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 d'étude d'Analyse ultramétrique
(Y. AMICE, G. CHRISTOL, P. ROBBA)
9e année, 1981/82, n° 24, 19 p.

10 mai 1982

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 σ, $\tau \in H$, $\sigma.\tau$ ou $\sigma\tau$ l'image de (σ, τ) par cette application. Si A et B sont deux parties non vides de H, on pose

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

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

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

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

NOTA BENE. - On voit aussitôt dans ces conditions que, si pour tout $\sigma, \tau \in H$, $\sigma.\tau$ 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

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

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

$$\forall\, \sigma, \tau \in H , \quad \sigma \in \tau.h \Longrightarrow \tau \in \sigma.h .$$

(*) 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 $\sigma \in H$, $\mathrm{card}(\sigma.h) = \mathrm{card}\ h$.

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 $\mu : H \longrightarrow H'$ est un morphisme d'hypergroupes si

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

(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 $\sigma, \tau \in h$, $\sigma.\tau \subset h$.

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

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

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

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

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

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

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

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

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

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

$$\sigma.\tau = \mathrm{corr}(\mathrm{gen}\ \sigma\ \ \mathrm{gen}\ \tau)$$

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

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 $s, t \in \mathrm{gen}\ \sigma$,

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

on a $sg = tg$, et $\mathrm{gen}\ G.g = sg$ 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 $\mathrm{gen}\ \sigma.g$. On voit que cette application est un isomorphisme de l'hypergroupe $H(E|K)$ sur l'hypergroupe c. g.

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

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

$$corr_N(gen_N\ \sigma\ \ gen_N\ \tau) = corr(gen\ \sigma\ \ gen\ \tau) = \sigma.\tau\ .$$

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 $L = inv\ h$ de E des invariants de h , et a 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 $w_K(K^*) = \underset{\sim}{Z}$, par Λ_K (resp. m_K) l'anneau de valuation (resp. l'idéal maximal) de K , par π_K une uniformisante de K , et par $\overline{K}$ 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 Λ_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 $\overline{E}|\overline{K}$ séparable, contient un unique sous-corps maximal T (corps d'inertie) tel que $T|K$ est non ramifiée avec $\overline{T} = \overline{E}$; de plus, $E|K$ est totalement ramifiée. On définit, par passage au quotient, une application $H(E|K) \longrightarrow H(\overline{E}|\overline{K})$, en posant, pour $\sigma \in H(E|K)$, $a \in \Lambda_E$,

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

Cette application est un morphsime surjectif d'hypergroupes. De plus

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

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 $v(\sigma) \geqslant -1$.

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

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

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

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

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

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

d'où

$$v(\sigma') \geqslant \upsilon \quad \text{et} \quad \sigma' \in h_\upsilon \ .$$

NOTA BENE. - Si $\nu \leqslant -1$, alors $h_\upsilon = H(E|K)$.

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 $v(\sigma) = w_E((\sigma\pi_E/\pi_E) - 1) \geqslant 0$,
- 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

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

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

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

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

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

donc

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

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

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

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

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

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

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

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

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

De plus, $\forall\, \upsilon \in \mathbb{Q}$, il existe $0 \leqslant q \leqslant m$ tel que $h_\upsilon = H_q$. On a

$$H_m = \{id_E\} \subset H_{m-1} \subset \ldots \subset H_0 \subset H_{-1} \subset H_{-2} = H(E|K) .$$

On dit que $H_{-1} = H(E|T)$ est le sous-hypergroupe d'inertie, et H_q , $0 \leqslant q \leqslant m-1$, 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 $E_q = \mathrm{inv}(H_q)$, $0 \leqslant q \leqslant m$; on a

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

Les corps $E_{-1} = T$ et E_q , $0 \leqslant q \leqslant m-1$, 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

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

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

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 $-2 \leqslant q \leqslant m-1$, on a

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

donc

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

de plus

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

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 $\mathfrak{A}_N = \mathfrak{A}_K[\beta]$, et $\alpha \in E$ tel que $\mathfrak{A}_E = \mathfrak{A}_K[\alpha]$. Posons, pour $s \in G(N|K)$, $a(s , N) = (s\beta - \beta)\ \mathfrak{A}_\Omega$ et pour $\sigma \in H(E|K)$, $a(\sigma , E) = (\sigma\alpha - \alpha)\ \mathfrak{A}_\Omega$. On sait (cf. [1], chapitre 5, § 4) que

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

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

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

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

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

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 $\geqslant -1$), on obtient

$$e_{N|E}(v(\sigma) + 1) = \Sigma_{s \in gen_N \sigma}(v_N(s) + 1)$$

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

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

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

$$e_{N|E}.(v(\sigma) + 1) = \Sigma_{s \in gen_N \sigma}(v_N(s) + 1) = 0 ;$$

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

Considérons $G_0 = \{s \in G ; \ v_N(s) \geqslant v_{N,0}\}$ 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 $gen_N \sigma \cap G_0 \neq \emptyset$.

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

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

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

(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 $\sigma H_0 \longrightarrow \theta_{-1}(\sigma H_0)$ 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 $\sigma H_0 \longrightarrow \theta_{-1}(\sigma H_0)$ est un isomorphisme d'hypergroupes de H_{-1}/H_0 sur $\theta_{-1}(H_{-1})$.

(i) Soient σ , $\tau \in H_{-1}$ et $s \in \mathrm{gen}_N \sigma \cap G_{-1}$; on a $\mathrm{gen}_N \sigma = s \in G(N|E)$; tout $s' \in \mathrm{gen}_N \sigma$ 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 $s' \in \mathrm{gen}_N \sigma$, $t' \in \mathrm{gen}_N \tau$; ainsi

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

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 σ , $\tau \in H_{-1}$, 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 $\sigma \ H_0 \longrightarrow \theta_{-1}(\sigma \ H_0)$ est une bijection de H_{-1}/H_0 sur $\theta_{-1}(H_{-1})$. Le reste se vérifie facilement.

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

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

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

COROLLAIRE 2. - <u>Soit</u> $A \subset H_{-1}$ <u>tel que</u> $\theta_{-1}(A)$ <u>est un sous-groupe de</u> $\theta_{-1}(H_{-1})$; <u>alors si</u> $\sigma \in H_{-1}$, $\theta_{-1}(\sigma \cdot A) = \theta_{-1}(\sigma) \cdot \theta_{-1}(A)$ <u>et</u> $A \cdot H_0/H_0$ <u>est un sous-hypergroupe de</u> 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 <u>le plus petit commun multiple des entiers</u> d_q .

Considérons $\pi_0 \in \Omega$ tel que $\pi_0^d = \pi_E$; un <u>sur-corps</u> L <u>de</u> 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 $\theta_q^{(\pi_0)} : H_q \longrightarrow \bar{L}$ $\theta_q^{(\pi_0)}(\sigma) = \overline{x_q(\sigma)}$. 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 $\eta \in \bar{L}$,

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

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 $d_q = p^{\upsilon_q}\,\delta_q$, $(p , \delta_q) = 1$, 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 $0 \leqslant q \leqslant m-1$; 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

$$\sigma\, H_{q+1} \longrightarrow \theta_q^{(\pi_0)}(\sigma\, H_{q+1}) = \theta_q^{(\pi_0)}(\sigma)$$

ne dépend que de la classe $\sigma\, H_{q+1}$; 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 $s \in \mathrm{gen}_L\,\sigma \cap G_0 \neq \emptyset$ (Remarque 6), on a $\mathrm{gen}_L\,\sigma = s\,G(L|E)$, et tout $s' \in \mathrm{gen}_L\,\sigma$ s'écrit $s' = s \circ g$, où $g \in G(L|E)$. Soit τ un autre élément de H_q. Considérons $\sigma' \in \sigma.\tau$; on a $\sigma' = (s' \circ t')_{|E}$ où $s' = s \circ g \in \mathrm{gen}_L\,\sigma$, $s \in G_0$, $g \in G(L|E)$ et $t' \in \mathrm{gen}_L\,\tau$. Ainsi

$$x_q(\sigma') = \frac{\sigma'\pi_E - \pi_E}{\alpha_q} = \frac{s' \circ t'(\pi_E) - \pi_E}{\alpha_q} = \frac{s'(\tau\pi_E) - \pi_E}{\alpha_q} = \frac{s'(\alpha_q\, x_q(\tau) + \pi_E) - \pi_E}{\alpha_q}$$

$$= \frac{s'(\alpha_q\, x_q(\tau))}{\alpha_q} + \frac{s'(\pi_E) - \pi_E}{\alpha_q}$$

$$= \frac{s'(\alpha_q\, x_q(\tau))}{\alpha_q} \times \frac{s'(\alpha_q)}{s'(\alpha_q)} + \frac{\sigma(\pi_E) - \pi_E}{\alpha_q} = s'(x_q(\tau)) \times \frac{s'(\alpha_q)}{\alpha_q} + x_q(\sigma)\ .$$

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

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

Ainsi

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

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

$$g(\pi_q)^{d_q} = g(\pi_q^{d_q}) = g(\pi_E) = \pi_E = \pi_q^{d_q}\ ;$$

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 $d_q = p^{\nu_q}\,\delta_q$ 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

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

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

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

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

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

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

En conclusion

$$\theta_q^{(\pi_0)}(\sigma.\tau) = \{\theta_q^{(\tau_0)}(\sigma') , \ \sigma' \in \sigma.\tau\}$$

$$= \{\bar{g}(\theta_q^{(\pi_0)}(\tau)).\beta_q(\bar{g}) + \theta_q^{(\pi_0)}(\sigma) , \ \bar{g} \in G(\bar{L}|\bar{E})\}$$

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

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

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

et

$$\theta_q^{(\pi_0)}(id_E) = 0 \in \theta_q^{(\pi_0)}(H_q) ;$$

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

Le reste se vérifie facilement.

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

$$H_0 = H_1 = \dots = H_q = \dots = H_{m-1} = H_m = \{id_E\} .$$

COROLLAIRE 2. - Les entiers $r_q = [H_q : H_{q+1}] = n_q/n_{q+1}$ (resp. $n_q = \text{card } H_q$) , $0 \leqslant q \leqslant m-1$, 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 $\mathfrak{D}_{E|K}$ la différente de l'extension séparable $E|K$ (avec $\bar{E}|\bar{K}$ séparable). On sait que, si $\alpha \in A_E$ est tel que $E = K[\alpha]$, alors $\mathfrak{D}_{E|K} = P'(\alpha).\Lambda_E$, où P est le polynôme minimal de α . Posons

$$\mathfrak{D}_{E|K} = \pi_E^{\mu_1} \Lambda_E ,$$

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

$$\mu_1(E|K) = w_E(P'(\alpha)) = \sum_{\sigma \neq id_E} w_E(\sigma\alpha - \alpha) = \sum_{\sigma \neq id_E} (v(\sigma) + 1)$$

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

avec

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

On déduit de la formule de transitivité des différentes :

$$\mathfrak{D}_{E|E'} = \mathfrak{D}_{E|E''} \, \mathfrak{D}_{E''|E'}$$

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

LEMME 6. - Soit $0 \leqslant q \leqslant m - 1$; 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, $0 \leqslant q \leqslant m-1$, 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

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

ce qui est absurde.

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

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

Supposons $E|K$ primitive ; alors $m \leqslant 1$; 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 $\overline{K}$ est fini ; si p est la caractéristique de $\overline{K}$, alors K est une extension finie de $\mathbb{Q}_p$ ou du coprs des séries formelles $\mathbb{F}_p((X))$.

THEOREME 1. - Soit K un corps de valuation discrète complet de corps résiduel $\overline{K}$ 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 $H_{-1} = \{id_E\}$; alors

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

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 $H_0 = \{id_E\}$. 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 card $\theta_{-1}(H_{-1}) = n$ est un nombre premier (distinct de p).

Désignons par $\underset{\sim}{F}_{p^r}$ le corps fini 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 $\bar{E} = \underset{\sim}{F}_{p^{f'}}$, où $f' = [\bar{E} : \underset{\sim}{F}_p]$. Alors, avec les notations de la proposition 2, le groupe de Galois $G(\bar{L}|\bar{E})$ est cyclique, engendré par l'automorphisme de Frobénius $\varphi_{f'} : \bar{L} \longrightarrow \bar{L}$, 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 $\underset{\sim}{F}_{p^{\nu_q}}$ de $\bar{L}$, où ν_q est le plus petit entier tel que $p^{\nu_q} \equiv 1 \pmod{d_q}$.

Désignons par φ'_0 la restriction de $\varphi_{f'}$ à $\underset{\sim}{F}_{p^{\nu_q}}$; c'est un automorphisme de $\underset{\sim}{F}_{p^{\alpha_q}}$. Considérons l'anneau (non nécessairement commutatif) $\underset{\sim}{F}_{p^{\nu_q}}[X, \varphi'_q]$ des polynômes relativement à φ'_q : $X \cdot \alpha = \varphi'_q(\alpha)\, X$, $\alpha \in \underset{\sim}{F}_{p^{\nu_q}}$. On sait que cet anneau (anneau des polynômes de Ore à coefficients dans $\underset{\sim}{F}_{p^{\nu_q}}$) 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 $\underset{\sim}{F}_{p^{\nu_q}}$ et par le générateur $\varphi_{f'}$ de $G(\bar{L}|\bar{E})$. Ainsi, on voit que $M_q^{(\pi_0)}$ est un $\underset{\sim}{F}_{p^{\nu_q}}[X, \varphi'_q]$-module à gauche si l'on pose, pour $S = \sum \alpha_j X^j \in \underset{\sim}{F}_{p^{\nu_q}}[X, \varphi'_q]$ et $\eta \in M_q^{(\pi_0)}$,

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

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 $\underset{\sim}{F}.\nu_0[X , \varphi_0']$-module simple.

On a $H(E|K) = H_{-1} = H_0$, $H_1 = \{id_E\}$ 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 $\underset{\sim}{F}.\nu_0[X , \varphi_0']$-module simple.

REMARQUE 7. - Soit S un élément de degré minimal, de l'annulateur du $\underset{\sim}{F}.\nu_0[X , \varphi_0']$-module $M_0^{(\pi_0)}$. L'extension $E|K$ est primitive si, et seulement si, S est irréductible ; on a alors $[E : K] = p^{u\nu_0}$, où $u = \deg S$.

Soit k un corps de caractéristique p ; on dit qu'un polynôme $P \in k[Y]$ 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 $\eta \longrightarrow \eta^{p^{f'}}$ si, et seulement si, P est dans $\underset{\sim}{F}.f'[Y]$, et M est un $\underset{\sim}{F}.r$-espace vectoriel si, et seulement si, $P \in \underset{\sim}{F}.\nu[Y]$. On déduit de ces conditions que M est un $\underset{\sim}{F}.\nu[X , \varphi_{f'}]$-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 $\underset{\sim}{F}.\nu[X , \varphi_{f'}]$ est appelé le polynôme de Ore associé à M .

REMARQUE 8. - Avec les notations du théorème 3, si $S_0 = \sum_{j=0}^{r} \alpha_j X^j \in \underset{\sim}{F}.\nu_0[X , \varphi_0']$ 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 $\underset{\sim}{F}.\nu_0[X , \varphi_0']$.

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 $P = \sum_{j=0}^{\cdot} a_{n-j} Y^j \in K[Y]$ un polynôme d'Eisenstein séparable ($a_0 = 1$, $a_{n-j} \in m_K$, $1 \leq j \leq n$, $a_n \notin m_K^2$). 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

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

et

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

(avec les notations du § 2). On en déduit aussitôt que <u>les pentes des segments du polynôme de Newton</u> 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

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

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

(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 $\mu_r , \mu_{r-1} , \cdots , \mu_0$, où $\mu_r = \min_{1 \leq j \leq n} (j + t_{n-j})$; et, ayant déterminé $\mu_r, \cdots, \mu_{u+1}$, on pose

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

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

Considérons la suite croissante (μ_{i_j}), $0 \leq j \leq s$, 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

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

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 polygône de Newton de $\Pi^{-n}\,\Theta(Y)$ (indéxés par des entiers i_q, $0 \leqslant q \leqslant m-1$) 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

$$\frac{\mu_{i_{j'}} - \mu_{i_j}}{p^{i_j} - p^{i_{j'}}} = \min_{t>j} \frac{\mu_{i_t} - \mu_{i_j}}{p^{i_j} - p^{i_t}} .$$

Soit s_q le nombre des points $(n - p^i, \mu_i - n)_{i_q \leqslant i \leqslant i_{q+1}}$, 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 $\beta_i^{p^{i_{q+1}}} = b_i/\pi^{\mu_i}$; 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 $n_q v_q \leqslant p/(p-1)\, e_0$.

(ii) Si la valuation p-adique de v_q est $\geqslant 1$, 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 $\epsilon = 1$, et

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

(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 $p^{\nu_0} \equiv 1 \pmod{d_0}$, $f' = [\bar{K} : \underset{\sim}{F}_p]$, $\bar{\beta}_u$ la classe de $b_p u/\pi^{\mu_u}$ dans $\bar{K}$ et U étant l'ensemble des entiers μ tels que $(\mu_u - \mu_r)/(p^r - p^\mu) = v_0$; le polynôme de Ore $S_0 = \sum_{u \in U} \bar{\beta}_u X^u$ est irréductible dans $\underset{\sim}{F}_{\nu_0}[X , \varphi_0']$.

EN RÉSUME : 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 $\underset{\sim}{Q}_2$.

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).