

GROUPE DE TRAVAIL D'ANALYSE ULTRAMÉTRIQUE

BERTIN DIARRA

Construction des extensions primitives d'un corps p -adique

Groupe de travail d'analyse ultramétrique, tome 9, n° 2 (1981-1982), exp. n° 24, p. 1-19

<http://www.numdam.org/item?id=GAU_1981-1982__9_2_A6_0>

© Groupe de travail d'analyse ultramétrique
(Secrétariat mathématique, Paris), 1981-1982, tous droits réservés.

L'accès aux archives de la collection « Groupe de travail d'analyse ultramétrique » 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.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

CONSTRUCTION DES EXTENSIONS PRIMITIVES D'UN CORPS p -ADIQUE

(d'après Marc KRASNER)

par Bertin DIARRA (*)

Dans une longue série d'articles (cf. par exemple [2], [3] ou [5], et plusieurs notes aux comptes rendus de l'Académie des sciences), Marc KRASNER a développé une théorie de la ramification non galoisienne des corps valués. Cette théorie a eu pour couronnement le calcul explicite du nombre des extensions de degré fini donné d'un corps p -adique (cf. [6]). Nous ne nous intéressons ici qu'au seul aspect de la caractérisation des extensions primitives des corps p -adiques basée sur cette théorie.

1. Hypergroupes de Galois.

Soit H un ensemble ; on appelle hypercomposition sur H une application de $H \times H$ dans l'ensemble des parties non vides $\mathcal{P}(H)^*$ de H ; on écrit pour $\sigma, \tau \in H$, $\sigma \cdot \tau$ ou $\sigma \tau$ l'image de (σ, τ) par cette application. Si A et B sont deux parties non vides de H , on pose

$$A \cdot B = \bigcup_{\sigma \in A, \tau \in B} \sigma \cdot \tau.$$

Un hypergroupe est un ensemble H muni d'une hypercomposition telle que

$$(i) \quad (\sigma \cdot \tau) \cdot \gamma = \sigma \cdot (\tau \cdot \gamma), \quad \forall \sigma, \tau, \gamma \in H,$$

$$(ii) \quad \sigma \cdot H = H \cdot \sigma = H, \quad \forall \sigma \in H.$$

NOTA BENE. - On voit aussitôt dans ces conditions que, si pour tout $\sigma, \tau \in H$, $\sigma \cdot \tau$ est réduit à un seul élément, alors H est un groupe.

Une partie non vide h d'un hypergroupe H est dite sous-hypergroupe de H , si h est un hypergroupe pour la loi induite par celle de H ; pour cela, il faut et il suffit que l'on ait

$$\sigma \cdot h = h \cdot \sigma = h, \quad \forall \sigma \in h.$$

On dit qu'un sous-hypergroupe h de H est réversible à gauche, si $(\sigma \cdot h)_{\sigma \in H}$ est une partition de H ; ce qui équivaut à

$$\forall \sigma, \tau \in H, \quad \sigma \in \tau \cdot h \implies \tau \in \sigma \cdot h.$$

(*) Texte reçu le 24 mai 1982.

Bertin DIARRA, Mathématiques pures, Université de Clermont-Ferrand-II, Complexe scientifique des Cézeaux, 63170 AUBIÈRE.

Considérons alors $H/h = \{\sigma.h, \sigma \in H\}$; comme

$$(\sigma.h).(\tau.h) = (\sigma.h.\tau).h,$$

on définit sur H/h une structure d'hypergroupe en posant

$$(\sigma.h) * (\tau.h) = \{s.h, s \in \sigma.h.\tau\},$$

et H/h est appelé quotient gauche de H par h .

NOTA BENE. - On a des définitions analogues de réversibilité à droite et d'hypergroupe quotient droite.

Soit G un groupe ; tout sous-groupe g de G est un sous-hypergroupe réversible à gauche. On obtient donc sur $H = G/g$ une structure d'hypergroupe quotient gauche. Les hypergroupes de la forme $H = G/g$ sont appelés hypergroupes de classes à gauche (hypergroupes c. g.)

LEMME 1. - Soit $H = G/g$ un hypergroupe c. g. Les sous-hypergroupes h de H sont de la forme $h = G'/g$, où G' est un sous-groupe de G qui contient g .

En effet, si $h = \{sg, s \in X_h \subset G\}$ est un sous-hypergroupe de $H = G/g$, considérons $G' = \bigcup_{s \in X_h} sg \subset G$. Comme, pour tout $s \in X_h$, $(sg) * h = h$, on a

$$(sg).G' = G'$$

et, pour tout $x \in G'$,

$$(xg).G' = G'.$$

Il vient que $e \in g.G'$; donc $g \cap G' \neq \emptyset$, $g \subset G'$ et $(xg).G' = xG' = G'$; ainsi l'inverse de x est dans G' . D'autre part, comme $(sg) * (tg) \subset h$ pour $s, t \in X_h$, on a $(sg).(tg) \subset G'$; mais si $x, y \in G'$, on a $xg = sg$, $y = tg$ avec $s, t \in X_h$; ainsi $(xg).(yg) \subset G'$ et $xy \in G'$; de plus $G'/g = h$.

COROLLAIRE.

(i) Tout sous-hypergroupe h d'un hypergroupe c. g. $H = G/g$ est réversible.

(ii) Si $h = G'/g$, où G' est un sous-groupe de G , on a $H/h = G/G'$. De plus, pour tout $\sigma \in H$, $\text{card}(\sigma.h) = \text{card } h$.

On pose $[H : h] = [G : G']$, appelé indice de h dans H .

REMARQUE 1 (théorème d'isomorphisme).

(i) Soient H et H' deux hypergroupes ; une application $\mu : H \rightarrow H'$ est un morphisme d'hypergroupes si

$$\mu(A.B) = \mu(A).\mu(B) \text{ pour tous } A, B \in \mathcal{P}(H)^*.$$

(ii) Soit H un hypergroupe c. g., et soient $h_1 \subset h_2$ deux sous-hypergroupes de H ; alors

$$H/h_2 \simeq (H/h_1)/(h_2/h_1)$$

On dit qu'un hypergroupe c. g. H est fini si $H = G/g$, où G est un groupe fini.

REMARQUE 2. - Une partie non vide h d'un hypergroupe c. g. fini H est un sous-hypergroupe de H si, et seulement si, pour tous $\sigma, \tau \in h$, $\sigma \cdot \tau \in h$.

Soient K un corps, $\Omega = \Omega_K$ une clôture algébrique de K . Si E est une extension algébrique finie de K , on pose

$$H(E|K) = \text{iso}_K(E, \Omega)$$

l'ensemble des K -isomorphismes de E dans Ω . Soit

$$G = \text{aut}_K(\Omega, \Omega)$$

le groupe des K -automorphismes de Ω ; pour tout $s \in G$,

$$\text{corr } s = s|_E \quad (\text{correspondant de } s)$$

l'application de G dans $H(E|K)$ définie par restriction.

Associons à toute partie Λ de $H(E|K)$,

$$\text{gen } \Lambda = \{s \in G; \text{corr } s \in \Lambda\} \quad (\text{générateur de } \Lambda).$$

Si l'on pose, pour $\sigma, \tau \in H(E|K)$,

$$\sigma \cdot \tau = \text{corr}(\text{gen } \sigma \text{ gen } \tau)$$

$$= \{\sigma' \in H(E|K); \text{corr}(s \circ t) = \sigma', \text{ où } s \in \text{gen } \sigma, t \in \text{gen } \tau\},$$

on définit sur $H(E|K)$ une structure d'hypergroupe, et $H(E|K)$ est appelé l'hypergroupe de Galois de l'extension $E|K$.

Puisque, pour tous $s, t \in \text{gen } \sigma$,

$$s^{-1} t \in g = \text{aut}_E(\Omega, \Omega) \subset G,$$

on a $sg = tg$, et $\text{gen } G \cdot g = sg$ est réduit à une seule classe modulo g . Ainsi, on définit une application de $H(E|K)$ dans G/g qui à σ associe la classe $\text{gen } \sigma \cdot g$. On voit que cette application est un isomorphisme de l'hypergroupe $H(E|K)$ sur l'hypergroupe c. g.

$$G/g = \text{aut}_K(\Omega, \Omega) / \text{aut}_E(\Omega, \Omega).$$

REMARQUE 3. - En fait $H(E|K)$ est un hypergroupe c. g. fini.

En effet, considérons une extension normale finie N/K telle que $K \subset E \subset N$. Si $G(N|K)$ et $G(N|E)$ sont les groupes de Galois des extensions normales $N|K$ et $N|E$ définissant corr_N et gen_N comme ci-dessus en remplaçant Ω par N , et G par

$G(N|K)$, on déduit du théorème de prolongement des K -isomorphismes que

$$\text{corr}_N(\text{gen}_N \sigma \text{ gen}_N \tau) = \text{corr}(\text{gen } \sigma \text{ gen } \tau) = \sigma \cdot \tau.$$

Ainsi $H(E|K) \simeq G(N|K)/G(N|E)$ et $H(E|K)$ est un hypergroupe c. g. fini.

NOTA BENE. - L'extension $E|K$ est normale si, et seulement si, $H(E|K)$ est un groupe.

Si l'on fait correspondre à tout sous-hypergroupe h de $H(E|K)$ le sous-corps $L = \text{inv } h$ de E des invariants de h , et à tout sous-corps L de E le sous-hypergroupe $H(E|L)$ de $H(E|K)$, on déduit de la démonstration du théorème classique de Galois le lemme suivant.

LEMME 2 : (Correspondance de Galois). - Soit $E|K$ une extension finie séparable, d'hypergroupe de Galois $H(E|K)$.

Si h est un sous-hypergroupe de $H(E|K)$, il existe un, et un seul, sous-corps L de E , $K \subset L \subset E$, tel que $H(E|L) = h$; cette correspondance étant bijective.

De plus,

$$H(L|K) \simeq H(E|K)/H(E|L).$$

2. Hypergroupes et nombres de ramification.

Soit K un corps de valuation discrète, complet. On désigne par w_K la valuation normalisée de K telle que $w_K(K^*) = \mathbb{Z}$, par Δ_K (resp. m_K) l'anneau de valuation (resp. l'idéal maximal) de K , par π_K une uniformisante de K , et par $\bar{K}$ le corps résiduel de K .

Soit $E|K$ une extension finie de K . On pose $e = e_{E|K}$ et $f = f_{E|K}$ l'indice de ramification et le degré résiduel de l'extension $E|K$; on a $(w_E)|_K = e w_K$, où w_E est la valuation normalisée de E .

Soit Ω la clôture algébrique de K ; on écrit, par abus de notation, w_K (resp. w_E) l'unique prolongement de w_K (resp. w_E) à Ω . On note Δ_Ω et m_Ω l'anneau et l'idéal de valuation de Ω .

Rappelons (cf. [7] ou [8]) que toute extension finie séparable $E|K$, d'extension résiduelle $\bar{E}|\bar{K}$ séparable, contient un unique sous-corps maximal T (corps d'inertie) tel que $T|K$ est non ramifiée avec $\bar{T} = \bar{E}$; de plus, $E|K$ est totalement ramifiée. On définit, par passage au quotient, une application $H(E|K) \longrightarrow H(\bar{E}|\bar{K})$, en posant, pour $\sigma \in H(E|K)$, $a \in \Delta_E$,

$$\bar{\sigma}(\bar{a}) = \overline{\sigma(a)}.$$

Cette application est un ~~morphisme~~ surjectif d'hypergroupes. De plus

$$H(E|T) = \{\sigma \in H(E|K) ; \bar{\sigma} = \text{id}_{\bar{E}}\} .$$

Dans toute la suite, on suppose les extensions $E|K$ et $\bar{E}|\bar{K}$ séparables. Dans ces conditions, il existe $\alpha \in \Lambda_E$ tel que $\Lambda_E = \Lambda_K[\alpha]$ et $E = K[\alpha]$.

On appelle nombre caractéristique (ou de ramification) de $E \in H(E|K)$, le nombre rationnel

$$v(\sigma) = w_E(\sigma\alpha - \alpha) - 1 .$$

On a $v(\sigma) \geq -1$.

REMARQUE 4. - $\forall \sigma \in H(E|K)$, $v(\sigma) = \min_{\alpha \in \Lambda_E} w_E(\sigma\alpha - \alpha) - 1$.

LEMME 3. - Soit $v \in \mathbb{Q}$; alors $h_v = \{\sigma \in H(E|K) ; v(\sigma) \geq v\}$ est un sous-hypergroupe de $H(E|K)$

Il suffit de montrer (Remarques 2 et 3) que si $\sigma, \tau \in h_v$, alors $\sigma \cdot \tau \in h_v$. Soit $\sigma' \in \sigma \cdot \tau$; on a $\sigma' = (s \circ t)|_E$ où $s \in \text{gen } \sigma$, $t \in \text{gen } \tau$; ainsi

$$w_E(\sigma'\alpha - \alpha) = w_E(s \circ t\alpha - \alpha) = w_E(s(t\alpha - \alpha) + s\alpha - \alpha)$$

$$\geq \min(w_E(s(t\alpha - \alpha)), w_E(s\alpha - \alpha))$$

$$= \min(w_E(t\alpha - \alpha), w_E(s\alpha - \alpha)) = \min(w_E(\tau\alpha - \alpha), w_E(\sigma\alpha - \alpha)) \geq v + 1,$$

d'où

$$v(\sigma') \geq v \text{ et } \sigma' \in h_v .$$

NOTA BENE. - Si $v \leq -1$, alors $h_v = H(E|K)$.

LEMME 4. - Soit T le sous-corps d'inertie de $E|K$. Soit π_E une uniformisante de E . Si $\sigma \in H(E|K)$, alors

- ou bien $\sigma \in H(E|T)$ et $v(\sigma) = w_E((\sigma\pi_E/\pi_E) - 1) \geq 0$,

- ou bien $\sigma \notin H(E|T)$ et $v(\sigma) = -1$.

En effet, puisque $E|T$ est totalement ramifiée, on a $E = T[\pi_E]$, et tout $a \in \Lambda_E$ s'écrit

$$a = \sum_{i=0}^{e-1} \beta_i \pi_E^i, \quad \beta_i \in \Lambda_T .$$

Alors, si $\sigma \in H(E|T)$; on a, d'une part

$$v(\sigma) \leq w_E(\sigma\pi_E - \pi_E) - 1 = w_E\left(\frac{\sigma\pi_E}{\pi_E} - 1\right)$$

et d'autre part, comme, pour tout $a = \sum_{j=0}^{e-1} \beta_j \pi_E^j \in \Lambda_E$,

$$\sigma a = \sum_{j=0}^{e-1} \beta_j \sigma(\pi_E)^j,$$

on a

$$w_E(\sigma a - a) \geq \min_{1 \leq j \leq e-1} w(\beta_j) + w_E(\sigma(\pi_E)^j - \pi_E^j) \geq w_E(\sigma \pi_E - \pi_E);$$

donc

$$v(\sigma) \geq w_E(\sigma \pi_E - \pi_E) - 1.$$

Il vient que $v(\sigma) = w_E((\sigma \pi_E / \pi_E) - 1) \geq 0$.

Si $\sigma \notin H(E|T)$, $\bar{\sigma} \neq \text{id}_{\bar{E}}$; il existe donc $b \in \Lambda_E$ tel que $\bar{\sigma}(\bar{b}) = \bar{b}$ dans $\bar{\Omega}$ ou encore $\sigma b - b \notin \mathfrak{m}_{\Omega}$, c'est-à-dire $w_E(\sigma b - b) = 0$. Ainsi

$$-1 = w_E(\sigma b - b) - 1 \geq v(\sigma) \geq -1.$$

NOTA BENE. - $h_0 = H(E|T)$.

Puisque $H(E|K)$ est fini, $(v(\sigma))_{\sigma \in H(E|K)}$ est fini.

On note (v_q) , $0 \leq q \leq m-1$, l'ensemble des nombres de ramification finis, strictement positifs, rangés dans l'ordre croissant : $0 < v_0 < v_1 < \dots < v_{m-1}$; les v_q , $0 \leq q \leq m-1$, sont appelés nombres de ramification propres.

On pose $v_{-2} = -1$, $v_{-1} = 0$ et $v_m = +\infty$, appelés nombres de ramification impropres.

Pour $0 \leq q \leq m$, on pose

$$H_q = H_q(E|K) = h_{v_q}.$$

Alors $H_{-2} = H(E|K)$, $H_{-1} = H(E|T)$, $H_m = \{\text{id}_E\}$.

De plus, $\forall v \in \mathbb{Q}$, il existe $0 \leq q \leq m$ tel que $h_v = H_q$. On a

$$H_m = \{\text{id}_E\} \subset H_{m-1} \subset \dots \subset H_0 \subset H_{-1} \subset H_{-2} = H(E|K).$$

On dit que $H_{-1} = H(E|T)$ est le sous-hypergroupe d'inertie, et H_q , $0 \leq q \leq m-1$, le q -ième hypergroupe de ramification de l'extension $E|K$.

NOTA BENE. - Si $E|K$ est galoisienne, les v_q sont des entiers rationnels ou $+\infty$; on retrouve les notions usuelles de groupe d'inertie et de groupes de ramification.

Considérons $E_q = \text{Inv}(H_q)$, $0 \leq q \leq m$; on a

$$H_q = H(E|E_q) \text{ et } E_{-2} = K \subset E_{-1} \subset E_0 \subset \dots \subset E_{m-1} \subset E_m = E.$$

Les corps $E_{-1} = T$ et E_q , $0 \leq q \leq m-1$, sont appelés corps d'inertie et

q-ième corps de ramification.

NOTA BENE. - $H(E_{-1}|K) \simeq H(E|K)/H_{-1} \simeq H(\bar{E}|\bar{K})$.

En particulier, on a le résultat suivant.

REMARQUE 5. - Si $\bar{K}$ est fini ; $H(E_{-1}|K) \simeq H(\bar{E}|\bar{K})$ est un groupe cyclique.

Posons

$$n_q = \text{card } H_q, \quad -2 \leq q \leq m;$$

$$r_q = [H_q : H_{q+1}] = \frac{n_q}{n_{q+1}}, \quad -2 \leq m \leq q-1,$$

r_q étant un indice de sous-hypergroupe est un entier. On a

$$n_{-2} = [E : K] = ef; \quad n_{-1} = e; \quad r_{-2} = f.$$

Pour $-2 \leq q \leq m-1$, on a

$$H_q/H_{q+1} \simeq H(E_{q+1}|E_q);$$

donc

$$r_q = [E_{q+1} : E_q];$$

de plus

$$e = n_{-1} = \prod_{-1 \leq q \leq m-1} r_q.$$

Considérons une extension galoisienne finie $N|K$ telle que $K \subset E \subset N$, et telle que $\bar{N}|\bar{K}$ est séparable (ou peut prendre l'extension galoisienne engendrée sur K par E).

Soit $G = G(N|K)$ le groupe de Galois de $N|K$; on a

$$H(E|K) \simeq G(N|K)/G(N|E).$$

Soient $\beta \in N$ tel que $A_N = A_K[\beta]$, et $\alpha \in E$ tel que $A_E = A_K[\alpha]$. Posons, pour $s \in G(N|K)$, $\alpha(s, N) = (s\beta - \beta) A_N$ et pour $\sigma \in H(E|K)$, $\alpha(\sigma, E) = (E\alpha - \alpha) A_N$. On sait (cf. [1], chapitre 5, § 4) que

$$\alpha(\sigma, E) = \sum_{s \in \text{gen}_N \sigma} \alpha(s, N).$$

où $\text{gen}_N \sigma = \{s \in G; \text{corr}_N s = s|_E = \sigma\}$; ce qui équivaut à

$$w_N(\alpha\sigma - \alpha) = \sum_{s \in \text{gen}_N \sigma} w_N(s\beta - \beta)$$

(l'hypothèse $N|K$ galoisienne n'est pas nécessaire). Comme $w_N = e_{N|E} w_E$ on a

$$w_N(\alpha\sigma - \alpha) = e_{N|E} w_E(\alpha\sigma - \alpha) = \sum_{s \in \text{gen}_N \sigma} w_N(s\beta - \beta).$$

Définissant v_N sur G par $v_N(s) = w_N(s\beta - \beta) - 1$ (nombre de ramification de $s \in G$; c'est un entier naturel ≥ -1), on obtient

$$e_{N|E}(v(\sigma) + 1) = \sum_{s \in \text{gen}_N \sigma} (v_N(s) + 1)$$

Soit $G_{-1} = \{s \in G; v_N(s) \geq 0\}$ le groupe d'inertie de l'extension galoisienne $N|K$.

LEMME 5. - Soit $\sigma \in H_{-1}$; alors $\text{gen}_N \sigma \cap G_{-1} = \emptyset$.

En effet, si $\sigma \in H(E|K)$ est tel que $\text{gen}_N \sigma \cap G_{-1} = \emptyset$, alors pour tout $s \in \text{gen}_N \sigma$, $v_N(s) < 0$; donc $v_N(s) = -1$, et

$$e_{N|E}(v(\sigma) + 1) = \sum_{s \in \text{gen}_N \sigma} (v_N(s) + 1) = 0;$$

d'où $v(\sigma) = -1$ et $\sigma \notin H_{-1}$.

Considérons $G_0 = \{s \in G; v_N(s) \geq v_{N,0}\}$ le premier groupe de ramification de $N|K$; on démontre à peu près comme ci-dessus la remarque suivante.

REMARQUE 6. - Soit $\sigma \in H_0$; alors $\text{gen}_N \sigma \cap G_0 \neq \emptyset$.

NOTA BENE. - On montre de façon générale que les sous-hypergroupes H_q de $H(E|K)$ s'obtiennent par passage au quotient à partir des sous-groupes d'inertie et de ramification de $G(N|K)$.

Soit $\sigma \in H_{-1}$, il est clair que $u_\sigma = \sigma\pi_E/\pi_E$ est une unité de N ; on a donc une application

$$\theta_{-1}: H_{-1} \rightarrow \bar{N}$$

qui à σ associe $\theta_{-1}(\sigma) = \bar{u}_\sigma \neq 0$.

On voit aussitôt que θ_{-1} est indépendante du choix de l'uniformisante π_E . Si $B \subset \bar{N}$, on note $\langle\langle B \rangle\rangle$ l'ensemble des conjugués par rapport à $\bar{E}$ dans $\bar{N}$ des éléments de B .

PROPOSITION 1.

(i) Soient $\sigma, \tau \in H_{-1}$; on a $\theta_{-1}(\sigma \cdot \tau) = \theta_{-1}(\sigma) \langle\langle \theta_{-1}(\tau) \rangle\rangle$.

(ii) $\theta_{-1}(H_{-1})$ est un sous-groupe multiplicatif fini de $\bar{N}$.

(iii) L'ensemble des $\sigma \in H_{-1}$ tels que $\theta_{-1}(\sigma) = 1$ est égal à H_0 ;
 $\theta_{-1}(\sigma H_0) = \theta_{-1}(\sigma)$ ne dépend que de la classe σH_0 , et $\sigma H_0 \mapsto \theta_{-1}(\sigma H_0)$ est une bijection de H_{-1}/H_0 sur $\theta_{-1}(H_0)$. Si l'on pose, pour $\zeta, \eta \in \bar{N}$,
 $\zeta * \eta = \zeta \langle\langle \eta \rangle\rangle$; l'application $\sigma H_0 \mapsto \theta_{-1}(\sigma H_0)$ est un isomorphisme d'hyper-
groupes de H_{-1}/H_0 sur $\theta_{-1}(H_{-1})$.

(i) Soient $\sigma, \tau \in H_{-1}$ et $s \in \text{gen}_N \sigma \cap G_{-1}$; on a $\text{gen}_N \sigma = s \in G(N|E)$; tout $s' \in \text{gen}_N \sigma$ s'écrit $s' = s \circ g'$ avec $g' \in G(N|E)$. Si $\sigma' \in \sigma \cdot \tau$, on a $\sigma' = (s' \circ t')|_E$ où $s' \in \text{gen}_N \sigma$, $t' \in \text{gen}_N \tau$; ainsi

$$u_{\sigma'} = \frac{\sigma' \pi_E}{\pi_E} = \frac{s' \circ t'(\pi_E)}{\pi_E} = \frac{s'(\pi_E)}{\pi_E} = s' \left(\frac{\pi_E}{\pi_E} \right) \times \frac{s'(\pi_E)}{\pi_E} = s \circ g'(u_\tau) \cdot \frac{\sigma(\pi_E)}{\pi_E} = s \circ g'(u_\tau) \cdot u_\sigma$$

Comme $s \in G_{-1}$, on a

$$s \circ g'(u_\tau) \equiv g'(u_\tau) \pmod{m_N}.$$

Il vient que

$$\theta_{-1}(\sigma \cdot \tau) = \{\bar{u}_{\sigma'}; \sigma' \in \sigma \cdot \tau\} = \{\bar{g}'(\bar{u}_\tau) \cdot \bar{u}_\sigma; \bar{g}' \in G(\bar{N}|\bar{E})\} = \theta_{-1}(\sigma) \langle \langle \theta_{-1}(\tau) \rangle \rangle.$$

(ii) Il est clair que, pour $\sigma, \tau \in H_{-1}$, on a

$$\theta_{-1}(\sigma) \theta_{-1}(\tau) \in \theta_{-1}(\sigma) \langle \langle \theta_{-1}(\tau) \rangle \rangle \subset \theta_{-1}(H_{-1})$$

et $1 \in \theta_{-1}(H_{-1})$.

Puisque $\theta_{-1}(H_{-1})$ est fini, c'est un sous-groupe multiplicatif de $\bar{N}$.

(iii) Dire que $\theta_{-1}(\sigma) = 1$ équivaut à dire que $v(\sigma) = w_E((\sigma \pi_E / \pi_E) - 1) > 0$ ou encore $v(\sigma) \geq v_0$; c'est-à-dire $\sigma \in H_0$. Pour $\sigma \in H_{-1}$, on a

$$\theta_{-1}(\sigma H_0) = \theta_{-1}(\sigma) \langle \langle \theta_{-1}(H_0) \rangle \rangle = \theta_{-1}(\sigma) \langle \langle 1 \rangle \rangle = \theta_{-1}(\sigma).$$

On en déduit aussitôt que $\sigma H_0 \rightarrow \theta_{-1}(\sigma H_0)$ est une bijection de H_{-1}/H_0 sur $\theta_{-1}(H_{-1})$. Le reste se vérifie facilement.

COROLLAIRE 1. - L'entier $r_{-1} = [H_{-1} : H_0]$ est premier à la caractéristique résiduelle p de K .

En effet, comme $\theta_{-1}(H_{-1})$ est un sous-groupe multiplicatif fini de $\bar{N}$, on sait dans ces conditions que $\theta_{-1}(H_{-1})$ est un groupe formé de racines de l'unité et est cyclique d'ordre premier à p . Mais

$$\text{card } \theta_{-1}(H_{-1}) = \text{card } H_{-1}/H_0 = [H_{-1} : H_0] = r_{-1};$$

ainsi $(r_{-1}, p) = 1$.

COROLLAIRE 2. - Soit $A \subset H_{-1}$ tel que $\theta_{-1}(A)$ est un sous-groupe de $\theta_{-1}(H_{-1})$; alors si $\sigma \in H_{-1}$, $\theta_{-1}(\sigma \cdot A) = \theta_{-1}(\sigma) \cdot \theta_{-1}(A)$ et $A \cdot H_0/H_0$ est un sous-hypergroupe de H_{-1}/H_0 .

Posons, pour $0 \leq q \leq m-1$, $v_q = j_q/d_q \in \mathbb{Q}$, $(j_q, d_q) = 1$. Soit d le plus petit commun multiple des entiers d_q .

Considérons $\pi_0 \in \Omega$ tel que $\pi_0^d = \pi_E$; un sur-corps L de E tel que $\pi_0 \in L$

et l'extension $L|K$ galoisienne avec $\bar{L}|\bar{K}$ séparable. Posons, pour $\sigma \in H_q$,

$$x_q(\sigma) = \frac{\sigma\pi_E - \pi_E}{\pi_0^{d(1+v_q)}};$$

comme $w_E(x_q(\sigma)) = v(\sigma) - v_q \geq 0$, on a

$$x_q(\sigma) \in \Lambda_L;$$

on définit alors une application $\theta_q^{(\pi_0)} : H_q \rightarrow \bar{L}$ $\theta_q^{(\pi_0)}(\sigma) = \overline{x_q(\sigma)}$. On écrit $\theta_q^{(\pi_0)}(H_q) = H_q^{(\pi_0)} \subset \bar{L}$.

Soit δ un entier positif, et soit $\bar{R}_\delta$ l'ensemble des racines δ -ièmes de l'unité contenues dans $\bar{L}$. On pose, pour $\eta \in \bar{L}$,

$$[\eta]_\delta = \cup \zeta \cdot \langle \langle \eta \rangle \rangle,$$

ζ parcourt $\bar{R}_\delta$ où $\langle \langle \eta \rangle \rangle$ est l'ensemble des $\bar{E}$ -conjugués de η . On a sur $\bar{L}$ une structure d'hypergroupe d'hypercomposition $\eta \otimes \eta' = \eta + [\eta']_\delta$.

On note δ_q l'entier tel que $d_q = p^{v_q} \delta_q$, $(p, \delta_q) = 1$, où p est la caractéristique de $\bar{K}$ si elle est non nulle, et 1 sinon. (En fait, $\delta_q = d_q$. cf. § 3)

PROPOSITION 2.

(i) Soit $0 \leq q \leq m-1$; si $\sigma, \tau \in H_q$, on a

$$\theta_q^{(\pi_0)}(\sigma \cdot \tau) = \theta_q^{(\pi_0)}(\sigma) + [\theta_q^{(\pi_0)}(\tau)]_{\delta_q}$$

(ii) $M_q^{(\pi_0)} = \theta_q^{(\pi_0)}(H_q)$ est un sous-groupe additif fini de $\bar{L}$

(iii) L'ensemble des $\sigma \in H_q$ tels que $\theta_q^{(\pi_0)}(\sigma) = 0$ est égal à H_{q+1} . La correspondance

$$\sigma \in H_{q+1} \rightarrow \theta_q^{(\pi_0)}(\sigma \in H_{q+1}) = \theta_q^{(\pi_0)}(\sigma)$$

ne dépend que de la classe $\sigma \in H_{q+1}$; c'est une bijection de H_q/H_{q+1} sur $M_q^{(\pi_0)}$ qui est un isomorphisme d'hypergroupes lorsque $M_q^{(\pi_0)}$ est muni de la loi $\eta \otimes \eta' = \eta + [\eta']_{\delta_q}$.

(i) Posons $\pi_q = \pi_0^{d/d_q}$ et $\alpha_q = \pi_0^{d(1+v_q)}$; on a

$$\pi_q^{d_q} = \pi_0^d = \pi_E; \quad \alpha_q = \pi_q^{j_q + d_q}$$

et

$$x_q(\sigma) = \frac{\sigma\pi_E - \pi_E}{\pi_q^{j_q + d_q}} = \frac{\sigma\pi_E - \pi_E}{\alpha_q}.$$

Soit $G_0 = G_0(L|K)$ le premier groupe de ramification de l'extension galoisienne $L|K$; soit $\sigma \in H_q \subseteq H_0$, alors, si $s \in \text{gen}_L \sigma \cap G_0 \neq \emptyset$ (Remarque 6), on a $\text{gen}_L \sigma = s G(L|E)$, et tout $s' \in \text{gen}_L \sigma$ s'écrit $s' = s \circ g$, où $g \in G(L|E)$. Soit τ un autre élément de H_q . Considérons $\sigma' \in \sigma \cdot \tau$; on a $\sigma' = (s' \circ t')|_E$ où $s' = s \circ g \in \text{gen}_L \sigma$, $s \in G_0$, $g \in G(L|E)$ et $t' \in \text{gen}_L \tau$. Ainsi

$$\begin{aligned} x_q(\sigma') &= \frac{\sigma' \pi_E - \pi_E}{\alpha_q} = \frac{s' \circ t'(\pi_E) - \pi_E}{\alpha_q} = \frac{s'(\tau \pi_E) - \pi_E}{\alpha_q} = \frac{s'(\alpha_q x_q(\tau) + \pi_E) - \pi_E}{\alpha_q} \\ &= \frac{s'(\alpha_q x_q(\tau))}{\alpha_q} + \frac{s'(\pi_E) - \pi_E}{\alpha_q} \\ &= \frac{s'(\alpha_q x_q(\tau))}{\alpha_q} \times \frac{s'(\alpha_q)}{s'(\alpha_q)} + \frac{\sigma(\pi_E) - \pi_E}{\alpha_q} = s'(x_q(\tau)) \times \frac{s'(\alpha_q)}{\alpha_q} + x_q(\sigma). \end{aligned}$$

Il vient que

$$x_q(\sigma') = s \circ g(x_q(\tau)) \times s\left(\frac{g(\alpha_q)}{\alpha_q}\right) \times \frac{s(\alpha_q)}{\alpha_q} + x_q(\sigma).$$

Comme $s \in G_0$, il est dans le groupe d'inertie de $L|K$; alors, pour tout $a \in L$, $a \neq 0$,

$$w_L\left(\frac{sa}{a} - 1\right) \geq 1 \quad \text{et} \quad \bar{s} = \text{id}_L.$$

Ainsi

$$\theta_q^{(\pi_0)}(\sigma') = \overline{x_q(\sigma')} = \overline{g(\theta_q^{(\pi_0)}(\tau))} \times \overline{\beta_q(g)} + \theta_q^{(\pi_0)}(\sigma) \quad \text{où} \quad \beta_q(g) = \frac{g(\alpha_q)}{\alpha_q}.$$

Puisque $g \in G(L|E)$ et $\pi_q^d = \pi_E$, on a

$$g(\pi_q)^d = g(\pi_q^d) = g(\pi_E) = \pi_E = \pi_q^d;$$

donc $g(\pi_q)/\pi_q$ est une racine d_q -ième de l'unité dans L . Sachant que $(j_q, d_q)=1$,

$$\beta_q(g) = \frac{g(\alpha_q)}{\alpha_q} = \left(\frac{g(\pi_q)}{\alpha_q}\right)^{j_q+d_q} = \left(\frac{g(\pi_q)}{\pi_q}\right)^{j_q}$$

est une racine d_q -ième de l'unité distincte de 1 si $g(\pi_q)/\pi_q$ l'est. Il vient que $\overline{\beta_q(g)}$ est une racine d_q -ième de l'unité dans $\bar{L}$. Mais $d_q = p^v \delta_q$ avec $(p, \delta_q) = 1$; ainsi $\overline{\beta_q(g)}$ est une racine δ_q -ième de l'unité dans $\bar{L}$.

D'autre part, si $g, g' \in G(L|E)$, on a

$$\beta_q(gg') = g(\beta_q(g')) \cdot \beta_q(g) \quad \text{et} \quad \overline{\beta_q(gg')} = \overline{g(\beta_q(g'))} \cdot \overline{\beta_q(g)}.$$

Mais si g' est dans le groupe d'inertie $G_{-1}(L|E)$ de l'extension galoisienne

$$\overline{\beta_q(g')} = \left(\frac{g'(\pi_q)}{\pi_q} \right) = 1 .$$

Donc si $g'' = g \cdot g' \in g \cdot G_{-1}(L|E)$, on a

$$\overline{\beta_q(g'')} = \overline{g(\beta_q(g'))} \cdot \overline{\beta_q(g)} = \overline{g(1)} \cdot \overline{\beta_q(g)} = \overline{\beta_q(g)} .$$

Ainsi $\overline{\beta_q(g)}$ est uniquement déterminé par $\overline{g} \in G(\overline{L}|\overline{E})$. Posant $\overline{\beta_q(g)} = \beta_q(\overline{g})$, on a, pour $g, g' \in G(\overline{L}|\overline{E})$,

$$\beta_q(\overline{gg'}) = \overline{g}(\beta_q(\overline{g'})) \cdot \beta_q(\overline{g}) ;$$

dans ces conditions, on sait qu'il existe $\overline{a}_q \in \overline{L}$, $\overline{a}_q \neq 0$ tel que $\beta_q(\overline{g}) = \overline{g}(\overline{a}_q) \cdot \overline{a}_q^{-1}$ pour tout $\overline{g}$. Alors, puisque les $\beta_q(\overline{g})$ sont racines δ_q -ième de l'unité, $\overline{a}_q^{\delta_q} \in \overline{E}$. On en déduit que $(\beta_q(\overline{g}) \mid \overline{g} \in G(\overline{L}|\overline{E}))$ est le groupe des racines δ_q -ième de l'unité contenues dans $\overline{L}$.

En conclusio:

$$\begin{aligned} \theta_q^{(\pi_0)}(\sigma \cdot \tau) &= \{ \theta_q^{(\pi_0)}(\sigma') , \sigma' \in \sigma \cdot \tau \} \\ &= \{ \overline{g}(\theta_q^{(\pi_0)}(\tau)) \cdot \beta_q(\overline{g}) + \theta_q^{(\pi_0)}(\sigma) , \overline{g} \in G(\overline{L}|\overline{E}) \} \\ &= \theta_q^{(\pi_0)}(\sigma) + [\theta_q^{(\pi_0)}(\tau)]_{\delta_q} . \end{aligned}$$

(ii) Il est clair que, si $\sigma, \tau \in H_q$, alors

$$\theta_q^{(\pi_0)}(\sigma) + \theta_q^{(\pi_0)}(\tau) \in \theta_q^{(\pi_0)}(\sigma \cdot \tau) \subset \theta_q^{(\pi_0)}(H_q)$$

et

$$\theta_q^{(\pi_0)}(\text{id}_{\overline{E}}) = 0 \in \theta_q^{(\pi_0)}(H_q) ;$$

puisque $\theta_q^{(\pi_0)}(H_q)$ est fini, c'est un sous-groupe additif de $\overline{L}$.

Le reste se vérifie facilement.

COROLLAIRE 1. - Si $\overline{K}$ est de caractéristique zéro, on a $M_q^{(\pi_0)} = (0)$, $0 \leq q \leq m-1$,
et

$$H_0 = H_1 = \dots = H_q = \dots = H_{m-1} = H_m = \{\text{id}_{\overline{E}}\} .$$

COROLLAIRE 2. - Les entiers $r_q = [H_q : H_{q+1}] = n_q / n_{q+1}$ (resp. $n_q = \text{card } H_q$),
 $0 \leq q \leq m-1$, sont des puissances de p .

COROLLAIRE 3. - Soit $A \subset H_q$; pour que

$$A/H_{q+1} = \{\sigma H_{q+1}, \sigma \in A\}$$

soit un sous-hypergroupe de H_q/H_{q+1} , il faut et il suffit que $\theta_q^{(\pi_0)}(A)$ soit un
sous-groupe additif de $\bar{L}$ stable par la multiplication par les éléments de $\bar{R}_{\delta_q}$
et par le groupe de Galois $G(\bar{L}|\bar{E})$.

3. Extensions primitives des corps p-adiques.

On dit qu'une extension $E|K$ est primitive si E ne contient aucun sous-corps
contenant K , distinct de E et K .

Pour qu'une extension séparable $E|K$ soit primitive, il faut et il suffit que
 $H(E|K)$ ne contienne aucun sous-hypergroupe propre. En particulier, une extension
galoisienne est primitive si, et seulement si, son groupe de Galois est cyclique
d'ordre un nombre premier.

NOTA BENE. - Si K est de caractéristique $p \neq 0$, les extensions primitives non
séparables de K sont les extensions radicielles de degré p . Il suffit donc de
faire l'étude des extensions primitives séparables.

Revenons aux notations du § 2 . Soit $\omega_{E|K}$ la différentielle de l'extension sépara-
ble $E|K$ (avec $\bar{E}|\bar{K}$ séparable). On sait que, si $\alpha \in A_E$ est tel que $E = K[\alpha]$,
alors $\omega_{E|K} = P'(\alpha) \cdot \Lambda_E$, où P est le polynôme minimal de α . Posons

$$\omega_{E|K} = \pi_E^{\mu_1} \Lambda_E ,$$

où $\mu_1 = \mu_1(E|K) = w_E(P'(\alpha))$ est l'exposant différentiel de $E|K$. Puisque
 $P'(\alpha) = \prod_{\sigma \neq \text{id}_E} (\alpha - \sigma\alpha)$, on a

$$\begin{aligned} \mu_1(E|K) &= w_E(P'(\alpha)) = \sum_{\sigma \neq \text{id}_E} w_E(\sigma\alpha - \alpha) = \sum_{\sigma \neq \text{id}_E} (v(\sigma) + 1) \\ &= n_{-1} - 1 + \sum_{q=0}^{m-1} (n_q - n_{q+1}) v_q = n_{-1} + \mu(E|K) - 1 \end{aligned}$$

avec

$$\mu(E|K) = \sum_{q=0}^{m-1} (n_q - n_{q+1}) v_q .$$

On déduit de la formule de transitivité des différentielles :

$$\omega_{E|E'} = \omega_{E|E''} \omega_{E''|E'}$$

et de l'expression ci-dessus des exposants différentiels le lemme suivant.

LEMME 6. - Soit $0 \leq q \leq m-1$; si $E_q \subset E' \subset E'' \subset E_{q+1}$, avec $E''|E'$ primitive,

alors $v_0(E''|E') = v_q(E|K) = v_q$ et $v_1(E''|E') = +\infty$.

COROLLAIRE. - Les dénominateurs d_q des v_q , $0 \leq q \leq m-1$, sont premiers à p ; c'est-à-dire $d_q = \delta_q$.

En effet, soit $E''|E'$ une extension primitive telle que $E_q \subset E' \subset E'' \subset E_{q+1}$. On déduit du corollaire de la proposition 2 que $[E'' : E'] = n''$ est une puissance de p . Comme

$$\mu_1(E''|E') = [E'' : E'] - 1 + \mu(E''|E') = (n'' - 1)(1 + v_0(E''|E')) = (n'' - 1)(1 + v_q) = k_q$$

est un entier, on a $(n'' - 1)(j_q + d_q) = d_q k_q$ où $v_q = j_q/d_q$, $(j_q, d_q) = 1$.

Si p divisait d_q , on aurait :

$$d_q \equiv 0 \pmod{p} \text{ et } j_q \equiv 0 \pmod{p},$$

ce qui est absurde.

Considérons la suite des sous-corps d'inertie et de ramification de l'extension $E|K$:

$$E_{-2} = K \subset E_{-1} \subset E_0 \subset \dots \subset E_{m-1} \subset E_m = E.$$

Supposons $E|K$ primitive; alors $m \leq 1$; car sinon, on aurait

$$K \subset E_0 \subset E_1 \subsetneq E_2 \subset E;$$

ce qui est absurde. Ainsi :

(i) Ou bien $m = -1$; alors $E_{-2} = K$; $E_{-1} = E$, et l'extension $E|K$ est non ramifiée;

(ii) ou bien $m = 0$; alors $E_{-2} = E_{-1} = K$; $E_0 = E$, et l'extension $E|K$ est totalement ramifiée sans nombre de ramification propre;

(iii) ou bien $m = 1$; alors $E_{-2} = E_{-1} = E_0 = K$; $E_1 = E$, et l'extension $E|K$ est totalement ramifiée ayant un seul nombre de ramification propre v_0 .

Nous allons supposer dans la suite (sauf pour le théorème 2) que le corps résiduel $\bar{K}$ est fini; si p est la caractéristique de $\bar{K}$, alors K est une extension finie de $\mathbb{Q}_p$ ou du corps des séries formelles $\mathbb{F}_p((X))$.

THEOREME 1. - Soit K un corps de valuation discrète complet de corps résiduel $\bar{K}$ fini.

Soit $E|K$ une extension séparable finie. Si $E_{-2} = K$ et $E_{-1} = E$, alors l'extension $E|K$ est non ramifiée cyclique de degré $[E : K] = f$. De plus, $E|K$ est primitive si, et seulement si, $[E : K] = f$ est un nombre premier.

On a $H_{-1} = \{\text{id}_E\}$; alors

$$H(E|K) = H(E|K)/H_{-1} \simeq H(\bar{E}|\bar{K}).$$

Puisque $\bar{K}$ est fini, $H(\bar{E}|\bar{K})$ est un groupe cyclique. Ainsi $E|K$ est primitive si, et seulement si, $H(E|K) \simeq H(\bar{E}|\bar{K})$ est un groupe cyclique d'ordre f premier.

THEOREME 2. - Soit K un corps de valuation discrète complet.

Soit $E|K$ une extension séparable finie telle que $E_{-2} = E_{-1} = K$ et $E_0 = E$.
L'extension $E|K$ est totalement ramifiée de degré n premier à p . De plus, $E|K$
est primitive si, et seulement si, $n = [E : K]$ est un nombre premier (distinct de
 p).

En effet, on a $H_{-1} = H(E|K)$ et $H_0 = \{\text{id}_E\}$. Alors

$$n = [E : K] = \text{card } H(E|K) = [H_{-1} : H_0] = r_{-1}$$

est premier à p (corollaire 1, prop. 1). De plus

$$\theta_{-1}(H_{-1}/H_0) = \theta_{-1}(H_{-1})$$

a le même nombre d'éléments que $H_{-1} = H(E|K)$. Comme $\theta_{-1}(H_{-1})$ est un sous-groupe multiplicatif d'ordre n d'un sur-corps de $\bar{K}$, c'est le groupe des racines n -ièmes de l'unité de ce corps. Pour que $E|K$ soit primitive, il faut et il suffit que $\theta_{-1}(H_{-1})$ ne contienne aucun sous-groupe multiplicatif propre (corollaire 2, prop. 1), ce qui équivaut à $\text{card } \theta_{-1}(H_{-1}) = n$ est un nombre premier (distinct de p).

Désignons par $\underline{F}_r$ le corps fini $\underline{F}_p^r$, $r \geq 1$. Supposons $\bar{K}$ fini; soit $E|K$ une extension séparable finie. Si p est la caractéristique de $\bar{K}$, on a $\bar{E} = \underline{F}.f'$, où $f' = [\bar{E} : \underline{F}_p]$. Alors, avec les notations de la proposition 2, le groupe de Galois $G(\bar{L}|\bar{E})$ est cyclique, engendré par l'automorphisme de Frobenius $\varphi_{f'} : \bar{L} \rightarrow \bar{L}$, où $\varphi_{f'}(\eta) = \eta^{p^{f'}}$.

Soit $0 \leq q \leq m-1$; comme le dénominateur d_q de v_q est premier à p , prenant L assez grand pour que $\bar{L}$ contienne toutes les racines d_q -ièmes de l'unité; on voit que $\bar{R}_{d_q}$ est le groupe multiplicatif du sous-corps $\underline{F}.\alpha_q$ de $\bar{L}$, où v_q est le plus petit entier tel que $p^{v_q} \equiv 1 \pmod{d_q}$.

Désignons par φ'_0 la restriction de $\varphi_{f'}$ à $\underline{F}.\alpha_q$; c'est un automorphisme de $\underline{F}.\alpha_q$. Considérons l'anneau (non nécessairement commutatif) $\underline{F}.\alpha_q[X, \varphi'_q]$ les polynômes relativement à $\varphi'_q : X.\alpha = \varphi'_q(\alpha) X$, $\alpha \in \underline{F}.\alpha_q$. On sait que cet anneau (anneau des polynômes de Ore à coefficients dans $\underline{F}.\alpha_q$) est principal à gauche et à droite.

On déduit de la proposition 2 que $M_q^{(\pi_0)}$ est un sous-groupe additif de $\bar{L}$ stable par la multiplication par les éléments de $\underline{F}.\alpha_q$ et par le générateur $\varphi_{f'}$ de $G(\bar{L}|\bar{E})$. Ainsi, on voit que $M_q^{(\pi_0)}$ est un $\underline{F}.\alpha_q[X, \varphi'_q]$ -module à gauche si l'on pose, pour $S = \sum \alpha_j X^j \in \underline{F}.\alpha_q[X, \varphi'_q]$ et $\eta \in M_q^{(\pi_0)}$,

$$S.\eta = \sum \alpha_j \varphi_{f'}^j(\eta).$$

Si $m = 1$, l'extension $E|K$ n'a qu'un seul nombre de ramification propre v_0 .

THEOREME 3. - Soit K un corps de valuation discrète complet de corps résiduel $\bar{K}$ fini.

Soit $E|K$ une extension séparable finie telle que $E_{-2} = E_{-1} = E_0 = K$ et $E_1 = E$; alors l'extension $E|K$ est totalement ramifiée de degré une puissance de p . De plus $E|K$ est primitive si, et seulement si, $M_0^{(\pi_0)}$ est un $\mathbb{F}_p \cdot v_0[X, \varphi'_0]$ -module simple.

On a $H(E|K) = H_{-1} = H_0$, $H_1 = \{\text{id}_E\}$ et

$$\theta_0^{(\pi_0)}(H_0) = \theta_0^{(\pi_0)}(H_0/H_1) = M_0^{(\pi_0)}$$

est un sous-groupe additif du corps fini $\bar{L}$. Comme $\theta_0^{(\pi_0)}$ est une bijection, on a

$$[E:K] = \text{card } H(E|K) = \text{card } H_0 = \text{card } M_0^{(\pi_0)}$$

est une puissance de p . On déduit aussitôt du corollaire 3 (prop. 2) que l'extension $E|K$ est primitive si, et seulement si, $M_0^{(\pi_0)}$ est un $\mathbb{F}_p \cdot v_0[X, \varphi'_0]$ -module simple.

REMARQUE 7. - Soit S un élément de degré minimal, de l'annulateur du $\mathbb{F}_p \cdot v_0[X, \varphi'_0]$ -module $M_0^{(\pi_0)}$. L'extension $E|K$ est primitive si, et seulement si, S est irréductible; on a alors $[E:K] = p^{u \cdot v_0}$, où $u = \deg S$.

Soit k un corps de caractéristique p ; on dit qu'un polynôme $P \in k[X]$ est additif si $P(Y+Z) = P(Y) + P(Z)$; on voit que $P = \sum_{j=0}^r \alpha_j Y^{p^j}$; les racines de P forment un groupe additif. Les sous-groupes additifs finis M de k sont en correspondance bijective avec les polynômes additifs unitaires séparables ayant toutes leurs racines dans k . On voit que M est stable par l'automorphisme $\eta \mapsto \eta^{p^{f'}}$ si, et seulement si, P est dans $\mathbb{F}_p \cdot f'[Y]$, et M est un $\mathbb{F}_p \cdot r$ -espace vectoriel si, et seulement si, $P \in \mathbb{F}_p \cdot v[Y]$. On déduit de ces conditions que M est un $\mathbb{F}_p \cdot v[X, \varphi_{f'}]$ -module à gauche; si $P = \sum_{j=0}^r \alpha_j Y^{p^j}$ est le polynôme correspondant à M , l'élément $S = \sum_{j=0}^r \alpha_j X^j$ de $\mathbb{F}_p \cdot v[X, \varphi_{f'}]$ est appelé le polynôme de Ore associé à M .

REMARQUE 8. - Avec les notations du théorème 3, si $S_0 = \sum_{j=0}^r \alpha_j X^j \in \mathbb{F}_p \cdot v_0[X, \varphi'_0]$ est le polynôme de Ore associé au groupe additif fini $M_0^{(\pi_0)}$, c'est un annulateur de $M_0^{(\pi_0)}$ de degré minimal. L'extension $E|K$ est primitive si, et seulement si, le polynôme de Ore S_0 , associé à $M_0^{(\pi_0)}$ est irréductible dans $\mathbb{F}_p \cdot v_0[X, \varphi'_0]$.

Les théorèmes 1, 2 et 3 montrent que l'étude des extensions primitives d'un corps local K se réduit essentiellement à celle des extensions primitives totalement ramifiées, c'est-à-dire à celle des polynômes d'Eisenstein.

Soit donc $P = \sum_{j=0}^n a_{n-j} Y^j \in K[Y]$ un polynôme d'Eisenstein séparable ($a_0 = 1$, $a_{n-j} \in \mathfrak{m}_K$, $1 \leq j \leq n$, $a_n \notin \mathfrak{m}_K^2$). Soit Π une racine de P , et posons $E = K[\Pi]$. Considérons le polynôme $\Theta(Y) = P(\Pi Y + \Pi) \in E[Y]$; les racines de Θ sont les $(\sigma\Pi/\Pi) - 1$, $\sigma \in H(E|K)$. Il est clair que si Z_q est l'ensemble des racines z de Θ telles que $w_E(z) = v_q$, alors

$$Z_q = \{z = \frac{\sigma\Pi}{\Pi} - 1, \sigma \in H_q, \sigma \notin H_{q+1}\}$$

et

$$\text{card } Z_q = n_q - n_{q+1}$$

(avec les notations du § 2). On en déduit aussitôt que les pentes des segments du polynôme de Newton de $\Theta(Y)$ ou de $\Pi^{-n} \Theta(Y)$ sont les nombres rationels v_q , $0 \leq q \leq m-1$. De plus, on voit que $M_q^{(\pi_0)}$ est égal à $\{\eta \in \bar{\Omega}; \bar{P}_q(\eta) = 0\}$ où $P_q(Y) = \prod_{z \in Z_q} (Y - (z/\Pi^v q))$.

On a $\Theta(Y) = \sum_{i=0}^n b_i Y^i$, où $b_i = \sum_{j=i}^n \binom{j}{i} a_{n-j} \Pi^j$, $1 \leq i \leq n$, $b_0 = 0$. Considérons $\alpha_{ij} = w_E(\binom{j}{i} \Pi^j)$ et $t_{n-j} = w_E(a_{n-j})$; alors

$$w_E(b_i) = \min_{1 \leq j \leq n} (\alpha_{ij} + t_{n-j}).$$

Posons $n = \epsilon p^r$, $(\epsilon, p) = 1$;

(a) si $p^u < i < p^{u+1}$, $u < r$, alors

$$w_E(b_i) \geq w_E(b_p^u)$$

(b) $w_E(b_p^r) = w_E(b_n) = n$.

Posons $w_u = w_E(b_p^u)$, $0 \leq u \leq r$, et définissons par récurrence descendante $\mu_r, \mu_{r-1}, \dots, \mu_0$, où $\mu_r = \min_{1 \leq j \leq n} (j + t_{n-j})$; et, ayant déterminé $\mu_r, \dots, \mu_{u+1}$, on pose

$$\mu_u = \min_{j \not\equiv 0 \pmod{p^{u+1}}, 1 \leq j \leq n} (\mu_{u+1} + e_0, j + t_{n-j}),$$

où e_0 est l'indice de ramification de l'extension $E|k$; $k = \mathbb{Q}_p$ ou $\mathbb{F}_p((X))$. On a le lemme suivant.

LEMME 7. - Si $\mu_u \neq \mu_{u-1}$, alors $\mu_u = w_u$ et si $\mu_u = \mu_{u-1}$, on a $\mu_u \leq w_u$.

Considérons la suite croissante (μ_i) , $0 \leq i \leq s$, extraite de (μ_u) , $0 \leq u \leq r$, telle que $\mu_{i_0} = \mu_r$, $\mu_{i_s} = \mu_0$, $\mu_{i_j} \neq \mu_{i_j} - 1$ et, d'une part si $i_j = u$, $\mu_{i_j} = w_u$, d'autre part si $i_j < u < i_{j-1}$, $\mu_{i_j} = \mu_u \leq w_u$, on a

$$\mu_{i_j} - \mu_{i_{j-1}} = \mu_{i_{j-1}-1} - \mu_{i_{j-1}} \leq e_0,$$

et si $\mu_{i,j} - \mu_{i,j-1} = e_0$, alors

$$\mu_{i,j} = m_{i,j} p^{i,j}, \quad (m_{i,j}, p) = 1.$$

On voit que les sommets du polygone de Newton de $\Pi^{-n} \phi(Y)$ (indéxés par des entiers i_q , $0 \leq q \leq m-1$) autres que $(0, 0)$ et $(n, +\infty)$ sont parmi les points $(n - p^{i,j}, \mu_{i,j} - n)$ du plan réel tels que, si $(n - p^{i,j}, \mu_{i,j} - n)$ et $(n - p^{i,j'}, \mu_{i,j'} - n)$ sont des sommets contigus, $j' < j$; alors j' est le plus grand entier tel que

$$\frac{\mu_{i,j'} - \mu_{i,j}}{p^{i,j'} - p^{i,j}} = \min_{t > j} \frac{\mu_{i,t} - \mu_{i,j}}{p^{i,t} - p^{i,j}}.$$

Soit s_q le nombre des points $(n - p^{i_q}, \mu_{i_q} - n)$, $i_q \leq i \leq i_{q+1}$, situés sur le segment joignant $(n - p^{i_q}, \mu_{i_q} - n)$ à $(n - p^{i_{q+1}}, \mu_{i_{q+1}} - n)$. Considérons $\beta_i \in \Omega$ tel que $\beta_i^{p^{i_{q+1}}} = b_i / \pi^{\mu_{i_q}}$; on a $w_E(\beta_i) = 0$ et il existe $\alpha_i \in K$ tel que $w_E(\alpha_i - \beta_i) > 0$.

LEMME 8. - On a

$$v_q = \frac{\mu_{i_q} - \mu_{i_{q+1}}}{p^{i_{q+1}} - p^{i_q}} = \frac{w_{i_q} - w_{i_{q+1}}}{p^{i_{q+1}} - p^{i_q}}; \quad n_q = p^{i_q},$$

et $M_q^{(\pi_0)}$ est l'ensemble des racines du polynôme $\sum_{j=0}^{s_q} \bar{\beta}_{i_j}(q) Y^{p^{i_j}(q)} \in \bar{K}[Y]$.

COROLLAIRE.

(i) On a $n_q v_q \leq p/(p-1) e_0$.

(ii) Si la valuation p-adique de v_q est ≥ 1 , on a $n_q v_q = \frac{p}{p-1} e_0$ et $r_q = p$.

Réunissant les théorèmes 2 et 3, on a le théorème suivant.

THEOREME 4. - Soit K un corps local, et soit $P \in K[Y]$ un polynôme d'Eisenstein séparable de degré $n = \epsilon p^r$, $(\epsilon, p) = 1$.

Toute extension $E|K$, telle que $E = K[\Pi]$, avec $P(\Pi) = 0$, est primitive si, et seulement si,

(i) ou bien $r = 0$, et $n = \epsilon$ est un nombre premier.

(ii) ou bien $c = 1$, et

(a) pour tout u , $0 \leq u < r$, $(\mu_0 - \mu_r)/(p^r - 1) \leq (\mu_u - \mu_r)/(p^r - p^u)$,

(b) d_0 étant le dénominateur de l'unique nombre de ramification propre

$v_0 = (\mu_0 - \mu_r)/(p^r - 1)$, α_0 le plus petit entier tel que $p^{\alpha_0} \equiv 1 \pmod{d_0}$,
 $f' = [\bar{K} : \bar{F}_p]$, $\bar{\beta}_u$ la classe de b_u/π^{μ_u} dans $\bar{K}$ et U étant l'ensemble des en-
tiers u tels que $(\mu_u - \mu_r)/(p^r - p^{\mu_u}) = v_0$; le polynôme de Ore $S_0 = \sum_{u \in U} \bar{\beta}_u X^u$
est irréductible dans $\bar{F}_p[X, \varphi'_0]$.

EN RÉSUMÉ : Les extensions primitives séparables d'un corps local K sont

- ou bien les extensions non ramifiées cycliques de degré un nombre premier ;
- ou bien les extensions totalement ramifiées de degré un nombre premier distinct de la caractéristique résiduelle p de K ;
- ou bien les extensions totalement ramifiées de degré une puissance de p , vérifiant les conditions (ii) du théorème 4.

Dans sa note aux Comptes rendus [4] Marc KRASNER donne la liste des extensions primitives de degré 8 de $\mathbb{Q}_2$.

L'exposé suit d'assez près [3] sauf que l'on se place dans la situation générale des corps de valuation discrète complets, ce qui impose la modification de certaines démonstrations. Dans [3], Marc KRASNER donne également des conditions pour que deux polynômes d'Eisenstein définissent la même extension.

RÉFÉRENCES

- [1] ARTIN (E.). - Algebraic numbers and algebraic functions. - New York, Gordon and Breach, 1967.
- [2] KRASNER (M.). - Sur la théorie de la ramification des idéaux des corps non-galoisiens de nombres algébriques, Mémoires de l'Académie de Belgique (classe des Sciences), t. 11, 1937, fasc. 4, p. 1-110.
- [3] KRASNER (M.). - Sur la primitivité des corps p -adiques, Mathematica, Cluj, t. 13, 1937, p. 72-191.
- [4] KRASNER (M.). - Le nombre des sur-corps primitifs d'un degré donné et le nombre des sur-corps métagaloisiens d'un degré donné d'un corps de nombres p -adiques, C. R. Acad. Sc., Paris, t. 206, 1938, Série A, p. 876-877.
- [5] KRASNER (M.). - La loi de Jordan-Hölder dans les hypergroupes et les suites génératrices des corps de nombres p -adiques, Duke Math. J., t. 7, 1940, p. 121-135.
- [6] KRASNER (M.). - Nombres des extensions d'un degré donné d'un corps p -adique, Colloques internationaux du CNRS, 143 : "Les tendances géométriques en algèbre et théorie des nombres [1964. Clermont-Ferrand]. - P. 143-169. - Paris, CNRS, 1966.
- [7] SERRE (J.-P.). - Corps locaux. - Paris, Hermann, 1962 (Actualités scientifiques et industrielles, 1296 ; Publications de l'Institut de Mathématiques de l'Université de Nancago, 8).
- [8] WEISS (E.). - Algebraic number theory. - New York, London, Mac Graw Hill Company, 1963 (International Series in pure and applied Mathematics).