69-70

C.

ASTÉRISQUE

1987/1979

NOMBRES TRANSCENDANTS ET GROUPES ALGÉBRIQUES

Michel WALDSCHMIDT

Complété par deux appendices
de Daniel BERTRAND et Jean-Pierre SERRE

(seconde édition)

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
Publié avec le concours du CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

TABLE DES MATIÈRES

INTRODUCTION 7

CHAPITRE 1. PRÉLIMINAIRES

§ 1.1. Nombres transcendants
a) Équations différentielles...................... 13
b) Ordre arithmétique........................... 15
c) Indépendance de logarithmes.................... 18
d) Hauteurs.................................... 19

§ 1.2. Groupes algébriques
a) Généralités 21
b) Fonctions et variétés abéliennes 22
c) Problèmes de rationalité....................... 25
d) Courbes elliptiques et extensions.............. 27
e) Dimension algébrique.......................... 28

§ 1.3. Exposant de Dirichlet généralisé
a) Introduction.................................. 28
b) Généralités sur $\mu(\Gamma, V)$ 29
c) Lien avec l'hypothèse d'un théorème de W.M. Schmidt.............................. 31
d) Sous-groupes de $\mathbb{R}^n$............................ 34
e) Hypersurfaces algébriques de $\mathbb{C}^n$................ 38

CHAPITRE 2. MATRICES ET NOMBRES TRANSCENDANTS

§ 2.1. Généralités
a) Sous-groupes à 1 paramètre de $GL_m(\mathbb{C})$......... 40
b) Homomorphismes analytiques de $\mathbb{C}^n$ dans $GL_m(\mathbb{C})$. 41

§ 2.2. Sous-groupes à un paramètre normalisés 42

§ 2.3. Sous-groupes à un paramètre sans normalisation
a) Points algébriques du graphe................... 44
b) Indépendance linéaire de points algébriques..... 45
c) Dimension algébrique.......................... 45

§ 2.4. Sous-groupes commutatifs à plusieurs paramètres normalisés
a) Transcendance des coordonnées de points algébriques 47
b) Indépendance linéaire de points algébriques 48
c) Dimension algébrique 51

§ 2.5. Homomorphismes analytiques de $\mathbb{C}^n$ dans $GL_m(\mathbb{C})$
a) Points algébriques du graphe 55
b) Dimension algébrique 57

CHAPITRE 3. SOUS-GROUPES A UN PARAMÈTRE NORMALISÉS

§ 3.1. Enoncés des principaux résultats 59

§ 3.2. Application aux groupes algébriques de dimension 2.
a) Variété abélienne simple de dimension 2 61
b) Produit de deux courbes elliptiques 62
c) Extension d'une courbe elliptique par le groupe additif 64
d) Produit d'une courbe elliptique par le groupe multiplicatif 65
e) Extension non triviale d'une courbe elliptique par le groupe multiplicatif 66

§ 3.3. Intégrales elliptiques
a) Formes differentielles sur une courbe elliptique 68
b) Intégrales elliptiques de première ou deuxième espèce 69
c) Périodes de certaines intégrales elliptiques de troisième espèce 71

§ 3.4. Démonstration du théorème 3.1.1. 73

§ 3.5. Indépendance linéaire et algébrique de périodes et quasi-périodes 73

CHAPITRE 4. SOUS-GROUPES A UN PARAMÈTRE SANS NORMALISATION

§ 4.1. Points algébriques du graphe 76

§ 4.2. Dimension algébrique 77

§ 4.3 Démonstrations 82

CHAPITRE 5. SOUS-GROUPES NORMALISÉS A PLUSIEURS PARAMÈTRES

§ 5.1. Le critère de transcendance de Bombieri 84

§ 5.2. Applications aux homorphismes analytiques normalisés de de $\mathbb{C}^n$ dans $G_{\mathbb{C}}$
a) Le théorème principal 85
b) Variétés abéliennes 86
c) Produit d'une variété abéliennes par le groupe additif 86
d) Extension d'une variété abélienne par le groupe additif 87
e) Produit d'une variété abélienne par le groupe multiplicatif 88
f) Extension d'une variété abélienne par le groupe multiplicatif 89
g) Application à la fonction bêta 90

§ 5.3. Généralisations du théorème de Schneider sur la fonction modulaire
a) Endomorphismes de variétés abéliennes 93
b) Transcendance de valeurs de fonctions arithmétiques automorphes 95

§ 5.4. Démonstration du théorème de Bombieri

CHAPITRE 6. VARIÉTÉS ABÉLIENNES SIMPLES DE TYPE C.M.

§ 6.1. Transcendance des coordonnées de points algébriques .. 103

§ 6.2. Indépendance linéaire de points algébriques 104

§ 6.3. Application aux homomorphismes analytiques de $\mathbb{C}^n$ dans $G_{\mathbb{C}}$.
a) Sous-groupes à 1 paramètre d'une variété abélienne simple 106
b) Cas général 107

CHAPITRE 7. LEMMES DE SCHWARZ EN PLUSIEURS VARIABLES

§ 7.1. Etude générale
a) Fonctions d'une variable 114
b) Un seul zéro d'ordre élévé 117
c) Majoration de θ_t 118
d) Majoration de θ_1 pour $S = \Gamma_N$ 119

§ 7.2. Produits cartésiens
a) Introduction.................................... 121
b) Formules d'interpolation........................ 122
c) Application aux sous-groupes de $\mathbb{C}^n$.............. 128

§ 7.3. Sous-groupes de la trace réelle de $\mathbb{C}^n$
a) Enoncés des résultats........................... 129
b) Un théorème de Masser et Moreau sur les polynômes à plusieurs variables.................. 130
c) Démonstration du théorème 7.3.4. 130

§ 7.4. La masse moyenne des zéros
a) Introduction.................................... 133
b) Fonctions sous-harmoniques...................... 136
c) Fonctions plurisousharmoniques.................. 138
d) Application aux fonctions analytiques............ 139

§ 7.5. Singularités d'hypersurfaces algébriques
a) Le théorème d'existence de Hörmander, Bombieri et Skoda.............................. 142
b) Sur les degrés d'hypersurfaces algébriques ayant des singularités données.................. 142
c) Un lemme de Schwarz pour les ensembles finis..... 144

§ 7.6. Compléments....................................... 147

CHAPITRE 8. HOMOMORPHISMES ANALYTIQUES DE $\mathbb{C}^n$ DANS $G_{\mathbb{C}}$

§ 8.1. Points algébriques du graphe 149

§ 8.2. Dimension algébrique
a) Utilisation du coefficient de densité............ 150
b) Sur une suggestion de Bombieri et Lang........... 151
c) Une autre suggestion. Lien avec un problème de Weil et Serre......................... 152

§ 8.3. Critères de transcendance
a) Enoncés des critères pour les fonctions entières.. 155
b) Le théorème de Baker par les fonctions de plusieurs variables.......................... 156
c) Enoncés des critères pour les fonctions méromorphes..................................... 157
d) Démonstration des critères....................... 159

APPENDICE I. PROBLÈMES LOCAUX, par Daniel BERTRAND

I Introduction

§ 1.1. Position du problème................................ 163
§ 1.2. Notations... 164

II Critéres de transcendance généraux

§ 2.1. Le cas normalisé.................................... 165
§ 2.2. Le cas non normalisé................................ 167
§ 2.3. Quelques mesures de répartition..................... 168
§ 2.4. Les lemmes de Schwarz............................... 169

III Le cas d'une variable

§ 3.1. Les situations locales 171
§ 3.2. La situation globale normalisée..................... 172
§ 3.3. La situation globale non normalisée................. 173

IV Résultats de transcendance

§ 4.1. Préliminaires....................................... 175
§ 4.2. Sous-groupes à plusieurs paramètres normalisés...... 181
§ 4.3. Sous-groupes non normalisés......................... 183
§ 4.4. Variétés abéliennes dégénérantes.................... 184
§ 4.5. Problèmes d'indépendance linéaire................... 185

V Applications

§ 5.1. Arithmétique des corps de nombres................... 187
§ 5.2. Géométrie diophantienne............................. 188

APPENDICE II. QUELQUES PROPRIÉTÉS DES GROUPES ALGÉBRIQUES COMMUTATIFS, par Jean-Pierre SERRE

§ 1. Compactification de G
1.1. Le groupe L...................................... 191
1.2. Compactification de L............................ 192
1.3. Construction de $\bar{G}$ 192
1.4. Diviseurs et plongements projectifs de $\bar{G}$...... 192
1.5. Une propriété des endomorphismes $[n]_G$.......... 193

§ 2. Hauteurs
2.1. Rappels 195
2.2. Hauteur sur $\bar{G}$ relativement à $D_{a,b}$ 196
2.3. Hauteur sur G : cas général 197

§ 3. Application exponentielle et uniformisation
3.1. Exponentielle.................................. 198
3.2. Préliminaires : algèbre affine de L........... 199
3.3. Préliminaires : périodes........................ 199
3.4. Croissance de certaines fonctions............... 200
3.5. Applications.................................... 201

RÉFÉRENCES.. 203

INDEX... 209

INDEX DES NOTATIONS 213

ABSTRACT 217

INTRODUCTION

Les principaux résultats classiques de transcendance concernant les fonctions exponentielle et elliptiques peuvent être énoncés sous l'une des deux formes suivantes.

Soient G' et G'' deux groupes algébriques commutatifs connexes définis sur le corps $\bar{\mathbb{Q}}$ des nombres algébriques, et $\varphi : G'_{\mathbb{C}} \to G''_{\mathbb{C}}$ un homomorphisme analytique.

(1) - Si aucune puissance de φ n'est rationnelle, alors le graphe de φ ne peut contenir "beaucoup" de points algébriques (sur $\bar{\mathbb{Q}}$).

(2) - Si la dimension algébrique de φ (c'est-à-dire la dimension algébrique de l'adhérence de Zariski de l'image de φ) est suffisamment grande, alors l'image de φ ne peut contenir "beaucoup" de points algébriques.

Dans chacune de ces 2 situations, on distinguera deux cas, suivant que l'on suppose ou non que φ est "normalisé" pour avoir une application linéaire tangente à l'origine définie sur $\bar{\mathbb{Q}}$.

Illustrons ceci par l'exemple de l'exponentielle usuelle.

(1) Soit $\varphi : \mathbb{C} \to \mathbb{C}^*$ un homomorphisme analytique non constant, c'est-à-dire

$$\varphi(z) = e^{\lambda z} \quad \text{où } \lambda \in \mathbb{C} \text{ , } \lambda \neq 0 .$$

a) Si φ est normalisé, c'est-à-dire si $\lambda \in \bar{\mathbb{Q}}$, le théorème de Hermite-Lindemann s'énonce : le graphe de φ ne contient pas de point algébrique différent de $(0,1)$.
b) Si on ne suppose plus λ algébrique, le théorème de Gel'fond Schneider (méthode de Schneider) s'énonce : les nombres algébriques γ tels que $\varphi(\gamma) \in \bar{\mathbb{Q}}^*$ forment un $\mathbb{Q}$-espace vectoriel de dimension ≤ 1.

(2) Soit $\varphi : \mathbb{C} \to \mathbb{C}^* \times \mathbb{C}^*$ un homomorphisme analytique, c'est-à-dire

$$\varphi(z) = (e^{\lambda_1 z} , e^{\lambda_2 z}), \quad \text{où } (\lambda_1 , \lambda_2) \in \mathbb{C}^2.$$

On suppose que la dimension algébrique de φ est 2, c'est-à-dire que λ_1 , λ_2 sont $\mathbb{Q}$-linéairement indépendants.
a) Si φ est normalisé, c'est-à-dire si $(\lambda_1 , \lambda_2) \in \bar{\mathbb{Q}}^2$, le théorème de Gel'fond

Schneider (méthode de Gel'fond) s'énonce : l'image de φ ne contient pas de point algébrique autre que $\varphi(0)$.

b) Si on ne suppose plus λ_1 et λ_2 algébriques, le théorème des six exponentielles s'énonce : les nombres complexes dont l'image par φ appartient à $\overline{\mathbb{Q}}^* \times \overline{\mathbb{Q}}^*$ forment un $\mathbb{Q}$-espace vectoriel de dimension ≤ 2

La première formulation du théorème de Gel'fond Schneider (septième problème de Hilbert) correspond à la démonstration originale de Schneider en 1934, la deuxième à celle de Gel'fond la même année.

Soient maintenant G' et G'' deux groupes algébriques commutatifs connexes définis sur $\overline{\mathbb{Q}}$. Supposons que G' soit de dimension 1. Dans la situation (1), on considère des points $\gamma_1,\dots,\gamma_\ell$ de $G'_{\overline{\mathbb{Q}}}$, $\mathbb{Z}$-linéairement indépendants, dont les images par φ appartiennent à $G''_{\overline{\mathbb{Q}}}$, et on suppose qu'aucune puissance de φ n'est rationnelle. Dans la situation (2), on considère des points $\gamma_1,\dots,\gamma_\ell$ de $G'_{\mathbb{C}}$, $\mathbb{Z}$-linéairement indépendants, dont les images par φ sont dans $G''_{\overline{\mathbb{Q}}}$, et on suppose que la dimension algébrique de φ est ≥ 2. On obtient alors les majorations de ℓ indiquées dans le tableau suivant

dim $G' = 1$	(1) Graphe de φ	(2) Image de φ
a) φ normalisé	$\ell = 0$	$\ell = 0$
b) sans normalisation	$\ell \leq 2$	$\ell \leq 4$

Enfin, quand dim $G' = n \geq 2$, les résultats que l'on connait se déduisent (en composant avec l'exponentielle de G') de l'étude d'un homomorphisme analytique $\varphi : \mathbb{C}^n \to G''_{\mathbb{C}}$. Si φ est normalisé, et s'il existe n points $\mathbb{C}$-linéairement indépendants dans $\mathbb{C}^n$ dont les images par φ appartiennent à $G''_{\overline{\mathbb{Q}}}$, alors la dimension algébrique de φ est $\leq n$. Quand φ n'est pas normalisé, nous introduirons une hypothèse sur l'indépendance linéaire des points $\gamma \in \mathbb{C}^n$ faisant intervenir les endomorphismes de $\mathbb{C}^n$.

L'intérêt de ces énoncés réside non seulement dans leur généralité, mais surtout dans les applications nouvelles qu'ils permettent d'atteindre. Ainsi on ne connaissait jusquà présent aucun résultat général sur les intégrales elliptiques de troisième espèce (troisième problème de Schneider [S 4]) Jointe à un théorème de Lang (correspondant à l'égalité $\ell = 0$ dans la situation (2) a) du tableau ci-dessus), la description (qui m'a été fournie par Serre) des extensions d'une courbe elliptique par le groupe multiplicatif permet de combler cette lacune. De manière générale, les applications que l'on obtient concernent les fonctions elliptiques (ainsi que les fonctions sigma et zêta de Weirstrass) et les fonctions abéliennes (ou quasi-abéliennes), et, par l'intermédiaire de la formule de Chowla Selberg, les fonctions gamma et bêta.

Le premier travail sur les propriétés de transcendance des fonctions elliptiques remonte à Siegel en 1932 [Si 1], et celui sur les fonctions abéliennes à Schneider en 1940 [S 2] L'étape suivante a été franchie par Lang en 1962, où il débutait l'étude générale que nous venons d'esquisser. En particulier c'est à lui que nous devons tous les résultats ci-dessus dans le cas où φ est normalisé [L 2]. Son livre [L 2] sur les nombres transcendants a joué un rôle important dans le développement de cette théorie. Plusieurs des problèmes qui y figurent sont maintenant résolus, notamment:

-[L 2] (p.20 et 30) : représentation de l'exponentielle d'un groupe algébrique commutatif connexe par des fonctions méromorphes d'ordre fini, et étude de la hauteur sur un tel groupe algébrique (cf. Serre <u>Appendice</u> II).
-[L 2] (p. 32) : intersection d'un sous-groupe à un paramètre d'une variété abélienne avec une section hyperplane ([Ax] ; cf. [L 3] p. 654).

-[L 2] (p. 41) . La suggestion de Nagata concernant les hypersurfaces algébriques a fait l'objet d'un important mémoire de Bombieri [Bom] dont nous parlerons au § 5.1 et au § 7.5.
-[L 2] (p.54) Extension des résultats de transcendance aux variétés abéliennes définies non plus sur un corps de nombres, mais sur une extension de $\mathbb{Q}$ de type de transcendance fini (cf. Altman [Al] ; voir aussi Serre, <u>Appendice</u> II).
-[L 2] (p. 103). Les analogues p-adiques des théorèmes de Schneider sur la fonction $\wp$ ont été tous démontrés par Bertrand [Be 3] ; (voir aussi l'<u>Appendice</u> I). .

D'autres problèmes de [L 2] ont été en partie résolus, en particulier
-[L 2] (p. 29 et 41) celui de la transcendance de chacune des coordonnées d'un point de $\mathbb{C}^g$ dont l'image par une représentation normalisée $\Theta : \mathbb{C}^g \to A_{\mathbb{C}}$ de l'exponentielle d'une variété abélienne est algébrique (travaux de Masser et Lang ; cf. § 6.1),
-[L 2] (p. 54 - 55) celui de l'analogue elliptique du théorème de Lindemann Weierstrass [C 1], [C 3],
-[L 2] (p. 20, 39 et 44) et enfin celui, auquel nous accorderons un intérêt particulier, de l'utilisation des fonctions de plusieurs variables dans la théorie des nombres transcendants.

Le plan de l'ouvrage est le suivant. Dans le premier chapitre, après des préliminaires sur les théorèmes de transcendance (en une variable) et des généralités sur les groupes algébriques, nous introduisons un "coefficient de répartition" $\mu(\Gamma,V)$ d'un $\mathbb{Z}$-module Γ de type fini dans un espace vectoriel V de dimension finie sur un corps de caractéristique nulle. Ce coefficient jouera un rôle important notamment dans l'étude du lemme de Schwarz en plusieurs variables. On l'utilisera surtout aux chapitres 7 et 8.

Le deuxième chapitre consiste en une traduction, en termes de matrices, des énoncés de transcendance du § 1.1. Nous obtenons ainsi les énoncés sur les groupes linéaires dont nous aurons besoin dans la suite.

Nous étudions ensuite les sous-groupes à 1 paramètre $\varphi : \mathbb{C} \to G_{\mathbb{C}}$, en commençant par le cas normalisé (Chapitre 3), qui conduit aux applications les plus intéressantes, et en continuant par le cas général (Chapitre 4) où certains des énoncés ne semblent pas les meilleurs possibles (ne serait-ce que le théorème des six exponentielles).

Le chapitre 5 concerne les homomorphismes analytiques normalisés $\varphi : \mathbb{C}^n \to G_{\mathbb{C}}$ surtout dans la situation (2) (image de φ). La situation (1)(graphe de φ) sera reprise aux § 6.1 et 6.2.

Il reste alors à étudier les homomorphismes analytiques $\varphi : \mathbb{C}^n \to G_{\mathbb{C}}$ sans hypothèse de normalisation. Si on s'intéresse au graphe de φ (situation (1)), on peut ramener cette étude à un problème d'indépendance linéaire de points algébriques sur des variétés abéliennes ; ce problème n'est résolu que dans le cas de variétés abéliennes de type C.M. C'est le sujet du chapitre 6.

Le chapitre 7 est une étude générale du lemme de Schwarz en plusieurs variables, décrivant les méthodes dont on dispose actuellement ainsi que les résultats que l'on peut espérer. Les problèmes qui y sont soulevés devraient être importants pour le développement futur de la théorie des nombres transcendants.

Ces lemmes de Schwarz sont appliqués au chapitre 8 pour l'étude du graphe, puis de l'image d'un homomorphisme analytique $\varphi : \mathbb{C}^n \to G_{\mathbb{C}}$. Cette étude est liée à un problème de Weil et Serre - qui est la motivation initiale du présent mémoire - sur certains types de caractères du groupe des classes d'idèles d'un corps de nombres algébriques.

Le premier appendice, par Daniel Bertrand, présente une étude du cas p-adique et de ses différentes applications. Le deuxième appendice, par Jean-Pierre Serre, fournit une démonstration de plusieurs propriétés des groupes algébriques commutatifs qui interviennent dans les démonstrations de transcendance.

Ce texte est une version développée de leçons données au Collège de France (cours Peccot) en 1977. Il a été enrichi de nombreuses suggestions et remarques-notamment

de D. Bertrand, D.W. Masser et J.P. Serre. En particulier, l'Appendice II écrit par Serre, et les exemples qu'il m'a communiqués (notamment la description des extensions d'une courbe elliptique par le groupe multiplicatif) sont la source de résultats nouveaux dans les chapitres 3, 4 et 5. J'ai bénéficié également, grâce à K. Ramachandra, d'un séjour très utile au Tata Institute fin 1976, où j'ai exposé une version préliminaire de ce travail.

J'exprime aussi ma reconnaissance à Madame Goyvaerts et à Madame Renault qui ont réalisé la frappe de ce texte.

CHAPITRE 1

PRÉLIMINAIRES.

Nous commençons par des résultats classiques sur les nombres transcendants (§ 1.1), puis sur les groupes algébriques (§ 1.2). Nous étudions ensuite une condition de répartition d'un module dans un espace vectoriel (§ 1.3) qui fera intervenir, outre de l'algèbre linéaire élémentaire, un théorème de W.M. Schmidt sur les approximations diophantiennes.

§ 1.1 - Nombres transcendants.

Nous présentons d'abord deux critères de transcendance selon lesquels des fonctions méromorphes dans $\mathbb{C}$ d'ordre fini qui ont beaucoup de points algébriques communs sont algébriquement dépendantes. Le premier (méthode de Gel'fond) suppose que les fonctions satisfont des équations différentielles, le second (méthode de Schneider) sera utile quand les fonctions satisfont un théorème d'addition algébrique. Tous deux ont leur source dans un travail important de Th. Schneider [S 3]. Nous énonçons ensuite un théorème de Baker sur l'indépendance linéaire de logarithmes de nombres algébriques. Nous verrons enfin quelques propriétés des hauteurs.

a) Equations différentielles.

Pour $z = (z_1, \dots, z_n) \in \mathbb{C}^n$, on pose $|z| = \left(\sum_{i=1}^{n} |z_i|^2\right)^{1/2}$; si g est une fonction entière dans $\mathbb{C}^n$, on pose, pour $R > 0$,

$$|g|_R = \sup_{|z|=R} |g(z)| .$$

Nous dirons qu'une fonction f méromorphe dans $\mathbb{C}^n$ est d'ordre strict inférieur ou égal à ρ s'il existe deux fonctions entières g_1, g_2 telles que $f = g_1/g_2$, et deux nombres positifs C_1, C_2 tels que

$$\log |g_j|_R \leq C_j R^{\rho} \qquad \text{pour tout } R \geq 1 \text{ et } j = 1,2 .$$

On vérifie que si f est entière dans $\mathbb{C}^n$, alors f est d'ordre strict $\leq \rho$ si et seulement si il existe $C > 0$ tel que

$$\log |f|_R \leq C R^{\rho} \qquad \text{pour tout } R \geq 1$$

(cf. par exemple [Le 2] 7.4.10 et 7.4.11, et [Wa 3] II lemme 3.6). Cette définition de l'ordre strict diffère d'un epsilon de la définition de l'ordre usuel ; cf. [B-L]. Elle correspond à la notion d'ordre $\leq \rho$ et de type fini (cf [Le 2] Chap. IV).

Le théorème suivant, qui concerne les fonctions méromorphes d'une variable, est connu sous le nom de critère de Schneider-Lang (cf. [S 4] th. 12, 13 ; [L 2] Chap. III, § 1, th. 1 ; [Wa 2] th. 3.3.1).

THÉORÈME 1.1.1 - Soient K un corps de nombres, et $f_1, \dots, f_h$ des fonctions méromorphes dans $\mathbb{C}$. On suppose que f_1, f_2 sont algébriquement indépendantes sur $\mathbb{Q}$, et sont d'ordre strict $\leq \rho_1, \rho_2$ respectivement. On suppose de plus que la dérivation $\frac{d}{dz}$ laisse stable l'algèbre $K[f_1, \dots, f_h]$.

Alors l'ensemble des nombres complexes w, qui ne sont pas pôles de $f_1, \dots, f_h$, et qui sont tels que

$$f_j(w) \in K \quad \text{pour} \quad 1 \leq j \leq h$$

est fini et a au plus $(\rho_1 + \rho_2)[K : \mathbb{Q}]$ éléments.

Nous démontrerons au chapitre 5 la généralisation à plusieurs variables de ce résultat, due à Bombieri. Nous verrons d'autre part au chapitre 3 que l'ensemble des w pourrait être infini si la dérivation laissait stable seulement le corps $K(f_1, \dots, f_h)$, ou encore si on n'excluait pas les pôles (cf § 3.2.e)

Pour $f_1(z) = z$ et $f_2(z) = e^z$, on déduit de 1.1.1 le théorème de Hermite-Lindemann :

COROLLAIRE 1.1.2 - Si α est un nombre algébrique non nul, le nombre e^{α} est transcendant.

Pour $f_1(z) = e^z$, $f_2(z) = e^{\beta z}$, on obtient le théorème de Gel'fond-Schneider :

COROLLAIRE 1.1.3 - Soient α et β deux nombres algébriques, $\alpha \neq 0$, $\beta \notin \mathbb{Q}$. Soit $\log \alpha$ une détermination non nulle du logarithme de α. Alors le nombre

$$\alpha^{\beta} = \exp(\beta \log \alpha)$$

est transcendant.

Nous verrons d'autres applications du théorème 1.1.1 au chapitre 3, notamment aux fonctions elliptiques.

En vue de la démonstration du théorème de Bombieri (Chap. 5), nous donnons ici le lemme technique que l'on utilise pour démontrer le théorème 1.1.1.

LEMME 1.1.4 - Soient $\mathcal{U}$ un ouvert de $\mathbb{C}$, et $f_1, \dots, f_h$ des fonctions analytiques dans $\mathcal{U}$. Il existe un entier $C > 0$ ayant la propriété suivante :

Soient K un corps de nombres, $L_1, \dots, L_h$ des entiers positifs ou nuls, et t un entier positif. On suppose que la dérivation $\frac{d}{dz}$ laisse stable l'algèbre $K[f_1, \dots, f_h]$.

Alors il existe un polynôme $P \in K[X_1, \dots, X_h]$ tel que

a) $$\frac{d^t}{dz^t} f_1^{L_1} \dots f_h^{L_h} = P(f_1, \dots, f_h).$$

b) Pour $1 \leq j \leq h$,

$$\deg_{X_j} P \leq L_j + Ct.$$

c) Les coefficients du polynôme

$$C^t P$$

sont des entiers algébriques de K, dont les conjugués sont en valeur absolue majorés par

$$C^{2t}(L_1 + \dots + L_h + t)^t.$$

Ce lemme résulte des arguments de la démonstration de [L 2] Chap. III, § 2, lemme 1, [Bom] lemme 1 et [Wa 2] lemme 3.3.2.

b) Ordre arithmétique

Quand α est un nombre algébrique dont le polynôme minimal sur $\mathbb{Z}$ est

$$a_0 X^d + a_1 X^{d-1} + \dots + a_d,$$

le nombre

$$H(\alpha) = \max_{0 \leq j \leq d} |a_j|$$

est appelée "hauteur usuelle" de α. (Nous verrons plus loin d'autres notions de hauteur.)

Pour des fonctions satisfaisant des équations différentielles, le critère de transcendance 1.1.1 a une forme agréable, car il n'y a pas d'hypothèse technique, grâce au lemme 1.1.4. Quand il n'y a pas d'équation différentielle, pour obtenir un critère analogue et général, on doit introduire des conditions sur les hauteurs des nombres que l'on considère. Nous le ferons en utilisant la notion d'ordre arithmétique de Lang [L 2] Chap.II, § 2 (légèrement modifié), que nous donnons tout de suite pour plusieurs variables.

DÉFINITION - Soient $\rho_1, \ldots, \rho_d$ des nombres réels positifs, $f = (f_1, \ldots, f_d)$ une application méromorphe de $\mathbf{C}^n$ dans $\mathbf{C}^d$, et Γ un sous-groupe de $\mathbf{C}^n$ de type fini et de rang ℓ sur $\mathbf{Z}$. On dit que f est <u>d'ordre arithmétique inférieur ou égal à</u> $(\rho_1, \ldots, \rho_d)$ <u>sur</u> Γ s'il existe

- des fonctions entières $g_1, \ldots, g_d$, d'ordre strict inférieur ou égal à $\rho_1, \ldots, \rho_d$ respectivement, telles que, pour $1 \leq j \leq d$, la fonction $g_j f_j$ soit entière d'ordre strict $\leq \rho_j$;
- un corps de nombres K ;
- une base $\gamma_1, \ldots, \gamma_\ell$ de Γ sur $\mathbf{Z}$;
- des nombres réels positifs c_1, c_2, c_3, c_4 ;
- et, pour tout entier $N \geq c_1$, un sous-ensemble S_N de l'ensemble

$$\Gamma_N = \{h_1\gamma_1 + \ldots + h_\ell\gamma_\ell \; ; \; (h_1, \ldots, h_\ell) \in \mathbf{Z}^\ell, \; |h_j| \leq N\},$$

avec

$$\operatorname{Card} S_N \geq c_2 N^\ell \qquad \text{pour } N \geq c_1,$$

et vérifiant les deux conditions suivantes

O.A.1. Pour $N \geq c_1$ et $\sigma \in S_N$, on a $f(\sigma) \in K^d$ et

$$\log H(f_j(\sigma)) \leq c_3 N^{\rho_j}, \quad (1 \leq j \leq d).$$

O.A.2. Pour $N \geq c_1$ et $1 \leq j \leq d$, la fonction g_j n'a pas de zéro dans S_N, et

$$\log \min_{\sigma \in S_N} |g_j(\sigma)| \geq -c_4 N^{\rho_j}.$$

En particulier f_j est d'ordre strict $\leq \rho_j$. D'autre part si f_j est entière la condition O.A.2. est automatiquement satisfaite avec la fonction g_j identique à 1.

Le critère de transcendance en 1 variable est le suivant

THÉORÈME 1.1.5 - <u>Soient</u> $f_1, \ldots, f_d$ <u>des fonctions méromorphes dans</u> $\mathbf{C}$, <u>algébriquement indépendantes sur</u> $\mathbf{Q}$. <u>Soit</u> Γ <u>un sous-groupe de</u> $\mathbf{C}$, <u>de rang</u> ℓ <u>sur</u> $\mathbf{Z}$; <u>on suppose que</u> $(f_1, \ldots, f_d)$ <u>est d'ordre arithmétique</u> $\leq (\rho_1, \ldots, \rho_d)$ <u>sur</u> Γ. <u>Alors</u>

$$\ell \leq \frac{\rho_1 + \ldots + \rho_d}{d - 1}.$$

(voir [S 3], [L 2] Chap.II, § 2, Th. 2, [Ra] Th. 1, [Wa 2] Th. 2.2.1 et Th. 4.5.1) Nous en démontrerons des généralisations à plusieurs variables au Chapitre 8.

On doit à K. Ramachandra la remarque suivante [Ra] (voir aussi [Wa 2] exercices 2.2.d et 4.5.a).

REMARQUE 1.1.6 - Sous les hypothèses du théorème 1.1.5, on suppose que $f_1, \ldots, f_d$ ont une période commune $\omega \neq 0$. Alors

$$\ell \leq \frac{\rho_1 + \ldots + \rho_d - 1}{d - 1}.$$

L'hypothèse O.A.1. ne peut pas être supprimée dans le théorème 1.1.5. En effet, il existe des fonctions entières, transcendantes, d'ordre $\leq \epsilon$ pour tout $\epsilon > 0$, telles que, pour tout $\alpha \in \overline{\mathbf{Q}}$, on ait $f(\alpha) \in \mathbf{Q}(\alpha)$ et même

$$\frac{d^t}{dz^t} f(\alpha) \in \mathbf{Q}(\alpha) \qquad \text{pour tout entier } t \geq 0.$$

Le théorème 1.1.5 généralise le théorème 1.1.3 de Gel'fond-Schneider (correspondant à $f_1(z) = z$, $f_2(z) = \alpha^z = \exp(z \log\alpha)$; pour la vérification de O.A.1, voir les remarques ci-dessous sur les hauteurs et la taille). D'autre part, quand on choisit $f_1(z) = e^{x_1 z}$, $f_2(z) = e^{x_2 z}$, ou bien $f_1(z) = e^{y_1 z}$, $f_2(z) = e^{y_2 z}$, $f_3(z) = e^{y_3 z}$, on obtient le théorème des six exponentielles, dû à Siegel, Lang et Ramachandra :

COROLLAIRE 1.1.7 - <u>Soient</u> x_1, x_2 <u>deux nombres complexes</u> $\mathbf{Q}$<u>-linéairement indépendants. Soient</u> y_1, y_2, y_3 <u>trois nombres complexes</u> $\mathbf{Q}$<u>-linéairement indépendants. L'un des six nombres</u>

$$e^{x_i y_j}, \qquad (i = 1,2 \; ; \; j = 1,2,3)$$

<u>est transcendant.</u>

Le <u>problème des quatre exponentielles</u> consiste à montrer que l'un des quatre nombres

$$e^{x_i y_j}, \qquad (i = 1,2 \; ; \; j = 1,2)$$

est transcendant (cf. [S 4] problème 1, [L 2] conjecture p. 11).

<u>Remarque sur les pôles.</u> Quand nous utiliserons la notion d'ordre arithmétique pour des fonctions qui ne sont pas entières, les fonctions g_j seront toujours composées d'une fonction thêta et d'une application linéaire (cf. lemme 1.2.2), et les sous-

ensembles S_N seront le plus souvent de la forme $T \cap \Gamma_N$, où T est un sous-ensemble de Γ satisfaisant les conditions suivantes.

LEMME 1.1.8 - Soient Γ un sous-groupe de type fini de $\mathbf{C}^n$, de rang ℓ sur $\mathbf{Z}$, et T un sous-ensemble de Γ. Les deux conditions suivantes sont équivalentes :

i) Il existe un ensemble fini F tel que Γ soit l'ensemble des $t + \gamma$, $t \in T$, $\gamma \in F$.

ii) Soit $\gamma_1, \ldots, \gamma_\ell$ une base de Γ sur $\mathbf{Z}$. Il existe un entier $c_5 \geqq 1$ tel que tout cube dans l'espace $\mathbf{R}^\ell$ de côté $\geqq c_5$ contienne un point $(h_1, \ldots, h_\ell) \in \mathbf{Z}^\ell$ vérifiant

$$h_1\gamma_1 + \ldots + h_\ell\gamma_\ell \in T .$$

Démonstration.

Pour $\gamma \in \Gamma$, $\gamma = h_1\gamma_1 + \ldots + h_\ell\gamma_\ell$, posons $\|\gamma\| = \max_{1 \leqq j \leqq \ell} |h_j|$. Si (i) est vrai, on prend $c_5 = 1 + 2 \max_{\gamma \in F} \|\gamma\|$. Si (ii) est vrai, on prend pour F l'ensemble des $\gamma \in \Gamma$ avec $\|\gamma\| \leqq c_5/2$.

On déduit immédiatement de (ii) la condition

$$\mathrm{Card}(T \cap \Gamma_N) \geqq c_2 N^\ell \qquad \text{pour } N \geqq c_1$$

requise dans la définition de l'ordre arithmétique.

c) Indépendance de logarithmes.

Le théorème de Hermite-Lindemann 1.1.2 montre que, si $\log\alpha$ est un logarithme non nul d'un nombre algébrique $\alpha \neq 0$, alors $\log\alpha$ est transcendant. Le théorème de Gel'fond-Schneider 1.1.3 exprime que, si $\log\alpha_1$, $\log\alpha_2$ sont deux logarithmes $\mathbf{Q}$-linéairement indépendants de nombres algébriques, alors ils sont aussi $\overline{\mathbf{Q}}$-linéairement indépendants. Gel'fond avait conjecturé un énoncé analogue pour plusieurs logarithmes, et avait montré l'importance fondamentale, pour plusieurs problèmes de théorie des nombres, qu'auraient des minorations non triviales des formes linéaires de n logarithmes de nombres algébriques (cf. [G] p. 126 et 177 notamment). Ce programme a été accompli par Baker, dont nous utiliserons le théorème sous la forme suivante [B] (th. 2.1)

THÉORÈME 1.1.9 - Soient $\alpha_1, \ldots, \alpha_n$ des nombres algébriques non nuls. Pour $1 \leqq j \leqq n$, soit $\log\alpha_j$ une détermination quelconque du logarithme de α_j. On

suppose que les nombres $\log\alpha_1, \ldots, \log\alpha_n$ sont $\mathbf{Q}$-linéairement indépendants. Alors les nombres

$$1, \log\alpha_1, \ldots, \log\alpha_n$$

sont $\overline{\mathbf{Q}}$-linéairement indépendants.

On conjecture en fait que les nombres $\log\alpha_1, \ldots, \log\alpha_n$ sont algébriquement indépendants. Plus généralement, la conjecture suivante [L 2] (p. 30-31) est réputée contenir toutes les conjectures raisonnables que l'on peut énoncer sur la transcendance et l'indépendance algébrique de nombres liés à la fonction exponentielle.

CONJECTURE DE SCHANUEL. 1.1.10 - Soient $x_1, \ldots, x_n$ des nombres complexes $\mathbf{Q}$-linéairement indépendants. Alors le degré de transcendance sur $\mathbf{Q}$ du corps

$$\mathbf{Q}(x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n})$$

est supérieur ou égal à n.

Les résultats les plus remarquables obtenus récemment dans cette direction sont dus à G.V. Chudnovsky [C 1], [C 3].

d) Hauteurs.

Soit K un corps de nombres. Notons $\{v\}$ l'ensemble des valeurs absolues de K, normalisées de telle façon que l'on ait, pour $x \in \mathbf{Q}$,

$$|x|_v = x \quad \text{si } v \text{ est archimédienne et } x > 0 ,$$

$$|p|_v = 1/p \quad \text{si } v \text{ prolonge la valeur absolue } p\text{-adique}.$$

Désignons par N_v le degré local en v. La formule du produit s'écrit

$$\prod_{\{v\}} |\alpha|_v^{N_v} = 1 \qquad \text{si } \alpha \in K , \alpha \neq 0 .$$

Si $P \in \mathbf{P}_\nu(K)$ a des coordonnées projectives $(x_o, \ldots, x_\nu)$, on définit la hauteur logarithmique absolue de P par

$$h(P) = \frac{1}{[K:\mathbf{Q}]} \sum_{\{v\}} N_v \log \max_{0 \leqq j \leqq \nu} |x_j|_v ,$$

qui ne dépend ni des coordonnées (x_j) de P, ni du corps de nombres K les contenant (cf. [L 1]).

Soit α un élément non nul de K ; on note $h(\alpha)$ la hauteur logarithmique absolue du point $P = (1,\alpha) \in \mathbf{P}_2(K)$.

Soit $\operatorname{den}\alpha$ le générateur positif de l'idéal des $m \in \mathbf{Z}$ tels que $m\alpha$ soit entier algébrique. D'autre part soit $|\overline{\alpha}|$ le maximum des valeurs absolues des conjugués de α. On définit la "taille" $s(\alpha)$ de α par

$$s(\alpha) = \log \max \{\operatorname{den}\alpha \, , \, |\overline{\alpha}|\} .$$

Si $d = [\mathbf{Q}(\alpha):\mathbf{Q}]$, on a

$$(1.1.11) \qquad s(\alpha) \leq d\,h(\alpha) .$$

Démonstration.

Comme $|\overline{\alpha}|$ est égal au maximum des $|\alpha|_v$ pour toutes les valeurs absolues archimédiennes v, on a

$$\log|\overline{\alpha}| \leq \sum_v \max\{\log|\alpha|_v \, , \, 0\}$$

Soit v une valeur absolue ultramétrique prolongeant la valeur absolue p-adique Posons

$$m_v = \frac{N_v}{\log p} \max\{\log|\alpha|_v \, , \, 0\}$$

Comme le groupe des valeurs de $\mathbf{Q}_p$ est $\mathbf{Z}$, m_v est un entier positif, et le nombre

$$\prod_p \prod_{v|p} p^{m_v}$$

est un multiple du dénominateur de α. D'où

$$\log \operatorname{den}\alpha \leq \sum_v N_v \max\{\log|\alpha|_v \, , \, 0\} ,$$

ce qui démontre (1.1.11).

On peut montrer d'autre part que $h(\alpha) \leq s(\alpha)$, et que la hauteur usuelle $H(\alpha)$ vérifie

$$d\,h(\alpha) - \log d \leq \log H(\alpha) \leq d\,h(\alpha) + d \log 2$$

Nous travaillerons toujours avec un degré borné. Dans la définition de l'ordre arithmétique, on peut donc remplacer $\log H(\alpha)$ par $h(\alpha)$ ou $s(\alpha)$. Nous démontrerons les critères avec $s(\alpha)$, et nous utiliserons $h(\alpha)$ pour en déduire les corollaires (cf. 1.1.11).

Signalons le fait que dans les problèmes de transcendance où le degré n'est pas borné, la notion de hauteur la plus commode est $h(\alpha)$, grâce à sa relation avec

la "mesure de Mahler" de α définie de la manière suivante : soit

$$f(X) = a_0 X^d + \dots + a_d = a_0 \prod_{j=1}^{d} (X - \alpha_j)$$

le polynôme minimal de α sur $\mathbf{Z}$. La formule de Jensen entraîne (cf. [Mah 1])

$$|a_0| \prod_{j=1}^{d} \max(1, |\alpha_j|) = \exp\left(\int_0^1 \log|f(e^{2i\pi t})|\,dt \right) ;$$

cette valeur commune est notée $M(\alpha)$; elle est liée à $h(\alpha)$ par l'égalité suivante [Be 4] (lemme 11) :

$$h(\alpha) = \frac{1}{d} \log M(\alpha) .$$

Pour terminer voici un résultat sur les hauteurs de polynômes, dû à Popken, Koksma (cf. [S 4] lemme 16), Gel'fond ([G] chap. III § 4, lemme 2) et Mahler [Mah 1] (cf. [Wa 2] p. 129), et qui nous sera utile au § 7.3.

La hauteur $H(P)$ d'un polynôme $P \in \mathbf{C}[X_1, \dots, X_n]$ est le maximum des valeurs absolues des coefficients de P.

LEMME 1.1.12 - Soient $P_1, \dots, P_m$ des polynômes de $\mathbf{C}[X_1, \dots, X_n]$, et soit d le degré de $P_1 \dots P_m$. Alors

$$H(P_1 \dots P_m) \geq e^{-nd} H(P_1) \dots H(P_m) .$$

§ 1.2 - Groupes algébriques.

Les variétés algébriques que l'on considérera seront définies sur un corps K de caractéristique 0, le plus souvent plongé dans $\mathbf{C}$.

a) Généralités.

Un groupe algébrique est une variété algébrique G munie d'une structure de groupe de telle manière que l'application

$$\begin{aligned} G \times G &\to G \\ (x,y) &\to xy^{-1} \end{aligned}$$

soit régulière (i.e. soit un "morphisme"). La variété sous-jacente à G est alors non singulière ("lisse"). On supposera généralement que G est connexe, c'est-à-dire que la variété sous-jacente à G est irréductible.

Exemple 1. La droite affine, munie de l'addition : c'est le groupe additif G_a .

Exemple 2. La droite affine privée de l'origine, munie de la multiplication : c'est le groupe multiplicatif G_m .

Exemple 3. Dans l'espace M_m des matrices carrées $m \times m$, l'ouvert GL_m muni de la multiplication : c'est le groupe linéaire général de degré m .

Un groupe algébrique est appelé linéaire si la variété algébrique G est affine, et il est appelé variété abélienne si la variété sous-jacente est projective et irréductible. Un groupe algébrique est linéaire si et seulement si il est isomorphe à un sous-groupe algébrique d'un groupe linéaire GL_m .

Le théorème suivant est dû à Chevalley [Sha] (Chap.III, § 3.3), [Ba 1] (Th. 3.2 p. 97), [Bor] (Th. 10.6, p. 244).

THÉORÈME 1.2.1 (Chevalley) - Soit G un groupe algébrique connexe. Le groupe G possède un sous-groupe linéaire connexe maximal L , et le quotient G/L est une variété abélienne.

Soit K un sous-corps de $\mathbf{C}$, et soit G un groupe algébrique sur K . On note T_G son algèbre de Lie, identifiée à son espace tangent à l'élément neutre, et G_K le groupe des points de G qui sont rationnels sur K . Le groupe $G_{\mathbf{C}}$ des points complexes de G est un groupe de Lie complexe d'algèbre de Lie $T_G(\mathbf{C}) = \mathbf{C} \otimes_K T_G$; on note $\exp : T_G(\mathbf{C}) \to G_{\mathbf{C}}$ son application exponentielle (Cf. Bourbaki, Groupes et Algèbres de Lie, Chap. III). Si le groupe algébrique G est connexe, le groupe de Lie $G_{\mathbf{C}}$ est aussi connexe.

Soit $\varphi : \mathbf{C}^n \to G_{\mathbf{C}}$ un homomorphisme analytique ; soit $\mathcal{L} = \mathrm{Lie}\,\varphi : \mathbf{C}^n \to T_G(\mathbf{C})$ l'application linéaire tangente à φ à l'origine ; alors $\varphi = \exp \circ \mathcal{L}$. Comme $\mathbf{C}^n$ est commutatif, l'adhérence de Zariski de $\varphi(\mathbf{C}^n)$ dans $G_{\mathbf{C}}$ est un groupe algébrique commutatif connexe.

Pour $n = 1$, si $\mathcal{L} : \mathbf{C} \to T_G(\mathbf{C})$ est une application linéaire, alors $\varphi = \exp \circ \mathcal{L}$ est un homomorphisme analytique de $\mathbf{C}$ dans $G_{\mathbf{C}}$ appelé sous-groupe à un paramètre de G si $\mathcal{L} \neq 0$.

Pour $n \geq 1$, on appellera sous-groupe (commutatif) à n paramètres de G tout homomorphisme analytique $\varphi : \mathbf{C}^n \to G_{\mathbf{C}}$ tel que l'application $\mathrm{Lie}\,\varphi : \mathbf{C}^n \to T_G(\mathbf{C})$ soit injective. Lorsque G est commutatif, si $\mathcal{L} : \mathbf{C}^n \to T_G(\mathbf{C})$ est une application linéaire, alors $\exp \circ \mathcal{L}$ est un homomorphisme analytique de $\mathbf{C}^n$ dans $G_{\mathbf{C}}$.

b) Fonctions et variétés abéliennes.

Soit Ω un réseau de l'espace $V = \mathbf{C}^g$, c'est-à-dire un sous-groupe discret de V de rang $2g$ sur $\mathbf{Z}$. Les quatre conditions suivantes sont équivalentes

(i) Le groupe quotient $\mathbf{C}^g/\Omega$ peut être plongé analytiquement dans un espace projectif $\mathbf{P}_\nu(\mathbf{C})$.

(ii) Il existe une forme de Riemann non dégénérée E sur V , relative à Ω , c'est-à-dire une forme bilinéaire alternée $E : V \times V \to \mathbf{R}$ qui prend ses valeurs dans $\mathbf{Z}$ sur $\Omega \times \Omega$ et telle que la forme $(x,y) \mapsto E(ix,y)$ soit symétrique, positive et non dégénérée.

(iii) Il existe une base de V telle que le réseau Ω ait une base sur $\mathbf{Z}$ formée de $2g$ vecteurs $\omega_1, \dots, \omega_{2g}$ dont les coordonnées soient les colonnes de la matrice

$$\begin{pmatrix} e_1^{-1} & 0 & 0 & \dots & 0 & \tau_{1,1} & \tau_{1,2} & \dots & \tau_{1,g} \\ 0 & e_2^{-1} & 0 & & 0 & \tau_{2,1} & \tau_{2,2} & \dots & \tau_{2,g} \\ 0 & 0 & e_3^{-1} & & 0 & \tau_{3,1} & \tau_{3,2} & \dots & \tau_{3,g} \\ & & & & & & & & \\ 0 & 0 & 0 & & e_g^{-1} & \tau_{g,1} & \tau_{g,2} & \dots & \tau_{g,g} \end{pmatrix}$$

où $e_1, \dots, e_g$ sont des entiers positifs, et la matrice $T = (\tau_{h,k})$ vérifie les conditions de Riemann :

T est symétrique : $\tau_{h,k} = \tau_{k,h}$;

si on décompose $T = T' + iT''$ en partie réelle et imaginaire, la matrice réelle symétrique T'' est positive et non dégénérée.

(iv) Il existe g fonctions méromorphes sur $\mathbf{C}^g$ algébriquement indépendantes, et périodiques par rapport à Ω .

Sous la condition (iv), le corps $\mathcal{F}_{\mathbf{C}}$ des fonctions méromorphes sur $\mathbf{C}^g$, périodiques par rapport à Ω , est une extension de type fini de $\mathbf{C}$, de degré de transcendance g . C'est le corps des fonctions abéliennes sur $\mathbf{C}^g$ par rapport à Ω .

La condition (i) implique que l'image de $\mathbf{C}^g/\Omega$ est une sous-variété algébrique fermée de l'espace projectif (théorème de Chow ; cf. par exemple [Sha] Chap. VIII, § 3, Th. 3). C'est une variété abélienne, et le corps des fonctions rationnelles sur cette variété est $\mathcal{F}_{\mathbf{C}}$.

Inversement, soit A une variété abélienne définie sur $\mathbf{C}$, et soit X un plongement de A dans un espace projectif $\mathbf{P}_\nu$. Soit $(t_1, \dots, t_g)$ une base sur $\mathbf{C}$ de l'espace tangent $T_A(\mathbf{C})$ à l'origine de la variété ; on note $j : \mathbf{C}^g \to T_A(\mathbf{C})$

l'isomorphe associé :

$$j(z_1, \dots, z_g) = z_1 t_1 + \dots + z_g t_g .$$

Alors l'application

$$\Theta = X \circ \exp \circ j : \mathbf{C}^g \to \mathbf{P}_\nu(\mathbf{C})$$

est un homomorphisme analytique, son noyau Ω est un réseau de $\mathbf{C}^g$, et Θ induit un isomorphisme entre $\mathbf{C}^g/\Omega$ et $A_{\mathbf{C}}$. Nous dirons que Θ est un homomorphisme thêta.

DÉFINITION - Soit Ω un réseau de $\mathbf{C}^g$. On appelle fonction thêta relative à Ω toute fonction θ entière dans $\mathbf{C}^g$ pour laquelle il existe deux applications $L : \mathbf{C}^g \times \Omega \to \mathbf{C}$ et $J : \Omega \to \mathbf{C}$, avec

$$\theta(z+\omega) = \theta(z) \exp\{2i\pi[L(z,\omega) + J(\omega)]\} , \quad (z \in \mathbf{C}^g , \omega \in \Omega) ,$$

et où l'application L est $\mathbf{C}$-linéaire en z. (Cf. [L4], [S.D], [We 2]).

Quitte à changer de coordonnées, on supposera que l'image de A dans $\mathbf{P}_\nu$ n'est pas contenue dans l'hyperplan $X_0 = 0$. Soit D le diviseur de A intersection de A avec cet hyperplan ; son image réciproque sur $\mathbf{C}^g$ est le diviseur d'une fonction thêta θ_0 (cf. [We 2] Chap. VI, n° 5, Th. 1). Pour $1 \leq i \leq \nu$, soit θ_i la fonction thêta obtenue en multipliant θ_0 par la fonction méromorphe déduite de X_i/X_0 ; θ_i vérifie la même formule de transformation que θ_0. Pour tout $z \in \mathbf{C}^g$, $(\theta_0(z), \dots, \theta_\nu(z))$ est un système de coordonnées projectives du point $\Theta(z)$, et

$$\mathcal{F}_{\mathbf{C}} = \mathbf{C}\left(\frac{\theta_1}{\theta_0}, \dots, \frac{\theta_\nu}{\theta_0}\right) .$$

Pour vérifier l'axiome 0.A.2 de la définition de l'ordre arithmétique (§ 1.1), nous utiliserons systématiquement le lemme suivant (l'application linéaire $\mathcal{L}_1 : \mathbf{C}^n \to \mathbf{C}^g$ sera de la forme $\mathbf{C}^n \xrightarrow{\mathcal{L}} \mathbf{C}^g \times \mathbf{C}^h \xrightarrow{p_1} \mathbf{C}^g$ où p_1 est la première projection).

LEMME 1.2.2 - Soient Ω un réseau de $\mathbf{C}^g$, θ une fonction thêta relative à Ω, telle que $\theta(0) \neq 0$, $\mathcal{L}_1 : \mathbf{C}^n \to \mathbf{C}^g$ une application linéaire non nulle, Γ un sous-groupe de type fini de $\mathbf{C}^n$, et $\gamma_1, \dots, \gamma_\ell$ une base de Γ sur $\mathbf{Z}$. Il existe un sous-ensemble T de Γ vérifiant les propriétés équivalentes du lemme 1.1.8, et tel que

$$\log \min_{\sigma \in T \cap \Gamma_N} |\theta \circ \mathcal{L}_1(\sigma)| \geq - c N^2 \quad \text{pour} \quad N \geq 1$$

où c ne dépend pas de N.

On a noté comme précédemment

$$\Gamma_N = \{h_1\gamma_1 + \dots + h_\ell \gamma_\ell \ ; \ (h_1, \dots, h_\ell) \in \mathbf{Z}^\ell , |h_j| \leq N\} .$$

Démonstration du lemme 1.2.2.

Soit H la forme de Riemann associée à θ ; H est une forme hermitienne positive semi-définie, et la fonction

$$\psi(z) = |\theta(z)| \exp\{- \frac{\pi}{2} H(z,z)\}$$

est périodique par rapport à Ω (cf. [L4] Chap. IV, § 2, Th. 3, [S.D] Chap. II, lemme 21, et [We 2] Chap. VI). Soit Δ un disque fermé de $\mathbf{C}^g$, de centre 0 et de rayon $\delta > 0$, dans lequel θ ne s'annule pas. En vertu de la continuité et de la périodicité de ψ, il existe $c_1 > 0$ tel que, pour tout $R \geq 1$, on ait

$$\log \inf\{|\theta(z)| \ ; \ z \in \mathbf{C}^g , |z| \leq R , s(z) \in s(\Delta)\} \geq - c_1 R^2 .$$

où $s : \mathbf{C}^g \to \mathbf{C}^g/\Omega$ est la surjection canonique.

On définit

$$T = \{\gamma \in \Gamma \ ; \ s \circ \mathcal{L}_1(\gamma) \in s(\Delta)\} .$$

Pour $\sigma \in \Gamma_N$, on a $|\mathcal{L}_1(\sigma)| \leq c_2 N$, d'où la minoration annoncée de $|\theta \circ \mathcal{L}_1(\sigma)|$.

De plus, comme $\mathbf{C}^g/\Omega$ est compact, il existe un nombre fini de disques de $\mathbf{C}^g$ de rayon $\delta/2$ dont les images par s recouvrent $\mathbf{C}^g/\Omega$. Dans chacun de ces disques, on choisit (quand c'est possible) un point de $\mathcal{L}_1(\Gamma)$. Soit F l'ensemble fini de points de Γ ainsi obtenus. Alors la condition (i) du lemme 1.1.8 est vérifiée. Le lemme 1.2.2 est ainsi démontré.

c) Problèmes de rationalité.

Soit G un groupe algébrique commutatif connexe de dimension D défini sur un sous-corps K de $\mathbf{C}$. On considère un plongement X de G dans un espace projectif $\mathbf{P}_\nu$, défini sur K. Soit $(t_1, \dots, t_D)$ une base sur K de T_G, et soit $j : \mathbf{C}^D \to T_G(\mathbf{C})$ l'isomorphisme associé. Les dérivations $\frac{\partial}{\partial z_i}$, $(1 \leq i \leq D)$ forment une base sur K de l'algèbre de Lie des dérivations invariantes de G. Nous appellerons représentation normalisée de l'exponentielle de G tout $(\nu+1)$-uplet $(\psi_0, \dots, \psi_\nu)$ de fonctions entières sur $\mathbf{C}^D$ tel que pour tout $z \in \mathbf{C}^D$, $(\psi_0(z), \dots, \psi_\nu(z))$ soit un système de coordonnées projectives du point

$$X \circ \exp \circ j(z) .$$

Dans le cas d'une variété abélienne (avec $\psi_j = \theta_j$) on dira que l'homomorphisme thêta $X \circ \exp \circ j$ est normalisé. Alors le corps

$$\mathcal{F}_K = K\left(\frac{\theta_1}{\theta_o}, \ldots, \frac{\theta_\nu}{\theta_o}\right)$$

est le corps des fonctions abéliennes définies sur K, et $\mathcal{F}_{\mathbf{C}} = \mathcal{F}_K \otimes_K \mathbf{C}$.

Revenons au cas général. Identifions G à une sous-variété de $\mathbf{P}_\nu$, et notons H_o l'hyperplan $X_o = 0$, et $\bar{G}$ l'adhérence de G. On suppose que la loi de composition de G se prolonge en un morphisme $G \times \bar{G} \to \bar{G}$ (cette condition est satisfaite par les plongements construits explicitement par Serre dans l'appendice 2). Les champs de vecteurs sur G définis par l'algèbre de Lie de G se prolongent en des champs de vecteurs sur $\bar{G}$. Comme $K[\frac{\psi_1}{\psi_o}, \ldots, \frac{\psi_\nu}{\psi_o}]$ est l'algèbre affine de $\bar{G} - \bar{G} \cap H_o$, on obtient l'énoncé suivant

PROPOSITION 1.2.3 - Soit $(\psi_o, \ldots, \psi_\nu)$ une représentation normalisée de l'exponentielle de G. Alors les dérivations $\frac{\partial}{\partial z_i}$, $(1 \leq i \leq D)$, laissent stable l'algèbre $K[\frac{\psi_1}{\psi_o}, \ldots, \frac{\psi_\nu}{\psi_o}]$.

Plaçons-nous maintenant dans le cas où K est le corps $\bar{\mathbf{Q}}$ des nombres algébriques. Nous dirons qu'un homomorphisme analytique $\varphi : \mathbf{C}^n \to G_{\mathbf{C}}$ est normalisé si $\varphi = \psi \circ \mathcal{L}$ où ψ est une représentation normalisée de l'exponentielle de G et $\mathcal{L} : \mathbf{C}^n \to \mathbf{C}^D$ est une application $\mathbf{C}$-linéaire définie sur $\bar{\mathbf{Q}}$. Cela revient à dire que $\mathrm{Lie}\,\varphi : \mathbf{C}^n \to T_G(\mathbf{C})$ est définie sur $\bar{\mathbf{Q}}$.

Soit $\varphi : \mathbf{C}^n \to G_{\mathbf{C}}$ un homomorphisme analytique de $\mathbf{C}^n$ dans $G_{\mathbf{C}}$, où G est un groupe algébrique défini sur $\bar{\mathbf{Q}}$. Nous dirons qu'un point $u \in \mathbf{C}^n$ est un point algébrique de φ si $\varphi(u)$ appartient à $G_{\bar{\mathbf{Q}}}$. Quand G est commutatif, les points algébriques de φ forment un $\mathbf{Q}$-espace vectoriel.

Considérons le cas particulier où φ est un homomorphisme thêta $\Theta : \mathbf{C}^g \to A_{\mathbf{C}}$ d'une variété abélienne A. Soit $\mathrm{End}\,A$ l'anneau des endomorphismes de A ; alors $\mathrm{End}_o A = \mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{End}\,A$ est une $\mathbf{Q}$-algèbre semi-simple, appelée algèbre d'endomorphismes de A. Tout élément de $\mathrm{End}_o A$ induit par Θ un endomorphisme de $\mathbf{C}^g$; on obtient un plongement (cf. [Shi 2] p. 126) :

$$\Phi : \mathrm{End}_o A \to M_g(\mathbf{C})$$

défini par

$$\Theta \circ \Phi(\lambda) = \lambda \circ \Phi$$

dont l'image est formée des éléments de $M_g(\mathbf{C})$ laissant stable $\Omega \otimes_{\mathbf{Z}} \mathbf{Q}$ où $\Omega = \ker \Theta$. Alors les points algébriques de Θ forment un module sur $\mathrm{End}_o A$.

d) Courbes elliptiques et extensions.

Si Ω est un réseau de $\mathbf{C}$, les conditions de Riemann (iii) consistent à écrire $\Omega = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 = (\mathbf{Z} + \mathbf{Z}\tau)\omega_1$, avec $\tau = \omega_2/\omega_1$, $\mathrm{Im}(\tau) > 0$. Un plongement analytique de $\mathbf{C}/\Omega$ dans $\mathbf{P}_2(\mathbf{C})$ est donné par $P : \mathbf{C} \to \mathbf{P}_2(\mathbf{C})$, $P(z) = (1, \wp(z), \wp'(z))$ pour $z \notin \Omega$ et $P(\omega) = (0,0,1)$ pour $\omega \in \Omega$, où $\wp$ est la fonction elliptique de Weierstrass associée à Ω. Elle vérifie une équation différentielle

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

avec

$$g_2 = 60\, s_4(\Omega), \quad g_3 = 140\, s_6(\Omega),$$

et

$$s_m(\Omega) = \sum_{\omega \in \Omega, \omega \neq 0} \omega^{-m} \qquad \text{pour } m > 2.$$

Une courbe elliptique est une variété abélienne de dimension 1. Soit $\mathcal{E}$ une courbe elliptique définie sur $\bar{\mathbf{Q}}$. On peut plonger $\mathcal{E}$ dans $\mathbf{P}_2$ de sorte que

$$\mathcal{E}_{\mathbf{C}} = \{(t,x,y) \in \mathbf{P}_2(\mathbf{C})\ ;\ y^2 t = 4x^3 - g_2 x t^2 - g_3 t^3\},$$

avec g_2 et g_3 algébriques, et si $\wp$ est la fonction elliptique de Weierstrass d'invariants g_2, g_3, les homomorphismes thêta sont les applications $z \mapsto P(\lambda z)$, $(\lambda \in \mathbf{C}, \lambda \neq 0)$. Un tel homomorphisme thêta est normalisé si et seulement si $\lambda \in \bar{\mathbf{Q}}$.

Compte tenu de la définition donnée plus haut dans le cas général, un nombre complexe u est un point algébrique de $\wp$ si $u \in \Omega$ ou $\wp(u) \in \bar{\mathbf{Q}}$. En particulier les points de torsion de $\wp$, c'est-à-dire les points $r\omega$, $(r \in \mathbf{Q}, \omega \in \Omega)$ sont des points algébriques de $\wp$.

Si $\mathcal{E}nd\,\mathcal{E}$ n'est pas réduit à $\mathbf{Z}$ on dit que $\wp$ (ou $\mathcal{E}$) admet la multiplication complexe ; alors $\mathcal{E}nd_o(\mathcal{E}) = \mathbf{Q}(\tau)$ est un corps quadratique imaginaire appelé corps de multiplication complexe de $\mathcal{E}$.

Pour l'étude des extensions d'une courbe elliptique (cf. § 3.2.b), nous aurons à utiliser les fonctions zêta et sigma de Weierstrass. La fonction sigma associée à Ω est le produit canonique

$$\sigma(z) = z \prod_{\omega \in \Omega, \omega \neq 0} \left(1 - \frac{z}{\omega}\right) \exp\left(\frac{z}{\omega} + \frac{z^2}{2\omega^2}\right);$$

sa dérivée logarithmique est la fonction zêta associée à Ω

$$\zeta(z) = \frac{\sigma'(z)}{\sigma(z)} = \frac{1}{z} + \sum_{\omega \in \Omega, \omega \neq 0} \left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right),$$

et la dérivée de $-\zeta$ est la fonction elliptique $\wp$ de Weierstrass.

Nous utiliserons la quasi-périodicité de ζ : pour $\omega = m_1\omega_1 + m_2\omega_2$ et $\eta = m_1\eta_1 + m_2\eta_2$, $(m_1, m_2 \in \mathbf{Z},\ \eta_j = 2\zeta(\omega_j/2))$, on a

$$\zeta(z+\omega) = \zeta(z) + \eta .$$

On en déduit

$$\sigma(z+\omega) = (-1)^{m_1+m_2+m_1m_2} \cdot \sigma(z) \exp(\eta(z+\tfrac{\omega}{2})) ,$$

donc σ est une fonction thêta relative à Ω.

e) Dimension algébrique.

Soient G un groupe algébrique connexe défini sur $\mathbf{C}$, $\varphi : \mathbf{C}^n \to G_{\mathbf{C}}$ un homomorphisme analytique. La dimension algébrique de φ est par définition la dimension de l'adhérence de Zariski de $\varphi(\mathbf{C}^n)$. Si X est un plongement de G dans un espace projectif $\mathbf{P}_\nu$, et $\varphi_o, \dots, \varphi_\nu$ des fonctions entières sur $\mathbf{C}^n$, avec $\varphi_o \neq 0$, telles que pour tout $z \in \mathbf{C}^n$, $(\varphi_o(z), \dots, \varphi_\nu(z))$ soit un système de coordonnées projectives de $X \circ \varphi$, alors la dimension algébrique de φ est égale au degré de transcendance sur $\mathbf{C}$ du corps $\mathbf{C}(\frac{\varphi_1}{\varphi_o}, \dots, \frac{\varphi_\nu}{\varphi_o})$.

Si $\varphi : \mathbf{C}^n \to G_{\mathbf{C}}$ est un sous-groupe (commutatif) à n paramètres de G de dimension algébrique n, alors $\varphi(\mathbf{C}^n)$ est un sous-groupe algébrique fermé de $G_{\mathbf{C}}$. En effet, quitte à remplacer $G_{\mathbf{C}}$ par la clôture de Zariski de $\varphi(\mathbf{C}^n)$, on peut supposer que G est commutatif connexe de dimension n. Alors $\varphi = \exp \circ \mathcal{L}$ où $\mathcal{L}$ est un isomorphisme de $\mathbf{C}^n$ sur l'espace tangent, donc $\varphi(\mathbf{C}^n) = G_{\mathbf{C}}$.

Soient A une variété abélienne, B un groupe linéaire, $\varphi_1 : \mathbf{C}^n \to A_{\mathbf{C}}$ et $\varphi_2 : \mathbf{C}^n \to B_{\mathbf{C}}$ deux homomorphismes analytiques de dimension algébrique d_1 et d_2 respectivement. Alors la dimension algébrique de l'homomorphisme

$$\begin{aligned} \mathbf{C}^n &\to A_{\mathbf{C}} \times B_{\mathbf{C}} \\ z &\to (\varphi_1(z), \varphi_2(z)) \end{aligned}$$

est égale à $d_1 + d_2$. On le montre soit en utilisant le fait que toute application rationnelle $B \to A$ est constante, soit à partir du corollaire 9 de [Br-K].

§ 1.3 - Exposant de Dirichlet généralisé.

a) Introduction.

Soient K un corps de caractéristique 0, V un K-espace vectoriel de dimen-

sion finie n, et Γ un sous-groupe de type fini de V, de rang ℓ sur $\mathbf{Z}$. On définit

$$\mu(\Gamma, V)$$

comme le plus petit des nombres

$$\frac{\operatorname{rang}_{\mathbf{Z}} s_{V/W}(\Gamma)}{\dim_K V/W} = \frac{\ell - \operatorname{rang}_{\mathbf{Z}}(\Gamma \cap W)}{n - \dim_K W}$$

quand W parcourt les sous-espaces vectoriels de V distincts de V et $s_{V/W}$ est la surjection canonique $V \to V/W$.

On a toujours $\mu(\Gamma, V) \leq \ell/n$. On dira que Γ est bien réparti dans V si $\mu(\Gamma, V) = \ell/n$.

Ce coefficient $\mu(\Gamma, V)$ joue un rôle important dans plusieurs problèmes diophantiens à plusieurs variables. Nous allons voir qu'il intervient dans le théorème de W.M. Schmidt généralisant aux approximations simultanées le théorème de Thue-Siegel-Roth. Nous le verrons apparaître aussi dans le lemme de Schwarz en plusieurs variables (Chap. 7).

Pour les applications que nous avons en vue, K sera $\mathbf{R}$ ou $\mathbf{C}$. Quand Γ est un sous-groupe de type fini de $\mathbf{C}^n$, on a

$$\mu(\Gamma, \mathbf{C}^n) \geq 2\mu(\Gamma, \mathbf{R}^{2n}) .$$

Si Γ est contenu dans la trace réelle $\mathbf{R}^n$ de $\mathbf{C}^n$, alors

$$\mu(\Gamma, \mathbf{C}^n) = \mu(\Gamma, \mathbf{R}^n) .$$

b) Généralités sur $\mu(\Gamma, V)$.

Remarquons d'abord que si $\mu(\Gamma, V) \neq 0$, alors Γ contient n éléments K-linéairement indépendants, et $\mu(\Gamma, V) \geq 1$.

Si $\ell = n+1$ et $\Gamma = \mathbf{Z}\gamma_1 + \dots + \mathbf{Z}\gamma_n + \mathbf{Z}\gamma_{n+1}$, avec $\gamma_1, \dots, \gamma_n$ K-linéairement indépendants et $\gamma_{n+1} = c_1\gamma_1 + \dots + c_n\gamma_n$, $(c_j \in K)$, alors Γ est bien réparti dans V si et seulement si $1, c_1, \dots, c_n$ sont $\mathbf{Q}$-linéairement indépendants.

Si Γ_1, Γ_2 sont deux sous-groupes de type fini de V, et $V_j = \bar{\Gamma}_j$ le sous-espace vectoriel engendré par Γ_j, on vérifie facilement que

$$\mu(\Gamma_1 + \Gamma_2, V_1 + V_2) \geq \min_{j=1,2} \mu(\Gamma_j, V_j) .$$

On en déduit que si $\Gamma_1, \dots, \Gamma_s$ sont des sous-groupes de type fini de $V_1, \dots, V_s$ respectivement, alors $\Gamma_1 \oplus \dots \oplus \Gamma_s$ est bien réparti dans $V_1 \oplus \dots \oplus V_s$ si et seulement si les deux propriétés suivantes sont satisfaites

i) pour tout $j = 1, \dots, s$, Γ_j est bien réparti dans V_j

ii) $\mu(\Gamma_1, \bar{\Gamma}_1) = \dots = \mu(\Gamma_s, \bar{\Gamma}_s)$.

Le résultat suivant nous sera très utile.

LEMME 1.3.1 - Soit Γ un sous-groupe de type fini de V de rang ℓ sur $\mathbf{Z}$. Il existe un sous-groupe Γ' de Γ qui est bien réparti dans le K-espace vectoriel $\bar{\Gamma}'$ qu'il engendre et tel que

$$\mu(\Gamma', \bar{\Gamma}') \geqq \ell/n .$$

Démonstration du lemme 1.3.1.

Si Γ est bien réparti dans V, on prend $\Gamma' = \Gamma$. Sinon, on démontre le résultat avec l'inégalité stricte par récurrence sur n.

On peut supposer $\bar{\Gamma} = V$. Soit W un sous-espace de V de dimension $\rho < n$ tel que

$$\mu(\Gamma, V) = \frac{\ell-\lambda}{n-\rho}$$

avec $\lambda = \mathrm{rang}_{\mathbf{Z}} \Gamma \cap W$, et $\frac{\ell-\lambda}{n-\rho} < \frac{\ell}{n}$, c'est-à-dire $\ell\rho < n\lambda$.

Si $\Gamma \cap W$ est bien réparti dans W, on a $\overline{\Gamma \cap W} = W$ et

$$\mu(\Gamma \cap W, W) = \frac{\lambda}{\rho} > \frac{\ell}{n} .$$

Sinon, on utilise l'hypothèse de récurrence : il existe un sous-groupe Γ' de $\Gamma \cap W$ bien réparti dans $\bar{\Gamma}'$ tel que

$$\mu(\Gamma', \bar{\Gamma}') > \frac{\lambda}{\rho} > \frac{\ell}{n} .$$

Nous aurons besoin également du résultat suivant.

LEMME 1.3.2 - Soit W un sous-espace de V de dimension $\rho < n$ tel que

$$\mu(\Gamma, V) = \frac{\ell-\lambda}{n-\rho}$$

où $\lambda = \mathrm{rang}_{\mathbf{Z}}(\Gamma \cap W)$. On suppose $\lambda > 0$. Alors

$$\mu(\Gamma \cap W, W) \geqq \mu(\Gamma, V) .$$

Démonstration du lemme 1.3.2.

Supposons $\mu(\Gamma \cap W, W) < \mu(\Gamma, V)$. Soit W_1 un sous-espace de W de dimension

$\rho_1 < \rho$ tel que

$$\mu(\Gamma \cap W, W) = \frac{\lambda-\lambda_1}{\rho-\rho_1}$$

où $\lambda_1 = \mathrm{rang}_{\mathbf{Z}}(\Gamma \cap W_1)$. Par hypothèse

$$\frac{\lambda-\lambda_1}{\rho-\rho_1} < \frac{\ell-\lambda}{n-\rho}$$

donc

$$\frac{\ell-\lambda_1}{n-\rho_1} < \frac{\ell-\lambda}{n-\rho}$$

ce qui contredit la définition de $\mu(\Gamma, V)$.

c) Lien avec l'hypothèse d'un théorème de W.M. Schmidt.

Soient K un corps de caractéristique nulle, n un entier positif, et Γ un sous-groupe de type fini de K^n. Soit $\gamma_1, \dots, \gamma_\ell$ une base de Γ sur $\mathbf{Z}$. Notons, pour $1 \leqq j \leqq \ell$,

$$\gamma_j = \begin{pmatrix} \gamma_{j,1} \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \gamma_{j,n} \end{pmatrix} .$$

La définition que nous avons donnée de $\mu(\Gamma, K^n)$ fait intervenir les vecteurs colonnes de la matrice

$$(\gamma_1, \dots, \gamma_\ell) = \begin{pmatrix} \gamma_{1,1} & \cdots & \gamma_{\ell,1} \\ \cdots & \cdots & \cdots \\ \gamma_{1,n} & \cdots & \gamma_{\ell,n} \end{pmatrix}$$

Nous allons donner une définition équivalente en terme des vecteurs lignes de cette matrice. Pour cela, on introduit les formes linéaires

$$L_s(X_1, \dots, X_\ell) = \sum_{j=1}^{\ell} \gamma_{j,s} X_j , \qquad (1 \leqq s \leqq n) .$$

Considérons un sous-espace S de K^ℓ, rationnel sur $\mathbf{Q}$ (c'est-à-dire défini par des équations linéaires à coefficients dans $\mathbf{Q}$). Soient d la dimension de S sur K, et r le rang sur K de la restriction à S de $L_1, \dots, L_n$. Nous démontrerons un peu plus loin le résultat suivant.

PROPOSITION 1.3.3 - Le nombre $\mu(\Gamma,K^n)$ est égal au minimum des nombres $\frac{\ell-d}{n-r}$ quand S parcourt les sous-espaces de K^ℓ rationnels sur $\mathbf{Q}$ pour lesquels $r<n$.

Par conséquent Γ est bien réparti dans K^n si et seulement si pour tout sous-espace de K^ℓ rationnel sur $\mathbf{Q}$, le rang r de la restriction à S de $L_1,\dots,L_n$ vérifie

$$r \geq \frac{n}{\ell} d .$$

Grâce à ce résultat, le théorème de W.M. Schmidt [Sc] (th. 7.E) s'énonce ainsi.

THÉORÈME 1.3.4 (W. Schmidt) - Soit Γ un sous-groupe de type fini de $\mathbf{R}^n \cap \overline{\mathbf{Q}}^n$ de rang $\ell > n$ sur $\mathbf{Z}$. Les deux conditions suivantes sont équivalentes

a) Γ est bien réparti dans $\mathbf{R}^n$

b) Si $\gamma_1,\dots,\gamma_\ell$ est une base de Γ sur $\mathbf{Z}$, alors pour tout $\epsilon>0$ il existe une constante $c(\epsilon)$ ne dépendant que de ϵ, n, $\gamma_1,\dots,\gamma_\ell$, telle que pour tout $N \geq 1$ on ait

$$\min\{|\gamma| \; ; \; \gamma\in\Gamma_N ,\ \gamma\neq 0\} \geq c(\epsilon) N^{1-\frac{\ell}{n}-\epsilon} ,$$

où

$$\Gamma_N = \{h_1\gamma_1+\dots+h_\ell\gamma_\ell \; ; \; (h_1,\dots,h_\ell)\in \mathbf{Z}^\ell ,\ |h_j| \leq N,\ (1\leq j\leq \ell)\} .$$

Nous reviendrons sur cette question quand nous aurons introduit la notion de coefficient de densité.

Démonstration de la proposition 1.3.3.

Nous démontrons la proposition 1.3.3 en deux temps. L'inégalité

$$\mu(\Gamma,K^n) \leq \min \frac{\ell-d}{n-r}$$

résulte du lemme suivant.

LEMME 1.3.5 - Soient d un entier, $1\leq d\leq \ell$, S un sous-espace de K^ℓ rationnel sur $\mathbf{Q}$ de dimension d, et r le rang de la restriction de $L_1,\dots,L_n$ à S. Il existe un sous-espace W de K^n, de dimension r, tel que

$$\mathrm{rang}_{\mathbf{Z}}(\Gamma\cap W) \geq d .$$

Démonstration du lemme 1.3.16.

Sur S on a $n-r$ relations indépendantes

$$\sum_{s=1}^{n} u_{s,k} L_s = 0 \qquad (1\leq k\leq n-r) ,$$

avec $u_{s,k}\in K$. La matrice $(u_{s,k})$ ayant pour rang $n-r$, l'application K-linéaire $p : K^n \to K^{n-r}$ définie par

$$p(x_1,\dots,x_n) = \Big(\sum_{s=1}^{n} u_{s,k}x_s\Big)_{1\leq k\leq n-r}$$

a pour noyau un sous-espace W de K^n, de dimension r, et pour $(\xi_1,\dots,\xi_\ell)\in S$ on a

$$\sum_{j=1}^{\ell} p(\gamma_j)\xi_j = 0 ,$$

d'où

$$\mathrm{rang}_{\mathbf{Z}}\, p(\Gamma) \leq \ell-d .$$

Pour établir l'inégalité

$$\mu(\Gamma,K^n) \geq \min \frac{\ell-d}{n-r} ,$$

on démontre le lemme suivant

LEMME 1.3.6 - Soient W un sous-espace de K^n de dimension ρ, et $\lambda = \mathrm{rang}_{\mathbf{Z}}(\Gamma\cap W)$. Il existe un sous-espace S de K^ℓ, rationnel sur $\mathbf{Q}$, de dimension λ, tel que le rang r de la restriction à S de $L_1,\dots,L_n$ vérifie

$$r \leq \rho .$$

Démonstration du lemme 1.3.6.

Soit $s : K^n \to K^n/W$ la surjection canonique. Comme $s(\Gamma)$ est de rang $\ell-\lambda$ sur $\mathbf{Z}$, il existe λ relations indépendantes

$$\sum_{j=1}^{\ell} a_{t,j}\, s(\gamma_j) = 0 , \qquad (1\leq t\leq \lambda) ,$$

avec $a_{t,j}\in\mathbf{Z}$. Soit S le sous-espace de K^ℓ engendré par les λ éléments

$$(a_{t,1},\dots,a_{t,\ell})\in K^\ell , \qquad (1\leq t\leq\lambda) .$$

Ecrivons, pour $x=(x_1,\dots,x_n)\in K^n$,

$$s(x) = \sum_{k=1}^{n-\rho}\sum_{s=1}^{n} u_{s,k}x_s e_k$$

où $e_1,\dots,e_{n-\rho}$ est une base de K^n/W sur K, et $u_{s,k}\in K$. Alors sur S

on a

$$\sum_{s=1}^{n} u_{s,k} L_s = 0 , \qquad (1 \leq k \leq n-\rho)$$

ce qui démontre l'inégalité $r \leq \rho$.

La proposition 1.3.3 résulte immédiatement des lemmes 1.3.5 et 1.3.6.

d) Sous-groupes de $\mathbf{R}^n$.

Soient $\Gamma = \mathbf{Z}\gamma_1 + \ldots + \mathbf{Z}\gamma_\ell$ un sous-groupe de type fini de $\mathbf{R}^n$ de rang ℓ sur $\mathbf{Z}$, et $\varkappa$ un nombre réel. Nous dirons que Γ a un coefficient de densité $\geq \varkappa$ dans $\mathbf{R}^n$ s'il existe deux nombres réels positifs c_1 , c_2 ne dépendant que de n , $\gamma_1, \ldots, \gamma_\ell$ et $\varkappa$ ayant la propriété suivante : pour tout $N \geq 1$ et tout $\zeta \in \mathbf{R}^n$ avec $|\zeta| \leq c_1 N$, il existe un élément γ de l'ensemble

$$\Gamma_N = \{h_1\gamma_1 + \ldots + h_\ell\gamma_\ell \; ; \; (h_1, \ldots, h_\ell) \in \mathbf{Z}^\ell, \; |h_j| \leq N\}$$

tel que

$$|\zeta - \gamma| \leq c_2 N^{1-\varkappa} .$$

Il est clair que, si cette propriété est vérifiée pour une base $\gamma_1, \ldots, \gamma_\ell$ de Γ sur $\mathbf{Z}$, alors elle est vérifiée pour toute base. D'autre part si Γ contient n éléments $\mathbf{R}$-linéairement indépendants, il suffit de vérifier la propriété pour les $\zeta \in \mathbf{R}^n$ avec $|\zeta| \leq 1$.

LEMME 1.3.7 - Si Γ a un coefficient de densité $\geq \varkappa$, alors

$$\varkappa \leq \mu(\Gamma, \mathbf{R}^n) .$$

Démonstration du lemme 1.3.7.

Si $p : \mathbf{R}^n \to \mathbf{R}^{n-\rho}$ est une application surjective, alors $p(\Gamma)$ a un coefficient de densité $\geq \varkappa$ relativement à $\mathbf{R}^{n-\rho}$. Il suffit donc que l'on démontre l'inégalité $\varkappa \leq \ell/n$ avec $\ell = \mathrm{rang}_{\mathbf{Z}}\Gamma$. Nous aurons besoin d'un résultat plus précis.

LEMME 1.3.8 - Soit Γ un sous-groupe de $\mathbf{R}^n$ de rang ℓ sur $\mathbf{Z}$, ayant un coefficient de densité $\geq \varkappa$. Soit $\gamma_1, \ldots, \gamma_\ell$ une base de Γ sur $\mathbf{Z}$. Soit η un nombre réel, $0 < \eta < 1$. Il existe des nombres réels positifs c_3 , c_4 , c_5 , ne dépendant que de n , $\varkappa$, $\gamma_1, \ldots, \gamma_\ell$ et η , avec la propriété suivante.

Soit N un entier, $N \geq c_3$. Soit

$$\Gamma_N = \{h_1\gamma_1 + \ldots + h_\ell\gamma_\ell \; ; \; (h_1, \ldots, h_\ell) \in \mathbf{Z}^\ell \; , \; |h_s| \leq N, \; 1 \leq s \leq \ell\} ,$$

et soit S_N un sous-ensemble de Γ_N , avec

$$\mathrm{Card}\, S_N \geq \eta \; \mathrm{Card}\, \Gamma_N .$$

Alors il existe un sous-ensemble E_N de S_N tel que

$$\mathrm{Card}\, E_N \geq c_4 N^{n\varkappa}$$

et

$$\min\{|\sigma - \sigma'| \; ; \; \sigma \in E_N , \; \sigma' \in E_N , \; \sigma \neq \sigma'\} \geq c_5 N^{1-\varkappa} .$$

Démonstration du lemme 1.3.8.

Soient c_1 , c_2 les nombres introduits dans la définition du coefficient de densité ; $c_6, \ldots, c_{10}$ désigneront des nombres réels positifs ne dépendant que de n , $\varkappa$, $\gamma_1, \ldots, \gamma_\ell$.

a) Soit M le nombre de points de Γ_{2N} dans la boule euclidienne $|\zeta| \leq 2c_2 N^{1-\varkappa}$. Montrons que $M \leq c_6 N^{\ell - n\varkappa}$. Pour cela on décompose le cube $[-c_3 N, c_3 N]^n$ en L_1^n cubes, avec $c_3 = c_1 n^{-1/2}$ et $L_1 = [c_7 N^{\varkappa}]$. Soit ζ un des centres d'un de ces petits cubes. Il existe $\gamma_\zeta \in \Gamma_N$ tel que

$$|\zeta - \gamma_\zeta| \leq c_2 N^{1-\varkappa} .$$

Soient $\gamma_1^o, \ldots, \gamma_M^o$ les éléments de Γ_{2N} vérifiant $|\gamma_s^o| \leq 2c_2 N^{1-\varkappa}$. Alors

$$|\zeta - \gamma_\zeta - \gamma_s^o| \leq 3c_2 N^{1-\varkappa} , \qquad (1 \leq s \leq M) .$$

Si

$$3c_2 N^{1-\varkappa} < c_3 \frac{N}{L_1} ,$$

ce qui est vérifié dès que $c_7 < \dfrac{c_3}{3c_2}$, les points $\gamma_\zeta - \gamma_s^o$, $(1 \leq s \leq M$, ζ centre d'un des petits cubes) sont deux à deux distincts. Or ils appartiennent à Γ_{3N} . D'où

$$L_1^n M \leq (6N + 1)^\ell ,$$

ce qui donne la majoration de M annoncée (et en particulier $\varkappa \leq \ell/n$) .

b) Dans une boule de rayon $c_2 N^{1-\varkappa}$, il y a au plus M points de Γ_N .

En effet, si $\gamma_1, \ldots, \gamma_h$, sont des éléments de Γ_N dans une même boule de rayon $c_2 N^{1-\varkappa}$, alors $\gamma_j - \gamma_1$, $(1 \leq j \leq h)$ sont des éléments de Γ_{2N} dans la boule $|\zeta| \leq 2c_2 N^{1-\varkappa}$.

c) Soit $c_8 = \sum_{s=1}^{\ell} |\gamma_s|$. On décompose le cube $[- c_8 N, c_8 N]^n$ en L_2^n cubes, avec $L_2 = [c_9 N^{\varkappa}]$, et $c_9 > \frac{c_8}{c_2}\sqrt{n}$, de telle manière que chacun des petits cubes soit contenu dans une boule de rayon $c_2 N^{1-\varkappa}$ (donc contienne au plus M points de Γ_N) . Comme S_N est contenu dans le cube $[- c_8 N, c_8 N]^n$, le nombre de ces petits cubes qui contiennent au moins un élément de S_N est supérieur ou égal à

$$\frac{1}{M} \operatorname{Card} S_N \geq \eta\, c_{10} N^{n\varkappa} .$$

Pour chacun de ces petits cubes on choisit un point σ de S_N , et l'ensemble E_N de ces points σ vérifie les propriétés requises.

REMARQUE 1.3.9 - Le lemme 1.3.7 exprime que le nombre $\mu(\Gamma, \mathbf{R}^n) - 1$ joue le rôle de l'exposant de Dirichlet pour la recherche d'un coefficient de densité. (*)

Quand on étudie la suite

$$\min\{|\gamma| \ , \ \gamma \in \Gamma_N \ , \ \gamma \neq 0\} \ , \quad N \geq 1 \ ,$$

le rôle de l'exposant de Dirichlet est joué par le nombre

$$\max \frac{d}{r} - 1 = \max \frac{\lambda}{\rho} - 1$$

(avec les notations par exemple du § 1.3.c ci-dessus). Dans le cas particulier $\Gamma = \mathbf{Z}\gamma_1 + \ldots + \mathbf{Z}\gamma_{n+2}$, avec $\gamma_1, \ldots, \gamma_n$ $\mathbf{R}$-linéairement indépendants et

$$\gamma_{n+1} = x_1 \gamma_1 + \ldots + x_n \gamma_n \ , \qquad \gamma_{n+2} = y\gamma_1 \ ,$$

$1, x_1, \ldots, x_n$ étant $\mathbf{Q}$-linéairement indépendants et y irrationnel, on a

$$\mu(\Gamma, \mathbf{R}^n) = 1 + \frac{1}{n-1} \ , \qquad \max \frac{\lambda}{\rho} = 2 \ .$$

Il existe évidemment des groupes Γ pour lesquels l'inégalité du lemme 1.3.7 n'est pas la meilleure possible (par exemple, pour $n = 1$, $\Gamma = \mathbf{Z} + \mathbf{Z}t$ où t est un nombre de Liouville). Le théorème 1.3.4 de W.M. Schmidt va nous permettre de montrer que cette inégalité est la meilleure possible quand $\Gamma \subset \overline{\mathbf{Q}}^n \cap \mathbf{R}^n$.

THÉORÈME 1.3.10 - Si Γ est un sous-groupe de $\mathbf{R}^n \cap \overline{\mathbf{Q}}^n$ de type fini sur $\mathbf{Z}$, pour tout $\varepsilon > 0$ Γ a un coefficient de densité $\geq \mu(\Gamma, \mathbf{R}^n) - \varepsilon$.

Démonstration du théorème 1.3.10.

Dans le cas où Γ est bien réparti dans $\mathbf{R}^n$, le résultat découle du théorème 1.3.4 et du lemme de transfert suivant [Ca] (Chap.V, th.II, VI, VII).

(*) On notera aussi que Γ est dense dans $\mathbf{R}^n$ si et seulement si $\mu(\Gamma, \mathbf{R}^n) > 1$.

LEMME 1.3.11 - Soit $\Gamma = \mathbf{Z}\gamma_1 + \ldots + \mathbf{Z}\gamma_\ell$ un sous-groupe de $\mathbf{R}^n$ de rang ℓ . Les conditions suivantes sont équivalentes.

(i) Pour tout $\varepsilon > 0$, Γ a un coefficient de densité $\geq (\ell/n) - \varepsilon$.

(ii) Pour tout $\varepsilon > 0$, il existe $c = c(\varepsilon) > 0$ tel que

$$\min\{|\gamma| \ ; \ \gamma \in \Gamma_N \ , \ \gamma \neq 0\} \geq c(\varepsilon)\, N^{1 - \frac{\ell}{n} - \varepsilon} \ .$$

Le théorème 1.3.10 étant ainsi démontré dans le cas où Γ est bien réparti dans $\mathbf{R}^n$, nous allons le démontrer dans le cas contraire par récurrence sur n . Soit W un sous-espace de $\mathbf{R}^n$ de dimension $\rho < n$ avec

$$\mu(\Gamma, \mathbf{R}^n) = \frac{\ell - \lambda}{n - \rho} \ , \qquad \lambda = \operatorname{rang}_{\mathbf{Z}} \Gamma \cap W \ .$$

Soit $\varkappa = \mu(\Gamma, \mathbf{R}^n) - \varepsilon$. Comme l'image $s(\Gamma)$ de Γ dans $\mathbf{R}^n/W$ est bien répartie dans $\mathbf{R}^n/W$, et que

$$\mu(s(\Gamma), \mathbf{R}^n/W) = \mu(\Gamma, \mathbf{R}^n) \ ,$$

$s(\Gamma)$ a un coefficient de densité $\geq \varkappa$ dans $\mathbf{R}^n/W$. De plus l'hypothèse de récurrence et le lemme 1.3.2 montrent que $\Gamma \cap W$ a un coefficient de densité $\geq \varkappa$ dans W .

Soit alors $\zeta \in \mathbf{R}^n$, $|\zeta| \leq c_{11} N$. Il existe $\gamma_1 \in \Gamma_{N/2}$ tel que

$$|s(\zeta) - s(\gamma_1)| \leq c_{12} N^{1-\varkappa} \ .$$

On en déduit $\zeta_2 \in W$, $|\zeta_2| \leq c_{13} N$, avec

$$|\zeta - \gamma_1 - \zeta_2| \leq c_{14} N^{1-\varkappa} \ .$$

Maintenant il existe $\gamma_2 \in \Gamma_{N/2}$, tel que

$$|\zeta_2 - \gamma_2| \leq c_{15} N^{1-\varkappa} \ ,$$

d'où

$$|\zeta - \gamma_1 - \gamma_2| \leq c_{16} N^{1-\varkappa} \ .$$

On connait d'autres exemples de sous-groupes de $\mathbf{R}^n$ ayant un coefficient de densité maximal ; c'est le cas pour $\Gamma = \mathbf{Z}\gamma_1 + \ldots + \mathbf{Z}\gamma_{n+1}$ quand $\gamma_j = e^{\theta_j}$, $\theta_j \in \mathbf{Q}$ $(1 \leq j \leq n+1)$ grâce à un résultat de Baker [B] (Théorème 10.1). D'autre part on a la proposition suivante, qui résulte du lemme 1.3.11 combiné à un théorème de Khintchine (cf. [Lu]).

PROPOSITION 1.3.12 - *Soient* ℓ *et* n *deux entiers,* $\ell \geqq n$. *Pour presque tout* $(\gamma_1, \ldots, \gamma_\ell) \in \mathbf{R}^{\ell n}$ *(au sens de la mesure de Lebesgue), le sous-groupe*

$$\Gamma = \mathbf{Z}\gamma_1 + \ldots + \mathbf{Z}\gamma_\ell$$

de $\mathbf{R}^n$ *a un coefficient de densité* $\geqq \frac{\ell}{n} - \epsilon$ *pour tout* $\epsilon > 0$.

e) *Hypersurfaces algébriques de* $\mathbf{C}^n$.

Soient S un sous-ensemble fini non vide de $\mathbf{C}^n$, et t un entier positif. On note $\omega_t(S)$ le plus petit des degrés des hypersurfaces algébriques ayant en chaque point de S une singularité d'ordre $\geqq t$:

$$\omega_t(S) = \min\{\deg P \; ; \; P \in \mathbf{C}[z_1, \ldots, z_n], \; P \neq 0, \quad D^\tau P(\sigma) = 0 \quad \text{pour}$$
$$\text{tout} \;\; \sigma \in S \;\; \text{et} \;\; \tau \in \mathbf{N}^n, \; |\tau| < t\} .$$

Ces nombres sont utiles dans l'étude du lemme de Schwarz à plusieurs variables ([Wa 3] II, § 5 ; cf. Chap. 7), et c'est un problème important et difficile de les minorer. La majoration est facile.

LEMME 1.3.13 - *On a*

$$\omega_t(S) \leqq (t+n-1)(\mathrm{Card}\, S)^{1/n} - (n-1) .$$

Démonstration du lemme 1.3.13.

Le système d'équations linéaires homogènes

$$D^\tau P(\sigma) = 0 \qquad (\sigma \in S, \; \tau \in \mathbf{N}^n, \; |\tau| < t)$$

dont les inconnues sont les coefficients de P admet une solution non triviale pour laquelle $\deg P \leqq \Delta$ dès que

$$\binom{\Delta + n}{n} > \binom{t + n - 1}{n} \mathrm{Card}\, S .$$

Soit Δ la partie entière de $(t+n-1)(\mathrm{Card}\, S)^{1/n} - (n-1)$. Alors, pour $1 \leqq k \leqq n$, on a $\Delta + k > (t+k-1)(\mathrm{Card}\, S)^{1/n}$. Donc $\omega_t(S) \leqq \Delta$. D'où le lemme.

Nous démontrerons au § 7.5 les inégalités

$$\frac{1}{n}\,\omega_1(S) \leqq \frac{1}{t}\,\omega_t(S) \leqq \omega_1(S) .$$

(La deuxième inégalité est triviale, alors que la démonstration de la première nécessite -jusqu'à présent- de l'analyse complexe.)

Considérons de nouveau un sous-$\mathbf{Z}$-module de type fini $\Gamma = \mathbf{Z}\gamma_1 + \ldots + \mathbf{Z}\gamma_\ell$ de $\mathbf{C}^n$,

de rang ℓ sur $\mathbf{Z}$. Pour $N \geqq 1$, notons comme d'habitude

$$\Gamma_N = \{h_1\gamma_1 + \ldots + h_\ell\gamma_\ell \; ; \; (h_1, \ldots, h_\ell) \in \mathbf{Z}^\ell , \quad |h_j| \leqq N\} .$$

LEMME 1.3.14 - *Il existe une constante* $c_{17} > 0$ *ne dépendant que de* $n, \gamma_1, \ldots, \gamma_\ell$, *telle que pour tout* t *et* N *entiers positifs on ait*

$$\omega_t(\Gamma_N) \leqq c_{17}\, t\, N^{\mu(\Gamma, \mathbf{C}^n)} .$$

Démonstration du lemme 1.3.14.

Le lemme 1.3.13 donne immédiatement

$$\omega_t(\Gamma_N) \leqq c_{18}\, t\, N^{\ell/n}$$

et on applique ce résultat à l'image de Γ dans $\mathbf{C}^n/W$, où W est un sous-espace de $\mathbf{C}^n$ de dimension $\rho < n$ tel que

$$\mu(\Gamma, \mathbf{C}^n) = \frac{\ell - \lambda}{n - \rho} , \qquad \lambda = \mathrm{rang}_{\mathbf{Z}}\, \Gamma \cap W .$$

Il serait intéressant de savoir si l'inégalité du lemme 1.3.14 est toujours la meilleure possible, autrement dit de savoir si

$$\omega_1(\Gamma_N) \geqq c_{19}(\epsilon) N^{\mu(\Gamma, \mathbf{C}^n) - \epsilon} \qquad \text{pour tout} \;\; \epsilon > 0 . \; (*)$$

Cette inégalité est vraie quand $\Gamma \subset \overline{\mathbf{Q}}^n \cap \mathbf{R}^n$: c'est une conséquence de l'énoncé suivant, que l'on déduit du théorème de Moreau [Mo] (cf. § 7.3 ci-dessous).

Soient E un sous-$\mathbf{R}$-espace vectoriel de $\mathbf{C}^n$ contenant n éléments $\mathbf{C}$-linéairement indépendants, et Γ un sous-groupe de type fini de E , ayant un coefficient de densité $\geqq \varkappa$ dans E . Alors

$$\omega_1(\Gamma_N) \geqq c_{20}\, N^\varkappa ,$$

où c_{20} ne dépend que de n , E et $\gamma_1, \ldots, \gamma_\ell$.

Si $E = \mathbf{C}^n$, un résultat de Masser [M 1] (Appendice 2) entraîne

$$\omega_1(\Gamma_N) \geqq c_{21}\, N^{2\varkappa} .$$

Nous reviendrons sur ces résultats au chapitre 7.

(*) cf § 7.6.

CHAPITRE 2

MATRICES ET NOMBRES TRANSCENDANTS

Le but de ce chapitre est de développer les résultats sur les groupes algébriques linéaires dont nous aurons besoin dans la suite .

Soit $\varphi : \mathbb{C}^n \to GL_m(\mathbb{C})$ un homomorphisme analytique ; nous étudions les points $\gamma \in \mathbb{C}^n$ (ou $\gamma \in \overline{\mathbb{Q}}^n$) pour lesquels $\varphi(\gamma) \in GL_m(\overline{\mathbb{Q}})$ Pour $n = 1$, puis pour $n \geq 2$, nous commençons par étudier le cas où φ est normalisé. Si l'on suppose $\gamma \in \overline{\mathbb{Q}}^n$, il suffit d'une hypothèse sur l'irrationalité de φ, sinon il faut faire intervenir la dimension algébrique de φ .

Nous montrons que cette étude se ramène à celle de la fonction exponentielle usuelle, et donc aux énoncés classiques de transcendance du § 1.1. C'est facile pour les sous-groupes à 1 paramètre ; c'est plus intéressant dans le cas de plusieurs variables, puisque les arguments d'algèbre linéaire qui interviennent nous seront utiles au chapitre 6 dans le cas d'un groupe algébrique (commutatif connexe) quelconque.

Enfin nous verrons que l'étude des points de $\mathbb{C}^n$ où un homomorphisme analytique $\varphi : \mathbb{C}^n \to GL_m(\mathbb{C})$ prend des valeurs algébriques est liée au problème consistant à montrer que, sous des hypothèses naturelles, un déterminant dont les coefficients sont des logarithmes de nombres algébriques ne s'annule pas.

§ 2.1 - Généralités.

a) Sous-groupes à 1 paramètre de $GL_m(\mathbb{C})$.

Soit $\varphi : \mathbb{C} \to GL_m(\mathbb{C})$ un sous-groupe à 1 paramètre, c'est-à-dire un homomorphisme analytique $z \mapsto \exp(Mz)$ dont la dérivée à l'origine $M = \varphi'(0) \in M_m(\mathbb{C})$ n'est pas nulle.

Si la matrice M est nilpotente, alors

$$\varphi(z) = \sum_{\text{finie}} \frac{1}{h!} M^h z^h$$

est une fonction rationnelle, chacune des cordonnées $\varphi_{i,j}$ de φ étant un polynôme. Dans le cas général, si $\lambda_1, \ldots, \lambda_r$ sont les valeurs propres distinctes de M,

alors chaque $\varphi_{i,j}$ est un polynôme exponentiel

$$\sum_{k=1}^{r} P_k(z) e^{\lambda_k z} .$$

Notons que si λ est une valeur propre de M, et $t \in \mathbb{C}$, alors $e^{\lambda t}$ est une valeur propre de la matrice $\varphi(t)$

b) Homomorphismes analytiques de $\mathbb{C}^n$ dans $GL_m(\mathbb{C})$.

Un homomorphisme analytique de $\mathbb{C}^n$ dans $GL_m(\mathbb{C})$ n'est autre qu'une application

$$(z_1, \ldots, z_n) \mapsto \exp\left(\sum_{j=1}^{n} M_j z_j\right)$$

où les matrices $M_1, \ldots, M_n$ commutent deux-à-deux.

Un exemple de sous-groupe commutatif à 2 paramètres de $GL_3(\mathbb{C})$ de dimension algébrique 3 est

(2.1.1) $$(z_1, z_2) \mapsto \begin{pmatrix} 2^{z_1+z_2} & z_1 2^{z_1+z_2} & (z_2 + \frac{1}{2} z_1^2) 2^{z_1+z_2} \\ 0 & 2^{z_1+z_2} & z_1 2^{z_1+z_2} \\ 0 & 0 & 2^{z_1+z_2} \end{pmatrix}$$

avec

$$M_1 = \begin{pmatrix} \log 2 & 1 & 0 \\ 0 & \log 2 & 1 \\ 0 & 0 & \log 2 \end{pmatrix} , \qquad M_2 = \begin{pmatrix} \log 2 & 0 & 1 \\ 0 & \log 2 & 0 \\ 0 & 0 & \log 2 \end{pmatrix}$$

Un exemple de sous-groupe commutatif à 2 paramètres de $GL_3(\mathbb{C})$ de dimension algébrique 3 est

(2.1.2) $$\varphi(z_1, z_2) = \begin{pmatrix} 2^{z_1} & 0 & 2^{z_1} z_2 \\ 0 & 3^{z_1} & 0 \\ 0 & 0 & 2^{z_1} \end{pmatrix}$$

avec

$$M_1 = \begin{pmatrix} \log 2 & 0 & 0 \\ 0 & \log 3 & 0 \\ 0 & 0 & \log 2 \end{pmatrix} , \qquad M_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Dans chacun de ces deux exemples on peut trouver un sous-groupe Γ de $\overline{\mathbb{Q}}^2$ dont l'image par φ soit algébrique, et qui ne soit pas de rang fini :

$$\Gamma = \{ (\alpha\,,\ r-\alpha)\ ;\ \alpha \in \overline{\mathbb{Q}}\,,\ r \in \mathbb{Q} \}$$

dans le premier cas, et $\Gamma = \mathbb{Q} \times \overline{\mathbb{Q}}$ dans le deuxième.

D'autre part si $p_1, \dots, p_{m-1}$ sont des nombres premiers deux-à-deux distincts,

$$(z_1\,,\ z_2) \mapsto \operatorname{diag}(e^{z_1}\,,\ e^{z_2\sqrt{p_1}}, \dots, e^{z_2\sqrt{p_{m-1}}}) \qquad (2.1.3)$$

est un sous-groupe commutatif normalisé à 2 paramètres de $GL_m(\mathbb{C})$, de dimension algébrique m, qui prend des valeurs dans $GL_m(\overline{\mathbb{Q}})$ aux points $(\log\alpha\,,\ 0)$, α algébrique $\neq 0$.

§ 2.2 - Sous-groupes à un paramètre normalisés.

Etant donné un homomorphisme analytique φ de $\mathbb{C}$ dans $GL_m(\mathbb{C})$, on se propose d'étudier les $u \in \mathbb{C}$ tels que $\varphi(u) \in GL_m(\overline{\mathbb{Q}})$. Nous commençons par le cas où φ est normalisé : $\varphi'(0) \in M_m(\overline{\mathbb{Q}})$.

THÉORÈME 2.2.1 - Soit $\varphi : \mathbb{C} \to GL_m(\mathbb{C})$ un sous-groupe à un paramètre tel que $\varphi'(0) \in M_m(\overline{\mathbb{Q}})$. S'il existe $u \in \mathbb{C}$, $u \neq 0$ tel que $\varphi(u) \in GL_m(\overline{\mathbb{Q}})$, alors, la dimension algébrique de φ est égale à 1.

COROLLAIRE 2.2.2 - Avec les notations du théorème 2.2.1, si φ n'est pas rationnel, alors u est transcendant.

Démonstration du Corollaire 2.2.2.

On applique le théorème 2.2.1 au sous-groupe à 1 paramètre $\psi : \mathbb{C} \to GL_{m+2}(\mathbb{C})$ défini par

$$\psi(z) = \exp\left\{ \begin{pmatrix} 0 & 1 & 0\dots0 \\ 0 & 0 & 0\dots0 \\ \vdots & \vdots & \varphi'(0) \\ 0 & 0 & \end{pmatrix} z \right\}.$$

Si u était algébrique, avec $\varphi(u) \in GL_m(\overline{\mathbb{Q}})$, on aurait $\psi(u) \in GL_{m+1}(\overline{\mathbb{Q}})$, et ψ serait de dimension 1, donc φ serait une fonction rationnelle

Le corollaire 2.2.2. contient le théorème de Hermite-Lindemann 1.1.2 correspondant à $m = 1$, $\varphi(z) = e^z$, et le théorème 2.2.1 contient le théorème de Gel'fond-Schneider 1.1.3 avec $m = 2$ et

$$\varphi(z) = \begin{pmatrix} e^z & 0 \\ 0 & e^{bz} \end{pmatrix} = \exp\left\{ \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} z \right\}, \quad u = \log a$$

Inversement, nous allons déduire le théorème 2.2.1 des théorèmes de Hermite-Lindemann et Gel'fond-Schneider.

LEMME 2.2.3 - Soit $\varphi : \mathbb{C} \to GL_m(\mathbb{C})$ un sous-groupe à 1 paramètre de dimension algébrique d, et soit δ le rang du sous - $\mathbb{Z}$ - module de $\mathbb{C}$ engendré par les valeurs propres $\lambda_1, \dots, \lambda_m$ de $\varphi'(0)$. Soit Ω un sous-corps algébriquement clos de $\mathbb{C}$ contenant les coefficients de la matrice $\varphi'(0)$.

a) Si $\varphi'(0)$ est diagonalisable, on a

$$\Omega\,[\{\varphi_{i,j}(z)\}_{1\leq i,\, j\leq m}] = \Omega\,[e^{\lambda_1 z}, \dots, e^{\lambda_m z}],$$

donc $d = \delta$.

b) Si $\varphi'(0)$ n'est pas diagonalisable, on a

$$\Omega\,[\{\varphi_{i,j}(z)\}_{1\leq i,\, j\leq m}] = \Omega\,[z\,,\ e^{\lambda_1 z}, \dots, e^{\lambda_m z}],$$

donc $d = \delta + 1$.

Démonstration du lemme 2.2.3.

Si $\qquad \psi(z) = P\,.\,\varphi(z)\,P^{-1}$ avec $P \in GL_m(\Omega)$, alors

$$\Omega\,[\{\psi_{i,j}\}_{1\leq i,\, j\leq m}] = \Omega\,[\{\varphi_{i,j}\}_{1\leq i,\, j\leq m}]$$

Comme $\qquad \psi(z) = \exp\,(P\,\varphi'(0)\,P^{-1}\,z)$, on en déduit a).

Pour b), on est ramené au cas

$$\varphi'(0) = \begin{pmatrix} M_1 & 0 & \dots & 0 \\ 0 & M_2 & \dots & 0 \\ . & . & \dots & . \\ 0 & 0 & \dots & M_r \end{pmatrix}$$

avec $r < m$ et

$$M_j = \begin{pmatrix} \lambda_j & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda_j & 1 & \dots & 0 & 0 \\ . & . & . & \dots & . & . \\ 0 & 0 & 0 & \dots & \lambda_j & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda_j \end{pmatrix},$$

et alors

$$\exp(M_j z) = \begin{pmatrix} 1 & z & \frac{z^2}{2!} & \cdot & \cdot & \cdot \\ 0 & 1 & z & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdot & \cdot & 1 \end{pmatrix} \cdot e^{\lambda_j z}$$

ce qui démontre le lemme 2.2.3.

Démonstration du théorème 2.2.1.

Si φ est une fonction rationnelle sa dimension algébrique est 1 . Sinon $\varphi'(0)$ admet une valeur propre non nulle, et le lemme 2.2.3 b) joint au théorème de Hermite-Lindemann montre que $\varphi'(0)$ est diagonalisable. Alors le théorème de Gel'fond-Schneider, grâce au lemme 2.2.3 a), montre que deux valeurs propres de $\varphi'(0)$ sont $\mathbb{Q}$-linéairement dépendantes, c'est-à-dire $\delta = 1$, donc $d = 1$.

Les seuls homomorphismes irrationnels φ vérifiant les hypothèses du théorème 2.2.1 sont donc, après un changement de base à coefficients algébriques, de la forme

$$\varphi(z) = \begin{pmatrix} e^{b_1 \lambda z} & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & e^{b_2 \lambda z} & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot & e^{b_m \lambda z} \end{pmatrix}$$

avec $\lambda \in \overline{\mathbb{Q}}$, $\lambda \neq 0$, et $b_1, \ldots, b_m$ entiers rationnels non tous nuls. Les $u \in \mathbb{C}$ tels que $\varphi(u) \in GL_m(\overline{\mathbb{Q}})$ sont alors les nombres de la forme $u = \frac{1}{\lambda} \log \alpha$, $\alpha \in \overline{\mathbb{Q}}$, $\alpha \neq 0$.

§ 2.3 - Sous-groupes à un paramètre sans normalisation

Nous considérons maintenant un sous-groupe à un paramètre $\varphi : \mathbb{C} \to GL_m(\mathbb{C})$ pour lequel nous ne faisons plus d'hypothèse algébrique sur $\varphi'(0)$.

a) Points algébriques du graphe.

Il peut exister un nombre algébrique $\gamma \neq 0$ tel que $\varphi(\gamma) \in GL_m(\overline{\mathbb{Q}})$, sans que φ soit rationnel (par exemple $m = 1$, $\varphi(z) = 2^z$, $\gamma \in \mathbb{Q}$). Dans ce cas les seuls nombres algébriques possédant cette propriété sont de la forme $\frac{p}{q}\gamma$, $\frac{p}{q} \in \mathbb{Q}$.

THÉORÈME 2.3.1 - Soit $\varphi : \mathbb{C} \to GL_m(\mathbb{C})$ un sous-groupe à un paramètre non rationnel. Si γ_1, γ_2 sont deux nombres algébriques tels que $\varphi(\gamma_1) \in GL_m(\overline{\mathbb{Q}})$ et

$\varphi(\gamma_2) \in GL_m(\overline{\mathbb{Q}})$, alors γ_1, γ_2 sont $\mathbb{Q}$-linéairement dépendants.

Démonstration du théorème 2.3.1 .

Soit λ une valeur propre non nulle de $\varphi'(0)$. Alors $e^{\lambda\gamma_j}$ est une valeur propre de $\varphi(\gamma_j)$, $(j = 1, 2)$, donc le théorème 2.3.1 est une nouvelle formulation du théorème de Gel'fond-Schneider.

b) Indépendance linéaire de points algébriques.

Soit $\varphi : \mathbb{C} \to GL_m(\mathbb{C})$ un sous-groupe à un paramètre non rationnel. Soient $u_1, \ldots, u_\ell$ des nombres complexes $\mathbb{Q}$-linéairement indépendants tels que

$$\varphi(u_j) \in GL_m(\overline{\mathbb{Q}}), \quad (1 \leq j \leq \ell).$$

Alors $u_1, \ldots, u_\ell$ sont $\overline{\mathbb{Q}}$-linéairement indépendants.

Cet énoncé est une conséquence immédiate du théorème 1.1.9 de Baker.

c) Dimension algébrique.

Soient $u_1, \ldots, u_\ell$ des nombres complexes $\mathbb{Q}$-linéairement indépendants tels que

$$\varphi(u_j) \in GL_m(\overline{\mathbb{Q}}), \quad (1 \leq j \leq \ell).$$

Si on veut majorer ℓ, on doit supposer que la dimension algébrique de φ est supérieure ou égale à 2 (cf. § 2.2). On conjecture alors que $\ell \leq 1$, mais on ne connait que le résultat suivant.

THÉORÈME 2.3.2 - Soit $\varphi : \mathbb{C} \to GL_m(\mathbb{C})$ un homomorphisme analytique de dimension algébrique d, et soit Γ un sous-groupe de $\mathbb{C}$ de rang ℓ sur $\mathbb{Z}$ tel que $\varphi(\Gamma) \subset GL_m(\overline{\mathbb{Q}})$. Alors $d \geq 2 \Rightarrow \ell \leq 2$ et $d \geq 3 \Rightarrow \ell \leq 1$.

Démonstration du théorème 2.3.2.

Soient $\lambda_1, \ldots, \lambda_\delta$ des valeurs propres $\mathbb{Q}$ - linéairement indépendantes de $\varphi'(0)$. Alors

$$e^{\lambda_i \gamma} \in \overline{\mathbb{Q}} \quad \text{pour} \quad 1 \leq i \leq \delta, \ \gamma \in \Gamma,$$

et le corollaire 1.1.7 donne la majoration $\ell\delta \leq \ell + \delta$. Si $d = \delta$, c'est le résultat désiré. D'après le lemme 2.2.3 il ne reste à étudier que le cas où $\varphi'(0)$ n'est pas diagonalisable. Nous allons montrer dans ce cas $d \geq 2 \Rightarrow \ell \leq 1$ comme conséquence du théorème de Gel'fond-Schneider.

Soit f l'une des coordonnées $\varphi_{i,j}$ de φ :

$$f(z) = \sum_{s=1}^{m} \sum_{k=1}^{\nu} a_{s,k} z^{k-1} e^{\lambda_s z} .$$

Soit $u \in \Gamma$ tel que $(\lambda_s - \lambda_t) . u \notin 2i\pi\mathbb{Z}$ pour $\lambda_s \neq \lambda_t$ (un tel u existe dès que $\ell \geqq 2$). Comme $f(hu) \in \bar{\mathbb{Q}}$ pour $h \in \mathbb{Z}$, on a

$$\sum_{s=1}^{m} \sum_{k=1}^{\nu} (a_{s,k} u^{k-1}) h^{k-1} (e^{\lambda_s u})^h \in \bar{\mathbb{Q}} \quad \text{pour tout} \quad h \in \mathbb{Z} ,$$

d'où l'on déduit par un calcul de déterminant [Wa 2] (p.175)

$$a_{s,k} u^{k-1} \in \bar{\mathbb{Q}} , \qquad (1 \leqq s \leqq m, \ 1 \leqq k \leqq \nu),$$

donc

$$f(z) \in \bar{\mathbb{Q}} \left[\frac{z}{u} , e^{\lambda_1 z}, \ldots, e^{\lambda_m z} \right],$$

ce qui montre que le corps

$$\bar{\mathbb{Q}}\left(\frac{z}{u} , e^{\lambda_1 z}, \ldots, e^{\lambda_m z} \right)$$

est une extension algébrique finie du corps

$$\bar{\mathbb{Q}}(\{ \varphi_{i,j} (z) \}_{1 \leqq i, j \leqq m}).$$

Si $\ell \geqq 2$, soit $u' \in \Gamma$ avec u, u' $\mathbb{Q}$-linéairement indépendants. Alors $u'/u \in \bar{\mathbb{Q}}$, $e^{\lambda_s u} \in \bar{\mathbb{Q}}$ et $e^{\lambda_s u'} \in \bar{\mathbb{Q}}$ pour $1 \leqq s \leqq m$, et on déduit du théorème de Gel'fond-Schneider $\lambda_s = 0$, $(1 \leqq s \leqq m)$, d'où $d = 1$.

Cette démonstration montre que le problème des quatre exponentielles (cf. §1.1) s'énonce, avec les notations du théorème 2.3.2,

$$d \geqq 2 \Rightarrow \ell \leqq 1 .$$

§ 2.4 - Sous-groupes commutatifs à plusieurs paramètres normalisés.

Quand on étudie les homomorphismes analytiques

$$\varphi : \mathbb{C}^n \to GL_m(\mathbb{C})$$

$$z \mapsto \exp\left(\sum_{j=1}^{n} M_j z_j\right)$$

normalisés : $M_j \in M_m(\bar{\mathbb{Q}})$, $(1 \leqq j \leqq n)$, on se ramène au cas de sous-groupes commutatifs à n paramètres de la manière suivante : si, disons, $M_1, \ldots, M_\nu$ sont $\bar{\mathbb{Q}}$-linéairement indépendants, et

$$M_j = \sum_{s=1}^{\nu} \beta_{j,s} M_s , \quad (1 \leqq j \leqq n),$$

alors $\varphi = \psi \circ \mathcal{L}$ où $\mathcal{L} : \mathbb{C}^n \to \mathbb{C}^\nu$ est l'application linéaire définie par

$$\mathcal{L}(z_1, \ldots, z_n) = \left(\sum_{j=1}^{n} \beta_{j,s} z_j \right)_{1 \leqq s \leqq \nu}$$

et ψ est un sous-groupe à ν paramètres de $GL_m(\mathbb{C})$:

$$\psi(t_1, \ldots, t_\nu) = \exp\left(\sum_{s=1}^{\nu} M_s t_s \right).$$

D'autre part, si φ est normalisé, et si $\gamma \in \bar{\mathbb{Q}}^n$, $\gamma \neq 0$, le sous-groupe à 1 paramètre $z \mapsto \varphi(\gamma z)$ est rationnel si et seulement si $\varphi(\gamma) \in GL_m(\bar{\mathbb{Q}})$ (cf. 2.2.2). Comme l'ensemble $\{ v \in \mathbb{C}^n$; $\varphi(v z)$ est une fonction rationnelle de $z \}$ est un sous-espace vectoriel de $\mathbb{C}^n$, et que pour $v \in \bar{\mathbb{Q}}^n$ dans ce sous-espace les coordonnées $\varphi_{i,j}(v z)$ sont des polynômes en z (à coefficients algébriques puisque $M_j \in M_m(\bar{\mathbb{Q}})$, autrement dit $\varphi(v z)$ est rationnelle sur $\bar{\mathbb{Q}}$), il est naturel de se placer sur un supplémentaire de ce sous-espace, autrement dit de supposer que pour tout $v \in \mathbb{C}^n$, $v \neq 0$, le sous-groupe à 1 paramètre $z \mapsto \varphi(vz)$ n'est pas rationnel.

a) Transcendance des coordonnées de points algébriques.

Un point $u \in \mathbb{C}^n$ est un point algébrique de φ si $\varphi(u) \in GL_m(\bar{\mathbb{Q}})$. Nous montrons que les coordonnées d'un tel point sont nulles ou transcendantes. Un exemple typique est le suivant :

$$\varphi(z_1 , z_2) = \begin{pmatrix} e^{z_1 + \sqrt{2} z_2} & 0 \\ 0 & e^{z_2} \end{pmatrix}$$

avec

$$u = (\log 2 , 0)$$

ou bien

$$u = (\log 2 - \sqrt{2} \log 3 , \ \log 3).$$

THÉORÈME 2.4.1.- Soit $\varphi : \mathbb{C}^n \to GL_m(\mathbb{C})$ un sous-groupe commutatif à n paramètres tel que, pour tout $v \in \mathbb{C}^n$, $v \neq 0$, le sous-groupe à 1 paramètre $z \mapsto \varphi(v z)$ ne soit pas rationnel. On suppose φ normalisé au sens où

$$M_j = \frac{\partial}{\partial z_j} \varphi(0) \in M_m(\bar{\mathbb{Q}}) , \qquad (1 \leqq j \leqq n).$$

Si $u \in \mathbb{C}^n$ est tel que $\varphi(u) \in GL_m(\bar{\mathbb{Q}})$, alors toute combinaison linéaire à coefficients algébriques des coordonnées de u est nulle ou transcendante.

Démonstration du théorème 2.4.1

Comme les matrices M_j commutent deux à deux, il existe $P \in GL_m(\bar{\mathbb{Q}})$ telle que

$$P M_j P^{-1} = \begin{pmatrix} \lambda_{j,1} & & * \\ & \ddots & \\ 0 & & \lambda_{j,m} \end{pmatrix}, \quad (1 \le j \le n)$$

Comme $\varphi(u) \in GL_m(\bar{\mathbb{Q}})$, pour $1 \le s \le m$ il existe un nombre algébrique non nul α_s et une détermination de son logarithme tels que, si $u = (u_1, \dots, u_n)$,

$$\sum_{j=1}^{n} \lambda_{j,s} u_j = \log \alpha_s \qquad (1 \le s \le m)$$

L'hypothèse sur l'irrationalité de φ signifie que la matrice $(\lambda_{j,s})_{1 \le j \le n,\, 1 \le s \le m}$ a pour rang n. Il existe donc des nombres algébriques $\beta_{j,s}$, $(1 \le j \le n, 1 \le s \le m)$ tels que

$$u_j = \sum_{s=1}^{m} \beta_{j,s} \log \alpha_j, \qquad (1 \le j \le n).$$

Le théorème 2.4.1 est donc une conséquence du théorème 1.1.9 de Baker.

b) Indépendance linéaire de points algébriques.

On note $e_1, \dots, e_n$ la base canonique de $\mathbb{C}^n$.

THÉORÈME 2.4.2 - Soit $\varphi : \mathbb{C}^n \to GL_m(\mathbb{C})$ un sous-groupe commutatif à n paramètres, avec $\frac{\partial}{\partial z_j} \varphi(0) \in M_m(\bar{\mathbb{Q}})$, tel que, pour tout $v \in \mathbb{C}^n$, $v \ne 0$, le sous-groupe à un paramètre $z \mapsto \varphi(vz)$ soit irrationnel.

Soient $u_1, \dots, u_\ell$ des éléments $\mathbb{Q}$-linéairement indépendants de $\mathbb{C}^n$ tels que $\varphi(u_s) \in GL_m(\bar{\mathbb{Q}})$, $(1 \le s \le \ell)$. Alors $e_1, \dots, e_n, u_1, \dots, u_\ell$ sont $\bar{\mathbb{Q}}$-linéairement indépendants.

Le cas $m = n = 1$, $\varphi(z) = e^z$ est le théorème 1.1.9. de Baker. Le cas général va s'en déduire, grâce aux lemmes suivants.

LEMME 2.4.3. - Soient $B_1, \dots, B_\ell \in M_m(\mathbb{C})$ des matrices commutant deux à deux, telles que $\exp(B_s) \in GL_m(\bar{\mathbb{Q}})$, $(1 \le s \le \ell)$. S'il existe des nombres algébriques

$\beta_1, \dots, \beta_\ell$, non tous nuls, tels que

$$\beta_1 B_1 + \dots + \beta_\ell B_\ell \in M_m(\bar{\mathbb{Q}}),$$

alors il existe des entiers rationnels $b_1, \dots, b_\ell$, non tous nuls, tels que la matrice $b_1 B_1 + \dots + b_\ell B_\ell$ soit nilpotente.

Démonstration du lemme 2.4.3.

On peut évidemment supposer $\beta_1 = 1$

On démontre le lemme par récurrence sur ℓ. Pour $\ell = 1$, le lemme signifie que si $B \in M_m(\bar{\mathbb{Q}})$ vérifie $\exp(B) \in GL_m(\bar{\mathbb{Q}})$, alors B est nilpotente. C'est le théorème de Hermite-Lindemann sous la forme 2.2.2.

Supposons le résultat démontré pour $\ell - 1$. Si l'une des matrices $B_1, \dots, B_\ell$ est nilpotente, le résultat est banal. Sinon il existe des valeurs propres $\lambda_1, \dots, \lambda_\ell$ simultanées de $B_1, \dots, B_\ell$ et non toutes nulles. Alors $\beta_1 \lambda_1 + \dots + \beta_\ell \lambda_\ell$ est une valeur propre de $\beta_1 B_1 + \dots + \beta_\ell B_\ell$, donc

$$e^{\beta_1 \lambda_1 + \dots + \beta_\ell \lambda_\ell} \in \bar{\mathbb{Q}}$$

Comme $e^{\lambda_s} \in \bar{\mathbb{Q}}$, $(1 \le s \le \ell)$, et comme $\beta_1 = 1$, on déduit du théorème de Baker sous la forme 2.4.4 l'existence d'entiers rationnels $b_1, \dots, b_\ell$, non tous nuls, tels que

$$b_1 \beta_1 + \dots + b_\ell \beta_\ell = 0 .$$

Disons par exemple $b_\ell \ne 0$. Alors

$$b_\ell \sum_{j=1}^{\ell} \beta_j B_j = \sum_{j=1}^{\ell-1} \beta_j (b_\ell B_j - b_j B_\ell) \qquad \text{appartient à } M_m(\bar{\mathbb{Q}}),$$

et comme

$$\exp(b_\ell B_j - b_j B_\ell) \in GL_m(\bar{\mathbb{Q}}),$$

on peut appliquer l'hypothèse de récurrence.

Nous avons utilisé le théorème 1.1.9 de Baker sous la forme suivante

LEMME 2.4.4. - Soient $\beta_{i,j}$, $(1 \le i \le h, 1 \le j \le k)$ des nombres algébriques, et $\alpha_1, \dots, \alpha_k$ des nombres algébriques non nuls. Pour $1 \le j \le k$, soit $\log \alpha_j$ une détermination non nulle du logarithme de α_j. On suppose

$$\sum_{j=1}^{k} \beta_{i,j} \log \alpha_j = 0, \qquad (1 \leq i \leq h).$$

<u>Alors il existe des entiers rationnels</u> $b_1, \ldots, b_k$, <u>non tous nuls</u>, <u>tels que</u>

$$\sum_{j=1}^{k} \beta_{i,j} b_j = 0, \qquad (1 \leq i \leq h).$$

En vue d'une application au chapitre 6 (cf. 6.3.3), nous déduisons cet énoncé du théorème 1.1.9 à l'aide du lemme suivant.

LEMME 2.4.5. - <u>Soient</u> D <u>un corps commutatif ou gauche</u>, A_1 <u>et</u> A_2 <u>deux sous-anneaux de</u> D, <u>avec</u> $A_1 \subset A_2$, <u>et</u> L <u>un sous-ensemble d'un</u> A_2 <u>module qui est un</u> A_1 - <u>module libre de rang fini tel que toute famille d'éléments de</u> L <u>libre sur</u> A_1 <u>soit aussi libre sur</u> A_2. <u>Soient</u> $\lambda_1, \ldots, \lambda_k$ <u>des éléments non nuls de</u> L, <u>et</u> $\beta_{i,j}$, $(1 \leq i \leq h,\ 1 \leq j \leq k)$ <u>des éléments de</u> A_2, <u>tels que</u>

$$\sum_{j=1}^{k} \beta_{i,j} \lambda_j = 0, \qquad (1 \leq i \leq h).$$

<u>Alors il existe des éléments</u> $b_1, \ldots, b_k$ <u>de</u> A_1, <u>non tous nuls</u>, <u>tels que</u>

$$\sum_{j=1}^{k} \beta_{i,j} b_j = 0, \qquad (1 \leq i \leq h).$$

Le lemme 2.4.4 correspond à $A_1 = \mathbf{Z}$, $A_2 = \overline{\mathbf{Q}}$, et L est le $\mathbf{Z}$-module engendré par $\lambda_j = \log \alpha_j$, $(1 \leq j \leq k)$. L'hypothèse sur l'indépendance linéaire est vérifiée par le théorème de Baker.

<u>Démonstration du lemme</u> 2.4.5.

Il n'y a pas de restriction à supposer que $\lambda_1, \ldots, \lambda_k$ engendrent le A_1-module L. Soit D_1 le corps des quotients de A_1, et $\lambda'_1, \ldots, \lambda'_r$ une base sur D_1 de $L \otimes_{A_1} D_1$:

$$m_j \lambda_j = \sum_{s=1}^{r} m_{j,s} \lambda'_s, \qquad (1 \leq j \leq k),$$

avec $m_j \in A_1$, $m_j \neq 0$, et $m_{j,s} \in A_1$ $(1 \leq j \leq k,\ 1 \leq s \leq r)$.

Donc

$$\sum_{j=1}^{k} \sum_{s=1}^{r} \beta_{i,j} \frac{m_{j,s}}{m_j} \lambda'_s = 0, \qquad (1 \leq i \leq h).$$

Comme par l'hypothèse $\lambda'_1, \ldots, \lambda'_r$ sont A_2-linéairement indépendants, on en déduit

$$\sum_{j=1}^{k} \beta_{i,j} \frac{m_{j,s}}{m_j} = 0, \qquad (1 \leq i \leq h,\ 1 \leq s \leq r).$$

On pose enfin

$$b_j = m_1 \cdots m_k \cdot m_{j,s} / m_j, \qquad (1 \leq j \leq k)$$

où s est choisi de telle manière que $m_{1,s}, \ldots, m_{k,s}$ ne soient pas tous nuls.

<u>Démonstration du théorème</u> 2.4.2.

Notons $u_s = (u_{s,j})_{1 \leq j \leq n}$, $(1 \leq s \leq \ell)$. Supposons

$$\beta_1 u_1 + \cdots + \beta_\ell u_\ell = \gamma$$

avec $\beta_1, \ldots, \beta_\ell$ nombres algébriques non tous nuls, et $\gamma = (\gamma_1, \ldots, \gamma_n) \in \overline{\mathbf{Q}}^n$. Alors, en posant

$$B_s = \sum_{j=1}^{n} M_j u_{s,j}, \qquad (1 \leq s \leq \ell),$$

on a

$$\sum_{s=1}^{\ell} \beta_s B_s = \sum_{j=1}^{n} \gamma_j M_j \in M_m(\overline{\mathbf{Q}}),$$

et le lemme 2.4.3 montre qu'il existe des nombres rationnels non tous nuls $b_1, \ldots, b_\ell$ tels que $\sum_{s=1}^{\ell} b_s B_s$ soit nilpotente. L'hypothèse sur l'irrationalité de φ implique

$$\sum_{s=1}^{\ell} b_s u_{s,j} = 0, \qquad (1 \leq j \leq n),$$

c'est-à-dire

$$b_1 u_1 + \cdots + b_\ell u_\ell = 0.$$

c) <u>Dimension algébrique</u>.

Il est facile de construire (cf. (2.1.3)) un sous-groupe commutatif à n paramètres normalisé $\varphi : \mathbf{C}^n \to GL_m(\mathbf{C})$, de dimension algébrique quelconque $\geq n$, qui prenne des valeurs dans $GL_m(\overline{\mathbf{Q}})$ en $n-1$ points $\mathbf{C}$-linéairement indépendants de $\mathbf{C}^n$. Mais on ne peut pas en faire autant avec n points $\mathbf{C}$-linéairement indépendants.

THÉORÈME 2.4.6. - *Soit* $\varphi : \mathbb{C}^n \to GL_m(\mathbb{C})$ *un homomorphisme analytique normalisé. S'il existe* n *points* $\mathbb{C}$*-linéairement indépendants de* $\mathbb{C}^n$ *dont l'image par* φ *soit dans* $GL_m(\overline{\mathbb{Q}})$*, alors la dimension algébrique de* φ *est inférieure ou égale à* n

Nous avons vu que le cas $n = 1$ (théorème 2.2.1) était équivalent aux théorèmes 1.1.2 et 1.1.3 de Hermite-Lindemann et Gel'fond-Schneider. Pour démontrer le cas général il faut utiliser le théorème de Baker.

La dimension algébrique de φ se détermine à partir de l'énoncé suivant. Pour

$$x = (x_1, \dots, x_n) \in \mathbb{C}^n \quad \text{et} \quad y = (y_1, \dots, y_n) \in \mathbb{C}^n,$$

on note
$$< x , y > = \sum_{s=1}^{n} x_s y_s .$$

LEMME 2.4.7. - *Soient* $x_1, \dots, x_h$ *des éléments de* $\mathbb{C}^n$*. Les fonctions entières de* n *variables complexes* $z = (z_1, \dots, z_n)$

$$z_1, \dots, z_n, \; e^{<x_1, z>}, \dots, e^{<x_h, z>}$$

engendrent une extension de $\mathbb{C}$ *dont le degré de transcendance est* $n + r$*, où* r *est le rang sur* $\mathbb{Z}$ *de* $\mathbb{Z} x_1 + \dots + \mathbb{Z} x_h$.

Démonstration du lemme 2.4.7.

On se ramène facilement à montrer que si $w_1, \dots, w_q$ sont des éléments deux-à-deux distincts de $\mathbb{C}^n$, et $P_1, \dots, P_q$ des polynômes non nuls de $\mathbb{C}[z] = \mathbb{C}[z_1, \dots, z_n]$, la fonction

$$F(z) = \sum_{k=1}^{q} P_k(z) \, e^{<w_k, z>}$$

n'est pas identiquement nulle.

On démontre ce résultat par récurrence sur n. Le cas $n = 1$ est facile (par récurrence sur q ; cf [Wa 2] (1.4.2)). Soit $z' = (z_1, \dots, z_{n-1}) \in \mathbb{C}^{n-1}$. Notons $Q_k \in \mathbb{C}[z_n]$ les polynômes

$$Q_k(z_n) = P_k(z', z_n), \qquad (1 \leq k \leq q).$$

Notons de même $w_k = (w'_k, w_{k,n})$, et soit $\{v_1, \dots, v_t\}$ l'ensemble des valeurs distinctes de $w_{k,n}$ $(1 \leq h \leq q)$. On a

$$F(z) = \sum_{j=1}^{t} \left(\sum_{k} Q_k(z_n) \, e^{<w'_k, z'>} \right) e^{v_j z_n} ,$$

où la deuxième somme est étendue aux k tels que $w_{k,n} = v_j$. Si $F = 0$, le résultat en une variable montre que chacun des polynômes en z_n

$$\sum_k Q_k(z_n) \, e^{<w'_t, z'>}$$

est identiquement nul. Dans une telle somme, les w'_k sont deux-à-deux distincts. En faisant varier z', on en déduit que les polynômes P_k sont identiquement nuls, grâce à l'hypothèse de récurrence.

Le lemme 2.4.7 permet de ramener la démonstration du théorème 2.4.6 à celle de l'énoncé suivant.

PROPOSITION 2.4.8. - *Soient* h *un entier,* $1 \leq h \leq n+1$, $\beta_1, \dots, \beta_h$ *des éléments* $\mathbb{Q}$*-linéairement indépendants de* $\overline{\mathbb{Q}}^n$ *, et* $u_1, \dots, u_n$ *des éléments* $\mathbb{C}$*-linéairement indépendants de* $\mathbb{C}^n$ *. Pour* $1 \leq j \leq n$, *on note* $u_j = (u_{j,s})_{1 \leq s \leq n}$ *. On suppose que les nombres*

$$u_{j,s} , \quad (1 \leq j \leq n , \; 1 \leq s \leq n - h + 1)$$

sont algébriques. Alors l'un au moins des nombres

$$e^{<\beta_i , u_j>}, \qquad (1 \leq i \leq h , 1 \leq j \leq n)$$

est transcendant.

Cela revient à dire que les $n + 1$ fonctions

$$z_1, \dots, z_{n-h+1} , \; e^{<\beta_1 , z>}, \dots, e^{<\beta_h , z>}$$

ne peuvent prendre simultanément des valeurs algébriques en n points $\mathbb{C}$-linéairement indépendants de $\mathbb{C}^n$.

Démonstration de la proposition 2.4.8.

Supposons les nombres $e^{<\beta_i , u_j>}$ tous algébriques. Notons $k = n - h + 1$, et soit $e_1, \dots, e_n$ la base canonique de $\mathbb{C}^n$. On se ramène facilement (par changement de base définie sur $\overline{\mathbb{Q}}$ et par récurrence sur n) au cas où $\beta_i = e_{k+i}$, $(1 \leq i \leq h - 1)$, et où les coordonnées $(\gamma_1, \dots, \gamma_n)$ de β_h sont telles que

$1, \gamma_{k+1}, \dots, \gamma_r$ soit une base sur $\mathbb{Q}$ du $\mathbb{Q}$-espace vectoriel engendré par $1, \gamma_{k+1}, \dots, \gamma_n$, avec $k+1 \leq r \leq n$.

Pour $1 \leq j \leq n$, soient $\alpha_{j,\ell}$, $(1 \leq \ell \leq n)$ et θ_j des nombres algébriques tels que

$$u_{j,s} = \alpha_{j,s}, \qquad (1 \leq s \leq k),$$

$$u_{j,t} = \log \alpha_{j,t}, \qquad (k+1 \leq t \leq n),$$

$$\sum_{s=1}^{k} \gamma_s \alpha_{j,s} + \sum_{t=k+1}^{n} \gamma_t \log \alpha_{j,t} = \log \theta_j .$$

De plus, soient $c_{t,i}$, $(0 \leq i \leq r, k+1 \leq t \leq n)$ des nombres rationnels tels que

$$\gamma_t = c_{t,0} + \sum_{i=k+1}^{r} c_{t,i} \gamma_i, \qquad (k+1 \leq t \leq n).$$

Alors, pour $1 \leq j \leq n$, on a

$$\sum_{i=k+1}^{r} \gamma_i \sum_{t=k+1}^{n} c_{t,i} \log \alpha_{j,t} = \log \theta_j - \sum_{t=k+1}^{n} c_{t,0} \log \alpha_{j,t} - \sum_{s=1}^{k} \gamma_s \alpha_{j,s} .$$

On utilise maintenant le théorème de Baker : sous la forme 1.1.9, il donne d'abord

$$\sum_{s=1}^{k} \gamma_s \alpha_{j,s} = 0, \qquad (1 \leq j \leq n).$$

Ensuite, grâce à 2.4.4 et à l'indépendance linéaire sur $\mathbb{Q}$ de $1, \gamma_{k+1}, \dots, \gamma_r$, on a

$$\sum_{t=k+1}^{n} c_{t,i} \log \alpha_{j,t} = 0, \qquad (k+1 \leq i \leq r, 1 \leq j \leq n).$$

Comme $r \geq k+1$, la matrice $(\log \alpha_{j,t})_{1 \leq j \leq n,\ k+1 \leq t \leq n}$ a un rang $< n-k$, donc $u_1, \dots, u_n$ sont $\mathbb{C}$-linéairement dépendants.

REMARQUE - Le théorème 2.4.6 [L 2] chap. IV § 4 Th.2. est plus ancien que le théorème de Baker. Mais il contient plus d'informations que les théorèmes de Hermite-Lindemann et Gel'fond-Schneider, puisqu'il entraîne, par exemple, la transcendance de l'un au moins des 2 nombres

$$2^{\sqrt{2}} 3^{\sqrt{3}}, \quad 5^{\sqrt{2}} 7^{\sqrt{3}}.$$

et plus généralement de l'un des nombres

$$\prod_{i=1}^{n} \alpha_{i,j}^{\beta_i}, \qquad (1 \leq j \leq n),$$

quand $1, \beta_1, \dots, \beta_n$ sont $\mathbb{Q}$-linéairement indépendants et

$$\det(\log \alpha_{ij}) \neq 0 .$$

§ 2.5 - Homomorphismes analytiques de $\mathbb{C}^n$ dans $GL_m(\mathbb{C})$.

Nous étudions maintenant la généralisation à plusieurs variables des résultats du § 2.3.

Soit $\varphi : \mathbb{C}^n \to GL_m(\mathbb{C})$ un homomorphisme analytique,

$$\varphi(z_1, \dots, z_n) = \exp\Big(\sum_{j=1}^{n} M_j z_j\Big).$$

La seule hypothèse que nous faisons sur les matrices $M_1, \dots, M_n$ est qu'elles ne sont pas toutes nilpotentes (et bien sûr qu'elles commutent deux à deux).

Un exemple de cette situation est donnée par le cas $m = 1$:

$$\varphi : \mathbb{C}^n \to \mathbb{C}^*$$

$$(z_1, \dots, z_n) \mapsto e^{\lambda_1 z_1 + \dots + \lambda_n z_n},$$

où $\lambda_1, \dots, \lambda_n$ sont des nombres complexes non tous nuls.

a) Points algébriques du graphe.

On souhaite majorer le nombre de $\gamma \in \overline{\mathbb{Q}}^n$, $\mathbb{Q}$-linéairement indépendants, tels que $\varphi(\gamma) \in GL_m(\overline{\mathbb{Q}})$. Les deux exemples (2.1.1) et (2.1.2) montrent qu'il faut imposer une hypothèse supplémentaire.

L'hypothèse la plus naturelle concerne l'irrationalité de φ. S'il existe $\gamma \in \overline{\mathbb{Q}}$, $\gamma \neq 0$, tel que $\varphi(\gamma.z)$ soit une fonction rationnelle de z, définie sur $\overline{\mathbb{Q}}$, alors $\varphi(\gamma.\alpha) \in GL_m(\overline{\mathbb{Q}})$ pour tout $\alpha \in \overline{\mathbb{Q}}$.

THÉORÈME 2.5.1 - Soit $\varphi : \mathbb{C}^n \to GL_m(\mathbb{C})$ un homomorphisme analytique. Soit Γ un sous-groupe de $\overline{\mathbb{Q}}^n$, de type fini et de rang ℓ sur $\mathbb{Z}$. On suppose que pour tout $\gamma \in \Gamma$, $\gamma \neq 0$, le sous-groupe à un paramètre $z \mapsto \varphi(\gamma z)$ n'est pas rationnel. Si $\varphi(\Gamma) \subset GL_m(\overline{\mathbb{Q}})$, alors $\ell \leq n$.

On en déduit par récurrence sur n que des éléments $\mathbb{Q}$-linéairement indépendants de Γ sont aussi $\mathbb{C}$-linéairement indépendants.

Pour arriver à ce résultat, nous passerons par un énoncé dans lequel on suppose seulement φ irrationnel. Comme nous l'avons vu, la conclusion ne peut pas être une majoration de ℓ. Ce sera seulement une majoration du nombre $\mu(\Gamma, \mathbb{C}^n)$ tel qu'il a été défini au § 1.3.

PROPOSITION 2.5.2. - *Soit* $\varphi : \mathbb{C}^n \to GL_m(\mathbb{C})$ *un homomorphisme analytique non rationnel. Soit* Γ *un sous-groupe de* $\overline{\mathbb{Q}}^n$ *de type fini tel que* $\varphi(\Gamma) \subset GL_m(\overline{\mathbb{Q}})$. *Alors* $\mu(\Gamma, \mathbb{C}^n) \leq 1$.

Démonstration de la proposition 2.5.2.

Supposons $\mu(\Gamma, \mathbb{C}^n) \geq 1$. On considère une base $\gamma_1, \dots, \gamma_\ell$ de Γ sur $\mathbb{Z}$ avec $\gamma_1, \dots, \gamma_n$ $\mathbb{C}$-linéairement indépendants. Notons $(\beta_{s,j})_{1 \leq j \leq n}$ les coordonnées de γ_s dans la base $\gamma_1, \dots, \gamma_n$:

$$\gamma_s = \sum_{j=1}^{n} \beta_{s,j} \gamma_j, \qquad (1 \leq s \leq \ell).$$

Soit $\lambda = (\lambda_1, \dots, \lambda_n) \in \mathbb{C}^n$ une valeur propre simultanée de $M_1, \dots, M_n$, avec $\lambda \neq 0$. Ecrivons $\langle \lambda, \gamma_s \rangle$ le produit scalaire de λ et γ_s, $(1 \leq s \leq \ell)$. Alors les nombres

$$\exp(\langle \lambda, \gamma_s \rangle) = \alpha_s, \qquad (1 \leq s \leq \ell)$$

sont algébriques, et si on pose $\log \alpha_s = \langle \lambda, \gamma_s \rangle$, on a

$$\log \alpha_s = \sum_{j=1}^{n} \beta_{s,j} \log \alpha_j, \qquad (1 \leq s \leq \ell)$$

Le lemme 2.4.4. montre l'existence d'entiers rationnels $b_1, \dots, b_\ell$, non tous nuls, tels que

$$b_s = \sum_{j=1}^{n} \beta_{s,j} b_j, \qquad (1 \leq s \leq \ell).$$

Soit $p : \mathbb{C}^n \to \mathbb{C}$ l'application $\mathbb{C}$-linéaire définie par

$$p(\gamma_j) = b_j, \qquad (1 \leq j \leq n)$$

On a évidemment

$$p(\gamma_s) = b_s, \qquad (1 \leq s \leq \ell)$$

donc $\mathrm{rang}_{\mathbb{Z}}\, p(\Gamma) = 1$, $\mathrm{rang}\, p = 1$, et, en posant $W = \ker p$, on voit que $\mu(\Gamma, \mathbb{C}^n) = 1$.

Démonstration du théorème 2.5.1.

Si $n = 1$, l'énoncé est équivalent au théorème 2.3.1. (c'est aussi une conséquence de la proposition 2.5.2).

On démontre le théorème par récurrence sur n. Si Γ ne contient pas n éléments $\mathbb{C}$-linéairement indépendants, le résultat est une conséquence de l'hypothèse de récurrence appliqué à la restriction de φ au $\mathbb{C}$-espace vectoriel engendré par Γ. Si Γ contient n éléments $\mathbb{C}$-linéairement indépendants, et s'il n'est pas bien réparti dans $\mathbb{C}^n$, il contient d'après la proposition 1.3.1 un sous-groupe Γ' qui est bien réparti dans le $\mathbb{C}$ - espace vectoriel $\overline{\Gamma}'$ qu'il engendre, et

$$\mu(\Gamma', \overline{\Gamma}') \geq \frac{1}{n} \mathrm{rang}_{\mathbb{Z}}\, \Gamma > 1 \; ;$$

La restriction de φ à $\overline{\Gamma}'$ contredit alors la proposition 2.5.2.

b) Dimension algébrique

Soit $\varphi : \mathbb{C}^n \to GL_m(\mathbb{C})$ un homomorphisme analytique. Sous des hypothèses raisonnables concernant l'irrationalité et la dimension algébrique de φ, on voudrait majorer le rang des sous-groupes Γ de $\mathbb{C}^n$ tels que $\varphi(\Gamma) \subset GL_m(\overline{\mathbb{Q}})$. Nous verrons au § 8.2 les quelques résultats partiels que l'on connait sur ce sujet. Nous donnons ici seulement un exemple (cf(2.1.3)). Soient $\Lambda = \mathbb{Z}\lambda_1 + \dots + \mathbb{Z}\lambda_m$ et $\Gamma = \mathbb{Z}\gamma_1 + \dots + \mathbb{Z}\gamma_\ell$ deux sous-groupes de type fini de $\mathbb{C}^n$, de rang m et ℓ respectivement. On considère le sous-groupe à n paramètres

$$\varphi : \mathbb{C}^n \to GL_m(\mathbb{C})$$

$$z \mapsto \mathrm{diag}\left(e^{\langle \lambda_1, z \rangle}, \dots, e^{\langle \lambda_m, z \rangle}\right),$$

dont la dimension algébrique est m. On suppose $\varphi(\Gamma) \subset GL_m(\overline{\mathbb{Q}})$.

Le problème posé peut alors être formulé des deux manières équivalentes suivantes

a) Majorer $\mu(\Gamma, \mathbb{C}^n)$ en fonction de m.

b) Majorer $\mu(\Lambda, \mathbb{C}^n)$ en fonction de ℓ.

On notera que $\mu(\Lambda, \mathbb{C}^n)$ est le plus grand des nombres rationnels $\delta \geq 0$ tels que, pour tout sous-espace vectoriel V de $\mathbb{C}^n$, la restriction de φ à V ait une dimension algébrique $\geq \delta \dim_{\mathbb{C}} V$.

Supposons $m = n+1$, $\mu(\Lambda, \mathbb{C}^n) = 1 + \frac{1}{n}$. On obtient alors des nombres algébriques non nuls $\alpha_{j,s}$, $(1 \leq j \leq \ell,\ 1 \leq s \leq n+1)$, et, pour $1 \leq j \leq \ell$, $1 \leq s \leq n+1$, une détermination du logarithme de $\alpha_{j,s}$, avec

$$\sum_{s=1}^{n} x_s \log \alpha_{j,s} = \log \alpha_{j,n+1}, \qquad (1 \leq j \leq \ell)$$

où $1, x_1, \ldots, x_n$ sont $\mathbb{Q}$-linéairement indépendants dans $\mathbb{C}$, et les ℓ points

$$(\log \alpha_{j,1}, \ldots, \log \alpha_{j,n}), \qquad (1 \leq j \leq \ell)$$

sont $\mathbb{Q}$-linéairement indépendants dans $\mathbb{C}^n$.

On est donc amené à minorer le rang de matrices dont les coefficients sont des logarithmes de nombres algébriques. Ce problème important (également en p-adique) n'est toujours pas résolu.

CHAPITRE 3

SOUS-GROUPES À UN PARAMÈTRE NORMALISÉS.

Cartier avait conjecturé que le théorème de Hermite-Lindemann devait pouvoir être généralisé aux variétés de groupe. Cette conjecture a été résolue en 1962 par S Lang :

Soit G un groupe algébrique commutatif défini sur $\overline{\mathbb{Q}}$, et soit α un élément algébrique non nul de l'espace tangent à l'origine, tel que $z \mapsto \exp(\alpha z)$ ne soit pas une fonction rationnelle. Alors $\exp(\alpha) \notin G_{\overline{\mathbb{Q}}}$.

Dans son livre sur les nombres transcendants, [L 2] (Chap. 3), Lang donne une généralisation semblable du théorème de Gel'fond-Schneider : s'il existe $t \in \mathbb{C}$, $t \neq 0$, tel que $\exp(\alpha t) \in G_{\overline{\mathbb{Q}}}$, alors le sous-groupe à 1 paramètre $z \mapsto \exp(\alpha z)$ a pour dimension algébrique 1. Il énonce ce résultat avec l'hypothèse supplémentaire que l'application exponentielle de G peut être représentée par des fonctions méromorphes d'ordre fini, mais Serre montre en appendice (Appendice II § 3) qu'une telle représentation existe toujours, avec des fonctions d'ordre ≤ 2.

Nous donnons d'abord les énoncés sur les groupes algébriques, puis nous en déduisons les conséquences sur les fonctions $\wp$, ζ et σ de Weierstrass (§ 3.2), et sur les intégrales elliptiques (§ 3.3). Le théorème principal 3.1.1 de ce chapitre est démontré au § 3.4.

Nous complétons ce chapitre par quelques énoncés sur l'indépendance linéaire et algébrique de périodes et quasi-périodes, dus à Masser, Chudnovsky et Laurent.

§ 3.1 - Enoncés des principaux résultats.

Les résultats de ce chapitre découlent tous de l'énoncé suivant

THÉORÈME 3.1.1 - Soit G un groupe algébrique commutatif connexe défini sur le corps $\overline{\mathbb{Q}}$. Soit $\varphi : \mathbb{C} \to G_{\mathbb{C}}$ un sous-groupe à un paramètre, normalisé pour avoir une dérivée algébrique à l'origine. S'il existe $t \in \mathbb{C}$, $t \neq 0$, tel que $\varphi(t) \in G_{\overline{\mathbb{Q}}}$, alors la dimension algébrique de φ est 1, donc $\varphi(\mathbb{C})$ est un sous-groupe algébrique fermé de dimension 1 de $G_{\mathbb{C}}$.

Nous démontrerons ce théorème au § 3.4. En voici quelques conséquences (cf. [L2] Chap.III et [L3] §4).

Si on considère un sous-groupe à 1 paramètre φ et que l'on applique le théorème 3.1.1 au sous-groupe à 1 paramètre $\Psi : \mathbf{C} \to \mathbf{C} \times G_{\mathbf{C}}$ de $G_a \times G$ défini par $\Psi(z) = (z , \varphi(z))$, on obtient le corollaire suivant.

COROLLAIRE 3.1.2 - Avec les notations du théorème 3.1.1, si $\varphi(z)$ n'est pas une fonction rationnelle de z, alors t est transcendant.

Dans le cas d'un groupe linéaire, on retrouve le théorème 2.2.1. et son corollaire 2.2.2. Dans le cas d'une variété abélienne, les deux énoncés précédents s'écrivent de la manière suivante.

COROLLAIRE 3.1.3 - Soient A une variété abélienne définie sur $\overline{\mathbf{Q}}$, et $\Theta : \mathbf{C}^g \to A_{\mathbf{C}}$ un homomorphisme thêta normalisé. Soit $\alpha \in \overline{\mathbf{Q}}^g$, $\alpha \neq 0$. S'il existe $t \in \mathbf{C}$, $t \neq 0$, tel que $\Theta(\alpha t) \in A_{\overline{\mathbf{Q}}}$, alors t est transcendant, et l'image du sous-groupe à 1 paramètre $z \to \Theta(\alpha z)$ est une courbe elliptique.

Le fait que t soit transcendant donne un résultat intéressant sur les points algébriques de Θ.

COROLLAIRE 3.1.4 - Soient A une variété abélienne définie sur $\overline{\mathbf{Q}}$, $\Theta : \mathbf{C}^g \to A_{\mathbf{C}}$ un homomorphisme thêta normalisé, et $u \neq 0$ un point algébrique de Θ. Alors l'une au moins des coordonnées de u est transcendante.

Autrement dit $e_1, \ldots, e_g$, u sont $\overline{\mathbf{Q}}$-linéairement indépendants, $(e_1, \ldots, e_g)$ désignant la base canonique de $\mathbf{C}^g$.

Les périodes de Θ sont évidemment des points algébriques de Θ, donc si ω est une période non nulle de Θ, l'une au moins des coordonnées de ω est transcendante.

En appliquant le théorème 3.1.1 au sous-groupe à 1 paramètre de $G_m \times A$

$$\Psi : \mathbf{C} \to \mathbf{C}^* \times A_{\mathbf{C}}$$

$$z \mapsto (e^z , \Theta(\alpha z)).$$

on voit que sous les hypothèses du corollaire 3.1.3 le nombre e^t est aussi transcendant.

COROLLAIRE 3.1.5 - Soient G' et G'' deux groupes algébriques commutatifs connexes définis sur $\overline{\mathbf{Q}}$, G' étant de dimension 1. Soit $\Psi : G'_{\mathbf{C}} \to G''_{\mathbf{C}}$ un homomorphisme analytique complexe dont l'application linéaire tangente $T_{G'}(\mathbf{C}) \to T_{G''}(\mathbf{C})$ est définie sur $\overline{\mathbf{Q}}$ et non nulle. S'il existe un point u de $G'_{\mathbf{C}}$ distinct de l'élément neutre tel que $\Psi(u) \in G''_{\overline{\mathbf{Q}}}$, alors $\Psi(G'_{\mathbf{C}})$ est un sous-groupe algébrique fermé de $G''_{\mathbf{C}}$ de dimension 1. Si de plus $u \in G'_{\overline{\mathbf{Q}}}$, alors une puissance de Ψ est un homomorphisme rationnel.

La première assertion se déduit du théorème 3.1.1 en composant Ψ avec l'exponentielle de G'. Pour la deuxième, il suffit de montrer que le graphe de φ est algébrique, et pour cela on considère l'homomorphisme $z \to (z , \Psi(z))$ de $G'_{\mathbf{C}}$ dans $G'_{\mathbf{C}} \times G''_{\mathbf{C}}$.

Pour étudier systématiquement les conséquences du théorème 3.1.1, nous considérons un homomorphisme analytique $\varphi : \mathbf{C} \to G_{\mathbf{C}}$ et nous écrivons G (groupe algébrique commutatif connexe) comme extension d'une variété abélienne A par un groupe linéaire L. Soit $\pi : G_{\mathbf{C}} \to A_{\mathbf{C}}$ la surjection canonique. Le cas où $\varphi(\mathbf{C}) \subset L_{\mathbf{C}}$ a été étudié au § 2.2. Si la dimension algébrique de $\pi \circ \varphi$ est supérieure ou égale à 2, il suffit d'étudier $\pi \circ \varphi$, c'est-à-dire de considérer le cas abélien. Si la dimension algébrique de $\pi \circ \varphi$ est égale à 1, on peut supposer que A est une courbe elliptique. Il suffit alors de considérer les extensions de courbes elliptiques par G_a ou G_m.

§ 3.2. Application aux groupes algébriques de dimension 2.

Nous étudions les conséquences du théorème 3.1.1. pour les groupes algébriques commutatifs connexes de dimension 2. Le cas linéaire ayant déjà été étudié au § 2.2, nous étudions successivement les cas suivants

a) Variété abélienne simple de dimension 2.
b) Produit de deux courbes elliptiques.
c) Extension d'une courbe elliptique par le groupe additif.
d) Produit d'une courbe elliptique par le groupe multiplicatif.
e) Extension non triviale d'une courbe elliptique par le groupe multiplicatif.

Les résultats des sections b, c et d fournissent des analogues elliptiques des théorèmes de Hermite Lindemann, et Gel'fond Schneider, et sont dus à Schneider [S1], [S4] (chap 2 §4).

a) Variété abélienne simple de dimension 2.

Soient A une variété abélienne simple de dimension $g \geqq 2$, définie sur $\overline{\mathbf{Q}}$, $\Theta : \mathbf{C}^g \to A_{\mathbf{C}}$ un homomorphisme thêta normalisé, et $u = (u_1, \ldots, u_g)$ un point algébrique non nul de Θ. Alors les coordonnées $u_1, \dots, u_g$ de u engendrent sur $\bar{\mathbb{Q}}$ un espace vectoriel de dimension ≥ 2. En effet, s'il n'en était pas ainsi, on aurait $u_j = \alpha_j t$, $(1 \leq j \leq g)$, avec $\alpha_j \in \bar{\mathbb{Q}}$ et $t \in \mathbb{C}$, $t \neq 0$, et le corollaire 3.1.3. fournirait une contradiction à l'hypothèse que A est simple.

Ce résultat est particulièrement intéressant quand $g = 2$ (cf.[F] Appendice 1).

THÉORÈME 3.2.1 - Soient A une variété abélienne simple de dimension 2 définie sur $\bar{\mathbb{Q}}$, $\Theta : \mathbb{C}^2 \to A_{\mathbb{C}}$ un homomorphisme thêta normalisé, et $u = (u_1, u_2)$ un point algébrique non nul de Θ. Alors u_1, u_2 sont $\bar{\mathbb{Q}}$-linéairement indépendants.

Dans le cas particulier où u est une période non nulle de Θ, D.W. Masser [M 4] a démontré que les trois nombres $1, u_1, u_2$ sont $\bar{\mathbb{Q}}$-linéairement indépendants. (cf. Th. 5.2.5 ci-dessous).

b) Produit de deux courbes elliptiques.

Quand on écrit le corollaire 3.1.3 pour le produit de deux courbes elliptiques, on obtient le résultat suivant, dû à Th. Schneider [S 1], [S 4] Th. 16.

THÉORÈME 3.2.2 - Soient $\wp, \wp^*$ deux fonctions elliptiques de Weierstrass algébriquement indépendantes, dont les invariants g_2, g_3 et g_2^*, g_3^* sont algébriques. Soit t un nombre complexe qui n'est pôle ni de $\wp$, ni de $\wp^*$. Alors l'un au moins des 2 nombres

$$\wp(t), \ \wp^*(t)$$

est transcendant.

On en déduit un résultat important sur l'indépendance linéaire de deux points algébriques d'une fonction elliptique.

COROLLAIRE 3.2.3 - Soit $\wp$ une fonction elliptique de Weierstrass d'invariants g_2, g_3 algébriques. On note $k = \mathrm{End}_0\, \mathcal{E}$ l'algèbre d'endomorphismes de la courbe elliptique $\mathcal{E}$ correspondante. Soient u_1, u_2 deux points algébriques de $\wp$ qui sont k-linéairement indépendants. Alors u_1, u_2 sont $\bar{\mathbb{Q}}$-linéairement indépendants

Démonstration du corollaire 3.2.3.

Soit $\beta \in \bar{\mathbb{Q}}$ tel que $u_2 = \beta u_1$. Notons $\wp^*(z) = \beta^2 \wp(\beta z)$. Ainsi $\wp^*$ est la fonction elliptique de Weierstrass associée au réseau $\beta^{-1}\Omega$, quand Ω est le réseau des périodes de $\wp$. Le théorème 3.2.2. avec $t = u_1$, montre que $\wp$ et $\wp^*$ sont algébriquement dépendantes. Si τ est le quotient de deux périodes fondamentales de $\wp$, on a

$$\begin{pmatrix} \beta \\ \beta\tau \end{pmatrix} = M \begin{pmatrix} 1 \\ \tau \end{pmatrix},$$

avec $M \in M_2(\mathbb{Q})$. On en déduit que τ est quadratique et $\beta \in \mathbb{Q}(\tau) = k$.

Le corollaire 3.2.3 montre que le quotient de deux périodes fondamentales est soit imaginaire quadratique (ce qui est le cas si et seulement si $\wp$ admet une multiplication complexe), soit transcendant. On en déduit le théorème de Schneider sur la fonction modulaire j. (cf. [S 4] th 17.) :

COROLLAIRE 3.2.4 - Si τ est un nombre complexe algébrique, de partie imaginaire positive, tel que $j(\tau)$ soit algébrique, alors τ est imaginaire quadratique

Démonstration du corollaire 3.2.4.

Pour tout réel $\lambda > 2$, notons

$$s_\lambda = s_\lambda(\tau) = \sum_{\substack{(m,n) \in \mathbb{Z}\times\mathbb{Z} \\ (m,n) \neq (0,0)}} (m + n\tau)^{-\lambda}$$

Le nombre

$$\Delta(1, \tau) = (60\, s_4)^3 - 27 \cdot (140\, s_6)^2$$
$$= 2^4 \cdot 3^3 \cdot 5^2 \cdot (20\, s_4^3 - 49\, s_6^2)$$

n'est pas nul (c'est le discriminant de la courbe elliptique associée au réseau de base $(1, \tau)$) et on a

$$j(\tau) = 2^{12} \cdot 3^6 \cdot 5^3 \cdot s_4^3 / \Delta(1, \tau)$$
$$= 1728 \cdot \frac{20\, s_4^3}{20\, s_4^3 - 49\, s_6^2}.$$

Soit ω_1 une racine douzième de $\Delta(1, \tau)$. Soit $\wp$ la fonction elliptique associée au réseau $\mathbb{Z}\omega_1 + \mathbb{Z}\tau\omega_1$. Les invariants de $\wp$ sont

$$g_2 = 60\, s_4 / \omega_1^4, \quad g_3 = 140\, s_6 / \omega_1^6,$$

donc sont algébriques ; comme le quotient τ de deux périodes fondamentales de $\wp$ est algébrique, il est imaginaire quadratique.

Voici une dernière conséquence du corollaire 3.2.3 dont nous reparlerons au §3. 3.

COROLLAIRE 3.2.5 - Soit $\wp$ une fonction elliptique de Weierstrass d'invariants algébriques. Soient λ un nombre complexe non nul, et γ_1, γ_2 deux nombres algébriques $\mathbb{Q}$-linéairement indépendants. Si $\wp(\lambda\gamma_1)$ et $\wp(\lambda\gamma_2)$ sont des nombres algébriques, alors $\wp$ admet une multiplication complexe, et γ_2/γ_1 appartient au corps de multiplication complexe

c) Extension d'une courbe elliptique par le groupe additif.

Considérons une courbe elliptique $\mathcal{E}$ définie sur $\overline{\mathbb{Q}}$, et une fonction elliptique $\wp$ de Weierstrass telle que l'application $P : \mathbb{C} \to \mathbb{P}_2(\mathbb{C})$ définie par $P(z) = (1, \wp(z), \wp'(z))$ paramètre les points de $\mathcal{E}_{\mathbb{C}}$.

Soient a, b deux nombres algébriques, $(a, b) \neq (0, 0)$. Soit G le groupe algébrique de dimension 2 dont l'application exponentielle est

$$(z, t) \mapsto (P(z), t + b\zeta(z)).$$

Ainsi G est extension de $\mathcal{E}$ par $\mathbb{G}_a$, et, si $b = 0$, alors $G = \mathbb{G}_a \times \mathcal{E}$.

La relation de Legendre

$$\eta_1\omega_2 - \eta_2\omega_1 = 2i\pi$$

montre que les deux fonctions $\wp(z)$, $az + b\zeta(z)$ sont algébriquement indépendantes, donc que le sous-groupe à 1 paramètre

$$\varphi : z \mapsto (P(z), az + b\zeta(z))$$

de G a pour dimension algébrique 2. Si $t \in \mathbb{C}$, $t \notin \Omega$, alors $\varphi(t)$ appartient à l'ouvert de G situé au dessus de $\mathcal{E} - \{0\}$, donc dire que $\varphi(t)$ n'appartient pas à $G_{\overline{\mathbb{Q}}}$ revient à dire que l'un des nombres $\wp(t)$, $at + b\zeta(t)$ est transcendant. On obtient ainsi le résultat suivant de Th. Schneider [S 1], [S 4] Th. 15.

THÉORÈME 3.2.6 - Soient $\wp$ une fonction elliptique d'invariants g_2, g_3 algébriques, ζ la fonction zêta de Weierstrass associée à $\wp$, a, b deux nombres algébriques non tous deux nuls, et t un nombre complexe non pôle de $\wp$. Alors l'un au moins des deux nombres.

$$\wp(t), \ at + b\zeta(t)$$

est transcendant.

Dans le cas $b = 0$, on en déduit l'analogue elliptique du théorème de Hermite-Lindemann : si α est un nombre algébrique non nul, alors α n'est pas pôle de $\wp$, et $\wp(\alpha)$ est transcendant. C'est le cas $g = 1$ du corollaire 3.1.4. que nous

énonçons sous la forme suivante.

COROLLAIRE 3.2.7 - Si u est un point algébrique non nul d'une fonction elliptique $\wp$ d'invariants g_2, g_3 algébriques, alors u est transcendant.

Enfin on déduit du théorème 3.2.6 l'indépendance linéaire sur $\overline{\mathbb{Q}}$ des 3 nombres $1, \omega, \eta$, quand ω est une période non nulle de $\wp$ et η la quasi-période correspondante de ζ :

$$\zeta(z+\omega) = \zeta(z) + \eta.$$

d) Produit d'une courbe elliptique par le groupe multiplicatif.

Si $\mathcal{E}$ est une courbe elliptique, le sous-groupe à 1 paramètre $z \mapsto (e^z, P(z))$ de $\mathbb{G}_m \times \mathcal{E}$ a pour dimension algébrique 2. On déduit alors du théorème 3.1.1 l'énoncé suivant, dû à Th. Schneider [S 1], [S 4] Th. 18.

THÉORÈME 3.2.8 - Soient $\wp$ une fonction elliptique de Weierstrass d'invariants g_2, g_3 algébriques, et t un nombre complexe qui n'est pas pôle de $\wp$. Alors l'un au moins des 2 nombres

$$e^t, \ \wp(t)$$

est transcendant.

Si u est un point algébrique non nul de $\wp$ et β un nombre algébrique non nul, on en déduit la transcendance du nombre $e^{\beta u}$. En particulier $\frac{u}{\pi}$ est transcendant.

Comme l'a remarqué D. Bertrand [B e 1], le théorème 3.2.8. contient un résultat de transcendance sur les séries d'Eisenstein normalisées de poids 4 et 6, définies par

$$E_{2k}(q) = 1 + (-1)^k \frac{4k}{B_k} \sum_{n=1}^{\infty} \sigma_{2k-1}(n)\, q^n,$$

pour $k = 2$ et 3, et $|q| < 1$, où B_k est le k ième nombre de Bernoulli ($B_2 = \frac{1}{30}$, $B_3 = \frac{1}{42}$, $\zeta(4) = \frac{\pi^4}{90}$, $\zeta(6) = \frac{\pi^6}{945}$), et $\sigma_{2k-1}(n) = \sum_{d|n} d^{2k-1}$.

COROLLAIRE 3.2.9 - Pour tout nombre complexe q vérifiant $0 < |q| < 1$, l'un au moins des deux nombres $E_4(q)$, $E_6(q)$ est transcendant.

Démonstration du corollaire 3.2.9.

Soit $\omega \in \mathbb{C}$ avec $\mathrm{Re}\,\omega < 0$ tel que $q = e^{\omega}$. Considérons le réseau $\Omega = \mathbb{Z}\omega + \mathbb{Z}\,2i\pi$. L'un des deux nombres $s_4(\Omega)$, $s_6(\Omega)$ est transcendant d'après le théorème 3.2.8 (avec $t = i\pi$). Or, pour $k = 2$ et $k = 3$,

$$s_{2k}(\Omega) = (2i\pi)^{-2k} \sum_{(m,n)\neq(0,0)} \left(m\frac{\omega}{2i\pi}+n\right)^{-2k}$$
$$= 2.(2i\pi)^{-2k}\left(\zeta(2k) + \sum_{m=1}^{\infty}\sum_{n=-\infty}^{+\infty}\left(m\frac{\omega}{2i\pi}+n\right)^{-2k}\right)$$

En dérivant la relation

$$\sum_{n=-\infty}^{+\infty}\frac{1}{z+n} = \pi i - 2\pi i \sum_{\nu=0}^{\infty} e^{2i\pi\nu z}$$

(les deux membres sont égaux à $\pi\frac{\cos\pi z}{\sin\pi z}$), on obtient

$$(-1)^{2k-1}(2k-1)!\sum_{n=-\infty}^{+\infty}(z+n)^{-2k} = -(2i\pi)^{2k}\sum_{\nu=1}^{\infty}\nu^{2k-1}e^{2i\pi\nu z},$$

d'où

$$s_{2k}(\Omega) = (2i\pi)^{-2k}.\ 2\zeta(2k)E_{2k}(q)$$
$$= (-1)^k\frac{B_k}{(2k)!}E_{2k}(q)$$

Comme les nombres de Bernoulli sont rationnels, le corollaire est démontré

e) Extension non triviale d'une courbe elliptique par le groupe multiplicatif.

Soient $\mathcal{E}$ une courbe elliptique définie sur $\bar{\mathbb{Q}}$, $P : z \mapsto (1, \wp(z), \wp'(z))$ une paramétrisation de $\mathcal{E}_{\mathbb{C}}$ par une fonction elliptique $\wp$ de Weierstrass, u_0 un point algébrique de $\wp$, et G l'extension correspondante de $\mathcal{E}$ par le groupe groupe multiplicatif $\mathbb{G}_m$. Comme nous avons déjà étudié l'extension triviale $\mathbb{G}_m\times\mathcal{E}$, nous choisissons pour u_0 un point d'ordre infini.

L'ouvert de G situé au dessus de $\mathcal{E}-\{0, u_0\}$ s'identifie au produit $\mathbb{G}_m\times(\mathcal{E}-\{0, u_0\})$. C'est un ouvert affine. Son algèbre de coordonnées est

$$\bar{\mathbb{Q}}\left[\wp(z), \wp'(z), e^t F(z), \frac{\wp'(z)+\wp'(u_0)}{\wp(z)-\wp(u_0)}, 1/e^t F(z)\right],$$

où

$$F(z) = \frac{\sigma(z-u_0)}{\sigma(z)\sigma(u_0)}e^{z\zeta(u_0)}.$$

Soit β un nombre algébrique. Comme u_0 n'est pas de torsion, les deux fonctions $\wp(z)$, $e^{\beta z}F(z)$ sont algébriquement indépendantes. On en déduit, grâce au

théorème 3.1.1, que si u est un point algébrique de $\wp$ tel que u, $u+u_0$ et $u-u_0$ ne soient pas pôles de $\wp$, alors le nombre $e^{\beta u}F(u)$ est transcendant.

L'hypothèse $\sigma(u+u_0)\neq 0$ est superflue. Pour le voir, on calcule $e^{\beta u}F(u)$ pour $2u+u_0\in\Omega$ (donc $u\notin\Omega$, $u\pm u_0\notin\Omega$) où $\Omega = \ker P$; on obtient ainsi la transcendance du nombre

$$\sigma(u_0)^2\exp\{-\eta u_0-(u_0-\omega)(\beta+\zeta(u_0))\},$$

grâce à la formule de multiplication de la fonction sigma : pour m entier positif, on a

$$\sigma(mz) = (-1)^{m-1}\sigma(z)^{m^2}\Psi_m(\wp(z), \wp'(z)),$$

où $\Psi_m(X, Y)$ est une fonction rationnelle de X, Y à coefficients dans $\mathbb{Q}(g_2, g_3)$.

THÉORÈME 3.2.10 - Soient β un nombre algébrique, $\wp$ une fonction elliptique de Weierstrass d'invariants g_2, g_3 algébriques, σ le produit canonique de Weierstrass associé au réseau Ω des périodes de $\wp$, et u, u_0 deux points algébriques de $\wp$. On suppose que u_0 n'est pas de torsion, et $u\notin\Omega$, $u-u_0\notin\Omega$. Alors le nombre

$$\frac{\sigma(u-u_0)}{\sigma(u)\sigma(u_0)}e^{(\beta+\zeta(u_0))u}$$

est transcendant

Le corollaire suivant donne la transcendance de la dérivée de $F(z)e^{\beta z}$ aux points $z=\omega-u_0$, c'est-à-dire aux points où F s'annule.

COROLLAIRE 3.2.11 - Soient ω une période de $\wp$, η la pseudo-période correspondante de ζ, et, comme précédemment, u_0 un point algébrique de $\wp$, qui n'est pas de torsion, et β un nombre algébrique. Alors le nombre

$$\sigma(u_0)^2\exp\{-\eta u_0-(u_0-\omega)(\beta+\zeta(u_0))\}$$

est transcendant.

Par exemple le nombre

$$\sigma(u_0)e^{-\frac{1}{2}u_0\zeta(u_0)}$$

est transcendant. On ne sait toujours pas si le nombre $\sigma(u_0)$ lui-même est transcendant, même quand u_0 est un point de torsion (non pôle) de $\wp$. Dans le même ordre d'idée, on ne connait pas la nature arithmétique du nombre

$$2^{5/4} \,.\, \pi^{1/2} \,.\, e^{\pi/8} \,.\, \Gamma(1/4)^{-2}$$

qui est la valeur au point 1/2 du produit canonique de Weierstrass associé au réseau $\mathbf{Z}[i]$ (correspondant à des invariants g_2, g_3 transcendants).

Enfin montrons que les quasi-périodes multiplicatives de la fonction $F(z)\,e^{\beta z}$ sont transcendantes. On choisit (dans le théorème 3.2.10) pour u un point de torsion, et on utilise le fait que les nombres

$$\frac{\sigma(u_o + \frac{\omega}{2})}{\sigma(u_o)\, \exp\{\eta(\frac{u_o}{2} + \frac{\omega}{8})\}} \quad \text{et} \quad \sigma(\tfrac{\omega}{2})\, e^{-\eta\omega/8}$$

sont algébriques.

COROLLAIRE 3.2.12. <u>Avec les notations du corollaire</u> 3.2.11, <u>pour</u> $\omega \neq 0$ <u>le nombre</u>

$$\exp\{\omega\, \zeta(u_o) - \eta u_o + \beta\omega\}$$

<u>est transcendant</u>.

En particulier le nombre $\zeta(u_o) - \frac{\eta}{\omega} u_o$ est transcendant. En fait G.V. Chudnovsky [C 1, C 3] a démontré que ce nombre est algébriquement indépendant de $\frac{\eta}{\omega}$. Nous indiquerons (sans démonstration) d'autres résultats aux § 3.3 et 3.5.

§ 3.3. <u>Intégrales elliptiques</u>

Nous interprétons les résultats du § 3.2. en termes d'intégrales elliptiques de première, deuxième ou troisième espèce.

a) <u>Formes différentielles sur une courbe elliptique</u>

Soit $\mathcal{E}_{\mathbf{C}}$ une courbe elliptique dans $\mathbf{P}_2(\mathbf{C})$, d'équation

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

Soit ξ une forme différentielle sur $\mathcal{E}$. Notons $(1, x_j, y_j)$, $(1 \leq j \leq k)$ les points (t, x, y) de $\mathcal{E}_{\mathbf{C}}$, distincts de $(0, 0, 1)$, où les résidus de ξ sont non nuls, et c_j, $(1 \leq j \leq k)$ ces résidus. Comme la somme de tous les résidus de ξ est nulle, on a $k = 0$ si et seulement si ξ est de première ou de deuxième espèce. Dans tous les cas la forme différentielle

$$\xi - \frac{1}{2}\sum_{j=1}^{k} c_j \frac{y + y_j}{x - x_j} \frac{dx}{y}$$

est de première ou de deuxième espèce. Donc il existe $a, b \in \mathbf{C}$, $\chi \in \mathbf{C}(x, y)$ tels que

$$\xi = \frac{1}{2}\sum_{j=1}^{k} c_j \frac{y + y_j}{x - x_j} \frac{dx}{y} + a\frac{dx}{y} + bx\frac{dx}{y} + d\chi.$$

Supposons que $\mathcal{E}$ et ξ sont définis sur $\overline{\mathbf{Q}}$: les nombres g_2, g_3, a, b, et c_j, x_j, y_j $(1 \leq j \leq k)$ sont algébriques, et $\chi \in \overline{\mathbf{Q}}(x, y)$

Si on paramètre $\mathcal{E}_{\mathbf{C}}$ par la fonction $\wp$ de Weierstrass, et si, pour $(x_j, y_j) = (\wp(u_j), \wp'(u_j))$, on note

$$F_{u_j}(z) = \frac{\sigma(z - u_j)}{\sigma(z)\,\sigma(u_j)}\, e^{\zeta(u_j) z},$$

alors

$$\xi = \frac{1}{2}\sum_{j=1}^{k} c_j \frac{F'_{u_j}(z)}{F_{u_j}(z)}\, dz + a\, dz + b\, d\zeta + d\chi.$$

<u>Nous dirons que</u> ξ <u>est de troisième espèce si</u> $k \geq 1$, $b = 0$ et $\chi = 0$ (donc ξ n'a pas de pôles d'ordre ≥ 2).

b) <u>Intégrales elliptiques de première ou deuxième espèce</u>.

Le théorème 3.2.6 de Schneider s'énonce sous la forme équivalente suivante (cf. [S 1], [S 4], [Si 2]).

THÉORÈME 3.3.1. - <u>Soient</u> $\mathcal{E}$ <u>une courbe elliptique définie sur</u> $\overline{\mathbf{Q}}$, <u>et</u> ξ <u>une forme différentielle de première ou deuxième espèce sur</u> $\mathcal{E}$, <u>définie sur</u> $\overline{\mathbf{Q}}$, <u>et qui n'est pas exacte</u>.

a) <u>Si</u> p_1, p_2 <u>sont deux points distincts de</u> $\mathcal{E}_{\overline{\mathbf{Q}}}$, <u>où</u> ξ <u>est holomorphe, et si</u> γ <u>est un chemin sur</u> $\mathcal{E}$ <u>d'origine</u> p_1 <u>et d'extrémité</u> p_2, <u>alors le nombre</u>

$$\int_{\gamma} \xi$$

<u>est transcendant</u>.

b) <u>Les périodes non nulles de</u> ξ <u>sont transcendantes</u>.

<u>Démonstration du théorème</u> 3.3.1.

a) L'hypothèse sur ξ signifie que

$$\xi = a\, dz + b\, d\zeta + d\chi$$

avec $(a, b) \neq (o, o)$. Soit $\mathcal{L}$ un chemin dans $\mathbf{C}$ dont l'image sur $\mathcal{E}$ par $P = (1, \wp, \wp')$ est γ. Notons u_1 l'origine de $\mathcal{L}$, u_2 son extrémité, avec

$P(u_j) = p_j$, $(j=1,2)$. On a

$$\int_\gamma \xi = \int_{\mathfrak{L}} a\,dz + b\,d\zeta + dX$$

$$= a(u_2 - u_1) + b\,(\zeta(u_2) - \zeta(u_1)) + X_2 - X_1$$

où les nombres $X_j = X(\wp(u_j), \wp'(u_j))$, $(j=1,\ 2)$ sont algébriques (par hypothèse $X(x\,,\ y)$ est régulière en $(\wp(u_j)\,,\ \wp'(u_j))$, $j = 1,2$).

D'après le théorème d'addition algébrique de la fonction zêta, le nombre

$$\zeta(u_2 - u_1) - (\zeta(u_2) - \zeta(u_1))$$

est algébrique, d'où le théorème en utilisant 3.2.6. pour $t = u_2 - u_1$.

b) Soient γ un chemin fermé sur $\mathcal{E}$, $\mathfrak{L}$ un chemin dans $\mathbb{C}$ dont l'image par P est γ, et $\omega = \int_{\mathfrak{L}} dz$, $\eta = \int_{\mathfrak{L}} d\zeta$. Si γ n'est pas homologue à 0, alors $\omega \neq 0$ et le nombre

$$\int_\gamma \zeta = a\,\omega + b\,\eta$$

est transcendant d'après 3.2.6.

On peut formuler d'autres résultats du § 3.2. en termes d'intégrales elliptiques de première ou deuxième espèce. Par exemple, pour le corollaire 3.2.3, on considère deux intégrales de première espèce sur $\mathcal{E}$ à coefficients algébriques entre des bornes algébriques. Si ces deux intégrales ont des valeurs linéairement indépendantes sur $\mathrm{End}_0\,\mathcal{E}$, alors ces valeurs sont $\overline{\mathbb{Q}}$- linéairement indépendantes. Ainsi le quotient d'une intégrale elliptique de première espèce (à coefficients algébriques et entre des bornes algébriques) par une période non nulle est un nombre soit rationnel, soit imaginaire quadratique, soit transcendant

Enfin le théorème 3.2.8 montre que si w est une période non nulle d'une intégrale elliptique de première espèce définie sur $\overline{\mathbb{Q}}$, alors e^w est transcendant .

Nous allons étendre cet énoncé à certaines intégrales elliptiques de troisième espèce, mais voici d'abord l'énoncé pour les intégrales de première ou deuxième espèce.

THÉORÈME 3.3.2 - <u>Soient $\mathcal{E}$ une courbe elliptique définie sur $\overline{\mathbb{Q}}$, et ξ une forme différentielle de première ou deuxième espèce sur $\mathcal{E}$. Alors les périodes non nulles de ξ ne sont pas des logarithmes de nombres algébriques</u>

Cet énoncé est équivalent à la transcendance du nombre

$$\exp\,(a\,\omega + b\,\eta)$$

quand ω est une période non nulle de $\wp$, et a,b des nombres algébriques non tous deux nuls. On ne peut pas appliquer le critère de Schneider Lang aux fonctions

$$\wp(z),\quad \exp(az + b\,\zeta(z)),\ \wp'(z)$$

avec les points $\frac{1}{2}\,\omega + k\,\omega$, $(k \in \mathbb{Z})$, car la deuxième fonction n'est pas méromorphe.

Le résultat (3.3.2) ci-dessus est un cas particulier d'un théorème de D.W. Masser [M 3] (p.152) qui montre que si $\log\alpha$ est un logarithme non nul d'un nombre algébrique, alors les nombres

$$1,\ \omega,\ \eta,\ \log\alpha$$

sont $\overline{\mathbb{Q}}$- linéairement indépendants

c) <u>Périodes de certaines intégrales elliptiques de troisième espèce</u>.

Dans [S 4] (problème 3), Schneider propose le problème suivant : chercher à démontrer des résultats de transcendance sur les intégrales elliptiques de troisième espèce.

Nous exposons ici les énoncés que l'on peut déduire du critère de Schneider Lang.

THÉORÈME 3.3.3 - <u>Soient $\mathcal{E}$ une courbe elliptique définie sur $\overline{\mathbb{Q}}$, et ξ une forme différentielle de troisième espèce sur $\mathcal{E}$ définie sur $\overline{\mathbb{Q}}$. On suppose que les résidus de ξ sont des nombres rationnels.</u>

<u>Si w est une période de ξ, alors le nombre e^w est soit égal à une racine de l'unité, soit transcendant</u>.

Si e est une racine du polynôme $4X^3 - g_2X - g_3$, les périodes de la forme différentielle

$$\frac{p}{q}\ \frac{y}{x-e}\ \frac{dx}{y}\ ,$$

(avec $\frac{p}{q} \in \mathbb{Q}$), sont des multiples rationnels de $2\,i\,\pi$.

<u>Démonstration du théorème</u> 3.3.3.

En multipliant ξ par un entier, on se ramène au cas où

$$\xi = \frac{1}{2}\sum_{j=1}^{k} c_j\,\frac{F'_{u_j}(z)}{F_{u_j}(z)}\,dz + \beta\,dz,$$

avec $\beta \in \overline{\mathbb{Q}}$, et $c_j \in \mathbb{Z}$, $(1 \leq j \leq k)$.

Soit γ un chemin fermé non homologue à 0 sur $\mathcal{E}$, $\mathfrak{L}$ un chemin dans $\mathbb{C}$ dont l'image par P est γ, et $\omega = \int_{\mathfrak{L}} dz$, $\eta = \int_{\mathfrak{L}} d\zeta$.

La quasi périodicité de F_{u_j} montre que

$$\int_{\mathfrak{L}} \frac{F'_{u_j}(z)}{F_{u_j}(z)}\,dz = \omega\,\zeta(u_j) - \eta\,u_j,\quad (1 \leq j \leq k),$$

donc, en posant

$$u = \sum_{j=1}^{k} c_j u_j ,$$

on a

$$w = \int_\gamma \xi = \omega \sum_{j=1}^{k} c_j \ \zeta(u_j) - \eta u - \beta\omega .$$

Or le nombre

$$\zeta(u) - \sum_{j=1}^{k} c_j \zeta(u_j)$$

est algébrique. Si u n'est pas un point de torsion, le corollaire 3.2.12 s'applique, et pour $w \neq o$ on a $e^w \notin \bar{\mathbb{Q}}$. Si u est de torsion, il existe un nombre algébrique β' tel que $w - \beta'\omega$ soit un multiple rationnel de $2 i \pi$. Si $\beta' = o$, e^w est une racine de l'unité. Si $\beta' \neq o$, le théorème 3.2.8. montre que $e^{\beta'\omega}$ est transcendant, donc e^w aussi.

Notons que la même méthode montre la transcendance du nombre

$$\exp\ (\int_\gamma \xi) ,$$

quand γ est un chemin sur $\mathcal{E}$, d'origine p_1 et d'extrémité p_2, où p_1, p_2 sont deux points distincts de $\mathcal{E}_{\bar{\mathbb{Q}}}$ où ξ est holomorphe, pourvu que $\int_\gamma \xi$ ne soit pas un multiple rationnel de $2 i \pi$.

D'autre part les périodes d'une forme différentielle elliptique quelconque sont de la forme

$$\sum_{j=1}^{k} c_j\ (\omega\zeta(u_j) - \eta u_j) + a\,\omega + b\,\eta .$$

Pour supprimer l'hypothèse que ξ est de troisième espèce dans le théorème 3.3.3, il suffirait que l'on montre que le nombre

$$\exp\ \{\omega\zeta(u) - \eta u + a\,\omega + b\,\eta\}$$

est soit une racine de l'unité, soit transcendant. Seul le cas où u est de torsion est résolu (cf. 3.3. 2).

Les résultats précédents sont ceux que l'on peut déduire du critère de Schneider Lang, c'est-à-dire de la méthode de transcendance classique de Gel'fond Schneider. En adaptant les arguments ajoutés à cette méthode par Baker et Masser, M. Laurent [La 2] a obtenu, sous les hypothèses du corollaire 3.2.12 (c'est-à-dire pour ω période non nulle et u_o point algébrique de $\wp$ non de torsion) l'indépendance linéaire sur $\bar{\mathbb{Q}}$ des 4 nombres

$$1,\ \omega,\ \eta,\ \eta u_o - \omega\,\zeta(u_o)$$

Par conséquent sous les hypothèses du théorème 3.3.3 le nombre w lui-même est nul ou transcendant. De plus si $\wp$ admet une multiplication complexe alors les 5 nombres

$$1,\ \omega,\ \eta,\ \eta u_o - \omega\,\zeta(u_o),\ 2 i \pi$$

sont $\bar{\mathbb{Q}}$-linéairement indépendants [La 2].

§ 3.4 - Démonstration du théorème 3.1.1.

Comme les objets figurant dans le théorème 3.1.1 ne font intervenir que des extensions finies de $\mathbb{Q}$, on peut y remplacer $\bar{\mathbb{Q}}$ par un corps de nombres K.

Soit $t \in \mathbb{C}$, $t \neq o$ tel que $\varphi(t) \in G_K$. On choisit un plongement de G dans $P_\nu(\mathbb{C})$, défini sur K, tel que des coordonnées projectives $(\varphi_o, \ldots, \varphi_\nu)$ de φ soient données par des fonctions φ_i entières d'ordre ≤ 2 (cf. Serre, Appendice II § 3). On peut aussi supposer

$$\varphi_o\ (ht) \neq 0 \quad \text{pour} \quad 0 \leq h \leq 4\,[K : \mathbb{Q}].$$

On aura donc

$$\frac{\varphi_i}{\varphi_o}\ (ht) \in K \ \text{pour} \quad 0 \leq h \leq 4\,[K : \mathbb{Q}].$$

Soit $j : \mathbb{C}^D \to T_G(\mathbb{C})$ un isomorphisme linéaire défini sur K, et soit $(\psi_o, \ldots, \psi_\nu)$ une représentation normalisée de l'exponentielle de G correspondant à j et au plongement de G dans $P_\nu\ (\mathbb{C})$ (cf. § 1.2). Ainsi $\varphi_i = \psi_i \circ j^{-1} \circ \mathfrak{L}$, où $\mathfrak{L} : \mathbb{C} \to T_G(\mathbb{C})$ est une application linéaire définie sur K. Comme les dérivations partielles $\frac{\partial}{\partial z_i}$, $(1 \leq i \leq D)$ laissent stable l'anneau $K\,[\frac{\psi_1}{\psi_o}, \ldots, \frac{\psi_\nu}{\psi_o}]$, on en déduit que la dérivation $\frac{d}{dz}$ laisse stable l'anneau $K\,[\frac{\varphi_1}{\varphi_o}, \ldots, \frac{\varphi_\nu}{\varphi_o}]$.

Le critère de Schneider Lang (Th. 1.1.1.) montre que le sous-groupe à 1 paramètre φ a pour dimension algébrique 1.

§ 3.5 - Indépendance linéaire et algébrique de périodes et quasi-périodes

Nous indiquons ici, sans démonstration, quelques développements récents de la théorie des nombres transcendants liés aux énoncés de ce chapitre, et notamment en ce qui concerne les nombres $\omega_1, \omega_2, \eta_1, \eta_2, 2 i \pi$. Pour un aperçu historique et des références plus complètes, nous renvoyons à [M 1], aux chapitres 6 et 7 de [B-M], et à [C 1] et [C 3].

Considérons une fonction elliptique $\wp$ de Weierstrass d'invariants g_2, g_3

algébriques, une base (ω_1, ω_2) du réseau des périodes de $\wp$, et les quasi-périodes correspondantes η_1, η_2 de la fonction zêta de Weierstrass. Nous avons vu au § 3.2 que Schneider avait démontré en 1936 l'indépendance linéaire sur $\overline{\mathbb{Q}}$ des trois nombres $1, \omega_1, \eta_1$. Après des énoncés partiels de Baker et Coates de 1968 à 1971, Masser à démontré en 1974 l'important résultat suivant [M 1] (Th II et III).

THÉORÈME 3.5.1 - Si $\wp$ n'admet pas de multiplication complexe, les six nombres

$$1, \omega_1, \omega_2, \eta_1, \eta_2, 2i\pi$$

sont linéairement indépendants sur $\overline{\mathbb{Q}}$. Si $\wp$ admet une multiplication complexe, ces six nombres engendrent un espace vectoriel sur $\overline{\mathbb{Q}}$ de dimension 4.

Dans le cas de multiplication complexe, il existe donc entre les six nombres une relation linéaire à coefficients algébriques indépendante de $\omega_2 - \tau\omega_1 = 0$. Si $A + BX + CX^2$ est le polynôme minimal de τ sur $\mathbb{Z}$, cette relation s'écrit

$$A\eta_1 - C\tau\eta_2 = \varkappa\omega_2,$$

avec $\varkappa \in \mathbb{Q}(g_2, g_3, \tau)$. Il y a de nombreuses démonstrations de cette relation (cf. [M 1] chap. III et appendice 1 ; [Br - K] appendice B ; [Be 6] § 3 remarque 3). On peut aussi la déduire de la formule

$$[\sigma(C\tau z)]^2 = (C\tau)^2 [\sigma(z)]^{2AC} e^{-\gamma z^2} Q(\wp(z)),$$

où $\gamma = \varkappa C\tau$ et $Q \in \mathbb{Q}(g_2, g_3, \tau)[X]$.

Masser [B - M] (chap. 6) a généralisé en partie son théorème 3.5.1 au cas où ω_1, ω_2 sont des périodes de deux fonctions elliptiques $\wp_1, \wp_2$ respectivement. Remarquons que $(\eta_1, \omega_1, \eta_2, \omega_2, 2i\pi)$ correspond alors à une période de l'exponentielle d'un groupe algébrique commutatif $G_1 \times G_2 \times \mathbb{G}_m$ de dimension 5, G_1 et G_2 étant des extensions de deux courbes elliptiques $\mathcal{E}_1$, $\mathcal{E}_2$ respectivement par le groupe additif. En rejoignant ainsi le thème général de notre étude, on constate qu'il y a encore beaucoup de travail à faire.

Les résultats d'indépendance algébrique sont encore plus récents. Les premiers énoncés utilisaient la notion de "type de transcendance" de Lang (cf. [Wa 1], [Br - K]). C'est en utilisant une mesure de transcendance de π, due à Feldman, que Chudnovsky a obtenu ses premiers résultats dans ce domaine. Puis il a réussi à appliquer le critère de transcendance de Gel'fond (cf [C 1], [C 3]) et il a démontré l'énoncé remarquable suivant.

THÉORÈME 3.5.2 - Soient ω une période non nulle, et η la quasi-période de ζ associée. Alors les deux nombres

$$\frac{\pi}{\omega}, \frac{\eta}{\omega}$$

sont algébriquement indépendants.

On en déduit que si $\wp$ admet une multiplication complexe, alors les deux nombres ω et π sont algébriquement indépendants. Comme la courbe $y^2 = 4x^3 - 4x$ admet la période

$$\omega = 2\int_1^{+\infty} \frac{dx}{\sqrt{4x^3 - 4x}} = \frac{1}{2} B(\frac{1}{4}, \frac{1}{2}) = \Gamma(1/4)^2 / 2\sqrt{2\pi}$$

et a multiplication complexe par i (puisque $g_3 = 0$), on en déduit l'indépendance algébrique de π et $\Gamma(\frac{1}{4})$. De même la courbe $y^2 = 4x^3 - 4$, qui admet la multiplication complexe par $\rho = e^{i\pi/3}$ et a une période égale à

$$\omega = 2\int_1^{+\infty} \frac{dx}{\sqrt{4x^3 - 4}} = \frac{1}{3} B(\frac{1}{6}, \frac{1}{2}) = \Gamma(1/3)^3 / 2^{4/3}.\pi,$$

montre que les nombres π et $\Gamma(1/3)$ sont algébriquement indépendants (cf. [C 1], [C 3], [Be 2], [Gr], [M 8], [Si 1]).

Nous reparlerons des fonctions gamma et bêta au chapitre 5. De l'équation différentielle

$$j'(\tau) = 18.\frac{\omega_1^2}{2i\pi}\,\frac{g_3}{g_2}\,j(\tau)$$

(cf. [L 3] p. 652, [Be 2], [Be 6]), on déduit que si τ est un nombre imaginaire quadratique du demi-plan supérieur tel que $j'(\tau)$ ne soit pas nul, alors π et $j'(\tau)$ sont algébriquement indépendants.

Enfin le théorème 3.5.2 peut s'énoncer de manière équivalente en termes de la fonction $J(q)$ définie pour $0 < |q| < 1$ par $J(e^{2i\pi\tau}) = j(\tau)$ pour $\mathrm{Im}(\tau) > 0$, et de l'opérateur $D = q\frac{d}{dq}$ (cf. [Be 6]) : si q est un nombre complexe, $0 < |q| < 1$, tel que $J(q)$ soit algébrique différent de 0 et 1728, alors les deux nombres $DJ(q)$, $D^2J(q)$ sont algébriquement indépendants. (On conjecture que dans ce cas q est transcendant ; cf [Mah 2], [Man] et la remarque suivant le corollaire 4.2.6).

Chudnovsky a démontré de nombreux autres résultats d'indépendance algébrique, ainsi que des versions effectives de certains de ses résultats, qui fournissent des corps de degré de transcendance 2 et de type de transcendance fini. Il est utile pour cela de connaître des mesures de transcendance des différents nombres dont la transcendance résulte du critère de Schneider Lang. Dans le cas des fonctions de Weierstrass une étude systématique a été entreprise par E. Reyssat [Re 1], [Re 2]. De manière plus générale mais moins précise, Brownawell et Masser ont obtenu une version quantitative du critère de Schneider Lang [Br - M], [M 8].

CHAPITRE 4

SOUS-GROUPES À UN PARAMÈTRE SANS NORMALISATION

Soient G' et G'' deux groupes algébriques commutatifs connexes définis sur $\overline{\mathbb{Q}}$, G' étant de dimension 1, et soit $\psi : G'_{\mathbb{C}} \to G''_{\mathbb{C}}$ un homomorphisme analytique complexe. S'il existe 3 éléments $\mathbb{Z}$-linéairement indépendants de $G'_{\overline{\mathbb{Q}}}$ dont les images par ψ sont dans $G''_{\overline{\mathbb{Q}}}$, alors une puissance de ψ est rationnelle.

Les premiers énoncés dans cette direction étaient dus à Lang [L2] (Chap. II, § 4) et [L3] § 4 et concernaient seulement le cas où G'' est une variété linéaire ou abélienne. De plus, le critère qu'utilisait Lang [L2] (Chap. II, § 2, Th.2) étant moins précis que celui de Ramachandra [Ra], Lang avait besoin de 7 points au lieu de 3. En choisissant $G' = \mathbb{G}_a$ et en prenant pour G'' une courbe elliptique avec multiplication complexe, on voit que 2 points ne suffisent pas.

Pour la démonstration, on peut se ramener au cas où G'' est une variété linéaire ou abélienne. Cette réduction n'est plus possible quand la dimension algébrique intervient, comme dans l'énoncé suivant :

avec les notations ci-dessus, s'il existe 5 points $\mathbb{Z}$-linéairement indépendants de $G'_{\mathbb{C}}$ dont les images par ψ sont dans $G''_{\overline{\mathbb{Q}}}$, alors l'image de ψ a une dimension ≤ 1. Ainsi, dans une variété abélienne, les seuls sous-groupes à 1 paramètre contenant 5 points algébriques $\mathbb{Z}$-linéairement indépendants sont les courbes elliptiques.

La démonstration utilise les résultats de Severi et Serre (Appendice II) sur la représentation de la fonction exponentielle de G'' par des fonctions méromorphes d'ordre ≤ 2, et sur la hauteur pour des groupes algébriques commutatifs connexes quelconques.

§ 4.1 - Points algébriques du graphe.

Soient G un groupe algébrique défini sur $\overline{\mathbb{Q}}$, et $\varphi : \mathbb{C} \to G_{\mathbb{C}}$ un sous-groupe à 1 paramètre. On s'intéresse aux nombres algébriques $\gamma \in \overline{\mathbb{Q}}$ dont l'image par φ est encore algébrique :

$$\varphi(\gamma) \in G_{\overline{\mathbb{Q}}} .$$

Nous avons vu dans le théorème 2.3.1 que si G est une variété linéaire, et si φ n'est pas rationnel, il ne peut pas exister deux tels points γ_1, γ_2, qui soient $\mathbb{Q}$-linéairement indépendants.

Ce résultat n'est plus vrai si on remplace le groupe linéaire par une courbe elliptique ayant multiplication complexe.

LEMME 4.1.1 - Soit $\mathcal{E}$ une courbe elliptique définie sur $\overline{\mathbb{Q}}$, ayant multiplication complexe. Soit τ le quotient de deux périodes fondamentales, et soit ω une période non nulle. Alors le sous-groupe à 1 paramètre

$$z \to P(\omega z)$$

prend des valeurs dans $\mathcal{E}_{\overline{\mathbb{Q}}}$ aux points de $\mathbb{Z} + \mathbb{Z}\tau$.

Inversement, si $\mathcal{E}$ est une courbe elliptique définie sur $\overline{\mathbb{Q}}$, et $\varphi : \mathbb{C} \to \mathcal{E}_{\mathbb{C}}$ un sous-groupe à 1 paramètre pour lequel il existe γ_1, $\gamma_2 \in \overline{\mathbb{Q}}$, $\mathbb{Q}$-linéairement indépendants, avec

$$\varphi(\gamma_j) \in \mathcal{E}_{\overline{\mathbb{Q}}}, \qquad (j=1,2) ,$$

alors $\mathcal{E}$ admet multiplication complexe, et γ_2/γ_1 appartient au corps de multiplication complexe (cf. 3.2.5). Donc si $\gamma_3 \in \overline{\mathbb{Q}}$ est tel que $\varphi(\gamma_3) \in \mathcal{E}_{\overline{\mathbb{Q}}}$, les trois nombres γ_1, γ_2, γ_3 sont $\mathbb{Q}$-linéairement dépendants. C'est ce résultat que nous allons étendre aux groupes algébriques quelconques.

THÉORÈME 4.1.2 - Soient G un groupe algébrique commutatif connexe défini sur $\overline{\mathbb{Q}}$, $\varphi : \mathbb{C} \to G_{\mathbb{C}}$ un sous-groupe à 1 paramètre non rationnel, et Γ un sous-groupe de $\overline{\mathbb{Q}}$ de rang ℓ sur $\mathbb{Z}$ tel que $\varphi(\Gamma) \subset G_{\overline{\mathbb{Q}}}$. Alors $\ell \leq 2$.

Le lemme 4.1.1 montre que l'égalité $\ell = 2$ peut avoir lieu quand G est un produit de courbes elliptiques, ou quand G est le produit de $\mathbb{G}_a$ par une courbe elliptique. Nous verrons au § 6.3 que si G est une variété abélienne simple de type C.M et de dimension ≥ 2, alors $\ell \leq 1$.

§ 4.2 - Dimension algébrique.

On considère de nouveau un groupe algébrique G défini sur $\overline{\mathbb{Q}}$, un sous-groupe à 1 paramètre $\varphi : \mathbb{C} \to G_{\mathbb{C}}$, et des nombres complexes $t_1, \ldots, t_\ell$, $\mathbb{Q}$-linéairement indépendants, tels que

$$\varphi(t_j) \in G_{\overline{\mathbb{Q}}}, \qquad (1 \leq j \leq \ell) .$$

On ne suppose plus que ces nombres sont algébriques, et on voudrait majorer ℓ. Une telle majoration n'est évidemment pas possible si la dimension algébrique d

de φ est égale à 1. Nous avons vu au § 2.3 que si G est une variété linéaire, on a $\ell d \leq \ell + d$, et que l'on conjecture dans ce cas l'inégalité stricte $\ell d < \ell + d$.

On ne peut pas conjecturer le même résultat dans le cas général : avec les notations du lemme 4.1.1, pour le sous-groupe à 1 paramètre

$$z \to (z, P(\omega z))$$

de $G_a \times \mathcal{E}$, on a $\ell = d = 2$. Il ne semble pas que l'on connaisse d'autre cas avec $\ell \geq 2$, $d \geq 2$ (cf. la conjecture de Lang [L3] p. 648).

THÉORÈME 4.2.1 - Soient G un groupe algébrique commutatif connexe défini sur $\overline{\mathbb{Q}}$, $\varphi : \mathbb{C} \to G_{\mathbb{C}}$ un sous-groupe à 1 paramètre, de dimension algébrique d, et Γ un sous-groupe de $\mathbb{C}$ de rang ℓ sur $\mathbb{Z}$ tel que $\varphi(\Gamma) \subset G_{\overline{\mathbb{Q}}}$. Alors

$$\ell d \leq \ell + 2d .$$

La conclusion s'écrit aussi

$$\ell \geq 3 \Rightarrow d \leq 3$$

$$\ell \geq 4 \Rightarrow d \leq 2$$

$$\ell \geq 5 \Rightarrow d = 1 .$$

La dernière implication donne le résultat suivant.

COROLLAIRE 4.2.2 - Soient G' et G'' deux groupes algébriques commutatifs connexes définis sur $\overline{\mathbb{Q}}$, G' étant de dimension 1. Soit $\psi : G'_{\mathbb{C}} \to G''_{\mathbb{C}}$ un homomorphisme analytique complexe non constant. S'il existe 5 points de $G'_{\mathbb{C}}$, linéairement indépendants sur $\mathbb{Z}$, dont les images par ψ soient dans $G''_{\overline{\mathbb{Q}}}$, alors l'image de ψ est un sous-groupe algébrique fermé de dimension 1 de G''.

Dans certains cas particuliers on peut raffiner la conclusion du théorème 4.2.1. En voici deux exemples (les démonstrations seront données au § 4.3).

REMARQUE 4.2.3 - Sous les hypothèses du théorème 4.2.1, on suppose que φ admet une période ω non nulle :

$$\varphi(z + \omega) = \varphi(z) .$$

Alors

$$\ell d < \ell + 2d .$$

REMARQUE 4.2.4 - Soient G un groupe algébrique commutatif connexe défini sur $\overline{\mathbb{Q}}$, $\varphi : \mathbb{C} \to G_{\mathbb{C}}$ un sous-groupe à 1 paramètre de G, et $\chi : \mathbb{C} \to \mathbb{C}^* \times G_{\mathbb{C}}$ le sous-groupe à 1 paramètre de $G_m \times G$ défini par

$$z \mapsto (e^z , \varphi(z)) .$$

Soient d la dimension algébrique de χ, et $t_1, \ldots, t_\ell$ des nombres complexes $\mathbb{Q}$-linéairement indépendants, vérifiant

$$e^{t_j} \in \overline{\mathbb{Q}} , \qquad (1 \leq j \leq \ell)$$

et

$$\varphi(t_j) \in G_{\overline{\mathbb{Q}}} , \qquad (1 \leq j \leq \ell) .$$

Alors

$$\ell d < \ell + 2d .$$

Si, de plus, χ est périodique, c'est-à-dire si φ admet la période $2i\pi$, alors

$$\ell \geq 3 \Rightarrow d = 1 .$$

La conclusion $\ell d < \ell + 2d$ s'écrit aussi

$$\ell \geq 3 \Rightarrow d \leq 2$$

$$\ell \geq 4 \Rightarrow d = 1 .$$

Nous allons déduire des énoncés précédents le corollaire suivant

COROLLAIRE 4.2.5 - Soient G' et G'' deux groupes algébriques commutatifs connexes définis sur $\overline{\mathbb{Q}}$, G' étant de dimension 1. Soit $\psi : G'_{\mathbb{C}} \to G''_{\mathbb{C}}$ un homomorphisme analytique complexe. S'il existe 3 points algébriques dans $G'_{\overline{\mathbb{Q}}}$ linéairement indépendants sur $\mathbb{Z}$ dont les images par ψ soient dans $G''_{\overline{\mathbb{Q}}}$, alors une puissance de ψ est un homomorphisme rationnel.

Cet énoncé améliore un résultat antérieur de Lang [L2] (Chap. II, § 4, Coroll. 2 du Th. 4) où 3 était remplacé par 7. Le lemme 4.1.1 montre qu'on ne peut pas remplacer 3 par 2, donc que le corollaire 4.2.5 est le meilleur possible dans le cas $G' = G_a$. Nous allons voir que si $G' = G_m$, alors on peut remplacer 3 par 2.

Démonstration du corollaire 4.2.5.

Si G' est une courbe elliptique, $G'_{\mathbb{C}}$ est compact, et le résultat est banal.

Si $G' = G_a$, alors ψ est rationnel d'après le théorème 4.1.2.

Il reste à considérer le cas où $G' = G_m$. Soit $\chi : \mathbb{C} \to \mathbb{C}^* \times G''_{\mathbb{C}}$ le sous-groupe à 1 paramètre de $G_m \times G''$ défini par

$$\chi(t) = (e^t , \psi(e^t)) .$$

Soient γ_1, γ_2 deux éléments multiplicativement indépendants de $\mathbb{C}^*$ tels que $\psi(\gamma_1) \in G''_{\overline{\mathbb{Q}}}$, $\psi(\gamma_2) \in G''_{\overline{\mathbb{Q}}}$. On choisit t_1, t_2 dans $\mathbb{C}$ tels que $e^{t_j} = \gamma_j$, $(j = 1,2)$.

Soit $t_3 = 2i\pi$. Alors t_1, t_2, t_3 sont $\mathbb{Q}$-linéairement indépendants, et comme X est périodique, la remarque 4.2.4 montre que le graphe de ψ est algébrique. Comme les seules fonctions méromorphes dans $\mathbb{C}^*$ qui soient algébriques sont les fonctions rationnelles, ψ est un homomorphisme rationnel.

Avec les remarques 4.2.3 et 4.2.4, les théorèmes 4.1.2 et 4.2.1 contiennent le théorème de Ramachandra [Ra] sur les fonctions algébriquement additives, ainsi que des généralisations aux fonctions zêta [Wa 1] et sigma. Nous donnons seulement un exemple, dû à Ramachandra [Ra] (p. 87).

COROLLAIRE 4.2.6 - Soient a et b deux nombres algébriques multiplicativement indépendants, $\log a$ et $\log b$ des déterminations quelconques de leurs logarithmes, et $\wp$ la fonction elliptique de réseau des périodes $\mathbb{Z}\log a + \mathbb{Z}\, 2i\pi$. Alors l'un au moins des deux nombres

$$j\left(\frac{\log a}{2i\pi}\right), \quad (\Delta(\log a\,,\, 2i\pi))^{-1/6}\,\wp(\log b)$$

est transcendant.

K. Mahler [Mah 2] et Yu.I. Manin [Man] ont posé le problème de la transcendance du nombre $j\left(\frac{\log a}{2i\pi}\right)$ (cf. [Be 6]).

Démonstration du corollaire 4.2.6.

Supposons le nombre $j\left(\frac{\log a}{2i\pi}\right)$ algébrique. Avec les notations habituelles (cf. la démonstration du lemme 3.2.4) on pose

$$\Delta = \Delta(\log a\,,\, 2i\pi) = (\log a)^{-12}\,\Delta\left(1, \frac{2i\pi}{\log a}\right),$$

et on choisit une racine douzième de Δ. La fonction

$$\wp^*(z) = \Delta^{-1/6}\,\wp(\Delta^{-1/12} z)$$

est une fonction elliptique de Weierstrass ayant des invariants g_2^*, g_3^* algébriques. Soit $\mathcal{E}^*$ la courbe elliptique correspondante, et soit $P^* = (1, \wp^*, (\wp^*)')$. Comme $2i\pi$ est période de $P^*(\Delta^{1/12} z)$, il existe un homomorphisme analytique complexe $\varphi : G_m \to \mathcal{E}^*_{\mathbb{C}}$ tel que $\varphi(e^z) = P^*(\Delta^{1/12} z)$. On applique alors la remarque qui suit le corollaire 4.2.5, avec les 2 points a et b.

Voici une autre conséquence de la remarque 4.2.4.

COROLLAIRE 4.2.7 - Soient A une variété abélienne définie sur $\overline{\mathbb{Q}}$, $\varphi : \mathbb{C} \to A_{\mathbb{C}}$ un sous-groupe à 1 paramètre de A, $\log\alpha_1, \ldots, \log\alpha_\ell$ des logarithmes $\mathbb{Q}$-linéairement indépendants de nombres algébriques. Si $\varphi(\log\alpha_j) \in A_{\overline{\mathbb{Q}}}$ pour $1 \leq j \leq \ell$, alors $\ell \leq 3$. De plus, si $\ell = 3$, alors $\varphi(\mathbb{C})$ est une courbe elliptique.

Ainsi, pour étudier le cas $\ell = 3$, on est amené à un problème analogue au théorème des 6 exponentielles (cf. 1.1.7) : soient $\log\alpha_1$, $\log\alpha_2$, $\log\alpha_3$ des logarithmes $\mathbb{Q}$-linéairement indépendants de nombres algébriques, et u_1, u_2, u_3 des points algébriques d'une fonction elliptique $\wp$ (avec g_2, g_3 algébriques). Peut-on avoir

$$\frac{u_1}{\log\alpha_1} = \frac{u_2}{\log\alpha_2} = \frac{u_3}{\log\alpha_3} \ ?$$

Quand on choisit pour G dans le théorème 4.2.1 un produit de courbes elliptiques, on obtient l'énoncé suivant (qui peut aussi être déduit des résultats de Ramachandra). Soient $\wp_1, \ldots, \wp_d$ des fonctions elliptiques de Weierstrass, d'invariants algébriques. Soit ℓ un entier, avec $\ell d > \ell + 2d$, et, pour $1 \leq j \leq d$, soient $u_{1,j}, \ldots, u_{\ell,j}$ des points algébriques $\mathbb{Q}$-linéairement indépendants de $\wp_j$. On suppose que les fonctions $\wp_1(u_{1,1}z), \ldots, \wp_d(u_{1,d}z)$ sont algébriquement indépendantes. Alors la matrice

$$(u_{i,j})_{1 \leq i \leq \ell,\ 1 \leq j \leq d}$$

a un rang supérieur ou égal à 2.

(La condition d'indépendance algébrique des fonctions $\wp_j(u_{1,j}z)$, $1 \leq j \leq d$, peut s'exprimer simplement en terme des algèbres d'endomorphismes des $\wp_j$; cf. [Br-K]).

Ce résultat est encore loin de ce que l'on espère, mais les remarques précédentes conduisent à des améliorations dans certains cas particuliers. Ainsi, d'après 4.2.3, si $\wp$ est une fonction elliptique d'invariants g_2, g_3 algébriques, et si (ω_1, ω_2) est un couple fondamental de périodes de $\wp$, avec $\tau = \omega_2/\omega_1$, alors les 3 nombres $\omega_2\tau$, $\omega_2\tau^2$, $\omega_2\tau^3$ sont des points algébriques de $\wp$ si et seulement si $\wp$ a multiplication complexe.

Pour améliorer ces résultats, il conviendrait de développer les méthodes d'indépendance algébrique. Grâce à Altman [Al] dans le cas abélien, et à Serre (Appendice II) dans le cas général, on peut même considérer des groupes algébriques définis sur une extension K de $\mathbb{Q}$ de type fini (cf. [L 2] p. 54). Il n'y a aucune difficulté à obtenir des énoncés dans lesquels on impose un type de transcendance à K, mais les méthodes de Chudnovsky [C 1], [C 2] devraient permettre de se débarrasser de cette restriction.

Pour l'énoncé le plus général qu'on puisse espérer, voir la conjecture de Grothendieck [L 2] (p. 42-44), [L 3] (§ 4) ainsi que les travaux récents de Deligne, Ribet et Shimura.

§ 4.3 - Démonstrations.

Nous allons démontrer les théorèmes 4.1.2 et 4.2.1, et les remarques 4.2.3 et 4.2.4. Grâce aux résultats du § 1.1.b, il suffit que l'on montre l'existence d'un plongement de G dans un espace projectif $\mathbf{P}_\nu(\mathbf{C})$, tel que φ ait des coordonnées projectives $(\varphi_0, \dots, \varphi_\nu)$ pour lesquelles les fonctions φ_j/φ_0 soient d'ordre arithmétique ≤ 2 sur Γ.

Nous énonçons ce résultat sous une forme un peu plus générale pour pouvoir l'appliquer au chapitre 8.

LEMME 4.3.1 - Soient G un groupe algébrique commutatif connexe défini sur $\overline{\mathbb{Q}}$, $\varphi : \mathbf{C}^n \to G_{\mathbf{C}}$ un homomorphisme analytique, et Γ un sous-groupe de type fini de $\mathbf{C}^n$ tel que $\varphi(\Gamma) \subset G_{\overline{\mathbb{Q}}}$. Alors il existe un plongement de G dans un espace projectif $\mathbf{P}_\nu(\mathbf{C})$ tel que φ ait des coordonnées projectives $(\varphi_0, \dots, \varphi_\nu)$ où $\varphi_0, \dots, \varphi_\nu$ sont entières d'ordre ≤ 2 et que l'application méromorphe $\left(\frac{\varphi_1}{\varphi_0}, \dots, \frac{\varphi_\nu}{\varphi_0}\right)$ soit d'ordre arithmétique ≤ 2 sur Γ.

Nous vérifierons l'axiome 0.A.2 sous la forme plus précise donnée par le lemme 1.1.8.

Démonstration du lemme 4.3.1.

Soit K un corps de nombres sur lequel G est défini, et tel que $\varphi(\Gamma) \subset G_K$. D'après le théorème de Chevalley 1.2.1, G est extension d'une variété abélienne A de dimension g définie sur K, par un groupe linéaire L de dimension h défini sur K. Notons $p_1 : \mathbf{C}^g \times \mathbf{C}^h \to \mathbf{C}^g$ la première projection, et $D = g + h$ la dimension de G.

D'après Serre (Appendice II, § 3) il existe une représentation

$$\psi = (\psi_0, \dots, \psi_\nu) : \mathbf{C}^g \times \mathbf{C}^h \to \mathbf{P}_\nu(\mathbf{C})$$

de l'exponentielle de G, telle que $\psi_0, \dots, \psi_\nu$ soient des fonctions entières dans $\mathbf{C}^D$ d'ordre ≤ 2, $\psi_0(0) \neq 0$, et $\psi_0 = \theta \circ p_1$, où θ est une fonction thêta relative à un réseau de $\mathbf{C}^g$.

Soit $\mathcal{L} : \mathbf{C}^n \to \mathbf{C}^g \times \mathbf{C}^h$ une application linéaire telle que $\varphi = \psi \circ \mathcal{L}$, et soit $\varphi_j = \psi_j \circ \mathcal{L}$, $(0 \leq j \leq \nu)$. Si l'application $p_1 \circ \mathcal{L}$ est nulle, alors

$$\mathcal{L}(\mathbf{C}^n) \subset \{0\} \times \mathbf{C}^h ,$$

donc $\varphi(\mathbf{C}^n) \subset L_{\mathbf{C}}$, et le lemme est banal. Si $\mathcal{L}_1 = p_1 \circ \mathcal{L}$ n'est pas nulle, les lemmes 1.1.8 et 1.2.2 permettent de vérifier l'axiome 0.A.2.

D'autre part, comme $\varphi(\Gamma) \subset G_K$, on a $\frac{\varphi_j}{\varphi_0}(\gamma) \in K$ pour $\gamma \in \Gamma$ tel que $\varphi_0(\gamma) \neq 0$, $(1 \leq j \leq \nu)$.

L'axiome 0.A.1 résulte alors de l'équivalence entre les différentes notions de hauteur (cf. § 1.1.d) et du fait que la hauteur logarithmique sur G_K relative au plongement choisi soit d'ordre ≤ 2 (cf. Serre Appendice II, § 2).

Démonstration du théorème 4.1.2.

On choisit parmi les fonctions φ_j/φ_0, $(1 \leq j \leq \nu)$, une fonction f qui n'est pas rationnelle, et on utilise le théorème 1.1.5 avec $d = 2$, $f_1(z) = z$, $f_2(z) = f(z)$, $\rho_1 = \epsilon$, $\rho_2 = 2$. La conclusion s'écrit $\ell \leq 2$. (Comme la dimension algébrique de φ n'intervient pas, on aurait pu se contenter de la démonstration dans le cas abélien ; cf. [Wa 3] I th. 6.2).

Démonstration du théorème 4.2.1.

Soient d la dimension algébrique de φ, et $f_1, \dots, f_d$ une base de transcendance sur $\overline{\mathbb{Q}}$ de $\overline{\mathbb{Q}}\left(\frac{\varphi_1}{\varphi_0}, \dots, \frac{\varphi_\nu}{\varphi_0}\right)$, avec $f_j \in \left\{\frac{\varphi_1}{\varphi_0}, \dots, \frac{\varphi_\nu}{\varphi_0}\right\}$, $1 \leq j \leq d$. On utilise le théorème 1.1.5 avec $\rho_1 = \dots = \rho_d = 1$; pour $d \geq 2$, la conclusion est $\ell \leq \frac{2d}{d-1}$.

Démonstration de la remarque 4.2.3.

Si φ admet une période $\omega \neq 0$, il en est de même des fonctions $\frac{\varphi_i}{\varphi_0}$, $(1 \leq i \leq \nu)$; la remarque 1.1.6 conduit, pour $d \geq 2$, à l'inégalité $\ell \leq \frac{2d-1}{d-1}$, ce qui équivaut à $\ell d < \ell + 2d$.

Démonstration de la remarque 4.2.4.

On choisit $f_1(z) = e^z$, et on complète par une base de transcendance $f_1, f_2, \dots, f_d$ de $\overline{\mathbb{Q}}\left(e^z, \frac{\varphi_1}{\varphi_0}, \dots, \frac{\varphi_\nu}{\varphi_0}\right)$, avec $f_j \in \left\{\frac{\varphi_1}{\varphi_0}, \dots, \frac{\varphi_\nu}{\varphi_0}\right\}$, $(2 \leq j \leq d)$, $\rho_1 = 1$, $\rho_2 = \dots = \rho_d = 2$.

CHAPITRE 5.

SOUS-GROUPES NORMALISÉS À PLUSIEURS PARAMÈTRES.

Soit $\varphi : \mathbb{C}^n \to G_{\mathbb{C}}$ un sous-groupe à n paramètres d'un groupe algébrique G défini sur $\overline{\mathbb{Q}}$. On suppose φ normalisé de telle manière que sa dérivée à l'origine soit algébrique : $\varphi = \exp \circ \mathcal{L}$, où l'application linéaire $\mathcal{L} : \mathbb{C}^n \to T_G(\mathbb{C})$ est définie sur $\overline{\mathbb{Q}}$.

D'après l'étude précédente, le premier problème naturel concerne la nature arithmétique des coordonnées des points $u \in \mathbb{C}^n$ tels que $\varphi(u) \in G_{\overline{\mathbb{Q}}}$. Il est naturel d'espérer que, sous des hypothèses convenables sur l'irrationalité de φ, les coordonnées non nulles de u soient transcendantes, et même que toute combinaison linéaire à coefficients algébriques de ces coordonnées soit nulle ou transcendante. Nous avons vu comment, dans le cas d'une variété linéaire, ce problème se ramenait au théorème de Baker sur l'indépendance linéaire de logarithmes usuels (cf. § 2.4). Dans le cas général ce problème est loin d'être résolu et nous verrons au chapitre suivant l'état actuel de nos connaissances dans le cas des variétés abéliennes.

Le deuxième problème, qui est l'objet du présent chapitre, concerne la dimension algébrique de φ : s'il existe n points de $\mathbb{C}^n$, $\mathbb{C}$-linéairement indépendants, dont les images par φ soient dans $G_{\overline{\mathbb{Q}}}$, alors la dimension algébrique de φ est égale à n. Ce résultat, dû à S. Lang, conduit à d'intéressantes généralisations du théorème de Schneider sur la fonction modulaire.

§ 5.1 - Le critère de transcendance de Bombieri.

Le critère 1.1.1. de Schneider Lang montre qu'un certain sous-ensemble de $\mathbb{C}$ (ensemble des points où des fonctions méromorphes, satisfaisant des équations différentielles, prennent simultanément des valeurs algébriques) est fini. En 1963, Lang (cf. [L 2] chap. IV § 1 Thm 1) a étendu ce critère à plusieurs variables, montrant que le sous-ensemble S correspondant de $\mathbb{C}^n$ ne peut pas contenir un produit $S_1 \times \ldots \times S_n$, avec $S_i \subset \mathbb{C}$ et $\operatorname{Card} S_i = +\infty$, $(1 \leq i \leq n)$. Nagata avait conjecturé que cet ensemble S était contenu dans une hypersurface algébrique ([L . 2] chap. IV) suggérant ainsi que le rôle du nombre $\operatorname{Card} S$, quand $n = 1$, peut être joué par le nombre $\omega_1(S)$ quand $n \geq 1$ (où $\omega_1(S)$ est le plus petit degré des hypersurfaces

algébriques passant par S, cf § 1.3). Cette conjecture de Nagata a été résolue par Bombieri [Bom].

THÉORÈME 5.1.1 - Soient K un corps de nombres, et $f_1, \ldots, f_h$ des fonctions méromorphes dans $\mathbb{C}^n$ avec $h \geq n+1$. On suppose que $f_1, \ldots f_{n+1}$ sont algébriquement indépendantes sur $\mathbb{Q}$ et sont d'ordre strict $\leq \rho_1, \ldots, \rho_{n+1}$ respectivement. On suppose de plus que les dérivations partielles $\frac{\partial}{\partial z_i}$, $(1 \leq i \leq n)$ laissent stable l'algèbre $K[f_1, \ldots, f_h]$.

Alors l'ensemble S des $w \in \mathbb{C}^n$, où $f_1, \ldots, f_h$ sont régulières et tels que

$$f_j(w) \in K \quad \text{pour} \quad 1 \leq j \leq h$$

est contenu dans une hypersurface algébrique de degré au plus

$$n(\rho_1 + \ldots + \rho_{n+1})\ [K : \mathbb{Q}].$$

Nous démontrerons ce théorème au § 5.4, ainsi que le corollaire suivant [L 2] (chap. IV § 1 Th. 1) qui en constitue la partie utile pour les applications.

COROLLAIRE 5.1.2 - Avec les notations du théorème 5.1.1, si $x_1, \ldots, x_n$ est une base de $\mathbb{C}^n$, et si pour $1 \leq j \leq n$, S_j est un sous-ensemble de $\mathbb{C}$, avec

$$S \supset \{s_1 x_1 + \ldots + s_n x_n \ ; \ (s_1, \ldots, s_n) \in S_1 \times \ldots \times S_n\},$$

alors

$$\min_{1 \leq j \leq n} \operatorname{Card} S_j \leq n\,(\rho_1 + \ldots + \rho_{n+1})\ [K : \mathbb{Q}].$$

En particulier S ne contient pas $\mathbb{Z} x_1 + \ldots + \mathbb{Z} x_n$.

§ 5.2. Applications aux homomorphismes analytiques normalisés de $\mathbb{C}^n$ dans $G_{\mathbb{C}}$.

a) Le théorème principal.

Tous les résultats de transcendance que nous déduirons du critère de Bombieri proviennent de l'énoncé suivant, qui généralise à plusieurs variables le théorème 3.1.1 (cf. [L 2] chap. IV § 4 Th. 2).

THÉORÈME 5.2.1 - Soient G un groupe algébrique commutatif connexe défini sur $\overline{\mathbb{Q}}$, $\varphi : \mathbb{C}^n \to G_{\mathbb{C}}$ un homomorphisme analytique normalisé, et Γ un sous-groupe de $\mathbb{C}^n$ contenant n éléments $\mathbb{C}$-linéairement indépendants, tel que $\varphi(\Gamma) \subset G_{\overline{\mathbb{Q}}}$.

Alors la dimension algébrique de φ est inférieure ou égale à n.

Par conséquent si φ est un sous-groupe à n paramètres de G, $\varphi(\mathbb{C}^n)$ est un sous-groupe algébrique fermé de G de dimension n.

Nous avons déjà vu ce résultat dans le cas linéaire (2.4.6). Dans le cas général, la démonstration est celle du théorème 3.1.1, en y remplaçant le théorème de Schneider Lang par le corollaire 5.1.2.

Nous allons étudier des conséquences du théorème 5.2.1 pour des variétés abéliennes, puis pour des extensions de variété abélienne par le groupe additif ou multiplicatif. Les premiers résultats dans ce domaine sont aussi dus à Th. Schneider et concernaient les jacobiennes [S 2] ; nous verrons pour terminer le théorème de Schneider sur la fonction bêta.

b) Variétés abéliennes.

Le résultat suivant avait été démontré par Schneider [S 2] (th. I) dans le cas particulier où les variétés abéliennes A_j sont des jacobiennes.

COROLLAIRE 5.2.2 - Soient $A_1, \dots, A_h$ des variétés abéliennes de dimension g, définies sur $\overline{\mathbb{Q}}$. Pour $1 \leq j \leq h$, soit $\Theta_j : \mathbb{C}^g \to A_j$ un homomorphisme thêta normalisé, et soit $\Omega_j = \ker \Theta_j$. Si $\Omega_1 \cap \dots \cap \Omega_h$ contient g éléments $\mathbb{C}$-linéairement indépendants, alors le sous-groupe à g paramètres

$$z \mapsto (\Theta_1(z), \dots, \Theta_h(z))$$

de $A_1 \times \dots \times A_h$ a pour dimension algébrique g.

Ce résultat signifie que $g+1$ fonctions abéliennes dans $\mathbb{C}^g$ définies sur $\overline{\mathbb{Q}}$ et admettant g périodes communes sont algébriquement dépendantes. Nous en verrons une application au § 5.3. Dans le cas $g = 1$, c'est un cas particulier du théorème 3.2.2.

c) Produit d'une variété abélienne par le groupe additif.

Si $x = (x_1, \dots, x_g)$ et $y = (y_1, \dots, y_g)$ sont deux éléments de $\mathbb{C}^g$, on note

$$< x , y > = x_1 y_1 + \dots + x_g y_g .$$

Considérons dans le produit $G_a \times A$, le sous-groupe à g paramètres normalisé

$$z \to (< \beta , z > ; \Theta(z)) ,$$

dont la dimension algébrique est $g+1$ quand β est un élément non nul de $\overline{\mathbb{Q}}^g$.

COROLLAIRE 5.2.3 - Soient A une variété abélienne de dimension g définie sur $\overline{\mathbb{Q}}$, $\Theta : \mathbb{C}^g \to A_{\mathbb{C}}$ un homomorphisme thêta normalisé, et $\omega_1, \dots, \omega_g$ des périodes $\mathbb{C}$-linéairement indépendantes de Θ. Pour $1 \leq j \leq g$, soient $\omega_{j,1}, \dots, \omega_{j,g}$ les coordonnées de ω_j dans $\mathbb{C}^g$. Si β est un élément non nul de $\overline{\mathbb{Q}}^g$, alors l'un

au moins des g nombres

$$< \beta, \omega_j > = \beta_1 \omega_{j,1} + \dots + \beta_g \omega_{j,g} , \quad (1 \leq j \leq g)$$

est transcendant.

En choisissant $\beta \in \overline{\mathbb{Q}}^g$ avec toutes ses coordonnées nulles sauf une, on voit que dans la matrice

$$(\omega_1, \dots, \omega_g) = \begin{pmatrix} \omega_{1,1} & \cdots & \omega_{g,1} \\ \cdot\,\cdot & \cdots & \cdot\,\cdot \\ \omega_{1,g} & \cdots & \omega_{g,g} \end{pmatrix}$$

il y a au moins un élément transcendant sur chacune des lignes. D'après 3.1.4, il en est de même sur chacune des colonnes (cf. [Be 2]).

d) Extension d'une variété abélienne par le groupe additif.

Soient A une variété abélienne de dimension g et η une forme différentielle de seconde espèce sur A ; η s'étend en une application $\mathbb{R}$-linéaire de $T_A(\mathbb{C})$ dans $\mathbb{C}$ dont on considère les $2g$ périodes sur le noyau Ω de l'exponentielle de A. On dira que η est triviale si elle est somme d'une différentielle de première espèce et d'une différentielle exacte.

COROLLAIRE 5.2.4 - Soient A une variété abélienne de dimension g définie sur $\overline{\mathbb{Q}}$, $\Omega \subset T_A(\mathbb{C})$ le noyau de l'exponentielle de A, $\omega_1, \dots, \omega_g$ des éléments $\mathbb{C}$-linéairement indépendants de Ω, et η une forme différentielle de seconde espèce sur A définie sur $\overline{\mathbb{Q}}$, non triviale. Alors un au moins des g nombres

$$\eta(\omega_j), \quad (1 \leq j \leq g)$$

est transcendant.

Démonstration du corollaire 5.2.4.

On déduit le corollaire 5.2.4 du théorème 5.2.1 de la manière suivante. Soit G l'extension de A par G_a associée à η ; on décompose l'espace tangent à l'origine de G :

$$T_G(\mathbb{C}) = T_A(\mathbb{C}) \oplus \mathbb{C},$$

et on considère l'homomorphisme $\varphi : T_A(\mathbb{C}) \to G_{\mathbb{C}}$ défini par $\varphi(z) = \exp_G(z, 0)$.

Comme la forme différentielle η n'est pas triviale, l'image de φ est dense dans $G_{\mathbb{C}}$; le théorème 5.2.1 montre que l'image par φ de $\mathbb{Z}\omega_1 + \dots + \mathbb{Z}\omega_g$ n'est pas contenue dans $G_{\overline{\mathbb{Q}}}$, d'où le corollaire 5.2.4.

Soient $\eta_1, \dots, \eta_g$ g formes différentielles de deuxième espèce telles que les extensions $G_1, \dots, G_g$ de A par $\mathbf{G}_a$ forment une base sur $\mathbf{C}$ de $\mathrm{Ext}(A, \mathbf{G}_a)$. Si Θ est un homomorphisme thêta de A, on peut paramétrer, pour $1 \leq j \leq g$, l'exponentielle de G_j grâce à Θ et à une fonction H_j méromorphe dans $\mathbf{C}^g$ telle que

$$H_j(z+\omega) = H_j(z) + \eta_j(\omega), \qquad (\omega \in \ker \Theta).$$

Ces fonctions $H_1, \dots, H_g$ sont algébriquement indépendantes sur le corps des fonctions abéliennes par rapport à $\ker \Theta$. On le voit par exemple de la manière suivante : pour $1 \leq j \leq g$, soit φ_j l'homomorphisme de $T_{G_j}(\mathbf{C}) = T_A(\mathbf{C}) \oplus \mathbf{C}$ dans G_j défini par $\varphi_j(z, t) = \exp_{G_j}(z, 0)$; alors l'image de $\varphi_1 \times \dots \times \varphi_g$ est dense dans $G_1 \times \dots \times G_g$. (Voir à ce sujet [C 1] où se trouvent les premiers éléments d'une étude de l'indépendance algébrique des $2g^2$ nombres

$$\omega_{j,i}, \ \eta_i(\omega_j), \ (1 \leq i, j \leq g)).$$

Quand A est une variété abélienne simple de dimension 2, Masser [M 5] a démontré la transcendance de chacun des nombres considérés dans les corollaires 5.2.3 et 5.2.4. Voici son énoncé sans démonstration.

THÉORÈME 5.2.5 - Sous les hypothèses des corollaires 5.2.3 et 5.2.4 avec $g = 2$ et A simple, soit $\omega = (\omega^1, \omega^2)$ une période non nulle de Θ ; alors les 5 nombres

$$1, \omega^1, \omega^2, \eta_1(\omega), \eta_2(\omega)$$

sont linéairement indépendants sur $\overline{\mathbf{Q}}$.

Si la variété abélienne A de dimension 2 n'est pas simple (c'est-à-dire est isogène à un produit de deux courbes elliptiques), Masser a également déterminé la dimension du $\overline{\mathbf{Q}}$- espace vectoriel engendré par ces 5 nombres [M 5], [B-M] Chap. 6.

e) Produit d'une variété abélienne par le groupe multiplicatif.

En considérant dans le produit $\mathbf{G}_m \times A$ un sous-groupe normalisé à g paramètres

$$z \mapsto (\exp \langle \beta, z \rangle, \Theta(z)),$$

on déduit du théorème 5.2.1 le corollaire suivant

COROLLAIRE 5.2.6 - Soient A une variété abélienne définie sur $\overline{\mathbf{Q}}$, $\Theta : \mathbf{C}^g \to A_{\mathbf{C}}$ un homomorphisme thêta normalisé, $\omega_1, \dots, \omega_g$ des périodes $\mathbf{C}$- linéairement indépendantes de Θ, et β un élément non nul de $\overline{\mathbf{Q}}^g$. Alors l'un au moins des g nombres

$$\exp \langle \beta, \omega_j \rangle, \qquad (1 \leq j \leq g)$$

est transcendant.

Ainsi, quand α est un nombre algébrique non nul, et h un entier, l'un au moins des g nombres

$$e^{\alpha \omega_{j,h}}, \qquad (1 \leq j \leq g)$$

est transcendant (on a noté comme précédemment $\omega_j = (\omega_{j,1}, \dots, \omega_{j,g})$). Dans le cas $g = 1$, on retrouve la transcendance du nombre $e^{\beta\omega}$ pour ω période non nulle de $\wp$ et $\beta \in \overline{\mathbf{Q}}$, $\beta \neq 0$ (cf. 3.2.8).

f) Extension d'une variété abélienne par le groupe multiplicatif.

Considérons maintenant un groupe algébrique G de dimension $g+1$, défini sur $\overline{\mathbf{Q}}$, extension de A par $\mathbf{G}_m$. On peut représenter son application exponentielle à l'aide d'un homomorphisme thêta (que nous choisissons normalisé) de A et d'une fonction $(z, t) \to F(z) e^t$ méromorphe dans $\mathbf{C}^{g+1}$, où F est une fonction méromorphe dans $\mathbf{C}^g$ telle que pour tout $\omega \in \Omega = \ker \Theta$ il existe $\lambda(\omega) \in \mathbf{C}$ avec

$$F(z+\omega) = F(z) e^{\lambda(\omega)}.$$

Nous supposerons que cette fonction F correspond à une représentation normalisé de l'application exponentielle de G, c'est-à-dire que les fonctions $(\frac{\partial}{\partial z_j} F) / F$, $(1 \leq j \leq g)$ sont $\overline{\mathbf{Q}}$ rationnelles sur A (quand $g = 1$, cette condition est remplie quand on choisit $\beta \in \overline{\mathbf{Q}}$ et

$$F(z) = \frac{\sigma(z-u_0)}{\sigma(z)\sigma(u_0)} e^{(\beta + \zeta(u_0))z} ;$$

cf. § 3.2. e).

COROLLAIRE 5.2.7 - Si G n'est pas isogène au produit $\mathbf{G}_m \times A$, et si $\omega_1, \dots, \omega_g$ sont g périodes $\mathbf{C}$- linéairement indépendantes, alors l'un des g nombres

$$\exp \lambda(\omega_j), \qquad (1 \leq j \leq g)$$

est transcendant.

L'hypothèse que G n'est pas isogène à $\mathbf{G}_m \times A$ montre que le sous-groupe à g paramètres

$$z \mapsto (F(z), \Theta(z))$$

a pour dimension algébrique $g+1$ (autrement dit a une image dense). Quand G est isogène à $\mathbb{G}_m \times A$, s'il suffit d'ajouter l'hypothèse que l'un des nombres $\exp \lambda(\omega_j)$, $(1 \leq j \leq g)$ n'est pas une racine de l'unité.

g) Application à la fonction bêta.

Soit $\mathcal{L}$ une courbe algébrique sans singularité de genre g dans $\mathbf{P}_2(\mathbf{C})$. Soient S la surface de Riemann de $\mathcal{L}$, $(C_j)_{1 \leq j \leq g}$ une base de l'espace de son homologie en dimension 1, et $(\xi_h)_{1 \leq h \leq g}$ une base de l'espace des formes différentielles de première espèce sur S. Pour $1 \leq j \leq 2g$, on note ω_j l'élément de $\mathbf{C}^g$ de composantes $(\omega_{1,j}, \ldots, \omega_{g,j})$ où

$$\omega_{h,j} = \int_{C_j} \xi_h \, , \quad (1 \leq h \leq g).$$

Soit Ω le réseau $\mathbf{Z}\,\omega_1 + \ldots + \mathbf{Z}\,\omega_{2g}$. La variété abélienne $\mathbf{C}^g/\Omega$ est la jacobienne de $\mathcal{L}$.

On suppose que la courbe $\mathcal{L}$ et les formes différentielles $\xi_1, \ldots, \xi_g$ sont définies sur $\overline{\mathbf{Q}}$; la jacobienne de $\mathcal{L}$ est une variété abélienne définie sur $\overline{\mathbf{Q}}$.

Soit ξ une forme différentielle non exacte de première ou de deuxième espèce, définie sur $\overline{\mathbf{Q}}$. Les corollaires 5.2.3 et 5.2.4 s'énoncent sous la forme suivante (qui était la formulation originale de Schneider [S 2] p. 113).

Si $\omega_1, \ldots, \omega_g$ sont $\mathbf{C}$-linéairement indépendants, alors l'un au moins des g nombres

$$\int_{C_j} \xi \, , \qquad (1 \leq j \leq g)$$

est transcendant.

En particulier l'un au moins des $2g$ nombres $\int_{C_j} \xi$, $(1 \leq j \leq 2g)$ est transcendant.

En voici une application [S 2] (p.113) concernant la fonction bêta.

THÉORÈME 5.2.8 - Soient a et b deux nombres non entiers tels que $-a$ $-b$ ne soit pas un entier ≥ 0. Alors le nombre

$$B\,(a\,,b) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}$$

est transcendant.

Démonstration du théorème 5.2.8.

Grâce à l'équation fonctionnelle de la fonction gamma, on peut supposer $0 < a < 1$, $0 < b < 1$. De plus, comme le nombre

$$B\,(a\,,1-a) = \Gamma(a)\,\Gamma(1-a) = \frac{\pi}{\sin a\pi}$$

est transcendant (pour a rationnel, $0 < a < 1$), on peut supposer $a+b \neq 1$. On écrit $a = \frac{r}{q}$, $b = 1 - \frac{s}{q}$, où p, q, r, s, sont des entiers positifs, $(r\,,p) = 1$, $(s\,,q) = 1$. On considère la courbe algébrique $\mathcal{L}$ d'équation non homogène

$$x^p + y^q = 1.$$

Comme

$$B(a\,,b) = \int_0^1 t^{a-1}(1-t)^{b-1}\,dt = p\int_0^1 x^{r-1}\,y^{-s}\,dx\,,$$

on considère la forme différentielle

$$\xi = x^{r-1}\,y^{-s}\,dx$$

Elle est de première espèce si $a+b < 1$, de deuxième espèce si $a+b > 1$. On peut extraire une base de l'homologie en dimension 1 à partir des chemins joignant les points ∞ et ζ_p^k, $(0 \leq k \leq p-1)$, où ζ_p est une racine primitive p-ième de l'unité. Par un changement de variable on voit que

$$\int_{C_j} \xi = \alpha_j\,B(a\,,b),$$

où α_j est un élément non nul de $\mathbf{Q}(\zeta_p)$. On en déduit le théorème 5.2.8.

Dans cet exemple le théorème de Schneider qui concerne une forme différentielle fixe et affirme la transcendance de l'un des nombres $\int_{C_j} \xi$, $(1 \leq j \leq g)$, donc, dans le cas de première espèce, la transcendance d'une au moins des composantes sur chaque ligne de la matrice $(\omega_1, \ldots, \omega_{2g}) = (\omega_{h,j})$, est plus précis que celui de Lang sur la transcendance d'une composante au moins de chaque colonne. La démonstration du théorème 5.2.8 de Schneider sur la fonction bêta nécessite plusieurs variables complexes (cf. [Be 2].)

Le théorème 5.2.5 peut être formulé ainsi [M 5] : supposons que la courbe $\mathcal{L}$ soit de genre 2 et que sa jacobienne ne soit pas isogène au produit de deux courbes elliptiques ; soient ξ une forme différentielle non exacte de première ou de deuxième espèce, définie sur $\overline{\mathbf{Q}}$, et C un chemin fermé sur S non homologue à 0 ; alors le nombre

$$\int_C \xi$$

est transcendant.

En voici une conséquence [M 5] : les cinq nombres $B\left(\frac{1}{2}\,,\frac{1}{5}m\right)$, $(1 \leq m \leq 5)$ sont linéairement indépendants sur $\overline{\mathbf{Q}}$.

Pour le voir, on considère la courbe $\mathcal{L}$ d'équation $y^2 t^4 + x^6 - x t^5 = 0$ dans $\mathbb{P}_2(\mathbb{C})$, les différentielles de première espèce $\xi_1 = \frac{dx}{y}$, $\xi_2 = x\frac{dx}{y}$, et les différentielles de deuxième espèce $\xi_3 = x^3 \frac{dx}{y}$, $\xi_4 = x^4 \frac{dx}{y}$.

La jacobienne de $\mathcal{L}$ est une variété abélienne simple de type C.M. et de dimension $g = 2$ (cf. § 6.1 ; si $\zeta^5 = 1$, on a un endomorphisme $t \mapsto t$, $x \mapsto \zeta x$, $y \mapsto \zeta^3 y$). On déduit de 5.2.5 l'indépendance linéaire sur $\overline{\mathbb{Q}}$ des cinq nombres

$$1, \int_0^1 \xi_1, \ldots, \int_0^1 \xi_4,$$

et le résultat annoncé s'en déduit.

Pour de plus amples renseignements sur les propriétés arithmétiques de valeurs de la fonction gamma, on pourra consulter [Be 2], [Gr], [M5], [C1] [La 1], et [M8] § II. Les seuls nombres rationnels entre 0 et 1 où l'on sache que la fonction gamma prend des valeurs transcendantes sont

$$1/6,\ 1/4,\ 1/3,\ 1/2,\ 2/3,\ 3/4,\ 5/6.$$

On sait seulement que deux des nombres π, $\Gamma(1/5)$, $\Gamma(2/5)$ sont algébriquement indépendants, mais on conjecture [C1] que si ℓ est un nombre premier impair, les $\frac{\ell+1}{2}$ nombres

$$\pi, \Gamma(1/\ell), \ldots, \Gamma((\ell-1)/2\ell)$$

sont algébriquement indépendants. Plus généralement, Rohrlich conjecture que les relations de distribution de la fonction $(2\pi)^{-1/2}\,\Gamma(z) = G(z)$: pour N entier positif,

$$\prod_{i=0}^{N-1} G\left(x+\frac{i}{N}\right) = N^{-x+\frac{1}{2}}\, G(Nx)$$

(pour $x \in \mathbb{C}$ tel que $Nx \notin \mathbb{Z}$) et la parité

$$G(-x) = G(x)^{-1}$$

engendrent un idéal de définition sur les nombres algébriques pour toutes les relations algébriques des valeurs de la fonction gamma pour $x \in \mathbb{Q}$, $x \neq 0$ (cf. S. Lang, relations de distributions et exemples classiques, Sém. Delange Pisot Poitou 1977/78).

Revenons aux intégrales abéliennes. Soit ξ une forme différentielle abélienne de troisième espèce (sans pôles d'ordre ≥ 2) définie sur $\overline{\mathbb{Q}}$ dont le diviseur résidu est à coefficients dans $\mathbb{Z}$. Si $\omega_1, \ldots, \omega_g$ sont $\mathbb{C}$-linéairement indépendants, et si g nombres

$$\exp\left(\int_{C_j} \xi\right), \qquad (1 \leq j \leq g)$$

ne sont pas tous racines de l'unité, alors le corollaire 5.2.7 montre que l'un au moins d'entre eux est transcendant

§ 5.3 - <u>Généralisations du théorème de Schneider sur la fonction modulaire</u>.

Nous déduisons du critère de transcendance 5.1.2 des analogues en dimension supérieure du théorème de Schneider sur la fonction modulaire j (corollaire 3.2.4).

a) <u>Endomorphismes de variétés abéliennes</u>

Nous commençons par un énoncé sur les endomorphismes de variétés abéliennes [S 2] (Thm I'), [L 2] (ch. IV § 4 Th 4), [Mor] (Th. 2).

Soient A une variété abélienne définie sur une extension algébrique K de $\mathbb{Q}$, $\Theta : \mathbb{C}^g \to A_{\mathbb{C}}$ un homomorphisme thêta normalisé, $\mathcal{F}_K$ le corps des fonctions K-rationnelles sur A, et $\mathcal{F}_{\mathbb{C}} = \mathcal{F}_K \otimes_K \mathbb{C}$ le corps des fonctions abéliennes par rapport à $\Omega = \ker \Theta$. On suppose que les endomorphismes de A sont définis sur K.

THÉORÈME 5.3.1 - <u>Soit $\mathcal{L}$ un endomorphisme $\mathbb{C}$-linéaire de $\mathbb{C}^g$ Les conditions suivantes sont équivalentes</u>.

(i) $\mathcal{L}$ <u>laisse</u> $\Omega \otimes_{\mathbb{Z}} \mathbb{Q}$ <u>stable, c'est-à-dire</u> $\mathcal{L}$ <u>représente un élément de</u> $(\mathrm{End}\, A) \otimes_{\mathbb{Z}} \mathbb{Q}$.

(ii) <u>Si</u> $f \in \mathcal{F}_K$, <u>alors</u> $f \circ \mathcal{L}$ <u>est algébrique sur</u> $\mathcal{F}_K$.

(iii) <u>Il existe</u> $\omega_1, \ldots, \omega_g \in \Omega$, $\mathbb{C}$-<u>linéairement indépendants, tels que</u> $\mathcal{L}(\omega_j) \in \Omega$, $(1 \leq j \leq g)$. <u>De plus l'endomorphisme</u> $\mathcal{L}$ <u>est défini sur</u> K.

<u>Démonstration du théorème 5.3.1</u>.

La seule partie "transcendante" de cet énoncé est l'implication (iii) $\Rightarrow$ (ii), et cette implication est le théorème I' de [S 2]. C'est une conséquence immédiate de son théorème I, c'est-à-dire du corollaire 5.2.2. : on choisit $h = 2$, $\Theta_1 = \Theta$, $\Theta_2 = \Theta \circ \mathcal{L}$, et l'hypothèse que $\mathcal{L}$ est défini sur K signifie que l'homorphisme thêta $\Theta \circ \mathcal{L}$ est normalisé. Si $(\theta_0, \ldots, \theta_\nu)$ sont des coordonnées projectives de Θ, le théorème 5.2.1 montre que le degré de transcendance sur K du corps

$$\mathcal{F}_K\left(\frac{\theta_1}{\theta_0} \circ \mathcal{L}, \ldots, \frac{\theta_\nu}{\theta_0} \circ \mathcal{L}\right)$$

est g, donc ce corps est une extension algébrique finie de $\mathcal{F}_K$.

L' implication (i) $\Rightarrow$ (iii) est banale.

Montrons (ii) $\Rightarrow$ (i). Supposons d'abord qu'il existe un entier $d > 0$ tel que

$$f \in \mathcal{F}_C \Rightarrow f \circ (d\,\mathcal{L}) \in \mathcal{F}_C$$

Comme l'ensemble des périodes communes aux éléments de $\mathcal{F}_C$ est Ω, on en déduit que $d\,\mathcal{L}$ laisse Ω stable. Il suffit par conséquent que l'on démontre le lemme suivant [Mor] (lemme 3).

LEMME 5.3.2 - Soit f une fonction méromorphe dans $\mathbb{C}^g$, algébrique sur $\mathcal{F}_C$. Alors il existe un entier $d > 0$ tel que $z \mapsto f(dz)$ appartienne à $\mathcal{F}_C$.

Démonstration du lemme 5.3.2.

Soient $f_1, \ldots, f_m$ des éléments de $\mathcal{F}_C$ tels que

$$f^m + f_1 f^{m-1} + \ldots + f_m = 0$$

Soit V un sous-ensemble analytique propre de $\mathbb{C}^g$ en dehors duquel $f, f_1, \ldots, f_m$ sont analytiques. Soit $\omega \in \Omega$. Pour $\ell_1, \ell_2 \in \mathbb{Z}$, notons

$$S_{\ell_1, \ell_2} = \{ z \in \mathbb{C}^g - V \; ; \; f(z + \ell_1 \omega) = f(z + \ell_2 \omega) \}$$

Comme, pour chaque $z \in \mathbb{C}^g - V$, le polynôme

$$X^m + f_1(z) X^{m-1} + \ldots + f_m(z)$$

a au plus m racines, $\mathbb{C}^g - V$ est la réunion des S_{ℓ_1, ℓ_2} pour $0 \leq \ell_1 < \ell_2 \leq m$.

Comme les ensembles S_{ℓ_1, ℓ_2} sont analytiques, il existe $\ell_1(\omega)$ et $\ell_2(\omega)$ tels que

$$\mathbb{C}^g - V = S_{\ell_1(\omega), \ell_2(\omega)} \quad \text{et} \quad \ell_1(\omega) \neq \ell_2(\omega).$$

Alors

$$f(z + \ell_1(\omega).\omega) = f(z + \ell_2(\omega).\omega) \quad \text{pour tout} \quad z \in \mathbb{C}^g.$$

Si d est un multiple des nombres $\ell_1(\omega) - \ell_2(\omega)$, ω décrivant une base de Ω sur $\mathbb{Z}$, alors $f(dz)$ admet Ω pour périodes.

On déduit du théorème 5.3.1 le résultat suivant [L 2] (chap. IV § 4 Th. 2).

COROLLAIRE 5.3.3 - Soit $\omega_1, \ldots, \omega_{2g}$ une base de Ω sur $\mathbb{Z}$, avec $\omega_1, \ldots, \omega_g$ $\mathbb{C}$-linéairement indépendants. On considère les matrices $g \times g$

$$W_1 = (\omega_1, \ldots, \omega_g), \quad W_2 = (\omega_{g+1}, \ldots, \omega_{2g}),$$

et

$$T = W_2 W_1^{-1}.$$

Si la matrice T a ses coefficients algébriques, alors elle représente un élément de $(\mathrm{End}\, A) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Dans le cas $g = 1$, on a $W_1 = \omega_1$, $W_2 = \omega_2$, $T = \tau$, et le résultat signifie que si τ est algébrique, alors il est imaginaire quadratique (cf. § 3.2)

A la fin du § 6.3, nous étudierons la matrice $W_1^{-1} W_2$ (cf. [L 2] p.40-41).

b) Transcendance de valeurs de fonctions arithmétiques automorphes

Le groupe $GL_2^+(\mathbb{R})$ opère sur le demi-plan supérieur $\mathfrak{h}$ par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az + b}{cz + d}$$

Soit $\Gamma = SL_2(\mathbb{Z})$. On obtient une surface de Riemann de genre 0 en compactifiant $\mathfrak{h}/\Gamma$ et le corps des fonctions rationnelles sur cette surface de Riemann est $\mathbb{C}(j)$, où j est la fonction modulaire.

Soit $\tau \in \mathfrak{h}$. Il existe un élément non scalaire de $GL_2^+(\mathbb{R})$ qui fixe τ si et seulement si τ est algébrique quadratique. Dans ce cas, la théorie classique de la multiplication complexe dit que $j(\tau)$ engendre sur $\mathbb{Q}(\tau)$ l'extension abélienne maximale non ramifiée de $\mathbb{Q}(\tau)$. Inversement, le théorème 5.3.2 de Schneider montre que si $j(\tau)$ et τ sont tous deux algébriques, alors τ est quadratique.

Cet énoncé a été étendu par Y. Morita [Mor] de la manière suivante.

Soit B une algèbre sur $\mathbb{Q}$ telle que

$$B \otimes_{\mathbb{Q}} \bar{\mathbb{Q}} \simeq M_2(\bar{\mathbb{Q}}) \quad , \quad B \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_2(\mathbb{R})$$

(algèbre de quaternions indéfinie). On choisit une représentation irréductible de B dans $M_2(\mathbb{R})$ telle que l'image de B soit contenue dans $M_2(\bar{\mathbb{Q}})$. Ainsi le groupe B^+ des éléments de B de norme réduite positive opère sur $\mathfrak{h}$ comme un sous-groupe de $GL_2^+(\mathbb{R})$.

Soient $\mathcal{O}$ un ordre maximal de B, et Γ le sous-groupe des unités de $\mathcal{O}$ formé des unités de norme réduite 1. G.Shimura [Shi 1] Thm 9 a construit une application holomorphe φ de $\mathfrak{h}$ dans un espace projectif vérifiant les deux propriétés suivantes :

(i) φ induit un isomorphisme birégulier de $\mathfrak{h}/\Gamma$ sur une courbe projective non singulière V.

(ii) Si $\tau \in \mathfrak{h}$ est fixe par un élément non scalaire de B^+, alors $\varphi(\tau)$ engendre une extension abélienne d'un corps imaginaire quadratique.

La fonction φ généralise donc la fonction j, et l'analogue du théorème de Schneider est le suivant [Mor] Thm 1 :

THÉORÈME 5.3.3 - Si τ et $\varphi(\tau)$ sont algébriques, alors τ est fixe par un élément non scalaire de B^+.

La démonstration de Morita utilise le théorème 5.3.1.

§ 5.4. Démonstration du théorème de Bombieri.

Nous allons effectuer la démonstration du théorème 5.1.1 en utilisant le lemme suivant, qui sera démontré au § 7.5.

LEMME 5.4.1 - Soit S un sous-ensemble fini de $\mathbb{C}^n$, et soit ϵ un nombre réel, $\epsilon > 0$. Il existe un nombre positif $r_o = r_o(S, \epsilon)$ tel que pour tout entier $t > 0$ et toute fonction entière non nulle f dans $\mathbb{C}^n$ satisfaisant

$$D^\tau f(\sigma) = 0 \qquad \text{pour} \qquad \sigma \in S, \tau \in \mathbb{N}^n, \ |\tau| < t,$$

on ait pour $R \geq r > r_o$

$$\operatorname{Log} |f|_r \leq \operatorname{Log} |f|_R - \left(\frac{\omega_1(S)}{n} - \epsilon\right) t \operatorname{Log}(R/4nr).$$

On a noté comme précédemment (§ 1.3) $\omega_1(S)$ le plus petit des degrés des hypersurfaces algébriques de $\mathbb{C}^n$ passant par S. Pour $\tau = (\tau_1, \ldots, \tau_n) \in \mathbb{N}^n$, D^τ est l'opérateur

$$\frac{\partial^{\tau_1}}{\partial z_1^{\tau_1}} \cdots \frac{\partial^{\tau_n}}{\partial z_n^{\tau_n}},$$

d'ordre $|\tau| = \tau_1 + \ldots + \tau_n$.

Nous utiliserons aussi une version à plusieurs variables du lemme 1.1.4 (cf. [L 2] Ch. IV §2 lemme 1, [Bom] lemme 1 ; voir aussi [Wa 3] II § 3 et [B-M] chap.11 § 3)

LEMME 5.4.2. - Soient U un ouvert de $\mathbb{C}^n$, et $f_1, \ldots, f_h$ des fonctions analytiques dans U. Il existe un entier $C_1 > 0$ ayant la propriété suivante

Soient K un corps de nombres, et $L_1, \ldots, L_h$, $t_1, \ldots, t_n$ des entiers positifs ou nuls, avec $|t| = t_1 + \ldots + t_n > 0$. On suppose que les dérivations $\frac{\partial}{\partial z_j}$, $(1 \leq j \leq n)$ laissent stable l'algèbre $K[f_1, \ldots, f_h]$.

Il existe un polynôme $P \in K[X_1, \ldots, X_h]$ tel que

a) $$D^t (f_1^{L_1} \cdots f_h^{L_h}) = P(f_1, \ldots, f_h).$$

b) Pour $1 \leq j \leq h$,

$$\deg_{X_j} P \leq L_j + C_1 |t|$$

c) Les coefficients du polynôme

$$C_1^{|t|} P$$

sont des entiers algébriques de K, dont les valeurs absolues des conjugués sont majorées par

$$C_1^{2|t|} (L_1 + \ldots + L_h + |t|)^{|t|}$$

Le lemme 5.4.1 nous permet de traiter les sous-ensembles finis de $\mathbb{C}^n$. Grâce à un argument de compacité (lemme 5.4.3) nous montrerons que c'est suffisant ici.

Soit $S_1 = \{\sigma_1, \ldots, \sigma_m\}$ un sous-ensemble fini de S :

$$f_j(\sigma_k) \in K \qquad \text{pour} \qquad 1 \leq j \leq h, \quad 1 \leq k \leq m.$$

Soit $\partial \in \mathbb{Z}$, $\partial > 0$ un dénominateur commun de ces hm nombres, et $\delta = [K : \mathbb{Q}]$.

Pour $1 \leq j \leq n+1$, on considère deux fonctions entières g_j, h_j, d'ordre strict $\leq \rho_j$, telles que $f_j = g_j / h_j$. Enfin pour $1 \leq j \leq n+1$, $1 \leq k \leq m$, on note $\tau_{j,k}$ un élément de $\mathbb{N}^n$ minimal dans l'ordre lexicographique (cf. [M 2] II p. 63) tel que

$$D^{\tau_{j,k}} h_j(\sigma_k) \neq 0.$$

Soit $0 < \epsilon < 1$. Soit $r_o(S_1, \epsilon) = r_o$ le nombre positif dont l'existence est affirmée par le lemme 5.4.1. Soit

$$r = \max\{r_o, \max_{1 \leq k \leq m} |\sigma_k|\}.$$

Soit N un entier suffisamment grand ; $c_2, \ldots, c_5$ désigneront des entiers indépendants de N et facilement calculables, et $\epsilon_1, \ldots, \epsilon_9$ seront des fonctions positives de N, tendant vers 0 quand N tend vers l'infini (N sera choisi assez grand pour que ces nombres ϵ_h soient tous inférieurs à ϵ).

a) Montrons qu'il existe un polynôme non nul

$$P_N \in \mathbb{Z}[X_1, \ldots, X_{n+1}]$$

de degré en X_j inférieur ou égal à

$$L_j = [N^{1-(\rho_j/(\rho_1 + \ldots + \rho_{n+1}))} (\operatorname{Log} N)^{1/n}],$$

$(1 \leq j \leq n+1)$, et de hauteur inférieure ou égale à $N^{\epsilon_1 N}$, tel que la fonction

$$F_N = P_N(f_1, \ldots, f_{n+1})$$

vérifie

$$D^t F_N(\sigma_k) = 0, \qquad \text{pour} \quad t \in \mathbb{N}^n, \quad |t| < N, k \in \mathbb{N}, 1 \leq k \leq m.$$

En utilisant le lemme 5.4.2, on écrit, pour $0 \le \lambda_j \le L_j$, $(1 \le j \le n+1)$ et $t \in \mathbb{N}^n$,

$$c_1^{|t|} D^t (f_1^{\lambda_1} \dots f_{n+1}^{\lambda_{n+1}})$$

comme un polynôme en $f_1, \dots, f_h$, de degré total $\le c_2 N$, et dont les coefficients sont des entiers de K dont tous les conjugués ont des valeurs absolues majorées par

$$c_1^{2|t|} (c_3 N + |t|)^{|t|}.$$

On écrit le polynôme inconnu P_N sous la forme

$$P_N(X_1, \dots, X_{n+1}) = \sum_{\lambda_1=0}^{L_1} \dots \sum_{\lambda_{n+1}=0}^{L_{n+1}} p(\lambda_1, \dots, \lambda_{n+1}) X_1^{\lambda_1} \dots X_{n+1}^{\lambda_{n+1}}$$

$$= \sum_{(\lambda)} p(\lambda) \prod_{j=1}^{n+1} X_j^{\lambda_j},$$

et on résout le système (dont les inconnues sont les coefficients $p(\lambda_1, \dots, \lambda_{n+1}) \in \mathbb{Z}$ de P)

$$c_1^{|t|} \delta^{c_2 N} . D^t F_N(\sigma_k) = 0 , \qquad (|t| < N , 1 \le k \le m).$$

C'est un système linéaire homogène, ayant moins de $m N^n$ équations, et plus de $N^n \operatorname{Log} N$ inconnues. Les coefficients de ce système sont des entiers de K :

$$c_1^{|t|} \delta^{c_2 N} D^t (f_1^{\lambda_1} \dots f_{n+1}^{\lambda_{n+1}})(\sigma_k),$$

dont les conjugués sont en valeur absolue majorés par $N^{c_4 N}$. Le lemme de Siegel (par exemple [Wa 2] lemme 1.3.1) montre qu'il existe une solution $p(\lambda) \in \mathbb{Z}$ vérifiant

$$0 < \max_{(\lambda)} |p(\lambda)| \le N^{c_5}.$$

b) <u>Soit</u> $t_o \in \mathbb{N}^n$, <u>minimal dans l'ordre lexicographique</u>, <u>tel qu'il existe</u> k_o, $1 \le k_o \le m$, <u>avec</u>

$$D^{t_o} F_N(\sigma_{k_o}) \ne 0.$$

<u>Soit</u> $M = |t_o|$. <u>Alors</u>

$$\operatorname{Log} |D^{t_o} F_N(\sigma_{k_o})| \ge -(\delta - 1 + \varepsilon_2) M \operatorname{Log} M.$$

L'existence de t_o provient de l'indépendance algébrique de $f_1, \dots, f_{n+1}$, et la construction de F_N implique $M \ge N$. Le nombre

$$c_1^M \delta^{c_2 M} D^{t_o} F_N(\sigma_{k_o}) = \sum_{(\lambda)} p(\lambda) c_1^M \delta^{c_2 M} D^{t_o} (f_1^{\lambda_1} \dots f_{n+1}^{\lambda_{n+1}})(\sigma_{k_o})$$

est un entier algébrique de K, dont tous les conjugués sont majorés en valeur absolue par $\exp\{(1+\varepsilon_3) M \operatorname{Log} M\}$. La norme sur $\mathbb{Q}$ de ce nombre est un entier rationnel non nul, donc de valeur absolue ≥ 1, ce qui donne l'estimation désirée.

c) <u>La fonction</u>

$$\Phi_N = F_N \prod_{j=1}^{n+1} h_j^{L_j}$$

<u>est entière dans</u> $\mathbb{C}^n$, <u>non identique à</u> 0, <u>et vérifie</u>

$$D^t \Phi_N(\sigma_k) = 0 \quad \underline{\text{pour}} \quad |t| < M, \ 1 \le k \le m$$

<u>et</u>

$$\operatorname{Log} |\Phi_N|_r \ge -(\delta - \varepsilon_4) M \operatorname{Log} M$$

C'est ici que nous utilisons la minimalité de t_o et des $\tau_{j,k}$. (cf. [M 2] II). Notons $t'_o = t_o + \sum_{j=1}^{n+1} \tau_{j,k_o} L_j$. Alors

$$D^{t'_o} \Phi_N(\sigma_{k_o}) = D^{t_o} F(\sigma_{k_o}) . \prod_{j=1}^{n+1} \left(D^{\tau_{j,k_o}} . h_j(\sigma_{k_o}) \right)^{L_j}$$

Comme les nombres

$$D^{\tau_{j,k_o}} h_j(\sigma_{k_o})$$

sont indépendants de N et non nuls, le membre de droite est minoré par $\exp\{-(\delta - 1 - \varepsilon_5) M \operatorname{Log} M\}$. D'un autre côté les inégalités de Cauchy donnent

$$\operatorname{Log} |D^{t'_o} \Phi_N(\sigma_{k_o})| \le \operatorname{Log} |\Phi|_r + (1+\varepsilon_6) M \operatorname{Log} M.$$

Le résultat annoncé s'en déduit.

d) <u>On a</u>

$$\omega_1(S_1) \le n \delta (\rho_1 + \dots + \rho_{n+1}).$$

On utilise le lemme 5.4.1 pour la fonction Φ_N avec $R = M^{1/(\rho_1 + \dots + \rho_{n+1})}$. Comme

$$\Phi_N = \sum_{(\lambda)} p(\lambda) \prod_{j=1}^{n+1} g_j^{\lambda_j} h_j^{L_j - \lambda_j},$$

et que les fonctions g_j et h_j sont entières d'ordre strict $\le \rho_j$, on a

$$\text{Log } |\Phi_N|_R \leq c_7 \, M \, \text{Log} \, M + \sum_{j=1}^{n+1} L_j \, R^{\rho_j}$$

$$\leq c_8 \, M \, \text{Log} \, M .$$

On en déduit donc

$$\frac{\omega_1(S_1)}{n} - \epsilon \leq \delta \, (\rho_1 + \ldots + \rho_{n+1}) + c_9$$

ce qui donne bien le résultat annoncé.

Il reste à s'affranchir de l'hypothèse sur la finitude de S_1.

LEMME 5.4.3 - Soient S un sous-ensemble de $\mathbb{C}^n$, et Δ un entier positif. On suppose que toute partie finie S_1 de S vérifie $\omega_1(S_1) \leq \Delta$. Alors S est contenu dans une hypersurface algébrique de degré $\leq \Delta$.

Démonstration du lemme 5.4.3.

Notons $\mathcal{P}$ l'ensemble des polynômes de $\mathbb{C}[z_1, \ldots, z_n]$ de degré $\leq \Delta$ et de hauteur 1. Dans l'espace $\mathbb{C}[z_1, \ldots, z_n]$ muni de la norme de la hauteur des polynômes, $\mathcal{P}$ est un compact. Pour toute partie finie S_1 de S notons $\mathcal{F}_{S_1}$ l'ensemble des éléments de $\mathcal{P}$ qui s'annulent sur S_1. D'après l'hypothèse, $\mathcal{F}_{S_1}$ est non vide. Comme S est réunion d'une famille croissante $\{S_1\}$ de parties finies, que $\mathcal{F}_{S_1}$ est fermé, et que

$$S_1' \subset S_1'' \Rightarrow \mathcal{F}_{S_1''} \subset \mathcal{F}_{S_1'} ,$$

l'intersection de ces $\mathcal{F}_{S_1}$ est non vide. Il existe donc un polynôme non identique à 0 de degré $\leq \Delta$ qui s'annule sur S.

Pour déduire le corollaire 5.1.2 du théorème de Bombieri, on utilise le lemme suivant, dont la démonstration est facile par récurrence sur n (cf. [Wa 3] II lemme 5.8). Nous l'énonçons avec des multiplicités, mais le cas $t = 1$ suffit ici.

LEMME 5.4.4 - Soient $S_1, \ldots, S_n$ des sous-ensembles finis de $\mathbb{C}$, et $S = S_1 \times \ldots \times S_n$ leur produit dans $\mathbb{C}^n$. Pour tout entier positif t, on a

$$\omega_t(S) = t \min_{1 \leq i \leq n} \text{Card } S_i$$

REMARQUES - Actuellement, toutes les applications du critère de Bombieri proviennent du théorème 5.2.1, donc du corollaire 5.1.2. La démonstration directe de ce corollaire 5.1.2 utilise un lemme de Schwarz beaucoup plus facile à démontrer que le lemme 5.4.1 (cf. § 7.2 Proposition 7.2.1) et qui conduit à la majoration

$$\min_{1 \leq j \leq n} \text{Card } S_j \leq (\rho_1 + \ldots + \rho_{n+1}) \, [K : \mathbb{Q}] .$$

D'autre part les équations différentielles des fonctions $f_1, \ldots, f_h$ n'ont été utilisées que pour la démonstration du lemme 5.4.2 ; par conséquent, de même que dans le cas d'une variable (cf. [S 3], [S 4] Th. 12, [Wa 1] Th. A), on peut remplacer l'hypothèse concernant les équations différentielles par des hypothèses techniques sur la taille des valeurs des dérivées des fonctions [Wa 3], [B - M] Chap 11. (ces hypothèses sont analogues aux axiomes 0.A.1 et 0.A.2. du § 1.1). Voici un exemple [Wa 3] (I Th.3.1) qui généralise le théorème I de [S 2]

THÉORÈME 5.4.5 - Soient K un corps de nombres, et $(w_1, \ldots, w_n)$ une base de $\mathbb{C}^n$. On note $E_K(w_1, \ldots, w_n)$ l'ensemble des fonctions méromorphes dans $\mathbb{C}^n$, d'ordre fini, admettant $w_1, \ldots, w_n$ pour périodes, anlytiques en 0, et dont le développement de Taylor à l'origine

$$f(z) = \sum_{h \in \mathbb{N}^n} a_h \, z^h$$

a pour coefficients a_h des éléments de K vérifiant, pour tout $h \in \mathbb{N}^n$, $|h| \geq 2$,

$$\text{Log } |a_h| \leq C(f) \, |h| \, \text{Log } |h|$$

et

$$V_1(f)^{|h|} \, [V_2(f) \, h \, !]^{V_3(f)} \quad a_h \quad \text{est entier sur } \mathbb{Z},$$

où $C(f)$, $V_1(f)$, $V_2(f)$, $V_3(f)$ sont des entiers positifs indépendants de h. Alors $E_K(w_1, \ldots, w_n)$ est un anneau intègre dont le corps des fractions L a un degré de transcendance sur K inférieur ou égal à n.

De plus, si les ν premières coodonnées de chacun des w_k sont algébriques, alors ce degré de transcendance est inférieur ou égal à $n - \nu$. En particulier si $w_1, \ldots, w_n$ apartiennent à $\bar{\mathbb{Q}}^n$, alors $E_K(w_1, \ldots, w_n)$ ne contient que les constantes.

On peut vérifier que les hypothèses techniques sont satisfaites quand on considère des fonctions à valeurs dans $\mathbb{Z}$ [Wa 3] II. (voir aussi [Sk]). c'est ainsi que Chudnovski [C 1] a démontré l'énoncé suivant

THÉORÈME 5.4.6. - Soit f une fonction transcendante méromorphe dans $\mathbb{C}^n$ d'ordre $\leq \rho$. L'ensemble des points algébriques $w \in \bar{\mathbb{Q}}^n$ où f est analytique et $D^k f(w) \in \mathbb{Z}$ pour tout $k \in \mathbb{N}^n$ est contenu dans une hypersurface algébrique de degré inférieur ou égal à $n \rho$.

CHAPITRE 6

VARIÉTÉS ABÉLIENNES SIMPLES DE TYPE C.M

Pour compléter l'étude précédente, il nous reste à étudier les homomorphismes analytiques de $\mathbb{C}^n$ dans un groupe algébrique, sans hypothèse de normalisation. Considérons d'abord les points algébriques du graphe d'un tel homomorphisme. Au chapitre 2, § 2.5, nous avons ramené cette étude, dans le cas d'un groupe linéaire, à un énoncé d'indépendance linéaire sur $\overline{\mathbb{Q}}$ de logarithmes de nombres algébriques. Au chapitre 4, § 4.1, nous avons vu que pour un sous-groupe à 1 paramètre d'une courbe elliptique, on se ramenait à l'indépendance linéaire sur $\overline{\mathbb{Q}}$ de points algébriques de $\wp$.

Nous allons effectuer la même démarche dans le cas général. On veut montrer que, sous des hypothèses naturelles concernant l'irrationalité de φ , si Γ est un sous-groupe de type fini de $\overline{\mathbb{Q}}^n$, de rang ℓ sur $\mathbb{Z}$, tel que $\varphi(\Gamma) \subset G_{\overline{\mathbb{Q}}}$, alors $\ell \leq 2n$. On ramène ce problème à celui de l'indépendance linéaire de points algébriques de variétés abéliennes simples.

Mais on ne sait résoudre actuellement ce problème d'indépendance linéaire que dans le cas d'une variété abélienne simple de type C.M., c'est-à-dire quand $(\mathrm{End}\, A) \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$ est un corps de degré $2g$ sur $\mathbb{Q}$ (où $g = \dim A$) .

Nous commençons par regrouper (sans tous les démontrer) les résultats de transcendance actuellement connus concernant les points algébriques de variétés abéliennes simples de type C.M. : chaque coordonnée d'un point algébrique non nul est transcendante (§ 6.1), et des points algébriques linéairement indépendants sur End A sont linéairement indépendants sur $(\mathrm{End}\, A).\overline{\mathbb{Q}}$ (§ 6.2). Pour le premier énoncé il faut normaliser "fortement" (cf. § 6.1) la représentation thêta, alors que pour le deuxième la normalisation habituelle suffit.

Au § 6.3 nous appliquons le théorème et la conjecture du § 6.2 à l'étude des points $\gamma \in \overline{\mathbb{Q}}^n$ où un homomorphisme analytique $\varphi : \mathbb{C}^n \to G_{\mathbb{C}}$ prend des valeurs dans $G_{\overline{\mathbb{Q}}}$.

§ 6.1 - Transcendance des coordonnées de points algébriques.

Soit A une variété abélienne définie sur un corps de nombres K . On suppose que $(\mathrm{End}\, A) \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$ est un corps de nombres k de degré $2g$ sur $\mathbb{Q}$. Alors A est simple, et on dit que A est de type C.M. Nous renvoyons aux travaux de Shimura cités en bibliographie une étude détaillée de ces variétés. Nous utiliserons seulement les faits suivants.

Le corps k est totalement imaginaire, extension quadratique d'un corps totalement réel. On suppose que K contient k ainsi que les conjugués de k . L'anneau End A est alors isomorphe à un ordre $\mathcal{O}$ de k . On peut choisir un homomorphisme thêta normalisé $\Theta : \mathbb{C}^g \to A_{\mathbb{C}}$ (c'est-à-dire choisir une K-base de l'espace tangent à l'origine de A) de manière à décrire l'isomorphisme $\mathcal{O} \to \mathrm{End}\, A$ de la façon suivante : il existe g plongements $\sigma_1, \ldots, \sigma_g$ de k dans $\mathbb{C}$ tels que pour $\gamma \in \mathcal{O}$ l'image de γ dans End A corresponde à la matrice diagonale $g \times g$

$$\begin{pmatrix} \gamma^{\sigma_1} & & 0 \\ & \ddots & \\ 0 & & \gamma^{\sigma_g} \end{pmatrix}$$

Autrement dit k opère sur $\mathbb{C}^g$ par

$$k \times \mathbb{C}^g \to \mathbb{C}^g$$

$$(\gamma ; (z_1, \ldots, z_g)) \mapsto (\gamma^{\sigma_1} z_1, \ldots, \gamma^{\sigma_g} z_g) .$$

Dans ces conditions nous dirons que l'homomorphisme thêta est fortement normalisé. Cette normalisation, qui intervient dans les travaux de Masser [M 2], [M 6], et [B.M] (chap.8), Lang [L 6] et Coates Lang [C-L], est définie dans le cas d'une variété abélienne quelconque par D. Bertrand [Be 5] et Appendice I .

L'énoncé suivant est dû à Lang [L 6] (Th. 1) et Masser [M 2] (III Cor.1) qui donne des exemples de jacobiennes de type C.M. [M 2] (III p. 563).

THÉORÈME 6.1.1 - Soient A une variété abélienne simple de type C.M., $\Theta : \mathbb{C}^g \to A_{\mathbb{C}}$ un homomorphisme thêta fortement normalisé et $u = (u_1, \ldots, u_g)$ un point algébrique non nul de Θ . Alors chacune des composantes u_j , $(1 \leq j \leq g)$ de u est transcendante.

Lang déduit cet énoncé du critère 5.1.1 de Bombieri. Masser déduit un résultat plus fort que le théorème 6.1.1 de son théorème sur l'indépendance linéaire de points algébriques de Θ (voir § 6.2 ci-dessous). Comme nous ne donnerons pas la démonstration du théorème 6.2.3 d'indépendance linéaire, nous reprenons ici le raisonnement de Lang, mais nous utilisons directement le théorème 5.2.1 sur les sous-groupes abéliens à n paramètres normalisés.

Démonstration du théorème 6.1.1.

Soit j un entier, $1 \leq j \leq g$, avec u_j algébrique (éventuellement nul). Pour $1 \leq i \leq g$, notons

$$\varepsilon_i = 1 \quad \text{et} \quad v_i = u_i \quad \text{si} \quad u_i \neq 0$$

$$\varepsilon_i = 0 \quad \text{et} \quad v_i = 1 \quad \text{si} \quad u_i = 0$$

On considère l'homomorphisme analytique normalisé

$$\varphi : \mathbb{C}^g \to \mathbb{C} \times A_{\mathbb{C}}$$
$$z \to (z_j, \Theta \circ \mathcal{L}(z)),$$

où

$$\mathcal{L}(z_1, \ldots, z_g) = (\varepsilon_1 z_1, \ldots, \varepsilon_g z_g).$$

Il prend des valeurs algébriques aux points

$$(\gamma^{\sigma_1} v_1, \ldots, \gamma^{\sigma_g} v_g)$$

Or ces points forment un réseau Γ de $\mathbb{C}^g$, donc Γ contient une base de $\mathbb{C}^g$ sur $\mathbb{C}$. (On n'utilise donc qu'une version affaiblie de l'hypothèse C.M.).

D'autre part, la variété abélienne A étant simple, l'homomorphisme analytique $\Theta \circ \mathcal{L} : \mathbb{C}^g \to A_{\mathbb{C}}$ a une image dense dans $A_{\mathbb{C}}$, donc a pour dimension algébrique g. On en déduit que la dimension algébrique de φ est $g+1$, ce qui contredit le théorème 5.2.1.

Démontrer 6.1.1 avec seulement une hypothèse de faible normalisation pour Θ reviendrait à montrer que $1, u_1, \ldots, u_g$ sont $\overline{\mathbb{Q}}$-linéairement indépendants [L6] (p. 292). Ce problème n'est toujours pas résolu [L5] (2.3).

§ 6.2 - Indépendance linéaire de points algébriques.

La conjecture suivante n'est pas la plus générale possible, mais elle suffit dans de nombreuses situations.

CONJECTURE 6.2.1 - Soient A une variété abélienne simple définie sur $\overline{\mathbb{Q}}$, $\Theta : \mathbb{C}^g \to A_{\mathbb{C}}$ un homomorphisme thêta normalisé et $u_1, \ldots, u_\ell$ deux points algébriques de Θ qui sont linéairement indépendants sur End A. Alors $u_1, \ldots, u_\ell$ sont linéairement indépendants sur $(\text{End } A).\overline{\mathbb{Q}}$.

Le cas particulier suivant est résolu dans le cas d'une courbe elliptique (cf. 3.2.3).

CONJECTURE 6.2.2 - Soient A une variété abélienne simple définie sur $\overline{\mathbb{Q}}$, $\Theta : \mathbb{C}^g \to A_{\mathbb{C}}$ un homomorphisme thêta normalisé, et u_1, u_2 deux points algébriques de Θ. On suppose qu'il existe un nombre algébrique $\beta \in \overline{\mathbb{Q}}$ tel que $u_2 = \beta u_1$. Alors u_1, u_2 sont linéairement dépendants sur End A.

Le premier cas particulier où la conjecture 6.2.1 a été résolue est celui d'une courbe elliptique ayant multiplication complexe, par Masser [M1] Thm V, Chap VII. (cf. [L7] Chap. 9). Les minorations les plus fines que l'on connaisse sont dues à M. Anderson [B-M] Chap 7 et [M8].
Ce résultat a été étendu aux variétés abéliennes de type C.M. par Lang [L6] et Masser [M2], et les minorations de formes linéaires ont ensuite été raffinées par Coates et Lang [C-L] puis Masser [M6].
Très récemment, d'autres cas particuliers de ces conjectures ont été obtenus par D. Bertrand et D.W. Masser à partir du critère 5.1.2. En particulier la conjecture 6.2.1 est maintenant résolue dans le cas d'une courbe elliptique.

Comme les énoncés 6.2.1 et 6.2.2 concernent en fait l'espace tangent à l'origine de la variété, ils sont indépendants du choix de l'homomorphisme thêta normalisé. Si on suppose que A est de type C.M. et que Θ est fortement normalisé, alors Masser [M2] III a démontré l'indépendance linéaire sur $(\text{End } A).\overline{\mathbb{Q}}$ des points

$$e_1, \ldots, e_g, \quad u_1, \ldots, u_\ell$$

(où $(e_1, \ldots, e_g)$ est la base canonique de $\mathbb{C}^g$; e_1 n'est pas un point algébrique de Θ, d'après 3.1.4 ou 6.1.1).

THÉORÈME 6.2.3 - Soient A une variété abélienne simple de type C.M. définie sur $\overline{\mathbb{Q}}$, $\Theta : \mathbb{C}^g \to A_{\mathbb{C}}$ un homomorphisme thêta fortement normalisé, et $u_1, \ldots, u_\ell$ des points algébriques de Θ qui sont linéairement indépendants sur End A. Alors

$$e_1, \ldots, e_g, \quad u_1, \ldots, u_\ell$$

sont linéairement indépendants sur $(\text{End } A).\overline{\mathbb{Q}}$.

Cet énoncé non homogène conduit à d'intéressants résultats de transcendance sur les coordonnées des u_j. [M2] III, Coroll. 2 et 3. En considérant des matrices de la forme

$$\text{diag}(0, \ldots 0, \beta, 0, \ldots, 0), \qquad \beta \in \overline{\mathbb{Q}},$$

on peut préciser le théorème 6.1.1.

COROLLAIRE 6.2.4 - Avec les notations du théorème 6.2.3, soient $(u_{j,1}, \dots, u_{j,g})$ les coordonnées de u_j dans $\mathbb{C}^g$, $(1 \leq j \leq \ell)$. Soit r un entier, $1 \leq r \leq g$. Alors les nombres $1, u_{1,r}, \dots, u_{\ell,r}$ sont $\bar{\mathbb{Q}}$-linéairement indépendants.

Le théorème 6.2.3 peut être considéré comme un raffinement du théorème 5.2.1 (cf. § 2.4.c), mais pour l'instant, avec une hypothèse restrictive sur le type C.M.

Le lien entre ces problèmes et des questions de géométrie diophantienne (que nous ne considérons pas ici) est la motivation essentielle des articles de Lang, Masser et Bertrand sur ce sujet. Le rapport entre l'étude de points entiers sur des courbes algébriques et des minorations de formes linéaires de logarithmes a été précisé par Gel'fond dans le cas multiplicatif, et Lang dans les cas elliptiques et abéliens.

§ 6.3 - Application aux homomorphismes analytiques de $\mathbb{C}^n$ dans $G_{\mathbb{C}}$.

Le but de cette partie est de montrer que la conjecture 6.2.1 donne une description satisfaisante des points algébriques $\gamma \in \bar{\mathbb{Q}}^n$ où un homomorphisme analytique $\varphi : \mathbb{C}^n \to G_{\mathbb{C}}$ prend des valeurs algébriques : $\varphi(\gamma) \in G_{\bar{\mathbb{Q}}}$. On ne suppose pas φ normalisé.

Nous énonçons les résultats sous l'hypothèse que les variétés abéliennes ont le type C.M. , mais la propriété essentielle que nous utilisons est le théorème 6.2.3.

a) Sous-groupes à un paramètre d'une variété abélienne simple.

Nous apportons d'abord un complément au théorème 4.1.2.

THÉORÈME 6.3.1 - Soient A une variété abélienne simple de type C.M., définie sur $\bar{\mathbb{Q}}$, et $\varphi : \mathbb{C} \to A_{\mathbb{C}}$ un sous-groupe à 1 paramètre de A. S'il existe deux nombres algébriques γ_1, γ_2 $\mathbb{Q}$-linéairement indépendants, dont les images par φ appartiennent à $A_{\bar{\mathbb{Q}}}$, alors A est une courbe elliptique.

Démonstration du théorème 6.3.1.

Soit $\Theta : \mathbb{C}^g \to A_{\mathbb{C}}$ un homomorphisme thêta fortement normalisé de A. Nous allons montrer qu'il existe un endomorphisme de A représenté par γI, où I est la matrice identité $g \times g$, et γ est un nombre algébrique irrationnel. Pour conclure, on peut par exemple considérer une période non nulle ω de Θ, et poser $\omega' = \gamma\omega$; le sous-$\mathbb{C}$-espace vectoriel $\mathbb{C}\omega$ de $\mathbb{C}^g$ contient alors un réseau $\mathbb{Z}\omega + \mathbb{Z}\omega'$ contenu dans $\ker \Theta$, et l'hypothèse sur la simplicité de A entraîne $g = 1$.

Notons $\varphi = \Theta \circ \mathcal{L}$, où $\mathcal{L} : \mathbb{C} \to \mathbb{C}^g$ est une application $\mathbb{C}$-linéaire, et

$$u_j = \mathcal{L}(\gamma_j), \quad j = 1,2 .$$

Comme $\gamma_1 u_2 = \gamma_2 u_1$, et comme $\mathrm{End}\, A \otimes_{\mathbb{Z}} \mathbb{Q}$ est un corps, le théorème 6.2.3 montre qu'il existe un entier $d > 0$ et un endomorphisme $\mathbb{C}$-linéaire M de $\mathbb{C}^g$ laissant $\ker \Theta$ stable, tels que $du_2 = Mu_1$. Soit $\gamma = d\gamma_2/\gamma_1$. Alors M admet u_1 comme vecteur propre. Comme toutes les coordonnées de u_1 sont non nulles (d'après 6.1.1 ou 6.2.4) et que A est de type C.M., on a $M = \gamma I$.

b) Cas général.

Soient G un groupe algébrique défini sur $\bar{\mathbb{Q}}$, Γ un sous-groupe de $\bar{\mathbb{Q}}^n$ de type fini et de rang ℓ sur $\mathbb{Z}$, et $\varphi : \mathbb{C}^n \to G_{\mathbb{C}}$ un homomorphisme analytique non rationnel tel que $\varphi(\Gamma) \subset G_{\bar{\mathbb{Q}}}$. On voudrait majorer ℓ.

On ne peut pas le faire sans hypothèse supplémentaire : si, par exemple, l'homomorphisme $z_1 \to \varphi(z_1, 0, \dots, 0)$ de $\mathbb{C}$ dans $G_{\mathbb{C}}$ est rationnel, alors Γ peut être n'importe quel sous-groupe de $\bar{\mathbb{Q}}.e_1$, où $e_1 = (1, 0, \dots, 0)$.

L'hypothèse la plus naturelle consiste à supposer que φ est irrationnel dans toutes les directions de Γ, c'est-à-dire que pour tout $\gamma \in \Gamma$, $\gamma \neq 0$, l'homomorphisme $t \to \varphi(\gamma t)$ de $\mathbb{C}$ dans $G_{\mathbb{C}}$ est irrationnel. Dans ce cas la meilleure majoration que l'on puisse espérer est

$$\ell \leq 2n ,$$

l'égalité étant atteinte quand G est un produit $\mathcal{E}_1 \times \dots \times \mathcal{E}_n$ de courbes elliptiques ayant multiplication complexe, et

$$\varphi(z_1, \dots, z_n) = (P_1(\omega_1 z_1), \dots, P_n(\omega_n z_n)) ,$$

ω_j étant une période non nulle de P_j, $(1 \leq j \leq n)$. Alors on peut prendre pour Γ un réseau dans $\mathbb{C}^n$. (Cf. 4.1.1).

L'hypothèse d'irrationnalité de φ dans toutes les directions présente un inconvénient. Si on démontre le résultat $\ell \leq 2n$ pour les variétés abéliennes (on sait déjà que $\ell \leq n$ pour les variétés linéaires ; cf. 2.5.1), cette hypothèse est un obstacle pour l'utilisation du théorème de Chevalley qui permettrait d'en déduire le cas général.

Pour cette raison on démontrera d'abord un énoncé dans lequel on ne fait pas l'hypothèse que φ est irrationnel dans toutes les directions. La conclusion, nous l'avons vu, ne peut pas être une majoration de ℓ. Ce sera seulement le fait que Γ ne peut pas avoir trop d'éléments dans toutes les directions.

Voici un exemple. Si $\mathcal{E}$ est une courbe elliptique avec multiplication complexe, définie sur $\bar{\mathbb{Q}}$, u_1, u_2 sont deux points algébriques non nuls de la fonction elliptique $\wp$ associée à $\mathcal{E}$, et si $\varphi : \mathbb{C}^2 \to \mathcal{E}_{\mathbb{C}}$ est défini par

$$\varphi(z_1, z_2) = P(u_1 z_1 + u_2 z_2) ,$$

on peut choisir pour Γ le réseau

$$\mathbf{Z}^2 + \mathbf{Z}(0,\tau) + \mathbf{Z}(\tau,0) ,$$

où $\tau = \frac{\omega_2}{\omega_1}$ est le quotient de deux périodes fondamentales de $\wp$. Si u_1 , u_2 sont $\mathbf{Q}(\tau)$-linéairement indépendants, il n'y a essentiellement pas d'autre $\gamma \in \overline{\mathbf{Q}}^2$ dont l'image par φ soit dans $\mathcal{E}_{\overline{\mathbf{Q}}}$. Mais si, par exemple, $u_2 = \tau u_1$, alors tous les points

$$(a + b\tau - \tau\alpha, \alpha) \qquad , \alpha \in \overline{\mathbf{Q}} , \quad a, b \in \mathbf{Q}$$

ont cette propriété ; néanmoins, si Γ est un sous-groupe de type fini de $\overline{\mathbf{Q}}^2$ tel que $\varphi(\Gamma) \subset \mathcal{E}_{\overline{\mathbf{Q}}}$, alors l'image de Γ par l'application

$$(z_1, z_2) \mapsto z_1 + \tau z_2$$

est un sous-groupe discret de $\mathbf{C}$ (en particulier $\mu(\Gamma, \mathbf{C}^2) \leq 2$.)

Nous résolvons ici un cas particulier de ce problème. Nous reviendrons sur cette question au chapitre 8.

THÉORÈME 6.3.2 - Soient G un groupe algébrique commutatif connexe défini sur $\overline{\mathbf{Q}}$, $\varphi : \mathbf{C}^n \to G_{\mathbf{C}}$ un homomorphisme analytique, et Γ un sous-groupe de type fini de $\overline{\mathbf{Q}}^n$ tel que $\varphi(\Gamma) \subset G_{\overline{\mathbf{Q}}}$. On suppose que pour tout $\gamma \in \Gamma , \gamma \neq 0$, l'homomorphisme $t \mapsto \varphi(\gamma t)$ de $\mathbf{C}$ dans $G_{\mathbf{C}}$ n'est pas rationnel. On suppose de plus que quand on écrit G comme extension d'une variété abélienne A par un groupe linéaire, A est isogène à un produit de variétés abéliennes simples de type C.M. Alors Γ est discret dans $\mathbf{C}^n$.

On effectue la démonstration du théorème 6.3.2 en 3 étapes

LEMME 6.3.3 - Soient A une variété abélienne simple de type C.M., $\varphi : \mathbf{C}^n \to A_{\mathbf{C}}$ un homomorphisme analytique non constant, et Γ un sous-groupe de type fini de $\overline{\mathbf{Q}}^n$ dont l'image par φ soit contenue dans $A_{\overline{\mathbf{Q}}}$. Alors il existe un sous-espace W de $\mathbf{C}^n$, $W \neq \mathbf{C}^n$, tel que l'image de Γ dans $\mathbf{C}^n/W$ soit un sous-groupe discret de $\mathbf{C}^n/W$.

Démonstration du lemme 6.3.3.

On considère un homomorphisme thêta normalisé $\Theta : \mathbf{C}^g \to A_{\mathbf{C}}$, une application linéaire $\mathcal{L} : \mathbf{C}^n \to \mathbf{C}^g$ telle que $\varphi = \Theta \circ \mathcal{L}$, et une base $\gamma_1 , \dots , \gamma_\ell$ de Γ sur $\mathbf{Z}$. Il n'y a pas de restriction à supposer $\gamma_1 , \dots , \gamma_n$ $\mathbf{C}$-linéairement indépendants. Notons alors

$$\gamma_j = \sum_{s=1}^{n} \beta_{j,s} \gamma_s , \qquad (1 \leq j \leq \ell) ,$$

où $\beta_{j,s}$ sont des nombres algébriques. Notons $u_j = \mathcal{L}(\gamma_j)$, $(1 \leq j \leq \ell)$. Ainsi

$$u_j = \sum_{s=1}^{n} \beta_{j,s} u_s , \qquad (1 \leq j \leq \ell) .$$

Comme A est simple, $(\operatorname{End} A) \otimes_{\mathbf{Z}} \mathbf{Q}$ est un corps commutatif. Grâce à l'hypothèse C.M. et au théorème 6.2.3, on peut utiliser le lemme 2.4.5 avec pour D le corps déduit de $(\operatorname{End} A) \otimes_{\mathbf{Z}} \mathbf{Q}$ par extension des scalaires avec $\overline{\mathbf{Q}}$, et $A_1 = \operatorname{End} A$, $A_2 = (\operatorname{End} A).\overline{\mathbf{Q}}$: il existe des endomorphismes $B_1 , \dots , B_\ell$ de $\mathbf{C}^g$, non tous nuls, laissant $\ker \Theta$ stable, tels que

$$B_j = \sum_{s=1}^{n} \beta_{j,s} B_s , \qquad (1 \leq j \leq \ell) .$$

Soit $\omega \in \mathbf{C}^g$ une période de Θ . Notons

$$\omega_j = B_j \omega , \qquad (1 \leq j \leq \ell) .$$

On choisit ω de telle manière que $\omega_1 , \dots , \omega_\ell$ ne soient pas tous nuls. On a

$$\omega_j = \sum_{s=1}^{n} \beta_{j,s} \omega_s , \qquad (1 \leq j \leq \ell) .$$

On considère l'application $\mathbf{C}$-linéaire $p : \mathbf{C}^n \to \mathbf{C}^g$ définie sur la base $(\gamma_1 , \dots , \gamma_n)$ par

$$p(\gamma_s) = \omega_s , \qquad (1 \leq s \leq n) .$$

Alors on a

$$p(\gamma_j) = \omega_j , \qquad (1 \leq j \leq \ell) ,$$

donc $p(\Gamma) \subset \Omega$. On pose alors $W = \ker p$.

REMARQUE 6.3.4 - On déduit évidemment du lemme 6.3.3

$$\mu(\Gamma, \mathbf{C}^n) \leq 2 .$$

Montrons que si $n < g$, on a

$$\mu(\Gamma, \mathbf{C}^n) < 2 .$$

(Dans le cas $n = 1$, cette inégalité équivaut au théorème 6.3.1). En effet, $p(\mathbf{C}^n)$ est un sous-espace propre de $\mathbf{C}^g$ (car $n < g$) , et la simplicité de A entraîne

$$\operatorname{rang}_{\mathbf{Z}} (\ker \Theta) \cap p(\mathbf{C}^n) < 2 \operatorname{rang} p .$$

Comme $p(\Gamma) \subset \ker \Theta$, on a

$$\operatorname{rang}_{\mathbf{Z}} p(\Gamma) < 2 \operatorname{rang} p .$$

LEMME 6.3.5 - Soit G un groupe algébrique commutatif connexe défini sur $\overline{\mathbf{Q}}$, extension par un groupe linéaire d'une variété abélienne isogène à un produit de variétés abéliennes simples de type C.M. Soient $\varphi : \mathbf{C}^n \to G_{\mathbf{C}}$ un homomorphisme analytique non rationnel, et Γ un sous-groupe de type fini de $\overline{\mathbf{Q}}^n$ tel que

$$\varphi(\Gamma) \subset G_{\overline{\mathbf{Q}}} .$$

Il existe un sous-espace W de $\mathbf{C}^n$, $W \neq \mathbf{C}^n$, tel que l'image de Γ dans $\mathbf{C}^n/W$ soit un sous-groupe discret de $\mathbf{C}^n/W$.

Démonstration du lemme 6.3.5.

Par hypothèse on a une suite exacte

$$0 \to L \to G \xrightarrow{\pi_1} A \to 0$$

où A est isogène à un produit de variétés abéliennes simples de type C.M., et L est linéaire. On considère deux cas

a) $\varphi(\mathbf{C}^n) \subset L_{\mathbf{C}}$. Alors, par la proposition 2.5.2, on a $\mu(\Gamma, \mathbf{C}^n) \leq 1$. Le résultat s'en déduit facilement.

b) L'application $\pi_1 \circ \varphi : \mathbf{C}^n \to A_{\mathbf{C}}$ n'est pas nulle. Il existe alors une variété abélienne simple de type C.M., soit B, et un homomorphisme rationnel $\pi_2 : A \to B$, tels que l'homomorphisme $\pi_2 \circ \pi_1 \circ \varphi : \mathbf{C}^n \to B_{\mathbf{C}}$ ne soit pas nul. On lui applique alors le lemme 6.3.3.

Dans cette démonstration il était essentiel que l'hypothèse sur φ ait été seulement le fait qu'il n'est pas rationnel. L'argument de passage au quotient n'aurait pas pu être utilisé avec l'hypothèse d'irrationnalité dans toutes les directions, comme dans l'énoncé du théorème 6.3.2.

Démonstration du théorème 6.3.2.

On démontre le théorème par récurrence sur n. Pour $n = 1$, le lemme 6.3.5 donne le résultat désiré (qui est un peu plus précis que le théorème 4.1.2 dans ce cas particulier).

Pour $n \geq 2$, on utilise le lemme 6.3.5 : soit $s : \mathbf{C}^n \to \mathbf{C}^n/W$ la surjection canonique ; on considère une base $\gamma_1, \ldots, \gamma_\ell$ de Γ sur $\mathbf{Z}$, telle que

$$s(\gamma_1), \ldots, s(\gamma_\lambda)$$

soient $\mathbf{Q}$-linéairement indépendants, et que $\gamma_{\lambda+1}, \ldots, \gamma_\ell$ appartiennent à W. D'après le lemme 6.3.5, $s(\gamma_1), \ldots, s(\gamma_\lambda)$ sont $\mathbf{R}$-linéairement indépendants, et l'hypothèse de récurrence appliquée à la restriction de φ à W montre que

$\gamma_{\lambda+1}, \ldots, \gamma_\ell$ sont $\mathbf{R}$-linéairement indépendants. On en déduit que $\gamma_1, \ldots, \gamma_\ell$ sont $\mathbf{R}$-linéairement indépendants.

Dans le théorème 6.3.2, on a supposé que l'anneau des endomorphismes de A était le plus gros possible, et on a montré, en particulier, que le rang ℓ de Γ sur $\mathbf{Z}$ vérifiait $\ell \leq 2n$.

Si on suppose qu'il y a moins d'endomorphismes que dans le cas C.M., on ne sait plus démontrer cette majoration (voir néanmoins le chapitre 8) alors que, de manière paradoxale, la conjecture 6.2.1 conduit à de meilleures majorations. En voici un exemple.

PROPOSITION 6.3.6 - Soit A une variété abélienne simple définie sur $\overline{\mathbf{Q}}$ et vérifiant la conjecture 6.2.1. Soient Γ un sous-groupe de $\overline{\mathbf{Q}}^n$ de rang $\ell \geq n+1$, et $\varphi : \mathbf{C}^n \to A_{\mathbf{C}}$ un homomorphisme analytique tel que $\varphi(\Gamma) \subset A_{\overline{\mathbf{Q}}}$ et $\Gamma \cap \ker \varphi = (0)$. Alors A admet des endomorphismes non triviaux.

L'hypothèse $\Gamma \cap \ker \varphi = (0)$ implique que pour tout $\gamma \in \Gamma$, $\gamma \neq 0$, l'homomorphisme $t \mapsto \varphi(\gamma t)$ de $\mathbf{C}$ dans $A_{\mathbf{C}}$ est irrationnel (c'est-à-dire ici non constant).

Démonstration de la proposition 6.3.6.

On démontre le résultat par récurrence sur n. Supposons, comme on peut le faire sans perte de généralité, $\ell = n+1$ et $\Gamma = \mathbf{Z}\gamma_1 + \cdots + \mathbf{Z}\gamma_\ell$ avec $\gamma_1, \ldots, \gamma_n$ $\mathbf{C}$-linéairement indépendants. Notons

$$\gamma_{n+1} = \beta_1 \gamma_1 + \cdots + \beta_n \gamma_n .$$

Supposons $\operatorname{End} A \simeq \mathbf{Z}$. Grâce à 6.2.1, en procédant comme dans la démonstration du lemme 6.3.3, on trouve des entiers rationnels $b_1, \ldots, b_{n+1}$ non tous nuls, tels que

$$b_{n+1} = \beta_1 b_1 + \cdots + \beta_n b_n .$$

Disons $b_1 \neq 0$. Soit

$$\gamma'_j = b_j \gamma_1 - b_1 \gamma_j , \qquad (1 \leq j \leq n+1) .$$

Alors

$$\gamma'_{n+1} = \beta_2 \gamma'_2 + \cdots + \beta_n \gamma'_n .$$

En considérant la restriction de φ à $\mathbf{C}\gamma'_2 + \cdots + \mathbf{C}\gamma'_n$, on voit grâce à l'hypothèse de récurrence que $\gamma'_2, \ldots, \gamma'_{n+1}$ sont $\mathbf{Q}$-linéairement dépendants, ce qui contredit l'indépendance linéaire sur $\mathbf{Q}$ de $\gamma_1, \ldots, \gamma_{n+1}$.

Exemple.

Soient A une variété abélienne simple définie sur $\bar{\mathbb{Q}}$, $\Theta : \mathbb{C}^g \to A_{\mathbb{C}}$ un homomorphisme thêta (normalisé ou non), et $(\omega_1, \ldots, \omega_{2g})$ une base de $\ker \Theta$ sur $\mathbb{Z}$, avec $\omega_1, \ldots, \omega_g$ $\mathbb{C}$-linéairement indépendants. On considère les matrices $g \times g$

$$W_1 = (\omega_1, \ldots, \omega_g) \quad , \quad W_2 = (w_{g+1}, \ldots, \omega_{2g}) \ .$$

Si l'une des colonnes de la matrice $W_1^{-1} W_2$ a ses coefficients algébriques, alors on a une relation

$$\omega_{g+k} = \beta_1 \omega_1 + \ldots + \beta_g \omega_g \ ,$$

avec $\beta_j \in \bar{\mathbb{Q}}$, $(1 \leq j \leq g)$, et $k \in \{1, \ldots, g\}$. La proposition 6.3.6 appliquée au sous-groupe à g paramètres

$$\varphi(z_1, \ldots, z_g) = \Theta(\omega_1 z_1 + \ldots + \omega_g z_g)$$

avec

$$\Gamma = \mathbb{Z}^g + \mathbb{Z}(\beta_1, \ldots, \beta_g)$$

montre que, si la conjecture 6.2.1 est vraie, alors A admet des endomorphismes non triviaux.

Remarquons enfin que si tous les coefficients de la matrice $W_1^{-1} W_2$ sont algébriques, alors φ prend des valeurs algébriques en tous les points d'un réseau de $\mathbb{C}^g$ (de rang $2g$ sur $\mathbb{Z}$) contenu dans $\bar{\mathbb{Q}}^g$.

CHAPITRE 7

LEMMES DE SCHWARZ EN PLUSIEURS VARIABLES

La généralisation à plusieurs variables des critères classiques de transcendance présente essentiellement une seule difficulté : il s'agit de l'estimation analytique donnée par le lemme de Schwarz et la formule de Jensen, qui permet d'améliorer le principe du maximum pour des fonctions ayant beaucoup de zéros. Plus généralement, un tel énoncé peut être étendu en un lemme d'approximation [Ro] exprimant en quelque sorte une propriété de "rigidité" des fonctions analytiques d'une variable : si une fonction entière a de nombreuses valeurs petites en des points bien répartis dans un disque, alors elle est petite dans tout le disque.

En plusieurs variables, le premier résultat [S 2] concernait le cas d'un produit cartésien. En 1970, Bombieri et Lang [B-L] ont introduit dans la théorie les résultats de Lelong [Le 1] sur la masse moyenne des zéros ; puis Bombieri [Bom], utilisant les estimations L^2 de Hörmander et les potentiels canoniques de Lelong, établit un lien avec les singularités d'hypersurfaces algébriques. Enfin Masser [M 1] et Moreau [Mo] ont obtenu des propriétés sur les polynômes à plusieurs variables dont nous montrerons qu'elle conduisent à de nouveaux lemmes de Schwarz.

Nous commençons par une étude générale (§ 7.1) au cours de laquelle nous donnons 3 démonstrations différentes pour le cas facile d'une variable (de manière à préparer l'exposé de la situation en plusieurs variables) ; nous montrons aussi quels sont les meilleurs résultats possibles en plusieurs variables.

Nous considérons au § 7.2 le cas "dégénéré" de produits cartésiens $S_1 \times \ldots \times S_n$ dans $\mathbb{C}^n$; on utilise alors des formules d'interpolation classiques, obtenues en itérant la formule intégrale de Cauchy.

Nous commençons au § 7.3 une étude du lemme de Schwarz pour des fonctions ayant de nombreux zéros dans la trace réelle de $\mathbb{C}^n$ (cette étude sera poursuivie dans [Wa 3] III). Le point de départ est une remarque de D.W. Masser [M 1] (appendice 2): on peut transformer les points de $B(0,1) \cap \mathbb{R}^n$ (trace réelle de la boule unité de $\mathbb{C}^n$) en les points du bord distingué d'un polydisque (Masser utilisait un logarithme, Moreau [Mo] a montré qu'une homographie est préférable). Nous utiliserons le théorème de Moreau (sans le redémontrer) pour en déduire un résultat d'approximation très précis. Nous verrons qu'un tel résultat d'approximation est équivalent à un énoncé sur les polynômes en plusieurs variables.

Nous exposons au § 7.4 les travaux de Lelong sur la masse moyenne des zéros d'une fonction entière dans $\mathbb{C}^n$. Le lemme de Schwarz auquel ils conduisent est celui de [B-L], utilisé ensuite par Bombieri [Bom].

Enfin au § 7.5 nous décrivons succintement la méthode de Bombieri [Bom] et ses applications aux singularités d'hypersurfaces algébriques [Wa 3] II ; nous utilisons un raffinement, dû à Skoda [Sk], du théorème d'existence de Hörmander Bombieri.

§ 7.1 - <u>Etude générale</u>

. Soit S un sous-ensemble fini de $\mathbb{C}^n$. Démontrer un "lemme de Schwarz" pour S, c'est trouver des nombres positifs θ_1, c_1, c_2 tels que pour toute fonction entière f dans $\mathbb{C}^n$ s'annulant sur S, et pour $R > r \geq c_1$, on ait

$$\log|f|_r \leq \log|f|_R - \theta_1 \log \frac{R}{c_2 r} . \tag{7.1.1}$$

Une telle estimation est d'autant plus utile que le nombre θ_1 est grand.

On s'intéressera aussi au cas de zéros multiples. Ici, on imposera le même minoration de la multiplicité pour tous les points de S. Etant donnée une fonction F analytique au voisinage de l'origine, on écrit son développement de Taylor en 0

$$F(z) = \sum_{h=0}^{\infty} P_h(z)$$

où P_h est un polynôme homogène de degré h, et on appelle <u>ordre du zéro</u> $z = 0$ <u>de</u> F le plus petit entier h tel que P_h ne soit pas le polynôme nul. Pour t entier positif, on cherche alors un nombre $\theta_t > 0$ tel que pour toute fonction entière f ayant en chaque point de S un zéro d'ordre $\geq t$, on ait, pour $R > r \geq c_1$,

$$\log|f|_r \leq \log|f|_R - \theta_t \log \frac{R}{c_2 r} \tag{7.1.2}$$

Nous considérons d'abord les deux cas faciles $n = 1$, et $\operatorname{Card} S = 1$, puis nous donnons une majoration de θ_t. Enfin nous étudions le cas particulier le plus important pour nous, celui où $S = \Gamma_N$, Γ étant un sous-groupe de type fini de $\mathbb{C}^n$.

a) <u>Fonctions d'une variable</u>.

Quand $n = 1$, on peut démontrer (7.1.2) avec $\theta_t = t \operatorname{Card} S$, $c_1 = \max\{|s| ; s \in S\}$ et $c_2 = 3$.

LEMME 7.1.3 - <u>Soient</u> $R > r$ <u>des nombres réels positifs</u>, t <u>un entier positif</u>, S <u>un sous-ensemble fini du disque</u> $|z| \leq r$ <u>de</u> $\mathbb{C}$, <u>et</u> f <u>une fonction entière d'une variable non identiquement nulle ayant en chaque point de</u> S <u>un zéro d'ordre</u> $\geq t$. <u>Alors</u>

$$\log|f|_r \leq \log|f|_R - t . \operatorname{Card} S . \log \frac{R-r}{2r} .$$

Cette inégalité n'améliore celle donnée par le principe du maximum

$$|f|_r \leq |f|_R$$

que si $R > 3r$, auquel cas $\frac{R-r}{2r} > \frac{R}{3r}$.

<u>Première démonstration du lemme</u> 7.1.3.

Pour $r_1 \leq R$, soient $\zeta_1, \ldots, \zeta_\nu$ les zéros de f de module inférieur ou égal à r_1, comptés avec multiplicité, où $\nu = \nu_f(0, r_1)$ est le nombre de zéros de f dans le disque $|z| \leq r_1$. On définit une fonction f_1 entière dans $\mathbb{C}$ par

$$f(z) = f_1(z) \prod_{1 \leq j \leq \nu} (z - \zeta_j) .$$

Les inégalités

$$|f_1|_r \leq |f_1|_R$$

$$|f|_r \leq |f_1|_R \, (r + r_1)^\nu$$

et

$$|f_1|_R \leq |f|_R \, (R - r_1)^{-\nu}$$

donnent

$$\log|f|_r \leq \log|f|_R - \nu_f(0, r_1) \log \frac{R - r_1}{r + r_1} \quad \text{pour } R \geq r , \ R \geq r_1 .$$

Sous les hypothèses du lemme 7.1.3 avec $r = r_1$ on a

$$\nu_f(0, r_1) \geq t \operatorname{Card} S.$$

<u>Deuxième démonstration du lemme</u> 7.1.3.

Soit $S = \{\sigma_1, \ldots, \sigma_s\}$ avec $s = \operatorname{Card} S$. On définit $u_0, u_1, \ldots, u_{st-1}$ par

$$u_{qt+r} = \sigma_{q+1} , \quad (0 \leq q \leq s-1 , \ 0 \leq r \leq t-1) .$$

Autrement dit on répète t fois chacun des éléments de S.

La relation

$$\frac{1}{\zeta - z} = \frac{1}{\zeta - u} + \frac{z-u}{\zeta - u} \cdot \frac{1}{\zeta - z}$$

donne par récurrence

$$\frac{1}{\zeta - z} = \sum_{0 \leq j < st} \frac{\prod_{i<j} (z-u_i)}{\prod_{\ell \leq j} (\zeta - u_\ell)} + \frac{\prod_{i<st} (z-u_i)}{(\zeta - z) \prod_{i<st} (\zeta - u_i)} .$$

On multiplie les deux membres par $\frac{1}{2i\pi} f(\zeta)$, et on intègre sur $|\zeta| = R$. On obtient alors la formule d'interpolation

$$f(z) = P(z) + f_1(z) \prod_{\sigma \in S} (z-\sigma)^t$$

avec

$$P(z) = \sum_{0 \leq j < st} a_j \prod_{i<j} (z - u_i) ,$$

$$a_j = \frac{1}{2i\pi} \int_{|\zeta| = R} f(\zeta) \prod_{\ell \leq j} (\zeta - u_\ell)^{-1} \, d\zeta ,$$

et

$$f_1(z) = \frac{1}{2i\pi} \int_{|\zeta| = R} f(\zeta) \prod_{\sigma \in S} (\zeta - \sigma)^{-t} \frac{d\zeta}{\zeta - z} .$$

On utilise maintenant l'hypothèse sur les zéros de f ; elle est équivalente à dire que le polynôme P est identiquement nul . On majore $|f_1|_r$ en utilisant l'expression intégrale de f_1 :

$$|f_1|_r \leq |f|_R (R-r)^{-ts} \frac{R}{R-r}$$

ce qui donne

$$|f|_r \leq |f|_R \left(\frac{2r}{R-r}\right)^{ts} \frac{R}{R-r} .$$

On utilise alors une idée de E. Landau [P-S] (Part IV Chap. 3 § 2) : appliquée à la fonction f^k , k entier ≥ 1 , cette inégalité donne

$$|f|_r^k \leq |f|_R^k \left(\frac{2r}{R-r}\right)^{kts} \frac{R}{R-r} .$$

Pour $k \to +\infty$ on obtient le résultat annoncé.

Troisième démonstration du lemme 7.1.3.

Soit $w \in \mathbb{C}$ tel que $|w| = r$ et $|f(w)| = |f|_r$. Soit $g(z) = f(z+w)$. On utilise la formule de Jensen (cf. § 7.4) :

$$\log|g(0)| = \frac{1}{2\pi} \int_0^{2\pi} \log|g(\rho e^{i\theta})| \, d\theta - \sum_{\{\zeta\}} \log \frac{\rho}{|\zeta|}$$

où $\{\zeta\}$ désigne l'ensemble des zéros de g (comptés avec multiplicité) dans le disque $|z| \leq \rho$. On choisit $\rho = R - r$. Comme

$$D(w, R-r) \subset D(0, R) ,$$

on a

$$|g|_\rho \leq |f|_R .$$

De plus pour $\sigma \in S$, $\zeta = \sigma - w$ est un zéro de g d'ordre $\geq t$ et $|\zeta| \leq 2r < R-r$. Donc

$$\sum_\zeta \log \frac{R-r}{|\zeta|} \geq st \log \frac{R-r}{2r} ,$$

ce qui démontre le lemme 7.1.3.

REMARQUE 7.1.4 - Si on remplace $z - \sigma$ par $\frac{R(z-\sigma)}{R^2 - z\bar{\sigma}}$ dans les démonstrations précédentes, on voit que l'on peut remplacer $\frac{R-r}{2r}$ par $\frac{R^2+r^2}{2rR}$ dans l'inégalité du lemme 7.1.3. (cf. [P-S], Vol I, Part III Chap. 4 n° 176 et Chap. 5 n° 232) .

b) Un seul zéro d'ordre élevé.

Pour les fonctions de plusieurs variables, le seul cas complétement trivial est celui où Card S = 1 . On peut alors choisir $\theta_t = t$, $c_1 = |\sigma|$ si $S = \{\sigma\}$, et $c_2 = 3$.

LEMME 7.1.5 - Soit f une fonction entière dans $\mathbb{C}^n$ ayant un zéro en un point σ d'ordre $\geq t$. Pour $R > r \geq |\sigma|$, on a

$$\log|f|_r \leq \log|f|_R - t \log \frac{R - |\sigma|}{r + |\sigma|} .$$

Démonstration du lemme 7.1.5.

Soit $w \in \mathbb{C}^n$ tel que $|w| = r$ et $|f(w)| = |f|_r$. On considère la fonction entière φ d'une seule variable complexe z définie par

$$\varphi(z) = f(\sigma + zw - z\sigma) .$$

Comme φ a un zéro d'ordre $\geqq t$ en $z = 0$, on est dans la situation classique du lemme de Schwarz à une variable : la fonction $z^{-t}\varphi(z)$ est entière, donc pour $R_2 \geqq R_1 > 0$,

$$R_1^{-t}|\varphi|_{R_1} \leqq R_2^{-t}|\varphi|_{R_2} .$$

On choisit $R_1 = 1$, $R_2 = \dfrac{R-|\sigma|}{r+|\sigma|}$. Les relations

$$|\varphi|_{R_2} \leqq |f|_{R_2(r+|\sigma|)+|\sigma|}$$

et

$$|\varphi(1)| = |f|_r$$

donnent le résultat annoncé.

Si on remplace les boules euclidiennes par des polydisques et que l'on note, pour $z = (z_1, \dots, z_n) \in \mathbb{C}^n$, et $r > 0$:

$$\|z\| = \max_{1 \leqq j \leqq n} |z_j| \quad \text{et} \quad \|f\|_r = \sup_{\|z\| = r} |f(z)| ,$$

la même démonstration donne

$$\log\|f\|_r \leqq \log\|f\|_R - t \log \frac{R-\|\sigma\|}{r+\|\sigma\|} .$$

Pour $\sigma = 0$ on obtient la formule habituelle pour une fonction ayant un zéro à l'origine d'ordre $\geqq t$:

(7.1.6) $$\|f\|_r \leqq \|f\|_R \cdot \left(\frac{R}{r}\right)^{-t} .$$

c) <u>Majoration de</u> θ_t.

La difficulté pour démontrer un lemme de Schwarz quand $\mathrm{Card}\, S \geqq 2$ provient du fait que pour $n \geqq 2$, les zéros d'une fonction analytique ne sont jamais des points isolés. On ne peut donc faire intervenir le nombre $\mathrm{Card}\, S$ que si les points de S possèdent certaines propriétés de bonne distribution. Regardons d'abord quel est le meilleur résultat possible.

Soit S un sous-ensemble fini de $\mathbb{C}^n$ vérifiant un lemme de Schwarz (7.1.2). Soit P un polynôme non nul de $\mathbb{C}[z]$ (où $z = (z_1, \dots, z_n)$) ayant en chaque point de S un zéro d'ordre $\geqq t$. On fixe $r = c_1$ et on fait tendre R vers

l'infini. On obtient $\theta_t \leqq \deg P$. Choisissons P de degré minimal, et soit $\omega_t(S)$ ce degré (cf. § 1.3.e). On a ainsi démontré

(7.1.7) $$\theta_t \leqq \omega_t(S) .$$

Ces nombres $\omega_t(S)$ jouent un rôle important dans la recherche de lemmes de Schwarz. Ils remplacent essentiellement la quantité $t\,\mathrm{Card}\, S$ du lemme 7.1.3. Nous verrons au § 7.5 qu'un sous-ensemble fini S de $\mathbb{C}^n$ vérifie un lemme de Schwarz 7.1.2 avec

$$\theta_t = \frac{t}{n}\,\omega_1(S) - \varepsilon t , \quad c_2 = 4n ,$$

et c_1 ne dépend que de n, S et ε (cf. lemme 5.4.1). Mais on verra aussi que c_1 ne peut pas dépendre uniquement de n, ε et $\max_{\sigma \in S} |\sigma|$, et la méthode ne permet pas de calculer c_1.

d) <u>Majoration de</u> θ_1 <u>pour</u> $S = \Gamma_N$.

Pour les applications que nous avons en vue ici, le cas particulier le plus important est celui où $t = 1$, et S est de la forme

$$\{h_1\gamma_1 + \dots + h_\ell\gamma_\ell \; ; \; (h_1, \dots, h_\ell) \in \mathbb{Z}^\ell , \; -N \leqq h_j \leqq N\} ,$$

où $\gamma_1, \dots, \gamma_\ell$ sont ℓ éléments $\mathbb{Q}$-linéairement indépendants de $\mathbb{C}^n$. On cherche alors à démontrer l'inégalité (7.1.1) avec $\theta_1 = c_3 N^m$, $c_1 = c_4 N$, et m, c_2, c_3, c_4 indépendants de N. On souhaite évidemment obtenir un nombre réel $m > 0$ aussi grand que possible.

DÉFINITION - Soit Γ un sous-groupe de $\mathbb{C}^n$ de type fini et de rang ℓ sur $\mathbb{Z}$, et soit $m \geqq 0$ un nombre réel. Nous dirons que Γ <u>vérifie un lemme de Schwarz avec l'exposant</u> m si pour toute base $\gamma_1, \dots, \gamma_\ell$ de Γ sur $\mathbb{Z}$, il existe des nombres réels positifs c_2, c_3, c_4, c_5 ne dépendant que de n, m, $\gamma_1, \dots, \gamma_\ell$ avec la propriété suivante : pour tout entier $N \geqq c_5$ et toute fonction entière f non identique à zéro et s'annulant en chaque point de l'ensemble

$$\Gamma_N = \{h_1\gamma_1 + \dots + h_\ell\gamma_\ell \; ; \; (h_1, \dots, h_\ell) \in \mathbb{Z}^\ell , \; -N \leqq h_j \leqq N\} ,$$

on a pour $R \geqq r \geqq c_4 N$

(7.1.8) $$\log|f|_r \leqq \log|f|_R - c_3 N^m \log \frac{R}{c_2 r} .$$

Si Γ vérifie un lemme de Schwarz avec l'exposant m, alors d'après (7.1.7) on a

$$\omega_1(\Gamma_N) \geqq c_3 N^m \quad \text{pour } N \geqq c_5 .$$

Le lemme 1.3.14 donne alors la majoration suivante de m :

LEMME 7.1.9 - <u>Si</u> Γ <u>vérifie un lemme de Schwarz avec l'exposant</u> m, <u>alors</u>

$$m \leqq \mu(\Gamma, \mathbb{C}^n) .$$

Soit $m_o = m_o(\Gamma)$ la borne supérieure des nombres réels m pour lesquels Γ vérifie un lemme de Schwarz avec l'exposant m. Nous démontrerons les résultats suivants :

(§ 7.2). Si $\mu(\Gamma, \mathbb{C}^n) \geqq 1$, alors $m_o \geqq 1$.

(§ 7.2). Si Γ est un produit cartésien $\Gamma_1 \times \ldots \times \Gamma_n$ dans $\mathbb{C}^n$, alors $m_o = \mu(\Gamma, \mathbb{C}^n)$.

(§ 7.3). Si $\Gamma \subset \overline{\mathbb{Q}}^n \cap \mathbb{R}^n$, alors $m_o = \mu(\Gamma, \mathbb{C}^n)$.

(§ 7.3). Soit $\ell \geqq n$. Pour presque tout $\Gamma \subset \mathbb{R}^n$ de rang ℓ, on a $m_o = \mu(\Gamma, \mathbb{C}^n)$.

(§ 7.4). Si $\mu(\Gamma, \mathbb{R}^{2n}) \geqq 1$, alors $m_o \geqq 2$.

(§ 7.4). Si $\Gamma \subset \overline{\mathbb{Q}}^n$, alors $m_o \geqq 2\mu(\Gamma, \mathbb{R}^{2n})$. Par conséquent si $\Gamma \subset \overline{\mathbb{Q}}^n$ est bien réparti dans $\mathbb{R}^{2n}$, alors $m_o = \mu(\Gamma, \mathbb{C}^n)$.

(§ 7.4). Soit $\ell \geqq 2n$. Pour presque tout $\Gamma \subset \mathbb{C}^n$ de rang ℓ, on a $m_o = \mu(\Gamma, \mathbb{C}^n)$.

Nous montrerons au chapitre 8 quelques conséquences que l'on pourrait déduire de l'égalité $m_o = \mu(\Gamma, \mathbb{C}^n)$ pour tout $\Gamma \subset \mathbb{C}^n$, que nous formulons sous forme de conjecture.

CONJECTURE 7.1.10 - <u>Soit</u> Γ <u>un sous-groupe de</u> $\mathbb{C}^n$ <u>de rang fini sur</u> $\mathbb{Z}$. <u>Pour tout</u> $\epsilon > 0$, Γ <u>vérifie un lemme de Schwarz avec l'exposant</u> $\mu(\Gamma, \mathbb{C}^n) - \epsilon$.

Le cas particulier $\Gamma \subset \overline{\mathbb{Q}}^n$ présente un certain intérêt. Nous l'appellerons "cas algébrique de la conjecture 7.1.10".

D'autre part à cause des problèmes dûs aux pôles des fonctions méromorphes dans les critères de transcendance, nous aurons besoin de versions raffinées du lemme de Schwarz, dans lesquelles nous ne supposons plus que f s'annule en tout point de Γ_N, mais seulement sur un sous-ensemble.

§ 7.2 - <u>Produits cartésiens</u>.

a) <u>Introduction</u>.

L'étude de produits cartésiens est une situation généralement considérée comme dégénérée pour plusieurs variables. Elle présente néanmoins un double intérêt ici. D'une part elle apparaît de manière naturelle dans de nombreux problèmes de transcendance (par exemple au chapitre 5). D'autre part elle fournit un exemple dans lequel on peut résoudre la conjecture 7.1.10 sans faire intervenir de considérations sur les distances mutuelles des points étudiés.

La recherche d'une majoration pour les fonctions entières dans $\mathbb{C}^n$ s'annulant sur un ensemble $S_1 \times \ldots \times S_n$ a été entreprise dès 1941 par Th. Schneider [S 2], qui inaugurait ainsi l'étude des propriétés arithmétiques de fonctions de plusieurs variables. Pour cela il étendait à n variables la formule intégrale de Cauchy. Cette méthode d'itération a été reprise notamment par F. Gross, S. Lang, puis A. Baker, et mise sous forme de lemme de Schwarz dans [Wa 3] I. Elle donne une généralisation naturelle de la deuxième démonstration de 7.1.3. En fait nous allons la présenter ici comme une généralisation de la première démonstration de 7.1.3 en introduisant des considérations élémentaires sur les idéaux qui permettent d'autres développements.

Soit $\mathfrak{J}$ un idéal de l'anneau des fonctions entières dans $\mathbb{C}^n$. On cherche des générateurs $g_1, \ldots, g_h$ de $\mathfrak{J}$, de telle manière que toute fonction $f \in \mathfrak{J}$ s'écrive

$$f = f_1 g_1 + \ldots + f_h g_h ,$$

avec des fonctions entières $f_1, \ldots, f_h$. Pour obtenir un lemme de Schwarz pour les éléments de $\mathfrak{J}$, il suffit que l'on ait de bonnes majorations des $|f_j|_R$ en fonction de $|f|_R$.

Par exemple soit $S = S_1 \times \ldots \times S_n$ un produit cartésien de sous-ensembles finis de $\mathbb{C}$, et soit t un entier positif. On choisit pour $\mathfrak{J}$ l'idéal

$$\{f \; ; \; D^{(\tau)} f(\sigma) = 0 \quad \text{pour } \sigma \in S, \; 0 \leqq \tau_j < t, \; 1 \leqq j \leqq n\} .$$

Cet idéal est engendré par les n polynômes

$$\prod_{\sigma_j \in S_j} (z_j - \sigma_j)^t , \; (1 \leqq j \leqq n) .$$

On peut démontrer ce résultat de manière élémentaire, par récurrence sur le nombre $\sum_{j=1}^{n} \operatorname{Card} S_j$. Mais on obtient des majorations plus précises des $|f_j|_R$ correspondants en exprimant ces coefficients f_j sous forme intégrale explicite. Le lemme de Schwarz que nous en déduirons est le suivant

PROPOSITION 7.2.1 - Soient $S_1, \ldots, S_n$ des sous-ensembles de $\mathbb{C}$, contenant chacun au moins s éléments distincts.

Soit $D(0,r_1) = \{z \in \mathbb{C}^n \; ; \; \|z\| \le r_1\}$ un polydisque de $\mathbb{C}^n$ contenant $S = S_1 \times \cdots \times S_n$.

Soit t un entier positif, et soit f une fonction entière vérifiant

$D^{(\tau)}f(\sigma) = 0$ pour $\sigma \in S$ et $(\tau) = (\tau_1, \ldots, \tau_n)$, $\tau_j \geqslant 0$, $\tau_1 + \ldots + \tau_n < t$.

Alors pour $R \geqq r$ et $R > r_1$ on a

$$\log \|f\|_r \le \log \|f\|_R - ts \log \frac{R-r_1}{r+r_1} .$$

Plus généralement, on obtiendra un lemme de Schwarz pour les éléments de l'idéal engendré par $P_1(z_1), \ldots, P_n(z_n)$, où $P_1, \ldots, P_n$ sont n polynômes à une variable.

b) Formules d'interpolation.

Nous commençons par exhiber une décomposition canonique des fonctions entières, associée à des polynômes $P_1, \ldots, P_n$ à une variable (ce qui correspond à un produit cartésien avec des multiplicités).

PROPOSITION 7.2.2 - Soient $P_1, \ldots, P_n$ des polynômes unitaires de $\mathbb{C}[X]$, de degrés respectifs $p_1, \ldots, p_n$. Soit f une fonction entière dans $\mathbb{C}^n$. Il existe une décomposition unique

$$f(z_1, \ldots, z_n) = \sum_{J \subset \{1, \ldots, n\}} \varphi_J(z_1, \ldots, z_n) \prod_{j \in J} P_j(z_j)$$

où, pour chaque sous-ensemble J de $\{1, \ldots, n\}$, φ_J est une fonction entière dans $\mathbb{C}^n$ et polynomiale en z_i de degré $< p_i$ pour $1 \le i \le n$ et $i \notin J$.

Ainsi $\varphi_\emptyset$ est un polynôme en $z_1, \ldots, z_n$, de degré $< p_i$ en z_i, $(1 \le i \le n)$.

Démonstration de l'unicité.

Pour $1 \leqq j \leqq n$, notons $\sigma_{j,\ell}$, $(0 \leqq \ell < q_j)$ les zéros distincts de P_j, et $\nu_{j,\ell}$ leur multiplicité, avec

$$p_j = \sum_{\ell=0}^{q_j-1} \nu_{j,\ell} .$$

Nous commençons par l'unicité de $\varphi_\emptyset$, c'est-à-dire par le résultat suivant

(7.2.3) Si $Q \in \mathbb{C}[X_1, \ldots, X_n]$ satisfait

$$D^{(\tau)}Q(\sigma_{1,\ell_1}, \ldots, \sigma_{n,\ell_n}) = 0$$

pour $(\tau) = (\tau_1, \ldots, \tau_n)$, $0 \le \tau_j < \nu_{j,\ell_j}$, $0 \le \ell_j < q_j$, $1 \le j \le n$, et si $\deg_{X_j} Q < p_j$, $(1 \le j \le n)$, alors $Q = 0$.

On démontre (7.2.3) par récurrence sur n, le cas $n = 1$ étant banal. Soit $0 \le \ell < q_n$ et $0 \le \tau < \nu_{n,\ell}$. Le polynôme

$$\frac{\partial^\tau}{\partial X_n^\tau} Q(X_1, \ldots, X_{n-1}, \sigma_{n,\ell}) \in \mathbb{C}[X_1, \ldots, X_{n-1}]$$

est identiquement nul grâce à l'hypothèse de récurrence.

Soient $z_1, \ldots, z_{n-1}$ des nombres complexes. Le polynôme

$$Q(z_1, \ldots, z_{n-1}, X) \in \mathbb{C}[X]$$

a un degré $< p_n$ et a au moins $\sum_{\ell=0}^{q_n-1} \nu_{n,\ell} = q_n$ zéros. Donc $Q = 0$.

On suppose maintenant que la fonction f de la proposition 7.2.2 est identiquement nulle, et on montre que chaque φ_J est nulle. Soit J_o un sous-ensemble de $\{1, \ldots, n\}$. Sans perte de généralité, on peut supposer $J_o = \{1, \ldots, k\}$ avec $0 \le k < n$, et on peut aussi supposer $\varphi_J = 0$ pour $J \subset J_o$, $J \ne J_o$.

Si J est un sous-ensemble de $\{1, \ldots, n\}$ qui n'est pas contenu dans J_o, on a

$$D^{(\tau)}\Big[\varphi_J \prod_{j \in J} P_j\Big](\sigma_{1,\ell_1}, \ldots, \sigma_{n,\ell_n}) = 0$$

pour $0 \le \ell_j < q_j$, $(1 \le j \le n)$, et $(\tau) = (\tau_1, \ldots, \tau_n)$ avec

$$\tau_j \geqq 0 \quad \text{pour} \quad j \in J_o$$

$$0 \le \tau_i < \nu_{i,\ell_i} \quad \text{pour} \quad i \notin J_o .$$

Donc pour les mêmes valeurs de (τ), $\ell_1,\dots,\ell_n$, la fonction

$$\psi(z_1,\dots,z_n) = -\varphi_{J_o}(z_1,\dots,z_n)\prod_{j\in J_o}P_j(z_j)$$

$$= \sum_{J\neq J_o}\varphi_J(z_1,\dots,z_n)\prod_{j\in J}P_j(z_j)$$

vérifie

$$D^{(\tau)}\psi(\sigma_{1,\ell_1},\dots,\sigma_{n,\ell_n}) = 0 .$$

Pour chaque $\tau_1,\dots,\tau_k$, $\ell_1,\dots,\ell_k$ avec $\tau_j \geqq 0$, $0\leqq \ell_j < q_j$, $(1\leqq j\leqq k)$, la fonction

$$(z_{k+1},\dots,z_n)\mapsto D^{(\tau_1,\dots,\tau_k,0,\dots,0)}\psi(\sigma_{1,\ell_1},\dots,\sigma_{k,\ell_k},z_{k+1},\dots,z_n)$$

est un polynôme de degré $< p_i$ en z_i, $(k < i \leqq n)$. D'après (7.2.3), ce polynôme est identiquement nul. Soient $z_{k+1},\dots,z_n$ des nombres complexes. Le développement de Taylor au point $\sigma_{1,\ell_1},\dots,\sigma_{k,\ell_k}$ de la fonction

$$(z_1,\dots,z_k)\mapsto \psi(z_1,\dots,z_k,z_{k+1},\dots,z_n)$$

montre que cette fonction est identiquement nulle donc $\varphi_{J_o} = 0$.

<u>Démonstration de l'existence</u>.

Pour $1\leqq j\leqq n$, on note $u_{j,k}$, $(0\leqq k < p_j)$ les racines de P_j comptées avec multiplicité, et on définit

$$P_{j,\ell}(X) = \prod_{0\leqq k<\ell}(X-u_{j,k}) \quad , \quad (0\leqq \ell\leqq p_j) .$$

Ainsi $P_{j,o}(X) = 1$ et $P_{j,p_j}(X) = P_j(X)$. Pour $J\subset\{1,\dots,n\}$, on définit

(7.2.4) $$\varphi_J(z_1,\dots,z_n) = \frac{1}{(2i\pi)^n}\int_{|\zeta_1|=R_1}\cdots\int_{|\zeta_n|=R_n} f(\zeta_1,\dots,\zeta_n)\ \times$$

$$\times\left(\prod_{i\notin J}\sum_{\ell=0}^{p_i-1}\frac{P_{i,\ell}(z_i)}{P_{i,\ell+1}(\zeta_i)}\right)\left(\prod_{j\in J}\frac{1}{(\zeta_j-z_j)P_j(\zeta_j)}\right)d\zeta_1\cdots d\zeta_n ,$$

où $R_1,\dots,R_n$ sont des nombres réels vérifiant

$$R_j > \max_{0\leqq \ell< p_j}|u_{j,\ell}| \quad , \quad (1\leqq j\leqq n) .$$

Montrons la formule désirée par récurrence sur n. Pour $n = 1$, c'est la formule d'interpolation classique à une variable (cf. la deuxième démonstration de 7.1.3) avec

$$\varphi_\emptyset(z) = \sum_{\ell=0}^{p-1}\left(\frac{1}{2i\pi}\int_{|\zeta|=R} f(\zeta)\prod_{k=0}^{\ell}(\zeta-u_k)^{-1}d\zeta\right)\prod_{k=0}^{\ell-1}(z-u_k)$$

et

$$\varphi_{\{1\}}(z) = \frac{1}{2i\pi}\int_{|\zeta|=R} f(\zeta)\prod_{k=0}^{p-1}(\zeta-u_k)^{-1}\frac{d\zeta}{\zeta-z} .$$

Supposons la formule démontrée pour $n-1$ variables. Soit $z_n\in\mathbb{C}$. D'après l'hypothèse de récurrence on a

$$f(z_1,\dots,z_n) = \sum_{J\subset\{1,\dots,n-1\}}\psi_J(z_1,\dots,z_n)\prod_{j\in J}P_j(z_j)$$

avec

$$\psi_J(z_1,\dots,z_n) = \frac{1}{(2i\pi)^{n-1}}\int_{|\zeta_1|=R_1}\cdots\int_{|\zeta_{n-1}|=R_{n-1}} f(\zeta_1,\dots,\zeta_{n-1},z_n)$$

$$\left(\prod_{\substack{i\notin J\\ 1\leqq i<n}}\sum_{\ell=0}^{p_i-1}\frac{P_{i,\ell}(z_i)}{P_{i,\ell+1}(\zeta_i)}\right)\left(\prod_{\substack{j\in J\\ 1\leqq j<n}}\frac{1}{(\zeta_j-z_j)P_j(\zeta_j)}\right)d\zeta_1\cdots d\zeta_{n-1} .$$

Pour $\zeta_1,\dots,\zeta_{n-1}\in\mathbb{C}$, on a, d'après la formule en une variable,

$$f(\zeta_1,\dots,\zeta_{n-1},z_n) = g_\emptyset(\zeta_1,\dots,\zeta_{n-1},z_n) + g_{\{1\}}(\zeta_1,\dots,\zeta_{n-1},z_n)P_n(z_n)$$

avec

$$g_\emptyset(\zeta_1,\dots,\zeta_{n-1},z_n) = \frac{1}{2i\pi}\int_{|\zeta_n|=R_n} f(\zeta_1,\dots,\zeta_n)\sum_{\ell_n=0}^{p_n-1}\frac{P_{n,\ell_n}(z_n)}{P_{n,\ell_n+1}(\zeta_n)}d\zeta_n$$

et

$$g_{\{1\}}(\zeta_1,\dots,\zeta_{n-1},z_n) = \frac{1}{2i\pi}\int_{|\zeta_n|=R_n} f(\zeta_1,\dots,\zeta_n)\frac{1}{(\zeta_n-z_n)P_n(\zeta_n)}d\zeta_n .$$

En reportant dans la formule donnant ψ_J , on trouve

$$\psi_J(z_1 ,\dots, z_n) = \varphi_J(z_1 ,\dots, z_n) + \varphi_{J \cup \{n\}}(z_1 ,\dots, z_n)P_n(z_n) .$$

Mais on décrit toutes les parties de $\{1 ,\dots, n\}$ en considérant tous les ensembles J et $J \cup \{n\}$, quand J décrit les parties de $\{1 ,\dots, n-1\}$. La proposition 7.2.2 est donc démontrée avec la formule (7.2.4).

Les relations (7.2.4) permettent de majorer les φ_J .

LEMME 7.2.5 - Avec les notations de la proposition 7.2.2, soient $\sigma_{j,\ell}$, $(0 \leq \ell < q_j)$ les zéros distincts de P_j , $(1 \leq j \leq n)$, et soient R , r, r_1 des nombres réels avec

$$R > r + 2r_1 \quad , \quad r_1 \geq |\sigma_{j,\ell}| \text{ , } (0 \leq \ell < q_j \text{ , } 1 \leq j \leq n) .$$

Pour tout $J \subset \{1 ,\dots, n\}$, on a

$$\|\varphi_J\|_r \leq \|f\|_R (R-r_1)^{-p_J} . \left(\frac{R}{R-r-2r_1}\right)^n ,$$

où

$$p_J = \sum_{j \in J} \deg P_j .$$

Démonstration du lemme 7.2.5.

On utilise la formule (7.2.4) avec $R_1 = \dots = R_n = R$. Comme $R > r + 2r_1$ on a $\dfrac{r+r_1}{R-r_1} < 1$. Pour $i \notin J$, on a

$$\left|\frac{P_{i,\ell}(z_i)}{P_{i,\ell+1}(\zeta_i)}\right| \leq \frac{(r+r_1)^{\ell}}{(R-r_1)^{\ell+1}} \quad , \quad |z_i| = r, |\zeta_i| = R ,$$

donc

$$\sum_{\ell=0}^{p_i-1} \left|\frac{P_{i,\ell}(z_i)}{P_{i,\ell+1}(\zeta_i)}\right| \leq \frac{1}{R-r-2r_1} .$$

Pour $j \in J$, on a

$$\left|\frac{1}{\zeta_j - z_j} \cdot \frac{1}{P_j(\zeta_j)}\right| \leq \frac{1}{(R-r_1)^{p_j}} \cdot \frac{1}{R-r} \text{ , } |z_j| = r, |\zeta_j| = R ,$$

d'où

$$\|\varphi_J\|_r \leq \|f\|_R \cdot \left(\frac{1}{R-r-2r_1}\right)^{n-\mathrm{Card}\, J} \cdot \left(\frac{1}{R-r_1}\right)^{p_J} \cdot \left(\frac{1}{R-r}\right)^{\mathrm{Card}\, J} \cdot R^n$$

ce qui démontre le lemme 7.2.5.

Supposons maintenant que la fonction f satisfasse

$$D^{(\tau)}f(\sigma_{1,\ell_1} ,\dots, \sigma_{n,\ell_n}) = 0$$

pour $(\tau) = (\tau_1 ,\dots, \tau_n)$, $0 \leq \tau_j < \nu_{j,\ell_j}$, $0 \leq \ell_j < q_j$, $1 \leq j \leq n$, où ν_{j,ℓ_j} est l'ordre de multiplicité de la racine σ_{j,ℓ_j} de P_j . D'après l'unicité de $\varphi_\emptyset$ (cf. 7.2.3), on a $\varphi_\emptyset = 0$.

Soit $p = \min\limits_{1 \leq j \leq n} \deg P_j$. Alors pour tout $J \subset \{1 ,\dots, n\}$ on a, d'après le lemme 7.2.5

$$\|\varphi_J\|_r \prod_{j \in J} \|P_j\|_r \leq \|f\|_R \cdot \left(\frac{r+r_1}{R-r_1}\right)^p \cdot \left(\frac{R}{R-r-2r_1}\right)^n$$

donc

$$\|f\|_r \leq \|f\|_R \cdot \left(\frac{r+r_1}{R-r_1}\right)^p \cdot \left(\frac{2R}{R-r-2r_1}\right)^n .$$

En prenant

$$P_j(z_j) = \prod_{\ell=0}^{s-1} (z_j - \sigma_{j,\ell})^t \quad , \quad (1 \leqslant j \leqslant n)$$

A. Azhari a montré que l'on avait, sous les hypothèses de la proposition 7.2.1.,

$$\|\varphi_\emptyset\|_r \leqslant \left(\frac{r+r_1}{R-r_1}\right)^{st} \|f\|_R \cdot \left(\frac{st\, R}{R-r_1}\right)^n .$$

La proposition 7.2.1. s'obtient alors en utilisant l'astuce de Landau (cf. p. 116).

D'autre part si on définit, pour $1 \leq j \leq n$,

$$f_j(z_1 ,\dots, z_n) = \sum_J \varphi_J(z_1 ,\dots, z_n) \prod_{h \in J, h \neq j} P_h(z_h) ,$$

où la somme est étendue aux sous-ensembles J de $\{j, j+1 ,\dots, n\}$ qui contiennent j , on déduit de la proposition 7.2.2 et du lemme 7.2.5 le corollaire suivant :

COROLLAIRE 7.2.6 - Soient $P_1, \dots, P_n$ des polynômes unitaires de $\mathbf{C}[X]$. Pour $1 \leqq j \leqq n$, on note p_j le degré de P_j, $\sigma_{j,\ell}$, $(0 \leqq \ell < q_j)$ les racines distinctes de P_j et $\nu_{j,\ell}$ leur multiplicité. Soient r, r_1, R des nombres réels,

$$r_1 \geqq |\sigma_{j,\ell}|, \quad (0 \leqq \ell < q_j, \ 1 \leqq j \leqq n) \quad \text{et} \quad R > r + 2r_1 .$$

Dans l'anneau des fonctions entières dans $\mathbf{C}^n$, l'idéal $\mathfrak{J}$ engendré par $P_1(z_1), \dots, P_n(z_n)$ est l'ensemble des fonctions f entières dans $\mathbf{C}^n$ et vérifiant

$$D^{(\tau)} f(\sigma_{1,\ell_1}, \dots, \sigma_{n,\ell_n}) = 0$$

pour $(\tau) = (\tau_1, \dots, \tau_n)$, $0 \leqq \tau_j < \nu_{j,\ell_j}$, $0 \leqq \ell_j < q_j$, $1 \leqq j \leqq n$.

De plus, si $f \in \mathfrak{J}$, il existe des fonctions entières $f_1, \dots, f_n$ vérifiant

$$f(z_1, \dots, z_n) = \sum_{j=1}^{n} f_j(z_1, \dots, z_n) P_j(z_j)$$

et

$$(R-r)^{p_j} \|f_j\|_r \leqq \|f\|_R \cdot \left(\frac{2R}{R-r-2r_1} \right)^n .$$

Pour $R \geqq 3r + 6r_1$, on a $\dfrac{2R}{R-r-2r_1} \leqq 3$.

c) Application aux sous-groupes de $\mathbf{C}^n$.

Soient $\Gamma_1, \dots, \Gamma_n$ des sous-groupes de $\mathbf{C}$ de rang $\ell_1, \dots, \ell_n$ sur $\mathbf{Z}$. Alors $\Gamma = \Gamma_1 \times \dots \times \Gamma_n$ est un sous-groupe de $\mathbf{C}^n$ de rang $\ell = \ell_1 + \dots + \ell_n$, et on a

$$\mu(\Gamma, \mathbf{C}^n) = \min_{1 \leqq j \leqq n} \ell_j .$$

Pour $1 \leqq j \leqq n$, soit $\gamma_{j,1}, \dots, \gamma_{j,\ell_j}$ une base de Γ_j sur $\mathbf{Z}$.
Pour $N \geqq 1$, notons

$$\Gamma_{j,N} = \left\{ \sum_{i=1}^{\ell_j} h_i \gamma_{j,i} \ ; \ (h_i) \in \mathbf{Z}^{\ell}, \ |h_i| \leqq N \right\}$$

et

$$\Gamma_N = \Gamma_{1,N} \times \dots \times \Gamma_{n,N}$$

$$= \left\{ \left(\sum_{i=1}^{\ell_j} h_{j,i} \gamma_{j,i} \right)_{1 \leqq j \leqq n} ; \ (h_{i,j}) \in \mathbf{Z}^{\ell}, \ |h_{i,j}| \leqq N \right\} .$$

Comme

$$\operatorname{Card} \Gamma_{j,N} \geqq N^{\ell_j} \geqq N^{\mu(\Gamma, \mathbf{C}^n)} ,$$

on en déduit que Γ vérifie un lemme de Schwarz avec l'exposant $\mu(\Gamma, \mathbf{C}^n)$.

Maintenant si Γ est un sous-groupe quelconque de $\mathbf{C}^n$ (de rang fini) tel que $\mu(\Gamma, \mathbf{C}^n) \geqq 1$, alors Γ contient n éléments $\gamma_1, \dots, \gamma_n$ $\mathbf{C}$-linéairement indépendants, et dans la base $\gamma_1, \dots, \gamma_n$ le sous-groupe $\mathbf{Z}\gamma_1 + \dots + \mathbf{Z}\gamma_n$ de Γ devient le produit cartésien $\mathbf{Z}^n$. Donc Γ vérifie un lemme de Schwarz avec l'exposant 1.

§ 7.3 - Sous-groupes de la trace réelle de $\mathbf{C}^n$.

a) Enoncés des résultats

Nous avons déjà remarqué que pour un sous-groupe Γ de la trace réelle $\mathbf{R}^n$ de $\mathbf{C}^n$, on a $\mu(\Gamma, \mathbf{C}^n) = \mu(\Gamma, \mathbf{R}^n)$. D'autre part D.W. Masser ([M1] appendice II) a montré comment des informations concernant les valeurs de polynômes sur la trace réelle pouvaient être transportées sur le bord distingué d'un polydisque dont on peut alors utiliser le rôle de frontière de Shilov. Nous allons démontrer le résultat suivant

THÉORÈME 7.3.1 - Soit Γ un sous-groupe de type fini de $\mathbf{R}^n$, ayant un coefficient de densité $\geqq \varkappa$. Alors Γ vérifie un lemme de Schwarz avec l'exposant $\varkappa$.

Le cas particulier le plus important se déduit alors du théorème 1.3.10.

COROLLAIRE 7.3.2 - Si Γ est un sous-groupe de type fini de $\mathbf{R}^n \cap \overline{\mathbf{Q}}^n$, alors pour tout $\epsilon > 0$ Γ vérifie un lemme de Schwarz avec l'exposant $\mu(\Gamma, \mathbf{C}^n) - \epsilon$.

De même on déduit de la proposition 1.3.12 le corollaire suivant

COROLLAIRE 7.3.3 - Soient n et ℓ des entiers, $\ell \geqq n$. Pour presque tout $(\gamma_1, \dots, \gamma_\ell) \in \mathbf{R}^{n\ell}$, pour tout $\epsilon > 0$ le sous-groupe de $\mathbf{C}^n$ engendré par $\gamma_1, \dots, \gamma_\ell$ vérifie un lemme de Schwarz avec l'exposant $\frac{\ell}{n} - \epsilon$.

On remarquera que dans ces conditions on a $\mu(\Gamma, \mathbf{R}^n) = \mu(\Gamma, \mathbf{C}^n) = \frac{\ell}{n}$.

Le théorème 7.3.1 est une conséquence de l'énoncé plus précis suivant

THÉORÈME 7.3.4 - Soit n un entier positif. Il existe des constantes positives c_6, c_7, c_8, ne dépendant que de n, ayant la propriété suivante. Soient r_1, r et R des nombres réels, $R \geqq r \geqq r_1 > 0$ et q, L deux entiers positifs.

Soient $f_1, \ldots, f_q$ des fonctions continues dans le polydisque

$$D(0,R) = \{z \in \mathbb{C}^n,\ \|z\| \leq R\},$$

analytiques à l'intérieur. Soient $S_1, \ldots, S_q$ des sous-ensembles de $\mathbb{C}^n$ tels que pour tout $\zeta \in D(0,r_1) \cap \mathbb{R}^n$, il existe $\sigma \in S = S_1 \cup \ldots \cup S_q$ avec

$$\|\zeta - \sigma\| \leq c_6\, r_1/qL .$$

Alors

$$\min_{1 \leq j \leq q} \|f_j\|_r \leq \left(\frac{c_7 r}{R}\right)^L \cdot \max_{1 \leq j \leq q} \|f_j\|_R + \left(\frac{c_8 r}{r_1}\right)^L \max_{1 \leq j \leq q} \sup_{\sigma \in S_j} |f_j(\sigma)| .$$

b) Un théorème de Masser et Moreau sur les polynômes à plusieurs variables.

L'outil essentiel de la démonstration est le résultat suivant de J.C. Moreau [Mo] qui améliore un énoncé antérieur de D.W. Masser (appendice 2 de [M1]).

THÉORÈME 7.3.5 - Il existe deux constantes c_9, c_{10}, positives ne dépendant que de n, telles que si $Q \in \mathbb{C}[X_1, \ldots, X_n]$ est un polynôme de degré (total) inférieur ou égal à L, et si $S \subset \mathbb{C}^n$ est tel que pour tout point $\zeta \in \mathbb{R}^n \cap B(0,1)$ de la trace réelle de la boule unité, la distance de ζ à S soit inférieure à $c_9 L^{-1}$, alors

$$H(Q) \leq e^{c_{10}L} \sup_{\sigma \in S} |Q(\sigma)| .$$

L'énoncé de D.W. Masser donnait seulement la nullité de Q sous l'hypothèse $Q(\sigma) = 0$ pour tout $\sigma \in S$ (et avec $c_9 L^{-1}$ remplacé par $c_9(L \log L)^{-1}$). Le fait que le résultat de Moreau soit très précis jouera un rôle fondamental.

Nous déduirons les énoncés du a) ci-dessus de ce théorème 7.3.5. En fait, le théorème 7.3.4 est une extension du théorème 7.3.5. En effet, si Q est un polynôme de degré $\leq L_1$ vérifiant les hypothèses du théorème 7.3.5 avec L remplacé par L_1, le théorème 7.3.4 avec $q = 1$, $r = r_1 = 1$, $L = 2L_1$ et $R \to +\infty$ montre que la conclusion du théorème 7.3.5 est vraie (avec $c_9 = 2c_6$).

c) Démonstration du théorème 7.3.4.

Soit j un entier, $1 \leq j \leq q$. On écrit le développement de Taylor de f_j à l'origine

$$f_j(z) = \sum_{h \in \mathbb{N}^n} a_{j,h}\, z^h$$

(avec $z^h = z_1^{h_1} \ldots z_n^{h_n}$) sous la forme

$$f_j = P_j + g_j ,$$

où

$$P_j(z) = \sum_{|h| < L} a_{j,h}\, z^h ,$$

et où $g_j = f_j - P_j$ a un zéro d'ordre $\geq L$ à l'origine. D'après (7.1.6), pour $0 \leq \rho \leq R$,

$$\|g_j\|_\rho \leq \left(\frac{\rho}{R}\right)^L \|g_j\|_R .$$

D'autre part il n'y a évidemment pas de restriction à supposer $S \subset D(0,2r_1)$; donc

$$\sup_{\sigma \in S_j} |P_j(\sigma)| \leq \sup_{\sigma \in S_j} |f_j(\sigma)| + \|g_j\|_{2r_1} .$$

De plus les inégalités de Cauchy

$$|a_{j,h}| \leq R^{-|h|} \|f_j\|_R$$

montrent que l'on a

$$\|P_j\|_R \leq \binom{L+n}{n} \|f_j\|_R ,$$

donc

$$\|g_j\|_R \leq \|f_j\|_R + \|P_j\|_R \leq c_{11}^L \|f_j\|_R .$$

Considérons maintenant les ensembles

$$S'_j = \left\{\frac{1}{r_1}\sigma,\ \sigma \in S_j\right\} , \quad (1 \leq j \leq q) ,$$

et

$$S' = S'_1 \cup \ldots \cup S'_q .$$

On choisit

$$c_6 = \min(1, c_9) .$$

Pour tout point ζ' de la trace réelle de la boule unité, il existe $\sigma' \in S'$ tel que

$$\|\zeta' - \sigma'\| \leq c_9/qL .$$

Posons

$$Q_j(z) = P_j(r_1 z) , \quad (1 \leq j \leq q) ,$$

de telle sorte que

$$\|Q_j\|_{\frac{r}{r_1}} = \|P_j\|_r$$

et

$$\sup_{\sigma' \in S'_j} |Q_j(\sigma')| = \sup_{\sigma \in S_j} |P_j(\sigma)| \ .$$

Nous utilisons maintenant le théorème 7.3.5 pour le polynôme $Q_1 \dots Q_q$:

$$H\Big(\prod_{j=1}^{q} Q_j\Big) \leq e^{c_{12}qL} \sup_{\sigma' \in S'} \prod_{j=1}^{q} |Q_j(\sigma')| \ .$$

Grâce au lemme 1.1.12, on a

$$\prod_{j=1}^{q} H(Q_j) \leq e^{nqL} H\Big(\prod_{j=1}^{q} Q_j\Big) \ .$$

D'autre part

$$\|Q_j\|_{\frac{r}{r_1}} \leq \binom{L+n}{n} H(Q_j) . \left(\frac{r}{r_1}\right)^L ,$$

donc on obtient

$$\prod_{j=1}^{q} \|P_j\|_r \leq \left(\frac{c_{13}r}{r_1}\right)^{qL} \prod_{j=1}^{q} \sup_{\sigma \in S_j} |P_j(\sigma)| \ .$$

Soit j_o avec

$$\|P_{j_o}\|_r = \min_{1 \leq j \leq q} \|P_j\|_r \ .$$

On a

$$\|P_{j_o}\|_r^q \leq \left(\frac{c_{13}r}{r_1}\right)^{qL} \prod_{j=1}^{q} \sup_{\sigma \in S_j} |P_j(\sigma)|$$

et

$$\|f_{j_o}\|_r \leq \|P_{j_o}\|_r + \|g_{j_o}\|_r$$

$$\leq \left(\frac{c_{14}r}{R}\right)^L . \|g_{j_o}\|_R + \left(\frac{c_{15}r}{r_1}\right)^L \max_{1 \leq j \leq q} \sup_{\sigma \in S_j} |f_j(\sigma)|$$

$$\leq \left(\frac{c_{16}r}{R}\right)^L \|f_{j_o}\|_R + \left(\frac{c_{15}r}{r_1}\right)^L \max_{1 \leq j \leq q} \sup_{\sigma \in S_j} |f_j(\sigma)| \ ,$$

ce qui démontre le théorème 7.3.4.

Pour d'autres développements de cette étude, voir § 7.6.

§ 7.4 - La masse moyenne des zéros.

a) Introduction

Les fonctions de plusieurs variables ne sont véritablement intervenues dans la théorie des nombres transcendants qu'en 1970, à partir d'un travail de Bombieri et Lang [B-L] dans lequel le rôle essentiel est joué par l'énoncé suivant, dû principalement à Lelong [Le 1].

PROPOSITION 7.4.1 - Soit f une fonction entière ayant des zéros $z_1, \dots, z_m$ (comptés avec multiplicité) dans une boule euclidienne $B(0, r)$. Soit δ un nombre réel vérifiant $\delta \leq r$ et

$$0 < \delta \leq \frac{1}{2} \min_{z_j \neq z_k} |z_j - z_k| \ .$$

Pour $R \geq r$ on a

$$\log|f|_r \leq \log|f|_R - m\left(\frac{\delta}{3r}\right)^{2n-2} \log\left(\frac{R}{4r}\right) \ .$$

En utilisant le lemme 1.3.8, on en déduit le résultat suivant.

THÉORÈME 7.4.2 - Soit Γ un sous-groupe de $\mathbb{C}^n$ de type fini sur $\mathbb{Z}$. Si Γ a un coefficient de densité relatif à $\mathbb{R}^{2n}$ supérieur ou égal à $\varkappa$, alors Γ vérifie un lemme de Schwarz avec l'exposant $2\varkappa$.

L'exemple le plus simple est celui d'un réseau, c'est-à-dire d'un sous-groupe bien réparti dans $\mathbb{R}^{2n}$ de rang $2n$. Alors $\mu(\Gamma, \mathbb{R}^{2n}) = 1$ et $\mu(\Gamma, \mathbb{C}^n) = 2$.

COROLLAIRE 7.4.3 - Soit Γ un réseau dans $\mathbb{C}^n$. Alors Γ vérifie un lemme de Schwarz avec l'exposant 2.

Ce résultat est très utile dans l'étude des points algébriques de fonctions abéliennes [M 2], [M 6], [L 6], [C-L].

Une autre conséquence du théorème 7.4.2 concerne le cas $\Gamma \subset \overline{\mathbb{Q}}^n$. Grâce au théorème 1.3.10, on obtient :

COROLLAIRE 7.4.4 - Soit Γ un sous-groupe de type fini de $\overline{\mathbb{Q}}^n$. Alors pour tout $\epsilon > 0$, Γ vérifie un lemme de Schwarz avec l'exposant $2\mu(\Gamma, \mathbb{R}^{2n}) - \epsilon$.

Enfin, en utilisant la proposition 1.3.12, on déduit du théorème 7.4.2 le corollaire suivant.

COROLLAIRE 7.4.5 - Pour presque tout sous-groupe Γ de $\mathbb{C}^n$ de rang $\ell \geqq 2n$, pour tout $\varepsilon > 0$, Γ vérifie un lemme de Schwarz avec l'exposant $\frac{\ell}{n} - \varepsilon$.

Pour un tel sous-groupe Γ on a, d'après le lemme 7.1.9, $\mu(\Gamma, \mathbb{C}^n) = \frac{\ell}{n}$.

REMARQUE 7.4.6 - Dans le théorème 7.4.2, et aussi par voie de conséquence dans ses corollaires 7.4.3, 7.4.4 et 7.4.5, l'estimation (7.1.8) donnée par le lemme de Schwarz reste valable si on remplace l'hypothèse $f(\gamma) = 0$ pour tout $\gamma \in \Gamma_N$ par

$$\operatorname{Card}\{\gamma \in \Gamma_N,\ f(\gamma) = 0\} \geqq \eta \operatorname{Card} \Gamma_N ,$$

avec $0 < \eta \leqq 1$. Les constantes c_2, c_3, c_4, c_5 intervenant dans (7.1.8) dépendent alors de η. Ce "lemme de Schwarz raffiné" est immédiat à partir du lemme 1.3.8 et de la proposition 7.4.1.

La démonstration de la proposition 7.4.1 repose sur l'étude de la masse moyenne $\nu_f(0,R)$ des zéros de la fonction f dans la boule $B(0,R)$, c'est-à-dire la moyenne sur cette boule de la distribution positive $\frac{1}{2\pi} \Delta \log|f|$.

En 1899, H. Poincaré avait, très laborieusement, obtenu le fait que localement $\log|f(z)|$ est un potentiel (de noyau $\|x - y\|^{-2n+2}$) de masse $2\pi\, d\sigma$, où $d\sigma$ est l'aire de $f = 0$, et son calcul est très compliqué, alors que c'est seulement le "Théorème de Gauss" des physiciens, moyennant l'usage des mesures de Radon.

Le premier calcul général remonte au mémoire [Le 1] de P. Lelong en 1950 - qui faisait suite à son important travail sur les fonctions plurisousharmoniques. La méthode des pavés d'inclusion qui y figure nous servira pour la démonstration de la proposition 7.4.1.

Le point de vue de Stoll [St] est différent : il donne une représentation de $\log f$ (et non seulement de $\log|f|$) mais qui ne converge qu'au voisinage de l'origine.

Ces travaux permettent de démontrer un lemme de Schwarz du type (7.1.2) dans lequel θ_t est remplacé par $\nu_f(0,t)$. (cf. [B-L], [Bom]); cet énoncé nous sera utile aussi au § 7.5. Il nécessite quelques propriétés des fonctions sous-harmoniques et plurisousharmoniques.

Pour présenter ces outils, voici une démonstration de la formule de Jensen pour les fonctions analytiques d'une variable complexe [Le 2] § 7.1.

Soit f une fonction analytique dans un voisinage d'un disque fermé $D(0,R)$ de $\mathbb{C}$. Notons $\{\zeta\}$ les zéros de f dans ce disque, comptés avec leur ordre de multiplicité. Comme la distribution $\frac{1}{2\pi} \Delta \log|z|$ est la mesure de Dirac δ_0 à l'origine, la distribution μ définie par $\frac{1}{2\pi} \Delta \log|f|$ dans $D(0,R)$ est

$$\mu = \sum_{\{\zeta\}} \delta_\zeta .$$

La fonction

$$\Phi(z) = \log|f(z)| - \sum_{\{\zeta\}} \log|z-\zeta|$$

est harmonique dans $D(0,R)$ (c'est le logarithme du module d'une fonction analytique sans zéros dans $D(0,R)$; on peut aussi remarquer que l'on a

$$(\log z) * \mu = \sum_{\{\zeta\}} \log|z-\zeta| ,$$

donc $\Delta\Phi = 0$). Si on note $\lambda(u;0,R)$ la moyenne d'une fonction u sur le cercle de centre 0 et de rayon R, on a

$$\Phi(0) = \lambda(\Phi;0,R) .$$

Supposons $f(0) \neq 0$. Alors

$$\Phi(0) = \log|f(0)| - \sum_{\{\zeta\}} \log|\zeta|$$

et

$$\lambda(\Phi;0,R) = \lambda(\log|f|;0,R) - \sum_{\{\zeta\}} \lambda(\log|z-\zeta|;0,R) .$$

Pour $w \in \mathbb{C}$ et $|z| = R$, on a

$$|z-w| = \frac{1}{R}|\bar{w}z - R^2| ;$$

la propriété de la moyenne pour les fonctions harmoniques donne alors :

$$\lambda(\log|z-w|;0,R) = \begin{cases} \log|w| & \text{si } |w| > R \\ \log R & \text{si } |w| < R \end{cases} .$$

Comme $|\zeta| \leqq R$, on obtient

$$\lambda(\log|z-\zeta|;0,R) = \operatorname{Log} R .$$

Enfin

$$\sum_{\{\zeta\}} \log \frac{R}{|\zeta|} = \sum_{\{\zeta\}} \int_{|\zeta| \leq t \leq R} \frac{dt}{t}$$

$$= \int_{0 \leq t \leq R} \left(\sum_{|\zeta| \leq t} 1 \right) \frac{dt}{t}$$

$$= \int_0^R \mu(t) \frac{dt}{t}$$

où $\mu(t)$ est la masse de $D(0,t)$ pour la mesure μ (c'est le nombre de zéros de f dans $|z| \leq t$).

Finalement on obtient

$$\log|f(0)| = \lambda(\log|f| \ ; 0,R) - \int_0^R \mu(t) \frac{dt}{t} .$$

b) Fonctions sous-harmoniques.

Pour simplifier les notations nous supposons $n \geqq 2$. Soit Ω un ouvert de $\mathbb{C}^n$ contenant la boule fermée $\bar{B}(0,R)$. On considère une fonction u sous-harmonique dans Ω, c'est-à-dire une application $u : \Omega \to [-\infty, +\infty[$ localement intégrale dont le Laplacien Δu est une distribution positive. La mesure de Riesz associée à u dans $B(0,R)$ est $\mu = \frac{1}{\theta_{2n}} \Delta u$ avec $\theta_{2n} = \frac{4\pi^n}{(n-2)!}$. Considérons les fonctions

$$h(z) = - |z|^{2-2n}$$

et

$$h*\mu(w) = - \int_{B(0,R)} \frac{d\mu(z)}{|w-z|^{2n-2}}$$

Alors $\frac{1}{\theta_{2n}} \Delta h$ est la distribution de Dirac à l'origine, et la fonction $\Phi = u - h*\mu$ est harmonique (son Laplacien est nul) dans $B(0,R)$.

On note $\mu(t)$ la masse de $B(0,t)$ pour la mesure μ, et $\nu(t) = \frac{2n-2}{t^{2n-2}} \mu(t)$, pour $0 < t \leqq R$. Comme le nombre

$$\frac{\theta_{2n}}{2\pi} \cdot \frac{t^{2n-2}}{2n-2} = \frac{\pi^{n-1}}{(n-1)!} t^{2n-2} = v_{2n-2} t^{2n-2}$$

est la mesure de Lebesgue de la boule de rayon t dans $\mathbb{R}^{2n-2}$, $\nu(t)$ est la masse moyenne de la distribution $\frac{1}{2\pi} \Delta u$ dans $B(0,t)$.

Pour $w \in \mathbb{C}^n$, $|w| < R$, notons

$$\lambda_w(u;0,R) = \frac{1}{\sigma_{2n} R} \int_{S(0,R)} u(z) \frac{R^2 - |w|^2}{|z-w|^{2n}} d\sigma(z) ,$$

où $d\sigma(z)$ est l'élément d'aire de la sphère $S(0,R)$ et $\sigma_{2n} = \frac{2\pi^n}{(n-1)!}$.

En particulier $\lambda_0(u;0,R)$ est la moyenne de u sur $S(0,R)$.

Si Φ est une fonction harmonique dans Ω, la formule de Poisson s'écrit

$$\Phi(w) = \lambda_w(\Phi;0,R) .$$

Ainsi

$$\lambda_w(1;0,R) = 1 .$$

Si u est sous-harmonique dans Ω, on obtient

$$u(w) = \lambda_w(u;0,R) + (h*\mu)(w) - \lambda_w(h*\mu;0,R) .$$

On remarque que pour $z \in B(0,R)$, la fonction

$$\varphi_z(x) = - \left(\frac{R|z|}{|R^2 z - |z|^2 x|} \right)^{2n-2}$$

est harmonique dans $|x| < R$, et coïncide sur $|x| = R$ avec la fonction

$$h_z(x) = h(z-x) .$$

On en déduit

$$\lambda_w(h*\mu;0,R) = \int_{B(0,R)} \lambda_w(\varphi_z;0,R) d\mu(z)$$

$$= \int_{B(0,R)} \varphi_z(w) d\mu(z) ,$$

d'où

$$u(w) = \lambda_w(u;0,R) - \int_{B(0,R)} \left(\varphi_z(w) - h_z(w) \right) d\mu(z) . \tag{7.4.7}$$

On vérifie que pour $|z| = t$, on a

$$\varphi_z(w) - h_z(w) \geqq - \left(\frac{R}{R^2 + t|w|} \right)^{2n-2} + \left(\frac{1}{|w|+t} \right)^{2n-2} ,$$

avec égalité pour $w = 0$. Intégrant par partie dans (7.4.7), on trouve

$$u(w) \leq \lambda_w(u;0,R) - \int_0^R \left[\left(1 + \frac{|w|}{t}\right)^{1-2n} - \frac{|w|}{R}\left(\frac{R}{t} + \frac{|w|}{R}\right)^{1-2n}\right] \nu(t)\, \frac{dt}{t} ,$$

et pour $w = 0$,

$$u(0) = \lambda_o(u;0,R) - \int_0^R \nu(t)\, \frac{dt}{t} , \tag{7.4.8}$$

ce qui est la formule de Jensen pour les fonctions sous-harmoniques (elle n'est intéressante que s'il existe $\varepsilon > 0$ avec $\mu(\varepsilon) = 0$).

Finalement, comme $\lambda_w(1;0,R) = 1$, on a

$$\lambda_w(u;0,R) \leq \sup_{S(0,R)} u ,$$

d'où

$$\sup_{S(0,r)} u \leq \sup_{S(0,R)} u - \int_0^R \left[\left(1 + \frac{|w|}{t}\right)^{1-2n} - \frac{|w|}{R}\left(\frac{R}{t} + \frac{|w|}{R}\right)^{1-2n}\right] \nu(t)\, \frac{dt}{t} . \tag{7.4.9}$$

(Le calcul précédent pour $w \neq 0$ repose sur une communication de J. Oesterlé. Voir aussi [St] § 1).

c) Fonctions plurisousharmoniques.

Soit u une fonction semi-continue supérieurement dans un ouvert Ω de $\mathbb{C}^n$ (pour tout $c \in \mathbb{R}$, $u(z) < c$ est un ouvert dans Ω) à valeurs dans $[-\infty, +\infty[$. On dira que u est plurisousharmonique dans Ω si pour tout polydisque compact $\{z + tw ; t \in \mathbb{C}, |t| \leq 1\}$ contenu dans Ω, l'application $t \mapsto u(z + tw)$ est sous-harmonique dans le disque unité de $\mathbb{C}$.

Quand Ω est connexe et que u n'est pas la constante $-\infty$, pour tout $(a_1, \dots, a_n) \in \mathbb{C}^n$ la distribution

$$\sum_{p=1}^{n} \sum_{q=1}^{n} \frac{\partial^2 u}{\partial z_p \partial \bar z_q} a_p \bar a_q$$

est positive (c'est un calcul facile quand u est de classe C^2, et on se ramène à ce cas par régularisation). Comme

$$\Delta = 4 \sum_{p=1}^{n} \sum_{q=1}^{n} \frac{\partial^2}{\partial z_p \partial \bar z_q} ,$$

on en déduit qu'une fonction plurisousharmonique dans Ω est aussi sous-harmonique dans Ω. De plus quand $\Omega \supset B(0,R)$ la fonction $t \mapsto \nu(t)$ (définie plus haut) est alors croissante (au sens large). Quand u est de classe C^2 on le voit en véri-

fiant la formule

$$\nu(t) = \int_{0<|z|<t} \left(\frac{i}{\pi}\partial\bar\partial u\right) \wedge \left(\frac{i}{2\pi}\partial\bar\partial \log|z|^2\right)^{n-1}$$

avec

$$\partial\bar\partial u = \sum_{p=1}^{n} \sum_{q=1}^{n} \frac{\partial^2 u}{\partial z_p \partial \bar z_q} dz_p \wedge d\bar z_q$$

Le cas général s'obtient à nouveau en régularisant.

Comme ν est une fonction croissante, si la fonction plurisousharmonique u n'est pas identique à $-\infty$ dans $B(0,R)$, la limite $\lim_{t\to 0} \nu(t)$ existe et est finie ; c'est la densité de ν en 0. Si $u > -\infty$ au voisinage de 0, cette densité est nulle.

La croissance de la fonction ν permet d'exploiter les formules (7.4.8) et (7.4.9) :

$$u(0) \leq \sup_{S(0,R)} u - \nu(r) \log\frac{R}{r} \tag{7.4.10}$$

et

$$\sup_{S(0,r)} u \leq \sup_{S(0,R)} u - \nu(r) \log\frac{R}{4nr} . \tag{7.4.11}$$

d) Application aux fonctions analytiques.

Soit Ω un ouvert de $\mathbb{C}^n$. Si f est analytique dans Ω, alors la fonction $\log|f|$ est plurisousharmonique dans Ω. Si $\Omega \supset \bar B(0,R)$, pour $0 < t \leq R$ l'aire des zéros de f dans $B(0,t)$ est la masse de $B(0,t)$ pour la mesure $\frac{1}{2\pi} \Delta \log|f|$; on note cette masse $\frac{\theta_{2n}}{2\pi} \mu_f(0,t)$, et on note $\nu_f(0,t) = \frac{2n-2}{t^{2n-2}} \mu_f(0,t)$ la masse moyenne des zéros de f dans $B(0,t)$.

De (7.4.11) on déduit l'énoncé suivant (cf. [Le 2] Prop. 7.4.2, [B-L] p. 5, [Bom] Prop. 4, [St] § 1, [Wa 3] I § 4) ;

THÉORÈME 7.4.12 - Soit f une fonction analytique dans un voisinage d'une boule $\bar B(0,R)$, non identique à zéro dans cette boule. Pour $0 < r \leq R$, on a

$$\log|f|_r \leq \log|f|_R - \nu_f(0,r) \log\frac{R}{4nr} .$$

On montre que $\nu_f(0,r)$ est la mesure projective de l'ensemble des zéros de f dans $B(0,r)$, c'est-à-dire la moyenne pour z dans $\mathbf{P}_n(\mathbb{C})$ du nombre de zéros de la fonction d'une variable $t \mapsto f(t\frac{z}{|z|})$. On en déduit que la densité de ν_f au point 0, c'est-à-dire le nombre (nombre de Lelong de f au point 0).

$$\nu_f(0) = \lim_{r\to 0} \nu_f(0,r) ,$$

est égal à l'ordre du zéro $z = 0$ de f. On définit plus généralement $\nu_f(w)$, pour $w \in B(0,R)$, comme étant le nombre de Lelong de $f(z+w)$ au point $z = 0$ (pour ces résultats voir [Le 1] et [Le 2] Chap. 7)

Démonstration de la proposition 7.4.1.

Notons $r_1 = 3r$, $R_1 = R - r$; on peut supposer $R_1 \geqq r_1$. Soit $w \in S(0,r)$ tel que $|f(w)| = |f|_r$. On applique (7.4.10) à la fonction $g(z) = f(z+w)$:

$$\log|f|_r \leq \log|g|_{R_1} - \nu_g(0,r_1) \log\frac{R_1}{r_1} .$$

Comme $B(w,R_1) \subset B(0,R)$, on a $|g|_{R_1} \leq |f|_R$. D'autre part les boules $B(z_j+w,\delta)$ sont contenues dans $B(0,r_1)$, donc

$$\mu_g(0,r_1) \geqq \sum_{z_j} \mu_g(z_j,\delta) ,$$

où la somme est étendue aux éléments distincts de $\{z_1, \dots, z_n\}$. On obtient

$$r_1^{2n-2}\nu_g(0,r_1) \geqq \delta^{2n-2} \sum_{z_j} \nu_j(z_j,\delta) .$$

La croissance de $\nu_g(z_j,\cdot)$ donne $\nu_g(z_j,\delta) \geqq \nu_g(z_j)$, et par hypothèse

$$\sum_{z_j} \nu_g(z_j) \geqq m .$$

D'où

$$\nu_g(0,r_1) \geqq \left(\frac{\delta}{r_1}\right)^{2n-2} m ,$$

ce qui démontre la proposition 7.4.1.

REMARQUE - On peut simplifier la démonstration du théorème 7.4.12, et même y remplacer $\log\frac{R}{4nr}$ par $\log\frac{R}{(4n-1)r}$. Au lieu d'utiliser (7.4.11) qui nécessitait les majorations fines (7.4.9) pour $w \neq 0$, on applique directement (7.4.8) à $u = \log|g|$ en conservant les notations de la démonstration de la proposition 7.4.1:

$$\log|f|_r \leqq \log|g|_{R_1} - \int_{2r}^{R_1} \nu_g(0,t)\,\frac{dt}{t} .$$

Mais $\mu_g(0,t) \geqq \mu_f(0,t-r)$ pour $t > r$. Il ne reste plus qu'à remarquer, comme

l'a fait M.C. Wairy, que pour $x > 1$

$$\int_1^x \left(\frac{t}{t+1}\right)^{2n-1} \frac{dt}{t} = \log\frac{x+1}{2} + \sum_{k=1}^{2n-2} \frac{1}{k}\left(2^{-k} - \left(\frac{x}{x+1}\right)^k\right)$$

$$\geqq \log\frac{x+1}{4n-2} .$$

On minore enfin $\frac{R-r}{(4n-2)r}$ par $\frac{R}{(4n-1)r}$ quand $R \geqq (4n-1)r$.

On notera cependant que (7.4.9) permet de remplacer $\log\frac{R}{4nr}$ par $\log\frac{R^2+r^2}{(4n-2)rR}$ dans le théorème 7.4.12.

On aurait pu démontrer le théorème 7.4.2 en utilisant la méthode du § 7.3. On remplace alors le théorème 7.3.5 de Moreau par le théorème A de [M 7] dont la démonstration dépend aussi de la masse moyenne des zéros. Cette deuxième méthode est alors plus compliquée, mais a l'avantage de conduire à un lemme d'approximation analogue au théorème 7.3.4.

THÉORÈME 7.4.13 - Soit S un sous-ensemble fini d'un polydisque $D(0, r_1)$. On définit des nombres réels δ, L, θ par

$$\delta = \min\{\|\sigma - \sigma'\| \ ; \ \sigma \in S, \sigma' \in S, \sigma \neq \sigma'\}$$

$$L = 2^{-7n}.(\delta/r_1)^{2n-2}.\ \mathrm{Card}\ S$$

$$\theta^2 = n^{-n}.(\delta/r_1)^{2n}\ .\ \mathrm{Card}\ S$$

Si f est une fonction entière dans $\mathbb{C}^n$, pour $R \geqq r \geqq r_1$ on a

$$\|f\|_r \leqq \left[c_1 \frac{r}{R}(1+\theta^{-n})\right]^L \|f\|_R + \left(c_2 \frac{r}{\theta^n r_1}\right)^L \max_{\sigma\in S}|f(\sigma)|$$

où c_1 et c_2 ne dépendent que de n.

Notons enfin que le théorème B de [M 7] permet d'améliorer cet énoncé quand S est une partie d'un réseau de type C.M.

§ 7.5. Singularités d'hypersurfaces algébriques.

Soit S un sous-ensemble fini de $\mathbb{C}^n$. Nous avons vu en (7.1.7) que si S vérifie un lemme de Schwarz (7.1.2), alors $\theta_t \leq \omega_t(S)$.

Nous allons montrer que la suite $\frac{1}{t}\omega_t(S)$ a une limite $\Omega(S)$ quand $t \to \infty$, que l'on a

$$\frac{1}{n}\omega_1(S) \leqq \Omega(S) \leqq \frac{1}{t}\omega_t(S) \leqq \omega_1(S) \quad \text{pour tout} \quad t \geqq 1 ,$$

et que, pour tout $\epsilon > 0$, S vérifie un lemme de Schwarz (7.1.2) avec

$$\theta_t = t(\Omega(S) - \epsilon) .$$

On en déduira en particulier le lemme 5.4.1 que l'on avait utilisé pour démontrer le théorème 5.1.1 de Bombieri.

a) Le théorème d'existence de Hörmander, Bombieri et Skoda.

La théorie des estimations L^2 et les théorèmes d'existence pour l'opérateur $\bar\partial$, dus à Hörmander, conduisent au théorème suivant

THÉORÈME 7.5.1 - Soit V une fonction plurisousharmonique dans $\mathbb{C}^n$, non identique à $-\infty$, et soit $\epsilon > 0$. Il existe une fonction F entière dans $\mathbb{C}^n$ et non identique à 0 , telle que

$$\int_{\mathbb{C}^n} |F(z)|^2 e^{-V(z)}(1+|z|^2)^{-n-\epsilon} d\lambda(z) < +\infty .$$

Bombieri [Bom] § IV a démontré ce théorème avec $-n-\epsilon$ remplacé par $-3n$; le raffinement est dû à Skoda [Sk] . L'exemple où V est constante montre qu'on ne peut pas remplacer ϵ par 0 .

b) Sur les degrés d'hypersurfaces algébriques ayant des singularités données.

Comme première application du théorème d'existence 7.5.1, nous démontrons le résultat suivant.

LEMME 7.5.2 - Soient S un sous-ensemble de $\mathbb{C}^n$, et t_1 , t_2 deux entiers positifs. Alors

$$\omega_{t_1}(S) \leqq \frac{t_1+n-1}{t_2}\omega_{t_2}(S) .$$

Démonstration du lemme 7.5.2.

Soit P un polynôme de degré $\omega_{t_2}(S)$ ayant en chaque point de S un zéro d'ordre $\geqq t_2$. Soit $\mu > \frac{2t_1+2n-2}{t_2}$. La fonction $V = \mu \log|P|$ est plurisousharmonique dans $\mathbb{C}^n$. Soit $\epsilon > 0$. D'après le théorème d'existence 7.5.1, il existe une fonction entière F , non identiquement nulle, telle que

$$\int_{\mathbb{C}^n} |F(z)|^2 |P(z)|^{-\mu} (1+|z|^2)^{-n-\epsilon} d\lambda(z) < +\infty .$$

Pour $\zeta \in \mathbb{C}^n$ et $r > 0$, comme $|F|^2$ est sous-harmonique, on a

$$|F(\zeta)|^2 \leqq \frac{1}{v_{2n}r^{2n}} \int_{B(\zeta,r)} |F(z)|^2 d\lambda(z) .$$

On en déduit l'existence d'une constante $c_1 > 0$, indépendante de ζ et r , telle que

$$|F(\zeta)|^2 \leqq c_1 \frac{1}{r^{2n}} \sup_{z\in B(\zeta,r)} \left(|P(z)|^{\mu}(1+|z|^2)^{n+\epsilon} \right) .$$

Choisissons d'abord $r = |\zeta-\sigma|$, où $\sigma \in S$. Pour ζ voisin de σ on obtient

$$|F(\zeta)|^2 \leqq c_2 |\zeta-\sigma|^{\mu t_2 - 2n} ,$$

ce qui montre que F a un zéro en chaque point de S d'ordre $\geqq \frac{\mu}{2}t_2 - n > t_1 - 1$.

Choisissons maintenant $|\zeta| = R$, $r = R/2$. Un calcul analogue donne

$$|F|_R^2 \leqq c_3 R^{\mu\omega_{t_2}(S) + 2\epsilon} ,$$

où c_3 ne dépend pas de R . Donc F est un polynôme de degré $\leqq \frac{1}{2}\mu\omega_{t_2}(S) + \epsilon$. Comme ce degré est un nombre entier, en choisissant les deux nombres ϵ et $\mu - \frac{2}{t_2}(t_1+n-1)$ suffisamment petits, ce degré est inférieur ou égal à la partie entière de $\frac{t_1+n-1}{t_2}\omega_{t_2}(S)$.

On déduit du lemme 7.5.2 que pour tout $t \geqq 1$,

$$\frac{1}{n}\omega_1(S) \leqq \frac{1}{t}\omega_t(S) .$$

Plus précisément, en faisant tendre séparément t_1 ou t_2 vers l'infini dans l'inégalité

$$\frac{1}{t_1+n-1}\omega_{t_1}(S) \leqq \frac{1}{t_2}\omega_{t_2}(S) ,$$

on obtient l'énoncé suivant (cf. [Wa 3] II Prop. 5.9) .

THÉORÈME 7.5.3 - Soit S un sous-ensemble fini de $\mathbb{C}^n$. La suite $(\frac{1}{t}\omega_t(S))_{t\geq 1}$ a une limite $\Omega(S)$ quand $t\to\infty$, et

$$\frac{1}{n}\omega_1(S)\leq\Omega(S)\leq\omega_1(S)\ .$$

De plus, pour tout entier $t\geq 1$, on a

$$\frac{1}{t+n-1}\,\omega_t(S)\leq\Omega(S)\leq\frac{1}{t}\omega_t(S)\leq\omega_1(S)\ .$$

Cette étude de la suite $(\frac{1}{t}\omega_t(S))_{t\geq 1}$ a été poursuivie récemment par G.V. Chudnovsky [C 2] qui appelle $\Omega(S)$ le degré singulier de S. Il remarque que si $S\subset\mathbb{C}^n$ contient exactement $n+1$ éléments qui ne sont pas tous sur un même hyperplan, alors $\omega_1(S)=2$, et

$$\Omega(S)=1+\frac{1}{n}=\frac{\omega_1(S)}{n}+\frac{n-1}{n}\ .$$

Il conjecture que dans tous les cas

$$\Omega(S)\geq\frac{1}{n}\,\omega_1(S)+\frac{n-1}{n}\ ,$$

résultat qu'il sait démontrer quand $n=2$ en utilisant la théorie des intersections. Il a aussi étudié l'ensemble des valeurs de $\Omega(S)$ quand S est un ensemble fini de $\mathbb{C}^2$, et montré que ces valeurs forment un ensemble fini si $\operatorname{Card} S\leq 9$. Il conjecture qu'il y a un nombre infini de valeurs possibles pour $\Omega(S)$ quand S décrit les sous-ensembles de $\mathbb{C}^2$ ayant 10 éléments. Enfin il a établi un lien entre cette étude et les travaux de Nagata sur le 14ème problème de Hilbert.

c) Un lemme de Schwarz pour les ensembles finis.

Le lemme de Schwarz suivant est utile quand on considère un ensemble fini fixe

THÉORÈME 7.5.4 - Soient S un sous-ensemble fini de $\mathbb{C}^n$, et ε un nombre réel, $\varepsilon>0$.

Il existe un nombre réel positif $r_0=r_0(S,\varepsilon)$ tel que pour tout entier $t>0$ et pour toute fonction entière f dans $\mathbb{C}^n$, ayant en chaque point de S un zéro d'ordre $\geqslant t$, on ait

$$\nu_f(0,r)\geq t(\Omega(S)-\varepsilon)\qquad\text{pour}\quad r\geq r_0\ .$$

Comme $\Omega(S)\geq\frac{1}{n}\omega_1(S)$, on obtient le lemme 5.4.1 (que nous avons utilisé pour la démonstration du théorème de Bombieri) en combinant ce résultat avec le théorème 7.4.12.

La démonstration que nous allons donner du théorème 7.5.4 ne permet pas de calculer r_0. Il serait très intéressant de savoir le faire, mais c'est un problème apparemment difficile.

La dépendance en ε est nécessaire : pour $S=\{(1,0)\ ;\ (1,1)\}\subset\mathbb{C}^2$, on a

$$r_0(S,\varepsilon)\to+\infty\qquad\text{quand}\quad\varepsilon\to 0$$

car pour $f(z_1,z_2)=z_1-1$ on a $\nu_f(0,r)<1$ pour tout $r>0$.

D'autre part pour $\varepsilon=1$ (par exemple) le nombre $r_0(S,1)$ ne dépend pas uniquement de $\max_{\sigma\in S}|\sigma|$. Pour le voir on choisit une fonction entière transcendante f (par exemple pour $n=2$, $f(z)=e^{z_1}-z_2-1$) telle que $S=\{z\in B(0,1)\ ,\ f(z)=0\}$ ne soit pas contenu dans une hypersurface algébrique. Il existe alors une suite $(S_j)_{j\geq 1}$ de sous-ensembles finis de S pour laquelle $\omega_1(S_j)$ tend vers l'infini. Alors $\nu_f(0,r_0(S_j,1))$ tend vers l'infini, donc $r_0(S_j,1)$ tend vers l'infini avec j.

Démonstration du théorème 7.5.4.

La démonstration repose sur les arguments et les résultats de [Bom] § VI. Nous aurons besoin de quelques propriétés des courants positifs fermés de type (1.1). Soit

$$T=\sum_{p=0}^{n}\sum_{q=0}^{n}T_{p,q}\,dz_p\wedge d\bar{z}_q$$

un tel courant (où $T_{p,q}$ sont des distributions) ; il est dit positif quand pour tout $w\in\mathbb{C}^n$ la distribution

$$\sum_{p=0}^{n}\sum_{q=0}^{n}T_{p,q}\,w_p\bar{w}_q$$

est positive. Alors

$$\sigma=2\sum_{p=1}^{n}T_{p,p}$$

est une mesure positive appelée trace de T. On note $\sigma_T(w,r)$ la mesure pour σ de la boule $B(w,r)\subset\mathbb{C}^n$, et on définit l'indicatrice projective de T par

$$\nu_T(w,r)=\frac{(n-1)!}{\pi^{n-1}}\,\frac{\sigma_T(w,r)}{r^{2n-2}}\ .$$

La densité (ou nombre de Lelong) $\nu_T(w)$ de T en w est la limite quand r tend vers 0 de $\nu_T(w,r)$ (la fonction $r\to\nu_T(w,r)$ est croissante quand T est fermé, c'est-à-dire $\partial T=\bar{\partial}T=dT=0$).

On démontre le théorème 7.5.4 par l'absurde. On suppose donc que pour tout entier positif N, il existe une fonction f_N entière dans $\mathbb{C}^n$ et un entier $t_N > 0$ tels que f_N ait en chaque point de S un zéro d'ordre $\geq t_N$, et que

$$\nu_{f_N}(0,N) \leq t_N(\Omega(S)-\varepsilon) .$$

On considère alors la suite des courants

$$T_N = \frac{1}{\pi t_N} \partial\bar{\partial} \log |f_N| .$$

Comme $\log|f_N|$ est plurisousharmonique T_N est positif ; il est de plus fermé pour les opérateurs ∂ et $\bar{\partial}$. Pour tout $s \in S$ et $N \geq 1$ la densité de T_N en s est ≥ 1 ; enfin pour tout $r \geq 1$ et tout $N \geq r$ l'indicatrice projective $\nu_{T_N}(0,r)$ est majorée par $\Omega(S)-\varepsilon$. On en déduit, en extrayant une suite faiblement convergente, l'existence d'un courant positif T, ∂ et $\bar{\partial}$ fermé, dont l'indicatrice projective est majorée par $\Omega(S)-\varepsilon$ sur toute boule de $\mathbb{C}^n$, et dont la densité est ≥ 1 en tout point de S (cf. [Bom] lemme 6).

On utilise alors la méthode de Lelong pour résoudre l'équation $\frac{1}{\pi}\partial\bar{\partial}V = T$ (comme T est positif, V sera plurisousharmonique). Pour cela on se ramène d'abord par translation au cas où $\frac{1}{r}\nu_T(0,r)$ est sommable à l'origine et on considère pour $w \in \mathbb{C}^n$, $z \in \mathbb{C}^n$, $w \neq 0$, le noyau canonique

$$e_n(w,z) = |w|^{2-2n} - |w-z|^{2-2n}$$

On pose alors

$$V(z) = \frac{(n-2)!}{2\pi^{n-1}} \int_{\mathbb{C}^n} e_n(w,z)\, d\sigma(0,w) .$$

On vérifie facilement que $\frac{1}{2\pi}\Delta V = \sigma$, mais Lelong a montré que l'on a même $\frac{1}{\pi}\partial\bar{\partial}V = T$. (cf. [Bom] p. 284).

Cette fonction plurisousharmonique V vérifie

$$V(z) \leq (\Omega(S)-\varepsilon + \underline{o}(1)) \log|z| \qquad \text{quand } |z| \to +\infty$$

et

$$V(z) \leq (1+\underline{o}(1)) \log|z-s| \qquad \text{quand } z \to s ,\ s \in S .$$

On utilise alors le théorème d'existence 7.5.1 pour la fonction μV, avec $\mu > 2(t+n-1)$, t entier positif. On en déduit (exactement comme dans la démonstration du lemme 7.5.2)

$$\frac{\omega_t(S)}{t+n-1} \leq \Omega(S)-\varepsilon \qquad \text{pour tout } t \geq 1 .$$

En faisant tendre t vers l'infini, on obtient une contradiction avec la définition de $\Omega(S)$.

(Pour de plus amples détails sur cette méthode, nous renvoyons à [Bom], ainsi qu'à l'exposé de P. Lelong au séminaire Bourbaki, n° 384, Lecture Notes 244 (1971), 29-45).

§ 7.6 - Compléments

Nous indiquons brièvement quelques développements de l'étude précédente, avec des références complémentaires.

L'étude faite au § 7.2 de certains idéaux de fonctions entières n'a fait intervenir que des considérations élémentaires. On peut la poursuivre en utilisant des outils plus puissants qui ont été développés en liaison avec le problème de la couronne ; voir en particulier : H. Skoda, Application des techniques L^2 à la théorie des idéaux d'une algèbre de fonctions holomorphes avec poids, Annales Sci. Ecole Normale Sup., 4e sér., 5 (1972), 545-579.

Au § 7.3 l'outil essentiel était le théorème 7.3.5 dont nous n'avons pas donné la démonstration. Celle-ci reposait à l'origine sur une inégalité de Bernstein, mais récemment J.C. Moreau en a donné une démonstration beaucoup plus simple et élégante, qui est reproduite au § 9.1 du volume : Transcendence methods, Queen's papers in pure and applied mathematics (Kingston, Ontario). De plus J.C. Moreau a étendu les résultats du § 7.3 au cas de zéros multiples ce qui le conduit à une nouvelle démonstration du théorème de Baker dans le cas non homogène (cf. § 8.3 b pour le cas homogène). Enfin le théorème 7.3.1 peut-être démontré en utilisant les outils du § 7.4 (i.e. en supposant dans la proposition 7.4.1 les z_j réels, et en remplaçant l'exposant $2n-2$ par $n-1$) grâce à un travail de Bo Berndtsson : Zeros of analytic functions of several variables, Arkiv för Mat., 16 (1978) 251-262.

En utilisant les arguments du § 7.3, avec la remarque que sur l'espace des polynômes $P \in \mathbb{C}[z_1,\ldots,z_n]$ de degré $< \omega_t(S)$ (où S est un sous-ensemble fini de $\mathbb{C}^n$ et t un entier positif) on définit une norme en posant

$$|P|_{S,t} = \max\left\{ \frac{1}{\tau!} |D^\tau P(\sigma)| \ ;\ |\tau| < t,\ \sigma \in S \right\}$$

J.C. Moreau a obtenu l'énoncé suivant (Sem. d'Analyse, Lecture Notes in Math, 822 (1980), 174-190.)

THÉORÈME 7.6.1. Soient S un sous-ensemble fini de $\mathbb{C}^n$, et t un entier positif. Il existe un nombre positif $r_1(S,t) = r_1$ tel que pour tout $R > r > r_1$ et toute fonction entière non nulle ayant en chaque point de S un zéro d'ordre $\geq t$, on ait

$$\log |f|_r \leq \log |f|_R - \omega_t(S) \log \frac{R}{e^n r} .$$

En combinant ce résultat avec les théorèmes 7.4.12 et 7.5.4, Moreau en déduit

COROLLAIRE 7.6.2 - Avec les mêmes notations, pour tout $\epsilon > 0$ il existe un nombre positif $r_2(S, \epsilon) = r_2$ (indépendant de t) tel que pour $R > r > r_2$ on ait

$$\log |f|_r \leq \log |f|_R - (\omega_t(S) - t\epsilon) \log \frac{R}{2e^n r}$$

Un travail récent de Choodnovsky (The degree of hypersurfaces containing lattices in $\mathbb{C}^n$; I, Planar case) permet de démontrer l'inégalité

$$\omega_1(\Gamma_N) \geq c\, N^{\mu(\Gamma, \mathbb{C}^2)}$$

quand Γ est un sous-groupe de type fini de $\mathbb{C}^2$, en accord avec la conjecture 7.1.10. (cf. la remarque après le lemme 1.3.14).

Dans les énoncés de transcendance en plusieurs variables (cf. par exemple 5.1.1 et 5.4.6), non seulement on montre qu'un ensemble S est contenu dans une hypersurface algébrique de degré $\leq \Delta$, mais on obtient le fait plus précis que tout sous-ensemble fini S_1 de S vérifie $\Omega(S_1) \leq \Delta/n$. Dans un mémoire sur les cycles holomorphes à coefficients positifs (à paraître dans le Séminaire d'Analyse, Lecture Notes in Math.), P.Lelong utilise une représentation globale d'un ensemble analytique complexe comme ensemble des points de densité d'un courant positif fermé (théorème de Siu), ce qui conduit au résultat suivant.

THEOREME 7.6.3 - Soit S un sous-ensemble de $\mathbb{C}^n$ et soit $\Omega > 0$. On suppose que toute partie finie S_1 de S vérifie $\Omega(S_1) \leq \Omega$. Alors il existe $n+1$ polynômes $P_1, \ldots, P_{n+1}$ de $\mathbb{C}[z] = \mathbb{C}[z_1, \ldots, z_n]$ tels que

a) L'ensemble S soit contenu dans l'ensemble algébrique Σ défini par

$$\Sigma = \{ z \in \mathbb{C}^n ;\ P_1(z) = \ldots = P_{n+1}(z) = 0 \} .$$

b) Le degré de P_1 soit inférieur ou égal à $n\,\Omega$.

c) La composante pure de codimension 1 de Σ ait un degré inférieur ou égal à Ω.

Dans le cas du théorème 5.1.1 de Bombieri, on vérifie l'hypothèse de 7.6.3 avec $\Omega = (\rho_1 + \ldots + \rho_{n+1})\,[K : \mathbb{Q}]$.

CHAPITRE 8

HOMOMORPHISMES ANALYTIQUES DE $\mathbb{C}^n$ DANS $G_{\mathbb{C}}$.

Nous reprenons d'abord l'étude commencée au § 6.3 des sous-groupes Γ de $\overline{\mathbb{Q}}^n$ où un homomorphisme analytique $\varphi : \mathbb{C}^n \to G_{\mathbb{C}}$ prend des valeurs algébriques. Si on suppose que la restriction de φ à toute droite complexe passant par un point de Γ est non rationnelle, on conjecture que le rang de Γ est majoré par 2n. Nous avons établi ce résultat au § 6.3 moyennant une hypothèse sur la structure de G. Nous le démontrons maintenant en supposant Γ contenu dans la trace réelle de $\mathbb{C}^n$.

Nous étudions ensuite les sous-groupes Γ de $\mathbb{C}^n$ tels que $\varphi(\Gamma) \subset G_{\overline{\mathbb{Q}}}$. Avec des hypothèses sur le coefficient de densité de Γ dans $\mathbb{R}^{2n}$ ou dans la trace réelle $\mathbb{R}^n$ de $\mathbb{C}^n$, on peut majorer la dimension algébrique de φ.

Enfin nous démontrons des critères de transcendance qui généralisent à plusieurs variables la méthode de Schneider. Cela nous permet de démontrer, dans le cas réel, le théorème de Baker sur l'indépendance linéaire de logarithmes de nombres algébriques. En contraste avec la méthode de Baker, cette nouvelle méthode utilise plusieurs variables et ne fait pas intervenir d'équations différentielles.

§ 8.1 - Points algébriques du graphe

Nous poursuivons l'étude commencée au § 2.5 et au § 6.3 b des sous-groupes Γ de $\overline{\mathbb{Q}}^n$ où un homomorphisme analytique $\varphi : \mathbb{C}^n \to G_{\mathbb{C}}$ prend des valeurs algébriques.

THÉORÈME 8.1.1 - Soient G un groupe algébrique défini sur $\overline{\mathbb{Q}}$, Γ un sous-groupe de type fini de $\overline{\mathbb{Q}}^n \cap \mathbb{R}^n$, de rang ℓ sur $\mathbb{Z}$, et $\varphi : \mathbb{C}^n \to G_{\mathbb{C}}$ un homomorphisme analytique tel que $\varphi(\Gamma) \subset G_{\overline{\mathbb{Q}}}$. On suppose que pour tout $\gamma \in \Gamma$, $\gamma \neq 0$, l'homomorphisme $t \to \varphi(\gamma t)$ de $\mathbb{C}$ dans $G_{\mathbb{C}}$ est irrationnel. Alors $\ell \leq 2n$.

L'hypothèse que Γ est inclus dans la trace réelle $\mathbb{R}^n$ de $\mathbb{C}^n$ est évidemment indésirable (cf. la conjecture 6.2.1 et le cas algébrique de la conjecture 7.1.10). En revanche l'hypothèse sur l'irrationalité de φ dans toutes les directions de Γ est naturelle. Néanmoins, pour les mêmes raisons qu'au § 6.3.b, il est nécessaire de démontrer d'abord un énoncé dans lequel on suppose seulement l'homomorphisme φ

non rationnel, la conclusion partant alors sur la répartition de Γ.

PROPOSITION 8.1.2 - *Soient* G *un groupe algébrique défini sur* $\overline{\mathbf{Q}}$, Γ *un sous-groupe de type fini de* $\overline{\mathbf{Q}}^n$ *de rang* ℓ *sur* $\mathbf{Z}$, *et* $\varphi : \mathbf{C}^n \to G_{\mathbf{C}}$ *un homomorphisme analytique non rationnel tel que* $\varphi(\Gamma) \subset G_{\overline{\mathbf{Q}}}$. *Alors on a*

$$\mu(\Gamma, \mathbf{R}^{2n}) \leq 1 .$$

Si, de plus, Γ *est contenu dans* $\mathbf{R}^n$, *alors*

$$\mu(\Gamma, \mathbf{C}^n) \leq 2 .$$

Il suffirait en fait de démontrer le résultat dans le cas où Γ est bien réparti dans $\mathbf{R}^{2n}$ (resp. dans $\mathbf{R}^n$) grâce au lemme 1.3.2. La conclusion s'écrit alors $\ell \leq 2n$.

Démonstration du théorème 8.1.1.

Montrons que le théorème 8.1.1 est une conséquence de la proposition 8.1.2. On utilise pour cela la proposition 1.3.1 : soit Γ' un sous-$\mathbf{Z}$-module de Γ, bien réparti dans le $\mathbf{C}$-espace $\overline{\Gamma}'$ qu'il engendre, tel que $\mu(\Gamma', \overline{\Gamma}') \geq \ell/n$. La restriction de φ à $\overline{\Gamma}'$ est un homomorphisme analytique non rationnel de $\overline{\Gamma}'$ dans $G_{\mathbf{C}}$; la proposition 8.1.2 donne $\mu(\Gamma', \overline{\Gamma}') \leq 2$, donc $\ell \leq 2n$.

Début de la démonstration de la proposition 8.1.2.

La proposition 4.3.1 ramène la démonstration à celle d'un critère de transcendance, que nous verrons au § 8.3.

Notons que si G est un groupe linéaire, on sait déjà grâce à 2.5.2 que

$$\mu(\Gamma, \mathbf{C}^n) \leq 1 .$$

On peut donc n'utiliser la proposition 4.3.1 que dans le cas où G est une variété abélienne simple (cf. la démonstration du lemme 6.3.5).

§ 8.2 - Dimension algébrique

a) Utilisation du coefficient de densité. (cf. § 1.3d)

Le résultat suivant améliore ceux de Bombieri et Lang [B-L], mais il est encore loin de ce que l'on peut espérer

THÉORÈME 8.2.1 - *Soient* G *un groupe algébrique commutatif connexe défini sur* $\overline{\mathbf{Q}}$, $\varphi : \mathbf{C}^n \to G_{\mathbf{C}}$ *un homomorphisme analytique de dimension algébrique* d, *et* Γ *un sous-groupe de* $\mathbf{C}^n$ *tel que* $\varphi(\Gamma) \subset G_{\overline{\mathbf{Q}}}$.

1) *Si* Γ *a un coefficient de densité* $\geq \varkappa_{2n}$ *dans* $\mathbf{R}^{2n}$, *alors* $\varkappa_{2n}(d-n) \leq d$.

2) *Si* $\Gamma \subset \mathbf{R}^n$ *et si* Γ *a un coefficient de densité* $\geq \varkappa_n$ *dans* $\mathbf{R}^n$, *alors*

$$\varkappa_n (d-n) \leq 2d.$$

Si G est un groupe linéaire on peut améliorer la conclusion en

$$\varkappa_{2n}(d-n) \leq d/2$$

et

$$\varkappa_n (d-n) \leq d.$$

Rappelons que l'on a $\varkappa_{2n} \leq \mu(\Gamma, \mathbf{R}^{2n}) \leq \frac{\ell}{2n}$ et $\varkappa_n \leq \mu(\Gamma, \mathbf{R}^n) \leq \frac{\ell}{n}$ (cf. § 1.3d)

On peut raffiner le théorème 8.2.1 de manière analogue à ce qui a été fait au § 4.2. On peut aussi y remplacer le corps des nombres algébriques par une extension de $\mathbf{Q}$ de type de transcendance $\leq \tau$.

D'autre part d'après le principe de transfert (1.3.11) on peut remplacer l'hypothèse sur le coefficient de densité de Γ par une minoration des éléments non nuls de Γ_N (cf. [Wa 3] I Th. 6.1).

Voici un corollaire du théorème 8.2.1 correspondant au cas $d = n+1$.

COROLLAIRE 8.2.2 - *Soient* G *un groupe algébrique commutatif connexe défini sur* $\overline{\mathbf{Q}}$, $\varphi : \mathbf{C}^n \to G_{\mathbf{C}}$ *un sous-groupe à* n *paramètres, et* Γ *un sous-groupe de* $\mathbf{C}^n$ *(resp. de* $\mathbf{R}^n$*) tel que* $\varphi(\Gamma) \subset G_{\overline{\mathbf{Q}}}$. *On suppose que* Γ *a un coefficient de densité* $\geq \varkappa_{2n}$ *(resp.* $\geq \varkappa_n$*) dans* $\mathbf{R}^{2n}$ *(resp. dans* $\mathbf{R}^n$*), avec* $\varkappa_{2n} > n+1$ *(resp.* $\varkappa_n > 2(n+1)$*). Alors* $\varphi(\mathbf{C}^n)$ *est un sous-groupe algébrique fermé de* $G_{\mathbf{C}}$ *de dimension* n.

b) Sur une suggestion de Bombieri et Lang

L'hypothèse sur le coefficient de densité de Γ est analogue à la condition de λ-distribution de [B-L] (avec $\lambda = \varkappa_{2n} - 1$). Cette notion n'est pas invariante par une transformation analytique. Bombieri et Lang ont suggéré [B-L] (p. 13) que leur condition de λ-distribution pourrait être remplacée par la condition que Γ est une somme directe $\Gamma = \Gamma_1 \oplus \ldots \oplus \Gamma_m$, où chaque Γ_i a pour rang n sur $\mathbf{C}$. Dans une situation telle que celle du corollaire 8.2.2, on demanderait seulement à m d'être grand par rapport à n.

Cette nouvelle hypothèse n'est pas suffisante. Pour le voir, on considère des nombres complexes $x_1, \ldots, x_{2m}$, $\mathbf{Q}$-linéairement indépendants, et, pour $1 \leq j \leq m$, on note Γ_j le sous-groupe de $\mathbf{C}^2$ engendré par $(1, x_j)$ et $(1, x_{m+j})$. Alors le sous-groupe Γ de $\mathbf{C}^2$ engendré par $(1, x_1), \ldots, (1, x_{2m})$ vérifie la condition requise $\Gamma = \Gamma_1 \oplus \ldots \oplus \Gamma_m$, où chaque Γ_j est de rang 2 sur $\mathbf{C}$.

Choisissons d'abord $x_1, \ldots, x_{2m}$ algébriques, et considérons le sous groupe à 2 paramètres de $GL_3(\mathbb{C})$ (cf. 2.1.2).

$$\varphi(z_1, z_2) = \begin{pmatrix} 2^{z_1} & 0 & z_2 2^{z_1} \\ 0 & 3^{z_1} & 0 \\ 0 & 0 & 2^{z_1} \end{pmatrix} = \exp(M_1 z_1 + M_2 z_2)$$

où

$$M_1 = \begin{pmatrix} \log 2 & 0 & 0 \\ 0 & \log 3 & 0 \\ 0 & 0 & \log 2 \end{pmatrix} \quad \text{et} \quad M_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Alors $\varphi(\Gamma) \subset GL_3(\overline{\mathbb{Q}})$ car $\Gamma \subset \mathbb{Z} \times \overline{\mathbb{Q}}$, et cependant φ a pour dimension algébrique 3.

Considérons maintenant une courbe elliptique $\mathcal{E}$ définie sur $\overline{\mathbb{Q}}$, paramétrée par $P = (1, \wp, \wp')$, dont le corps des endomorphismes est k. Choisissons pour $x_1, \ldots, x_{2m}$ des points algébriques de $\wp$, avec x_1, x_2 k-linéairement indépendants, et soit φ le sous-groupe à 2 paramètres de $\mathcal{E} \times \mathcal{E} \times \mathcal{E}$ défini par

$$\varphi(z_1, z_2) = (P(x_1 z_1), P(x_2 z_1), P(z_2)).$$

Alors $\varphi(\Gamma)$ est contenu dans le groupe points algébriques de $\mathcal{E} \times \mathcal{E} \times \mathcal{E}$, et φ a pour dimension algébrique 3.

La possibilité de construire ces contre-exemples provient du fait que $\mu(\Gamma, \mathbb{C}^n) = 1$. Pour obtenir la conclusion du corollaire 8.2.2, il est nécessaire de supposer $\mu(\Gamma, \mathbb{C}^n)$ grand. Nous ne chercherons pas le meilleur énoncé possible, mais seulement celui que laisse espérer la conjecture 7.1.10, compte tenu des méthodes actuelles de la théorie des nombres transcendants.

c) Une autre suggestion. Lien avec un problème de Weil et Serre.

PROBLÈME 8.2.3 - Soient G un groupe algébrique défini sur $\overline{\mathbb{Q}}$, $\varphi : \mathbb{C}^n \to G_{\mathbb{C}}$ un homomorphisme analytique de dimension algébrique $d > n$, et Γ un sous-groupe de $\mathbb{C}^n$ tel que $\varphi(\Gamma) \subset G_{\overline{\mathbb{Q}}}$. Montrer que l'on a

$$\mu(\Gamma, \mathbb{C}^n) \leq \frac{2d}{d-n}.$$

De plus, si G est un groupe linéaire, alors

$$\mu(\Gamma, \mathbb{C}^n) \leq \frac{d}{d-n}$$

Dans le cas où Γ est bien réparti dans $\mathbb{C}^n$; la conclusion devient, en notant ℓ le rang de Γ sur $\mathbb{Z}$.

$$\ell(d-n) \leq 2\,dn$$

dans le cas général, et

$$\ell(d-n) \leq dn$$

dans le cas linéaire. L'hypothèse de bonne répartition ne fait intervenir que de l'algèbre linéaire, alors que le théorème 8.2.1, ne permet d'arriver à ces inégalités que moyennant des hypothèses métriques.

Dans le cas linéaire, on est amené à étudier la situation suivante (cf. § 2.5.b). Soient $\Gamma = \mathbb{Z}\gamma_1 + \ldots + \mathbb{Z}\gamma_\ell$ et $\Lambda = \mathbb{Z}\lambda_1 + \ldots + \mathbb{Z}\lambda_d$ deux sous-groupes de $\mathbb{C}^n$ de rang ℓ et d respectivement. On suppose que les nombres $\exp\langle \gamma, \lambda \rangle$, $(\gamma \in \Gamma, \lambda \in \Lambda)$ sont algébriques. La conjecture 7.1.10 entraîne alors facilement (cf. théorème 8.3.1 ci-dessous) l'inégalité $\mu(\Gamma) \leq \frac{\ell}{d} + 1$. (On écrit $\mu(\Gamma)$ pour $\mu(\Gamma, \mathbb{C}^n)$). On remarque alors que si W est un sous-espace de $\mathbb{C}^n$, les fonctions $\exp\langle \gamma, z \rangle$, $(\gamma \in \Gamma)$, restreintes à W, engendrent un corps de degré de transcendance $\geq \mu(\Gamma) \dim_{\mathbb{C}} W$. Le lemme 1.3.1 permet alors d'en déduire

$$\mu(\Gamma)\,\mu(\Lambda) \leq \mu(\Gamma) + \mu(\Lambda),$$

ce qui est une généralisation agréable de la conclusion du cas $n = 1$: $\ell d \leq \ell + d$ (théorème des six exponentielles 1.1.7). En utilisant à nouveau le lemme 1.3.1, on obtient $\mu(\Gamma) \leq d/(d-n)$, qui est l'inégalité demandée dans 8.2.3. Ceci montre que la conjecture 7.1.10 dans le cas $\ell = n + 1$ permettrait de résoudre le problème suivant.

(8.2.4) Soient $x_1, \ldots, x_n$ des nombres complexes, et $\alpha_{j,s}$ $(1 \leq j \leq d,\ 1 \leq s \leq n)$ des nombres algébriques non nuls. Pour $1 \leq j \leq d,\ 1 \leq s \leq n$, soit $\log \alpha_{j,s}$ une détermination quelconque du logarithme de $\alpha_{j,s}$. On suppose que les d points

$$(\log \alpha_{j,1}, \ldots, \log \alpha_{j,n}) \in \mathbb{C}^n, \qquad (1 \leq j \leq d)$$

sont $\mathbb{Q}$-linéairement indépendants dans $\mathbb{C}^n$, et que les d nombres

$$\prod_{s=1}^{n} \alpha_{j,s}^{x_s}, \qquad (1 \leq j \leq d)$$

sont algébriques. Montrer que si $d \geq n^2 + n + 1$, alors $1, x_1, \ldots, x_n$ sont $\mathbb{Q}$-linéairement dépendants

En voici une conséquence

(8.2.5) Soient k un corps de nombres de degré d sur $\mathbb{Q}$, σ les plongements de k dans $\mathbb{C}$, (x_σ) un élement de $\mathbb{C}^d$, et f un idéal entier de k. On note $k^*(f)$ le sous-groupe de k^* formé des quotients d'entiers congrus à 1 modulo f. On suppose que pour tout $\alpha \in k^*(f)$ le nombre

$$\prod_\sigma |\sigma\alpha|^{x_\sigma}$$

est algébrique. Alors $\alpha_\sigma \in \mathbb{Q}$ si σ est un plongement réel, et $x_\sigma + x_{\bar\sigma} \in \mathbb{Q}$ si σ et $\bar\sigma$ sont des plongements complexes conjugués. Si de plus il existe un corps de nombres K contenant tous les nombres $\prod_\sigma |\sigma\alpha|^{x_\sigma}$, alors $x_\sigma \in \mathbb{Z}$ si σ est réel et $x_\sigma + x_{\bar\sigma} \in 2\,\mathbb{Z}$ si σ et $\bar\sigma$ sont conjugués.

Ce problème 8.2.5. apparaît dans un article de Weil [We 3] et, dans le cas p-adique, dans le livre de Serre [Se 4] (Chap. III § 3). Il permettrait de montrer que si χ est un caractère du groupe des classes d'idèles de k pour lequel les coefficients de la série L de Hecke associée à χ sont algébriques (resp. dans un corps de nombres), alors χ est de type (A) (resp. de type (A_0)) au sens de [We 3].

Nous avons dit que le problème 8.2.5 est une conséquence de la conjecture 7.1.10 dans le cas $\ell = n+1$ (il suffit en fait d'obtenir un lemme de Schwarz avec un exposant strictement plus grand que 1 quand $\mu(\Gamma) = 1+\frac{1}{n}$; on notera que le nombre de variables qui interviennent est le rang du groupe des unités de k). Il est aussi facile de déduire 8.2.5 de la conjecture de Schanuel 1.1.10.

En utilisant une version quantitative du théorème de Kronecker [Ca] chap. V th. XVII, conjointement avec le lemme de Schwarz 7.3.4, on peut obtenir quelques résultats (cf. [Wa 3] III) dont voici un exemple .

THÉORÈME 8.2.6 – Avec les hypothèses 8.2.4, si $x_1,\ldots,x_n$ sont réels, pour tout $C > 0$ vérifiant $C < \frac{d}{n} - 1$, il existe un entier H_0 tel que tout $H > H_0$ l'inégalité

$$|h_0 + h_1 x_1 + \ldots + h_n x_n| < H^{-C}$$

ait une solution $(h_0,\ldots,h_n) \in \mathbb{Z}^{n+1}$ avec

$$0 < \max_{0 \le i \le n} |h_i| \le H .$$

En particulier pour $n = 2$ en utilisant une minoration de Feldman sur les formes linéaires de logarithmes (cf. [Wa 2] th. 8.4.1) on peut résoudre le problème 8.2.4 en supposant $(x_1, x_2) \in \mathbb{R}^2$ et d infini.

COROLLAIRE 8.2.7 – Soient x_1 et x_2 deux nombres réels. On suppose qu'il existe une infinité de couples (p_1, p_2) de nombres premiers, $p_1 \neq p_2$, tels que $p_1^{x_1} p_2^{x_2}$ soit algébrique. Alors l'un des nombres x_1, x_2 est rationnel.

§ 8.3 – Critères de transcendance.

La première démonstration de transcendance utilisant des fonctions de plusieurs variables sans équations différentielles (méthode de Schneider) a été donnée par Serre en 1966 [Se 3] dans le cas p-adique (voir à ce sujet l'Appendice 1). Un analogue complexe a été obtenu par Bombieri et Lang [B-L] quatre ans plus tard ; ils donnent un énoncé local, pour des fonctions analytiques dans une boule de $\mathbb{C}^n$. Un critère valable pour des fonctions méromorphes dans $\mathbb{C}^n$ se trouve dans [Wa 3] I. Tous ces énoncés imposent des conditions très restrictives sur les points que l'on considère.

Nous donnons ici des variantes de ces critères, et nous en déduirons un énoncé dans lequel n'intervient aucune condition sur la répartition des points ; à la place figure une hypothèse naturelle sur la transcendance de la fonction considérée.

Nous étudions d'abord les fonctions entières, car l'absence de pôles simplifie beaucoup la situation ; nous appliquons ensuite ces résultats à la transcendance de $\alpha_1^{\beta_1} \ldots \alpha_n^{\beta_n}$ quand $\beta_1,\ldots,\beta_n$ sont réels. Enfin nous donnons les critères pour les fonctions méromorphes.

a) Enoncés des critères pour les fonctions entières.

Le critère suivant généralise à n variables le théorème 1.1.5 dans le cas de fonctions entières.

THÉORÈME 8.3.1 – Soient $f_1,\ldots, f_d$ des fonctions entières dans $\mathbb{C}^n$ algébriquement indépendantes sur $\mathbb{Q}$, et Γ un sous-groupe de type fini de $\mathbb{C}^n$ de rang ℓ sur $\mathbb{Z}$. On suppose que l'application $(f_1,\ldots, f_d)$ est d'ordre arithmétique $\le (\rho_1,\ldots,\rho_d)$ sur Γ.

1) Si Γ vérifie un lemme de Schwarz avec l'exposant m, alors

$$md \le \ell + \rho_1 + \ldots + \rho_d .$$

2) Si Γ a un coefficient de densité $\ge \varkappa_{2n}$ dans $\mathbb{R}^{2n}$, alors

$$2\,\varkappa_{2n}(d-n) \le \rho_1 + \ldots + \rho_d .$$

3) Si $\Gamma \subset \mathbb{R}^n$ et si Γ a un coefficient de densité $\ge \varkappa_n$ dans $\mathbb{R}^n$, alors

$$\varkappa_n (d-n) \le \rho_1 + \ldots + \rho_d .$$

Dans tous les cas, la meilleure majoration de ℓ que l'on puisse en déduire est

$$\ell\,(d-n) \le n\,(\rho_1 + \ldots + \rho_d),$$

et la conjecture 7.1.10 permettrait d'obtenir cette inégalité sous la seule hypothèse que Γ est bien réparti dans $\mathbb{C}^n$.

Si Γ est un sous-groupe de $\overline{\mathbb{Q}}^n \cap \mathbb{R}^n$ et si $f_j(z) = z_j$, $(1 \leq j \leq n)$ avec $d > n$, le théorème 1.3.10 et la partie 3 du théorème 8.3.1 donnent

$$(8.3.2) \qquad \mu(\Gamma, \mathbb{C}^n) \leq \frac{\rho_{n+1} + \dots + \rho_d}{d-n}.$$

Nous allons en déduire le corollaire suivant.

COROLLAIRE 8.3.3 - Soient f une fonction entière dans $\mathbb{C}^n$, et Γ un sous-groupe de $\overline{\mathbb{Q}}^n \cap \mathbb{R}^n$ de type fini et de rang ℓ sur $\mathbb{Z}$. On suppose que pour tout $\gamma \in \Gamma, \gamma \neq 0$, la fonction entière d'une variable complexe $t \to f(\gamma t)$ n'est pas rationnelle. Si f est d'ordre arithmétique $\leq \rho$ sur Γ, alors $\ell \leq n\rho$.

Démonstration du corollaire 8.3.3.

La méthode est celle qui nous a permis de déduire le théorème 8.1.1 de 8.1.2. On utilise d'abord la proposition 1.3.1 : il existe un sous-groupe Γ' de Γ, bien réparti dans le $\mathbb{C}$-espace vectoriel $\overline{\Gamma}'$ qu'il engendre, tel que $\mu(\Gamma', \overline{\Gamma}') \geq \ell/n$. La restriction de f à $\overline{\Gamma}'$ est une fonction entière non rationnelle qui avec Γ' vérifie les hypothèses du théorème 8.3.1. On obtient ainsi, grâce à (8.3.2) :

$$\mu(\Gamma', \overline{\Gamma}') \leq \rho,$$

d'où le corollaire.

b) Le théorème de Baker par les fonctions de plusieurs variables.

En utilisant d'une part l'inégalité (8.3.2) avec $d = \ell = n+1$, $\mu(\Gamma, \mathbb{C}^n) = 1 + \frac{1}{n}$, et d'autre part le corollaire 8.3.3 dans le cas $\ell = n+1$, on obtient l'énoncé suivant.

COROLLAIRE 8.3.4 - Soient f une fonction entière dans $\mathbb{C}^n$, et $\beta_1, \dots, \beta_n$ des nombres algébriques réels. On suppose que les nombres

$$f(h_1 + h_0\beta_1, \dots, h_n + h_0\beta_n), \quad (h_0, h_1, \dots, h_n) \in \mathbb{Z}^{n+1}$$

sont algébriques, et plus précisément que f est d'ordre arithmétique $\leq \rho$ sur $\Gamma = \mathbb{Z}^n + \mathbb{Z}(\beta_1, \dots, \beta_n)$, avec $\rho < 1 + \frac{1}{n}$.

a) Si f n'est pas rationnelle, alors $1, \beta_1, \dots, \beta_n$ sont $\mathbb{Q}$-linéairement dépendants.

b) Si, pour tout $\gamma \in \Gamma, \gamma \neq 0$, la fonction $t \to f(\gamma t)$ n'est pas rationnelle, alors $\beta_1, \dots, \beta_n$ sont tous rationnels.

En choisissant

$$f(z_1, \dots, z_n) = \alpha_1^{z_1} \dots \alpha_n^{z_n},$$

On en déduit un cas particulier du théorème 1.1.9 de Baker sous les deux formes équivalentes suivantes.

1) Soient $\beta_1, \dots, \beta_n$ des nombres algébriques réels, avec $1, \beta_1, \dots, \beta_n$ $\mathbb{Q}$-linéairement indépendants, $\alpha_1, \dots, \alpha_n$ des nombres algébriques non nuls, et, pour $1 \leq i \leq n$, $\log \alpha_i$ une détermination non nulle du logarithme de α_i. Alors le nombre

$$\alpha_1^{\beta_1} \dots \alpha_n^{\beta_n} = \exp\left(\sum_{i=1}^{n} \beta_i \log \alpha_i\right)$$

est transcendant.

2) Soient $\log \alpha_1, \dots, \log \alpha_n$ des logarithmes $\mathbb{Q}$-linéairement indépendants de nombres algébriques. Alors $\log \alpha_1, \dots, \log \alpha_n$ sont linéairement indépendants sur $\overline{\mathbb{Q}} \cap \mathbb{R}$.

Dans son état actuel, la méthode de Baker utilise des propriétés spécifiques de la fonction exponentielle (ou des fonctions elliptiques ou abéliennes) et ne permet pas d'obtenir des énoncés généraux du style de 8.3.4. Cependant les travaux récents de Nesterenko, Brownawell et Masser [Br-M] pourraient changer la situation.

c) Énoncés des critères pour les fonctions méromorphes.

La généralisation aux fonctions méromorphes de la deuxième partie du critère 8.3.1 est assez facile.

THÉORÈME 8.3.5 - Soient $f_1, \dots, f_d$ des fonctions méromorphes dans $\mathbb{C}^n$ algébriquement indépendantes sur $\mathbb{Q}$, et Γ un sous-groupe type fini de $\mathbb{C}^n$ de rang ℓ sur $\mathbb{Z}$. On suppose que l'application $(f_1, \dots, f_d)$ est d'ordre arithmétique $\leq (\rho_1, \dots, \rho_d)$ sur Γ. Si Γ a un coefficient de densité $\geq \varkappa_{2n}$ dans $\mathbb{R}^{2n}$, alors

$$2\varkappa_{2n}(d-n) \leq \rho_1 + \dots + \rho_d.$$

Nous avons vu que le théorème 8.3.1 contenait un cas particulier du théorème 1.1.9 de Baker sur l'indépendance linéaire de logarithmes de nombres algébriques. De même le théorème 8.3.5 contient un cas particulier du théorème 6.2.3 de Masser sur l'indépendance linéaire de points algébriques de fonctions thêta de variétés abéliennes simples de type C.M. Par exemple si $\wp$ est une fonction elliptique d'invariants g_2, g_3 algébriques, ayant multiplication complexe dans $k = \mathbb{Q}(\tau)$, si

$u_1, \dots, u_n$ sont des points algébriques non nuls de $\mathfrak{p}$, et si $\beta_j = b_j + b_{n+j}\tau$, $1 \leq j \leq n$ sont des nombres algébriques (avec b_j, b_{n+j} réels) tels que $\beta_1 u_1 + \dots + \beta_n u_n$ soit un point algébrique de $\mathfrak{p}$, alors $1, b_1, \dots, b_{2n}$ sont $\mathbb{Q}$-linéairement dépendants ; plus précisément il existe des entiers rationnels $a_1, \dots, a_{2n}$, non tous nuls, tels que l'on ait simultanément

$$\sum_{j=1}^{2n} a_j b_j \in \mathbb{Z}$$

et, en écrivant $\tau^2 = c\tau + d$,

$$\sum_{j=1}^{n} a_{n+j} b_j + \sum_{j=1}^{n} (c\, a_{n+j} + d\, a_j) b_{n+j} \in \mathbb{Z}$$

(ces conditions expriment que le $\mathbb{Z}[\tau]$-module Γ engendré dans $\mathbb{C}^n$ par la base canonique de $\mathbb{C}^n$ et par l'élément $(\beta_1, \dots, \beta_n)$ vérifie $\mu(\Gamma, \mathbb{R}^{2n}) = 1$; cela résulte de la proposition 8.1.2 appliquée à l'homomorphisme

$$(z_1, \dots, z_n) \mapsto P(u_1 z_1 + \dots + u_n z_n)$$

de $\mathbb{C}^n$ dans la courbe elliptique associée à $\mathfrak{p}$). En fait, le théorème 6.2.3 de Masser montre que les nombres complexes $1, \beta_1, \dots, \beta_n$ sont linéairement dépendants sur $\mathbb{Q}(\tau)$. C'est évidemment ce qu'on aurait obtenu si la conclusion du théorème 8.3.5 avait été (pour $d > n$)

$$\mu(\Gamma, \mathbb{C}^n) \leq \frac{\rho_1 + \dots + \rho_d}{d-n}$$

L'extension de la troisième partie du critère 8.3.1 aux fonctions méromorphes est plus délicate.

THÉORÈME 8.3.6 - Soient $f_1, \dots, f_d$ des fonctions méromorphes dans $\mathbb{C}^n$ algébriquement indépendantes sur $\mathbb{Q}$, et Γ un sous-groupe de type fini de $\mathbb{R}^n$ de rang ℓ sur $\mathbb{Z}$. On suppose qu'il existe un corps de nombres K, une base $(\gamma_1, \dots, \gamma_\ell)$ de Γ sur $\mathbb{Z}$, un sous-ensemble T de Γ, et un nombre positif c tels que les propriétés suivantes soient vérifiées.

a) Pour $1 \leq j \leq d$, la fonction f_j vérifie les axiomes 0.A.1 et 0.A.2. (cf. § 1.1) avec

$$S_N = \Gamma_N \cap T.$$

b) Tout cube de $\mathbb{R}^\ell$ de côté $\geq c$ contient un point $(h_1, \dots, h_\ell) \in \mathbb{Z}^\ell$ pour lequel

$$h_1\gamma_1 + \dots + h_\ell\gamma_\ell \in T.$$

Alors, si Γ a un coefficient de densité $\geq \varkappa_n$ dans $\mathbb{R}^n$, on a

$$\varkappa_n (d-n) \leq \rho_1 + \dots + \rho_d.$$

Grâce au théorème 1.3.10 et à la proposition 4.3.1, les résultats des § 8.1 et 8.2 se déduisent facilement de ces deux derniers critères.

d) Démonstration des critères

Nous allons démontrer simultanément les 3 théorèmes 8.3.1, 8.3.5 et 8.3.6. Pour cela nous définissons des nombres m, h en distinguant 3 cas :

1er cas : $h = \ell$ pour la première partie du théorème 8.3.1

2e cas : $m = 2\varkappa_{2n}$, $h = 2n\,\varkappa_{2n}$ pour la deuxième partie du théorème 8.3.1 et pour le théorème 8.3.5.

3e cas : $m = \varkappa_n$, $h = n\varkappa_n$ pour la troisième partie du théorème 8.3.1 (auquel cas on note $T = \Gamma$) et pour le théorème 8.3.6.

Ainsi la conclusion s'écrit toujours

$$md \leq h + \rho_1 + \dots + \rho_d.$$

Le choix de m est justifié par les théorèmes 7.3.1 et 7.4.2, et le choix de h par le lemme 1.3.8.

Pour chaque entier N suffisamment grand $(N \geq c_1)$, on construit un sous-ensemble E_N de Γ_N, vérifiant

$$c_2 N^h \leq \operatorname{Card} E_N \leq c_3 N^h$$

de la manière suivante

1er cas : on choisit $E_N = \Gamma_N$

2e cas : grâce au lemme 1.3.8 (dans lequel S_N est donné par l'hypothèse sur l'ordre arithmétique), il existe un sous-ensemble E_N de S_N tel que

$$\operatorname{Card} E_N \geq c_2 N^h \quad \text{et}$$

$$\min \{ |\sigma - \sigma'| \;;\; \sigma \in E_N,\ \sigma' \in E_N,\ \sigma \neq \sigma' \} \geq c_4 N^{1-\varkappa_{2n}}$$

Cette dernière condition entraîne $\operatorname{Card} E_N \leq c_3 N^h$.

3e cas : On utilise d'abord le lemme 1.1.8 : soient $t_1, \dots, t_q \in \Gamma$ tels que $\Gamma = T_1 \cup \dots \cup T_q$ où $T_j = T + t_j$ (Si $T = \Gamma$ on peut choisir $q = 1$, $t_1 = 0$).

On recouvre $B(0, c_5 N) \cap \mathbb{R}^n$ par $c_6 N^h$ boules de rayon $c_7 N^{1-\kappa n}$. Dans chacune on choisit un point γ de $\Gamma_{[N/2]}$; si j est l'indice tel que $\gamma \in T_j$, on pose $\sigma = \gamma - t_j$, et on définit E_N comme l'ensemble de ces σ.

On note $\rho = (\rho_1 + \dots + \rho_d)/d$, et on suppose $m > \rho + \frac{h}{d}$. On veut obtenir une contradiction. On remarque d'abord qu'il n'y a pas de restriction à supposer

$$\max_{1 \leq j \leq d} \rho_j < \rho + \frac{h}{d}$$

(cf. [Wa 2] p 52). Pour $1 \leq j \leq d$, on définit une fonction L_j de N (pour $N \geq c_1$) par

$$L_j = c_7 \, N^{\rho + \frac{h}{d} - \rho_j}$$

avec

$$c_7^d = 2\, c_3 \, [K : \mathbb{Q}] \, .$$

<u>Premier pas</u>. <u>Soit</u> N <u>un entier</u>, $N \geq c_1$. <u>Il existe un polynôme non nul</u>

$$P_N \in \mathbb{Z}[X_1, \dots, X_d]$$

<u>de degré en</u> X_j <u>inférieur ou égal à</u> L_j, $(1 \leq j \leq d)$, <u>et de hauteur inférieure ou égale à</u> $\exp(c_8 N^{\rho + \frac{h}{d}})$, <u>tel que la fonction</u>

$$F_N = P_N(f_1, \dots, f_d)$$

<u>vérifie</u>

$$F_N(\gamma) = 0 \quad \underline{\text{pour tout}} \quad \gamma \in E_N \, .$$

On doit pour cela résoudre un système de $\mathrm{Card}\, E_N$ équations linéaires homogènes en au moins $L_1 \dots L_d$ inconnues, à coefficients dans K. L'axiome 0.A.1 (joint à l'équivalence des différentes notions de hauteurs ; cf § 1.1) permet de majorer le logarithme des valeurs absolues des conjugués des coefficients de ce système (après les avoir multipliés par un dénominateur commun pour qu'ils soient entiers algébriques) par $c_9 \sum_{j=1}^{d} L_j N^{\rho_j}$. (Cette majoration est expliquée en détail dans [Wa 2] § 2.2). Le lemme de Siegel donne le résultat annoncé.

<u>Deuxième pas</u>. <u>Pour chaque entier</u> $M \geq N$, <u>on a</u>

$(I)_M$ $$F_N(\gamma) = 0 \quad \underline{\text{pour}} \quad \gamma \in E_M$$

<u>et</u>

$(II)_M$ $$\log |G_N|_{M \log M} \leq - M^m$$

<u>où on a noté</u>

$$G_N = F_N \prod_{j=1}^{d} g_j^{[L_j]} \, .$$

(La fonction g_j est le dénominateur de f_j donné par les axiomes d'ordre arithmétique).

Le premier pas montre que $(I)_N$ est vérifiée. D'autre part si on démontre la propriété $(II)_M$ pour tout M on en déduira que G_N est identiquement nulle, en contradiction avec l'indépendance algébrique sur $\mathbb{Q}$ des fonctions $f_1, \dots, f_d$. Donc le deuxième pas terminera la démonstration.

<u>Montrons que</u> $(II)_M \Rightarrow (I)_{M+1}$ <u>pour</u> $M \geq N$.

Les points de E_{M+1} sont dans la boule $B(0, M \log M)$; par l'axiome 0.A.2, on déduit de $(II)_M$

$$|F_N(\gamma)| \leq \exp(-c_{10} M^m) \qquad \text{pour } \gamma \in E_{M+1}$$

(on utilise l'hypothèse $m > \rho + \frac{h}{d}$). Le dénominateur et les valeurs absolues des conjugués de $F_N(\gamma)$ sont majorés par $\exp(c_{11} M^{\rho + \frac{h}{d}})$. La norme de $F_N(\gamma)$ sur $\mathbb{Q}$ est donc nulle, d'où $(I)_{M+1}$

<u>Il reste à démontrer que</u> $(I)_M \Rightarrow (II)_M$ <u>pour</u> $M \geq N$.

La fonction entière G_N a un zéro en chaque point de E_M. Pour $R = M(\log M)^2$, un calcul facile (utilisant le fait que les fonctions entières g_j et $f_j g_j$ sont d'ordre $\leq \rho_j$) montre que

$$\log |G_N|_R \leq c_{12} \, [M (\log M)^2]^{\rho + \frac{h}{d}} .$$

Il reste à vérifier

$$\log |G_N|_{M \log M} \leq \log |G_N|_R - c_{13} M^m \log \log M.$$

Dans le 1er cas c'est immédiat grâce à l'hypothèse que le sous-groupe Γ vérifie un lemme de Schwarz avec l'exposant m.

Dans le 2e cas c'est une conséquence de la proposition 7.4.1.

Dans le 3e cas on utilise le théorème 7.3.4 pour les fonctions $f_j(z) = G_N(z - t_j)$ avec $L = c_{14} M^m$. Pour $r = c_{15} M \log M$ on a

$$|G_N|_{M \log M} \leq \min_{1 \leq j \leq q} |f_j|_r ,$$

ce qui termine la démonstration.

REMARQUE 8.3.7. Sous les hypothèses de la première partie du théorème 8.3.1, si les fonctions $f_1, \ldots, f_d$ admettent des périodes communes $\omega_1, \ldots, \omega_\theta \in \Gamma$ linéairement indépendantes sur $\mathbb{Q}$, alors

$$m d \leq \ell + \rho_1 + \ldots + \rho_d - \theta .$$

(Comparer avec la remarque 1.1.6). Pour le démontrer, on peut supposer $\Gamma = \mathbb{Z} \gamma_1 + \ldots + \mathbb{Z} \gamma_{\ell-\theta} + \mathbb{Z} \omega_1 + \ldots + \mathbb{Z} \omega_\theta$. On reprend alors la démonstration précédente, avec $h = \ell - \theta$, et

$$E_N = \{ h_1 \gamma_1 + \ldots + h_{\ell-\theta} \gamma_{\ell-\theta} ; -N \leq h_j \leq N, (1 \leq j \leq \ell-\theta) \},$$

et on remarque que la propriété $(I)_M$ implique

$$F_N(\gamma) = 0 \quad \text{pour tout} \quad \gamma \in \Gamma_M .$$

Société Mathématique de France
Astérisque 69-70 (1979) p. 163-189

Appendice I

Problèmes locaux

par
Daniel BERTRAND

I - INTRODUCTION

§ 1.1 . Position du problème

Soient G un groupe algébrique commutatif connexe défini sur un corps de nombres F, TG l'espace tangent à l'origine de G, et k le complété de F en une place v de F. L'ensemble $G(k)$ des points k-rationnels de G est un groupe de Lie v-adique, et chaque application exponentielle v-adique sur G définit un difféomorphisme local $\exp_{G(k)}$ de $TG(k)$ dans $G(k)$. Si v est une place infinie, ce difféomorphisme admet un prolongement analytique sur $TG(\mathbb{C})$, dont les propriétés arithmétiques ont fait l'objet des chapitres précédents(1). Supposant désormais que v est une place finie $\mathfrak{p}$ de F, nous nous proposons d'aborder les questions de transcendance liées à $\exp_{\mathfrak{p}} = \exp_{G(k)}$. Cette étude est motivée par plusieurs applications arithmétiques, qui seront détaillées à la fin de l'appendice.

C'est précisément l'absence d'un prolongement analytique naturel de l'application $\exp_{\mathfrak{p}}$ qui fournit le principal obstacle à la recherche des analogues $\mathfrak{p}$-adiques des résultats de [W]. Elle conduit à faire jouer, dès l'énoncé des critères de transcendance, un rôle central aux équations fonctionnelles satisfaites par $\exp_{\mathfrak{p}}$ (théorèmes d'addition et de multiplication ; rappelons que, dans le cas complexe -cf. [W], chap.8 - , ces propriétés n'apparaissent que dans les situations "non normalisées").

Parallèlement aux applications exponentielles, nous étudierons les uniformisantes des groupes $G(k)$ qui, comme les variétés abéliennes dégénérantes, admettent, parmi

(1) "Nombres transcendants et groupes algébriques", par Michel Waldschmidt (noté [W] dans ce qui suit).

leurs revêtements non ramifiés, des tores $(k^*)^n$. Les démonstrations de leurs propriétés arithmétiques sont alors très proches de la théorie complexe.

Les parties II et III de cet appendice sont consacrées à des critères de transcendance $\mathfrak{p}$-adiques. La quatrième partie, qui forme le coeur du présent travail, réunit les résultats de transcendance qu'on déduit de ces critères pour les sous-groupes à plusieurs paramètres de $G(k)$. Nous n'avons pas détaillé ce qu'ils expriment sur des groupes algébriques particuliers car, en l'absence de périodes non nulles liées à $\exp_p$, aucun nombre "naturel" n'apparaîtrait dans ces applications. En revanche, la considération des homomorphismes analytiques de $(k^*)^n$ dans les variétés abéliennes dégénérantes permet d'étudier les valeurs de certaines séries d'Eisenstein.

La dernière partie de l'appendice est donc consacrée aux applications de ces résultats de transcendance (et des généralisations qu'en fournit la théorie des formes linéaires de logarithmes) à diverses branches de la théorie des nombres. Les unes concernent l'arithmétique des corps de nombres, les autres la géométrie diophantienne.

§ 1.2 Notations

On désigne par k un corps non archimédien complet de caractéristique nulle, et de caractéristique résiduelle $p \neq 0$. On note $\mathcal{O}$ son anneau d'entiers et $|\ |$ sa valeur absolue, normalisée par $|p| = p^{-1}$. On suppose (ce qui ne restreint pas la généralité des résultats de transcendance) que k est plongé dans le complété $\mathbb{C}_p$ d'une clôture algébrique du corps des nombres p-adiques $\mathbb{Q}_p$, et on désigne par $\bar{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}_p$. Dans la pratique, k sera soit $\mathbb{C}_p$, soit un corps localement compact (on notera alors δ son degré sur $\mathbb{Q}_p$).

Soit $f(X) = \sum_{\nu \in \mathbb{Z}^n} a_\nu X_1^{\nu_1} \ldots X_n^{\nu_n}$ une série de Laurent formelle à n variables à coefficients dans k. Pour tout nombre réel $r > 0$, on pose :

$$|f|_r = \sup_{\nu \in \mathbb{Z}^n} |a_\nu|\, r^{\|\nu\|},$$

où $\|\nu\| = \nu_1 + \ldots + \nu_n$ désigne la longueur du n-uple ν. Les séries de Taylor f telles que $|f|_1$ est fini s'identifient aux fonctions strictement analytiques sur $\mathcal{O}^n$, dont l'ensemble sera noté $\mathcal{A}(\mathcal{O}^n)$.

La hauteur $H(P)$ d'un polynôme P à coefficients entiers algébriques désigne le maximum des hauteurs "usuelles" (au sens de [W], § 1.1.b) de ses coefficients.

Soit Γ un $\mathbb{Z}$-module libre de type fini. A toute base $\mathcal{B} = \{\gamma_1, \ldots, \gamma_\ell\}$ de Γ

sur $\mathbb{Z}$, et à tout entier $N \geq 0$, on associe l'ensemble

$$\Gamma_N = \Gamma_N(\mathcal{B}) = \{\sum_{i=1}^{\ell} h_i \gamma_i \ ;\ h_i \in \mathbb{Z} \ ;\ 0 \leq h_i \leq N\}$$

Certaines des définitions données plus bas font intervenir les ensembles $\Gamma_N(\mathcal{B})$. On pourra vérifier qu'elles sont indépendantes du choix d'une base $\mathcal{B}$ de Γ. On n'a donc pas explicité la dépendance en $\mathcal{B}$ des constantes apparaissant dans leurs énoncés.

Pour des raisons de clarté, on a enfin distingué, dans certains énoncés, l'algèbre Lie G des dérivations invariantes sur un groupe algébrique connexe G de son espace tangent à l'origine TG.

II - CRITERES DE TRANSCENDANCE GENERAUX

Les résultats rassemblés dans cette partie se rapportent à l'étude des sous-groupes à n paramètres $\mathfrak{p}$-adiques. Aussi n'y considère-t-on que des fonctions analytiques sur un voisinage de l'origine de k^n, que l'on peut, sans perte de généralité, identifier à $\mathcal{O}^n$. Comme dans le cas complexe, on est amené à distinguer deux situations, suivant que les fonctions considérées satisfont des équations différentielles algébriques (cas normalisé) ou non. Les critères de transcendance obtenus sont exposés aux §§ 2.1 et 2.2. Les outils d'analyse ultramétrique nécessaires à leur démonstration sont développés au § 2.4.

§ 2.1 Le cas normalisé

Dans les applications que nous avons en vue, le théorème 1 joue le rôle du corollaire 5.1.2 de [W]. Mais il concerne les solutions de systèmes différentiels vérifiant de plus une famille d'équations fonctionnelles.

On suppose donnés dans tout ce paragraphe n endomorphismes $\pi_1, \ldots, \pi_n$ du $\mathcal{O}$-module $\mathcal{O}^n$ tels que, pour tout n-uple $\nu = (\nu_1, \ldots, \nu_n)$ d'entiers rationnels >0, l'endomorphisme

$$\tau_\nu = \nu_1 \pi_1 + \ldots + \nu_n \pi_n$$

soit injectif.

A tout élément ν de $\mathbb{N}^n$, et tout élément f de $\mathcal{A}(\mathcal{O}^n)$, on associe l'élément

$$T_\nu f = f \circ \tau_\nu$$

de $\mathcal{A}(\mathcal{O}^n)$, et le n-uple

$$\underset{\sim}{f} = (f \circ \pi_1, \ldots, f \circ \pi_n)$$

d'éléments de $\mathcal{H}(\mathcal{O}^n)$.

Définition 1 : on dira qu'une famille $\{f_1,\dots,f_\ell\}$ d'éléments de $\mathcal{H}(\mathcal{O}^n)$ est d'ordre arithmétique fonctionnel fini (relativement à $\pi_1,\dots,\pi_n$) s'il existe un corps de nombres K, d'anneau d'entiers I, et des nombres réels ρ et c tels que, pour tout élément ν de $\mathbb{N}^n$, il existe 2ℓ éléments

$$\{P_{i,\nu}\ ,\ Q_{i,\nu}\ ;\ i=1,\dots,\ell\}\ \text{de}\ I\,[X_{sj}\ ;\ s=1,\dots,\ell\ ;\ j=1,\dots,n\,]$$

de degrès totaux $\leqq c\,\|\nu\|^\rho$, de hauteurs $\leqq \exp(c\,(1+\|\nu\|^\rho))$ tels que, pour $i=1,\dots,\ell$:

$$T_\nu\, f_i = P_{i,\nu}\,(\underset{\sim}{f}_1,\dots,\underset{\sim}{f}_\ell)\,/\,Q_{i,\nu}\,(\underset{\sim}{f}_1,\dots,\underset{\sim}{f}_\ell).$$

Un élément ζ de $\mathcal{O}^n$ sera dit régulier pour $\{f_1,\dots,f_\ell\}$ si, pour tout n-uple ν et tout indice i, il existe une telle représentation de $T_\nu f_i$ vérifiant en outre : $Q_{i,\nu}\,(\underset{\sim}{f}_1(\zeta),\dots,\underset{\sim}{f}_\ell(\zeta)) \neq 0$.

Le théorème 1 généralise à plusieurs variables le théorème 1 de [Be 3].

THÉORÈME 1 : Soit $\{f_1,\dots,f_\ell\}$ une famille d'éléments de $\mathcal{H}(\mathcal{O}^n)$ d'ordre arithmétique fonctionnel fini. On suppose que le corps $\bar{\mathbb{Q}}\,(f_1,\dots,f_\ell)$ a un degré de transcendance $\geqq n+1$ sur $\bar{\mathbb{Q}}$, et qu'il existe n dérivations k-linéairement indépendantes de Lie (k^n) opérant sur l'algèbre $\bar{\mathbb{Q}}\,[f_i \circ \pi_j\ ;\ i=1,\dots,\ell\ ;\ j=1,\dots,n\,]$. Soit ζ un élément de $\mathcal{O}^n$, régulier pour $\{f_1,\dots,f_\ell\}$, et tel que $\pi_1(\zeta),\dots,\pi_n(\zeta)$ soient linéairement indépendants sur k. Alors, l'un au moins des nombres $f_i \circ \pi_j(\zeta)$ $(i=1,\dots,\ell\ ;\ j=1,\dots,n)$ est transcendant.

La démonstration du théorème 1 suit la démarche de [Be 3], §1.3. Supposant que les fonctions $f_1,\dots,f_\ell$ prennent simultanément des valeurs algébriques en ζ, on construit, grâce au principe des tiroirs et au lemme 1 énoncé plus bas, une fonction F, analytique sur $\mathcal{O}^n$, s'annulant à un ordre de multiplicité élevé aux points de l'ensemble $\{\tau_\nu(\zeta)\ ;\ \nu_i \in p\mathbb{N}\ ;\ 0<\nu_i \leqq N\}$, où N est un entier suffisamment grand. Le lemme de Schwarz sur les produits (§ 2.4, lemme 4) permet de majorer $|F|_{p^{-1}}$. Le lemme 1, joint à la formule du produit sur les corps de nombres, fournit la contradiction désirée (2).

LEMME 1 - Soient $\{f_1,\dots,f_\ell\}$ une famille d'éléments de $\mathcal{H}(\mathcal{O}^n)$ d'ordre arithmétique fonctionnel fini. On reprend les notations qui lui sont associées par la définition 1. On suppose qu'il existe n éléments k-linéairement indépendants $D_1,\dots,D_n$ de Lie (k^n) opérant sur l'algèbre $I[\underset{\sim}{f}_1,\dots,\underset{\sim}{f}_\ell]$. Pour tout n-uple

(2) Voir D. Bertrand, Groupe de Travail d'Analyse ultramétrique, Paris, 1978-79, exposé n° 9 .

σ de $\mathbb{N}^n$, on note D^σ l'opérateur $D_1^{\sigma_1}\dots D_n^{\sigma_n}$. Alors, il existe un nombre réel $\gamma=\gamma(f_1,\dots,f_\ell)$ vérifiant la propriété suivante. Soient $L_1,\dots,L_\ell$ des entiers $\geqq 0$ de somme L, H un entier >0 et P un élément de $I[X_1,\dots,X_\ell]$ de degré $\leqq L_i$ en X_i, de hauteur $\leqq H$. Pour tout couple (σ,ν) d'éléments de $\mathbb{N}^n$, la fonction $F=P(f_1,\dots,f_\ell)$ vérifie :

$$\Big(\prod_{i=1}^{\ell} Q_{i,\nu}^{L_i}\,(\underset{\sim}{f}_1,\dots,\underset{\sim}{f}_\ell)\Big)\, D^\sigma\, T_\nu F = R_{\sigma,\nu,P}\,(\underset{\sim}{f}_1,\dots,\underset{\sim}{f}_\ell) + \sum_{\substack{\|\varkappa\|<\|\sigma\| \\ \varkappa_j \leqq \sigma_j}} r_{\varkappa,\nu,P}\, D^\varkappa\, T_\nu F\,,$$

où les fonctions $r_{\varkappa,\nu,P}$ sont analytiques sur $\mathcal{O}^n$, et $R_{\sigma,\nu,P}$ désigne un élément de $I[X_{ij}\ ;\ i=1,\dots,\ell\ ;\ j=1,\dots,n\,]$ de degrés partiels $\leqq \gamma\,(\|\sigma\|+L_i\,\|\nu\|^\rho)$ en $X_{i1},\dots,X_{i,n}$, de hauteur

$$\leqq H\,(1+\gamma\,(\|\sigma\|+L\,\|\nu\|^\rho))^{\gamma\|\sigma\|}\ \exp(\gamma(\|\sigma\|+L\,(1+\|\nu\|^\rho)))\ .$$

Ce lemme, qui généralise une idée de Baker et Coates (voir [M 1], lemme 7.7. ; [Be 3], lemme 2), améliore, en point régulier pour $\{f_1,\dots,f_\ell\}$, les estimations de hauteur fournies par le lemme 5.4.2 de [W].

§ 2.2 Le cas non normalisé

L'énoncé obtenu dans ce cas concerne les valeurs de fonctions algébriquement indépendantes, sur un sous-groupe Γ de $\mathcal{O}^n$. Comme dans le cas complexe (voir [W], théorème 8.3.1), il fait intervenir une propriété métrique de Γ, caractérisée par son coefficient de densité $\varkappa(\Gamma,k^n)$. Pour alléger l'écriture (et pour pouvoir disposer plus tard d'un lemme de transfert, cf. § 2.3), nous supposerons ici k localement compact. On note δ son degré sur $\mathbb{Q}_p$, e son indice de ramification, f son degré résiduel, et $\mathfrak{p}$ l'idéal maximal de $\mathcal{O}$.

Définition 2 . On appelle coefficient de densité (relativement au corps localement compact k) d'un sous-groupe Γ de type fini de $\mathcal{O}^n$, et on note $\varkappa(\Gamma,k^n)$, le maximum des nombres réels $\varkappa$ vérifiant la propriété suivante : il existe un nombre réel $c=c(\varkappa)$ tel que, pour tout entier $\nu\geqq 0$, la restriction à $\Gamma_{[cp^{f\nu/\varkappa}]}$ de la projection canonique : $\mathcal{O}^n \to (\mathcal{O}/\mathfrak{p}^\nu)^n$ est surjective.

Avec les notations de [Se 3], où $k=\mathbb{Q}_p$, Γ est alors dit $(1/\varkappa)$ - dense ; une normalisation différente est proposée dans [F], chapitre 3, § 5. Nous précisons au § 2.3 certaines propriétés du coefficient $\varkappa(\Gamma,k^n)$.

La définition suivante reprend celle de [W], § 1.1.b.

Définition 3 . Soient f un élément de $\mathcal{H}(\mathcal{O}^n)$, Γ un sous-groupe de $\mathcal{O}^n$ de type fini, et ρ un nombre réel. On dira que f est d'ordre arithmétique inférieur ou *égal à* ρ *sur* Γ s'il existe un corps de nombres K et un nombre réel c tels que, pour tout entier $N \geqq 1$ et tout élément γ de Γ_N, le nombre $f(\gamma)$ est un élément de K de hauteur $\leqq \exp(c N^{\rho})$.

Le théorème 2 a été démontré par Serre (voir [Se 3], théorème 2) lorsque les fonctions f_i sont des exponentielles, et que $k = \mathbb{Q}_p$. Il est énoncé par Flicker (voir [F], chapitre 3, § 5) lorsque tous les ρ_i sont égaux. La démonstration du cas général suit celle du théorème 8.3.1 (2e et 3e partie) de [W]. Nous nous bornerons à signaler que les estimations analytiques sont ici fournies par le lemme 5 du § 2.4.

THÉORÈME 2 . *Soient* $\rho_1,\dots,\rho_d$ *des nombres réels,* Γ *un sous-groupe de type fini de* $\mathcal{O}^n$, *et* $f_1,\dots,f_d$ *des éléments de* $\mathcal{H}(\mathcal{O}^n)$ *d'ordre arithmétique respectivement inférieur ou égal à* $\rho_1,\dots,\rho_d$ *sur* Γ. *On suppose que les fonctions* $f_1,\dots,f_d$ *sont algébriquement indépendantes sur* $\mathbb{Q}$. *Alors* :

$$\varkappa(\Gamma,k^n)\,(d-n) \leqq \rho_1 + \dots + \rho_d .$$

§ 2.3 . Quelques mesures de répartition

Dans ce qui suit, Γ désigne un sous-groupe de type fini de $\mathcal{O}^n$, de rang ℓ sur $\mathbf{Z}$. On ne suppose k localement compact que lorsque le coefficient de densité $\varkappa(\Gamma,k^n)$ entre en jeu.

Rappelons tout d'abord la définition de l'*exposant de Dirichlet* $\mu(\Gamma,k^n)$, donnée au § 1.3.a de [W] dans un cadre général : c'est le plus petit des nombres $(\ell - \mathrm{rg}_{\mathbf{Z}}(\Gamma \cap \mathcal{V}))/(n - \dim_k \mathcal{V})$, où $\mathcal{V}$ parcourt l'ensemble des k-sous-espaces vectoriels de k^n de dimension $< n$. On notera que si k est une extension algébrique de degré δ de $\mathbb{Q}_p$, alors

$$\mu(\Gamma,k^n) \geqq \delta\,\mu(\Gamma,\mathbb{Q}_p^{\delta n}) ;$$

lorsque Γ est inclus dans $\mathbb{Q}_p^n$, on a de plus :

$$\mu(\Gamma,k^n) = \delta\,\mu(\Gamma,\mathbb{Q}_p^{\delta n}) = \mu(\Gamma,\mathbb{Q}_p^n).$$

Parallèlement au cas complexe (voir [W], théorème 1.3.4), on peut, grâce à l'analogue p-adique, dû à Schlickewei (voir [Schl], théorème 1.1), du théorème de W. Schmidt, caractériser les sous-groupes bien répartis de $(\overline{\mathbb{Q}} \cap \mathbf{Z}_p)^n$ de la façon suivante.

LEMME 2 . *Soit* Γ *un sous-groupe de* $(\overline{\mathbb{Q}} \cap \mathbf{Z}_p)^n$ *de rang fini* $\ell > n$. *Les propriétés suivantes sont équivalentes* :

i) $\mu(\Gamma,\mathbb{Q}_p^n) = \ell / n$

ii) *pour tout nombre réel* $\epsilon > 0$, *il existe une constante* $c(\epsilon) > 0$ *telle que, pour tout entier* $N \geqq 1$:

$$\min\{|\gamma| \; ; \; \gamma \in \Gamma_N , \; \gamma \neq 0\} \geqq c(\epsilon) N^{-(\ell/n) - \epsilon} .$$

Supposons maintenant k localement compact. On prendra garde au fait que la définition du coefficient de densité de Γ fait intervenir une normalisation différente de celle du cas complexe (voir [W], § 1.3.b). En particulier, on a :

$$\varkappa(\Gamma,k^n) = \delta\,\varkappa(\Gamma,\mathbb{Q}_p^{\delta n}) .$$

Néanmoins, les énoncés du § 1.3 de [W] se traduisent sans difficulté en $\mathfrak{p}$-adique. Ainsi, $(\mathcal{O}/\mathfrak{p}^{\nu})^n$ a $p^{f \nu n}$ éléments, dont les distances relatives sont minorées par $p^{-\nu/e}$. Donc on peut associer à tout nombre réel $\varkappa < \varkappa(\Gamma,k^n)$ une constante $C(\varkappa)$ telle que, pour tout entier $N \geqq 1$, il existe un sous-ensemble S_N de Γ_N, ayant plus de $C(\varkappa)N^{\varkappa n}$ éléments, dont les distances relatives sont minorées par $C(\varkappa)N^{-\varkappa/\delta}$. En conséquence :

$$\varkappa(\Gamma,k^n) \leqq \mu(\Gamma,k^n).$$

Le lemme 2, joint à un lemme de transfert p-adique (voir [Lu], lemme 3.16 et théorème 3.20) entraîne alors :

LEMME 3 . *Soit* Γ *un sous-groupe de type fini de* $(\overline{\mathbb{Q}} \cap \mathbf{Z}_p)^n$. *On a* :

$$\varkappa(\Gamma,\mathbb{Q}_p^n) = \mu(\Gamma,\mathbb{Q}_p^n) .$$

Dans le même ordre d'idées, on déduit de l'analogue p-adique du théorème de Khintchine (voir [Lu], théorèmes 4.22 et 4.24) que, si $\ell \geqq n$ désignent deux entiers > 0, le groupe $\Gamma = \mathbf{Z}\gamma_1 \oplus \dots \oplus \mathbf{Z}\gamma_\ell$ a un coefficient de densité égal à ℓ / n pour presque tout ℓ-uple $\{\gamma_1,\dots,\gamma_\ell\}$ d'éléments de $\mathcal{O}^n$ (au sens de la mesure de Haar sur $\mathcal{O}^{\ell n}$).

§ 2.4 . Les lemmes de Schwarz

Il s'agit d'améliorer le principe du maximum pour des fonctions analytiques s'annulant sur un ensemble S donné. Nous distinguerons deux types d'énoncés, suivant que S est soumis à des conditions linéaires ou métriques.

Définition 4 . Soit θ une fonction numérique sur $\mathbf{N}^2$. On dira qu'un sous-groupe Γ de $\mathcal{O}^n$ vérifie *un lemme de Schwarz* (*avec multiplicités*) *de type* θ s'il existe un nombre réel $c > 0$ tel que, pour tout entier $N \geqq 1$ et tout élément f de $\mathcal{H}(p^{-1}\mathcal{O}^n)$ s'annulant à l'ordre t sur Γ_N, on a :

$$|f|_1 \leqq p^{-c\,\theta(t\,,\,N)}\,|f|_p \,.$$

On vérifie aisément que $\theta(t\,,N)$ est majoré par $t\,N^{\mu(\Gamma\,,\,k^n)}$ (voir [W], lemme 7.1.7.), et un raisonnement à une variable montre que $\theta(t,N)$ peut être choisi égal à t. La première minoration non triviale de θ a été obtenue par Serre ([Se 3], proposition 2) lorsque $t = 1$, et sous une hypothèse métrique sur Γ. Le cas des multiplicités quelconques a été traité par Robba [Ro], auquel nous empruntons tous les énoncés de ce paragraphe.

Le lemme 4 correspond à une condition linéaire.

LEMME 4 - Soit Γ un sous-groupe de type fini de $\mathcal{O}^n$, tel que $\mu(\Gamma,k^n)$ soit $\geqq 1$. Alors Γ vérifie un lemme de Schwarz de type $\theta(t,N) = tN$.

En effet, Γ contient par hypothèse n éléments k-linéairement indépendants. Un changement de variables permet alors de supposer que Γ_N contient le produit $\{1,\dots,N\}^n$. On conclut au moyen du théorème 2.3.1 de [Ro].

Le lemme 5 répond à la fois aux théorèmes 7.3.1 et 7.4.2 de [W]. On suppose maintenant k localement compact.

LEMME 5 - Soit Γ un sous-groupe de type fini de $\mathcal{O}^n$. Pour tout nombre réel $\epsilon > 0$, Γ vérifie un lemme de Schwarz de type

$$\theta(t,N) = t\,N^{\varkappa(\Gamma,k^n)-\epsilon} \,.$$

Considérons en effet, pour tout nombre réel $\varkappa < \varkappa(\Gamma,k^n)$ et tout entier $N \geqq 1$, le sous-ensemble S_N de Γ_N défini au § 2.3, et soit σ_N la distance relative minimale des éléments de S_N. D'après le théorème 3.3.2 de [Ro], Γ vérifie un lemme de Schwarz de type

$$\theta(t,N) = t\,(\mathrm{card}\,S_N)\,\sigma_N^{\delta(n-1)} \,.$$

Le lemme 5 en découle.

Remarque 1 - Robba déduit de ces résultats le corollaire suivant ([Ro], théorème 3.4.1) : soit S un sous-ensemble de $\mathcal{O}^n$ tel que tout point de $\mathcal{O}^n$ soit à une distance $\leqq L^{-1/\delta}$ de S ; tout élément P de $k[X_1,\dots,X_n]$ de degré $\leqq L$ vérifie alors :

$$|P|_1 \leqq C^L \sup_{\gamma\in S} |P(\gamma)|,$$

où $C = p^{1/(p-1)}$. En reprenant la démarche exposée au §§ 7.3 et 7.4 de [W], on pourra, inversement, établir la minoration

$$\theta(1,N) \geqq N^{\varkappa(\Gamma,k^n)-\epsilon}$$

à partir de ce corollaire.

Remarque 2 : D'après le lemme 3, on peut, lorsque $k = \mathbb{Q}_p$, et que Γ est composé d'éléments algébriques sur $\mathbb{Q}$, remplacer l'exposant $\varkappa(\Gamma,k^n)-\epsilon$ par $\mu(\Gamma,k^n)-\epsilon$ dans la conclusion du lemme 5. Est-ce encore le cas lorsque Γ est un sous-groupe de type fini de $\mathcal{O}^n$ quelconque?

III - LE CAS D'UNE VARIABLE

Les critères de transcendance de la 2e partie (et, plus particulièrement, le théorème 2) peuvent être améliorés de façon notoire dans le cas unidimensionnel. Par ailleurs, un lemme de Schwarz sur les couronnes permet d'étudier les fonctions méromorphes sur k^*. Ces dernières conduisent à des situations "globales" qui, à l'instar du cas complexe, fournissent de meilleurs critères de transcendance. On les étudie aux § § 2.3 (où sont également traitées certaines fonctions méromorphes sur $(k^*)^n$) et 2.4 .

§ 3.1 . Les situations locales

L'amélioration obtenue dans le cas normalisé concerne l'hypothèse de régularité introduite au théorème 1, qui peut maintenant être omise. Par ailleurs, on peut supposer, sans perte de généralité, que l'endomorphisme π_1 est l'identité.

PROPOSITION 1 - Soit $\{f_1,\dots, f_\ell\}$ une famille d'éléments de $\mathcal{H}(\mathcal{O})$ d'ordre arithmétique fonctionnel fini. On suppose que l'algèbre $\bar{\mathbb{Q}}[f_1,\dots, f_\ell]$ a un degré de transcendance $\geqq 2$ sur $\bar{\mathbb{Q}}$, et qu'il existe une dérivation non nulle de Lie (k) la laissant stable. Soit ζ un élément non nul de $\mathcal{O}$. Alors, l'un au moins des nombres $f_1(\zeta),\dots, f_\ell(\zeta)$ est transcendant.

La démonstration de la proposition 1 suit celle du théorème 1. Mais, lorsque ζ n'est pas un point régulier pour $\{f_1,\dots,f_\ell\}$, le lemme 1 ne permet en général plus d'estimer la hauteur de $D^\sigma T_\nu F(\zeta)$, et il convient de généraliser son énoncé de la façon suivante : soit s l'ordre en ζ de la fonction

$$Q_{\nu,P} = \prod_{i=1}^{\ell} Q_{i,\nu}^{L_i}\,(f_1,\dots, f_\ell) \,;$$

alors

$$D^s Q_{\nu,P}\,(\zeta)\,D^\sigma\,T_\nu\,F\,(\zeta) = R_{s+\sigma,\nu,P}\,(f_1,\dots, f_\ell)\,(\zeta)\,+$$

$$+ \sum_{0\leqq\varkappa<\sigma} r_{s+\varkappa,\nu,P}\,(\zeta)\,D^\varkappa\,T_\nu\,F(\zeta) \,.$$

Il reste à majorer s . On utilise à cet effet un théorème de Brownawell et Masser [Br - M] sur les algèbres différentielles de type fini, en vertu duquel l'ordre de

$Q_{\nu,P}$ en tout point de $\mathcal{O}$ est majoré par $c\,L\,\nu^{2^{\ell-1}\rho}$, où c désigne un nombre réel ne dépendant que de $f_1,\dots,f_\ell$.

Remarque 3 : La proposition 1 est encore valable quand on remplace les fonctions τ_ν auxquelles sont associés les opérateurs T_ν (voir § 2.1) par une suite de contractions analytiques sur $\mathcal{O}$ plus générales. Ceci permet en particulier d'étudier directement les propriétés de transcendance des fonctions logarithmes de certaines lois de groupes formels.(3)

L'amélioration obtenue dans le cas non normalisée est plus fondamentale.

PROPOSITION 2 - *Soient $\rho_1,\dots,\rho_d$ et ℓ des nombres réels, Γ un sous-groupe de type fini de $\mathcal{O}$ de rang $\leq \ell$, et $f_1,\dots,f_d$ des éléments de $\mathcal{H}(\mathcal{O})$ d'ordre arithmétique respectivement inférieur ou égal à $\rho_1,\dots,\rho_d$ sur Γ. On suppose que les fonctions $f_1,\dots,f_d$ sont algébriquement indépendantes sur $\mathbb{Q}$. Alors :*

$$\ell\,(d-n) \leq \rho_1+\dots+\rho_d\,.$$

En d'autres termes, le coefficient de densité $\varkappa(\Gamma,\mathcal{O})$ peut ici être remplacé par le rang $\mu(\Gamma,k)$ de Γ. En effet, tout sous-groupe Γ de $\mathcal{O}$ de rang ℓ vérifie un lemme de Schwarz de type $\theta(t,N)=tN^\ell$. Ceci résulte aisément de la multiplicativité des normes $\{\ |\ |_r\ ;\ 0<r\leq 1\}$ sur l'algèbre de Banach $\mathcal{H}(\mathcal{O})$ (voir(4) [Se 3], proposition 2).

§ 3.2 - La situation globale normalisée

Les fonctions méromorphes sur k^* ou $(k^*)^n$ étudiées ci-dessous apparaîtront au § 3 comme uniformisantes de certaines variétés abéliennes. Signalons dès à présent qu'on peut, dans tous les énoncés obtenus dans ce cadre, remplacer le corps ultramétrique k par le corps des nombres complexes (voir [Be 1], remarque 3, et [F], chapitre 5, § 3).

Définition 5 - Soient $\mathcal{M}((k^*)^n)$ le corps des fractions de l'anneau $\mathcal{H}((k^*)^n)$ des séries de Laurent convergeant sur $(k^*)^n$, et $\{\sigma,\rho\}$ un couple de nombres réels ≥ 0. On dira qu'un élément f de $\mathcal{M}((k^*)^n)$ est *d'ordre inférieur ou égal à* $\{\sigma,\rho\}$ s'il existe deux nombres réels c_1 et c_2 et deux éléments g_1 et g_2 de $\mathcal{H}((k^*)^n)$ tels que $f=g_1/g_2$, et que, pour $i=1,2$, et pour tout nombre réel $r>0$:

$$\log|g_i|_r \leq c_i(r+r^{-1})^\sigma(\log(r+r^{-1}))^\rho$$

(3) Voir D. Bertrand, Séminaire Delange-Pisot-Poitou, 1976/77, exposé n° 1.

(4) Le premier lemme de Schwarz à une variable p-adique a été énoncé par K. Mahler (Compositio math., 2, 1935, pp. 259-275, proposition 3).

La proposition 3 répond au théorème 1.1.1 de [W].

PROPOSITION 3 - *Soient K un corps de nombres, σ et ρ deux nombres réels ≥ 0, et $f_1,\dots,f_\ell$ des éléments de $\mathcal{M}(k^*)$ d'ordre inférieur ou égal à $\{\sigma,\rho\}$. On suppose que l'algèbre $K[f_1,\dots,f_\ell]$ a un degré de transcendance ≥ 2 sur K, et qu'il existe une dérivation non nulle de Lie (k^*) la laissant stable. Alors, l'ensemble des éléments de k^* où $f_1,\dots,f_\ell$ prennent simultanément des valeurs dans K est fini, et a au plus $4\,\sigma[K:\mathbb{Q}]$ éléments.*

La démonstration de la proposition 3 est donnée dans [Be 1]. Elle repose sur un lemme de Schwarz sur les couronnes $\mathcal{C}_r=\{z\in k^*,\ r^{-1}<|z|<r\}$ de k (voir [Be 1], lemme 2) :

LEMME 6 - *Soient R et r deux nombres réels, $R>r>1$, et f une fonction analytique sur $\mathcal{C}_R$ admettant h zéros (comptés avec leurs ordres de multiplicité) dans $\mathcal{C}_r$. Alors*

$$\sup(|f|_r, |f|_{1/r}) \leq (r/R)^{(1-\alpha)h/2}\sup(|f|_R, |f|_{1/R}),$$

où $\alpha=(\log r)/\log R$.

Faute d'un lemme de Schwarz pour les fonctions analytiques sur $(k^*)^n$ (ou, plus généralement, sur le complémentaire d'un diviseur algébrique de k^n), la proposition 3 n'a pas encore été généralisée à plusieurs variables. Néanmoins, le lemme 6 permet, comme l'a montré Flicher, de traiter certaines situations pluridimensionnelles. Nous énonçons son résultat sous la forme suivante (voir [F], chapitre 5, proposition 1) :

THÉORÈME 3 - *Soient K un corps de nombres, ρ un nombre réel >0, et $f_1,\dots,f_\ell$ des éléments de $\mathcal{M}((k^*)^n)$ d'ordre inférieur ou égal à $\{0,\rho\}$. On suppose que l'algèbre $K[f_1,\dots,f_\ell]$ a un degré de transcendance $\geq n+1$ sur K, et qu'il existe n dérivations de Lie $(k^*)^n$ la laissant stable. Alors, pour tout élément ζ de $(k^*)^n$ où les fonctions $f_1,\dots,f_\ell$ sont définies, l'un au moins des nombres $f_1(\zeta),\dots,f_\ell(\zeta)$ est transcendant.*

Cet énoncé suffira pour les applications que nous avons en vue.

§ 3.3 - La situation globale non normalisée

La définition 3 du § 2.2. (voir [W], § 1.1 b) s'adapte aux fonctions méromorphes sur k^* de la façon suivante.

Définition 6 - Soient $\{f_1,\dots,f_d\}$ une famille d'éléments de $\mathcal{M}(k^*)$, $\rho_1,\dots,\rho_d$ des nombres réels >0, et Γ un sous-groupe libre de k^* de rang fini ℓ sur

$\mathbf{Z}$. On dira que $\{f_1,\ldots,f_d\}$ est d'ordre arithmétique inférieur ou égal à $\{\rho_1,\ldots,\rho_d\}$ sur Γ s'il existe un corps de nombres K, des nombres réels $c_1,\ldots,c_4 > 0$ et, pour $i = 1,\ldots,d$, une représentation $g_{i,1}/g_{i,2}$ de f_i formée d'éléments de $\mathcal{H}(k^*)$ d'ordre inférieur ou égal à $\{0,\rho_i\}$, tels que, pour tout entier $N \geq c_1$, un sous-ensemble S_N de Γ_N, de cardinal $\geq c_2 N^{\ell}$, vérifie les conditions suivantes : pour $i = 1,\ldots,d$, et tout élément γ de S_N, $|g_{i,2}(\gamma)|$ est minoré par $\exp(-c_3 N^{\rho_i})$ et $f_i(\gamma)$ est un élément de K de hauteur $\leq \exp(c_4 N^{\rho_i})$.

L'analogue complexe de la proposition 4 est, après synthèse de Fourier, une conséquence immédiate de la remarque 1.1.6 de [W].

PROPOSITION 4 - Soient $\rho_1,\ldots,\rho_d$ des nombres réels > 0, Γ un sous-groupe libre de k^* de rang fini ℓ sur $\mathbf{Z}$, et $\{f_1,\ldots,f_d\}$ une famille d'éléments de $\mathcal{M}(k^*)$ d'ordre arithmétique inférieur ou égal à $\{\rho_1,\ldots,\rho_d\}$ sur Γ. On suppose que les fonctions $f_1,\ldots,f_d$ sont algébriquement indépendantes sur $\mathbf{Q}$. Alors :

$$\ell(d-1) \leq \rho_1 + \ldots + \rho_d - d .$$

Démonstration (voir également [W], § 8.3.d) : Posons $\rho = (\rho_1+\ldots+\rho_d)/d$. On peut, sans perte de généralité, supposer que chacun des ρ_i est $< \rho + (\ell/d)$. On désigne par N un entier arbitrairement grand, et par C_1, C_2, C_3 des nombres réels > 0 indépendants de N. Le principe des tiroirs permet de construire un élément P non nul de $\mathbf{Z}[X_1,\ldots,X_d]$, de hauteur $\leq \exp(C_1 N^{\rho+(\ell/d)})$, de degré $L_i \leq N^{\rho+(\ell/d)-\rho_i}$ en X_i, tel que la fonction $F = P(f_1,\ldots,f_\ell)$ s'annule aux points de l'ensemble S_N associé par la définition 6 à $\Gamma_N = \{\gamma_1^{n_1}\ldots\gamma_\ell^{n_\ell} ; 0 \leq n_i \leq N\}$. Posons $C_2 = 1 + \sup_i(|\gamma_i| + |\gamma_i|^{-1})$, $r = C_2^N$, $R = C_2^{2N}$ (de sorte que $r/R = C_2^{-N}$), $G = (\prod_{i=1}^{\ell} g_{i,2}^{L_i})\, F$, et supposons que, contrairement à la conclusion du théorème 4, on ait l'inégalité : $\ell + 1 > \rho + (\ell/d)$.

Le lemme 6 entraîne alors :

$$\sup(|G|_r, |G|_{1/r}) \leq (r/R)^{N^{\ell}/4} \sup(|G|_R, |G|_{1/R})$$
$$\leq \exp(-C_3 N^{\ell+1}).$$

On conclut en reprenant le raisonnement par récurrence exposé au § 8.3.d de [W].

IV - RESULTATS DE TRANSCENDANCE

Nous sommes maintenant en mesure d'étudier les propriétés arithmétiques des homomorphismes analytiques $\mathfrak{p}$-adiques d'un sous-groupe $\mathcal{G}'$ d'un groupe algébrique G' dans un groupe algébrique G. Le cas où G' est une puissance du groupe additif fait l'objet des §§ 4.1 à 4.3, où sont tout d'abord précisés les propriétés des sous-groupes à plusieurs paramètres $\mathfrak{p}$-adiques de G. On traite au § 4.4 le cas où G' est une puissance de groupe multiplicatif, et G une variété abélienne dégénérante. Enfin, le § 4.5 réunit, sans démonstrations, les résultats que fournit la méthode de Baker.

§ 4.1 - Préliminaires

a) Sous-groupes à plusieurs paramètres.

(Le corps ultramétrique k est ici supposé localement compact). Soient $\mathfrak{G}$ un groupe de Lie sur k de dimension finie, et $T\mathfrak{G}$ son espace tangent à l'origine. L'application logarithme de $\mathfrak{G}$, définie de façon canonique sur la réunion des sous-groupes compacts de $\mathfrak{G}$, induit sur un sous-groupe ouvert $\mathfrak{G}'$ de $\mathfrak{G}$ un difféomorphisme à valeurs dans $T\mathfrak{G}$, dont l'inverse est une application exponentielle de $\mathfrak{G}$. Les autres applications exponentielles de $\mathfrak{G}$ n'en diffèrent que par des homomorphismes à valeurs dans le sous-groupe de torsion de $\mathfrak{G}$, et définissent, sur un sous-groupe compact ouvert $\mathcal{C}$ de $T\mathfrak{G}$ suffisamment "petit", une même application $\exp_{\mathfrak{G}}$, strictement analytique sur $\mathcal{C}$. Du point de vue de la théorie des nombres transcendants, on pourra donc se limiter à l'étude des valeurs de $\exp_{\mathfrak{G}}$. Nous spécifions ci-dessous une représentation de l'application $\exp_{\mathfrak{G}}$ lorsque $\mathfrak{G}$ provient d'un groupe algébrique commutatif (5).

Soient donc G un groupe algébrique commutatif connexe, de dimension g, défini sur un corps de nombres F, k le complété de F en une place finie $\mathfrak{p}$ de F, et $X = \{X_0,\ldots,X_N\}$ les coordonnées d'un plongement projectif ψ de G défini sur F. Quitte à faire une extension finie de F, on peut, après un choix convenable du plongement ψ, se placer dans les hypothèses du § 1 de l'Appendice II (6). D'autre part, on peut, sans perte de généralité, supposer que l'image $\mathcal{G}$ du sous-groupe $\mathcal{C}$ de $TG(k)$ par l'application $\exp_{G(k)}$ est contenue dans l'ouvert affine G_0 défini par $X_0 \neq 0$. C'est dans ce cadre que nous nous plaçons désormais.

(5) Pour plus de détails sur l'application logarithme et les applications exponentielles des groupes de Lie ultramétriques, on pourra consulter "Lie algebras and Lie groups", de J-P. Serre, ainsi que le chapitre III (en particulier les §§ 4 et 7) de "Groupes et algèbres de Lie", de N. Bourbaki et la notice historique qui s'y réfère. Voir également J.I. Igusa, Proc. Nat. Ac. Sc., 42, 1956, pp. 540-541, pour le cas des groupes commutatifs, et [Be 5], pour les propriétés métriques des exponentielles sur les variétés abéliennes.

(6) "Quelques propriétés des groupes algébriques commutatifs", par J-P. Serre (noté [S] dans ce qui suit).

Afin de représenter $\exp_{G(k)}$ par des fonctions (strictement analytiques) de g variables, nous fixons une base $\mathcal{D} = \{D_1,\dots,D_g\}$ de $TG(k)$ formée d'éléments de $TG(F)$ (ceci est licite, car $TG(F)$ est une F-structure sur $TG(k)$ - voir [Bo], chapitre AG, § 11), et nous identifions k^g à $TG(k)$ par un isomorphisme h appliquant $\mathcal{O}^g$ dans $\mathcal{E}$ et tel que, pour $i=1,\dots,g$, $d(\exp_{G(k)} \circ h)(\partial/\partial z_i)$ et D_i soient F-linéairement dépendants. On dira alors que le système de fonctions

$$\varepsilon_{\mathcal{D}} = \{f_i = (X_i / X_o) \circ \exp_{G(k)} \circ h \,;\, i = 1,\dots,N\}$$

est une représentation analytique normalisée de $\exp_{G(k)}$. Il est formé d'éléments de $\mathcal{K}(\mathcal{O}^n)$. De plus, le choix du plongement projectif ψ mentionné ci-dessus permet d'affirmer (voir [W], proposition 1.2.3) que l'algèbre $F[f_1,\dots,f_N]$ est stable par les opérateurs $\partial/\partial z_1,\dots,\partial/\partial z_g$.

Exemple : Soit A une courbe elliptique définie sur F, dont l'image par ψ soit la cubique d'équation $X_o^2 X_2 - 4X_1^3 + g_2 X_1 X_2^2 + g_3 X_2^3 = 0$. Une représentation analytique normalisée de l'exponentielle $\mathfrak{p}$-adique sur A est donnée par le système

$$f_1(z) = (\wp/\wp')(pz),\ f_2(z) = (1/\wp')(pz)$$

où $\wp$ et $\wp' = (d/dz)\wp$ désignent les fonctions elliptiques de Weil-Lutz associées aux images de g_2 et g_3 dans k[7].

Considérons, plus généralement, un sous-groupe φ à n paramètres de $G(k)$. La commutativité de G, jointe aux remarques préliminaires, permet de se limiter à l'étude des homomorphismes

$$\varphi = \exp_{G(k)} \circ \mathcal{L},$$

où $\mathcal{L}$ est un élément de $\mathrm{End}_k(k^n, TG(k))$ appliquant $\mathcal{O}^n$ dans $\mathcal{E}$.

Définition 7 - Un sous-groupe à n paramètres de $G(k)$ sera dit normalisé si sa différentielle à l'origine est un élément de $\mathrm{End}_F(TF^n, TG(F))$

Les propriétés fonctionnelles des sous-groupes à plusieurs paramètres de $G(k)$ résultent des formules d'addition et de multiplication suivantes, qui généralisent, en le précisant, un résultat d'Altman sur les variétés abéliennes (voir [Al], théorème 3.5). On note I l'anneau des entiers du corps de nombres F.

LEMME 7 - Il existe un nombre réel C_n ne dépendant que de G, ψ et n, et vérifiant la propriété suivante. Pour tout élément $P = (P_1,\dots,P_n)$ de G^n, et tout élément $\nu = (\nu_1,\dots,\nu_n)$ de $\mathbf{N}^n$, il existe un voisinage de Zariski $\mathcal{V}_{P,\nu}$ de P

(7) Voir A.Weil, C.R.A.S. Paris, 203,1936, pp. 22.24; E. Lutz, J. Crelle, 177, 1937, pp. 238-247 ; et [Be 4].

dans G^n, et un $(N+1)$-uple

$$F_{P,\nu} = (F_{o,P,\nu},\dots,F_{N,P,\nu})$$

de polynômes n-homogènes en $(N+1)n$ variables X_{sj} $(s=0,\dots,N\,;\,j=1,\dots,n)$, à coefficients dans I, de degrés $\leq C_n\|\nu\|^2$ par rapport à chaque $(N+1)$-uple de variables $(X_{o,j},\dots,X_{N,j})$, de hauteurs $\leq \exp(C_n(1+\|\nu\|^2))$, tels que, pour tout élément $Q=(Q_1,\dots,Q_n)$ de $\mathcal{V}_{P,\nu}$, le point $\nu_1 Q_1 + \dots + \nu_n Q_n$ admette pour système de coordonnées projectives :

$$\{X_i(\nu_1 Q_1 + \dots + \nu_n Q_n) = F_{i,P,\nu}(X_s(Q_j)\,;\, s = 0,\dots,N\,;\, j=1,\dots,n)\,;\, i=0,\dots,N\}.$$

La démonstration du lemme 7 est donnée au § 4.1.b. On en déduit l'énoncé suivant, relatif à la donnée de n endomorphismes $\pi_1,\dots,\pi_n$ de $\mathcal{O}^n$ quelconques.

COROLLAIRE - Soit $\varphi : \mathcal{O}^n \to G(k)$ un sous-groupe à n paramètres de $G(k)$. Alors le système $\{\varphi_1,\dots,\varphi_N\}$ d'éléments de $\mathcal{K}(\mathcal{O}^n)$ représentant φ dans les coordonnées affines $\{X_i/X_o\,;\, i = 1,\dots,N\}$ est d'ordre arithmétique fonctionnel fini. Plus précisément, le nombre ρ (resp. le corps K) qui lui est associé par la définition 1 peut être choisi égal à 2 (resp. à F). Enfin, tout point de $\mathcal{O}^n$ est régulier pour $\{\varphi_1,\dots,\varphi_N\}$.

Démonstration - Soient ζ un point de $\mathcal{O}^n$, et $P = (P_1,\dots,P_n)$ l'élément de $G^n(k)$ défini, pour $j = 1,\dots,n$, par

$$P_j = \varphi \circ \pi_j(\zeta).$$

Soit par ailleurs $\nu = (\nu_1,\dots,\nu_n)$ un élément de $\mathbf{N}^n$, et posons, avec les notations du lemme 7 :

$$R_{i,\nu}(x_{sj},\, s = 1,\dots,N\,;\, j = 1,\dots,n) = F_{i,P,\nu}(\xi_{sj}\,;\, s = 0,\dots,N\,;\, j=1,\dots,n),$$

$$S_\nu(x_{sj}\,;\, s = 1,\dots,N\,;\, j = 1,\dots,n) = F_{o,P,\nu}(\xi_{sj}\,;\, s = 0,\dots,N\,;\, j=1,\dots,n),$$

où $\xi_{sj} = x_{sj}$ (resp. $\xi_{oj} = 1$) pour $s = 1,\dots,N$ (resp. $s = 0$).

Puisque $\mathcal{G}$ est un sous-groupe de $G(k)$ contenu dans $G_o(k)$, les points $P_1,\dots,P_n$ et $\nu_1 P_1 + \dots + \nu_n P_n$ n'appartiennent pas au diviseur d'équation $X_o = 0$. En particulier, $S_\nu\left(\frac{X_s(P_j)}{X_o(P_j)}\,;\, s = 1,\dots,N\,;\, j = 1,\dots,n\right)$ est non nul, et l'on a, pour $i = 1,\dots,N$:

$$\varphi_i(\tau_\nu(\zeta)) = \frac{X_i}{X_o} \circ \varphi(\nu_1 \pi_1(\zeta) + \dots + \nu_n \pi_n(\zeta)) = \frac{R_{i,\nu}(\underset{\sim}{\varphi}_1(\zeta),\dots,\underset{\sim}{\varphi}_N(\zeta))}{S_\nu(\underset{\sim}{\varphi}_1(\zeta),\dots,\underset{\sim}{\varphi}_N(\zeta))}.$$

Soient enfin $\mathcal{V}_{P,\nu}(k)$ l'ouvert de $G^n(k)$ formé des points k-rationnels de l'ouvert de Zariski $\mathcal{V}_{P,\nu}$ et $\mathcal{V}$ l'image réciproque par l'application $\underset{\sim}{\varphi} = (\varphi \circ \pi_1, \ldots, \varphi \circ \pi_n)$ de la trace de $\mathcal{V}_{P,\nu}(k)$ sur l'ensemble $\underset{\sim}{\varphi}(\mathcal{O}^n)$. D'après la remarque précédente, le polynôme S_ν ne s'annule en aucun point de $\underset{\sim}{\varphi}(\mathcal{V})$, et l'on a, pour tout élément z de $\mathcal{V}$:

$$\varphi_i(\tau_\nu(z)) = (R_{i,\nu}/S_\nu)(\underset{\sim}{\varphi}_1(z), \ldots, \underset{\sim}{\varphi}_N(z)).$$

Comme $\mathcal{V}$ est un ouvert non vide de $\mathcal{O}^n$, on en déduit les équations fonctionnelles

$$T_\nu \varphi_i = \frac{R_{i,\nu}(\underset{\sim}{\varphi}_1, \ldots, \underset{\sim}{\varphi}_N)}{S_\nu(\underset{\sim}{\varphi}_1, \ldots, \underset{\sim}{\varphi}_N)} \quad (i = 1, \ldots, N).$$

D'après le lemme 7, la famille $\{\varphi_1, \ldots, \varphi_N\}$ est donc d'ordre arithmétique fonctionnel fini (relativement à $\pi_1, \ldots, \pi_n$), et la construction précédente montre que le point ζ est régulier pour $\{\varphi_1, \ldots, \varphi_N\}$.

<u>Remarque</u> 4 - Le lemme 7 fournit une démonstration indirecte de la proposition 5 de [S]. Son corollaire entraîne en particulier que, pour tout sous-groupe Γ de $\mathcal{O}^n$ tel que $\varphi(\Gamma)$ soit inclus dans $G(F)$, les fonctions $\varphi_1, \ldots, \varphi_N$ sont d'ordre arithmétique inférieur ou égal à 2 sur Γ.

b) <u>Démonstration du lemme</u> 7.

La démonstration du lemme 7 repose sur le corollaire 2 de la proposition 3 de [S], et sur la formule d'addition suivante, qui résulte de la définition des groupes algébriques, jointe à leur quasi-compacité.

(*) il existe un nombre réel c_o, ne dépendant que de G et de ψ, et vérifiant la propriété suivante. Pour tout élément (P_1, P_2) de $G \times G$, il existe un voisinage $\mathcal{U}_{P_1,P_2}$ de (P_1, P_2) dans $G \times G$, et un $(N+1)$-uple

$$\mathcal{F}_{P_1,P_2} = (\mathcal{F}_{o,P_1,P_2}, \ldots, \mathcal{F}_{N,P_1,P_2})$$

de polynômes bihomogènes en $2(N+1)$ variables, à coefficients dans I, de degré $\leq c_o$ par rapport à chaque $(N+1)$-uple de variables, de hauteur $\leq \exp(c_o)$, tel que, pour tout élément (Q_1, Q_2) de $\mathcal{U}_{P_1,P_2}$, le point Q_1+Q_2 admette pour système de coordonnées projectives :

$$\{X_i(Q_1+Q_2) = \mathcal{F}_{i,P_1,P_2}(X_o(Q_1), \ldots, X_N(Q_1)\ ;\ X_o(Q_2), \ldots, X_N(Q_2))\ ;\ i = 0, \ldots, N\}.$$

On rappelle d'autre part que la hauteur du produit de k éléments $F_1, \ldots, F_k$ de $I[X_o, \ldots, X_N]$ vérifie l'inégalité :

$$H(F_1 \ldots F_k) \leq \prod_{i=1}^{k} (H(F_i) \prod_{j=o}^{N} (1 + \deg_{X_j} F_i)).$$

Démontrons tout d'abord le lemme 7 lorsque $n=1$. Fixons un entier $\ell > \sup(\sqrt{c_o}, 2)$. Pour $a = 0, \ldots, \ell$, on note :

$$\varphi^{(a)} = (\varphi_o^{(a)}, \ldots, \varphi_N^{(a)})$$

l'un des $(N+1)$-uples de polynômes homogènes à coefficients dans I, de degré a^2, qui expriment la loi de multiplication par a sur G, et dont l'existence est assurée par le corollaire 2 de la proposition 3 de [S]. On désigne par $c_1, \ldots, c_4$ des nombres réels > 0 ne dépendant que de c_o, N, ℓ, et $\varphi^{(o)}, \ldots, \varphi^{(\ell)}$.

Considérons la suite de $(N+1)$-uples de polynômes homogènes

$$\varphi_{\ell^m} = (\varphi_{o,\ell^m}, \ldots, \varphi_{N,\ell^m})$$

définis par récurrence sur m par les relations :

$$\varphi_{i,1} = X_i\ ;\ \varphi_{i,\ell^{m+1}} = \varphi_i^{(\ell)}(\varphi_{o,\ell^m}, \ldots, \varphi_{N,\ell^m}) \quad (i = 0, \ldots, N).$$

Pour tout point Q de G, et tout entier $m > 0$, le point $\ell^m Q$ admet, d'après [S], pour système de coordonnées projectives :

$$X_i(\ell^m Q) = \varphi_{i,\ell^m}(X(Q)) \quad (i = 0, \ldots, N).$$

Par ailleurs, on vérifie par récurrence sur $m > 0$ que les polynômes φ_{i,ℓ^m} sont de degré $\leq \ell^{2m}$, et de hauteur $\leq \exp(2c_2\,\ell^{2m} - c_2\,\ell^m)$, où

$$c_2 = 3(\ell^2+1)(N+1)\log(1+\ell) + \max_{i=0,\ldots,N} \log H(\varphi_i^{(\ell)}).$$

Pour $a = 1, \ldots, \ell-1$, et $m \geq 0$, posons alors :

$$\varphi_{a\ell^m} = \varphi_{\ell^m} \circ \varphi^{(a)}.$$

Les composantes de $\varphi_{a\ell^m}$ sont des polynômes homogènes de degré $\leq c_3\,\ell^{2m}$, de hauteur $\leq \exp(c_3 \ell^{2m})$, et, pour tout point Q de G, le point $a\ell^m Q$ admet pour système de coordonnées projectives $\{\varphi_{a\ell^m}(X(Q))\}$, en vertu de la définition de $\varphi^{(a)}$.

Pour tout entier $t \geq 0$, soit enfin $\mathcal{L}_t$ l'ensemble des entiers $\nu > 0$ tels que $[(\log \nu)/(\log \ell)] = t$. Tout élément ℓ_t de $\mathcal{L}_t$ s'écrit de façon unique sous la forme $a\ell^t + \ell_{t-1}$, où $a \in \{1, \ldots, \ell-1\}$ et $\ell_{t-1} \in \mathcal{L}_{t-1} \cup \{0\}$. Pour tout point P de G, on définit, par récurrence sur t, un voisinage $\mathcal{V}_{P,\ell_t}$ de P dans G

et un $(N+1)$-uple F_{P,ℓ_t} de polynômes homogènes de la façon suivante : si $\ell_{t-1}=0$, alors, $\mathcal{V}_{P,\ell_t} = G$ et $F_{P,\ell_t} = \varphi_{\ell_t}$; dans les autres cas, $\mathcal{V}_{P,\ell_t}$ est la trace sur $\mathcal{V}_{P,\ell_{t-1}}$ de l'image réciproque de l'ouvert $\mathcal{U}_{a\ell^t P, \ell_{t-1} P}$ par le morphisme de G dans $G \times G$ défini par

$$Q \to (a\ell^t\, Q\,,\, \ell_{t-1} Q),$$

et

$$F_{P,\ell_t} = \mathcal{F}_{a\ell^t P,\ell_{t-1}P}\,(\varphi_{a\ell^t}\,,\, F_{P,\ell_{t-1}}).$$

D'après la formule d'addition (*) et les étapes précédentes, le multiple $\ell_t Q$ d'un point Q de $\mathcal{V}_{P,\ell_t}$ admet pour système de coordonnées projectives

$$\{X_i\,(Q) = F_{i,P,\ell_t}\,(X(Q))\ ;\ i = 0,\dots, N\}.$$

On vérifie alors, par récurrence sur t, que, pour $\ell_t \in \mathcal{L}_t$, les polynômes F_{i,P,ℓ_t} sont de degré inférieur ou égal à

$$c_o c_3 \ell^{2t} + c_o c_3 \sum_{j=0}^{t-1} c_o^{j+1}\, \ell^{2(t-1-j)} = c_3 \sum_{j=0}^{t} c_o^{j+1}\, \ell^{2(t-j)}\ ,$$

et de hauteur

$$H(F_{i,P,\ell_t}) \leqq \exp\Big(c_4 \sum_{j=0}^{t} c_o^{j+1}\, \ell^{2(t-j)}\Big),$$

où c_4 satisfait à l'inégalité :

$$c_4 \geqq \max\,(2\,c_3\,,\ 6\,(N+1)c_o \log\,(1 + c_o c_4 \ell)).$$

Or ℓ^2 est $> c_o$. Le choix

$$C_1 = (c_4\, c_o\, \ell^2 / (\ell^2 - c_o)) + \max_{i=0,\dots,N} \log H\,(\varphi_i^{(o)})$$

permet alors de conclure la preuve du lemme 7, dans le cas $n=1$.

Le cas général se traite par récurrence sur n. Pour tout élément $P = (P_1,\dots,P_n)$ de G^n, et tout élément $\nu = (\nu_1,\dots,\nu_n)$ de $\mathbf{N}^n$, on note $\mathcal{V}_{P,\nu}$ la trace sur l'ouvert $\mathcal{V}_{(P_1,\dots,P_{n-1})\,,\,(\nu_1,\dots,\nu_{n-1})} \times \mathcal{V}_{P_n,\nu_n}$ de l'image réciproque de l'ouvert $\mathcal{U}_{\nu_1 P_1+\dots+\nu_{n-1} P_{n-1}\,,\,\nu_n P_n}$ par le morphisme de G^n dans $G \times G$ défini par

$$(Q_1,\dots,Q_n) \to (\nu_1 Q_1 + \dots + \nu_{n-1} Q_{n-1}\,,\ \nu_n Q_n),$$

et on pose

$$F_{P,\nu} = \mathcal{F}_{\nu_1 P_1+\dots+\nu_{n-1} P_{n-1}\,,\,\nu_n P_n}\,(F_{(P_1,\dots,P_{n-1})\,,\,(\nu_1,\dots,\nu_{n-1})}\,,\ F_{P_n,\nu_n}).$$

Alors, $\mathcal{V}_{P,\nu}$ est un voisinage de P dans G^n, et les pas précédents de la récurrence, joints à la formule d'addition (*), entraînent que, pour tout élément $(Q_1,\dots,Q_n)$ de $\mathcal{V}_{P,\nu}$, le point $\nu_1 Q_1+\dots+\nu_n Q_n$ admet pour système de coordonnées projectives :

$$\{X_i\,(\nu_1 Q_1+\dots+\nu_n Q_n) = F_{i,P,\nu}\,(X(Q_1),\dots, X(Q_n))\ ;\ i = 0,\dots,N\}.$$

On vérifie enfin que les polynômes $F_{i,P,\nu}$ sont de degré par rapport à $X(Q_j)$ inférieur ou égal à

$$\sup(c_o\, C_{n-1}\,(\nu_1+\dots+\nu_{n-1})^2\,,\ c_o\, C_1 \nu_n^2) \leqq c_o\,(C_1 + C_{n-1})\,\|\nu\|^2\,,$$

et de hauteur inférieure ou égale à

$$(1+c_o)^{2(N+1)}\, e^{c_o}\,(1 + (C_1 + C_{n-1})\,\|\nu\|^2)^{n\, c_o (N+1)}\ \exp(c_o\,(1+(C_1 + C_{n-1})\,\|\nu\|^2)).$$

Il existe donc un nombre réel C_n répondant aux conditions du lemme 7.

§ 4.2 - Sous-groupes à plusieurs paramètres normalisés.

On rapprochera l'énoncé obtenu dans cette situation du théorème 5.2.1 de [W]. On rappelle que la dimension algébrique d'un sous-groupe à n paramètres désigne la dimension de la clôture de Zariski de son image.

THÉORÈME FONDAMENTAL I : Soient G un groupe algébrique commutatif connexe, défini sur un corps de nombres, φ un sous-groupe à n paramètres normalisé de $G(k)$, et Γ un sous-groupe de $\mathcal{O}^n$ contenant n éléments k-linéairement indépendants, dont les images par φ appartiennent à $G(\overline{\mathbb{Q}})$. On fait de plus l'hypothèse suivante :

(H) il existe un élément u de $\mathcal{O}^n$, et n endomorphismes $\pi_1,\dots,\pi_n$ de $\mathcal{O}^n$, définis sur $\overline{\mathbb{Q}}$, tels que, pour tout n-uple $(\nu_1,\dots,\nu_n)$ d'entiers > 0, l'endomorphisme $\nu_1\pi_1+\dots+\nu_n\pi_n$ soit injectif, et tels que les points $\pi_1(u),\dots,\pi_n(u)$ engendrent Γ.

Alors, la dimension algébrique de φ est $\leqq n$.

Démonstration : (On reprend les notations du corollaire du lemme 7). D'après le choix du plongement projectif ψ, et puisque φ est normalisé, tout élément de Lie (F^n) opère sur l'algèbre $\overline{\mathbb{Q}}\,[\varphi_1,\dots,\varphi_N]$. Les endomorphismes $d\pi_1,\dots,d\pi_n$ étant définis sur $\overline{\mathbb{Q}}$, la même propriété est satisfaite par l'algèbre $\overline{\mathbb{Q}}\,[\varphi_i \circ \pi_j\ ;\ i=1,\dots,N\ ;\ j=1,\dots,n]$. Dans ces conditions, le corollaire du lemme 7 montre que les hypothèses du théorème 1 sont satisfaites par le système $\{\varphi_1,\dots\varphi_N\}$

et le point u. Puisque chacune des fonctions $\varphi_i \circ \pi_j$ $(i=1,\dots,N;\ j=1,\dots,n)$ y prend une valeur algébrique, le degré de transcendance de l'algèbre $\bar{\mathbb{Q}}[\varphi_1,\dots,\varphi_N]$ est $\leq n$.

Il est probable que, dans l'énoncé du théorème I, l'hypothèse (H) soit superflue. Dans le cas $n=1$, elle est automatiquement vérifiée, et ce théorème permet de retrouver les résultats de K. Mahler sur les propriétés arithmétiques de la fonction exponentielle $\mathfrak{p}$-adique ordinaire (analogues des théorèmes de Hermite-Lindemann [8] et de Gel'fond-Schneider [9] ; il contient donc les analogues $\mathfrak{p}$-adiques des théorèmes 2.2.1, 2.2.2 et 2.3.1 de [W]). Plus généralement il fournit une version $\mathfrak{p}$-adique à tous les énoncés du chapitre 3 de [W] ne faisant pas intervenir de périodes.

Considérons maintenant le cas où G est une variété abélienne A définie sur un corps de nombres. Soient $\epsilon_{\mathfrak{p}}$ une représentation analytique normalisée de $\exp_{A(k)}$, et u un point nul de $\mathcal{O}^g$ où les composantes de $\epsilon_{\mathfrak{p}}$ prennent simultanément des valeurs algébriques. D'après [Be 3], proposition 2, l'une au moins des coordonnées de u est transcendante. Le théorème I permet de préciser cet énoncé sous certaines hypothèses sur l'algèbre d'endomorphismes $\mathrm{End}_o A$ de A.

Définition 8 - Soit A une variété abélienne simple de dimension g, définie sur un corps de nombres F. On dira que A est de type R.M. (multiplications réelles) s'il existe un plongement dans $\mathrm{End}_o A$ d'un corps totalement réel K de degré g sur $\mathbb{Q}$ (une variété abélienne de type C.M. est donc de type R.M.). Quitte à étendre F, on peut alors construire une base $\{D_1,\dots,D_g\}$ de $TA(F)$ formée de vecteurs propres pour l'action de K sur $TA(k)$. Une représentation analytique $\epsilon_{\mathfrak{p}}$ de l'application $\exp_{A(k)}$ sera dite fortement normalisée si elle correspond aux choix d'une telle base.

THÉORÈME 4 : Soient A une variété abélienne simple définie sur $\bar{\mathbb{Q}}$, de dimension g et de type R.M., $\epsilon_{\mathfrak{p}}$ une représentation analytique fortement normalisée de $\exp_{A(k)}$, et u un point non nul de $\mathcal{O}^g$ où les composantes de $\epsilon_{\mathfrak{p}}$ prennent simultanément des valeurs algébriques. Alors, chacune des coordonnées de u est transcendante.

La démonstration du théorème 4 reprend celle du théorème 6.1.1 de [W], où était déjà signalé le caractère surabondant de l'hypothèse C.M. Il suffit ici de noter que si $\tau_1,\dots,\tau_g$ désignent une base de l'anneau des entiers du corps K, et $\sigma_1,\dots,\sigma_g$ ses différents plongements dans k, la matrice $[(\sigma_i(\tau_j))\ ;\ 1\leq i, j\leq g]$ a un rang égal à g, puisque le carré de son déterminant est le discriminant du corps K. D'autre part, K étant un corps, tout endomorphisme non nul de k^n provenant de l'action de K sur $TA(k)$ est injectif.

(8) Voir K. Mahler, J. Crelle, 169, 1932 pp. 61-66.
(9) Voir K. Mahler, Compositio math., 2, 1935, pp. 259-275.

Remarque 5 - Bien entendu, l'analogue complexe du théorème 4 est également satisfait [10]. Il permet en particulier d'étudier les périodes de certaines formes modulaires de poids 2.

§ 4.3 - Sous-groupes non normalisés.

Nous rassemblons sous un seul énoncé les versions $\mathfrak{p}$-adiques des théorèmes 2.3.1, 2.5.1, 4.1.2, 4.2.1, 8.1.1 et 8.2.1 de [W].

THÉORÈME FONDAMENTAL II : Soient G un groupe algébrique commutatif connexe, défini sur $\bar{\mathbb{Q}}$, φ un sous-groupe à n paramètres de $G(k)$, de dimension algébrique d, et Γ un sous-groupe de $\mathcal{O}^n$ de rang fini ℓ sur $\mathbb{Z}$, tel que $\varphi(\Gamma)\subset G(\bar{\mathbb{Q}})$. Alors

i) le coefficient de densité de Γ vérifie

$$\varkappa(\Gamma, k^n)\,(d-n) \leq 2d\ ;$$

de plus, $2d$ peut être remplacé par d quand G est un groupe linéaire, et $\varkappa(\Gamma,k^n)$ par ℓ quand $n=1$;

ii) on suppose maintenant que Γ est formé d'éléments de $\bar{\mathbb{Q}}^n$, et que, pour tout élément non nul u de k^n, le sous-groupe à un paramètre $z\mapsto\varphi(zu)$ n'est pas rationnel. On a, dès que $\Gamma\subset \mathbb{Z}_p^n$:

$$\ell \leq 2n\ ;$$

de plus, $2n$ peut être remplacé par n quand G est un groupe linéaire, et l'hypothèse $\Gamma\subset\mathbb{Z}_p^n$ peut être supprimée quand $n=1$.

La démonstration de ce théorème repose sur le théorème 2, la proposition 2 et le lemme 3, joints aux techniques élaborées dans [W]. Elle n'offre pas de changement notoire par rapport au cas complexe, et nous l'omettrons.

La première partie du théorème II contient les résultats de Serre sur les caractères de $\mathcal{O}^n$ (voir [Se 3]) et un énoncé de Flicker sur les variétés abéliennes ([F], chapitre 3, § 5). La deuxième partie fournit une nouvelle démonstration de l'analogue $\mathfrak{p}$-adique du théorème de Gel'fond-Schneider [11]. Par ailleurs, elle admet, pour le sous-groupe $(z_1,\dots,z_n)\mapsto\alpha_1^{z_1}\cdots\alpha_n^{z_n}$ du groupe multiplicatif, le corollaire suivant (voir [W], § 8.3), où Log désigne la fonction logarithme $\mathfrak{p}$-adique.

PROPOSITION 5 - Soient $\alpha_1,\dots,\alpha_n$ des unités de $\mathcal{O}$ algébriques sur $\mathbb{Q}$, et multiplicativement indépendantes. Alors, les nombres $\mathrm{Log}\,\alpha_1,\dots,\mathrm{Log}\,\alpha_n$ sont linéairement indépendants sur $\bar{\mathbb{Q}}\cap\mathbb{Q}_p$.

(10) Voir D. Bertrand, C.R.A.S. Paris, 288, 1979, pp. 531-534.
(11) Voir Veldkamp, J. London Math. Soc., 15, 1940, pp. 183-192.

Nous verrons au paragraphe 4.5 comment la méthode de Baker permet d'améliorer certains des énoncés de ce paragraphe.

§ 4.4 - Variétés abéliennes dégénérantes

(On ne suppose plus ici k localement compact). Nous étudions maintenant les homomorphismes analytiques (au sens de la définition 5 du § 3.2) d'une puissance du groupe multiplicatif dans un groupe algébrique. La situation la mieux connue concerne les variétés abéliennes dégénérantes. Plus précisément, soit Γ un sous-groupe discret libre et de rang maximal de $(k^*)^g$, qui vérifie les conditions de Riemann. Alors, l'espace holomorphe $(k^*)^g/\Gamma$ est isomorphe à une variété abélienne [12] $A_\Gamma(k)$. Dans un sytème de coordonnées associé à un plongement projectif ψ de A_Γ, tout homomorphisme analytique de $(k^*)^g$ dans $A_\Gamma(k)$ s'exprime par une famille $\{\theta_o,\ldots,\theta_N\}$ de fonctions thêta. Ces fonctions sont analytiques sur $(k^*)^g$, et leurs équations fonctionnelles montrent qu'elles sont d'ordre inférieur ou égal $\{0,2\}$.

L'énoncé suivant est dû (sous une formulation différente) à Flicker (voir [F], chapitre 5). Il généralise le théorème 2 de [Be 1], qui concernait les courbes elliptiques de Tate.

THÉORÈME FONDAMENTAL III - Soient A_Γ une variété abélienne dégénérante de dimension g, définie sur un corps de nombres, χ un homomorphisme analytique de $(k^*)^g$ sur $A_\Gamma(k)$ dont la dérivée à l'origine est injective, et $\{D_1,\ldots,D_g\}$ une base de Lie $(k^*)^g$ définie sur $\bar{\mathbb{Q}}$. Alors, l'une au moins des dérivations $d\chi(D_i)$ $(i=1,\ldots,g)$ de Lie $A_\Gamma(k)$ n'est pas définie sur $\bar{\mathbb{Q}}$.

Démonstration - Considérons un plongement projectif ψ de A_Γ, défini sur $\bar{\mathbb{Q}}$, et tel que $\psi\circ\chi(1,\ldots,1)=(1,0,\ldots,0)$, et soit $\{\theta_o,\ldots,\theta_N\}$ la représentation analytique de χ associée à ψ. On peut, sans restreindre la généralité, supposer que la base $\{D_1,\ldots,D_g\}$ est formée de vecteurs $\{z_1\,\partial/\partial z_1,\ldots,z_g\,\partial/\partial z_g\}$. Dans ces conditions, les fonctions $f_o(z)=z_1$, $f_1(z)=(\theta_1/\theta_o)(z),\ldots,f_N(z)=(\theta_N/\theta_o)(z)$ prennent simultanément des valeurs dans $\bar{\mathbb{Q}}$ au point $(1,\ldots,1)$. En vertu du théo-

(12) L'étude analytique de ces variétés, initiée par Tate dans le cas des courbes elliptiques (voir P. Roquette : Analytic Theory of elliptic functions over local fields, Hamburger Math. Einzelschr. 1, 1970) et par Morikawa (Nagoya Math. J., 20, 1962, pp. 1-27 et 231-250) dans le cas général, a été en particulier poursuivie par Mc Cabe (Ph. D. Thesis, Harvard, 1968), Raynaud (Actes C.I.M., Nice, 1970, 1, pp. 473-477), Mumford (Compo. Math. 24, 1972, pp. 239-271) et Gerritzen (Math. Ann., 196, 1972, 323-346). Les techniques de géométrie analytique rigide développées par ces derniers auteurs sont résumées dans un exposé de M. Van der Put paru au Groupe d'étude d'Analyse ultramétrique, Paris, 1975/76, fasc 2, n° J 7. Pour une approche plus élémentaire, voir H. Tapia-Recillas, Nagoya Math. J., 69, 1978, pp. 65-96.

rème 3, les dérivations $D_1,\ldots,D_g$ ne peuvent pas laisser stable l'algèbre $\bar{\mathbb{Q}}[f_o,\ldots,f_N]$, dont le degré de transcendance sur $\mathbb{Q}$ est égal à $g+1$, ni donc l'algèbre $\bar{\mathbb{Q}}[f_1,\ldots,f_N]$.

Le théorème III exprime que les dérivées logarithmiques des quotients $\theta_1/\theta_o,\ldots,\theta_N/\theta_o$, relativement aux opérateurs $D_1,\ldots,D_g$, ne peuvent toutes prendre des valeurs algébriques en l'origine de $(k^*)^g$. Cet énoncé concerne donc en fait les valeurs de formes modulaires [13]. On obtient ainsi, dans le cas des courbes elliptiques (voir [Be 1], théorème 2 ; et [W], § 3.2).

COROLLAIRE - Soient E_4 et E_6 les séries d'Eisenstein normalisées de poids 4 et 6, et q un élément de k tel que $0<|q|<1$. Alors, l'un au moins des nombres $E_4(q)$, $E_6(q)$ est transcendant.

Il serait très intéressant de démontrer, sous les hypothèses du théorème III, la transcendance de chacune des dérivations $d_\chi(D_i)$, et d'en expliciter d'autres corollaires, par exemple pour les formes modulaires de Hilbert.

Remarque 6 - Soit E_2 la série d'Eisenstein normalisée de "poids" 2. En considérant la dérivée logarithmique d'une fonction thêta associée à la courbe elliptique $A_{<q>}$, on déduit de la proposition 3 que l'un au moins des nombres $(E_4^3/E_6^2)(q)$, $(E_2\,E_4/E_6)(q)$ est transcendant (voir [Be 6], lemme 2). Plus généralement [14], on montre que, pour tout élément q de k tel que $0<|q|<1$, le corps $\mathbb{Q}(E_2(q), E_4(q), E_6(q))$ a un degré de transcendance $\geqq 2$ sur $\mathbb{Q}$.

Les résultats précédents ne permettent pas d'étudier les valeurs de l'invariant modulaire $J(q)$ lorsque q est algébrique (voir [Man], § 5 ; et [Be 6], conjectures 1 et 2). La proposition 6 fournit une autre approche de cette question (cf. [W], corollaire 4.2.6).

PROPOSITION 6 - Soient χ un homomorphisme analytique non constant de k^* sur une courbe elliptique de Tate d'invariant $J(q)$ algébrique, et u un élément de k^* algébrique sur $\mathbb{Q}$, qui n'est pas racine de l'unité. Alors, q et $\chi(u)$ ne peuvent être tous deux définis sur $\bar{\mathbb{Q}}$.

La proposition 6 découle de la proposition 4, appliquée au groupe Γ engendré par q et u.

§ 4.5 - Problèmes d'indépendance linéaire

Les démonstrations des résultats établis jusqu'à présent n'ont fait intervenir que des variantes des méthodes de Gel'fond et de Schneider (voir [Wa 2], chapitres

(13) Voir par exemple A. Weil, Comm. P.A. Maths., 39, 1976, pp. 813-819, et G. Shimura, Duke Math. J., 44, 1977, pp. 365-387.
(14) Voir D. Bertrand, Astérisque, 61, 1979, pp.29-34.

2 et 3). Nous passons maintenant en revue les résultats que fournit la méthode de Baker. Ce sont essentiellement les énoncés du § 4.3 qu'elle permet d'améliorer. Ainsi, on aura bien entendu reconnu, dans la conclusion de la proposition 5, un cas particulier d'un résultat de Brumer ([Bru], théorème 1), qui obtenait en 1967 une version $\mathfrak{p}$-adique du théorème de Baker (voir [W], théorème 1.1.9) dans le cas homogène. Plus généralement, on a (15) :

THÉORÈME 5 - Soient $\alpha_1,\dots,\alpha_n$ des unités de $\mathcal{O}$ algébriques sur $\mathbb{Q}$, et multiplicativement indépendantes. Alors, les nombres $\mathrm{Log}\,\alpha_1,\dots,\mathrm{Log}\,\alpha_n$ et 1 sont linéairement indépendants sur $\overline{\mathbb{Q}}$.

En vertu du théorème 5, l'hypothèse $\Gamma \subset \mathbb{Z}_p^n$ de la 2ème partie du théorème II peut être supprimée lorsque G est un groupe linéaire, la conclusion demeurant : $\ell \leq n$ (voir [W], théorème 2.5.1). On obtient également les analogues $\mathfrak{p}$-adiques des théorèmes 2.4.1 et 2.4.2 de [W].

Une version $\mathfrak{p}$-adique des résultats de Masser, Coates et Lang sur les variétés abéliennes de type CM (voir [W], théorème 6.2.3 et [M2]) a été obtenue dans [B-F] (16). Contrairement à celle du théorème 4, sa démonstration repose sur le lemme 5 du § 2.3 et met en jeu des hypothèses métriques qui ne sont satisfaites que sous certaines conditions sur $\mathfrak{p}$. On note $\{e_1,\dots e_g\}$ la base canonique de k^g et p le nombre premier que divise $\mathfrak{p}$.

THÉORÈME 6 - Soient A une variété abélienne simple de dimension g, définie sur un corps de nombres F, et telle que $\mathrm{End}_0 A$ soit isomorphe à une extension quadratique totalement imaginaire L d'un corps totalement réel K de degré g. On note $\epsilon_{\mathfrak{P}}$ une représentation analytique fortement normalisée de l'application $\exp_{A(k)}$, et $u_1,\dots,u_\ell$ des éléments de $\mathcal{O}^g$, linéairement indépendants sur $\mathrm{End}_0 A$, où les composantes de $\epsilon_{\mathfrak{P}}$ prennent simultanément des valeurs algébriques. On suppose que p se décompose totalement dans K, et que les idéaux de K divisant p ont le même type de décomposition dans L. Alors $e_1,\dots,e_g,u_1,\dots,u_\ell$ sont linéairement indépendants sur $(\mathrm{End}_0 A)_{\overline{\mathbb{Q}}}$.

La condition imposée à p est indésirable, bien qu'on puisse la rapprocher de l'hypothèse faite sur les places à l'infini de L.. Une conjecture générale concernant ce problème est proposée dans [Be 5].

COROLLAIRE - On reprend les hypothèses 6, et on note φ un sous-groupe à un paramètre de $A(k)$. S'il existe deux nombres algébriques $\mathbb{Q}$-linéairement indépendants dont les images par φ appartiennent à $A(\overline{\mathbb{Q}})$, alors A est une courbe elliptique.

(15) Pour un aperçu historique de la théorie des formes linéaires de logarithmes $\mathfrak{p}$-adiques, voir A. van der Poorten, chapitre 2 de [Ba-M], § 1.

(16) Le cas des courbes elliptiques avait été traité dans [Be 4].

La démonstration de ce corollaire est identique à celle du théorème 6.3.1 de [W]. On peut néanmoins éviter le passage aux périodes complexes en remarquant qu'avec les notations de [W], le corps $\mathbb{Q}(\gamma)$ est une extension quadratique de $\mathbb{Q}$ incluse dans L. De plus, les restrictions à $\mathbb{Q}(\gamma)$ des plongements de L dans $\overline{\mathbb{Q}}$ qui définissent le "type C.M." de la variété abélienne A se confondent. Ceci contredit (17) la simplicité de A .

V - APPLICATIONS

Nous rassemblons au paragraphe 5.1 les applications à l'étude des corps de nombres des énoncés de transcendance établis ci-dessus. Les résultats obtenus sont de nature qualitative. En revanche, les applications décrites au paragraphe 5.2 font appel à des versions quantitatives des résultats de [W] et de leurs analogues $\mathfrak{p}$-adiques.

§5.1 - Arithmétique des corps de nombres

Le théorème II i) du paragraphe 4.3 (voir [Se 3]) a été utilisé par Serre, dans ses travaux sur les représentations p-adiques, pour démontrer le résultat suivant ([Se 4], chapitre 3, § 3.1) :

Soient K un corps de nombres, et ρ une représentation abélienne p-adique, rationnelle et semi-simple, de $\mathrm{Gal}\,(K^{alg}/K)$. On suppose que K est un compositum d'extensions quadratiques. Alors, ρ est localement algébrique.

Une version plus forte du théorème II permettrait d'étendre cet énoncé à tous les corps des nombres (voir [Se 4], chapitre 3, p.27). On pourra rapprocher ce problème de la question posée à la remarque 2 du § 2.4 (voir également [W], § 8.2.c.).

Le lien entre le problème de Leopoldt sur le régulateur p-adique des corps de nombres totalement réels et le 7ème problème de Hilbert a été noté par Ax (18). Les résultats de transcendance, dûs à Mahler, que contient le théorème 1 du § 4.2, lui ont permis de traiter le cas des extensions abéliennes de $\mathbb{Q}$ d'exposant ≤ 4 ou égal à 6. Le théorème 5 du § 4.5 (voir [Br]) entraîne ([Br], théorème 2) :

Soient K une extension abélienne de $\mathbb{Q}$, et p un nombre premier. Le régulateur p-adique de K n'est pas nul.

Les questions de transcendance posées par le cas général sont décrites aux §§ 2.5 et 8.2 de [W]. D'autres approches du problème sont d'ailleurs possibles (19).

(17) Voir par exemple D. Mumford, "Abelian varieties", p. 214.
(18) J. Ax, Illinois J. of Math., 9, 1969, pp. 584-589.
(19) Voir J-P. Serre, C.R.A.S. Paris, 1978, 287, pp. 183-188 (théorème 3.14)

Signalons enfin une récente application du théorème 5 à l'étude des fonctions L p-adiques de Kubota et Leopoldt $L_p(s,\psi)$ associées aux caractères de Dirichlet à valeurs dans C_p. Elle est due à Ferrero et Greenberg[20] :

Soit ψ un caractère de Dirichlet primitif impair. La fonction $L_p(s,\psi)$ ne peut admettre le point $s=0$ pour zéro d'ordre 2.

§ 5.2 Géométrie diophantienne

Soient C une courbe algébrique de genre $\geqq 1$, définie sur un corps de nombres K, et φ une fonction K-rationnelle sur C. On se propose d'étudier la variation du plus grand facteur premier $\pi_\varphi(P)$ du dénominateur de $\varphi(P)$ en fonction de la hauteur $H_\varphi(P)$ de $\varphi(P)$. D'après le théorème de Siegel-Mahler-Lang, dont la démonstration n'est pas effective, $\pi_\varphi(P)$ croît avec $H_\varphi(P)$.

Pour plusieurs classes de courbes, les énoncés quantitatifs de la théorie des formes linéaires de logarithmes (qui précisent le théorème 1.1.9 de [W] et le théorème 5 du § 4.5) fournissent une réponse entièrement effective au problème. Nous renvoyons au chapitre 3 de [Ba-M], où sont passés en revue les différents résultats acquis par cette méthode. Mentionnons toutefois l'énoncé suivant, dû à Coates[21] et qui permet en principe de déterminer, à isomorphisme près, toutes les courbes elliptiques de conducteur donné[22] :

Si x et y sont des entiers premiers entre eux de module $\leqq X$, le plus grand facteur premier de $y^2 - x^3$ est minoré par $10^{-3}(\log\log X)^{1/4}$.

La théorie des formes linéaires d'intégrales abéliennes (qui répond au théorème 6.2.3 de [W] et au théorème 6 du § 4.5) permet également d'étudier certains types d'équations diophantiennes (voir [Ma 2], III, et [B-F]). Mais elle fait appel au théorème de Mordell-Weil sur la jacobienne de la courbe C, et n'est donc en général pas effective. Les résultats qualitatifs qu'elle fournit sont néanmoins beaucoup plus précis que les précédents. On pourra ainsi comparer l'estimation effective obtenue par Kotov[23] pour une courbe elliptique quelconque E :

---

(20) B. Ferrero - R. Greenberg, Invent. Math., 50, 1978, pp. 91-102

(21) J. Coates, Acta Arithm., 26, 1970, pp. 425-435.

(22) Le cas du conducteur 11 a été traité par Agrawal, Coates, Hunt et van der Poorten (à paraître).

(23) S.V. Kotov, Dokl. A.N.B.S.S.R., 1977, 21, pp. 101-104.

$$\pi_\varphi(P) \gg (\log\log H_\varphi(P).\ \log\log\log H_\varphi(P))^{1/2}$$

au théorème 3 de [Be 4], qui fournit, quand E admet des multiplications complexes, et pour un nombre réel $\gamma = \gamma(E,K) > 0$, l'estimation ineffective :

$$\pi_\varphi(P) \gg (\log H_\varphi(P))^\gamma.$$

De plus, et c'est là son principal intérêt, cette seconde méthode permettrait, sous certaines conjectures, de traiter toutes les courbes de genre $\geqq 1$ (voir [L 5], et [Be 5], corollaire 2).

Société Mathématique de France
Astérisque 69-70 (1979) p. 191-202

Appendice II

Quelques propriétés des groupes algébriques commutatifs

par

Jean-Pierre SERRE

Soit G un groupe algébrique commutatif connexe sur un corps k de caractéristique 0. Dans les pages qui précèdent, M.Waldschmidt et D.Bertrand utilisent les propriétés suivantes du groupe G :

1) existence d'une compactification projective lisse ;

2) croissance au plus quadratique de la fonction hauteur, lorsque k est algébrique sur $\mathbf{Q}$;

3) uniformisation par des fonctions entières d'ordre ≤ 2 , lorsque $k = \mathbf{C}$.

Ce sont ces propriétés que je me propose de démontrer. La méthode suivie, inspirée de Severi [Sev] et Weil [We 1], consiste à se ramener, par une fibration convenable, aux deux cas particuliers déjà connus : celui où G est un groupe linéaire, et celui où G est une variété abélienne.

§ 1. Compactification de G

1.1. Le groupe L

On sait ([Ba 1], [Ros 1]) que G possède un plus grand sous-groupe linéaire connexe L. Le groupe L se décompose en $L = L_u \times L_m$, où L_u est unipotent et L_m est de type multiplicatif. Pour simplifier, nous supposerons (*) que L_m est déployé sur k, i.e. produit de groupes isomorphes au groupe multiplicatif $\mathbf{G}_m$ (on peut toujours se ramener à ce cas par extension finie du corps de base). Comme L_u est produit de groupes isomorphes au groupe additif $\mathbf{G}_a$ (loc.cit.), on peut écrire L comme un produit

$$L = \prod_{\alpha} L_{\alpha} ,$$

(*) On pourrait se débarrasser de cette hypothèse en utilisant les compactifications de L_m construites par J-L.Brylinski (C.R.A.S., 288, 1979, p. 137-139).

où les L_α sont égaux à $\mathbf{G}_a$ ou à $\mathbf{G}_m$. Dans ce qui suit, nous choisirons une telle décomposition.

1.2. *Compactification de* L

Soit $\bar{L}_\alpha$ l'unique courbe lisse, complète et connexe contenant L_α . On peut identifier $\bar{L}_\alpha$ à la *droite projective* P_1 ; on a

$$\bar{L}_\alpha - L_\alpha = \{\infty\} \text{ si } L_\alpha = \mathbf{G}_a \quad \text{et} \quad \bar{L}_\alpha - L_\alpha = \{0,\infty\} \text{ si } L_\alpha = \mathbf{G}_m .$$

Nous choisirons pour compactification de L le produit

$$\bar{L} = \prod_\alpha \bar{L}_\alpha .$$

Soit $L^\infty = \bar{L} - L$; on a :

$$L^\infty = \bigcup_\alpha L^\infty_\alpha , \quad \text{où } L^\infty_\alpha = \{\bar{L}_\alpha - L_\alpha\} \times \prod_{\beta \neq \alpha} \bar{L}_\beta .$$

(Noter que $\bar{L}$ et L^∞ *dépendent* de la décomposition $L = \prod L_\alpha$ choisie.)

1.3. *Construction de* $\bar{G}$

Soit $A = G/L$. Le groupe A est une *variété abélienne*, et la projection canonique $p : G \to A$ fait de G un *espace fibré principal* localement trivial, de base A et de groupe structural L (cf. [Ros 1]). Or la loi de composition $L \times L \to L$ se prolonge en $L \times \bar{L} \to \bar{L}$, autrement dit définit une action de L sur $\bar{L}$. On peut donc parler de l'espace fibré $\bar{G} = G \times^L \bar{L}$ *associé* à l'espace fibré principal G, et de fibre type $\bar{L}$. (Si G s'obtient en "recollant" des $U_i \times L$, où les U_i sont des ouverts de A, $\bar{G}$ s'obtient en recollant les $U_i \times \bar{L}$.) Nous noterons encore par p la projection de l'espace fibré $\bar{G}$ sur sa base A. Comme A et $\bar{L}$ sont complètes et lisses, il en est de même de $\bar{G}$. De plus, l'injection $L \to \bar{L}$ définit un plongement de G dans $\bar{G}$ qui identifie G à un ouvert dense de $\bar{G}$; ainsi, $\bar{G}$ est une *compactification lisse* de G.

La loi de composition $G \times G \to G$ *se prolonge* en $G \times \bar{G} \to \bar{G}$, autrement dit définit une action de G sur $\bar{G}$; cela résulte de la propriété analogue pour L et $\bar{L}$. En particulier, tout champ de vecteurs invariant sur G se prolonge à $\bar{G}$; si U est un ouvert affine de $\bar{G}$, un tel champ définit une *dérivation* de l'algèbre affine de U.

1.4. *Diviseurs et plongements projectifs de* $\bar{G}$

Chacun des L^∞_α définit une sous-variété $G^\infty_\alpha = G \times^L L^\infty_\alpha$ de $\bar{G}$. Si l'on pose $G^\infty = \bigcup_\alpha G^\infty_\alpha$, on a $G^\infty = \bar{G} - G$; c'est la sous-variété "à l'infini" de $\bar{G}$. Chacune des composantes irréductibles des G^∞_α et de G^∞ est de codimension 1 ; cela permet d'identifier les G^∞_α et G^∞ à des *diviseurs positifs* de $\bar{G}$.

Soit d'autre part D un diviseur de A, et soit $\tilde{D} = p^*(D)$ son image réciproque

par $p : \bar{G} \to A$. Si a et b sont des entiers, notons $D_{a,b}$ le diviseur $a\tilde{D} + bG^\infty$.

PROPOSITION 1 - *Supposons* D *ample. Il existe alors des entiers* $a \geqq 1$ *et* $b \geqq 1$ *tels que le diviseur* $D_{a,b} = a\tilde{D} + bG^\infty$ *de* $\bar{G}$ *soit ample*.

Il est clair que L^∞ est un diviseur ample (et même très ample) de $\bar{L}$. Comme $G^\infty = G \times^L L^\infty$, il en résulte que G^∞ est *relativement ample* vis-à-vis de $p : \bar{G} \to A$, au sens de Grothendieck, EGA II.4.6. La prop.1 s'en déduit en appliquant EGA II.4.6.13.(ii).

COROLLAIRE - *Il existe des entiers* $a \geqq 1$ *et* $b \geqq 1$ *tels que* $D_{a,b}$ *soit très ample, et que le plongement projectif de* $\bar{G}$ *défini par la série linéaire complète* $|D_{a,b}|$ *transforme* $\bar{G}$ *en une variété projectivement normale*.

Si (a,b) est un couple d'entiers satisfaisant aux conditions de la prop.1, tout multiple assez grand de (a,b) a les propriétés énoncées dans le corollaire ; cela se voit en appliquant des résultats standard sur les diviseurs amples et très amples, cf. [H], chap.II, §§ 5,6,7 et exerc.5.14.

Remarques

1) On peut préciser la prop.1, et prouver que $D_{a,b}$ est ample (resp. très ample) pour *tout* couple (a,b) tel que $a \geqq 1$ (resp. $a \geqq 3$) et $b \geqq 1$.

2) Soit $E_{a,b}$ le fibré de rang 1 associé au diviseur $D_{a,b}$ et soit $S_{a,b} = H^0(\bar{G}, E_{a,b})$ l'espace des sections de ce fibré. (Un élément de $S_{a,b}$ peut être identifié à une fonction rationnelle f sur $\bar{G}$ telle que $(f) \geqq - D_{a,b}$.) Soit $\{X_0,\ldots,X_N\}$ une base de $S_{a,b}$. Le cor. à la prop.1 revient à dire que l'on peut choisir $a \geqq 1$ et $b \geqq 1$ tels que :

(i) les sections $(X_0,\ldots,X_N)$ ne s'annulent simultanément en aucun point de $\bar{G}$;

(ii) si $\mathbf{P}_N$ est l'espace projectif de dimension N, le morphisme $X : \bar{G} \to \mathbf{P}_N$ défini par $(X_0,\ldots,X_N)$ est un plongement ;

(iii) pour qu'un diviseur positif Φ de $\bar{G}$ soit linéairement équivalent à $m\,D_{a,b}$ (avec $m \geqq 1$), il faut et il suffit qu'il existe un polynôme homogène $\varphi(X_0,\ldots,X_N)$ de degré m, non identiquement nul sur $\bar{G}$, dont le diviseur des zéros soit Φ. (Autrement dit, pour tout $m \geqq 1$, les hypersurfaces de degré m de $\mathbf{P}_N$ découpent sur $\bar{G}$ la série linéaire *complète* $|m\,D_{a,b}|$.)

1.5. *Une propriété des endomorphismes* $[n]_G$

Soit n un entier $\neq 0$. Notons $[n]_G$ (resp. $[n]_A$, $[n]_L$) l'endomorphisme $x \mapsto nx$ de G (resp. A , L).

PROPOSITION 2 - Les morphismes $[n]_L : L \to L$ et $[n]_G : G \to G$ se prolongent en des morphismes
$$[n]_L : \bar{L} \to \bar{L} \quad \text{et} \quad [n]_G : \bar{G} \to \bar{G} .$$

L'assertion relative à L se vérifie aussitôt sur la décomposition $\bar{L} = \coprod \bar{L}_\alpha$. Celle relative à G se ramène à la précédente grâce à la fibration de $\bar{G}$ sur A de fibre $\bar{L}$.

La proposition suivante indique quelle est l'image réciproque par $[n]_G : \bar{G} \to \bar{G}$ des diviseurs G^∞_α et $\tilde{D}$ définis au n° 1.4.

PROPOSITION 3 - (a) Si $L_\alpha = \mathbf{G}_a$, on a $[n]^*_G(G^\infty_\alpha) = G^\infty_\alpha$.

(b) Si $L_\alpha = \mathbf{G}_m$, on a $[n]^*_G(G^\infty_\alpha) = |n|\, G^\infty_\alpha$.

(c) Soit D un diviseur de A dont la classe d'équivalence soit symétrique (i.e. invariante par $x \mapsto -x$). On a les équivalences linéaires suivantes :
$$[n]^*_A(D) \sim n^2 D \quad \text{et} \quad [n]^*_G(\tilde{D}) \sim n^2 \tilde{D}.$$

Les assertions (a) et (b) se ramènent, grâce à la fibration de $\bar{G}$, aux assertions analogues pour $\bar{L}$, lesquelles se vérifient par calcul direct. En ce qui concerne (c), la formule relative à $[n]_A$ est bien connue ([Mu], p.59, cor.3), et celle relative à $[n]_G$ s'en déduit en appliquant p^* aux deux membres.

Soient a et b des entiers. Posons, comme au n° 1.4 :
$$D_{a,b} = a\tilde{D} + b\,G^\infty = a\tilde{D} + b\sum_\alpha G^\infty_\alpha .$$

COROLLAIRE 1 - On a
$$[n]^*_G(D_{a,b}) \sim n^2 D_{a,b} - b\,Z_n ,$$
où Z_n est un diviseur positif de $\bar{G}$ à support contenu dans G^∞.

D'après la prop.3, on a
$$[n]^*_G(D_{a,b}) \sim n^2 a\tilde{D} + b\sum_\alpha c_{\alpha,n} G^\infty_\alpha ,$$
où $c_{\alpha,n}$ est égal à 1 si $L_\alpha = \mathbf{G}_a$, et à $|n|$ si $L_\alpha = \mathbf{G}_m$. Le corollaire en résulte, en posant
$$Z_n = \sum_\alpha (n^2 - c_{\alpha,n})\, G^\infty_\alpha .$$

Supposons maintenant maintenant que D soit ample, que les entiers a et b soient $\geqq 1$, et que les propriétés (i), (ii), (iii) de la Remarque 2) du n°1.4 soient satisfaites. Identifions $\bar{G}$ à une sous-variété de $\mathbf{P}_N$ grâce à $X = (X_o,\ldots,X_N)$. Sous ces hypothèses, on a :

COROLLAIRE 2 - Pour tout $n \in \mathbf{Z}$, il existe $N+1$ polynômes
$$\varphi^{(n)}_o(X_o,\ldots,X_N) \;,\ldots,\; \varphi^{(n)}_N(X_o,\ldots,X_N) ,$$
homogènes de degré n^2, à coefficients dans k, ne s'annulant simultanément en aucun point de G, et tels que, pour tout point $x = (x_o,\ldots,x_N)$ de G, on ait
$$(*) \qquad [n]_G(x) = (\varphi^{(n)}_o(x),\ldots,\varphi^{(n)}_N(x)) .$$

Cela se déduit sans difficulté du cor.1. Indiquons rapidement comment. Soit H_i le diviseur de $\bar{G}$ découpé par l'hyperplan $X_i = 0$ de $\mathbf{P}_N$, et soit $H_{i,n} = [n]^*_G(H_i)$ son image réciproque par $[n]_G$. D'après le cor.1, on a
$$H_{i,n} + b\,Z_n \sim n^2 D_{a,b} .$$

Vu la propriété (iii), il existe un polynôme homogène $\varphi^{(n)}_i(X)$ de degré n^2 dont le diviseur des zéros est $H_{i,n} + b\,Z_n$. Quitte à multiplier les $\varphi^{(n)}_i$ par des scalaires, on peut s'arranger pour que, pour tout couple (i,j), la fonction rationnelle $\varphi^{(n)}_i / \varphi^{(n)}_j$ soit l'image réciproque de la fonction X_i / X_j par $[n]_G$. On constate alors que les $\varphi^{(n)}_i$ répondent à la question.

Remarque. Lorsque $|n| \geqq 2$, le support de Z_n est égal à G^∞, et les $\varphi^{(n)}_i(X)$ sont tous nuls sur G^∞. Cela montre que la formule (*) ne s'étend pas aux points de G^∞.

§ 2. Hauteurs

Dans ce §, on suppose k algébrique sur $\mathbf{Q}$.

2.1. Rappels

Si $x \in \mathbf{P}_N(k)$ est un point rationnel de l'espace projectif $\mathbf{P}_N$, on note $h(x)$ la hauteur logarithmique normalisée de x (cf. par exemple Waldschmidt, I, 1.d) ; c'est un nombre réel $\geqq 0$, invariant par extension des scalaires. Si V est une k-variété, et si $\varphi : V \to \mathbf{P}_N$ est un morphisme de V dans $\mathbf{P}_N$, on note
$$h_\varphi : V(k) \to \mathbf{R}_+$$
la fonction définie par $h_\varphi(x) = h(\varphi(x))$.

Supposons V projective. Deux fonctions réelles f et f' sur $V(k)$ sont dites équivalentes (ce que l'on écrit $f \sim f'$) si $|f - f'|$ est bornée. A tout diviseur de Cartier Δ de V, on peut attacher une fonction $h_\Delta : V(k) \to \mathbf{R}$, définie à équivalence près (au sens ci-dessus), et caractérisée par les propriétés :

(i) h_Δ ne dépend que de la classe d'équivalence linéaire de Δ ;

(ii) $h_\Delta + h_{\Delta'} \sim h_{\Delta+\Delta'}$;

(iii) Si $\varphi : V \to \mathbf{P}_N$ est un morphisme, et si Δ est l'image réciproque par φ d'un hyperplan de $\mathbf{P}_N$, on a

$$h_\varphi \sim h_\Delta \ .$$

2.2. Hauteur sur $\bar{G}$ relativement à $D_{a,b}$

On revient aux notations du § 1 . En particulier, on choisit un diviseur ample D de $A = G/L$ dont la classe d'équivalence soit symétrique (cf. prop.3) et l'on choisit des entiers $a,b \geqq 1$ tels que le diviseur $D_{a,b} = a\tilde{D} + b\,G^\infty$ soit très ample. On note

$$\varphi : \bar{G} \to \mathbf{P}_N$$

un plongement projectif de $\bar{G}$ correspondant à la série linéaire $|D_{a,b}|$, cf. n°1.4. On s'intéresse à la fonction hauteur h_φ relative à φ . Puisque $D_{a,b} = a\tilde{D} + b\,G^\infty$, on a

$$h_\varphi \sim a\,h_{\tilde{D}} + b\,h_{G^\infty}$$

et l'on est ramené à étudier les deux fonctions $h_{\tilde{D}}$ et h_{G^∞} .

(1) La fonction $h_{\tilde{D}}$

On a $\tilde{D} = p^*(D)$, où p désigne la projection de $\bar{G}$ sur A. Il en résulte que $h_{\tilde{D}} \sim h_D \circ p$, où h_D est la fonction hauteur sur A relativement au diviseur D. D'après Néron [N 1] on peut choisir h_D dans sa classe d'équivalence de telle sorte que ce soit une forme quadratique sur le groupe $A(k)$, et ce choix est unique. On a $h_D(x) = 0$ si $x \in A(k)$ est d'ordre fini, et $h_D(x) > 0$ sinon. Quitte à remplacer $h_{\tilde{D}}$ par une fonction équivalente, on peut supposer que $h_{\tilde{D}} = h_D \circ p$, et l'on voit alors que $h_{\tilde{D}}$ est une forme quadratique sur $G(k)$, à valeurs $\geqq 0$, invariante par translation par $L(k)$.

(2) La fonction h_{G^∞}

Cette fonction est "presque" invariante par translation :

LEMME 1 - *Pour tout* $x_o \in G(k)$, *les fonctions*

$$x \mapsto h_{G^\infty}(x) \qquad \text{et} \qquad x \mapsto h_{G^\infty}(x + x_o)$$

sont équivalentes.

Soit f l'automorphisme $x \mapsto x + x_o$ de la variété G. On a vu au n° 1.3 que f se prolonge en un automorphisme de $\bar{G}$, et l'on a $f^*(G^\infty) = G^\infty$. Il en résulte que

$$h_{G^\infty} \circ f \sim h_{G^\infty} ,$$

d'où le lemme.

LEMME 2 - *Soient* $x_1,\dots,x_m$ *des éléments de* $G(k)$. *Il existe des nombres réels* A *et* B *tels que*

$$|h_{G^\infty}(n_1 x_1 + \dots + n_m x_m)| \leqq A + B \sum |n_i| \qquad \text{pour tout} \quad (n_i) \in \mathbf{Z}^m .$$

Le lemme 1 montre qu'il existe $B_i \in \mathbf{R}$ tel que

$$|h_{G^\infty}(x + x_i) - h_{G^\infty}(x)| \leqq B_i \qquad \text{pour tout } x \in G(k)$$

On prend alors $A = h_{G^\infty}(0)$ et $B = \sup B_i$. L'inégalité cherchée se démontre immédiatement par récurrence sur $\sum |n_i|$.

Soit Γ un sous-groupe de type fini de $G(k)$. On peut exprimer le lemme 2 en disant que h_{G^∞} a une croissance au plus linéaire sur Γ. Comme $h_{\tilde{D}}$ est quadratique, on en déduit :

PROPOSITION 4 - *Sur* Γ, *la fonction hauteur* h_φ *est somme de la forme quadratique* $a\,h_{\tilde{D}}$ (déduite de la forme de Néron h_D sur $A(k)$) *et d'une fonction à croissance au plus linéaire*.

2.3. Hauteur sur G : cas général

PROPOSITION 5 - *Soit* $\psi : G \to \mathbf{P}_M$ *un morphisme de* G *dans un espace projectif, et soient* $x_1,\dots,x_m$ *des éléments de* $G(k)$. *Il existe des nombres réels* A *et* C *tels que*

$$h_\psi(n_1 x_1 + \dots + n_m x_m) \leqq A + C\left(\sum |n_i|\right)^2 \qquad \text{pour tout} \quad (n_i) \in \mathbf{Z}^m .$$

(En d'autres termes, la croissance de h_ψ sur le sous-groupe Γ engendré par les x_i est au plus quadratique.)

C'est vrai lorsque ψ est le plongement φ du n° 2.2, d'après la prop.4. Le cas général résulte de là, et du lemme élémentaire suivant (dont la vérification est laissée au lecteur) :

LEMME 3 - *Soit* V *une variété algébrique. Soient*

$$\varphi : V \to \mathbf{P}_N \qquad \text{et} \qquad \psi : V \to \mathbf{P}_M$$

des morphismes de V *dans des espaces projectifs. Supposons que* φ *soit un plongement* (de sorte que V s'identifie à une sous-variété localement fermée de $\mathbf{P}_N$). *Il existe alors* $\lambda, \mu \in \mathbf{R}$ *tels que*

$$h_\psi \leqq \lambda + \mu\, h_\varphi \qquad \text{sur} \quad V(k).$$

Autrement dit, on a $h_\psi = \underline{O}(h_\varphi)$.

§ 3. Application exponentielle et uniformisation

Dans ce §, le corps de base est le corps $\mathbf{C}$ des nombres complexes.

3.1. Exponentielle

Soit $t(G)$ l'algèbre de Lie de G, autrement dit l'espace tangent à G en l'élément neutre ; c'est un espace vectoriel complexe de dimension égale à $\dim G$. Nous noterons

$$\exp_G : t(G) \to G(\mathbf{C})$$

l'application exponentielle de G (Bourbaki, LIE III §6) ; rappelons que l'on peut caractériser $\exp_G$ par les deux propriétés suivantes :

a) c'est un homomorphisme de groupes de Lie complexes ;

b) son application tangente à l'élément neutre est l'identité.

Puisque G est connexe pour la topologie de Zariski, $G(\mathbf{C})$ est connexe pour la topologie usuelle. Il en résulte que $\exp_G$ est surjective ; si l'on note Ω_G son noyau ("groupe des périodes" de G), on obtient un isomorphisme de groupes de Lie complexes

$$t(G)/\Omega_G \simeq G(\mathbf{C}).$$

Soit f une fonction rationnelle sur G. On peut identifier f à une fonction méromorphe sur $G(\mathbf{C})$ (et même sur $\bar{G}(\mathbf{C})$). La fonction $F = f \circ \exp_G$ est une fonction méromorphe sur $t(G)$ invariante par Ω_G ; nous verrons plus loin (n°3.5) que F est d'ordre strict ≤ 2.

3.2. Préliminaires : algèbre affine de L

Nous utiliserons pour L, L_α, A, ... des notations

$$t(L),\ t(L_\alpha),\ t(A),\dots$$

$$\exp_L,\ \exp_{L_\alpha},\ \exp_A,\dots$$

$$\Omega_L,\ \Omega_{L_\alpha},\ \Omega_A,\ \dots$$

analogues à celles définies ci-dessus pour G. Comme L_α est, soit $\mathbf{G}_a$, soit $\mathbf{G}_m$, son algèbre de Lie $t(L_\alpha)$ s'identifie à $\mathbf{C}$; nous noterons e_α la base canonique de $t(L_\alpha)$; on a

$$\exp_{L_\alpha}(ze_\alpha) = \begin{cases} z \in \mathbf{G}_a(\mathbf{C}) = \mathbf{C} & \text{si } L_\alpha = \mathbf{G}_a \\ e^z \in \mathbf{G}_m(\mathbf{C}) = \mathbf{C}^* & \text{si } L_\alpha = \mathbf{G}_m. \end{cases}$$

Le groupe des périodes de L_α est réduit à 0 si $L_\alpha = \mathbf{G}_a$, et c'est l'ensemble des multiples entiers de $(2\pi i)e_\alpha$ si $L_\alpha = \mathbf{G}_m$.

Comme L est produit des L_α, $t(L)$ est somme directe des $t(L_\alpha)$, donc a pour base la famille des e_α. Si $z \in t(L)$, on notera z_α ses coordonnées par rapport

à cette base ; on a

$$z = \sum_\alpha z_\alpha e_\alpha .$$

Soit Λ_L l'algèbre affine de L. L'application $f \mapsto f \circ \exp_L$ identifie Λ_L à la sous-algèbre de l'algèbre des fonctions holomorphes sur $t(L)$ engendrée par les z_α (pour $L_\alpha = \mathbf{G}_a$) et les e^{z_α} et les e^{-z_α} (pour $L_\alpha = \mathbf{G}_m$).

Base de Λ_L

Soit N_L l'ensemble des familles $n = (n_\alpha)$, où n_α est un entier ≥ 0 si $L_\alpha = \mathbf{G}_a$ et un entier de signe quelconque si $L_\alpha = \mathbf{G}_m$. Si $n = (n_\alpha)$ appartient à N_L, posons

$$|n| = \operatorname{Sup} |n_\alpha|$$

et

$$e_n(z) = \prod_{L_\alpha = \mathbf{G}_a} z_\alpha^{n_\alpha} \prod_{L_\alpha = \mathbf{G}_m} e^{n_\alpha z_\alpha}.$$

Les fonctions $e_n(z)$, $n \in L$, forment une base de l'algèbre affine Λ_L.

Pôles

Soit $f \in \Lambda_L$. On peut considérer f comme une fonction rationnelle sur la variété projective L, n'ayant pas de pôle en dehors de L^∞, cf. n°1.2. Si b est un entier ≥ 0, on a

$$(f) \geq -bL^\infty$$

si et seulement si f est combinaison linéaire des $e_n(z)$ avec $|n| \leq b$.

3.3. Préliminaires : périodes

Puisque $A = G/L$, on a $t(A) = t(G)/t(L)$ et $\Omega_A = \Omega_G/\Omega_L$.

Choisissons un supplémentaire de $t(L)$ dans $t(G)$. Cela nous permet d'identifier $t(G)$ à $t(L) \oplus t(A)$, et d'écrire tout élément t de $t(G)$ comme un couple :

$$t = (z,u) \quad \text{avec} \quad z \in t(L) \quad \text{et} \quad u \in t(A).$$

L'image de Ω_G par la projection $t \mapsto u$ est Ω_A. Choisissons un sous-groupe $\tilde{\Omega}_A$ de Ω_G qui se projette isomorphiquement sur Ω_A (c'est possible, puisque Ω_A est libre sur $\mathbf{Z}$). On a

$$\Omega_G = \tilde{\Omega}_A \oplus \Omega_L$$

et l'on sait (cf. n°3.2) que Ω_L admet pour base les $(2\pi i)e_\alpha$ pour $L_\alpha = \mathbf{G}_m$. Si $\omega \in \Omega_A$, nous noterons $\tilde{\omega}$ son image réciproque dans $\tilde{\Omega}_A$. On a

$$\tilde{\omega} = (\eta_\omega, \omega) \quad \text{avec} \quad \eta_\omega \in t(L).$$

L'application $\omega \mapsto \eta_\omega$ est un $\mathbf{Z}$-homomorphisme de Ω_A dans $t(L)$. Une fonction $F = F(z,u)$ sur $t(G)$ est invariante par $\tilde{\Omega}_A$ si et seulement si

$$F(z+\eta_\omega\,,\ u+\omega) = F(z,u) \qquad \text{pour tout } \omega \in \Omega_A\,.$$

Pour qu'une telle fonction soit invariante par Ω_G il faut et il suffit qu'elle soit invariante par Ω_L , i.e. qu'elle soit invariante par $z \mapsto z_\alpha + 2\pi i$ (pour $L_\alpha = G_m$) .

3.4. Croissance de certaines fonctions

Revenons à la situation du §1 , et choisissons un diviseur positif et ample D de A. On sait (cf. [We 2]) qu'il existe une fonction thêta sur $t(A)$ dont le diviseur est l'image réciproque de D par $\exp_A$. Soit $\theta = \theta(u)$ une telle fonction. On a

$$\theta(u+\omega) = \theta(u)e^{E(u,\omega)} \qquad (u \in t(A),\ \omega \in \Omega_A)\,.$$

Nous n'aurons pas besoin de la forme explicite de $E(u,\omega)$, mais seulement de sa croissance à l'infini :

$$|E(u,\omega)| = \underline{O}(1+|u|^2+|\omega|^2).$$

Soient a et b des entiers $\geqq 1$. Soit $D_{a,b} = a\widetilde{D} + b\,G^\infty$ le diviseur de $\bar{G}$ défini au n° 1.4. Notons $S_{a,b}$ l'espace vectoriel des fonctions rationnelles f sur $\bar{G}$ telles que $(f) \geqq -D_{a,b}$. Si $f \in S_{a,b}$, notons $F = F(z,u)$ la fonction $f \circ \exp_G$ sur $t(G) = t(L) \oplus t(A)$, et posons :

$$\widetilde{F}(z,u) = \theta(u)^a F(z,u)\,.$$

Il est clair que $\widetilde{F}$ est holomorphe. De plus :

PROPOSITION 7 - La fonction $\widetilde{F}$ est d'ordre strict $\leqq 2$.

Remarquons d'abord que, pour tout $u \in t(A)$, la fonction $z \mapsto \widetilde{F}(z,u)$ appartient à l'algèbre affine de L, et que son diviseur est $\geqq -b\,L^\infty$. D'après le n°3.2, on peut donc écrire cette fonction sous la forme

$$\widetilde{F}(z,u) = \sum_{|n|\leqq b} e_n(z)\,\psi_n(u)\,,$$

avec $\psi_n(u) \in \mathbf{C}$. Le fait que $\widetilde{F}(z,u)$ soit holomorphe en u entraîne, par un argument standard, qu'il en est de même des ψ_n ; en particulier, les ψ_n sont bornés sur tout compact. Ce fait, joint à la croissance au plus exponentielle des $e_n(z)$, entraîne que, pour tout compact K de $t(A)$, il existe une constante C_K telle que

$$|\widetilde{F}(z,u)| \leqq \exp\{C_K(1+|z|)\} \qquad \text{pour } u \in K,$$

autrement dit

$$|\widetilde{F}(z,u)| \leqq \exp\{\underline{O}(1+|z|)\} \qquad \text{pour } u \in K.$$

Choisissons K de telle sorte que $K + \Omega_A = t(A)$: c'est possible puisque $t(A)/\Omega_A \simeq A(\mathbf{C})$ est compact. Pour tout $u \in t(A)$ il existe $\omega \in \Omega_A$ tel que $u + \omega \in K$. On a

$$|\omega| = |u| + \underline{O}(1)\,.$$

Puisque F est invariante par Ω_G , on a

$$F(z+\eta_\omega, u+\omega) = F(z,u)$$

d'où

$$\widetilde{F}(z+\eta_\omega, u+\omega) = \widetilde{F}(z,u)\,\exp\{a\,E(u,\omega)\}\,,$$

ou encore

$$\widetilde{F}(z,u) = \widetilde{F}(z+\eta_\omega, u+\omega)\,\exp\{-a\,E(u,\omega)\}.$$

On a vu que

$$|E(u,\omega)| = \underline{O}(1+|u|^2+|\omega|^2) = \underline{O}(1+|u|^2)\,.$$

D'autre part, puisque $u+\omega$ appartient à K, et que $|\eta_\omega| = \underline{O}(|\omega|)$, on a

$$|\widetilde{F}(z+\eta_\omega,\ u+\omega)| \leqq \exp\{\underline{O}(1+|z|+|u|)\}\,.$$

En combinant ces deux majorations, on en déduit :

$$|\widetilde{F}(z,u)| \leqq \exp\{\underline{O}(1+|z|+|u|^2)\}\,,$$

ce qui montre bien que $\widetilde{F}$ est d'ordre $\leqq 2$ au sens strict.

Remarque

Ecrivons $\widetilde{F}(z,u)$, comme ci-dessus, sous la forme

$$\widetilde{F}(z,u) = \sum_{|n|\leqq b} e_n(z)\,\psi_n(u)\,.$$

La prop.7 équivaut à dire que les fonctions $\psi_n(u)$ sont d'ordre strict $\leqq 2$. Il devrait être possible (en suivant [Sev]) de préciser ce résultat, et de prouver que ces fonctions s'expriment algébriquement au moyen de dérivées itérées de fonctions thêta.

3.5. Application

Supposons les entiers a et b choisis de telle sorte que $D_{a,b}$ soit très ample, ce qui est possible d'après le cor. à la prop. 1. Soit $\{f_0,\dots,f_N\}$ une base de l'espace vectoriel $S_{a,b}$, et soit φ le plongement de $\bar{G}$ dans l'espace projectif $\mathbf{P}_N$ défini par les f_i . Posons, comme ci-dessus :

$$F_i(z,u) = f_i \circ \exp_G$$

et

$$\widetilde{F}_i(z,u) = \theta(u)^a F_i(z,u)\,.$$

D'après la prop.7, les $\widetilde{F}_i$ sont des fonctions holomorphes d'ordre strict $\leqq 2$. De plus :

PROPOSITION 8 - (i) Les fonctions $(\widetilde{F}_0,\dots,\widetilde{F}_N)$ ne s'annulent simultanément en aucun point de $t(G)$.

(ii) L'application $\Phi : t(G) \to \mathbf{P}_N$ définie par les $(\widetilde{F}_i)$ est égale à $\varphi \circ \exp_G$.

Soit $t \in t(G)$, et soit $x = \exp_G(t) \in G(\mathbf{C})$. Puisque $D_{a,b}$ est très ample, il existe un indice i tel que le diviseur

$$(f_i) + D_{a,b} = (f_i) + a\tilde{D} + b\,G^{\infty}$$

ne passe pas par x. Comme l'image réciproque de ce diviseur par $\exp_G$ est égale au diviseur de $\tilde{F}_i$, ce dernier ne passe pas par t. On a donc $\tilde{F}_i(t) \neq 0$, ce qui démontre (i). L'assertion (ii) résulte de ce que $\tilde{F}_i / \tilde{F}_j = F_i / F_j = f_i / f_j \circ \exp_G$.

COROLLAIRE 1 - <u>L'application Φ définit par passage au quotient un isomorphisme de $G(\mathbf{C}) = t(G) / \Omega_G$ sur une sous-variété localement fermée de $\mathbf{P}_N$</u>.

C'est clair.

COROLLAIRE 2 - <u>Soit f une fonction rationnelle sur G. On peut écrire $f \circ \exp_G$ sous la forme</u>

$$f \circ \exp_G = R(\tilde{F}_o,\ldots,\tilde{F}_N) \,/\, S(\tilde{F}_o,\ldots,\tilde{F}_N)$$

<u>où R et S sont des polynômes homogènes de même degré tels que $S(\tilde{F}_o,\ldots,\tilde{F}_N)$ ne soit pas identiquement nul</u>.

En effet, il suffit de choisir R et S tels que

$$f = R(f_o,\ldots,f_N) \,/\, S(f_o,\ldots,f_N) \,,$$

ce qui est possible puisque φ est un plongement de $\bar{G}$ dans $\mathbf{P}_N$.

COROLLAIRE 3 - <u>Si f est une fonction rationnelle sur G, la fonction $f \circ \exp_G$ est une fonction méromorphe d'ordre strict ≤ 2</u>.

Cela résulte du cor.2 et du fait que les $\tilde{F}_i$ sont d'ordre strict ≤ 2.

RÉFÉRENCES

[Ba 1] BARSOTTI, I. - Structure theorems for group varieties, Annali di Mat., 38 (1955), 77-119.

[H] HARTSHORNE, R. - <u>Algebraic Geometry</u>, GTM 52, Springer-Verlag, 1977.

[Mu] MUMFORD, D. - <u>Abelian Varieties</u>, Oxford Univ.Press, 1970.

[N 1] NÉRON, A. - Quasi-fonctions et hauteurs sur les variétés abéliennes, Ann. of Math., 82 (1965), 249-331.

[Ros 1] ROSENLICHT, M. - Some basic theorems on algebraic groups, Amer.J.Math., 78 (1956), 401-443.

[Sev] SEVERI, F. - <u>Funzioni Quasi Abeliane</u>, Pont. Acad.Sc., Vatican, 1947.

[We 1] WEIL, A. - Variétés abéliennes, Colloque d'Algèbre et Théorie des Nombres, C.N.R.S. (1949), 125-128.

[We 2] WEIL, A. - <u>Introduction à l'étude des variétés kählériennes</u>, Hermann, 1958.

RÉFÉRENCES

[Al] ALTMAN, A.- The size function on abelian varieties ; Trans. A.M.S., 164 (1972), 153-161.

[Ax] AX, J.- Some topics in differential algebraic geometry ; Amer. J. Math., 94 (1972), 1195-1213.

[B] BAKER, A.- <u>Transcendental number theory</u> ; Cambridge Univ. Press, 1975.

[B-M] BAKER, A., and MASSER, D.W. (ed.). - <u>Transcendence theory</u> : <u>advances and applications</u> ; Proc. Conf. Cambridge (1976), Academic Press, 1977.

[Ba 1] BARSOTTI, I.- Structure theorems for group varieties ; Annali di Mat., 38 (1955), 77-119.

[Ba 2] BARSOTTI, I.- Factor sets and differentials on Abelian varieties ; Trans. A.M.S., 84 (1957), 85-108.

[Be 1] BERTRAND, D.- Séries d'Eisenstein et transcendance ; Bull. Soc. Math. France, 104 (1976), 309-321.

[Be 2] BERTRAND, D.- Transcendance de valeurs de la fonction gamma ; Sém. Delange Pisot Poitou, 17 (1975/76), G8.

[Be 3] BERTRAND, D.- Sous-groupes à un paramètre p-adique de variétés de groupe ; Invent. Math., 40 (1977), 171-193.

[Be 4] BERTRAND, D.- Approximations diophantiennes p-adiques sur les courbes elliptiques admettant une multiplication complexe ; Compositio Math., 37 (1978), 21-50.

[Be 5] BERTRAND, D.- Fonctions abéliennes p-adiques. Définitions et conjectures ; Groupe d'Etude d'Analyse Ultramétrique, 4 (1976/77), n° 21.

[Be 6] BERTRAND, D.- Fonctions modulaires, courbes de Tate et indépendance algébrique ; Sém. Delange Pisot Poitou, 19 (1977/78), n° 36.

[B-F] BERTRAND, D., and FLICKER, Y. - Linear forms on abelian varieties over local fields ; Acta Arith., 38 (1980), 47-61.

[Bom] BOMBIERI, E. - Algebraic values of meromorphic maps ; Invent. Math., 10 (1970), 267-287 ; 11 (1970), 163-166.

[B-L] BOMBIERI, E., and LANG, S. - Analytic subgroups of group varieties ; Invent. Math., 11 (1970), 1-14.

[Bor] BOREL, A. - <u>Linear algebraic groups</u> ; Benjamin, 1969.

[Br-K] BROWNAWELL, W.D, and KUBOTA, K.K. - The algebraic independence of Weierstrass functions and some related numbers ; Acta Arith., 33 (1977), 111-149.

[Br-M] BROWNAWELL, W.D, and MASSER, D.W. - Multiplicity estimates for analytic functions. Crelle 314 (1980), 200-216 et Duke Math. J. 47 (1980), 273-295.

[Bru] BRUMER, A.- On the units of algebraic number fields ; Mathematika, 14 (1967) 121-124.

[Ca] CASSELS, J.W.S.- An introduction to diophantine approximation ; Cambridge Tracts n° 45, Cambridge Univ. Press, 1965.

[C 1] CHUDNOVSKY, G.V.- Algebraic independence of values of exponential and elliptic functions ; Proc. Int. Congress of Math., Helsinki (1978).

[C 2] CHUDNOVSKY, G.V.- Singular points on complex hypersurfaces and multidimensional Schwarz lemma ; Sém. Delange Pisot Poitou, 19 (1977/78).

[C 3] CHUDNOVSKY, G.V.- Transcendence and algebraic independence of constants connected with exponential and elliptic functions.
Elliptic analogue of Lindemann Weierstrass theorems.
Preprints. (voir Math. Surveys and Monographs N°19, A.M.S. 1984).

[C-L] COATES, J., and LANG, S.- Diophantine approximation on abelian varieties with complex multiplication ; Invent. Math., 34 (1976), 129-133.

[F] FLICKER, Y.- Transcendence theory over local fields ; Thèse Ph.D., Cambridge, 1978.

[G] GEL'FOND, A.O.- Transcendental and algebraic numbers ; GITTL, 1952 ; Dover, 1960.

[Gr] GROSS, B.H.- On the periods of abelian integrals and a formula of Chowla and Selberg ; Invent. Math., 45 (1978), 193-211.

[H] HARTSHORNE, R.- Algebraic Geometry, GTM 52, Springer-Verlag, 1977.

[K-W] KRAZER, A., und WIRTINGER, W.- Abelsche Funktionen und allgemeine Thetafunktionen ; Enc. Mat. Wiss. II B-7, (1920).

[L 1] LANG, S.- Diophantine Geometry ; Interscience tracts, n° 11, 1962.

[L 2] LANG, S.- Introduction to transcendental numbers ; Addison-Wesley, 1966.

[L 3] LANG, S.- Transcendental numbers and diophantine approximations ; Bull. A.M.S., 77 (1971), 635-677.

[L 4] LANG, S.- Introduction to algebraic and abelian functions ; Addison-Wesley, 1972.

[L 5] LANG, S.- Higher dimensional diophantine problems ; Bull. A.M.S., 80 (1974), 779-787.

[L 6] LANG, S.- Diophantine approximation on abelian varieries with complex multiplication ; Advances in Math., 17 (1975), 281-336.

[L 7] LANG, S.- Elliptic curves, diophantine analysis ; Grund. der math. Wiss., 231, Springer-Verlag, 1978.

[La 1] LAURENT, M.- Approximation de valeurs de la fonction bêta. Ann. Toulouse 2 (1980), 53-65.

[La 2] LAURENT, M.- Transcendance de périodes d'intégrales elliptiques Crelle J. 316 (1980), 122-139 et 333 (1982), 144-161.

[Le 1] LELONG, P.- Propriétés métriques des variétés analytiques complexes définies par une équation ; Annales E.N.S., 67 (1950), 393-419.

[Le 2] LELONG, P.- Fonctionnelles analytiques et fonctions entières (n variables); Presses Univ. Montréal, 28, 1968.

[Lu] LUTZ, E.- Sur les approximations diophantiennes linéaires p-adiques ; Hermann, 1955.

[Mah 1] MAHLER, K.- On some inequalities for polynomials in several variables ; J. London Math. Soc., 37 (1962), 341-344.

[Mah 2] MAHLER, K.- On the coefficients of the 2^n-th transformation polynomial for $j(\omega)$; Acta Arith., 21 (1972), 89-97.

[Man] MANIN, Yu.V.- Corps cyclotomiques et courbes modulaires (en russe) ; Usp. Mat. Nauk, 26 (1971), 7-71.

[M 1] MASSER, D.W.- Elliptic functions and transcendence ; Lecture Notes in Math., 437, Springer-Verlag, 1975.

[M 2] MASSER, D.W.- Linear forms in algebraic points of abelian functions ; I, Math. Proc. Camb. Phil. Soc., 77 (1975), 499-513 ; II, id., 79 (1976), 55-70 ; III, Proc. London Math. Soc., 33 (1976), 549-564.

[M 3] MASSER, D.W.- A note on a paper of Franklin ; Acta Arith., 31 (1976), 143-152.

[M 4] MASSER, D.W.- On the periods of abelian functions in two variables ; Mathematika, 22 (1975), 97-107.

[M 5] MASSER, D.W.- The transcendence of certain quasi-periods associated with abelian functions in two variables ; Comp. Math., 35 (1977), 239-258.

[M 6] MASSER, D.W.- Diophantine approximation and lattices with complex multiplication ; Invent. Math., 45 (1978), 61-82.

[M 7] MASSER, D.W.- Polynomial interpolation in several variables ; J. Approximation Theory, 24 (1978), 18-34.

[M 8] MASSER, D.W.- Some recent results in transcendence theory ; Journées Arithmétiques Luminy 1978, Astérisque , 61 (1979) p. 145-154

[Mo] MOREAU, J.C.- Zéros de polynômes en plusieurs variables ; C.r. Acad. Sci. Paris, Ser. A, 282 (1976), 771-774.

[Mor] MORITA, Y.- On transcendency of special values of arithmetic automorphic functions ; J. Math. Soc. Japan, 24 (1972), 268-274.

[Mu] MUMFORD, D.- Abelian Varieties, Oxford Univ. Press, 1970.

[N 1] NÉRON, A.- Quasi-fonctions et hauteurs sur les variétés abéliennes ; Ann. of Math., 82 (1965), 249-331 (voir aussi Sém. Bourbaki, 1963/64, n° 274).

[N 2] NÉRON, A.- Hauteurs et fonctions thêta ; Rend. Sem. Mat. e Fis. Milano, 46 (1976), 111-135.

[Ra] RAMACHANDRA, K.- Contributions to the theory of transcendental numbers ; Acta Arith., 14 (1968), 65-88.

[Re 1] REYSSAT, E.- Approximation algébrique de nombres liés aux fonctions elliptiques et exponentielle. Bull. Soc. Math. France, 108 (1980), 47-79.

[Re 2] REYSSAT, E.- Approximation de valeurs de la fonction sigma de Weierstrass. Annales Toulouse 2 (1980), 79-91

[Ri] RIBET, K.- Dividing rational points on abelian varieties of C.M. type ; Comp. Math., 33 (1976), 69-74.

[Ro] ROBBA, Ph.- Lemmes de Schwarz et lemmes d'approximations p-adiques en plusieurs variables ; Invent. Math. 48 (1978), 245-277.

[Ros 1] ROSENLICHT, M.- Some basic theorems on algebraic groups ; Amer. J. Math., 78 (1956), 401-443.

[Ros 2] ROSENLICHT, M.- Extensions of vector groups by abelian varieties ; Amer. J. Math., 80 (1958), 685-714.

[Sch] SCHLICKEWEI, H.P.- Linearformen mit algebraischen Koeffizienten ; Manuscripta Math., 18 (1976) 147-185.

[Sc] SCHMIDT, W.M.- Approximation to algebraic numbers ; L'Enseignement Math., 17 (1971), 188-253 ; Monographie n° 19, 1972.

[S 1] SCHNEIDER, Th.- Arithmetische Untersuchungen elliptischer Integrale ; Math. Annalen, 113 (1937), 1-13.

[S 2] SCHNEIDER, Th.- Zur Theorie der Abelschen Funktionen und Integrale ; J. reine u. angew. Math., 183 (1941), 110-128.

[S 3] SCHNEIDER, Th.- Ein Satz über ganzwertige Funktionen als Prinzip für Transzendenzbeweise ; Math. Annalen, 121 (1949), 131-140.

[S 4] SCHNEIDER, Th.- Introduction aux nombres transcendants ; Grundlehren der Mat. Wiss., 81, Springer-Verlag, 1957 ; Gauthier-Villars, 1959.

[Se 1] SERRE, J.P.- Groupes algébriques et corps de classes ; Hermann, 1959.

[Se 2] SERRE, J.P.- Morphismes universels et différentielles de troisième espèce ; Sém. C. Chevalley, E.N.S., 1958/59, n° 11.

[Se 3] SERRE, J.P.- Dépendance d'exponentielles p-adiques ; Sém. Delange Pisot Poitou, 7 (1965/66), n° 15.

[Se 4] SERRE, J.P.- Abelian l-adic representations and elliptic curves, Benjamin, 1968.

[Sev] SEVERI, F.- Funzioni Quasi Abeliane ; Pont. Acad. Sc., Vatican, 1947.

[Sha] SHAFAREVICH, I.R.- Basic algebraic geometry ; Grund. der math. Wiss., 213, Springer-Verlag, 1974.

[Shi 1] SHIMURA, G.- Automorphic functions and number theory ; Lecture Notes in Math., 54, Springer-Verlag, 1968.

[Shi 2] SHIMURA, G.- Introduction to the arithmetic theory of automorphic functions ; Publ. Math. Soc. Japan, Princeton Univ. Press, 1971.

[S-T] SHIMURA, G., and TANIYAMA, Y.- Complex multiplication of abelian varieties and its applications to number theory ; Publ. Math. Soc. Japan, 6 (1961).

[Si 1] SIEGEL, C.L.- Über die Perioden elliptischer Funktionen ; J. reine u. angew. Math., 167 (1932), 62-69.

[Si 2] SIEGEL, C.L.- Transcendental numbers ; Ann. of Math. Studies, 16, Princeton Univ. Press, 1949.

[Si 3] SIEGEL, C.L.- Topics in complex function theory ; (3 vol.), Interscience tracts, n° 25, 1969-73.

[Sk] SKODA, H.- Estimations L^2 pour l'opérateur $\bar{\partial}$ et applications arithmétiques ; Sém. P. Lelong, 1975/76 ; Lectures Notes in Math., 578 (1977), 314-323.

[St] STOLL, W.- Normal families of non-negative divisors ; Math. Zeitschr., 84 (1964), 154-218.

[S.D] SWINNERTON-DYER, H.P.F.- Analytic theory of abelian varieties ; London Math. Soc. Lecture Notes, 14, Cambridge Univ. Press, 1974.

[Wa 1] WALDSCHMIDT, M.- Propriétés arithmétiques des valeurs de fonctions méromorphes algébriquement indépendantes ; Acta Arith., 23 (1973), 19-88.

[Wa 2] WALDSCHMIDT, M.- Nombres transcendants ; Lecture Notes in Math., 402, Springer-Verlag, 1974.

[Wa 3] WALDSCHMIDT, M.- Propriétés arithmétiques de fonctions de plusieurs variables ; I, Sém. P. Lelong, 1974/75 ; Lecture Notes in Math., 524 (1976), 106-129 ; II, id., 1975/76, 578 (1977), 108-135 ; III, id., 1978/79, 822 (1980), 332-356.

[We 1] WEIL, A.- Variétés abéliennes ; Colloque d'Algèbre et Théorie des Nombres, C.N.R.S. (1949), 125-128.

[We 2] WEIL, A.- Introduction à l'étude des variétés kähleriennes ; Hermann, 1958.

[We 3] WEIL, A.- On a certain type of characters of the idèle-class group of an algebraic number-field ; Proc. Intern. Symp. Alg. Geom., Tokyo Nikko 1955, Tokyo (1956), 1-7.

[P-S] POLYA, G., and SZEGÖ, G. - Problems and theorems in analysis ; I, Grund. der Math. Wiss., 193, Springer-Verlag, 1972. II, id. 216, 1976.

INDEX

Algèbre d'endomorphismes. (p. 26).
Algébrique (Point). (p. 26, 27).

Baker (Théorème 1.1.9). (p. 18 ; § 8.3.b).
Bernouilli (Nombres). (p. 65, 66).
Bien réparti. (p. 29).
Bombieri (Critère 5.1.1). (p. 85).

Chevalley (Théorème 1.2.1). (p. 22).
Coefficient de densité. (§ 1.3.d ; p. 129, 133, 150, 151, 155, 167).
Compactification. (II § 1).

Degré singulier. (p. 144).
Dénominateur. (p. 20).
Dimension algébrique. (p. 28, 45, 51, 57 ; § 4.2, 8.2).

Eisenstein (Séries). (p. 65, 185).
Endomorphismes. (p. 26, 93).
Existence (Théorème). (p. 142).
Exponentielle. (p. 22, 25, 173 ; II § 3).
Exponentielles (Problème des quatre exponentielles). (p. 17).
Exponentielles (Théorème des six exponentielles). (p. 17).
Exposant de Dirichlet. (p. 36, 168).
Exposant (Lemme de Schwarz). (p. 119).

Fonction abélienne. (p. 23).
Fonction arithmétique automorphe. (p. 95).
Fonction bêta. (p. 90, 91).
Fonction elliptique. (p. 27, § 3.2, p. 77, 80, 81, 105, 107, 158, 176).
Fonction gamma. (p. 75, 92).
Fonction modulaire. (p. 63, 75, 80, 185).
Fonction plurisousharmonique. (p. 138).
Fonction sigma. (p. 27, 28 ; § 3.2, 3.3 ; p. 74, 80).
Fonction sous-harmonique. (p. 136).
Fonction thêta. (p. 24, 184).
Fonction zêta. (p. 27, 28 ; § 3.2, 3.3, 3.5 ; p. 80).

Forme différentielle. (p. 68, 87).
Formules de multiplication (p. 176, 195).

Gel'fond-Schneider (Théorème 1.1.3). (p. 14, 182).
Géométrie diophantienne. (p. 106, 188)
Grothendieck (Conjecture). (p. 82).
Groupe algébrique. (p. 21).
Groupe multiplicatif. (p. 22, 172).

Hauteur (p. 15, 19, 21 ; II § 2).
Hermite-Lindemann (Théorème 1.1.2). (p. 14, 182).
Hilbert (Septième problème). (p. 2).
Hilbert (Quatorzième problème). (p. 144).

Indépendance algébrique. (p. 75).
Indépendance de logarithmes. (p. 18, 58, 81, 183).
Indépendance linéaire. (p. 45, 48, 74 ; § 6.2 ; p. 186).
Indicatrice projective d'un courant. (p. 145).
Intégrales abéliennes (§ 5.2).
Intégrales elliptiques. (§ 3.3, 3.5).

Jensen (Formule). (p. 134, 135, 136).

Khintchine (Théorème). (p. 37).

Lelong (Nombre de Lelong). (p. 140, 145).
Logarithme. (p. 172, 175).

Masse moyenne. (p. 133).
Mesure de Mahler. (p. 21).
Multiplication complexe. (p. 27, 63, 77 ; Chap. 6)
Multiplication réelle. (p. 182).

Normalisation (de l'exponentielle). (p. 25, 26, 176).
Normalisation forte. (p. 103, 182).
Normalisée (Hauteur logarithmique). (p. 164, 195).
Normalisés (Sous-groupes à n paramètres). (p. 26, 176).

Ordre. (II § 3.4 et 3.5).
Ordre arithmétique. (p. 16, 168, 174).
Ordre arithmétique fonctionnel. (p. 166).
Ordre d'un zéro. (p. 114).
Ordre strict. (p. 13).

Régulateur p-adique. (p. 58, 177).
Répartition. (p. 29).
Riemann (Conditions). (p. 23).

Schanuel (Conjecture 1.1.10). (p. 19, 154).
Schmidt (Théorème 1.3.4). (p. 32, 169).
Schneider (Théorème sur la fonction modulaire 3.2.4). (p. 63).
Schneider-Lang (Critère 1.1.1). (p. 14).
Schwarz (Lemmes). (Chap. 7 ; p. 114, 119, 169, 173).
Singularités d'hypersurfaces algébriques. (p. 38, 100 ; § 7.5).
Sous-groupe à n paramètres. (p. 22, 176).

Taille. (p. 20).
Thêta (Homomorphisme). (p. 24, 26, 103, 184).
Transfert (Lemme). (p. 37, 154, 169).
Torsion (Point). (p. 27).

Variété abélienne dégénérante. (p. 184).
Variété abélienne de type CM (Chap. 6).
Variété abélienne de type RM (p. 182).

INDEX DES NOTATIONS

$\lvert\overline{\alpha}\rvert$	Maison de α . (p. 20).
B_k	Nombres de Bernouilli. (p. 65).
$B(0,R)$	$= \{z \in \mathbb{C}^n \; ; \; \lvert z\rvert \leq R\}$ Boule euclidienne de centre 0 et de rayon R dans $\mathbb{C}^n$.
$\overline{\Gamma}$	Sous-espace vectoriel engendré par Γ . (p. 29).
$\Gamma_N = \Gamma_N(\mathcal{B})$	$= \{h_1\gamma_1 + \dots + h_\ell\gamma_\ell \; ; \; (h_1, \dots, h_\ell) \in \mathbb{Z}^\ell, \; \max_{1 \leq j \leq \ell} \lvert h_j\rvert \leq N\}$.(p.16,164).
$D(0,R)$	$= \{z \in \mathbb{C}^n \; ; \; \lVert z\rVert \leq R\}$ Polydisque dans $\mathbb{C}^n$. (p. 122).
D^τ	$= \dfrac{\partial^{\tau_1}}{\partial z_1^{\tau_1}} \cdots \dfrac{\partial^{\tau_n}}{\partial z_n^{\tau_n}}$, $\tau = (\tau_1, \dots, \tau_n) \in \mathbb{N}^n$. (p. 96).
den α	Dénominateur de α . (p. 20).
∂ , $\overline{\partial}$	$\partial = \sum_{j=1}^{n} \dfrac{\partial}{\partial z_j} dz_j$, $\overline{\partial} = \sum_{j=1}^{n} \dfrac{\partial}{\partial \overline{z}_j} d\overline{z}_j$. (p. 139).
$\Delta(\omega_1, \omega_2)$	Discriminant du réseau $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. (p. 63, 80).
Δ	Laplacien. (p. 138).
E_{2k}	Séries d'Eisenstein. (p. 65, 185).
$(\mathrm{End}_0\, A)_{\overline{\mathbb{Q}}}$	$= (\mathrm{End}\, A).\overline{\mathbb{Q}}$. (p. 102, 183)
exp	Exponentielle. (p. 22, 163).
$\mathcal{E}$	Courbe elliptique. (p. 27).
$\lvert f\rvert_r$	Borne supérieure de $\lvert f\rvert$ sur $B(0,r)$. (p. 13).
$\lVert f\rVert_r$	Borne supérieure de $\lvert f\rvert$ sur $D(0,r)$. (p. 118).
$\mathcal{F}$	Corps des fonctions abéliennes. (p. 23).
g_2 , g_3	Invariants d'une fonction $\wp$. (p. 27).
G_K , $G(K)$	Groupe des points de G rationnels sur K . (p. 22, 163).

ζ	Fonction zêta de Weierstrass. (p. 27).
$h(P)$, $h(\alpha)$	Hauteur logarithmique absolue. (p. 19).
$H(P)$, $H(\alpha)$	Hauteur usuelle. (p. 21, 15).
η_1 , η_2	Quasi-périodes de ζ . (p. 28).
θ_{2n}	$= \frac{4\pi^n}{(n-2)!}$. (p. 136)
θ_t	Coefficient dans la définition du lemme de Schwarz 7.12. (p. 114).
Θ	Homomorphisme thêta. (p. 24).
j	Invariant modulaire. (p. 63).
J	Fonction modulaire : $J(e^{2i\pi\tau}) = j(\tau)$. (p. 75, 185).
k	Corps archimédien complet de caractéristique nulle et de caractéristique résiduelle $p > 0$. (p. 164).
Lie G	Algèbre des dérivations invariantes. (p. 165).
λ	$\lambda(u;0,R)$, $\lambda_W(u;0,R)$. Moyennes de u sur $S(0,R)$. (p. 135, 137).
$M(\alpha)$	Mesure de Mahler. (p. 21).
$\mu(\Gamma,V)$, $\mu(\Gamma)$	Coefficient de répartition (exposant de Dirichlet généralisé). (p. 29, 153).
μ	Mesure de Riesz. (p. 136).
$\mu(t)$	Masse de $B(0,t)$ pour la mesure μ . (p. 136).
$\nu(t)$, $\nu_f(0,t)$	Masse moyenne des zéros. (p. 115, 136, 139).
$\nu_T(w,r)$	Indicatrice projective d'un courant T . (p. 145).
$\nu_f(0)$, $\nu_T(w)$	Nombre de Lelong (densité). (p. 140, 145).
$\\|\nu\\|$	$= \nu_1 + \dots + \nu_n$. Longueur de $\nu = (\nu_1, \dots, \nu_n) \in \mathbb{N}^n$. (p. 164).
$\mathcal{O}$	Anneau des entiers de k . (p. 164).
$\wp$	Fonction elliptique de Weierstrass. (p. 27) ; de Weil-Lutz. (p. 176).
$P(z)$	$= (1, \wp(z), \wp'(z))$. (p. 27).
$S(0,R)$	$= \{z \in \mathbb{C}^n \,;\, \|z\| = R\}$. Sphère euclidienne de centre 0 et de rayon R dans $\mathbb{C}^n$.

$s(\alpha)$	Taille de α . (p. 20).
$s_\lambda(\Omega)$	$= \sum_{\omega \in \Omega, \omega \neq 0} \omega^{-\lambda}$ pour $\lambda > 2$. (p. 27, 63).
σ	Fonction sigma de Weierstrass. (p. 27).
TG , T_G, $t(G)$	Espace tangent à l'origine (p. 22, 163, 198).
T_ν	Opérateurs (p. 166).
$\|\tau\|$	$= \tau_1 + \dots + \tau_n$. Longueur de $\tau = (\tau_1, \dots, \tau_n) \in \mathbb{N}^n$. (p. 96, 147).
$< x,y >$	$= \sum_{j=1}^{n} x_j y_j$ pour $x = (x_1, \dots, x_n) \in \mathbb{C}^n$, $y = (y_1, \dots, y_n) \in \mathbb{C}^n$. (p. 52, 56, 86).
ω_1 , ω_2	Couple de périodes fondamentales d'un réseau de $\mathbb{C}$. (p. 27).
$\omega_1(S)$	Plus petit des degrés des hypersurfaces algébriques passant par S dans $\mathbb{C}^n$. (p. 38, 96).
$\omega_t(S)$	Plus petit des degrés des hypersurfaces algébriques ayant en chaque point de S une singularité d'ordre $\geq t$. (p. 38, 119).
$\Omega(S)$	$= \lim_{t \to +\infty} \omega_t(S)/t$. Degré singulier. (p. 144).
$\|z\|$	$= (\sum_{j=1}^{n} \|z_j\|^2)^{1/2}$. Norme euclidienne. (p. 13).
$\\|z\\|$	$= \max_{1 \leq j \leq n} \|z_j\|$. (p. 118).

ABSTRACT

The aim of this work is to study the algebraic points on the graph or on the image of an analytic homomorphism $\varphi : G'_{\mathbb{C}} \to G''_{\mathbb{C}}$, where G' and G" are two connected commutative algebraic groups which are defined over the field $\bar{\mathbb{Q}}$ of algebraic numbers. Assuming that no power of φ is rational, one gets (in certain circumstances) upper bounds for the number of $\mathbb{Z}$-linearly independent algebraic points on the graph. For the study of the image one has to assume that the algebraic dimension of (the Zariski closure of the image of) φ is sufficiently large.

The first chapter introduces some basic results on transcendental numbers and algebraic groups, together with the definition and study of a distribution coefficient (the generalized Dirichlet exponent) which will play an important role in several dimensional problems.

The second chapter gives at an elementary level the results on linear groups which will be needed in the sequel.

The third chapter deals with one-parameter subgroups $\varphi : \mathbb{C} \to G_{\mathbb{C}}$ whose derivatives at the origin is defined over $\bar{\mathbb{Q}}$ (such homomorphisms are called "normalized"). Among the applications of the general theorem (mainly due to Lang, with a refinement using a result of Serre, Appendice II), worth mentioning is the case where G is an extension of an elliptic curve by the multiplicative group : using a description (communicated by Serre) of the exponential map of such a group, one gets results on elliptic integrals of the third kind.

In chapter 4 there is no arithmetic assumption on the derivative at the origin of $\varphi : \mathbb{C} \to G_{\mathbb{C}}$. Then there are at most two linearly independent algebraic points on the graph, and a similar statement holds for the image.

In chapter 5 we begin the study in several variables : let $\varphi : \mathbb{C}^n \to G_{\mathbb{C}}$ be a normalized analytic homomorphism. Using a result of Bombieri (generalizing the so-called Schneider-Lang criterion) one gets a several dimensional generalization of the results of chapter 3.

In the case of abelian varieties of CM type, deep results on linear independence have been derived by Masser and Lang. In chapter 6 these results are used for the study of the algebraic points on the graph of a (non-normalized) analytic homomorphism $\varphi : \mathbb{C}^n \to G_{\mathbb{C}}$.

ABSTRACT

A different subject is treaded in chapter 7, where we give a general treatment of the Schwarz lemma in several variables. This leads to important problems for higher dimensional diophantine investigations.

These Schwarz lemmas are used in chapter 8 for the study of the graph and the image of an analytic homomorphism $\varphi : \mathbb{C}^n \to G_{\mathbb{C}}$, in connection with a problem of Weil and Serre on a certain type of characters of the idèle-class group of an algebraic number field.

The first appendix, by Daniel Bertrand, gives a survey of the p-adic case and of its applications. The second appendix, by Jean-Pierre Serre, provides a proof of several properties of commutatives algebraic groups which are needed in transcendence proofs.

ASTÉRISQUE

1973 :	1	- Y. MEYER - Trois problèmes sur les sommes trigonométriques.
	2-3	- Colloque international du CNRS - Équations aux dérivées partielles linéaires (Orsay, 1972).
	4	- Séminaire K.G.B. - Sur les marches aléatoires (Rennes, 1972).
	5	- R. KAUFMAN and Th. KÖRNER - Pseudofunctions and Helson sets.
	6	- A. HATCHER and J. WAGONER - Pseudo-isotopies of compact manifolds.
	7-8	- Colloque sur les singularités en géométrie analytique (Cargèse, 1972).
	9	- J. PELLAUMAIL - Une nouvelle construction de l'intégrale stochastique.
	10	- A. ESCASSUT et Ph. ROBBA - Prolongement analytique et algèbres de Banach ultramétriques.

1974 :	11	- B. MAUREY - Théorèmes de factorisation pour les opérateurs linéaires à valeurs dans les espaces L^p.
	12	- F. LAUDENBACH - Topologie de la dimension trois : homotopie et isotopie. (Épuisé)
	13-14	- A. GUICHARDET - Systèmes dynamiques non commutatifs.
	15	- B. MAISONNEUVE - Systèmes régénératifs.
	16	- A. DOUADY - J.-L. VERDIER - Séminaire de géométrie analytique.
	17	- A. DOUADY - J.-L. VERDIER - Séminaire de géométrie analytique.
	18	- E. BOMBIERI - Le grand crible dans la théorie analytique des nombres (2^{e} édition).
	19	- S. ALINHAC - P. BOLLEY - J. CAMUS - B. HANOUZET - B. HELFFER - C. ZUILY Sur quelques équations aux dérivées partielles singulières.
	20	- H. C. PINKHAM - Deformations of algebraic varieties with $\mathbb{G}_m$ action.

1975 :	21	- N. EL KAROUI - H. REINHARD - Compactification et balayage de processus droits.
	22-23	- Ph. COURRÈGE - P. PRIOURET - P. RENOUARD - M. YOR - Oscillateur anharmonique, processus de diffusion et mesures quasi-invariantes.
	24-25	- Journées arithmétiques de Bordeaux (1974).
	26	- J. LANNES - F. LATOUR - Forme quadratique d'enlacement et applications.
	27	- R. CORI - Un code pour les graphes planaires et ses applications.
	28-29	- A. DENJOY - Évocation de l'homme et de l'œuvre.
	30	- R. ROUSSARIE - Modèles locaux de champs et de formes.

1976 :	31	- J. E. FRANKE - S. NEWHOUSE - J. PALÍS - M. M. PEIXOTO - Trois études en dynamique qualitative.
	32-33	- Colloque Analyse et Topologie en l'honneur de H. CARTAN, 2^{e} édition.
	34-35	- Journées "Équations aux dérivées partielles" de Rennes.
	36-37	- A. DOUADY - J.-L. VERDIER - Séminaire de géométrie analytique.
	38-39	- Journées Algorithmiques (Paris, 1975).
	40	- International Conference on Dynamical Systems in Mathematical Physics (Rennes, 1975).

1977 :	41-42	- Journées Arithmétiques de Caen (1976).
	43-44	- Théorie de la robustesse et estimation d'un paramètre (Orsay-Paris VII, 1974-1975).
	45	- D. LEHMANN - Théorie homotopique des formes différentielles (d'après D. Sullivan).
	46	- J.-P. SERRE - Arbres, amalgames, SL_2, 3^{e} édition.
	47-48	- J.-M. FONTAINE - Groupes p- divisibles sur les corps locaux.
	49	- Dynamical Systems I, Warsaw (1977), 2^{e} édition.
	50	- Dynamical Systems II, Warsaw (1977), 2^{e} édition.

1978 :	51	- Dynamical Systems III, Warsaw (1977), 2^{e} édition.
	52-53	- Temps locaux (Paris VI, 1976-1977).
	54	- A. BEAUVILLE - Surfaces algébriques complexes, 3^{e} édition.
	55	- Représentations des groupes localement compacts et applications aux algèbres d'opérateurs (Orléans, 1973-1974).
	56	- M. SHUB - Stabilité globale des systèmes dynamiques, 2^{e} édition.
	57	- R. R. COIFMAN - Y. MEYER - Au-delà des opérateurs pseudo-différentiels, 2^{e} édition.
	58	- Première classe de Chern et courbure de Ricci : preuve de la conjecture de Calabi (Séminaire Palaiseau, 1978), 2^{e} édition.
	59-60	- Journées singulières de Dijon.

1979 :	61	- Journées Arithmétiques de Luminy (1978).
	62	- P. DOMBROWSKI - 150 Years after Gauss' "disquisitiones generales circa superficies curvas", 2^{e} édition.
	63	- Journées de Géométrie Algébrique de Rennes (juillet 1978), I.
	64	- Journées de Géométrie Algébrique de Rennes (juillet 1978), II.
	65	- Journées de Géométrie Algébrique de Rennes (juillet 1978), III.
	66-67	- Travaux de Thurston sur les surfaces (Séminaire Orsay).
	68	- Grandes déviations et applications statistiques (Séminaire Orsay, 1977-1978).
	69-70	M. WALDSCHMIDT - Nombres transcendants et groupes algébriques (2^{e} édition).

1980 :	71-72	- Les équations de Yang-Mills (Séminaire E.N.S., 1977-1978).
	73	- Modèles de l'arithmétique (Séminaire Paris VII) - K. MC ALOON.
	74	- Journées sur les marches aléatoires (Nancy, 1979).
	75-76	- Analyse des systèmes (Bordeaux, 11-16 septembre 1978).
	77	- R. R. COIFMAN - R. ROCHBERG - M. H. TAIBLESON - G. WEISS - Representation theorems for Hardy spaces.
	78	- A. LOUVEAU - Ensembles analytiques et boréliens dans les espaces produits.
	79	- N. KATZ - Sommes exponentielles, rédigé par G. LAUMON.
	80	- Analyse sur les variétés (Metz, 1979).

1981 :	81	- P. BUSER and H. KARCHER - Gromov's almost flat manifolds.
	82-83	- Caractéristique d'Euler-Poincaré (Séminaire E.N.S. 1978-1979).
	84-85	- Géodésiques et diffusions en temps petit (Séminaire de probabilités, université de Paris VII).
	86	- Séminaire sur les pinceaux de courbes de genre au moins deux (L. SZPIRO).
	87-88	- Tableaux de Young et foncteurs de Schur en algèbre et géométrie (Toruń, 1980).
	89-90	- Analytic solutions of partial differential equations (Trento, 1981).

1982 :	91	- C. DE CONCINI, D. EISENBUD, C. PROCESI - Hodge Algebras.
	92-93	- SÉMINAIRE BOURBAKI, volume 1981/82, exposés 579-596.
	94	- JOURNÉES ARITHMÉTIQUES, Metz (1981).
	95	- J. SJÖSTRAND - Singularités analytiques microlocales (suivi d'un texte avec B. LASCAR sur l'équation de Schrödinger).
	96	- C. S. SESHADRI - Fibrés vectoriels sur les courbes algébriques (rédigé par J.-M. DREZET).
	97	- D. CERVEAU, J.-F. MATTEI - Formes intégrables holomorphes singulières.
	98-99	- Bifurcation, théorie ergodique et applications (Dijon, juin 1981).
	100	- Analyse et topologie sur les espaces singuliers (CIRM 1981) - Vol. I.

1983 : 101-102 - Analyse et Topologie sur les espaces singuliers (CIRM, 1981) - Vol. II - III.
103-104 - M. R. HERMAN - Sur les courbes invariantes par les difféomorphismes de l'anneau, Vol. 1.
105-106 - SÉMINAIRE BOURBAKI, volume 1982/83, exposés 597-614.
107-108 - III^{e} rencontre de géométrie du Schnepfenried (mai 1982), Vol. 1.
109-110 - III^{e} rencontre de géométrie du Schnepfenried (mai 1982), Vol. 2.

1984 : 111 - J. HARTHONG - Études sur la mécanique quantique.
112 - B. HELFFER - Théorie spectrale pour des opérateurs globalement elliptiques.
113-114 - Homotopie algébrique et algèbre locale (CIRM, 1982), J. M. LEMAIRE, J. C. THOMAS.
115 - M. H. SLIMAN - Théorie de Mackey pour les groupes adéliques.
116 - Structure transverse des feuilletages, Toulouse 1982.
117 - J. LIPMAN - Dualizing sheaves, differentials and residues on algebraic varieties.
118 - Variational methods for equilibrium problems of fluids, Trento 1983.
119-120 - Cohomologie p-adique.

1985 : 121-122 - SÉMINAIRE BOURBAKI, volume 1983/84, exposés 615-632.
123 - B. A. KUPERSHMIDT - Discrete lax equations and differential-difference calculus.
124-125 - Homologie, groupes Ext^{n}, représentations de longueur finie des groupes de Lie.
126 - Géométrie des surfaces K3 : modules et périodes. Séminaire Palaiseau.
127 - Séminaire sur les Pinceaux Arithmétiques : la conjecture de Mordell (L. SZPIRO).
128 - M. KASHIWARA, P. SCHAPIRA - Microlocal study of sheaves.
129 - L. MORET-BAILLY - Pinceaux de variétés abéliennes.
130 - Systèmes différentiels et singularités (C.I.R.M. 1983) édité par A. GALLIGO, M. GRANGER, Ph. MAISONOBE.
131 - Colloque en l'honneur de L. SCHWARTZ, Volume 1.
132 - Colloque en l'honneur de L. SCHWARTZ, Volume 2.
N° hors série : Elie Cartan et les mathématiques d'aujourd'hui - Lyon, 25-29 juin 1984.

1986 : 133-134 - SÉMINAIRE BOURBAKI, volume 1984/85, exposés 633-650.
135-136 - Analyse harmonique des mesures, B. HOST, J.-F. MÉLA, F. PARREAU.
137 - K. HULEK - Projective geometry of elliptic curves.
138-139 - M. CHAPERON - Géométrie différentielle et singularités de systèmes dynamiques.
140-141 - J.-L. BRYLINSKI, T. MONTEIRO FERNANDES - Géométrie et analyse microlocales.
142-143 - M. ENGUEHARD, T. PETERFALVI - Révision dans les groupes finis. Groupes du type de Lie de rang 1.
144 - M. R. HERMAN - Sur les courbes invariantes par les difféomorphismes de l'anneau, Vol. 2.

1987 : 145-146 - SÉMINAIRE BOURBAKI, volume 1985/86, exposés 651-668.
147-148 - JOURNÉES ARITHMÉTIQUES, Besançon (24-28 juin 1985).

INSTRUCTIONS AUX AUTEURS

ASTÉRISQUE, revue éditée par la Société Mathématique de France, est reproduit par procédé offset. Ceci exclut toute possibilité d'y apporter des modifications ultérieures. Si un manuscrit ne se prête pas à la reproduction directe, il sera retourné pour une nouvelle frappe. De ce fait, les indications suivantes doivent être scrupuleusement suivies :

La frappe doit être effectuée sur des feuilles imprimées spéciales qui peuvent être fournies sur demande au Secrétariat*. Le texte doit tenir dans le cadre complet (format dactylographié 18 × 25,5 cm), le trait de pagination se situant en bas du texte.

Les manuscrits doivent être tapés avec interligne de 1 1/2. Pour obtenir une reproduction convenable, il est recommandé de se servir d'une machine électrique (par exemple d'utiliser une boule IBM 72 " courrier ", le texte étant tapé avec caractères pica 10 frappés avec espacement de 10). Ne pas laisser de " blancs " inutiles, pour respecter une densité de texte ; nous conseillons de prévoir un minimum de 27 lignes dactylographiées par page.

Les corrections ne doivent être faites qu'avec du blanc couvrant ou par découpage. Tous les symboles qui ne sont pas tapés à la machine doivent être tracés soit avec un stylet à l'encre de chine, soit avec un stylo-bille fin noir ; ne pas souligner avec des couleurs.

Il serait prudent, avant de poursuivre la frappe, d'adresser au Secrétariat de la Revue, une copie des 5 ou 6 premières pages du chapitre I (et non de l'introduction) à l'adresse mentionnée ci-dessous.

(*) Société Mathématique de France - Revue Astérisque - B.P. 126-05 - 75226 PARIS CEDEX.

PRÉSENTATION D'UN MANUSCRIT

1) Table des matières

2) Texte

3) Bibliographie
Les références bibliographiques doivent être numérotées, complètes et exactes, citées par ordre alphabétique.

4) Abstract ou résumé en français ou en anglais

5) Le début de chaque paragraphe se place à 3, 4 ou 5 espaces du bord du cadre.
Les textes des théorèmes, propositions, etc. sont soulignés (pas de soulignement sous la ponctuation, ni sous les symboles mathématiques).
Les accents doivent être mis sur les titres en majuscules.
Ne pas paginer à la machine, *mais au crayon hors du cadre.*

6) Pour un colloque ou séminaire, *à chaque exposé ou conférence* :
— prévoir, avant le titre, un espace en haut du cadre (interligne 2) pour les références de publication ;
— en fin de texte, placer, à droite de celui-ci, le nom, prénom et adresse professionnelle de l'auteur.

INSTRUCTIONS TO AUTHORS

The journal ASTERISQUE, published by the Société Mathématique de France, uses the offset process of reproducing manuscripts photographically, so that late changes at the proof stage are excluded. Any manuscript not suitable for direct reproduction will be returned for retyping. Because of this, the following instructions should be carefully observed :

Manuscripts must be typed on specially prepared paper available on demand from the secretary*. The text must remain in the indicated frame (18 × 25.5 cm) ; page numbers will be added below the text.

Manuscripts must be typed with 1 1/2 spaces between lines. An electric typewriter is recommended (with, for instance, an IBM 72 "Courrier" ball, using Pica 10 characters on 10 spacing). Avoid wasting space unnecessarily : we suggest a minimum of 27 typed lines per page.

Corrections must be made with white correcting fluid or by cutting. All symbols which are not typed must be traced carefully with Indian ink or with a fine black ball-point pen ; do not underline in colour.

We suggest sending the first of 5 or 6 pages of the first chapter (not the introduction) to the address below for approval before typing the remainder of the text.

(*) Société Mathématique de France - Revue Astérisque - B.P. 126-05 - 75226 PARIS CEDEX.

PRESENTATION OF A MANUSCRIPT

1) Table of contents

2) Text

3) Bibliography
Bibliographical references must be numbered, exact and complete, and listed in alphabetical order.

4) Abstract in French or in English

5) Each new paragraph should begin either 3, 4 or 5 spaces from the edge of the indicated frame.
Statements of theorems, propositions, and so on... should be underlined (but do not underline punctuation, nor mathematical symbols).
Accents on capital letters should not be omitted.
Do not type page numbers. They should be written in pencil outside the rectangular frame.

6) In the case of a conference or a seminar, for *each talk or lecture* :
— leave 2 blank lines above the title to allow for bibliographical details ;
— at the end of the text, give the surname, christian name and professional address of the author on the right-hand side of the page.