Werk

Titel: Equations diophantiennes exponentielles.

Autor: Laurent, Michel

Jahr: 1984

PURL: https://resolver.sub.uni-goettingen.de/purl?356556735_0078|log19

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Invent. math. 78, 299–327 (1984)

Inventiones mathematicae

Equations diophantiennes exponentielles

Michel Laurent

Institut Henri Poincaré, 11 rue Pierre et Marie Curie, Paris V^e, France

§ 1. Introduction

Soit G un groupe algébrique commutatif, défini sur le corps $\mathbb{C}$ des nombres complexes, dont la loi de groupe est notée multiplicativement. On suppose que G ne contient pas de sous-groupe algébrique isomorphe au groupe additif $\mathbb{G}_a$. Soit Γ un sous-groupe de $G(\mathbb{C})$, de rang fini, c'est-à-dire tel qu'il existe un sous-groupe Γ' de Γ, de type fini, et tel que le groupe quotient Γ/Γ' soit de torsion. Soit enfin V une sous-variété algébrique de G. Sous ces hypothèses, S. Lang ([3], p. 220) a formulé la

Conjecture. *L'ensemble $V \cap \Gamma$ est réunion finie de sous-ensembles de la forme $\gamma(H \cap \Gamma)$, où γ désigne un élément de Γ et H un sous-groupe algébrique de G, tels que $\gamma H \subseteq V$.*

Nous nous proposons de vérifier cette conjecture lorsque G est un tore linéaire, ce que nous supposerons désormais.

Le cas particulier où V est une courbe et Γ un sous-groupe de type fini a été établi par S. Lang ([3], Chap. 8, § 3). Ce résultat a ensuite été étendu par P. Liardet à un sous-groupe de rang fini ([4], th. 4 bis et [3], chap. 8, § 7). Tous deux utilisent de façon essentielle le théorème d'approximation de Thue-Siegel-Roth: celui-ci est employé directement par Liardet dans son travail, tandis que Lang passe par l'intermédiaire du théorème de Siegel sur les points entiers des courbes algébriques. Notons que C. Chabauty avait énoncé auparavant une telle conjecture (remarque de la p. 166 de [1]), dans le cas particulier où Γ est le groupe des unités d'un corps de nombres K, considéré comme sous-groupe du tore linéaire G obtenu à partir du groupe multiplicatif $\mathbb{G}_m$ par restriction des scalaires de K à $\mathbb{Q}$ (voir le § 8). Il avait obtenu des résultats dans ce cadre, grâce à des arguments p-adiques (méthode de Skolem).

Le résultat principal obtenu ici est le théorème 2 du § 3, qui démontre et précise la conjecture ci-dessus de la façon suivante. On donne tout d'abord une description explicite des sous-groupes H intervenant dans cet énoncé. Remarquons que dans un tore linéaire G (de caractéristique 0), il y a cor-

respondance bijective entre les sous-groupes algébriques H de G et les sous-groupes $\hat{H}$ du groupe des caractères algébriques de G, le sous-groupe H étant égal à l'intersection des noyaux des éléments de $\hat{H}$. En d'autres termes, si l'on choisit une présentation déployée de G, tout sous-groupe algébrique H de G, est défini par un système d'équations monomiales. Les «directions» H possibles sont alors en nombre fini, et leurs équations monomiales sont déterminées explicitement à partir des diverses partitions $\mathscr{P}$ du *support* $\mathscr{L}$ d'un système d'équations définissant la variété V (voir le §3). De plus, si H est ainsi associé à la partition $\mathscr{P}$, «l'origine» γ appartient nécessairement à une sous-variété $V_{\mathscr{P}}$ de V, fibrée par H, obtenue en scindant les équations définissant V suivant la partition $\mathscr{P}$. On utilise alors un résultat intermédiaire (le théorème 1 du §2), qui peut être vu essentiellement comme un corollaire des travaux de W. Schmidt (Chap. 6 de [11]) et de H.P. Schlickewei ([8]) généralisant le théorème de Thue-Siegel-Roth. De façon inverse, notons que le théorème 1 se déduit du théorème 2, lorsque V est un hyperplan et Γ un groupe produit.

Dans les §4 à 7, nous examinons les questions d'effectivité que pose naturellement le théorème 2. Nous avons décomposé $V \cap \Gamma$ en un nombre fini de classes $\gamma(H \cap \Gamma)$, dont les directions $H \cap \Gamma$ sont bien déterminées. Par contre, les origines γ ne sont définies que modulo le sous-groupe $H \cap \Gamma$. Dans les théorèmes 3 et 4, nous montrons qu'il est possible de choisir une origine γ dans une telle classe, ayant une hauteur $H_{\varphi}(\gamma)$, (définie au §4), comparable à celle des polynômes définissant la variété V.

Grâce à un tel contrôle quantitatif, nous pouvons alors déduire du théorème 2 des résultats généraux concernant la structure des solutions d'un système d'équations exponentielles mixtes, par exemple, les équations exponentielles-polynômes (théorèmes 5 et 6 du §8). Toute solution d'un tel système se décompose en produit de deux termes: le premier facteur est prépondérant et ne dépend que de la structure multiplicative du système considéré, tandis que le deuxième facteur, qui peut être considéré comme un terme reste, dépend de la «croissance» des coefficients du système.

Enfin, dans le §9, nous retrouvons les résultats classiques de W. Schmidt sur les équations normiques (Chap. 7 de [11]), comme corollaire de la description explicite fournie par le théorème 2, dans le cas particulier où V est une variété linéaire.

§2. Some d'unites

Nous nous proposons de montrer ici le

Théorème 1. *Soient l un entier $\geqq 1$, Δ un sous-groupe de rang fini de $\mathbb{C}^*$. A homothétie près, il n'y a qu'un nombre fini de l-uplets $U=(u_1, \ldots, u_l)$, tels que*

i) *$u_1, \ldots, u_l$ appartiennent à Δ;*

ii) *$u_1 + \ldots + u_l = 0$;*

iii) *toute somme partielle des $u_1, \ldots, u_l$ est non nulle.*

Lorsque Δ est un groupe de type fini, le théorème a été prouvé indépendamment par J.H. Evertse [2], et par H.P. Schlickewei, A.J. Van der

Poorten [10], grâce à des arguments diophantiens (essentiellement le «théorème du sous-espace» du § 3, Chap. 6 de [11]). Désignons par Δ' un sous-groupe de type fini de Δ, tel que le quotient Δ/Δ' soit un groupe de torsion. Nous allons nous ramener au cas particulier des groupes de type fini, en construisant par extensions successives du groupe Δ', un groupe de type fini Δ'', tel que tout l-uplet U vérifiant i), ii), iii) soit homothétique à un l-uplet U'' dont les coordonnées appartiennent à Δ''. Nous utiliserons pour cela, des arguments de théorie de Kummer.

2.1. Donnons tout d'abord quelques résultats généraux de nature galoisienne.

Soit K un corps de type fini sur $\mathbb{Q}$. Dans tout le § 2, G désignera le groupe $\mathrm{Gal}(\bar{K}/K)$ d'une clôture algébrique $\bar{K}$ de K. Pour tout entier $n \geqq 1$, notons $\mu_n \subseteq \bar{K}^*$ le groupe des racines n-ièmes de l'unité et

$$G_n = \mathrm{Gal}(K(\mu_n)/K).$$

Le groupe G_n agit par exponentiation sur le groupe μ_n, ce qui permet d'identifier G_n, de la manière usuelle, à un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$. Soit

$$n = \prod_p p^{\nu_p}$$

la décomposition de n en facteurs premiers. L'isomorphisme canonique

$$(\mathbb{Z}/n\mathbb{Z})^* \xrightarrow{\sim} \prod_p (\mathbb{Z}/p^{\nu_p}\mathbb{Z})^*$$

nous permet aussi d'identifier G_n à un sous-groupe du produit ci-dessus.

Pour tout nombre premier p, tout entier $r \geqq 0$ et $s \geqq 1$, désignons par $\Omega_p^{r,s}$ le sous-groupe de $(\mathbb{Z}/p^s\mathbb{Z})^*$ formé des unités x qui sont de la forme

$$x = 1 + p^r y, \qquad y \in \mathbb{Z}/p^s\mathbb{Z}.$$

Lemme 1. *Il existe une suite d'entiers $m_p \geqq 0$, p décrivant l'ensemble des nombres premiers, nulle pour presque tout p, telle que pour tout entier $n = \prod_p p^{\nu_p}$ le groupe G_n contienne le sous-groupe*

$$\Omega_n = \prod_p \Omega_p^{m_p, \nu_p}.$$

Preuve. En d'autres termes, par passage à la limite projective sur n, il s'agit de montrer que l'image du groupe G dans le produit $\prod_p \mathbb{Z}_p^*$ est ouverte.

La propriété est bien connue lorsque K est un corps de nombres. Dans le cas général, désignons par K_0 la clôture algébrique de $\mathbb{Q}$ dans K. Alors K_0 est un corps de nombres. De plus, les extensions $\bar{\mathbb{Q}}/K_0$ et K/K_0 sont linéairement disjointes. La suite m_p associée à K_0 convient alors aussi pour le corps K. □

Le groupe de Galois G_n agit sur le groupe μ_n qui est ainsi muni d'une structure de G_n-module. On a alors le

Lemme 2. *Le cardinal de $H^1(G_n, \mu_n)$ est borné indépendamment de n.*

Preuve. Remarquons tout d'abord que l'on peut supposer sans restriction que l'entier m_2 fourni par le lemme 1 est $\geqq 2$. Pour tout nombre premier p et tout entier $v \geqq 1$, le groupe $\Omega_p^{m_p, v}$ est alors cyclique et il est facile de vérifier que le groupe de cohomologie

$$H^1(\Omega_p^{m_p, v}, \mu_{p^v}) = \{1\}.$$

Soit $n = \prod_p p^{v_p}$ la décomposition de n en facteurs premiers. La décomposition associée $\mu_n = \prod_p \mu_{p^{v_p}}$ induit un isomorphisme canonique

$$H^1(\Omega_n, \mu_n) \xrightarrow{\sim} \prod_p H^1(\Omega_p^{m_p, v_p}, \mu_{p^{v_p}})$$

d'où l'on déduit que $H^1(\Omega_n, \mu_n) = \{1\}$. La suite exacte d'inflation-restriction de G_n à Ω_n

$$1 \longrightarrow H^1(G_n/\Omega_n, \mu_n^{\Omega_n}) \xrightarrow{\text{Inf}} H^1(G_n, \mu_n) \xrightarrow{\text{Res}} H^1(\Omega_n, \mu_n)$$

montre alors que

$$H^1(G_n, \mu_n) \xrightarrow{\sim} H^1(G_n/\Omega_n, \mu_n^{\Omega_n}).$$

Désignons par ϕ la fonction indicatrice d'Euler et notons

$$a = \prod_p p^{m_p}.$$

Le cardinal de G_n/Ω_n est $\leqq \phi(a)$ et le sous-groupe $\mu_n^{\Omega_n}$ des éléments de μ_n invariants sous l'action de Ω_n est égal à μ_a. L'ordre de ce dernier groupe de cohomologie est donc borné. □

2.2. Dans une première étape, nous allons montrer le résultat suivant

Il existe un sous-groupe de type fini $\Delta_1 \subseteq \Delta$, tel que tout l-uplet $U = (u_1, \ldots, u_l)$ satisfaisant les conditions i), ii), iii) *soit homothétique à un l-uplet U'' dont les coordonnées u_i'' sont de la forme*

$$u_i'' = \zeta_i u_i', \qquad (1 \leqq i \leqq l),$$

où ζ_i désigne une racine de l'unité et où $u_i' \in \Delta_1$.

Preuve. Fixons un sous-corps $K \subseteq \mathbb{C}$, de type fini sur $\mathbb{Q}$, contenant le groupe de type fini $\Delta' \subseteq \Delta$. On pourra supposer sans restriction que la première coordonnée $u_1 = 1$.

Choisissons un entier $n \geqq 1$, tel que les nombres

$$v_i = u_i^n \qquad (1 \leqq i \leqq l),$$

appartiennent à Δ', et désignons par f_i les 1-cocycles continus de G à valeur dans μ_n définis par

$$f_i(\sigma) = \sigma u_i / u_i, \qquad \text{pour } \sigma \in G,\ 1 \leqq i \leqq l.$$

La théorie de Kummer établit un isomorphisme canonique entre les groupes $H^1(G, \mu_n)$ et $K^*/(K^*)^n$, qui associe précisément à la classe de cohomologie du cocycle f_i, la classe $v_i \bmod (K^*)^n$.

Conjugant alors l'équation ii), nous obtenons les relations

$$\sum_{i=1}^{l} u_i f_i(\sigma) = 0, \quad \text{pour tout } \sigma \in G.$$

Soit $H_n = \mathrm{Gal}(\bar{K}/K(\mu_n))$ et soit χ_i $(1 \leqq i \leqq l)$ la restriction de f_i à H_n. Puisque H_n agit trivialement sur μ_n, les cocycles χ_i sont des caractères du groupe H_n. Les relations ci-dessus, restreintes à H_n, induisent l'identité

$$\sum_{i=1}^{l} u_i \chi_i = 0.$$

Regroupant dans cette équation les caractères χ_i égaux, on obtient une relation de dépendance linéaire entre caractères distincts, dont les coefficients sont somme de tout ou partie des u_i. Si la suite $\chi_1, \ldots, \chi_l$ contient au moins deux caractères distincts, ces coefficients sont tous non nuls, d'après la condition iii). Le théorème d'Artin nous affirme alors que cette hypothèse est impossible. Les caractères χ_i sont donc tous égaux à $\chi_1 = 1$. Autrement dit, les classes de cohomologie des cocycles f_i appartiennent au noyau de l'application de restriction de G_n à H_n. La suite exacte d'inflation-restriction

$$1 \longrightarrow H^1(G_n, \mu_n) \xrightarrow{\text{Inf}} H^1(G, \mu_n) \xrightarrow{\text{Res}} H^1(H_n, \mu_n) = \mathrm{Hom}(H_n, \mu_n)$$

identifie alors ce noyau à $H^1(G_n, \mu_n)$. D'après le lemme 1, l'ordre de ce groupe est borné indépendamment de n. Il existe donc un entier $b \geqq 1$, ne dépendant que de K, tel que les classes de cohomologie des cocycles f_i^b, $(1 \leqq i \leqq l)$, soient nulles. Les nombres v_i^b appartiennent alors à $(K^*)^n$ et l'on a

$$u_i^{bn} = v_i^b = w_i^n, \quad \text{avec } w_i \in K^*, \ (1 \leqq i \leqq l).$$

Désignons par Δ'_∞ le sous-groupe de $\mathbb{C}^*$ formé des nombres complexes z dont une puissance z^k, $k \in \mathbb{Z}$, $k \neq 0$, appartient à Δ'. D'après le lemme 7.1 du § 8 de [3], le sous-groupe $\Delta'_\infty \cap K^*$ est de type fini. Par construction, les nombres complexes w_i $(1 \leqq i \leqq l)$ appartiennent à ce sous-groupe. On a alors la décomposition

$$u_i = \zeta_i u_i', \quad (1 \leqq i \leqq l),$$

où ζ_i est une racine de l'unité et où $u_i' = w_i^{1/b}$ appartient au sous-groupe de type fini

$$\Delta_1 = (\Delta'_\infty \cap K^*)^{1/b}. \quad \square$$

2.3. Utilisant une idée de H. Mann [5], nous allons maintenant contrôler, après homothétie convenable, l'ordre des racines de l'unité ζ_i apparaissant dans la section 2.2.

Après extension de type fini du corps K, on peut supposer sans restriction que $\Delta_1 \subseteq K$. Fixons alors une suite d'entiers (m_p) vérifiant le lemme 1, et désignons par S la réunion de l'ensemble des nombres premiers $\leqq l$ et de l'ensemble des nombres premiers p tels que $m_p \geqq 1$. Cet ensemble S est fini. On notera μ_S le sous-groupe de $\bar{K}^*$, formé des racines de l'unité dont l'ordre est un produit de puissances d'éléments de S. Dans cette deuxième étape, nous allons montrer que:

Tout l-uplet $U=(u_1, \ldots, u_l)$ *satisfaisant les conditions* i), ii), iii) *est homothétique à un l-uplet* U'' *dont les coordonnées* u_i'' *sont de la forme*

$$u_i''=\zeta_i u_i', \quad (1 \leqq i \leqq l),$$

avec $\zeta_i \in \mu_S$ *et* $u_i' \in \Delta_1$.

Preuve. D'après la section 2.2, on peut supposer que

$$u_i=\zeta_i u_i', \quad (1 \leqq i \leqq l),$$

où ζ_i est une racine de l'unité et où $u_i' \in \Delta_1$. Désignons maintenant par n un multiple commun des ordres des racines de l'unité ζ_i, $(1 \leqq i \leqq l)$, et décomposons $n=\prod p^{v_p}$ en facteurs premiers.

Fixons un facteur premier p et désignons par ζ une racine primitive de l'unité d'ordre p^{v_p}. Chaque racine ζ_i se décompose alors, de façon unique, en un produit

$$\zeta_i=\xi_i \zeta^{s_i}, \quad 0 \leqq s_i < p^{v_p}, \ (1 \leqq i \leqq l),$$

où ξ_i est une racine de l'unité d'ordre premier à p. Nous allons montrer que, si $p \notin S$, les exposants s_i sont tous égaux, disons à s. Par l'homothétie de rapport ζ^{-s}, on éliminera ainsi la partie p-primaire des racines de l'unité ζ_i $(1 \leqq i \leqq l)$, pour tout premier $p \notin S$.

Notons, pour simplifier, $v_p=v$ et effectuons la division euclidienne de s_i par p^{v-1}:

$$s_i=q_i p^{v-1}+r_i, \quad 0 \leqq r_i < p^{v-1}, \quad 0 \leqq q_i < p, \quad (1 \leqq i \leqq l).$$

Puisque $p > l$, il existe un entier q, $0 \leqq q < p$, qui n'apparaît pas dans la suite des quotients $q_1, \ldots, q_l$. En multipliant alors tous les ζ_i par $\zeta^{-(1+q)p^{v-1}}$, on peut supposer que $q=p-1$. On a alors la majoration

$$s_i \leqq (p-2)p^{v-1}+r_i < p^v - p^{v-1} = \phi(p^v), \quad (1 \leqq i \leqq l).$$

Supposons que les exposants s_i $(1 \leqq i \leqq l)$ ne soient pas tous égaux. Alors le polynôme

$$P(X)=\sum_{i=1}^{l} u_i' \xi_i X^{s_i}$$

est non identiquement nul. En effet, le coefficient p_σ du monôme X^σ dans P est égal à $\sum_{s_i=\sigma} u_i' \xi_i$. On a donc

$$\zeta^\sigma p_\sigma = \sum_{s_i=\sigma} u_i' \xi_i \zeta^{s_i} = \sum_{s_i=\sigma} u_i.$$

D'après la condition iii), les coefficients p_σ ne sont pas tous nuls.

D'autre part, les coefficients du polynôme P appartiennent au corps $K(\xi_1, \ldots, \xi_l)$ et l'on a

$$P(\zeta) = \sum_{i=1}^{l} u_i' \xi_i \zeta^{s_i} = \sum_{i=1}^{l} u_i = 0.$$

Il s'ensuit que P est divisible par le polynôme minimal de ζ sur le corps $K(\xi_1, \ldots, \xi_l)$. Comme $m_p = 0$, $(p \notin S)$, l'extension $K(\xi_1, \ldots, \xi_l, \zeta)/K(\xi_1 \ldots \xi_l)$ est, d'après le lemme 1, de degré maximal $\phi(p^\nu)$. Ceci est impossible puisque le degré de P est majoré par

$$\max_i (s_i) < \phi(p^\nu). \quad \square$$

2.4. Soient (m_p) et S comme ci-dessus. Notons

$$m_p' = \max(1, m_p), \qquad c = \prod_{p \in S} p^{m_p'},$$

et considérons le groupe de type fini

$$\Delta'' = \mu_c \Delta_1.$$

Alors tout l-uplet $U = (u_1, \ldots, u_l)$ *satisfaisant les conditions* i), ii) iii) *est homothétique à un l-uplet* U'' *dont les coordonnées appartiennent à* Δ''.

Preuve. D'après la section 2.3, on peut supposer que

$$u_i = \zeta_i u_i', \qquad (1 \leqq i \leqq l),$$

où $u_i' \in \Delta_1$ et $\zeta_i \in \mu_S$. Désignons par

$$n = \prod_p p^{\nu_p}$$

le plus petit multiple commun de c et des ordres des racines de l'unité ζ_i, $(1 \leqq i \leqq l)$. Soit ζ une racine primitive de l'unité d'ordre n. Les racines ζ_i se mettent alors sous la forme

$$\zeta_i = \zeta^{s_i}, \quad 0 \leqq s_i < n, \quad (1 \leqq i \leqq l).$$

Notons $m = n/c$ et effectuons, cette fois-ci, la division euclidienne de s_i par m:

$$s_i = q_i m + r_i, \quad 0 \leqq r_i < m, \quad (1 \leqq i \leqq l).$$

On en déduit une décomposition de ζ_i en produit

$$\zeta_i = \xi_i \zeta^{r_i}, \qquad (1 \leqq i \leqq l)$$

où $\xi_i = \zeta^{q_i m}$ appartient à μ_c. Comme précédemment, nous allons montrer que tous les exposants r_i sont égaux. Supposons qu'il n'en soit pas ainsi. Alors le polynôme

$$P(X) = \sum_{i=1}^{l} u_i' \xi_i X^{r_i}$$

est non identiquement nul (même démonstration qu'en 2.3). Les coefficients du polynôme P appartiennent au corps $K(\mu_c)$. De plus

$$P(\zeta)=\sum_{i=1}^{l} u_i' \xi_i \zeta^{r_i}=\sum_{i=1}^{l} u_i=0.$$

Il s'ensuit que P divise le polynôme minimal de ζ sur $K(\mu_c)$.

D'autre part, avec les notations du lemme 1, le groupe de Galois de $K(\mu_n)$ sur $K(\mu_c)$, vu comme sous-groupe de G_n, s'identifie au produit

$$\prod_p \Omega_p^{m_p', v_p}.$$

En particulier, l'extension $K(\mu_n)/K(\mu_c)$ est de degré maximal $m=n/c$. D'où la contradiction, puisque le degré de P est majoré par

$$\max_i (r_i)<m. \quad \square$$

§ 3. Preuve de la conjecture

3.1. On peut supposer sans restriction que le tore linéaire G est déployé et on identifiera $G(\mathbb{C})$ à $(\mathbb{C}^*)^n$ muni de la structure de groupe produit. Si $X=(X_1, \ldots, X_n)$ désigne l'élément générique de $G(\mathbb{C})$ et $\lambda=(\lambda_1, \ldots, \lambda_n)$ désigne un n-uplet d'entiers $\geqq 0$, on notera de la façon usuelle

$$X^\lambda = X_1^{\lambda_1} \ldots X_n^{\lambda_n}.$$

Soit

$$P_i(X)=\sum_{\lambda \in \mathscr{L}_i} p_i(\lambda) X^\lambda = 0, \quad (i \in I),$$

un système d'équations de la variété V, où $\mathscr{L}_i$ désigne le *support* du polynôme P_i, c'est-à-dire l'ensemble des exposants λ pour lesquels le coefficient $p_i(\lambda)$ du monôme X^λ dans le polynôme P_i, est non nul. Il est commode de considérer le *support* $\mathscr{L}$ de ce système d'équations, c'est-à-dire la réunion disjointe

$$\mathscr{L}=\coprod_{i \in I} \mathscr{L}_i$$

des ensembles $\mathscr{L}_i$. Une partition $\mathscr{P}$ de $\mathscr{L}$ équivaut donc à la donnée de partitions

$$\mathscr{L}_i=\coprod_{j \in J_i} \mathscr{L}_{i,j}$$

pour chacun des ensembles $\mathscr{L}_i$.

Nous dirons qu'une telle partition $\mathscr{P}$ est *compatible* avec un élément $\gamma \in \Gamma$ si

$$\sum_{\lambda \in \mathscr{L}_{i,j}} p_i(\lambda) \gamma^\lambda = 0 \tag{1}$$

pour tout couple d'indices $i \in I$ et $j \in J_i$. De plus, si toute partition $\mathscr{P}'$ de $\mathscr{L}$ plus fine que $\mathscr{P}$, n'est pas compatible avec γ, autrement dit, si pour tout $i \in I$, $j \in J_i$ et

pout toute partie propre $\mathscr{L}' \subset \mathscr{L}_{i,j}$, on a

$$\sum_{\lambda \in \mathscr{L}'} p_i(\lambda)\, \gamma^{\lambda} \neq 0, \tag{2}$$

nous dirons que la partition $\mathscr{P}$ est *compatible maximale* avec γ.

Pour toute partition $\mathscr{P}$ de $\mathscr{L}$, désignons par $H_{\mathscr{P}}$ le sous-groupe algébrique de G, défini par le système d'équations

$$X^{\lambda} = X^{\lambda'}, \tag{3}$$

pour tout couple d'éléments λ, λ' appartenant à un même sous-ensemble $\mathscr{L}_{i,j}$.

Nous pouvons maintenant énoncer et démontrer une version plus précise de la conjecture de S. Lang:

Théorème 2. *Il existe un nombre fini de couples* $(\gamma, \mathscr{P})$, *formés d'une partition* $\mathscr{P}$ *de* $\mathscr{L}$, *compatible maximale avec* $\gamma \in \Gamma$, *tels que*

$$V \cap \Gamma = \bigcup_{(\gamma, \mathscr{P})} \gamma(H_{\mathscr{P}} \cap \Gamma).$$

3.2. Désignons par $\mathscr{T}$ l'ensemble des parties T de V de la forme γH, où γ désigne un élément de Γ et H un sous-groupe algébrique de G.

Lemme 3. *Les éléments maximaux de l'ensemble* $\mathscr{T}$, *ordonné par inclusion, sont de la forme* $\gamma H_{\mathscr{P}}$, *où la partition* $\mathscr{P}$ *de* $\mathscr{L}$ *est compatible maximale avec* $\gamma \in \Gamma$.

Preuve. Remarquons tout d'abord que si la partition $\mathscr{P}$ de $\mathscr{L}$ est compatible avec $\gamma \in \Gamma$, l'ensemble $\gamma H_{\mathscr{P}}$ est contenu dans V, et appartient donc à $\mathscr{T}$. Cela résulte de (1) et (3).

Pour tout exposant λ, notons χ_λ le caractère algébrique du tore linéaire G défini par

$$\chi_\lambda(X) = X^{\lambda}, \quad (X \in G(\mathbb{C})).$$

Soit alors $T = \gamma H$ un élément maximal de $\mathscr{T}$. Définissons une partition $\mathscr{P}$ de $\mathscr{L}$ de la façon suivante. Pour tout $i \in I$, considérons la suite $\chi_\lambda|_H$ des restrictions à H des caractères χ_λ, lorsque λ décrit $\mathscr{L}_i$. Désignons par χ_j^H, $j \in J_i$, les différents caractères de H intervenant dans cette suite, et notons $\mathscr{L}_{i,j}$ le sous-ensemble de $\mathscr{L}_i$, formé des exposants $\lambda \in \mathscr{L}_i$ tels que

$$\chi_\lambda|_H = \chi_j^H.$$

Les ensembles $\mathscr{L}_{i,j}$ ainsi déterminés définissent une partition $\mathscr{P}$ de $\mathscr{L}$:

$$\mathscr{L} = \coprod_{i \in I} \coprod_{j \in J_i} \mathscr{L}_{i,j}.$$

Par définition de $\mathscr{P}$, il est clair que

$$H \subseteq H_{\mathscr{P}}. \tag{4}$$

L'inclusion $T = \gamma H \subseteq V$, se traduit pour tout $i \in I$, par une relation linéaire entre les caractères χ_j^H

$$\sum_{\lambda \in \mathscr{L}_i} p_i(\lambda)\, \gamma^{\lambda}\, \chi_\lambda|_H = \sum_{j \in J_i} \Big(\sum_{\lambda \in \mathscr{L}_{i,j}} p_i(\lambda)\, \gamma^{\lambda} \Big) \chi_j^H = 0.$$

Le théorème d'indépendance linéaire d'Artin montre alors que les coefficients

$$\sum_{\lambda\in\mathscr{L}_{i,j}} p_i(\lambda)\,\gamma^\lambda, \quad (i\in I,\ j\in J_i),$$

de ces relations linéaires, sont tous nuls. Autrement dit, la partition $\mathscr{P}$ est compatible avec γ. On déduit alors de (4) que

$$T=\gamma H\subseteq \gamma H_{\mathscr{P}}\subseteq V.$$

Par maximalité de T, il s'ensuit que $T=\gamma H_{\mathscr{P}}$. Le lemme est donc démontré si la partition $\mathscr{P}$ de $\mathscr{L}$ est compatible maximale avec γ. Sinon, choisissons une partition $\mathscr{P}'$ de $\mathscr{L}$, plus fine que $\mathscr{P}$, qui soit compatible maximale avec γ. Le même argument montre que

$$T=\gamma H_{\mathscr{P}'}. \quad \square$$

Remarque. La réciproque du lemme est fausse: il se peut qu'un élément $T\in\mathscr{T}$ soit de la forme $\gamma H_{\mathscr{P}}$, où $\mathscr{P}$ est compatible maximale avec $\gamma\in\Gamma$, sans être maximal dans $\mathscr{T}$.

Lemme 4. *Les éléments maximaux de l'ensemble $\mathscr{T}$ sont en nombre fini.*

Preuve. Les partitions $\mathscr{P}$ de $\mathscr{L}$ sont en nombre fini. D'après le lemme 3, il suffit de montrer que pour chaque partition $\mathscr{P}$, les classes modulo $H_{\mathscr{P}}$ de l'ensemble $E_{\mathscr{P}}$ des éléments $\gamma\in\Gamma$ satisfaisant les conditions (1) et (2), sont en nombre fini.

Pour tout $i\in I$, $j\in J_i$, notons $l_{i,j}$ le cardinal de l'ensemble $\mathscr{L}_{i,j}$, et considérons le morphisme

$$\varphi_{\mathscr{P}}: G\to\prod_{i\in I}\prod_{j\in J_i}\mathbb{P}^{l_{i,j}-1},$$

produit des morphismes

$$\varphi_{i,j}: G\to\mathbb{P}^{l_{i,j}-1}, \quad (i\in I,\ j\in J_i),$$

qui associent à tout $X\in G(\mathbb{C})$, le point de coordonnées homogènes

$$(\ldots, X^\lambda, \ldots)_{\lambda\in\mathscr{L}_{i,j}}.$$

Le morphisme $\varphi_{\mathscr{P}}$ induit, par passage au quotient, un plongement

$$G/H_{\mathscr{P}}\hookrightarrow\prod_{i\in I}\prod_{j\in J_i}\mathbb{P}^{l_{i,j}-1}.$$

Il suffit donc de montrer que l'image $\varphi_{\mathscr{P}}(E_{\mathscr{P}})$ est finie.

Désignons par Δ le sous-groupe multiplicatif de $\mathbb{C}^*$, engendré par les coefficients $p_i(\lambda)$ et par les coordonnées des éléments de Γ. De même que Γ, le sous-groupe Δ est de rang fini. Pour tout $i\in I$, $j\in J_i$, $\gamma\in E_{\mathscr{P}}$, soit $U(i,j,\gamma)$ le $l_{i,j}$-uplet de coordonnées

$$(\ldots, p_i(\lambda)\,\gamma^\lambda, \ldots)_{\lambda\in\mathscr{L}_{i,j}}.$$

Fixons maintenant i et j. Les conditions (1) et (2) montrent que, pour tout $\gamma\in E_{\mathscr{P}}$, les $l_{i,j}$-uplets $U(i,j,\gamma)$ satisfont les hypothèses du théorème 1. Les classes

de ces vecteurs, dans l'espace projectif $\mathbb{P}^{l,-1}$ sont donc en nombre fini. Il s'ensuit que l'ensemble $\varphi_{i,j}(E_{\mathscr{P}})$ est fini. □

3.3. Le théorème 2 est alors une conséquence immédiate des lemmes 3 et 4. A tout élément $\xi \in V \cap \Gamma$, associons l'ensemble $T=\{\xi\}$, qui appartient à $\mathscr{T}$. La partie T est contenue dans un élément maximal de $\mathscr{T}$, qui d'après le lemme 3, est de la forme $\gamma H_{\mathscr{P}}$. Il suffit alors de remarquer que

$$(\gamma H_{\mathscr{P}}) \cap \Gamma = \gamma(H_{\mathscr{P}} \cap \Gamma).$$

§ 4. Versions semi-effectives du théorème 2

4.1. Rappelons tout d'abord brièvement la notion de *hauteur absolue* dans un espace projectif (voir, par exemple, le Chap. 3 de [3]).

Soit K un corps de nombres de degré d sur $\mathbb{Q}$. Pour toute place v de K, notons d_v le degré de l'extension $K_v/\mathbb{Q}_v$, où K_v (resp. $\mathbb{Q}_v$) désigne le complété de K (resp. $\mathbb{Q}$) en la place v. A chaque place v de K, correspond une unique valeur absolue $|.|_v$ sur K, normalisée par

$$|x|_v = x^{(d_v/d)}, \text{ pour tout } x \in \mathbb{Q},\ x \geqq 0, \text{ si } v \text{ est archimédienne,}$$
$$|p|_v = p^{-(d_v/d)}, \text{ si } v \text{ divise le nombre premier } p.$$

Soient l un entier $\geqq 1$ et $U=(u_1, \ldots, u_l)$ un l-uplet dont les coordonnées u_j, $(1 \leqq j \leqq l)$ appartiennent à K. On appelle *hauteur absolue* de U le produit

$$H(U) = \prod_v \max_{1 \leqq j \leqq l} (|u_j|_v),$$

où v décrit l'ensemble des places de K. Notons que $H(U)$ ne dépend pas du choix d'un corps de rationalité K pour les coordonnées u_j. De plus, la formule du produit montre que pour tout $\alpha \in K^*$, on a

$$H(\alpha U) = H(U).$$

Par passage au quotient, on définit ainsi la hauteur d'un point de l'espace projectif $\mathbb{P}^{l-1}(\bar{\mathbb{Q}})$.

Enfin, si P désigne un polynôme non nul, à coefficients dans $\bar{\mathbb{Q}}$, de support $\mathscr{L}$, on notera $H(P)$ la hauteur absolue d'un l-uplet ($l=\text{card } \mathscr{L}$) obtenu en ordonnant, de façon quelconque, les coefficients du polynôme P.

4.2. Reprenons maintenant les notations du § 3 et supposons de plus qu'il existe un corps de nombres K tel que

i) $\Gamma \subseteq (K^*)^n$
ii) $p_i(\lambda) \in K, \quad (i \in I,\ \lambda \in \mathscr{L}_i)$.

Nous nous proposons de majorer la hauteur (en un sens à préciser) des «origines» γ intervenant dans le théorème 2.

Pour chaque partition $\mathscr{P}$ de $\mathscr{L}$, nous avons défini en 3.2 des morphismes projectifs

$$\varphi_{i,j}: G \to \mathbb{P}^{l_{i,j}-1}, \qquad (i \in I, j \in J_i)$$

où $l_{i,j} = \mathrm{card}(\mathscr{L}_{i,j})$. Nous avons ensuite prouvé que les images $\varphi_{i,j}(E_{\mathscr{P}})$ de l'ensemble $E_{\mathscr{P}}$ des éléments $\gamma \in \Gamma$, tels que la partition $\mathscr{P}$ soit compatible maximale avec γ, étaient des ensembles finis. Voici une version quantitative de ce résultat:

Théorème 3. *Soient $\mathscr{P}$ une partition de $\mathscr{L}$ et ε un réel >0. Il existe une constante c_1, ne dépendant que de $\mathscr{L}$, $\mathscr{P}$, Γ, ε, telle que pour tout élément $\gamma \in E_{\mathscr{P}}$, on ait la majoration*

$$H(\varphi_{i,j}(\gamma)) \leqq c_1 H(P_{i,j})^{l_{i,j}-1+\varepsilon}, \qquad (i \in I, j \in J_i)$$

où $P_{i,j}$ désigne le polynôme tronqué

$$P_{i,j}(X) = \sum_{\lambda \in \mathscr{L}_{i,j}} p_i(\lambda) X^{\lambda}.$$

Remarque 1. La démonstration proposée ici ne fournit pas une détermination effective de la constante c_1 ci-dessus. L'ineffectivité provient uniquement de l'emploi dans la démonstration du lemme 7 (§ 5), d'arguments utilisant le théorème du «sous-espace» de W. Schmidt, qui demeure pour le moment ineffectif (tout comme le théorème de Thue-Siegel-Roth).

Remarque 2. A $\varepsilon > 0$ près, l'exposant $l_{i,j} - 1 + \varepsilon$ est le meilleur possible. Voici un exemple où il est optimal.

Soient n un entier $\geqq 2$, $a_1, \ldots, a_n$ des entiers $\geqq 2$, premiers entre eux deux à deux. Désignons par Γ le sous-groupe produit de $(\mathbb{Q}^*)^n$

$$\Gamma = a_1^{\mathbb{Z}} \times \ldots \times a_n^{\mathbb{Z}},$$

et choisissons une suite (γ_k) d'éléments de Γ, tels que chaque n-uplet γ_k ait des coordonnées du même ordre de grandeur. Par exemple, soit

$$\gamma_k = (a_1^{r_{1,k}}, \ldots, a_n^{r_{n,k}}), \qquad r_{j,k} = [k \log a_1 / \log a_j], \qquad (1 \leqq j \leqq n, k \geqq 1).$$

Pour tout $k \geqq 1$, le principe des tiroirs (lemme 1.3.2 de [12]) permet de construire une forme linéaire

$$P_k(X) = \sum_{j=1}^{n} p_{j,k} X_j$$

non identiquement nulle, à coefficients entiers, s'annulant en $X = \gamma_k$, dont la hauteur $H(P_k)$ satisfait l'inégalité

$$n^{-1} H(P_k)^{n-1} \leqq a_1^k = \max_j (a_j^{r_{j,k}}).$$

Il résulte tout d'abord du théorème 3 que, pour k suffisamment grand, les polynômes P_k ont un même support $\mathscr{L}$, de cardinal n, et que la partition triviale de $\mathscr{L}$ (formée d'une seule partie $\mathscr{L}_{i,j} = \mathscr{L}$) est compatible maximale

avec γ_k, relativement à l'équation $P_k(X)=0$. Autrement dit, toute somme partielle des

$$p_{j,k}\, a_j^{r_{j,k}}, \qquad (1 \leqq j \leqq n),$$

est non nulle. L'inégalité ci-dessus montre alors que la majoration fournie par le théorème 3, pour la partition triviale de $\mathscr{L}$, est optimale (au ε près).

4.3. Les morphismes $\varphi_{i,j}$ induisent par passage au quotient des morphismes (notés aussi $\varphi_{i,j}$)

$$\varphi_{i,j}\colon G/H_{\mathscr{P}} \to \mathbb{P}^{J_{i,j}-1}, \qquad (i \in I, j \in J_i),$$

de telle sorte que l'inégalité du théorème 3 s'interprète comme une majoration de la hauteur, relative à $\varphi_{i,j}$, de la classe $\gamma H_{\mathscr{P}}$. De façon générale, tout morphisme projectif

$$\varphi\colon G \to \mathbb{P}^{\nu},$$

défini sur $\bar{\mathbb{Q}}$, induit sur $G(\bar{\mathbb{Q}})$ une hauteur H_φ:

$$H_\varphi(\gamma) = H(\varphi(\gamma)).$$

Un tel morphisme φ étant fixé, nous allons montrer qu'il est possible de choisir dans chaque classe $\gamma(H_{\mathscr{P}} \cap \Gamma)$, avec $\gamma \in E_{\mathscr{P}}$, un représentant γ', dont la hauteur $H_\varphi(\gamma')$ est comparable à la hauteur des polynômes P_i, $(i \in I)$. De façon plus précise, on a le

Théorème 4. *Il existe des constantes c_2 et c_3, ne dépendant que de $\mathscr{L}$, Γ, φ, telles que $V \cap \Gamma$ soit réunion finie de sous-ensembles de la forme $\gamma(H_{\mathscr{P}} \cap \Gamma)$, où $\mathscr{P}$ désigne une partition de $\mathscr{L}$, compatible maximale avec $\gamma \in \Gamma$, et où γ satisfait de plus la majoration*

$$H_\varphi(\gamma) \leqq c_2 (\max_{i \in I} H(P_i))^{c_3}.$$

Remarque. Cet énoncé est semi-effectif dans le sens suivant. La constante c_3 est effectivement calculable en fonction de $\mathscr{L}$ et de φ, tandis que la constante c_2 sera évaluée à partir de la constante ineffective c_1, intervenant dans le théorème 3.

§ 5. Quelques lemmes metriques

Soient K un corps de nombres, de degré d sur $\mathbb{Q}$, S un ensemble fini de places de K, contenant l'ensemble S_∞ des places archimédiennes de K, et l un entier $\geqq 2$. De façon usuelle, on notera $\mathcal{O}$ l'anneau des entiers de K, $\mathcal{O}_S$ l'anneau des S-entiers de K, $\mathcal{O}_S^*$ le groupe multiplicatif des S-unités de K.

5.1. Pour tout l-uplet $U=(u_1, \ldots, u_l)$ de K^l, nous appellerons *taille* de U, le nombre

$$t(U) = \max_{\sigma, j} (|\sigma u_j|),$$

où $j=1,\ldots,l$, et où σ décrit l'ensemble des plongements de K dans $\mathbb{C}$. Pour toute place v de K, il est commode d'introduire la *hauteur locale en* v:

$$H_v(U)=\max_{1\leqq j\leqq l}(|u_j|_v),$$

où les valeurs absolues $|\cdot|_v$ sont normalisée comme dans le §4, de telle sorte que

$$H(U)=\prod_v H_v(U).$$

On a alors

$$t(U)=\max_{v\in S_\infty}(H_v(U)^{d/d_v}).$$

Le lemme suivant, essentiellement standard, permet de relier les notions de hauteur absolue et de taille d'un l-uplet U:

Lemme 5. *Il existe une constante c_4, ne dépendant que de K, satisfaisant la propriété suivante. Pour tout l-uplet U dont les coordonnées $u_j (1\leqq j\leqq l)$ appartiennent à K, il existe $\alpha\in K^*$ tel que*

i) $\alpha u_j\in\mathcal{O}$, $\quad(1\leqq j\leqq l)$,

ii) $H(U)\leqq t(\alpha U)\leqq c_4 H(U)$,

Si toutes les coordonnées u_j appartiennent à $\mathcal{O}_S$, le nombre α satisfait de plus l'inégalité

iii) $\prod_{v\in S}|\alpha|_v\leqq c_4$.

Preuve. Soit $x=(x_v)$ un idèle de K. Le théorème de Minkowski adélique affirme alors l'existence d'un élément $\alpha\in K^*$ tel que

$$|\alpha|_v\leqq|x_v|_v,$$

pour toute place v de K, pourvu que la valeur absolue de x, i.e. le produit

$$\prod_v|x_v|_v$$

soit $\geqq c_4$, où c_4 désigne une constante $\geqq 1$, ne dépendant que de K.

On peut supposer sans restriction que $U\neq 0$. Choisissons un idèle x de K tel que

$$|x_v|_v=H_v(U)^{-1}, \quad \text{si } v\notin S_\infty,$$
$$|x_v|_v=(c_4 H(U))^{d_v/d}H_v(U)^{-1}, \quad \text{si } v\in S_\infty.$$

Il existe donc $\alpha\in K^*$ tel que

$$H_v(\alpha U)\leqq 1, \quad \text{si } v\notin S_\infty,$$
$$H_v(\alpha U)\leqq(c_4 H(U))^{d_v/d}, \quad \text{si } v\in S_\infty.$$

On vérifie alors aisèment les conditions i) et ii), ainsi que l'inégalité

$$\prod_{v\notin S_\infty}H_v(\alpha U)\geqq c_4^{-1}.$$

Si toutes les coordonnées u_j appartiennent à $\mathcal{O}_S$, il s'ensuit que

$$\prod_{v\notin S}|\alpha|_v \geqq \prod_{v\notin S} H_v(\alpha U) \geqq \prod_{v\notin S_\infty} H_v(\alpha U) \geqq c_4^{-1}.$$

L'inégalité iii) se déduit alors de la formule du produit. □

5.2. Soit $U=(u_1,\ldots,u_l)$ un l-uplet $\in(\mathcal{O}_S)^l$. Ses coordonnées u_j, $(1\leqq j\leqq l)$, appartiennent à $\mathcal{O}_S^*$ si et seulement si le produit

$$\prod_{j=1}^{l}\prod_{v\in S}|u_j|_v = 1.$$

Ce produit mesure, en quelque sorte, la «distance» du l-uplet U au sous-ensemble $(\mathcal{O}_S^*)^l\subset(\mathcal{O}_S)^l$. Dans cet optique, on a le

Lemme 6. *Soit ε un nombre réel >0. Il existe une constante $c_5>0$, ne dépendant que de l, K, S, ε, telle que pour tout l-uplet $U=(u_1,\ldots,u_l)$ vérifiant*

i) $u_j\in\mathcal{O}_S$, $(1\leqq j\leqq l)$,

ii) $u_1+\ldots+u_l=0$,

iii) *toute somme partielle des u_j est non nulle,*

on ait la minoration:

$$\prod_{j=1}^{l}\prod_{v\in S}|u_j|_v \geqq c_5\Big(\prod_{v\in S}H_v(U)\Big)H(U)^{-\varepsilon}.$$

Remarque 1. On a $\prod_{v\in S}H_v(U)\geqq H(U)$.

Remarque 2. Ce lemme peut être considéré comme une forme quantitative du théorème 1, dans le cas particulier où le groupe $\Delta=\mathcal{O}_S^*$. En effet, nous en déduisons une minoration de la «distance» du l-uplet U au sous-ensemble $(\mathcal{O}_S^*)^l$, en fonction de sa hauteur $H(U)$. En particulier, si $U\in(\mathcal{O}_S^*)^l$, la hauteur $H(U)$ est bornée.

La démonstration du lemme 6 est basée sur le résultat suivant dû à J.H. Evertse (Th. 2 de [2]):

Lemme 7. *Soient T une partie non vide de S et ε un réel >0. Il existe une constante ineffective $c_6>0$, ne dépendant que de l, K, S et ε, telle que pour tout l-uplet $U=(u_1,\ldots,u_l)$ vérifiant*

i) $u_j\in\mathcal{O}$, $(1\leqq j\leqq l)$,

ii) *pour toute partie non vide $J\subseteq\{1,\ldots,l\}$, $\sum_{j\in J}u_j\neq 0$*

on ait la minoration:

$$\Big(\prod_{j=1}^{l}\prod_{v\in S}|u_j|_v\Big)\prod_{v\in T}\Big|\sum_{j=1}^{l}u_j\Big|_v \geqq c_6\Big(\prod_{v\in T}H_v(U)\Big)t(U)^{-\varepsilon}.$$

Preuve du lemme 6. Désignons par $T\subseteq S$, l'ensemble des places $v\in S$, pour lesquelles

$$|u_1|_v \leqq \max_{2\leqq j\leqq l}(|u_j|_v).$$

En permutant éventuellement les coordonnées de U, on peut supposer sans restriction que T est non vide. Puisque $U \in (\mathcal{O}_S)^l$, il existe α dans K^* satisfaisant les propriétés i), ii), iii) du lemme 5. Soit

$$U' = (\alpha u_2, \ldots, \alpha u_l).$$

Pour toute place $v \in T$, on a donc les égalités

$$H_v(U') = H_v(\alpha U) = |\alpha|_v H_v(U).$$

D'autre part, le $(l-1)$-uplet U' satisfait les hypothèses du lemme 7. On a donc la minoration

$$\left(\prod_{j=2}^{l} \prod_{v \in S} |\alpha u_j|_v\right) \prod_{v \in T} \left|\sum_{j=2}^{l} \alpha u_j\right|_v \geqq c_6 \left(\prod_{v \in T} H_v(U')\right) t(U')^{-\varepsilon}.$$

On déduit alors de la majoration iii) du lemme 5 que

$$\left(\prod_{j=2}^{l} \prod_{v \in S} |u_j|_v\right) \prod_{v \in T} |u_1|_v \geqq c_7 \left(\prod_{v \in T} H_v(U)\right) t(U')^{-\varepsilon}.$$

Pour toute place $v \in S \setminus T$, par définition de T, on a

$$|u_1|_v = H_v(U).$$

If suffit alors de remarquer que

$$t(U') \leqq t(\alpha U) \leqq c_4 H(U). \quad \square$$

§ 6. Preuve du théorème 3

Choisissons tout d'abord un ensemble fini S de places de K, contenant l'ensemble S_∞ des places archimédiennes de K, tel que les coordonnées des éléments de Γ soient des S-unités de K.

Fixons une partition $\mathcal{P}$ de $\mathcal{L}$ et un couple d'indices $i \in I$, $j \in J_i$. On identifiera le polynôme $P_{i,j}$ avec le $l_{i,j}$-uplet déterminé par ses coefficients $p_i(\lambda)$, ordonnés de façon quelconque. D'après le lemme 5, il existe $\alpha \in K^*$ tel que les $\alpha p_i(\lambda)$, $(\lambda \in \mathcal{L}_{i,j})$, soient entiers et tel que l'on ait

$$H(P_{i,j}) \leqq t(\alpha P_{i,j}) \leqq c_4 H(P_{i,j}).$$

A tout élément $\gamma \in E_{\mathcal{P}}$, associons le $l_{i,j}$-uplet

$$U_\gamma = (\ldots, \alpha p_i(\lambda) \gamma^\lambda, \ldots)_{\lambda \in \mathcal{L}_{i,j}}.$$

Les conditions (1) et (2) du § 3 montrent que le $l_{i,j}$-uplet U_γ satisfait les hypothèses i), ii) et iii) du lemme 6. Soit

$$\varepsilon' = \varepsilon/(l_{i,j} + \varepsilon).$$

On a alors la minoration

$$\prod_{\lambda}\prod_{v}|\alpha p_i(\lambda)\gamma^{\lambda}|_v \geqq c_5\Big(\prod_{v} H_v(U_\gamma)\Big) H(U_\gamma)^{-\varepsilon'},$$

où λ décrit $\mathscr{L}_{i,j}$ et v décrit S. Comme les puissances γ^{λ} intervenant ci-dessus sont des S-unités, cette inégalité se réduit à

$$\prod_{\lambda}\prod_{v}|\alpha p_i(\lambda)|_v \geqq c_5\Big(\prod_{v} H_v(U_\gamma)\Big) H(U_\gamma)^{-\varepsilon'}.$$

Par abus de notation, identifions $\varphi_{i,j}(\gamma)\in\mathbb{P}^{l_{i,j}-1}$, au $l_{i,j}$-uplet de coordonnées $(\ldots,\gamma^{\lambda},\ldots)_{\lambda\in\mathscr{L}_{i,j}}$. Pour toute place v, on a alors la minoration

$$H_v(U_\gamma) \geqq H_v(\varphi_{i,j}(\gamma)) \min_{\lambda}(|\alpha p_i(\lambda)|_v).$$

Il s'ensuit que

$$\Big(\prod_{v\in S} H_v(\alpha P_{i,j})\Big)^{l_{i,j}-1} \geqq c_5\Big(\prod_{v\in S} H_v(\varphi_{i,j}(\gamma))\Big) H(U_\gamma)^{-\varepsilon'}.$$

Utilisant de nouveau le fait que les γ^{λ} sont des S-unités, remarquons que le produit de droite:

$$\prod_{v\in S} H_v(\varphi_{i,j}(\gamma)) = H(\varphi_{i,j}(\gamma)).$$

Majorons maintenant le membre de gauche. Si v est une place non-archimédienne de S, on a

$$H_v(\alpha P_{i,j}) \leqq 1,$$

puisque les coordonnées de $\alpha P_{i,j}$ sont entières. D'autre part, si v est archimédienne, on a les majorations

$$H_v(\alpha P_{i,j}) \leqq t(\alpha P_{i,j})^{d_v/d} \leqq (c_4 H(P_{i,j}))^{d_v/d}.$$

Notant que $\sum_{v\in S_\infty} d_v = d$, on obtient finalement l'inégalité

$$H(P_{i,j})^{l_{i,j}-1} \geqq c_8 H(\varphi_{i,j}(\gamma)) H(U_\gamma)^{-\varepsilon'}.$$

Il suffit alors de remarquer que

$$H(U_\gamma) \leqq H(\alpha P_{i,j}) H(\varphi_{i,j}(\gamma)) = H(P_{i,j}) H(\varphi_{i,j}(\gamma)).$$

§ 7. Preuve du théorème 4

7.1. Un sous-espace vectoriel réel $\mathscr{E}\subseteq\mathbb{R}^r$ est dit rationnel sur $\mathbb{Q}$, si $\mathscr{E}$ peut être défini par un système d'équations linéaires à coefficients dans $\mathbb{Q}$, ou de façon équivalente, s'il existe une base de $\mathscr{E}$ formée d'éléments de $\mathbb{Q}^r$. Le groupe $\mathscr{E}\cap\mathbb{Z}^r$ est alors un réseau de $\mathscr{E}$.

Soient K un corps de nombres et S un ensemble fini de places de K, contenant toutes les places archimédiennes de K. On a alors le

Lemme 8. *Soient $\alpha_1, \ldots, \alpha_r$ des S-unités de K. Le sous-espace vectoriel $\mathscr{E} \subseteq \mathbb{R}^r$, défini par le système d'équations*

$$\sum_{j=1}^{r} x_j \log|\alpha_j|_v = 0, \quad (v \in S),$$

est rationnel sur $\mathbb{Q}$.

Preuve. Soit s le cardinal de l'ensemble S. Considérons le plongement logarithmique

$$\mathrm{LOG}: \mathscr{O}_S^* \to \mathbb{R}^s,$$

qui associe à toute S-unité α, le s-uplet

$$\mathrm{LOG}(\alpha) = (\log|\alpha|_v)_{v \in S}.$$

Alors $\mathscr{E}$ s'identifie à l'espace vectoriel des relations linéaires liant les vecteurs $\mathrm{LOG}(\alpha_1), \ldots, \mathrm{LOG}(\alpha_r)$ de $\mathbb{R}^s$.

L'homomorphisme LOG induit une injection

$$\mathscr{O}_S^* \otimes_{\mathbb{Z}} \mathbb{R} \hookrightarrow \mathbb{R}^s,$$

autrement dit, l'espace $\mathscr{E}$ est engendré par les relations multiplicatives liant les éléments $\alpha_1, \ldots, \alpha_r$ dans le groupe $\mathscr{O}_S^*$. □

7.2. Démontrons maintenant le théorème 4.

Soit

$$\gamma_j = (\gamma_{1,j}, \ldots, \gamma_{n,j}), \quad (1 \leqq j \leqq r),$$

un système générateur du groupe Γ. Soit S un ensemble fini de places de K, contenant l'ensemble des places archimédiennes de K, tel que les coordonnées $\gamma_{i,j}$ $(1 \leqq i \leqq n,\ 1 \leqq j \leqq r)$ soient des S-unités.

Fixons une partition $\mathscr{P}$ de $\mathscr{L}$, et posons

$$A = \max_{i \in I,\, j \in J_i} (l_{i,j} \log H(P_{i,j})) + \log c_1,$$

où c_1 désigne la constante intervenant dans le théorème 3, associée au choix (arbitraire) de $\varepsilon = 1$. Nous allons montrer que, pour tout élément $\gamma \in E_{\mathscr{P}}$, il existe $\delta \in H_{\mathscr{P}} \cap \Gamma$ vérifiant l'inégalité

$$H_\varphi(\gamma\delta) \leqq \exp(c_9 A + c_{10}),$$

où c_9 et c_{10} désignent des constantes effectivement calculables en fonction du système générateur $\{\gamma_j\}$ choisi, de S, et de φ.

Désignons par $\mathscr{M}$ le sous-ensemble des n-uplets de $\mathbb{Z}^n$ de la forme

$$\mu = \lambda - \lambda',$$

où λ et λ' appartiennent à une même partie $\mathscr{L}_{i,j}$, $(i \in I, j \in J_i)$.

Par passage au logarithme et décomposition de la hauteur en produit de hauteurs locales, on déduit du théorème 3 les inégalités

$$\sum_{v\in S} \max(0, \log|\gamma^{\mu}|_v) \leqq A,$$

pour tout $\mu\in\mathscr{M}$.

Soit $v=(v_1,\ldots,v_r)$ un r-uplet d'entiers tel que

$$\gamma = \prod_{j=1}^{r} \gamma_j^{v_j}.$$

Si $\mu=(\mu_1,\ldots,\mu_n)$, l'inégalité ci-dessus s'écrit

$$\sum_{v\in S} \max\left(0, \sum_{i=1}^{n}\sum_{j=1}^{r} \mu_h v_j \log|\gamma_{i,j}|_v\right) \leqq A.$$

Désignons alors par $L_{\mu,v}$, $(\mu\in\mathscr{M}, v\in S)$, la forme linéaire de $\mathbb{R}^r$ définie par

$$L_{\mu,v}(x_1,\ldots,x_r) = \sum_{j=1}^{r} x_j \log\left|\prod_{i=1}^{n} \gamma_{i,j}^{\mu_i}\right|_v = \sum_i \sum_j \mu_i x_j \log|\gamma_{i,j}|_v.$$

Remarquons que si $\mu\in\mathscr{M}$, alors $-\mu\in\mathscr{M}$. Il s'ensuit que

$$|L_{\mu,v}(v)| \leqq A,$$

pour tout élément $\mu\in\mathscr{M}$, et toute place $v\in S$.

Soit t la dimension du sous-espace vectoriel $\mathscr{E}\subseteq\mathbb{R}^r$, défini par le système d'équations

$$L_{\mu,v}(x_1,\ldots,x_r)=0, \quad (\mu\in\mathscr{M}, v\in S).$$

D'après le lemme 8, $\mathscr{E}$ est une intersection de sous-espaces rationnels sur $\mathbb{Q}$, donc est rationnel sur $\mathbb{Q}$. Il s'ensuit que, si w désigne l'ordre du groupe des racines de l'unité contenues dans K, le sous-groupe

$$\mathscr{R} = w(\mathscr{E}\cap\mathbb{Z}^r)$$

est un réseau de $\mathscr{E}$.

Après ré-indexation éventuelle des coordonnées de $\mathbb{R}^r$, on peut supposer sans restriction que la projection canonique $\mathbb{R}^r\to\mathbb{R}^t$, définie par le tronquage des t premières coordonnées, induit un isomorphisme de $\mathscr{E}$ sur $\mathbb{R}^t$. Désignons alors par ξ l'unique point de $\mathscr{E}$ de coordonnées

$$\xi=(v_1,\ldots,v_t,z_{t+1},\ldots,z_r).$$

Puisque $\mathscr{R}$ est un réseau de $\mathscr{E}$, il existe un point $\rho=(\rho_1,\ldots,\rho_r)$ dans $\mathscr{R}$ tel que

$$\|\xi-\rho\| \leqq c_{11},$$

où $\|.\|$ désigne le maximum des valeurs absolues des coordonnées du r-uplet considéré.

Nous allons vérifier que

$$\delta = \prod_{j=1}^{r} \gamma_j^{-\rho_j}$$

convient. Montrons tout d'abord que δ appartient à $H_{\mathscr{P}} \cap \Gamma$. Pour tout $\mu \in \mathscr{M}$ et toute place $v \in S$, on a

$$\log|\delta^{\mu}|_v = \log\Big|\prod_i \prod_j \gamma_{i,j}^{-\mu_i \rho_j}\Big|_v = -L_{\mu,v}(\rho) = 0.$$

Puisque tous les entiers ρ_j sont des multiples entiers de w, il existe $\delta_1 \in \Gamma$, tel que

$$\delta = \delta_1^w.$$

Les égalités ci-dessus montrent que

$$|\delta_1^{\mu}|_v = 1, \quad (\mu \in \mathscr{M},\ v \in S).$$

Il s'ensuit que, pour tout exposant $\mu \in \mathscr{M}$, le nombre δ_1^{μ} est une racine de l'unité, contenue dans K. On a donc

$$\delta^{\mu} = 1, \quad (\mu \in \mathscr{M}),$$

autrement dit, δ appartient au sous-groupe algébrique $H_{\mathscr{P}}$ (formule 3 du § 3).

On a d'autre part

$$|v_j - \rho_j| \leqq c_{11}, \quad (1 \leqq j \leqq t),$$

$$|L_{\mu,v}(v-\rho)| = |L_{\mu,v}(v)| \leqq A, \quad (\mu \in \mathscr{M},\ v \in S).$$

Or les formes linéaires

$$x_1, \ldots, x_t, \quad L_{\mu,v}(x_1, \ldots, x_r), \quad (\mu \in \mathscr{M},\ v \in S),$$

sont de rang maximal, égal à r. Le système d'inéquations ci-dessus est donc inversible. On en déduit la majoration

$$\|v - \rho\| \leqq c_{12} A.$$

Comme

$$\gamma\delta = \prod_{j=1}^{r} \gamma_j^{(v_j - \rho_j)},$$

il s'ensuit que

$$H_{\varphi}(\gamma\delta) \leqq \exp(c_9 A + c_{10}).$$

§ 8. Equations exponentielles mixtes

8.1. Soient n un entier $\geqq 1$, $(\mathscr{L}_i)_{i \in I}$ une famille finie de parties finies $\subseteq \mathbb{N}^n$, K un corps de nombres, Γ un sous-groupe de type fini de $(K^*)^n$. Soient

$$p_{i,\lambda} \colon \Gamma \to K^*, \quad (i \in I,\ \lambda \in \mathscr{L}_i),$$

des fonctions quelconques de la variable $\gamma \in \Gamma$, à valeur dans K^*.

Nous nous proposons de décrire l'ensemble des solutions $\gamma \in \Gamma$ du système d'équations

$$\sum_{\lambda \in \mathscr{L}_i} p_{i,\lambda}(\gamma)\gamma^{\lambda} = 0, \quad (i \in I). \tag{5}$$

Les équations exponentielles étudiées dans le § 3, correspondent à des fonctions $p_{i,\lambda}$ constantes.

Notons

$$\mathscr{L}=\coprod_{i\in I}\mathscr{L}_i.$$

Soit $\mathscr{P}$ une partition de $\mathscr{L}$, induisant sur chacun des sous-ensembles $\mathscr{L}_i$ une partition

$$\mathscr{L}_i=\coprod_{j\in J_i}\mathscr{L}_{i,j}.$$

Comme précédemment, nous désignerons par $H_{\mathscr{P}}$ le sous-groupe algébrique de $(\mathbb{C}^*)^n$ défini par les équations (3) du § 3. De façon analogue, nous dirons que la partition $\mathscr{P}$ est *compatible* avec la solution γ du système d'équations (5) si

$$\sum_{\lambda\in\mathscr{L}_{i,j}} p_{i,\lambda}(\gamma)\gamma^{\lambda}=0, \qquad (i\in I,\ j\in J_i).$$

Si de plus, pour tout $i\in I$, $j\in J_i$ et toute partie propre $\mathscr{L}'\subset\mathscr{L}_{i,j}$, on a

$$\sum_{\lambda\in\mathscr{L}'} p_{i,\lambda}(\gamma)\gamma^{\lambda}\neq 0,$$

nous dirons que la partition $\mathscr{P}$ est *compatible maximale* avec γ.

Pour chaque $\gamma\in\Gamma$, notons

$$M(\gamma)=\max_{i\in I}(H(P_{i,\gamma})),$$

où $P_{i,\gamma}$ désigne le polynôme

$$P_{i,\gamma}(X)=\sum_{\lambda\in\mathscr{L}_i} p_{i,\lambda}(\gamma)X^{\lambda}, \qquad (i\in I,\ \gamma\in\Gamma).$$

Fixons comme dans le § 4 un morphisme projectif φ, induisant une hauteur H_φ sur $G(\bar{\mathbb{Q}})$. On a alors le

Théorème 5. *Il existe une constante ineffective $c_{13}>0$, ne dépendant que de $\mathscr{L}$, de Γ et de φ, ainsi qu'une constante $c_{14}>0$, effectivement calculable en fonction de $\mathscr{L}$ et de °, satisfaisant la propriété suivante. Pour toute solution $\gamma\in\Gamma$ du système d'équations* (5) *et toute partition $\mathscr{P}$ de $\mathscr{L}$, compatible maximale avec γ, il existe $\delta\in\Gamma$, $\eta\in\Gamma$ tels que*

a) $\gamma=\delta\eta$,

b) $H_\varphi(\delta)\leqq c_{13}M(\gamma)^{c_{14}}$,

c) $\eta\in H_{\mathscr{P}}\cap\Gamma$.

Preuve. Considérons la variété affine V_γ d'équations

$$P_{i,\gamma}(X)=0, \qquad (i\in I).$$

Par construction, $\gamma\in V_\gamma\cap\Gamma$. Il suffit alors d'utiliser la description de $V_\gamma\cap\Gamma$ fournie par le théorème 4. □

Remarque. On obtient ainsi une décomposition de γ dans laquelle le facteur η appartient à certains sous-groupes déterminés par la structure multiplicative du

système d'équations (5), c'est-à-dire la donnée du support $\mathscr{L}$ et du groupe Γ. La hauteur du facteur δ est comparable à $M(\gamma)$ qui peut être vu comme une mesure de la croissance arithmétique des fonctions $p_{i,\lambda}$. Cette décomposition est non triviale si la fonction $M(\gamma)$ est «petite» devant $H_\varphi(\gamma)$.

8.2. Comme exemple d'application du théorème 5, examinons le cas particulier des équations *exponentielles-polynômes.*

Soient donnés un ensemble fini d'indices L et une partition de L:

$$L=\coprod_{i\in I} L_i.$$

Pour tout $l\in L$, soit Q_l un polynôme en r variables, à coefficients dans un corps de nombres K. Soient enfin

$$a_{k,l}, \quad (1\leqq k\leqq r,\ l\in L),$$

des éléments de K^*. On considère le système d'équations

$$\sum_{l\in L_i} Q_l(\mu)\prod_{k=1}^{r} a_{k,l}^{m_k}=0, \quad (i\in I), \tag{6}$$

en entiers $\mu=(m_1,\ldots,m_r)$.

Pour toute partition $\mathscr{P}$ de L, induisant une partition

$$L_i=\coprod_{j\in J_i} L_{i,j}$$

sur chacun des sous-ensembles L_i, on désignera par $\mathscr{H}_\mathscr{P}$ le sous-groupe de $\mathbb{Z}^r$, formé des éléments $\mu=(m_1,\ldots,m_r)$ tels que

$$\prod_{k=1}^{r} a_{k,l}^{m_k}=\prod_{k=1}^{r} a_{k,l'}^{m_k},$$

pour tout couple d'éléments l, l' appartenant à un même sous-ensemble $L_{i,j}$, $(i\in I, j\in J_i)$. De façon analogue, on dira que $\mathscr{P}$ est *compatible* avec une solution μ du système d'équations (6) si

$$\sum_{l\in L_{i,j}} Q_l(\mu)\prod_{k=1}^{r} a_{k,l}^{m_k}=0, \quad (i\in I,\ j\in J_i).$$

Si de plus, pour tout $i\in I$, $j\in J_i$ et toute partie propre $L'\subset L_{i,j}$, on a

$$\sum_{l\in L'} Q_l(\mu)\prod_{k=1}^{r} a_{k,l}^{m_k}\neq 0,$$

on dira que la partition $\mathscr{P}$ est *compatible maximale* avec μ.

Notons enfin

$$\|\mu\|=\max_{1\leqq k\leqq r}(|m_k|).$$

Le résultat suivant précise, de façon quantitative le théorème 2 de [10].

Théorème 6. *Soit μ une solution du système d'équations* (6) *telle que les nombres $Q_l(\mu)$, $(l\in L)$, soient tous non nuls. Soient $\mathscr{P}$ une partition de L, compatible maximale avec μ. Il existe $\mu'\in\mathbb{Z}^r$, $\mu''\in\mathbb{Z}^r$ tels que*

a) $\mu=\mu'+\mu''$,

b) $\|\mu'\|\leqq c_{15}\log\|\mu\|+c_{16}$,

c) $\mu''\in\mathscr{H}_{\mathscr{P}}$,

où c_{15} et c_{16} désignent des constantes indépendantes de μ.

Preuve. Numérotons les éléments de l'ensemble L et considérons les s-uplets

$$\alpha_k=(a_{k,l_1},\ldots,a_{k,l_s}),\qquad (1\leqq k\leqq r)$$

où $s=\mathrm{card}(L)$.

Complétons alors le s-uplet α_k par $\beta_k\in K^*$ de telle sorte que les n-uplets, $(n=s+1)$,

$$\gamma_k=(\alpha_k,\beta_k),\qquad (1\leqq k\leqq r)$$

soient linéairement indépendants dans le groupe multiplicatif $(K^*)^n$.

Pour chaque $l=l_j\in L$, soit

$$\lambda(l)=(0,\ldots,1,\ldots,0)$$

le n-uplet dont le $j^{\text{ème}}$ terme est égal à 1 et dont les autres termes sont égaux à 0. On a alors

$$a_{k,l}=\gamma_k^{\lambda(l)},\qquad (1\leqq k\leqq r,\ l\in L).$$

Notons $\mathscr{L}_i$, $(i\in I)$, l'ensemble des exposants $\lambda(l)$ lorsque l décrit L_i et posons

$$\mathscr{L}=\coprod_{i\in I}\mathscr{L}_i.$$

On va maintenant se ramener à la situation du théorème 5. Soit Γ le sous-groupe libre de $(K^*)^n$ engendré par les γ_k, $(1\leqq k\leqq r)$.

Définissons tout d'abord des fonctions

$$p_\lambda\colon\ \Gamma\to K^*,\qquad (\lambda\in\mathscr{L})$$

de la façon suivante. Le choix de la base

$$\mathscr{B}=(\gamma_1,\ldots,\gamma_r)$$

de Γ, nous permet d'identifier Γ à $\mathbb{Z}^r$. Si le r-uplet $\mu=(m_1,\ldots,m_r)$ n'annule aucun des polynômes Q_l, $(l\in L)$, posons

$$p_\lambda(\gamma)=Q_l(\mu),\qquad (\lambda\in\mathscr{L}),$$

où $\lambda=\lambda(l)$ et $\gamma=\prod_{k=1}^{r}\gamma_k^{m_k}$. Sinon, posons (de façon arbitraire)

$$p_\lambda(\gamma)=1,\qquad (\lambda\in\mathscr{L}).$$

A tout r-uplet μ satisfaisant les hypothèses du théorème 6, correspond ainsi une solution $\gamma\in\Gamma$ du système d'équations

$$\sum_{\lambda\in\mathscr{L}_i}p_\lambda(\gamma)\gamma^\lambda=0,\qquad (i\in I),$$

qui est du type envisagé dans la section 8.1. Dans ce cas particulier, on a

$$M(\gamma) \leqq c_{17} \|\mu\|^{c_{18}}.$$

De plus, les sous-groupes $H_{\mathscr{P}} \cap \Gamma \subseteq \Gamma$ s'identifient à $\mathscr{H}_{\mathscr{P}} \subseteq \mathbb{Z}^r$, via le choix de la base $\mathscr{B}$.

D'autre part, pour tout plongement projectif φ de $G(\mathbb{C}) = (\mathbb{C}^*)^n$, il existe des constantes positives c_{19} et c_{20} (indépendantes de μ) telles que

$$c_{19} \|\mu\| \leqq \log H_{\varphi}(\gamma) \leqq c_{20} \|\mu\|.$$

Le théorème 5 nous fournit alors une décomposition $\gamma = \delta\eta$. Les r-uplets μ' et μ'' des coordonnées de δ et de η dans la base $\mathscr{B}$ vérifient alors les conditions a), b), c). □

Remarque. Grâce à un exemple simple, déjà examiné dans [10], nous allons maintenant vérifier que la majoration b) ci-dessus est optimale, (à la valeur des constantes c_{15} et c_{16} près).

Fixons

$$I = \{1\}, \quad L = L_1 = \{1, 2\}, \quad r = 2, \quad K = \mathbb{Q}, \quad a_{1,1} = a_{2,2} = 2,$$
$$a_{1,2} = a_{2,1} = 1, \quad Q_1(m_1, m_2) = m_1, \quad Q_2(m_1, m_2) = -1.$$

Le système d'équations (6) s'écrit alors

$$m_1 2^{m_1} - 2^{m_2} = 0.$$

Ses solutions entières sont donc

$$m_1 = 2^h, \quad m_2 = h + 2^h, \quad (h \text{ entier} \geqq 0).$$

Il y a deux partitions de L. Soient $\mathscr{P}_1$ la partition triviale (réduite à un seul sous-ensemble) et $\mathscr{P}_2$ la partition de L en deux sous-ensembles à un élément, auxquelles correspondent les sous-groupes de $\mathbb{Z}^2$:

$$\mathscr{H}_{\mathscr{P}_1} = \mathbb{Z}(1, 1), \quad \mathscr{H}_{\mathscr{P}_2} = \mathbb{Z}^2.$$

Remarquons que pour toute solution $\mu = (m_1, m_2)$ de l'équation, la partition $\mathscr{P}_1$ est compatible maximale avec μ. La décomposition du théorème 6 s'écrit

$$2^h = m_1' + m_1'', \quad h + 2^h = m_2' + m_2''$$

avec $m_1'' = m_2''$. On a donc

$$h = m_2 - m_1 = m_2' - m_1' \leqq 2 \|\mu'\| \leqq 2c_{15} \log(h + 2^h) + 2c_{16}.$$

§ 9. Application aux equations normiques

Nous nous proposons de déduire du théorème 2 les résultats classiques de W. Schmidt (th. 4.B du Chap. 7 de [11]) concernant les équations normiques

(= norm-form equation), ainsi que leurs généralisations p-adiques, dues à H.P. Schlickewei (th. 1.2 de [9]).

9.1. Il s'agit essentiellement de décrire l'intersection d'un groupe multiplicatif avec un espace vectoriel.

De façon plus précise, soient k un corps de type fini sur $\mathbb{Q}$, K une extension finie de k, M un k sous-espace vectoriel de K, Γ un sous-groupe de type fini $\subseteq K^*$. On a alors le

Théorème 7. *L'ensemble $M \cap \Gamma$ est réunion finie de sous-ensembles de la forme $\gamma(\Gamma \cap F^*)$, où F désigne un sous-corps de K contenant k, et γ un élément de Γ, tels que $\gamma F \subseteq M$.*

Preuve. Soit n le degré de K/k. Supposons que k soit plongé dans $\mathbb{C}$, et désignons par

$$\mathscr{S} = \{\sigma_1, \ldots, \sigma_n\}$$

l'ensemble des k-isomorphismes de K dans $\mathbb{C}$. Soit

$$\tau = \sigma_1 \times \ldots \times \sigma_n$$

le plongement canonique de K^* dans $(\mathbb{C}^*)^n$. Un élément x de K^* appartient alors à M, si et seulement si, son image $\tau(x)$ appartient à la sous-variété V de $(\mathbb{C}^*)^n$, définie par le système d'équations

$$P_i(X) = \sum_{k=1}^{n} \sigma_k(\alpha_i) X_k = 0, \qquad (1 \leqq i \leqq r),$$

où l'on a choisi une base $(\alpha_1, \ldots, \alpha_r)$ de l'orthogonal du k-espace vectoriel M relativement à la forme bilinéaire non dégénérée $Tr_{K/k}(xy)$. Le théorème 2 fournit alors une décomposition finie de $V \cap \tau(\Gamma)$ en sous-ensembles de la forme

$$\tau(\gamma)(H_{\mathscr{P}} \cap \tau(\Gamma)),$$

où $\mathscr{P}$ désigne, comme d'habitude, une partition du support $\mathscr{L}$ du système d'équations ci-dessus, compatible maximale avec l'élément $\tau(\gamma)$ du sous-groupe $\tau(\Gamma) \subseteq (\mathbb{C}^*)^n$. Dans ce cas particulier, les supports $\mathscr{L}_i$ des polynômes P_i, $(1 \leqq i \leqq r)$, s'identifient à $\mathscr{S}$. Une partition $\mathscr{P}$ de $\mathscr{L}$ équivaut donc à la donnée de r partitions

$$\mathscr{S} = \coprod_{j \in J_i} \mathscr{S}_{i,j}, \qquad (1 \leqq i \leqq r).$$

Désignons par $F_{\mathscr{P}}$ le sous-corps de K, formé des éléments $x \in K$ tels que

$$\sigma(x) = \sigma'(x),$$

pour tout couple σ, σ' d'éléments appartenant à un même $\mathscr{S}_{i,j}$. Alors

$$\tau^{-1}(H_{\mathscr{P}} \cap \tau(K^*)) = F_{\mathscr{P}}^*,$$

$$\tau^{-1}(H_{\mathscr{P}} \cap \tau(\Gamma)) = \Gamma \cap F_{\mathscr{P}}^*.$$

D'autre part, par construction de V, on a

$$\tau^{-1}(V \cap \tau(K^*)) = M \setminus \{0\}.$$

Puisque la partition $\mathscr{P}$ est compatible avec $\tau(\gamma)$, il s'ensuit que

$$\begin{aligned}\tau(\gamma F_{\mathscr{P}}^*) &= \tau(\gamma)\tau(F_{\mathscr{P}}^*) = \tau(\gamma)(H_{\mathscr{P}} \cap \tau(K^*)) \\ &= (\tau(\gamma)H_{\mathscr{P}}) \cap \tau(K^*) \subseteq V \cap \tau(K^*) = \tau(M \setminus \{0\}).\end{aligned}$$

On en déduit que $\gamma F_{\mathscr{P}} \subseteq M$. Remarquons enfin que

$$\tau^{-1}(V \cap \tau(\Gamma)) = M \cap \Gamma.$$

La décomposition de $M \cap \Gamma$, déduite de celle de $V \cap \tau(\Gamma)$ par l'isomorphisme inverse τ^{-1}, possède bien les propriétés annoncées. □

Remarque. On peut interpréter géométriquement la démonstration ci-dessus de la façon suivante. Considérons le tore linéaire G, défini sur k, déduit du groupe multiplicatif $\mathbb{G}_m$ par restriction des scalaires de K à k (cf. §1.4 de [6]). Le groupe $G(k)$ des points k-rationnels de G est isomorphe à K^*, et les plongements $\sigma \in \mathscr{S}$ s'identifient à des caractères algébriques de G, agissant sur $G(k) = K^*$ par σ. La famille $(\sigma_1, \ldots, \sigma_n)$ forme alors une base du groupe des caractères de G, et le plongement τ se prolonge en une trivialisation de G, après extension des scalaires de k à $\bar{k}$. Il s'agit alors de décrire l'intersection d'un sous-groupe

$$\Gamma \subseteq K^* = G(k)$$

avec l'ensemble $M \setminus \{0\}$ des points k-rationnels de la sous-variété algébrique $\tau^{-1}(V)$. Dans la preuve ci-dessus, nous avons décomposé, grâce au théorème 2, l'image

$$\tau(\Gamma \cap \tau^{-1}(V)) = V \cap \tau(\Gamma)$$

de cette intersection, utilisant essentiellement la linéarité de V.

9.2. Soient R une $\mathbb{Z}$-algèbre intègre de type fini, de corps de fractions k, U un sous-groupe du groupe des unités de R. Soient K une extension finie de k, $\mathscr{M}$ un R-module de type fini $\subseteq K$, et a un élément non nul de k.

On considère l'équation suivante, dite équation normique

$$N_{K/k}(\mu) = a\nu,$$

où les inconnues μ et ν appartiennent respectivement à $\mathscr{M}$ et à U. Autrement dit, il s'agit de déterminer le sous-ensemble Σ des éléments μ d'un module donné $\mathscr{M}$, dont la norme relative à l'extension K/k appartient à la classe aU.

Pour tout corps intermédiaire F, $k \subseteq F \subseteq K$, désignons par R_F la fermeture intégrale de R dans F. Notons R_F^* le groupe des unités de l'anneau R_F, et U_F le sous-groupe de R_F^*, formé des éléments $u \in R_F^*$ tels que

$$N_{K/k}(u) \in U.$$

Soit enfin M le k-espace vectoriel engendré dans K par les éléments de $\mathscr{M}$. On a alors le

Théorème 8. *L'ensemble Σ est réunion finie de sous-ensembles de la forme*

$$(\mu U_F)\cap\mathscr{M},$$

où F désigne un sous-corps de K contenant k et μ un élément de Σ, tels que $\mu F\subseteq M$.

Remarque. Le R-module $(\mu F)\cap\mathscr{M}$ est alors homothétique à un R-module complet de F (i.e.: le k-espace vectoriel engendré par ses éléments est égal à F). Le théorème ci-dessus permet donc de scinder l'équation normique la plus générale, en un nombre fini d'équations normiques relatives à des modules complets de sous-corps de K.

Preuve du théorème 8. D'après un théorème de Nagata, l'anneau R_K est une $\mathbb{Z}$-algèbre de type fini. Il s'ensuit que le groupe R_K^* des unités de R_K est de type fini [7]. D'autre part, l'anneau R_K, noethérien et intégralement clos, admet une théorie des diviseurs. Pour tout diviseur premier $\mathfrak{P}$ de R_K, au-dessus du premier

$$\mathfrak{p}=\mathfrak{P}\cap R_k$$

de R_k, notons $f_{\mathfrak{P}}$ le degré résiduel en $\mathfrak{P}$ de l'extension K/k. A tout élément $\mu\in K^*$, est associé un diviseur

$$(\mu)=\prod_{\mathfrak{P}}\mathfrak{P}^{n_{\mathfrak{P}}},$$

avec $n_{\mathfrak{P}}\in$. Par passage à la norme, on en déduit l'égalité

$$(N_{K/k}(\mu))=\prod_{\mathfrak{P}}\mathfrak{p}^{f_{\mathfrak{P}}n_{\mathfrak{P}}}$$

entre diviseurs de R_k.

Supposons maintenant que $\mu\in\Sigma$. Il s'ensuit que pour tout premier $\mathfrak{p}$ de R_k, on a la relation

$$a_{\mathfrak{p}}=\sum_{\mathfrak{P}\mid\mathfrak{p}}f_{\mathfrak{P}}n_{\mathfrak{P}},$$

où $(a)=\prod_{\mathfrak{p}}\mathfrak{p}^{a_{\mathfrak{p}}}$ désigne la décomposition de (a) dans le groupe des diviseurs de R_k.

D'autre part, il existe une suite $(b_{\mathfrak{P}})$, associée au R-module $\mathscr{M}$ de type fini, ne contenant qu'un nombre fini de termes non nuls, telle que l'on ait la minoration

$$n_{\mathfrak{P}}\geqq b_{\mathfrak{P}},$$

pour tout premier $\mathfrak{P}$ de R_K.

Il n'y a donc qu'un nombre fini de possibilités pour la suite $(n_{\mathfrak{P}})$ des exposants de (μ). Il s'ensuit que l'ensemble Σ est contenu dans une réunion finie de classes modulo R_K^*. Soit αR_K^* l'une de ces classes, d'intersection non vide avec Σ. On peut alors supposer sans restriction que $\alpha\in\Sigma$, de telle sorte que

$$(\alpha R_K^*)\cap\Sigma=(\alpha U_K)\cap\mathscr{M}.$$

Par l'homothétie α^{-1}, on est donc ramené à étudier l'intersection

$$U_K \cap (\alpha^{-1}\mathscr{M}).$$

Le théorème 7 fournit alors une décomposition de $U_K \cap (\alpha^{-1}M)$ en sous-ensembles de la forme

$$\gamma(U_K \cap F^*) = \gamma U_F$$

avec $\gamma F \subseteq \alpha^{-1}M$. Il suffit alors de choisir, de façon quelconque, un élément μ dans chacun des sous-ensembles

$$(\alpha\gamma U_F) \cap \mathscr{M}$$

qui sont non vides, pour obtenir le théorème 8. □

9.3. Dans certains cas particuliers, on peut préciser le théorème 8 de la façon suivante.

Pour tout sous-corps F de K, contenant k, notons

$$M_F = \bigcap_{\xi \in F^*} (\xi M)$$

le plus grand F-espace vectoriel contenu dans M, et posons

$$\mathscr{M}_F = \mathscr{M} \cap M_F.$$

Supposons que $\mathscr{M}_F$ ne soit pas réduit à $\{0\}$. Désignons alors par $\mathcal{O}_F$ le *stabilisateur* de $\mathscr{M}_F$ dans F, c'est à dire l'ensemble des éléments $x \in F$, tels que $x\mathscr{M}_F \subseteq \mathscr{M}_F$. On a alors

$$R \subseteq \mathcal{O}_F \subseteq R_F, \qquad k\mathcal{O}_F = F.$$

Soient $\mathcal{O}_F^*$ le groupe des unités de $\mathcal{O}_F$ et U_F' le sous-groupe

$$U_F' = U_F \cap \mathcal{O}_F^*.$$

Désignons par $(u_j)_{j \in J}$, un système de représentants de U_F modulo U_F'. Pour tout élément $\mu \in M_F$, l'ensemble

$$(\mu U_F) \cap \mathscr{M}$$

se décompose alors en une somme disjointe de classes

$$(\mu u_j) U_F',$$

où j décrit l'ensemble des indices $j \in J$, tels que $\mu u_j \in \mathscr{M}$. On a donc le

Théorème 9. *Supposons que pour tout corps intermédiaire F, $k \subseteq F \subseteq K$, tels que $\mathscr{M}_F \neq \{0\}$, le sous-groupe U_F' soit d'indice fini dans U_F. Alors l'ensemble Σ est réunion finie de classes de la forme*

$$\mu U_F',$$

où μ appartient à $\mathscr{M}_F \cap \Sigma$.

Notons que l'on a un plongement naturel

$$U_F/U'_F \hookrightarrow R_F^*/\mathcal{O}_F^*.$$

Les conditions du théorème 9 sont donc satisfaites si l'on suppose, à fortiori, que pour tout corps intermédiaire F, le groupe $\mathcal{O}_F^*$ est d'indice fini dans R_F^*. C'est notamment le cas, quel que soit le module $\mathcal{M}$, lorsque

$$R=\mathbb{Z} \quad \text{ou} \quad R=\mathbb{Z}\left[\frac{1}{p_1},\ldots,\frac{1}{p_t}\right]$$

($p_1,\ldots,p_t$ désignent des nombres premiers). On retrouve ainsi les énoncés de [9] et de [11]. Notons cependant que lorsque la dimension de R est >1, ces conditions ne sont généralement pas vérifiées, même si l'anneau R est intégralement clos, auquel cas on a l'égalité

$$U'_F = U_F \cap \mathcal{O}_F^* = U_F \cap \mathcal{O}_F.$$

On construit alors aisèment des exemples d'équations normiques où la description finie du théorème 9 est fausse.

Bibliographie

1. Chabauty, C.: Sur les équations diophantiennes liées aux unités d'un corps de nombres algébriques fini. Annali di Math. **17**, 127–168 (1938)
2. Evertse, J.H.: On sums of S-units and linear recurrences. Compositio Math. (à paraître)
3. Lang, S.: Fundamentals of diophantine geometry. Berlin-Heidelberg-New York: Springer 1983
4. Liardet, P.: Sur une conjecture de S. Lang. Astérisque, n° 24–25. Soc. Math. Fr 187–209 (1975)
5. Mann, H.B.: On linear relations between roots of unity. Mathematika, London **12**, 107–117 (1965)
6. Ono, T.: Arithmetic of algebraic tori. Annals of Math. **74**, 101–139 (1961)
7. Samuel, P.: A propos du théorème des unités. Bull. Sci. Math. **90**, 89–96 (1966)
8. Schlickewei, H.P.: The p-adic Thue-Siegel-Roth-Schmidt theorem. Archiv der Math. **29**, 267–270 (1977)
9. Schlickewei, H.P.: On norm-form equations. J. of Number Theory **9**, 370–380 (1977)
10. Schlickewei, H.P., Van der Poorten, A.J.: The growth conditions for recurrences sequences, Report 82.0041, Macquarie University, N.S.W. Australia 1982
11. Schmidt, W.: Diophantine approximation. Lecture Notes in Mathematics vol. 785. Berlin-Heidelberg-New York: Springer 1980
12. Waldschmidt, M.: Nombres transcendants. Lecture Notes in Mathematics vol. 402. Berlin-Heidelberg-New York: Springer 1974

Oblatum 2-VII-1984