et $\varphi : T_G(\mathbb{C}) \to \mathbb{C}$ une forme linéaire. On suppose que le noyau de φ ne contient aucun sous-espace non nul de $T_G(\mathbb{C})$ de la forme $T_{G'}(\mathbb{C})$. Alors*

$$\mathrm{rang}_{\mathbb{Z}}\big(\varphi^{-1}(\mathbb{Q}) \cap \mathcal{L}_{\overline{\mathbb{Q}}}(G)\big) \leq 1 + \big(\alpha(G) - \kappa\big)(d-1).$$

Appliquons ce résultat à une variété abélienne simple. On utilise encore la remarque suivante : si $\omega_1, \ldots, \omega_k$ sont k périodes de Ω_A, linéairement indépendantes sur $\mathbb{Z}$, telles que $\varphi(\omega_i) \in \mathbb{Q}$ pour $1 \leq i \leq k$, alors $\kappa \geq \max\{0, k-1\}$.

Corollaire 5.3. – *Soient A une variété abélienne simple de dimension g, $\varphi : T_A(\mathbb{C}) \to \mathbb{R}$ une forme linéaire non nulle et Y un sous-groupe de $\mathcal{L}_{\overline{\mathbb{Q}}}(A)$ de rang m. On pose $k = \mathrm{rang}_{\mathbb{Z}}\big(Y \cap \Omega_A\big)$. On suppose*

$$m \geq \begin{cases} 2g^2 - g + 1 - k(g-1) & \text{si } k \geq 1, \\ 2g^2 - 2g + 2 & \text{si } k = 0. \end{cases}$$

Alors $\varphi(Y) \not\subset \mathbb{Q}$.

Remarque. Le rang sur $\mathbb{Z}$ de $\Gamma = \exp_A(Y)$ est $\ell = m - k$, et la condition sur m s'écrit aussi :

$$\ell \geq \begin{cases} 2g^2 - g + 1 - kg & \text{si } k \geq 1, \\ 2g^2 - 2g + 2 & \text{si } k = 0. \end{cases}$$

On a toujours $k \leq g$; dans le cas le plus favorable $k = g$, la condition s'écrit $m \geq g^2 + 1$, ou encore $\ell \geq g^2 - g + 1$; on retrouve bien entendu l'hypothèse de la proposition 4.1 – partie a) – du chapitre IV.

c) Transcendance.

Le corollaire 5.3 donne un résultat d'irrationalité ; il est naturel de poser la question de la transcendance de l'un au moins des nombres $\varphi(y_j)$, $(1 \leq j \leq \ell)$. On obtient encore un tel énoncé en utilisant le théorème du sous-groupe algébrique, non plus directement pour G, mais pour le produit $\mathbb{G}_{\mathrm{a}} \times G$.

Proposition 5.4. – *Soient G un groupe algébrique commutatif de dimension d défini sur le corps $\overline{\mathbb{Q}}$ et $\varphi : T_G(\mathbb{C}) \to \mathbb{C}$ une forme linéaire. On suppose que le noyau de φ ne contient pas de sous-espace non nul de $T_G(\mathbb{C})$ de la forme $T_{G'}(\mathbb{C})$. On suppose aussi qu'il n'y a pas de morphisme non constant de groupes algébriques de $\mathbb{G}_{\mathrm{a}}$ dans G. Soit κ le rang sur $\mathbb{Z}$ de $\Omega_G \cap \mathrm{Ker}\ \varphi$. Alors*

$$\dim_{\mathbb{Q}}\big(\varphi^{-1}(\overline{\mathbb{Q}}) \cap \mathcal{L}_{\overline{\mathbb{Q}}}(G)\big) \leq \big(\alpha(G) - \kappa\big)d.$$

Démonstration. On considère le groupe algébrique $G^* = \mathbb{G}_{\mathrm{a}} \times G$, qui est de dimension $d^* = d + 1$ et satisfait $\alpha(G^*) = \alpha(G)$. L'hypothèse $\mathrm{Hom}(\mathbb{G}_{\mathrm{a}}, G) = 0$ assure que tout sous-groupe algébrique connexe du produit $\mathbb{G}_{\mathrm{a}} \times G$ est de la forme $\{0\} \times G'$ ou $\mathbb{G}_{\mathrm{a}} \times G'$, pour un sous-groupe algébrique (connexe) G' de G. On définit un sous-espace $\mathcal{V}$ de $T_{G^*}(\mathbb{C})$ par

$$\mathcal{V} = \big\{\big(\varphi(z), z\big) \,;\, z \in T_G(\mathbb{C})\big\}.$$

Le rang de $\mathcal{V}\cap\Omega_{G^*}$ est encore κ. Le fait que le noyau de φ ne contienne pas de sous-espace non nul de $T_G(\mathbb{C})$ de la forme $T_{G'}(\mathbb{C})$ va nous permettre de vérifier que $\mathcal{V}$ ne contient pas de sous-espace non nul de $T_{G^*}(\mathbb{C})$ de la forme $T_{G''}(\mathbb{C})$, avec G'' sous-groupe algébrique de G^* défini sur $\overline{\mathbb{Q}}$. En effet, étant donné que $\mathcal{V}$ ne contient pas $\mathbb{C}\times\{0\}$, si G'' est un tel sous-groupe algébrique connexe, alors G'' s'écrit $\{0\}\times G'$, avec G' sous-groupe algébrique de G, et $T_{G'}(\mathbb{C})$ est contenu dans le noyau de φ. Alors $G'=0$. Pour conclure on applique le théorème 2.3 du chapitre IV, en remarquant que l'on a

$$\mathcal{L}_{\overline{\mathbb{Q}}}(G^*)=\overline{\mathbb{Q}}\times\mathcal{L}_{\overline{\mathbb{Q}}}(G),\quad \text{et}\quad \dim_{\mathbb{Q}}\big(\mathcal{V}\cap\mathcal{L}_{\overline{\mathbb{Q}}}(G^*)\big)=\dim_{\mathbb{Q}}\big(\varphi^{-1}(\overline{\mathbb{Q}})\cap\mathcal{L}_{\overline{\mathbb{Q}}}(G)\big).$$

□

Remarque. L'hypothèse $\mathrm{Hom}(\mathbb{G}_{\mathrm{a}},G)=0$ de la proposition 5.4 est nécessaire : si on considère le groupe algébrique $\mathbb{G}_{\mathrm{a}}\times\mathbb{G}_{\mathrm{m}}$ et la forme linéaire $\varphi(z_1,z_2)=z_1+z_2$, la condition sur le noyau de φ est bien satisfaite, et pourtant

$$\varphi^{-1}(\overline{\mathbb{Q}})\cap\mathcal{L}_{\overline{\mathbb{Q}}}(G)=\varphi^{-1}(\overline{\mathbb{Q}})\cap(\overline{\mathbb{Q}}\times\mathcal{L})=\overline{\mathbb{Q}}\times\{0\}$$

n'est pas de dimension finie sur $\mathbb{Q}$.

Corollaire 5.5. – *Soient A une variété abélienne simple de dimension g définie sur $\overline{\mathbb{Q}}$, Y un sous-groupe de de $\mathcal{L}_{\overline{\mathbb{Q}}}(A)$ de rang m et $\varphi: T_G(\mathbb{C})\to\mathbb{C}$ une forme linéaire non nulle. On suppose que Y contient k éléments linéairement indépendants $\omega_1,\dots,\omega_k$ de Ω_A tels que $\varphi(\omega_i)\in\mathbb{Z}$ pour $1\le i\le k$. On suppose enfin*

$$m\ge\begin{cases}2g^2+g+1-kg & \text{si } k\ge 1,\\ 2g^2+1 & \text{si } k=0.\end{cases}$$

Alors $\varphi(Y)\not\subset\overline{\mathbb{Q}}$.

On peut énoncer l'hypothèse sur le rang en terme du paramètre $\ell=m-k$, qui est majoré par le rang sur $\mathbb{Z}$ de $\Gamma=\exp_A(Y)$:

$$\ell\ge\begin{cases}2g^2+g+1-k(g+1) & \text{si } k\ge 1,\\ 2g^2+1 & \text{si } k=0.\end{cases}$$

Quand $k=g$; l'hypothèse s'écrit $m\ge g^2+g+1$, ou encore $\ell\ge g^2+1$.

d) Groupes linéaires.

En considérant des variétés abéliennes simples, nous avons évité les difficultés qui apparaissent avec les sous-groupes algébriques : il suffit de supposer $\varphi\neq 0$ pour assurer que le noyau de φ ne contient pas de sous-espace non nul de la forme $T_{G'}(\mathbb{C})$. Nous traitons maintenant un autre exemple pour montrer comment surmonter cette difficulté. On travaille avec des logarithmes usuels de nombres algébriques :

$$\mathcal{L}=\mathcal{L}_{\overline{\mathbb{Q}}}(\mathbb{G}_{\mathrm{m}})=\{z\in\mathbb{C}\,;\,e^z\in\overline{\mathbb{Q}}^{\times}\}.$$

Proposition 5.6. – *Soient n et ℓ des entiers positifs, y_{ij}, $(1\le i\le n,\ 1\le j\le\ell)$ des éléments $\mathbb{Z}$-linéairement indépendants de $\mathcal{L}$, et $\varphi:\mathbb{C}^n\to\mathbb{C}$ une forme linéaire non nulle. Pour $1\le j\le\ell$ on définit $y_j\in\mathcal{L}^n$ par $y_j=(y_{1j},\dots,y_{nj})$, et on désigne par Y le sous-groupe de $\mathcal{L}^n$ engendré par $y_1,\dots,y_\ell$.*
a) On a

$$\mathrm{rang}_{\mathbb{Z}}\varphi(Y)\ge\ell-n^2+n.$$

b) Si $\ell\ge n^2-n+2$, alors un au moins des ℓ nombres $\varphi(y_j)$, $(1\le j\le\ell)$, est irrationnel.
c) Si $\ell\ge n^2+1$, alors un au moins des nombres $\varphi(y_j)$, $(1\le j\le\ell)$, est transcendant.

Démonstration.
a) La partie a) de la proposition 5.6 se déduit du théorème du sous-groupe linéaire (théorème 2.6 du chapitre III) de la manière suivante. Soit W le plus grand sous-espace de $\mathbb{C}^n$, rationnel sur $\mathbb{Q}$ et contenu dans $\mathrm{Ker}\ \varphi$. On désigne par d la codimension de W dans $\mathbb{C}^n$ et on identifie le quotient $\mathbb{C}^n/W$ avec $\mathbb{C}^d$ en choisissant une base de $\mathbb{C}^n/W$ rationnelle sur $\mathbb{Q}$ (c'est l'image par la surjection canonique $\mathbb{C}^n\to\mathbb{C}^n/W$ de d éléments de $\mathbb{Q}^n$ linéairement indépendants modulo W). Soit $\mathcal{V}$ l'hyperplan $(\mathrm{Ker}\ \varphi)/W$ dans $\mathbb{C}^d$. D'après le théorème du sous-groupe linéaire (avec $d_0=0$), on a

$$\dim_{\mathbb{Q}}(\mathcal{V}\cap\mathcal{L}^d)\le d(d-1).$$

L'hypothèse d'indépendance linéaire des y_{ij} assure $Y\cap W=\{0\}$, donc $\mathrm{rang}_{\mathbb{Z}}(Y/Y\cap W)=\mathrm{rang}_{\mathbb{Z}}Y=\ell$ et

$$\mathrm{rang}_{\mathbb{Z}}(Y\cap\mathrm{Ker}\ \varphi)=\mathrm{rang}_{\mathbb{Z}}(Y/Y\cap W)\cap\mathcal{V}\le\dim_{\mathbb{Q}}(\mathcal{V}\cap\mathcal{L}^d)\le d(d-1)\le n(n-1).$$

Par conséquent on a

$$\mathrm{rang}_{\mathbb{Z}}\varphi(Y)=\mathrm{rang}_{\mathbb{Z}}Y-\mathrm{rang}_{\mathbb{Z}}(Y\cap\mathrm{Ker}\ \varphi)\ge\ell-n(n-1).$$

b) La partie b) de la proposition 5.6 résulte de la partie a). On remarquera d'ailleurs qu'elle implique la partie a) du corollaire 2.11 du chapitre III dans le cas $d_0=0$.
c) On va encore utiliser le théorème du sous-groupe linéaire, mais avec $d_0=1$. On désigne encore par W le plus grand sous-espace de $\mathbb{C}^n$, rationnel sur $\mathbb{Q}$ et contenu dans $\mathrm{Ker}\ \varphi$; si d_1 désigne la codimension de W dans $\mathbb{C}^n$, le choix d'une base de $\mathbb{C}^n/W$ rationnelle sur $\mathbb{Q}$ revient à considérer une surjection $s:\mathbb{C}^n\to\mathbb{C}^{d_1}$ de noyau W vérifiant $s(\mathbb{Q}^n)=\mathbb{Q}^{d_1}$. On considère l'hyperplan

$$\mathcal{V}=\big\{\big(\varphi(z),s(z)\big)\,;\,z\in\mathbb{C}^n\big\}$$

de $\mathbb{C}\times\mathbb{C}^{d_1}$. On a $\mathcal{V}\cap(\mathbb{C}\times\{0\})=\{0\}$ car $W\subset\mathrm{Ker}\ \varphi$, et $\mathcal{V}\cap(\{0\}\times\mathbb{Q}^{d_1})=\{0\}$ car W a été choisi maximal. On déduit du théorème 2.6 du chapitre III :

$$\dim_{\mathbb{Q}}\big(\mathcal{V}\cap(\overline{\mathbb{Q}}\times\mathcal{L}^{d_1})\big)\le d_1^2.$$

Comme $Y\cap W=\{0\}$, le sous-groupe

$$\big\{\big(\varphi(y),s(y)\big)\,;\,y\in Y\big\}$$

de $\mathcal{V}$ est de rang $\ell\ge n^2+1>d_1^2$. Il n'est donc pas contenu dans $\overline{\mathbb{Q}}\times\mathcal{L}^{d_1}$, ce qui montre que $\varphi(Y)$ n'est pas contenu dans $\overline{\mathbb{Q}}$. □

Exercice. Déduire le théorème des six exponentielles (Th. 1.7 du Chap. III) de la partie a) de la proposition 5.6, et le théorème de Gel'fond-Schneider (Th. 1.3 du Chap. III) de la partie c) de la proposition 5.6.

§6. Approximation diophantienne dans les groupes algébriques

a) Variétés abéliennes

Soient K un corps de nombres et A une variété abélienne simple sur K de dimension g. On plonge A dans un espace projectif sur K, et on choisit aussi une base de $T_A(\mathbb{C})$. Soient $y_1, \dots, y_m$ des éléments de $T_A(\mathbb{C})$, linéairement indépendants sur $\mathbb{Z}$, tels que les points $\gamma_j = \exp_A(y_j)$, $(1 \le j \le m)$ appartiennent à $A(K)$. Enfin soient $\omega_1, \dots, \omega_g$ des éléments linéairement indépendants de $\Omega_A = \mathrm{Ker}\ \exp_A$.

Théorème 6.1*.
a) On suppose $m \ge 2g^2 - 2g + 2$. Il existe une constante positive C_1, dépendant de A, $y_1, \dots, y_m$, $\omega_1, \dots, \omega_g$ et de K, ayant la propriété suivante : si $\varphi : T_A(\mathbb{C}) \longrightarrow \mathbb{C}$ est une forme linéaire non nulle, et si on pose

$$S = \max\bigl\{2\,,\ \max_{1\le i\le g} |\varphi(\omega_i)|\bigr\},$$

alors

$$\max_{1\le j\le m} \|\varphi(y_j)\| \ge \exp\bigl(-C_1 S^{\kappa_1}\bigr),$$

avec

$$\kappa_1 = g + \frac{2g^3}{m - 2g^2 + 2g - 1}.$$

b) On suppose $m \ge 2g^2 + 1$. Il existe une constante positive C_2, dépendant de A, $y_1, \dots, y_m$ et de K, ayant la propriété suivante : si $\varphi : T_A(\mathbb{C}) \longrightarrow \mathbb{C}$ est une forme linéaire non nulle, si $\beta_1, \dots, \beta_m$ sont des éléments de K, et si on pose

$$\log B = \max\bigl\{1\,,\ \max_{1\le j\le m} \mathrm{h}(\beta_j)\bigr\},$$

alors

$$\max_{1\le j\le m} |\varphi(y_j) - \beta_j| \ge \exp\bigl(-C_2 (\log B)^{\kappa_2}\bigr),$$

avec

$$\kappa_2 = 1 + \frac{2g^2}{m - 2g^2}.$$

Noter que l'on a

$$\theta_1 = \frac{1}{\kappa_1} = \frac{1}{g} - \frac{2g}{m + 2g - 1} \qquad \text{et} \quad \theta_2 = \frac{1}{\kappa_2} = 1 - \frac{2g^2}{m}.$$

Il est vraisemblable que l'on peut préciser le théorème 6.1* de la manière suivante :

(?) *a) On suppose que l'ensemble $\{y_1, \dots, y_m\}$ contient $\{\omega_1, \dots, \omega_g\}$; si $m \ge g^2 + 1$, il existe deux constantes positives C_1' et κ_1' ayant la propriété suivante : si $\varphi : T_A(\mathbb{C}) \longrightarrow \mathbb{C}$ est une forme linéaire non nulle, et si on pose*

$$S = \max\bigl\{2\,,\ \max_{1\le i\le g} |\varphi(\omega_i)|\bigr\},$$

alors

$$\max_{1\le j\le m} \|\varphi(y_j)\| \ge \exp\bigl(-C_1' S^{\kappa_1'}\bigr).$$

(?) *b) On suppose que l'ensemble $\{y_1, \dots, y_m\}$ contient $\{\omega_1, \dots, \omega_g\}$; si $m \ge g^2 + g + 1$, il existe deux constantes positives C_2' et κ_2' ayant la propriété suivante : si $\varphi : T_A(\mathbb{C}) \longrightarrow \mathbb{C}$ est une forme linéaire non nulle, si $\beta_1, \dots, \beta_m$ sont des éléments de K, et si on pose*

$$\log B = \max\bigl\{1\,,\ \max_{1\le j\le m} \mathrm{h}(\beta_j)\bigr\},$$

alors

$$\max_{1\le j\le m} |\varphi(y_j) - \beta_j| \ge \exp\bigl(-C_2' (\log B)^{\kappa_2'}\bigr).$$

Démonstration du théorème 3.1. Si ℓ est le rang du groupe de Mordell-Weil $A(K)$, alors le sous-groupe $\exp_{A,\mathbb{R}}^{-1}\bigl(A(K)\bigr)$ de $T_A(\mathbb{R})$ est de rang $m = \ell + g$. On choisit des éléments linéairement indépendants $\omega_1, \dots, \omega_g$, $y_1, \dots, y_\ell$ dans $\exp_{A,\mathbb{R}}^{-1}\bigl(A(K)\bigr)$ avec $\omega_1, \dots, \omega_g$ dans $\Omega_{A,\mathbb{R}} = \mathrm{Ker}\ \exp_{A,\mathbb{R}}$ et on pose

$$Y = \mathbb{Z}\omega_1 + \dots + \mathbb{Z}\omega_g + \mathbb{Z}y_1 + \dots + \mathbb{Z}y_\ell.$$

On utilise le théorème 6.1*, partie b), avec $y_{\ell+j} = \omega_j$, $(1 \le j \le g)$, en prenant pour β_j un entier à distance minimale de y_j, $(1 \le j \le \ell)$. Pour tout $\varphi \in \Omega^*$, $\varphi \ne 0$, on a (avec les notations du théorème 6.1*)

$$\max_{1\le j\le m} \|\varphi(y_j)\| \ge 1/F(S)$$

avec $F(S) = \exp\{C_2 (\log S)^{\kappa_2}\}$. Le lemme 4.2 appliqué au $\mathbb{R}$-espace vectoriel $T_A(\mathbb{R})$ permet de conclure. □

Remarque. Pour $\ell \ge 2g^2 - 3g + 2$, la partie a) du théorème 6.1* donne

$$\max_{1\le j\le m} \|\varphi(y_j)\| \ge 1/F(S)$$

avec $F(S) = \exp\{C_1 (\log S)^{\kappa_1}\}$. Alors le lemme 4.2 permet de conclure

$$\eta_A(H) \le C(\log\log H)^{-\theta_1}$$

comme cela a été annoncé après le théorème 3.1.

b) Groupe multiplicatif

Le lemme 4.5 ramène la démonstration du théorème 3.2 à un problème d'approximation diophantienne : il s'agit de minorer $\max_{1\le j\le \ell} \|\varphi(y_j)\|$ quand φ est une forme linéaire non nulle sur $\mathbb{C}^n$ et $y_1, \dots, y_\ell$ sont des éléments de $\mathcal{L}^n$.

Théorème 6.2*. – *Soient y_{ij} $(1 \le i \le d,\ 1 \le j \le \ell)$ des éléments de $\mathcal{L}$ linéairement indépendants sur $\mathbb{Q}$. On définit, pour $1 \le j \le \ell$,*

$$y_j = (y_{1j}, \dots, y_{dj}) \in \mathcal{L}^d.$$

a) On suppose $\ell \ge d^2-d+2$. Il existe une constante positive C_1 ayant la propriété suivante : si S est un nombre réel ≥ 2, si $\sigma_1, \dots, \sigma_d$ sont des nombres réels satisfaisant

$$0 < \max_{1\le i\le d} |\sigma_i| \le S,$$

et si $\varphi : \mathbb{C}^d \longrightarrow \mathbb{C}$ désigne la forme linéaire $(z_1, \dots, z_d) \to \sigma_1 z_1 + \cdots + \sigma_d z_d$, alors

$$\max_{1\le j\le \ell} \|\varphi(y_j)\| \ge \exp\bigl(-C_1 S^{\kappa_1}\bigr)$$

avec

$$\kappa_1 = d + \frac{d^3}{\ell - d^2 + d - 1}.$$

b) On suppose $\ell \ge d^2+1$. Il existe une constante positive C_2 ayant la propriété suivante : si $\varphi : \mathbb{C}^d \longrightarrow \mathbb{C}$ est une forme linéaire non nulle, si $\beta_1, \dots, \beta_m$ sont des éléments de K, et si on pose

$$\log B = \max\bigl\{1\,,\ \max_{1\le j\le m} \mathrm{h}(\beta_j)\bigr\},$$

alors

$$\max_{1\le j\le \ell} |\varphi(y_j) - \beta_j| \ge \exp\bigl(-C_2 (\log B)^{\kappa_2}\bigr)$$

avec

$$\kappa_2 = 1 + \frac{d^2}{\ell - d^2}.$$

On notera que l'on a

$$\theta_1 = \frac{1}{\kappa_1} = \frac{1}{d} - \frac{d}{\ell + d - 1} \qquad \text{et} \quad \theta_2 = \frac{1}{\kappa_2} = 1 - \frac{d^2}{\ell}.$$

Exercice.
a) Soient α_1, α_2 deux nombres complexes algébriques non nuls. On choisit des déterminations de leurs logarithmes, $\log\alpha_1$ et $\log\alpha_2$, et on suppose que ces deux nombres $\log\alpha_1$ et $\log\alpha_2$ sont linéairement indépendants sur $\mathbb{Q}$. Soit K un corps de nombres contenant α_1 et α_2. Déduire du théorème 6.2 qu'il existe une constante $C > 0$, dépendant seulement de*

$\log\alpha_1, \log\alpha_2$ et K, ayant la propriété suivante : si β est un élément de K, et si B est un nombre réel qui satisfait $\log B \ge \max\{1, \mathrm{h}(\beta)\}$, alors

$$|\beta\log\alpha_1 - \log\alpha_2| \ge \exp\bigl\{-C(\log B)^2\bigr\}.$$

b) En déduire l'énoncé suivant. Soient α_1, α_2 deux nombres algébriques réels positifs multiplicativement indépendants. Il existe une constante $c > 0$ ayant la propriété suivante : pour tout $x \in \mathbb{R}_+^*$ et pour tout nombre réel $T \ge \log\max\{2, |x|\}$, il existe $(t_1, t_2) \in \mathbb{Z}^2$ vérifiant $\max\{|t_1|, |t_2|\} \le T$ et

$$\bigl|x - \alpha_1^{t_1}\alpha_2^{t_2}\bigr| \le \exp\bigl\{-c(\log T)^{1/2}\bigr\}.$$

Démonstration du théorème 3.2. Pour $1 \le j \le \ell$, on pose

$$y_{\nu j} = \log\gamma_{\nu j}, \qquad (1 \le \nu \le r_1),$$

puis on choisit $y_{r_1+1,j}, \dots, y_{nj}$ dans $\mathbb{C}$ tels que $\exp(y_{\nu j}) = y_{\nu j}$ pour $r_1 < \nu \le n$. On pose encore $y_{\nu j} = \overline{y}_{\nu - r_1, j}$ pour $n < \nu \le d$ et $1 \le j \le \ell$. Les $d\ell$ nombres $y_{\nu j}$, $(1 \le \nu \le d$, $1 \le j \le \ell)$ sont alors $\mathbb{Q}$-linéairement indépendants. On peut appliquer le théorème 6.2* (en prenant pour β_j un entier à distance minimale de $\varphi(y_j)$) pour vérifier l'hypothèse du lemme 4.5. Soit $\zeta \in (\mathbb{R}_+^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$; on pose $z_\nu = \log\zeta_\nu$ pour $1 \le \nu \le r_1$; ensuite, pour $r_1 < \nu \le n$ on définit $z_{r_1+\nu}$ comme la détermination principale du logarithme de $\zeta_{r_1+\nu}$. Ainsi on a, pour $1 \le \nu \le n$,

$$|z_\nu|^2 \le \bigl(\log|\zeta_\nu|\bigr)^2 + \pi^2 \le 22\bigl(\log(2 + |\zeta_\nu|)\bigr)^2,$$

et

$$1 + |z_\nu| \le 7\log(2 + |\zeta_\nu|).$$

Le théorème 3.2 résulte alors du lemme 4.5. □

Exercice. Si, dans l'énoncé du théorème 3.2, on remplace l'hypothèse $\ell > d^2$ par $\ell > d^2 - d + 1$, alors on obtient la conclusion avec l'estimation

$$\max_{1\le i\le n} \bigl|\zeta_i - \gamma_{i1}^{t_1}\cdots\gamma_{i\ell}^{t_\ell}\bigr| \le C(\log\log T)^{-\theta} \quad \text{et} \quad \theta = \frac{\ell - d^2 + d - 1}{d(\ell + d - 1)}.$$

Références

[B 1979] Baker, Alan.— *Transcendental number theory.* Cambridge University Press, London-New York, 1975. x+147 pp.
Second edition (Repr. of 1975 with additional material) Cambridge University Press, 1979. x+164 pp.
Reissue by Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1990. x+165 pp.
`Zbl 297.10013, 497.10023, 715.11032` `MR 54 #10163, 91f:11049`

[BDGP 1995] Barré-Sirieix, Katia ; Diaz, Guy ; Gramain, François ; Philibert, Georges.— Une preuve de la conjecture de Mahler-Manin. Invent. Math. **124** (1996), no. 1–3, 1–9.
`Zbl 853.11059` `MR 96j:11103`

[Be 1995] Bertrand, Daniel.— Points rationnels sur les sous-groupes compacts des groupes algébriques. Exp. Math. **4** (1995), no. 2, 145–151.
`Zbl 859.11046` `MR 97h:14038`

[BeM 1980] Bertrand, Daniel ; Masser, David.— Linear forms in elliptic integrals. Invent. Math. **58** (1980), no. 3, 283–288.
`Zbl 425.10041` `MR 81e:10032`

[Bo 1974] Bourbaki, Nicolas.— *Eléments de mathématiques.* Première partie : Les structures fondamentales de l'analyse. Livre III, Topologie générale ; chapitre V : *Groupes à un paramètre.* chapitre VII : *Les groupes additifs* $\mathbb{R}^n$. Actualités Sci. Ind. **1029**, Hermann, Paris, 1947 et 1974. ii+132 pp.
`Zbl 337.54001` `MR 9,261a`
General topology. Chapters 5–10. Translated from the French. Reprint of the 1966 edition. Elements of Mathematics. Springer-Verlag, Berlin-New York, 1989. iv+363 pp.
`Zbl 683.54004` `MR 90a:54001b`

[Ca 1957] Cassels, J.W.S.— *An Introduction to Diophantine Approximation.* Cambridge Tracts in Mathematics and Mathematical Physics, No. **45**, Cambridge University Press, New York, 1957. x+166 pp.
Reprint of the 1957 edition. Hafner Publishing Co., New York, 1972. x+169 pp.
`Zbl 098.26301` `MR 19,396h, 50 #2084`

[CT 1992] Colliot-Thélène, Jean-Louis.— L'arithmétique des variétés rationnelles. Ann. Fac. Sci. Toulouse, VI. Sér., Math. **1** (1992), no. 3, 295–336.
`Zbl 787.14012` `MR 94i:11040`

[CSS 1997] Colliot-Thélène, Jean-Louis ; Skorobogatov, Alexei Nikolaïevitch ; Swinnerton-Dyer, Sir Peter.— Double fibres and double covers : Paucity of rational points. Acta Arith. **79** (1997), no. 2, 113–135.
`Zbl 863.14011` `MR 98a:11081`

[D 1997] Diaz, Guy.— La conjecture des quatre exponentielles et les conjectures de D. Bertrand sur la fonction modulaire. J. Théor. Nombres Bordeaux **9** (1997), no. 1, 229–245.
`MR 1 469 670`

[D 1972] Dieudonné, Jean.— *Éléments d'Analyse.* Cahiers Scientifiques, t. 1, Fasc. **28** (1972), t.2, **31** (1974), t.3, **33** (1974), t.4, **34** (1971), t.5, **38** (1975), t.6, **39** (1975) ; Gauthier-Villars.
`MR 38 #4246, 38 #4247, 42 #5266, 50 #14507, 57 #7632, 57 #7633, 58 #13103, 58 #29825a, 83d:00002, 84a:57021`

[G 1952] Gelfond, Alexandre O.— *Transcendentnye i algebraičeskie čisla.* (Russian) Gosudarstv. Izdat. Tehn.-Teor. Lit., Moscow, 1952. 224 pp.
Transcendental and algebraic numbers. Translated from the first Russian edition by Leo F. Boron, Dover Publications Inc., New York 1960. vii+190 pp.
`Zbl 090.26103` `MR 15,292e, 22 #2598`

[G-G 1993] Gordon, Daniel ; Grant, David.— Computing the Mordell-Weil rank of Jacobians of curves of genus two. Trans. Amer. Math. Soc. **337** (1993), no. 2, 807–824.
`Zbl 790.14028` `MR 93h:11057`

[Gr 1960] Grothendieck, Alexandre.— Fondements de la géométrie algébrique ; Extrait du séminaire Bourbaki 1957–62, exp. n° **195**, 12ème année, 1959/60 (Février 1960), (22 pp.) : Techniques de descente et théorèmes d'existence en géométrie algébrique, II : le théorème d'existence en théorie formelle des modules. Secrétariat Mathématique, 11, rue P. Curie, Paris 5ème.
`Zbl 234.14007` `MR 26 #3566`

[H-W 1979] Hardy, G.H. ; Wright, E.M.— *An Introduction to the Theory of Numbers.* Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979. xvi+426 pp.
`Zbl 423.10001` `MR 81i:10002`

[H 1977] Hartshorne, Robin.— *Algebraic Geometry.* Graduate Texts in Mathematics **52**, Springer-Verlag, New York-Heidelberg, 1977. xvi+496 pp. Corr. 3rd printing, 1983.
`Zbl 531.14001` `MR 57 #3116`

[HK 1993] Hirata-Kohno, Noriko.— Approximations simultanées sur les groupes algébriques commutatifs. Compos. Math. **86** (1993), no. 1, 69–96.
`Zbl 776.11038` `MR 94b:11067`

[Hu 1992] Huisman, Johan.— The underlying real algebraic structure of complex elliptic curves. Math. Ann. **294** (1992), no. 1, 19–36.
`Zbl 757.14030` `MR 93i:14029`

[Hu 1993] Huisman, Johan.— Heights on Abelian varieties ; in *Diophantine Approximation and Abelian varieties,(Soesterberg, 1992),* 51–61, Lecture Notes in Math., **1566**, Springer, Berlin, 1993.
`Zbl 811.14026` `MR 1 289 003`

[K-W 1993] Kuwata, Masato ; Wang, Lan.— Topology of rational points on isotrivial elliptic surfaces. Internat. Math. Res. Notices (1993), no. 4, 113–123.
`Zbl 804.14008` `MR 94a:11079`

[L 1966] Lang, Serge.— *Introduction to Transcendental Numbers.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1966. vi+105 pp.
`Zbl 144.04101` `MR 35 #5397`

[L 1971] Lang, Serge.— Transcendental numbers and Diophantine approximations. Bull. Amer. Math. Soc. **77** (1971), 635–677.
`Zbl 218.10053` `MR 44 #6615`

[L 1978] Lang, Serge.— *Elliptic curves : Diophantine analysis.* Grundlehren der Mathematischen Wissenschaften **231**, Springer-Verlag, Berlin-New York, 1978. xi+261 pp.
`Zbl 388.10001` `MR 81b:10009`

[L 1983] Lang, Serge.— *Fundamental of Diophantine geometry.* Springer-Verlag, New York-Berlin, 1983. xviii+370 pp.
`Zbl 528.14013` `MR 85j:11005`

[L 1991] Lang, Serge.— *Number theory III. Diophantine geometry.* Encyclopaedia of Mathematical Sciences, Gamkrelidze, R.V.(ed.) **60**, Springer-Verlag, Berlin, 1991. xiv+296 pp.
`Zbl 744.14012` `MR 93a:11048`
Survey of Diophantine Geometry. Transl. from the Russian. Corr. 2nd printing. Berlin : Springer, 1997. xi+298 pp.
`Zbl 970.22332`

[L 1993] Lang, Serge.— *Algebra.* Third edition. Reading, MA : Addison Wesley, 1993. xv+906 pp.
`Zbl 193.34701, 712.00001, 848.13001` `MR 33 #5416, 86j:00003`

[LB 1992] Lange, Herbert ; Birkenhake, Christina.— *Complex Abelian varieties.* Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], **302**, Springer-Verlag, Berlin, 1992. viii+435 pp.
`Zbl 779.14012` `MR 94j:14001`

[Mat 1995] Matiyasevich, Yuri V.— *Hilbert's tenth problem.* Translated from the 1993 Russian original by the author. Foundations of Computing Series. MIT Press, Cambridge, MA, 1993. xxiv+264 pp. (*voir* Smoryński, Craig ; book review in Bull. Amer. Math. Soc. **32** (1995), no. 1, 114–119).
`MR 94m :03002b`

[Maz 1978] Mazur, Barry.— Rational isogenies of prime degree (with an appendix by D. Goldfeld). Invent. Math. **44** (1978), no. 2, 129–162.
`Zbl 386.14009` `MR 80h:14022`

[Maz 1992] Mazur, Barry.— The topology of rational points. Experiment. Math. **1** (1992), no. 1, 35–45.
`Zbl 784.14012` `MR 93j:14020`

[Maz 1994] Mazur, Barry.— Questions of decidability and undecidability in number theory. J. Symbolic Logic **59** (1994), no. 2, 353–371.
`Zbl 814.11059` `MR 96c:03091`

[Maz 1995] Mazur, Barry.— Speculations about the topology of rational points : an up-date. *Columbia University Number Theory Seminar (New-York 1992),* Astérisque **128** (1995), 4, 165–181.
`Zbl 851.14009` `MR 96c:11068`

[NZM 1991] Niven, Ivan ; Zuckerman, Herbert S. ; Montgomery, Hugh L.— *An Introduction to the Theory of Numbers.* Fifth edition. John Wiley & Sons, Inc., New York, 1991. xiv+529 pp.
`Zbl 742.11001` `MR 91i:11001`

[Ra 1968] Ramachandra, K.— Contributions to the theory of transcendental numbers. I, II. Acta Arith. **14** (1968), 65–72, 73–88.
`Zbl 176.33101` `MR 37 #165`

[Rau 1976] Rauzy, Gérard.— *Propriétés statistiques de suites arithmétiques.* Le Mathématicien, No. **15**. Collection SUP. Presses Universitaires de France, Paris, 1976. 133 pp.
`Zbl 337.10036` `MR 53 #13152`

[R-H 1994] Ribet, Kenneth A. ; Hayes, B.— Fermat's last Theorem and modern arithmetic. American Scientist **82** (1994), 144–156.

[Ri 1994] Ribenboim, Paulo.— *Nombres premiers : mystères et records.* Mathématiques. Presses Universitaires de France, Paris, 1994. xx+279 pp.
`Zbl 842.11001` `MR 95j:11004`

[Ro 1993] Rohrlich, David.— Variation of the root number in families of elliptic curves. Compositio Math. **87** (1993), no. 2, 119–151.
`Zbl 791.11026` `MR 94d :11045`

[R 1988a] Roy, Damien.— Sur la conjecture de Schanuel pour les logarithmes de nombres algébriques. *Groupe d'Études sur les Problèmes Diophantiens 1988-1989,* Publ. Math. Univ. P. et M. Curie (Paris VI) **90**, N° 6, 12 pp.

[R 1988b] Roy, Damien.— Matrices dont les coefficients sont des formes linéaires. *Séminaire de Théorie des Nombres, Paris 1987–88,* 273–281, Prog. Math. **81**, Birkhäuser Verlag, Boston, MA, 1990.
`MR 91c:11038`

[R 1990a] Roy, Damien.— Sur une version algébrique de la notion de sous-groupe minimal relatif de $\mathbb{R}^n$. Bull. Soc. Math. Fr. **118** (1990), no. 2, 171–191.
`Zbl 729.12014` `MR 92c:11066`

[R 1990b] Roy, Damien.— Sous-groupes minimaux des groupes de Lie commutatifs réels, et applications arithmétiques. Acta Arith. **56** (1990), no. 3, 257–269.
`Zbl 672.10024, 708.11033` `MR 92f:11098`

[R 1991] Roy, Damien.— Transcendance et questions de répartition dans les groupes algébriques. *Approximations Diophantiennes et Nombres Transcendants (Luminy, 1990),* 249–274, de Gruyter, Berlin, 1992.
`Zbl 763.11031` `MR 93h:11077`

[R 1992a] Roy, Damien.— Matrices whose coefficients are linear forms in logarithms. J. Number Theory **41** (1992), no. 1, 22–47.
`Zbl 763.11030` `MR 93d:11077`

[R 1992b] Roy, Damien.— Simultaneous approximation in number fields. Invent. Math. **109** (1992), no. 3, 547–556.
`Zbl 780.11060` `MR 93f:11087`

[R 1995] Roy, Damien.— Points whose coordinates are logarithms of algebraic numbers on algebraic varieties. Acta Math. **175** (1995), no. 1, 49–73.
`Zbl 833.11031` `MR 96i:11079`

[S-S 1958] Schinzel, André ; Sierpiński, Waclaw.— Sur certaines hypothèses concernant les nombres premiers. Acta Arith. **4** (1958), 185–208 ; **5** (1958), 259 ; **7** (1961/1962), 1–8.
`Zbl 082.25802` `MR 21 #4936, 24 #A70`

[Sc 1980] Schmidt, Wolfgang M.— *Diophantine Approximation.* Lecture Notes in Math. **785**. Springer, Berlin, 1980. x+299 pp.
`Zbl 421.10019` `MR 81j:10038`

[Sch 1957] Schneider, Theodor.— *Einführung in die transzendenten Zahlen.* Die Grundlehren der Mathematischen Wissenschaften **81**, Berlin-Göttingen-Heidelberg : Springer-Verlag, 1957. v+150 pp.
Introduction aux Nombres Transcendants. Traduit de l'allemand par P. Eymard, Gauthier-Villars, Paris 1959. viii+151 pp.
`Zbl 077.04703` `MR 19,252f, 21 #5620`

[Se 1979] Serre, Jean-Pierre.— Quelques propriétés des groupes algébriques commutatifs. Soc. Math. France, Astérisque **69/70** (1979), 191–202. Deuxième édition, 1987 (appendice de [W 1979]).
`Zbl 428.10017` `MR 88i:11047`

[Se 1989] Serre, Jean-Pierre.— *Lectures on the Mordell-Weil theorem.* Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt. Aspects of Mathematics **E15**. Braunschweig Wiesbaden : Friedr. Vieweg & Sohn, 1989. x+218 pp. 3rd ed. 1997.
`Zbl 676.14005, 863.14013` `MR 90e:11086`

[Si 1949] Siegel, Carl Ludwig.— *Transcendental Numbers.* Annals of Mathematics Studies **16**, Princeton University Press, Princeton, N. J., 1949. viii+102 pp.
`Zbl 039.04402` `MR 11,330c`

[Sil 1986] Silverman, Joseph H.— *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics **106**, New York Springer-Verlag 1986. xii+400 pp. Corrected reprint, 1995.
`Zbl 585.14026` `MR 87g:11070, 95m:11054`
Advanced topics in the Arithmetic of Elliptic Curves. Graduate Texts in Mathematics **151**. Springer-Verlag, New York, 1994. xiv+525 pp.
`Zbl 950.00161` `MR 96b:11074`

[SwD 1974] Swinnerton-Dyer, H.P.F.— *Analytic theory of Abelian varieties.* London Mathematical Society Lecture Note Series, **14**. Cambridge University Press, London-New York, 1974. viii+90 pp.
`Zbl 299.14021` `MR 51 #3180`

[W 1974] Waldschmidt, Michel.— *Nombres transcendants.* Lecture Notes in Mathematics **402**. Springer-Verlag, Berlin-New York, 1974. viii+277 pp.
`Zbl 302.10030` `MR 50 #12931`

[W 1979] Waldschmidt, Michel.— *Nombres transcendants et groupes algébriques.* Appendices par Daniel Bertrand et Jean-Pierre Serre. Astérisque **69–70** , Société Mathématique de France, Paris, 1979. 218 pp. Deuxième édition 1987.
`Zbl 428.10017` `MR 82k:10041, 88i:11047`

[W 1983a] Waldschmidt, Michel.— Dépendance de logarithmes dans les groupes algébriques. In : *Approximations Diophantiennes et Nombres Transcendants (Luminy, 1982),* 289–328, Progr. Math. **31**, Birkhäuser, Boston, Mass., 1983.
`Zbl 513.14028` `MR 84k:10032`

[W 1983b] Waldschmidt, Michel.— Sous-groupes analytiques de groupes algébriques. Ann. of Math. (2) **117** (1983), no. 3, 627–657.
`Zbl 579.14039` `MR 84j:10046`

[W 1988] Waldschmidt, Michel.— On the transcendence methods of Gel'fond and Schneider in several variables. *New advances in transcendence theory* (Durham, 1986), 375–398, Cambridge Univ. Press, Cambridge-New York, 1988.
`Zbl 659.10035` `MR 90d:11089`

[W 1987] Waldschmidt, Michel.— Dependence of logarithms of algebraic points. *Number theory, Vol. II (Budapest, 1987),* 1013–1035, Colloq. Math. Soc. János Bolyai **51**, North-Holland, Amsterdam, 1990.
`Zbl 714.11043` `MR 91g:11076`

[W 1991] Waldschmidt, Michel.— Transcendental numbers and functions of several variables. In : *Advances in Number Theory (Kingston, ON, 1991),* 67–80, Oxford Sci. Publ., Oxford Univ. Press, New York, 1993.
`Zbl 791.11032` `MR 96i:11076`

[W 1994] Waldschmidt, Michel.— Densité de points rationnels sur un groupe algébrique. Experiment. Math. **3** (1994), no. 4, 329–352.
`Zbl 837.11040` `MR 96h:11071`

[W 1995] Waldschmidt, Michel.— Densité de points rationnels sur un groupe algébrique. Errata. Experiment. Math. **4** (1995), no. 3, 255.
`Zbl 853.11057` `MR 97d:11112`

[W 1996] Waldschmidt, Michel.— Dependence of logarithms on commutative algebraic groups. Symposium on Diophantine Problems (Boulder, CO, 1994). Rocky Mountain J. Math. **26** (1996), no. 3, 1199–1223.
`Zbl 970.34897` `MR 97k:11111`

[W 1997] Waldschmidt, Michel.— Approximation simultanée par des produits de puissances de nombres algébriques. Acta Arith. **79** (1997), no. 2, 137–162.
`Zbl 863.11044` `MR 98b:11083`

[W 1998] Waldschmidt, Michel.— Density measure of rational points on abelian varieties. Soumis ; Institut de Mathématiques de Jussieu, Prépublication **84** (Septembre 1996).

[Wa 1994] Wang, Lan.— Rational points and canonical heights on $K3$ surfaces in $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$. *Recent developments in the inverse Galois problem (Seattle, WA, 1993),* 273–289, Contemp. Math., **186**, Amer. Math. Soc., Providence, RI, 1995.
`Zbl 849.14010` `MR 97a:14023`

[Wa 1995] Wang, Lan.— Brauer-Manin obstruction to weak approximation on abelian varieties. Israel J. Math. **94** (1996), 189–200.
`Zbl 870.14032` `MR 97e:11069`

[We 1982] Weil, André.— *Adèles and algebraic groups.* With appendices by M. Demazure and Takashi Ono. Progress in Mathematics, **23**, Birkhäuser, Boston, Mass., 1982. iii+126 pp.
`Zbl 493.14028` `MR 83m:10032`

[Wü 1989] Wüstholz, Gisbert.— Algebraische Punkte auf analytischen Untergruppen algebraischer Gruppen. Ann. of Math. (2) **129** (1989), no. 3, 501–517.
`Zbl 675.10025` `MR 90g:11101`

Index