Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Françoise Bertrandias

Éléments algébriques de l'algèbre $V_E(Q)$

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 5 (1963-1964), exp. n° 19, p. 1-15

<http://www.numdam.org/item?id=SDPP_1963-1964__5__A12_0>

Séminaire DELANGE-PISOT
(Théorie des Nombres)
5e année, 1963/64, n° 19

ÉLÉMENTS ALGÉBRIQUES DE L'ALGÈBRE $V_E(Q)$

par Mme Françoise BERTRANDIAS

Dans cet exposé, on se propose l'étude, dans différentes algèbres sur le corps Q des rationnels, des éléments algébriques sur Q, en liaison avec des éléments algébriques particuliers étudiés précédemment (ensembles $\mathcal{S}$). Le plan est le suivant :

§ 1 : Définitions - Notations.

§ 2 : Eléments algébriques de l'algèbre $\Omega_E(Q) \cong \prod_{p \in E} \Omega_p$. Résultat essentiel : le lemme 1.

§ 3 : Eléments algébriques de l'algèbre $V_E(Q) \cong \prod_{p \in E} Q_p$. Résultat essentiel : le théorème 1, obtenu en utilisant un "théorème de Minkowski" pour des systèmes de formes linéaires à coefficients dans des Q_p, en nombre fini.

§ 4 : Une caractérisation des éléments algébriques de $V_E(Q)$: théorème 2.

1. Définitions - Notations.

1.1. - Q_p désigne le corps des nombres p-adiques, Ω_p sa clôture algébrique, P l'ensemble de toutes les valuations distinctes non équivalente de Q, en convenant de désigner par l'indice 0 la valuation ordinaire ($Q_0 = R$, $\Omega_0 = C$, R corps des réels, C corps des complexes). E désignera un sous-ensemble fini non vide de P (contenant ou non la valuation ordinaire).

Pour un élément ξ_0 de R, $|\xi_0|_0$ désigne la valeur absolue ordinaire.
Pour un élément ξ_p de Q_p, $|\xi_p|_p$ désigne la valeur absolue p-adique telle que $|p|_p = 1/p$.

Soit $V(Q)$ la sous-algèbre de l'algèbre produit $\prod_{p \in P} Q_p$ (algèbre produit de Q-algèbres au sens de BOURBAKI, [2], § 8-10), définie par

$$V(Q) = \{\xi = (\xi_p)_{p \in P} \; ; \; \xi_p \in Q_p \text{ et } |\xi_p|_p \leqslant 1$$

sauf pour un nombre fini de p au plus $\}$.

Soit $\Omega(Q)$ la sous-algèbre de l'algèbre produit $\prod_{p \in P} \Omega_p$ définie par

$$\Omega(Q) = \{\xi = (\xi_p)_{p\in P} \; ; \; \xi_p \in \Omega_p \text{ et } |\xi_p|_p \leqslant 1$$

sauf pour un nombre fini de p au plus $\}$.

$V(Q)$ est une sous-algèbre de $\Omega(Q)$. Ces deux algèbres ont le même élément unité qu'on notera e et qui est défini par $e_p = 1$ ($p \in P$). L'élément nul de $\Omega(Q)$ ($\xi_p = 0$, $p \in P$) sera noté 0 . Si $r \in Q$, on note $r\xi$ l'élément $(r\xi_p)_{p\in P}$.

Le sous-anneau de $\Omega(Q)$ isomorphe à Q , qui est l'ensemble des éléments $r.e$ ($r \in Q$), sera désigné par $Q.e$.

On définit dans $\Omega(Q)$ la pseudo-valuation [6]

$$\|\xi\| = \sup_{p\in P} |\xi_p|_p \; .$$

1.2. - Soit $\Omega_E(Q)$ (resp. $V_E(Q)$) la sous-algèbre de $\Omega(Q)$ définie par :

$$\Omega_E(Q) = \{\xi \in \Omega(Q) \; ; \; \xi_p = 0 \text{ si } p \notin E\}$$

$$(\text{resp. } V_E(Q) = \{\xi \in V(Q) \; ; \; \xi_p = 0 \text{ si } p \notin E\}) .$$

$\Omega_E(Q)$ (resp. $V_E(Q)$) est isomorphe à l'algèbre produit $\prod_{p\in E} \Omega_p$ (resp. $\prod_{p\in E} Q_p$). $V_E(Q)$ est une sous-algèbre de $\Omega_E(Q)$.

Ces 2 algèbres ont le même élément unité : e_E de composante 1 ou 0 dans Q_p suivant que $p \in E$ ou non.

Si $\xi \in \Omega(Q)$, $\xi.e_E$ est l'élément de $\Omega_E(Q)$ ayant même projection ξ_p que ξ dans Ω_p ($p \in E$).

Le sous-anneau de $V_E(Q)$ isomorphe à Q :

$$Q.e_E = \{re_E \; , \; r \in Q\}$$

sera noté Q_E .

On désignera fréquemment $\Omega_E(Q)$ et $V_E(Q)$ par Ω_E et V_E .

Si $(E_i)_{i=1,\ldots,m}$ désigne une partition de E , $e_E = \sum_{i=1}^{m} e_{E_i}$. Donc si $\xi \in \Omega_E$,

$$\xi = \xi e_E = \sum_{i=1}^{m} \xi e_{E_i} \qquad \text{où } \xi e_{E_i} \in \Omega_{E_i} .$$

Ω_E est l'anneau composé direct des anneaux Ω_{E_i} ($i = 1 , \ldots , m$) (composé direct au sens de BOURBAKI, [2], § 8-11).

Si E se réduit à un élément $E = (p)$, on notera $e_E = e_{(p)}$; $\Omega_E = \Omega_{(p)}$.

1.3. - Théorème d'Artin ([1], § 2.2). - On démontre que pour tout élément ξ de $V(Q)$, il existe une décomposition unique :

$$\xi = eH(\xi) + \varepsilon(\xi)$$

où $H(\xi) \in Q$ et $\varepsilon(\xi) \in V(Q)$ avec

$$\begin{cases} -1/2 \leqslant \varepsilon_0(\xi) < 1/2 \\ |\varepsilon_p(\xi)|_p \leqslant 1 \end{cases} \qquad (p \in P).$$

Si $\xi \in V_E(Q)$, $0 = H(\xi) + \varepsilon_p(\xi)$, si $p \notin E$. Il en résulte $H(\xi) \in Z_E$, où Z_E est l'anneau des rationnels de la forme

$$\frac{n}{\prod_{p \in E} p^{\nu_p}} \qquad (n, \nu_p \in Z).$$

2. Eléments algébriques de $\Omega_E(Q)$.

2.1 (BOURBAKI [3], chap. 4, § 2 et [4], § 11, Exercice 1). - Soit A une algèbre, avec élément unité e, sur le corps K (qu'on identifie à la sous-algèbre $K.e$). Pour tout polynôme $f = a_0 + a_1 + \ldots + a_n X^n$ de l'anneau $K[X]$ et tout élément $\xi \in A$, on pose : $f(\xi) = a_0 e + a_1 \xi + \ldots + a_n \xi^n$.

L'application $f \to f(\xi)$ de l'algèbre $K[X]$ dans l'algèbre A est une représentation. L'image de $K[X]$ dans cette représentation est la sous-algèbre de A engendrée par e et ξ, qu'on note $K[\xi]$. $K[\xi]$ est isomorphe à l'algèbre quotient $K[X]/\alpha$ où α est l'idéal de $K[X]$ formé des polynômes f tels que $f(\xi) = 0$ (on dit que ξ est racine de f).

Si $K[\xi]$ est de dimension finie sur K, on dit que ξ est algébrique sur K. L'idéal α est alors de la forme (f_0) où f_0 est un polynôme unitaire différent de 0 de $K[X]$, qu'on appelle polynôme minimal de ξ et qu'on note $Pm_A(\xi, X)$. Par définition, le degré de ξ est le degré s de son polynôme minimal. $s = [K[\xi] : K]$: on dira que $K[\xi]$ est un anneau d'éléments algébriques de degré s. Les éléments de $K[\xi]$ sont de degré $\leqslant s$, et s'expriment de manière unique par rapport à la base $(e, \xi, \ldots, \xi^{s-1})$:

$$f(\xi) = b_0 e + b_1 \xi + \ldots + b_{s-1} \xi^{s-1} \qquad (b_i \in K).$$

Si $\eta \in K[\xi]$ est de degré s, $(e, \eta, \ldots, \eta^{s-1})$ est une base de $K[\xi]$ donc $K[\eta] = K[\xi]$.

Si le polynôme minimal de ξ est irréductible dans $K[X]$, $K[\xi]$ est un corps.

Si $Pm_A(\xi , X) = X^s + a_1 X^{s-1} + \ldots + a_s$, on appellera norme de ξ le rationnel

$$Nm_A(\xi) = (-1)^s a_s .$$

2.2. - Ces notions, appliquées au cas $K = Q.e$, $A = \Omega(Q)$ (resp. $K.Qe_E = Q_E$, $A = \Omega_E(Q)$) permettent de définir des éléments algébriques ξ dans $\Omega(Q)$ (resp. $\Omega_E(Q)$). On notera $Q.e[\xi]$ (resp. $Q_E[\xi]$) les algèbres correspondantes. " ξ élément entier algébrique" signifiera : "les coefficients du polynôme minimal sont entiers rationnels".

Si $\xi \in \Omega(Q)$ est algébrique sur $Q.e$, sa composante $\xi.e_p$ dans $\Omega_{(p)}$ est algébrique sur $Q.e_p$ et on a :

$$Pm_{\Omega}(\xi , X) = \operatorname*{ppcm}_{p\in P} Pm_{\Omega_{(p)}}(\xi e_{(p)} , X) = \operatorname*{ppcm}_{p\in P} Pm_{\Omega_p}(\xi_p , X)$$

$Pm_{\Omega_p}(\xi_p , X)$ est le polynôme irréductible de ξ_p , élément de Q_p , sur Q . Conséquence : <u>tous les facteurs irréductibles d'un polynôme minimal sont distincts</u>.

La composante $\xi.e_E$ de $\xi \in \Omega(Q)$ dans $\Omega_E(Q)$ est algébrique sur Q_E , et on a :

$$Pm_{\Omega_E(Q)}(\xi e_E , X) \text{ divise } Pm_{\Omega(Q)}(\xi , X) .$$

En particulier, si $\xi e_E = \xi$, c'est-à-dire $\xi \in \Omega_E(Q)$, on voit que :

$$Pm_{\Omega(Q)}(\xi , X) = \begin{cases} Pm_{\Omega_E(Q)}(\xi , X) & \text{si } X \mid Pm_{\Omega_E}(\xi , X) \\ XPm_{\Omega_E(Q)}(\xi , X) & \text{si } X \nmid Pm_{\Omega_E}(\xi , X) \end{cases}$$

Par la suite, on se limitera à l'étude des <u>éléments algébriques</u> ξ <u>de</u> $\Omega_E(Q)$.

ξ étant algébrique et $(E_i)_{i=1,\ldots,m}$ étant une partition quelconque de E , la composante ξe_{E_i} de ξ dans Ω_{E_i} est algébrique, et on a

$$Pm_{\Omega_E}(\xi , X) = \operatorname*{ppcm}_{i=1,\ldots,m} Pm_{\Omega_{E_i}}(\xi e_{E_i} , X) .$$

<u>Soit</u> $(E_0)^{\xi}_{0=1,\ldots,m}$ <u>la partition particulière de</u> E <u>associée à l'élément algébrique</u> ξ <u>de</u> Ω_E <u>de la manière suivante</u> : $p \in E_i$ <u>si</u> $p \in E$ <u>et</u> $\xi.e_{E_i}$ <u>est racine dans</u> Ω_{E_i} <u>de</u> f_i , <u>où</u> $f = \prod_{i=1}^{m} f_i$ <u>est la décomposition en facteurs irréductibles dans</u> $Q[X]$ <u>du polynôme minimal de</u> ξ

$$f(X) = Pm_{\Omega_E}(\xi , X) .$$

On a alors

$$f_i = Pm_{\Omega_{E_i}}(\xi e_{E_i}, X) .$$

D'où :

$$Pm_{\Omega_E}(\xi, X) = \prod_{i=1}^{m} Pm_{\Omega_{E_i}}(\xi e_{E_i}, X)$$

Si $\alpha = g(\xi)$, $(g \in Q[X])$ est un élément de $Q_E[\xi]$, sa composante αe_{E_i} dans Ω_{E_i} est un élément de $Q_{E_i}[\xi e_{E_i}]$, car

$$\alpha e_{E_i} = g(\xi).e_{E_i} = g(\xi e_{E_i}) .$$

De manière plus précise, on a le résultat suivant :

LEMME 1. - Tout anneau $Q_E[\xi]$ d'éléments algébriques de $\Omega_E(Q)$ est composé direct de m corps $Q_{E_i}[\xi e_{E_i}]$ d'éléments algébriques de $\Omega_{E_i}(Q)$, où $(E_i)_{i=1,\ldots,m}^{\xi}$ est la partition de E associée à l'élément algébrique ξ .

Démonstration. - Il reste à démontrer que, étant donnés m éléments algébriques α_i appartenant respectivement à $Q_{E_i}[\xi e_{E_i}]$, l'élément α de Ω_E de composantes α_i dans Ω_{E_i} (c'est-à-dire : $\alpha = \sum_{i=1}^{m} \alpha_i e_{E_i}$) appartient à $Q_E[\xi]$,

$$\alpha_i = g_i(\xi e_{E_i}) \qquad \text{où } g_i \in Q[X] .$$

Comme les $f_i = Pm_{\Omega_{E_i}}(\xi_i, X)$ sont premiers entre eux dans $Q[X]$, il existe un polynôme $g \in Q[X]$, unique mod f , tel que

$$g \equiv g_i \mod f_i .$$

Or $\alpha_i = g_i(\xi e_{E_i}) = g(\xi e_{E_i})$. D'où :

$$\alpha = \sum_{i=1}^{m} e_{E_i} g(\xi e_{E_i}) = g(\xi) .$$

Remarque. - $Q_E[\xi]$ étant isomorphe à $Q[X]/(f)$ et $Q_{E_i}[\xi]$ à $Q[X]/(f_i)$, le lemme 1 est équivalent au résultat suivant :

L'anneau $Q[X]/(f)$ est isomorphe à l'anneau produit des m corps $Q[X]/(f_i)$.

Exemple. - Si $Pm_{\Omega_E}(\xi, X)$ est le produit de k facteurs du 1er degré, où k est le nombre d'éléments de E , $Q_E[\xi]$ est isomorphe à Q^k .

Notation. - ξ étant un élément algébrique de Ω_E , $\xi_p^{(i)}$ ($i = 1 , \ldots , s$)

désignent les racines dans Ω_p de $Pm_{\Omega_E}(\xi , X)$ (polynôme minimal de degré s, dont les racines dans Ω_p sont distinctes puisque tous ses facteurs irréductibles sont distincts). Si $p \in E$, $\xi_p^{(1)} = \xi_p$. On a la relation :

$$Nm_{\Omega_E}(\xi) = \prod_{i=1}^{s} \xi_p^{(i)} \qquad (\forall\ p \in P)$$

3. Anneaux d'éléments algébriques de $V_E(Q)$.

3.1. - Si un élément γ de V_E est algébrique sur Q_E, l'algèbre $Q_E[\gamma]$ est contenue dans V_E : on la désignera par "anneau d'éléments algébriques de V_E".

On se propose de démontrer pour $Q_E[\gamma]$ un résultat généralisant le suivant : Dans tout corps $Q(\gamma)$ de nombres algébriques contenu dans R, il existe des éléments de l'ensemble S ayant le degré du corps [7].

Les ensembles de V_E généralisant l'ensemble S de R sont les ensembles $\mathfrak{S}_E^{p'}$ définis comme suit. (Voir également [1], avec des notations différentes.)

p' désignant une valuation figurant ou non dans E, $\mathfrak{S}_E^{p'}$ est l'ensemble des éléments

$$\theta = \sum_{p \in E} \theta_p\, e_{(p)} \qquad (\theta_p \in Q_p)$$

de V_E racines d'un polynôme f unitaire de $Q[X]$, tel que $f(0) \neq 0$, et vérifiant les conditions : $(\overline{C}_p)$ $(p \in E)$; $(\overline{\Gamma}_p)$ $(p \in \complement_P E)$ et $(C_{p'})$ ou $(\Gamma_{p'})$ suivant que $p' \in E$ ou non. Les conditions (C) et (Γ) sont les suivantes :

$(\overline{C}_p)$ $|\theta_p|_p > 1$. Les autres racines de f dans Ω_p appartiennent au disque

$$|X|_p \leqslant 1 .$$

$(\overline{\Gamma}_p)$ Les racines de f dans Ω_p appartiennent au disque $|X|_p \leqslant 1$.

$(C_{p'})$ $|\theta_{p'}|_{p'} > 1$. Les autres racines de f dans $\Omega_{p'}$ appartiennent au disque

$$|X|_{p'} < 1 .$$

$(\Gamma_{p'})$ Les racines de f dans $\Omega_{p'}$ appartiennent au disque $|X|_p < 1$

Propriétés :

1° Le polynôme f, figurant dans la définition, est de la forme :

$$q\, f(X) = q\, X^s + q_1\, X^{s-1} + \ldots + q_s \qquad (q \text{ et } q_i \in Z)$$

où $q = \prod_{p \in E^-} p^{n_p}$ et $(q , q_1) = 1$, $q_s \neq 0$.

De plus on montre que $f = Pm_{\Omega_E}(\theta , X)$.

Notation. - E^- désigne l'ensemble E d'où l'on exclut (0) éventuellement. E^+ désigne l'ensemble $E \cup (0)$.

2° On montre facilement que si $\theta \in \mathcal{S}_E^{p'}$, $\theta^n \in \mathcal{S}_E^{p'}$ (n entier > 0) et que les polynômes $Pm_{\Omega_E}(\theta^n , X)$ sont premiers entre eux 2 à 2, et ont tous le degré s .

3° Il existe la relation suivante entre les ensembles $\mathcal{S}_E^{p'}$ et $\mathcal{S}_{E_i}^{p'}$:

$(E_i)_{i=1,2,\ldots,m}$ étant une partition de E , et θ_i appartenant à $\mathcal{S}_{E_i}^{p'}$, $(i = 1 , \ldots , m)$, l'élément θ de V_E défini par : $\theta = \sum_{i=1}^{m} \theta_i e_{E_i}$ appartient à $\mathcal{S}_E^{p'}$ (se démontre en utilisant les relations entre polynômes minimaux dans Ω_E et Ω_{E_i} du § 2.2).

3.2. - On démontrera d'abord le résultat annoncé dans le cas particulier où $Q_E[\gamma]$ est un corps :

LEMME 2. - Dans tout corps $Q_E[\gamma]$ d'éléments algébriques de $V_E(Q)$, il existe des éléments de l'ensemble $\bigcap_{p' \in F} \mathcal{S}_E^{p'}$ ayant le degré du corps (F sous-ensemble fini de P).

3.2.1. - On suppose $Q_E[\gamma]$ engendré par un élément entier algébrique γ , et on cherche un élément θ de $Q_E[\gamma]$ de la forme :

$$\theta = \frac{\alpha}{\prod_{p \in E^-} p^r} \qquad (1) \qquad (r \text{ entier} > 0)$$

où α est un élément entier algébrique de $Q_E[\gamma]$ de la forme :

$$\alpha = x_0 e_E + x_1 \gamma + \ldots + x_{s-1} \gamma^{s-1} \qquad (x_i \in Z)$$

(s est le degré de $Q_E[\gamma]$), ce qu'on notera

$$\alpha = \Lambda(\gamma , x) .$$

On a : $\alpha_p = x_0 + x_1 \gamma_p + \ldots + x_{s-1} \gamma_p^{s-1}$ $(p \in E)$, ce qu'on notera :

$$\alpha_p = \Lambda(\gamma_p , x) .$$

Pour tout $p \in P$, on pose :

$$\alpha_p^{(i)} = x_0 + x_1 \gamma_p^{(i)} + \ldots + x_{s-1} \gamma_p^{(i)\,s-1} = \Lambda(\gamma_p^{(i)} , x)$$

($\gamma_p^{(i)}$ défini dans le § 2.2).

Pour que θ , défini par (1), soit un élément de $Q_E[\gamma]$ de degré s , il suffit

que les inégalités : A_p $(p \in E^-)$, B_p $(p \in F^-$, $p \notin E)$ et A_0 ou B_0 suivant que $(0) \in E$ ou non, soient vérifiées. (A_p) et (B_p) sont définies par :

(A_p) $(p \neq (0))$ $\quad |\alpha_p|_p > p^{-r} \qquad |\alpha_p^{(i)}|_p \leqslant p^{-(r+1)} \qquad (i = 2, \ldots, s)$

(A_0) $\quad |\alpha_0|_0 > \prod_{p \in E^-} p^r \qquad |\alpha_0^{(i)}|_0 \leqslant \eta \prod_{p \in E^-} p^r \qquad (i = 2, \ldots, s)$

(B_p) $(p \neq 0)$ $\quad |\alpha_p^{(i)}|_p \leqslant p^{-1} \qquad (i = 1, 2, \ldots, s)$

(B_0) $\quad |\alpha_0^{(i)}|_0 \leqslant \eta \prod_{p \in E^-} p^r \qquad (i = 1, 2, \ldots, s)$

où η désigne un nombre réel : $0 < \eta < 1$.

En effet les racines dans Ω_p du polynôme $Pm_{\Omega_E}(\alpha , X)$ figurent parmi les $\alpha_p^{(i)}$ $(i = 1 , 2 , \ldots , s)$ $(\alpha_p = \alpha_p^{(1)})$; or α est de degré s , car un système d'inégalités (A_p) entraîne que α_p est de degré s dans Q_p . Donc les $\alpha_p^{(i)}$ sont les racines de $Pm_{\Omega_E}(\alpha , X)$. Les conditions (A_p) $(p \in E^-)$, (B_p) $(p \in F^-$, $p \notin E)$, (A_0) ou (B_0) suivant que $(0) \in E$ ou non, entraînent alors immédiatement pour le polynôme $Pm_{\Omega_E}(\theta , X)$ les propriétés (C_p) $(p \in E^-)$, (Γ_p) $(p \in F^-$, $p \notin E)$, (C_0) ou (Γ_0) suivant que $(0) \in E$ ou non, θ appartient donc à $\bigcap_{p' \in F \cup E^+} S_E^{p'}$ qui est contenu dans $\bigcap_{p' \in F} S_E^{p'}$.

3.2.2. - La recherche d'un élément $x = (x_0 , \ldots , x_{s-1})$ de Z^s tel que les formes linéaires $\Lambda(\gamma_p^{(i)} , x)$ vérifient les conditions (A_p) et (B_p) nécessite le résultat intermédiaire suivant :

LEMME 3. - Soient :

$L_0^{(i)}(x)$ $(i = 1 , \ldots , s)$, s formes linéaires en $x_0 , \ldots , x_{s-1}$, à coefficients dans R , de déterminant $\Delta_0 \neq 0$.

$L_p^{(i)}(x)$ $(i = 1 , \ldots , s)$, s formes linéaires en $x_0 , \ldots , x_{s-1}$, à coefficients dans Q_p , de déterminant $\Delta_p \neq 0$.

Il existe un système $x = (x_0 , \ldots , x_{s-1})$ d'entiers non tous nuls, tels que :

$$|L_0^{(i)}(x)|_0 \leqslant c_i \qquad (i = 1 , 2 , \ldots , s)$$

$$|L_p^{(i)}(x)|_p \leqslant p^{-\lambda_{p,i}} \qquad (i = 1 , 2 , \ldots , s) \text{ et } p \in E^-$$

si on a la relation :

$$\prod_{i=1}^{s} c_i \prod_{p \in E^-} p^{-\sigma_p} \geqslant |\Delta_0|_0 \prod_{p \in E} |\Delta_p|_p \qquad \text{avec } \sigma_p = \sum_{i=1}^{s} \lambda_{p,i}$$

(E^- ensemble fini de nombres premiers distincts, c_i réel > 0 , $\lambda_{p,i}$ entier).

Cette propriété résulte du théorème de Minkowski et de l'évaluation du déterminant $m(G)$ du sous-réseau G de Z^s : $G = \bigcap_{p \in E} G_p$, où le réseau G_p est défini par :

$$|L_p^{(i)}(x)|_p \leqslant p^{-\lambda_{p,i}} . \qquad (i = 1 , 2 , \ldots , s)$$

Mlle E. LUTZ [5] démontre que :

$$m(G) = \prod_{p \in E} m(G_p) \qquad ([5], \text{ I, § 5})$$

et

$$m(G_p) = p^{\sigma_p} |\Delta_p|_p \qquad ([5], \text{ I, § 3 et 4})$$

Remarque. - On peut remplacer l'hypothèse $L_0^{(i)}(x)$ à coefficients dans R , par $L_0^{(i)}(x)$ à coefficients dans C , à condition qu'avec chaque forme figure sa conjuguée et que les 2 formes soient majorées en valeur absolue par le même coefficient c_i .

3.2.3. - Application à la recherche d'un $x \in Z^s$ tel que les formes linéaires $\Lambda(\gamma_p^{(i)} , x)$ vérifient les conditions (A_p) et (B_p) .

Afin de pouvoir appliquer le lemme 3, il faut se ramener à des majorations de valeurs absolues de formes linéaires à coefficients dans C ou dans Q_p .

$$\Lambda(\gamma_p^{(i)} , x) = x_0 + x_1 \gamma_p^{(i)} + \ldots + x_{s-1} \gamma_p^{(i)\,s-1} \qquad (p \neq (0) \text{ et } \gamma_p^{(i)} \neq \gamma_p)$$

est à coefficients dans Ω_p .

Si $p \notin E$, les inégalités $|x_j|_p \leqslant p^{-1}$ $(j = 0 , \ldots , s - 1)$ entraîneront

$$|\Lambda(\gamma_p^{(i)} , x)|_p \leqslant p^{-1}$$

c'est-à-dire la condition (B_p) . On posera donc :

$$(2) \qquad L_p^{(i)}(x) = x_{i-1} \text{ et } \lambda_{p,i} = 1 \qquad (i = 1 , \ldots , s) .$$

Si $p \in E$, $\gamma_p^{(i)}$ est algébrique de degré s sur Q , mais de degré $\leqslant s - 1$ sur Q_p , puisque $Pm_{\Omega_E}(\gamma , X)$ a une racine γ_p dans Q_p , c'est-à-dire

$$\gamma_p^{(i)\,s-1} = c_{s-2,p} \gamma_p^{(i)\,s-2} + \ldots + c_{0,p} \qquad (\text{où } c_{h,p} \in Q_p \text{ et } |c_{h,p}|_p \leqslant 1) .$$

On a

$$\Lambda(\gamma_p^{(i)} , x) = x_0 + c_{0,p} x_{s-1} + \ldots + (x_{s-2} + c_{s-2,p} x_{s-1}) \gamma_p^{(i)\,s-2} .$$

Les inégalités

$$|x_j + c_{j,p}\, x_{s-1}|_p \leqslant p^{-(r+1)} \qquad (j = 0 , \dots , s - 2)$$

entraîneront

$$|\Lambda(\gamma_p^{(i)} , x)|_p \leqslant p^{-(r+1)}$$

c'est-à-dire les $s - 1$ dernières égalités de la condition (A_p) . On posera donc

$$L_p^{(i)}(x) = x_{i-2} + c_{i-2,p}\, x_{s-1} \qquad (i = 2 , \dots , s) \tag{3}$$

et

$$\lambda_{p,i} = r + 1$$

Les formes $\Lambda(\gamma_0^{(i)} , x)$ sont à coefficients dans $\mathbf{C}$, 2 à 2 conjuguées. On posera donc simplement :

$$L_0^{(i)}(x) = \Lambda(\gamma_0^{(i)} , x) \qquad (i = 1 , 2 , \dots , s)$$

et, lorsqu'on a affaire à des majorations, c'est-à-dire pour $i = 2 , \dots , s$ $((0) \in E)$ et $i = 1 , 2 , \dots , s$ $((0) \notin E)$, on posera

$$c_i = \eta \prod_{p \in E^-} p^r .$$

Restent les formes $\Lambda_p(\gamma_p , x)$ $(p \in E)$ pour lesquelles les conditions A_p imposent des minorations en valeur absolue. Or la formule du produit des valuations appliquée au rationnel :

$$\prod_{i=1}^{s} \Lambda(\gamma_p^{(i)} , x) = \prod_{i=1}^{s} \alpha_p^{(i)}$$

(rationnel indépendant de p , non nul si $x \neq (0 , \dots , 0)$, car dans Q_p tout $\gamma_p^{(i)}$ est exactement de degré s sur Q , ici intervient l'hypothèse $Q_E[\gamma]$ est un corps) donne :

$$\prod_{p \in E^+} \prod_{i=1}^{s} |\Lambda(\gamma_p^{(i)} , x)|_p \geqslant 1 .$$

D'où pour tout $p' \in E^+$:

$$|\Lambda(\gamma_{p'} , x)|_{p'} \geqslant \left(\prod_{i=2}^{s} |\Lambda(\gamma_{p'}^{(i)} , x)|_{p'} \prod_{\substack{p \in E^+ \\ p \neq p'}} |\Lambda(\gamma_p^{(i)} , x)|_p \right)^{-1} \tag{4}$$

c'est-à-dire une minoration de $|\Lambda(\gamma_{p'} , x)|_{p'}$ en fonction des majorations en valeur absolue de toutes les formes

$$\Lambda(\gamma_p^{(i)} , x) , \quad (p \in E^+ , \ \gamma_p^{(i)} \neq \gamma_p)$$

et en particulier de majorations en valeur absolue des formes $\Lambda(\gamma_p , x)$ ($p \in E$,

$p \neq p'$).

On posera donc :

$$L_p^{(1)}(x) = \Lambda(\gamma_p , x) \qquad (p \in E) . \tag{5}$$

Le choix des majorations correspondantes :

$$p^{-\lambda_{p,1}} \text{ et } c_1 \qquad (\text{si } (0) \in E)$$

est assez arbitraire pourvu évidemment qu'on les choisisse supérieures aux minorations des conditions A_p . On prendra :

$$c_1 = \prod_{p \in E^-} p^{2r} \quad (\text{si } (0) \in E) \quad \text{et} \quad \lambda_{p,1} = [r/2] \qquad (p \in E^-)$$

On peut alors appliquer le lemme 3 aux formes linéaires définies à partir des formes $\Lambda(\gamma_p^{(i)} , x)$ par les conditions (2) , (3) , (5) de ce § 3.2.3. et aux $\lambda_{p,i}$ et c_i associés. En effet, on démontre aisément que les déterminants correspondants Δ_0 et Δ_p sont $\neq 0$.

Le reste de la démonstration consiste en la recherche d'un réel η $(0 < \eta < 1)$ et d'un entier positif r tels que l'inégalité du lemme 3 soit vérifiée et que le 2e membre de (4) soit supérieur à p'^{-r} (pour $p' \in E^-$) et supérieur à $\prod_{p \in E^-} p^r$ (pour $p' = (0)$ si $(0) \in E$).

On trouve les conditions suivantes :

<u>Si $(0) \in E$</u> :

$$\begin{cases} \eta^{s-1}\, a^{2r-[r/2]} \geqslant a^{s-1}\, b^s\, |\Delta_0|_0 \prod_{p \in E^-} |\Delta_p|_p \\ \eta^{-(s-1)}\, a^{-2r+[r/2]} \left(\inf_{p \in E^-} p\right)^{r-[r/2]} > a^{-(s-1)} \end{cases}$$

<u>Si $(0) \notin E$</u> :

$$\begin{cases} \eta^{s}\, a^{r-[r/2]} \geqslant b^s\, |\Delta_0|_0 \prod_{p \in E} |\Delta_p|_p \\ \eta^{-s}\, a^{r-[r/2]} \left(\inf_{p \in E} p\right)^{r-[r/2]} > a^{s-1} \end{cases}$$

(où $a = \prod_{p \in E^-} p$ et $b = \prod_{\substack{p \in F^- \\ p \notin E}} p$).

Il est possible de choisir $\eta(r)$ tel que, <u>pour</u> r <u>assez grand</u>, ces inégalités soient vérifiées. On peut définir η par exemple par

$$\eta^{s-1}\, a^{2r-[r/2]} = \left(\inf_{p\in E} p\right)^{r/3} \qquad \text{si } (0)\in E\,,$$

$$\eta^{s}\, a^{r-[r/2]} = \left(\inf_{p\in E} p\right)^{r/3} \qquad \text{si } (0)\notin E\,.$$

On a donc construit un élément α de $Q_E[\gamma]$ vérifiant les conditions (A_p) et (B_p) du § 3.2.1. : la démonstration du lemme 2 est terminée.

3.3. - On peut alors démontrer le résultat plus général :

THÉORÈME 1. - Dans tout anneau $Q_E[\gamma]$ d'éléments algébriques de $V_E(Q)$, il existe des éléments de l'ensemble $\bigcap_{p'\in F} \mathcal{S}_E^{p'}$ ayant le degré de l'anneau (F sous-ensemble fini de P).

Démonstration. - Soit $(E_i)_{i=1,\dots,m}^{\gamma}$ la partition de E relative à l'élément algébrique γ (§ 2.2), et soit s_i le degré du corps $Q_{E_i}[\gamma e_{E_i}]$, corps d'éléments algébriques de V_{E_i}.

Le lemme 3 démontre l'existence d'un élément θ_i de $Q_{E_i}[\gamma e_{E_i}]$, de degré s_i appartenant à $\bigcap_{p'\in F} \mathcal{S}_{E_i}^{p'}$. La propriété 3 des ensembles $\mathcal{S}_E^{p'}$ (§ 3.1) montre que les θ_i^n ($n = 1, 2, \dots$) sont des éléments de degré s_i de $Q_{E_i}[\gamma e_{E_i}]$, et que leurs polynômes minimaux sont premiers entre eux 2 à 2.

On peut choisir un système $(n_1, \dots, n_m)$ d'entiers positifs tels que les polynômes $\mathrm{Pm}_{\Omega_{E_i}}(\theta_i^{n_i}, x)$ $(i = 1, \dots, m)$ soient premiers entre eux 2 à 2.

Soit $\theta = \sum_{i=1}^{m} \theta_i^{n_i} e_{E_i}$. θ appartient à $\bigcap_{p'\in F} \mathcal{S}_E^{p'}$ (propriété 3 des ensembles $\mathcal{S}_E^{p'}$ (§ 3.1)).

D'autre part :

$$\mathrm{Pm}_{\Omega_E}(\theta, X) = \operatorname*{ppcm}_{i=1,\dots,m} \mathrm{Pm}_{\Omega_{E_i}}(\theta e_{E_i}, X) \qquad (\S\ 2.2).$$

Il en résulte que θ est de degré s.

4. Une caractérisation des éléments algébriques de $V_E(Q)$.

4.1. - Les nombres algébriques réels peuvent être caractérisés par l'existence d'approximations rationnelles "régulièrement réparties" [7].

Cette propriété se généralise aux éléments algébriques de $V_E(Q)$, le rôle de Z

étant alors joué par le sous-anneau de Q_E : $Z_E \cdot e_E$, où Z_E est l'anneau des rationnels $\dfrac{m}{\prod_{p \in E^-} p^{\nu_p}}$ (§ 1.3).

THÉORÈME 2. - Un élément α de $V_E(Q)$ est algébrique sur Q_E si et seulement s'il existe deux suite infinies (u_n) et (v_n) de rationnels de l'anneau Z_E telles que :

$$\|v_n \alpha - u_n e_E\| < c\rho^n$$

$$\|v_{n+1} e_E - v_n \theta\| < c\rho^n$$

et éventuellement, si $(0) \notin E$:

$$|u_n|_0 < c\rho^n$$

$$|v_{n+1}|_0 < c\rho^n$$

où ρ et c sont des réels : $0 < \rho < 1$, $0 < c$, et θ un élément de $V_E(Q)$ tel que $|\theta_p|_p > 1$ $(p \in E)$.

Le degré s de α vérifie l'inégalité

$$s - 1 \leqslant \frac{1}{k\eta}$$

où k est le nombre d'éléments de E^+ et η le réel > 0 défini par

$$\rho = \left(\prod_{p \in E} |\theta_p|_p \right)^{-\eta} .$$

La démonstration utilise le théorème 1, pour le cas $F = E^+$, et une caractérisation de l'ensemble $\bigcap_{p' \in E^+} \mathbb{S}_E^{p'}$ au moyen de la décomposition d'Artin (§ 1.3) (cas particulier de la caractérisation donnée dans [1], § 3.1) :

Soit θ un élément de V_E tel que $|\theta_p|_p > 1$ $(p \in E)$. θ appartient à $\bigcap_{p' \in E^+} \mathbb{S}_E^{p'}$ si et seulement s'il existe un élément inversible λ de V_E tel que :

$$\sup_{p' \in E^+} |\varepsilon_{p'}(\lambda\theta^n)|_{p'} < c\rho^n$$

($n > n_0$, c réel > 0 , ρ réel : $0 < \rho < 1$).

λ est alors un élément algébrique de $Q_E[\theta]$.

Dans le cas où $\theta \in \bigcap_{p' \in E^+} \mathbb{S}_E^{p'}$, on peut choisir pour λ tout élément entier algébrique de $Q_E[\theta]$, et l'on a (pour $n > n_0$) :

$$H(\lambda\theta^n) = Nm_{\Omega_E}(\lambda\theta^n)$$

$$\varepsilon_p(\lambda\theta^n) = -\sum_{i=2}^{s} \lambda_p^{(i)}\, \theta_p^{(i)^n} \qquad (p \in E)$$

$$= -H(\lambda\theta^n) \qquad (p \notin E)\ .$$

4.2. - Principe de la démonstration. - Elle est analogue à la démonstration classique [7].

Si α est algébrique, on écrit $\alpha = \lambda/\mu$, où λ et μ sont 2 éléments entiers algébriques de $Q_E[\alpha]$, et on prend pour θ un élément de $\bigcap_{p' \in E^+} S_E^{p'}$ appartenant à $Q_E[\alpha]$. Les rationnels : $u_n = H(\lambda\theta^n)$, $v_n = H(\mu\theta^n)$ remplissent les conditions énoncées. Réciproquement, s'il existe 2 suites (u_n) et (v_n) vérifiant les conditions du théorème, on montre que $\frac{e_E \cdot v_n}{\theta^n} \to \mu$ et que

$$\sup_{p' \in E^+} |\varepsilon_{p'}(\mu\theta^n)|_{p'} < K\rho^n\ .$$

D'où il résulte : θ appartient à l'ensemble $\bigcap_{p' \in E^+} S_E^{p'}$, et μ est un élément algébrique de $Q_E[\theta]$.

Par raisonnement analogue, on montre que $\frac{e_E \cdot u_n}{\theta^n} \to \lambda$, et que λ est un élément algébrique de $Q_E[\theta]$. On en déduit facilement $\alpha = \frac{\lambda}{\mu}$; α est un élément algébrique de $Q_E[\theta]$.

L'inégalité vérifiée par le degré s de α résulte de la formule du produit des valuations appliquée au rationnel $Nm_{\Omega_E}(\theta)$.

BIBLIOGRAPHIE

[1] BERTRANDIAS (Françoise). - Caractérisation des ensembles S_q par la répartition modulo 1 en p-adique, Séminaire Dubreil-Pisot : Algèbre et théorie des nombres, t. 17, 1963/64, n° 11, 20 p.

[2] BOURBAKI (Nicolas). - Algèbre, Chapitre 1, 2e édition. - Paris, Hermann, 1958 (Act. scient. et ind., 934 = 1144 ; Bourbaki, 4).

[3] BOURBAKI (Nicolas). - Algèbre, Chapitres 4-5, 2e édition. - Paris, Hermann, 1959 (Act. scient. et ind., 1102 ; Bourbaki, 11).

[4] BOURBAKI (Nicolas). - Algèbre, Chapitre 8.-- Paris, Hermann, 1958 (Act. scient. et ind., 1261 ; Bourbaki, 23).

[5] LUTZ (Elisabeth). - Sur les approximations diophantiennes linéaires P-adiques. - Paris, Hermann, 1955 (Act. scient. et ind., 1224 ; Publ. Inst. Math. Univ. Strasbourg, 12).

[6] MAHLER (K.). - Lectures on diophantine approximations, Part 1. - Ann Arbor, University of Notre-Dame, 1961.

[7] PISOT (Charles). - Sur quelques approximations rationnelles caractéristiques des nombres algébriques, C. R. Acad. Sc. Paris, t. 206, 1938, p. 1862-1864.