PUBLICATIONS

MATHEMATIQUES

D'ORSAY

N° 77-74

APPROXIMATION DES NOMBRES ALGEBRIQUES

par

Maurice MIGNOTTE

Université de Paris-Sud

Département de Mathématique

Bât. 425

91405 ORSAY France

PUBLICATIONS

MATHEMATIQUES

D'ORSAY

N° 77-74

APPROXIMATION DES NOMBRES ALGEBRIQUES

par

Maurice MIGNOTTE

Université de Paris-Sud

Département de Mathématique

Bât. 425

91405 ORSAY France

INTRODUCTION

Ces notes sont issues d'un cours enseigné à Orsay au printemps 1975. Les deux résultats fondamentaux démontrés ici sont le théorème de Roth sur l'approximation rationnelle des nombres algébriques et sa généralisation à l'approximation simultanée des nombres algébriques, due à W. M. Schmidt.

Les connaissances requises se limitent aux rudiments de la théorie des nombres algébriques. Sauf pour la démonstration des théorèmes de W. M. Schmidt utilisant des résultats de géométrie des nombres -qui sont indiqués en appendice- les préliminaires qui nous sont nécessaires sont présentés dans le premier chapitre. Il s'agit d'estimations, du type de celle de Liouville, permettant de minorer le module d'un nombre algébrique non nul et d'un lemme 'de Siegel' sur la résolution en nombres entiers de systèmes d'inéquations linéaires, dont la preuve repose sur le célèbre principe des tiroirs de Dirichlet.

Le théorème de Roth est l'aboutissement d'une suite de travaux de Thue, Siegel, Dyson et Gel'fond. Le second chapitre contient la démonstration des résultats de ces différents auteurs. Nous avons tenu à offrir au lecteur la possibilité de suivre en détail l'évolution de cette théorie. C'est, à notre point de vue, un exemple privilégié en mathématiques où il est possible de mettre en évidence la progression historique d'un théorème. Le théorème de Liouville date de 1844, celui de Thue de 1908 et Roth démontra le sien en 1955. Dans cette lente progression il n'y a pas eu de rupture, chacun des successeurs de Liouville ne fit qu'ajouter une nouvelle pierre à un même

édifice, mais la durée de cette construction témoigne du mérite de ceux qui ont su apporter une idée originale. Pour résumer, Liouville utilisait une approximation rationnelle d'un nombre algébrique a , Thue eut l'idée géniale de considérer simultanément deux approximations de a , Siegel construisit un polynôme d'approximation plus général que celui de Thue, cette construction de Siegel fut elle-même généralisée par Dyson et Gel'fond, enfin Roth considéra simultanément un grand nombre d'approximations de a (idée déjà utilisée par Schneider). Ces idées sont simples mais leur application nécessitait la mise en oeuvre de techniques profondes permettant de trouver des conditions suffisantes pour qu'un polynôme de plusieurs variables, à coefficients entiers, ne s'annule pas en un point rationnel.

La méthode de Thue et ses généralisations sont par nature ineffectives : elle ne permettent pas de déterminer les solutions des inéquations diophantiennes considérées. Cependant, elles peuvent conduire à une majoration du nombre de ces solutions. Dans le second chapitre l'étude des théorèmes de Thue et de Gel'fond nous permet de déterminer des classes d'inéquations pour lesquelles on sait déterminer toutes ces solutions sauf peut-être l'une d'entre elles, ces résultats améliorent des théorèmes de Davenport et Schinzel.

Le troisième chapitre contient la démonstration du théorème de Roth. Nous revenons ensuite sur le problème de la majoration du nombre de solutions des inéquations considérées. Ces résultats sont appliqués à certaines équations diophantiennes ainsi qu'à l'étude du développement en fraction continue des nombres algébriques.

Le quatrième et dernier chapitre est tout entier consacré à la démonstration des théorèmes de W. M. Schmidt qui portent sur l'approximation simultanée des nombres algébriques réels par des rationnels, l'approximation des nombres algébriques par des nombres algébriques de de degré donné et sur certaines équations diophantiennes à plusieurs variables.

Certains des exercices proposés apportent des compléments au cours, d'autres en sont des applications directes. Plusieurs qui suivent le premier chapitre sont très utiles en théorie des nombres transcendants.

De nombreuses questions importantes ne sont pas abordées ici. En premier lieu, les améliorations effectives du théorème de Liouville, obtenues pour la première fois par A. Baker dans le cas de certains nombres algébriques, en reprenant une méthode déjà utilisée par Siegel, puis, en toute généralité et à nouveau par Baker, grâce à des minorations de formes linéaires en logarithmes de nombres algébriques. Comme l'indique W. M. Schmidt dans l'introduction de sa monographie il est possible que la méthode de Gel'fond et Baker joue un rôle croissant dans le futur au sein de la théorie de l'approximation diophantienne des nombres algébriques. C'est ainsi que, dernièrement, T. Cusik a otbenu par cette voie un théorème effectif sur certaines formes linéaires en nombres algébriques et que K. Győry a démontré des minorations de discrimiants de polynômes. Il n'est pas question non plus de l'approximation diophantienne p-adique, dont l'importance a été mise en évidence d'abord par K. Mahler et qui a donné lieu à de nombreux travaux parmi lesquels, récemment, la généralisation p-adique des théorèmes de W. M. Schmidt

par H. P. Schlickewei et -indépendamment- par Dubois et G. Rhin. La bibliographie contient de nombreuses références relatives à ces différents sujets et surtout ils sont abordés dans l'excellente monographie de Schmidt qui fait le point sur l'essentiel des résultats antérieurs à 1972.

Ces pages ont été dactylographiées, avec beaucoup de soin et de compétence, par Sylvie Lutzing ; je l'en remercie très vivement.

TABLE DES MATIERES

NOTATIONS ET DEFINITIONS

1. Pour z complexe, on note

$$z^* = \max(1, |z|) .$$

2. Pour un nombre réel α, on pose

$[\alpha] = n$, où n désigne l'entier défini par les conditions $n \leq \alpha < n+1$,

c'est la partie entière de α,

$\{\alpha\} = \alpha - [\alpha]$, partie fractionnaire de α,

$\|\alpha\| = \mathrm{Min}(\{\alpha\}, 1-\{\alpha\})$, distance de α à l'entier le plus proche.

3. Si $P = \sum_{i=0}^{d} a_i X^{d-i}$ est un polynôme à coefficients complexes, on pose

$\|P\| = \max_{d} |a_i|$, c'est la hauteur de P,

$\|P\|_1 = \sum_{i=0}^{d} |a_i|$,

$\|P\|_2 = \left(\sum_{i=0}^{d} |a_i|^2 \right)^{1/2}$.

Le nombre d est appelé le degré de P, et noté $\deg(P)$. Le nombre a_0 est appelé le coefficient dominant de P.

Plus généralement, si Q est un polynôme à plusieurs variables, $\|Q\|$ désignera encore le maximum des modules des coefficients de Q, et $\|Q\|_1$ la somme des modules de ces coefficients.

4. Soit α un nombre complexe. Si l'application $\mathbb{Q}[X] \to \mathbb{C}$, $P \mapsto P(\alpha)$ est injective, α est dit transcendant. Dans le cas contraire, α est dit algébrique ; le noyau de l'application précédente est un idéal de $\mathbb{C}[X]$; il existe un polynôme Q unique à coefficients entiers, premiers entre eux

dans leur ensemble, de coefficient dominant positif, qui engendre cet idéal ; ce polynôme est appelé le polynôme minimal de α. On définit le degré de α $\deg\alpha = \deg Q$, la hauteur de α est la quantité $\|\alpha\|_\infty = \|Q\|$. On pose ainsi $\|\alpha\|_2 = \|Q\|_2$, $\|\alpha\|_1 = \|Q\|_1$.

Les racines de $Q(X)$ sont appelées les conjugués de α, elles sont simples.

I. Préliminaires.

1. Approximation des nombres réels par les nombres rationnels.

Le premier résultat de cette théorie, démontré par Dirichlet en 1842, est une application bien connue du principe des tiroirs.

THEOREME 1. - Soient α et Q deux nombres réels, Q supérieur à 1. Alors, il existe des entiers p et q tels que

$$1 \leq q < Q \quad \text{et} \quad |\alpha q - p| \leq Q^{-1}.$$

▶ Nous nous contenterons de démontrer ce résultat lorsque Q est entier. Découpons l'intervalle $[0,1]$ en Q intervalles $[\frac{i}{Q};\frac{i+1}{Q}]$, i variant de 0 à $Q-1$. L'un de ces intervalles contient au moins deux des $Q+1$ points $0, 1, \{\alpha\}, \{2\alpha\}, \ldots, \{(Q-1)\alpha\}$. D'où l'existence d'entiers r_1, r_2, s_1, s_2 tels que

$$0 \leq r_2 < r_1 \leq Q-1 \quad \text{et} \quad |(r_1\alpha - s_1) - (r_2\alpha - s_2)| \leq Q^{-1}.$$

Les nombres $p = s_1 - s_2$ et $q = r_1 - r_2$ vérifient les inégalités du théorème. ◀

COROLLAIRE. - Pour tout nombre réel irrationnel α, il existe une infinité de nombres rationnels p/q distincts qui vérifient l'inégalité

$$|\alpha - \frac{p}{q}| < \frac{1}{q^2} .$$

► C'est une conséquence facile du théorème 1 .◄

2. Approximation des nombres algébriques par des nombres réels.

En 1844, Liouville démontra le résultat fondamental suivant.

THEOREME 2. - Soit α un nombre algébrique réel de degré d. Alors, il existe une constante positive calculable $c = c(\alpha)$, telle que l'on ait

$$|\alpha - \frac{p}{q}| > \frac{c}{q^d}$$

pour tout nombre rationnel p/q distinct de α.

► 1. Soit P le polynôme minimal de α. Considérons le nombre

$$\gamma = P(p/q) ,$$

où p/q est un rationnel distinct de α. Par construction, γ n'est pas nul.

2. Majorons γ . On a

$$\gamma = P(p/q) - P(\alpha) = (\frac{p}{q} - \alpha)\, P'(x) \quad , \quad \text{pour un } x \in]p/q, \alpha[\ .$$

Si p/q vérifie $|\alpha - p/q| \leq 1$, on en déduit

$$|\gamma| \leq |\alpha - \frac{p}{q}| \, (d^2 \, \|P\| \, (|\alpha| + 1)^d) \ .$$

3. Le nombre γ est rationnel, non nul, et admet q^d comme dénominateur. D'où la minoration

$$|\gamma| \geq q^{-d} \ .$$

4. Pour $|\alpha - p/q| \leq 1$, l'encadrement précédent de $|\gamma|$ conduit à l'inégalité

$$|\alpha - \frac{p}{q}| \geq \frac{(d^2 \, \|\alpha\|_\infty \, (|\alpha| + 1)^d)^{-1}}{q^d} \quad ,$$

qui est aussi vérifiée pour $|\alpha - p/q| > 1$. ◄

Nous avons volontairement détaillé la démonstration de ce théorème, en mettant en évidence les étapes suivantes

- choix d'une fonction auxiliaire (ici le polynôme P) ,
- construction d'un nombre convenable γ non nul,
- majoration de γ (obtenue par un raisonnement analytique),

- minoration de $|\gamma|$ (qui résulte des propriétés arithmétiques de γ) ,
- conclusion.

On retrouvera le même schéma de démonstration pour les théorèmes de Thue, Siegel, Roth. Il est à noter que ce schéma se retrouve aussi dans la plupart des démonstrations de la Théorie des Nombres Transcendants (voir par exemple [93]) .

Ce théorème permit à Liouville de démontrer pour la première fois l'existence de nombres transcendants, en construisant explicitement de tels nombres. Par exemple :

COROLLAIRE. - Si $\epsilon = (\epsilon_n)_{n\geq 0}$, $\epsilon_n \in \{0,1\}$, $\sum_{n\geq 0} \epsilon_n = +\infty$, le nombre

$$\alpha_\epsilon = \sum_{n\geq 0} \epsilon_n 2^{-n!}$$

est transcendant.

Ce corollaire, dont la démonstration est laissée au lecteur, montre que l'ensemble des nombres transcendants de Liouville a la puissance du continu.

3. Une inégalité sur les racines d'un polynôme.

THEOREME 3. - Soit

$$P = \sum_{i=0}^{d} a_i X^{d-i} = a_0(X - z_1) \dots (X - z_d)$$

un polynôme à coefficients complexes. Alors, l'inégalité

$$|a_0|\, z_1^* \dots z_d^* \leq \|P\|_2$$

a lieu.

▶ Il suffit de considérer le cas où les racines de P sont non nulles.

Si R désigne un polynôme à coefficients complexes et si α est un nombre complexe non nul, un calcul algébrique immédiat conduit à la relation

$$\|(X - \alpha)\, R(X)\|_2 = |\alpha|\, \|(X - \bar{\alpha}^{-1})\, R(X)\|_2 .$$

Supposons que $z_1, \dots, z_k$ soient les racines de P contenues dans le disque $|z| < 1$. En appliquant plusieurs fois l'égalité précédente, il vient

$$\begin{aligned}
\|P\|_2 &= |a_0|\, \|(X - z_1) \dots (X - z_d)\|_2 \\
&= |a_0|\, |z_1 \dots z_k|\, \|(X - \bar{z}_1^{-1}) \dots (X - \bar{z}_k^{-1})\, (X - z_{k+1}) \dots (X - z_d)\|_2 \\
&\geq |a_0|\, |z_1 \dots z_k|\, |\bar{z}_1^{-1} \dots \bar{z}_k^{-1}\, z_{k+1} \dots z_d| \\
&= |a_0|\, |z_{k+1} \dots z_d| ,
\end{aligned}$$

ce qui n'est rien d'autre que l'inégalité cherchée.

COROLLAIRE. - Soient Q et R des polynômes à coefficients entiers et soit α une racine de Q. Alors, si Q et R n'ont pas de racine commune, on a

$$|R(\alpha)| \geq \|R\|_1^{-q+1} \, \|Q\|_2^{-r} \, \alpha^{*r} \quad , \quad \text{où} \quad q = \deg Q \ , \quad r = \deg R \ .$$

▶ Soit b le coefficient dominant de Q. Considérons le nombre

$$\gamma = b^r \, R(\alpha_1) \ldots R(\alpha_q) \ ,$$

où $\alpha_1 = \alpha$, α_2, ..., α_q sont les racines de Q. C'est un entier non nul, puisqu'il est égal au résultant des polynômes Q et R. On a

$$\begin{aligned} 1 \leq |\gamma| &\leq |R(\alpha)| \ |b|^r \ \|R\|_1^{q-1} \ (\alpha_2^* \ldots \alpha_q^*)^r \\ &\leq |R(\alpha)| \ \|R\|_1^{q-1} \ \alpha^{*r} \ \|Q\|_2^r \quad \text{(grâce au théorème 3)} \ . \end{aligned}$$

D'où le résultat. ◀

4. Sur la résolution en nombres entiers des systèmes linéaires.

Encore une application du principe des tiroirs.

THEOREME 4. - Soient $L_1, \ldots, L_m$ des formes linéaires à coefficients réels, en n variables $(n > m)$.
Alors, pour tout entier positif H, il existe des entiers $x_1, \ldots, x_n$, non tous nuls, de valeur absolue majorée par H, tels que

$$|L_j(x_1,\ldots,x_n)| < \|L_j\|_1 \, H^{-(n-m)/m} \quad , \quad \underline{\text{pour}} \ j = 1,\ldots,m \ .$$

► Soit E l'ensemble des n-uples $(x_1,\ldots,x_n)$ d'entiers tels que $0 \le x_i \le H$, $i = 1,\ldots,n$. L'application $(L_1,\ldots,L_m)$ envoie E dans un parallélépipède C de $\mathbb{R}^m$ dont les côtés ont pour longueur $\|L_j\|_1 \, H$. Soit ℓ l'entier défini par les inégalités $\ell^m < (H+1)^n \le (\ell+1)^m$. Partageons C en ℓ^m petits parallélépipèdes égaux.

. On a $\ell^m < \text{Card } E = (H+1)^n$; par conséquent, deux éléments $\underline{x}'$ et $\underline{x}''$ de E ont une image dans un même petit parallélépipède. Alors, $\underline{x} = \underline{x}' - \underline{x}''$ convient. ◄

COROLLAIRE. - Soient les formes linéaires

$$L_j(X) = \sum_{i=1}^{n} u_{ij} \, X_i \quad , \quad j = 1,\ldots,m_1 + m_2 \ ,$$

où les u_{ij} sont réels pour $j = 1,\ldots,m_1$ et complexes pour $j > m_1$. On suppose n supérieur à $m = m_1 + 2\,m_2$. Alors, pour tout entier positif H, il existe des entiers $x_1,\ldots,x_n$, non tous nuls, de valeur absolue majorée par H, tels que

$$|L_j(x_1,\ldots,x_n| < \|L_j\|_1 \quad H^{-(n-m)/m} \quad \text{pour } j = 1,\ldots, m_1 \ ,$$

et

$$|L_j(x_1,\ldots,x_n)| < \sqrt{2} \, \|L_j\|_1 \ H^{-(n-m)/m} \ \text{pour } j = m_1+1,\ldots,m_1+m_2 \ .$$

NOTES.

§ 1. Le corollaire au théorème 1 a été amélioré par Hurwitz en 1891 :

pour tout irrationnel réel α , il existe une infinité de rationnels irréductibles p/q vérifiant $|\alpha - p/q| < \frac{1}{\sqrt{5}\, q^2}$, de plus la constante $\sqrt{5}$ est la meilleure possible. Ce résultat a été précisé par Markov [38], voir à ce sujet le second chapitre de l'ouvrage de Cassels [10]. Le théorème de Hurwitz est contenu dans un résultat d'Emile Borel, [9], qui dit que, de trois réduites successives de α , l'une au moins vérifie l'inégalité ci-dessus. La théorie des fractions continues a été étendue à certains corps quadratiques imaginaires par G . Poitou [55] qui a, en particulier, démontré les variantes du théorème de Hurwitz valables pour ces corps.

§ 2. Le théorème de Liouville montre en particulier que le corollaire du théorème 1 est, à une constante multiplicative près, le meilleur possible pour les nombres irrationnels quadratiques réels.
Le théorème de Roth (voir chapitre III) montre que l'exposant deux est le meilleur possible pour les nombres algébriques réels.

§ 3. A. Schinzel m'a signalé que le théorème 2 figure dans un article de Landau [28], datant de 1905 . La démonstration algébrique qui figure ici semble originale, elle est extraite de [42]. Pour des compléments, voir les exercices.
Le corollaire du théorème 2 implique une variante de l'inégalité, dite de la taille (voir [93], introduction), qui permet de minorer le module d'un nombre algébrique non nul, à savoir $|\alpha| \geq \|\alpha\|_2^{-1}$. Il est à noter qu'il contient aussi une forme raffinée du théorème de Liouville :

$$|\alpha - \frac{p}{q}| \geq \frac{\alpha^*}{\|\alpha\|_2} \frac{1}{(|p|+|q|)^d} .$$

EXERCICES.

1. Soit α algébrique réel de degré d, admettant P pour polynôme minimal. Démontrer que l'on a

$$\liminf q^{d-1} \|q\alpha\| \geq \frac{1}{|P'(\alpha)|} \quad \text{si } q \to +\infty .$$

Si α est un nombre quadratique réel et si D désigne le discriminant de P, en déduire que

$$\liminf q \|q\alpha\| \geq D^{-1/2} ,$$

et en particulier,

$$\liminf q \|q\alpha\| \geq \frac{1}{\sqrt{5}} \text{ pour } \alpha = \frac{1+\sqrt{5}}{2} .$$

(C'est la partie "facile" du théorème de Hurwitz.)

2. Soit $\psi : \mathbb{N} \to \mathbb{R}$ une fonction positive. Montrer que si la série $\sum_{q \geq 1} \psi(q)$ est convergente alors l'ensemble des réels α tels que l'inégalité $\|q\alpha\| < \psi(q)$ admette une infinité de solutions entières est de mesure de Lebesgue nulle. En déduire que l'ensemble des nombres de Liouville est de mesure nulle. (Si on suppose ψ décroissante et la série divergente alors le même ensemble est de mesure pleine. Ce résultat est dû à Kintchine , pour une démonstration voir, par exemple, Cassels [10], chapitre VII.)

3. Démontrer le théorème 3 en utilisant la formule de Parseval (voir, par exemple, [40], lemme 2).

4. Soit P un polynôme non nul défini comme au théorème 2. Démontrer l'inégalité

$$\prod_{i=1}^{d} \min(1, |z_i|) \geq |a_d| \, \|P\|_2^{-1} .$$

5. Soit P le polynôme défini au théorème 3, P non nul.

a) Démontrer que toute racine z_i de P vérifie

$$|z_i| < \frac{\|P\|}{|a_0|} + 1 .$$

b) Si P est à coefficients entiers, montrer que toute racine non nulle de P vérifie

$$|z_i| > (\|P\| + 1)^{-1} .$$

6. Démontrer que la norme quadratique est la meilleure possible dans le théorème 3. De manière précise, démontrer que, pour tout $\lambda > 2$, on peut construire un polynôme P unitaire admettant une racine z vérifiant $|z| > \|P\|_\lambda$. (Si $P = \Sigma a_i X^{d-i}$, on a posé $\|P\|_\lambda = (\Sigma |a_i|^\lambda)^{1/\lambda}$). (Un exemple est donné en [42].)

7. Démontrer que dans le théorème 2 on a en fait

$$|a_0|^2 \prod z_i^{*2} + |a_d|^2 \prod z_i^{*-2} \leq \|P\|_2 .$$

De plus, si les racines z_i sont réelles positives alors

$$|a_0|^2 \prod z_i^{*2} + (2^d - 1)\,|a_d|^2 \prod z_i^{*-2} \leq \|P\|_2 .$$

8. Soient $Q_1, \ldots, Q_m, R$ des polynômes unitaires et $Q = Q_1 \ldots Q_m R$. On pose $D = \deg(Q_1 \ldots Q_m)$. Démontrer la majoration

$$\prod_{i=1}^{m} \|Q_i\|_1 \leq 2^D \|Q\| .$$

(Voir [42] pour un exemple d'utilisation dans un algorithme de factorisation des polynômes à coefficients entiers.)

9. Utiliser le théorème 3 pour obtenir une majoration du discriminant de P.

10. Lorsque P est à coefficients entiers et n'a que des racines simples, donner une minoration non triviale de $|P'(\alpha)|$, pour toute racine α de P.

11. Grâce au théorème 3, minorer $|\beta - \alpha|$, pour α et β algébriques distincts.

12. Soient P et Q deux polynômes non constants, de degré respectif p et q, à coefficients entiers et premiers entre eux. Démontrer que, pour

tout nombre complexe ω, on a

$$\max(|P(\omega)|, |Q(\omega)|) > (\|P\|^q \|Q\|^p (p+2)^{q/2} (q+2)^{p/2})^{-1} .$$

(Considérer le résultant R de P et Q. Le majorer en faisant apparaître $P(\omega)$ ou $Q(\omega)$ dans une des colonnes. Conclure en utilisant la minoration triviale $|R| \geq 1$. Voir Gel'fond [22], chap. III, lemme 5.)

13. Soit $P = a_0(X - z_1) \ldots (X - z_d)$ un polynôme à coefficients entiers. Démontrer que, pour tout sous-ensemble $\{i_1, \ldots, i_k\}$ de $\{1, \ldots, d\}$, le nombre $a_0 z_{i_1} \ldots z_{i_k}$ est un entier algébrique.
(Démontrer d'abord, par récurrence sur deg Q, que si Q est un polynôme dont les coefficients sont des entiers algébriques et si $Q(\alpha) = 0$ alors $\frac{Q(X)}{X-\alpha}$ est encore à coefficients entiers algébriques. Appliquer ensuite ce résultat au polynôme $\frac{P(X)}{(X-z_{i_1}) \ldots (X-z_{i_k})}$. Voir, par exemple, [11] lemme 1,8, ou [80] lemme 17.)

14. Soient m formes linéaires $L_1, \ldots, L_m$, en n variables, à coefficients entiers, vérifiant $\|L_j\|_1 \leq A$ pour $j = 1, \ldots, m$. Démontrer qu'il existe des entiers $x_1, \ldots, x_n$, non tous nuls, majorés par $A^{m/(n-m)}$ tels que $L_j(x_1, \ldots, x_n) = 0$ pour $j = 1, \ldots, m$. (Appliquer le théorème 4.)

15. Principe des tiroirs et considérations probabilistes.
Soient m formes linéaires $L_1, \ldots, L_m$ en n variables, à coefficients réels, vérifiant $\|L_j\| \leq A_j$ pour $j = 1, \ldots, m$. Pour tout X entier

vérifiant $(X+1)^{n/m} > 2$, il existe des entiers $(x_1, \ldots, x_n)$ non tous nuls tels que $\max_i |x_i| \leq X$ et

$$\max_j |L_j(x_1, x_2, \ldots, x_n)| < (\log 18\, m)^{1/2} (\sqrt{n}\, A_j(X+1))/((X+1)^{n/m}-2) .$$

(Soit $E = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n , \ 0 \leq x_i \leq X$ pour $i = 1, \ldots, n\}$. Afin de présenter l'idée des indications qui suivent considérons le cas $m = 1$. Pour $n = 1$, l'ensemble $L_1(E)$ est constitué par des points équidistribués sur un intervalle. Par contre, pour $n \geq 2$, ces points sont distribués de manière irrégulière, une forte proportion d'entre eux étant concentrée autour d'une valeur moyenne. De manière plus précise, leur distribution s'approche, pour n tendant vers l'infini, de celle de la loi de Gauss (théorème de la limite centrale). On n'appliquera donc pas le principe des tiroirs à $L(E)$ tout entier, mais à une partie de $L(E)$ où les points sont suffisamment denses. Posons $N = \text{Card } E$, $\lambda = (\log (18\, m)/5)^{1/2}$, $L_j = \sum_i a_{i_j} x_i$, $F_j = \{x \in E ; \left| \sum_{1 \leq i \leq n} a_{i_j} (x_i - X/2) \right| \leq \lambda \sqrt{n}\, (X+1)A\}$, $F = \bigcap_{1 \leq j \leq m} F_j$, $F'_j = E - F_j$, $N' = \text{Card } F$, $N'_j = \text{Card } F'_j$. On peut se ramener à $A_1 = \ldots = A_m = A$. En utilisant la même méthode que dans la démonstration du lemme III. 1 , démontrer les majorations $N'_j \leq 2\, N \exp(-6\, \lambda^2)$, d'où $N' \geq N(1 - 2m \exp(-6\, \lambda^2))$. Par construction $L(F)$ est contenu dans un cube de côté $2\, \lambda \sqrt{n}\, A(X+1)$ que l'on découpe en h^m petits cubes égaux, h étant le plus grand entier vérifiant $h^m < N'$. Conclure. - Voir [46] pour plus de détails.)

16. Géométrie des nombres et formes quadratiques.

1°) Soit F une forme quadratique définie positive, en n variables, de discriminant D . Démontrer qu'il existe $x \in \mathbb{Z}^n$, non nul, tel que

$$F(x) \leq n\, D^{1/n} .$$

(Soit t un nombre positif. Alors, l'ellipsoïde $F(x) \leq t$ a pour volume $V(t) = t^{n/2} D^{-1/2} \Pi^{n/2} / \Gamma(1+n/2)$. D'après le théorème de Minkowski, cet ellipsoïde contient un point non nul de $\mathbb{Z}^n$ si t vérifie $V(t) \geq 2^n$. Conclure.)

2°) Soit n un entier positif. Soit L une forme linéaire en n variables, à coefficients réels, avec $\|L\| = A$. Démontrer que, pour $t > \sqrt{n}\ (n+1)^{1/2n}$ il existe $x_1, \ldots, x_n$ entiers avec $0 < \max |x_i| < t$ et $|L(x_1, \ldots, x_n)| < n^{n/2} \sqrt{n+1}\ A\, t^{-n+1}$. (Appliquer 1°) à la forme quadratique $F(X) = s^2 \sum_{1 \leq j \leq m} L_j^2(X) + \|X\|^2$, où $\|x\|^2 = x_1^2 + \ldots + x_n^2$, $s \geq A^{-1}$. Voir Mahler [37], ou [44].)

17. Systèmes linéaires à coefficients dans un corps de nombres.

On considère m formes linéaires $L_1, \ldots, L_m$ en n variables $n > d\,m$, dont les coefficients sont des entiers d'un corps de nombres fixé K de degré d, majorés ainsi que leurs conjugués par un entier A. Alors le système $L_1(X) = \ldots = L_m(X) = 0$ admet une solution entière $(x_1, \ldots, x_n)$ non triviale vérifiant

$$\max |x_i| \leq (2(n\,A)^d)^{m/(n-md)} .$$

(Considérer les $m\,d$ formes linéaires $\sigma_h L_j$ où $\{\sigma_1, \ldots, \sigma_d\}$ est l'ensemble des différents plongements de K dans $\mathbb{C}$. Appliquer le théorème 4 avec un choix convenable des paramètres et utiliser le fait que pour $x_1, \ldots, x_n$ entiers les nombres $\prod_{1 \leq h \leq d} \sigma_h L_j(x_1, \ldots, x_n)$ sont des entiers rationnels. Voir [44]) [Ce résultat est à comparer au lemme classique sur la résolution de tels systèmes qui figure par

exemple dans l'ouvrage de Schneider [80], lemme 30 et aussi à un résultat de Schinzel [63].]

18. Sur les multiples des polynômes irréductibles.

Soient $\theta_1, \ldots, \theta_d$ les racines d'un polynôme irréductible à coefficients entiers, de coefficient dominant positif égal à q. Alors il existe un polynôme P de degré au plus n, à coefficients entiers, qui s'annule aux points θ_i, de hauteur majorée par $q\,\theta_1^* \ldots \theta_d^*$ dès que n vérifie

$$(1+\epsilon)^{(n+1-d)/d}/\sqrt{n+1} \geq 2(\text{Log } 18\,d)^{1/2}\, q\,\theta_1^* \ldots \theta_d^*\,,$$

où

$$[q\,\theta_1^* \ldots \theta_d^*] + 1 = (1+\epsilon)\, q\,\theta_1^* \ldots \theta_d^*\,.$$

(Généraliser l'exercice 16 au cas où les formes linéaires sont à coefficients complexes. Appliquer ce résultat aux formes $L_j(X) = \sum_{i=0}^{n} X_i\,\theta_j^i$, $j = 1, \ldots, r+s$ où les θ_j sont numérotés de telle sorte que θ_j soit réel pour $j = 1, \ldots, r$ et $\theta_{j+r+s} = \overline{\theta}_{j+r}$ pour $j = 1, \ldots, s$. Soit Q le polynôme ainsi obtenu, il vérifie $q^n |Q(\theta_1) \ldots Q(\theta_d)| < 1$. Conclure en montrant que le nombre de gauche de cette inégalité est un entier rationnel. Voir [44] ou [46].) [L'existence d'un tel polynôme a été démontrée pour la première fois par Martine Pathiaux [53].]

19. Mesures de transcendance et mesures d'approximation.

1°) Soit α un nombre transcendant. Une fonction f positive de $\mathbb{N}^2$ dans $\mathbb{R}$ telle que $|P(\alpha)| > f(n, H)$ pour tout polynôme non nul de degré au plus n et de hauteur majorée par H est appelée une mesure de transcendance. Démontrer que l'on a nécessairement

$f(n, H) \geq (2\alpha^*)^n H^{-n}$ pour toute mesure de transcendance de α.

2°) Soit α un nombre transcendant. Une fonction g positive de $\mathbb{N}^2$ dans $\mathbb{R}$ telle que $|\alpha - \xi| > g(n, H)$ pour tout nombre algébrique ξ de degré au plus n et de hauteur majorée par H est appelée une mesure d'approximation. Démontrer que si f est une mesure de transcendance de α et g une mesure d'approximation de α, on a

$$g(n, H) \geq f(n, H)\, H^{-n}\, e^{-3n} .$$

20. Une forme effective du théorème de l'élément primitif.
Soit $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ un corps de nombres de degré d. Alors il existe des entiers $a_2, \ldots, a_k$, avec $0 \leq a_i \leq d(d-1)/2$ pour $i = 2, \ldots, k$, tels que le nombre $\alpha = \alpha_1 + a_2\alpha_2 + \ldots + a_k \alpha_k$ engendre K (i.e. $K = \mathbb{Q}(\alpha)$. (Il suffit de considérer le cas $k = 2$. Si $\sigma_1, \ldots, \sigma_d$ désignent les plongements de K dans $\mathbb{C}$ considérer le polynôme

$$P(X) = \prod_{1 \leq i < j \leq d} (\sigma_i(\alpha_1 + X\alpha_2) - \sigma_j(\alpha_1 + X\alpha_2))$$

et démontrer qu'il existe n tel que $P(n) \neq 0$ et $0 \leq n \leq d(d-1)/2$. Conclure. Voir [44] pour plus de détails. [Comparer ce résultat au lemme 1.6 de Masser [39]. Ce résultat est très utile en théorie des nombres transcendants (cf. par exemple [49]).]

21. Quelques remarques élémentaires sur le comportement de $\|\theta^n\|$. (voir [48]). Soit θ un nombre réel supérieur à 1. Pour $n \geq 0$ désignons par a_n un entier à distance minimale de θ_n.
1°) Soit L une forme linéaire à coefficients entiers telle que

$$L(a_0, \ldots, a_N) = 0$$

et

$$\|\lambda\,\theta^n\| < ((\theta+1)\,\|L\|_1)^{-1} \quad \text{pour} \quad n = 0,\ 1,\ 2,\ \ldots$$

Démontrer que l'on a $L(1, \theta, .., \theta^N) = 0$.

(Démontrer par récurrence que l'on a $L(a_k, \ldots, a_{k+N}) = 0$ pour tout $k \geq 0$).

2°) Démontrer qu'une condition nécessaire et suffisante pour que θ soit entier est que l'on ait $\|\theta^n\| < (\theta+2)^{-2}$ pour $n \geq 1$.

3°) Démontrer que s'il existe λ positif et un entier positif N tels que

$$\|\lambda\,\theta^n\| < ((1+\theta)(N+1)(a_0+\ldots+a_N)^{1/N})^{-1} \quad \text{pour} \quad n = 0,\ 1,\ \ldots$$

alors θ est un nombre algébrique de degré au plus N . En déduire que la condition $\|\theta^n\| = \theta\,(1/n)$ implique que θ est un nombre algébrique (de Pisot).

[Ces résultats sont à rapprocher du théorème suivant de Pisot : si $\Sigma\,\|\theta^n\|^2$ converge alors θ est algébrique. Une variante du résultat de la question 3°) figure dans un article de Pisot [54].]

22. Minoration de formes linéaires en logarithmes de nombres algébriques. Soient $\alpha_1, \ldots, \alpha_n$ des nombres algébriques et $b_1, \ldots, b_n$ des entiers avec $\max |b_i| = H$. Démontrer qu'il existe une constante positive C , effectivement calculable, telle que

$$b_1 \log \alpha_1 + \ldots + b_n \log \alpha_n \neq 0 \Rightarrow |b_1 \log \alpha_1 + \ldots + b_n \log \alpha_n| > e^{-CH} .$$

(Soit a_j $(1 \leq j \leq n)$ le coefficient dominant du polynôme minimal de α_j ou α_j^{-1} selon que b_j est positif ou non. Considérer le nombre algébrique

$$w = a_1^{|b_1|} \ldots a_n^{|b_n|} \, (\alpha_1^{b_1} \ldots \alpha_n^{b_n} - 1) .$$

Le minorer et conclure en utilisant l'inégalité $|z| \geq e^{-|z|} |e^z - 1|$.)

II. Le théorème de Thue-Siegel-Dyson-Gel'fond.

Dans tout ce chapitre α désigne un nombre algébrique réel de degré d, supérieur ou égal à trois.

1. Construction d'une fonction auxiliaire.

LEMME 1. - Soient r, s et ℓ des entiers positifs vérifiant $(r+1)(s+1) > d\ell$. Alors il existe un polynôme non nul, à coefficients entiers

$$A(X, Y) = \sum_{i=0}^{r} \sum_{j=0}^{s} a_{ij} X^i Y^j$$

tel que

$$\frac{\partial^{h+k}}{\partial X^h \partial Y^k} A(\alpha, \alpha) = 0$$

pour un ensemble E de ℓ couples (h, k) vérifiant $h+k < \ell$, et

$$\operatorname{Log} \|A\| \leq c_1 (r+s)\ell \,/\, ((r+1)(s+1) - d\ell) .$$

▶ Pour (h, k) parcourant E, il s'agit d'annuler les expressions

$$\varphi_{h,k} = \frac{1}{h!} \frac{1}{k!} \frac{\partial^{h+k}}{\partial X^h \partial Y^k} A(\alpha, \alpha) = \sum_{i=0}^{r} \sum_{j=0}^{s} \binom{i}{h} \binom{j}{k} a_{ij} \alpha^{i+j-h-k} ,$$

considérées comme formes linéaires en les inconnues a_{ij} .

On a la majoration

$$\|\varphi_{h,k}\|_1 \leq (2\alpha^*)^{r+s} .$$

Le théorème I. 4 montre l'existence d'une solution entière (a_{ij}) non triviale des inégalités

$$|\varphi_{h,k}| < (2\alpha^*)^{r+s} \; H^{-((r+1)(s+1)-\ell)/\ell} \qquad \text{pour } (h,k) \in E ,$$

$$\max |a_{ij}| \leq H \quad \text{(entier)} .$$

Si $\varphi_{h,k}$ n'est pas nul, le corollaire du théorème I. 4 fournit la minoration

$$|\varphi_{h,k}| \geq (2^{r+s} H)^{-d+1} \; \|\alpha\|_2^{-(r+s)} \; \alpha^{*\,r+s} .$$

D'où le résultat cherché si on choisit

$$H = [(2^d \|\alpha\|_2)^{(r+s)\ell/((r+1)(s+1) - d\ell)}] + 1 .$$

On peut donc prendre

$$c_1 = \mathrm{Log}(2^{d+1} \|\alpha\|_2) . \blacktriangleleft$$

2. La méthode de Thue.

2.1. Choix des paramètres.

Soit $p > \frac{d}{2} + 1$. On prend ϵ , $0 < \epsilon < 1/3$, tel que $p > 1 + (1+3\epsilon)\frac{d}{2}$. L'entier positif $\ell \geq 2$ sera choisi plus loin. On pose

$$r = [(1+\epsilon)d\ \ell/2]\ ,\quad s = 1\ ,\quad E = \{(h, 0);\ h = 0, \ldots, \ell-1\}\ .$$

Le polynôme construit plus haut est donc de la forme

$$A(X, Y) = P(X) - Y\ Q(X)\ ,$$

avec

$$\text{Log}\ (\max(\|P\|,\ \|Q\|)) \leq 2\ell\ \epsilon^{-1}\ c_1\ .$$

On suppose que l'inégalité

$$(1) \qquad |\alpha - \frac{p}{q}| < q^{-\rho} \qquad (\rho < d)$$

admet une infinité de solutions rationnelles. On peut donc choisir deux solutions p_1/q_1 et p_2/q_2 irréductibles, $q_2 > q_1 > 0$, telles que q_1 et $\log q_2/\log q_1$ soient assez grands.

2.2. Construction de γ non nul.

Considérons le polynôme

$$W(X) = P(X)\ Q'(X) - P'(X)\ Q(X)\ .$$

D'après le choix de A, α est une racine d'ordre au moins $\ell - 1$ de W. Montrons que W n'est pas nul. Dans le cas contraire, P et Q seraient proportionnels et donc divisibles par $(X-\alpha)^{\ell}$, ce qui est impossible puisqu'ils ne sont pas tous deux nuls et que leur degré est plus petit que $d\ell$.

De plus,

$$\|W\| \leq 2(r+1)^3 \|P\| \|Q\| \leq e^{c_2 \ell}, \quad c_2 = 12 \ell \varepsilon^{-1} c_1 .$$

En appliquant le lemme de Gauss (voir appendice), on obtient

$$v := \text{ordre}\,(W, p_1/q_1) \leq \frac{\log \|W\|}{\log q_1} \leq \frac{c_2 \ell}{\log q_1} .$$

Ce qui implique que les quotients

$$P^{(j)}(p_1/q_1) \,/\, Q^{(j)}(p_1/q_1) \quad , \quad j = 0, \ldots, v+1 ,$$

ne sont pas tous égaux. Ainsi il existe $j \leq v+1$ tel que le nombre

$$\gamma := \frac{1}{j!} \frac{\partial^j A}{\partial X^j} \left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) = \frac{1}{j!} \left(P^{(j)}(p_1/q_1) - \frac{p_2}{q_2} Q^j(p_1/q_1)\right)$$

soit non nul. On supposera $\log q_1 > 2c_2$; alors $j < \ell$.

2.3. Majoration de γ.

On a l'inégalité

$$|\gamma| \leq \frac{1}{j!}\left(|P^{(j)}(p_1/q_1) - \alpha\, Q^{(j)}(p_1/q_1)| + |\alpha - p_2/q_2|\ |Q^{(j)}(p_2/q_2)|\right).$$

D'après le choix de A,

$$\frac{1}{j!}\,|P^{(j)}(p_1/q_1) - \alpha\, Q^{(j)}(p_1/q_1)| = \left|\frac{1}{j!}\,\frac{\partial^j}{\partial X^j}\ A\left(\frac{p_1}{q_1}, \alpha\right)\right|$$

$$= \left|\sum_{h \geq \ell} \left(\alpha - \frac{p_1}{q_1}\right)^{h-j} \binom{h}{j} \frac{\partial^h}{h!\,\partial X^h}\ A(\alpha, \alpha)\right| \leq \left|\alpha - \frac{p_1}{q_1}\right|^{\ell-j} r\, 2^{2r}\, \|A\| \alpha^{*r+1},$$

et

$$\left|\frac{1}{j!}\, Q^{(j)}(p_1/q_1)\right| \leq 2^r\, \|A\|\, (p_1/q_1)^{*r}.$$

En appliquant (1), il vient

$$|\gamma| \leq r\, 2^{2r(q_1^{-\rho(\ell-j)} + q_2^{-\rho})}\, \|A\|\, (\alpha^*+1)^r \leq e^{c_3 \ell} \max(q_1^{-\rho(\ell-j)}, q_2^{-\rho}),$$

où $c_3 = 2\, e^{-1}\, c_1 + (3 + \mathrm{Log}(\alpha^*+1))d$.

2.4. Minoration de $|\gamma|$.

Clairement,

$$|\gamma| \geq q_1^{-r+j}\, q_2^{-1}.$$

2.5. Conclusion.

L'encadrement précédent de $|\gamma|$ donne, en choisissant $\ell = [\log q_2/\log q_1] + 1$, et en utilisant la majoration $j \leq v+1$,

$$q_1^{-r-(v+1)(\rho-1)} \; q_2^{(\rho-1)} \le e^{c_3 \ell} .$$

En tenant compte de la majoration antérieure de v, on en déduit

$$(\rho-1-(1+\epsilon)\frac{d}{2} - \frac{c_2+c_3}{\log q_1}) \ell \le \rho - 1 .$$

Pour $\log q_1 > (c_2 + c_3)/\epsilon$, on a donc

$$(\rho-1-(1+2\epsilon)\frac{d}{2}) \ell \le \rho - 1 ,$$

et en particulier

$$\ell \le 2/\epsilon \qquad \text{(on a supposé } 1+(1+3\epsilon)\frac{d}{2} < \rho < d) .$$

Nous avons donc obtenu le théorème de Thue : pour $\rho > \frac{d}{2} + 1$ l'inégalité (1) n'a qu'un nombre fini de solutions rationnelles. Mais, en analysant la démonstration, on constate qu'on a démontré le résultat suivant :

(T) Pour $\rho > 1+(1+3\epsilon)d/2$, $\epsilon > 0$, si (1) admet une solution p_1/q_1 avec $q_1 > Q(\alpha, \epsilon)$ (explicite) alors toute autre solution p_2/q_2, avec $q_2 > q_1$, vérifie

$$\frac{\log q_2}{\log q_1} < \frac{\rho-1}{\rho-1-(1+2\epsilon)d/2} .$$

3. La méthode de Siegel.

3. 1. On considère encore, si elles existent, deux solutions irréductibles p_1/q_1 et p_2/q_2 de (1) telles que $q_2 > q_1 > 0$, q_1 assez grand. On pose

$$\ell = [\frac{\log q_2}{\log q_1}] \quad , \quad r = \frac{(1+\epsilon)d\ell}{s+1} \quad , \quad E = \{(h, 0),\ h = 0, \ldots, \ell-1\} .$$

où ϵ est un nombre positif très petit et s un entier positif plus petit que d . On utilise la fonction auxiliaire A construite au lemme 1 , qui vérifie donc

$$\text{Log } \|A\| \leq (2d\ \ell/\epsilon)c_1 .$$

3. 2. Pour construire γ nous avons besoin du lemme suivant.

LEMME 2. - Soit K un corps de caractéristique 0 et soient $f_1, \ldots, f_n \in K(X)$, linéairement indépendants sur K . Alors, le wronskien

$$W = W(f_1, \ldots, f_n) = \begin{vmatrix} f_1 & \ldots\ldots & f_n \\ f_1' & \ldots\ldots & f_n' \\ \ldots & \ldots & \ldots \\ f_1^{(n-1)} & \ldots\ldots & f_n^{(n-1)} \end{vmatrix}$$

n'est pas nul.

▶ Le cas $n = 1$ est trivial. Récurrence sur n. Supposons le résultat vrai pour $n - 1$ facteurs. Posons $g_k = \frac{d}{dX}(f_k/f_n)$ pour $k = 1, \ldots, n-1$. L'indépendance des f_i entraîne celle des g_k. L'hypothèse de récurrence implique donc

$$W(g_1, \ldots, g_{n-1}) \neq 0 .$$

La conclusion résulte de la relation

$$W(f_1, \ldots, f_n) = f_n^{\,n} \; W(g_1, \ldots, g_{n-1}) . \blacktriangleleft$$

Dans la démonstration du théorème de Thue nous avons rencontré le cas particulier $n = 2$ de ce lemme.

Nous nous proposons maintenant de majorer la quantité

$$u = \text{ordre } (A(X, p_2/q_2),\ p_1/q_1) .$$

On procèdera en plusieurs étapes.

1) Remarquons d'abord que le polynôme $A(X, p_2/q_2)$ n'est pas identiquement nul. On a

$$A(X, p_2/q_2) = \sum_{i=0}^{r} \Big(\sum_{j=0}^{s} a_{ij} (p_2/q_2)^j \Big) X^i ,$$

et il existe i_0 tel que le polynôme $\sum_j a_{i_0 j} Y^j$ soit non nul. D'après

le lemme de Gauss, on a

$$\Sigma\ a_{i_0 j}(p_2/q_2)^j \neq 0 \quad \text{si} \quad q_2 > \max\ |a_{i_0 j}|,$$

et cette dernière condition a lieu pour

$$\log q_1 > 4d\ c_1/\epsilon\ ,$$

ce qu'on supposera vérifié (on a alors

$$\log q_2 \geq \frac{\ell}{2}\ \log q_1 > 2d\ c_1\ \ell/\epsilon \geq \|A\|)\ .$$

2) Parmi les écritures possibles

$$A(X, Y) = \sum_{k=0}^{t} U_k(X)\ V_k(Y)\ ,$$

où U_k et V_k sont des polynômes à coefficients rationnels (il en existe : $A = \sum_{j=0}^{s} (\sum_{i=0}^{r} a_{ij} X^i) Y^j)$, choisissons en une où t est minimal (donc $t \leq s$) . Alors $U_0, \ldots, U_t$ (et $V_0, \ldots, V_t$) sont linéairement indépendants sur $\mathbb{Q}$. Le polynôme $W(X) = W(U_0, \ldots, U_t)$ est non nul d'après le lemme 2 . De plus, d'après 1) , l'un des $V_k(p_2/q_2)$ n'est pas nul ; On suppose que tel est le cas pour $V_0(p_2/q_2)$. De la relation

$$(2) \qquad W(X)\ V_0(Y) = \begin{vmatrix} A(X,\ Y) & U_2(X) \ldots\ U_t(X) \\ \frac{\partial}{\partial X}\ A(X,\ Y) & \frac{\partial}{\partial X}\ U_2(X) \\ \ldots\ldots\ldots\ldots\ldots\ldots & \\ \frac{\partial^t}{\partial X^t}\ A(X,\ Y) \ldots\ldots\ldots & \end{vmatrix}$$

on déduit

$$\text{ordre}\ (A(X,\ p_2/q_2),\ p_1/q_1) \leq t + \text{ordre}\ (W(X),\ p_1/q_1)\ .$$

3) Il reste à majorer l'ordre de W au point p_1/q_1. D'après (2) et le choix de A, on a

$$\text{ordre}\ (V_0(\alpha)\ W(X),\ \alpha) \geq \ell - t\ ,$$

avec $V_0(\alpha)$ non nul, puisque $\deg V_0 \leq s < d$. Donc W est de la forme $W = R^{\ell-t}\ W_0$, où R désigne le polynôme minimal de α. On en déduit

$$\text{ordre}\ (W,\ p_1/q_1) \leq \text{ordre}\ (W_0,\ p_1/q_1) \leq \deg(W_0) \leq (t+1)r - d(\ell - t)\ .$$

4) En conclusion, on a montré qu'il existe j tel que le nombre

$$\gamma := \frac{1}{j!}\ \frac{\partial^j}{\partial X^j}\ A(p_1/q_1,\ p_2/q_2)$$

soit non nul, avec

$$j \le t+(t+1)r-d(\ell-t) \le \epsilon\, d\, \ell + (d+1)s < \epsilon\, d\, \ell + d^2 \ .$$

3.3. La même méthode qu'en 2.3. fournit la majoration

$$|\gamma| \le 2r\, 2^{2r}\, \|A\|(\alpha^*+1)^r \ \max\,(q_1^{-\rho(\ell-j)},\ q_2^{-\rho})$$
$$\le e^{c_4 \ell} \max\,(q_1^{-\rho(\ell-j)},\ q_2^{-\rho})\ ,\ c_4 = 2c_1 d\ \epsilon^{-1} + (4+\mathrm{Log}(\alpha^*+1))d.$$

3.4. On a encore

$$|\gamma| \ge q_1^{-r+j}\, q_2^{-s} \ .$$

3.5. De l'encadrement de γ, en tenant compte du choix de r, ℓ et de la majoration de j, on obtient

$$(\log q_1\,(\rho - \tfrac{1+\epsilon}{s+1}\ d-s-(\rho-1)\epsilon\, d) - c_4)\,\ell \le \log q_1\,(s+(\rho-1)d^2) \ .$$

Soit ρ vérifiant

$$\rho > \min_{1\le s\le d}\ (\frac{d}{s+1} - s) \ ,$$

et soit s un entier où ce minimum est atteint.
Alors, pour ϵ assez petit et $\log q_1$ assez grand, le coefficient de ℓ dans l'inégalité ci-dessus est positif, il en résulte que ℓ est borné, donc aussi $\log q_2/\log q_1$. Le théorème de Siegel est donc démontré.
Plus précisément nous avons obtenu le résultat suivant.

(S) Pour des paramètres ρ , ϵ , s (s entier, $0 < s < d$) vérifiant

$$\rho(1-\epsilon\, d) > (1+\epsilon)\, d/(s+1) + s \ ,$$

on peut déterminer une quantité $Q_1(\alpha, \epsilon)$ telle que si p_1/q_1 et p_2/q_2 sont deux solutions irréductibles de (1) , avec $q_2 > q_1 > Q_1(\alpha, \epsilon)$ alors on a

$$[\log q_2/\log q_1] \leq \frac{s+(\rho-1)d^2}{\rho(1-\epsilon\, d) - \frac{(1+\epsilon)d}{s+1} - s} \ .$$

4. La méthode de Dyson-Gel'fond.

4.1. Soient deux solutions irréductibles p_1/q_1 , p_2/q_2 de (1) , avec $q_2 > q_1 > 0$, q_1 assez grand. On pose $\omega = \text{Log } q_2/\text{Log } q_1$. Soient maintenant ϵ un nombre positif fixé ($\epsilon < 1$) et ℓ un entier très grand. On choisit

$$r = [(d\ell(1+\epsilon)\,(\omega+\rho-1))^{1/2}] \ , \quad s = [(d\ell(1+\epsilon)/(\omega+\rho-1)^{1/2}] \ ,$$
$$E = \{(h,\, k) \in \mathbb{N}^2 \ ; \ \frac{h}{a} + \frac{k}{b} < 1\} \quad \text{où} \quad a = \sqrt{2\omega\ell} - \omega \ , \quad b = \sqrt{2\ell/\omega} - 1 \ .$$

Alors,

$$\text{Card}(E) \leq (a+1)\,(b+1)/2 \leq \ell \ .$$

On applique le lemme 1 (qui est encore vrai pour Card $E \leq \ell$) , ici $(r+1)\,(s+1) \geq (1+\epsilon)\, d\, \ell$, donc on trouve

$$\log \|A\| \leq c_1(r+s)/d \ \varepsilon \ .$$

4.2. On cherche à nouveau à majorer la quantité

$$u = \text{ordre } (A(X,\ p_2/q_2)\ ,\ p_1/q_1) \ .$$

On considère comme plus haut une écriture la plus courte possible

$$A(X,\ Y) = \sum_{k=0}^{t} U_k(X)\ V_k(Y) \qquad (\text{donc } t \leq s)\ ,$$

et on lui associe les wronskiens

$$U^*(X) = \frac{1}{1!\ldots t!}\ W(U_0,\ldots,U_t)\ ,\ V^*(Y) = \frac{1}{1!\ldots t!}\ W(V_0,\ldots,V_t)$$

qui vérifient la relation

$$W(X,\ Y) := U^*(X)\ V^*(Y) = \det\left(\frac{1}{i!j!}\ \frac{\partial^{i+j}}{\partial X^i \partial Y^j}\ A(X,\ Y)\right) .$$

D'après le lemme 2 , W n'est pas nul ; de plus, c'est un polynôme à coefficients entiers et le lemme de Gauss implique que W admet une factorisation

$$W = U(X)\ V(Y)\ ,$$

où U et V sont à coefficients entiers.

La hauteur de W majore celle de U et V , on en déduit

$$\mathrm{Log}(\max(\|U\|,\ \|V\|)) \le \mathrm{Log}(2^{2t(r+s)}\ t!\ \|A\|^t)$$
$$< t(r+s)\ (3+c_1/d\epsilon) \le 6d(3+c_1/d\epsilon)\ \ell\ .$$

Pour $\log q_1 \ge 6(3d+c_1/\epsilon)\ \ell/\omega\epsilon$, ce qu'on supposera, on a donc $V(p_2/q_2) \neq 0$, ce qui montre que le polynôme $A(X,\ p_2/q_2)$ n'est pas nul. On a alors

$$u \le t + [(\mathrm{Log}\|W\|)/\mathrm{Log}\ q_1] = t+\epsilon\omega\ .$$

D'où l'existence d'un entier $j \le s+\epsilon\omega$ tel que le nombre

$$\gamma := \frac{1}{j!}\frac{\partial^j}{\partial X^j}\ A(p_1/q_1,\ p_2/q_2)$$

soit non nul.

4.3. En utilisant la formule de Taylor au point $(\alpha,\ \alpha)$, il vient

$$|\gamma| \le 4.\ 2^{2(r+s)}\ \|A\| \max_{\frac{h}{a}+\frac{k}{b}\ge 1} \left(\left|\alpha-\frac{p_1}{q_1}\right|^{h-j} \left|\alpha-\frac{p_2}{q_2}\right|^{k}\right)$$
$$\le \exp((3+c_1/d\epsilon)(r+s)) \max_{\frac{h}{a}+\frac{k}{b}\ge 1} (q_1^{-\rho(h-j)}\ q_2^{-\rho k})\ .$$

4.4. La minoration de $|\gamma|$ est toujours aussi facile,

$$|\gamma| \ge q_1^{-(r-j)}\ q_2^{-s}\ .$$

4.5. En comparant la minoration et la majoration de $|\gamma|$, il vient

$$r+(\rho-1+(1+\epsilon)\omega)s \geq -\epsilon\,\omega\sqrt{d(\omega+\rho-1)/\ell} + \rho\, a\,.$$

On en déduit

$$2\sqrt{d\;\ell(\omega+\rho-1)} + 2\epsilon\sqrt{d\;\ell} - \rho\sqrt{2\omega\ell}+\rho\omega+\epsilon\omega\sqrt{d(\omega+\rho-1)/\ell} \geq 0\,.$$

Choisissons $\ell = [d(\omega+\rho-1)\epsilon^{-2}]+1$; l'inégalité précédente implique alors

$$2(1+\epsilon)\sqrt{d(\omega+\rho-1)} > (1-\epsilon)\rho\sqrt{2\omega}\,,$$

ou

$$\omega(\rho^2-2(\tfrac{1+\epsilon}{1-\epsilon})^2\,d) < 2(\tfrac{1+\epsilon}{1-\epsilon})^2\,d(\rho-1)\,.$$

Nous avons démontré le résultat suivant.

(G) <u>Pour</u> $\rho > ((1+\epsilon)/(1-\epsilon))\sqrt{2\,d}$, $0<\epsilon<1$, <u>si</u> (1) <u>admet une solution irréductible</u> p_1/q_1 <u>avec</u> $q_1 > Q_2(\alpha,\epsilon)$ <u>(effectif) alors toute autre solution irréductible</u> p_2/q_2, <u>avec</u> $q_2 > q_1$, <u>vérifie</u>

$$\frac{\log q_2}{\log q_1} < \frac{2d(\rho-1)}{(\frac{1-\epsilon}{1+\epsilon})^2\,\rho^2 - 2d}\,.$$

5. <u>Complément au théorème de Thue-Siegel-Dyson-Gel'fond</u>.

1. Considérons deux solutions irréductibles p_1/q_1 et p_2/q_2 de (1) vérifiant $q_2 > q_1$, on a

$$1 \leq |p_1 q_2 - p_2 q_1| \leq q_2 |p_1 - \alpha q_1| + q_1 |p_2 - \alpha q_2|$$
$$< q_2 q_1^{-\rho+1} + q_1 q_2^{-\rho+1} < 2 q_1 q_2^{-\rho+1} ,$$

et donc

$$2 q_2 > q_1^{\rho-1} .$$

Posons $\omega = \log q_2 / \log q_1$. Soit $\eta > 0$ fixé, d'après l'inégalité précédente et l'assertion (G) , pour $\rho > \sqrt{2d}$, on a

(3) $$\rho - 1 - \eta < \omega < (2d(\rho-1)/(\rho^2 - 2d)) + \eta \quad , \quad \text{si} \quad q_1 > Q_3(\alpha, \eta) \quad \text{(effectif)} .$$

D'où, en particulier, la proposition suivante.

LEMME 3. - Soit α un nombre algébrique de degré d , alors pour $\rho > 2\sqrt{d}$, on peut déterminer $Q_4(\alpha, \rho)$ tel que l'inégalité

$$|\alpha - p/q| < q^{-\rho}$$

admette au plus une solution irréductible vérifiant $q > Q_4(\alpha, \rho)$.

2. Grâce à la méthode de Thue, nous allons éliminer l'intervalle (3) . Nous avons besoin de quelques lemmes algébriques.

LEMME 4. - Soient α, β, γ trois nombres distincts, ℓ un entier positif. Alors s'il existe des formes binaires A, B, C de degré au plus m , non toutes nulles, vérifiant

$$(X-\alpha)^{\ell} A(X, Y) + (X-\beta)^{\ell} B(X, Y) + (X-\gamma)^{\ell} C(X, Y) = 0$$

<u>on a</u> $m \geq [h/2]$.

▶ Supposons l'assertion du lemme fausse. Par multiplication par une puissance convenable de Y , on peut se ramener au cas où les formes A, B, C, non toutes nulles, ont un degré maximal m égal à $[\ell/2]-1$. On peut supposer B et C non nulles, et, par translation, α égal à zéro. Appliquons maintenant l'opérateur $(\partial/\partial Y)^m$ à la relation du lemme, nous obtenons une identité de la forme

$$(X-\beta Y)^{\ell-m} B_1(X, Y) + (X-\gamma Y)^{\ell-m} C_1(X, Y) = 0 \ ,$$

où B_1 et C_1 sont des formes de degré au plus m , non nulles (du fait que X^{ℓ} ne divise ni B ni C). Cette nouvelle égalité est impossible puisqu'elle implique que $(X-\beta Y)^{\ell-m}$ divise C_1 , et donc $\ell-m > m$. Cette contradiction achève la démonstration. ◀

COROLLAIRE. - <u>Soit</u> α <u>un nombre algébrique cubique et soit un système du type</u>

$$P_0^{(i)}(\alpha) + \alpha P_i^{(i)}(\alpha) = 0 \quad , \quad i = 0, 1, \ldots, \ell-1 \ ,$$

<u>où les</u> P_i <u>sont des polynômes à coefficients entiers, non tous nuls, de degré maximal</u> r . <u>Alors on a</u> $r \geq [3\ell/2]$.

▶ Le système ci-dessus équivaut à une relation de la forme

$$P(X, Y) + \alpha\, Q(X, Y) = (X-\alpha Y)^{\ell}\, A(X, Y) \ ,$$

où A est une forme binaire de degré au plus $r-\ell$. En remplaçant α par ses conjugués, on obtient deux nouvelles relations analogues. En éliminant P et Q entre ces trois relations, on aboutit à une identité semblable à celle du lemme, avec des formes de degré au plus $r-\ell$. On a donc $r-\ell \geq [\ell/2]$. Ou $r \geq [3\ell/2]$. ◀

LEMME 5. - Soient α un nombre algébrique irrationnel de degré d et P et Q deux polynômes à coefficients entiers de degré plus petit que d, non nuls. Alors le système

$$P'(\alpha) + \alpha\, Q'(\alpha) = P(\alpha) + \alpha\, Q(\alpha) = 0$$

est impossible.

▶ Supposons que ce système admette des solutions vérifiant les hypothèses du lemme. Le polynôme $P'(X) + X\, Q'(X)$, dont le degré est plus petit que d et qui s'annule en α, est nul. Il en résulte d'une part que le degré de Q est plus petit que $d-1$ et, par intégration, que le polynôme $P(X) + X\, Q(X) - R(X)$ est nul, si $R(X)$ désigne la primitive de Q qui s'annule en zéro. On déduit de la première assertion et de la relation $P(\alpha) + \alpha\, Q(\alpha) = 0$ que le polynôme $P(X) + X\, Q(X)$ est nul. L'application de la seconde assertion montre que R est nul. Il en résulte que P et Q sont nuls. Cette contradiction termine la démonstration. ◀

COROLLAIRE. - Les seuls polynômes à coefficients entiers de degré au plus $d+\ell-2$ vérifiant

$$P_0^{(i)}(\alpha) + \alpha P_1^{(i)}(\alpha) = 0 \quad , \quad \text{pour} \quad i = 0, 1, \ldots, \ell-1 \qquad (\ell \geq 3) \ ,$$

où α est un irrationnel algébrique de degré d, sont les polynômes nuls.

> Appliquer le lemme aux polynômes $P = P_0^{(\ell-2)}$ et $Q = P_1^{(\ell-2)}$.<

LEMME 6. - Soit $h(X) = f(X)/g(X)$ une fraction rationnelle sur $\mathbb{Z}$, irréductible, non nulle, de degré d (égal au maximum des degrés de f et g). Soit a un nombre rationnel tel que $f(a)\,g(a)$ soit non nul, alors on a

$$(2d(\|f\|_2 \|g\|_2)^{d-1})^{-1} \|a\|^d \leq \|h(a)\| \leq \max(\|f\|_1, \|g\|_1)\, \|a\|^d \ .$$

> L'inégalité de droite est évidente. Considérons celle de gauche. Soient F et G les formes binaires associées respectivement à f et g. Si R désigne le résultant des polynômes f et g, il existe des formes S, T, U, V à coefficients entiers telles que l'on ait

$$S F + T G = R X^k \quad , \quad U F + V G = R Y^k \ .$$

Il en résulte que si $a = p/q$, où p et q sont premiers entre eux, le p. g. c. d. de $F(p, q)$ et $G(p, q)$ divise R. On a donc

$$\|h(a)\| \geq \max(|F(p, q)|, |G(p, q)|)/|R| \ .$$

Reste à minorer le nombre de droite. On peut supposer $\|a\| = q$. On considère alors à nouveau la relation

$$U(p, q)\, F(p, q) + V(p, q)\, G(p, q) = R\, q^{k} \ ,$$

où

$$k = \deg(F) + \deg(G) - 1 \ , \ \deg U = \deg(G) - 1, \ \deg V = \deg(F) - 1 \ .$$

Par conséquent,

$$\max(|F(p, q)|, |G(p, q)|) \geq |R/2d|\, q^{d} / \max(\|U\|, \|V\|) \ .$$

L'écriture des formules de Cramer donnant U et V conduit, en utilisant l'inégalité de Hadamard sur les déterminants, à la majoration

$$\max(\|U\|, \|V\|) \leq \|f\|_2^{\deg(g)-1}\, \|g\|_2^{\deg(f)-1} / |R| \ .$$

D'où le résultat.<

3. Reprenons la méthode de Thue. Nous considérons des fonctions auxiliaires non nulles, à coefficients entiers,

$$A(X, Y) = P_0(X) + Y\, P_1(X) \ ,$$

où les P_i ont pour degré maximal r , et qui vérifient

$$\frac{\partial^h}{\partial X^h} A(\alpha, \alpha) = 0 \quad \text{pour} \quad h = 0, 1, \ldots, \ell - 1 \ , \quad (\ell \geq 2) \ ,$$

où ℓ ne prendra qu'un nombre fini de valeurs. Dans ces conditions (voir exercice 1) $\|A\|$ sera majoré par une constante ne dépendant que de α. Soit alors un nombre γ non nul de la forme

$$\gamma = \frac{\partial^j}{\partial X^j} \; A(p_1/q_1, \; p_2/q_2) \; .$$

L'encadrement de γ (voir 2.3 et 2.4)

$$q_1^{-r+j} \; q_2^{-1} \leq |\gamma| < e^{c_5} \max(q_1^{-\rho(\ell-j)}, \; q_2^{-\rho})$$

montre que ω n'appartient pas à l'intervalle $I_\ell = [\alpha(r,j)-\eta, \; \beta(r,j)+\eta]$, où

$$\alpha(r, \; j) = (r-j)/(\rho-1) \quad , \quad \beta(r, \; j) = \rho(\ell-j)-(r-j) \; ,$$

dès que q_1 vérifie $\log q_1 \geq c_5/\eta$. D'après les inégalités (3), dès que l'union de certains intervalles I_ℓ recouvre l'intervalle $[\rho-1-\eta, \; \Omega+\eta]$, où $\Omega = \Omega(\rho) = 2d(\rho-1)/(\rho^2-2d)$, on aboutit à une contradiction. Si ρ_d désigne un nombre tel que pour $\rho > \rho_d$ cette condition ait lieu pour η assez petite, on aura prouvé que pour tout nombre algébrique de degré d et pour $\rho > \rho_d$ on peut déterminer effectivement toutes les solutions irréductibles de (1) sauf au plus l'une d'elles. L'existence de ce nombre ρ_d a été démontrée en 1., avec $\rho_d = 2\sqrt{d}$. Nous allons chercher pour $d = 3$ et 4 un nombre ρ_d aussi petit que possible.

Il nous faudra utiliser des informations plus précises sur les fonctions

auxiliaires A. Nous ne considèrerons que des polynômes A de degré minimal, ce qui impose que le p.g.c.d. D de P_0 et P_1 est une puissance de F, le polynôme minimal de α, et de plus $r \le [d\,\ell/2]$. Notons aussi que si $A(p_1/q_1, p_2/q_2) = 0$, et si $Q_0 = P_0/D$, $Q_1 = P_1/D$, on a

$$Q_0(p_1/q_1)/Q_1(p_1, q_1) = -q_2/p_2 .$$

On peut borner explicitement les hauteurs de Q_0 et Q_1 (par exemple en utilisant l'exercice I.8). Le lemme 6 montre alors que l'on a

(4) $$r\text{-deg } D - \eta < \omega < r\text{-deg } D + \eta \qquad \text{si } j = 1$$

pour $q > Q_4(\alpha)$ (effectif).

4. Soit α un irrationnel cubique. Le corollaire du lemme 4 montre que l'on a nécessairement $r = [3\ell/2]$ et $D = 1$. Pour chaque valeur de ℓ on a donc deux possibilités (dès que q_1 est assez grand)

(i) $j = 0$ et $\omega \notin J_\ell = [\alpha_\ell + \eta, \beta_\ell - \eta]$, où $\alpha_\ell = r/(\rho-1)$, $\beta_\ell = \rho\ell - r$,

(ii) $j = 1$ et $r - \eta < \omega < r + \eta$.

Notons que les valeurs de r sont distinctes et donc que la seconde possibilité ne peut se produire qu'au plus une fois. De plus, pour $\rho > 1+\sqrt{3}$, on a $\alpha_2 < \rho - 1$, $\beta_6 > \Omega$, et

$$\begin{aligned}\beta_\ell - \alpha_{\ell+1} &= \ell\rho - [3\ell/2] - [3(\ell+1)/2]/(\rho-1)\\ &\geq \ell\rho - 3\ell/2 - (3(\ell+1)-1)/(2(\rho-1))\\ &= (1-3/(2\rho-2))\rho\ell - 1/(\rho-1)\\ &> (\sqrt{3}-1)\ell/2 - 1\sqrt{3} \geq \sqrt{3}-1-1\sqrt{3} > 0 \ ,\end{aligned}$$

donc les intervalles $J_2, \ldots, J_6$ recouvrent $[\rho-1-\eta, \Omega+\eta]$ dès que η est assez petit. Ainsi, la seconde approximation p_2/q_2 ne peut exister que si (ii) se produit et, de plus, (ii) ne peut se produire que pour une valeur de ℓ telle que r appartienne à l'intervalle $[\alpha_\ell, \beta_\ell]$. Or,

$$r \leq \beta_\ell \Rightarrow 2[3\ell/2] \leq \ell\rho \Rightarrow (\ell \text{ impair et } 3\ell-1 < \ell\rho) \Rightarrow \ell = 3 \ .$$

Mais pour $\ell = 3$, on a $r = 4$ et comme $\alpha_4 < 4 < \beta_4$ la possibilité (ii) est encore exclue. On peut donc prendre $\rho_3 = 1 + \sqrt{3}$.

5. Considérons maintenant le cas $d = 4$. Supposons $\rho > (3+\sqrt{13})/2$ et q_1 assez grand. Si $\alpha_\ell = 2\ell/(\rho-1)$ et $\beta_\ell = \ell(\rho-2)$, on a pour $\ell \geq 2$

$$\beta_\ell - \alpha_{\ell+1} = (\rho-2-2/(\rho-1))\ell - 2/(\rho-1) \geq 2(\rho-2-3/(\rho-1)) > 0 \ ,$$

$\alpha_2 < \rho-1$ et $\beta_4 > \alpha_6$.

Considérons particulièrement le cas $\ell = 6$. On a $\alpha(6, j) \leq \alpha_6 < 6$. Minorons $\beta(6, j)$. Si r est au plus égal à 11 alors $\beta(6, j) \geq 5\rho-10$. Sinon, on peut trouver deux solutions $A = P_0 + Y P_1$, $A_1 = P_2 + Y P_3$ telles que $\deg P_0 = \deg P_3 = 12$, $\deg P_1 < 12$, $\deg P_2 < 12$. Le

polynôme $P_0P_3-P_1P_2$ n'est pas nul, on peut donc trouver γ non nul avec $j = 0$. Dans les deux cas, $\beta(6, j) > \Omega(\rho)$ et donc $\omega < \alpha_6+\eta < 6-\eta$. Pour $\ell = 4$, on a $6 \le r \le 8$ (d'après le lemme 1 et le corollaire du lemme 5), $D = 1$ car $r > 4$ pour $\ell = 3$ (d'après le corollaire du lemme 5) ; la majoration $\omega < 6-\eta$ jointe à (4) montre que j est nul. Donc $\omega < \alpha_4+\eta < 5-\eta$. Pour $\ell = 3$ on a $5 \le r \le 6$, $D = 1$ (car $r \ge 4$ pour $\ell = 2$), la relation (4) montre encore que j est nul. Donc $\omega < \alpha_3+\eta < 4-\eta$. Pour $\ell = 2$ on a $r = 4$, $D = 1$ et $j = 0$. On a recouvert l'intervalle $[\rho-1-\eta, \Omega+\eta]$. Ainsi $\rho_4 = (3+\sqrt{13})/2$ convient.

6. Résumons les résultats obtenus.

PROPOSITION. - Soit α un nombre algébrique de degré $d \ge 3$. Il existe un nombre $\rho_d < d$ tel que pour $\rho > \rho_d$ on puisse déterminer toutes les solutions irréductibles de l'inégalité

$$|\alpha-p/q| < q^{-\rho}$$

sauf au plus l'une d'entre elles. On peut choisir

$$\rho_3 = 1 + \sqrt{3}$$
$$\rho_4 = (3 + \sqrt{13})/2$$
$$\rho_d = 2\sqrt{d} \quad \text{pour} \quad d \ge 5 .$$

NOTES. -

§ 4 Notre théorème (G) améliore le théorème de Gel'fond ([22], th. 1, chapitre 1) en ce sens qu'il fournit une meilleure majoration de $\log q_2/\log q_1$.

§ 5 C'est Schinzel [61] qui le premier démontra l'existence de ρ_d pour $d \geq 5$), il obtient $\rho_d = 3\sqrt{d/2}$ en utilisant le théorème 1, chap. 1, de l'ouvrage de Gel'fond [22]. Indépendamment, Davenport [15] démontra l'existence de ρ_d (pour $d \geq 3$) en utilisant la méthode de Thue. La valeur obtenue par Davenport est de la forme $d/2+0(1)$. Nous indiquons dans le tableau suivant la comparaison entre ces résultats et les nôtres.

d	Schinzel	Davenport	notre méthode
3		2,732	
4		3,828	3,415
5	4,743	4,236	3,646
6	5,196	4,832	4,236
7	5,612	5,238	4,622
8	6	5,899	5
9	6,364	6,357	5,677
10	6,708	6,916	6,154
11	7,305	7,326	6,563
12	7,348	7,928	6,929

La démonstration donnée ici pour $d = 3$ est extraite de l'article de Davenport.

Il est à noter que des améliorations effectives du théorème de Liouville sont connues. Baker [2, 3] fut le premier à obtenir un tel résultat pour certains nombres algébriques, comme par exemple $\sqrt[3]{2}$. Puis

Baker [8] et Feldman [21] démontrèrent que pour tout nombre algébrique α de degré $d \geq 3$ il existe $\rho = \rho(\alpha) < d$ tel que l'on puisse effectivement déterminer toutes les solutions de l'inégalité (1). Il n'en reste pas moins que dans tous les cas les valeurs de $\rho(\alpha)$ sont proches de d, donc très supérieures à ρ_d. A l'heure actuelle on ne connaît aucun exemple d'une forme effective au théorème d'approximation de Thue. Ainsi, la connaissance de ρ_d présente encore aujourd'hui un intérêt. Par exemple, elle permet d'obtenir des informations sur certaines équations déophantiennes qui résistent à l'étude par toute autre méthode générale (voir III. 5).

Exercices

1. Soient m et n deux entiers, $m \geq n$. Si le système à coefficients entiers

$$a_{i1} X_1 + \ldots + a_{in} X_n = 0 \quad \text{pour} \quad i = 1, \ldots, m$$

admet une solution entière non triviale, démontrer qu'il admet une solution entière $(x_1, \ldots, x_n)$ non triviale et telle que

$$0 < \max_i |x_i| \leq (\sqrt{n-1}\, A)^{n-1} \quad , \text{ où } \quad A = \max_{i,j} |a_{ij}| .$$

(Soit r le rang du système, $r < n$. En changeant éventuellement la numérotation on peut supposer que le déterminant Δ de la matrice des (a_{ij}) $(1 \leq i, j \leq r)$ est non nul. Le déterminant de la matrice

$(a_{ij})_{1\leq i,j\leq r+1}$ est nul, soit x_j le cofacteur de $a_{r+1,j}$ pour $j = 1, \ldots, r+1$ et $x_j = 0$ pour $j = r+2, \ldots, m$, on a donc

$$a_{i1} x_1 + \ldots + a_{in} x_n = 0 \quad \text{pour} \quad 1 \leq i \leq r+1 .$$

Ces égalités sont encore vérifiées pour $i = r+2, \ldots, n$ puisque les $m-r-1$ dernières équations sont des combinaisons linéaires des r premières. Majorer les x_j. Voir [20], chap. II.)

2. 1°) Démontrer le résultat suivant.

Soient $\alpha_1, \ldots, \alpha_k$ des nombres distincts et ℓ un entier positif, alors s'il existe des formes $A_1(X, Y), \ldots, A_2(X, Y)$ de degré maximal m, non toutes nulles telles que l'on ait

$$(X-\alpha_1 Y)^{\ell} A_1(X, Y) + \ldots + (X-\alpha_k Y)^{\ell} A_k(X, Y) = 0$$

on a nécessairement $m \geq [\ell/(k-1)]$.

2°) En déduire que si α est un nombre algébrique de degré d et si le système

$$P_0^{(i)}(\alpha) + \alpha P_1^{(i)}(\alpha) + \ldots + \alpha^s P_s^{(i)}(\alpha) = 0 \quad i = 0, \ldots, \ell-1$$
$$(s \leq d-2)$$

admet une solution non triviale à coefficients entiers alors on a

$$\max (\deg (P_i)) \geq [(s+2)\ell/(s-1)] .$$

3. Généraliser le théorème de Thue en démontrant que si K est un corps de nombres fixé et si α est un nombre algébrique de degré $d \geq 3$ sur K l'inégalité

$$|\alpha-\beta| < \|\beta\|_1^{-\rho}$$

n'a qu'un nombre fini de solutions β dans K pour $\rho > 1+d/2$.

4. Soient $\alpha_1, \ldots, \alpha_n$ des nombres algébriques non nuls. Soit $\epsilon > 0$ fixé démontrer que la relation

$$(R) \qquad 0 < |\alpha_1^{b_1} \ldots \alpha_{n-1}^{b_{n-1}} - \alpha_n| < e^{-\epsilon H} \quad , \quad H = \max |b_i| \ ,$$

n'a qu'un nombre fini de solutions entières $b_1, \ldots, b_{n-1}$.
(Raisonner par l'absurde. Supposer que la relation ci-dessus a une infinité de solutions entières $b_1, \ldots, b_{n-1}$. Soit s un entier positif fixé. Quitte à restreindre l'ensemble des $(b_1, \ldots, b_{n-1})$, on peut supposer que ces nombres sont de la forme $b_j = s\, b'_j + r_j$ où les $r_1, \ldots, r_{n-1}$ sont fixes et vérifient $0 \leq r_j < s$. Si $\alpha = \alpha_1^{b'_1} \ldots \alpha_{n-1}^{b'_{n-1}}$ et $\omega = \alpha_1^{r_1} \ldots \alpha_{n-1}^{r_{n-1}}$ alors (R) implique

$$0 < |\alpha^s - \alpha_n/\omega| < e^{-\epsilon\, s\, H'/3} \quad , \text{ où } H' = \max_j b'_j \ .$$

En déduire qu'il existe une racine s-ième de α_n/ω , disons β , telle que les inégalités

$$0 < |\alpha - \beta| < e^{-\epsilon\, s\, H'/4}$$

admettent une infinité de solutions. Démontrer qu'il existe une constante C, qui ne dépend que de $\alpha_1, \ldots, \alpha_{n-1}$, telle que l'on ait $\|\alpha\|_1 \leq e^{C H'}$. En choisissant s assez grand, conclure grâce à l'exercice 3.)

5. Minorations de formes linéaires en logarithmes de nombres algébriques (suite).

De l'exercice précédent déduire que si $\alpha_1, \ldots, \alpha_n$ sont des nombres algébriques et si ε est un nombre positif fixé alors la relation

$$0 < |b_1 \log \alpha_1 + \ldots + b_n \log \alpha_n| < e^{-\varepsilon H}$$

n'a qu'un nombre fini de solutions entières $b_1, \ldots, b_n$ de valeur absolue au plus H.

III. La méthode de Roth.

L'objet principal de ce chapitre est la démonstration du célèbre théorème de Roth.

THEOREME 1. - Soit α un nombre algébrique réel de degré $d \geq 3$. L'inégalité

$$(1) \qquad |\alpha - p/q| < q^{-\rho}$$

n'admet qu'un nombre fini de solutions si ρ est un nombre fini, $\rho > 2$.

Nous aurons pour cela besoin d'un certain nombre de lemmes.

1. Construction de la fonction auxiliaire.

1. Un lemme combinatoire.

LEMME 1. - Soient $r_1, \ldots, r_m$ des entiers positifs. Le nombre N de solutions entières $(i_1, \ldots, i_m)$ des inégalités

$$0 \leq i_h \leq r_h \quad (h = 1, \ldots, m) \quad \text{et} \quad \sum_{h=1}^{m} i_h/r_h \leq (0,5 - s)m ,$$

s réel positif, vérifie la majoration

$$N \le (r_1+1) \dots (r_m+1) \exp(-6m\, s^2/c) , \quad c := \sum_{h=1}^{m} (1+r_h^{-1})^2/m .$$

> Soit u une variable positive. Considérons les quantités

$$F_h(u) = \sum_{0\le i_h\le r_h} \exp(u(i_h/r_h - 1/2)) , \quad h = 1, \dots , m ,$$

$$F(u) = F_1(u) \dots F_m(u) = \sum_{0\le i_1\le r_1} \dots \sum_{0\le i_m\le r_m} \exp(u \sum_{1\le h\le m} (i_h/r_h - 1/2))$$

On a

$$F_h(u) = \mathrm{sh}((r_h+1)\, u/2r_h)/(u/2r_h) \le (r_h+1)\, \frac{\mathrm{sh}((r_h+1)\, u/2r_h)}{(r_h+1)\, u/2r_h}$$

et l'inégalité (voir exercice 1)

$$\mathrm{sht}/t \le \exp (t^2/6)$$

fournit la majoration

$$F_h(u) \le (r_h+1) \exp(((r_h+1)(u/2r_h))^2/6) .$$

Par conséquent,

$$F(u) \le (r_1+1) \dots (r_m+1) \exp (c\, m\, u^2/2\, 4) .$$

Nous allons maintenant minorer $F(u)$ en fonction de N. En effectuant la transformation $(i_1, \dots , i_m) \mapsto (r_1-i_1, \dots , r_m-i_m)$, nous constatons que N est aussi égal au nombre de solutions des inégalités

$$0 \le i_h \le r_h \quad (h = 1, \dots, m) \quad , \quad i_1/r_1 + \dots + i_m/r_m \ge (0,5+s)m \ .$$

D'où la minoration

$$F(u) \ge N \ \exp(s\,u\,m) \ .$$

Le résultat découle de l'encadrement de $F(12\ s/c)$.<

2. Le polynôme d'approximation.

LEMME 2.- Soit α un nombre algébrique de degré d. Soit $\lambda > 1$. Soient $r_1, \dots, r_m$ des entiers positifs et soit s un réel positif qui vérifient

$$m\,s^2 \ge c \log(\lambda d)/6 \quad , \quad c := \sum_{1 \le h \le m} (1+r_h^{-1})^2/m \ .$$

Alors il existe un polynôme non nul, à coefficients entiers,

$$A(X_1, \dots, X_m) = \sum_{0 \le i_1 \le r_1} \dots \sum_{0 \le i_m \le r_m} a_{i_1 \dots i_m} X_1^{i_1} \dots X_m^{i_m}$$

tel que

$$\|A\| \le 2(4^d \ \|\alpha\|_2)^{(r_1+\dots+r_m)/(d(\lambda-1))}$$

et

$$\frac{\partial^{j_1+\dots+j_m}}{\partial X_1^{j_1} \dots \partial X_m^{j_m}} A(\alpha, \dots, \alpha) = 0 \quad \text{si} \quad \sum_{1 \le h \le m} j_h/r_h \le (0,5-s)m \ .$$

> La démonstration est analogue à celle du lemme II. 1 . Le lemme 1 permet de majorer le nombre d'équations à résoudre. <

2. Le lemme de Roth.

Dans tout ce paragraphe nous suivrons d'assez près la présentation de [35, chap. V], auquel nous renvoyons le lecteur pour plus de détails.

1. Wronskiens généralisés.

Soient $f_1, \ldots, f_n$ des polynômes en m variables à coefficients dans un corps de caractéristique zéro. Un opérateur différentiel $\dfrac{\partial^{j_1+\ldots+j_m}}{j_1!\ldots j_m!\,\partial X_1^{j_1}\ldots\partial X_m^{j_m}}$ sera noté D et $j_1+\ldots+j_m$ sera appelé son ordre. On appelle wronskien généralisé un déterminant du type $\det (D_i f_j)_{1\le i,j\le n}$, où chaque D_i est d'ordre inférieur à i. Le lemme II. 2 admet la généralisation suivante.

LEMME 3. - Soient $f_1, \ldots, f_n$ des polynômes en m variables, à coefficients dans un corps K de caractéristique zéro, linéairement indépendants sur K. Alors l'un au moins des wronskiens de $f_1, \ldots, f_n$ n'est pas nul.

> Soit g un majorant strict du degré des f_j. Les fonctions $\Phi_j(X) = f_j(X, X^g, \ldots, X^{g^{n-1}})$ sont aussi linéairement indépendantes sur K. Le lemme II. 2 montre que le wronskien des Φ_j n'est pas nul. Ce wronskien s'exprime linéairement en fonction de wronskiens généralisés des f_j, ce qui montre que ces derniers ne sont pas tous nuls. <

2. Une identité.

De même que dans le cas de deux variables, on décompose un polynôme A en m variables, à coefficients entiers, sous la forme

$$A(X_1,\dots,X_m) = \sum_{1\le i\le m} P_i(X_1,\dots,X_{m-1})\, Q_i(X_m) ,$$

avec n minimal, les P_i et Q_i étant à coefficients rationnels. Les P_i d'une part, les Q_i d'autre part, sont alors linéairement indépendants sur $\mathbb{Q}$. Il existe alors un wronskien U^* (respectivement V^*) des P_i (resp. des Q_i) non nul, soit

$$U^* = \det (D'_i\, P_h) \quad , \quad V^* = \det (D''_j\, Q_k) \ .$$

Si $D_{ij} = D'_i\, D''_j$, on a la relation

$$W(X_1,\dots,X_m) := U^*(X_1,\dots,X_{m-1})\, V^*(X_m) = \det (D_{ij} A) \ ,$$

qui montre que W est à coefficients entiers. Le lemme de Gauss montre alors l'existence de polynômes à coefficients entiers U et V, proportionnels à U^* et V^*, tels que

$$W(X_1,\dots,X_m) = U(X_1,\dots,X_{m-1})\, V(X_m) \ .$$

Si $\deg_{X_i} A \le r_i$ pour $i = 1, \dots, m$, on démontre facilement la majoration

$$\|W\| \le 2^{2n(r_1+\dots+r_m)}\, n!\, \|A\|^n \ .$$

De plus,

$$\max(\|U\|, \|V\|) \le \|W\| \quad \text{et} \quad \deg_{X_i}(W) \le n\, r_i \ .$$

3. L'indice d'un polynôme.

L'indice d'un polynôme $A(X_1, \ldots, X_m)$ non nul, relativement à des réels positifs $\rho_1, \ldots, \rho_m$, en un point $\alpha_1, \ldots, \alpha_m$ est défini par

$$J(A;\rho_1,\ldots,\rho_m;\alpha_1,\ldots,\alpha_m) = \mathrm{Min}\Big(\frac{j_1}{\rho_1}+\ldots+\frac{j_m}{\rho_m}\ ;\ \frac{\partial^{j_1+\ldots+j_m}}{\partial X_1^{j_1}\ldots\partial X_m^{j_m}} A(\alpha_1,\ldots,\alpha_m)\neq 0\Big).$$

Si A est nul, on convient que $J(A) = \infty$. L'indice possède les propriétés suivantes

(i) $\quad J(A+B) \ge \min(J(A), J(B))$,

(ii) $\quad J(A\,B) = J(A) + J(B)$,

(iii) $\quad J\Big(\dfrac{\partial^{\ell_1+\ldots+\ell_m}}{\partial X_1^{\ell_1}\ldots\partial X_m^{\ell_m}} A\Big) \ge \max\Big(0,\ J(A) - \sum_{1\le h\le m} \ell_h/\rho_h\Big)$.

On s'intéresse à la quantité

$$\Theta_m = \Theta_m(a\ ;\ r_1, \ldots, r_m\ ;\ H_1, \ldots, H_m) = \max J(A;r_1,\ldots,r_m;\beta_1,\ldots,\beta_m)$$

où le maximum est étendu à l'ensemble (fini) des polynômes non nuls $A \in \mathbb{Z}[X_1, \ldots, X_m]$, vérifiant $\|A\| \le a$ et $\deg_{X_i} A \le r_i$, et des rationnels $\beta_1, \ldots, \beta_m$ tels que $\|\beta_i\|_\infty = H_i$.

Le lemme de Gauss implique la majoration

$$\Theta_1(a\ ;\ r\ ;\ H) \le [\log a/\log H]/r \ .$$

4. Une majoration de Θ_m en fonction de Θ_{m-1}.

Pour t fixé, $0 < t < 1/2$ et c fixé, $0 < c \leq 1$, on dira que des entiers positifs $b, s_1, \ldots, s_m, K_1, \ldots, K_m$ possèdent la propriété Γ_m si, soit

1) $m = 1$, $K_1^{tc} \geq 16$, $b \leq K_1^{c s_1 t}$,

soit

2) $m \geq 2$, $\max(s_2/s_1, \ldots, s_m/s_{m-1}) \leq t$, $s_h \log K_h \geq c\, s_1 \log K_1$ $(h = 2, \ldots, m)$, $\min(K_i^{tc}) \geq 2^{4m^2}$, $b \leq K_1^{c s_1 t/m}$.

Supposons que $a, r_1, \ldots, r_m, H_1, \ldots, H_m$ possèdent la propriété Γ_m. Montrons que $b = 2^{2n(r_1+\ldots+r_m)}\, n!\, a^m$, $\rho_1 = n r_1, \ldots, \rho_{m-1} = n r_{m-1}$, $H_1, \ldots, H_{m-1}$ vérifient Γ_{m-1} si on a $n \leq r_m + 1$. La seule condition non évidente porte sur la majoration de b. Notons d'abord que l'on a

$$2^{2n(r_1+\ldots+r_m)}\, n! \leq 2^{2n(r_1+\ldots+r_m)}\, 2^{n r_m} \leq 2^{2n r_1(1+2^{-1}+\ldots+2^{-m}+2^{-m})} = 2^{4n r_1}.$$

Il s'agit de vérifier que l'on a $h \leq K_1^{n r_1 t\, c/(m-1)}$. Pour cela il suffit que l'on ait

$$2^{4r_1} a \leq K_1^{c\, t\, r_1/(m-1)} \quad \text{et} \quad 16 \leq K_1^{c\, t((m-1)^{-1}-m^{-1})}.$$

Ces inégalités résultent de la minoration $K_1^{tc} \geq 2^{4m^2}$. La construction du paragraphe 2 permet maintenant de passer de m à $m-1$ variables.

Soient A, $\beta_1, \ldots, \beta_m$ tels que $\|A\| \le a$, $\deg_{X_i} A \le r_i$, $\|\beta_i\|_\infty = H_i$ et
$J(A) := J(A; r_1, \ldots, r_m; \beta_1, \ldots, \beta_m) = \Theta_m(a; r_1, \ldots, r_m; H_1, \ldots, H_m)$

(une telle égalité a lieu puisque Θ_m est égal au maximum d'un ensemble fini). Si U, V et W désignent les polynômes construits plus haut à partir de A, on a $\|U\| \, \|V\| \le b$ et $\deg_{X_i} W \le \rho_i$ et

$$J(W; \rho_1, \ldots, \rho_m; \beta_1, \ldots, \beta_m) = J(U; \rho_1, \ldots, \rho_{m-1}; \beta_1, \ldots, \beta_{m-1}) + J(V; \rho_m; \beta_m)$$
(d'après (ii))
$$\le \Theta_{m-1}(b; \rho_1, \ldots, \rho_{m-1}; H_1, \ldots, H_{m-1}) + \Theta_1(b; \rho_m; H_m) ,$$

où $b, \rho_1, \ldots, \rho_{m-1}$, $H_1, \ldots, H_{m-1}$ possèdent la propriété Γ_{m-1},

$$\Theta_1(b; \rho_m; H_m) \le [\log b / \log H_m] / \rho_m \le \log b / (c \, \rho_1 \log H_1) \le t ,$$

et

$$J(W) := J(W; r_1, \ldots, r_m; \beta_1, \ldots, \beta_m) = n \, J(W; \rho_1, \ldots, \rho_m; \beta_1, \ldots, \beta_m) .$$

En développant le déterminant W, on obtient

$$J(W) \ge \min_{i_1, \ldots, i_n \text{ distincts}} J(D_{i_1, 1} A \ldots D_{i_n, n} A) \quad \text{(d'après (i))}$$

$$\ge \min_{i_1, \ldots, i_n \text{ distincts}} \Big(\sum_{1 \le j \le n} D_{i_j, j} A \Big) \quad \text{(d'après (ii))}$$

$$\ge \sum_{1 \le j \le n} \max\Big(0, \; J(A) - \frac{n-1}{r_{m-1}} - \frac{j-1}{r_m}\Big) \quad \text{(grâce à (iii))}$$

$$\geq \sum_{1\leq j\leq n} \max(0,\ J(A) - t - (j-1)/r_m) \qquad \text{(puisque } n-1 \leq r_m \leq t\, r_{m-1}\text{)}$$

$$= \sum_{j=1}^{\min(n,N)} (J(A) - t - (j-1)/r_m) \quad , \quad \text{où } N = \lceil (J(A)-t)r_m \rceil + 1 \ .$$

Distinguons deux cas. Si $N \geq n$ on obtient les inégalités

$$J(A) \leq t + J(W)/n + 1/2$$

et

$$J(A) \leq t + 2J(W)/n \ .$$

Tandis que $N < n$ implique

$$J(A) \leq t + 2\sqrt{J(W)/n} \ .$$

D'où les majorations

- dans le premier cas

$$\Theta_m(a;r_1,\ldots,r_m;H_1,\ldots,H_m) \leq 2t+\Theta_{m-1}(b;\rho_1,\ldots,\rho_{m-1};H_1,\ldots,H_{m-1})+1/2$$

et

$$\Theta_m(a;r_1,\ldots,r_m;H_1,\ldots,H_m) \leq 3t+2\ \Theta_{m-1}(b;\rho_1,\ldots,\rho_{m-1};H_1,\ldots,H_{m-1})$$

- dans le second cas

$$\Theta_m(a;r_1,\ldots,r_m;H_1,\ldots,H_m) \leq t+2(\Theta_{m-1}(b;\rho_1,\ldots,\rho_{m-1};H_1,\ldots,H_{m-1})+t)^{1/2} \ .$$

5. Le lemme de Roth.

Nous sommes maintenant en mesure de démontrer le résultat suivant :

LEMME 4. - Si les nombres $a; r_1, \ldots, r_m; H_1, \ldots, H_m$ vérifient la propriété Γ_m alors, pour $t \leq \min((3+2\sqrt{2})^{-2^{m-2}}, 1/4)$, on a

$$\Theta_m(a; r_1, \ldots, r_m; H_1, \ldots, H_m) + t \leq (3 + 2\sqrt{2})t^{2^{-m+1}} .$$

> Récurrence sur m. Le cas $m = 1$ a déjà été vu. Supposons $m \geq 2$. D'après l'hypothèse de récurrence et le paragraphe qui précède, on a

$$\Theta_m + t \leq 2t + 2 \max((3 + 2\sqrt{2})t^{2^{-m+2}}, (3 + 2\sqrt{2})^{1/2} t^{2^{-m+1}})$$
$$\leq (1 + 2(3 + 2\sqrt{2})^{1/2})t^{2^{-m+1}} = (3 + 2\sqrt{2})t^{2^{-m+1}} .<$$

Le lemme 4 conduit à la variante suivante du lemme de Roth.

LEMME 5. - Soit $\epsilon \geq 2/m$ fixé. Soient t et c positifs, $t \leq \text{Min}(6^{-2^{(1-\epsilon)m}}, 1/4)$, $c \leq 1$. Soient $a, r_1, \ldots, r_m, H_1, \ldots, H_m$ des entiers positifs, $m \geq 2$, tels que

$$r_{h+1} \leq t\, r_h \quad (h = 1, \ldots, m-1), \quad r_h \log H_h \geq c\, r_1 \log H_1 \quad (h = 2, \ldots, m)$$

$$H_h \geq 2^{4m^2/tc}, \quad a \leq H_1^{c\, t\, r_1/m} .$$

Soient $\beta_1, \ldots, \beta_m$ des rationnels vérifiant $\|\beta_h\|_\infty = H_h$ pour $h = 1, \ldots, m$. Soit un polynôme non nul $A \in \mathbb{Z}[X_1, \ldots, X_m]$ tel que

$$\|A\| \le a \ , \ \deg_{X_h} A \le r_h \ \underline{\text{pour}} \ \ h = 1, \ldots , m \ .$$

Alors il existe $\ell_1, \ldots, \ell_m$ vérifiant

$$\sum_{1 \le h \le m} \ell_h / r_h \le 2\epsilon \ m$$

telsque

$$\gamma := \frac{\partial^{\ell_1 + \ldots + \ell_m}}{\ell_1! \ldots \ell_m! \ \partial X_1^{\ell_1} \ldots \partial X_m^{\ell_m}} \ A(\beta_1, \ldots, \beta_m)$$

soit non nul.

> Soit Φ_k la borne supérieure de $\Theta_k(b; \rho_1, \ldots, \rho_k; K_1, \ldots, K_k)$ pour des entiers $b, \rho_1, \ldots, \rho_k, K_1, \ldots, K_k$ vérifiant la propriété Γ_k , alors

$$J(A; r_1, \ldots, r_m; \beta_1, \ldots, \beta_m) \le \Phi_m \ .$$

Il suffit donc de vérifier la majoration $\Phi_m \le 2\epsilon \ m$. Soit la suite Ψ_k définie par

$$\Psi_1 = t \ , \ \Psi_{k+1} = \begin{cases} t + 2(t + \Psi_k)^{1/2} & \text{si } \Psi_k \le 1-t \\ 2t + \Psi_k + 1/2 & \text{sinon} \ . \end{cases}$$

Notons que la suite Ψ_k est croissante. Démontrons, par récurrence, que Ψ_k majore Φ_k . C'est vrai pour $k = 1$. Supposons ce résultat démontré jusqu'à l'indice k . Examinons Φ_{k+1} . Si $\Phi_{k+1} \le 1-t$ on a soit $\Psi_k > 1-t$ et alors $\Psi_{k+1} > \Psi_k > \Phi_{k+1}$, soit $\Psi_k \le 1-t$ et alors

$$\Phi_{k+1} \le t + 2 \max (\Phi_k + t,\ (\Phi_k + t)^{1/2}) \le t + 2 \max (\Psi_k + t,\ (\Psi_k + t)^{1/2}) = \Psi_{k+1} .$$

Si $\Phi_{k+1} > 1 - t$ considérons un polynôme B tel que $J(B) = \Theta_{k+1} > 1-t$, dans l'étude du paragraphe 4 c'est la première majoration qui s'applique et on a

$$\Theta_{k+1} \le \operatorname{Min} \left(2(t + \Psi_k) + t\ ,\ 2t + \Psi_k + \frac{1}{2}\right)$$

$$\le \begin{cases} 2(t+\Psi_k)^{1/2} + t = \Psi_{k+1} & \text{si} \quad \Psi_k \le 1-t \\ 2t + \Psi_k + \frac{1}{2} = \Psi_{k+1} & \text{si} \quad \Psi_k > 1-t \ , \end{cases}$$

donc encore $\Phi_{k+1} \le \Psi_{k+1}$.

Il ne reste plus qu'à étudier la croissance de la suite Ψ_k . Soit j le plus grand indice tel que l'on ait $\Psi_j \le 1-t$. Si $j \ge m-1$ alors $\Psi_m \le 2(t+\Psi_{m-1})^{1/2} + t \le 2+t \le 2\epsilon\, m$. Supposons donc $j < m$, alors

$$\Psi_m \le t + 2 + (m-j-1)\,(2t+1/2) .$$

La démonstration du lemme 4 montre que

$$t \le 6^{-2^k} \Rightarrow \Psi_{k+1} \le 6\, t^{2^{-k+1}} \le 1-t .$$

On a donc $j \ge (1-\epsilon)m$ et encore

$$\Psi_m \le (2t+1/2)\,\epsilon\, m + 3/2 \le 2\epsilon\, m \ .<$$

3. Démonstration du théorème de Roth.

1. Choix des paramètres.

Pour des raisons de commodité, on considère au lieu de (1) l'équation

$$(1)' \qquad |\alpha - p/q| < \max(|p|, |q|)^{-\rho}$$

Il est équivalent de supposer qu'il existe $\rho > 2$ tel que (1) admette une infinité de solutions ou qu'il existe $\rho > 2$ tel que (1)' admette une infinité de solutions. Soit $\rho > 2$ tel que (1)' admette une infinité de solutions, $\rho < d$. Posons $\rho = 2 + \xi$ et

$$m = [0,\ 7\ (\log(d+1))\ \rho^2\ \xi^{-2}] + 1\ ,\quad t = \exp(-2^{m+2})\ ,\quad c = 1\ ,$$
$$\lambda = (d+1)/d,\ s = \xi/(\sqrt{4,2\ \rho})\ ,\quad \text{donc}\ 6\ m\ s^2 = (1+\eta)\log(d+1), \eta > 0\ .$$

Soient $\beta_h = p_h/q_h$ des solutions irréductibles de (1)' telles que, si $\|\beta_h\| = H_h$, on ait

$$H_1 \geq \max((5^d\ \|\alpha\|_2)^{25}\ ,\ 2^{4m^2/t})$$

et

$$\log H_{h+1} \geq 2\ t^{-1} \log H_h\ ,\quad h = 1, \ldots, m-1\ .$$

On choisit ensuite r_1 très grand et r_h $(h = 2, \ldots, m)$ vérifiant

$$r_h \geq r_1 \log H_1 / \log H_h > r_h - 1\ ,\quad \text{donc}\ r_h < t\ r_{h-1}\ .$$

On peut supposer r_1 très grand, d'où en particulier $c \leq 1+\eta$ (notation des lemmes 1 et 2). On considère alors le polynôme A construit grâce au lemme 2. Le lemme 4 s'applique et montre que l'on a

$$J(A;r_1,\dots,r_m;\beta_1,\dots,\beta_m) \le e^{-6} ,$$

d'où l'existence d'un nombre γ non nul de la forme

$$\gamma = \frac{\partial^{\ell_1+\dots+\ell_m}}{\ell_1!\dots\ell_m!\,\partial X_1^{\ell_1}\dots\partial X_m^{\ell_m}} A(\beta_1,\dots,\beta_m)$$

avec

$$\Lambda := \ell_1/r_1 + \dots + \ell_m/r_m \le e^{-6} .$$

2. Encadrement de γ.

Le nombre γ est rationnel et admet $q_1^{r_1}\dots q_m^{r_m}$ comme dénominateur, il vérifie donc

$$|\gamma| \ge |q_1^{r_1}\dots q_m^{r_m}|^{-1} \ge H_1^{-m\,r_1/(1-1/r_m)} .$$

Majorons $|\gamma|$. De la formule de Taylor au point $(\alpha,\dots,\alpha)$ résulte la relation

$$\gamma = \sum_{0\le j_1\le r_1} \dots \sum_{0\le j_m\le r_m} \frac{\partial^{j_1+\dots+j_m}}{j_1!\dots j_m!\,\partial X_1^{j_1}\dots\partial X_m^{j_m}} A(\alpha,\dots,\alpha)\binom{j_1}{\ell_m}\dots \binom{j_m}{\ell_m}(\beta_1-\alpha)^{j_1-\ell_1}\dots(\beta_m-\alpha)^{j_m-\ell_m} .$$

On en déduit

$$|\gamma| \le 4^{r_1+\dots+r_m}\,\|A\| \max_{(j_1,\dots,j_m)\in J} |\beta_1-\alpha|^{j_1-\ell_1}\dots|\beta_m-\alpha|^{j_m-\ell_m}$$

où J désigne l'ensemble des indices tels que

$$\frac{\partial^{j_1+\ldots+j_m}}{\partial X_1^{j_1}\ldots\partial X_m^{j_m}} A(\alpha,\ldots,\alpha) \neq 0 \ .$$

D'après les propriétés de A et des β_h il en résulte

$$|\gamma| \leq (5^d\|\alpha\|_2)^{2r_1} \max_{j_1/r_1+\ldots+j_m/r_m > (1/2-s)m} H_1^{-\rho\, r_1(\Sigma\, j_h/r_h - \Lambda)}$$

$$\leq H_1^{-r_1(\rho((1/2-s)m-e^{-6}) - 0,04)}$$

3. Conclusion.

Du fait que r_m peut être choisi arbitrairement grand, de l'encadrement de $|\gamma|$ résulte l'inégalité

$$m \geq m\rho(1/2-s) - e^{-6}\ \rho - 0,04 \ ,$$

soit

$$0,7(\log(d+1))\rho^2\xi^{-1}\ (0,5 - \sqrt{1/4,2}) - e^{-6}\rho - 0,04 \leq 0 \ .$$

On vérifie que cette inégalité est impossible pour $2 < \rho < d$. Cette contradiction achève la démonstration.

4. Majoration du nombre d'approximations.

La démonstration du théorème de Roth ne permet pas de déterminer effectivement toutes les solutions de l'inégalité (1). Cependant, Davenport et Roth [16] ont déterminé une borne $N = N(\alpha, \rho)$ du nombre de solutions de (1) pour $\rho > 2$. On peut en fait démontrer un résultat plus fort qui généralise les résultats du paragraphe II. 5.

THEOREME 2.- Soit α un nombre algébrique réel de degré d. Soit ρ un réel fixé, $2 < \rho < d$. Alors le nombre N de solutions rationnelles irréductibles de l'inégalité

$$|\alpha - p/q| < M q^{-\rho} , \tag{2}$$

qui vérifient

$$\max(|p|, q) \geq Q , \quad Q := \max ((5^d \|\alpha\|_2)^{25} , 2^{4m^2/t}, (\alpha(2\alpha^*)^\rho M)^{100/\xi})$$

où

$$\xi = \rho - 2 , \quad m = [0,715(\log(d+1))\ \rho^2\ \xi^{-2}] + 1 \quad \text{et} \quad t = \exp(-2^{m+2})$$

vérifie la majoration

$$N < m(1+5.2^m/\log(1+99\xi/100)) .$$

En particulier, pour $\xi < 0,005$ on a $N \leq (d+1)^{2\xi^{-2}}$.

On notera surtout que ce théorème donne, au delà d'une limite effectivement calculable $Q = Q(\alpha, M, \rho)$, une majoration de N qui ne dépend que de ξ et du degré de α.

> Pour toute solution p/q de (2), de hauteur H, vérifiant $q \geq Q$, on a $|\alpha - p/q| < 1$, donc $q > |p|(2\alpha^*)^{-1}$, et

$$|\alpha - p/q| < M q^{-\rho} \leq (M(2^\alpha)^\rho)\ H^{-\rho} \leq 0,5.H^{-(\rho-\xi/100)} .$$

On est donc ramené à l'équation (1') avec un exposant $2+99\xi/100$. Comme dans la démonstration du théorème de Roth, on aboutit à une contradiction si on considère des solutions de (2) $x_1,\dots,x_m$ de hauteur $H_1,\dots,H_m$ vérifiant

$$H_1 \geq Q \quad \text{et} \quad \log H_{k+1} \geq (2/t) \log H_k \quad \text{pour} \quad k = 1,\dots,m-1 \ .$$

Soit $y_1,\dots,y_N$ la suite des rationnels, de hauteurs h_i croissantes $\geq Q$, qui vérifient (2). Les inégalités

$$(h_i\, h_{i+1})^{-1} \leq |y_i - y_{i+1}| \leq |\alpha - y_i| + |\alpha - y_{i+1}| < h_i^{-(2+99\xi/100)}$$

conduisent à la minoration

$$\log h_{i+1} > (1+99\xi/100) \log h_i \ .$$

Si $k = [\log(2/t)/\log(1+99\xi/100)] + 1$, on peut donc choisir $x_1 = y_1$, $x_2 = y_{1+k}$, $x_3 = y_{1+2k}$, ... D'après ce qui précède le nombre de choix des x_i est inférieur à m. D'où la majoration $N < m\,k$, ce qui démontre le théorème. <

Considérons maintenant le développement en fraction continue d'un nombre algébrique réel irrationnel α. Soient p_1/q_1, p_2/q_2, ... les réduites successives. Rappelons que l'on a

$$(3) \qquad |\alpha - p_n/q_n| < 1/(q_n\, q_{n+1}) \quad , \quad \text{pour} \quad n = 1,\ 2,\ \dots$$

Davenport et Roth [16] ont démontré la majoration

$$\log \log q_n < c(\alpha) n (\log n)^{-1/2} .$$

On peut démontrer le résultat plus fort suivant.

THEOREME 3. - Soient $p_1/q_1, \ldots, p_n/q_n, \ldots$ les réduites successives du développement en fraction continue d'un nombre algébrique réel α de degré $d \geq 3$. Alors il existe $n(\alpha)$ calculable tel que

$$\log \log q_n \leq n (2(\log(d+1))/\log n)^{1/2} \quad \text{si} \quad n \geq n(\alpha) .$$

> Si $q_{n+1} > q_n^{1+\xi}$, l'inégalité (3) montre que (1) a lieu avec $\rho = 2+\xi$. Le théorème 2 fournit une majoration du nombre $N(\xi)$ de solutions de (1) vérifiant $q_n > Q(\xi)$. De plus le théorème de Liouville fournit l'inégalité $q_{n+1} < q_n^{c_1}$ (c_1 calculable) pour $n \geq 1$. Il en résulte la majoration

$$\log q_n \leq \log Q(\xi) + (1+\xi)^n c_1^{N(\xi)} \log q_1 .$$

D'où la conclusion en choisissant $\xi = (1,99 \log (d+1)/\log n)^{1/2}$ et en utilisant les expressions de $Q(\xi)$ et $N(\xi)$. <

COROLLAIRE. - Pour tout d, il existe une constante $c(d)$ telle que, pour tout α algébrique de degré d, on ait

$$\limsup ((\log \log q_n)(\log n)^{1/2}/n) \leq c(d) ,$$

où q_n désigne le dénominateur de la n-ième réduite du développement de

α . De plus, $c(d) \leq (2 \log (d+1))^{1/2}$.

Les résultat de Davenport et Roth permirent à Baker [1] de construire des nombres transcendants, tandis que le théorème 3 permet de construire des nombres d'un type semblable dont on sait qu'ils ne sont pas algébriques de degré $\leq d$, voir [43] .

5. Application aux équations diophantiennes.

1. Soit F une forme binaire de degré d , à coefficients entiers, sans facteur multiple non constant. Soient x et y des entiers tels que $F(x, y)$ soit non nul. Nous nous proposons de minorer $F(x, y)$. Sans perte de généralité, on peut supposer $|y| \geq |x|$. Supposons aussi $F(X, 0)$ non nul. Posons alors $f(X) = F(X, 1)$. Soient $\alpha_1, \ldots, \alpha_d$ les zéros du polynôme f , numérotés de telle sorte que l'on ait $|x/y-\alpha_1| \leq \ldots \leq |x/y-\alpha_d|$, et donc $|x/y-\alpha_i| \geq |\alpha_1-\alpha_i|/2$ pour $i \geq 2$. On a

$$\begin{aligned} |F(x,y)| &= |b|\ |y|^d |x/y-\alpha_1| \ldots |x/y-\alpha_d| \\ &\geq |b|\ |y|^d |x/y-\alpha_1|\ |\alpha_1-\alpha_2| \ldots |\alpha_1-\alpha_d|\ 2^{-d+1} \\ &= |y|^d |x/y-\alpha_1|\ |f'(\alpha_1)|\ 2^{-d+1} \ , \end{aligned}$$

où b désigne le coefficient dominant de f . Reste à minorer $|f'(\alpha_1)|$. Pour cela considérons le discriminant de f , il vérifie

$$\begin{aligned} 1 \leq |\mathrm{Discr}(f)|^{1/2} &= |b|^{d-2}\ |f'(\alpha_1)| \prod_{2 \leq i < j \leq d} |\alpha_i-\alpha_j| \\ &\leq |f'(\alpha_1)|\ 2^{(d-2)(d-1)/2}\ |b\, \alpha_2^* \ldots \alpha_d^*|^{d-2} \quad \text{(utiliser } |\alpha_i-\alpha_j| \leq 2\alpha_i^* \alpha_j^*\text{)} \\ &\leq |f'(\alpha_1)|\ (2^{(d-1)/2} \|f\|_2)^{d-2} \quad \text{(grâce au théorème I. 1)} \ . \end{aligned}$$

On a donc

$$|F(x, y)| \geq |y|^{d}\, 2^{-d(d-1)/2} \|F\|_2^{-d+2} \operatorname*{Min}_i |x/y-\alpha_i| \ .$$

La démonstration de ce résultat prouve qu'il reste encore vrai si Y divise $F(X, Y)$. Nous obtenons ainsi la proposition suivante.

PROPOSITION 1. - Soit F une forme binaire de degré d, à coefficients entiers, sans facteur multiple non constant, de la forme

$$F(X, Y) = b\,(\beta_1 X-\alpha_1 Y)\ldots(\beta_d X-\alpha_d Y) \quad , \quad \beta_i = 0 \text{ ou } 1 \ .$$

Alors pour tout couple (x, y) d'entiers on a la minoration

$$|F(x, y)| \geq \max(|x|, |y|)^{d-1}\, 2^{-d(d-1)/2}\, \|F\|_2^{-d+2} \operatorname*{Min}_i |\beta_i x-\alpha_i y| \ .$$

2. Examinons quelques conséquences de la proposition et des théorèmes d'approximation que nous avons démontrés.
D'après le théorème de Roth, pour tout $\varepsilon > 0$, on a, pour x/y différent des α_i,

$$\operatorname*{Min}_i |x/y-\alpha_i| \geq c'\, |y|^{-2-\varepsilon} \ .$$

On obtient donc le corollaire suivant.

COROLLAIRE 1. - Soit F une forme binaire homogène de degré d à

coefficients entiers, sans facteur multiple non constant. Alors, pour tout ε positif il existe une constante $C = C(\varepsilon, F)$ (non effective) telle que

$$|F(x, y)| \geq C\,(|x| + |y|)^{d-2-\varepsilon}$$

pour tout couple d'entiers (x, y) n'annulant pas F.

Ce corollaire a pour conséquence le résultat suivant.

COROLLAIRE 2. - Soit F une forme binaire vérifiant les hypothèses du corollaire 1 et soit G un polynôme de degré total inférieur à $d-2$. Alors l'équation

$$F(x, y) = G(x, y)$$

n'a qu'un nombre fini de solutions entières qui n'annulent pas F.

En particulier.

COROLLAIRE 3. - Soit F une forme binaire de degré $d \geq 3$ à coefficients entiers, sans facteur multiple non constant. Pour tout entier $m \neq 0$ donné, l'équation de Thue

(4) $$F(x, y) = m$$

n'a qu'un nombre fini de solutions entières.

3. Voyons le cas où F est réductible et à coefficients entiers. Alors les α_i sont de degré inférieur à d et, d'après le théorème de Liouville, il existe une constante positive calculable c_1 telle que

$$|x/y-\alpha_i| \geq c_1 (|x|+|y|)^{-d+1} \quad \text{si} \quad x/y \neq \alpha_i \ .$$

D'où l'existence d'une constante positive effective c_2 telle que, si $x\,y\,F(x, y) \neq 0$, on ait l'inégalité

$$|F(x, y)| \geq c_2(|x|+|y|) \ ,$$

qui d'ailleurs reste valable sous l'hypothèse plus faible $F(x, y) \neq 0$. Dans ce cas, l'équation (4) n'a qu'un nombre fini de solutions, que l'on peut déterminer effectivement.

4. Supposons maintenant F à coefficients entiers et irréductible. Si on dispose d'un raffinement effectif du théorème de Liouville

$$|\alpha-p/q| > \varphi(H)\, H^{-d} \ , \quad \text{où} \quad H = \|p/q\|_\infty \ ,$$

φ étant une fonction calculable qui tend vers l'infini avec H, alors

$$|F(x, y)| \geq \varphi_1(\max(|x|, |y|)) \quad \text{pour} \quad x, y \quad \text{entiers},$$

où φ_1 est une fonction calculable qui tend vers l'infini avec la variable. Par conséquent, la relation

$$|F(x, y)| = m$$

implique $m \geq \varphi_1(\max(|x|, |y|))$, ce qui montre qu'on peut alors déterminer effectivement toutes les solutions de l'équation de Thue.

5. Dans le cas général de l'équation $F(x, y) = G(x, y)$ considérée au corollaire 1 , le mieux que nous puissions faire est le résultat suivant.

THEOREME 4.- Soit $F(X, Y)$ une forme binaire irréductible de degré $d \geq 3$, à coefficients entiers, et soit $G(X, Y)$ un polynôme de degré total au plus $d-3$. Alors le nombre N_1 de solutions entières de l'équation

$$F(x, y) = G(x, y)$$

qui vérifient $\max(|x|, |y|) \geq Q$, où Q est effectivement calculable, satisfait à l'inégalité

$$N \leq 2^7 (\log (d+1)) (d+1)^{6,47} .$$

Il est à noter que la borne N ne dépend que de d . De plus, les résultats du paragraphe II. 5 permettent de remplacer cette majoration par $N_1 \leq d^2$ lorsque d et d' vérifient $d' < d-\rho_d$, et Q est convenablement choisi.

> Supposons d'abord qu'il existe des solutions avec y nul, x est alors racine d'un polynôme à coefficients entiers non trivial et de hauteur majorée par $\max(\|F\|, \|G\|)$, ce qui implique $|x| \leq \max(\|F\|, \|G\|) + 1$. On peut donc se limiter à l'étude des

solutions x', y' pour lesquelles y' n'est pas nul. Pour une telle solution soit t l'entier défini par les conditions $x' = t\,x$, $y' = t\,y$ où x et y sont des entiers premiers entre eux et y est positif. Alors t est solution d'un polynôme non nul de degré d et prend donc au plus d valeurs, de plus pour tout x et y on peut borner t par $(\|F\|_1+\|G\|_1)\ \max(|x|, |y|)^d$. Par conséquent, pour Q assez grand N_1 est majoré par d fois le nombre de solutions de l'inégalité

$$|F(x, y)| \leq \|G\|_1 \max(|x|, |y|)^{d'}, \quad \text{avec } (x, y) = 1 ,$$

vérifiant $\max(|x|, |y|) > Q^{1/(d+2)}$. D'après la proposition 1, pour une solution de l'inégalité précédente il existe un indice i tel que l'on ait

$$|x/y-\alpha_i| \leq M \max(|x|, |y|)^{d'-d} .$$

Avec les notations du théorème 2, on a donc

$$N_1 \leq d^2 N .$$

On conclut en appliquant ce théorème. <

EXERCICES.

1. En étudiant les dérivées successives de la fonction $\mathrm{Log}(\mathrm{sht}/t)$ démontrer l'inégalité

$$\mathrm{sht}/t \leq \exp(t^2/6) .$$

2. Soient $P_1, \ldots, P_n$ des formes binaires de degrés respectifs $p_1, \ldots, p_n$,

à coefficients entiers tels que les racines de chaque polynôme $P(x, 1)$ soient des irrationnels distincts. Soit $P(X_1, Y_1, \ldots, X_n, Y_n)$ un polynôme tel que pour $k = 1, \ldots, n$ on ait $p_k \geq \deg_{X_k} P + \deg_{Y_k} P + 3$. Alors l'équation

$$P(x_1, y_1) \ldots (P(x_n, y_n) = P(x_1, y_1, \ldots, x_n, y_n)$$

n'a qu'un nombre fini de solutions entières non triviales (i.e. vérifiant $(x_1^2+y_1^2)\ldots(x_n^2+y_n^2) \neq 0$).

[Comparer ce résultat au théorème VII, chap. I, de l'ouvrage de Gel'fond [22]].

IV. Les théorèmes de W. Schmidt.

1. Introduction.

1. Dans ce chapitre les problèmes suivants seront en particulier abordés : approximation des nombres algébriques par des nombres algébriques de degré borné, approximation simultanée des nombres algébriques par des nombres rationnels. Considérons d'abord l'approximation simultanée des nombres réels par des rationnels. Les premiers résultats dans ce domaine sont encore dus à Dirichlet.

THEOREME 1. - *Soient* $\alpha_1, \ldots, \alpha_n$ *des nombres réels et soit* Q *un entier supérieur à* 1 . *Alors il existe un entier* q *vérifiant* *

$$1 \leq q < Q^n \quad \text{et} \quad \|q\,\alpha_i\| \leq 1/Q \quad \text{pour} \quad i = 1, \ldots, n .$$

La démonstration est une généralisation immédiate de celle donnée au chapitre I pour le cas $n = 1$.

COROLLAIRE. - *Soient* $\alpha_1, \ldots, \alpha_n$ *des nombres réels non tous rationnels. Alors il existe une infinité de n-uples* $(p_1/q, \ldots, p_n/q)$ *avec* $q > 0$, *tels que* $q, p_1, \ldots, p_n$ *soient premiers entre eux, qui vérifient*

$$|\alpha_i - p_i/q| < q^{-1-1/n} , \quad i = 1, \ldots, n .$$

* Dans tout ce chapitre $\| \ \|$ désigne la distance à l'entier le plus proche.

THEOREME 2. - Soient $\alpha_1,\ldots,\alpha_n$ des nombres réels et soit Q un entier supérieur à 1. Alors il existe n entiers non tous nuls $q_1,\ldots,q_n$ vérifiant

$$|q_i| < Q^{1/n} \text{ pour } i = 1,\ldots,n \text{ et } \|\alpha_1 q_1+\ldots+\alpha_n q_n\| < 1/Q .$$

COROLLAIRE. - Soient $1, \alpha_1,\ldots,\alpha_n$ des nombres réels, linéairement indépendants sur $\mathbb{Q}$. Alors il existe une infinité de n-uples d'entiers premiers entre eux $q_1,\ldots,q_n$, non tous nuls vérifiant

$$\|\alpha_1 q_1 + \ldots + \alpha_n q_n\| < q^{-n} , \text{ où } q = \max(|q_1|,\ldots,|q_n|) .$$

2. Notre but est de démontrer les théorèmes suivants, tous dûs à W. Schmidt.

THEOREME 3. - Soient $1, \alpha_1,\ldots, \alpha_n$ des nombres algébriques linéairement indépendants sur $\mathbb{Q}$ et soit ϵ positif. Il existe seulement un nombre fini d'entiers q tels que l'on ait

$$\|q\,\alpha_1\| \ldots \|q\,\alpha_n\| < q^{-1-\epsilon} .$$

Le résultat suivant est une conséquence immédiate de ce théorème.

COROLLAIRE. - Soient $\alpha_1,\ldots,\alpha_n$, ϵ comme au théorème 1. Il existe seulement un nombre fini d'entiers q tels que

$$\|q\,\alpha_i\| \le q^{-(1/n)-\epsilon} \text{ pour } i = 1,\ldots,n .$$

Par dualité, on peut déduire du théorème 3 le théorème ci-dessous.

THEOREME 4. - Soient $1, \alpha_1, \ldots, \alpha_n$ des nombres algébriques linéairement indépendants sur les rationnels. Alors, pour tout ϵ positif, il n'existe qu'un nombre fini $q_1, \ldots, q_n$ de n-uples d'entiers non nuls tels que

$$\|q_1\alpha_1 + \ldots + q_n\alpha_n\| < |q_1 \ldots q_n|^{-1-\epsilon} .$$

D'où :

COROLLAIRE. - Soient $\alpha_1, \ldots, \alpha_n, \epsilon$ comme au théorème 4. Il y a seulement un nombre fini de n-uples d'entiers non nuls $q_1, \ldots, q_n$ vérifiant

$$\|q_1\alpha_1 + \ldots + q_n\alpha_n\| < q^{-n-\epsilon} , \quad \text{où} \quad q = \max(|q_1|, \ldots, |q_n|) .$$

3. Du théorème 4 résulte un théorème sur l'approximation des nombres algébriques par des nombres algébriques de degré borné.

THEOREME 5. - Soit α un nombre algébrique de degré supérieur à n et soit ϵ positif. Il existe au plus un nombre fini de nombres algébriques β, de degré au plus n, et vérifiant

$$|\alpha-\beta| < \|\beta\|_\infty^{-n-1-\epsilon} .$$

> Soit P le polynôme minimal de β. On a alors

$$|P(\alpha)| < n(|\alpha|+1)^n \|\beta\|_\infty |\beta-\alpha| \quad \text{si} \quad |\beta-\alpha| < 1 .$$

D'où le résultat en appliquant le théorème 4 aux nombres $\alpha, \alpha^2, \ldots, \alpha^d$ si d est le degré de β .<

2. Un lemme combinatoire.

Le résultat suivant généralise le lemme III.1 .

LEMME 1.- Soient des entiers positifs $n, r_1, \ldots, r_m$ et ϵ un réel, $0 < \epsilon < 1$. Alors le nombre de $n.m$ uples $(i_{1,1}, \ldots, i_{1,n} ; i_{2,1}, \ldots, i_{2,n} ; \ldots ; \ldots, i_{m,n})$ d'entiers naturels vérifiant

(1) $$i_{h,1} + \ldots + i_{h,n} = r_h \quad \text{pour} \quad h = 1, \ldots, m$$

et

$$\Big| \sum_{1 \le h \le m} i_{h,1}/r_h - m/n \Big| \ge \epsilon\, m$$

est au plus égal à

$$2 \binom{r_1+n-1}{n-1} \ldots \binom{r_m+n-1}{n-1} \exp(-\epsilon^2 m/3) .$$

> Désignons par M_1 (resp. M_2) le nombre des $(i_{h,k})$ vérifiant (1) et

$$\sum_{1 \le h \le m} i_{h,1}/r_h \le m/n - \epsilon\, m \qquad (\text{resp. } \ge m/n + \epsilon\, m) .$$

Majorons M_1 . Pour cela, considérons l'expression

$$S = \Sigma \exp\left(\epsilon\left(m/n - \sum_{1 \le h \le m} i_{h,1}/r_h\right)/2\right) ,$$

où la somme est étendue à l'ensemble des éléments de $\mathbb{N}$ nul vérifiant (1) . On a d'abord

$$M_1 \leq S \exp(-\epsilon^2 m/2) .$$

En regroupant les termes de S en $i_{1,1},\ldots,i_{m,1}$ constants et en utilisant le fait que le nombre de solutions de (1) en entiers naturels est $\binom{r_h+n-1}{n-1}$, on obtient

$$S = \prod_{1\leq j\leq m} \left(\sum_{c_j=0}^{r_j} f_j(c_j) \exp(\epsilon (1/n - c_j/r_j)/2) \right) , \quad \text{où } f_j(c) = \binom{r_j-c+n-2}{n-2} .$$

Considérons les facteurs de ce produit. Pour $r = r_j$, $c = c_j$ et $f = f_j$, on a

$$\sum_{0\leq c\leq r} f(c) \exp(\epsilon(1/n - c/r)/2)$$

$$\leq \sum_{0\leq c\leq r} f(c) (1+\epsilon(1/n - c/r)/2 + 2(\epsilon(1/n - c/r)/2)^2/3) \quad (\text{car } e^x \leq 1+x+2x^2/3 \text{ si } |x| \leq 1/2)$$

$$\leq \Big(\sum_{0\leq c\leq r} f(c) \Big)(1+\epsilon^2/6) + (\epsilon/2) \sum_{0\leq c\leq r} (1/n - c/r) f(c) \quad (\text{car } |1/n - c/r| \leq 1)$$

$$= \Big(\sum_{0\leq c\leq r} f(c) \Big)(1+\epsilon^2/6) \leq \binom{r+n-1}{n-1} \exp(\epsilon^2/6) \quad (\text{car } 1+x < e^x \text{ si } x > 0) .$$

L'égalité ci-dessus provient de la relation

$$\sum_{0\leq c\leq r} \left(\binom{r-c+n-2}{n-2} \Big/ \binom{r-c-n-1}{n-1} \right) = r/n ,$$

que l'on vérifie comme suit. Soit l'ensemble des $\binom{r+c+n-1}{n-1}$ points

$(i_1,\dots,i_n)$ de $\mathbb{N}^n$ vérifiant $i_1 + \dots + i_n = r$, affectés chacun d'une probabilité $\binom{r-c+n-1}{n-1}^{-1}$. La relation ci-dessus expr que l'espérance de la variable i_1 est égale à r/n (on a en effet $E(i_1) = \dots = E(i_n)$ et $E(i_1+\dots+i_n) = r$) .

D'où les majorations

$$S \le \Big(\prod_{1\le j\le m} \binom{r_j+n-1}{n-1} \Big) \exp(m\,\epsilon^2/6) \ ,$$

et

$$M_1 \le \Big(\prod_{1\le j\le m} \binom{r_j+n-1}{n-1} \Big) \exp(-m\,\epsilon^2/3) \ .$$

Une démonstration analogue conduit à la même majoration pour M_2 . D'où le lemme. <

3. L'indice.

On considère des polynômes P en $m\,n$ variables $X_{h,k}$ $(1 \le h \le m$, $1 \le k \le n)$, à coefficients réels. Soient L_h $(1 \le h \le m)$ des formes linéaires non nulles en $X_{h,1},\dots,X_{h,n}$. L'indice d'un polynôme P non nul par rapport aux L_h et à des entiers positifs $r_1,\dots,r_m$ est, par définition, égal au maximum des nombres $j_1/r_1+\dots+j_m/r_m$ tels que $L_1^{j_1} \dots L_m^{j_m}$ divise P (comme l'ensemble des nombres $j_1/r_1 + \dots + j_m/r_m$ est fini , il existe bien un tel nombre maximal) . Par convention, l'indice du polynôme nul est infini. L'indice possède les propriétés suivantes :

(I_1) $\quad I(P+Q) \ge \min(I(P), I(Q))$, l'égalité a lieu si $I(P) \ne I(Q)$,

(I_2) $\quad I(PQ) = I(P) + I(Q)$,

$$(I_3) \qquad I\left(\frac{\partial^{j_{1,1}+\ldots+j_{m,n}}}{\partial X_{1,1}^{j_{1,1}} \ldots \partial X_{m,n}^{j_{m,n}}} P\right) \geq I(P) - \sum_{1 \leq h \leq m} ((j_{h,1}+\ldots+j_{h,n})/r_h)$$

dont la démonstration est laissée au lecteur.

REMARQUES. -

1. Soit T l'espace défini par les équations $L_1 = \ldots = L_m = 0$. Supposons que chaque L_h contienne effectivement la variable $X_{h,1}$ (i.e. $\frac{\partial L_h}{\partial X_{h,1}} \neq 0$) . Alors l'indice P est au moins égal à c si, et seulement si, pour tous les $(j_1, \ldots, j_m)$ vérifiant $j_1/r_1+\ldots+j_m/r_m < c$ le polynôme $\frac{\partial^{j_1+\ldots+j_m}}{\partial X_{1,1}^{j_1} \ldots \partial X_{1,m}^{j_m}} P$ s'annule sur T .

2. Cette définition de l'indice généralise celle de Roth rencontrée au chapitre III . En effet, l'indice de Roth d'un polynôme $P(X_1, \ldots, X_m)$ en un point $(p_1/q_1, \ldots, p_m/q_m)$ est égal à l'indice du polynôme $X_{2,1}^{d_1} \ldots X_{2,m}^{d_m} P(X_{1,1}/X_{2,1}, \ldots, X_{1,m}/X_{2,m})$ par rapport aux formes linéaires $L_h = q_h X_{1,h} - p_h X_{2,h}$ et aux r_h , où d_h désigne le degré de P en X_h .

4. Le polynôme auxilaire.

LEMME 2. - Pour chaque $h = 1, \ldots, m$ soient n formes linéaires $L_{h,1}, \ldots, L_{h,n}$ non nulles en $X_{h,1}, \ldots, X_{h,n}$ à dont les coefficients sont des entiers algébriques réels appartenant un corps K de degré d . Soit ϵ positif inférieur à 1 vérifiant $\exp(\epsilon^2 m/3) > 2d\,n$. Alors il existe un

polynôme $P(X_{1,1},\dots,X_{1,n},\dots,X_{m,n})$ non nul, à coefficients entiers, homogène de degré r_h en $X_{h,1},\dots,X_{h,n}$ $(h = 1,\dots,m)$, tel que

(i) $\quad \|P\| \le C_1^{\,r_1+\dots+r_m}$

(ii) $\quad \mathrm{Ind}\,(P;L_{1,k},\dots,L_{m,k}\,;\,r_1,\dots,r_m) \ge (n^{-1}-\epsilon)m$ pour $k = 1,\dots,n$.

En outre, si on suppose les $L_{h,j}$ linéairement indépendants, dans les développements

$$(2)\qquad \frac{\partial^{j'_{1,1}+\dots+j'_{m,n}}}{j'_{1,1}!\dots j'_{m,n}!\,\partial X_{1,1}\dots\partial X_{m,n}}P = \sum_{(j)} d_{j'}(j)\,L_{1,1}^{j_{1,1}}\dots L_{m,n}^{j_{m,n}},$$

on a

$$|d_j(j')| \le C_2^{\,r_1+\dots+r_m},$$

$d_j(j_{1,1},\dots,j_{m,n}) = 0$ si pour $k = 1,\dots,n$ on a $\sum_{1\le h\le m} j_{h,k}/r_h - m/n < -\epsilon m\,(j_1/r_1+\dots+j_m/r_m)$

et

(iii) $\quad d_j(j_{1,1},\dots,j_{m,n}) \ne 0$ implique $\left|\sum_{1\le h\le m} j_{h,k}/r_h - m/n\right| \le (n-1)(\epsilon m + j_1/r_1+\dots+j_m/r_m)$, $\quad k = 1,\dots,n$.

> Sans perte de généralité, on peut supposer que, pour chaque h, k, le coefficient $(\alpha_{h,k})$ de $X_{h,1}$ dans $L_{h,k}$ n'est pas nul. D'après la remarque 1, la condition (ii) équivaut au fait que les polynômes $(j_1!\dots j_m!)^{-1}(\partial/\partial X_{1,1})^{j_1}\dots(\partial/\partial X_{m,1})^{j_m}P =: P^{(j)}$ s'annulent sur l'espace d'équations $L_{1,k} = \dots = L_{m,k} = 0$ pour $(j_1,\dots,j_m)$ vérifiant $j_1/r_1+\dots+j_m/r_m < (1/n-\epsilon)m$; ce qui s'écrit

$$(3) \qquad P^{(j)}(-L_{1,k}(0, X_{1,2}, \ldots, X_{1,n}), \alpha_{1,k}X_{1,2}, \ldots, \alpha_{1,k}X_{1,n}; \ldots) = 0 \ .$$

D'après les conditions d'homogénéité imposées à P, cette relation revient à annuler $f_1(j_1) \ldots f_m(j_m)$ (notations du lemme 1) coefficients. Chacun de ces coefficients est une forme linéaire en les coefficients de P, dont les coefficients sont des entiers de K. Il nous faut majorer les coefficients de ces formes linéaires. Chaque terme du membre gauche de (3) est la somme d'au plus $N := \binom{r_1+n-1}{n-1} \ldots \binom{r_m+n-1}{n-1}$ termes dont la hauteur est majorée par $(n\,B)^{r_1+\ldots+r_m}$, où B désigne un entier majorant la hauteur des coefficients des $L_{h,k}$. On a donc à résoudre un système de $\ell\, M_1$ équations, avec $M_1 \leq N \exp(-\epsilon^2 m/3)$ d'après le lemme 1, de hauteur au plus $(2n^n B)^{r_1+\ldots+r_m}$. D'après le théorème I.4 (voir aussi l'exercice I.17) il existe une solution P vérifiant (i) avec

$$C_1 = 2\, n^{2n} B \ .$$

Nous laissons au lecteur le soin de vérifier que la majoration des $|d_j(j')|$ a lieu avec

$$C_2 = 2\, C_1\, n\, G \ ,$$

où G désigne un majorant de la valeur absolue des coefficients des matrices inverses des matrices dont les lignes sont constituées par les coefficients des formes linéaires $L_{h,k}$.

D'après (I_3), l'indice de $P^{(j)}$ par rapport à $(L_{1,k}, \ldots, L_{m,k}; r_1, \ldots, r_m)$ est minoré par

$$(1/n-\epsilon)m - (j_1/r_1+\ldots+j_m/r_m)$$

donc si $d_j(j_{1,1},\ldots,j_{m,n})$ n'est pas nul on a

$$\sum_{1\le h\le m} j_{h,k}/r_h - m/n \ge -\epsilon m - (j_1/r_1+\ldots+j_m/r_m) \ .$$

De plus, $P^{(j)}$ est homogène en $L_{h,1},\ldots,L_{h,n}$ de degré au plus r_h, ce qui implique

$$\sum_{1\le k\le n} j_{h,k}/r_h \le 1 \ , \quad \text{donc} \quad \sum_{1\le k\le n} \Big(\sum_{1\le h\le m} j_{h,k}/r_h - m/n \Big) \le 0 \ .$$

D'où (iii) .<

5. Grilles.

Soit T un hyperplan de $\mathbb{R}^k$ engendré par des vecteurs $u_1,\ldots,u_{k-1}$. Par une grille de taille s sur T on désignera l'ensemble des points $w_1u_1 + \ldots + w_{k-1}u_{k-1}$ où les w_i parcourent les entiers de 1 à s. Le lemme suivant, dû à W. Schmidt, est fondamental pour la suite.

LEMME 3. - Soit $P(X_{1,1},\ldots,X_{m,n})$ un polynôme de degré total $\le r_h$ en $X_{h,1},\ldots,X_{h,n}$ $(h = 1,\ldots,m)$. Soient $T_1,\ldots,T_m$ des hyperplans de $\mathbb{R}^n$. Soit G_h une grille de taille s_h sur T_h pour $h = 1,\ldots,m$. Soient $t_1,\ldots,t_m$ des entiers positifs vérifiant $s_h(t_h+1) > r_h$ pour $h = 1,\ldots,m$. On suppose que les polynômes $(\partial/\partial X_{1,1})^{t_{1,1}} \ldots (\partial/\partial X_{m,n})^{t_{m,n}} P$ s'annulent sur $T_1 \times \ldots \times T_m$ (on identifie $\mathbb{R}^{mn}$ et $(\mathbb{R}^n)^m$) dès que l'on a

$$t_{h,1}+\ldots+t_{h,n} \leq t_h \quad \text{pour} \quad h = 1,\ldots,m .$$

Alors P s'annule sur $T_1 \times \ldots \times T_m$.

> Il suffit d'abord de démontrer le résultat pour $m = 1$, le cas général s'en déduit par récurrence sur m. De plus, par une transformation linéaire convenable, on se ramène au cas où la grille est définie par les vecteurs $(1,0,\ldots,0),\ldots,(0,\ldots,0,1,0)$. Il suffit donc de montrer qu'un polynôme Q de degré total au plus r, en k variables, est nul si ses dérivées partielles d'ordre au plus t s'annulent aux s^k points*. Si $k = 1$ le résultat est trivial. Raisonnons par récurrence sur k. Pour $h = 1,\ldots,s$ soit e_h le plus grand entier $\leq t$ tel que $(X_1-h)^{e_h}$ divise Q. Considérons le polynôme $R = (X_1-1)^{-e_1} \ldots (X_1-s)^{-e_s} Q$. Soit i tel que $e_i = e$ soit minimal. On vérifie que le polynôme $R(X_1,\ldots,X_{i-1},i,X_{i+1},\ldots,X_k)$ ainsi que ses dérivées partielles d'ordre au plus $t-e$ s'annule aux points $(w_1,\ldots,w_{i-1},w_{i+1},\ldots,w_k)$ pour $w_j = 1,\ldots,s$, comme sond degré est au plus $r-e_1-\ldots-e_s \leq r-e\ s < s(t-e+1)$ l'hypothèse montre que ce polynôme est nul. Il en résulte que $(X_1-1)^{t+1} \ldots (X_1-s)^{t+1}$ divise Q. En comptant les degrés on aboutit au fait que Q est nul.<

6. Minoration de l'indice par rapport à certaines formes linéaires rationnelles.

Dans toute la suite on posera $\ell = n-1$. Soient $w_1,\ldots,w_\ell$ des vecteurs de $\mathbb{Z}^n$ linéairement indépendants, il existe unf forme linéaire M non nulle à coefficients entiers premiers entre eux dans leur ensemble qui

* entiers $(w_1,\ldots,w_k)$, $1 \leq w_i \leq s$ $(1 \leq i \leq k)$, pour t vérifiant $s(t+1) > r$.

s'annule aux points w_i (M est unique au facteur ± 1 près), on notera $M\{w_1,\dots,w_\ell\}$ une telle forme.

LEMME 4. - Soient $c_1,\dots,c_n$ des nombres réels, $|c_i| \le 1$ pour $i = 1,\dots,n$, $c_1+\dots+c_n = 0$. Soient ϵ et δ des nombres positifs vérifiant $16\, n^2\, \epsilon < \delta < 1$. Soient $L_1,\dots,L_n$ des formes linéaires en m variables telles que les hypothèses du lemme 2 soient satisfaites en posant $L_{h,i} = L_i(X_{h,1},\dots,X_{h,n})$. Soit P le polynôme construit à ce lemme. Soient $Q_1,\dots,Q_m$ des réels tels que

$$Q_h^{\epsilon} > \max\left(2^n C_2,\ n(1+1/\epsilon)\right) \quad \text{pour } h = 1,\dots,m \tag{4}$$

et

$$r_1 \log Q_1 \le r_h \log Q_h \le (1+\epsilon) r_1 \log Q_1 \quad (h = 1,\dots,m)\ . \tag{5}$$

Soient enfin, pour $h = 1,\dots,m$, des points $w_{h,1},\dots,w_{h,\ell}$ de $\mathbb{R}^n$ à coordonnées entières, linéairement indépendants tels que l'on ait

$$|L_j(w_{h,k})| \le Q_h^{c_j-\delta} \quad (1 \le j \le n,\ 1 \le k \le \ell,\ 1 \le h \le m)\ . \tag{6}$$

Alors P vérifie

$$\mathrm{Ind}\,(P\ ;\ M_1,\dots,M_m\ ;\ r_1,\dots,r_m) \ge \epsilon\, m\ ,$$

où M_h est une forme linéaire en $X_{h,1},\dots,X_{h,n}$ du type $M_h = M\{w_{h,1},\dots,w_{h,\ell}\}$.

> D'après la remarque 1 et le lemme 3 il suffit de montrer que les dérivées partielles $P^{(j)}$ s'annulent aux points $(v_1,\dots,v_m)$,

où chaque v_h parcourt la grille G_h de taille $1+[1/\epsilon]$ sur les vecteurs $w_{h,1}, \ldots, w_{h,\ell}$ pour tout (j) vérifiant $\sum_{1\le h\le m} j_{h,k}/r_h < 2\,\epsilon\, m$, $k = 1,\ldots,n$. (on applique le lemme 3 avec $s_h = 1+[1/\epsilon]$ et $t_h = [\epsilon\, r_h]$ et on utilise l'inégalité $\epsilon m+[r_1\epsilon]/r_1+\ldots+[r_m\epsilon]/r_m \le 2\,\epsilon\, m$). On utilise les expressions (2). De (4), (6) et $16\, n^2\epsilon < \delta$, on déduit les majorations

$$|L_k(v_h)| \le n(1+[1/\epsilon]) \max_i |L_k(w_{h,i})| \le Q_h^{\,c_k - 15\, n^2\epsilon}$$

pour $k = 1,\ldots,n$ et $h = 1,\ldots,m$.

En utilisant (iii) et (5), on vérifie que si $d^{(j)}(j_{1,1},\ldots,j_{m,n})$ n'est pas nul on a

$$(7)\qquad \Big|\sum_{1\le h\le m} j_{h,k} \log Q_h - r_1 \log Q_h\, m/n\Big| \le 7\,\epsilon\, m\, n \log Q_1 \quad (k = 1,\ldots,n),$$

ce qui implique

$$(8)\qquad |L_k(v_1)^{j_{1,k}} \ldots L_k(v_m)^{j_{m,k}}| \le Q_1^{\,r_1 m c_k/n - \epsilon\, r_1 mn}, \quad k = 1,\ldots,n.$$

On en déduit que les $P^{(j)}(v_1,\ldots,v_m)$ considérés vérifient

$$|P^{(j)}(v_1,\ldots,v_m)| \le (2\,C_2)^{r_1+\ldots+r_m} \max \Big|\prod_{1\le k\le n} L_k(v_1)^{j_{1,k}} \ldots L_k(v_m)^{j_{m,k}}\Big|$$

(où le maximum est étendu aux $(j_{1,1},\ldots,j_{m,n})$ vérifiant (7) (utiliser le lemme 2))

$$\le (2^n C_2)^{r_1+\ldots+r_m}\, Q_1^{-r_1\, m\, n^2\,\epsilon}$$ (utiliser (8) et la relation $c_1+\ldots+c_n = 0$)

$$\le (2^n C_2)^{r_1+\ldots+r_m} (Q_1^{-r_1} \ldots Q_m^{-r_m})^{\epsilon\, n^2/(1+\epsilon)}$$ (grâce à (5))

$\leq (2^n C_2 Q_1^{-\epsilon})^{r_1} \ldots (2^n C_2 Q_m^{-\epsilon})^{r_m}$ (on a $0 < \epsilon < 1 \leq n-1$)

< 1 (d'après (4)).

D'où le résultat puisque les $P^{(j)}(v_1, \ldots, v_m)$ sont des entiers rationnels.<

7. Une généralisation du lemme de Roth.

Le lemme suivant fournit, sous certaines hypothèses, une majoration de l'indice. Il est dû à W. Schmidt.

LEMME 5. - Soit $\epsilon > 0$ fixé. Soit m un entier avec $\epsilon m > 2$. On pose $t = \exp(-2^{m+3}/\epsilon m)$. Soit $P(X_{1,1}, \ldots, X_{m,n})$ un polynôme à coefficients entiers, non nul, homogène de degré r_h en $X_{h,1}, \ldots, X_{h,n}$ $(h = 1, \ldots, m)$ avec $r_{h+1} \leq t\, r_h$ $(h = 1, \ldots, m-1)$. Soient $M_1, \ldots, M_m$ des formes linéaires non nulles à coefficients entiers, premiers entre eux dans leur ensemble. Soit τ un réel positif, $\tau \leq n$. On suppose que les inégalités suivantes ont lieu

$$\|M_h\|^{r_h} \geq \|M_1\|^{r_1 \tau}, \quad \|M_h\|^{t\tau} \geq 2^{4m^2 n^2} \quad (h = 1, \ldots, m)$$

et que P vérifie

$$\|P\| \leq \|M_1\|^{r_1 t_\tau / n^2 m}.$$

Alors, on a

$$\mathrm{Ind}\,(P\,;\, M_1, \ldots, M_m\,;\, r_1, \ldots, r_m) < \epsilon\, m.$$

> Posons $M_h = m_{h,1} X_{h,1} + \ldots + m_{h,n} X_{h,n}$. Sans perte de généralité, on suppose que $\|M\|_h = m_{h,1}$ pour $h = 1, \ldots, m$. On peut aussi supposer que l'on a p.g.c.d. $(m_{h,1}, m_{h,2}) \leq |m_{h,1}|^{(\ell-1)/\ell}$. (En effet, si $d_{h,j}$ = p.g.c.d. $(m_{h,1}, m_{h,j})$, $d_{h,2} \ldots d_{h,n}$ divise $m_{h,1}^{n-2}$ puisque, pour tout p premier, on a $v_p(d_{h,i}) \leq v_p(m_{h,1})$ et $\min(v_p(d_{h,2}), \ldots, v_p(d_{h,n})) = 0$).

Quitte à diviser P par des puissances convenables des $X_{h,k}$ $(h = 1, \ldots, m,$ $k = 3, \ldots, n)$ (ce qui ne modifie pas son indice par rapport aux M_h) on peut supposer qu'aucune d'elles ne divise P. Considérons maintenant le polynôme $Q(X_1, \ldots, X_m) = P(X_1, 1, 0, \ldots, 0 ; X_2, 1, 0, \ldots, 0 ; \ldots)$. C'est un polynôme non nul, à coefficients entiers, dont la hauteur est majorée par celle de P (car P est homogène par rapport à chaque groupe de variables). Posons $q_h = m_{h,1}/d_{h,2}$ et $p_h = -m_{h,2}/d_{h,2}$. On a alors

$$I(Q ; r_1, \ldots, r_m ; p_1/q_1, \ldots, p_m/q_m) \geq \mathrm{Ind}(P ; M_1, \ldots, M_m ; r_1, \ldots, r_m)$$

Pour conclure il suffit de vérifier qu'on peut appliquer le lemme de Roth avec $c = \tau/n$, ce qui ne présente aucune difficulté. <

8. Bases duales.

On note $x.y$ le produit scalaire de deux vecteurs x et y de $\mathbb{R}^n$. A une base $(a_1, \ldots, a_n)$ de $\mathbb{R}^n$ correspond une base $(a_1^*, \ldots, a_n^*)$, appelée duale, qui vérifie $a_i . a_j^* = \delta_{i,j}$.

LEMME 6. - Soient $(a_1, \ldots, a_n)$ et $(b_1, \ldots, b_n)$ deux bases de déter-

minants respectifs D et E. Soient $\lambda_1, \ldots, \lambda_n$ tels que $|a_i . b_j| \leq \lambda_j$ $(1 \leq i, j \leq n)$. Alors on a

$$|a_i^* . b_j^*| \leq n!\ \lambda_1 \cdots \lambda_{j-1}\ \lambda_{j+1} \cdots \lambda_n / |DE| \quad \text{pour} \quad 1 \leq i, j \leq n .$$

> On vérifie la relation

$$\sum_{1 \leq i \leq n} (a_i . x)(a_i^* . y) = x . y$$

par linéarité en choisissant $x = a_1^*, \ldots, a_n^*$ et $y = a_1, \ldots, a_n$. Donc, en particulier,

$$\sum_{1 \leq i \leq n} (a_i . b_h)(a_i^* . b_j^*) = b_h . b_j^* = \delta_{h,j} \quad (1 \leq h, j \leq n) .$$

Il en résulte que l'on a

$$a_i^* . b_j^* = A_{i,j} / \det A ,$$

où A est la matrice des $a_i . b_j$ $(1 \leq i, j \leq n)$ et A_{ij} le cofacteur de $a_i . b_j$ dans cette matrice. D'après les hypothèses du lemme on a $\det A = D\,E$ et $|A_{ij}| \leq (n-1)!\ \lambda_1 \cdots \lambda_{j-1}\ \lambda_{j+1} \cdots \lambda_n$. D'où le résultat.<

Soient $a_1, \ldots, a_n$ une base de déterminant D. On considère les parallélépipèdes

(9) $\quad \Pi = \{x\ ;\ |a_i . x| \leq 1 \ \text{ pour } \ 1 \leq i \leq n\}$, $\Pi^* = \{x ; |a_i^* . x| \leq 1 \text{ pour } 1 \leq i \leq n\}$.

Leurs volumes respectifs sont $2^n/|D|$ et $2^n|D|$. Soient $\lambda_1,\dots,\lambda_n$ les minima successifs de Π (voir appendice) et $\lambda_1^*,\dots,\lambda_n^*$ ceux de Π. Par définition, il existe des points à coordonnées entières $w_1,\dots,w_n$ qui vérifient $|a_i.w_j| \le \lambda_j$ pour $1 \le i,j \le n$. D'après le corollaire du théorème sur les minima successifs, si $E = \det(w_1,\dots,w_n)$, on a $|E| \le n!$. Les points $E\,w_1^*,\dots,E\,w_n^*$ sont à coordonnées entières. D'après le lemme 6, et les majorations $|a_i.w_j| \le \lambda_j$ on a

$$|a_i^*.w_j^*| \le n!\ \lambda_1\dots\lambda_{j-1}\ \lambda_{j+1}\dots\lambda_n/|D\,E| \le n!(|E|\lambda_j)^{-1},$$

puisque $(2^n/|D|)\lambda_1\dots\lambda_n \le 2^n$ par le théorème de Minkowoki. Comme les $E\,w_i^*$ sont des vecteurs linéairement indépendants de Z^n, on obtient

$$\lambda_j^* \le n!/\lambda_{n+1-j} \quad \text{pour } j = 1,\dots,n .$$

Du théorème des minima successifs résulte la minoration

$$(\lambda_1\lambda_n^*)\dots(\lambda_n\lambda_1^*) \ge (2^n/(n!\,2^n|D|^{-1}))(2^n/(n!\,2^n|D|) = (n!)^{-2} .$$

On en déduit $\lambda_j^*\lambda_{n+1-j} \ge (n!)^{-n-1}$ pour $j = 1,\dots,n$. D'où le résultat suivant.

LEMME 7 (Mahler).- Soit $a_1,\dots,a_n$ une base de $\mathbb{R}^n$ et $a_1^*,\dots,a_n^*$ la base duale. Soient $\lambda_1,\dots,\lambda_n$ et $\lambda_1^*,\dots,\lambda_n^*$ les minima successifs des ensembles Π et Π^* définis par (9). Alors on a

$$(n!)^{-n-1} \le \lambda_j^*\,\lambda_{n+1-j} \le n! \quad (j = 1,\dots,n) .$$

De plus, si $w_1,\dots,w_n$ sont des vecteurs à coordonnées entières vérifiant $|a_i.w_j| \le \lambda_j$ $(1 \le i,j \le n)$, alors si $w_1^*,\dots,w_n^*$ sont les vecteurs duaux on a

$$|a_i^*.w_j^*| \le n!(|E|\lambda_j)^{-1} \quad , \text{ où } E = \det(w_1,\dots,w_n) , \quad 1 \le i,j \le n .$$

9. Le théorème de l'avant dernier minimum.

Le résultat suivant constitue l'outil principal de la preuve des théorèmes 3 et 4.

LEMME 8. - Soit un entier ≥ 2, S un sous ensemble non vide de $\{1,\dots,n\}$. Soit $a_1,\dots,a_n$ une base de $\mathbb{R}^n$, où les a_i sont à coordonnées algébriques. Soient $A_1,\dots,A_n$ des nombres positifs avec $A_1\dots A_n=1$ On pose

$$\Pi = \{x; |a_i.x| \le A_i , \ 1 \le i \le n\} , \ \Pi^* = \{x; |a_i^* x| \le A_i^{-1} , \ 1 \le i \le n\} .$$

Soit $\delta > 0$. Il existe un nombre $Q_2 = Q_2(\delta, a_1,\dots,a_n, S)$ positif qui possède la propriété suivante :
Si Q vérifie $Q > Q_2$, $Q \ge \max(A_1,\dots,A_1^{-1},\dots,A_n^{-1})$ et $A_i Q^{\delta/2} \ge 1$ pour i parcourant S et si l'avant dernier des minima successifs $\lambda_1,\dots,\lambda_n$ de Π vérifie $\lambda_\ell < Q^{-\delta}$ alors, si $w_1,\dots,w_n$ sont des points de $\mathbb{Z}^n$ linéairement indépendants, on a

$$(10) \qquad |a_i^* w_n^*| \le n!\,|D|\, A_i^{-1}\, Q^{-\delta\ell} , \quad 1 \le i \le n , \ (D = \det(a_1,\dots,a_n))$$

et

(11) $\qquad a_i^* w_n^* = 0$ pour i parcourant S .

> Notons que le point difficile est (11) . Preuve de (10) : on applique le lemme 7 aux bases duales (a_i/A_i) et $(A_i\, a_i^*)$, on obtient $|a_i^* . w_n^*| \le n!\, A_i^{-1}\, \lambda_n^{-1}$, et la majoration de λ_ℓ jointe au théorème des minima successifs implique

(12) $\qquad \lambda_n^{-1}\, n!\, |D|\, \lambda_1 \ldots \lambda_\ell \le n!\, |D|\, \lambda_\ell^{\ell} < n!\, |D|\, Q^{-\delta\, \ell}$.

Posons $A_i = Q^{c_i}$. La condition $A_1 \ldots A_n = 1$ implique $c_1 + \ldots + c_n = 0$. Un procédé classique permet de se ramener au cas où les c_i sont fixes. Soit N un entier positif. Alors il existe des rationnels $c_1', \ldots, c_n'$ de dénominateur N vérifiant $|c_i' - c_i| < 1/N$ $(1 \le i \le n)$ et $c_1' + \ldots + c_n' = 0$ $|c_i'| \le 1$ $(1 \le i \le n)$. En choisissant $N = [9/\delta]+1$, $\delta_1 = (8/9)\delta$, on obtient $c_i' + (3/4)\delta_1 \ge 0$ pour i dans S . Alors si $w_1, \ldots, w_n$ sont des points entiers linéairement indépendants et vérifient $|a_i . w_j| \le \lambda_j\, A_i^{c_i'}$, on a $|a_i . w_j| \le \lambda_j\, Q^{c_i' + 1/N}$. Il en résulte que si $\Pi' = \{x;\ |a_i . x| \le Q^{c_i'}\}$ admet λ'_ℓ pour avant dernier minimum on a $\lambda'_\ell < Q^{1/N}\, \lambda_\ell < Q^{-\delta 1}$. De plus les points $w_1, \ldots, w_\ell$ appartiennent à $\lambda_\ell\, Q^{1/N}\, \Pi'$, et tout w' entier indépendant des $w_1, \ldots, w_\ell$ vérifie $\max_i (|a_i . w'| / A_i) \ge \lambda_n$ et donc $\max_i (|a_i . w'|\, Q^{-c_i' + 1/N}) \ge \lambda_n$, ce qui montre que w' n'appartient pas à $\lambda_\ell\, Q^{1/N}\, \Pi'$ pour $Q^{\delta n} > n!\, |D|$ (on sait que $\lambda_n > Q^{\delta \ell}\, (n!\, |D|)^{-1}$, donc $\lambda_n > \lambda_\ell\, Q^{\delta n}/(n!\, |D|)$) . Ainsi les $w'_1, \ldots, w'_\ell$ appartiennent à l'espace engendré par $w_1, \ldots, w_\ell$, donc $w_n'^*$ est proportionnel à w_n^* . Si la conclusion du lemme est fausse, il existe des nombres $i \in S$ et

$c'_1, \ldots, c'_n$ fixes tels que l'ensemble des nombres Q pour lequels on a $\lambda'_\ell < Q^{-\delta_1}$ et $a_i^* . w_n^* \neq 0$ est non borné. Supposons que ceci ait lieu. On peut aussi supposer que les composantes des a_i sont des entiers algébriques. Soit δ_2 avec $0 < \delta_2 \leq \delta_1$. Prenons ϵ positif vérifiant $16n^2\epsilon < \delta_2$ et m entier $> 3\,\epsilon^{-2} \log(2\,n\,d)$, où d est le degré du corps de nombres engendré par les coordonnées des a_i. Soient $L_1, \ldots, L_n$ les formes linéaires définies par $L_i(x) = a_i . x$ $(1 \leq i \leq n)$. Choisissons $Q_1, \ldots, Q_m$ tels que les conditions (4) et (5) du lemme 4 aient lieu. Considérons le polynôme P construit au lemme 2. Soient $w_{h,1}, \ldots, w_{h,n}$ des points entiers indépendants avec $w_{h,j} \in \lambda_j \Pi'(Q_h)$ pour $j = 1, \ldots, n$ (où $\lambda_j = \lambda_j(Q_h)$). Alors la condition (6) du lemme 4 est satisfaite (avec δ_2 au lieu de δ). Si $M_1, \ldots, M_m$ sont les formes définies au lemme 4, on obtient l'inégalité

$$\mathrm{Ind}(P\,;\, M_1, \ldots, M_m\,;\, r_1, \ldots, r_m) \geq \epsilon\, m\,.$$

Supposons que l'on ait prouvé l'existence de constantes C_3, C_4 et C_5 telle que l'on ait

(13) $\quad Q_h^{C_3} \leq \|M_h\| \leq Q_h^{C_4}$ $(h = 1, \ldots, m)$ pour $Q_h > C_5$ (ce qu'on suppose vérifié)

On a alors $\|M_h\|^{r_h} \geq \|M_1\|^{r_1 \tau}$ pour $h = 1, \ldots, m$, où $\tau = C_4/C_3$. Pour Q_1 assez grand, les autres conditions du lemme 5 sont vérifiées. On obtient la majoration

$$\mathrm{Ind}(P\,;\, M_1, \ldots, M_m\,;\, r_1, \ldots, r_m) < \epsilon\, m\,.$$

On aboutit à la contradiction souhaitée.

Démontrons (13). Pour simplifier les notations nous supprimerons l'indice h. Le lemme 7 appliqué aux bases duales $(Q^{-c'_j} a_j)$ et $(Q^{c_j} a^*_j)$ et (12) conduisent à la majoration

$$(14) \qquad |a_j^* . w_n^*| \le n!/(|E|\ \lambda_n\ Q^{c'_j}) < (n!)^2\ |D/E|\ Q^{-\delta_1 \ell\ -c'_j} \quad (i = 1, \ldots, n).$$

Puisque les a_i^* sont linéairement indépendants et les $|c_i|$ au plus égaux à 1, il existe une constante C_6, que de n et de $a_1, \ldots, a_n$, telle que l'on ait $|w_n^*| \le C_6\ Q^{1-\delta_1 \ell}$, donc $|w_n^*| \le Q$ pour Q assez grand. Minorons $|w_n^*|$. De (14) et de $c'_i + 3\delta_1/4 \ge 0$, on tire

$$(15) \qquad 0 < |a_i^* . w_n^*| < Q^{-\delta/5} \quad \text{pour Q assez grand.}$$

Le nombre $|a_i^* . w_n^*|$ est algébrique, son dénominateur est borné (celui des a_i^* est fixe, celui de w^* divise E et, d'après le corollaire du théorème des minima successifs, E divise n!), soit d^* son degré. On a donc $|\text{Norm}\ (a_i^* . w_n^*)| \ge C_7$, ce qui implique $|a_i^* . w_n^*| > C_8\ |w_n^*|^{1-d^*}$. Cette inégalité, jointe à (15), montre que l'on a $d^* \ge 2$ et donc $|w_n^*| \le Q^{-\delta/5}/C_8$ pour Q assez grand. Pour démontrer (13) il suffit maintenant de comparer $\|M\|$ et $|w_n^*|$. Considérons le vecteur (encore noté M) de $\mathbb{Z}^n$ ayant pour composantes les coefficients de M. Par hypothèse on a $w_i . M = 0$, $1 \le i < n$, donc M et w_n^* sont proportionnels. Soit $M = \lambda\ w_n^*$. De $w_n . w_n^* = 1$ on déduit que λ est entier. Du fait que $E\ w_n^*$ est entier (avec $E | n!$) et que les composantes de M ont un p.g.c.d égal à 1, λ divise E. D'où le résultat.<

COROLLAIRE. - Soient $a_1,\dots,a_n$, δ comme dans le lemme 8. Supposons qu'il existe un ensemble non borné $\mathfrak{Q}$ de nombre Q tel qu'à chacun d'eux soient associés des nombres positifs vérifiant $A_1 \dots A_n = 1$ et $\max(A_1,\dots,A_n, A_1^{-1},\dots,A_n^{-1}) \le Q$. On suppose encore que pour tout $Q \in \mathfrak{Q}$ l'avant dernier minimum de $\Pi = \Pi(Q)$ vérifie $\lambda_\ell < Q^{-\delta}$. Alors, pour un sous-ensemble $\mathfrak{Q}'$ non borné de $\mathfrak{Q}$, les vecteurs $w_n^* = w_n^*(Q)$ coïncident.

> Pour une partie non bornée de $\mathfrak{Q}$, l'ensemble $S = S(Q) = \{ i; A_i Q^{\delta/2} \ge 1 \}$ est le même (non vide). On se limite à ces valeurs de Q qui sont supérieures à Q_2. Alors $a_i^* . w_n^* = 0$ pour i dans S et $|a_i^* . w_n^*| \le n! \, |D| \, A_i^{-1} \, Q^{\delta} \, \ell$, $1 \le i \le n$. Soient $\lambda_1^*,\dots,\lambda_n^*$ les minima successifs de Π^*. D'après le lemme 7, on a $\lambda_2^* \ge (\lambda_\ell \, n!^{n+1})^{-1}$, donc $\lambda_2^* > 1$ pour Q assez grand (car $\lambda_\ell < Q^{-\delta}$) ; en d'autres termes, pour Q assez grand, les points entiers de $\Pi^*(Q)$ appartiennent à une droite fixe. Soit M le vecteur associé à w_n^* comme dans la démonstration du lemme. La majoration des $|a_i^* . w_n^*|$ jointe à $|M| \le n! \, |w_n^*|$ montre que M appartient à Π^*. Donc, pour Q assez grand, M prend au plus deux valeurs et w_n^* ne prend qu'un nombre fini de valeurs. D'où le résultat. <

10. Le lemme de Davenport.

Ce résultat permet, sous certaines hypothèses, de montrer que les minima λ_ℓ et λ_n d'un parallélépipède sont assez voisins.

LEMME 9.- Soit $a_1, \ldots, a_n$ une base de $\mathbb{R}^n$ et $\lambda_1, \ldots, \lambda_n$ les minima de l'ensemble $\Pi = \{x ; |a_i . x| \leq 1 \text{ pour } 1 \leq i \leq n\}$. Soient des nombres positifs $\rho_1 \geq \rho_2 \geq \ldots \geq \rho_n$ qui vérifient $\rho_1 \lambda_1 \leq \rho_2 \lambda_2 \leq \rho_n \lambda_n$. Alors, après une permutation convenable des a_i, les minima $\lambda'_1, \ldots, \lambda'_n$ de $\Pi' = \{x ; |a_i . x| \leq 1/\rho_i , 1 \leq i \leq n\}$ vérifient

$$2^{-n} \lambda_j \rho_j \leq \lambda'_j \leq 2^{n^2} n! \lambda_j \rho_j .$$

De plus, si $(w_1, \ldots, w_n)$ est une base de $\mathbb{Z}^n$ vérifiant $w_j \in \lambda_j \Pi$ $(1 \leq j \leq n)$, tout vecteur w linéairement indépendant des $w_1, w_2, \ldots, w_{j-1}$ vérifie

$$\max_{1 \leq i \leq n} (\rho_i |a_i . w|) \geq 2^{-n} \rho_j \lambda_j .$$

> Par homogénéité, on peut supposer que le déterminant des a_i et le produit des ρ_i sont égaux à 1. Soit T_j l'espace engendré par les vecteurs $w_1, \ldots, w_j$. Pour chaque $j \geq 2$, il existe une relation linéaire de la forme $u_1 a_1 . w + \ldots + u_j a_j . w = 0$ caractérisent les points de T_{j-1} parmi ceux de T_j. On permute les L_j de sorte que chaque $|u_j|$ soit maximal. On a alors

$$|a_j . w| \leq |a_1 . w| + \ldots + |a_{j-1} . w| \quad \text{si } w \in T_{j-1}$$

d'où l'on déduit

$$|a_1 . w| + \ldots + |a_j . w| \geq 2^{j-n} (|a_1 . w| + \ldots + |a_\ell . w|) \quad \text{si } w \in T_{j-1}$$

$(1 \leq j \leq n)$.

De plus, si w est dans T_j sans appartenir à T_{j-1} on a $\max_{1\le i\le n} |a_i.w| \ge \lambda_j$, donc l'inégalité ci-dessus implique alors

$$\max(\rho_1|a_1.w|,\dots,\rho_n|a_n.w|) \ge (2^{j-n}/j)\rho_j\lambda_j \ge 2^{-n}\rho_j\lambda_j .$$

Du fait que les $\rho_j\lambda_j$ sont croissants, cette minoration a lieu pour $w \notin T_{j-1}$. Donc $\lambda'_j \ge 2^{-n}\rho_j\lambda_j$. La borne supérieure est obtenue en utilisant la relation $\rho_1\dots\rho_n = 1$ et les inégalités $\lambda'_1\dots\lambda'_n \le 1$ et $\lambda_1\dots\lambda_n \ge 1/n!$ déduites du théorème des minima successifs.<

11. Le théorème des deux derniers minima.

LEMME 10. - *Soient* $a_1,\dots,a_n$ *des vecteurs linéairement indépendants de* $\mathbb{R}^n$ *à coordonnées algébriques réelles,* $c_1,\dots,c_n$ *des réels vérifiant* $c_1+\dots+c_n = 0$, $\max|c_i| \le 1$. *Soient* $\lambda_1,\dots,\lambda_n$ *les minima successifs de* $\Pi(Q) = \{x ; |a_i.x| \le Q^{c_i},\ 1 \le i \le n\}$. *Soient* $w_1,\dots,w_n$ *une base de* Z^n *avec* $w_j \in \lambda_j \Pi$ $(1 \le j \le n)$. *Supposons qu'il existe* $\delta > 0$ *et que un ensemble non borné de* Q *on ait* $\lambda_\ell < \lambda_n Q^{-\delta}$ *alors il existe un ensemble non borné de* Q *tels que les* w_n^* *coïncident.*

> Posons $\rho_0 = (\lambda_1\dots\lambda_{\ell-1}\lambda_\ell^2)^{1/n}$, $\rho_1 = \rho_0/\lambda_1,\dots,\rho_\ell = \rho_0/\lambda_\ell$ et $\rho_n = \rho_0/\lambda_\ell$. On a $\rho_1\dots\rho_n = 1$. Le lemme 9 s'applique et montre qu'il existe une permutation $\rho'_1,\dots,\rho'_n$ des ρ_i telles que les λ'_i relatifs à $\Pi' = \{x ; |a_i.x| \le Q^{c_i}/\rho'_i\}$ vérifient la conclusion de ce lemme. En particulier,

$$\lambda'_\ell \le 2^{n^2} n!\ \rho_\ell\ \lambda_\ell = 2^{n^2} n!\ \rho_0 \ll (\lambda_\ell/\lambda_n)^{1/n} < Q^{-\delta/n},$$

où les constantes impliquées par $\ll$ dépendent des a_i. Par ailleurs pour $x \in \mathbb{Z}^n$ non nul on a $\max |a_i.x| \gg |x| \ge 1 \ge Q^{c_j-1}$ $(1 \le j \le n)$, donc $\lambda_1 \gg Q^{-1}$. En sens contraire, si $(e_1,\dots,e_n)$ désigne la base canonique de $\mathbb{R}^n$, on a $|a_i.e_j| \ll 1 \le Q^{c_k+1}$ $(1 \le i,j,k \le n)$, donc $\lambda \ll Q$. On a $\rho_1 = \rho_0/\lambda_1 \ll (\lambda_\ell/\lambda_n)^{1/n}/\lambda_1 \le 1/\lambda_1 \ll Q$ et $\rho_n = \rho_0/\lambda_\ell \gg (\lambda_\ell/\lambda_n)^{1/n}/\lambda_\ell \ge 1/\lambda_n \gg 1/Q$. Par conséquent $Q^{-1} \ll \rho_n \le \dots \le \rho_1 \ll Q$. Considérons les nombres $A_i = Q^{e_i}/\rho'_i$. Il vérifient $Q^{-2} \ll A_i \ll Q^2$ $(1 \le i \le n)$, $A_1 \dots A_n = 1$. Pour Q assez grand, les hypothèses du lemme 8 et de son corollaire sont satisfaites (à quelques changements de notations près) pour le parallélépipède Π', ce qui prouve qu'un certain w'_n est le même pour un ensemble non borné de Q. Un argument déjà employé prouve que w_n^* et $w_n'^*$ sont proportionnels et que le facteur de proportionnalité ne prend qu'un nombre fini de valeurs. D'où la conclusion.

12. Algèbre extérieure.

Pour $0 \le p \le n$ on considère la puissance extérieure $\Lambda^p\mathbb{R}^n$, elle admet pour base les vecteurs $e_T = e_{i_1} \wedge \dots \wedge e_{i_p}$ $(i_1 < \dots < i_p)$ où $T = \{i_1,\dots,i_p\}$ parcourt les parties à p éléments de $\{1,\dots,n\}$ et où $e_1,\dots,e_n$ désigne la base canonique de $\mathbb{R}^n$ (on pose $e_\emptyset = 1$). L'espace $G = \bigoplus_{0\le p\le n} \Lambda^p\mathbb{R}^n$ est muni d'une structure d'algèbre définie par

$$e_T \wedge e_S = \begin{cases} 0 & \text{si } T \cap S \ne \emptyset \\ (-1)^\sigma e_{T\cup S} & \text{sinon,} \end{cases}$$

où σ désigne la signature de la permutation qui réordonne les éléments de $T \cup S$ dans l'ordre croissant. On munit $\Lambda^p \mathbb{R}^n$ du produit scalaire défini par

$$e_T \cdot e_S = \delta_{S,T} \quad (= 1 \text{ si } T = S \ , \ 0 \text{ sinon}) .$$

On a l'identité de Laplace

$$(x_1 \Lambda \dots \Lambda x_p) . (y_1 \Lambda \dots \Lambda y_p) = \det(x_i . y_j)_{1 \le i, j \le p} \qquad (x_i, \ y_j \in \mathbb{R}^n) \ .$$

En fait $x_1 \Lambda \dots \Lambda x_p$ a pour composantes les mineurs d'ordre p extraits de la matrice ayant $x_1, \dots, x_p$ pour lignes, il est non nul si et seulement si $x_1, \dots, x_p$ sont indépendants.

LEMME 11.- Soit $a_1, \dots, a_n$ une base de $\mathbb{R}^n$. Soit $1 \le p \le n$. Pour $S = \{i_1, \dots, i_p\}$, $1 \le i_1 < \dots < i_p \le n$, on pose

$$a_S = a_{i_1} \Lambda \dots \Lambda a_{i_p} .$$

Alors les $\binom{n}{p}$ vecteurs a_S constituent une base de $\Lambda^p \mathbb{R}^n$. On a

$$\det(a_S) = \det(a_i)^t \ , \quad \text{où} \quad t = \binom{n-1}{p-1} .$$

Si $(a_1^*, \dots, a_n^*)$ est la base duale de $(a_1, \dots, a_n)$ dans $\mathbb{R}^n$ alors les vecteurs

$$a_S^* = a_{i_1}^* \Lambda \dots \Lambda a_{i_p}^*$$

constituent la base duale de (a_S) dans $\Lambda^p\mathbb{R}$.

> La première assertion est évidente. Nous admettrons la seconde. La troisième résulte de l'identité de Laplace.<

13. "Compound bodies" de Mahler.

Soit $a_1,\dots,a_n$ une base de $\mathbb{R}^n$, de déterminant 1. Soit

$$\Pi = \{x \in \mathbb{R}^n ;\ |a_i.x| \le 1 ,\ \ 1 \le i \le n\} .$$

Soit p, $1 \le p \le n$. On pose (voir les notations du paragraphe 12)

$$\Pi_p = \{x \in \Lambda^p\mathbb{R}^n ;\ \ |a_T.x| \le 1 ,\ \ T \in C(n\ p)\} ,$$

où $C(n,p)$ désigne l'ensemble des parties de $\{1,\dots,n\}$ comportant p élements.

Le volume de Π_p est $2^{\binom{n}{p}}$. Soient $\lambda_1,\dots,\lambda_n$ les minima de Π. Pour $T \in C(n,p)$ on pose $\lambda_T = \prod_{i\in T} \lambda_i$. On ordonne : $\lambda_{T_1} \le \lambda_{T_2} \le \dots$ Soient des w_i entiers associés aux minima λ_i. On pose $w_T = w_{i_1} \wedge \dots \wedge w_{i_p}$ pour $T = \{i_1,\dots,i_p ;\ 1 \le i_1 < \dots < i_p \le n\}$ parcourant $C(\ ,p)$. D'après l'identité de Laplace,

$$a_T.w_S = \det(a_i.w_j) \quad (\text{avec } |a_i.w_j| \le \lambda_j ,\ \ 1 \le i,\ j \le n)$$

donc

$$|a_T.w_S| \le p!\ \lambda_S .$$

LEMME 12 (Mahler). - Soit (ν_i) la suite des minima de Π_p. On a

$$(p!^k k!)^{-1} \lambda_{T_i} \leq \nu_i \leq p! \lambda_{T_i} \quad , \qquad 1 \leq i \leq \binom{n}{p} =: k \ .$$

> La majoration des ν_i résulte de ce qui précède. Comme d'habitude, la minoration résulte des inégalités

$$\lambda_1 \cdots \lambda_\ell \leq 1 \quad , \qquad \nu_1 \cdots \nu_k \geq 1/k! \ . <$$

14. Le théorème du sous-espace.

Ce résultat contient en substance les théorèmes 3 et 4 et d'autres plus généraux qui seront démontrés dans la suite.

THEOREME 6. - Soient $L_1, \ldots, L_n$ des formes linéaires indépendantes en $x = (x_1, \ldots, x_n)$, à coefficients réels algébriques. Soient $c_1, \ldots, c_n$ des constantes de module ≤ 1 et de somme nulle. Posons, pour $Q > 0$,

$$\Pi = \Pi(Q) = \{x \ ; \ |L_j(x)| \leq Q^{c_j} \ , \ 1 \leq j \leq n\} \ .$$

Soient $\lambda_i = \lambda_i(Q)$, $1 \leq i \leq n$, les minima successifs de Π. Supposons qu'il existe δ positif, un entier d, $1 \leq d < n$, et un ensemble $\mathfrak{Q}$ non borné de réels positifs tels que l'on ait

$$\lambda_d < \lambda_{d+1} Q^{-\delta} \quad \text{si} \quad Q \in \mathfrak{Q} \ . \tag{16}$$

Alors il existe un sous espace rationnel S_d fixe, de dimension d, et un sous ensemble non borné $\mathfrak{Q}$ de $\mathfrak{Q}$ tels que les d premiers minima de $\Pi(Q)$ soient atteints en des points de S_d lorsque Q appartient à $\mathfrak{Q}$.

> On peut supposer que le déterminant des L_i est égal à 1 . On définit les vecteurs a_i par $L_i(x) = a_i . x$, $1 \le i \le n$. Posons $p = n-d$. Pour $T \in C(n, p)$, on pose $c_T = \sum_{i \in T} c_i$. Alors $\sum c_T = 0$ et $|c_T| \le p$. Soit $\Pi = \{x ; |a_i . x| \le Q^{c_i} , 1 \le i \le n\}$. On a alors

$$\Pi_p = \{x \in \Lambda^p \mathbb{R}^n ; |a_T . x| \le Q^{c_T} , T \in C(n, p)\} .$$

Comme plus haut on ordonne les T de sorte que l'on ait $\lambda_{T_1} \le \ldots \le \lambda_{T_k}$. Clairement, on peut prendre

$$T_k = \{n-p+1, \ldots, n\} = \{d+1, \ldots, n\} , \quad T_{k-1} = \{d, d+2, \ldots, n\} .$$

D'après le lemme 12 ,

$$\nu_k \ll \lambda_{d+1}\lambda_{d+2}\cdots\lambda_n \ll \nu_k , \quad \nu_{k-1} \ll \lambda_d\lambda_{d+2}\cdots\lambda_n \ll \nu_{k-1} ,$$

et (16) donne $\nu_{k-1} \ll \nu_k Q^{-\delta}$, soit $\nu_{k-1} < \nu_k Q^{-\delta/2}$ pour Q assez grand. On applique le lemme 10 aux vecteurs a_T , constantes c_T et à Π_p . (le fait que l'on ait seulement $|c_T| \le p$ n'a aucune importance). On conclut que si $v_1, \ldots v_k$ sont les points entiers de $\Lambda^p \mathbb{R}^n$ où les minima de Π_p sont atteints, le vecteur v_k^* est le même pour Q parcourant une partie $\mathfrak{Q}'$ non bornée de $\mathfrak{Q}$.

Soient $w_1, \ldots, w_n$ des points entiers de $\mathbb{R}^n$ où sont atteints les minima successifs de Π. Avec les notations du paragraphe précédent, on a

$$|a_S \cdot w_T| \ll \nu_\ell \, Q^{c_s} \quad \text{pour} \quad T \neq T_k \ ,$$

d'après le lemme 12. La majoration $\nu_{k-1} \ll \nu_k \, Q^{-\delta}$ montre que les w_T, $T \neq T_k$, appartiennent à l'espace engendré par $v_1, \ldots, v_{k-1}$. Donc $(w_{T_k})^*$ est proportionnel à v_k^*, où $(w_T)^* = (w^*)_T$ (lemme 11), soit

$$w_{d+1}^* \wedge \cdots \wedge w_n^* = \lambda \, v_k^* \neq 0 \ .$$

Soit S^* l'espace engendré par $w_{d+1}^*, \ldots, w_n^*$. La relation précédente montre que $x \in S^*$ si et seulement si $x \wedge v_k^* = 0$. Comme v_k^* est fixe pour $Q \in \mathfrak{Q}'$, S^* l'est aussi. D'où la conclusion avec S_d égal à l'orthogonal de S^*.<

COROLLAIRE. - Soient $L_1, \ldots, L_n$, $c_1, \ldots, c_n$, δ comme dans le théorème 6. Supposons qu'il existe un ensemble non borné de réels positifs Q tels que les inégalités

$$|L_j(x)| \leq Q^{c_j - \delta} \qquad (1 \leq j \leq n) \tag{17}$$

admettent une solution $x = x(Q)$ entière non nulle. Alors il existe un ensemble non borné de valeurs de Q pour lesquelles x appartient à un sous espace rationnel S_d fixe de dimension d, $1 \leq d < n$.

> Soit Q tel que (17) ait une solution entière non triviale. Soient

$w_1, \ldots, w_n$ des points entiers indépendants avec $w_i \in \lambda_i \Pi$ $(1 \le i \le n)$ et soit S_i l'espace engendré par $w_1, \ldots, w_i$. L'inégalité (17) implique $\lambda_1 \le Q^{-\delta}$ et donc $\lambda_\ell > 1$ pour $Q > Q_0$, ce qu'on supposera. Il existe donc $\delta_1 > 0$ et d, $1 \le d < n$, tels que $\lambda_d < \lambda_{d+1} Q^{-\delta_1}$. On a $x \in S_d$. D'où la conclusion, grâce au théorème.<

15. Le théorème fondamental.

Nous considérons des formes linéaires $L(x)$, $x = (x_1, \ldots, x_n)$, à coefficients réels ou complexes. Un système de telles formes $L_1, \ldots, L_t$ sera dit symétrique si en même temps qu'une forme L il contient la conjuguées complexe de L.

THEOREME 6. - Soit $L_1, \ldots, L_t$ un système symétrique de formes linéaires à coefficients algébriques. Soit $\eta > 0$. Alors les conditions suivantes sont équivalentes.

(a) Il existe une constante $c_1 = c_1(L_1, \ldots, L_t; \eta)$ et une infinité de points entiers x solutions de l'inégalité

$$|L_1(x) \ldots L_t(x)| \le c_1 |x|^{t-\eta}$$

(b) Il existe un sous espace rationnel S_d de $\mathbb{R}^n$, de dimension d $(1 \le d \le n)$, et un système symétrique $L_{i_1}, \ldots, L_{i_m}$ $(1 \le m \le t$, $i_1 < \ldots < i_m)$, dont la restriction à S_d a un rang égal à r avec

$$r \le d\, m/\eta \quad \text{et} \quad r < d .$$

> 1. Si le système contient une forme linéaire proportionnelle à une forme à coefficients réels R, d après le théorème I.4, pour $n \geq 2$ il existe une infinité de points x entiers qui vérifient $|R(x)| \ll |x|^{1-n}$ (où la constante impliquée par $\ll$ ne dépend que des L_i) et donc aussi $|L_1(x) \ldots L_t(x)| \ll |x|^{t-n}$. Dans le cas $n \geq 3$, on arrive à la même conclusion en considérant si nécessaire les parties réelles et imaginaires de deux formes conjuguées.

Si une des formes L_j du système s'annule en un point entier $\neq 0$ alors (a) a lieu pour tout η positif ainsi que (b) en prenant L_j ou $(L_j, \overline{L}_j)$ comme système symétrique, $r = 0$, et pour espace la droite rationnelle contenant x.

Si pour tout $x \neq 0$ entier on a $L_1(x) \ldots L_t(x) \neq 0$, alors pour $n = 1$ on a toujours $L_1(x) \ldots L_t(x) \gg |x|^t$, et ceci a encore lieu pour $n = 2$ si aucune des L_i n'est proportionnelle à une forme réelle. Dans ces deux cas (a) n'a jamais lieu et (b) non plus (en effet on a nécessairement $r = n$ et donc pas $r < d$).

Nous pouvons donc nous limiter à démontrer le théorème sous les hypothèses supplémentaires : aucune des formes L_j ne s'annule en un point entier non nul, on a $n \geq 2$ et même $n \geq 3$ si aucune des formes L_j n'est proportionnelle à une forme réelle, η vérifie $\eta > n$.

2. Démontrons l'implication (b) $\Rightarrow$ (a). Sans perte de généralité nous supposons que la condition (b) a lieu avec les formes $L_1, \ldots, L_m$. Les restrictions des parties réelles et imaginaires de ces formes à S_d ont

aussi un rang r, et sontdonc combinaisons de formes réelles $R_1, \ldots, R_r$. Supposons que les restrictions des formes $R_1, \ldots, R_r, X_{r+1}, \ldots, X_d$ à S_d soient indépendantes. D'après le théorème, pour tout Q positif, il existe x entier non nul dans S_d vérifiant

$$|R_i(x)| \ll Q^{r-d} \quad (1 \leq i \leq r) \quad \text{et} \quad |x_j| \leq Q^r \quad (r+1 \leq j \leq d),$$

ce qui implique $|x| \ll Q^r$ et

$$|L_1(x) \ldots L_m(x)| \ll R_1(x) \ldots R_m(x)\, L_{m+1}(x) \ldots L_t(x)$$
$$\ll |x|^{(m/r)(r-d)+t-m} \ll |x|^{t-\eta}.$$

En faisant croître Q on voit que cette inégalité a une infinité de solutions entières dans S_d.

3. Démontrons l'implication (a) $\Rightarrow$ (b) dans le cas où les formes linéaires considérées sont réelles.

Soit d le plus petit entier tel qu'il existe un espace rationnel S_d et une constante c pour lesquels l'inégalité

$$|L_1(x) \ldots L_t(x)| \leq c\, |x|^{t-\eta} \tag{18}$$

admette une infinité de solutions entières dans S_d. Le cas $d = 1$ est exclu puisqu'il implique l'existence de x entier non nul avec $L_1(x) \ldots L_t(x) = 0$. Sans perte de généralité on peut supposer que les solutions entières $x \in S_d$ de (18) vérifient

$$0 < |L_1(x)| \leq \ldots \leq |L_t(x)| .$$

Soit u le rang de la restriction des formes $L_1, \ldots, L_t$ à S_d. Soit i_1 le plus petit entier tel que L_{i_1} ne s'annule pas sur S_d, par hypothèse $i_1 = 1$. Soit i_2 le plus petit entier tel que le système (L_{i_1}, L_{i_2}) ait un rang 2 sur S_d ... Et ainsi de suite, jusqu'à i_u. Le produit $|L_1(x) \ldots L_t(x)|$ pour x dans S_d ne diffère de $|L_1(x)|^{i_2-1} |L_{i_2}(x)|^{i_3-i_2} \ldots |L_{i_{u-1}}(x)|^{i_u-i_{u-1}} |L_{i_u}(x)|^{t+1-i_u}$ que par un facteur positif borné inférieurement et supérieurement.

Supposons que $M_1 = L_1$, $M_2 = L_{i_2}, \ldots$, $M_u = L_{i_u}$, $M_{u+1} = X_{u+1}, \ldots, M_d = X_d$ soient indépendants sur S_d, soit $P(x)$ leur produit. A chaque x correspondent des réels $(p; p_1, \ldots, p_d)$ définis par $P(x) = |x|^p$, $M_j(x) = |x|^{p_j+(p/d)}$ $(1 \leq j \leq d)$. Soit $(q ; q_1, \ldots, q_d)$ un point limite des $(p ; p_1, \ldots, p_d)$. On a $q \leq d$, $q_1 + \ldots + q_d = 0$, $q_1 \leq \ldots \leq q_u$. Du fait que pour x dans S_d l'ordre de grandeur de $|x|$ est le même que celui de $\mathrm{Max}(|M_1(x)|, \ldots, |M_d(x)|)$, on a $\mathrm{Max}(q_1, \ldots, q_d) = 1-q/d$. Pour $\epsilon > 0$, il existe une infinité de nos points x qui vérifient

$$(19) \qquad |x|^{q_j+(q/d)-\epsilon} \leq |M_j(x)| \leq |x|^{q_j+(q/d)+\epsilon} , \quad 1 \leq j \leq d .$$

Montrons que l'on a $q \geq 0$. Supposons le contraire. Soit ϵ assez petit pour que l'on ait $\epsilon+(q/d) < 0$. La somme des exposants dans le terme droit de (19) est alors négative. Le corollaire du théorème 5 s'applique et contredit la définition de d.

De (18) et (19) on déduit l'encadrement

$$|x|^{H+(tq/d)-t\varepsilon} \ll |L_1(x) \dots L_t(x)| \ll |x|^{t-\eta} ,$$

où

$$H = q_1(i_2-1)+q_2(i_3-i_2) + \dots + q_u(t+1-i_u) .$$

Ainsi H vérifie

$$H \leq t-\eta - (tq/d) + t\varepsilon .$$

D'après ce qui précède on a aussi

(20) $\quad q_1 + \dots + q_u + (d-u) \geq 0 \quad$ et $\quad q_1 \leq \dots \leq q_u \leq 1 .$

D'après le lemme 13 ci-dessous (avec $a = d-u$, $a_1 = i_2-1$, $a_2 = i_3-i_2, \dots,$ $a_u = t+1-i_u$) , la fonction $H(q_1,\dots,q_u)$ où les q_i vérifient les contraintes (20) atteint son minimum en un point qui vérifie $q_1 + \dots + q_u + (d-u) = 0$ avec $q_1 = \dots = q_r < q_{r+1} = \dots = q_u = 1$ pour un certain r , $1 \leq r \leq u$. Posons $q_1 = \dots = q_r = z$, alors $z = 1-(d/r)$. On a donc

$$z(i_{r+1}-1)+(t+1-i_{r+1}) \leq H \leq t-\eta+t\varepsilon \quad (\text{où } i_{r+1} = t+1 \text{ lorsque } r = u) ,$$

ce qui implique

(21) $\qquad d(i_{r+1}-1)/r \geq \eta-t\varepsilon .$

Nous allons montrer que l'on a $u < d$. Supposons $u = d$. Nous savons que

$$q_1 + \ldots + q_u = 0 \quad \text{et} \quad q_1 \leq \ldots \leq q_u = 1-(q/d) .$$

Une variante du lemme 13 montre que le minimum de H pour des q_i vérifiant les conditions ci-dessus est atteint en un point tel que $q_1 = \ldots = q_r \leq q_{r+1} = \ldots = q_u = 1-(q/d)$ pour un certain r vérifiant $1 \leq r < u$. Posons à nouveau $q_1 = \ldots = q_r = z$, on a $z = 1-(d/r)-(q/d)+(q/r)$ et

$$z(i_{r+1}-1) + (1-(q/d))(t+1-i_{r+1}) \leq H \leq t-\eta-(tq/d)+t\varepsilon \quad .$$

On en déduit l'inégalité

$$t(1-(q/d)) - ((d/r) - (q/r))\,(i_{r+1}-1) \leq t(1-q/d))-\eta+t\varepsilon \ ,$$

qui jointe à $q \geq 0$ contredit (21).

Il existe donc $r < d$ tel que (21) ait lieu. Posons $m = i_{r+1}-1$. Considérons les m formes $L_1, \ldots, L_m$. Elles ont un rang r sur S_d, avec $md/r \geq \eta-t\varepsilon$. A chaque $\varepsilon > 0$ assez petit on peut faire correspondre de tels r, m, et m formes linéaires extraites de $L_1, \ldots, L_t$ qui possèdent ces propriétés, et une infinité de ces choix coïncident, d'où le théorème dans le cas de formes réelles.

4. Démontrons enfin l'implication (a) $\Rightarrow$ (b) dans le cas où le système contient des formes complexes. Nous écrirons $L = L^R + i\,L^I$ la décomposition en partie réelle et partie imaginaire d'une forme linéaire.

Soit donc un système $L_1, \ldots, L_t$ symétrique vérifiant la condition (a). Choisissons d et c_2 comme précédemment. On a encore $d \geq 2$ et on considère encore une infinité de solutions entières x de (18) qui vérifient $0 < |L_1(x)| < \ldots < |L_t(x)|$. Sans perte de généralité, on peut supposer que ces points vérifient $|L_i^R(x)| \geq |L_i^I(x)|$ et $L_i^R(x)\, L_i^I(x) \geq 0$. Nous définissons alors des formes M_i de la manière suivante : $M_i = L_i$ si L_i est réelle ; sinon, si L_i et L_{i+1} sont complexes conjugués (une telle numérotation est possible !), $M_i = L_i^R$ et $M_{i+1} = L_i^R + L_i^I$ ou $M_i = L_i^R + L_i^I$ et $M_{i+1} = L_i^R$ (ce choix va être précisé plus loin), en tout cas $|L_i(x)|$ $(= |L_{i+1}(x)|)$, $|M_i(x)|$ et $|M_{i+1}(x)|$ ont le même ordre de grandeur. Nous posons $M_i = L_i^R$ et $M_{i+1} = L_i^R + L_i^I$ à moins que L_i^R soit sur S_d une combinaison linéaire des $L_1, \ldots, L_{i-1}$ sans que L_i^I le soit. Sinon nous posons $M_i = L_i^R + L_i^I$ et $M_{i+1} = L_i^R$. Avec ce choix lorsque M_{i+1} sur S_d est indépendant de $M_1, \ldots, M_i$ alors M_i sur S_d est indépendant de $M_1, \ldots, M_{i-1}$.

Soit u le rang des $L_1, \ldots, L_t$ sur S_d. Le rang de $M_1, \ldots, M_t$ sur S_d est aussi égal à u. On définit $M_{i_1}, \ldots, M_{i_u}$ de même que $L_{i_1}, \ldots, L_{i_u}$ plus haut $(i_1 = 1)$. On a

$$|L_1(x) \ldots L_t(x)| \gg\ll |M_1(x) \ldots M_t(x)|$$
$$\gg\ll |M_1(x)|^{i_2 - 1} |M_{i_2}(x)|^{i_3 - i_2} \ldots |M_{i_{u-1}}(x)|^{i_u - i_{u-1}} |M_{i_u}(x)|^{t+1-i_u}$$

(où $A \gg\ll B$ signifie $A \ll B$ et $B \ll A$). On peut choisir ε assez petit pour que l'on ait $\eta - t\varepsilon > n$ (on a $\eta > n$). L'étude précédente montre qu'il existe r, $1 \leq r \leq u$, $r < d$, tel que (21) ait lieu (avec

$i_{r+1} = t+1$ si $r = u$). Si $m = i_{r+1}-1$, les formes $M_1,\dots,M_m$ ont un rang r sur S_d avec $m\,d/r \geq \eta - t\varepsilon > n$ et donc $m > r \geq 1$. Nous considérons trois cas :

(i) Le système $L_1,\dots,L_m$ est symétrique ; il a un rang r sur S_d, $r < d$, $m\,d/r \geq \eta - t\varepsilon$.

(ii) Le système $L_1,\dots,L_m$ n'est pas symétrique et M_{m+1} sur S_d dépend linéairement de $M_1,\dots,M_m$. Dans ce cas $M_1,\dots,M_{m+1}$ a un rang r sur S_d, le système $L_1,\dots,L_{m+1}$ est symétrique, a un rang r sur S_d avec $r < d$ et $(m+1)d/r > \eta - t\varepsilon$.

(iii) Le système $L_1,\dots,L_m$ n'est pas symétrique et M_{m+1} est indépendant de $M_1,\dots,M_m$ sur S_d. Dans ce cas M_m sur S_d est linéairement indépendant de $M_1,\dots,M_{m-1}$. Le rang de $M_1,\dots,M_{m-1}$ et celui de $L_1,\dots,L_{m-1}$ sur S_d sont égaux à $r-1$. On a alors $r \geq 2$ et $m > r$, ce qui implique $(m-1)\,d/(r-1) \geq m\,d/r \geq \eta - t\varepsilon$. Le système $L_1,\dots,L_{m-1}$ est symétrique, a un rang $r-1$ sur S_d, avec $r-1 < d$ et $(m-1)d/(r-1) \geq \eta - t\varepsilon$.

On conclut comme dans le cas réel. <

LEMME 13. - Soient $a, a_1,\dots,a_u$ des nombres réels positifs ou nuls. Alors la fonction $H(x_1,\dots,x_u) = a_1x_1 + \dots + a_ux_u$, pour des x_i vérifiant $x_1 + \dots + x_u + a \geq 0$ et $x_1 \leq \dots \leq x_u \leq 1$, atteint son mini-

mum en un point tel que l'on ait $x_1 + \ldots + x_u + a = 0$ et $x_1 = \ldots = x_r < x_{r+1} = \ldots = x_u = 1$ pour un certain r, $1 \leq r \leq u$.

> Il est clair que H atteint son minimum en un point de l'hyperplan $x_1 + \ldots + x_u + a = 0$. Les conditions $x_1 \leq \ldots \leq x_u \leq 1$ et $x_1 + \ldots + x_u + a = 0$ définissent un polytope de dimension $u-1$. Le minimum de H est atteint en point extrémal et ce polytope, d'où la conclusion.<

16. Preuves des théorèmes 3 et 4.

1. Considérons d'abord le théorème 3. Il est clair qu'il suffit de considérer le cas où les nombres algébriques $\alpha_1, \ldots, \alpha_n$ sont réels. Soient les formes linéaires $L_j = \alpha_j X_{n+1} - X_j$ pour $j = 1, \ldots, n$. Le théorème 3 sera démontré si pour $\eta = n+1+(\epsilon/2)$ on prouve que la condition a) du théorème 6 n'a pas lieu ou encore que b) n'a pas lieu. Il suffit tout simplement de vérifier que les formes linéaires $L_1, \ldots, L_n$ sont linéairement indépendantes, ce qui résulte directement de l'indépendance linéaire sur les rationnels des nombres $1, \alpha_1, \ldots, \alpha_n$.

2. Pour démontrer le théorème 4 on peut encore supposer $\alpha_1, \ldots, \alpha_n$ réels. On considère cette fois les formes linéaires $L_1 = X_1$, $L_2 = X_2, \ldots, L_n = X_n$, $L_{n+1} = \alpha_1 X_1 + \ldots + \alpha_n X_n - X_{n+1}$. Soit $\eta = n+1+(\epsilon/2)$. Grâce au théorème 6 il suffit de montrer que la condition b) n'a pas lieu, ce qui résulte à nouveau de l'indépendance de $1, \alpha_1, \ldots, \alpha_n$ sur $\mathbb{Q}$.

17. Un théorème sur les formes normiques.

Nous appelons forme normique une expression de la forme

$$N(x_1, \ldots, x_n) = \mathfrak{N}(\alpha_1 x_1 + \ldots + \alpha_n x_n) ,$$

où les x_i parcourent les entiers rationnels et où $\alpha_1, \ldots, \alpha_n$ sont des éléments fixés d'un corps de nombres K, $\mathfrak{N}$ désignant la norme de K sur $\mathbb{Q}$.

Soit k le degré de K. Il existe k isomorphismes de K dans $\mathbb{C}$, nous notons $\beta^{(1)}, \ldots, \beta^{(k)}$ les images d'un élément β de K par ces différents isomorphismes. Posons

$$M(x) = \alpha_1 x_1 + \ldots + \alpha_n x_n ,$$

alors $$N(x) = \mathfrak{N}(M(x)) = M^{(1)}(x) \ldots M^{(k)}(x) ,$$

où

$$M^{(i)}(x) = \alpha_1^{(i)} x_1 + \ldots + \alpha_n^{(i)} x_n \qquad (i = 1, \ldots, k) .$$

Grâce au théorème de Minkowski sur les formes linéaires on voit facilement qu'en dehors des cas $n = 1$ ou $n = 2$ et $M^{(1)}, \ldots, M^{(k)}$ conjuguées par paires (sur $\mathbb{C}$), il existe une infinité de points entiers x vérifiant

$$|N(x)| \leq C|x|^{k-n}$$

pour une constante C convenable. Le théorème ci-dessous montre que, sous certaines hypothèses, cet exposant est le meilleur possible.

Soit ω un élément primitif de K et $K^* = Q(\omega^{(1)}, \ldots, \omega^{(k)})$ la fermeture galoisienne de K. Soit G le groupe de Galois de K^*, on dit que K est h fois transitif si G opérant sur l'ensemble $\{\omega^{(1)}, \ldots, \omega^{(k)}\}$ est h fois transitif, c'est-à-dire si pour toute suite $(\omega^{(i_1)}, \ldots, \omega^{(i_h)})$ de h éléments distincts de $\{\omega^{(1)}, \ldots, \omega^{(k)}\}$ il existe un élément φ de G tel que $\varphi(\omega^{(1)}) = \omega^{(i_1)}, \ldots, \varphi(\omega^{(h)}) = \omega^{(i_h)}$. On vérifie que cette définition ne dépend pas du choix de ω.

THEOREME 7. - Soit $M(x) = \alpha_1 x_1 + \ldots + \alpha_n x_n$ une forme linéaire à coefficients dans un corps K qui est $n-1$ fois transitif et telle que n conjugués quelconques $M^{(i_1)}, \ldots, M^{(i_n)}$ de M sont linéairement indépendants. Alors, pour tout ϵ positif, il existe seulement un nombre fini de points entiers x tels que

$$\mathfrak{N}(M(x)) \leq |x|^{k-n-\epsilon},$$

où $\mathfrak{N}$ désigne la norme de K sur $\mathbb{Q}$.

Il est facile de vérifier que ce théorème contient comme cas particulier le théorème du chapitre III.

COROLLAIRE. - Soient M comme dans le théorème, $N(x) = \mathfrak{N}(M(x))$, et $P(x)$ un polynôme de degré total plus petit que $k-n$. Alors l'équation diophantienne

$$N(x) = P(x)$$

n'admet qu'un nombre fini de solutions.

Preuve du théorème.

> Il est facile de voir que l'hypothèse du théorème implique que le rang d'un système de m formes distinctes $M^{(i)}$ est égal à $\min(n, m)$. Soit S_d un sous espace rationnel de dimension d et soit r le rang de la restriction de m formes $M^{(i)}$ distinctes. Nous allons montrer que l'on a

$$r = \min(d, m) .$$

Il est clair que le membre de droite majore r. L'égalité a lieu pour $m \geq n$ puisque dans ce cas le rang sur $\mathbb{R}^n$ de la famille des $M^{(i)}$ est égal à n. Supposons donc $m < n$. Du fait que K est m fois transitif r est égal au rang de la restriction à S^d de toute famille $M^{(e_1)}, \ldots, M^{(e_m)}$ pour $e_1 < \ldots < e_m$. Si ce rang est plus petit que m, il en résulte qu'il est égal au rang de la restriction à S^d de la famille $M^{(1)}, \ldots, M^{(k)}$, c'est-à-dire à d.

Supposons maintenant que l'inégalité du théorème ait une infinité de solutions. On applique le théorème 6 au formes $M^{(1)}, \ldots, M^{(k)}$ avec $\eta = n+\epsilon$. D'où l'existence d'un sous espace rationnel non nul S_d de $\mathbb{R}^n$ de dimension d, et d'une famille de formes $M^{(i_1)}, \ldots, M^{(i_m)}$ dont la restriction à S_d à un rang r qui vérifie $r \leq d\, m/(n+\epsilon)$ et $r < d$, donc $r < \min(d, m)$. Contradiction.<

APPENDICE

1. Le lemme de Gauss.

Il s'agit du résultat suivant.

THEOREME 1. - Soient P et Q deux polynômes non nuls en n variables $X_1, \ldots, X_n$ et à coefficients entiers. Si on note $\mathrm{cont}(R)$ le p.g.c.d. des coefficients d'un tel polynôme R, alors

$$\mathrm{cont}(PQ) = \mathrm{cont}(P) \cdot \mathrm{cont}(Q) \ .$$

> Il est clair qu'il suffit de prouver ce résultat lorsque les quantités $\mathrm{cont}(P)$ et $\mathrm{cont}(Q)$ sont égales à 1. De même que pour le lemme III. 3, une transformation du type $X_i \mapsto X^{g^{i-1}}$ $(i = 1, \ldots, n)$ pour un entier g assez grand permet de se ramener au cas d'une seule variable. Posons

$$P(X) = \sum_{i=0}^{k} a_h X^h \ , \quad Q(X) = \sum_{j=0}^{k} b_h X^h \ .$$

Soit maintenant p un nombre premier quelconque. Par hypothèse p ne divise ni tous les a_h ni tous les b_h. Soit alors i (resp. j) le plus petit indice tel que p ne divise pas a_h (resp. b_h), alors le coefficient du terme degré $(i+j)$ du produit PQ est congru à $a_i b_j$ modulo p, donc il n'est pas divisible par p [nous avons redémontré que l'anneau $\mathbb{F}_p[X_1, \ldots, X_n]$ est intègre !]. Ainsi p ne divise pas $\mathrm{cont}(PQ)$. D'où la conclusion. <

COROLLAIRE 1. - Soient deux polynômes $P(X_1,\ldots,X_n)$ et $Q(X_1,\ldots,X_n)$ à coefficients rationnels. Si les coefficients de PQ et de P sont entiers alors ceux de Q le sont aussi lorsque $\mathrm{cont}(P)$ est égal à 1.

> Soit t un entier positif tel que tQ soit à coefficients entiers. D'après le théorème et la relation $\mathrm{cont}(P) = 1$, on a $t\,\mathrm{cont}(PQ) = \mathrm{cont}(tPQ) = \mathrm{cont}(P)\,\mathrm{cont}(tQ) = \mathrm{cont}(tQ)$, ce qui montre que t divise les coefficients de tQ. Donc Q est à coefficients entiers. <

COROLLAIRE 2. - Soient deux polynômes $P(X_1,\ldots,X_n)$ et $Q(X_1,\ldots,X_n)$ à coefficients rationnels. Alors si le produit PQ est à coefficients entiers il existe un entier positif k tel que les polynômes kP et $k^{-1}Q$ soient à coefficients entiers.

> Soit k le plus petit entier tel que kP soit à coefficients entiers. Alors $\mathrm{cont}(kP) = 1$. On conclut grâce au corollaire précédent. <

2. Géométrie des nombres.

1. Les résultats qui suivent concernent la présence de points à coordonnées entières dans certains domaines de l'espace euclidien $\mathbb{R}^n$.

Soit R un sous-ensemble de $\mathbb{R}^n$, pour λ réel on désigne par λR l'ensemble des points λx où x parcourt R ; R est dit symétrique si $-R = R$. Si, pour tout $\lambda \in [0, 1]$, R contient $\lambda R + (1-\lambda)R$ on dit que R est convexe.

THEOREME 1 (Blichfeldt). - Soit R une région mesurable (pour la mesure de Lebesgue μ) de $\mathbb{R}^n$ vérifiant $\mu(R) > 1$. Il existe alors deux points de R dont la différence est à coordonnées entières.

> A tout point u à coordonnées entières associons l'ensemble

$$S_u = \{x = (x_1, \ldots, x_n) \; ; \; 0 \leq x_i < 1 \text{ pour } i = 1, \ldots, n \text{ et } x+u \in R\} .$$

Les ensembles $u+S_u$ constituent une partition de R, par conséquent

$$\sum_{u \in \mathbb{Z}^n} \mu(S_u) = \sum \mu(u+S_u) > 1 .$$

Mais l'union des S_u étant contenue dans un cube de côté 1 a un volume au plus égal à 1. Il s'ensuit qu'il existe un point commun à deux ensembles S_u et $S_{u'}$ $(u \neq u')$; autrement dit il existe deux points x et y de R vérifiant $x-y = u-u'$, d'où le résultat. <

THEOREME 2 (Minkowski) . - Toute région convexe et symétrique de $\mathbb{R}^n$ dont la mesure de Lebesgue est plus grande que 2^n contient un point à coordonnées entières autre que l'origine.

> Soit R une telle région. Le domaine $\frac{1}{2}R$ a un volume supérieur à 1. D'après le théorème précédent il existe deux points distincts x et x' de $\frac{1}{2}R$ dont la différence u est à coordonnées entières. On conclut en vérifiant que u appartient à R. En effet, $-2x' \in R$ (symétrie de R) et $u = \frac{1}{2}(2x) + \frac{1}{2}(-2x') \in R$ (convexité de R). <

Un raisonnement simple, laissé au lecteur, conduit au résultat suivant.

COROLLAIRE (Minkowski). - Toute région compacte convexe et symétrique de $\mathbb{R}^n$ dont la mesure de Lebesgue est au moins égale à 2^n contient un point à coordonnées entières autre que l'origine.

2. Introduisons maintenant la notion de minima successifs. Dans toute la suite R désignera un domaine compact symétrique et convexe. Pour λ positif assez petit l'ensemble λR ne contient aucun point de $\mathbb{Z}^n$ autre que l'origine tandis que pour λ assez grand cet ensemble contient une base de $\mathbb{Z}^n$. Ces remarques justifient la définition suivante : pour $i = 1, \ldots, n$ on pose

$$\lambda_i = \inf \{\lambda ; \lambda > 0 , \text{ rang } (\lambda R \cap \mathbb{Z}^n) \geq i\} .$$

Les nombres λ_i sont appelés les minima successifs de R. Ils vérifient

$$0 < \lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_n .$$

Du fait que R est compact, λR contient i points linéairement indépendants de $\mathbb{Z}^n$ pour $\lambda = \lambda_i$, mais ceci n'a pas lieu pour $\lambda < \lambda_i$. D'où l'existence de n points linéairement indépendants $x_1, \ldots, x_n$ à coordonnées entières tels que $x_i \in \lambda_i R$ $(i = 1, \ldots, n)$.

Le théorème 2 équivaut à la majoration $\lambda_1^n \mu(R) \leq 2^n$. Le théorème fondamental suivant renforce considérablement ce résultat.

THEOREME 3 (Minkowski). - Les minima successifs d'un convexe compact symétrique R vérifient

$$2^n/n! \leq \lambda_1 \cdots \lambda_n \mu(R) \leq 2^n \ .$$

> Il n'existe pas encore de démonstration simple de l'inégalité de droite, nous l'admettrons donc (voir, par exemple, [10], appendix B). Par contre l'inégalité de gauche est presque triviale : soient $x_1, \ldots, x_n$ des points définis comme ci-dessus, alors R contient l'enveloppe convexe E de ces points et on a donc

$$\mu(R) \geq \mu(E) = \frac{2^n |\mathrm{Det}(x_1, \ldots, x_n)|}{n! \lambda_1 \cdots \lambda_n} \geq \frac{2^n}{n! \lambda_1 \cdots \lambda_n} \ .<$$

L'inégalité ci-dessus, jointe à la majoration de $\lambda_1 \cdots \lambda_n$ fournie par le théorème, fournit le résultat suivant.

COROLLAIRE. - <u>Soient</u> $x_1, \ldots, x_n$ <u>des points à coordonnées entières de</u> $\lambda_n R$ <u>qui sont linéairement indépendants, on a alors</u>

$$|\det(x_1, \ldots, x_n)| \leq n! \ .$$

BIBLIOGRAPHIE

[1] BAKER A. - Continued fractions of transcendental numbers, Mathematika, t. 9, 1962, p. 1-8.

[2] BAKER A. - Rational approximations to certain algebraic numbers, Proc. London Math. Soc., t. 14, fasc. 3, 1964, p. 385-398.

[3] BAKER A. - Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers, Quart. J. Math. Oxford Ser., t. 15, fasc. 2, 1964, p. 375-383.

[4] BAKER A. - Simultaneous rational approximations to certain algebraic numbers, Proc. Camb. Phil. Soc., t. 63, 1967, p. 693-702.

[5] BAKER A. - Contributions to the theory of diophantine equations (I). On the representations of integers by binary forms, Phil. Trans. Royal Soc. London, ser. A, t. 263, p. 173-191.

[6] BAKER A. - Effective methods in diophantine problems, Proc. of Symp. in Pure Math. XX, (1969 Number Theory Institute), New-York, 1971, p. 195-205.

[7] BAKER A. - Effective methods in diophantine problems (II), Proc. of Symp. in Pure Math. XXIV (Analytic Number Theory), 1973, p. 1-7.

[8] BAKER A. - A sharpening of the bounds for linear forms in logarithms (II), Acta Arithm., t. 24, 1973, p. 33-36.

[9] BOREL E. - Contribution à l'analyse arithmétique du continu, J. de Math. pures et appl., t. 9, fasc. 5, 1903, p. 329-375.

[10] CASSELS J. W. S. - An introduction to diophantine approximation, Cambridge Tracts, n. 45, 1957, Cambridge University Press.

[11] CIJSOUW P. L. - Transcendance measures, thèse, University of Amsterdam, 1972.

[12] COATES J. - An effective p-adic analogue of a theorem of Thue, Acta Arithm., t. 15, 1969, p. 279-305.

[13] COATES J. - Notes on diophantine approximations. Classicaly effective methods in diophantine Analysis, course at Harvard University, 1969/70.

[14] CUGIANI M. - Sulla approssimabilita dei numeiri algebrici mediante numeiri razionali, Ann. Mat. Purs Appl., t. 48, fasc. 4, 1959, p. 135-145.

[15] DAVENPORT H. - A note on Thue's theorem, Mathematika, t. 15, 1968, p. 76-87.

[16] DAVENPORT H. et ROTH K. F. - Rational approximations to algebraic numbers, Mathematika, t. 2, 1955, p. 160-167.

[17] DIRICHLET L. G. P. - Verrallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen, S. B. Preuss. Akad. Wiss., 1842, p. 93-95.

[18] DUBOIS E. et RHIN G. - Théorème de W. M. Schmidt en g^*-adique, Séminaire de théorie des nombres, Caen, 1974.

[19] DYSON F. J. - The approximation to algebraic numbers by rationals, Acta Math., t. 79, 1947, p. 225-240.

[20] ELLISON W. J. - Diophantine equations, Cours à Bordeaux, 1971/72.

[21] FELDMAN N. I. - An effective refinement of the exponent in Liouville's theorem, Math. USSR Izvestija, t. 5, 1971, p. 985-1000, (en russe), Izv. Akad. Nauk SSSR, Ser. Mat., t. 35, 1971, p. 973-990.

[22] GEL'FOND A.O. - Transcendental and algebraic numbers, New-York, Dover Publications, 1960, (en russe) Moskva, Edition d'Etat de Littérature technique 1952.

[23] GUTING R. - Approximation of algebraic numbers by algebraic numbers, Mich. Math. J., t. 8, 1961, p. 149-159.

[24] GUTING R. - Polynomials with multiple zeroes, Mathematika, t. 14, p. 181-196.

[25] HARDY G.H. et WRIGHT E.M. - The Theory of Numbers, 4° edition, 1960, Oxford at the Clarendon Press.

[26] KASCH F. - Zur Annäherung algebraischer Zahlen durch arithmetisch charakterisierte rationale Zahlen, Math. Nachr., t. 10, 1953, p. 85-98.

[27] KOKSMA J.F. - Diophantische Approximationen, Ergebnisse d. Math. u. Grenzgeb., n. 4, 1936, Springer Verlag, Berlin.

[28] LANDAU E. - Sur quelques théorèmes relatifs aux zéros des fonctions analytiques, Bull. Soc. Math. France, t. 33, 1905, p. 251-261.

[29] LANG S. - Diophantine Geometry, Interscience tracts in pure and applied math., n. 11, 1962, J. Wiley & Sons, New-York, London.

[30] LANG S. - Introduction to diophantine approximations, 1966, Addison Wesley Publi. Co., Reading Massachussets.

[31] LEVEQUE W.J. - Topics in number theory, 1955, Addison-Wesley Publ. Co., Reading Massachussets.

[32] LIOUVILLE J. - Sur des classes très étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques, C. r. Acad. Sci., Paris, t. 18, p. 883-885 et 910-911, 1844.

[33] MAHLER K. - Zur Approximation algebraischer Zahlen (II). Uber die Anzahl der Darstellungen ganzer Zahlen durch binäre Formen, Acta Math., t. 62, 1933, p. 91-166.

[34] MAHLER K. - Ein Analogon zu einem Schneiderschen Satz, Neder. Akad. Wetensch. Proc., t. 39, 1936, p. 633-640 et 729-737.

[35] MAHLER K. - Lectures on diophantine approximation, 1961, Notre Dame University.

[36] MAHLER K. - On the approximation of algebraic numbers by algebraic integers, J. Austral. Math. Soc., t. 3, 1963, p. 408-434.

[37] MAHLER K. - Lectures on transcendental numbers, Lecture Notes, n° 546, 1976, Springer Verlag, Berlin.

[38] MARKOV A. - Sur les formes quadratiques binaires indéfinies, Math. Ann., t. 15, 1879, p. 381-409.

[39] MASSER D. - Elliptic Functions and Transcendence, Lecture Notes in Math., n° 437, 1975, Springer-Verlag, Berlin.

[40] MIGNOTTE M. - Critères d'irréductibilité de polynômes sur un corps de nombres, Enseignement Math., t. 18, 1972, p. 191-200.

[41] MIGNOTTE M. - Une généralisation d'un théorème de Cugiani-Mahler, Acta Arithm., t. 22, 1972, p. 57-67.

[42] MIGNOTTE M. - An inequality about factors of polynomials, Math. of Comp. t. 28, 1974, p. 1-5.

[43] MIGNOTTE M. - Quelques remarques sur l'approximation rationnelle des nombres algébriques, Grelles J., t. 262/63, 1974, p. 341-347.

[44] MIGNOTTE M. - Sur la résolution de systèmes linéaires en nombres entiers, Séminaire DELANGE-PISOT-POITOU, G. E., 1973/74, n° G16, 5 p. .

[45] MIGNOTTE M. - Approximation des nombres algébriques par certaines suites de rationnels, Rendiconti di Palermo (à paraître, 35 p.).

[46] MIGNOTTE M. - Sur les multiples des polynômes irréductibles, Bull. Soc. Math. de Belgique, t. 27, 1975, p. 95-99.

[47] MIGNOTTE M. - Démonstration probabiliste d'un lemme combinatoire pour l'approximation diophantienne des nombres algébriques, Colloquium Math., t. 30, 1974, p. 109-119.

[48] MIGNOTTE M. - A characterization of integers, (à paraître, Am. Math. Monthly).

[49] MIGNOTTE M. - WALDSCHMIDT M. - Approximation des valeurs de fonctions transcendantes, Indag. Math., t. 37, 1975, p. 213-223.

[50] NIVEN I. - Diophantine Approximations, Interscience tracts in pure and applied Math., n° 14, 1963, J. Wiley & Sons, New-York - London.

[51] PARRY C. J. - The p-adic generalisation of the Thue-Siegel theorem, J. London Math. Soc., t. 15, 1940, p. 293-305.

[52] PARRY C. J. - The β-adic generalisation of the Thue-Siegel theorem, Acta Math., t. 83, 1950, p. 1-100.

[53] PATHIAUX M. - Sur les multiples des polynômes irréductibles associés à certains nombres algébriques, Séminaire DELANGE-PISOT-POITOU, 1972/73, n° 13, 9 p. .

[54] PISOT CH. - Répartition (mod. 1) des puissances successives des nombres réels, Comm. Math. Helv., 19, 1946, 153-159.

[55] POITOU G. - Sur l'approximation des nombres complexes par les nombres des corps imaginaires quadratiques dénués d'idéaux non principaux, particulièrement lorsque vaut l'algorithme d'Euclide, Ann. Sci. Ecole Norm. Sup., t. 70, fasc. 3, 1953, p. 199-265.

[56] RAMACHANDRA K. - Approximation of algebraic numbers, Nach. d. Akad. d. Wiss. in Göttingen, Math. Phys. Kl., 1966, p. 45-52.

[57] RAUZY G. - Approximation rationnelle des nombres algébriques, cours polycopié, Paris.

[58] RIDOUT D. - Rational approximations to algebraic numbers, Mathematika, t. 4, 1957, p. 125-131.

[59] RIDOUT D. - The p-adic generalization of the Thue-Siegel-Roth Theorem, Mathematika, t. 5, 1958, p. 40-48.

[60] ROTH K. F. - Rational approximation to algebraic numbers, Mathematika, t. 2, 1955, p. 1-20.

[61] SCHINZEL A. - Review of a paper by Hyyrö, Zentralblatt Math., t. 137, 1967, p. 257-258.

[62] SCHINZEL A. - An improvement of Runge's Theorem on diophantine equations, Commentarii Pontif. Acad. Soc. 2, n° 20, 1968.

[63] SCHINZEL A. - On two theorems of Gel'fond and some of their applications, Acta Arith., t. 13, 1967, p. 177-236.

[64] SCHLICKEWEI H. P. - On the fractional parts of the sum of powers of rational numbers, Mathematika, t. 22, 1975, p. 154-155.

[65] SCHLICKEWEI H. P. - Linearformen mit algebraischen Koeffizienten, Manuscripta math., t. 18, 1976, p. 147-185.

[66] SCHLICKEWEI H. P. - Die p-adische Verallgemeinerung des Satzes von Thue-Siegel-Roth-Schmidt, J. f. d. Reine u. Angew. Math. (à paraître).

[67] SCHLICKEWEI H. P. - On norm formeequations, J. Number Th. (à paraître).

[68] SCHLICKEWEI H. P. - On products of special linear forms with algebraic coefficients, Acta Arith., t. 31 (à paraître).

[69] SCHLICKEWEI H. P. - Über die diophantische Gleichung $x_1+x_2+\ldots+x_n = 0$, Acta Arith., t. 33 (à paraître).

[70] SCHMIDT W. M. - Zur simultanen Approximation algebraischer Zahlen durch rationale, Acta Math., t. 114, 1965, p. 159-209.

[71] SCHMIDT W. M. - On simultaneous approximation of two algebraic numbers by rationals, Acta Math., t. 119, 1967, p. 27-50.

[72] SCHMIDT W. M. - Simultaneous approximation to algebraic numbers by rationals, Acta Math., t. 125, 1970, p. 189-201.

[73] SCHMIDT W. M. - Linear forms with algebraic coefficients I , J. Number Th., t. 3, 1971, p. 253-277.

[74] SCHMIDT W. M. - Linearformen mit algebraischen Koeffizienten II, Math. Ann., t. 191, 1971, p. 1-20.

[75] SCHMIDT W. M. - Norm form equations, Annals of Math., t. 96, 1972, p. 526-551.

[76] SCHMIDT W. M. - Simultaneous approximation to algebraic numbers by elements of a number field, Monat. für Math., t. 79, 1975, p. 55-66.

[77] SCHMIDT W. M. - Approximation to algebraic numbers, Monographie n° 19 de l'Enseignement Mathématique, 1972, Genève.

[78] SCHNEIDER TH. - Über die Approximation algebraischen Zahlen, J. Reine angew. Math., t. 175, 1936, p. 182-192.

[79] SCHNEIDER TH. Zur Annäherung der algebraischen Zahlen durch rationale, J. Reine angew. Math., t. 188, 1950, p. 115-128.

[80] SCHNEIDER TH. - Einführung in die transzendenten Zahlen, Grundlehren 81, 1956, Springer Verlag, Berlin-Göttingen-Heidelberg ; traduction française, Introduction aux Nombres Transcendants, 1959, Gauthier-Villars, Paris.

[81] SIEGEL C. L. - Approximation algebraischer Zahlen, Math. Zeitschr., t. 10, 1921, p. 173-213.

[82] SIEGEL C. L. - Über Naherrungswerte algebraischer Zahlen, Math. Ann., t. 84, 1921, p. 80-99.

[83] SIEGEL C. L. - Über einige Anwendungen diophantisches Approximation, Abh. d. Preuss Akad. d. Wiss., Math. Phys., Nr. 1, 1929.

[84] SIEGEL C. L. - Die Gleichung $ax^n - by^n = c$, Math. Ann., t. 114, 1937, p. 57-88.

[85] SIEGEL C. L. - Eine Erläuterungen zu Thues Untersuchen über Annäherungswerte algebraischer Zahlen und diophantische Gleichungen, Nachr. Akad. Wiss. Göttingen, Math. Phys. Kl., Nr. 8, 1970.

[86] SPRINDZUCK V. G. - An effective estimate of rational approximations to algebraic numbers (en russe), Dokl. Akad. Nauk Belorusskoj SSR, t. 14, fasc. 8, 1970, p. 681-684.

[87] SPRINDZUCK V. G. - Rational approximations to algebraic numbers (en russe), Isvestia Akad. Nauk SSR, t. 5, 1971.

[88] SPRINDZUCK V. G. - An improvement of the estimate to rational approximations to algebraic numbers (en russe), Dokl. Akad. Nauk Belorusskoy SSR, t. 15, fasc. 2, 1971, p. 101-104.

[89] STEPANOV S. A. - The approximation of an algebraic number by algebraic numbers of a special form (en russe), Vesnik Moskov. Univ., Ser. I, Math. Meh., t. 22, fasc. 6, 1967, p. 78-86.

[90] THUE A. - Bermerkungen über gewisse Näherungsbrüche algebraischer Zahlen. Über Annäherungswerte der reelen Wurzel der ganzen Funktion dritten Grades $x^3 - ax - b$. On en general i store hele tal ulsbar ligning. Skrifter udgivne of Videnskabs-Selskabeb i Christiana, 1908.

[91] THUE A. - Über Annäherungswerte algebraischer Zahlen, J. für Math., t. 135, 1909, p. 284-305.

[92] WALLISER R. - Zur Approximation algebraischer Zahlen durch arithmetisch charakterisierte algebraische Zahlen, Arch. Math., Basel, t. 20, 1969, p. 384-391.

[93] WALDSCHMIDT M. - Nombres transcendants, Lecture Notes, n° 402, 1974, Springer Verlag, Berlin.

[94] WIRSING E. - On approximation of algebraic numbers by algebraic numbers of bounded degree, Proc. of Symp. in pure Math. XX, (1969 Number Theory Institute), 1971, p. 213-247.

[95] CUSICK T. W. - Effective lower bounds for some linear forms, Trans. Am. Math. Soc., t. 222, 1976, p. 289-302.

[96] GYÖRY K. - Sur les polynômes entiers et de discriminant donné, III, Publ. math. Debrecen, t. 23, 1976, p. 142-165.

[97] BAKER A. - Transcendental number theory, 1975, Cambridge University Press.

N° d'impression 245

3ème trimestre 1977