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. nº 19, p. 1-15

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

© Séminaire Delange-Pisot-Poitou. Théorie des nombres (Secrétariat mathématique, Paris), 1963-1964, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.



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 S). Le plan est le suivant :

- § 1 : Définitions Notations.
- § 2 : Eléments algébriques de l'algèbre $\Omega_E(Q)\cong \prod \Omega$. Résultat essentiel : le lemme 1.
- § 3 : Eléments algébriques de l'algèbre $V_E(Q)\cong \bigcap_{p\in E}Q_p$. 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 $V_{\rm E}({\rm Q})$: 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 O la valuation ordinaire ($Q_0 = R$, $\Omega_0 = C$, R corps des réels, C corps des complexes). E désignera un sous-ensemble <u>fini</u> 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 $\prod\limits_{p\in P}Q$ (algèbre produit de Q-algèbres au sens de BOURBAKI, [2], § 8-10), définie par

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

sauf pour un nombre fini de p au plus } .

Soit $\Omega(\mathbb{Q})$ la sous-algèbre de l'algèbre produit $\prod\limits_{\mathbf{p}\in\mathbf{P}}\Omega$ 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 } .

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

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

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

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

1.2. - Soit $\Omega_{\rm E}({\rm Q})$ (resp. ${\rm V_E}({\rm Q})$) la sous-algèbre de $\Omega({\rm Q})$ définie par :

$$\Omega_{\mathbf{E}}(\mathbf{Q}) = \{ \xi \in \Omega(\mathbf{Q}) ; \xi_{\mathbf{p}} = 0 \text{ si } \mathbf{p} \notin \mathbf{E} \}$$

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

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

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 $\xi \in \Omega(\mathbb{Q})$, $\xi \cdot e_E$ est l'élément de $\Omega_E(\mathbb{Q})$ ayant même projection ξ que ξ dans Ω ($p \in E$).

Le sous-anneau de $V_{\rm E}({\rm Q})$ isomorphe à ${\rm Q}$:

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

sera noté ${f Q}_{
m E}$.

On désignera fréquemment $\,\Omega_{\rm E}^{}({\rm Q})\,\,$ et $\,{\rm V}_{\rm E}^{}({\rm Q})\,\,$ par $\,\Omega_{\rm E}^{}\,\,$ et $\,{\rm V}_{\rm E}^{}\,\,$.

 $\Omega_{\rm E}$ est l'anneau composé direct des anneaux $\Omega_{\rm E}$ (i = 1 , ... , 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. - <u>Théorème d'Artin</u> ([1], § 2.2). - On démontre que <u>peur tout élément</u> ξ <u>de</u> V(Q), <u>il existe une décomposition unique</u>:

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

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

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

Si $\xi \in V_E(Q)$, $0 = H(\xi) + \epsilon_p(\xi)$, si $p \not\in E$. Il en résulte $H(\xi) \in Z_E$, où Z_E est l'anneau des rationnels de la forme

$$\frac{n}{\prod\limits_{p\in\mathbb{Z}}\nu^{p}} \qquad \qquad (n,\nu_{p}\in\mathbb{Z}).$$

2. Eléments algébriques de $\Omega_{\rm E}({\bf Q})$.

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 $f = a_0 + a_1 + \cdots + a_n \times^n$ de l'anneau K[X] et tout élément $\xi \in A$, on pose : $f(\xi) = a_0 + a_1 + \cdots + a_n + a_n + a_n + \cdots + a_n + a$

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 <u>la sous-algèbre de A engendrée par</u> e <u>et</u> 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[ξ] est de dimension finie sur K , on dit que ξ est <u>algébrique</u> 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 <u>polynôme minimal de</u> 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 <u>anneau d'éléments algébriques</u> de degré s . Les éléments de $K[\xi]$ sont de degré s , et s'expriment de manière unique par rapport à la base $(e, \xi, \ldots, \xi^{s-1}):$

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

Si $\eta \in K[\xi]$ est de degré s , (e , η , ... , η^{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 $Pm_{A}(\xi$, $X) = X^{S} + a_{1} X^{S-1} + \dots + a_{S}$, 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 $\xi \in \Omega(\mathbb{Q})$ est algébrique sur \mathbb{Q} .e , sa composante ξ .e dans $\Omega_{(p)}$ est algébrique sur \mathbb{Q} .e et on a :

$$Pm_{\Omega}(\xi, X) = ppcm Pm_{\Omega(p)}(\xi e_{(p)}, X) = ppcm Pm_{\Omega(p)}(\xi_{p}, X)$$

 $\Pr_{\mathbb{Q}_p}(\xi_p,X)$ est le polynôme irréductible de ξ_p , élément de \mathbb{Q}_p , sur \mathbb{Q} . Conséquence : tous les facteurs irréductibles d'un polynôme minimal sont distincts.

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

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

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

$$\operatorname{Pm}_{\Omega(Q)}(\xi, X) = \begin{cases} \operatorname{Pm}_{\Omega_{E}(Q)}(\xi, X) & \text{si } X \mid \operatorname{Pm}_{\Omega_{E}}(\xi, X) \\ \operatorname{XPm}_{\Omega_{E}(Q)}(\xi, X) & \text{si } X \not \mid \operatorname{Pm}_{\Omega_{E}}(\xi, X) \end{cases}$$

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

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

$$\operatorname{Pm}_{\Omega_{E}}(\xi, X) = \operatorname{ppcm}_{i=1,\dots,m} \operatorname{Pm}_{\Omega_{E_{i}}}(\xi e_{E_{i}}, X)$$
.

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

$$f(X) = Pm_{\Omega_{\overline{E}}}(\xi, X)$$
.

On a alors

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

D'où:

$$P_{\Sigma}(\xi, X) = \prod_{i=1}^{m} P_{\Sigma}(\xi e_{E_i}, X)$$

Si $\alpha=g(\xi)$, $(g\in \mathbb{Q}[\mathbb{X}])$ est un élément de $\mathbb{Q}_{E}[\xi]$, sa composante αe_{E} dans $\Omega_{E_{i}}$ est un élément de $\mathbb{Q}_{E_{i}}[\xi e_{E_{i}}]$, car

$$\alpha e_{E_{i}} = g(\xi) \cdot e_{E_{i}} = g(\xi e_{E_{i}})$$
.

De manière plus précise, on a le résultat suivant :

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

$$\alpha_{i} = g_{i}(\xi e_{E_{i}})$$
 où $g_{i} \in Q[X]$.

Comme les $f_i = Pm_{\Omega_{\hat{E}_i}}(\xi_i, X)$ 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 $\alpha_i = g_i(\xi e_E) = g(\xi e_E)$. 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) . $\underline{\text{Exemple.}} \text{-Si Pm}_{\widehat{\Sigma}_E}(\xi \text{ , X}) \text{ est le produit de k facteurs du ler degré, où k}$ est le nombre d'éléments de E , $\mathbb{Q}_E[\xi]$ est isomorphe à \mathbb{Q}^k .

Notation. - ξ étant un élément algébrique de $\Omega_{\rm E}$, $\xi_{\rm p}^{\rm (i)}$ (i = 1 , ... , s)

désignent les racines dans Ω_p de $\operatorname{Pm}_{\Omega_p}(\xi,X)$ (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 :

$$\operatorname{Mm}_{\Omega_{E}}(\xi) = \prod_{i=1}^{s} \xi_{p}^{(i)} \qquad (\forall p \in P)$$

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 $\mathbb{Q}_{\underline{E}}[\gamma]$ un résultat généralisant le suivant : Dans tout corps $\mathbb{Q}(\gamma)$ 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 $\mathbb{S}_E^{p^t}$ définis comme suit. (Voir également [1] , avec des notations différentes.)

p' désignant une valuation figurant ou non dans E , $\mathbb{S}_{E}^{p'}$ <u>est l'ensemble des éléments</u>

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

 (\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 $\left| X \right|_p \leqslant 1$.

(Cp,) $|\theta_p,p_i| > 1$. Les autres racines de f dans Ω_p , appartiennent au disque $|X|_p$, < 1 .

($\Gamma_{\rm p}$,) Les racines de f dans $\Omega_{\rm p}$, appartiennent au disque $\left| X \right|_{\rm p} < 1$

Propriétés:

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

$$q f(X) = q X^{S} + q_{1} X^{S-1} + \cdots + q_{S}$$
 (q et $q_{1} \in Z$)
où $q = \prod_{p \in E} p$ et $(q, q_{1}) = 1$, $q_{S} \neq 0$.

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

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 $\theta \in \mathbb{S}_E^{p'}$, $\theta^n \in \mathbb{S}_E^{p'}$ (n entier > 0) et que les polynômes $\Pr_E(\theta^n, X)$ sont premiers entre eux 2 à 2, et ont tous le degré s .

3.2. – On démontrera d'abord le résultat annoncé dans le cas particulier où $Q_{_{\!\rm E}}[\gamma]$ est un corps :

LERE 2. - Dans tout corps $Q_E[\gamma]$ d'éléments algébriques de $V_E(Q)$, il existe des éléments de l'ensemble $\bigcap_{E \in F} S_E^p$ 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 :

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

où α est un élément entier algébrique de $\,{\boldsymbol{Q}}_{\!\!E}[\gamma]\,$ de la forme :

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

(s est le degré de $\mathbb{Q}_{\mathbb{E}}[\gamma]$), ce qu'on notera

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

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

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

$$\alpha_{p}^{(i)} = x_{0} + x_{1} \gamma_{p}^{(i)} + \dots + x_{s-1} \gamma_{p}^{(i)}^{s-1} = \Lambda(\gamma_{p}^{(i)}, x)$$

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

Pour que θ , défini par (1), soit un élément de $\mathbb{Q}_{\underline{F}}[\gamma]$ de degré s , il suffit

que les inégalités : A_p ($p \in E^-$), B_p ($p \in F^-$, $p \not\in E$) 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) ($p \neq (0)$) $|\alpha_p|_p > p^{-r}$ $|\alpha_p^{(i)}|_p \leqslant p^{-(r+1)}$ (i = 2, ..., s)

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

$$|\alpha_0|_0 > \prod_{p \in E} p^r \qquad |\alpha_0^{(i)}|_0 \leq \eta \prod_{p \in E} p^r \qquad (i = 2, ..., s)$$

$$(B_p)$$
 $(p \neq 0)$ $|\alpha_p^{(i)}|_p \leq p^{-1}$ $(i = 1, 2, ..., s)$

$$|\alpha_0^{(i)}|_0 \le \eta \prod_{p \in E} p^r$$
 (i = 1, 2, ..., s)

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

En effet les racines dans $\Omega_{\rm p}$ du polynôme $\Pr_{\Omega_{\rm E}}(\alpha, X)$ figurent parmi les $\alpha_p^{(i)}$ (i=1 , 2 , ... , 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 $Pm_{\Omega_p}(\alpha, X)$. 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 $\Pr_{\Omega_E}(\theta$, X) les propriétés (C_p) $(p \in E^-)$, (Γ_p)

3.2.2. La recherche d'un élément $x=(x_0^-,\dots,x_{s-1}^-)$ 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 , ... , s) , s formes linéaires en x_0 , ... , x_{s-1} , à coefficients dans R , de déterminant $\Delta_0 \neq 0$.

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

Il existe un système $x = (x_0, \dots, x_{s-1})$ d'entiers non tous nuls, tels que : $\left|L_{0}^{(i)}(x)\right|_{0} \leq c_{i}$ (i = 1, 2, ..., s)

$$|L_{p}^{(i)}(x)|_{p} \le p^{-\lambda}_{p,i}$$
 (i = 1, 2, ..., s) et $p \in E^{-\lambda}$

si on a la relation

$$\prod_{i=1}^{s} \mathbf{c}_{i} \prod_{p \in E} p^{-\sigma_{p}} \geqslant |\Delta_{0}|_{0} \prod_{p \in E} |\Delta_{p}|_{p} \quad \text{avec} \quad \sigma_{p} = \sum_{i=1}^{s} \lambda_{p,i}$$

(E ensemble fini de nombres premiers distincts, e_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 : G = $\bigcap_{p \in E}$ G , où le réseau G est défini par:

$$|L_{p}^{(i)}(x)|_{p} \le p^{-\lambda}p,i$$
 (i = 1, 2,..., s)

Mlle E. LUTZ [5] démontre que :

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

et

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

Remarque. - On peut remplacer l'hypothèse $L_0^{(i)}(x)$ à coefficients dans R, par $L_{\cap}^{(i)}(x)$ 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

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 $\, {\bf Q}_{_{
m D}} \,$.

$$\Lambda(\gamma_p^{(i)}, x) = x_0 + x_1 \gamma_p^{(i)} + \dots + x_{s-1} \gamma_p^{(i)}$$
 (p \(\phi \) (0) et \(\gamma_p^{(i)} \neq \gamma_p \) est \(\text{à coefficients dans } \(\Omega_p \).

Si $p \notin E$, les inégalités $|x_j|_p \le p^{-1}$ (j = 0, ..., s - 1) entraîneront $\left| \Lambda(\gamma_{D}^{(i)}, x) \right|_{D} \leq p^{-1}$

c'est-à-dire la condition ($\mathbf{B}_{_{\mathrm{D}}})$. On posera donc :

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

$$\gamma_{p}^{(i)^{s-1}} = c_{s-2,p} \gamma_{p}^{(i)^{s-2}} + \dots + c_{0,p}$$
 (où $c_{h,p} \in Q_{p}$ et $|c_{h,p}|_{p} \le 1$).

On a

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

Les inégalités

$$|x_{j} + c_{j,p} x_{s-1}|_{p} \le p^{-(r+1)}$$
 (j = 0, ..., s - 2)

entraîneront

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

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

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

et

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

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

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

et, lorsqu'on a affaire à des majorations, c'est-à-dire pour i=2, ..., s $((0) \in E)$ et i=1, 2, ..., s $((0) \not\in E)$, 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 , ... , 0) , car dans \mathbb{Q}_p tout $\gamma_p^{(i)}$ est exactement de degré s sur \mathbb{Q} , ici intervient l'hypothèse $\mathbb{Q}_E[\gamma]$ est un corps) donne :

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

D'où pour tout $p' \in E^+$:

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

c'est-à-dire une minoration de $|\Lambda(\gamma_p, x)|_p$ en fonction des majorations en valeur absolue de toutes les formes

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

et en particulier de majorations en væleur absolue des formes $\; \Lambda(\gamma_{_{\rm D}} \; , \; x) \;$ ($p \, \in \, E$,

 $p \neq p'$).

On posera donc:

(5)
$$L_{p}^{(1)}(x) = \Lambda(\gamma_{p}, x) \qquad (p \in E).$$

Le choix des majorations correspondantes :

$$p^{-\lambda}p^{1}$$
 et c_1 (si (0) $\in E$)

est assez arbitraire pourvu évidemment qu'on les choisisse supérieures aux minorations des conditions $\,{\rm A}_{\rm p}\,$. On prendra :

$$\mathbf{c}_1 = \prod_{p \in E} p^{2r} \quad (\text{si } (0) \in E) \quad \text{et } \lambda_{p,1} = [r/2] \qquad (p \in E)$$

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 $\,\eta\,$ (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 (pour p' = (0) si $(0) \in E$).

On trouve les conditions suivantes :

Si $(0) \in E$:

$$\begin{cases} \eta^{s-1} \ a^{2r-[r/2]} \geqslant a^{s-1} \ b^{s} \ |\Delta_{0}|_{0} \prod_{p \in E} |\Delta_{p}|_{p} \\ \eta^{-(s-1)} \ a^{-2r+[r/2]} \left(\inf_{p \in E} p\right)^{r-[r/2]} > a^{-(s-1)} \end{cases}$$

$$\begin{cases} \eta^{s} a^{r-\lceil r/2 \rceil} \geqslant b^{s} |\Delta_{0}|_{0} \prod_{p \in E} |\Delta_{p}|_{p} \\ \eta^{-s} a^{r-\lceil r/2 \rceil} \left(\inf_{p \in E} p\right)^{r-\lceil r/2 \rceil} > a^{s-1} \end{cases}$$

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

Il est possible de choisir η(r) tel que, pour r assez grand, ces inégalités soient vérifiées. On peut définir η par exemple par

19-12

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

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

On a donc construit un élément α de $\mathbb{Q}_{E}[\gamma]$ vérifiant les conditions (\mathbb{A}_{p}) et (\mathbb{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 $\bigcap_{p'\in F} S_E^{p'}$ ayant le degré de l'anneau (F sous-ensemble fini de P).

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

On peut choisir un système (n_1, \ldots, n_m) d'entiers positifs tels que les polynômes $Pm_{\Omega_i}(\theta_i, x)$ $(i=1, \ldots, m)$ soient premiers entre eux 2 à 2.

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

D'autre part :

$$Pm_{\Omega_{E}}(\theta, X) = ppcm \quad Pm_{\Omega_{E}}(\theta_{E}, X)$$
 (§ 2.2).

Il en résulte que θ est de degré s .

4. Une caractérisation des éléments algébriques de $V_{E_i}(Q)$.

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 $V_{\rm E}({\tt Q})$, 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 $\frac{m}{\prod_{p} p}$ (§ 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 :

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

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

et éventuellement, si (0) ∉ 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

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

La démonstration utilise le théorème $\hat{1}$, pour le cas $F=E^+$, et une caractérisation de l'ensemble $\bigcap_{\substack{p'\in E^+\\ E}} \mathbb{S}_E^{p'}$ 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 $|\theta|_p > 1$ ($p \in E$). θ appartient à $\bigcap_{p' \in E} S_E^{p'}$ si et seulement s'il existe un élément inversible λ de V_E tel que : $p' \in E$

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

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

 λ est alors un élément algébrique de $\mathbf{Q}_{\underline{E}}[\boldsymbol{\theta}]$.

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

$$H(\lambda \theta^{n}) = N_{m_{\Omega_{E}}}(\lambda \gamma^{n})$$

$$\varepsilon_{p}(\lambda \theta^{n}) = -\sum_{i=2}^{s} \lambda_{p}^{(i)} \theta_{p}^{(i)^{n}} \qquad (p \in E)$$

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

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 $\mathbb{Q}_{E}[\alpha]$, et on prend pour θ un élément de $\bigcap_{\substack{p'\in E^+\\ E'}}\mathbb{S}_{E}^{p'}$ appartenant à $\mathbb{Q}_{E}[\alpha]$. 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

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

D'où il résulte : θ appartient à l'ensemble $\bigcap_{p'\in E^+}\mathbb{S}_E^{p^4} \ , \ \text{et} \ \mu \ \text{est un élément algébrique de } \mathbb{Q}_E[\theta] \ .$

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

L'inégalité vérifiée par le degré s de α résulte de la formule du produit des valuations appliquée au rationnel Nm (Θ) .

BIBLIOGRAPHIE

- [1] BERTRANDIAS (Françoise). Caractérisation des ensembles Sq par la répartition modulo 1 en p-adique, Séminaire Dubreil-Pisot : Algebre et théorie des nombres, t. 17, 1963/64, nº 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.