ANNALES SCIENTIFIQUES DE L'É.N.S.

JEAN-MARC FONTAINE

**Groupes de ramification et représentations d'Artin**

*Annales scientifiques de l'É.N.S. 4e série*, tome 4, nº 3 (1971), p. 337-392

<http://www.numdam.org/item?id=ASENS_1971_4_4_3_337_0>

*Ann. scient. Éc. Norm. Sup.*,
4e série, t. 4, 1971, p. 337 à 392.

# GROUPES DE RAMIFICATION ET REPRÉSENTATIONS D'ARTIN

PAR JEAN-MARC FONTAINE.

## INTRODUCTION.

Soit E un corps de caractéristique o et soit $\overline{E}$ une clôture algébrique de E. Soit $\alpha$ une représentation d'un groupe fini G par des matrices à coefficients dans $\overline{E}$ et soit $\varphi$ le caractère de cette représentation. On dit que $\alpha$ est *rationnelle sur* E s'il existe une représentation de G par des matrices à coefficients dans E dont le caractère est $\varphi$.

Soit K un corps local, c'est-à-dire un corps muni d'une valuation discrète pour laquelle il est complet. Soit L une extension finie galoisienne de K telle que l'extension résiduelle soit séparable. Soit G le groupe de Galois de l'extension. On sait définir la représentation d'Artin de l'extension, que l'on note $a_G$, et qui est une représentation de G. Le but de cet article est de chercher à quelles conditions $a_G$ est rationnelle sur E. On montrera, en particulier, les résultats suivants (*cf.* § 7, th. 1 et 2) :

THÉORÈME A. — *Si l'extension* L/K *est totalement ramifiée et si la caractéristique du corps résiduel est différente de* 2, *alors* $a_G$ *est rationnelle sur* E *si et seulement si l'algèbre* E[G] *est décomposée.*

(On dit qu'une algèbre semi-simple est *décomposée* si c'est un produit fini d'algèbres de matrices sur des corps commutatifs.)

THÉORÈME B. — *Si le corps résiduel* $k$ *de* K *est parfait, la représentation d'Artin de l'extension est rationnelle sur le corps des vecteurs de Witt de* $k$.

(Ce résultat avait été conjecturé par Serre.)

Nous utiliserons fréquemment certains des résultats que l'on trouve dans le livre de Serre sur les corps locaux ([7], cité CL).

Le groupe d'inertie de l'extension L/K est un groupe de type $R_p$, c'est-à-dire le produit semi-direct d'un groupe cyclique d'ordre premier à $p$ par un $p$-sous-groupe invariant. Les algèbres de groupes de type $R_p$ ont été étudiées dans [2] (cité DAG), et nous nous y réfèrerons souvent.

Le principe de la méthode suivie consiste à se ramener au cas où le groupe de Galois de l'extension a une structure très simple (groupe « de type $C_p$ ou $C'_p$ », lorsque la caractéristique $p$ du corps résiduel de K est différente de 2, et groupe de quaternions généralisé, lorsqu'elle est égale à 2).

Cet article comprend deux chapitres.

Le premier chapitre, où il n'est pas question de représentations, donne tous les résultats sur les corps locaux que nous utiliserons. Le premier paragraphe énonce un certain nombre de propriétés essentielles sur les groupes de ramification. Le deuxième indique comment construire des extensions modérement ramifiées; les résultats qu'il contient serviront à l'étude du problème de la rationalité lorsque l'extension L/K n'est pas totalement ramifiée. Le troisième donne quelques propriétés de ce que l'on appelle « les automorphismes sauvagement ramifiés » (*cf.* [6]); l'une d'entre elles sera utilisée dans le paragraphe 4. Dans ce dernier, on étudie, lorsque $p=2$, la ramification des extensions totalement ramifiées dont le groupe de Galois est isomorphe à un groupe de quaternions généralisé ou à un groupe diédral.

Le deuxième chapitre est consacré à l'étude des représentations d'Artin. Le paragraphe 5 donne quelques rappels sur la théorie des représentations. Dans le paragraphe 6, on définit la représentation d'Artin et on en donne une décomposition canonique. Dans le paragraphe 7 enfin, on étudie le problème de la rationalité de cette représentation.

# CHAPITRE I.

## Extensions galoisiennes des corps locaux.

### 1. Groupes de ramification.

1.1. Groupes de type $R_p$ (*cf.* DAG, n^os^ 6.1 et 7.1). — Soit $p$ un nombre premier et soit G un groupe fini. On dit que G est *de type* $R_p$ si c'est le produit semi-direct d'un groupe cyclique d'ordre premier à $p$ par un $p$-sous-groupe invariant.

Si G désigne un groupe de type $R_p$, on note P son $p$-sous-groupe de Sylow et H un sous-groupe cyclique de G, d'ordre premier à $p$, tel que $G = HP$. On note $n(G) = n$ l'ordre de H.

Si G est un groupe de type $R_p$, on dit qu'il est *de type* $C_p$ si P est abélien de type $(p, p, \ldots, p)$ et si, considéré comme $\mathbf{F}_p[H]$-module, il est isotypique. On note alors H′ le noyau de la représentation canonique de H dans P et G′ le produit direct $H' \times P$ (on voit que G′ est le centralisateur de P dans G). On pose $m(G) = (H' : 1)$ et $d(G) = (H : H')$ [on a donc $n(G) = m(G)\, d(G)$].

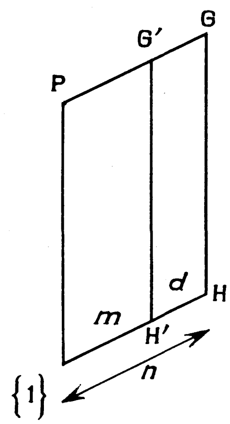


Fig. 1.

Soit G un groupe de type $R_p$. Soit $\lambda$ un entier strictement positif et soit

$$G = \Gamma_0 \supset \Gamma_1 \supset \ldots \supset \Gamma_{\lambda+1} = \{1\} \tag{1}$$

une suite de sous-groupes invariants de G vérifiant $\Gamma_j \neq \Gamma_{j+1}$, pour $j = 1, 2, \ldots, \lambda$. On dit que (1) est *une* $C_p$-*suite associée à* G si les conditions suivantes sont réalisées :

(i) le groupe $\Gamma_0/\Gamma_1$ est cyclique d'ordre premier à $p$;

(ii) pour $j = 1, 2, \ldots, \lambda$, le groupe $\Gamma_j/\Gamma_{j+1}$ est un groupe abélien de type $(p, p, \ldots, p)$, contenu dans le centre de $\Gamma_1/\Gamma_{j+1}$, qui, considéré comme $\mathbf{F}_p[\Gamma_0/\Gamma_1]$-module, est isotypique.

Dans ces conditions, on voit que $\Gamma_1 = P$ et que $\Gamma_0/\Gamma_1$ est canoniquement isomorphe à H. Par abus d'écriture, pour tout $j$ non nul, nous notons H l'image de H dans $G/\Gamma_{j+1}$.

Il est clair que, pour tout $j$ non nul, le groupe $H\Gamma_j/\Gamma_{j+1}$ est de type $C_p$. On dit que la famille des $H\Gamma_j/\Gamma_{j+1}$ est *la famille des groupes de type* $C_p$

*correspondant à la suite* (1) et que $H\Gamma_j/\Gamma_{j+1}$ est le $j^{\text{ième}}$ *terme de la famille.* On voit qu'il est défini (par le choix de H) à un isomorphisme près. Une famille de groupes de type $C_p$ correspondant à une suite associée à G est appelée *un système complet de groupes de type* $C_p$ *associés à* G.

1.2. Extensions des corps locaux. — Soit K un *corps local*, c'est-à-dire un corps muni d'une valuation discrète pour laquelle il est complet. On appelle *valuation normalisée* de K la valuation $v$ de K telle que $v(\mathbf{K}^\star) = \mathbf{Z}$.

Soit L une extension finie de K. Si $v'$ désigne la valuation normalisée de L, on appelle *indice de ramification* de l'extension, et on note $e_{L/K}$, l'indice du groupe $v'(K^\star)$ dans $\mathbf{Z}$.

On dit que l'extension L/K est :

— *non ramifiée,* si $e_{L/K} = 1$ et si l'extension résiduelle est séparable;

— *totalement ramifiée,* si le corps résiduel de L est le même que celui de K.

On appelle *corps d'inertie* de l'extension, et on note $L_0$, l'extension maximale non ramifiée de K contenue dans L. Si l'extension L/K est galoisienne, on appelle *groupe d'inertie* de l'extension L/K le groupe de Galois de l'extension $L/L_0$.

Dans toute la suite de cet article, sauf mention explicite du contraire, on désigne par K un corps local et par $p$ la caractéristique de son corps résiduel. On suppose $p \neq 0$. On désigne par L une extension finie galoisienne de K et on suppose *l'extension résiduelle séparable.* L'extension $L_0/K$ est non ramifiée et l'extension $L/L_0$ est alors totalement ramifiée. On désigne par G le groupe de Galois de l'extension L/K et par $G_0$ son groupe d'inertie.

1.3. La $C_p$-suite associée a l'extension L/K. — Soit $v'$ la valuation normalisée de L et soit $\pi$ une uniformisante de L (c'est-à-dire, un élément dont la valuation est égale à 1). On définit l'application $i_G$ de G dans $\mathbf{Z} \cup \{\infty\}$ par

$$i_G(s) = \begin{cases} -1 & \text{si } s \notin G_0, \\ v'((s-1)\pi/\pi) & \text{si } s \in G_0 - \{1\}, \\ +\infty & \text{si } s = 1. \end{cases}$$

On sait (*cf.* CL, lemme 1, p. 69) que $i_G$ ne dépend pas du choix de l'uniformisante $\pi$.

Pour tout $i \in \mathbf{R}$, on note $G_i$ l'ensemble des éléments $s$ de G tels que $i_G(s) \geq i$. On vérifie immédiatement que $G_0$ est bien le groupe d'inertie de l'extension. Les $G_i$ forment une suite décroissante de sous-groupes invariants de G et $G_i$ est réduit à l'élément neutre pour $i$ assez grand (*cf.* CL, prop. 1, p. 70). La famille des $G_i$ munit G d'une filtration dont la fonction d'ordre est $i_G$. Pour tout $i \in \mathbf{R}$, si $i'$ est le plus petit entier $\geqq i$, on a $G_{i'} = G_i$. Si $i$ est entier, le groupe $G_i$ s'appelle le $i^{\text{ième}}$ *groupe de ramification* de l'extension. Les sauts de la filtration (c'est-à-dire les entiers $i$ tels que $G_i \neq G_{i+1}$) s'appellent les *nombres de ramification* de l'extension. Posons $i_0 = 0$ et désignons par $i_1, i_2, \ldots, i_\lambda$ les nombres de ramification strictement positifs de l'extension, rangés par ordre croissant. On appelle *suite des nombres de ramification* de l'extension la suite

$$i_0 < i_1 < \ldots < i_\lambda.$$

*Remarque.* — On désigne parfois (*cf.*, par exemple, CL, chap. IV) par $i_G$ la fonction définie ci-dessus augmentée d'une unité. Mais, de toute façon, c'est la fonction définie ici qu'on prend comme fonction d'ordre de la filtration de G.

Posons, pour $j = 0, 1, \ldots, \lambda$, $\Gamma_j = G_{i_j}$ et $\Gamma_{\lambda+1} = \{1\}$. On obtient une suite

$$G \supset \Gamma_0 \supset \Gamma_1 \supset \ldots \supset \Gamma_\lambda \supset \Gamma_{\lambda+1} = \{1\} \tag{1'}$$

de sous-groupes invariants de G, vérifiant $\Gamma_j \neq \Gamma_{j+1}$ pour $j = 1, 2, \ldots, \lambda$.

Proposition 1.1. — *Supposons* $e_{L/K} \neq 1$. *Alors le groupe* $G_0 = \Gamma_0$ *est de type* $R_p$ *et la suite*

$$\Gamma_0 \supset \Gamma_1 \supset \ldots \supset \Gamma_\lambda \supset \Gamma_{\lambda+1} = \{1\} \tag{1}$$

*est une* $C_p$*-suite associée à* $G_0$. *De plus, si* $n$ *désigne l'ordre de* $\Gamma_0/\Gamma_1$, *le corps résiduel de* $L_0$ *contient les racines* $n^{\text{ièmes}}$ *de l'unité.*

*Démonstration* (*voir* aussi [4]). — Il est clair que l'on peut supposer l'extension totalement ramifiée. On a alors $K = L_0$ et $G = G_0$. Le corps résiduel $k$ de K est aussi celui de L. Soit $\pi$ une uniformisante de L. On sait (*cf.* CL, prop. 6 et 7, p. 74) que :

(i) l'application $s \mapsto s(\pi)/\pi$ définit par passage au quotient un isomorphisme $\theta_0$ (indépendant du choix de $\pi$) de $G_0/G_1$ sur un sous-groupe du groupe multiplicatif $k^*$ de $k$;

(ii) pour tout $i > 0$, l'application $s \mapsto (s-1)\,\pi/\pi^{i+1}$ définit par passage au quotient un isomorphisme $\theta_i$ (dépendant du choix de $\pi$) de $G_i/G_{i+1}$ sur un sous-groupe du groupe additif de $k$.

Comme $\Gamma_0 = G_0$ et $\Gamma_1 = G_1$, $\theta_0$ est un isomorphisme de $\Gamma_0/\Gamma_1$ sur un sous-groupe de $k^*$. On en déduit que $\Gamma_0/\Gamma_1$ est cyclique d'ordre premier à $p$ et que si $n$ désigne son ordre, $k^*$ contient les racines $n^{\text{ièmes}}$ de l'unité.

Pour $j = 1, 2, \ldots, \lambda$, on a $\Gamma_j = G_{i_j}$ et $\Gamma_{j+1} = G_{i_{j+1}} = G_{i_j+1}$. Posons $\rho_j = \theta_{i_j}$. On voit que $\rho_j$ est un isomorphisme de $\Gamma_j/\Gamma_{j+1}$ sur un sous-groupe du groupe additif de $k$. Par conséquent, $\Gamma_j/\Gamma_{j+1}$ est un groupe abélien de type $(p, p, \ldots, p)$. Le groupe $\Gamma_1$ est donc un $p$-sous-groupe invariant de $\Gamma_0$ et $\Gamma_0$ est bien un groupe de type $R_p$ dont le $p$-groupe de Sylow est $\Gamma_1$.

Pour tout $h$ dans $\Gamma_0$ et pour tout $\tau$ dans $G_i/G_{i+1}$, on a (*cf.* CL, prop. 9, p. 77) $\theta_i(h\tau h^{-1}) = \theta_0(h)^i \theta_i(\tau)$, ou encore

$$\rho_j(h\tau h^{-1}) = \theta_0(h)^{i_j}\rho_j(\tau) \qquad \text{pour} \quad \tau \in \Gamma_j/\Gamma_{j+1}. \tag{2}$$

Si $h$ appartient à $\Gamma_1$, on a $\theta_0(h) = 1$ et, par conséquent, $\rho_j(h\tau h^{-1}) = \rho_j(\tau)$. On en déduit que, pour $j \geqq 1$, $\Gamma_j/\Gamma_{j+1}$ est contenu dans le centre de $\Gamma_1/\Gamma_{j+1}$. Il est alors clair que $\Gamma_j/\Gamma_{j+1}$ est un $\mathbf{F}_p[\Gamma_0/\Gamma_1]$-module semi-simple. Si $\tau$ et $\tau'$ sont deux éléments différents de l'unité de $\Gamma_j/\Gamma_{j+1}$, il résulte de la formule (2) que les $\mathbf{F}_p[\Gamma_0/\Gamma_1]$-modules simples qu'ils engendrent sont isomorphes. Tous les sous-$\mathbf{F}_p[\Gamma_0/\Gamma_1]$-modules simples non triviaux de $\Gamma_j/\Gamma_{j+1}$ sont donc isomorphes.

C. Q. F. D.

La suite (1) [resp. (1′)] est appelée la $C_p$-*suite* (resp. $C_p'$-*suite*) *associée à l'extension.*

Nous dirons que l'extension L/K est une *bonne extension* s'il existe un sous-groupe H de G tel que G soit égal au produit semi-direct de H par $\Gamma_1$. On voit qu'alors H est canoniquement isomorphe au groupe $G/\Gamma_1$. On pose $H_0 = H \cap \Gamma_0$; on voit que $\Gamma_0$ est égal au produit semi-direct de $H_0$ par $\Gamma_1$.

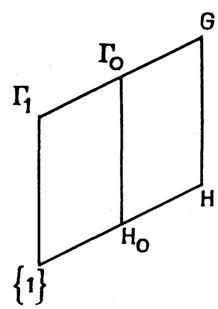


Fig. 2.

On vérifie immédiatement que, si le degré de l'extension résiduelle est premier à $p$, l'extension L/K est une bonne extension.

L'extension L/K est appelée *une* $C_p$-*extension* si elle est totalement ramifiée et si elle a un et un seul nombre de ramification strictement positif. On voit que cela revient à dire que $G = \Gamma_0$ et que la $C_p$-suite associée à l'extension L/K est de la forme

$$G = \Gamma_0 \supset \Gamma_1 \supset \Gamma_2 = \{1\}.$$

En particulier, le groupe G est alors de type $C_p$.

L'extension L/K est appelée *une* $C'_p$*-extension* si c'est une bonne extension et si l'extension $L/L_0$ est une $C_p$-extension. On voit que la deuxième condition revient à dire que la $C'_p$-suite associée à l'extension L/K est de la forme

$$G \supset \Gamma_0 \supset \Gamma_1 \supset \Gamma_2 = \{1\}.$$

Soit L/K une bonne extension. Pour $j = 1, 2, \ldots, \lambda$, désignons par $L_{j+1}$ (resp. $K_j$) le corps fixe du groupe $\Gamma_{j+1}$ (resp. $H.\Gamma_j$). L'extension $L_{j+1}/K_j$ est galoisienne de groupe de Galois $A_j = H.\Gamma_j/\Gamma_{j+1}$. On vérifie (*cf.* CL, cor. à la prop. 3, p. 71 et prop. 2, p. 70) que l'extension $L_{j+1}/K_j$ a un et un seul nombre de ramification strictement positif et qu'il est égal à $i_j$. On en déduit que $L_{j+1}/K_j$ est une $C'_p$-extension. On vérifie immédiatement que le groupe d'inertie de l'extension $L_{j+1}/K_j$ est $A^I_j = H_0.\Gamma_j/\Gamma_{j+1}$ et que $A^I_j$ est le $j^{\text{ième}}$ groupe de type $C_p$ correspondant à la $C_p$-suite (1).

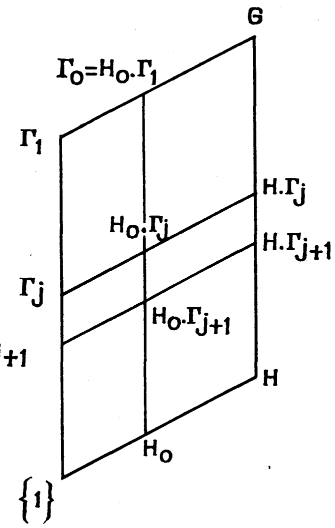


Fig. 3.

La famille des extensions $L_{j+1}/K_j$, pour $j = 1, 2, \ldots, \lambda$, est appelée *un système complet de* $C'_p$*-extensions associées à l'extension* L/K et $L_{j+1}/K_j$ est appelée la $j^{\text{ième}}$ *extension* de ce système.

Un tel système n'est pas, en général, unique puisque les $K_j$ dépendent du choix de H, mais, si $L_{j+1}/K_j$ et $L_{j+1}/K'_j$ désignent le $j^{\text{ième}}$ terme de deux systèmes distincts, il est clair que leurs groupes de Galois sont isomorphes en tant que groupes filtrés.

Une extension totalement ramifiée est évidemment une bonne extension. Un système complet de $C'_p$-extensions associées à l'extension $L/L_0$ s'appelle *un système complet de* $C_p$-*extensions associées à* $L/K$. On peut définir un tel système que l'extension soit bonne ou non.

1.4. Nombres supérieurs de ramification. — Pour $i$ négatif, posons $(G_0 : G_i) = 1/(G_i : G_0)$. Considérons l'application $\varphi_{L/K}$ de $\mathbf{R}$ dans lui-même définie par

$$\varphi_{L/K}(i) = \int_0^i dx/(G_0 : G_x).$$

La fonction $\varphi_{L/K}$ est une fonction continue, linéaire par morceaux et croissante (*cf.* CL, prop. 12, p. 80). Notons $\psi_{L/K}$ l'application réciproque. Pour tout $u \in \mathbf{R}$, on pose $G^u = G_{\psi_{L/K}(u)}$. La famille des $G^u$ munit G d'une filtration appelée la *filtration supérieure* de G. Pour $j = 0, 1, \ldots, \lambda$, posons $u_j = \varphi_{L/K}(i_j)$. Le nombre rationnel $u_j$ s'appelle le $j^{\text{ième}}$ *nombre supérieur de ramification* de l'extension et la suite

$$0 = u_0 < u_1 < \ldots < u_\lambda$$

s'appelle *la suite des nombres supérieurs de ramification de l'extension.* Les $u_j$, pour $j > 0$, sont les sauts $> 0$ de la filtration supérieure de G.

Pour $j = 0, 1, \ldots, \lambda$, posons $e_j = (\Gamma_0 : \Gamma_{j+1})$. Posons $n = e_0$ et, pour tout $j$, $e'_j = e_j/n$. On voit que $n$ est un entier premier à $p$ et que $e'_j = (\Gamma_1 : \Gamma_{j+1})$ est une puissance positive de $p$. Il résulte immédiatement de la définition que l'on a

$$\begin{cases} u_0 = 0; \\ u_1 = i_1/e_0 = i_1/n; \\ u_j = i_1/e_0 + (i_2 - i_1)/e_1 + \ldots + (i_j - i_{j-1})/e_{j-1} \\ \quad = (1/n) \times [i_1 + (i_2 - i_1)/e'_1 + \ldots + (i_j - i_{j-1})/e'_{j-1}]. \end{cases}$$

On en déduit que, pour $j = 1, 2, \ldots, \lambda$,

$$(3) \quad e_j u_j - i_j = (e_j/e_0 - e_j/e_1) i_1 + \ldots + (e_j/e_{j-2} - e_j/e_{j-1}) i_{j-1} + (e_j/e_{j-1} - e_j/e_j)\, i_j.$$

Si l'extension L/K est abélienne, les $u_j$ sont des entiers (théorème de Hasse-Arf, *cf.* CL, p. 84). En général, ce n'est plus le cas, mais il résulte de la définition que les $e_{j-1} u_j$ sont des entiers.

**Proposition 1.2.** — *Soit* $L/K$ *une* $C_p$*-extension. Soit* $G$ *son groupe de Galois et soit* $i$ *son unique nombre de ramification* $> 0$. *Soit* $np^r$ *son degré, avec* $(n, p) = 1$, *et soit* $m = m(G)$ *l'entier défini dans* 1.1. *Alors :*

(i) *on a* $(i, n) = m$;

(ii) *le nombre* $(p^r - 1)\, i/n$ *est entier.*

*Démonstration.* — Soit $H$ un sous-groupe de $G$ isomorphe à $\Gamma_0/\Gamma_1$. Le groupe $H$ est un groupe cyclique d'ordre $n$. Le $p$-groupe de Sylow de $G$ est $\Gamma_1$ et, pour tout $t \in \Gamma_1 - \{1\}$, la formule (2) s'écrit

$$\rho_1(hth^{-1}) = \theta_0^i(h)\,\rho_1(t) \quad \text{pour tout } h \text{ dans } H.$$

Comme $\rho_1$ est un isomorphisme de $\Gamma_1$ sur un sous-groupe du groupe additif du corps résiduel de $K$, on voit qu'un élément $h$ de $H$ est dans le centralisateur de $\Gamma_1$ dans $G$ si et seulement si $\theta_0^i(h) = 1$.

Soit $h_0$ un générateur du groupe $H$. Il est clair que $\theta_0(h_0)$ est une racine primitive $n^{\text{ième}}$ de l'unité. Posons $d' = n/(n, i)$ et $d = d(G) = n/m$. On voit que, pour $h \in H$, $\theta_0^i(h) = 1$ si et seulement si $h$ est une puissance de $h_0^{d'}$. On doit donc avoir $d' = d$ et, par conséquent, $(n, i) = m$, ce qui démontre l'assertion (i).

Si $P_1$ est un sous-$\mathbf{F}_p[H]$-module simple de $\Gamma_1$ et si $p^{r_1}$ désigne le nombre de ses éléments, on sait (*cf.* DAG, n° 6.1.2) que $d$ divise $p^{r_1} - 1$. Le groupe $\Gamma_1$ est d'ordre $p^r$. Comme $\Gamma_1$ est produit direct de $\mathbf{F}_p[H]$-modules simples isomorphes à $P_1$, l'entier $r_1$ divise $r$. Par conséquent, $d$ divise $p^r - 1$. Comme $m$ divise $i$, on voit que $n = md$ divise $(p^r - 1)\, i$, d'où l'assertion (ii). C. Q. F. D.

Revenons au cas d'une extension finie galoisienne quelconque.

**Proposition 1.3.** — *Pour* $j = 1, 2, \ldots, \lambda$, $(e_{j-1} u_j - i_j)/n$ *est entier.*

*Démonstration.* — Posons $q_j = (\Gamma_j : \Gamma_{j+1})$. On a $q_j = e_j/e_{j-1} = e'_j/e'_{j-1}$. On voit que

$$\begin{aligned}(e_{j-1} u_j - i_j)/n &= (1/n) \times [e'_{j-1} i_1 + (e'_{j-1}/e'_1)(i_2 - i_1) + \ldots + (e'_{j-1}/e'_{j-2})(i_{j-1} - i_{j-2}) - i_{j-1}] \\ &= (1/n) \times [(e'_{j-1}/e'_1)(q_1 - 1)\, i_1 + (e'_{j-1}/e'_2)(q_2 - 1)\, i_2 + \ldots + (q_{j-1} - 1)\, i_{j-1}].\end{aligned}$$

Soit $(L_{j+1}/K_j^0)_{j=1,2,\ldots,\lambda}$ un système complet de $C_p$-extensions associées à l'extension $L/K$. Pour tout entier $\mu$ compris entre $1$ et $j - 1$, il résulte de l'assertion (ii) de la proposition 1.2, appliquée à $L_{\mu+1}/K_\mu^0$, que $(q_\mu - 1)\, i_\mu/n$ est un entier naturel. La proposition résulte alors de ce que les $e'_{j-1}/e'_\mu$ sont aussi des entiers naturels. C. Q. F. D.

## 2. Extensions modérément ramifiées.

2.1. Le groupe $H^q(L/K, \mu')$ d'une extension non ramifiée. — Soit $p$ un nombre premier. Soit K un corps quelconque et soit L une extension finie galoisienne de K. Soit G le groupe de Galois de l'extension. On note $\mu'(L)$ le groupe des racines de l'unité, d'ordre premier à $p$, contenues dans L. Il est clair que $\mu'(L)$ est un sous-G-module du groupe multiplicatif de L. Pour tout entier $q$ positif, on écrit $H^q(L/K, \mu')$ au lieu de $H^q(G, \mu'(L))$. On a un homomorphisme naturel de $H^q(L/K, \mu')$ dans $H^q(L/K)$.

Revenons au cas où K est un corps local dont le corps résiduel est de caractéristique $p$. Supposons de plus l'extension L/K non ramifiée. Soit $\tilde{K}$ (resp. $\tilde{L}$) le corps résiduel de K (resp. L). Le groupe de Galois G de l'extension L/K s'identifie au groupe de Galois de l'extension résiduelle $\tilde{L}/\tilde{K}$ et les G-modules $\mu'(L)$ et $\mu'(\tilde{L})$ s'identifient. Les groupes $H^q(L/K, \mu')$ et $H^q(\tilde{L}/\tilde{K}, \mu')$ peuvent donc s'identifier.

Proposition 2.1. — *Supposons l'extension* L/K *non ramifiée. Alors un élément de* $H^q(L/K, \mu')$ *s'annule dans* $H^q(L/K)$ *si et seulement s'il s'annule dans* $H^q(\tilde{L}/\tilde{K})$.

*Démonstration.* — Si $q = 0$, l'assertion est triviale. Supposons $q \geqq 1$. Soit $U_L$ le groupe des unités de L et soit $v$ sa valuation normalisée. On a la suite exacte de G-modules

$$1 \to U_L \to L^* \xrightarrow{v} \mathbf{Z} \to 0.$$

Le choix d'une uniformisante $\pi$ de K permet, comme l'extension est non ramifiée, d'identifier $L^*$ à $U_L \times \mathbf{Z}$ (produit direct de G-modules) et cette suite est décomposée. On peut donc identifier $H^q(L/K)$ au produit direct $H^q(G, U_L) \times H^q(G, \mathbf{Z})$.

Soit $\mathfrak{p}$ l'idéal maximal de l'anneau des entiers de L et soit $U_L^1 = 1 + \mathfrak{p}$. On sait (*cf.* CL, lemme 2, p. 193) que, pour $q \geqq 1$, $H^q(G, U_L^1) = 0$. Comme on a la suite exacte de G-modules

$$1 \to U_L^1 \to U_L \to \tilde{L}^* \to 1,$$

on en déduit que l'application canonique de $H^q(G, U_L)$ sur $H^q(\tilde{L}/\tilde{K})$ est un isomorphisme.

L'assertion résulte alors trivialement de ce que l'image de $H^q(L/K, \mu')$ dans $H^q(L/K)$ est contenue dans $H^q(G, U_L)$.

C. Q. F. D.

*Remarque.* — Si le corps résiduel est fini ou quasi-fini, et si $q \geqq 1$, $H^q(\tilde{L}/\tilde{K})$ est trivial et tout élément de $H^q(L/K, \mu')$ s'annule dans $H^q(L/K)$.

2.2. EXTENSIONS MODÉRÉMENT RAMIFIÉES (ÉTUDE DIRECTE). — On dit qu'une extension finie d'un corps local est *modérément ramifiée* si l'indice de ramification de l'extension est premier à $p$ et si l'extension résiduelle est séparable. Lorsque l'extension est galoisienne, cela revient à dire que son groupe d'inertie est d'ordre premier à $p$.

Soit M une extension finie galoisienne du corps local K et soit J le groupe de Galois de l'extension. Supposons l'extension résiduelle séparable. Soit A un sous-groupe invariant de J et soit L le corps fixe de A. Supposons l'extension M/L totalement et modérément ramifiée. Soit $n$ l'ordre de A. On sait (*cf.* n° 1.3) que $\tilde{L}$, donc aussi L, contient le groupe $\mu_n$ des racines $n^{\text{ièmes}}$ de l'unité et que $\theta_0$ est un isomorphisme de A sur $\mu_n$.

PROPOSITION 2.2. — *Soit* G *le groupe de Galois de l'extension* L/K. *L'application* $\theta_0$ *est un* G-*isomorphisme de* A *sur* $\mu_n$ *et l'image par* $\theta_0$ *de l'élément* $\varepsilon$ *de* $H^2(G, A)$ *correspondant à la suite exacte*

$$1 \to A \to J \to G \to 1$$

*s'annule dans* $H^2(L/K)$.

*Démonstration.* — Par transport de structure, il est clair que l'isomorphisme $\theta_0$ est un G-isomorphisme. Il est immédiat que l'image canonique de $\varepsilon$ dans $H^2(J, A)$ est o. Par conséquent, l'image canonique de $\theta_0(\varepsilon)$ dans $H^2(M/K)$ est o. Comme l'application canonique de $H^2(L/K)$ dans $H^2(M/K)$ est injective (*cf.* CL, prop. 6, p. 164), on en déduit que $\theta_0(\varepsilon)$ s'annule dans $H^2(L/K)$.

C. Q. F. D.

2.3. CONSTRUCTION D'UNE EXTENSION MODÉRÉMENT RAMIFIÉE. — Soit K un corps quelconque. Soit L une extension finie galoisienne de K. Soit G le groupe de Galois de l'extension. Soit A un groupe fini abélien muni d'une structure de G-module et soit J une extension de G par A définie par une suite exacte

$$1 \to A \to J \to G \to 1. \tag{4}$$

Soit M une extension galoisienne de K contenant L. Soit J' (resp. A') le groupe de Galois de l'extension M/K (resp. M/L). Nous disons que l'extension $M/K$ est *associée à la suite* (4) s'il existe un isomorphisme $\varphi$ de $A$ sur $A'$ et un isomorphisme $\Phi$ de $J$ sur $J'$ tels que le diagramme suivant soit commutatif :

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d, "\varphi"] & J \arrow[r] \arrow[d, "\Phi"] & G \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & A' \arrow[r] & J' \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

Revenons au cas où $K$ est un corps local, dont le corps résiduel est de caractéristique $p$.

Proposition 2.3. — *Soit* $L$ *une extension finie galoisienne non ramifiée du corps local* $K$. *Soit* $G$ *le groupe de Galois de l'extension* $L/K$. *Soit* $A$ *un groupe cyclique fini, d'ordre premier à* $p$, *muni d'une structure de* $G$-*module et soit*

$$1 \to A \to J \to G \to 1 \tag{4}$$

*une suite exacte de groupes. Pour qu'il existe une extension galoisienne* $M$ *de* $K$, *contenant* $L$, *associée à la suite* (4), *telle que l'extension* $M/L$ *soit totalement et modérément ramifiée, il faut et il suffit qu'il existe un* $G$-*plongement* $\chi$ *de* $A$ *dans* $L^*$ *tel que l'image par* $\chi$ *de l'élément de* $H^2(G, A)$ *correspondant à la suite* (4) *soit* $0$ *dans* $H^2(L/K)$.

*Dans ces conditions, on peut choisir* $M$ *pour que l'homomorphisme* $\theta_0$ *attaché à l'extension coïncide avec* $\chi$.

*Démonstration.* — Les conditions sont nécessaires d'après la proposition 2.2. Montrons qu'elles sont suffisantes.

Soit $n$ l'ordre de $A$. L'existence de $\chi$ entraîne que $L^*$ contient le groupe $\mu_n$ des racines $n^{\text{ièmes}}$ de l'unité et $\chi$ est un $G$-isomorphisme de $A$ sur $\mu_n$.

Soit $S$ une section de $G$ dans $J$. Soit $\varepsilon$ le cocycle de $G$ à valeurs dans $A$ correspondant à $S$. Si $\chi(\varepsilon)$ s'annule dans $H^2(L/K)$, il existe une application $\lambda$ de $G$ dans $L^*$ telle que, pour tout couple $g$, $g'$ d'éléments de $G$, on ait $\chi(\varepsilon_{g,g'}) = g(\lambda_{g'})\lambda_g\lambda_{gg'}^{-1}$. On a donc $g(\lambda_{g'}^n)\lambda_g^n\lambda_{gg'}^{-n} = \chi(\varepsilon_{gg'}^n) = 1$ et l'application de $G$ dans $L^*$ définie par $g \mapsto \lambda_g^n$ est un cocycle. Comme le groupe $H^1(L/K)$ est réduit à l'élément neutre (« théorème 90 » de Hilbert), on en déduit qu'il existe un élément $\pi_0$ de $L^*$ tel que, pour tout $g$ dans $G$, on ait $g(\pi_0) = \lambda_g^n . \pi_0$. Pour tout $a$ dans $K^*$, l'élément $a\pi_0$ a la même propriété. Comme l'extension $L/K$ est non ramifiée, on peut choisir pour $\pi_0$ une uniformisante de $L$.

Soit $\pi$ un élément d'une clôture algébrique de $L$ vérifiant $\pi^n = \pi_0$ et soit $M = L(\pi)$. Comme $\pi_0$ est une uniformisante de $L$, $M$ est une extension totalement ramifiée de $L$ de degré $n$ et $\pi$ est une uniformisante de $M$, Pour tout $g$ dans G, notons $S_g$ l'élément de J correspondant à la section S. Tout élément de J s'écrit de manière unique sous la forme $hS_g$, avec $h \in A$ et $g \in G$. On vérifie immédiatement qu'il existe un unique automorphisme $\Phi_{hS_g}$ de M prolongeant $g$ et appliquant $\pi$ sur $\chi(h)\lambda_g\pi$. On voit tout de suite que $\Phi$ est un isomorphisme de G sur un sous-groupe du groupe des K-automorphismes de M. Comme l'ordre de G est égal au degré de l'extension M/K, on voit que l'extension M/K est galoisienne. Il est immédiat qu'elle est associée à la suite (4) et que l'homomorphisme $\theta_0$ attaché à l'extension coïncide avec $\chi$.

C. Q. F. D.

## 3. Sur les automorphismes sauvagement ramifiés.

3.1. Définitions. Premières propriétés (*cf.* [6]). — Soit L un corps local. Soit A l'anneau des entiers de L et soit $\mathfrak{p}$ l'idéal maximal de l'anneau des entiers de A. Soit $k = A/\mathfrak{p}$ le corps résiduel de L et soit $p$ la caractéristique de $k$. On suppose $p \neq 0$. Soit C un *système de représentants*, contenant o, de $k$ dans L. On pose $C^\star = C - \{0\}$.

Soit $v$ la valuation normalisée de L. On dit qu'un automorphisme $s$ de L est *sauvagement ramifié* (sous-entendu, relativement à C) si $s$ agit trivialement sur C et si, pour tout $a$ dans $L^\star$, on a $v((s-1)\,a) > v(a)$. Il est clair que l'ensemble $S^L$ des automorphismes sauvagement ramifiés de L forme un groupe.

Soit $\pi$ une uniformisante de L. Pour tout $s$ dans $S^L - \{1\}$, on pose $i_L(s) = v((s-1)\,\pi) - 1$. Il est clair que $i_L(s)$ est un entier $> 0$ qui ne dépend pas du choix de $\pi$. On pose $i_L(1) = +\infty$.

Pour tout entier positif $i$, on note $S_i^L$ l'ensemble des éléments $s$ de $S^L$ qui vérifient $i_L(s) \geqq i$. L'ensemble $S_i^L$ est un sous-groupe invariant de $S^L$ et la famille des $S_i^L$ munit $S^L$ d'une filtration dont la fonction d'ordre est $i_L$. De plus, on a $S^L = S_1^L$.

Pour tout $s$ dans $S_i^L$, on note $\theta_i(s)$ l'image canonique dans $k$ de $(s-1)\pi/\pi^{i+1}$. L'élément $\theta_i(s)$ dépend du choix de l'uniformisante $\pi$, et, pour $\pi$ fixé, $\theta_i$ définit, par passage au quotient, un isomorphisme de $S_i^L/S_{i+1}^L$ sur un sous-groupe du groupe additif de $k$.

Pour tout entier naturel $j$, désignons par $O(j)$ le plus grand entier $n$ tel que $p^n$ divise $j$. Pour tout $s$ dans $S^L$, l'entier $i_L(s^j)$ ne dépend que de $O(j)$ et, si on pose $i_L(s^{p^r}) = i_r$ pour $r \geqq 0$, on a $i_{r+1} > i_r$, sauf si $s^{p^r} = 1$. En particulier, tout élément d'ordre fini de $S^L$ est d'ordre une puissance de $p$, et, si $k$ est fini, le groupe $S^L$ est un pro-$p$-groupe (limite projective des $S^L/S_i^L$).

Tout élément $a$ de L s'écrit sous la forme $a = \sum_{\gg -\infty}^{+\infty} c_j \pi^j$, avec $c_j \in C$. Tout automorphisme $s$ de $S^L$ est donc complètement déterminé par la donnée de l'élément $b_s$ de $\mathfrak{p}$ défini par $b_s = (s-1)\pi/\pi$.

Pour tout entier $n$ premier à $p$ et pour tout élément $b$ de $U_L^1 = 1 + \mathfrak{p}$, il existe un et un seul élément $b'$ de $U_L^1$ tel que $b'^n = b$. On pose $b' = b^{1/n}$.

Soit $a$ un élément de L tel que $v(a) = n \not\equiv 0 \pmod{p}$. Posons $b = s(a)/a$. L'élément $b$ appartient à $U_L^1$. Il est clair qu'il existe une uniformisante $\pi'$ de L et un élément $c$ de $C^*$ tels que $a = c\pi'^n$. On a donc $s(\pi'^n)/\pi'^n = b$ et, par conséquent, $s(\pi') = \pi' b^{1/n}$. Tout élément $s$ de $S^L$ est donc entièrement déterminé par la donnée de $s(a)/a$.

Soit G un sous-groupe fini de $S^L$ et soit K le corps fixe de G. L'extension L/K est galoisienne de groupe de Galois G. Comme les éléments de $S^L$ laissent fixes les éléments de C, C est contenu dans K et K a le même corps résiduel $k$ que L. L'extension L/K est donc totalement ramifiée. Il est immédiat que, pour tout $s$ dans G, $i_G(s) = i_L(s)$ et que la restriction de $\theta_i$ à $G_i$ n'est autre que l'application $\theta_i$ définie au nº 1.3.

Réciproquement, si L est une $p$-extension finie galoisienne totalement ramifiée d'un corps local K et si on prend pour système de représentants C un système contenu dans K, on voit que le groupe de Galois de l'extension s'identifie à un sous-groupe de $S^L$.

Soit $e$ l'indice de ramification absolu de L. Si la caractéristique de L est égale à $p$, on pose $e = +\infty$. Si $e$ est fini, le groupe $S^L$ est fini. Comme tout élément $u$ d'ordre $p$ vérifie $i_L(u) \leq e/(p-1)$ (*cf.*, par exemple, infra, cor. à la prop. 4.2), on a $S_n^L = \{1\}$, pour tout entier $n$ strictement supérieur à $e/(p-1)$. Si $e = +\infty$, il n'en est plus de même. On vérifie immédiatement que, pour tout $a$ dans L, vérifiant $v(a) \not\equiv 0 \pmod{p}$, et pour tout $b$ dans $U_L^1$, il existe un et un seul élément $s$ de $S^L$ tel que $s(a)/a = b$.

Proposition 3.1. — *Soit $i$ un entier $\geq 1$. Soit $s$ un élément de $S_i^L$ et soit $c$ le relèvement de $\theta_i(s)$ dans C. Soit $n$ un entier quelconque et soit $a$ un élément de $\mathfrak{p}^n$.*

(i) *On a*

$$(s-1)\,a \equiv nca\pi^i \pmod{\mathfrak{p}^{n+i+1}}.$$

*En particulier, on a $v((s-1)\,a) \geq n+i$, avec égalité si et seulement si*

$$v(a) = n, \qquad i_L(s) = i \quad \text{et} \quad n \not\equiv 0 \pmod{p}.$$

(ii) *Pour tout entier $j > 0$, on a*

$$(s-1)^j a \equiv n(n+i)\ldots(n+(j-1)\,i)\,c^j a\pi^{ji} \pmod{\mathfrak{p}^{n+ji+1}}.$$

*En particulier, on a* $v((s-1)^j a) \geq n + ji$, *avec égalité si et seulement si* $v(a) = n$, $i_L(s) = i$ *et les entiers* $n$, $n+i$, $\ldots$, $n+(j-1)i$ *sont premiers à* $p$.

*Démonstration.* — La deuxième assertion se déduit immédiatement de la première par récurrence sur $j$.

On a $s(\pi) \equiv \pi(1 + c\pi^i) \pmod{\mathfrak{p}^{i+1}}$ et, par conséquent, pour tout $l$,

$$s(\pi^l) \equiv \pi^l(1 + lc\pi^i) \qquad \pmod{\mathfrak{p}^{l+i+1}}.$$

Si $a = \sum_{l=n}^{+\infty} c_l \pi^l$, avec $c_l \in C$, on en déduit que $(s-1)\,a \equiv ncc_n \pi^{n+i} \pmod{\mathfrak{p}^{n+i+1}}$ ou encore que $(s-1)\,a \equiv nca\pi^i \pmod{\mathfrak{p}^{n+i+1}}$. On a donc $v((s-1)\,a) \geq n+i$, avec égalité si et seulement si $v(a) = n$ et $nc \not\equiv 0 \pmod{\mathfrak{p}}$. La deuxième condition revient à dire que $n$ est premier à $p$ et que $c \in C^*$, ou encore que $i_L(s) = i$.

C. Q. F. D.

Corollaire. — *Si* $e = +\infty$, *pour tout* $s$ *dans* $S^L$, *on a* $i(s^p) \geq p\, i(s)$, *avec égalité si et seulement si* $i(s) \equiv 0 \pmod{p}$.

En effet, comme $s^p - 1 \equiv (s-1)^p \pmod{p}$, on a $(s^p - 1)\pi = (s-1)^p \pi$. Posons $i(s) = i$. On a

$$i(s^p) + 1 = v((s-1)^p \pi) \qquad \text{et} \qquad v((s-1)^p\pi) \geq 1 + pi,$$

avec égalité si et seulement si les entiers $1$, $1+i$, $\ldots$, $1+(p-1)i$ sont tous premiers à $p$, ce qui se produit si et seulement si $p$ divise $i$.

Nous disons qu'un élément $s$ de $S^L$ est *régulier* si $i(s)$ est premier à $p$.

3.2. Automorphismes d'ordre $p$. — Soit $u$ un élément d'ordre $p$ de $S^L$ et soit K le corps fixe de $u$. L'extension L/K est une extension cyclique de degré $p$, totalement ramifiée. En particulier, on voit que tout élément $a$ de L peut se mettre sous la forme

$$a = b + \beta, \qquad \text{avec} \qquad b \in K \qquad \text{et} \qquad v(\beta) \not\equiv 0 \qquad \pmod{p}.$$

Si $e = +\infty$, il résulte du corollaire à la proposition 3.1 que $u$ est régulier. Si $e$ est fini, on sait (*cf.*, par exemple, infra, cor. à la prop. 4.2) que, si $u$ n'est pas régulier, alors $i_L(u) = e/(p-1)$.

Proposition 3.2. — *Soit* $u$ *un élément régulier, différent de* 1, *de* $S^L$. *Posons* $i = i_L(u)$. *Pour que* $u$ *soit d'ordre* $p$, *il faut et il suffit qu'il existe un élément* $a$ *de* L *qui vérifie* $v(a) = -i$ *et* $(u-1)\,a \equiv 1 \pmod{\mathfrak{p}^{e-(p-1)i}}$. *S'il en est ainsi,* $\theta_i(u)$ *est égal à l'image canonique de* $-1/ia\pi^i$ *dans* $k$.

*Démonstration.* — La condition est nécessaire : Soit K le corps fixe de $u$ et soit $b$ un élément de L vérifiant $v(b) = -(p-1)\,i$. D'après la proposition 3.1, on a $v((u-1)^{p-1}b) = 0$. Comme

$$(u-1)^{p-1} \equiv 1 + u + \ldots + u^{p-1} \qquad (\operatorname{mod} p),$$

on a

$$\operatorname{Tr}_{L/K}(b) \equiv (u-1)^{p-1}b \quad (\operatorname{mod} \mathfrak{p}^{e-(p-1)i}) \qquad \text{et} \qquad v(\operatorname{Tr}_{L/K}(b)) = 0.$$

Posons $b' = b/\operatorname{Tr}_{L/K}(b)$. On a

$$v(b') = -(p-1)\,i \qquad \text{et} \qquad \operatorname{Tr}_{L/K}(b') = 1.$$

Posons $a = (u-1)^{p-2}b'$. D'après la proposition 3.1, on a $v(a) = -i$. Enfin, on a

$$(u-1)\,a = (u-1)^{p-1}b' \equiv \operatorname{Tr}_{L/K}(b') \qquad (\operatorname{mod} \mathfrak{p}^{e-(p-1)i});$$

donc, $(u-1)\,a \equiv 1 \ (\operatorname{mod} \mathfrak{p}^{e-(p-1)i})$.

La condition est suffisante car, si

$$(u-1)\,a \equiv 1 \qquad (\operatorname{mod} \mathfrak{p}^{e-(p-1)i}),$$

on a, d'après la proposition 3.1, $(u-1)^p a \equiv 0 \ (\operatorname{mod} \mathfrak{p}^e)$. Comme $u^p - 1 \equiv (u-1)^p \ (\operatorname{mod} p)$ on a

$$(u^p-1)\,a \equiv (u-1)^p a \qquad (\operatorname{mod} \mathfrak{p}^{e-i}).$$

On a donc $(u^p-1)\,a \equiv 0 \ (\operatorname{mod} \mathfrak{p}^{e-i})$ et, par conséquent, $i_L(u^p) \geqq e \geqq e/(p-1)$, ce qui entraîne $u^p = 1$.

Enfin, soit $c$ le relèvement de $\theta_i(u)$ dans C. Si $a$ est un élément de L tel que $v(a) = -i$, il résulte de la proposition 3.1 que $(u-1)\,a \equiv -ica\pi^i$ $(\operatorname{mod} \mathfrak{p})$. Si $(u-1)\,a \equiv 1 \ (\operatorname{mod} \mathfrak{p}^{e-(p-1)i})$, on en déduit que $\theta_i(u)$ est égal à l'image canonique de $-1/ia\pi^i$ dans $k$.

C. Q. F. D.

*Remarque.* — On pourrait aussi déduire ce résultat du fait bien connu (*cf.* [3]) que L est le corps de rupture d'un polynôme d'Artin-Schreier à coefficients dans K.

3.3. Le groupe $S^{L/K}$. — Dans toute la suite de ce paragraphe, on désigne par $u$ un élément *régulier d'ordre p* de $S^L$, par K le corps fixe de $u$ et on pose $i = i_L(u)$. On note $v_K$ la valuation normalisée de K.

Il est clair que l'ensemble $S^{L/K}$ des éléments de $S^L$ qui commutent avec $u$ forme un sous-groupe de $S^L$. Si $s$ est un élément de $S^{L/K}$, on vérifie immédiatement que sa restriction $\bar{s}$ à K est un élément du groupe $S^K$

des automorphismes de K qui laissent fixe chaque élément de C. L'application $s \mapsto \bar{s}$ est un homomorphisme de $S^{L/K}$ dans $S^K$ dont le noyau est le groupe cyclique engendré par $u$.

La norme de L à K de $\pi$ est une uniformisante $\pi_K$ de K et il est immédiat que $\pi_K \equiv \pi^p (\bmod\, \mathfrak{p}^{p+1})$. On note $\theta_j^K$ l'application qui, à $\sigma$ dans $S_j^K$, fait correspondre l'image canonique dans $k$ de $(\sigma - 1)\pi_K/\pi_K^{j+1}$.

Pour tout entier naturel $j$, posons

$$N_j(x) = \begin{cases} x^p & \text{si } j < i, \\ x^p - (\theta_i(u))^{p-1}x & \text{si } j = i, \\ -(\theta_i(u))^{p-1}x & \text{si } j > i. \end{cases} \tag{5}$$

Enfin, rappelons que la fonction $\varphi_{L/K}$ définie au n° 1.4 prend les valeurs

$$\varphi_{L/K}(j) = \begin{cases} j & \text{si } j \leqq i \\ i + (j-i)/p & \text{si } j \geqq i. \end{cases}$$

PROPOSITION 3.3. — *Soit $a$ un élément de L vérifiant*

$$v(a) = -i \quad \text{et} \quad (u-1)a \equiv 1 \quad (\bmod\, \mathfrak{p}^{e-(p-1)i}).$$

*Soit $s$ un élément de $S^L$. Posons $i' = i_L(s)$. Pour que $s$ et $u$ commutent, il faut (et, si $e = +\infty$, il suffit) qu'il existe un élément $b$ de K tel que $(s-1)a \equiv b\, (\bmod\, \mathfrak{p}^{e-pi+i'})$. S'il en est ainsi, les conditions suivantes sont réalisées :*

(i) *On a $i' \equiv i\, (\bmod\, p)$, $v_K(b) = -(i-i')/p$ et l'image canonique de $b\pi_K^{(i'-i)/p}$ dans $k$ est $\theta_{i'}(s)/\theta_i(u)$.*

(ii) *On a*

$$i_K(\bar{s}) \geqq \varphi_{L/K}(i') \tag{6}$$

*et $\theta^K_{\varphi_{L/K}(i')}(\bar{s}) = N_{i'}(\theta_{i'}(s))$. En particulier, si $i \neq i'$, on a l'égalité dans* (6); *et, si $i = i'$, l'inégalité* (6) *est stricte si et seulement s'il existe un entier $n$ tel que $\theta_i(s) = \theta_i(u^n)$.*

*Démonstration.* — D'après la proposition 3.2, $a$ existe. On a

$$us(a) - su(a) = (u-1)(s-1)a - (s-1)(u-1)a.$$

Il résulte de la proposition 3.1 que

$$(s-1)(u-1)a \equiv 0 \quad (\bmod\, \mathfrak{p}^{e-(p-1)i+i'}).$$

Si on pose $(s-1)\,a = b + \beta$, avec $b \in K$ et $v(\beta) \not\equiv 0 \pmod p$, on a

$$(u-1)(s-1)\,a = (u-1)\,\beta \qquad \text{et} \qquad v((u-1)(s-1)\,a) = v(\beta) + i.$$

Si $s$ et $u$ commutent, on a donc

$$v(\beta) + i \geqq e - (p-1)\,i + i', \qquad \text{d'où} \qquad v(\beta) \geqq e - pi + i',$$

et la condition est nécessaire. Si $e = +\infty$, on a $(s-1)(u-1)\,a = 0$. Si $(s-1)\,a \in K$, on a $(u-1)(s-1)a = 0$, donc $us(a) = su(a)$. Ceci entraîne que $us = su$ et la condition est suffisante.

Supposons que $s$ et $u$ commutent. Soit $b \in K$ tel que $(s-1)\,a \equiv b \pmod{\mathfrak{p}^{e-pi+i'}}$. On a

$$v((s-1)\,a) = -i + i' < e - pi + i', \qquad \text{puisque} \quad e - (p-1)\,i > 0.$$

On en déduit que $v(b) = -i + i'$. Comme l'extension L/K est totalement ramifiée, on a donc $i \equiv i' \pmod p$ et $v_K(b) = -(i-i')/p$. Soit $c$ (resp. $d$) le relèvement de $\theta_i(u)$ [resp. $\theta_{i'}(s)$] dans C. D'après la proposition 3.1, on a

$$(s-1)\,a \equiv -ida\pi^{i'} \qquad (\mathrm{mod}\,\mathfrak{p}^{-i+i'+1}).$$

Il résulte de la proposition 3.2 que $-1/ia\pi^i \equiv c \pmod{\mathfrak{p}}$. Comme $\pi_K \equiv \pi^p \pmod{\mathfrak{p}^{p+1}}$ et comme $(s-1)\,a \equiv b \pmod{\mathfrak{p}^{-i+i'+1}}$, on en déduit que $b \equiv d/c\pi_K^{(i-i')/p} \pmod{\mathfrak{p}^{-i+i'+1}}$, ou encore que l'image canonique de $b\pi_K^{(i'-i)/p}$ dans $k$ est $\theta_{i'}(s)/\theta_i(u)$.

Posons $a^p - a = a' + \alpha$ avec $a' \in K$ et $v(\alpha) \not\equiv 0 \pmod p$. On a

$$v((u-1)(a^p - a)) = v(\alpha) + i.$$

Or $u(a) \equiv a + 1 \pmod{\mathfrak{p}^{e-(p-1)i}}$ et, par conséquent,

$$u(a^p) \equiv a^p + 1 \qquad (\mathrm{mod}\,\mathfrak{p}^{e-(p-1)i}).$$

Donc $(u-1)(a^p - a) \equiv 0 \pmod{\mathfrak{p}^{e-(p-1)i}}$. On en déduit que $v(\alpha) \geqq e - pi$, autrement dit, $a' \equiv a^p - a \pmod{\mathfrak{p}^{e-pi}}$.

Posons $s(a) = a + b + \lambda$. On a $v(\lambda) \geqq e - pi + i'$. Si on pose $s(a^p) = a^p + b^p + \lambda'$, on voit que $\lambda'$ est de la forme $\lambda' = \lambda^p + p\,\mu(a, b, \lambda)$, où $\mu(x, y, z)$ est un polynôme homogène de degré $p$ à coefficients dans $\mathbf{Z}$, de degré $p-1$ relativement à chaque variable. Comme $v(a) < v(b) < v(\lambda)$, on en déduit que

$$v(\mu(a, b, \lambda)) \geqq (p-1)\,v(a) + v(b) = -pi + i'.$$

Posons $r = \min\{e - pi + i',\ p(e - pi + i')\}$. On a

$$v(\lambda^p) \geqq p(e - pi + i') \geqq r,$$

et

$$v(p\,\mu(a, b, \lambda)) = e + v(\mu(a, b, \lambda)) \geqq e - pi + i' \geqq r.$$

On a donc $s(a^p) \equiv a^p + b^p \pmod{\mathfrak{p}^r}$. Or la congruence $a' \equiv a^p - a \pmod{\mathfrak{p}^{e-pi}}$ implique

$$(s - 1)\,a' \equiv (s - 1)\,a^p - (s - 1)\,a \qquad (\operatorname{mod} \mathfrak{p}^{e-pi+i'}).$$

Cette dernière congruence est vraie, *a fortiori*, modulo $\mathfrak{p}^r$, et on en déduit que

$$(s - 1)\,a' \equiv b^p - b \qquad (\operatorname{mod} \mathfrak{p}^r).$$

Soit $n$ un entier $\leqq i_K(\bar{s})$. Soit $d'$ le relèvement de $\theta_n^K(\bar{s})$ dans C. Comme

$$a' \equiv a^p - a \qquad (\operatorname{mod} \mathfrak{p}^{e-pi}),$$

on a $v_K(a') = -\,i$. D'après la proposition 3.1, on a donc

$$v_K((\bar{s} - 1)\,a') = i_K(\bar{s}) - i \qquad \text{et} \qquad (\bar{s} - 1)\,a' \equiv -\,id'\,a'\,\pi_K^n \qquad (\operatorname{mod} \mathfrak{p}_K^{-i+n+1}),$$

en désignant par $\mathfrak{p}_K$ l'idéal maximal de l'anneau des entiers de K. On a

$$-\,1/ia\pi^i \equiv c \quad (\operatorname{mod} \mathfrak{p}), \qquad a' \equiv a^p \quad (\operatorname{mod} \mathfrak{p}^{-pi+1}) \qquad \text{et} \qquad \pi_K \equiv \pi^p \quad (\operatorname{mod} \mathfrak{p}^{p+1}).$$

On en déduit que

$$(\bar{s} - 1)\,a' \equiv -\,id'(-\,1/ic^p\,\pi^{pi})\,\pi^{np} \qquad (\operatorname{mod} \mathfrak{p}^{p(n-i)+1})$$

ou que

(7) $$(\bar{s} - 1)\,a' \equiv d'/c^p\,\pi^{p(i-n)} \qquad (\operatorname{mod} \mathfrak{p}^{p(n-i)+1}).$$

Si $i' < i$, $v_K(b^p - b) = -\,i + i'$. On a $p(-\,i + i') < e - pi + i'$ puisque $(p - 1)i' < e$ et $p(-\,i + i') < p(e - pi + i')$ puisque $(p^2 - p)\,i < pe$. On a donc $v(b^p - b) < r$ et

$$i_K(\bar{s}) - i = v_K((\bar{s} - 1)\,a') = v_K(b^p - b) = -\,i + i'.$$

D'où $i_K(\bar{s}) = i' = \varphi_{L/K}(i')$.

De plus, comme $b \equiv d/c\pi^{-i'+i} \pmod{\mathfrak{p}^{-i+i'+1}}$, on a

$$(\bar{s} - 1)\,a' \equiv d^p/c^p\,\pi^{p(i-i')} \qquad (\operatorname{mod} \mathfrak{p}^{p(i'-i)+1}).$$

En appliquant la formule (7) pour $n = i'$, on voit que

$$d'/c^p\,\pi^{p(i-i')} \equiv d^p/c^p\,\pi^{p(i-i')} \qquad (\operatorname{mod} \mathfrak{p}^{p(i'-i)+1}),$$

ou encore que $d' \equiv d^p \pmod{\mathfrak{p}}$. On a donc $\theta_{i'}^{K}(\bar{s}) = (\theta_{i'}(s))^p = N_{i'}(\theta_{i'}(s))$.

Si $i' > i$, $v_K(b^p - b) = -(i-i')/p$. On a

$$-i+i' < e - pi + i' < p(e - pi + i'), \qquad \text{car} \quad e - pi + i' = e - (p-1)i + (i'-i) > 0.$$

On a donc $v(b^p - b) < r$ et

$$i_K(\bar{s}) - i = v_K((\bar{s}-1)a') = v_K(b^p - b) = -(i-i')/p.$$

D'où $i_K(\bar{s}) = i + (i'-i)/p = \varphi_{L/K}(i')$.

De plus, on a $(\bar{s}-1)a' \equiv -d/c\pi^{i-i'} \pmod{\mathfrak{p}^{i'-i+1}}$ et, si on pose $n = \varphi_{L/K}(i')$, la formule (7) montre que

$$-d/c\pi^{i-i'} \equiv d'/c^p \pi^{p(i-n)} \qquad (\operatorname{mod} \mathfrak{p}^{p(n-i)+1})$$

ou que $-d/c \equiv d'/c^p \pmod{\mathfrak{p}}$ ou encore que $d' \equiv -c^{p-1}d \pmod{\mathfrak{p}}$. On a donc

$$\theta_n^K(\bar{s}) = -(\theta_i(u))^{p-1}\theta_{i'}(s) = N_{i'}(\theta_{i'}(s)).$$

Si $i' = i$, $v_K(b^p - b) \geqq 0$. On a $r > 0$ et on en déduit $i_K(\bar{s}) \geqq i = \varphi_{L/K}(i')$.

De plus, on a $b^p - b \equiv (d/c)^p - d/c \pmod{\mathfrak{p}}$. En appliquant la formule (7) pour $n = i$, on voit que $(d/c)^p - d/c \equiv d'/c^p \pmod{\mathfrak{p}}$ ou encore $d' \equiv d^p - c^{p-1}d \pmod{\mathfrak{p}}$. On a donc

$$\theta_i^K(\bar{s}) = (\theta_i(s))^p - (\theta_i(u))^{p-1}\theta_i(s) = N_i(\theta_i(s)).$$

De plus, on voit que $i_K(\bar{s}) = i$, sauf si et seulement si $\theta_i(\bar{s}) = 0$, c'est-à-dire s'il existe un entier $n$ tel que $\theta_i(s) = n\theta_i(u) = \theta_i(u^n)$.

C. Q. F. D.

Proposition 3.4. — *Soit $s$ un élément de $S^L$ qui commute avec $u$. Posons*

$$i_0 = i_L(s), \qquad i_1 = i_L(s^p) \qquad \text{et} \qquad i'_0 = i_K(\bar{s}).$$

*Supposons les entiers $i_0$, $i_1$ et $i'_0$ finis et premiers à $p$. Alors on a*

$$i_1 \geqq \min\{p(p-1)i'_0 + i_0,\ e,\ e - (p-1)i + pi_0\}.$$

*Si $p(p-1)i'_0 + i_0 < \min\{e,\ e - (p-1)i + pi_0\}$, on a*

$$i_1 \geqq p(p-1)i'_0 + i_0,$$

*avec l'égalité si et seulement si $i'_0 + (i - i_0)/p \equiv 0 \pmod{p}$. Dans ce cas, on a*

$$\theta_{i_1}(s^p) = -\theta_{i_0}(s)(\theta_{i'_0}^K(\bar{s}))^{p-1}.$$

*Démonstration.* — Soit $a$ un élément de L tel que $v(a) = -i$ et $(u-1)a \equiv 1 \pmod{\mathfrak{p}^{e-(p-1)i}}$. D'après la proposition 3.3, il existe un élément $b$ de K et un élément $\beta$ de L, vérifiant $v(\beta) \geqq e - pi + i_0$, tels que $(s-1)a = b + \beta$.

Comme $s^p - 1 \equiv (s-1)^p \pmod{p}$, on a

$$(s^p - 1)\, a \equiv (s-1)^p a \qquad \pmod{\mathfrak{p}^{e-i}}.$$

Or $(s-1)^p a = (\bar{s}-1)^{p-1} b + (s-1)^{p-1}\beta$. D'après la proposition 3.1, on a $v((s-1)^{p-1}\beta) \geqq e - pi + pi_0$. On a donc

$$(s^p - 1)\, a \equiv (\bar{s}-1)^{p-1} b \qquad \pmod{\mathfrak{p}^{\min\{e-i,\, e-pi+pi_0\}}}.$$

D'après la proposition 3.1, comme $v_{\mathrm{K}}(b) = -(i - i_0)/p$, on a

$$v_{\mathrm{K}}((\bar{s}-1)^{p-1} b) \geqq -(i-i_0)/p + (p-1)\, i'_0,$$

avec l'égalité si et seulement si $-(i-i_0)/p \equiv i'_0 \pmod{p}$. On a donc

$$v((\bar{s}-1)^{p-1} b) \geqq -i + i_0 + p(p-1)\, i'_0$$

avec l'égalité si et seulement si $i'_0 + (i - i_0)/p \equiv 0 \pmod{p}$. Comme $v((s^p - 1)\, a) = -i + i_1$, on voit que

$$i_1 \geqq \min\{p(p-1)\, i'_0 + i_0,\ e\ ,\ e - (p-1)\, i + pi_0\}$$

et que, si $p(p-1)\, i'_0 + i_0 < \min\{e, e - (p-1)\, i + pi_0\}$, on a

$$i_1 \geqq p(p-1)\, i'_0 + i_0$$

avec l'égalité si et seulement si $i'_0 + (i-i_0)/p \equiv 0 \pmod{p}$.

Supposons que nous soyons dans ce dernier cas et désignons par $c$, $d$, $d'$ et $d_1$ les relèvements respectifs dans C de $\theta_i(u)$, $\theta_{i_0}(s)$, $\theta^{\mathrm{K}}_{i'_0}(\bar{s})$ et $\theta_{i_1}(s^p)$. D'après la proposition 3.1, on a

$$(s^p - 1)\, a \equiv (\bar{s}-1)^{p-1} b \equiv i'_0 (2 i'_0) \ldots (p-1)\, i'_0\, d'^{p-1} b\, \pi_{\mathrm{K}}^{(p-1)i'_0} \equiv -\, d'^{p-1} b\, \pi_{\mathrm{K}}^{(p-1)i'_0}$$
$$\pmod{\mathfrak{p}^{p(-(i-i_0)/p + (p-1)i'_0)+1}}.$$

D'après la proposition 3.3, $b\,\pi_{\mathrm{K}}^{(i_0-i)/p} \equiv d/c \pmod{\mathfrak{p}}$. Comme $\pi_{\mathrm{K}} \equiv \pi^p \pmod{\mathfrak{p}^{p+1}}$, on en déduit que

$$(s^p - 1)\, a \equiv -\,(d'^{p-1} d/c)\, \pi^{-i+i_0+p(p-1)i'_0} \qquad \pmod{\mathfrak{p}^{-i+i_0+p(p-1)i'_0+1}}.$$

D'après la proposition 3.1, $(s^p - 1)\, a \equiv -\, i d_1 a \pi^{i_1} \pmod{\mathfrak{p}^{i_1-i+1}}$. Comme, d'après la proposition 3.2, $c \equiv -1/ia\pi^i \pmod{\mathfrak{p}}$, on en déduit que

$$(s^p - 1)\, a \equiv (d_1/c)\, \pi^{i_1-i} \qquad \pmod{\mathfrak{p}^{i_1-i+1}}.$$

Finalement, on voit que $-dd'^{p-1}/c \equiv d_1/c \pmod{\mathfrak{p}}$, ou que $d_1 \equiv -dd'^{p-1} \pmod{\mathfrak{p}}$, c'est-à-dire que

$$\theta_{i_1}(s^p) = -\theta_{i_0}(s)\,(\theta^{\mathrm{K}}_{i'_0}(\bar{s}))^{p-1}.$$

C. Q. F. D.

Corollaire. — *Soit $s$ un élément de $\mathrm{S}^{\mathrm{L}}$ d'ordre $p^2$. Posons*

$$i_{\mathrm{L}}(s) = i_0, \qquad i_{\mathrm{L}}(s^p) = i_1 \qquad \textit{et} \qquad u_1 = i_0 + (i_1 - i_0)/p.$$

*Supposons que $i_0 < e/p^2(p-1)$ et que $u_1 = pi_0$. Alors*

$$\theta_{i_1}(s^p) = -(\theta_{i_0}(s))^{p^2-p+1}.$$

En effet, on sait (*cf.*, par exemple, infra, prop. 4.1) que $i_0 < e/p^2(p-1)$ entraîne $i_0 \not\equiv 0 \pmod{p}$ (puisque $e/p^2$ est l'indice de ramification absolu du corps fixe de $s$). Posons $u = s^p$. Comme $i(u) = i_1 \equiv i_0 \pmod{p}$, on a $i_1 \not\equiv 0 \pmod{p}$ et $u$ est régulier. On est dans les conditions d'application de la proposition 3.4, avec $i = i_1$ et, d'après la proposition 3.3, $i'_0 = i_0$ [en particulier, $i'_0 \not\equiv 0 \pmod{p}$].

Comme $i_0 < e/p^2(p-1)$ et comme $p^2 - p + 1 < p^2(p-1)$, on a $(p^2 - p + 1)\, i_0 < e$. De même, l'inégalité $i_0 < e/p^2(p-1)$ entraîne $i_0(p(p^2 - p + 1) - p) < e$, ce qui peut encore s'écrire

$$(p^2 - p + 1)\, i_0 < e - (p-1)(p^2 - p + 1)\, i_0 + pi_0 = e - (p-1)\, i + pi_0.$$

Finalement, $(p^2 - p + 1)\, i_0 < \min\{e,\ e - (p-1)\, i + pi_0\}$.

Comme $i'_0 + (i - i_0)/p = i_0 + (i_1 - i_0)/p = u_1 \equiv 0 \pmod{p}$, on retrouve que $i_1 = (p^2 - p + 1)\, i_0$ et on a

$$\theta_{i_1}(s^p) = -\theta_{i_0}(s)\,(\theta^{\mathrm{K}}_{i'_0}(\bar{s}))^{p-1}.$$

D'après la proposition 3.3, $\theta^{\mathrm{K}}_{i'_0}(\bar{s}) = \theta^{\mathrm{K}}_{i_0}(\bar{s}) = (\theta_{i_0}(s))^p$, et, finalement,

$$\theta_{i_1}(s^p) = -(\theta_{i_0}(s))^{p^2-p+1}.$$

*Remarque.* — Par une méthode analogue, on peut déduire de la proposition 3.3 une minoration non triviale de $i_{\mathrm{L}}(\tau)$, lorsque $\tau$ est le commutateur de deux éléments $s$ et $t$ de $\mathrm{S}^{\mathrm{L}}$ qui commutent avec $u$. Ceci permet d'obtenir une minoration non triviale de $i_{\mathrm{G}}(\tau)$ lorsque $\tau$ est le commutateur de deux éléments $s$ et $t$ du groupe de Galois G d'une extension finie galoisienne totalement ramifiée d'un corps local K. Par exemple, lorsque $e = +\infty$, on trouve que, si $i_{\mathrm{G}}(s) \leq i_{\mathrm{G}}(t)$, alors $i_{\mathrm{G}}(\tau) \geq pi_{\mathrm{G}}(s) + i_{\mathrm{G}}(t)$.

## 4. Sur quelques extensions totalement ramifiées.

4.1. Rappels sur les corps locaux a corps résiduel algébriquement clos. — Nous allons, dans ce paragraphe, utiliser les méthodes de [11], que nous citerons CRAC. Rappelons brièvement certains résultats.

Pour tout groupe profini H, muni de sa topologie naturelle, on note H' l'adhérence de son groupe des commutateurs et $\hat{H}$ le quotient H/H'.

Soit

$$1 \to G_L \to G_K \to J \to 1 \tag{8}$$

une suite exacte de groupes profinis, dans laquelle on suppose J fini. Le groupe J opère de façon naturelle sur $\hat{G}_L$ de la manière suivante :

Soit $\bar{s}$ un élément de J et soit $\hat{a}$ un élément de $\hat{G}_L$. Soit $s$ un relèvement de $\bar{s}$ dans $G_K$ et soit $a$ un relèvement de $\hat{a}$ dans $G_L$. On vérifie immédiatement que l'image $\widehat{sas^{-1}}$ de $sas^{-1}$ dans $\hat{G}_L$ ne dépend pas du choix des représentants $s$ et $a$. On pose $\bar{s}(\hat{a}) = \widehat{sas^{-1}}$.

L'injection canonique de $G_L$ dans $G_K$ définit, par passage au quotient, un homomorphisme $i$ de $\hat{G}_L$ dans $\hat{G}_K$. Le transfert est une application de $\hat{G}_K$ dans $\hat{G}_L$ que nous notons $t$; il est défini, par passage à la limite, à partir de la définition usuelle du transfert dans le cas des groupes finis. Pour tout $u$ dans $\hat{G}_L$, posons $N(u) = \prod_{\sigma \in J} \sigma(u)$. On vérifie facilement que $t.i = N$.

Soit E un corps local à corps résiduel algébriquement clos. Soit $\mathfrak{p}_E$ l'idéal maximal de l'anneau des entiers de E et soit $U_E$ le groupe des unités de E. Posons $U_E^{(0)} = U_E$ et, pour tout entier $n$ strictement positif, $U_E^{(n)} = 1 + \mathfrak{p}_E^n$. Pour simplifier l'écriture, on écrit, pour tout entier $n$ positif, $U_E^n$ au lieu de $U_E^{(n)}$. La famille des $U_E^n$ munit $U_E$ d'une filtration.

Pour tout groupe proalgébrique B et pour tout entier $n$ positif, on désigne par $\pi_n(B)$ le $n^{\text{ième}}$ groupe d'homotopie de B. Soit $B_0$ la composante connexe de B. Alors $\pi_0(B) = B/B_0$ (*cf.* [8], p. 35), $\pi_1(B)$ s'appelle le groupe fondamental de B (*ibid.*, déf. 1, p. 38) et, pour $i \geqq 2$, $\pi_i(B) = 1$ (*ibid.*, th. 2, p. 62). Si

$$1 \to B' \to B \to B'' \to 1$$

est une suite exacte de groupes proalgébriques, et si B' est connexe, on a $\pi_0(B') = 1$ et, par conséquent, la suite exacte d'homotopie se réduit à

$$1 \to \pi_1(B') \to \pi_1(B) \to \pi_1(B'') \to 1.$$

Pour tout entier $n$ positif, $U_E^n$ est un groupe proalgébrique. Le groupe $\pi_1(U_E^n)$ s'identifie à un sous-groupe de $\pi_1(U_E)$ et la famille des $\pi_1(U_E^n)$ munit $\pi_1(U_E)$ d'une filtration. On voit que, pour tout $n$, $U_E^n$ est connexe; par conséquent, $\pi_1(U_E^n/U_E^{n+1})$ s'identifie à $\pi_1(U_E^n)/\pi_1(U_E^{n+1})$.

Soit $\overline{E}$ une clôture algébrique de E et soit $G_E$ le groupe de Galois de l'extension $\overline{E}/E$. Le groupe $\hat{G}_E$ s'identifie au groupe de Galois de l'extension abélienne maximale $E_{ab}$ de E contenue dans $\overline{E}$. Pour toute extension galoisienne F de E, contenue dans $\overline{E}$, notons $g_{F/E}$ le groupe de Galois de l'extension F/E. Le groupe $\hat{G}_E$ est encore la limite projective des groupes $g_{F/E}$, pour F parcourant l'ensemble des extensions finies abéliennes de E.

Si F est une extension finie abélienne de E, la filtration en numérotation supérieure, définie au nº 1.4, munit $g_{F/E}$ d'une structure de groupe filtré. Si F′ est une extension finie abélienne de E contenant F, pour tout entier $n$, l'image canonique de $g_{F'/E}^n$ dans $g_{F/E}$ est $g_{F/E}^n$ (*cf.* CL, prop. 14, p. 81). On peut donc munir le groupe $\hat{G}_E$ d'une structure de groupe filtré.

Dans ces conditions (*cf.* CRAC, th. 1, p. 129 et 139), il existe un isomorphisme naturel $\theta$ de $\pi_1(U_E)$ sur $\hat{G}_E$ qui est un isomorphisme de groupes filtrés.

Soit alors K un corps local à corps résiduel algébriquement clos et soit $\overline{K}$ une clôture algébrique de K. Soit L une extension finie galoisienne de K contenue dans $\overline{K}$. Soit $G_K$ (resp. $G_L$, J) le groupe de Galois de l'extension $\overline{K}/K$ (resp. $\overline{K}/L$, L/K). On a la suite exacte

$$1 \to G_L \to G_K \to J \to 1. \tag{8}$$

Le groupe $U_L$ est un J-module; par transport de structure, on en déduit une structure de J-module sur $\pi_1(U_L)$ et l'application $\theta$ définie ci-dessus est un J-isomorphisme.

De plus l'injection de $U_K$ dans $U_L$ définit une injection $j$ de $\pi_1(U_K)$ dans $\pi_1(U_L)$ qui applique $\pi_1(U_K)$ sur $\pi_1(U_L)^J$ (*cf.* CRAC, prop. 4, p. 120). De même, la norme de $U_L$ dans $U_K$ définit un homomorphisme N de $\pi_1(U_L)$ dans $\pi_1(U_K)$ et les deux diagrammes suivants sont commutatifs (*cf.* CRAC, prop. 7, p. 122) :

$$\begin{array}{ccc} \pi_1(U_K) & \xrightarrow{j} & \pi_1(U_L) \\ {\scriptstyle\theta}\downarrow & & \downarrow{\scriptstyle\theta} \\ \hat{G}_K & \xrightarrow{i} & \hat{G}_L \end{array} \tag{9}$$

$$\begin{array}{ccc} \pi_1(U_L) & \xrightarrow{N} & \pi_1(U_K) \\ {\scriptstyle\theta}\downarrow & & \downarrow{\scriptstyle\theta} \\ \hat{G}_L & \xrightarrow{i} & \hat{G}_K \end{array} \tag{9'}$$

## 4.2. Rappels sur les $p$-extensions abéliennes des corps locaux.

Proposition 4.1. — *Soit $p$ un nombre premier et soit* L *un corps local à corps résiduel algébriquement clos de caractéristique $p$. Soit $e$ l'indice de ramification absolu de* L. *Pour tout $n \in \mathbf{R}$, posons* $P(n) = \min\{pn, n+e\}$. *Alors, pour tout entier $n \geqq 0$, $(\pi_1(U_L^n))^p$ est contenu dans $\pi_1(U_L^{P(n)})$. De plus :*

(i) *si $n \neq e/(p-1)$,* $\pi_1(U_L^{P(n)}) = (\pi_1(U_L^n))^p \pi_1(U_L^{P(n)+1})$;

(ii) *si $n = e/(p-1)$, le quotient de $\pi_1(U_L^{P(n)})$ par $(\pi_1(U_L^n))^p \pi_1(U_L^{P(n)+1})$ est cyclique d'ordre $p$.*

*Démonstration.* — Il est clair que l'application $\gamma$ définie par $\gamma(\alpha) = \alpha^p$ est un endomorphisme de groupes proalgébriques et que l'endomorphisme de $\pi_1(U_L)$ induit par $\gamma$ est l'élévation à la puissance $p^{\text{ième}}$.

Si $n \neq e/(p-1)$, on sait (*cf.* CRAC, prop. 6, p. 113) que $\gamma$ applique $U_L^n$ dans $U_L^{P(n)}$ et que la suite

$$1 \to U_L^{n+1} \to U_L^n \xrightarrow{\gamma} U_L^{P(n)}/U_L^{P(n)+1} \to 1$$

est exacte. Comme $U_L^{n+1}$ est connexe, on en déduit la suite exacte

$$1 \to \pi_1(U_L^{n+1}) \to \pi_1(U_L^n) \xrightarrow{\pi_1(\gamma)} \pi_1(U_L^{P(n)}/U_L^{P(n)+1}) \to 1.$$

Comme $\pi_1(U_L^{P(n)}/U_L^{P(n)+1})$ s'identifie à $\pi_1(U_L^{P(n)})/\pi_1(U_L^{P(n)+1})$, on en déduit que

$$\pi_1(U_L^{P(n)}) = (\pi_1(U_L^n))^p \pi_1(U_L^{P(n)+1}).$$

En particulier, $(\pi_1(U_L^n))^p$ est contenu dans $\pi_1(U_L^{P(n)})$.

Si $n = e/(p-1)$, on sait (*cf.* CRAC, prop. 6, p. 113) que l'application $\gamma$, qui applique $U_L^n$ dans $U_L^{P(n)}$, définit par passage au quotient un épimorphisme de $U_L^n$ sur $U_L^{P(n)}/U_L^{P(n)+1}$, que le noyau de cette application est un sous-groupe V de $U_L^n$ contenant $U_L^{n+1}$ et que le quotient $V/U_L^{n+1}$ est cyclique d'ordre $p$. On a donc la suite exacte

$$1 \to U_L^{n+1} \to V \to \mathbf{Z}/p\mathbf{Z} \to 0.$$

Comme $U_L^{n+1}$ est connexe, on voit que $\pi_0(V)$ peut s'identifier à $\mathbf{Z}/p\mathbf{Z}$. Comme $U_L^n$ est connexe, la suite exacte

$$1 \to V \mapsto U_L^n \xrightarrow{\gamma} U_L^{P(n)}/U_L^{P(n)+1} \to 1$$

donne naissance à la suite exacte d'homotopie

$$1 \to \pi_1(V) \to \pi_1(U_L^n) \xrightarrow{\pi_1(\gamma)} \pi_1(U_L^{P(n)}/U_L^{P(n)+1}) \to \mathbf{Z}/p\mathbf{Z} \to 0.$$

Comme $\pi_1(U_L^{P(n)}/U_L^{P(n)+1})$ s'identifie à $\pi_1(U_L^{P(n)})/\pi_1(U_L^{P(n)+1})$, on en déduit que $(\pi_1(U_L^n))^p$ est contenu dans $\pi_1(U_L^{P(n)})$ et que le quotient de $\pi_1(U_L^{P(n)})$ par $(\pi_1(U_L^n))^p\pi_1(U_L^{P(n)+1})$ est cyclique d'ordre $p$. C. Q. F. D.

PROPOSITION 4.2. — *Soit $p$ un nombre premier et soit* L *un corps local à corps résiduel de caractéristique $p$. Soit $e$ l'indice de ramification absolu de* L. *Soit* M *une $p$-extension finie abélienne totalement ramifiée de* L *et soit* G *le groupe de Galois de l'extension muni de sa filtration supérieure* (*cf.* n° 1.4). *Pour tout entier $n \geq 0$, posons $P(n) = \min\{pn, n+e\}$ et désignons par $P(G^n)$ le sous-groupe de* G *formé des puissances $p^{\text{ièmes}}$ des éléments de $G^n$. Alors, pour tout entier $n \geq 0$, le groupe $P(G^n)$ est contenu dans $G^{P(n)}$. De plus,*

(i) *si* $n \neq e/(p-1)$, $G^{P(n)} = P(G^n).G^{P(n)+1}$;

(ii) *si* $n = e/(p-1)$, *le groupe* $G^{P(n)}/P(G^n).G^{P(n)+1}$ *est cyclique d'ordre $p$ ou* 1.

*Démonstration.* — Supposons d'abord le corps résiduel de L algébriquement clos. Soit $\theta_L$ l'épimorphisme canonique de $\pi_1(U_L)$ sur G. Compte tenu de ce que $\theta_L$ est un épimorphisme de groupes filtrés, l'assertion résulte trivialement de la proposition 4.1. En particulier, dans le cas (ii), $\theta_L$ définit, par passage au quotient, un épimorphisme $\rho$ de $\pi_1(U_L^{P(n)})/(\pi_1(U_L^n))^p\pi_1(U_L^{P(n)+1})$ sur $G^{P(n)}/P(G^n).G^{P(n)+1}$. Ce dernier groupe est d'ordre $p$ ou 1 suivant que $\rho$ est injectif ou non.

Si le corps résiduel de L n'est pas algébriquement clos, considérons la complétion $\overline{L}$ d'une clôture algébrique de L contenant M. On vérifie facilement (*cf.* CRAC, Rem. 2, p. 139) qu'il existe un sous-corps L' de $\overline{L}$ contenant L qui est complet pour le prolongement de la valuation de L à L', dont le corps résiduel est algébriquement clos, et qui est tel que $e_{L'/L} = 1$ (ceci signifiant que, pour toute extension finie N de L, contenue dans L', on a $e_{N/L} = 1$). En particulier, la valuation de L' est discrète et L et L' ont même indice de ramification absolu. Soit M' le composé de L' et M. On voit que l'extension M'/L' est galoisienne et que les groupes de Galois des extensions M/L et M'/L' sont canoniquement isomorphes en tant que groupes filtrés. C. Q. F. D.

COROLLAIRE. — *Si l'extension* M/L *est abélienne de type* $(p, p, \ldots, p)$ *et si* $n > 0$ *est un nombre supérieur de ramification de l'extension, on a*

— *ou bien* $0 < n < ep/(p-1)$ *et* $n \not\equiv 0 \pmod p$;

— *ou bien* $n = ep/(p-1)$.

*De plus, si* $e' = e/(p-1)$ *est entier, le groupe* $G^{pe'}$ *est au plus d'ordre* $p$.

En effet, s'il existait un entier $m$, $> 0$ et $\neq e/(p-1)$, tel que $n = \mathrm{P}(m)$ soit un nombre supérieur de ramification et si $s$ était un élément de $G^n - G^{n+1}$, il existerait, d'après (i), un élément $t$ de G tel que $t^p \equiv s \pmod{G^{n+1}}$ et le groupe $G/G^{n+1}$ ne serait pas de type $(p, p, \ldots, p)$. On doit donc avoir $n \leqq ep/(p-1)$ [car sinon on aurait $n = \mathrm{P}(m)$ avec $m = n - e \neq e/(p-1)$] et, si $n < ep/(p-1)$, $n \not\equiv 0 \pmod p$ [car sinon on aurait $n = \mathrm{P}(m)$ avec $m = n/p \neq e/(p-1)$]. En particulier, si $e' = e/(p-1)$ est entier, on a $G^{pe'+1} = \{1\}$. Par hypothèse, $\mathrm{P}(G^{e'}) = \mathrm{P}(G) = \{1\}$ et l'assertion (ii) montre que $G^{\mathrm{P}(e')}/\mathrm{P}(G^{e'})\, G^{\mathrm{P}(e')+1} = G^{pe'}$ est au plus d'ordre $p$.

Proposition 4.3. — *Avec les hypothèses et les notations de la proposition* 4.2, *supposons de plus l'extension* M/L *cyclique de degré* $p^\lambda$, *avec* $\lambda > 0$. *Soient*

$$u_1 < u_2 < \ldots < u_\lambda$$

*les nombres supérieurs de ramification,* $>0$, *de l'extension. Alors on a*

(*a*) $u_1 = ep/(p-1)$ *ou* $0 < u_1 < ep/(p-1)$ *et* $u_1 \not\equiv 0 \pmod p$;

(*b*) *pour* $j = 1, 2, \ldots, \lambda - 1$ :

(i) *si* $u_j \geqq e/(p-1)$, $u_{j+1} = u_j + e$;

(ii) *si* $u_j < e/(p-1)$,

*ou bien* $u_{j+1} = pu_j$,

*ou bien* $u_{j+1} = ep/(p-1)$,

*ou bien* $pu_j < u_{j+1} < ep/(p-1)$ *et* $u_{j+1} \not\equiv 0 \pmod p$.

*Démonstration.* — Pour $j = 1, 2, \ldots, \lambda$, posons, comme au n° 1.3, $\Gamma_j = G^{u_j}$ et posons $\Gamma_{\lambda+1} = \{1\}$.

Désignons par M′ le corps fixe de $\Gamma_2$. L'assertion (*a*) résulte du corollaire précédent appliqué à l'extension M′/L.

Soit $s$ un générateur de $\Gamma_j$. Alors $s^p$ est un générateur de $\mathrm{P}(\Gamma_j) = \Gamma_{j+1}$ et il résulte de la proposition 4.2 que $u_{j+1} \geqq \mathrm{P}(u_j)$. Si $u_{j+1} = \mathrm{P}(m)$, avec $m$ entier $\neq e/(p-1)$, alors si $t$ est un générateur de $\Gamma_{j+1}$, il résulte de la proposition précédente qu'il existe un élément $s$ de $G^m$ et un élément $t_1$ de $\Gamma_{j+2}$ tels que $t = s^p t_1$. Posons $t' = tt_1^{-1}$. On voit que $t'$ est un générateur de $\Gamma_{j+1}$ et que $s^p = t'$. Donc $u_j \geqq m$. Si on avait $u_j > m$, on aurait $u_{j+1} = \mathrm{P}(m) < \mathrm{P}(u_j)$, ce qui contredirait $u_{j+1} \geqq \mathrm{P}(u_j)$. On a donc :

$$\left\{\begin{array}{l} u_{j+1} \geqq \mathrm{P}(u_j) \\ \textit{si } u_{j+1} = \mathrm{P}(m), \quad \textit{avec } m \textit{ entier} \neq e/(p-1), \qquad \textit{alors} \quad u_j = m. \end{array}\right.$$

Si $u_j \geqq e/(p-1)$, on a $u_{j+1} \geqq \mathrm{P}(u_j) = u_j + e$. Si on avait $u_{j+1} > u_j + e$, on aurait $u_{j+1} = \mathrm{P}(m)$, avec $m = u_{j+1} - e > u_j$, ce qui est impossible. Donc $u_{j+1} = u_j + e$ et l'assertion (i) du (*b*) est établie.

Si $u_j < e/(p-1)$, on doit avoir $u_{j+1} \geqq \mathrm{P}(u_j) = pu_j$. Si on avait $u_{j+1} > ep/(p-1)$, on aurait $u_{j+1} = \mathrm{P}(m)$, avec $m = u_{j+1} - e > e/(p-1) > u_j$, ce qui est impossible. On a donc $pu_j \leqq u_{j+1} \leqq ep/(p-1)$. Si on avait $pu_j < u_{j+1} < ep/(p-1)$ avec $u_{j+1} \equiv 0 \pmod p$, on aurait $u_{j+1} = \mathrm{P}(m)$, avec $m = u_{j+1}/p > u_j$, ce qui est impossible. Les seuls cas possibles sont bien ceux qui ont été énoncés dans l'assertion (ii) du (*b*).

C. Q. F. D.

*Remarque.* — On trouvera dans la thèse de E. Maus ([5], § 6) une démonstration de la proposition 4.3 (énoncée sous une forme légèrement différente), ainsi que des réciproques, dans le cas où le corps résiduel de K est fini ou quasi-fini).

4.3. Extensions diédrales et quaternioniennes généralisées. — Soit

$$1 \to \mathrm{A} \to \mathrm{G} \to \mathrm{J} \to 1$$

une suite exacte de groupes finis vérifiant les conditions suivantes :

(i) le groupe A est cyclique d'ordre $2^\lambda$ ($\lambda$ étant un entier $\geqq 2$);

(ii) le groupe J est cyclique d'ordre 2;

(iii) l'action de l'élément $s$ de J différent de 1 sur A est donnée par

$$a \mapsto a^{-1} \quad \text{pour tout } a \text{ dans A.}$$

On vérifie immédiatement que l'on est dans l'un des deux cas suivants :

— ou bien G est le produit semi-direct de J par le sous-groupe invariant A et G est isomorphe au groupe diédral d'ordre $2^{\lambda+1}$;

— ou bien G est isomorphe au groupe des quaternions généralisé d'ordre $2^{\lambda+1}$.

Proposition 4.4. — *Soit* K *un corps local dont le corps résiduel est de caractéristique* 2. *Avec les notations qui précèdent, soit* M *une extension galoisienne totalement ramifiée de* K *dont le groupe de Galois est* G. *Soit* L *le corps fixe de* A *et soit* $e$ *l'indice de ramification absolu de* L.

(*a*) *Si* G *est diédral, ou si* $\lambda \geqq 3$, *les nombres supérieurs de ramification de l'extension* M/L *sont des entiers impairs.*

(*b*) *Si* G *est isomorphe au groupe des quaternions d'ordre* 8, *alors :*

(i) *ou bien les nombres supérieurs de ramification de l'extension* M/L *sont des entiers impairs;*

(ii) *ou bien le nombre de ramification de l'extension quadratique* L/K *est e et il existe un entier impair i, vérifiant* $i < e$, *tel que les nombres supérieurs de ramification de l'extension* M/L *sont i et* $2e$;

(iii) *ou bien le nombre de ramification de l'extension quadratique* L/K *est un entier impair u, vérifiant* $u < e$, *et les nombres supérieurs de ramification de l'extension* M/L *sont u et* $2u$.

*Démonstration* (d'après J.-P. Serre). — Il est clair que, de la même manière que pour la proposition 4.2, on peut se ramener au cas où le corps résiduel de K est algébriquement clos. Nous allons supposer qu'il en est ainsi et commencer par établir deux lemmes.

LEMME 1. — *Pour tout entier* $n \geq 0$, *soit* $t(G_K^n)$ *l'image de* $G_K^n$ *par le transfert de* $G_K$ *dans* $G_L$. *On a* $\hat{G}_L^{2n} = t(G_K^n)\,\hat{G}_L^{2n+1}$.

*Démonstration.* — Comme l'extension L/K est de degré 2 et totalement ramifiée, on a la suite exacte

$$1 \to U_K^{n+1} \to U_K^n \to U_L^{2n}/U_L^{2n+1} \to 1.$$

Comme $U_K^{n+1}$ est connexe, on en déduit la suite exacte

$$1 \to \pi_1(U_K^{n+1}) \to \pi_1(U_K^n) \to \pi_1(U_L^{2n}/U_L^{2n+1}) \to 1.$$

Comme $\pi_1(U_L^{2n}/U_L^{2n+1})$ s'identifie à $\pi_1(U_L^{2n})/\pi_1(U_L^{2n+1})$, on voit que

$$\pi_1(U_L^{2n}) = j(\pi_1(U_K^n))\,\pi_1(U_L^{2n+1}).$$

Comme $\theta(\pi_1(U_L^{2n})) = \hat{G}_L^{2n}$ et $\theta(\pi_1(U_L^{2n+1})) = \hat{G}_L^{2n+1}$, on a

$$\hat{G}_L^{2n} = \theta j(\pi_1(U_K^n))\,G_L^{2n+1}.$$

L'assertion résulte alors de la commutativité du diagramme (9) qui montre que

$$\theta j(\pi_1(U_K^n)) = t\,\theta(\pi_1(U_K^n)) = t(\hat{G}_K^n).$$

C. Q. F. D.

LEMME 2. — *Soit u l'unique nombre de ramification de l'extension* L/K. *Pour tout entier n positif, posons*

$$\psi(n) = \begin{cases} n & si\ n \leq u, \\ u + 2(n-u) & si\ n > u. \end{cases}$$

*Alors, pour tout entier n différent de u, on a* $\hat{G}_K^n = i(\hat{G}_L^{\psi(n)})\,\hat{G}_K^{n+1}$.

*Démonstration.* — Pour tout entier $n \neq u$, la norme applique $U_L^{\psi(n)}$ dans $U_K^n$ et, par passage au quotient, on en déduit la suite exacte (*cf.* CRAC, prop. 5, p. 130)

$$1 \to U_L^{\psi(n)+1} \to U_L^{\psi(n)} \to U_K^n/U_K^{n+1} \to 1.$$

Comme $U_L^{\psi(n)+1}$ est connexe, on en déduit la suite exacte

$$1 \to \pi_1(U_L^{\psi(n)+1}) \to \pi_1(U_L^{\psi(n)}) \to \pi_1(U_K^n/U_K^{n+1}) \to 1.$$

Comme $\pi_1(U_K^n/U_K^{n+1})$ s'identifie à $\pi_1(U_K^n)/\pi_1(U_K^{n+1})$, on voit que

$$\pi_1(U_K^n) = N(\pi_1(U_L^{\psi(n)}))\,\pi_1(U_K^{n+1}).$$

Comme $\theta(\pi_1(U_K^n)) = \hat{G}_K^n$ et $\theta(\pi_1(U_K^{n+1})) = \hat{G}_K^{n+1}$, on a

$$\hat{G}_K^n = \theta\, N(\pi_1(U_L^{\psi(n)}))\,\hat{G}_K^{n+1}.$$

L'assertion résulte alors de la commutativité du diagramme (9′) qui montre que

$$\theta\, N(\pi_1(U_L^{\psi(n)})) = i\,\theta(\pi_1(U_L^{\psi(n)})) = i(\hat{G}_L^{\psi(n)}).$$

C. Q. F. D.

*Suite de la démonstration de la proposition* 4.4. — Soit $\beta$ l'application canonique de $\hat{G}_L$ dans A. Il est clair que $\beta$ est un J-épimorphisme. Pour tout $x$ dans $\hat{G}_L$, on a donc

$$\beta(s(x)) = s(\beta(x)) = \beta(x^{-1}) \qquad \text{ou encore} \qquad \beta(N(x)) = 1.$$

Ceci revient à dire que $\beta$ est trivial sur le groupe $N(\hat{G}_L) = ti(\hat{G}_L)$.

[*Remarque.* — Inversement, on voit que, l'extension L/K étant donnée, tout épimorphisme de $\hat{G}_L$ sur A qui est trivial sur $N(\hat{G}_L)$ définit une extension galoisienne M de K dont le groupe de Galois est du type de G.]

Soit $\alpha$ l'épimorphisme canonique de $\hat{G}_K$ sur $\hat{G}$. Il est clair que le diagramme suivant est commutatif

(10)
$$\begin{array}{ccc} \hat{G}_K & \xrightarrow{\alpha} & \hat{G} \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle t} \\ \hat{G}_L & \xrightarrow{\beta} & A \end{array}$$

On vérifie immédiatement que le transfert de $\hat{G}$ dans A est trivial si et seulement si le groupe G est diédral. Par conséquent :

(*a*) si le groupe G est diédral, $\beta$ est trivial sur $t(\hat{G}_K)$;

(*b*) si le groupe G est quaternionien, $\beta$ est trivial sur $ti(\hat{G}_L) = N(\hat{G}_L)$.

*Fin de la démonstration dans le cas diédral.* — Lorsque G est diédral, la proposition 4.4 revient à affirmer que, pour tout entier $n$, $\beta(\hat{G}_L^{2n}) = \beta(\hat{G}_L^{2n+1})$. Comme $\beta$ est trivial sur $t(\hat{G}_K)$, il suffit de vérifier que $\hat{G}_L^{2n}$ est contenu dans $t(\hat{G}_K)\hat{G}_L^{2n+1}$, ce qui résulte du lemme 1.

Avant d'achever la démonstration dans le cas quaternionien, nous allons établir deux autres lemmes.

LEMME 3. — *Si* G *est quaternionien, pour tout entier* $n$, *différent de* $u$, $2n$ *n'est pas nombre supérieur de ramification de l'extension* M/L.

*Démonstration.* — Le lemme revient à affirmer que, pour tout entier $n$, différent de $u$, $\beta(\hat{G}_L^{2n}) = \beta(\hat{G}_L^{2n+1})$. D'après le lemme 1, $\hat{G}_L^{2n} = t(\hat{G}_K^n)\hat{G}_L^{2n+1}$. D'après le lemme 2, si $n \neq u$, $\hat{G}_K^n = i(\hat{G}_L^{\psi(n)})\hat{G}_K^{n+1}$. Comme $ti = \mathrm{N}$, on en déduit que

$$\hat{G}_L^{2n} = \mathrm{N}(\hat{G}_L^{\psi(n)})\, t(\hat{G}_K^{n+1})\, \hat{G}_L^{2n+1}.$$

Comme $t(\hat{G}_K^{n+1})$ est contenu dans $\hat{G}_L^{2n+2}$ (*cf.* lemme 1, appliqué à $n+1$), donc *a fortiori* dans $\hat{G}_L^{2n+1}$, on a $\hat{G}_L^{2n} = \mathrm{N}(\hat{G}_L^{\psi(n)})\hat{G}_L^{2n+1}$. Comme $\beta$ est trivial sur N, on a $\beta(\hat{G}_L^{2n}) = \beta(\hat{G}_L^{2n+1})$. C. Q. F. D.

LEMME 4. — *Si* G *est quaternionien et si* $2u$ *est nombre de ramification de l'extension* M/L, *alors les autres nombres supérieurs de ramification de l'extension sont* $< 2u$.

*Démonstration.* — Le lemme revient à affirmer que, si $\beta(\hat{G}_L^{2u})$ contient strictement $\beta(\hat{G}_L^{2u+1})$, alors $\beta(\hat{G}_L^{2u+1}) = \{1\}$.

D'après le lemme 1, $\beta(\hat{G}_L^{2u}) = \beta\, t(\hat{G}_K^u)\, \beta(\hat{G}_L^{2u+1})$. Si $\beta(\hat{G}_L^{2u})$ contient strictement $\beta(\hat{G}_L^{2u+1})$, on voit que $\beta\, t(\hat{G}_K^u)$ n'est pas contenu dans $\beta(\hat{G}_L^{2u+1})$. D'après le lemme 1, $t(\hat{G}_K^{u+1})$ est contenu dans $\hat{G}_L^{2(u+1)}$, donc dans $\hat{G}_L^{2u+1}$. On en déduit que $\beta\, t(\hat{G}_K^{u+1})$ est contenu dans $\beta(\hat{G}_L^{2u+1})$. Donc, $\beta\, t(\hat{G}_K^{u+1})$ est strictement contenu dans $\beta\, t(\hat{G}_K^u)$. Soit A′ l'image par le transfert de $\hat{G}$ dans A. Il est clair que A′ est le sous-groupe de A d'ordre 2. Il résulte de la commutativité du diagramme (10) que, pour tout entier $n$ positif, on a ou bien $\beta\, t(\hat{G}_K^n) = \mathrm{A}'$, ou bien $\beta\, t(\hat{G}_K^n) = \{1\}$. Comme A′ est d'ordre premier, on a donc nécessairement $\beta\, t(\hat{G}_K^u) = \mathrm{A}'$ et $\beta\, t(\hat{G}_K^{u+1}) = \{1\}$. D'après le lemme 1, on a $\hat{G}_L^{2u} = t(\hat{G}_K^u)\hat{G}_L^{2u+1}$. Comme $\beta\, t(\hat{G}_K^u) = \mathrm{A}'$, on en déduit que $\beta(\hat{G}_L^{2u}) = \mathrm{A}'\beta(\hat{G}_L^{2u+1})$. Si $\beta(\hat{G}_L^{2u+1}) \neq \{1\}$, on aurait $\mathrm{A}' \subset \beta(\hat{G}_L^{2u+1})$ et, par conséquent, $\beta(\hat{G}_L^{2u}) = \beta(\hat{G}_L^{2u+1})$, contrairement à l'hypothèse. Donc $\beta(\hat{G}_L^{2u+1}) = \{1\}$. C. Q. F. D.

*Fin de la démonstration dans le cas quaternionien.* — Si $2u$ n'est pas nombre supérieur de ramification, la proposition résulte du lemme 3. Supposons que $2u$ soit nombre supérieur de ramification de l'extension M/L. Avec les notations de la proposition 4.3, il résulte du lemme 4 que $u_\lambda = 2u$. Appliquons le (*b*) de la proposition 4.3. Comme $2u \equiv 0 \pmod 2$, si on est dans le cas (ii), c'est-à-dire si $u_{\lambda-1} < e$, on a

($c$ 1) ou bien $2u = u_\lambda = 2u_{\lambda-1}$;

($c$ 2) ou bien $2u = u_\lambda = 2e$.

Si on est dans le cas (i), c'est-à-dire si $u_{\lambda-1} \geqq e$, on a $u_\lambda = u_{\lambda-1} + e$. Mais il résulte du corollaire à la proposition 4.2 appliqué à l'extension L/K que $u \leqq e$. Donc $u_{\lambda-1} = 2u - e \leqq e$. Par conséquent, $u_{\lambda-1} = e$ et $u_\lambda = 2e$. On est dans le cas ($c$ 2).

Supposons $u_{\lambda-1} > u$. Comme dans ($c$ 1) on a $u_{\lambda-1} = u$, on serait dans le cas ($c$ 2). On aurait donc $u = e$ et $u_{\lambda-1} > e$. D'après la proposition 4.3, on aurait $u_\lambda = u_{\lambda-1} + e > 2e = 2u$. Donc, dans les deux cas, on a

$$u_{\lambda-1} \leqq u < u_\lambda. \tag{11}$$

Soit $i_G$ (resp. $i_A$) la fonction d'ordre de la filtration de G (resp. A) et soit $s$ le générateur du groupe de Galois J de l'extension quadratique L/K. Soit $i = \max_{\sigma \mapsto s}(i_G(\sigma))$ et soit $\sigma$ un relèvement de $s$ dans G tel que $i_G(\sigma) = i$. On a $\varphi_{M/K}(i) = u$ (*cf.* CL, prop. 14, p. 81). Comme $\varphi_{M/K} = \varphi_{M/L} \circ \varphi_{L/K}$ (*cf.* CL, prop. 15, p. 81), on a $\varphi_{M/L}(\varphi_{L/K}(i)) = u$. Comme $i \geqq \varphi_{L/K}(i)$ et comme $\varphi_{M/L}$ est une fonction croissante, on en déduit que $\varphi_{M/L}(i) \geqq u$. Soient $i_{\lambda-1} < i_\lambda$ les deux plus grands nombres de ramification de l'extension M/L. On a $u_{\lambda-1} = \varphi_{M/L}(i_{\lambda-1})$ et l'inégalité (11) montre que $\varphi_{M/L}(i) \geqq u \geqq u_{\lambda-1} = \varphi_{M/L}(i_{\lambda-1})$. On en déduit que $i \geqq i_{\lambda-1}$, ou que $i + 1 > i_{\lambda-1}$. Donc $A_{i+1} \subset A_{i_\lambda} = A'$.

On sait (*cf.* CL, prop. 10, p. 77) que, pour tout couple $t$, $t'$ d'éléments de G, on a $i_G(tt't^{-1}t'^{-1}) \geqq i_G(t) + i_G(t')$. Pour tout $a \in G$, on a donc

$$i_G(\sigma a \sigma^{-1} a^{-1}) \geqq i + i_G(a) \geqq i + 1. \tag{12}$$

Soit $\overline{G}$ le quotient de G par A'. Pour tout $t$ dans G, notons $\bar{t}$ son image dans $\overline{G}$. On sait (*cf.* CL, cor. à la prop. 3, p. 71) que $i_{\overline{G}}(\bar{t}) \geqq i_G(t)$. Pour tout $a \in G$, $\sigma a \sigma^{-1} a^{-1} \in A$ et la formule (12) montre que $\sigma a \sigma^{-1} a^{-1} \in A_{i+1} \subset A'$. Donc $\bar{\sigma}\bar{a}\bar{\sigma}^{-1}\bar{a}^{-1} = 1$ et $\overline{G}$ est abélien. Il est immédiat que ceci entraîne $\lambda = 2$.

Supposons que $2u = u_2 = 2e$. On a donc $u = e$ et, d'après (11), $u_1 \leqq e$. Soit L' le corps fixe de A'. Comme le nombre de ramification d'une extension quadratique de K est $\leqq e$ (*cf.* cor. à la prop. 4.2), on voit que, si on avait $u_1 = e$, l'extension biquadratique $L'/K$ aurait un seul nombre de ramification qui serait $e$, ce qui est impossible d'après le corollaire à la proposition 4.2. On a donc $u_1 < e$ et, d'après ce même corollaire, $u_1 \not\equiv 0 \pmod 2$. On est donc dans le cas (ii) du (*b*) de la proposition 4.4.

Sinon, on a $2u = u_2 = 2u_1$. On a donc $u_1 = u$ et $u_2 = 2u$. Comme $u_1 = u$, il résulte du lemme 3 que $u$ est impair et on est dans le cas (iii) du (*b*) de la proposition 4.4.

C. Q. F. D.

COROLLAIRE. — *Soit $u$ le nombre de ramification de* $L/K$. *Si* $G$ *est diédral ou si* $G$ *est quaternionien d'ordre au moins* 16, *et si* $u \neq e$, *les nombres supérieurs de ramification de l'extension* $M/K$ *sont des entiers.*

En effet, il résulte du corollaire à la proposition 4.2 que $u \not\equiv 0 \pmod 2$. Soient

$$u_1 < u_2 < \ldots < u_\lambda$$

les nombres supérieurs de ramification $> 0$ de l'extension $M/L$. Posons $u_0 = 0$ et $u_{\lambda+1} = +\infty$. Il est immédiat que les nombres supérieurs de ramification $> 0$ de l'extension $M/K$ sont (*cf.* CL, prop. 15, p. 81), si $u_j \leqq u < u_{j+1}$,

$$u_1 < u_2 < \ldots < u_j \leqq u < u + (u_{j+1} - u)/2 < \ldots < u + (u_\lambda - u)/2.$$

Comme $u$ et les $u_i$ sont des entiers impairs, on voit que ces nombres sont tous entiers (en fait, on vérifie facilement que l'on a toujours $u \leqq u_2$).

*Remarques :*

(*a*) Lorsque $K$ est de caractéristique $p$, on a toujours $u \neq e$. On est donc dans les conditions d'application du corollaire précédent.

(*b*) Lorsque la caractéristique de $K$ est nulle, il n'en est plus ainsi. Nous allons donner un exemple de chacun des cas possibles lorsque $u = e$.

Prenons $K = \mathbf{Q}_2$ et $L = \mathbf{Q}_2(\sqrt{2})$. Alors l'extension $L/K$ est de degré 2, totalement ramifiée et son unique nombre de ramification est $u = 2$. L'indice de ramification absolu de $L$ est $e = 2 = u$. Soit $\beta$ un épimorphisme de $L^*$ sur le groupe $\mathbf{Z}/2^\lambda\mathbf{Z}$ tel que la restriction de $\beta$ au groupe des unités $U_L$ soit surjective. L'application de réciprocité associe à $\beta$ une extension cyclique $M$ de $L$ de degré $2^\lambda$, totalement ramifiée. Les nombres supérieurs de ramification de l'extension $M/L$ sont les entiers $n$ tels que $\beta(U_L^{n+1}) \neq \beta(U_L^n)$. On vérifie sans difficulté que l'extension $M/K$ est galoisienne de groupe de Galois $G$ isomorphe au groupe diédral ou au groupe des quaternions généralisé d'ordre $2^{\lambda+1}$ si et seulement si $\beta(N_{L/K}(L^\star)) = 0$ et qu'alors G est isomorphe au groupe des quaternions généralisés si et seulement si $\beta(K^\star) \neq 0$.

Le groupe $K^\star$ (resp. $L^\star$) est le produit direct du $\mathbf{Z}$-module libre engendré par 2 (resp. $\sqrt{2}$) et de $U_K$ (resp. $U_L$). Le groupe $U_K$ (resp. $U_L$) est le produit direct du groupe cyclique d'ordre 2 engendré par $-1$ et du $\mathbf{Z}_p$-module libre de rang 1 (resp. 2) engendré par 5 (resp. $1+\sqrt{2}$ et 5). Il est immédiat que $N_{L/K}(L^\star)$ est engendré topologiquement par 2, $-1$ et 25.

Désignons par 1 un générateur de $\mathbf{Z}/2^\lambda\mathbf{Z}$.

— Définissons $\beta$ par $\beta(\sqrt{2}) = \beta(-1) = \beta(5) = 0$, $\beta(1+\sqrt{2}) = 1$. On vérifie que l'extension M de K ainsi définie est une extension galoisienne, de groupe de Galois isomorphe au groupe diédral d'ordre $2^{\lambda+1}$, et que les nombres supérieurs de ramification de l'extension M/L sont 1, 3, ..., $2\lambda+1$.

— Définissons $\beta$ par $\beta(\sqrt{2}) = \beta(-1) = 0$, $\beta(5) = 2^{\lambda-1}$, $\beta(1+\sqrt{2}) = 1$. On vérifie que l'extension M de K ainsi définie est une extension galoisienne, de groupe de Galois isomorphe au groupe des quaternions généralisés d'ordre $2^{\lambda+1}$, et que les nombres supérieurs de ramification de l'extension M/L sont

(i) si $\lambda = 2$ : 1 et 4;

(ii) si $\lambda > 2$ : 1, 3, ..., $2\lambda+1$.

### 4.4. Extensions quaternioniennes.

Proposition 4.5. — *Soit* K *un corps local dont le corps résiduel* $k$ *est de caractéristique* 2 *et soit* M *une extension galoisienne totalement ramifiée de* K *dont le groupe de Galois* G *est isomorphe au groupe des quaternions d'ordre* 8. *Alors :*

(i) *ou bien les nombres supérieurs de ramification de l'extension* M/K *sont des entiers;*

(ii) *ou bien il existe un entier impair* $u$ *tel que les nombres supérieurs de ramification de l'extension* L/K *sont* $u$ *et* $3u/2$. *On a alors* $G = G_u$ *et* $G_{u+1}$ *est le centre de* G. *De plus, l'image par* $\rho_1$ *de* $G_u/G_{u+1}$ *est stable par multiplication par les racines cubiques de l'unité [en d'autres termes,* $k$ *contient une racine cubique de l'unité* $\varepsilon$, *différente de* 1, *et si* $c$ *est un élément non nul de* $\rho_1(G_u)$, *on a* $\rho_1(G_u) = \{0, c, \varepsilon c, \varepsilon^2 c\}$].

(L'application $\rho_1 = \theta_u$ a été définie au n° 1.3.)

*Démonstration.* — Soit A′ le centre de G et soit M′ le corps fixe de A′. Il est clair que A′ est cyclique d'ordre 2. On voit que, si $a'$ désigne l'unique générateur de A′, $i_G(A')$ est égal au plus grand nombre de ramification $i'$ de l'extension. Si $s \in G - A'$, on a $i_G(s) < i'$, car $s^2 = a'$ et $i_G(s) < i_G(s^2)$. On en déduit que $A' = G_{i'}$ et (*cf.* CL, cor. à la prop. 3, p. 71) que les nombres de ramification de l'extension biquadratique M′/K sont les nombres de ramification de l'extension M/K qui sont $< i'$. Soit $e_K$ l'indice de ramification absolu de K. Il résulte du corollaire à la proposition 4.2 que

(*a*) ou bien M′/K a deux nombres de ramification distincts $i_1 < i_2$ et on a

$$i_2 \leqq 2\, e_K \qquad \text{et} \qquad i_1 \not\equiv 0 \pmod 2;$$

(*b*) ou bien M′/K a un seul nombre de ramification $i_1$ et on a

$$i_1 < 2\, e_K \qquad \text{et} \qquad i_1 \not\equiv 0 \pmod 2.$$

— Dans le cas (*a*), l'extension M/K a trois nombres de ramification $i_1 < i_2 < i'$ distincts. Soit L le corps fixe de $G_{i_2}$. Si on pose $A = G_{i_2}$ et si on note J le groupe de Galois de l'extension L/K, on est dans la situation du (*b*) de la proposition 4.4, avec $e = 2\, e_K$, le nombre de ramification de l'extension L/K étant $i_1$. Comme $i_1 < 2\, e_K = e$, on n'est pas dans le cas (ii). Comme $i_1 < i_2$ et comme le plus petit nombre de ramification de l'extension M/L est $i_2$, on n'est pas dans le cas (iii). On est donc dans le cas (i) et les nombres supérieurs de ramification de l'extension M/L sont des entiers impairs $v = i_2 < w$. Comme $i_1$ est impair, les nombres supérieurs de ramification de M/K qui sont $i_1$, $i_1 + (v - i_1)/2$ et $i_1 + (w - i_1)/2$, sont entiers.

— Dans le cas (*b*), l'extension M/K a deux nombres de ramification $i_1 < i'$ distincts et ses nombres supérieurs de ramification sont $u = i_1$ et $v' = i_1 + (i' - i_1)/4$. Soit A un sous-groupe de G d'indice 2 et soit L son corps fixe. On est dans la situation du (*b*) de la proposition 4.4, avec $e = 2\, e_K$, le nombre de ramification de l'extension quadratique L/K étant $i_1$, tandis que les nombres supérieurs de ramification de l'extension M/L sont $u = i_1$ et $v = i_1 + (i' - i_1)/2$. Si on est dans le cas (i), $u$ et $v$ sont des entiers impairs et, comme $i_1$ est impair, $u = i_1$ et

$$v' = i_1 + (i' - i_1)/4 = i_1 + (v - i_1)/2$$

sont entiers. Le cas (ii) est impossible car $i_1 \neq e$.

Dans le cas (iii) enfin, on a $v = 2u$ et, par conséquent,

$$v' = u + (v - u)/2 = 3u/2.$$

Soit alors $(\bar{s}, \bar{t})$ un système de générateurs de $G_u/G_{u+1}$ et soit $s$ (resp. $t$) un relèvement de $\bar{s}$ (resp. $\bar{t}$) dans G. Soit $L_s$ (resp. $L_t$) le corps fixe de $s$ (resp. $t$). Il est clair que les extensions $M/L_s$ et $M/L_t$ sont toutes deux cycliques de degré 4, totalement ramifiées, avec $u$ et $2u$ comme nombres supérieurs de ramification. L'indice de ramification absolu de M est $4e$ et on a $u < 4e/4$. Comme $s^2 = t^2$, il résulte du corollaire à la proposition 3.4 que

$$\theta_{3u}(s^2) = -(\theta_u(s))^{2^2-2+1} = -(\theta_u(t))^{2^2-2+1}.$$

On a donc $(\theta_u(s))^3 = (\theta_u(t))^3$ ou encore $(\rho_1(s))^3 = (\rho_1(t))^3$. Comme $(\bar{s}, \bar{t})$ est un système de générateurs du groupe $G_u/G_{u+1}$, on a $\rho_1(s) \neq \rho_1(t)$. Il existe donc une racine primitive cubique de l'unité $\varepsilon$ du corps résiduel telle que $\rho_1(t) = \varepsilon\rho_1(s)$ et on a

$$\rho_1(st) = \rho_1(s) + \rho_1(t) = \varepsilon^2 \rho_1(s).$$

C. Q. F. D.

Corollaire. — *Soit* K *un corps local dont le corps résiduel est de caractéristique* 2 *et ne contient pas les racines cubiques de l'unité. Soit* M *une extension galoisienne de* K, *totalement ramifiée, de groupe de Galois isomorphe au groupe des quaternions d'ordre* 8. *Alors les nombres supérieurs de ramification de l'extension sont des entiers.*

C'est évident puisque si ce ne sont pas des entiers, on a

$$\rho_1(G_u) = \{0, c, \varepsilon c, \varepsilon^2 c\}, \qquad \text{avec} \quad c \neq 0;$$

et la racine primitive cubique de l'unité $\varepsilon$ appartient donc au corps résiduel.

*Remarque.* — En revanche, si le corps résiduel contient les racines cubiques de l'unité, les nombres supérieurs de ramification peuvent ne pas être entiers (*cf.* [10], § 4).

# CHAPITRE II.

## Représentations d'Artin et de Swan.

### 5. Rappels sur la théorie des représentations (*cf.* DAG, § 2).

Dans tout ce paragraphe, on désigne par E un corps de caractéristique o, par $\overline{E}$ une clôture algébrique de E et par G un groupe fini.

Une fonction centrale $\chi$ de G à valeurs dans $\overline{E}$ est appelée un *caractère* de G (on dit parfois un *caractère propre*) s'il existe une représentation $\alpha$

de G par des matrices à coefficients dans $\overline{E}$ dont la trace est $\chi$. La représentation $\alpha$ est alors définie par $\chi$ à un isomorphisme près.

Si $\chi$ est un caractère, on appelle *noyau* de $\chi$ le noyau de la représentation définie par $\chi$ et on dit que $\chi$ est fidèle si cette représentation est fidèle. On dit que $\chi$ est *absolument irréductible* si la représentation est irréductible sur $\overline{E}$.

Un caractère $\chi$ de G est dit *rationnel sur* E s'il existe une représentation de G par des matrices à coefficients dans E dont le caractère est $\chi$. Par abus de langage, on dit aussi que la représentation définie par $\chi$ est rationnelle sur E.

Soit $\chi$ un caractère absolument irréductible de G. Soit $m$ le p. g. c. d. des entiers $n$ strictement positifs tels que $n\chi$ soit rationnel sur $E(\chi)$ [on note $E(\chi)$ le corps engendré sur E par les valeurs de $\chi$]. Alors, $m\chi$ est rationnel sur E. L'entier $m$ s'appelle l'*indice de Schur* de $\chi$ sur E et se note $m_E(\chi)$.

Soit $\varphi$ un caractère de G. Pour que $\varphi$ soit rationnel sur E, il faut et il suffit que les conditions suivantes soient réalisées :

(i) le caractère $\varphi$ est à valeurs dans E;

(ii) pour tout caractère absolument irréductible $\chi$ de G, $m_E(\chi)$ divise le produit scalaire $(\varphi, \chi)$.

On dit qu'une algèbre semi-simple est *décomposée* si c'est un produit d'algèbres de matrices sur des corps commutatifs.

L'algèbre E [G] est semi-simple. Elle est décomposée si et seulement si les indices de Schur sur E de tous les caractères absolument irréductibles de G sont égaux à 1. Cela revient à dire que tout caractère de G à valeurs dans E est rationnel sur E.

Soit $\varphi$ un caractère de G à valeurs dans E et soit $\varphi = \sum a_i \chi_i$ sa décomposition canonique en somme de caractères absolument irréductibles $\chi_i$. Soit $n$ un entier $\geqq 1$. On voit que $n\varphi$ est rationnel sur E si et seulement si, pour tout $i$, $m_E(\varphi)$ divise $na_i$. Soit $m$ le p. g. c. d. des entiers $n$ tels que $n\varphi$ est rationnel sur E. Alors, $m\varphi$ est rationnel sur E. L'entier $m$ s'appelle l'*indice de Schur* de $\varphi$ sur E et se note $m_E(\varphi)$.

Si $\varphi$ est un caractère absolument irréductible de G à valeurs dans E, les deux définitions de l'indice de Schur de $\varphi$ sur E coïncident bien. On notera que l'on n'a défini l'indice de Schur sur E d'un caractère $\varphi$ qui n'est pas absolument irréductible que lorsque $\varphi$ est à valeurs dans E.

Soit $\varphi$ un caractère de G à valeurs dans E et soit F une extension finie de E. Si $\varphi$ est rationnel sur F, alors $m_E(\varphi)$ divise le degré de l'extension F/E.

## 6. Définition et décomposition canonique des représentations d'Artin et de Swan.

Dans tout ce paragraphe et dans le suivant, les hypothèses et les notations sont celles du paragraphe 1.

6.1. Définition.

*a. Le cas d'une extension totalement ramifiée.* — Supposons l'extension L/K totalement ramifiée. Considérons les fonctions de G à valeurs dans **Z** définies par

$$(13)\qquad \begin{cases} a_G(s) = -(i_G(s)+1) & \text{si} \quad s \neq 1, \\ a_G(1) = \sum\limits_{s\neq 1} (i_G(s)+1); \end{cases}$$

$$(13')\qquad \begin{cases} sw_G(s) = -i_G(s) & \text{si} \quad s \neq 1, \\ sw_G(1) = \sum\limits_{s\neq 1} i_G(s). \end{cases}$$

On sait (*cf.* CL, th. 1, p. 107) que $a_G$ est un caractère. La représentation définie par $a_G$, à un isomorphisme près, s'appelle la *représentation d'Artin de l'extension* L/K. On en déduit facilement que $sw_G$ est aussi un caractère. La représentation définie par $sw_G$, à un isomorphisme près, a été appelée par Grothendieck la *représentation de Swan de l'extension* L/K (*cf.* [9], n° 19.1). Soit $u_G$ le caractère de la représentation d'augmentation de G (c'est-à-dire du quotient de la représentation régulière par la représentation unité). On voit que $a_G$ et $sw_G$ sont liés par la relation

$$a_G = sw_G + u_G.$$

Remarquons que

$$sw_G(1) = (e_\lambda/e_0 - e_\lambda/e_1)\, i_1 + (e_\lambda/e_1 - e_\lambda/e_2)\, i_2 + \ldots + (e_\lambda/e_{\lambda-1} - e_\lambda/e_\lambda)\, i_\lambda,$$

ou encore, d'après la formule (3) du paragraphe 1,

$$(14)\qquad sw_G(1) = e_\lambda u_\lambda - i_\lambda.$$

*b. Le cas général.* — Revenons au cas général. Désignons par $f$ le degré de l'extension résiduelle. Soit $G_0$ (resp. $L_0$) le groupe (resp. le corps) d'inertie de l'extension. On définit la *représentation d'Artin* (resp. *de Swan*) de l'extension L/K comme la représentation de G induite par la représentation d'Artin (resp. de Swan) de l'extension $L/L_0$.

Il est clair que la restriction de $i_G$ à $G_0$ est $i_{G_0}$. Comme tous les $G_i$ sont invariants dans G, on en déduit que, si $a_G$ (resp. $sw_G$) désigne le caractère de la représentation d'Artin (resp. de Swan) de l'extension L/K, on a

$$a_G(s) = \begin{cases} 0 & \text{si } s \notin G_0, \\ -f(i_G(s)+1) & \text{si } s \in G_0 - \{1\}, \\ f \sum_{s \in G_0 - \{1\}} (i_G(s)+1) & \text{si } s = 1; \end{cases}$$

$$sw_G(s) = \begin{cases} 0 & \text{si } s \notin G_0, \\ -f\, i_G(s) & \text{si } s \in G_0 - \{1\}, \\ f \sum_{s \in G_0 - \{1\}} i_G(s) = f(e_\lambda u_\lambda - i_\lambda) & \text{si } s = 1. \end{cases}$$

## 6.2. Décomposition canonique.

Proposition 6.1. — *Soient, pour* $j = -1, 0, 1, \ldots, \lambda$, $r_j$ *le caractère de* $G_0$ *défini par la représentation régulière de* $G_0/\Gamma_{j+1}$ *et* $r_j^*$ *le caractère de* G *induit apr* $r_j$. *Pour* $j = 0, 1, \ldots, \lambda$, *posons* $\varphi_j = r_j - r_{j-1}$ *et* $\varphi_j^* = r_j^* - r_{j-1}^*$. *Alors :*

(i) *les fonctions* $\varphi_j$ *(resp.* $\varphi_j^*$*) sont des caractères de* $G_0$ *(resp.* G*) deux à deux orthogonaux et* $\varphi_j^*$ *est induit par* $\varphi_j$;

(ii) *on a*

$$sw_{G_0} = \sum u_j \varphi_j, \tag{15}$$

$$a_{G_0} = \sum (u_j + 1)\varphi_j \tag{16}$$

*et*

$$sw_G = \sum u_j \varphi_j^*; \tag{15'}$$

$$a_G = \sum (u_j + 1)\varphi_j^*; \tag{16'}$$

(iii) *pour tout* $j$, $u_j\varphi_j$ *et* $(u_j+1)\varphi_j$ *[resp.* $u_j\varphi_j^*$ *et* $(u_j+1)\varphi_j^*$*] sont des caractères de* $G_0$ *(resp. de* G*).*

*Démonstration :*

(i) Pour tout caractère absolument irréductible $\chi$ de $G_0$, désignons par $d_\chi$ le degré de $\chi$. Soit $X_j$ l'ensemble des caractères absolument irréductibles de $G_0$ dont le noyau contient $\Gamma_{j+1}$. Il est clair que $r_j = \sum_{\chi \in X_j} d_\chi \chi$.

Comme $X_{j-1}$ est contenu dans $X_j$, on en déduit que $\varphi_j = r_j - r_{j-1} = \sum_{\chi \in X_j - X_{j-1}} d_\chi \chi$.

est un caractère. L'orthogonalité des $\varphi_j$ résulte de ce que les ensembles $X_j - X_{j-1}$ sont deux à deux disjoints. Il est clair que les valeurs de $\varphi_j$ sont

$$\varphi_j(s) = \begin{cases} 0 & \text{si } s \notin \Gamma_j, \\ -e_{j-1} & \text{si } s \in \Gamma_j - \Gamma_{j+1}, \\ e_j - e_{j-1} & \text{si } s \in \Gamma_j. \end{cases} \tag{17}$$

Il est évident que $\varphi_j^*$ est le caractère de G induit par $\varphi_j$. Il résulte des valeurs de $\varphi_j$ et de l'invariance de $\Gamma_j$ et $\Gamma_{j+1}$ dans G que la restriction à $G_0$ de $\varphi_j^*$ est égale à $f\varphi_j$. L'orthogonalité des $\varphi_j^*$ résulte alors immédiatement de l'orthogonalité des $\varphi_j$ et de la formule de réciprocité de Frobenius.

(ii) Soit $L_{j+1}$ le corps fixe de $\Gamma_{j+1}$ et soit $sw_j$ (resp. $a_j$) le caractère de $G_0$ défini par la représentation de Swan (resp. d'Artin) de l'extension $L_{j+1}/L_0$. Comme $sw_0 = 0$, on a

$$sw_{G_0} = sw_\lambda = \sum_1^\lambda (sw_j - sw_{j-1}).$$

Pour tout $s \in G$, notons $\bar{s}$ son image canonique dans $G/\Gamma_{j+1}$. Pour tout $s$ n'appartenant pas à $\Gamma_{j+1}$, on a (*cf.* CL, cor. à la prop. 3, p. 71) :

$$i_{G/\Gamma_{j+1}}(\bar{s}) = i_G(s).$$

Avec les notations du paragraphe 1, on a donc

— si $s \in G_0 - \Gamma_{j+1}$, $sw_j(s) = -i_G(s) = sw_{G_0}(s)$;

— si $s \in \Gamma_{j+1}$, $sw_j(s) = \sum_{\substack{t \in G/\Gamma_{j+1} \\ t \neq 1}} i_{G/\Gamma_{j+1}}(t) = e_j u_j - i_j$, d'après (14), puisque (*cf.* CL, cor. à la prop. 3, p. 71 et prop. 14, p. 81) le plus grand nombre de ramification (resp. le plus grand nombre supérieur de ramification) de l'extension $L_{j+1}/L_0$ est $i_j$ (resp. $u_j$).

Comme $u_j = u_{j-1} + (i_j - i_{j-1})/e_{j-1}$, on voit que :

— si $s \in \Gamma_j - \Gamma_{j+1}$,

$$(sw_j - sw_{j-1})(s) = -i_j - (e_{j-1}u_{j-1} - i_{j-1}) = -e_{j-1}u_j;$$

— si $s \in \Gamma_{j+1}$,

$$(sw_j - sw_{j-1})(s) = (e_j u_j - i_j) - (e_{j-1}u_{j-1} - i_{j-1}) = (e_j - e_{j-1})u_j.$$

On a donc

$$(sw_j - sw_{j-1})(s) = \begin{cases} 0 & \text{si } s \notin \Gamma_j, \\ -e_{j-1}u_j & \text{si } s \in \Gamma_j - \Gamma_{j+1}, \\ (e_j - e_{j-1})u_j & \text{si } s \in \Gamma_{j+1}. \end{cases}$$

On en déduit que $sw_j - sw_{j-1} = u_j \varphi_j$ et que, par conséquent, $sw_{G_0} = \sum_0^\lambda u_j \varphi_j$. Comme $a_{G_0} = sw_{G_0} + u_{G_0}$ et comme $u_{G_0} = \sum_0^\lambda \varphi_j$, on voit que $a_{G_0} = \sum_0^\lambda (u_j + 1)\varphi_j$. Les formules donnant $a_G$ et $sw_G$ s'en déduisent trivialement.

(iii) Comme les $\varphi_j$ sont des caractères orthogonaux, le fait que $a_{G_0}$ et $sw_{G_0}$ sont des caractères de $G_0$ entraîne que $u_j \varphi_j$ et $(u_j + 1)\varphi_j$ sont des caractères de $G_0$. Comme $\varphi_j^*$ est induit par $\varphi_j$, $u_j \varphi_j^*$ [resp. $(u_j + 1)\varphi_j^*$] est induit par $u_j\ \varphi_j$ [resp. $(u_j + 1)\ \varphi_j$] et est donc un caractère de G.

C. Q. F. D.

Corollaire. — *Soit* E *un corps de caractéristique* o. *Alors :*

(i) *on a* $m_E(a_G) = m_E(sw_G)$;

(ii) *l'entier* $m_E(sw_G)$ *est le p. p. c. m. des* $m_E(u_j \varphi_j^*)$.

L'assertion (i) résulte de ce que $a_G$ et $sw_G$ diffèrent par le caractère $u_{G_0}^*$ induit par $u_{G_0}$ qui est rationnel sur $\mathbf{Q}$, donc *a fortiori* sur E. L'assertion (ii) résulte de ce que les caractères $u_j \varphi_j^*$ sont orthogonaux et à valeurs dans $\mathbf{Q}$, donc dans E.

*Remarque.* — Si l'extension $L/L_0$ est abélienne, les $u_j$ sont des entiers et les expressions (15′) et (16′) fournissent une interprétation des représentations d'Artin et de Swan qui sont alors rationnelles sur n'importe quel corps de caractéristique o.

## 7. Rationalité des représentations d'Artin et de Swan.

Dans ce paragraphe, les hypothèses et les notations sont les mêmes que dans les paragraphes 1 et 6. En particulier, K est un corps local à corps résiduel de caractéristique $p \neq 0$, L est une extension finie galoisienne de K et on suppose l'extension résiduelle L/K séparable. Au groupe de Galois G de l'extension L/K, on associe la suite

$$G \supset \Gamma_0 \supset \Gamma_1 \supset \ldots \supset \Gamma_\lambda \supset \Gamma_{\lambda+1} = \{1\} \tag{1'}$$

de sous-groupes invariants de G.

On désigne par E un *corps de caractéristique* o.

LEMME 1. — *Soient* J *et* J′ *deux sous-groupes de* G *vérifiant* $\Gamma_1 \subset J' \subset J$. *Posons* $f_J = (J : J \cap \Gamma_0)$ *et* $f_{J'} = (J' : J' \cap \Gamma_0)$. *Alors, avec des notations évidentes,*

(i) *la restriction de* $sw_J$ *à* J′ *est* $(f_J/f_{J'}).sw_{J'}$;

(ii) *le caractère de* J *induit par* $sw_{J'}$ *est* $(J : J').(f_{J'}/f_J).sw_J$.

*Démonstration.* — Posons $J_0 = J \cap \Gamma_0$. Le groupe $J_0$ est le groupe d'inertie de l'extension associée à J. Comme $i_{J_0}(s) = i_G(s)$ et comme $i_G(s) = 0$ si $s \in \Gamma_0 - \Gamma_1$, il résulte du nº 6.1 que

$$sw_{J_0}(s) = \begin{cases} 0 & \text{si } s \notin \Gamma_1, \\ -i_G(s) & \text{si } s \in \Gamma_1 - \{1\}, \\ e_\lambda u_\lambda - i_\lambda & \text{si } s = 1. \end{cases}$$

Comme $sw_J$ est le caractère de J induit par $sw_{J_0}$ et comme les $\Gamma_j$, pour $j \geq 1$, sont invariants dans J, on en déduit que

$$sw_J(s) = \begin{cases} 0 & \text{si } s \notin \Gamma_1, \\ -f_J i_G(s) & \text{si } s \in \Gamma_1 - \{1\}, \\ f_J(e_\lambda u_\lambda - i_\lambda) & \text{si } s = 1 \end{cases}$$

et on a des formules analogues pour $sw_{J'}$. L'assertion (i) est alors immédiate. Si on désigne par $sw^*_{J'}$ le caractère de J induit par $sw_{J'}$, l'assertion (ii) résulte de ce que, comme les $\Gamma_j$, pour $j \geq 1$, sont invariants dans J, on a, pour tout $s \in \Gamma_1$, $sw^*_{J'}(s) = (J : J')\, sw_{J'}(s)$.

C. Q. F. D.

7.1. ÉTUDE DU CAS $p = 2$. — Si $p = 2$, $\Gamma_0$ est un groupe de type $R_2$. On sait (*cf.* DAG, § 7, nº 4) que, pour tout caractère $\chi$ de $\Gamma_0$ à valeurs dans E, $2\chi$ est rationnel sur E. Par conséquent, $m_E(sw_{\Gamma_0})$ est égal à 1 ou 2. Comme $sw_G$ est induit par $sw_{\Gamma_0}$, il en est de même de $sw_G$. On a donc

$$m_E(sw_G) = \begin{cases} 1 & \text{si } sw_G \text{ est rationnel sur E}, \\ 2 & \text{sinon}. \end{cases}$$

*a. Réduction aux 2-extensions.*

PROPOSITION 7.1. — *Supposons* $p = 2$. *Soit* P *un* 2-*sous-groupe de Sylow de* G *et soit* N *le corps fixe de* P. *Les assertions suivantes sont équivalentes :*

(i) *la représentation de Swan de l'extension* L/K *est rationnelle sur* E;

(ii) *la représentation de Swan de l'extension* L/N *est rationnelle sur* E.

*Démonstration.* — Soit $f = 2^r f'$, avec $f'$ impair, le degré de l'extension résiduelle et soit $n = (\Gamma_0 : \Gamma_1)$. On a $P \cap \Gamma_0 = \Gamma_1$ et, avec les notations du lemme 1, $f_P = (P : \Gamma_1) = 2^r$, tandis que $f_G = f$. Enfin $(G : P) = nf'$.

Il résulte du lemme 1 que le caractère de G induit par $sw_P$ est $(nf' \times 2^r/f)\, sw_G = n\, sw_G$. Si $sw_P$ est rationnel sur E, il en est donc de même de $n\, sw_G$. Comme $n$ est impair, $sw_G$ est aussi rationnel sur E et (ii) implique (i).

Il résulte du lemme 1 que la restriction de $sw_G$ à P est $(f/2^r)\, sw_P = f' sw_P$. Si $sw_G$ est rationnel sur E, il en est donc de même de $f' sw_P$. Comme $f'$ est impair, $sw_P$ est aussi rationnel sur E et (i) implique (ii).

C. Q. F. D.

Corollaire. — *Si $p = 2$, les représentations d'Artin et de Swan de l'extension* L/K *sont rationnelles sur toute extension de degré pair de* $\mathbf{Q}_2$.

En effet, on sait (*cf.* DAG, n° 4.2) que, si E est une extension de degré pair de $\mathbf{Q}_2$ et si P est un 2-groupe, l'algèbre E[P] est décomposée.

*b. Réduction aux extensions quaternioniennes.* — Soit P un 2-groupe et soit $\chi$ un caractère absolument irréductible de P. Soit $n$ un entier $\geq 2$. On dit que $\chi$ est *de type* $H_n$ s'il existe un sous-groupe H de P et un caractère absolument irréductible $\xi$ de H, à valeurs dans $\mathbf{Q}(\chi)$, tels que les conditions suivantes soient réalisées :

(18)
- (i) le caractère $\chi$ est induit par $\xi$;
- (ii) le quotient de H par le noyau H' de $\xi$ est isomorphe au groupe des quaternions généralisés d'ordre $2^{n+1}$.

Au corps E, on peut associer un nombre $\mathfrak{r}(E)$ appartenant à $\mathbf{N} \cup \{\infty\}$, supérieur ou égal à 2, qui a la propriété suivante (*cf.* DAG, prop. 4.2) :

*Soit* P *un* 2-*groupe et soit* $\varphi$ *un caractère de* P *à valeurs dans* E. *Pour que* $\varphi$ *soit rationnel sur* E, *il faut et il suffit que, pour tout entier $n$ satisfaisant* $2 \leq n < \mathfrak{r}(E)$, *et pour tout caractère absolument irréductible* $\chi$ *de* P *de type* $H_n$, $(\varphi, \chi)$ *soit pair.*

Revenons à l'extension galoisienne L/K. Supposons que $p = 2$ et que l'extension L/K soit une 2-extension. Soit K' une extension de K contenue dans L et soit L' une extension de K' contenue dans L. Soit $n$ un entier $\geq 2$. On dit que l'extension L'/K' est une $H_n$-*extension associée à l'extension* L/K si l'extension K'/K est totalement ramifiée et si l'extension L'/K' est galoisienne, de groupe de Galois isomorphe au groupe des quaternions généralisés d'ordre $2^{n+1}$. On note G' le groupe de Galois de l'extension L'/K'.

PROPOSITION 7.2. — *Supposons $p = 2$ et supposons que l'extension* L/K *soit une* 2-*extension. Les assertions suivantes sont équivalentes :*

(i) *la représentation d'Artin de l'extension* L/K *est rationnelle sur* E;

(ii) *pour tout entier $n$ vérifiant $2 \leq n < \mathfrak{r}(\mathrm{E})$, pour toute $\mathrm{H}_n$-extension* L'/K' *associée à* L/K, *et pour tout caractère fidèle $\xi$ de* G', *l'entier $(a_{\mathrm{G}'}, \xi)$ est pair.*

*Démonstration.* — Soit K' un corps compris entre K et L et soit H le groupe de Galois de l'extension L/K'. Soit $f'$ le degré de l'extension résiduelle associée à K'/K. Il existe un entier positif $\lambda$ tel que l'on ait (*cf.* CL, prop. 4, p. 108) :

$$\mathrm{Res}_{\mathrm{H}}(a_{\mathrm{G}}) = \lambda\, r_{\mathrm{H}} + f'.a_{\mathrm{H}}. \tag{19}$$

Comme $r_{\mathrm{H}}$ est rationnel sur $\mathbf{Q}$, on en déduit que, si $a_{\mathrm{G}}$ est rationnel sur E, $f'.a_{\mathrm{H}}$ l'est aussi. Si l'extension K'/K est totalement ramifiée, $a_{\mathrm{H}}$ est donc rationnel sur E. Soit H' un sous-groupe invariant de H et soit L' le corps fixe de H'. Posons $\mathrm{G}' = \mathrm{H}/\mathrm{H}'$. On sait (*cf.* CL, prop. 3, p. 108) que, avec les notations de CL, on a $a_{\mathrm{G}'} = a_{\mathrm{H}}^{\natural}$. (Si $a_{\mathrm{H}}$ est le caractère d'une représentation linéaire de H dans un espace vectoriel V sur $\mathbf{C}$, alors $a_{\mathrm{H}}^{\natural}$ est le caractère de la représentation de G' définie par $\mathbf{C}[\mathrm{G}'] \otimes_{\mathbf{C}[\mathrm{H}]} \mathrm{V}$.)

Si $a_{\mathrm{H}}$ est rationnel sur E, $a_{\mathrm{G}'}$ l'est donc aussi. Soit $n$ un entier vérifiant $2 \leq n < \mathfrak{r}(\mathrm{E})$. Supposons que G' soit isomorphe au groupe des quaternions d'ordre $2^{n+1}$. Si $\xi$ est un caractère fidèle de G', $\xi$ est un caractère de type $\mathrm{H}_n$. Si $a_{\mathrm{G}'}$ est rationnel sur E, $(a_{\mathrm{G}'}, \xi)$ doit donc être pair et (i) implique (ii).

Réciproquement, comme $a_{\mathrm{G}}$ est à valeurs dans $\mathbf{Q}$, donc dans E, pour que $a_{\mathrm{G}}$ soit rationnel sur E, il (faut et il) suffit que, pour tout caractère absolument irréductible $\chi$ de G de type $\mathrm{H}_n$, avec $2 \leq n < \mathfrak{r}(\mathrm{E})$, $(a_{\mathrm{G}}, \chi)$ soit pair. Soit $\chi$ un tel caractère. Il existe un sous-groupe H de G et un caractère $\xi$ de H tels que les conditions (18) soient satisfaites.

D'après la formule de réciprocité de Frobenius, on a $(a_{\mathrm{G}}, \chi) = (\mathrm{Res}_{\mathrm{H}}(a_{\mathrm{G}}), \xi)$. Soit K' (resp. L') le corps fixe de H (resp. H') et soit $f'$ le degré de l'extension résiduelle associée à l'extension K'/K. D'après (19), on a

$$\mathrm{Res}_{\mathrm{H}}(a_{\mathrm{G}}) = \lambda\, r_{\mathrm{H}} + f'.a_{\mathrm{H}}.$$

Donc $(a_{\mathrm{G}}, \chi) = \lambda(r_{\mathrm{H}}, \xi) + f'(a_{\mathrm{H}}, \xi)$. Comme $r_{\mathrm{H}}$ est rationnel sur E, 2 divise $(r_{\mathrm{H}}, \xi)$ et la parité de $(a_{\mathrm{G}}, \chi)$ est égale à celle de $f'(a_{\mathrm{H}}, \xi)$. Si l'extension K'/K n'est pas totalement ramifiée, 2 divise $f'$ et, par conséquent, $(a_{\mathrm{G}}, \chi)$ est pair. Si l'extension K'/K est totalement ramifiée, l'extension L'/K' est une $\mathrm{H}_n$-extension associée à L/K. Comme $a_{\mathrm{H}/\mathrm{H}'} = a_{\mathrm{H}}^{\natural}$ et comme le noyau de $\xi$ est H', il résulte de la formule de réciprocité de Frobenius que $(a_{\mathrm{H}}, \xi) = (a_{\mathrm{H/H'}}, \xi)$. Si $(a_{\mathrm{H/H'}}, \xi)$ est pair, $(a_{\mathrm{G}}, \chi)$ l'est aussi et (ii) implique (i).

C. Q. F. D.

*c. Le cas des extensions quaternioniennes.*

PROPOSITION 7.3. — *Supposons* $p = 2$. *Soit* $n$ *un entier* $\geqq 2$. *Supposons le groupe de Galois* G *de l'extension* L/K *isomorphe au groupe des quaternions généralisé d'ordre* $2^{n+1}$. *Soit* $\chi$ *un caractère absolument irréductible et fidèle de* G. *Alors :*

(i) *si l'extension* L/K *est non ramifiée,* $(a_{\mathrm{G}}, \chi) = 0$;

(ii) *si l'extension* L/K *est ramifiée,* $(a_{\mathrm{G}}, \chi)$ *est pair si et seulement si le plus grand nombre supérieur de ramification de l'extension est un entier.*

*Démonstration.* — Soit A un sous-groupe cyclique de G d'indice 2. Il est invariant dans G (son choix est d'ailleurs unique, sauf dans le cas $n = 2$). Soit $\xi$ un caractère fidèle de degré 1 de A et soit $\chi$ le caractère de G induit par $\xi$. Il est clair que $\chi$ est de type $\mathrm{H}_n$, que ses valeurs sont

$$\chi(s) = \begin{cases} 0 & \text{si } s \notin \mathrm{A}, \\ \xi(s) + (\xi(s))^{-1} & \text{si } s \in \mathrm{A} \end{cases}$$

et que tout caractère de G de type $\mathrm{H}_n$ est de ce type.

Soit $\omega$ une racine primitive $2^n$-ième de l'unité. Le corps $\mathbf{Q}(\omega + \omega^{-1})$ est de degré $2^{n-2}$ sur $\mathbf{Q}$ et on en déduit que le caractère $\chi$ a $2^{n-2}$ conjugués distincts. Comme $sw_{\mathrm{G}}$ est à valeurs dans $\mathbf{Q}$, si $\chi'$ est un caractère conjugué de $\chi$, on a $(sw_{\mathrm{G}}, \chi') = (sw_{\mathrm{G}}, \chi)$. Si $\varphi$ désigne le caractère de G qui est la somme de tous les conjugués distincts de $\chi$, on a donc $(sw_{\mathrm{G}}, \varphi) = 2^{n-2}(sw_{\mathrm{G}}, \chi)$.

Soit $c$ l'unique élément de G d'ordre 2. On vérifie facilement que

$$\varphi(s) = \begin{cases} 0 & \text{si } s \notin \{1, c\}, \\ -2^{n-1} & \text{si } s = c, \\ 2^{n-1} & \text{si } s = 1. \end{cases}$$

On a donc

$$(sw_{\mathrm{G}}, \varphi) = 2^{-(n+1)}(2^{n-1} sw_{\mathrm{G}}(1) - 2^{n-1} sw_{\mathrm{G}}(c)) = 2^{-2}(sw_{\mathrm{G}}(1) - sw_{\mathrm{G}}(c))$$

et

$$(sw_{\mathrm{G}}, \chi) = 2^{-n}(sw_{\mathrm{G}}(1) - sw_{\mathrm{G}}(c)).$$

Si l'extension L/K est non ramifiée, on a $a_{\mathrm{G}} = 0$. Par conséquent, $(a_{\mathrm{G}}, \chi) = 0$ et l'assertion (i) est établie.

Supposons l'extension L/K ramifiée. Soit $e$ son indice de ramification et soit $f$ le degré de l'extension résiduelle. Soit $i_\lambda$ (resp. $u_\lambda$) le plus grand nombre (resp. nombre supérieur) de ramification de l'extension L/K. Comme $c$ est l'unique élément de G d'ordre 2, on a $i_G(c) = i_\lambda$. La formule (14) du n° 6.1 montre que

$$\begin{cases} sw_G(1) = f(e_\lambda u_\lambda - i_\lambda), \\ sw_G(u) = -fi_\lambda. \end{cases}$$

Par conséquent, $(sw_G, \chi) = 2^{-n}(f(e_\lambda u_\lambda - i_\lambda) - (-fi_\lambda)) = 2^{-n}fe_\lambda u_\lambda$. Comme $fe_\lambda$ est le degré de l'extension, on a $(sw_G, \chi) = 2\, u_\lambda$. On voit que $(sw_G, \chi)$ est pair si et seulement si $u_\lambda$ est un entier. L'assertion (ii) résulte alors de ce que $(sw_G, \chi)$ et $(a_G, \chi)$ ont la même parité.

C. Q. F. D.

*d. Une application.*

Proposition 7.4. — *Supposons que $p = 2$ et supposons que le corps résiduel de* K *ne contienne pas les racines cubiques de l'unité. Alors, les représentations d'Artin et de Swan de l'extension* L/K *sont rationnelles sur* $\mathbf{Q}_2$.

*Démonstration.* — Soit P un 2-sous-groupe de Sylow du groupe de Galois G de l'extension et soit N le corps fixe de P. Soit $k$ le corps résiduel de K. L'extension $k(\sqrt[3]{1})/k$ étant de degré 2 et l'extension N/K étant de degré impair, le corps résiduel de N ne contient pas les racines cubiques de l'unité. Il résulte donc de la proposition 7.1 qu'il suffit de démontrer la proposition 7.4 lorsque l'extension L/K est une 2-extension. Comme $\mathfrak{r}(\mathbf{Q}_2) = 3$ (*cf.* DAG, n° 4.2), il suffit de montrer (*cf.* propositions 7.2 et 7.3) que le plus grand nombre de ramification $u_\lambda$ de toute $H_4$-extension L'/K' ramifiée associée à l'extension L/K est un entier. Si l'extension L'/K' n'est pas totalement ramifiée, son groupe d'inertie est un sous-groupe propre du groupe des quaternions usuels et est donc abélien. Par conséquent, $u_\lambda$ est entier. Si l'extension L'/K' est totalement ramifiée, le corps résiduel de K', étant le même que celui de K, ne contient pas les racines cubiques de l'unité. Donc, d'après le corollaire à la proposition 4.5, $u_\lambda$ est un entier.

C. Q. F. D.

7.2. Réduction aux bonnes extensions. — Supposons maintenant $p \neq 2$.

Soit $f$ le degré de l'extension résiduelle L/K. On a $f = (G : \Gamma_0)$. Pour tout nombre premier $l$ choisissons un $l$-sous-groupe de Sylow $\overline{G}(l)$ de $G/\Gamma_0$. Soit $G(l)$ l'image réciproque de $\overline{G}(l)$ dans G. Soit $K(l)$ le corps fixe de $G(l)$. L'extension $L/K(l)$ est une extension galoisienne dont l'extension résiduelle est une $l$-extension. Pour $l$ différent de $p$, l'extension résiduelle est donc de degré premier à $p$ et l'extension $L/K(l)$ est une bonne extension (*cf.* nº 1.3). Enfin, pour tout nombre premier $l$ ne divisant pas $f$, on a évidemment $\overline{G}(l) = \{1\}$ et, par conséquent, $G(l) = \Gamma_0$ et $K(l) = L_0$. Désignons par $sw_{(l)}$ le caractère de la représentation de Swan de l'extension $L/K(l)$.

Proposition 7.5. — *Supposons $p \neq 2$. Alors, $m_E(sw_G)$ est le p. g. c. d. de $m_E(sw_{\Gamma_0})$ et des $m_E(sw_{(l)})$ pour $l$ divisant $f$ et différent de $p$.*

*Démonstration.* — Pour tout nombre premier $l$ (y compris $l = p$), soit $m_l$ l'indice de Schur de $sw_{(l)}$ sur E et soit $f_l$ l'indice de $G(l)$ dans G. Soit $m$ l'indice de Schur de $sw_G$ sur E.

Il résulte du lemme 1 que $sw_G$ est induit par $sw_{(l)}$. Par conséquent, comme $m_l sw_{(l)}$ est rationnel sur E, $m_l sw_G$ est rationnel sur E et $m$ divise $m_l$. Donc $m$ divise le p. g. c. d. des $m_l$, pour tout $l$.

D'après le lemme 1, la restriction de $sw_G$ à $G(l)$ est $f_l sw_{(l)}$. Comme $m.sw_G$ est rationnel sur E, $m.f_l sw_{(l)}$ est rationnel sur E. Donc $m_l$ divise $m.f_l$. Comme $f_l$ est premier à $l$, on en déduit que la $l$-composante de $m_l$ divise la $l$-composante de $m$. Par conséquent, le p. g. c. d. des $m_l$, pour tout $l$, divise $m$.

Finalement, $m$ est le p. g. c. d. des $m_l$, pour tout $l$. Pour achever la démonstration de la proposition 7.5, il suffit donc d'établir le lemme suivant :

Lemme 2. — *Pour tout nombre premier $l$ ne divisant pas $f$ et pour $l = p$, on a $m_E(sw_{(l)}) = m_E(sw_{\Gamma_0})$.*

*Démonstration.* — Pour $l$ ne divisant pas $f$, c'est évident car $sw_{(l)} = sw_{\Gamma_0}$.

Le groupe $\Gamma_0$ étant de type $R_p$, avec $p \neq 2$, l'indice de Schur sur E de tout caractère de $\Gamma_0$ à valeurs dans E divise $(\Gamma_0 : \Gamma_1)$ (*cf.* DAG, prop. 7.1 et cor. à la prop. 6.6) et est donc premier à $p$. Par conséquent, $m_E(sw_{\Gamma_0})$ est premier à $p$. Comme la restriction à $\Gamma_0$ de $sw_{(p)}$ est égale au produit d'une puissance de $p$ par $sw_{\Gamma_0}$, on en déduit que $m_E(sw_{(p)}) = m_E(sw_{\Gamma_0})$.

C. Q. F. D.

## 7.3. Réduction aux $C'_p$-extensions.

Proposition 7.6. — *Supposons $p \neq 2$. Supposons que l'extension $L/K$ soit une bonne extension. Soit $(L_{j+1}/K_j)_{j=1,2,\ldots,\lambda}$ un système complet de $C'_p$-extensions associées à l'extension $L/K$. Soit $sw^j$ le caractère de la repré-*

*sentation de Swan de l'extension* $L_{j+1}/K_j$. *Alors* $m_E(sw_G)$ *est le p. p. c. m. des* $m_E(sw^j)$.

*Démonstration.* — D'après le corollaire à la proposition 6.1, $m_E(sw_G)$ est le p. p. c. m. des $m_E(u_j\varphi_j^*)$ (*cf.* prop. 6.1 pour la définition des $\varphi_j$ et des $\varphi_j^*$). Il suffit donc d'établir le résultat suivant :

LEMME 3. — *Pour tout* $j$, *on a* $m_E(sw_j) = m_E(u_j\varphi_j^*)$.

*Démonstration.* — Le caractère $u_j\varphi_j^*$ est le caractère d'une représentation de $G/\Gamma_{j+1}$ et le caractère $sw^j$ est le caractère d'une représentation du sous-groupe $A_j = H.\Gamma_j/\Gamma_{j+1}$. (Rappelons que le groupe H a été défini, lors de l'introduction de la notion de « bonne extension », au n° 1.3, comme un sous-groupe de G tel que G s'identifie au produit semi-direct de H par $\Gamma_1$.) Quitte à passer au quotient, on peut donc supposer que $\Gamma_{j+1} = \{1\}$. Soit $f$ le degré de l'extension résiduelle associée à L/K. Si on pose $H_0 = H \cap \Gamma_0$, on a $f = (G : \Gamma_0) = (H : H_0)$. Il résulte de la formule (17) du n° 6.2 et de l'invariance de $\Gamma_j$ dans $A_j$ que l'on a [en posant $e_j = (\Gamma_0 : 1)$, $e_{j-1} = (\Gamma_0 : \Gamma_j)$]

$$u_j\varphi_j^*(s) = \begin{cases} 0 & \text{si } s \notin \Gamma_j, \\ -fu_j e_{j-1} & \text{si } s \in \Gamma_j - \{1\}, \\ fu_j(e_j - e_{j-1}) & \text{si } s = 1. \end{cases}$$

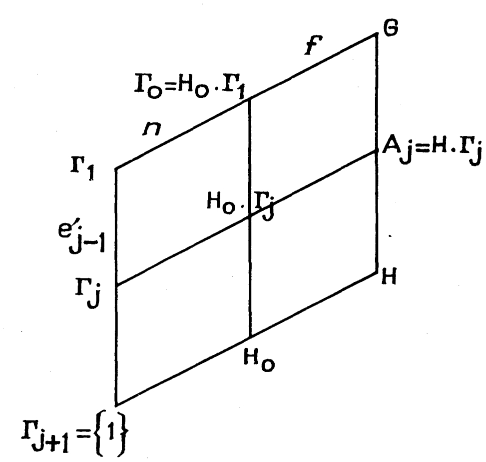


Fig. 4.

Soit $R_j$ le caractère de la représentation régulière de $H_0.\Gamma_j$ et soit $\overline{R}_j$ le caractère de $H_0.\Gamma_j$ défini par la représentation régulière de $H_0.\Gamma_j/\Gamma_j$. Soit $\Phi_j = R_j - \overline{R}_j$ et soit $\Phi_j^*$ le caractère de $A_j$ induit par $\Phi_j$. Il est clair que $\Phi_j^*$ est rationnel sur $\mathbf{Q}$ et, comme $\Gamma_j$ est invariant dans $A_j$, on voit que ses valeurs sont [en posant $n=(\Gamma_0:\Gamma_1)=(H_0:1)$]

$$\Phi_j^*(s)=\begin{cases} 0 & \text{si } s\notin\Gamma_j,\\ -fn & \text{si } s\in\Gamma_j-\{1\},\\ fn(e_j/e_{j-1}-1) & \text{si } s=1.\end{cases}$$

Appliquons la proposition 6.1 à l'extension $L_{j+1}/K_j$. Cette extension a un seul nombre de ramification $>0$ qui est $i_j$ et son unique nombre supérieur de ramification $>0$ est $\varphi_{L_{j+1}/K_j}(i_j)=i_j/n$. La formule (15') montre donc que $sw^j=(i_j/n)\Phi_j^*$.

Posons $e'_{j-1}=e_{j-1}/n=(\Gamma_1:\Gamma_j)$. On voit que

$$sw^j=(i_j/n)\Phi_j^*=e'_{j-1}u_j\Phi_j^*-(e'_{j-1}u_j-i_j/n)\Phi_j^*.$$

Comme $e'_{j-1}u_j-i_j/n$ est entier (*cf.* prop. 1.3) et comme $\Phi_j^*$ est rationnel sur $\mathbf{Q}$, on en déduit que $m_E(sw^j)=m_E(e'_{j-1}u_j\Phi_j^*)$. Il suffit donc de montrer que

$$m_E(e'_{j-1}u_j\Phi_j^*)=m_E(u_j\varphi_j^*).$$

Comme la restriction de $u_j\varphi_j^*$ à $A_j$ est $e'_{j-1}u_j\Phi_j^*$, $m_E(e'_{j-1}u_j\Phi_j^*)$ divise $m_E(u_j\varphi_j^*)$.

Comme $(G:A_j)=e'_{j-1}$ et comme $\Gamma_j$ est invariant dans G, le caractère de G induit par $e'_{j-1}u_j\Phi_j^*$ est $e'_{j-1}u_j\varphi_j^*$. Donc $m_E(e'_{j-1}u_j\varphi_j^*)$ divise $m_E(e'_{j-1}u_j\Phi_j^*)$.

Or (*cf.* prop. 6.1) $u_j\varphi_j$ est un caractère de $\Gamma_0$ à valeurs dans E et $\Gamma_0$ est un groupe de type $R_p$, avec $p\neq 2$. Il en résulte (*cf.* DAG, prop. 7.1 et cor. à la prop. 6.6) que $m_E(u_j\varphi_j)$ est premier à $p$. Comme $u_j\varphi_j^*$ est induit par $u_j\varphi_j$, il en est de même de $m_E(u_j\varphi_j^*)$. Comme $e'_{j-1}$ est une puissance de $p$, on a donc $m_E(e'_{j-1}u_j\varphi_j^*)=m_E(u_j\varphi_j^*)$ et $m_E(u_j\varphi_j^*)$ divise $m_E(e'_{j-1}u_j\Phi_j^*)$.

Finalement, $m_E(e'_{j-1}u_j\Phi_j^*)=m_E(u_j\varphi_j^*)$.

C. Q. F. D.

## 7.4. Le cas des extensions totalement ramifiées.

Théorème 1. — *Supposons $p\neq 2$. Supposons l'extension* L/K *totalement ramifiée. Soit* $(A_j)_{j=1,2,\ldots,\lambda}$ *un système complet de groupes de type* $C_p$ *associés à* G (*cf.* n° 1.1). *Les assertions suivantes sont équivalentes :*

(i) *la représentation d'Artin (ou de Swan) de l'extension* L/K *est rationnelle sur* E;

(ii) *l'algèbre* E[G] *est décomposée;*

(iii) *pour* $j=1, 2, \ldots, \lambda$, *l'algèbre* $E[A_j]$ *est décomposée.*

*Démonstration.* — L'équivalence des assertions (ii) et (iii) a été démontrée dans DAG (§ 7, théorème 5) et il est clair que (ii) entraîne (i). Il suffit donc de montrer que (i) implique (ii) ou (iii) pour un choix particulier des $A_j$.

Commençons par le cas particulier où l'extension L/K est une $C_p$-extension (*cf.* n° 1.3). Soient alors P le $p$-sous-groupe de Sylow de G et $i$ l'unique nombre de ramification $>$ o de l'extension. Il est clair que les valeurs de $sw_G$ sont

$$sw_G(s) = \begin{cases} 0 & \text{si } s \notin P, \\ -i & \text{si } s \in P - \{1\}, \\ i(q-1) & \text{si } s = 1, \end{cases}$$

en désignant par $q$ l'ordre de P. Posons $m(G) = m$ et $d(G) = d$ (*cf.* n° 1.1). Soit $\theta_G$ la fonction centrale sur G à valeurs dans $\mathbf{Z}$ définie par

$$\theta_G(s) = \begin{cases} 0 & \text{si } s \notin P, \\ -m & \text{si } s \in P - \{1\}, \\ m(q-1) & \text{si } s = 1. \end{cases}$$

On sait (*cf.* DAG, prop. 6.4) que $\theta_G$ est un caractère de G, à valeurs dans $\mathbf{Q}$, et que $\theta_G$ est rationnel sur E si et seulement si l'algèbre E [G] est décomposée. On voit que $sw_G = (i/m)\,\theta_G$. Comme $i/m$ est un entier premier à $d$ (*cf.* prop. 1.2) et comme l'indice de Schur de $\theta_G$ divise $d$ (*cf.* DAG, cor. à la prop. 6.6), on en déduit que $sw_G$ est rationnel sur E si et seulement si $\theta_G$ l'est, donc si et seulement si l'algèbre E [G] est décomposée.

*Revenons au cas général.* — Soit $(L_{j+1}/K_j)_{j=1,2,\ldots,\lambda}$ un système complet de $C_p$-extensions associées à l'extension L/K et soit $A_j$ le groupe de Galois de l'extension $L_{j+1}/K_j$. La famille des $A_j$ est un système complet de groupes de type $C_p$ associé à G. Soit $sw^j$ le caractère de la représentation de Swan de l'extension $L_{j+1}/K_j$. Il résulte de la proposition 7.6 que, si $sw_G$ est rationnel sur E, chaque $sw^j$ est rationnel sur E. On vient de voir que ceci entraîne que l'algèbre E $[A_j]$ est décomposée. Donc (i) implique (iii) pour ce choix particulier des $A_j$.

C. Q. F. D.

Étant donné un corps E de caractéristique o et un groupe G de type $R_p$, on sait à quelles conditions l'algèbre E [G] est décomposée (*cf.* DAG, th. 4 et 5). Le théorème 1 résoud donc complètement le problème de la rationalité des représentations d'Artin et de Swan dans le cas où $p \neq 2$ et où l'extension est totalement ramifiée. Le résultat suivant avait été conjecturé par Serre :

PROPOSITION 7.7. — *Soit $k$ le corps résiduel de* K *et soit $k_0$ la fermeture algébrique de $\mathbf{F}_p$ dans $k$. Soit* $W(k_0)$ *le corps des vecteurs de Witt sur $k_0$. Soit* L *une extension finie galoisienne totalement ramifiée de* K. *Les représentations d'Artin et de Swan de l'extension* L/K *sont rationnelles sur* $W(k_0)$.

*Démonstration :*

(*a*) Si $p \neq 2$, on sait (*cf.* prop. 1.1) que $k$ contient les racines $n^{\text{ièmes}}$ de l'unité [avec $n = (\Gamma_0 : \Gamma_1)$]. Il en est donc de même de $k_0$ et de $W(k_0)$. On en déduit que l'algèbre $W(k_0)[G]$ est décomposée (*cf.* DAG, § 6, cor. 5 au th. 4 et § 7, th. 5).

(*b*) Si $p = 2$ et si $k$ contient les racines cubiques de l'unité, $k_0$ et $W(k_0)$ les contiennent aussi. Le corps $W(k_0)$ est donc une extension de $\mathbf{Q}_2(\sqrt[3]{1})$. Les représentations d'Artin et de Swan de L/K sont rationnelles sur $\mathbf{Q}_2(\sqrt[3]{1})$ (cor. à la prop. 7.1), donc *a fortiori* sur $W(k_0)$.

(*c*) Si $p = 2$ et si $k$ ne contient pas les racines cubiques de l'unité, les représentations d'Artin et de Swan de L/K sont rationnelles sur $\mathbf{Q}_2$ (prop. 7.4), donc *a fortiori* sur $W(k_0)$ qui est une extension de $\mathbf{Q}_2$.

C. Q. F. D.

7.5. RATIONALITÉ SUR LE CORPS DES VECTEURS DE WITT. — Nous nous proposons, pour terminer, de donner un résultat analogue à celui de la proposition 7.7 qui soit valable dans le cas général.

THÉORÈME 2. — *Soit* K′ *un corps local de caractéristique* 0 *qui a le même corps résiduel que* K. *Alors les représentations d'Artin et de Swan de l'extension* L/K *sont rationnelles sur* K′.

Avant de démontrer ce théorème, remarquons qu'il admet le corollaire suivant :

COROLLAIRE. — *Supposons le corps résiduel* $\tilde{\mathrm{K}}$ *de* K *parfait. Alors les représentations d'Artin et de Swan de l'extension* L/K *sont rationnelles sur le corps des vecteurs de Witt de* $\tilde{\mathrm{K}}$.

*Démonstration du théorème* 2. — Remarquons que, lorsque $p = 2$, le théorème 2 se démontre de la même manière que la proposition 7.7. Supposons donc $p \neq 2$. Nous allons décomposer la démonstration du théorème en trois parties.

(*a*) *Un lemme préliminaire.*

LEMME 4. — *Soit* $K'$ *un corps local de caractéristique* o. *Soit* $L'$ *une extension finie galoisienne modérément ramifiée de* $K'$. *Soit* J *le groupe de Galois de l'extension et soit* A *son groupe d'inertie. Soit* $\eta$ *un caractère de* J *induit par un caractère* $\xi$ *de* A. *Alors,* $\eta$ *est rationnel sur* $K'$.

*Démonstration.* — Soit $L'_0$ le corps fixe de A et soit G le groupe de Galois de l'extension $L'_0/K'$. On a la suite exacte

$$1 \to A \to J \to G \to 1.$$

Soit S une section de G dans J et soit $\varepsilon$ le 2-cocycle de G à valeurs dans A correspondant à S. On sait (prop. 2.3) que $\theta_0$ est un G-isomorphisme de A sur un sous-groupe du groupe multiplicatif de $L'_0$ et qu'il existe une application $\lambda$ de G dans $L'_0$ telle que, pour tout couple $g$, $g'$ d'éléments de G, on a $\theta_0(\varepsilon_{g,g'}) = g(\lambda_{g'})\lambda_g\lambda_{gg'}^{-1}$.

Il est clair qu'il suffit de démontrer le lemme lorsque $\xi$ est de degré 1. Il existe alors un entier $i \geqq 0$ tel que $\xi = \theta_0^i$. Soit $f$ le degré de l'extension $L'_0/K'$. Le corps $L'_0$ est un espace vectoriel de dimension $f$ sur $K'$. Nous allons faire opérer le groupe J sur $L'_0$ de la manière suivante :

— pour $h \in A$, $h.\alpha = \xi(h)\alpha$;
— pour $g \in G$, $S_g.\alpha = \lambda_g^i g(\alpha)$;
— pour $s \in J$, de la forme $s = hS_g$, avec $h \in A$ et $g \in G$, $hS_g.\alpha = h.(S_g.\alpha)$.

D'une part, $S_g.(h.\alpha) = S_g.(\xi(h)\alpha) = \lambda_g^i g.(\xi(h)).g(\alpha)$. Or

$$S_g h = S_g h S_g^{-1} S_g = g(h) S_g \quad \text{et} \quad S_g h.\alpha = g(h).(S_g.\alpha) = \lambda_g^i \xi(g(h)) g(\alpha).$$

On en déduit que $S_g.(h.\alpha) = S_g h.\alpha$ puisque $\xi = \theta_0^i$ est, comme $\theta_0$, un G-isomorphisme.

D'autre part, $S_g.(S_{g'}.\alpha) = S_g.(\lambda_{g'}^i g'(\alpha)) = \lambda_g^i g(\lambda_{g'}^i) gg'(\alpha)$. Or

$$S_g S_{g'} = \varepsilon_{g,g'} S_{gg'} \quad \text{et} \quad S_g S_{g'}.\alpha = \varepsilon_{g,g'}.(S_{gg'}.\alpha) = \xi(\varepsilon_{g,g'})\lambda_{gg'}^i gg'(\alpha).$$

On a donc $S_g.(S_{g'}.\alpha) = S_g S_{g'}.\alpha$.

Comme, pour $s \in J$ et pour $a \in K'$, on a $s.(a\alpha) = a(s.\alpha)$, on a ainsi muni $L'_0$ d'une structure de $K'[J]$-module. Soit $\eta'$ le caractère de la représentation de J ainsi définie. Pour $h \in A$ et $g \in G$, $\eta'(hS_g)$ est la trace de l'application $\alpha \mapsto \xi(h)\lambda_g^i g(\alpha)$. Or on vérifie que, pour tout $\lambda$ dans $L'_0$, la trace de l'application $\alpha \mapsto \lambda g(\alpha)$ est o si $g \neq 1$ et $\mathrm{Tr}_{L'_0/K'}(\lambda)$ si $g = 1$. On a donc

$$\eta'(hS_g) = \begin{cases} 0 & \text{si } g \neq 1, \\ \mathrm{Tr}_{L'_0/K'}(\xi(h)) = \sum_{g \in G} \xi(ghg^{-1}) \end{cases}$$

et le caractère $\eta'$, qui est rationnel sur K', est égal au caractère $\eta$ de J induit par $\xi$.

C. Q. F. D.

($b$) *Le cas d'une* $C'_p$*-extension.*

LEMME 5. — *Le théorème 2 est vrai dans le cas où l'extension* L/K *est une* $C'_p$*-extension.*

*Démonstration.* — On a alors (*cf.* n° 1.3) $\Gamma_2 = \{1\}$ et le groupe de Galois de l'extension est le produit semi-direct d'un groupe H isomorphe à $G/\Gamma_1$ par le groupe $P = \Gamma_1$.

Faisons opérer G sur P de la manière suivante :

— le groupe P opère sur lui-même par les translations : $s : \sigma \mapsto s\sigma$;

— le groupe H opère sur P par les automorphismes intérieurs :

$$h : \quad \sigma \mapsto h\sigma h^{-1}.$$

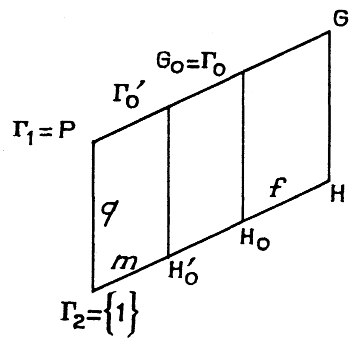


Fig. 5.

On en déduit une représentation de G sur l'espace vectoriel des fonctions sur P à valeurs dans **Q**. Soit $\varphi$ le caractère de cette représentation. Pour tout $g$ dans G de la forme $g = hs$, avec $h \in H$ et $s \in P$, $\varphi(g)$ est égal au nombre de solutions dans P de l'équation en $\sigma hs\sigma : h^{-1} = \sigma$ ou $\sigma^{h^{-1}} = s$. Soit $H_0 = H \cap \Gamma_0$ et soit $H'_0$ le noyau de la représentation canonique de $H_0$ dans P. On vérifie immédiatement que, pour tout $h$ appartenant à $H_0 - H'_0$, l'application $\sigma \mapsto \sigma^{h-1}$ est un automorphisme de P. Soit $q$ l'ordre de P. On voit que les valeurs de la restriction de $\varphi$ à $H_0 . P$ sont

$$\varphi(s) = \begin{cases} 1 & \text{pour} \quad s \in H_0 . P - H'_0 . P, \\ 0 & \text{pour} \quad s \in H'_0 . P - H'_0, \\ q & \text{pour} \quad s \in H'_0. \end{cases}$$

Soit $\chi$ le caractère du quotient de la représentation définie par $\varphi$ par la représentation unité de G. On voit que $\chi$ est un caractère rationnel sur **Q** et que les valeurs de la restriction de $\chi$ à $H_0.P$ sont

$$\chi(s)=\begin{cases} 0 & \text{pour } s\in H_0.P-H'_0.P, \\ -1 & \text{pour } s\in H'_0.P-H'_0, \\ q-1 & \text{pour } s\in H'_0. \end{cases}$$

Le groupe $\Gamma_0 = H_0.P$ est de type $C_p$. Posons $m = m(\Gamma_0) = (H'_0 : 1)$. Soit $\xi_1$ un caractère fidèle de degré 1 de $\Gamma_0/P$ et soit $\xi = \sum_{j=1}^{m} \xi_1^j$.

Montrons d'abord que le caractère $\eta$ de G/P induit par $\xi$ est rationnel sur K'.

Soit $\tilde{L}$ (resp. $\tilde{K}$) le corps résiduel de L (resp. K). Soit $L'_0$ une extension galoisienne non ramifiée de K' telle que le corps résiduel de $L'_0$ soit $\tilde{K}$-isomorphe à $\tilde{L}$. Si on les identifie, le groupe de Galois de l'extension $L'_0/K'$ est canoniquement isomorphe à $G/\Gamma_0$. Soit $\varepsilon$ l'élément de $H^2(G/\Gamma_0, \Gamma_0/P)$ associé à la suite exacte

$$1 \to \Gamma_0/P \to G/P \to G/\Gamma_0 \to 1.$$

L'image de $\varepsilon$ par l'application $\theta_0$ s'annule dans $H^2(L_0/K)$ (*cf.* prop. 2.2). Donc $\theta_0(\varepsilon)$ s'annule dans $H^2(\tilde{L}/\tilde{K})$ et aussi dans $H^2(L'_0/K')$ (*cf.* prop. 2.1). On peut donc construire, d'après la proposition 2.3, une extension modérément ramifiée L' de K' contenant $L'_0$ qui est associée à la suite exacte

$$1 \to \Gamma_0/P \to G/P \to G/\Gamma_0 \to 1$$

et dont le groupe d'inertie s'identifie à $\Gamma_0/P$. Donc, d'après le lemme 4, $\eta$ est rationnel sur K'.

Il est clair que la restriction de $\xi$ à $\Gamma'_0/P = H'_0.P/P$ est le caractère de la représentation régulière de $\Gamma'_0/P$. Soit $f$ le degré de l'extension résiduelle L/K. Comme $\Gamma'_0/P$ et $\Gamma_0/P$ sont invariants dans G/P, on voit que

$$\eta(s)=\begin{cases} 0 & \text{pour } s\notin\Gamma_0, \\ ? & \text{pour } s\in\Gamma_0-\Gamma'_0, \\ 0 & \text{pour } s\in\Gamma'_0-P, \\ mf & \text{pour } s\in P, \end{cases}$$

en notant encore $\eta$ le caractère de G défini par $\eta$.

Soit $\psi = \chi\eta$. Le caractère $\psi$ est rationnel sur K′ et l'on a

$$\psi(s) = \begin{cases} 0 & \text{pour } s \notin \mathrm{P}, \\ -mf & \text{pour } s \in \mathrm{P} - \{1\}, \\ mf(q-1) & \text{pour } s = 1. \end{cases}$$

Soit $i$ l'unique nombre de ramification $> 0$ de l'extension. Il résulte de la définition de la représentation de Swan que les valeurs de $sw_{\mathrm{G}}$ sont

$$sw_{\mathrm{G}}(s) = \begin{cases} 0 & \text{pour } s \notin \mathrm{P}, \\ -fi & \text{pour } s \in \mathrm{P} - \{1\}, \\ fi(q-1) & \text{pour } s = 1. \end{cases}$$

On a donc $sw_{\mathrm{G}} = (i/m)\psi$. Comme $i/m$ est un entier naturel (prop. 1.2), on voit que $sw_{\mathrm{G}}$ est aussi rationnel sur K′. C. Q. F. D.

(*c*) *Fin de la démonstration du théorème* 2. — Supposons d'abord que l'extension L/K soit une bonne extension. Soit $\mathrm{L}_{j+1}/\mathrm{K}_j$ une $\mathrm{C}'_p$-extension associée à L/K. Il est clair que le corps résiduel de $\mathrm{K}_j$ est le même que celui de K, donc que celui de K′ et, d'après le lemme 5, la représentation de Swan de l'extension $\mathrm{L}_{j+1}/\mathrm{K}_j$ est rationnelle sur K′. Comme ceci est vrai pour tout $j$, il résulte de la proposition 7.6 que la représentation de Swan de l'extension L/K est rationnelle sur K′.

Enfin, si l'extension L/K est quelconque, il existe une extension $\mathrm{L}'_0$ de K′ de degré $f$ dont le corps résiduel est le même que celui de L et $sw_{\Gamma_0}$ est rationnel sur $\mathrm{L}'_0$. Donc, $m_{\mathrm{K}'}(sw_{\Gamma_0})$ divise $f$.

Soit $l$ un nombre premier divisant $f$ différent de $p$. Soit, comme au n° 7.2, $\overline{\mathrm{G}}(l)$ un $l$-sous-groupe de Sylow de $\mathrm{G}/\Gamma_0$ et soit $\mathrm{G}(l)$ l'image réciproque de $\overline{\mathrm{G}}(l)$ dans G. Soit $\mathrm{K}(l)$ le corps fixe de $\mathrm{G}(l)$. L'extension $\mathrm{L}/\mathrm{K}(l)$ est une bonne extension. Il est clair qu'il existe une extension $\mathrm{M}_l$ de K′ de degré premier à $l$ qui a même corps résiduel que $\mathrm{K}(l)$. D'après ce qui précède, $sw_{(l)}$ est rationnel sur $\mathrm{M}_l$ et $m_{\mathrm{K}'}(sw_{(l)})$ est premier à $l$.

On a vu que $m_{\mathrm{K}'}(sw_{\Gamma_0})$ est premier à $p$. Comme $m_{\mathrm{K}'}(sw_{\Gamma_0})$ divise $f$ et comme pour tout nombre premier $l$ divisant $f$ et différent de $p$, $m_{\mathrm{K}'}(sw_{(l)})$ est premier à $l$, le p. g. c. d. de $m_{\mathrm{K}'}(sw_{\Gamma_0})$ et de ces $m_{\mathrm{K}'}(sw_{(l)})$ est égal à 1. Il résulte alors de la proposition 7.5 que $sw_{\mathrm{G}}$ est rationnel sur K′.

C. Q. F. D.

## BIBLIOGRAPHIE.

[1] J.-M. Fontaine, *Rationalité des représentations d'Artin et de Swan* (*C. R. Acad. Sc.*, t. 270, série A, 1970, p. 93-95).

[2] J.-M. Fontaine, *Sur la décomposition des algèbres de groupes* (*Ann. scient. Éc. Norm. Sup.*, t. 4, 1971, fasc. 1, p. 121-180; cité DAG).

[3] R. MACKENZIE and G. WHAPLES, *Artin-Schreier equations in characteristic zero* (*Amer. J. Math.*, t. 78, 1956, p. 473-485).
[4] E. MAUS, *Die gruppentheoretische Struktur der Verzweigungsgruppenreihen* (*J. reine ang. Math.*, t. 230, 1968, p. 1-28).
[5] E. MAUS, *Existenz $\mathfrak{p}$-adischer Zahlkörper zu vorgegebenem Verzweigungsverhalten* (*Dissertation*, Hamburg, 1965).
[6] S. SEN, *On automorphisms of local fields* (*Ann. of Math.*, t. 90, 1969, p. 33-46).
[7] J.-P. SERRE, *Corps locaux*, 2e éd., Hermann, Paris, 1968 (cité CL).
[8] J.-P. SERRE, *Groupes proalgébriques* (*Publ. Math. IHES*, no 7, 1960).
[9] J.-P. SERRE, *Représentations linéaires des groupes finis*, 2e éd., Hermann, Paris, 1971.
[10] J.-P. SERRE, *Sur la rationalité des représentations d'Artin* (*Ann. of Math.*, t. 72, 1960, p. 405-420).
[11] J.-P. SERRE, *Sur les corps locaux à corps résiduel algébriquement clos* (*Bull. Soc. math. Fr.*, t. 89, 1961, p. 105-154; cité CRAC).

(Manuscrit reçu le 11 mars 1971.)

Jean-Marc FONTAINE,
27, boulevard Arago,
75-*Paris*, 13e.