SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

MICHEL WALDSCHMIDT

Minorations du rang p-adique du groupe des unités

Séminaire de théorie des nombres de Grenoble, tome 9 (1980-1981), exp. n° 5, p. 1-20

<http://www.numdam.org/item?id=STNG_1980-1981__9__A5_0>

Séminaire de Théorie des Nombres
30 avril 1981
Grenoble

MINORATIONS DU RANG p-ADIQUE DU GROUPE DES UNITES

par Michel WALDSCHMIDT

Le texte qui suit est celui de l'exposé que Michel WALDSCHMIDT a fait au Colloque de Théorie des Nombres de Budapest (20 au 26 juillet 1981) sur le même sujet et qu'il a eu la gentillesse de nous communiquer. Ce texte paraîtra dans les actes du Congrès de Budapest sous le titre :
A lower bound for the p-adic rank of the units of an algebraic number field.

Let K be a totally real Galois extension of $\mathbb{Q}$ with Galois group G. When p is a prime, we denote by r_p the p-adic rank of the units of K. Leopoldt's conjecture asserts that $r_p = r$, where $r = [K:\mathbb{Q}] - 1$. When G is abelian, this equality has been proved by J. Ax and A. Brumer. An extension of their method enabled M. Emsalem, H.H. Kisilevsky and D.B. Wales to prove [1] :

$$r_p \geq \left(\sum_{\chi} d_\chi\right) - 1 ,$$

where χ runs over the characters of G irreductible over $\mathbb{Q}_p$, and d_χ is the degree of χ. Their main tool is a p-adic transcendence result on the non-vanishing of linear forms in logarithms of algebraic numbers (theorem of Baker-Brumer).

We give here an other lower bound for r_p , namely

$$r_p \geq r/2 \ .$$

We also use a p-adic transcendence result, but now it concerns exponential functions in several variables [4]. It is worth to notice that the transcendence proof, which rests on an extension of Schneider's method, enables one to give a new proof of the theorem of Baker-Brumer.

The number r_p is equal to the rank of a matrix

$$(\log_p \sigma\tau\epsilon)_{\sigma\in G,\ \tau\in G} \ ,$$

where ϵ is a Minkowski unit such that $|\sigma\epsilon - 1|_p < 1$ for all $\sigma \in G$. According to Dirichlet units theorem, the rank of the matrix

$$(\log|\sigma\tau\epsilon|)_{\sigma\in G,\ \tau\in G}$$

is equal to r . Our inequality $r_p \geq r/2$ will be a consequence of a more general result which compares the rank of a matrix $(\log_p \alpha_{ij})$ with the rank of a real matrix $(\log|\alpha_{ij}|)$.

The arrangement of this paper is as follows. In section 1 we state two lower bounds for the rank of $(\log_p \alpha_{ij})$, first in terms of the rank of $(\log|\alpha_{ij}|)$ with the natural logarithms of the modules, then in terms of the rank of $(\log \alpha_{ij})$ with complex determinations of the logarithms. In section 2 we give a corollary of these statements, and we study the situation from a conjectural point of view. In section 3 we introduce a coefficient $\theta^*(A)$, where $A = (\alpha_{ij})$. In §4 we state the main result of this paper, which gives a lower bound for the rank of $(\log_p \alpha_{ij})$ in terms of $\theta^*(A)$, and we deduce from it the results of §1. In section 5 we sketch the proof of the main result. Finally section 6 is devoted to further results on the subject.

Throught this paper we denote by $\bar{\mathbb{Q}}$ an algebraic closure of $\mathbb{Q}$, $\mathbb{C}_p$ is a completion of an algebraic closure of $\mathbb{Q}_p$, $\mathrm{rk}\, M$ is the rank of a matrix M , and $\deg P$ is the (total) degree of a polynomial P .

1. - ON THE RANK OF MATRICES WHOSE ENTRIES ARE LOGARITHMS OF ALGEBRAIC NUMBERS

We first give a lower bound for the p-adic rank in terms of the rank of a real matrix (cf. [4], 2.2.p). This is precisely the result which is used for the problem of the p-adic regulator.

THEOREM 1.1. - Let k be a number field, φ an embedding of k into $\mathbb{C}$, and φ_p an embedding of k into $\mathbb{C}_p$. Let α_{ij}, $(1 \le i \le d, 1 \le j \le \ell)$ be elements of k such that

$$|\varphi_p \alpha_{ij}|_p = 1 , \qquad (1 \le i \le d , 1 \le j \le \ell) .$$

We consider the two matrices

$$M^\circ = (\log|\varphi\alpha_{ij}|)_{1 \le i \le d , 1 \le j \le \ell}$$

where log is the natural logarithm, and

$$M_p = (\log_p \varphi_p \alpha_{ij})_{1 \le i \le d , 1 \le j \le \ell} .$$

Then

$$\mathrm{rk} M_p \ge \frac{1}{2} \mathrm{rk} M^\circ .$$

There is no inequality in the other direction : if we choose algebraic numbers α_{ij} with $\alpha_{ij} = 1$ for $i \neq j$ and $|\varphi \alpha_{ii}| = 1$, α_{ii} not root of unity, we get $\mathrm{rk} M_p = \min(d, \ell)$, while $\mathrm{rk} M^\circ = 0$.

We give now a lower bound for $\mathrm{rk} M_p$ in terms of the rank of a complex matrix $(\log\varphi\alpha_{ij})$, where, for each (i,j), we choose a determination of the logarithm of $\varphi\alpha_{ij}$. It is obviously necessary to make some assumption on these logarithms (take for instance all α_{ij} equal to 1). For the application to the next section, it would be sufficient to assume that

$$\left(\sum_{i=1}^{d} \sum_{j=1}^{\ell} \mathbb{Z} \log \varphi\alpha_{ij} \right) \cap 2i\pi \mathbb{Z} = 0 .$$

Such a choice is possible if and only if the subgroup of $\bar{\mathbb{Q}}^*$ generated by the $d\ell$ numbers α_{ij} is torsion free.

In the next result we use a slightly weaker hypothesis.

THEOREM 1.2. - With the assumptions of theorem 1.1, we choose, for $1 \le i \le d$, $1 \le j \le \ell$, a determination of the logarithm of $\varphi\alpha_{ij}$. We assume further that if $(a_1,\dots,a_d) \in \mathbb{Z}^d$ and $(b_1,\dots,b_\ell) \in \mathbb{Z}^\ell$ are any elements such that the number

$$\lambda = \sum_{i=1}^{d} \sum_{j=1}^{\ell} a_i b_j \log \varphi\alpha_{ij}$$

belongs to $2i\pi\mathbb{Z}$, then $\lambda = 0$.

We consider the matrix

$$M = (\log \varphi\alpha_{ij})_{1\le i\le d,\ 1\le j\le \ell} .$$

Then

$$\mathrm{rk}M_p \ge \frac{1}{2}\,\mathrm{rk}M .$$

The same method yields other inequalities like

$$\mathrm{rk}M_{p_1} \ge \frac{1}{2}\,\mathrm{rk}M_{p_2} \quad \text{and} \quad \mathrm{rk}M \ge \frac{1}{2}\,\mathrm{rk}M_p .$$

2. - THE NUMBERS $r(\Gamma)$ AND $r_p(\Gamma)$

Let Γ be a finitely generated subgroup of $\bar{\mathbb{Q}}^{*d}$ of rank ℓ over $\mathbb{Z}$. We first consider an embedding of $\bar{\mathbb{Q}}$ into $\mathbb{C}$, and we denote by $\exp : \mathbb{C}^d \to \mathbb{C}^{*d}$ the exponential map :

$$\exp t = (e^{t_1},\dots,e^{t_d}) \quad \text{for} \quad t = (t_1,\dots,t_d) \in \mathbb{C}^d .$$

We define $r(\Gamma)$ as the minimum of the numbers

$$\dim_{\mathbb{C}} (\mathbb{C}z_1 + \dots + \mathbb{C}z_\ell) ,$$

as $(z_1,\dots,z_\ell)$ runs over the ℓ-tuples of elements of $\mathbb{C}^d$ such that $\exp z_1,\dots,\exp z_\ell$ generate a subgroup of finite index of Γ. Equivalently,

$r(\Gamma)$ is the minimum of the ranks of matrices

$$(\log \gamma_{ij})_{1\le i\le d,\ 1\le j\le \ell}$$

where $\gamma_1,\dots,\gamma_\ell$ are multiplicatively independant elements of Γ, with $\gamma_j = (\gamma_{1j},\dots,\gamma_{dj})$, and $\log \gamma_{ij}$ is any determination of the logarithm of γ_{ij} ; the minimum is taken over the γ_j and the determinations of the logarithms.

We further write $r^\circ(\Gamma)$ for the rank of any matrix

$$(\log|\gamma_{ij}|)_{1\le i\le d,\ 1\le j\le \ell}\ ;$$

it does not depend on the choice of $\gamma_1,\dots,\gamma_\ell$ multiplicatively independent elements of Γ.

We will now define, for all prime numbers p outside a finite set, a number $r_p(\Gamma)$ in a similar way. We first choose $\gamma_1,\dots,\gamma_\ell$ multiplicatively independent in Γ. Let p be a prime ; we consider an embedding of $\bar{\mathbb{Q}}$ into $\mathbb{C}_p$ and we assume that all coordinates γ_{ij} of γ_j, for $1\le i\le d$ and $1\le j\le \ell$, are p-adic units. This condition on p may depend on the embedding of $\bar{\mathbb{Q}}$ into $\mathbb{C}_p$, but does not depend on the choice of $\gamma_1,\dots,\gamma_\ell$. Almost all p (i.e. all p but a finite number) satisfy this requirement (for all embeddings of $\bar{\mathbb{Q}}$ into $\mathbb{C}_p$) ; moreover, if the γ_{ij} are all algebraic units, then all p satisfy it. We now define $r_p(\Gamma)$ as the rank of the matrix

$$(\log_p \gamma_{ij})_{1\le i\le d,\ 1\le j\le \ell}\ .$$

Once more this number does not depend on the choice of $\gamma_1,\dots,\gamma_\ell$ multiplicatively independent in Γ, but it depends on Γ and on the embedding of $\bar{\mathbb{Q}}$ into $\mathbb{C}_p$.

From theorems 1.1 and 1.2 we will deduce the following :

COROLLARY 2.1. - We have $r_p(\Gamma) \ge \frac{1}{2} r^\circ(\Gamma)$ and $r_p(\Gamma) \ge \frac{1}{2} r(\Gamma)$.

Also $r_{p_1}(\Gamma) \ge \frac{1}{2} r_{p_2}(\Gamma)$ and $r(\Gamma) \ge \frac{1}{2} r_p(\Gamma)$.

Proof of corollary 2.1. - We choose $\gamma_1,\dots,\gamma_\ell$ in Γ multiplicatively independent. The inequality $r_p(\Gamma) \geq \frac{1}{2} r^\circ(\Gamma)$ is a straightforward consequence of theorem 1.1 with $\alpha_{ij} = \gamma_{ij}$. For the second inequality, we consider the subgroup of $\bar{\mathbb{Q}}^*$ generated by the $d\ell$ numbers γ_{ij}, $(1\leq i\leq d\,,\ 1\leq j\leq \ell)$; let a be the order of the torsion subgroup. Next, let $\beta_1,\dots,\beta_m$ be a basis of the (free) group generated by the $d\ell$ numbers γ_{ij}^a in $\bar{\mathbb{Q}}^*$. Thus there exist integers $a_{ijs} \in \mathbb{Z}$, $(1\leq i\leq d\,,\ 1\leq j\leq \ell\,,\ 1\leq s\leq m)$, which are uniquely determined, satisfying

$$\gamma_{ij}^a = \prod_{s=1}^{m} \beta_s^{a_{ijs}} \quad , \qquad (1\leq i\leq d\,,\ 1\leq j\leq \ell) \ .$$

We take any determinations of the logarithms of $\beta_1,\dots,\beta_m$. Since $\beta_1,\dots,\beta_m$ are multiplicatively independent, the numbers $\log\beta_1,\dots,\log\beta_m$, $2i\pi$ are $\mathbb{Q}$-linearly independent. If we set $\alpha_{ij} = \gamma_{ij}^a$, we can define $\log\alpha_{ij}$ by

$$\log\alpha_{ij} = \sum_{s=1}^{m} a_{ijs}\log\beta_s \quad , \qquad (1\leq i\leq d\,,\ 1\leq j\leq \ell) \ ,$$

and we get

$$\Big(\sum_{i=1}^{d}\sum_{j=1}^{\ell} \mathbb{Z}\log\alpha_{ij}\Big) \cap 2i\pi\mathbb{Z} = 0 \ .$$

From theorem 1.2, we conclude

$$r_p(\Gamma) = \mathrm{rk}(\log_p\alpha_{ij}) \geq \frac{1}{2}\mathrm{rk}(\log\alpha_{ij}) \geq \frac{1}{2}\, r(\Gamma) \ .$$

We now describe the situation from a conjectural point of view.

CONJECTURE 2.2. - *For all those* p *for which* $r_p(\Gamma)$ *is defined, we have*

$$r_p(\Gamma) = r(\Gamma) \geq r^\circ(\Gamma) \ .$$

Furthermore, let $\gamma_1,\dots,\gamma_\ell$ *be multiplicatively independent elements in* Γ, *and let* $\log\gamma_{ij}$ *satisfy*

$$\Big(\sum_{i=1}^{d}\sum_{j=1}^{\ell} \mathbb{Z}\log\gamma_{ij}\Big) \cap 2i\pi\mathbb{Z} = 0 \ .$$

Then the rank of the matrix

$$M = (\log\gamma_{ij})_{1\leq i\leq d\,,\ 1\leq j\leq \ell}$$

is equal to $r(\Gamma)$.

According to this conjecture, the number $r(\Gamma)$ (resp. $r_p(\Gamma)$) does not depend on the chosen embedding of $\bar{\mathbb{Q}}$ into $\mathbb{C}$ (resp. into $\mathbb{C}_p$). Of course, in general, $r^\circ(\Gamma)$ may well depend on the choice of this embedding (i.e. of the choice of the absolute values $|\gamma_{ij}|$). Also, for a given p, the fact that $r_p(\Gamma)$ is defined depends on the embedding of $\bar{\mathbb{Q}}$ into $\mathbb{C}_p$. But if conjecture 2.2 holds, there is a natural definition for $r_p(\Gamma)$ for all p and all embeddings $\bar{\mathbb{Q}} \subset \mathbb{C}_p$.

From the definition of $r(\Gamma)$, it is obvious that $\mathrm{rk}M \geq r(\Gamma)$. Let us show that the inequality $r_p(\Gamma) \geq \mathrm{rk}M$ is a consequence of the following standard conjecture (which is a special case of the p-adic Schanuel's conjecture ; see [4] p. 127).

CONJECTURE 2.3. - *Let $\alpha_1,\ldots,\alpha_m$ be p-adic units in $\mathbb{C}_p$, which are algebraic over $\mathbb{Q}$, and multiplicatively independent. Then the numbers $\log_p \alpha_1,\ldots,\log_p \alpha_m$ are algebraically independent.*

We need the following lemma :

LEMMA 2.4. - *Let K be a field, $A_1,\ldots,A_m$ be elements of $K[X_1,\ldots,X_n]$, and let $P \in K[X_1,\ldots,X_{n+m}]$. If the polynomial*

$$P(X_1,\ldots,X_n,A_1,\ldots,A_m)$$

is the zero polynomial in $K[X_1,\ldots,X_n]$, then P belongs to the ideal $\mathfrak{I}$ of $K[X_1,\ldots,X_{n+m}]$ generated by the m polynomials $X_{n+j}-A_j$, $(1\leq j\leq m)$.

Proof of lemma 2.4. - We consider the field $L = K(X_1,\ldots,X_n)$. The image of P in $L[T_1,\ldots,T_m]$ under the obvious map $X_{n+j} \mapsto T_j$ belongs to the ideal generated by $T_1-A_1,\ldots,T_m-A_m$. This means that there exist $Q_o \in K[X_1,\ldots,X_n]$, $Q_o \neq 0$, and $Q_1,\ldots,Q_m$ in $K[X_1,\ldots,X_{n+m}]$, such that

$$Q_o(X_1,\ldots,X_n)P(X_1,\ldots,X_{n+m}) = \sum_{j=1}^{m} Q_j(X_1,\ldots,X_{n+m})(X_{n+j}-A_j(X_1,\ldots,X_n)) .$$

It is now sufficient to notice that the ideal $\mathfrak{J}$ is prime, since the quotient $K[X_1,\dots,X_{n+m}]/\mathfrak{J}$ is isomorphic to $K[X_1,\dots,X_n]$.

Proof of the inequality $r_p(\Gamma) \geq rkM$ in 2.2 as a consequence of 2.3.

Assume that the rank r of M satisfies $r > r_p(\Gamma)$. We write all the determinants $r \times r$ out of the matrix $(\log_p \gamma_{ij})$. We get finitely many polynomials $P_1,\dots,P_k$ in $d\ell$ indeterminates X_{ij} , $(1 \leq i \leq d\,,\ 1 \leq j \leq \ell)$, with rational coefficients, which all vanish at the point $(\log_p \gamma_{ij})$.

We select among the $d\ell$ numbers $\log_p \gamma_{ij}$ a basis of the $\mathbb{Q}$-vector space they generate, and we write this basis $\log_p \gamma_{i(s),j(s)}$, $1 \leq s \leq m$. Next let a_{ijs} , a , be rational integers, with $a > 0$, such that

$$a \log_p \gamma_{ij} = \sum_{s=1}^{m} a_{ijs} \log_p \gamma_{i(s),j(s)} \quad , \qquad (1 \leq i \leq d\,,\ 1 \leq j \leq \ell) \ .$$

By assumption the numbers γ_{ij} are p-adic units, and for a p-adic unit $u \in \mathbb{C}_p$ the condition $\log_p u = 0$ means that u is a root of unity. Therefore there exists a positive integer b such that

$$\gamma_{ij}^{ab} = \prod_{s=1}^{m} \gamma_{i(s),j(s)}^{a_{ijs}b} \quad , \qquad (1 \leq i \leq d\,,\ 1 \leq j \leq \ell) \ .$$

Thanks to our assumption on the complex logarithms $\log \gamma_{ij}$ in 2.2, we conclude

$$a \log \gamma_{ij} = \sum_{s=1}^{m} a_{ijs} \log \gamma_{i(s),j(s)} \quad , \qquad (1 \leq i \leq d\,,\ 1 \leq j \leq \ell) \ .$$

We now use 2.3 : the numbers $\log_p \gamma_{i(s),j(s)}$ are algebraically independent. From lemma 2.4 (with $n = d\ell - m$) we see that the polynomials $P_1,\dots,P_k$ belong to the ideal of $\mathbb{Q}[\{X_{ij}\}_{1 \leq i \leq d\,,\ 1 \leq j \leq \ell}]$ generated by the $d\ell$ polynomials

$$aX_{ij} - \sum_{s=1}^{m} a_{ijs} X_{i(s),j(s)} \quad , \qquad (1 \leq i \leq d\,,\ 1 \leq j \leq \ell) \ .$$

Therefore $P_1,\dots,P_k$ vanish at the complex point $(\log \gamma_{ij})$, which contradicts the assumption $r = rkM$.

The same proof shows that the inequality $r_p(\Gamma) \geq r^\circ(\Gamma)$ is a consequence of 2.3. Similarly, it is easy to deduce the inequality $r(\Gamma) \geq r_p(\Gamma)$ from the following classical conjecture :

CONJECTURE 2.5. - If $\log \alpha_1, \ldots, \log \alpha_m$ are $\mathbb{Q}$-linearly independent logarithms of complex algebraic numbers, then they are algebraically independent.

Another consequence of 2.5 is $r(\Gamma) \geq r^\circ(\Gamma)$. As pointed out to me by E. Reyssat, this inequality depends on the fact that the coordinates of the elements of Γ are algebraic numbers. For instance let Γ be the subgroup of $\mathbb{C}^{*2}$ generated by $\begin{pmatrix} e^{\pi} \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ e^{\pi} \end{pmatrix}$. We can define $r(\Gamma)$ and $r^\circ(\Gamma)$ as before (in spite of the fact that Γ is not included in $\bar{\mathbb{Q}}^{*2}$). Then $r^\circ(\Gamma) = 2$; but $r(\Gamma) = 1$, because $\begin{pmatrix} e^{2\pi} \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ e^{2\pi} \end{pmatrix}$ generate a subgroup of finite index of Γ , and

$$\det \begin{vmatrix} 2\pi & -2i\pi \\ 2i\pi & 2\pi \end{vmatrix} = 0 .$$

3 - THE COEFFICIENT θ^*

If the rank of the matrix $M_p = (\log_p \alpha_{ij})$ is "small", then there are "many" linear relations with coefficients in $\mathbb{C}_p$ between, say, the rows of M_p . Our aim is to show that, in this case, and assuming the α_{ij} are algebraic, there are "many" linear relations with rational coefficients between the $d\ell$ entries $\log_p \alpha_{ij}$ of M_p . This means that there are "many" multiplicative relations between the $d\ell$ algebraic numbers α_{ij} . In order to count these relations, we introduce a coefficient θ^* , which is the multiplicative analog of the coefficient θ of [4]. It will satisfy $0 \leq \theta^* \leq \ell/d$, and "many" multiplicative relations between the α_{ij} means that θ^* is small.

Notation. Let G be a commutative group ; we write the law of G multiplicatively. Let α_{ij} , $(1 \leq i \leq d, 1 \leq j \leq \ell)$ be elements of G . We write

$$A = (\alpha_{ij})_{1 \leq i \leq d,\ 1 \leq j \leq \ell} ,$$

and we define

$$\theta^*(A) = \min \frac{\ell-\lambda}{d-\delta} ,$$

where λ and δ run over the integers, $0 \le \lambda \le \ell$, $0 \le \delta < d$, such that there exist $p_1,\dots,p_{d-\delta}$ in $\mathbf{Z}^d$, linearly independent, and $q_1,\dots,q_\lambda$ in $\mathbf{Z}^\ell$, linearly independent, with

$$p_s = (p_{s1},\dots,p_{sd}) \in \mathbf{Z}^d , \qquad (1 \le s \le d-\delta)$$

and

$$q_t = (q_{1t},\dots,q_{\ell t}) \in \mathbf{Z}^\ell , \qquad (1 \le t \le \lambda) ,$$

satisfying

$$\prod_{i=1}^{d} \prod_{j=1}^{\ell} \alpha_{ij}^{p_{si}q_{jt}} = 1 , \qquad (1 \le s \le d-\delta , 1 \le t \le \lambda) .$$

If the law of G is written additively, we write θ instead of θ^*.

In this section we give some lower bounds for θ^*.

LEMMA 3.1. - Assume $G = \mathbf{C}^*$. If the matrix $(\log|\alpha_{ij}|)$ is of rank d, then $\theta^*(A) \ge 1$.

Proof. - Using the definition of θ^*, we write $\theta^*(A) = (\ell-\lambda)/(d-\delta)$. From the relations

$$\prod_{i=1}^{d} \prod_{j=1}^{\ell} \alpha_{ij}^{p_{si}q_{jt}} = 1 ,$$

we deduce

$$\sum_{i=1}^{d} \sum_{j=1}^{\ell} p_{si}q_{jt} \log|\alpha_{ij}| = 0 .$$

Therefore there exist a regular $d \times d$ matrix P with integer entries, and a regular $\ell \times \ell$ matrix Q with integer entries, such that

$$P(\log|\alpha_{ij}|)Q = \begin{pmatrix} M_1 & 0 \\ M_2 & M_3 \end{pmatrix}$$

where M_3 is a matrix with δ rows and λ columns (and M_1 has $d-\delta$ rows and $\ell-\lambda$ columns). Hence

$$\mathrm{rk}(\log|\alpha_{ij}|) \le \ell - \lambda + \delta \ .$$

This completes the proof of lemma 3.1.

The same proof works for complex logarithms, provided that the relations

$$\prod_{i=1}^{d}\prod_{j=1}^{\ell}\alpha_{ij}^{p_{si}q_{jt}} = 1$$

imply

$$\sum_{i=1}^{d}\sum_{j=1}^{\ell} p_{si}q_{jt}\log\alpha_{ij} = 0 \ .$$

Therefore we get the following result :

LEMMA 3.2. - Assume $G = \mathbb{C}^*$. For $1 \le i \le d$, $1 \le j \le \ell$, let $\log\alpha_{ij}$ be a determination of the logarithm of α_{ij} . Assume that the condition

$$\sum_{i=1}^{d}\sum_{j=1}^{\ell} a_i b_j \log\alpha_{ij} = 2i\pi c$$

for rational integers $a_1,\dots,a_d$, $b_1,\dots,b_\ell$ and c implies $c = 0$.

If the matrix $(\log\alpha_{ij})$ is of rank d , then $\theta^*(A) \ge 1$.

Similarly, for $G = \mathbb{C}_p^*$ and $|\alpha_{ij}|_p = 1$, if the matrix $(\log_p\alpha_{ij})$ is of rank d , then $\theta^*(A) \ge 1$.

Remark. - The assumption $\theta^*(A) \ge 1$ is not sufficient to ensure that the rank of $(\log|\alpha_{ij}|)$, or of $(\log\alpha_{ij})$, is equal to d . An obvious example ([4] example 7, p. 113) is $\alpha_{ij} = \exp(\sqrt{p_i p_{d+j}})$, where $p_1,\dots,p_{d+\ell}$ are distinct primes. In the following more subtle example, due to M. Langevin, the numbers α_{ij} are rational :

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 1/5 \\ 3 & 5 & 1 \end{pmatrix}$$

and $\ell = d = 3$, $\theta^*(A) = 1$, $\mathrm{rk}(\log|\alpha_{ij}|) = 2$.

The conjecture 2.2 suggests that it should be possible to describe the number $r(\Gamma)$ solely in terms of $\Gamma \subset \bar{\mathbb{Q}}^{*d}$, by algebraic means, without involving a transcendental parametrization by the exponential function.

We will see below (§4) that it is possible to give a lower bound for $r_p(\Gamma)$ (and also $r(\Gamma)$) in terms of θ^*, but the result does not seem best possible, and, in view of Langevin's example, the complete conjectural description of the situation is not clear. If we take Schanuel's conjecture for granted, the problem is reduced to the study of the rank of a matrix $M = M_1X_1 + \ldots + M_sX_s$, where $M_1, \ldots, M_s$ have coefficients in a field K (say $K = \mathbb{Q}$), and $X_1, \ldots, X_s$ are indeterminates over K.

4. - THE MAIN RESULT

In this section we deduce theorems 1.1 and 1.2 from the following result (see [4], 2.1.p).

THEOREM 4.1. - Let α_{ij}, $(1 \le i \le d, 1 \le j \le \ell)$ be elements of $\mathbb{C}_p$, which are algebraic over $\mathbb{Q}$, and satisfy $|\alpha_{ij}|_p = 1$. Define

$$M_p = (\log_p \alpha_{ij})_{1 \le i \le d,\, 1 \le j \le \ell},$$

and

$$A = (\alpha_{ij})_{1 \le i \le d,\, 1 \le j \le \ell}.$$

Then

$$\mathrm{rk} M_p \ge d \frac{\theta^*(A)}{1 + \theta^*(A)}.$$

Proof of theorem 1.1. - Define $r = \mathrm{rk} M^\circ$. Let $i(1), \ldots, i(r)$ be integers, with $1 \le i(1) < \ldots < i(r) \le d$ such that the matrix

$$\tilde{M}^\circ = (\log|\varphi \alpha_{i(s),j}|)_{1 \le s \le r,\, 1 \le j \le \ell}$$

has rank r . By lemma 3.1, we get, for $\widetilde{A} = (\alpha_{i(s),j})_{1\le s\le r,\ 1\le j\le \ell}$

$$\theta^*(\widetilde{A}) \ge 1 .$$

By theorem 4.1 the matrix $\widetilde{M}_p = (\log_p \varphi\alpha_{i(s),j})_{1\le s\le r,\ 1\le j\le \ell}$ satisfies

$$\mathrm{rk}\widetilde{M}_p \ge r/2 .$$

Since $\mathrm{rk}M_p \ge \mathrm{rk}\widetilde{M}_p$, theorem 1.1 follows.

Proof of theorem 1.2. - The proof is the same, using now lemma 3.2, together with the fact that the only number of the form

$$\lambda = \sum_{s=1}^{r} \sum_{j=1}^{\ell} a_s b_j \log\varphi\alpha_{i(s),j}$$

with $a_s \in \mathbb{Z}$, $b_j \in \mathbb{Z}$, which belongs to $2i\pi\mathbb{Z}$, is $\lambda = 0$.

5. - SCHNEIDER's METHOD IN SEVERAL VARIABLES

The proof of theorem 4.1 can be divided in two parts. In the first one, we assume $\mathrm{rk}M_p < d$, and we construct a sequence of non-zero polynomials $P_S(X_1,\dots,X_d)$, $S \ge S_o$, such that

$$P_S\left(\prod_{j=1}^{\ell} \alpha_{1j}^{h_j},\dots,\prod_{j=1}^{\ell} \alpha_{dj}^{h_j}\right) = 0$$

for all $(h_1,\dots,h_\ell) \in \mathbb{Z}^\ell$ satisfying $0 \le h_j \le S$, $(1\le j\le \ell)$. Moreover we give an upper bound for the degree of P_S :

$$\deg P_S \le C_1 S^{n/(d-n)} ,$$

where $n = \mathrm{rk}M_p$, and C_1 does not depend on S .

The second part is a "zero estimate", due to D.W. Masser [2]. It gives a lower bound for the degree of a polynomial satisfying such conditions :

$$\deg P_S \ge C_2 S^{\theta^*(A)} .$$

Theorem 4.1 follows at once.

Because of the finiteness of the radius of convergence of the exponential function, it is convenient to assume $|\alpha_{ij}-1|_p < 1$ for $1\le i\le d$, $1\le j\le \ell$. Let us show first that this involves no loss of generality.

Let a be a positive integer such that

$$|\log_p \alpha_{ij}|_p < p^a \quad , \qquad (1\le i\le d, 1\le j\le \ell) \ .$$

Define

$$\tilde{\alpha}_{ij} = \exp(p^a \log_p \alpha_{ij}) \ .$$

Then

$$|\tilde{\alpha}_{ij}-1|_p < 1 \quad , \quad \log_p \tilde{\alpha}_{ij} = p^a \log_p \alpha_{ij} \quad ,$$

and if we set

$$\tilde{M}_p = (\log_p \tilde{\alpha}_{ij}) \quad , \quad \text{and} \quad \tilde{A} = (\tilde{\alpha}_{ij}) \ ,$$

we have

$$\mathrm{rk} M_p = \mathrm{rk} \tilde{M}_p \quad , \quad \theta^*(A) = \theta^*(\tilde{A}) \ .$$

PROPOSITION 5.1. - Let α_{ij} $(1\le i\le d, 1\le j\le \ell)$ be algebraic numbers in $\mathbb{C}_p$ with $|\alpha_{ij}-1|_p < 1$. Assume that the rank n of the matrix $M_p = (\log_p \alpha_{ij})$ satisfies $n < d$. Then there exist positive integers S_o and C_1, and a sequence of non-zero polynomials $(P_S)_{S\ge S_o}$ in $\mathbb{Z}[X_1,\dots,X_d]$, with

$$\deg P_S \le C_1 S^{n/(d-n)} \ ,$$

such that

$$P_S\left(\prod_{j=1}^{\ell} \alpha_{1j}^{h_j},\dots,\prod_{j=1}^{\ell} \alpha_{dj}^{h_j}\right) = 0$$

for all $(h_1,\dots,h_\ell) \in \mathbb{Z}^\ell$ satisfying $0 \le h_j \le S$, $(1\le j\le \ell)$.

Sketch of the proof of proposition 5.1, following [4]. - We select n columns of M_p which are $\mathbb{C}_p$-linearly independent ; let their index be

$j(1),\dots,j(n)$, with $1 \le j(1) < j(2) < \dots < j(n) \le d$. We define, for $1 \le j \le \ell$, $y_j = (y_{j1},\dots,y_{jn}) \in \mathbb{C}_p^n$ by

$$\log_p \alpha_{ij} = \sum_{\nu=1}^{n} y_{j\nu} \log \alpha_{i,j(\nu)} , \qquad (1 \le i \le d , 1 \le j \le \ell) .$$

Now we write the unknown polynomial P_S , for large S , in the following form :

$$P_S(X_1,\dots,X_d) = \sum_{(\lambda)} p(\lambda) X_1^{\lambda_1} \dots X_d^{\lambda_d} ,$$

where $\lambda = (\lambda_1,\dots,\lambda_d)$ runs over the elements of $\mathbb{Z}^d$ satisfying $\lambda_i \ge 0$, $\lambda_1 + \dots + \lambda_d \le D$; thus $D = D_S$ will be an upper bound for the degree of P_S .

Let us consider the function

$$F_S(z) = \sum_{(\lambda)} p(\lambda) \prod_{i=1}^{d} \prod_{\nu=1}^{n} \alpha_{i,j(\nu)}^{\lambda_i z_\nu}$$

which is analytic for $z = (z_1,\dots,z_n)$ in the disk $|z|_p < p^{1/(p-1)}$ of $\mathbb{C}_p^n$ (here $|z|_p = \max_{1 \le \nu \le n} |z_\nu|_p$). For each $(h_1,\dots,h_\ell) \in \mathbb{Z}^\ell$, we have

$$F_S(h_1 y_1 + \dots + h_\ell y_\ell) = \sum_{(\lambda)} p(\lambda) \prod_{i=1}^{d} \prod_{j=1}^{\ell} \alpha_{ij}^{\lambda_i h_j}$$

$$= P_S\left(\prod_{j=1}^{\ell} \alpha_{1j}^{h_j}, \dots, \prod_{j=1}^{\ell} \alpha_{dj}^{h_j} \right) .$$

Now the strategy is as follows.

First step.

We construct P_S (i.e. the $p(\lambda) \in \mathbb{Z}$) such that many derivatives of F_S at the origin are small, namely

$$\left| \frac{1}{\tau!} D^\tau F(0) \right|_p \le e^{-U} \qquad \text{for} \quad \tau = (\tau_1,\dots,\tau_n) , \quad \|\tau\| < C_3 U ,$$

where $U = U_S$ is a new parameter. Moreover we solve this system of inequalities with integers $p(\lambda)$, not all zero, in the range

$$-e^{C_4 U} \le p(\lambda) \le e^{C_4 U} .$$

The number of inequalities we have to solve is about U^n , and the number of unknowns is about D^d . It turns out that such a construction is possible, using a suitable version of Siegel's lemma, provided that $U \le C_5 D^{d/n}$.

Second step.

A rather simple p-adic analytic estimate shows that

$$|F_S(z)|_p \le e^{-C_6 U} \quad \text{for} \quad |z|_p \le 1 .$$

Third step.

We consider the number $F_S(h_1 y_1 + \dots + h_\ell y_\ell)$, for some $(h_1,\dots,h_\ell) \in \mathbb{Z}^\ell$, $0 \le h_j \le S$. Using classical algebraic arguments ("size inequality" : a non zero algebraic number cannot be too small), we show that this number is zero, which is the desired conclusion.

Now for this last step we need an upper bound of the shape $DS \le C_7 U$, and since $U \le C_5 D^{d/n}$ we must take $D \ge C_1 S^{n/(d-n)}$.

The second part of the proof is the zero estimate of D.W. Masser.

PROPOSITION 5.2. - Let K be a field of characteristic zero, α_{ij} $(1 \le i \le d , 1 \le j \le \ell)$ be elements of K^* , $A = (\alpha_{ij})$, and D , S positive integers. Assume that there exist $p(\lambda) \in K$, (for $(\lambda) = (\lambda_1,\dots,\lambda_d)$, $\lambda_i \ge 0$, $\lambda_1 + \dots + \lambda_d \le D$), not all zero, such that

$$\sum_{(\lambda)} p(\lambda) \prod_{i=1}^{d} \prod_{j=1}^{\ell} \alpha_{ij}^{\lambda_i h_j} = 0$$

for all $(h_1,\dots,h_\ell) \in \mathbb{Z}^\ell$, $0 \le h_j \le S$. Then

$D \ge (S/d)^{\theta^*(A)}$.

We deduce proposition 5.2 from theorem 2 of [2] in the following way. We first notice that the statement of proposition 5.2 involves only finitely many elements of K , and therefore we may assume, without loss of generality, that

K is finitely generated over $\mathbb{Q}$. If we wish, we can embed K in $\mathbb{C}$. Next, for $z = (z_1,\dots,z_d) \in K^{*d}$ and $h = (h_1,\dots,h_d) \in \mathbb{Z}^d$, we write

$$z^h = (z_1^{h_1},\dots,z_d^{h_d}) \in K^{*d} .$$

Finally let Γ be the subgroup of K^{*d} generated by the ℓ elements

$$(\alpha_{1j},\dots,\alpha_{dj}) \in K^{*d} , \qquad (1\le j\le \ell) .$$

For $1\le r\le d$, define ℓ_r as the maximum rank of any subgroup Γ' of Γ such that there exists a subgroup H of $\mathbb{Z}^d$, of rank r, satisfying

$$\gamma^h = 1 \quad \text{for all } \gamma\in\Gamma' , \ h\in H .$$

It is plain that

$$\theta^*(A) = \min_{1\le r\le d} \frac{\ell-\ell_r}{r} .$$

Therefore, with the notations of [2],

$$\theta^*(A) = \chi(\Gamma, \mathbb{Z}^d) .$$

Indeed, if $X = \mathbb{Z}x_1+\dots+\mathbb{Z}x_d$ and $Y = \mathbb{Z}y_1+\dots+\mathbb{Z}y_\ell$ are two finitely generated subgroups of $\mathbb{C}^n$ of rank d and ℓ respectively, and if

$$\alpha_{ij} = \exp(\langle x_i, y_j\rangle) , \quad \text{and} \quad A = (\alpha_{ij}) ,$$

then

$$\chi(Y,X) = \theta^*(A) .$$

Thus proposition 5.2 is equivalent to theorem 2 of [2].

In the proof of theorem 4.1, we use proposition 5.2 with $K = \bar{\mathbb{Q}}$ (there is no need of a p-adic zero estimate).

Also it is important to notice that the hypothesis $\mathrm{rk}M_p < d$ has been used only in the first part of the proof (proposition 5.1), not in the zero estimate. As a consequence, the zero estimate 5.2 is sufficient for quantitative results (there is no need of a "small value lemma").

As shown in [2], the exponent $\theta^*(A)$ in proposition 5.2 is best possible. Therefore it is very likely that proposition 5.1 is not best possible.

The proof sketched here works as well in the complex case, and gives the same lower bound : $d\theta^*/(1+\theta^*)$ for the rank of $(\log \alpha_{ij})$, for any determinations of the logarithms. The difference between the two cases arises only if we intend to bound the rank of $(\log \alpha_{ij})$ not in terms of the multiplicative coefficient θ^* of (α_{ij}), but in terms of the additive coefficient θ of the matrix of the logarithms. In the p-adic case both coefficients obviously coincide, but in the complex case, because of $2i\pi$, we have only the inequality

$$\theta((\log \alpha_{ij})) \geq \theta^*((\alpha_{ij})) .$$

However the inequality

$$r \geq d\theta/(1+\theta) , \quad \text{with} \quad r = \mathrm{rk}(\log \alpha_{ij}) , \quad \theta = \theta((\alpha_{ij}))$$

can be deduced from the complex analog of theorem 4.1 (see [4], 7.2 ; this is the place where the technical lemmas 5.3 and 5.4 of [4] are needed).

6. - FURTHER RESULTS

The construction of the auxiliary function can be performed in a very general context [4]. Also the zero estimate has been extended by Masser and Wüstholz [3] to arbitrary commutative group varieties, and they are developing their method to a very large extent. Therefore the method presented here is capable of a large generalization which I hope to develop somewhere else. As an illustration, here is the elliptic analog to theorem 1.2, when we replace $\bar{\mathbb{Q}}^{*d}$ by $E(\bar{\mathbb{Q}})^d$, where E is an elliptic curve which is defined over $\bar{\mathbb{Q}}$. (Cf. [3] §8).

Let γ_{ij}, $(1 \leq i \leq d, 1 \leq j \leq \ell)$ be $d\ell$ points in $E(\bar{\mathbb{Q}})$. We choose any representation of the complex exponential of $E(\mathbb{C})$ (say by a Weierstrass

elliptic function), and, for $1 \le i \le d$, $1 \le j \le \ell$, we choose $u_{ij} \in \mathbb{C}$ whose image by this exponential is γ_{ij} . We denote by r the rank of the matrix

$$(u_{ij})_{1 \le i \le d,\ 1 \le j \le \ell} .$$

Let k be the field of endomorphisms of E , and $\mathfrak{L}$ be the kernel of our exponential, which gives an isomorphism between $\mathbb{C}/\mathfrak{L}$ and $E(\mathbb{C})$. Assume that for any $(a_1,\dots,a_d) \in k^d$ and any $(b_1,\dots,b_\ell) \in \mathbb{Z}^\ell$, if the number

$$\lambda = \sum_{i=1}^{d} \sum_{j=1}^{\ell} a_i b_j u_{ij}$$

belongs to $\mathfrak{L}$, then $\lambda = 0$.

Now let p be a prime ; consider a p-adic representation of the exponential map of $E(\mathbb{C}_p)$, and <u>assume</u> that there exists $u_{ij}^{(p)}$ in $\mathbb{C}_p$ (in the neighbourhood of zero where the exponential is defined) whose image by this exponential is γ_{ij} . Denote by r_p the rank of the matrix

$$\left(u_{ij}^{(p)}\right)_{1 \le i \le d,\ 1 \le j \le \ell} .$$

Then

$$r_p \ge r/3 .$$

Finally we mention the following recent works which are connected with this subject.

• P. Philippon gave an elliptic analog to lemmas 5.3 and 5.4 of [4] (see the end of section 5 above).

• N. Sebti-Chaouni worked out the proof of Baker's theorem by Schneider's method in several variables (see [2] p. 94). She had to improve theorem B of [3].

• Yu Kun Rui did the same in the elliptic case with complex multiplication, i.e. gave a new proof of Masser's theorem on linear forms of elliptic integrals, and also gave an effective lower bound.

• J.C. Moreau derived a simplified proof of the theorem of Masser and Wüstholz [3] by replacing commutative algebra by algebraic geometry.

REFERENCES

[1] M. EMSALEM, H.H. KISILEVSKY, and D.B. WALES. - In preparation.

[2] D.W. MASSER. - On polynomials and exponential polynomials in several variables ; Invent. math., 63 (1981), 81-95.

[3] D.W. MASSER and G. WÜSTHOLZ. - Zero estimates on group varieties ; Invent. math., to appear.

[4] M. WALDSCHMIDT. - Transcendance et exponentielles en plusieurs variables ; Invent. math., 63 (1981), 97-127.

Laboratoire de Mathématiques Pures - Institut Fourier
dépendant de l'Université Scientifique et Médicale de Grenoble
associé au C.N.R.S.
B.P. 116
38402 ST MARTIN D'HERES (France)