SUR LA PRIMITIVITÉ DES CORPS $\mathfrak{P}$-ADIQUES

par

M. Krasner

(à Paris).

Reçu le 17 Novembre 1937

L'objet du présent travail est l'étude dans les corps non-galoisiens de nombres $\mathfrak{P}$-adiques des questions analogues à celles dont s'occupa dans le cas galoisien M. Öystein Ore et auxquelles sont consacrés ses 2 mémoires dans »*Mathematische Annalen*« T. 100 et 102, intitulées »Abriss einer aritmethischen Theorie Galois'schen Köper«. Il s'agit de construire la théorie de la ramification dans les corps $\mathfrak{P}$-ad ques non-galoisiens, analogue à celle de M. Hilbert pour les corps galoisiens, de trouver les conditions nécessaires et suffisantes pour qu'un corps $\mathfrak{P}$-adique soit primitif (ou une équation d'Eisenstein soit primitive (1)) par rapport à un de ses sous-corps donné, d'étudier les formes canoniques qu'on peut donner à une équation d'Eisenstein primitive (1) par la transformation de Tschirnhausen, d'étudier la génération d'un corps $\mathfrak{P}$ adique par adjonction successive de racines d'équations d'Eisenstein primitives (1) et enfin il s'agira de certaines propriétés remarquables des développements des racines d'une équation d'Eisenstein primitive (1) en séries de puissances fractionnaires d'une autre d'entre elles.

Notation:

Ensembles: La *réunion* d'ensembles A, B, C,... sera désignée AuBuCu... ou S(A, B, C, ...). L'intersection de ces ensembles sera désignée AnBnCn... ou D(A, B, C, ...). *On n'employera jamais de signes* + *et.*, ces signes étant *réservés uniquement pour les opérations algébriques de l'addition et de la multiplication (composition).* Par contre, pour désigner la différence de deux ensembles on emploiera le signe —.

(1) Il s'agit de primitivité $\mathfrak{P}$-adique.

L'ensemble d'objets $a, b, c, \ldots$ sera noté $\{a, b, c, \ldots\}$. Le nombre d'éléments d'un ensemble A sera noté (A).

Si A, B sont ensembles d'éléments susceptibles d'être additionés, multipliés, composés, A+B, AB désignent respectivement l'ensemble de tous les $a+b$, *ab distincts* tels que $a \in A$ et $b \in B$.

Si pour tous les éléments a d'un ensemble A est définie une fonction $f(a)$, B étant un sous-ensemble de A, $f(B)$ désigne l'ensemble de tous les $f(a)$ *distincts* pour $a \in B$.

Groupes: Au lieu d'écrire des mots „à droite", „à gauche" spécifiant le coté où se fait la composition des certains objets (ou avec certains objets) quand cette composition est non commutative, il sera toujours placé au dessus du mot ou de la lettre figurant l'objet en question une flèche $\rightarrow$ ou $\leftarrow$. Par exemple, „idéal" désigne „idéal à à droite".

Ceci posé, la classe $\overrightarrow{\alpha G}$ (resp. classe $\overleftarrow{G\alpha}$) d'un $\alpha \in G$ suivant un sous-groupe $\overrightarrow{g}$ du groupe G est αg (resp. $g\alpha$). Quand une classe $\overrightarrow{\alpha g}$ ou une réunion de classes $\overrightarrow{Cg}$ ($C \in G$) seront régardés non comme ensembles d'éléments de G, mais comme resp. un élément ou un sous-ensemble de l'ensemble de toutes les classes de G suivant g, ils seront désignés resp. $\overrightarrow{\alpha g}\ \overrightarrow{g}$ et $\overrightarrow{Cg}/\overrightarrow{g}$.

Anneaux non commutatifs: Les signes idéal $\overrightarrow{\ }$, idéal $\overleftarrow{\ }$, diviseur $\overrightarrow{\ }$, diviseur $\overleftarrow{\ }$, multiple $\overleftarrow{\ }$, multiple $\overrightarrow{\ }$ sont clairs. Un idéal $\overrightarrow{\ }$ (idéal $\overleftarrow{\ }$) principal qui est l'ensemble de multiples $\overrightarrow{\ }$ (multiples $\overleftarrow{\ }$) d'un élément α sera désigné $\overrightarrow{(\alpha)}$ $\overleftarrow{((\alpha))}$. Au lieu de „A est diviseur $\overrightarrow{\ }$ (diviseur $\overleftarrow{\ }$) de B" on écrira encore „$A \mid B$" („$A \mid B$") et „$B \equiv 0 \pmod{A}$" [$B \equiv 0 \pmod{A}$] [on dira „congrû" („congrû")]. Dans les anneaux où il y a un élément I bilatère, un élément a sera dit unité $\overrightarrow{\ }$ (unité $\overleftarrow{\ }$) s'il existe dans l'anneau un élément b tel que $ab = I$ ($ba = I$).

Si deux éléments d'un tel anneau a et a' sont tels que à la fois $\overrightarrow{a \mid a'}$ et $\overrightarrow{a' \mid a}$ ($\overleftarrow{a \mid a'}$ et $\overleftarrow{a' \mid a}$) ils seront dits associés $\overrightarrow{\ }$ (associés $\overleftarrow{\ }$).

(Pour que a et a' non diviseurs de zéro soient associés (associés) il faut et il suffit que $a' = a\varepsilon$ ($a' = \varepsilon a$), où ε est une unité (unité)).

Corps: Si K est un surcorps algébrique d'un corps k, au lieu de dire d'un objet qu'il est „dans (de) K par rapport à k" on dira qu'il est „dans le K/k". Si $K \supset \overline{K} \supset k$ cela s'écrira aussi $K/k = \overline{K}/k$ et $K/k/\overline{K}/k$ signifiera la même chose que $K/\overline{K}$.

L'ensemble de tous les isomorphismes de K/k sera désigné par $G_{K/k}$. L'isomorphisme identique de K sera désigné par 1_K.

Le degré de K/k sera désigné par (K/k).

A partir du § 2 il s'agira seulement de deux catégories de corps:

I. Corps p-adiques: Il y aura un corps de nombres p-adiques k de degré fini qui servira de corps de base et son extension algébrique de degré fini, corps $\mathfrak{P}$-adique K, dont les propriétés par rapport à k sont à étudier.

Tous les autres corps qui seront employés seront notés par la lettre K ou le signe K/k accompagnées de signes ou d'indices. Parfois il faudra employer un surcorps Galoisien de K/k sans que le choix spécial de ce corps importe. Il sera désigné K^*/k. Par contre, le corps de Galois de K/k (c'est-à-dire K^*/k minimal) sera désigné $K^\cdot/k$.

La base sera très rarement autre que k. Pour cette cause, dans tous les énoncés et démonstrations, quand un objet se rapporte au cas où la base est k, toute indication sur la base sera supprimée dans le symbôle qui note cet objet.

La seule exception à cette régle aura lieu si l'énoncé en question est la définition de ce symbôle.

L'idéal premier de K sera noté $\mathfrak{P}$, celui d'un corps noté K ou K/k et accompagné de signes ou d'indices — par $\mathfrak{P}$ accompagné des mêmes signes ou indices sur la même place. Le degré, l'ordre par rapport à k de ces idéaux seront désignés par f, e accompagnés des mêmes signes, le degré et l'ordre *absolus* par les lettres, F, E accompagnés des mêmes signes.

Le degré et l'ordre absolus de $\mathfrak{p}$ seront désignés par f_0, e_0.

Le premier rationnel divisible par $\mathfrak{p}$ sera désigné par p.

Norme dans K_1/K_2 sera désignée par N_{K_1/K_2}, norme absolue dans K_1 sera désignée par $N_{K_1}^+$.

Les isomorphismes d'un corps désigné par K avec les signes autres que les indices en bas (par exemple K_1) seront notés par σ accompagné des mêmes signes et, eventuellement, avec encore, des indices en bas.

La différente de K_1/K_2 sera notée δ_{K_1/K_2}.

II. Corps finis de caractéristique p. (Champs de Galois): Nous considérerons deux corps finis de caractéristique p ayant le même nombre d'éléments comme identiques indépendamment de leur origine: Ceci est justifié par le fait que 1). de deux champs de Galois de même caractéristique un est isomorphe à un sous-corps de l'autre 2). deux champs de Galois isomorphes, contenus dans un même surchamps sont identiques. Nous employerons, en général, pour le champs de Galois de p^ϕ éléments la notation $Cg(p^\phi)$ ou Ω_ϕ. Toutefois, si nous voudrons marquer l'origine du corps fini de classes [mod $\mathfrak{P}$ (accompagné de signes)] dans K (accompagné des mêmes signes) nous l'écrirons V (accompagné des mêmes signes). Le corps de classes (mod $\mathfrak{p}$) dans k sera écrit v.

Forme fondamentale: Une *forme fondamentale* de K sera notée

$$\xi = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_N x_N$$

où N est le degré absolu de K.

Remarque: Dans les symbôles employés au cours des démonstrations il sera toujours supprimée toute indication dont la suppression ne peut pas conduire à un malentedu.

Dans les énoncés, une indication ne sera jamais supprimée qu'en vertu d'une convention spéciale (telle que celle pour k).

Remarque: Les mots „limite", „convergence", etc. seront emloyés uniquement dans le sens $\mathfrak{P}$-adique.

J'employerai au cours de ce travail le

Théorème de Hilbert N° 41: Si $K \supset \overline{K} \supset k$, on a

$$\vartheta_{K/k} = \vartheta_{K/\overline{K}} \vartheta_{\overline{K}/k}.$$

§ 1. — Hypergroupes et isomorphismes des corps.

Hypergroupes: Cette notion fut introduite récémment (1934) par M. F. Marty.

Définition 1: Un ensemble K organisé par une loi de composition ab de chaque couple a, b de ses éléments s'appelle *hypergroupe* par rapport à cette loi de composition si

1° ab est un sous-ensemble non-vide de K.

2° $(ab)c = a(bc)$ (*loi associative*).

3° Pour chaque couple $a, c \in H$ il existe $x \in H$ tel que $c \in ax$ et il existe $x' \in H$ tel que $c \in x'a$ (2).

DÉFINITION 2: Un sous-ensemble h de H qui est un hypergroupe par rapport à la loi de composition de H s'appelle *sous-hypergroupe* de H.

REMARQUE: Pour tout $h \subset H$ la condition 2° est vérifiée d'elle-même. Donc, pour que h soit un sous-hypergroupe de H, il faut et il suffit que les conditions 1° et 3° soient vérifiées.

DÉFINITION 3: Un sous-hypergroupe h de H s'appelle *semi-invariant* ($\overleftarrow{\text{semi-invariant}}$) si pour tout $c \in H$ on a

$$hc \supseteq ch \qquad (\text{resp. } ch \supseteq hc).$$

Si h est à la fois semi-invariant et semi-invariant il est dit *invariant*.

DÉFINITION 4: Deux hypergroupes K et K' s'appelent *isomorphes* s'il existe une correspondance biunivoque A de H à H' telle que pour tout couple $a, b \in H$ on a

$$A(a)\,A(b) = A(ab) \qquad (\text{Notation: } H \sim H').$$

REMARQUE: Une telle correspondance A s'appelle un *isomorphisme* de H à H'.

HYPERGROUPES DE CLASSES: Considérons l'ensemble $\overrightarrow{G/g}$ de classes d'un groupe G suivant un de ses sous-groupes g. Soit $a = \alpha g/g$ et $b = \beta g/g$ ($\alpha, \beta \in G$) deux éléments de cet ensemble. Définissons une loi de composition ab par

$$ab = \alpha g \beta g/g.$$

Cette loi est non contradictoire parce que $\alpha g \beta . g$ est une réunion de classes suivant g. ab n'est pas vide, donc 1° est satisfait. Comme $(\alpha g \beta g)\gamma g = \alpha g(\beta g \gamma g)$, 2° est satisfait. Enfin, si $a = \alpha g$, $c = \gamma g$ ($\alpha\gamma \in G$), on peut trouver β et $\beta' \in G$ tels que $\gamma \in \alpha g \beta$ et $\gamma \in \beta' g \alpha$ d'où, si $b = \beta g/g$, $b' = \beta' g/g$, on a $c \in ab$ et $c \in b'a$ et 3° est vérifiée. Donc $\overrightarrow{G/g}$ ainsi organisé est un hypergroupe. On l'appelera *hypergroupe de classes* de G suivant g et, dorénavant, $\overrightarrow{G/g}$ désignera non l'ensemble des classes de G suivant g tout court, mais cet ensemble organisé en hypergroupe comme il est dit.

(2) *C. R.* 1935; *Annales de l'Ecole Normale Sup.* 1936.

Théorème I. *Pour que* $\overrightarrow{C/g}$ *soit un sous-hypergroupe de* $\overrightarrow{G/g}$ *il faut et il suffit que* $C \supset G$ *soit un sous-groupe de* G. *Donc tout sous-hypergroupe d'un hypergroupe de classes est hypergroupe de classes.*

DÉMONSTRATION: Si $C \supset G$ est un sous-groupe de G et $a = \alpha g/g$ $b = \beta g/g$ sont éléments de $\overrightarrow{C/g}$, αg, $\beta g \subset C$ et $\alpha g \beta g \subset C$, donc $ab \subset \overrightarrow{C/g}$ et 1° est vérifié. Si αg, $\gamma g \subset C$ et $\alpha g \beta g \supset \gamma g$ on a $\alpha g \beta \supset \tau$ où $\tau \in \gamma g \subset C$, donc il y a $\rho \in \alpha g \subset C$ tel que $\rho\beta = \tau$ c'est-à-dire $\beta \in C$ et $b \in \overrightarrow{C/g}$; de la même manière on démontre l'existence de $b' \in \overrightarrow{C/g}$ tel que $b'a \ni c$ et $\overrightarrow{C/g}$ est un sous hypergroupe de $\overrightarrow{G/g}$.

Inversement, soit $\overrightarrow{G/g}$ un sous-hypergroupe de $\overrightarrow{G/g}$; on a $\overrightarrow{C/g}.\overrightarrow{C/g} = \overrightarrow{C/g}$, d'où $CC = C$. De plus, si $\alpha \in C$ et $a = \alpha g/g$, on a $a.\overrightarrow{C/g}.a = \overrightarrow{C/g}$ c'est-à-dire $\alpha g C = C$ et $\alpha C = C$. Il y a donc $a' \in C$ tel que $aa' = 1$ et C est un groupe. C. q. f. d.

CONSÉQUENCE: Le quotient du nombre d'éléments d'un hypergroupe de classes $\overrightarrow{G/g}$ par le nombre d'éléments d'un de ses sous-hypergroupes $h = \overrightarrow{C/g}$ est un nombre entier. Ce nombre sera désigné $(H : h)$.

En effet, c'est l'indice $(G : C)$.

DÉFINITION 5: Si $h = \overrightarrow{C/g}$ est un sous-hypergroupe de classes $H = \overrightarrow{G/g}$ et $c \in \overrightarrow{G/g}$, l'ensemble ch s'appelle la classe de c suivant h. La même définition s'appliquera aux hypergroupes isomorphes à un hypergroupe de classes.

Théorème II. *Deux classes* $A_1 = c_1 h$ *et* $A_2 = c_2 h$ *ou bien coïncident, ou bien sont disjointes. Une classe* ch *est la classe de chacun de ses éléments. Le nombre d'éléments de* ch *est égal à celui de* h.

DÉMONSTRATION: On a, si $c = \gamma g/g$, que $ch = \gamma g C g/g = \gamma C/g$, car

$g \subset C$. γC est une classe suivant C. Il contient autant de classes suivant g que C lui-même c'est-à-dire ch contient autant d'éléments que h. Si $c_1 = \gamma_1 g/g$ et $c_2 = \gamma_1 g/g$ on a $c_1 h = \gamma_1 C/g$ et $c_2 h = \gamma_2 C/g$ donc ou bien $c_1 h = c_2 h$ ou bien $c_1 h \cap c_2 h$ est vide. Enfin, si $c' \in ch$, et $c' = \gamma' g$, on a $\gamma' g \subset \gamma C$, donc $\gamma' g C \subset \gamma C C = \gamma C$ c'est-à-dire $c'h \subset ch$. Comme $c'h \cap ch$ n'est pas vide, on a $c'h = ch$. C. q. f. d.

Considérons l'ensemble de classes suivant h dans H. Quand ces classes seront régardées comme éléments de cet ensemble elles seront désignées par ch/h. Et plus généralement, une réunion de classes Ch régardée comme ensemble de ces classes sera désignée par Ch/h. Ceci posé, définissons la loi de composition dans l'ensemble H/h pour tout couple $a_1 = c_1 h/h$ et $a_2 = c_2 h/h$ de cet ensemble par

$$a_1 a_2 = c_1 h c_2 h/h.$$

Or, si

$$c_1 = \gamma_1 G/g \quad , \quad c_2 = \gamma_2 G/g$$

on a

$$c_1 h c_2 h = \gamma_1 C \gamma_2 C/g.$$

On voit donc que l'ensemble H/h ainsi organisé est isomorphe à G/C donc H/h est un hypergroupe isomorphe à un hypergroupe de classes.

Définition 6: L'hypergroupe H/h précédemment défini s'appelle hypergroupe *quotient* de l'hypergroupe de classes H par son sous-hypergroupe h.

Théorème III („loi d'isomorphisme"). *Si* H *est un hypergroupe de classes et* h_1, h_2 *sont sous hypergroupes de* H *tels que* $H \supset h_1 \supset h_2$, *on a*

$$H/h_1 \simeq H/h_2 / h_1/h_2$$

Démonstration: On a, si $H = G/g$, $h_1 = C_1/g$, $h_2 = C_2/g$ que $H/h_1 \simeq G/C_1$, $H/h_2 \simeq G/C_2$, et $h_1/h_2 \simeq C_1/C_2$. Or d'après la définition de H/h on a $G/C_2 / C_1/C_2 \simeq G/C_1$. C. q. f. d.

Conséquence: $(H : h_1) = \dfrac{(H : h_2)}{(h_1 : h_2)}$.

Hypergroupes$_C$:

Définition 7: Un hypergroupe H s'appelle un hypergroupe$_C$ s'il existe un hypergroupe de classes G/g tel que $H \simeq G/g$.

Il est évident que les théorèmes précédents s'appliquent à tous les hypergroupes$_C$.

En particulier: Tout sous-hypergroupe d'un hypergroupe$_C$ est un hypergroupe$_C$ et pour les classes suivant ce sous-hypergroupe ont lieu le Théorème II et les résultats permettant la définition 6. Si $h_2 \subset h_1$ sont sous-hypergroupes d'un hypergroupe$_C$ H, $H/h_1 \simeq H/h_2 / h_1/h_2$.

Hypergroupes$_C$ finis.

Définition: Un hypergroupe$_C$ H s'appelle *fini* s'il existe un hypergroupe de classes $G/g \simeq H$, où G a un nombre fini d'éléments.

Théorème IV. *Pour qu'un sous-ensemble h d'un hypergroupe$_C$ fini* H *soit un sous-hypergroupe de H il faut et il suffit que pour chaque couple a, b d'éléments de h on ait $ab \subset h$.*

Démonstration: Il suffit de démontrer ce théorème pour l'hypergroupe $G/g \simeq H$, où G et d'ordre fini; soit $C/g \subset G/g$. $C \subset G$ a un nombre fini d'éléments. Donc, pour que C soit un groupe, il faut et il suffit que $CC = C$. Cela équivaut à $C/g . C/g = C/g$ et le théorème est démontré.

Correspondants et générateurs: Soient k un corps et $\bar{K}$ et $K \supset \bar{K}$ deux surcorps algébriques de k. La théorie de Galois montre que tout isomorphisme σ de K/k appliqué aux éléments de $\bar{K}$ produit un isomorphisme $\bar{\sigma}$ de $\bar{K}/k$ et que tout $\bar{\sigma} \in G_{\bar{K}/k}$ peut être obtenu de cette manière.

Définition 7: L'isomorphisme $\bar{\sigma}$ de $\bar{K}/k$ tel que pour tout $\alpha \in \bar{K}$ a lieu $\bar{\sigma}\alpha = \sigma\alpha$ s'appelle *correspondant* de σ dans $\bar{K}$ (Notation: $\bar{\sigma} = \text{corr.}_{\bar{K}} \sigma$).

Définition 8: L'ensemble A des tous les $\sigma \in G_{K/k}$ tels que $\text{corr.}_{\bar{K}} \sigma = \bar{\sigma}$ ($\bar{\sigma} \in G_{\bar{K}/k}$), s'appelle *l'ensemble générateur* de $\bar{\sigma}$ dans K (Notation: $A = \text{gen.}_K \bar{\sigma}$). Ces définitions s'étendent, comme il a été indiqué au début, à des ensembles de σ ou de $\bar{\sigma}$.

HYPERGROUPE DE K/k : Soit K/k un corps algébrique et K^*/k un surcorps galoisien de K/k. Les $\mathrm{gen}_{k^*}\sigma$, $\sigma \in G_{K/k}$, sont des classes suivant $G_{K^*/K}$ dans $G_{K^*/k}$. Donc, si l'on définit dans l'ensemble $G_{K/k}$ la loi de composition $\sigma_1\sigma_2$ de tout couple σ_1, σ_2 d'éléments de cet ensemble par

$$\sigma_1\sigma_2 = \mathrm{corr.}_K \{\mathrm{gen.}_{K^*}\sigma_1 \cdot \mathrm{gen.}_{K^*}\sigma_2\}$$

$G_{K/k}$ sera organisé en un $\overrightarrow{\text{hypergroupe}}_c$ isomorphe à $\overrightarrow{G_{K^*/k}/G_{K^*/K}}$.

DÉFINITION 9 : $G_{K/k}$ organisé en hypergroupe comme il a été indiqué s'appelle *l'hypergroupe de* K/k.

A partir de ce moment $G_{K/k}$ désignera non l'ensemble d'isomorphismes de K/k, mais cet ensemble régardé comme hypergroupe de K/k.

Théorème V. *Si* $K \supseteq \overline{K} \supseteq k$, $G_{K/\overline{K}}$ *est un sous hyper-groupe de* $G_{K/k}$.

$G_{\overline{K}/k} \sim \overrightarrow{G_{K/k}/G_{K/\overline{K}}}$ *et cet isomorphisme se réalise par la correspondance* $\overline{\sigma} \to \overrightarrow{\mathrm{gen.}_k \overline{\sigma}/G_{K/\overline{K}}}$.

Inversement, si C est un sous-hypergroupe de $G_{K/k}$ il existe un $\overline{K}$, $K \supseteq \overline{K} \supseteq k$, tel que $C = G_{K/\overline{K}}$.

DÉMONSTRATION : L'isomorphisme $G_{K/k} \sim \overrightarrow{G_{K^*/k}/G_{K^*/K}}$ est réalisé par la correspondance $\sigma \to \overrightarrow{\mathrm{gen.}_{K^*}\sigma/G_{K^*/K}}$, donc à $G_{K/\overline{K}}$ correspond dans cet isomorphisme $\overrightarrow{\mathrm{gen}_{K^*}G_{K/\overline{K}}/G_{K^*/K}} = \overrightarrow{G_{K^*/\overline{K}}/G_{K^*/K}}$. Mais $G_{K^*/\overline{K}}$ est un sous-groupe de $G_{K^*/K}$, donc $\overrightarrow{G_{K^*/\overline{K}}/G_{K^*/K}}$ est un sous-hypergroupe de $\overrightarrow{G_{K^*/k}/G_{K^*/K}}$ et $G_{K/\overline{K}}$ celui de $G_{K/k}$.

On a

$$G_{\overline{K}/k} \sim \overrightarrow{G_{K^*/k}/G_{K^*/\overline{K}}} \sim \overrightarrow{G_{K^*/k}/G_{K^*/K}} \Big/ \overrightarrow{G_{K^*/\overline{K}}/G_{K^*/K}} \sim \overrightarrow{G_{K/k}/G_{K/\overline{K}}}.$$

A $\overline{\sigma}$ correspond successivement $\overrightarrow{\mathrm{gen}_{K^*}\overline{\sigma}/G_{K^*/\overline{K}}}$, $\overrightarrow{\mathrm{gen}_{K^*}\overline{\sigma}/G_{K^*/K}} \Big/ \overrightarrow{G_{K^*/\overline{K}}/G_{K^*/K}}$ et $\mathrm{corr}_K \overrightarrow{\mathrm{gen}_{K^*}\overline{\sigma}/\mathrm{corr}_K G_{K^*/\overline{K}}} = \overrightarrow{\mathrm{gen}_K \overline{\sigma}/G_{K/\overline{K}}}$.

Enfin, si C est un sous-hypergroupe de $G_{K/k}$ on a $C \sim \overrightarrow{A/G_{K^*/K}}$ et $A = \mathrm{gen}_{K^*}C \supseteq G_{K^*/K}$ est un groupe. Donc, si $\overline{K}$ est le corps qui appartient à A dans K^*, on a $K \supseteq \overline{K} \supseteq k$, et $G_{K/\overline{K}} = \mathrm{corr}_K G_{K^*/\overline{K}} = \mathrm{corr}_K \mathrm{gen}_{K^*}C = C$ et le théorème est démontré.

REMARQUE : On dira de $\overline{K}$ qu'il *appartient* à $G_{K/\overline{K}}$ dans K/k.

Théorème VI. *Pour que* K/k *soit galoisien il faut et il suffit que* $G_{K/k}$ *soit groupe.*

DÉMONSTRATION : On a $G_{K/k} \sim \overrightarrow{G_{K^*/k}/G_{K^*/K}}$. $G_{K/k}$ est groupe si $G_{K^*/K}$ est sous-groupe invariant de $G_{K^*/k}$ et dans ce cas seulement. Le théorème est démontré.

REMARQUE : Les hypergroupes dont il s'agira dans la suite de ce travail seront toujours $\overrightarrow{\text{hypergroupes}}_c$ finis.

§ 2. — Théorie de la ramification dans les corps $\mathfrak{P}$-adiques.

Soient

k — un corps de nombres p-adiques.

K — une extension algébrique de degré fini de k. N — degré absolu de K.

$\mathfrak{P}$, $\mathfrak{p}$, p — resp. idéaux premiers de K et de k et premier rationnel qu'ils divisent.

e, f, E, F, e_0, f_0 resp. ordre et degré de $\mathfrak{P}$ dans K/k, ordre et degré absolus de $\mathfrak{P}$ et ceux de $\mathfrak{p}$.

$$\xi = \sum_{q=1}^{N} \alpha_q x_q$$ — une forme fondamentale de K.

On aura à envisager parfois un surcorps galoisien K^*/k de K/k, l'idéal premier de K^* sera désigné par $\mathfrak{P}^*$, son degré absolu par F^*.

Pour désigner les mêmes objets dans le corps de GALOIS $K^\cdot/k$ de K/k on écrira $\mathfrak{P}^\cdot$, $F^\cdot$.

DÉFINITIONS.

DÉFINITION 1 : *Nombre caractéristique* $v(\sigma)$ d'un $\sigma \in G_k$ est l'ordre en $\mathfrak{P}$ de $\overline{\sigma\xi - \xi}$ diminué d'une unité.

CONSÉQUENCE : $v(\sigma)$ est un nombre rationnel $\geqq -1$.

Si α est un élément quelconque algébrique par rapport à k, son ordre en $\mathfrak{P}$ sera désigné par $\omega_{\mathfrak{P}}(\alpha)$. L'ensemble de tous les entiers de K sera désigné par I(K).

LEMME 1 : $v(\sigma) = \mathrm{Min}\,[\omega_{\mathfrak{P}}(\sigma\alpha - \alpha)]_{\alpha \in \mathrm{I(K)}} - 1$.

DÉMONSTRATION : On a $\overline{\sigma\xi - \xi} = (\sigma\alpha_1 - \alpha_1, \sigma\alpha_2 - \alpha_2, \ldots, \sigma\alpha_N - \alpha_N)$, donc $\omega(\overline{\sigma\xi - \xi}) \geqq \mathrm{Min}\,[\omega(\sigma\alpha - \alpha)]_{\alpha \in \mathrm{I(K)}}$, car $\alpha_1, \alpha_2, \ldots, \alpha_N \in \mathrm{I(K)}$.

D'autre part, pour tout $\alpha \in I(K)$ il existent des entiers rationnels $a_1, a_2, \ldots, a_n$ tels que $\alpha = a_1\alpha_1 + a_2\alpha_2 + \ldots + a_N\alpha_N$, donc $\omega(\sigma\alpha - \alpha) \geqq \omega(\overline{\sigma\xi - \xi})$ et $\text{Min}\,[\omega(\sigma\alpha - \alpha)]_{\alpha \in I(K)} \geqq \omega(\overline{\sigma\xi - \xi})$, ce qui démontre le lemme.

LEMME 2 : Si $\sigma \in G_K$, $\sigma\mathfrak{P} = \mathfrak{P}$.

DÉMONSTRATION : $\sigma\mathfrak{P}$ est l'idéal premier de $\sigma K \subset K^*$. Dans K^* il n'y a qu'un seul idéal premier $\mathfrak{P}^*$. Donc $\mathfrak{P}$ et $\sigma\mathfrak{P}$ sont puissances de $\mathfrak{P}^*$; et comme $N^+_{K^*}(\mathfrak{P}) = N^+_{K^*}(\sigma\mathfrak{P})$, leurs exposants doivent être égaux, c'est-à-dire $\mathfrak{P} = \sigma\mathfrak{P}$. C. q. f. d.

LEMME 3 : Ou bien $v(\sigma) = -1$, ou bien $v(\sigma) \geqq 0$.

DÉMONSTRATION : D'après un théorème connu de HENSEL il existe dans le corps $\mathfrak{P}$-adique K une racine $N^+_K(\mathfrak{P}) - 1 = p^F - 1^{\text{ième}}$ de l'unité ρ congrue (mod $\mathfrak{P}$) a un entier $\alpha \not\equiv 0 \pmod{\mathfrak{P}}$ de K. Il en suit $\sigma\alpha \equiv \sigma\rho \pmod{\sigma\mathfrak{P} = \mathfrak{P}}$.

Si $\sigma\rho \equiv \rho \pmod{\mathfrak{P}^*}$, puisque $\sigma\rho$ est encore une racine $p^F - 1^{\text{ième}}$ de l'unité, on a $\sigma\rho = \rho$, donc $\sigma\alpha \equiv \sigma\rho \equiv \rho \equiv \alpha \pmod{\mathfrak{T}}$, c'est-à-dire $v(\sigma) \geqq 0$. Si $\sigma\rho \not\equiv \rho \pmod{\mathfrak{P}^*}$, $\sigma\alpha - \alpha \equiv \sigma\rho - \rho \pmod{\mathfrak{P}}$ est premier à $\mathfrak{P}$ et $v(\sigma) = -1$. C. q. f. d.

LEMME 4 : Si $\pi \in I(K)$ est d'ordre 1 en $\mathfrak{P}$ et si $v(\sigma) \geqq 0$, $v(\sigma) = \omega\left(\frac{\sigma\pi}{\pi} - 1\right)$.

DÉMONSTRATION : Il existe, d'après le lemme 1, $\alpha \in I(K)$ tel que $\omega(\sigma\alpha - \alpha) = 1 + v(\sigma)$. On peut écrire

$$\alpha \equiv \sum_{i=1}^{q} \rho_i \pi^{u_i} \pmod{\mathfrak{P}^{2+v(\sigma)}}$$

où les $\rho_i\,(i = 1, \ldots, q)$ sont racines $p^F - 1^{\text{ièmes}}$ d'unité et où les u_i sont des entiers rationnels tels que $0 \leqq u_1 < u_2 < \ldots < u_q < 2 + v(\sigma)$. On a $\sigma\rho_i = \rho_i$, donc

$$\sigma\alpha - \alpha = \sum_{i=1}^{q} \rho_i[(\sigma\pi)^{u_i} - \pi^{u_i}] \equiv 0 \;[\text{mod } (\sigma\pi - \pi)]$$

d'où $\omega(\sigma\alpha - \alpha) \geqq \omega(\sigma\pi - \pi)$. Mais, comme $\pi \in I(K)$, $\omega(\sigma\pi - \pi) \leqq 1 + v(\sigma) = \omega(\sigma\alpha - \alpha)$; d'où le lemme.

Théorème I. *Si a est un nombre rationnel, l'ensemble de tous les $\sigma \in G_K$ tels que $v(\sigma) \geqq a$ est un sous-hypergroupe de G_K.*

DÉMONSTRATION : Distinguons deux cas : 1° $a \geqq 0$. Soit $v(\sigma_1) \geqq a$, $v(\sigma_2) \geqq a$, $\sigma \in \sigma_1\sigma_2$. Il existent $\sigma_1^*, \sigma_2^* \in G_{K^*}$ tels que $\sigma_1 = \text{corr.}_K\sigma_1^*$, $\sigma_2 = \text{corr.}_K\sigma_2^*$, $\sigma = \text{corr.}_K(\sigma_1^*\sigma_2^*)$. On a

$$\sigma\pi - \pi = \sigma^*\sigma_2^*\pi - \pi = \sigma_1^*(\sigma_2^*\pi - \pi) + \sigma_1^*\pi - \pi = \sigma_1^*(\sigma_2\pi - \pi) + \sigma_1\pi - \pi.$$

Comme $\sigma_1^*\mathfrak{P} = \mathfrak{P}$, $\omega[\sigma_1^*(\sigma_2\pi - \pi)] = \omega(\sigma_2\pi - \pi) = 1 + v(\sigma_2) \geqq 1 + a$. Comme $\omega(\sigma_1\pi - \pi) \geqq 1 + a$, on a $v(\sigma) = \omega(\sigma\pi - \pi) - 1 \geqq (1 + a) - 1 = a$.

2° $a \leqq 0$. Si $a > -1$, la condition $v(\sigma) \geqq a$ équivaut, d'après le lemme 1, à $v(\sigma) \geqq 0$. Si $a \leqq -1$, l'ensemble des σ tels que $v(\sigma) \geqq a$ est G_K, donc un hypergroupe. Le théorème est démontré (3).

Soit

$$v_0(K/k),\ v_1(K/k), \ldots \qquad \ldots, v_{m-1}(K/k),\ v_m(K/k) = +\infty$$

l'ensemble de tous les nombres caractéristiques *positifs* distincts des $\sigma \in G_{K/k}$ (4), écrits dans l'ordre des grandeurs croissantes. Posons de plus, par convention spéciale,

$$v_{-2}(K/k) = -1, \quad v_{-1}(K/k) = 0.$$

DÉFINITON 2 : $v_q(K/k)\,(-2 \leqq q \leqq m)$ s'appelle le $q^{\text{ième}}$ *nombre de ramification* de K/k. Si $q = -2$, -1 ou m, ce nombre de ramification sera dit *impropre*, sinon il sera dit *propre*.

DÉFINITION 3 : L'ensemble $\overset{(q)}{V}_{K/k}$ de tous les $\sigma \in G_{K/k}$ tels que $v(\sigma) \geqq v_q(K/k)\,(-2 \leqq q \leqq m)$ (cet ensemble est, d'après le théorème I, un sous-hypergroupe de $G_{K/k}$) s'appelle *l'hypergroupe de ramification d'ordre* q de K/k (5).

Le sous-corps $(K/k)_q$ (6) de K/k qui appartient à $\overset{(q)}{V}_{K/k}$ dans K/k (théorème VI du § 1) s'appelle *corps de ramification d'ordre* q de K/k.

On voit que : $G_{K/k} = \overset{(-2)}{V}_{K/k} \supseteq \overset{(-1)}{V}_{K/k} \supseteq \overset{(0)}{V}_{K/k} \supset \overset{(1)}{V}_{K/k} \supset \ldots \supset \overset{(m-1)}{V}_{K/k} \supset \overset{(m)}{V}_{K/k} = \{1_K\}$.
$K/k = (K/k)_m \supset (K/k)_{m-1} \supset \ldots \supset (K/k)_1 \supset (K/k)_0 \supseteq (K/k)_{-1} \supseteq (K/k)_{-2} = k/k$;
$\overset{(-2)}{V}_{K/k}$, $\overset{(-1)}{V}_{K/k}$, $\overset{(0)}{V}_{K/k}$ et $(K/k)_{-2}$, $(K/k)_{-1}$, $(K/k)_0$ ont des noms spéciaux. Ils s'appellent hypergroupes et corps resp. de *décomposition*, *d'inertie*

(3) Cette démonstration simple de cet important théorème m'a été indiquée par M. CLAUDE CHEVALLEY, après la lecture de ma démonstration primitive, beaucoup plus compliquée. Je l'en remercie.

(4) $v(\sigma) = +\infty$ si $\sigma = 1_K$ et dans ce cas seulement.

(5) Habituellemet cet hypergroupe est désigné par $\overset{(q-1)}{V}_{K/k}$, [où si l'on le désigne par $\overset{(q)}{V}_{K/k}$, on désigne le nombre de ramification correspondant par $v_{q+1}(K/k)$]. C'est sur le conseil de M. CLAUDE CHEVALLEY que je me suis écarté de cette ancienne notation qui, en effet, est très incommode.

(6) On désignera ce corps par K_q, si l'on ne voudra pas attirer l'attention sur la base k.

et de *ramification* de K/k. On désigne aussi $G_{K/k}=V^{(-2)}_{K/k}$ par $Z_{K/k}$, $V^{(-1)}_{K/k}$ par $T_{K/k}$, et $V^{(0)}_{K/k}$ par $V_{K/k}$. De plus, M. Hensel appelle $(K/k)_{-1}$ *corps de coëfficients* de K/k et M. Ore appelle $(K/k)_0$ *corps régulier* de K/k.

Le nombre d'éléments de $V^{(q)}$ sera désigné par $n_q(K/k)(-2\leqq q\leqq m)$. On posera $(-2\leqq q<m)$

$$r_q(K/k)=\frac{n_q(K/k)}{n_{q+1}(K/k)}$$

$r_q(K/k)=(V^{(q)}_{K/k}:V^{(q+1)}_{K/k})$, donc, d'après § 1, est un *entier*.

Hypergroupe : $G_K/T_K\sim G_{(K/k)_{-1}}$. Soient $\mathfrak{o}$, $\mathfrak{O}$, $\mathfrak{O}^*$ (7) les corps finis des classes (mod. $\mathfrak{P}^*$) resp. dans k, K, K*. Considérons un $\sigma\in G_K$. α, β, γ étant des entiers de K, $\alpha+\beta\equiv\gamma \pmod{\mathfrak{P}}$ entraîne $\sigma\alpha+\sigma\beta\equiv\sigma\gamma \pmod{\sigma\mathfrak{P}=\mathfrak{P}}$, $\alpha.\beta\equiv\gamma \pmod{\mathfrak{P}}$ entraîne $\sigma\alpha.\sigma\beta\equiv\sigma\gamma \pmod{\mathfrak{P}}$, et $\alpha\equiv\beta \pmod{\mathfrak{P}}$ entraîne $\sigma\alpha\equiv\sigma\beta \pmod{\mathfrak{P}}$. Donc σ produit un isomorphisme de $\mathfrak{O}/\mathfrak{o}$. $\mathfrak{O}/\mathfrak{o}$ étant un sous-corps galoisien de $\mathfrak{O}^*/\mathfrak{o}$, cet isomorphisme est un automorphisme et, en vertu des proprités connues des champs de Galois, il existent des entiers rationnels i tels que pour tout $\alpha\in I(K)$ oo ait

$$\sigma\alpha\equiv\alpha^{N^+(\mathfrak{p})^i}.$$

Désignons par $i_k(\sigma)$ l'ensemble des tous les i vérifiant la congruence précédente. $i_k(\sigma)$ est, manifestement, une classe des entiers rationnels (mod f).

Soit ρ' une racine primitive (mod $\mathfrak{P}$) dans K. Soit $f(x)=0$ l'équation irréductible dans k à laquelle satisfait ρ'. Quelque soit l'entier rationnel i, il existe un zéro ρ'' de $f(z)$ tel que $\rho''\equiv\rho'^{N^+(\mathfrak{p})^i} \pmod{\mathfrak{P}^*}$ Tous les zéros de $f(x)$ étant conjugués par rapport à k, et $\rho'^{N^+(\mathfrak{p})^{i_1}}$ n'étant congrû (mod $\mathfrak{P}^*$) à $\rho'^{N^+(\mathfrak{p})^{i_2}}$ que si $i_1\equiv i_2 \pmod f$, on voit que $i_k(G_{K/k})$ est l'ensemble de toutes les classes rationnelles (mod f).

Théorème II. *$i_k(\sigma_1\sigma_2)=i_k(\sigma_1)+i_k(\sigma_2)$. La correspondance $\sigma T_{K/k}/T_{K/k}\to i_k(\sigma T_{K/k})$ est un isomorphisme de $G_{K/k}/T_{K/k}$ au groupe additif de toutes les classes rationnelles (mod f). $T_{K/k}$ est invariant dans $G_{K/k}$.*

(7) Donc $\mathfrak{o}=\Omega_{f_0}$, $\mathfrak{O}=\Omega_F$, $\mathfrak{O}^*=\Omega_{F^*}$.

Démonstration. Si $\sigma\in\sigma_1\sigma_2$, il existent $\sigma_1^*,\sigma_2^*\in G_{K^*}$ tels que $\sigma_1=\mathrm{corr}._K\sigma_1^*$, $\sigma_2=\mathrm{corr}._K\sigma_2^*$, $\sigma=\mathrm{corr}._K(\sigma_1^*\sigma_2^*)$. Si $\alpha\in I(K)$ on a $\sigma_2^*\alpha-\alpha^{N_k^+(\mathfrak{p})^{i_k(\sigma_2)}}\equiv 0 \pmod{\mathfrak{P}^*}$, d'où $\sigma_1^*\left(\sigma_2^*\alpha-\alpha^{N_k^+(\mathfrak{p})^{i_k(\sigma_2)}}\right)\equiv 0 \pmod{\sigma_1^*\mathfrak{P}^*=\mathfrak{P}^*}$ et $\sigma\alpha=\sigma_1^*\sigma_2^*$. $\alpha\equiv(\sigma_1^*\alpha)^{N_k^+(\mathfrak{p})^{i_k(\sigma_2)}}\equiv\left(\alpha^{N_k^+(\mathfrak{p})^{i_k(\sigma_1)}}\right)^{N_k^+(\mathfrak{p})^{i_k(\sigma_2)}}\equiv\alpha^{N_k^+(\mathfrak{p})^{i_k(\sigma_1)+i_k(\sigma_2)}}$; d'où $i_k(\sigma)=i_k(\sigma_1)+i_k(\sigma_2)$.

$i_k(\sigma)=0$ équivant à $\sigma\in T_K$. Donc $i_k(\sigma_1)=i_k(\sigma)$, si $\sigma_1\in\sigma T_K$: inversement, soit $i_k(\sigma_1)=i_k(\sigma)$. D'après la définition de l'hypergroupe il existe $\sigma_2\in G_k$ tel que $\sigma_1\in\sigma\sigma_2$. On a $i_k(\sigma_2)=i_k(\sigma_1)-i_k(\sigma)=0$, donc $\sigma_2\in T_K$. et $\sigma_1\in\sigma T_K$. $\sigma T_K/T_K\to i_k(\sigma T_K)$ est une correspondance biunivoque de G_K/T_K à $i_k(G_K)$, c'est-à-dire à l'ensemble de toutes les classes rationnelles (mod. f). Comme $i_k(\sigma_1\sigma_2)=i_k(\sigma_1)+i_k(\sigma_2)$, cette correspondance est l'isomorphisme de G_K/T_K au groupe additif de ces classes.

La formule précédente étant symétrique par rapport à σ_1 et σ_2, on voit que $i_k(\sigma_1)=i_k(\sigma)$ équivaut aussi à $\sigma_1\in T_K\sigma$, d'où $T_K\sigma=\sigma T_K$,

C. q. f. d.

Conséquence : $G_K/T_K\sim G_{K_{-1}}$ est un groupe cyclique d'ordre f. $(K/k)_{-1}$ est cyclique de degré f.

Théorème III. *$n_{-2}(K)=ef$, $n_{-1}(K)=e$, $r_{-2}(K)=f$.*

Démonstration : On a $\mathfrak{P}^{n_{-2}(K)}=N_{K/k}(\mathfrak{P})=\mathfrak{p}^f=\mathfrak{P}^{ef}$; d'où $n_{-2}(K)=ef$. Ensuite, $r_{-1}(K)=(V_K^{(-2)}:V_K^{(-1)})=(K_{-1}:k)=f$. D'où $n_{-1}(K)=\frac{n_{-2}(K)}{r_{-2}(K)}=\frac{ef}{f}=e$.

C. q. f. d.

Lemme 5 : $(K/k)_{-1}$ est le plus grand sous-corps non ramifié de K/k et le plus petit sous-corps de K/k par rapport auquel K est complètement ramifié.

Démonstration : Pour que $\overline{K}/k\subseteqq K/k$ soit non ramifié il faut et il suffit que l'ordre de $\mathfrak{P}$ dans $K/\overline{K}$ et dans K/k soit le même, c'est-à-dire, d'après le théorème II, que $T_{K/\overline{K}}=T_{K/k}\cap G_{K/\overline{K}}=T_{K/k}$, c'est-à-dire que $G_{K/\overline{K}}\supseteq T_{K/k}$. Pour que $K/\overline{K}$ soit complètement ramifié il faut et il suffit que $G_{K/\overline{K}}=T_{K/\overline{K}}=T_{K/k}\cap G_{K/\overline{K}}$, c'est-à-dire $G_{K/\overline{K}}\subseteqq T_{K/k}$. Le lemme est démontré.

Hypergroupe $T_K/V_K\sim G_{K_0/K_{-1}}$.

DÉFINITION 5 : Si $\sigma \in T_K$, $\beta_{-1}(\sigma)$ désigne la classe (mod $\mathfrak{P}^*$) qui contient $\frac{\sigma\pi}{\pi}$ [$\pi \in I(K)$ est d'ordre 1 en $\mathfrak{P}$].

REMARQUE : $\beta_{-1}(\sigma)$ ne dépend pas du choix de π, car si $\omega(\pi_1)=1$, on a $\pi_1 = \alpha\pi$ où $\alpha \in I(K) \equiv\!\!| \equiv 0 \pmod{\mathfrak{P}}$, et $\frac{\sigma\pi_1}{\pi_1} = \frac{\sigma\alpha}{\alpha} \cdot \frac{\sigma\pi}{\pi} \equiv \frac{\sigma\pi}{\pi} \pmod{\mathfrak{P}^*}$, parce que $\sigma\alpha \equiv \alpha \pmod{\mathfrak{P}}$.

$\beta_{-1}(\sigma)$ est un élément de $\mathfrak{O}^*$ Considérons le corps $\mathfrak{O}^*/\mathfrak{O}$; le groupe de $\mathfrak{O}^*/\mathfrak{O}$ est la période d'un automorphisme $\mathfrak{Z}$ de $\mathfrak{O}^*$ donné par

$$\mathfrak{Z}\alpha^* = \alpha^{*N_k^+(\mathfrak{P})} = \alpha^{*F} \quad \text{pour tout} \quad \alpha^* \in \mathfrak{O}^*$$

Désignons par $\langle\alpha^*\rangle_F$ l'ensemble de tous les conjugués distincts d'un $\alpha^* \in \mathfrak{O}^*$ par rapport à $\mathfrak{O}$.

LEMME 6 : Si $\sigma \in T_K$, $\mathrm{gen}_{K^*}\sigma \cap T_{K^*}$ n'est pas vide.

DÉMONSTRATION : Soit $\sigma^* \in \mathrm{gen}_{K^*}\sigma$. Pour chaque $\alpha^* \in I(K^*)$ on a $\sigma^*\alpha^* \equiv \alpha^{*N_k^+(\mathfrak{p})^{i_k(\sigma^*)}} \pmod{\mathfrak{P}^*}$, et, en particulier, si $\alpha \in I(K)$, on a

$$\alpha = \sigma\alpha = \sigma^*\alpha \equiv \alpha^{N_k^+(\mathfrak{p})^{i_k(\sigma^*)}} \pmod{\mathfrak{P}^*}.$$

Il s'ensuit $i_k(\sigma^*) \equiv 0 \pmod f$. Donc, si $i = \frac{i_k(\sigma^*)}{f}$, i est une classe $\left(\mathrm{mod}\ \frac{f^*}{f} = f_{K^*/K}\right)$, et il y a $\sigma_1^* \in G_{K^*/K}$ tel que $i_K(\sigma_1^*) = i$. On a $\sigma_1^*\alpha^* = \alpha^{*N_k^+(\mathfrak{P})^i} \equiv \alpha^{*N_k^+(\mathfrak{p})^{if}}$, c'est-à-dire $i_k(\sigma_1^*) = i_k(\sigma^*)$; d'où $i_K(\sigma^*\sigma_1^{*-1}) = 0$, donc $\sigma^*\sigma^{*-1} \in \mathrm{gen}_{K^*}\sigma$ est aussi contenu dans $T_{K^*/k}$. C. q. f. d.

Théorème IV. *Si* $\sigma_1, \sigma_2 \in T_K$ *on a*

$$\beta_{-1}(\sigma_1, \sigma_2) = \beta_{-1}(\sigma_1).\langle\beta_{-1}(\sigma_2)\rangle_F$$

$\beta_{-1}(T_K)$ *est un groupe multiplicatif de classes* (*mod* $\mathfrak{P}^*$) *dans* K^*. *La correspondance* $\sigma V_K/V_K \to \beta_{-1}(\sigma V_K)$ *est un isomorphisme de* T_K/V_K *à* $\beta_{-1}(T_K)$ *organisé en hypergroupe par la loi de composition* $*$ *donnée par*

$$a * b = a.\langle b\rangle_F$$

V_K *est un sous-hypergroupe semi-invariant de* T_K.

DÉMONSTRATION : Soit $\sigma_1^* \in \mathrm{gen}_{K^*}\sigma_1 \cap T_{K^*/k}$. On a $\mathrm{gen}_{K^*}\sigma_1 = \sigma_1^* G_{K^*/K}$.

$$\frac{\sigma_1\sigma_2\pi}{\pi} = \frac{\mathrm{gen}_{K^*}\sigma_1(\sigma_2\pi)}{\pi} = \left\{\sigma^*\left(\frac{\sigma_2\pi}{\pi}\right) \cdot \frac{\sigma^*\pi}{\pi}\right\}_{\sigma^* \in \mathrm{gen}_{K^*}\sigma_1} = \sigma_1^* G_{K^*/K}\left(\frac{\sigma_2\pi}{\pi}\right) \cdot \frac{\sigma_1\pi}{\pi}$$

Or, puisque $\sigma_1^* \in T_{K^*/k}$, on a que $i_k(\sigma_1^* G_{K^*/K}) = i_k(G_{K^*/K})$, c'est-à-dire est l'ensemble de toutes les classes (mod f^*) divisibles par f. Il s'ensuit que $\sigma_1^* G_{K^*/K}\left(\frac{\sigma_2\pi}{\pi}\right) \equiv G_{K^*/K}\left(\frac{\sigma_2\pi}{\pi}\right) \equiv \langle\beta_{-1}(\sigma_2)\rangle_F \pmod{\mathfrak{P}^*}$ et que

$$\beta_{-1}(\sigma_1\sigma_2) = \beta_{-1}(\sigma_1).\langle\beta_{-1}(\sigma_2)\rangle_F.$$

Puisque $\langle\beta_{-1}(\sigma_2)\rangle_F \ni \beta_{-1}(\sigma_2), \beta_{-1}(T_K)$ est un groupe multiplicatif. $\beta_{-1}(\sigma) = 1$ équivaut à $\sigma \in V_K$. Comme $\langle 1\rangle_F = \{1\}$, on a, quand $\sigma_1 \in \sigma V_K (\sigma \in T_K)$, $\beta_{-1}(\sigma_1) = \beta_{-1}(\sigma).\langle 1\rangle_F = \beta_{-1}(\sigma)$. Inversement, soit $\beta_{-1}(\sigma_1) = \beta_{-1}(\sigma)$. Il existe $\sigma_2 \in T_K$ tel que $\sigma_1 \in \sigma\sigma_2$, parce que T_K est un hypergroupe. On a $\beta_{-1}(\sigma_1) \in \beta_{-1}(\sigma).\langle\beta_{-1}(\sigma_2)\rangle_F$. Donc $\langle\beta_{-1}(\sigma_2)\rangle_F \ni 1$; donc $\langle\beta_{-1}(\sigma_2)\rangle_F = \langle 1\rangle_F = \{1\}$ et $\beta_{-1}(\sigma_2) = 1$; donc $\sigma_2 \in V_K$ et $\sigma_1 \in \sigma V_K$. La correspondance $\sigma V_K/V_K \to \beta_{-1}(\sigma V_K)$ est bien l'isomorphisme indiqué.

Définissons une autre loi de composition dans l'ensemble T_K par

$$\overline{\sigma_1\sigma_2} = \mathrm{corr}_K\{(\mathrm{gen}_{K^*}\sigma_1 \cap T_{K^*/k}).(\mathrm{gen}_{K^*}\sigma_2 \cap T_{K^*/k})\} =$$

$$= \mathrm{corr}_K\{(\mathrm{gen}^{K^*}\sigma_1 \cap T_{K^*/k}).\mathrm{gen}_{K^*}\sigma_2\}.$$

On a, σ étant un élément quelconque de T_K,

$$\overline{\sigma T_K} = \mathrm{corr}_K\{(\mathrm{gen}_K\sigma_1^* \cap T_{K^*/k}).\mathrm{gen}_{K^*}T_K\} = \mathrm{corr}_K\mathrm{gen}_{K^*}T_K = T_K$$

et

$$\overline{T_K\sigma} = \mathrm{corr}_K\{(\mathrm{gen}_{K^*}T_K \cap T_{K^*/k}).\mathrm{gen}_{K^*}\sigma\} = \mathrm{corr}_K\{T_{K^*/k}.\mathrm{gen}_{K^*}\sigma\} \supseteq \mathrm{corr}T_{K^*/k} = T_K$$

(parce que $\mathrm{gen}_{K^*}\sigma \cap T_{K^*/k}$ n'est pas vide).

Donc T_K ainsi organisé est un hypergroupe. On voit facilement que

$$\beta_{-1}(\overline{\sigma_1\sigma_2}) = \beta_{-1}(\sigma_1).\beta_{-1}(\sigma_2)$$

d'où il suit

$$\overline{V_K\sigma} = \overline{\sigma V_K} \qquad (\sigma \in T_K).$$

On a, manifestement, $V_K\sigma \supseteq \overline{V_K\sigma}$ et $\overline{\sigma V_K} \subseteq \sigma V_K$. Or $\sigma_1 \in \sigma V_K$ et $\sigma_1 \in \overline{\sigma V_K}$ équivalent à $\beta_{-1}(\sigma_1) = \beta_{-1}(\sigma)$; d'où $\overline{\sigma V_K} = \sigma V_K$ et $V_K\sigma \supseteq \sigma V_K$. C. q. f. d.

CONSÉQUENCE : L'ordre de $\beta_{-1}(T_K)$ est égal à $r_{-1}(K)\ N_K^+(\mathfrak{P}) - 1 = p^F - 1 \equiv 0 \pmod{r_{-1}(K)}$. $t_{-1}(K)$ est premier à p. $\beta_{-1}(T_K)$ est le groupe de racines $r_{-1}(K)^{\text{ièmes}}$ de l'unité dans $\mathfrak{O}^*$.

DÉMONSTRATION : Il suffit de prendre $K^* = K^{\cdot}$.

Théorème V. *Si* $A \subset T_K$ *est tel que* $\beta_{-1}(A)$ *est un groupe multiplicatif et si* $\sigma \in T_K$, *on a*

$$\beta_{-1}(\sigma A) = \beta_{-1}(\sigma)\ \beta_{-1}(A).$$

En particulier $\overrightarrow{AV_K/V_K}$ est un sous-hypergroupe de $\overrightarrow{T_K/V_K}$.

DÉMONSTRATION : Chaque élément de $\langle\alpha^*\rangle_F (\alpha^* \in \mathfrak{O}^*)$ a la forme $\mathfrak{Z}^i\alpha^* = \alpha^{*p^{iF}}$, donc est une puissance de α^*. Il en résulte, que si V^* est un groupe multiplicatif d'éléments de $\mathfrak{O}^*$ et si $\alpha^* \in V^*$, aussi $\langle\alpha^*\rangle_F \subset V^*$. Donc $\langle\beta_{-1}(A)\rangle_F = \beta_{-1}(A)$ et $\beta_{-1}(\sigma A) = \beta_{-1}(\sigma).\beta_{-1}(A)$. En particulier, $\beta_{-1}(AV_K . AV_K) = \beta_{-1}(A).\beta_{-1}(A) = \beta_{-1}(A)$;d'où $AV_K . AV_K = AV_{K^*}$, et $\overrightarrow{AV_K/V_K}$ est un sous-hypergroupe de $\overrightarrow{T_K/V_K}$ (Théorème IV du § 1).

C. q. f. d.

HYPERGROUPES $V_K/V_K \simeq G_{K_{q+1}/K_q}$ $\overset{(q)\to(q+1)}{}$ $(q = 0, 1, \ldots, m-1)$. Soient D le plus petit comun dénominateur de tous les $v_q(K/k)$ propres, π un entier de K d'ordre 1 en $\mathfrak{P}$, et $\pi_0^D = \pi$; soit K^*/k un surcorps galoisien de K contenant π_0.

DÉFINITION 6 : Si $m > q \geqq 0$ et si $\sigma \in \overset{(q)}{V}_{K/k}$, $\beta_q^{(\pi_0)}(\sigma)$ désigne la classe (mod $\mathfrak{P}^*$) dans K^* qui contient $\dfrac{\sigma\pi - \pi}{\pi_0^{D(1+v_q(K/k))}}$

$\beta_q^{(\pi_0)}(\overset{(q)}{V}_{K/k})$ sera désigné par $M_q^{(\pi_0)}(K/k)$.

REMARQUE : Si l'on choisit autrement π et π_0, par exemple si l'on prend $\pi'_0 \equiv \lambda\pi_0$ (mod $\mathfrak{P}^*$) ($\lambda^D \in K$, $\lambda \equiv\!|\equiv 0$ (mod $\mathfrak{P}^*$)), tous les éléments de $M_q(K/k)$ se multiplient par le même facteur $\equiv \lambda^{-Dv_q(K/k)}$ (mod $\mathfrak{P}^*$) si δ_q est le dénominateur de $v_q(K/k)$ et si $\mu_q = (\delta_q v_q, p^F - 1)$, l'ensemble des facteurs ainsi obtenus est l'ensemble des racines $(p^F - 1)\dfrac{\delta_q}{\mu_q}$ ièmes de l'unité dans $\mathfrak{O}^*$. Si $\bar{\delta}_q$ est le plus grand diviseur de δ_q qui est premier à p, il y en a $(p^F - 1)\dfrac{\bar{\delta}_q}{\mu_q}$ différents.

Théorème (de M. HILBERT). *Si K^*/k est galoisien, $n_0(K^*/k)$ est une puissance de p.*

DÉMONSTRATION : Soit $\sigma^* \in V_{K^*}$ et $v(\sigma^*) \neq +\infty$. Si π^* est d'ordre 1 en $\mathfrak{P}^*$, on a

$$\sigma^*\pi^* \equiv \pi^*(1 + \beta\pi^{*v(\sigma^*)}) \text{ (mod } \mathfrak{P}^{*v(\sigma^*)+2}) \quad (\beta \in I(K^*)).$$

Or, puisque $\sigma^* \in V_{K^*}$, on a $\sigma^{*a}(\beta\pi^{*v(\sigma^*)+1}) \equiv \beta\pi^{*v(\sigma^*)+1} (\text{mod } \mathfrak{P}^{*(\sigma^*)+2})$ c'est-à-dire $\sigma^{*a+1}\pi^* = \sigma^{*a}(\pi^* + \beta\pi^{*v(\sigma^*)+1}) = \sigma^{*a}\pi^* + \beta\pi^{*v(\sigma^*)+1} (\text{mod } \mathfrak{P}^{*v(\sigma^*)+2})$ d'où l'on déduit

$$\sigma^{*a}\pi^* \equiv \pi^*(1 + a\beta\pi^{*v(\sigma^*)}) \quad (\text{mod } \pi^{*v(\sigma^*)+2})$$

en, particulier, $\sigma^{*p}\pi^* \equiv \pi^* (\text{mod } \mathfrak{P}^{*v(\sigma^*)+2})$, d'où $v(\sigma^{*p}) > v(\sigma^*)$, et en général, si $v(\sigma^{*p^j}) \neq +\infty$, on a $v(\sigma^*) < v(\sigma^{*p}) < v(\sigma^{*p^2}) < \ldots < (\sigma^{*p^j})$. Comme il n'y a qu'un nombre fini de $v_q(K)$ différents, il doit exister un j tel que $v(\sigma^{*p^j}) = +\infty$, c'est-à-dire $\sigma^{*p^j} = 1_{K^*}$; d'où le théorème.

LEMME 7 : Si $\sigma \in V_K$, $\text{gen}_{K^*}\sigma \cap V_{K^*/k}$ n'est pas vide.

DÉMONSTRATION : $\text{gen}_{K^*}\sigma \cap T_{K^*/k}$ n'est pas vide. Soit $\sigma^* \in \text{gen}_{K^*}\sigma \cap T_{K^*/k}$. On a, si $\omega_{\mathfrak{P}^*}(\pi^*) = 1$

$$\sigma^*\pi^* \equiv \beta_{-1}(\sigma^*)\pi^* \text{ (mod } \mathfrak{P}^{*2}).$$

Or, si $\omega_{\mathfrak{P}}(\pi) = 1$, $\pi\pi^{-n_{-1}(K^*/K)}$ est un entier de K^* premier à $\mathfrak{P}^*$. Il s'ensuit que $\sigma\pi = \sigma^*\pi = \sigma^*(\pi\pi^{*-n_{-1}(K^*/K)})(\sigma^*\pi^*)^{n_{-1}(K^*/K)} \equiv \pi\pi^{*-n_{-1}(K^*/K)} \cdot (\beta_{-1}(\sigma^*)\pi^*)^{-n_{-1}(K^*/K)} \equiv \beta_{-1}(\sigma^*)^{n_{-1}(K^*/K)}.\pi$ (mod $\mathfrak{P}\mathfrak{P}^*$) ; d'où

$$\beta_{-1}(\sigma) = \beta_{-1}(\sigma^*)^{n_{-1}(K^*/K)}$$

$\beta_{-1}(\sigma) = 1$ et $n_{-1}(K^*/K) = r_{-1}(K^*/K)n_0(K^*/K)$. D'après le théorème précédent de HILBERT $n_0(K^*/K)$ est une puissance de p. Comme l'ordre de $\beta_{-1}(\sigma^*)$ dans le groupe multiplicatif $\beta_{-1}(T_{K^*/K})$ est premier à p, on a

$$\beta_{-1}(\sigma^*)^{r_{-1}(K^*/K)} = 1$$

c'est-à-dire d'après la conséquence du théorème IV, $\beta_{-1}(\sigma^*) \in \beta_{-1}(T_{K^*/K})$. Il existe $\sigma_1^* \in T_{K^*/K}$ tel que $\beta_{-1}(\sigma_1^*) = \beta_{-1}(\sigma^*)$ et $\beta_{-1}(\sigma^*\sigma_1^{*-1}) = 1$ c'est-à-dire $\sigma^*\sigma_1^{*-1} \in \text{gen}_{K^*}\sigma$ est aussi dans $V_{K^*/k}$. C. q. f. d.

DÉFINITION 7 : Si $\alpha^* \in \mathfrak{O}^*$ et si ζ est une racine $\delta^{\text{ième}}$ primitive de l'unité dans $\mathfrak{O}^*$

$$[\alpha^*]_{F,\delta} = \langle\alpha^*\rangle_F \cup \zeta.\langle\alpha^*\rangle_F \cup \zeta^2\langle\alpha^*\rangle_F \cup \ldots \quad \ldots \cup \zeta^{\delta-1}\langle\alpha^*\rangle_F.$$

Théorème VI. *Si $\sigma_1, \sigma_2 \in \overset{(q)}{V}_K$ et si $\bar{\delta}_q$ est le plus grand facteur du dénominateur δ_q de $v_q(K)$ premier à p,*

$$\beta_q^{(\pi_0)}(\sigma_1\sigma_2) = \beta_q^{(\pi_0)}(\sigma_1) + \left[\beta_q^{(\pi_0)}(\sigma_2)\right]_{F,\bar{\delta}_q}.$$

DÉMONSTRATION. Soit K^* un surcorps galoisien de K contenant π_0, et soit $\bar{\pi}_0 = \pi_0^{\frac{D}{\delta_q}}$. Soit $\gamma(\sigma^*)$ la classe (mod $\mathfrak{P}^*$) contenant $\dfrac{\sigma^*\bar{\pi}_0}{\bar{\pi}_0}$.

Soit U l'ensemble de systèmes $[i_K(\sigma^*), \gamma(\sigma^*)]$ pour tous $\sigma^* \in G_{K^*/K}$, c'est-à-dire $U = \{[i_K(\sigma^*), \gamma(\sigma^*)]\}_{\sigma^* \in G_{K^*/K}}$. Montrons que U est le produit,

au sens de la théorie des ensembles, d'ensembles $i_K(G_{K^*/K})$ et $\gamma(T_{K^*/K})$. En effet, d'abord, comme $\sigma^*\pi = \pi$, on a $\gamma(\sigma^*)^{\overline{\delta}_q} = 1$. Or, si $\sigma_1^* \in T_{K^*/K}$, et si $n_{-1}(K^*/K) = n\delta_q$, on a $r_{-1}(K^*/K) = (r_{-1}(K^*/K), n).\overline{\delta}_q$ (8) (parceque $n_0(K^*/K)$ est une puissance de p). On a évidemment $\gamma(\sigma_1^*) = \beta_{-1}(\sigma_1^*)^n$, d'où, puisque $\beta_{-1}(T_{K^*/K})$ est l'ensemble de toutes les racines $r_{-1}(K^*/K)^{\text{ièmes}}$ de l'unité dans $\mathfrak{O}^*$, $\gamma(T_{K^*/K})$ est l'ensemble de toutes les racines $\overline{\delta}_q^{\text{ièmes}}$ de l'unité dans $\mathfrak{O}^*$. Donc, quelque soit $\alpha^* \in \gamma(T_{K^*/K})$, il existe un $\sigma_1^* \in T_{K^*/K}$ tel que $\gamma(\sigma_1^*\sigma^*) \equiv \frac{\sigma_1^*\sigma^*\overline{\pi}}{\overline{\pi}} \equiv \sigma_1^*\left(\frac{\sigma^*\overline{\pi}_0}{\overline{\pi}_0}\right)\cdot\frac{\sigma_1^*\overline{\pi}_0}{\overline{\pi}_0} \equiv \gamma(\sigma_1).\gamma(\sigma^*)$ est égal à α^*. Comme $\sigma_1^*\sigma^* \in G_{K^*/K}$ et $i_K(\sigma_1^*\sigma^*) = i_K(\sigma_1^*) + i_K(\sigma^*) = i_K(\sigma^*)$ (parce que $\sigma_1 \in T_{K^*/K}$), on voit bien que

$$U = i_K(G_{K^*/K}) \times \gamma(T_{K^*/K})$$

Ceci posé, soient $v_q(K) = \frac{u_q}{\delta_q}$ $((u_q, \delta_q) = 1)$ et $\sigma_1, \sigma_2 \in \overset{(q)}{V}_K$. On a

$$\beta_q^{(\pi_0)}(\sigma_1\sigma_2) \equiv \frac{\sigma_1\sigma_2\pi - \pi}{\pi_0^{D(1+v_q)}} \equiv \left\{\sigma^*\left(\frac{\sigma_2\pi - \pi}{\overline{\pi}_0 u_q + \delta_q}\right)\left(\frac{\sigma^*\overline{\pi}_0}{\overline{\pi}_0}\right)^{u_q+\delta_q} + \frac{\sigma^*\pi - \pi}{\pi_0^{D(1+v_q)}}\right\}_{\sigma^* \in \mathrm{gen}_{K^*}\sigma_1} =$$

$$= \left\{\sigma^*\beta_q^{(\pi_0)}(\sigma_2).\left(\frac{\sigma^*\overline{\pi}_0}{\overline{\pi}_0}\right)^{u_q+\delta_q} + \beta_q^{(\pi_0)}(\sigma_1)\right\}_{\sigma^* \in \mathrm{gen}_{K^*}\sigma_1}.$$

Or, si $\sigma_1^* \in \mathrm{gen}_{K^*}\sigma_1 \cap V_{K^*}$, on a $\mathrm{gen}_{K^*}\sigma_1 = \sigma_1^* G_{K^*/K}$. Donc, il existe $\sigma_0^* \in G_{K^*/K}$ tel que $\sigma^* = \sigma_1^*\sigma_0$, et $\sigma^*\beta_q^{(\pi_0)}(\sigma_2).\left(\frac{\sigma^*\overline{\pi}_0}{\pi_0}\right)^{v_q+\delta_q} =$

$$= \sigma_1^*\sigma_0^*\beta_q^{(\pi_0)}(\sigma_2).\sigma_1^*\left(\frac{\sigma_0^*\overline{\pi}_0}{\overline{\pi}_0}\right)^{u_q+\delta_q}\left(\frac{\sigma_1^*\overline{\pi}_0}{\overline{\pi}_0}\right)^{u_q+\delta_q} = \sigma_0^*\beta_q^{(\pi_0)}(\sigma_2).\left(\frac{\sigma_0^*\overline{\pi}_0}{\overline{\pi}_0}\right)^{u_q+\delta_q} =$$

$$= \mathfrak{Z}^{i_K(\sigma_0^*)}\beta_q^{(\pi_0)}(\sigma_2).\gamma(\sigma_0^*)^{u_q+\delta_q}.$$

L'ensemble de tous les σ_0^* des $\sigma^* \in \mathrm{gen}_{K^*}\sigma_1$ est $G_{K^*/K}$. Comme $i_K(G_{K^*/K})$ est l'ensemble de toutes les classes (mod $f_{K^*/K}$), et $\gamma(T_{K^*/K})$, donc aussi $\{\gamma(\sigma_0^*)^{u_q+\delta_q}\}_{\sigma^* \in T_{K^*/K}}$ est l'ensemble de toutes les racines $\overline{\delta}_q$-ièmes de l'unité dans $\mathfrak{O}^*$, on a, d'après ce qui précède, que

$$\{\mathfrak{Z}^{i_K(\sigma_0^*)}\beta_q^{(\pi_0)}(\sigma_2).\gamma(\sigma_0^*)^{u_q+\delta_q}\}_{\sigma_0^* \in G_{K^*/K}} = [\beta_q^{(\pi_0)}(\sigma_2)]_{F,\overline{\delta}_q}$$

et que $\beta_q^{(\pi_0)}(\sigma_1\sigma_2) = \beta_q^{(\pi_0)}(\sigma_1) + [\beta_q^{(\pi_0)}(\sigma_2)]_{F,\overline{\delta}_q}$. C. q. f. d.

Théorème VII. *Si* $0 \leqq q < m$, $M_q^{(\pi)}(K/k)$ *est un module dans* $\mathfrak{O}^*$ *et la correspondance* $\sigma\,\overset{(q+1)}{V}_K \,/\, \overset{(q+1)}{V}_K \to \beta_q^{(\pi)}(\sigma\,\overset{(q+1)}{V}_K)$ *est un isomorphis-*

(8) a, b étant des entiers rationnels, (a, b) désigne leur p. g. c. d., et $m(a, b)$ désigne leur p. p. c. m.

me de $\overset{(q+1)}{V}_K / \overset{(q)}{V}_K$ *à l'ensemble* $M_q^{(\pi_0)}(K/k)$ *organisé en hypergroupe par la loi de composition de tout couple d'éléments* a, b *donnée par*

$$a * b = a + [b]_{F,\overline{\delta}_q}$$

$r_q(K/k)$ *et* $n_q(K/k)$ *sont puissances de* p, *soit* $n_q(K/k) = p^{l_q(K/k)}$ *et* $r_q(K/k) = p^{l_q(K/k)}.l_q(K/k) \leqq F^*$.

Démonstration : Puisque $[\alpha^*]_{F,\delta} \supset \langle\alpha^*\rangle_F \ni \alpha^*, \beta_q^{(\pi_0)}(\sigma_1\sigma_2) = \beta_q^{(\pi_0)}(\sigma_1) + [\beta_q^{(\pi_0)}(\sigma_2)]_{F,\overline{\delta}_q} \ni \beta_q^{(\pi_0)}(\sigma_1) + \beta_q^{(\pi_0)}(\sigma_2)$, c'est-à-dire $M_q^{(\pi_0)}(K)$ est un module. Comme c'est un sous-module de $\mathfrak{O}^* = \Omega_{F^*}$, son nombre d'éléments est une puissance de p.

$\sigma \in \overset{(q+1)}{V}_K$ équivaut à $\beta_q^{(\pi_0)}(\sigma) = 0$. Comme $[0]_{F,\overline{\delta}_q} = \{0\}$, il s'ensuit que, si $\sigma_1 \in \sigma\,\overset{(q+1)}{V}_K$, $\beta_q^{(\pi_0)}(\sigma_1) = \beta_q^{(\pi_0)}(\sigma)$. Inversement, soit $\beta_q^{(\pi_0)}(\sigma_1) = \beta_q^{(\pi_0)}(\sigma)$. Il existe $\sigma_2 \in \overset{(q)}{V}_K$ tel que $\sigma_1 \in \sigma\sigma_2$. On a $\beta_q^{(\pi_0)}(\sigma) = \beta_q^{(\pi_0)}(\sigma_1) \in \beta_q^{(\pi_0)}(\sigma) + [\beta_q^{(\pi_0)}(\sigma_2)]_{F,\overline{\delta}_q}$ d'où $0 \in [\beta_q^{(\pi_0)}(\sigma_2)]_{F,\overline{\delta}_q}$, c'est-à-dire il y a un $\zeta^a.\mathfrak{Z}^i\beta_q^{(\pi_0)}(\sigma_2) = 0$, d'où $\beta_q^{(\pi_0)}(\sigma_2) = \mathfrak{Z}^{-i}(\zeta^{-a}.0) = \mathfrak{Z}^{-i}.0 = 0$ et $\sigma_2 \in \overset{(q+1)}{V}_K$. Il s'ensuit que $\sigma\,\overset{(q+1)}{V}_K \,/\, \overset{(q+1)}{V}_K \to \beta_q^{(\pi_0)}(\sigma\,\overset{(q+1)}{V}_K)$ est l'isomorphisme indiqué et que le nombre d'éléments de $M_q^{(\pi_0)}(K)$ est $r_q(K)$. Donc $r_q(K)$ est une puissance de p, et aussi $n_q(K) = \prod_{s=q}^{m-1} r_q(K)$ est une puissance de p. Si l'on prend $K_1^* = K^*$ et si π^* est un entier de K^* d'ordre 1 en $\mathfrak{P}^*$, les classes (mod $\mathfrak{P}^*$) qui contiennent $(\sigma \in \overset{(q)}{V}_K)$ $\frac{\sigma\pi - \pi}{\pi\pi^{*\omega_{\mathfrak{P}^*}(\pi)v_q(K)}}$ ne différent de $\beta_q^{(\pi_0)}(\sigma)$ correspondants que par le même facteur

$$\lambda = \frac{\pi_0^{Dv_q(K)}}{\pi^{*\omega_{\mathfrak{P}^*}(\pi)v_q(K)}} \equiv\!\!\!| \equiv 0 \pmod{\mathfrak{P}^*}.$$

Donc le nombre des classes distinctes parmi ces classes, qui est $\leqq N_{K^*}^+(\mathfrak{P}^*) = p^{lF^*}$, est $p^{l_q(K)}$, ce qui montre que $l_q(K) \leqq F^*$. Le théorème est démontré.

Théorème VIII. $\overset{(q+1)}{V}_K$ *est un sous-hypergroupe semi-invariant de* $\overset{(q)}{V}_K$.

Démonstration : analogue à celle de la dernière partie du théo-

rème IV. On se sert de la loi de composition $(\sigma_1, \sigma_2 \in \overset{(q)}{V}_K)$

$$\overline{\sigma_1\sigma_2} = \mathrm{corr}_K \{(\mathrm{gen}_{K^*}\, \sigma_1 \cap V_{K^*/k})\,(\mathrm{gen}_{K^*}\sigma_2 \cap V_{K^*/k})\}.$$

LEMME 8: La différente de K/k $\vartheta_{K/k} = \mathfrak{P}^{n-1(K/k)-1+u_{K/k}}$ où

$$u_{K/k} = \sum_{q=0}^{m-1} v_q(K/k)\,[n_q(K/k) - n_{q+1}(K/k)]\ (9).$$

DÉMONSTRATION: $\vartheta_{K/k} = \prod_{\sigma \in G'_{K/k}} (\overline{\sigma\xi - \xi})$, où $G'_{K/k} = G_{K/k} - \{1_K\}$. Or $\overline{\sigma\xi - \xi} = \mathfrak{P}^{1+v(\sigma)}$; il y a $n_q(K) - n_{q+1}(K)$ de σ tels que $v(\sigma) = v_q(K)$. Etant donné que $v_{-2}(K) = -1$, $v_{-1}(K) = 0$, $n_m(K) = 1$ et que $\sigma \in G'_{K/k}$ sauf si $v(\sigma) = +\infty = v_m$, on voit que l'égalité écrite est exacte.

LEMME 9: Si $K_q \subseteq K' \subset K'' \subseteq K_{q+1}$ et si K''/K' est primitif ($q = 0, 1, \ldots, m-1$)

$$v_0(K''/K') = v_q(K),\ v_1(K''/K') = +\infty.$$

DÉMONSTRATION: Dans $G'_{K/K'}$ il y a $(K : K') - n_{q+1}(K)$ de σ tels que $v(\sigma) = v_q(K)$, $n_{q+1}(K) - n_{q+2}(K)$ de σ tels que $v(\sigma) = v_{q+1}(K)$, $n_{q+2}(K) - n_{q+3}(K)$ de σ tels que $v(\sigma) = v_{q+2}(K), \ldots, n_{m-1}(K) - n_m(K)$ de σ tels que $v(\sigma) = v_{m-1}(K)$, parceque $\overset{(q)}{V}_K \supseteq G_{K/K'} \supset \overset{(q+1)}{V}_K$. On voit, puisque K/K' est complètement ramifié, que

$$\vartheta_{K/K'} = \mathfrak{P}^{(K:K')-1+v_q(K)[(K:K')-n_{q+1}(K)]+\sum_{s=q+1}^{m-1} v_s(K)\,[n_s(K)-n_{s+1}(K)]}$$

est de même

$$\vartheta_{K/K''} = \mathfrak{P}^{(K:K'')-1+v_q(K)[(K:K'')-n_{q+1}(K)]+\sum_{s=q+1}^{m-1} v_s(K)[n_s(K)-n_{s+1}(K)]}.$$

Or, si K''/K' est primitif, tous les éléments de $G_{K''/K'}$ sauf $1_{K''}$ doivent avoir la même nombre caractéristique, car autrement, d'après le théorème I, $G_{K''/K'}$ aurait de vrais (c'est-à-dire $\neq G_{K''/K'}$ et $\neq 1_{K''}$) sous-hypergroupes. Soit v ce nombre caractéristique. Soit $\mathfrak{P}''$ l'idéal premier de K''. Comme K/K'' est complètement ramifié, on a $\mathfrak{P}'' = \mathfrak{P}^{(K:K'')}$ et

$$\vartheta_{K''/K'} = \mathfrak{P}''^{[(K'':K')-1]\,(1+v)} = \mathfrak{P}^{[(K:K')-(K:K'')]\,(1+v)}.$$

Comme

$$\vartheta_{K/K'} = \vartheta_{K/K''}\vartheta_{K''/K'}$$

(9) MM. HENSEL et ORE appellenu $u_{K/k}$ *nombre supplémentaire.* („*Supplementzahl*") *de* K/k.

on a

$$[(K:K') - (K:K'')]\,(1+v) =$$

$$= \left[(K:K') - 1 + v_q(K)[(K:K') - n_{q+1}(K)] + \sum_{s=q+1}^{m-1} v_s(K)\,[n_s(K) - n_{s+1}(K)]\right] -$$

$$- \left[(K:K'') - 1 + v_q(K)[(K:K'') - n_{q+1}(K)] + \sum_{s=q+1}^{m-1} v_s(K)\,[n_s(K) - n_{s+1}(K)]\right] =$$

$$= [(K:K') - (K:K'')]\,[1 + v_q(K)].$$

Donc $v = v_q(K) > 0$

c'est-à-dire $v = v_0(K'/K'')$, $v_1(K'/K'') = +\infty$. C. q. f. d.

Théorème IX. *Les dénominateurs* δ_q *de* $v_q(K)$ $(q = 0, 1, \ldots, m-1)$ *sont premiers à* p, (*c'est-à-dire* $\overline{\delta_q} = \delta_q$).

DÉMONSTRATION: On peut surement trouver un corps K''/K' primitif tel que $K_q \subseteq K' \subset K'' \subseteq K_{q+1}$; on a $v_0(K''/K') = v_q(K)$. On a

$$u_{K''/K'} = [(K'':K') - 1]\,v_0(K''/K') = [(K'':K') - 1]\,v_q(K).$$

Or $\vartheta_{K''/K'} = \mathfrak{P}''^{(K'':K'')-1+u_{K''/K'}}$ est un idéal de K'', donc $u_{K''/K'}$ est entier, et, de plus, $(K'':K')$ est une puissance de p. Donc $(K'':K') \equiv 1$ (mod. δ_q) et si $(\delta_q, p) \neq 1$, on aurait $0 \equiv 1$ (mod. p), ce qui est absurde. Le théorème est démontré.

CONSÉQUENCE: Donc $[\alpha^*]_{F,\overline{\delta_q}} = [\alpha^*]_{F,\delta_q}$ et on peut écrire $(\sigma_1, \sigma_2 \in \overset{(q)}{V}_K)$

$$\beta_q^{(\pi_0)}(\sigma_1\sigma_2) = \beta_q^{(\pi_0)}(\sigma_1) + \left[\beta_q^{(\pi_0)}(\sigma_2)\right]_{F,\delta_q}.$$

Théorème X. $M_q^{(\pi_0)}(K)$ *admet comme opérateurs la multiplication par la racine primitive* $\delta_q^{\text{ième}}$ *de l'unité dans* $\mathfrak{O}^*$, ζ *et la transformation* $\mathfrak{Z} = \{\alpha^* \to \alpha^{*p^F}\}_{\alpha^* \in \mathfrak{O}^*}$.

Pour qu'un sous-ensemble $A \,/\, \overset{(q+1)}{V}_K$ *de* $\overset{(q)}{V}_K \,/\, \overset{(q+1)}{V}_K$ *soit un sous-hypergroupe de* $\overset{(q)}{V}_K \,/\, \overset{(q+1)}{V}_K$ *il faut et il suffit que* $\beta_q^{(\pi_0)}(A)$ *soit un module dans* $\mathfrak{O}^*$ *admettant les mêmes opérateurs.*

DÉMONSTRATION: Si $A \,/\, \overset{(q+1)}{V}_K$ st sous-hypergroupe de $\overset{(q)}{V} \,/\, \overset{(q+1)}{V}_K$, A l'est de $\overset{(q)}{V}_K$, donc $\beta_q^{(\pi_0)}(A) = \beta_q^{(\pi_0)}(1_K.A) = 0 + \left[\beta_q^{(\pi_0)}(A)\right]_{F,\delta_q} = \left[\beta_q^{(\pi_0)}(A)\right]_{F,\delta_q}$.

Donc $\beta_q^{(\pi_0)}(A)$ admet les opérateurs indiqués. Si $A = G_{K/\overline{K}}$, $\beta_q^{(\pi_0)}(A) = M_0^{(\pi_0)}(K/\overline{K})$, donc est, d'après le théorème VII, un module.

Inversnment, si $\beta_q^{(\pi_0)}(A)$ satisfait aux conditions indiquées, on a, si $b \in A$, que $\left|\beta_q^{(\pi_0)}(b)\right|_{F,\delta_q} \subset \beta_q^{(\pi_0)}(A)$. Donc si $a, b \in A$, on a $\beta_q^{(\pi_0)}(ab) = \beta_q^{(\pi_0)}(a) + \left[\beta_q^{(\pi_0)}(b)\right]_{F,\delta_q} \subset \beta_q^{(\pi_0)}(A)$, donc $ab \subset A\,{}^{(q+1)}V_K = A$ et, d'après le théorème IV du § 1, A est un sous-hypergroupe de ${}^{(q)}V_K$. C. q. f. d.

Définition 8: Un module dans $\mathfrak{O}^*$ qui admet les opérateurs indiqués dans l'énoncé du théorème X s'appelle un W_{F,ψ_q}-module, où ψ_q est l'exposant auquel appartient $p \pmod{\delta_q}$.

§ 3. — Primitivité des corps $\mathfrak{P}$-adiques. Préliminaires.

On sait qu'un corps K/k s'appelle *primitif* s'il n'existe de corps contenant k et contenus dans K autres que k et K.

Il s'agit de trouver la condition nécessaire et suffisante pour qu'un corps $\mathfrak{P}$-adique K/k soit primitif.

Théorème I. *Pour que* K/k *soit primitif il faut qu'ait lieu un des trois cas suivants :*

a) $(K/k)_{-2} = K/k$, $(K/k)_{-1} = (K/k)_0 = K/k$

b) $(K/k)_{-2} = (K/k)_{-1} = k/k$, $(K/k)_0 = K/k$

c) $(K/k)_{-2} = (K/k)_{-1} = (K/k)_0 = k/k$, $(K/k)_1 = K/k$.

(On dira encore que le corps K/k du cas *a* est un corps de coefficients, et on appelera les cas *b* et *c* encore respectivement cas régulier et cas irrégulier de M. Ore).

Démonstration: On a par définition

$$k/k = (K/k)_{-2} \subseteq (K/k)_{-1} \subseteq (K/k)_0 \subset (K/k)_1 \subset \cdots \subset (K/k)_m = K/k$$

si $m > 1$, on a $k/k \subseteq (K/k)_0 \subset (K/k)_1 \subset (K/k)_2 \subseteq K/k$, donc $k/k \subset (K/k)_1 \subset K/k$ et K/k est imprimitif. Donc $m \leq 1$. Il n'y a que trois possibilités, *a)* $K/k = (K/k)_{-1}$, *b)* $(K/k)_{-1} \neq K/k = (K/k)_0$, *c)* $K/k = (K/k)_1$. Dans le cas *a*, puisque $(K/k) \subseteq (K/k)_0 \subseteq K/k$, $(K/k)_0 = K/k$. Dans le cas *b* on a $k/k \subseteq (K/k)_{-1} \subset K/k$ Si $(K/k)_{-1} \neq k/k$, K/k est imprimitif, d'où

$(K/k)_{-1} = k/k$. Enfin, dans le cas *c* on a $k/k \subseteq (K/k)_{-1} \subseteq (K/k)_0 \subset (K/k)_1 = K/k$, d'où, de la même manière, $(K/k)_0 = (K/k)_{-1} = k/k$. C. q. f. d.

Les cas *a* et *b* ont été complètement analysés par MM. Hensel et Ore. Il s'agira, par conséquent, dans ce travail du cas *c*. Toutefois, j'expose brièvement aussi la théorie des cas *a* et *b*, et je la fais d'un point de vue différent de celui de ces auteurs.

Cas *a*.

Théorème II. *Si* $K/k = (K/k)_{-1}$, K/k *est cyclique de degré* f *non ramifié. Il est primitif si son degré est un nombre premier et dans ce cas seulement.*

Démonstration : Si $K/k = (K/k)_{-1}$, on a $T_K = \{1_K\}$, donc $G_K \simeq \overrightarrow{Z_K/T_K}$. Mais ce dernier hypergroupe est un groupe cyclique d'ordre f, d'où (théorème VI du § 1) le théorème.

M. Hensel montre que $(K/k)_{-1} = K(\rho)/k$, où ρ est une racine primitive $(p^F-1)^{\text{ième}}$ de l'unité c'est-à-dire que $(K/k)_{-1}$ s'obtient par adjonction à k d'un nombre satisfaisant dans k à une équation binôme $x^{p^F-1}-1=0$, en général non irréductible. Celà donne une autre démonstration du théorème II.

Cas *b*.

Théorème III. Si $(K/k)_0/(K/k_{-1})$, K/k *est complètement ramifié de degré* h *premier à* p. *Pour que* K/k *soit primitif il faut et il suffit que* $h = (K:k)$ *soit premier.*

Démonstration : Comme $r_{-2}(K/k) = n_0(K/k) = 1$, $h = (K:k) = n_{-2}(K/k) = r_{-1}(K/k)$ est premier à p. On a $G_K = T_K$ et $V_K = \{1_K\}$, donc $G_K \simeq \overrightarrow{T_K/V_K}$. Pour que K/k soit primitif il faut et il suffit que G_K, donc $\overrightarrow{T_K/V_K}$ n'ait pas d'autres sous-hypergroupes que G_K et $\{1_K\}$, c'est-à-dire, d'après le théorème V du § 2, que $\beta_{-1}(G_K)$, qui est le groupe multiplicatif de toutes les racines $h^{\text{èmes}}$ de l'unité dans $\mathfrak{O}^*$, n'ait pas d'autres sous-groupes multiplicatifs que lui même et 1. Ceci n'a lieu que si h est premier. C. q. f. d.

Conséquence : Si K/k est primitif, (K/k) est ou bien un nombre premier autre que p, ou bien une puissance de p (dans le cas *c*).

Remarque : Le fait que le degré d'un corps $\mathfrak{P}$-adique primitif K/k est la puissance d'un premier (ce fait est une partie de la conséquence précédente) peut être aussi régardé comme conséquence de ce

que les corps $\mathfrak{P}$-adiques sont *métacycliques*. On a, en effet, le théorème général suivant de la théorie de GALOIS (voir : H. WEBER : „Lehrbuch der Algebra" T. 2, Buch 3) : Le degré d'un corps métacyclique primitif est la puissance d'un premier.

Théorème IV. *Le corps de* GALOIS K^*/k *de* $K/k = (K/k)_0/(K/k)_{-1}$ *s'obtient par l'adjonction à* K *des racines h-ièmes de l'unité.* K^*/K *est non ramifié.*

DÉMONSTRATION : K/k étant complètement ramifié, on a $K = k(\pi)$. Donc K^* s'obtient en adjoignant à K tous les $\sigma\pi$, $\sigma \in G'_{K/k}$. En particulier, K^* contient tous les $\frac{\sigma\pi}{\pi}$, et, étant un corps $\mathfrak{P}^*$-adique, il contient aussi toute racine de l'unité d'ordre premier à p congrue (mod $\mathfrak{P}^*$) à un $\frac{\sigma\pi}{\pi}$ ($\sigma \in G'_{K/k}$). Donc K^* contient toutes les racines h-ièmes de l'unité.

Inversement, adjoignons à K toutes ces racines de l'unité. Soit K' le corps ainsi obtenu. Quelque soit $\sigma \in G'_{K/k}$, il existe $\rho(\sigma) \in I(K')$ tel que $\frac{\sigma\pi}{\pi} \equiv \rho(\sigma) \pmod{\mathfrak{P}^*}$. Comme $\pi, \rho(\sigma) \in K'$, les conjugués de $\frac{\sigma\pi}{\pi} - \rho(\sigma)$ par rapport à K' se trouvent parmi les $\frac{\sigma_1\pi}{\pi} - \rho(\sigma)$ ($\sigma_1 \in G_{K/k}$). Or, puisque $G_{K/k} = T_{K/k}/V_{K/k}$, on ne peut avoir $\beta_{-1}(\sigma_1) = \beta_{-1}(\sigma)$ que si $\sigma_1 = \sigma$. Donc, si $\sigma' \neq \sigma$, $\frac{\sigma_1\pi}{\pi} \not\equiv \frac{\sigma\pi}{\pi} \pmod{\mathfrak{P}^*}$. Or $\frac{\sigma\pi}{\pi} - \rho(\sigma) \equiv 0 \pmod{\mathfrak{P}^*}$. D'où, quand $\sigma' \neq \sigma$, $\frac{\sigma_1\pi}{\pi} - \rho(\sigma) \not\equiv 0 \pmod{\mathfrak{P}^*}$.

Mais K' étant un corps $\mathfrak{P}'$-adique, deux conjugués par rapport à K' doivent avoir le même ordre en $\mathfrak{P}^*$ (Lemme 2 du § 2). Donc si $\sigma_1 \neq \sigma$, $\frac{\sigma_1\pi}{\pi} - \rho(\sigma)$ n'est pas un conjugué de $\frac{\sigma\pi}{\pi} - \rho(\sigma)$. $\frac{\sigma\pi}{\pi} - \rho(\sigma)$ n'a d'autres conjugués par rapport à K' que lui-même, donc est un élément de K'. Il en est de même pour $\sigma\pi = \pi\left[\rho(\sigma) + \left(\frac{\sigma\pi}{\pi} - \rho(\sigma)\right)\right]$. Donc K' contient tous les $\sigma\pi$, $\sigma \in G'_{K/k}$; donc $K' \supseteq K^*$. Comme $K^* \supseteq K'$, on a $K^* = K'$.

C. q. f. d.

M. HENSEL démontre les théorèmes III et IV en montrant que si K/k est complètement ramifié et si $h = (K : k)$ est premier à p, $K = k(\sqrt[h]{\pi})$, où π est un nombre de k d'ordre 1 en p. Je démontre

au § 10 un théorème dont le théorème indiqué de M. HENSEL est un cas très particulier, et sa méthode de démonstration peut être regardée comme une généralisation de celle de M. HENSEL. Mais on peut aussi démontrer le théorème de M. HENSEL à partir du théorème IV de ce §, au moyen de la théorie des corps Kummeriens.

CAS *c*.

Si $K/k = (K/k)_1/(K/k)_0$, K/k n'a qu'un seul nombre de ramification propre $v_0(K/k)$. Ce nombre sera désigné simplement par $v(K/k)$ (ou même v), son dénominateur sera désigné par δ, l'exposant auquel appartient $p \pmod\delta$ sera désigné par ψ, enfin $M_0^{(\pi_0)}(K/k)$ sera désigné par $M^{(\pi_0)}(K/k)$ (ou même $M^{(\pi_0)}$).

Théorème V. *Pour que* $K/k = (K/k)_1/(K/k)_0$ *soit primitif, il faut et il suffit que* $M_0^{(\pi_0)}(K/k)$ *n'ait d'autres sous-*$W_{F,\psi}$*-modules que lui-même et* $\{0\}$.

DÉMONSTRATION : Comme $G_K = V_K^{(0)}$ et $V_K^{(1)} = \{1_K\}$, on a $G_K \sim V_K^{(0)\to(1)}/V_K$. D'après le théorème X du § 2, pour que $A/V_K^{\to(1)}$ soit sous-hypergroupe de $V_K^{(0)\to(1)}/V_K$, c. à. d. pour que A soit celui de G_K, il faut et il suffit que $\beta_0^{(\pi_0)}(A)$ soit un sous-$W_{F,\delta}$-module de $M^{(\pi_0)}$. D'où le théorème.

Théorème VI. *Si* $K/k = (K/k)_1/(K/k)_0$, *et si* ϕ *est le plus petit entier tel que* $\Omega_\phi \supseteq M^{(\pi_0)}(K/k)$, *le corps de* GALOIS K^*/k *de* K/k *est sous-corps du corps* $K_{\phi,\delta}/k$ *obtenu et adjoignant à* K/k *le nombre* $\sqrt[\delta]{\pi}$ *et toutes les racines* $p^\phi - 1^{\text{ièmes}}$ *de l'unité.* $(K^*/K)_0 = K^*/K$.

DÉMONSTRATION : Quelque soit $\sigma \in G_{K/k}$, $I(K_{\phi,\delta})$ contient un nombre $\rho(\sigma)$ tel que $\frac{\sigma\pi - \pi}{\pi\pi_0^{Dv}} \equiv \rho(\sigma) \pmod{\mathfrak{P}^*}$ où K/k est un surcorps galoisien de $K_{\phi,\delta}/k$. D'autre part, puisque $M^{(\pi_0)}(K/k)$ est un Ω_ψ-module, on a $\phi \equiv 0 \pmod\psi$, donc $p^\phi - 1 \equiv 0 \pmod\delta$; il en résulte que $K_{\phi,\delta}$ contient toutes les racines $\delta^{\text{ièmes}}$ de l'unité, et comme π_0^{Dv} ne diffère d'une puissance de $\sqrt[\delta]{\pi}$ que par un facteur racine $\delta^{\text{ième}}$ de l'unité, $\pi_0^{Dv} \in K_{\phi,\delta}$. Comme $K_{\phi,\delta} \ni \pi$, tous les conjugués de $\frac{\sigma\pi - \pi}{\pi\pi_0^{Dv}} - \rho(\sigma)$ par rapport à

$K_{\phi,\delta}$ sont parmi les nombres $\frac{\sigma_1\pi-\pi}{\pi\pi_0^{Dv}} - \rho(\sigma)$ ($\sigma_1 \in G_{K/k}$). Or, puisque $G_{K/k} = V^{(0)}_{K/k} / V^{(1)}_{K/k}$, $\beta_0^{(\pi_0)}(\sigma_1) = \beta_0^{(\pi_0)}(\sigma)$ n'a lieu que si $\sigma_1 = \sigma$. Donc, puisque $\frac{\sigma\pi - \pi}{\pi\pi_0^{Dv}} - \rho(\sigma) \equiv 0 \pmod{\mathfrak{P}^*}$, on a, quand $\sigma' \neq \sigma$, $\frac{\sigma'_1\pi-\pi}{\pi\pi_0^{Dv}} - \rho(\sigma) \neq 0 \pmod{\mathfrak{P}^*}$. Par conséquent, $\frac{\sigma\pi - \pi}{\pi\pi_0^{Dv}} - \rho(\sigma)$ n'a d'autres conjugués par rapport à $K_{\phi,\delta}$ que lui-même, donc est élément de $K_{\phi,\delta}$. Il en est de même pour $\sigma\pi = \pi\pi_0^{Dv} \cdot \left[\rho(\sigma) + \left(\frac{\sigma\pi - \pi}{\pi\pi_0^{Dv}} - \rho(\sigma)\right)\right] + \pi$. $K_{\phi,\delta}$ contient tous les $\sigma\pi$, $\sigma \in G_{K/k}$, donc $K_{\phi,\delta} \supseteq K^*$. On a $n_{-1}(K_{\phi,\delta}/K) = \delta \equiv\!\!\!| \equiv 0 \pmod{p}$, donc aussi $n_{-1}(K^*/k) \equiv\!\!\!| \equiv 0 \pmod{p}$. Par conséquent, $(K^*/K)_0 = K^*/K$.

C. q. f. d.

Théorème VII. *Le groupe de* Galois $\mathfrak{G}$ *de* K/k *est au plus 3-transitif. Pour que* $\mathfrak{G}$ *puisse être 2-transitif il faut que* K/k *soit primitif et complètement ramifié. Pour que* $\mathfrak{G}$ *puisse être 3-transitif il faut, de plus, que* $(K:k)$ *soit une puissance de* p.

Démonstration : μ étant un entier $< (K:k)$, $\mathfrak{G}$ n'est pas μ-transitif, si, et seulement si l'on peut adjoindre à k $\mu - 1$ conjugués d'un nombre α tel que $K = k(\alpha)$ de manière à ce que les $(K:k) - \mu + 1$ conjugués restants de α ne soient pas tous conjugués entre eux par rapport au corps ainsi formé. De plus, $\mathfrak{G}$ n'est jamais $(K:k)$-transitif. Ceci posé, soit d'abord $f > 1$. $K = k(\alpha)$ contient une racine primitive p^F—$1^{\text{ième}}$ de l'unité ρ. Si $\sigma_1\alpha$ et $\sigma_2\alpha$ ($\sigma_1, \sigma_2 \in G'_{K/k}$) sont conjugués par rapport à $K = k(\alpha)$, $\sigma_1\rho = \rho^{N^+(\mathfrak{p})^{i_k(\sigma_1)}}$ et $\sigma_2\rho = \rho^{N^+(\mathfrak{p})^{i_k(\sigma_2)}}$ le sont aussi. Mais ceci n'est possible, puisque $\rho \in K$, que si $i_k(\sigma_1) = i_k(\sigma_2)$. Donc, si $(K:k) \neq 2$, il existe $\sigma_1\alpha$ et $\sigma_2\alpha$ ($\sigma_1, \sigma_2 \in G'_{K/k}$) non conjugués par rapport à K et $\mathfrak{G}$ n'est pas 2-transitif. Si $(K:k) = f = 2$, $\mathfrak{G}$ n'est pas non plus 2-transitif. Supposons maintenant que $f = 1$, mais que K/k n'est pas primitif. Alors $K = k(\pi)$. S'ils existent $\sigma_1, \sigma_2 \in G'_{K/k}$ tels que $v(\sigma_1) \neq v(\sigma_2)$, $\sigma_1\pi - \pi$ et $\sigma_2\pi - \pi$ ne sont pas conjugués par rapport à K, donc $\sigma_1\pi$ et $\sigma_2\pi$ ne le sont pas non plus ; $\mathfrak{G}$ n'est pas 2-transitif. Si tous les $v(\sigma)$ des $\sigma \in G'_{K/k}$ sont égaux, deux cas peuvent se présenter : α) les $v(\sigma)$ sont nuls : alors $(K:k) = h$ est premier à p et h n'est pas premier (cas K/k n'est pas primitif). Soit h_1 un facteur propre de h. Ils existent $\sigma_1, \sigma_2 \in G'_{K/k}$ tels que $\beta_{-1}(\sigma_1)^{h_1} = 1$ et $\beta_{-1}(\sigma_2)^{h_1} \neq 1$. Alors $\left(\frac{\sigma_1\pi}{\pi}\right)^{h_1} - 1$ et $\left(\frac{\sigma_2\pi}{\pi}\right)^{h_1} - 1$ ne sont pas conjugués par rapport à K, et $\sigma_1\pi$ et $\sigma_2\pi$ ne le sont pas non plus ; $\mathfrak{G}$ n'est pas 2-transitif. β) $v(\sigma) = v_0(K/k) > 0$ pour tout $\sigma \in G'_{K/k}$, et, puisque K/k n'est pas primitif, $M^{(\pi_0)}(K/k)$ a un sous-module propre M tel que $[M]_{F,\delta} = M$. Supposons que $0 \neq \beta_0^{(\pi_0)}(\sigma_1) \in M$. Soit $\sigma_2\pi$ un conjugué de $\sigma_1\pi$ par rapport à K. Alors, manifestement, pour une racine δ-ième convenable de l'unité ε, $\frac{\sigma_2\pi - \pi}{\varepsilon\pi\pi_0^{Dv}} \in \frac{\beta^{(\pi_0)}(\sigma_2)}{\varepsilon}$ conjugué par rapport à K de $\frac{\sigma_1\pi - \pi}{\pi\pi_0^{Dv}} \in \beta_0^{(\pi_0)}(\sigma_1)$.

Mais alors il existe un i tel que $\frac{\sigma_2\pi - \pi}{\varepsilon\pi\pi_0^{Dv}} \equiv \left(\frac{\sigma_1\pi - \pi}{\pi\pi_0^{Dv}}\right)^{N_K^+(\mathfrak{P})^i}$, c'est-à-dire $\beta_0^{(\pi_0)}(\sigma_2) = \varepsilon\ \mathfrak{Z}^i\beta_0^{(\pi_0)}(\sigma_1) \in [M]_{F,\delta} = M$. Donc, si $\beta_0^{(\pi_0)}(\sigma_2)$ n'est pas dans M, $\sigma_2\pi$ n'est pas conjugué de $\sigma_1\pi$ par rapport à K ; $\mathfrak{G}$ n'est pas 2-transitif.

Supposons que K/k soit primitif et complètement ramifié. Alors, ou bien $(K/k) = h$ est premier autre p, ou bien $(K:k)$ est une puissance de p. Dans le premier cas, soit $\sigma \in G'_{K/k}$. $k(\pi, \sigma\pi)$ contient $\frac{\sigma\pi}{\pi}$, donc contient toutes les racines $h^{\text{ièmes}}$ de l'unité, et, de plus, $k(\pi, \sigma\pi) \supset k(\pi) = K$. Donc $k(\pi, \sigma\pi) = K^*$ et $\mathfrak{G}$ n'est pas 3-transitif. Dans le deuxième cas, supposons d'abord que $(K:k) > p$. Alors on peut trouver $\sigma_1, \sigma_2 \in G'_{K/k}$ tels que $\frac{\beta_0^{(\pi_0)}(\sigma_2)}{\beta_0^{(\pi_0)}(\sigma_1)}$ ne soit pas dans Ω_1. $k(\pi, \sigma_1\pi, \sigma_2\pi)$ contient $\frac{\sigma_2\pi - \pi}{\sigma_1\pi - \pi}$ et $\sigma_1\pi - \pi$. Il existe σ_3 tel que $\beta_0^{(\pi_0)}(\sigma_3) = \beta_0^{(\pi_0)}(\sigma_1) + \beta_0^{(\pi_0)}(\sigma_2)$, et σ_3 est distinct des $\sigma_1, \sigma_2, 1_K$. $\frac{\sigma_3\pi - \pi}{\sigma_1\pi - \pi} - \frac{\sigma_2\pi - \pi}{\sigma_1\pi - \pi} - 1 \equiv 0 \pmod{\mathfrak{P}^*}$. D'autre part, puisque $G_{K/k} = V^{(0)}_{K/k} / V^{(1)}_{K/k}$, tous les autres $\frac{\sigma\pi - \pi}{\sigma_1\pi - \pi} - \frac{\sigma_2\pi - \pi}{\sigma_1\pi - \pi} - 1$ ($\sigma \in G_{K/k}$) sont incongrûs à 0 (mod $\mathfrak{P}^*$). Donc $\frac{\sigma_3\pi - \pi}{\sigma_1\pi - \pi} - \frac{\sigma_2\pi - \pi}{\sigma_1\pi - \pi} - 1$ n'a d'autres conjugués par rapport à K lui-même et il en est de même pour $\sigma_3\pi$. Donc $\mathfrak{G}$ n'est pas 4-transitif. Enfin, si $(K:k) = p$, soit $\sigma \in G'_{K/k}$. Si $\sigma_1 \in G_{K/k}$, $\frac{\sigma_1\pi - \pi}{\sigma\pi - \pi}$ est congrù (mod $\mathfrak{P}^*$) à un entier rationnel $\theta(\sigma_1)$; et $\theta(\sigma_1) = \theta(\sigma_2)$ seulement si $\sigma_1 = \sigma_2$. Donc

$\frac{\sigma_1\pi - \pi}{\sigma\pi - \pi}$ n'a d'autres conjugués par rapport à $k(\pi, \sigma\pi)$ que lui-même, ét $\mathfrak{G}$ n'est pas 3-transitif. Le théorème est démontré.

Conséquence : Le groupe de Galois d'un corps $\mathfrak{P}$-adique ne peut être à la fois imprimitif et 2-transitif.

§ 4. — L'étude d'un anneau non commutatif.

L'anneau $W_{a,b}$.

Considérons les systèmes $\lambda = \{\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots\}$ d'éléments $\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots$ du champ de Galois Ω_b tels que $\alpha_n = 0$ pour tout $n > m(\lambda)$, où $m(\lambda)$ est un entier dépendant de λ α_n s'appelera la $n^{ième}$ composante de λ et sera désignée encore par λ_n.

Définissons dans l'ensemble de tous les λ de cette forme les opérations d'addition et de multiplication (non commutative en général) par

$$(\lambda+\mu)_n = \lambda_n + \mu_n$$

$$(\lambda\mu)_n = \sum_{n_1+n_2=n} \lambda_{n_1} \mu_{n_2}^{p^{n_1 a}}.$$

On vérifie facilement que l'ensemble de tous les

$$\lambda = \{\lambda_n\}_{n=0,1,\ldots,\infty;\ \lambda_n = 0,\ \text{si } n > m(\lambda)}$$

ainsi organisé est un anneau. Cet anneau sera désigné $W_{a,b}$. Un élément de $W_{a,b}$ de forme $\{\alpha, 0, 0, \ldots\}$ sera identifié avec l'élément α de Ω_b, donc désigné par α. L'élément $\{0, 1, 0, 0, \ldots\}$ sera désigné par z_a. On voit donc que

$$\lambda = \sum_{n=0}^{m(\lambda)} \lambda_n z_a^n \qquad (\text{on pose } z_n^0 = 1).$$

Mettons de coté l'élément 0 de $\Omega_{a,b}$. Pour tout autre élément λ de $W_{a,b}$ il existe un $\nu(\lambda)$ tel que $\lambda_{\nu(\lambda)} \neq 0$ et $\lambda_n = 0$ si $n > \nu(\lambda)$. Ce $\nu(\lambda)$ s'appelera le *degré* de λ. L'ensemble des éléments de $W_{a,b}$ autres que 0 sera désigné par $W'_{a,b}$.

Théorème I. *Si* $\lambda, \mu \in W'_{a,b}$, $\nu(\lambda\mu) = \nu(\lambda) + \nu(\mu)$.

Démonstration : $\lambda\mu = \sum_{n_1=0}^{\nu(\lambda)} \lambda_{n_1} z_a^{n_1} \cdot \sum_{n_2=0}^{\nu(\lambda)} \mu_{n_2} z_a^{n_2} =$

$$= \lambda_{\nu(\lambda)} \mu_{\nu(\mu)}^{p^{a\nu(\lambda)}} z_a^{\nu(\lambda)+\nu(\mu)} + \sum_{n=0}^{\nu(\lambda)+\nu(\mu)-1} (\lambda\mu)_n z_a^n$$

Or, si $\lambda_{\nu(\lambda)} \neq 0$ et $\mu_{\nu(\mu)} \neq 0$, aussi $\mu_{\nu(\mu)}^{p^{a\nu(\lambda)}} \neq 0$ et $\lambda_{\nu(\lambda)} \mu_{\nu(\mu)}^{p^{a\nu(\lambda)}} \neq 0$ (parce que Ω_b est corps). D'où le théorème.

Conséquence : Dans $W'_{a,b}$ il n'y a pas de diviseur de 0. Si $\lambda, \mu', \mu'' \in W'_{a,b}$ et $\lambda\mu = \lambda\mu''$ ($\mu'\lambda = \mu''\lambda$) on a $\mu' = \mu''$.

Démonstration : Si $\lambda, \mu \in W'_{a,b}$, il existe $\nu(\lambda)$ et $\nu(\mu)$ et $(\lambda\mu)_{\nu(\lambda)+\nu(\mu)} \neq 0$, donc $\lambda\mu \neq 0$. Si $\lambda\mu' = \lambda\mu''$ (resp. $\mu'\lambda = \mu''\lambda$), on a $\lambda(\mu' - \mu'') = 0$ d'où, si $\lambda \neq 0$, $\mu' - \mu'' = 0$. C. q. f. d.

Conséquence : Les seules unités $\overleftarrow{\text{et}}$ unités $\overrightarrow{\text{de}}$ $W_{a,b}$ sont les éléments de Ω_b.

Démonstration : Soit ε une unité $\overleftarrow{\text{de}}$ $W_{a,b}$. Il existe, par définition, $\varepsilon' \in W_{a,b}^*$ tel que $\varepsilon'\varepsilon = 1$. Mais aucun des ε, ε' n'est nul, car autrement $\varepsilon'\varepsilon = 0$. Donc $\nu(\varepsilon') + \nu(\varepsilon) = \nu(1) = 0$, et $\nu(\varepsilon) = 0$, c'est-à-dire $\varepsilon \in \Omega_b$. Comme Ω_b est un corps, la reciproque est aussi vraie.

Démonstration analogue pour les unités.

Centre de $W_{a,b}$. Pour qu'un élément λ de $W_{a,b}$ appartienne à son centre, il faut et il suffit qu'il soit permutable avec z_a et avec les éléments de Ω_b. Soit $\alpha \in \Omega_b$. On a

$$(\alpha\lambda)_n = \alpha\lambda_n \qquad (\lambda\alpha)_n = \lambda_n \alpha^{p^{an}};$$

pour que

$$\alpha\lambda = \lambda\alpha$$

il faut et il suffit que pour tout $\alpha \in \Omega_b$ et pour tout n on ait $\lambda_n(\alpha^{p^{an}} - \alpha) = 0$, c'est-à-dire que soit $\lambda_n = 0$, soit $an \equiv 0 \pmod{b}$; donc, si $\lambda_n \neq 0$ $n \equiv 0 \left(\mathrm{mod}\ \frac{b}{(a,b)}\right)$. C'est-à-dire si $\nu(\lambda) = \frac{b}{(a,b)} \cdot \nu'(\lambda)$,

$$\lambda = \sum_{n=0}^{\nu'(\lambda)} \lambda_{\frac{b}{(a,b)}n} z_a^{\frac{b}{(a,b)}n}.$$

On a d'autre part $(z_a\lambda)_n = \lambda_n^{p^{-a}}$, $(\lambda z_a)_n = \lambda_n$, donc, pour que

$$z_a\lambda = \lambda z_a$$

il faut et il suffit que pour chaque n on ait $\lambda_n^{p^{-a}} = \lambda_n$ c'est-à-dire $\lambda_n \in \Omega_a$. Comme $\lambda_n \in \Omega_b$, on doit avoir $\lambda_n \in \Omega_a \cap \Omega_b = \Omega_{(a,b)}$.

On a

$$z_a^{\overleftarrow{(a,b)}}\alpha = \alpha^{p^{\overleftarrow{\frac{ab}{(a,b)}}}} z_a^{\overleftarrow{(a,b)}} = \alpha^{p^{m(a,b)}} z_a^{\overleftarrow{(a,b)}}$$

où $m(a, b)$ est le p. p. c. m de a, b.

Si l'on associe à λ appartenant au centre de $W_{a,b}$ l'élément $\overline{\lambda}$ de $W_{(a,b),\,m(a,b)}$ tel que $\overline{\lambda}_n = \lambda\, {}_{\overleftarrow{(a,b)}}{}^n$, on voit que le centre de $W_{a,b}$ est isomorphe à $W_{m(a,b),\,(a,b)}$. Nous considérerons ces deux anneaux comme identiques, en identifiant $\overline{\lambda}$ avec λ (il suffit pour cela d'identifier $z_a^{\overleftarrow{(a,b)}}$ avec $z_{m(a,b)}$).

$W_{m(a,b),\,(a,b)}$ est son propre centre car $[(a, b), m(a, b)] = (a, b)$, $m[(a, b), m(a, b)] = m(a, b)$.

Donc $W_{m(a,b),\,(a,b)}$ est isomorphe à l'anneau de polynomes dans $\Omega_{(a,b)}$, et les éléments de $W_{m(a,b)\,(a,b)}$ se décomposent, et d'une seule manière, à facteurs éléments de $\Omega_{(a,b)}$ près, en produits d'éléments indécomposables.

Divisibilité dans $W_{a,b}$.

Théorème II. *Si* $A, B \neq 0 \in W_{a,b}$ *il existe* $\lambda, \lambda', C, C' \in W_{a,b}$ *tels que*
1. $A = \lambda B + C = B\lambda' + C'$,
2. *Si* $C \neq 0$ *(resp.* $C' \neq 0$*),* $\nu(C) < \nu(B)$ [resp. $\nu(C') < \nu(B)$].

Démonstration : Si $\nu(A) < \nu(B)$ (ou $A = 0$) il suffit de poser $\lambda = \lambda' = 0$, $C = C' = A$. Supposons que le théorème soit exact quand $\nu(A) < m$, où $m \geq \nu(B)$. Montrons qu'il est vrai encore quand $\nu(A) = m$. Soient x, x éléments de Ω_b et $y = xz_a^{\nu(A)-\nu(B)} = xz_a^{m-\nu(B)}$, $y' = x'z_a^{m-\nu(B)}$. Les dégrés de $A - yB$ et de $A - By'$ ne dépassent pas m et on a

$$(A - yB)_m = A_m - xB^{p^{a[m-\nu(B)]}}_{\nu(B)};$$

$$(A - By')_m = A_m - x'^{p^{a\nu(B)}} B_{\nu(B)} = (A_m^{p^{-a\nu(B)}} - x' B^{p^{-a\nu(B)}}_{\nu(B)})^{p^{a\nu(B)}}$$

$B_{\nu(B)}$, donc aussi $B^{p^{-a\nu(B)}}_{\nu(B)}$ et $B^{p^{a[m-\nu(B)]}}_{\nu(B)}$ sont non nuls. Il existe $x, x' \in \Omega_b$ tels que $A_m - xB^{p^{a[m-\nu(B)]}}_{\nu(B)} = a - x'B^{p^{-a\nu(B)}}_{\nu(B)} = 0$ et alors $A' = A - yB$ et $A'' = A - By$ sont de degré $< m$. Il existe, par suite, $\mu, \mu', C, C' \in W_{a,b}$ tels que $\nu(C) < \nu(B)$ [resp. $\nu(C') < \nu(B)$] ou $C = 0$ ($C' = 0$) et que $A' = \mu B + C$, $A'' = B\mu' + C'$. Si l'on pose $\lambda = y + \mu$, $\lambda' = y' + \mu'$ on voit que le théorème est vrai pour $\nu(A) = m$, ce qui le démontre complètement.

Définition 1 : C, C' s'appellent les *moindres restes* de A resp. $\overleftarrow{\text{mod B}}$, $\overrightarrow{\text{mod B}}$.

Remarque : Il n'y a qu'un seul moindre reste de A ($\overleftarrow{\text{mod B}}$) [resp. ($\overrightarrow{\text{mod B}}$)]. En effet, si par exemple $A = \lambda B + C = \mu B + D$, $C \neq D$ et $\nu(C) < \nu(B)$ (ou $C = 0$), on a $D = (\lambda - \mu)B + C$, d'où $\nu(D) \geq \nu(B)$.

Théorème III. *Tout idéal unilatèral ou bilatère de* $W_{a,b}$ *est principal.*

Démonstration : Démontrons d'abord le théorème pour les $\overleftarrow{\text{idéaux}}$, la démonstration pour les $\overrightarrow{\text{idéaux}}$ sera analogue. Soient Λ un $\overleftarrow{\text{idéal}}$ de $W_{a,b}$ et λ — un élément non nul de Λ de moindre degré possible. [Il en existe, si $\Lambda \neq (0)$]. Le moindre reste γ de tout autre $\lambda' \in \Lambda$ ($\overleftarrow{\text{mod } \lambda}$) est encore dans Λ. Donc, puisque $\nu(\gamma) < \nu(\lambda)$ ou $\gamma = 0$, on doit avoir $\gamma = 0$, c'est-à-dire tous les éléments de Λ sont $\overleftarrow{\text{multiples}}$ de λ et $\Lambda = \overleftarrow{(\lambda)}$. Il reste à démontrer le théorème pour les idéaux bilatères. Soit Λ un tel idéal. Alors il existe $\lambda, \lambda' \in W_{a,b}$ tels que $\Lambda = \overleftarrow{(\lambda)} = \overrightarrow{(\lambda')}$. Comme, si $\varepsilon \in \Omega_b$, on a $\overleftarrow{(\varepsilon\lambda)} = \overleftarrow{(\lambda)}$ et $\overrightarrow{(\lambda\varepsilon)} = \overrightarrow{(\lambda)}$, on peut supposer $\lambda_{\nu(\lambda)} = \lambda'_{\nu(\lambda')} = 1$. $\lambda' \in \Lambda$, donc $\lambda' = \mu\lambda$ et $\nu(\lambda') \geq \nu(\lambda)$. De même $\lambda \in \Lambda$, donc $\lambda = \lambda'\mu'$ et $\nu(\lambda) \geq \nu(\lambda')$. D'où $\nu(\lambda) = \nu(\lambda')$, $\nu(\mu) = \nu(\lambda') - \nu(\lambda) = 0$, donc $\mu \in \Omega_b$ et comme $1 = \lambda'_{\nu(\lambda)} = \mu\lambda_{\nu(\lambda)} = \mu$, on a $\lambda = \lambda'$ et $\Lambda = \overleftarrow{(\lambda)} = \overrightarrow{(\lambda)}$.

C. q. f. d.

Théorème IV. *Si* $\overleftarrow{(\lambda)} = \overrightarrow{(\lambda)}$, λ *est associé du produit d'un élément du centre de* $W_{a,b}$ *par une puissance de* z_a *et reciproquement.*

Démonstration : Faisons correspondre à chaque λ un λ^* défini par $\lambda_n^* = \lambda_n^{p^{-a}}$ $(n = 0, 1, \ldots, \infty)$. On voit que $\lambda z_a = z_a \lambda^*$. Nous posons de plus, $\lambda = {}^*(\lambda^*)$:

Soit $\overleftarrow{(\lambda)} = \overrightarrow{(\lambda)}$ et $\lambda_0 = \lambda_1 = \ldots = \lambda_{r-1} = 0$, $\lambda_r \neq 0$. On a $\lambda = \mu z_a^r$ où $\mu_n = \lambda_{n+r}$ et $\mu_0 \neq 0$. Si $\mu' = \{|((\mu^*)^*), \ldots,]^*\}^*$ (r fois), on a $\lambda = \mu z_a^r = z_a^r \mu'$.

Si $\varepsilon \in \Omega_b$, on a $\varepsilon\lambda = \lambda'\mu$ où $\nu(\mu) = \nu(\varepsilon\lambda) - \nu(\lambda) = 0$, c'est-à-dire $\mu \in \Omega_b$. Donc $\overleftarrow{(\varepsilon\lambda)} = \overleftarrow{(\lambda)} = \overrightarrow{(\lambda)} = \overrightarrow{(\lambda\mu)} = \overrightarrow{(\varepsilon\lambda)}$ et on peut supposer $(\varepsilon\lambda)_{\nu(\lambda)} = 1$. Nous posons donc $\lambda_{\nu(\lambda)} = 1$.

On doit avoir $z_a\lambda = \lambda\gamma$ où $\gamma \in W_{a,b}$; on a $v(\gamma) = v(z_a\lambda) - v(\lambda) = 1$ c'est-à-dire $\gamma = \rho z_a + \tau$, $\rho, \tau \in \Omega_b$. On a $(z_a\lambda)_r = 0$ et $[\lambda(\rho z_a + \tau)]_r = \lambda_r \tau^{p^{ar}}$, donc $\tau = 0$. D'autre part $(z_a\lambda)_{v(\lambda)} = 1^{p^a} = 1$ et $(\lambda\rho z_a)_{v(\lambda)} = \lambda_{v(\lambda)}\, \rho^{p^{av(\lambda)}} = \rho^{p^{av(\lambda)}}$, d'où $\rho = 1$ c'est-à-dire $z_a\lambda = \lambda z_a$ ou $z_a \mu z_a^r = \mu z_a^{r+1} = \mu z_a . z_a^r$ donc $\mu z_a = z_a \mu$ et $\mu = \mu'$.

Cela posé, soit α un élément quelconque de $W_{a,b}$. On doit avoir $\alpha\lambda = \lambda\alpha'$, c'est-à-dire en particulier, si $\beta = {}^*\{{}^*[\ldots({}^*({}^*(\alpha)))\ldots]\}$ (r fois) on a $\beta\lambda = \lambda\beta$, c'est-à-dire $\beta z_a^r \mu = z_a^r \mu \beta'$. Mais $\beta z_a^r = z_a^r \alpha$, d'où $\alpha\mu = \mu\beta'$, c'est-à-dire $\overleftarrow{(\mu)} \supseteq \overrightarrow{(\mu)}$; de la même manière on voit que $\overrightarrow{(\mu)} \supseteq \overleftarrow{(\mu)}$ c'est-à-dire $\overleftarrow{(\mu)} = \overrightarrow{(\mu)}$. On a $\mu_{v(\mu)} = 1$ et $\mu_0 \neq 0$.

μ est permutable avec z_a. Soit $\varepsilon \in \Omega_b$. On a $\varepsilon\mu = \mu\varepsilon'$ où $v(\varepsilon') = v(\varepsilon\mu) - v(\mu) = 0$, c'est-à-dire $\varepsilon' \in \Omega_b$. Donc, puisque $(\varepsilon\mu)_0 = \varepsilon\mu_0$ et $(\mu\varepsilon')_0 = \varepsilon'\mu_0$ on a $\varepsilon = \varepsilon'$ et μ est permutable avec les éléments de Ω_b. Donc μ appartient au centre de $W_{a,b}$.

Si, inversement $\lambda = \mu z_a^r$ où $\mu \varepsilon W_{m(a,b),(a,b)}$, on a pour $\alpha \in W_{a,b}$, $\alpha\lambda = \alpha\mu z_a^r = \mu\alpha z_a^r = \mu z_a \alpha^* z_a^{r-1} = \ldots = \mu z_a^r \alpha' = \lambda\alpha'$ où $\alpha' = \{[\ldots(((\alpha^*)^*)^*)^*\ldots]^*\}^*$, ($r$ fois)

donc $\overleftarrow{(\lambda)} \supseteq \overrightarrow{(\lambda)}$. De même $\overrightarrow{(\lambda)} \supseteq \overleftarrow{(\lambda)}$, donc $\overleftarrow{(\lambda)} = \overrightarrow{(\lambda)}$. Si $\varepsilon \in \Omega_b$, on a $\varepsilon\lambda = \lambda\varepsilon'$ où $\varepsilon' \in \Omega_b$, donc $\overleftarrow{(\varepsilon\lambda)} = \overleftarrow{(\lambda)} = \overrightarrow{(\lambda)} = \overrightarrow{(\lambda\varepsilon')} = \overrightarrow{(\varepsilon\lambda)}$ et le théorème est démontré.

Théorème V. A, B, . . . , L *étant éléments de* $W_{a,b}$, *il y a un et un seul* $\overleftarrow{\text{multiple}}$ ($\overrightarrow{\text{multiple}}$) *commun* $\overleftarrow{\mathfrak{M}}(A, B, \ldots, L)$ [$\overrightarrow{\mathfrak{M}}(A, B, \ldots, L)$] *de* A, B, . . . , L *tel que* 1. $\overleftarrow{\mathfrak{M}}(A, B, \ldots, L)_{v[\overleftarrow{\mathfrak{M}}(A, B, \ldots, L)]} = 1$ $[\overrightarrow{\mathfrak{M}}(A, B, \ldots, L)]_{v[\overrightarrow{\mathfrak{M}}(A, B, \ldots, L)]} = 1$]. 2. *Tout* $\overleftarrow{\text{multiple}}$ ($\overrightarrow{\text{multiple}}$) *commun de* A, B, . . . , L *est son* $\overleftarrow{\text{multiple}}$ ($\overrightarrow{\text{multiple}}$).

Démonstration : L'ensemble des $\overleftarrow{\text{multiples}}$ ($\overrightarrow{\text{multiples}}$) communs de A, B, . . . , L est un $\overleftarrow{\text{idéal}}$ ($\overrightarrow{\text{idéal}}$) Λ. Soit $\Lambda = \overleftarrow{(\lambda)}$. Si $(\varepsilon\lambda)_{v(\lambda)} = 1$ ($\varepsilon \in \Omega_b$), on peut poser $\overleftarrow{\mathfrak{M}}(A, B, \ldots, L) = \varepsilon\lambda$. Si λ et λ' satisfont aux conditions du théorème, $\lambda - \lambda'$ est encore un $\overleftarrow{\text{multiple}}$ de A, B, . . . , L c'est-à-dire $\lambda - \lambda' \in \Lambda$ et, de plus, $(\lambda - \lambda')_{v(\lambda)} = 1 - 1 = 0$. Comme $\Lambda = \overleftarrow{(\lambda)}$, on doit avoir $\lambda = \lambda'$. C. q. f. d.

Définition 2 : $\overleftarrow{\mathfrak{M}}(A, B, \ldots, L)$ [resp. $\overrightarrow{\mathfrak{M}}(A, \ldots, L)$ s'appelle *le plus petit commun* $\overleftarrow{\text{multiple}}$ (resp. $\overrightarrow{\text{multiple}}$) de A, B, . . . , L.

Théorème VI. *Si* A, B, . . . , L $\in W_{a,b}$, *parmi les* $\overleftarrow{\text{diviseurs}}$ ($\overrightarrow{\text{diviseurs}}$) *communs de* A, B, . . , L *il y a un et un seul* $\overleftarrow{\mathfrak{D}}(A, B, \ldots, L)$ [$\overrightarrow{\mathfrak{D}}(A, B, \ldots, L)$] *tel que* 1. $\overleftarrow{\mathfrak{D}}(A, B, \ldots, L)_{v[\overleftarrow{\mathfrak{D}}(A, B, \ldots, L)]} = 1$ [$\overrightarrow{\mathfrak{D}}(A, B, \ldots, L)_{v[\overrightarrow{\mathfrak{D}}(A, B, \ldots, L)]} = 1$]. 2. *Tout* $\overleftarrow{\text{diviseur}}$ ($\overrightarrow{\text{diviseur}}$) *commun de* A, B . . . , L *le divise* ($\overrightarrow{\text{divise}}$).

Démonstration : Si $\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_s\}$ est l'ensemble de tous les $\overleftarrow{\text{diviseurs}}$ ($\overrightarrow{\text{diviseurs}}$) communs de A, B, . . . , L, il suffit de poser

$\overleftarrow{\mathfrak{D}}(A, B, \ldots, L) = \overrightarrow{\mathfrak{M}}(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_s)$, $\overrightarrow{\mathfrak{D}}(A, B, \ldots, L) = \overleftarrow{\mathfrak{M}}(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_s)$.

Définition 3 : $\overleftarrow{\mathfrak{D}}(A, B, \ldots, L)$ [resp. $\overrightarrow{\mathfrak{D}}(A, B, \ldots, L)$] s'appelle le *plus grand commun* $\overleftarrow{\text{diviseur}}$ (resp. $\overrightarrow{\text{diviseur}}$) de A, B, . . . , L.

Définition 4 : Si $\overleftarrow{\mathfrak{D}}(A, B) = 1$ [resp. $\overrightarrow{\mathfrak{D}}(A, B) = 1$], A, B sont dits *premiers* (resp. *premiers*) *entre eux*.

Soient $\mathfrak{R}$, $\mathfrak{S}$ deux éléments de $W_{a,b}$. Soient $r = v(\mathfrak{R})$, $s = v(\mathfrak{S})$. Désignons par m, m', d, d' les degrés resp. de $\overleftarrow{\mathfrak{M}}(\mathfrak{R}, \mathfrak{S})$, $\overrightarrow{\mathfrak{M}}(\mathfrak{R}, \mathfrak{S})$, $\overrightarrow{\mathfrak{D}}(\mathfrak{R}, \mathfrak{S})$, $\overleftarrow{\mathfrak{D}}(\mathfrak{R}, \mathfrak{S})$.

Théorème VII. $r + s = m + d = m' + d'$,

Démonstration : Il suffit de démontrer ce théorème dans l'hypothèse $d = 0$ (resp. $d' = 0$), parceque si par exemple $\mathfrak{R} = \mathfrak{R}'$. $\overrightarrow{\mathfrak{D}}(\mathfrak{R}, \mathfrak{S})$, $\mathfrak{S} = \mathfrak{S}'$. $\overrightarrow{\mathfrak{D}}(\mathfrak{R}, \mathfrak{S})$, on a $\overrightarrow{\mathfrak{D}}(\mathfrak{R}', \mathfrak{S}') = 1$ et $\overleftarrow{\mathfrak{M}}(\mathfrak{R}, \mathfrak{S}) = \overleftarrow{\mathfrak{M}}(\mathfrak{R}', \mathfrak{S}')$. $\overrightarrow{\mathfrak{D}}(\mathfrak{R}, \mathfrak{S})$; d'où, si le théorème est exact pour $d = 0$, on a $m = d + [(r - d) + (s - d)] = r + s - d$, et le théorème est vrai dans le cas général.

Ceci posé, soit $\overrightarrow{\mathfrak{D}}(\mathfrak{R}, \mathfrak{S}) = 1$. Soit $\sum_{q=0}^{s-1} \alpha_{iq} z_a^q$ le moindre reste de $z_a^i \mathfrak{R}$ (mod $\overleftarrow{\mathfrak{S}}$). On peut trouver $\lambda_0, \lambda_1, \ldots, \lambda_s \in \Omega_b$, non tous nuls,

tels que le système $\sum_{q=0}^{s} a_{iq}\lambda_i = 0$ $(q = 0, 1, \ldots, s-1)$ soit satisfaite. Mais alors, si $\lambda = \sum_{q=0}^{s} \lambda_q z_a^q$, on a $\lambda\mathfrak{R} \overleftarrow{\equiv} 0 \pmod{\mathfrak{S}}$, c'est-à-dire $\lambda\mathfrak{R} \overleftarrow{\equiv} 0 \pmod{\overleftarrow{\mathfrak{M}}(\mathfrak{S}, \mathfrak{R})}$. Ainsi $m \leq \nu(\lambda\mathfrak{R}) = \nu(\lambda) + \nu(\mathfrak{R}) \leq s + r$. De même $m' \leq r + s$. Soit $\overleftarrow{\mathfrak{M}}(\mathfrak{R}, \mathfrak{S}) = \lambda\mathfrak{R} = \lambda'\mathfrak{S}$; soit $l = \nu(\lambda)$, $l' = \nu(\lambda')$. Si $m < r + s$, on a $l < s, l' < r$. Considérons $\overrightarrow{\mathfrak{M}}(\lambda, \lambda')$. On a $\overleftarrow{\mathfrak{M}}(\mathfrak{R}, \mathfrak{S}) \overrightarrow{\equiv} 0 \pmod{\overrightarrow{\mathfrak{M}}(\lambda, \lambda')}$. Soient $\overleftarrow{\mathfrak{M}}(\mathfrak{R}, \mathfrak{S}) = \overrightarrow{\mathfrak{M}}(\lambda, \lambda').\Delta$ et $\overrightarrow{\mathfrak{M}}(\lambda, \lambda') = \lambda\rho = \lambda'\zeta$. On a $\mathfrak{R} = \rho\Delta$, $\mathfrak{S} = \zeta\Delta$, d'où $\Delta \overrightarrow{|} \overrightarrow{\mathfrak{D}}(\mathfrak{R}, \mathfrak{S}) = 1$, c.à.d. $\nu(\Delta) \leq 0$ et $\Delta = 1$. Donc $\overrightarrow{\mathfrak{M}}(\lambda, \lambda') = \overleftarrow{\mathfrak{M}}(\mathfrak{R}\ \mathfrak{S})$ et son degré est $r + l = s + l' > l + l'$. D'autre part, si $\lambda = \overleftarrow{\mathfrak{D}}(\lambda, \lambda').\mu$, $\lambda' = \overleftarrow{\mathfrak{D}}(\lambda, \lambda').\mu'$, on a que $\mu\mathfrak{R} = \mu'\mathfrak{S}$ est encore un multiple commun non nul de $\mathfrak{R}$, $\mathfrak{S}$, donc $\overrightarrow{\mathfrak{D}}(\lambda, \lambda') = 1$. Le degré de $\overrightarrow{\mathfrak{M}}(\lambda, \lambda')$ devrait donc être $\leq l + l'$ et on a une contradiction. Donc $m < r + s$ est impossible, et $m = r + s$. C. q. f. d.

DÉFINITION 5 : Un élément λ de $W_{a,b}$ non contenu dans Ω_b s'appelle *premier* s'il n'a d'autres diviseurs que ses associés et les éléments de Ω_b.

REMARQUE : Si λ est premier, il n'a d'autres diviseurs que ses associés et les éléments de Ω_b. En effet, soit $\lambda \overleftarrow{\equiv} 0 \pmod{\lambda'}$, où λ' n'est pas dans Ω_b et n'est pas associé de λ. Alors $0 < \nu(\lambda') < \nu(\lambda)$ et $\lambda = \lambda''\lambda'$; mais il s'ensuit que λ'' est diviseur de λ et $\nu(\lambda) > \nu(\lambda'') > 0$, c'est-à-dire λ n'est pas premier.

REMARQUE : Si λ' est premier et λ'' est quelconque, $\overleftarrow{\mathfrak{D}}(\lambda', \lambda'')$ $[\overrightarrow{\mathfrak{D}}(\lambda', \lambda'')]$ est ou bien $= 1$, ou bien associé (associé) de λ'.

Théorème VIII. *Soit $\lambda', \lambda'', \ldots, \lambda^{(q)}$ un ensemble d'éléments premiers de $W_{a,b}$ tels que pour tout i, $1 \leq i < q$, $\lambda^{(i+1)}$ est premier (premier) à $\overleftarrow{\mathfrak{M}}(\lambda', \lambda'', \ldots, \lambda^{(i)})$ $[\overrightarrow{\mathfrak{M}}(\lambda', \lambda'', \ldots, \lambda^{(i)}]$. Alors* 1. *Un quelconque de ces éléments est premier (resp. premier) au p. p. c. m. (m) de tous les autres.* 2. *S'il existe un élément premier λ de $W_{a,b}$ qui divise (divise) le p. p. c. m (m.) de tous ces éléments sans diviser (diviser) aucun de p. p. c. m. (m.) de tous ces éléments sauf un, tous les $\lambda'\lambda'', \ldots, \lambda^{(q)}$ et λ sont de même degré.*

DÉMONSTRATION : Posons $\mathfrak{M} = \overleftarrow{\mathfrak{M}}(\lambda', \lambda'', \ldots, \lambda^{(q)})$, $\mathfrak{M}_i = \overleftarrow{\mathfrak{M}}(\lambda', \lambda'', \ldots, \lambda^{(i-1)}, \lambda^{(i+1)}, \ldots, \lambda^{(q)})$. Soit $\nu(\lambda^{(i)}) = l_i$. On voit que $\nu(\mathfrak{M}) = l_1 + l_2 + \ldots + l_q$, $\nu(\mathfrak{M}_i) = l_1 + l_2 + \cdots + l_{i-1} + l_{i+1} + \cdots + l_q = \nu(\mathfrak{M}) - l_i$. Si $\lambda^{(i)}$ n'est pas premier à $\mathfrak{M}_i$, on a $\mathfrak{M} = \overleftarrow{\mathfrak{M}}(\lambda', \lambda'', \ldots, \lambda^{(i-1)}, \lambda^{(i)}, \lambda^{(i+1)}, \ldots, \lambda^{(q)}) = \overleftarrow{\mathfrak{M}}(\mathfrak{M}_i, \lambda^{(i)}) = \mathfrak{M}_i$ parceque $\overrightarrow{\mathfrak{D}}(\lambda^{(i)}, \mathfrak{M}_i) \neq 1$, donc est associé de $\lambda^{(i)}$ et $\mathfrak{M}_i \overleftarrow{\equiv} 0 \pmod{\lambda^{(i)}}$; c'est-à-dire $l_i = 0$, ce qui est absurde. Si $\lambda \overrightarrow{|} \mathfrak{M}$ sans diviser $\mathfrak{M}_i$, on a $\overleftarrow{\mathfrak{M}}(\lambda, \mathfrak{M}_i) \overrightarrow{|} \overleftarrow{\mathfrak{M}}(\lambda, \mathfrak{M}) = \mathfrak{M}$ et $\nu[\overleftarrow{\mathfrak{M}}(\lambda, \mathfrak{M}_i)] = \nu(\mathfrak{M}_i) + \nu(\lambda) = \nu(\mathfrak{M}) - l_i + \nu(\lambda)$. Soit que $\overleftarrow{\mathfrak{M}}(\lambda, \mathfrak{M}_i) \neq \mathfrak{M}$ $\overleftarrow{\mathfrak{M}}(\lambda, \mathfrak{M}_i, \lambda^{(i)})$. Dans, ce cas $\lambda^{(i)}$ ne divise pas $\overleftarrow{\mathfrak{M}}(\lambda\ \mathfrak{M}_i)$, donc $\overrightarrow{\mathfrak{D}}(\lambda^{(i)}, \overleftarrow{\mathfrak{M}}(\lambda, \mathfrak{M}_i)) = 1$ et $\nu(\mathfrak{M}) = \nu[\overleftarrow{\mathfrak{M}}(\lambda, \mathfrak{M}_i)] + l_i = \nu(\mathfrak{M}) + \nu(\lambda)$, c'est-à-dire $\nu(\lambda) = 0$ ce qui est absurde, parceque alors $\lambda \in \Omega_q$ et divise $\mathfrak{M}_i$. Donc $\overleftarrow{\mathfrak{M}}(\lambda, \mathfrak{M}_i) = \mathfrak{M}$ et $\nu(\mathfrak{M}) = \nu(\mathfrak{M}) - l_i + \nu(\lambda)$, d'où $l_i = \nu(\lambda)$. Appliquant cela à chaque i on a $l_1 = l_2 = \cdots = l_q = \nu(\lambda)$. C. q. f. d.

CONSÉQUENCE : $\lambda', \lambda'', \ldots, \lambda^{(q)}$ étant les éléments premiers de $W_{a,b}$ d'un même degré l, tout diviseur (diviseur) premier de

$$\overleftarrow{\mathfrak{M}}(\lambda', \lambda'', \ldots, \lambda^{(q)})\ [\overrightarrow{\mathfrak{M}}(\lambda', \lambda'', \ldots, \lambda^{(q)})]$$

est de degré l.

DÉMONSTRATION : On peut extraire un sous-ensemble $\{\lambda^{(i_1)}, \lambda^{(i_2)}, \ldots \lambda^{(i_s)}\}$, $(1 \leq i_1 < i_2 < \cdots < i_s \leq q)$ de $\{\lambda', \lambda'', \ldots, \lambda^{(q)}\}$ tel que λ divise le p. p. c. m. de tous ces éléments sans diviser aucun des p. p. c. m de tous ces éléments sauf un. Dès lors, en appliquant le théorème VIII, on voit que $\nu(\lambda) = l$. C. q. f. d.

Rapports de divisibilité entre les éléments de $W_{a,b}$ *et les éléments de son centre :*

Nous dirons „élément premier du centre (de $W_{a,b}$)" pour désigner un élément du centre de $W_{a,b}$ qui ne se décompose pas en éléments *du centre* de $W_{a,b}$ qui ne soient pas ses associés ou unités.

Nous dirons „élément du centre (de $W_{a,b}$) premier dans $W_{a,b}$" pour désigner un élément du centre de $W_{a,b}$ premier en tant que élément de $W_{a,b}$.

Si $z^i\lambda = \lambda' z^i$, λ' sera encore désigné par $z^i\lambda z^{-i}$. On a évidemment, $z^{i_1}(z^{i_2}\lambda z^{-i_2})z^{-i_1} = z^{i_1+i_2}\lambda z^{-(i_1+i_2)}$; si $\alpha \in \Omega_b$, on a $z^i \alpha z^{-i} = \alpha^{p^{ai}}$. La transformation $\lambda \to z^i\lambda z^{-i}$ est un automorphisme de $W_{a,b}$. Il en est de même de la transformation $\lambda \to \alpha\lambda\alpha^{-1}$, $\alpha \in \Omega'_b$. On a d'ailleurs

$$z^i(\alpha\lambda\alpha^{-1})z^{-i} = \alpha^{p^{ai}} \cdot z^i\lambda z^{-i} \cdot \alpha^{-p^{ai}}.$$

Pour que λ soit dans le centre de $W_{a,b}$ il faut et il suffit que $z\lambda z^{-1} = \lambda$ et $\alpha\lambda\alpha^{-1} = \lambda$ pour tout $\alpha \in \Omega'_b$. Ceci posé on a

Théorème IX. *Si* $\bar\lambda$ *est un élement du centre de* $W_{a,b}$ *et si* $\lambda \in W_{a,b}$ *est diviseur de* λ, *il est aussi diviseur de* $\bar\lambda$

Démonstration : Soit $\bar\lambda = \lambda\lambda'$. On a $\lambda'\lambda\lambda' = \lambda'\bar\lambda = \bar\lambda\lambda'$, donc $\lambda'\lambda = \bar\lambda$ et $\lambda \mid \bar\lambda$. C. q. f. d.

Théorème X. *Si* $\bar\lambda$ *est un élément premier du centre de* $W_{a,b}$, *tous les diviseurs premiers de* $\bar\lambda$ *dans* $W_{a,b}$ *ont le même degré.*

Démonstration : Soit λ un diviseur premier de $\bar\lambda$ dans $W_{a,b}$. Puisque $\alpha.z^i\bar\lambda z^{-i}.\alpha^{-1} = \alpha\bar\lambda\alpha^{-1} = \bar\lambda$ pour tout $\alpha \in \Omega'_b$, $\alpha.z^i\lambda z^{-i}\alpha^{-1}$ est encore un diviseur premier de $\bar\lambda$. Donc, si $z^n\lambda z^{-n} = \lambda$, et si

$$L = \mathfrak{M}(\alpha.z^i\lambda z^{-i}.\alpha^{-1})_{\alpha\in\Omega'_b},\ i = 0, 1, \ldots, n-1,$$

on a $\bar\lambda \equiv 0 \pmod L$. D'autre part

$$zLz^{-1} = \mathfrak{M}[z.(\alpha.z^i\lambda z^{-i}.\lambda^{-1})z^{-1}]_{\alpha\in\Omega'_b,\ i=0,1,\ldots,n-1}$$

$$= \mathfrak{M}(\alpha^{p^a}.z^{i+1}\lambda z^{-(i+1)}\alpha^{-p^a})_{\alpha\in\Omega'_b,\ i=0,1,\ldots n-1},$$

et comme $z^n\lambda z^{-n} = \lambda$ et $\{\alpha^{p^a}\}_{\alpha\in\Omega'_b} = \Omega'_b$, on a $zLz^{-1} = L$. De même, si $\beta \in \Omega'_b$, on a $\beta(\alpha z^i\lambda z^{-i}\alpha^{-1}).\beta^{-1} = \alpha\beta.z^i\lambda z^{-i}(\alpha\beta)^{-1}$ et $\{\beta\alpha\}_{\alpha\in\Omega'_b} = \beta\Omega'_b = \Omega'_b$, d'où $\beta L\beta^{-1} = L$. Donc L est un élément de centre et comme $v(L) \neq 0$, on a

$L = \bar\lambda$. Donc $\bar\lambda$ est p. p. c. m. d'éléments premiers de $W_{a,b}$ tous de même degré; donc, d'après la conséquence du théorème VIII, tout autre diviseur (donc aussi diviseur) premier de $\bar\lambda$ dans $W_{a,b}$ a le même degré. C. q. f. d.

Soit $\frac{a}{(a,b)} = e_1$, $\frac{b}{(a,b)} = e_2$. Alors le degré commun des tous les diviseurs premiers de $\bar\lambda$ dans $W_{a,b}$ sera désigné par $m_{e_1,e_2}(\bar\lambda)$.

L'hypothèse suivante, dont je ne possède pas encore de démonstration, me semble exacte : pour e_1, e_2 $[(e_1, e_2) = 1]$ donnés, $m_{e_1,e_2}(\bar\lambda)$ ne dépend que de $m_{1,1}(\bar\lambda)$, c'est-à-dire si $m_{1,1}(\bar\lambda') = m_{1,1}(\bar\lambda'')$, aussi $m_{e_1,e_2}(\bar\lambda') = m_{e_1,e_2}(\bar\lambda'')$.

Théorème XI. λ *étant un élément premier de* $W_{a,b}$, *il existe un et un seul (à association près) élément premier* $\bar\lambda$ *du centre de* $W_{a,b}$ *dont* λ *est diviseur.*

Démonstration : L'ensemble d'éléments du centre, divisibles par λ est un idéal, soit $(\bar\lambda)$. Supposons que $\bar\lambda$ n'est pas premier, c'est-à-dire $\bar\lambda = \bar\lambda'\bar\lambda''$ $(\bar\lambda', \bar\lambda'' \in W_{m(a,b),(a,b)})$ avec $v(\bar\lambda') \neq 0$, $v(\bar\lambda'') \neq 0$. Il en résulte que $\mathfrak{D}(\lambda, \bar\lambda'') = 1$, d'où $\mathfrak{M}(\lambda, \bar\lambda'')$ a le degré $v(\lambda) + v(\bar\lambda'')$; et, comme $\bar\lambda''\lambda = \lambda\bar\lambda''$ est multiple de λ et de $\bar\lambda''$, on a, si l'on suppose $\lambda_{v(\lambda)} = \bar\lambda_{v(\bar\lambda)} = \bar\lambda'_{v(\bar\lambda')} = \bar\lambda''_{v(\bar\lambda'')} = 1$, ce qu'on peut faire, que $\mathfrak{M}(\lambda, \bar\lambda'') = \lambda\bar\lambda''$. D'où $\bar\lambda = \mathfrak{M}(\lambda, \bar\lambda) = \mathfrak{M}(\lambda, \bar\lambda', \bar\lambda) = \mathfrak{M}(\bar\lambda, \lambda\bar\lambda'') = \mathfrak{M}(\bar\lambda'\bar\lambda'', \lambda\bar\lambda'') = \mathfrak{M}(\bar\lambda', \lambda).\bar\lambda''$. On voit de même que $\mathfrak{M}(\bar\lambda', \lambda) = \lambda\bar\lambda'$, d'où $\bar\lambda = \lambda\bar\lambda'\bar\lambda'' = \lambda\bar\lambda$ et $\lambda = 1$, ce qui est absurde. Donc $\bar\lambda$ est premier. C. q. f. d.

Théorème XII. *Si* $\bar\lambda'$ *et* $\bar\lambda''$ *sont deux éléments premiers du centre de* $W_{a,b}$ *et* λ', λ'' *deux diviseurs premiers dans* $W_{a,b}$ *de* $\bar\lambda'$, $\bar\lambda''$ *resp., il existent* $\lambda''' \mid \bar\lambda'$ *et* $\lambda'''' \mid \bar\lambda''$ *tels que* $\lambda'\lambda'' = \lambda''''\lambda'''$.

Démonstration : *Si* $\bar\lambda', \bar\lambda''$ sont associés on peut poser $\lambda'''' = \lambda'$ et $\lambda''' = \lambda''$. Supposons donc, que $\bar\lambda', \bar\lambda''$ ne soient pas associés. Supposons que $\mathfrak{D}(\lambda'\lambda'', \bar\lambda') = 1$. Alors, comme dans le théorème précédent

$\overleftarrow{\mathfrak{M}}(\lambda'\lambda'', \bar\lambda')=\lambda'\lambda''\bar\lambda'$ et $\bar\lambda''\bar\lambda'=\overleftarrow{\mathfrak{M}}(\lambda'\lambda'', \bar\lambda', \bar\lambda''\bar\lambda')=\overleftarrow{\mathfrak{M}}(\lambda'\lambda''\bar\lambda', \bar\lambda''\bar\lambda')=$
$=\overleftarrow{\mathfrak{M}}(\lambda'\lambda'', \bar\lambda''\bar\lambda').\bar\lambda'$, c'est-à-dire $\bar\lambda''=\overleftarrow{\mathfrak{M}}(\bar\lambda'', \lambda'\lambda'')$; donc $\lambda'\lambda''$ et aussi λ' est diviseur de $\bar\lambda''$, ce qui est impossible. Donc $\overrightarrow{\mathfrak{D}}(\lambda'\lambda'', \bar\lambda')\neq 1$. Posons $\lambda'''=\overrightarrow{\mathfrak{D}}(\lambda'\lambda'', \bar\lambda')$ et $\lambda'\lambda''=\lambda''''\lambda'''$. λ'''' divise $\bar\lambda'\bar\lambda''$. S'il a un diviseur commun μ de degré >0 avec $\bar\lambda'$, il a aussi, d'après ce qui précède, un diviseur commun μ' de degré >0 avec $\bar\lambda'$ ce qui est impossible. Donc tout diviseur premier de λ'''' doit diviser $\bar\lambda''$; de plus $\nu(\lambda'''')>0$, car autrement $\lambda'\lambda''$ et aussi λ'' diviserait $\bar\lambda'$. Donc, si λ''' et λ'''' ne sont pas premiers $m_{e_1,e_2}(\bar\lambda')+m_{e_1,e_2}(\bar\lambda'')=\nu(\lambda''''\lambda''')>m_{e_1,e_2}(\bar\lambda')+m_{e_1,e_2}(\bar\lambda'')$, ce qui est absurde. Le théorème est démontré.

Théorème XIII *Si un élément $\bar\lambda$ du centre de $W_{a,b}$ est premier avec un $\lambda\in W_{a,b}$ et si $\lambda'\in W_{a,b}$, $\overleftarrow{\mathfrak{D}}(\bar\lambda, \lambda'\lambda)=\overleftarrow{\mathfrak{D}}(\bar\lambda, \lambda')$ et $\overrightarrow{\mathfrak{D}}(\bar\lambda, \lambda\lambda')=\overrightarrow{\mathfrak{D}}(\bar\lambda, \lambda')$.*

Démonstration : On montre de la même manière que dans le théorème précédent que λ divise un élément $\bar\mu$ du centre de $W_{a,b}$ premier avec $\bar\lambda$. On a que $\overleftarrow{\mathfrak{D}}(\bar\lambda, \lambda'\lambda)$ divise $\overleftarrow{\mathfrak{D}}(\bar\lambda, \lambda'\bar\mu)$. On a $\overrightarrow{\mathfrak{M}}(\bar\lambda, \lambda'\bar\mu)=$
$=\overrightarrow{\mathfrak{M}}(\bar\lambda, \bar\mu, \lambda'\bar\mu)=\overrightarrow{\mathfrak{M}}[\overrightarrow{\mathfrak{M}}(\bar\lambda, \bar\mu), \lambda'\bar\mu]$. Or $\overrightarrow{\mathfrak{M}}(\bar\lambda, \bar\mu)=\bar\lambda\bar\mu$, d'où $\overrightarrow{\mathfrak{M}}(\bar\lambda, \lambda'\bar\mu)=$
$=\overrightarrow{\mathfrak{M}}(\bar\lambda\bar\mu, \lambda'\bar\mu)=\overrightarrow{\mathfrak{M}}(\bar\lambda, \lambda').\bar\mu$. Donc si d^*, d désignent les degrés de $\overleftarrow{\mathfrak{D}}(\bar\lambda', \lambda'\bar\mu)$ et de $\overleftarrow{\mathfrak{D}}(\bar\lambda, \lambda')$ resp. on a $\nu(\bar\lambda)+[\nu(\lambda')+\nu(\bar\mu)]-d^*=[\nu(\bar\lambda)+\nu(\lambda')-d]+\nu(\bar\mu)$ c'est-à-dire $d^*=d$; puisque $\overleftarrow{\mathfrak{D}}(\bar\lambda, \lambda')\mid\overleftarrow{\mathfrak{D}}(\bar\lambda, \lambda'\lambda)\mid\overleftarrow{\mathfrak{D}}(\bar\lambda, \lambda'\bar\mu)$, on a $\overleftarrow{\mathfrak{D}}(\bar\lambda, \lambda')=$
$=\overleftarrow{\mathfrak{D}}(\bar\lambda, \lambda'\bar\mu)=\overleftarrow{\mathfrak{D}}(\bar\lambda, \lambda'\lambda)$ Démonstration analogue pour l'autre égalité.

C. q. f. d.

Théorème XIV. *Si $\lambda', \lambda'', \ldots, \lambda^{(q)}$ sont tous diviseurs d'un $\bar\lambda$ du centre de $W_{a,b}$, $\lambda'\lambda''\ldots\lambda^{(q)}$ divise $\bar\lambda^q$.*

Démonstration : Soit $\lambda'\mu'=\lambda''\mu''=\ldots=\lambda^{(q)}\mu^{(q)}=\bar\lambda$. Alors
$\mu^{(q)}\mu^{(q-1)}\ldots\mu''\mu'\lambda'\lambda''\ldots\lambda^{(q-1)}\lambda^{(q)}=\mu^{(q)}\mu^{(q-1)}\ldots\mu''\bar\lambda''\ldots\lambda^{(q-1)}\lambda^{(q)}=$
$=\mu^{(q)}\mu^{(q-1)}\ldots\mu''\lambda''\ldots\lambda^{(q-1)}\lambda^{(q)}.\bar\lambda=\ldots\ldots=\mu^{(q)}\mu^{(q-1)}\ldots\lambda^{(q-1)}\lambda^{(q)}.\bar\lambda^2=\ldots$
$\ldots=\mu^{(q)}\mu^{(q-1)}\lambda^{(q-1)}\lambda^{(q)}.\bar\lambda^{q-2}=\ldots=\bar\lambda^q$.

C. q. f. d.

Les décompositions normales et l'invariance de la suite d'indices d'un élément de $W_{a,b}$.

λ étant un élément de $W_{a,b}$, $\lambda=\lambda'\lambda''\ldots\lambda^{(s)}$, où $\lambda', \lambda'', \ldots, \lambda^{(s)}$ sont premiers, s'appelle une *décomposition* de λ. La suite $\nu(\lambda'), \nu(\lambda''), \ldots, \nu(\lambda^{(s)})$ s'appelle la *suite d'indices* de cette décomposition. La décomposition $\lambda=\lambda'\lambda''\ldots\lambda^{(s)}$ s'appelle *normale* s'il y a q éléments premiers $\bar\lambda', \bar\lambda'', \ldots, \bar\lambda^{(q)}$, dont aucun couple $\bar\lambda_i, \bar\lambda_j$ $(i\neq j)$ n'est pas d'associés, et une suite d'entiers $i_1=1<i_2<i_3<\ldots<i_q<s$ tels que $\lambda', \lambda'', \ldots, \lambda^{(i_2-1)}$ soient tous diviseurs de $\bar\lambda', \lambda^{(i_2)}, \lambda^{(i_2+1)}, \ldots, \lambda^{(i_3-1)}$ ceux de $\bar\lambda'', \ldots, \lambda^{(i_q)}, \lambda^{(i_q+1)}, \ldots, \lambda^{(s)}$ ceux de $\bar\lambda^{(q)}$.

Soit $\lambda=\lambda'\lambda''\ldots\lambda^{(s)}$ une décomposition de λ; soit que $\lambda^{(i)}\mid\bar\lambda^{(r_1)}$, $\lambda^{(i+1)}\mid\bar\lambda^{(r_2)}$. Il existe $\mu^{(i)}\mid\bar\lambda^{(r_2)}$ et $\mu^{(i+1)}\mid\bar\lambda^{(r_1)}$ premiers, tels que $\lambda^{(i)}\lambda^{(i+1)}=\mu'^{(i)}\mu^{(i+1)}$ (th. XII). $\lambda=\lambda'\lambda''\ldots\lambda^{(i-1)}\mu^{(i)}\mu^{(i+1)}\lambda^{(i+2)}\ldots\lambda^{(s)}$ est encore une décomposition de λ. Elle s'appelle *voisine* de la décomposition précédente. Il est évident que les suites d'indices sont les mêmes dans ces deux décompositions (à l'ordre près).

Deux décompositions $\lambda'\lambda''\ldots\lambda^{(s)}$ et $\tau'\tau''\ldots\tau^{(s)}$ de λ sont dites *équivalentes* s'il existe une suite de décompositions de λ, $\mu'\mu''\ldots\mu^{(s)}$, $\nu'\nu''\ldots\nu^{(s)}, \ldots, \xi'\xi''\ldots\xi^{(s)}$ telles que $\mu'\mu''\ldots\mu^{(s)}$ soit voisine de $\lambda\lambda'\ldots\lambda^{(s)}$, $\nu'\nu''\ldots\nu^{(s)}$ soit voisine de $\mu'\mu''\ldots\mu^{(s)}, \ldots, \tau'\tau''\ldots\tau^{(s)}$ soit voisine de $\xi'\xi''\ldots\xi^{(s)}$. Les décompositions équivalentes ont la même suite d'indices à l'ordre près ; de plus, $\bar\lambda$ étant un élément premier quelconque du centre de $W_{a,b}$, dans ces deux décompositions il y a le même nombre de $\lambda^{(i)}$ diviseurs de $\bar\lambda$.

Théorème XV. *$\bar\lambda$ étant un élément premier du centre de $W_{a,b}$ non premier avec λ, il existe pour toute décomposition de λ une décomposition équivalente normale où $\bar\lambda'=\bar\lambda$.*

Dans deux décompositions quelconques de λ les suites d'indices sont les mêmes à l'ordre près et il y a le même nombre de $\lambda^{(i)}$ diviseurs de $\bar\lambda$. Si $\lambda=\lambda'\lambda''\ldots\lambda^{(s)}$ et si $\lambda^{(i)}$ divise un élément premier $\bar\lambda$ du centre de $W_{a,b}$, $\bar\lambda$ n'est pas premier avec λ.

Démonstration : Si $\bar\lambda$ n'est divisible par aucun des $\lambda^{(s)}$ et si $\lambda=\lambda'\lambda''\ldots\lambda^{(s)}$, on trouve par application repetée du théorème XIII que $\bar\lambda$ est premier à λ. Donc, si cela n'a pas lieu, il y a des $\lambda^{(s)}$, soient

$\lambda^{(i_1)}, \lambda^{(i_2)}, \ldots, \lambda^{(i_q)}$, $1 \leqq i_1 < i_2 < \cdots < i_q \leqq s$, qui divisent $\bar{\lambda}$. Si $i_1 > 1$, il y a $\mu^{(i_1-1)} | \bar{\lambda}$ et $\mu^{(i_1)}$ premiers tels que $\lambda^{(i_1-1)}\lambda^{(i_1)} = \mu^{(i_1-1)}\mu^{(i)}$. Donc $\lambda'\lambda'' \ldots \lambda^{(i_1-2)}\mu^{(i_1-1)}\mu^{(i_1)}\lambda^{(i_1+1)} \ldots \lambda^{(i)}$ est une décomposition équivalente à la précédente, où $i'_1 = i_1 - 1$, $i'_2 = i_2 \ldots$, $i'_q = i_q$. On continue ce procédé jusqu'à ce que i_1 devient 1. On applique ensuite le même procédé à i_2 jusqu'à ce que i_2 devient 2, ensuite à i_3 etc. On arrive finalement à une décomposition de forme $\lambda = \mu'\mu'' \ldots \mu^{(q)}.\mu^{(q+1)} \ldots \mu^{(s)}$ où $\mu', \mu'', \ldots, \mu^{(q)}$ divisent $\bar{\lambda}$ et les autres $\mu^{(i)}$ ne le divisent pas. Soit $\mu = \mu^{(q+1)} \ldots \mu^{(s)}$. En prenant $\bar{\mu}$ non premier à μ, on leur applique le même procédé. Soit $\mu = \nu^{(q+1)}\nu^{(q+2)} \ldots \nu^{(q+r)}.\nu^{(q+r+1)} \ldots \nu^{(s)}$ où $\nu^{(q+1)}, \nu^{(q+2)}, \ldots, \nu^{(q+r)}$ divisent $\bar{\mu}$ et les autres $\nu^{(i)}$ ne le divisent pas. Soit $\nu = \nu^{(q+r+1)} \ldots \nu^{(s)}$. On choisit $\bar{\nu}$ non premier à ν, on applique le même procédé etc., et finalement on arrive à la décomposition normale voulue.

Si $\lambda^{(i)}$ divise $\bar{\lambda}$, on voit par le même procédé que $\bar{\lambda}$ ne peut pas être premier à λ. Par l'application répétée du théorème XIII on voit que si $j \geqq q$, $\mathfrak{D}(\bar{\lambda}^j, \lambda) = \lambda'\lambda'' \ldots \lambda^{(q)}$. Soient $\lambda = \lambda'\lambda'' \ldots \lambda^{(s_1)} = \mu'\mu'' \ldots \mu^{(s_2)}$ deux décompositions quelconques de λ. Soit $\bar{\lambda}$ un élément du centre de $W_{a,b}$ non premier à λ ; soit $\Lambda'\Lambda'' \ldots \Lambda^{(q_1)}\Lambda^{(q_1+1)} \ldots \Lambda^{(s_1)}$ et $M'M'' \ldots M^{(q_2)}M^{(q_2+1)} \ldots M^{(s_2)}$ les décompositions normales où $\bar{\lambda}' = \bar{\lambda}$ qui leur sont équivalentes et où $\Lambda', \Lambda'', \ldots, \Lambda^{(q_1)}$, $M', M'', \ldots, M^{(q_2)}$ divisent $\bar{\lambda}$ et où les autres $\Lambda^{(i)}, M^{(s)}$ ne le divisent pas. Alors, si $l \geqq q_1$, $l \geqq q_2$, $\overleftarrow{\mathfrak{D}}(\bar{\lambda}^l, \lambda) = \Lambda'\Lambda'' \ldots \Lambda^{(q_1)} = M'M'' \ldots M^{(q_2)}$ c. à. d. $q_1 . m_{e_1,e_2}(\bar{\lambda}) = q_2 . m_{e_1,e_2}(\bar{\lambda})$; donc $q_1 = q_2$. S'il y a q'_1 de $\lambda^{(i)}$ et q'_2 de $\mu^{(j)}$ qui divisent $\bar{\lambda}$ on a $q'_1 = q_2$, $q'_2 = q_2$, donc $q'_1 = q'_2$. En appliquant le même procédé à tous les $\bar{\lambda}$ non premiers avec λ, et, en se rappellant que tous les diviseurs premiers de $\bar{\lambda}$ ont le même degré $m_{e_1,e_2}(\bar{\lambda})$, on voit l'exactitude du théorème.

C. q. f. d.

Théorème XVI. *Deux décompositions quelconques d'un* $\lambda \in W_{a,b}$ *sont équivalentes.*

Démonstration : Soient $\lambda = \lambda'\lambda'' \ldots \lambda^{(s_1)}$ et $\lambda = \mu'\mu'' \ldots \mu^{(s_2)}$ deux décompositions de λ. On a vu que $s_1 = s_2$. Désignons ce nombre par $s(\lambda)$. Supposons le théorème démontré pour tous les λ_0 telsque $s(\lambda_0) < s(\lambda)$. On a $\lambda' | \overleftarrow{\lambda}$ et $\mu' | \overleftarrow{\lambda}$. Donc $\overrightarrow{\mathfrak{M}}(\lambda', \mu') | \overleftarrow{\lambda}$. λ', μ' étant premiers, ils sont ou bien associés, ou bien premiers entre eux. Dans le premier cas, soit $\mu' = \lambda'\varepsilon$. Alors la décomposition $\lambda' . \varepsilon\mu'' . \mu''' \ldots \ldots \mu^{[s(\lambda)]}$ est voisine de $\mu'\mu'' \ldots \mu^{s(\lambda)}$, et, puisque $\varepsilon\mu'' . \mu''' \ldots \mu^{[s(\lambda)]} = \lambda''\lambda''' \ldots \lambda^{[s(\lambda)]}$, elle est aussi équivalente à $\lambda'\lambda'' \ldots \lambda^{[s(\lambda)]}$, et le théorème est prouvé dans ce cas. Si $\overleftarrow{\mathfrak{D}}(\lambda', \mu') = 1$, on a $\overrightarrow{\mathfrak{M}}(\lambda', \mu') = \lambda'\xi = \mu'\eta$. Posons $\lambda = \overrightarrow{\mathfrak{M}}(\lambda', \mu') . \zeta$, et soit $\zeta = \nu'\nu'' \ldots \nu^{[s(\lambda)-2]}$ une décomposition de ζ. $\lambda'\xi\nu'\nu'' \ldots \nu^{[s(\lambda)-2]}$ et $\mu'\eta\nu'\nu'' \ldots \nu^{[s(\lambda)-2]}$ sont deux décompositions voisines de λ. D'autre part, puisque $\xi\nu'\nu'' \ldots \nu^{[s(\lambda)-2]} = \lambda''\lambda''' \ldots \lambda^{[s(\lambda)]}$, $\lambda'\xi\nu'\nu'' \ldots \nu^{[s(\lambda)-2]}$ est équivalente avec $\lambda'\lambda'' \ldots \lambda^{[s(\lambda)]}$, et, pour une cause analogue, $\mu'\eta\nu'\nu'' \ldots \nu^{[s(\lambda)-2]}$ est équivalente avec $\mu'\mu'' \ldots \mu^{[s(\lambda)]}$. La théorème est complètement prouvé.

§ 5. Première forme de la condition de primitivité

Revenons à la notation de l'étude du cas c dans le § 3. Soient A, B deux opérateurs de $M^{(\pi_0)}$. A+B et AB désignent les opérateurs de ce module tels que pour tout $\alpha \in M^{(\pi_0)}$

$$(A+B)\alpha = A\alpha + B\alpha$$

$$(AB)\alpha = A(B\alpha).$$

Désignons par $\lambda = \sum_{q=0}^{n} \alpha_q z_\Gamma^q$, où $\alpha_1, \alpha_2, \ldots, \alpha_n \in \Omega_\psi$, l'opérateur tel que pour tout $\alpha \in M^{(\pi_0)}$

$$\lambda\alpha = \sum_{q=0}^{n} \alpha_q \alpha^{\nu^{Fq}}.$$

Les λ sont éléments de $W_{F,\psi}$, et un même opérateur est désigné par une infinité de λ. Il est facile de vérifier que si à chaque λ on fait correspondre l'opérateur de $M^{(\pi_0)}$ qu'il désigne, on établit une homomorphie de $W_{a,b}$ sur un certain ensemble d'opérateurs de $M^{(\pi_0)}$. Dans cette homomorphie à z_F correspond l'opérateur $\mathfrak{Z}$, et à $\alpha \in \Omega_\psi$ — l'opération de multiplication par α.

Soit $\mathfrak{R}$ l'ensemble de tous les $\lambda \in W_{F,\psi}$ qui représentent l'opérateur 0 (c'est-à-dire tel que pour tout $\alpha \in M^{(\pi_0)}$ on ait $0\alpha = 0$). Dans ce cas, si Γ est l'anneau de tous les opérateurs représentés par les $\lambda \in W_{F,\psi}$, on a $\Gamma \simeq W_{F,\psi}/\mathfrak{R}$ et $\mathfrak{R}$ est un idéal bilatère de $W_{F,\psi}$. On

adonc, d'après le § 4, $\mathfrak{R}=(R)$. Puisque $(\mathfrak{Z}^{f_{K^*/K}}-1)\alpha=\alpha^{p^{F^*}\cdot f_{K^*/K}}-\alpha=\alpha^{p^{F^*}}-\alpha=0$ pour tout $\alpha\in M^{(\pi_0)}$, on voit que $z_F^{f_{K^*/K}}-1\equiv 0 \pmod R$, c'est-à-dire R est premier à z_F. Il en résulte, d'après le théorème IV du § 4, que si l'on prend $R_{\nu(R)}=1$, R est dans le centre de $W_{F,\psi}$.

Soit $\alpha\in M^{(\pi_0)}$. Les $\lambda\in W_{F,\psi}$ tels que $\lambda\alpha=0$ forment un idéal, soit $(\overleftarrow{R_\alpha})$. Soit r_α le degré de R_α. $z_F=\mathfrak{Z}$ est un automorphisme de $M^{(\pi_0)}$ et aussi la multiplication par un $\beta\neq 0\in\Omega'_\psi$ l'est. Or $z_F R_\alpha z_F^{-1}(\mathfrak{Z}_F\alpha)=z_F R_\alpha\alpha=$ $=z_F 0=0$ et $z_F^{-1}R_{z_F\alpha}z_F.\alpha=z_F^{-1}R_{z_F\alpha}z_F.[z_F^{-1}(z_F\alpha)]=z_F^{-1}R_{z_F\alpha}(z_F\alpha)=$

$$=z_F^{f_{K^*/K}-1}R_{z_F\alpha}(z_F\alpha)=z_F^{f_{K^*/K}-1}0=0$$

c'est-à-dire $(\overleftarrow{R_{z_F\alpha}})=(z_F\overleftarrow{R_\alpha}z_F^{-1})$. De même $(\overleftarrow{R_{\beta\alpha}})=(\beta\overleftarrow{R_\alpha}\beta^{-1})$. Il s'ensuit que $\overleftarrow{\mathfrak{M}(R_\alpha)}_{\alpha\in M^{(\pi_0)}}$ est permutable avec z_F et les $\beta\in\Omega_\psi$, c'est-à-dire est élément du centre de $W_{F,\psi}$. D'où

$$R=\overleftarrow{\mathfrak{M}(R_\alpha)}_{\alpha\in M^{(\pi_0)}}.$$

Théorème I. *Si* $K/k=(K/k)_1/(K/k)_0$, *pour que* K/k *soit primitif il faut et il suffit qu'il y ait dans* $M^{(\pi_0)}(K/k)$ *un* $\alpha\neq 0$ *tel que* R_α *soit premier et que* $(K:k)=p^{\psi r_\alpha}$. *Si cela a lieu pour un des* $\alpha\neq 0\in M^{(\pi_0)}(K/k)$, *cela a lieu pour tous les* $\alpha\neq 0\in M^{(\pi_0)}(K/k)$.

Démonstration : Soit $\alpha\neq 0\in M^{(\pi_0)}$. Si R_α n'est pas premier, par exemple si $R_\alpha=\lambda'\lambda''$, $\lambda''\alpha\in M^{(\pi_0)}$ et $R_{\lambda''\alpha}=\lambda'$. α étant quelconque, l'ensemble de tous les $\lambda\alpha$, $\lambda\in W_{F,\psi}$ est évidemment un $W_{F,\psi}$-module. Comme $\alpha, z_F\alpha, \ldots, z_F^{r_\alpha-1}\alpha$ sont linéairement indépendants par rapport à Ω_ψ et comme tout λ est congru suivant R_α à un élément de degré $<r_\alpha$, on voit que cette module a juste $p^{\psi r_\alpha}$ éléments. Donc, puisque $0<\nu(\lambda')<\nu(R_\alpha)$ on voit que $W_{F,\psi}(\lambda''\alpha)$ a $p^{\psi\nu(\lambda')}<p^{\psi r_\alpha}$ éléments et a plus d'un élément, et que $M^{(\pi_0)}$ a au moins $p^{\psi r_\alpha}$ éléments, c'est-à-dire a un sous-$W_{F,\psi}$-module autre que lui-même et $\{0\}$. Si R_α est premier mais $(K:k)>p^{\psi r_\alpha}$, $M^{(\pi_0)}$ a encore un sous-$W_{F,\psi}$-module autre que lui-même et $\{0\}$. Donc, si la condition indiquée n'est pas satisfaite, pour *tous* les $\alpha\neq 0\in M^{(\pi_0)}$, K/k est imprimitif. Supposons, d'autre part, qu'elle est satisfaite pour *un* $\alpha\neq 0\in M^{(\pi_0)}$. Alors tous les $\alpha\in M^{(\pi_0)}$ ont la forme $\lambda\alpha$, $\lambda\in W_{F,\psi}$. Soit M un sous-$W_{F,\psi}$-module de $M^{(\pi_0)}$ autre que $\{0\}$. Soit $\lambda\alpha\neq 0$ un élément de $\bar{M}$. λ est premier à R_α. Pour que $\lambda'(\lambda\alpha)=0$ il faut que $\lambda'\lambda\equiv 0 \pmod{R_\alpha}$ c'est-à-dire $\lambda'\lambda\equiv 0 \pmod{\mathfrak{M}(R_\alpha,\lambda)}$; mais $\nu(R_\alpha,\lambda)=\nu(R_\alpha)+\nu(\lambda)=r_\alpha+\nu(\lambda)$, donc $\nu(\lambda')\geqq r_\alpha$; on en déduit $r_{\lambda\alpha}=r_\alpha$ et $\bar{M}$ contient au moins $p^{\psi r_\alpha}$ éléments, c'est-à-dire $\bar{M}=M^{(\pi_0)}$ et K/k est primitif. C. q. f. d.

Soit

$$\varepsilon_1=\frac{F}{(F,\psi)},\qquad \varepsilon_2=\frac{\psi}{(F,\psi)}.$$

On peut donner à la condition de primitivité la forme symétrique suivante :

Théorème II. *Pour que* $K/k=(K/k)_1/(K/k)_0$ *soit primitif il faut et il suffit que* R *soit premier dans* $W_{m(F,\psi),(F,\psi)}$ *et que* $(K:k)=p^{\psi m_{\varepsilon_1,\varepsilon_2}(R)}$.

Démonstration : S'il y a $\alpha\neq\in M^{(\pi_0)}$ tel que R_α est premier et que tout $\alpha\in M^{(\pi_0)}$ a la forme $\lambda\alpha$, $\lambda\in W_{F,\psi}$, on a, étant donné que si $R\alpha_1=0$ et $R\alpha_2=0$, aussi $R(\alpha_1+\alpha_2)=R\alpha_1+R\alpha_2=0$, que

$$R=\overleftarrow{\mathfrak{M}(\beta z_F^i R_\alpha z_F^{-i}\beta^{-1})}_{\beta\in\Omega'_\psi};\ i=0,1\,2,\ldots,f_{K^*/K}-1$$

c'est-à-dire R est un élément premier du centre de $W_{F,\psi}$. Par conséquent $r_\alpha=m_{\varepsilon_1,\varepsilon_2}(R)$ et $(K:k)=p^{\psi r_\alpha}=p^{\psi m_{\varepsilon_1,\varepsilon_2}(R)}$. Supposons inversement que R est premier dans $W_{m(a,b),(a,b)}$ et que $(K:k)=p^{\psi m_{\varepsilon_1,\varepsilon_2}(R)}$. R_α est diviseur de R et $r_\alpha\leqq m_{\varepsilon_1,\varepsilon_2}(R)$; mais aucun diviseur propre de R ne peut pas être de degré $<m_{\varepsilon_1,\varepsilon_2}(R)$. Donc $r_\alpha=m_{\varepsilon_1,\varepsilon_2}(R)$. Si $R_\alpha=\lambda'\lambda''$, où $0<\nu(\lambda')<\nu(R_\alpha)$, on a $\nu(\lambda')\neq 0<m_{\varepsilon_1,\varepsilon_2}(R)$. Donc R_α est premier et

$$(K:k)=p^{\psi m_{\varepsilon_1,\varepsilon_2}(R)}=p^{\psi r_\alpha}.$$

C. q. f. d.

§ 6. — Deuxième forme de la condition de primitivité

Soit χ un corps de caractéristique p, et soit $f(x)$ un polynome (en x) dans χ dont tous les zéros sont simples. On peut se démander : Quelle est la condition nécessaire et suffisante pour que l'ensemble M de tous les zéros de $f(x)$ soit un module ? La réponse a cette question est donnée par le

Théorème I. *Les zéros du polynôme* $f(x)=\Sigma\varkappa_a x^a$ *dans* χ *sont simples et leur ensemble* M *est un module si, et seulement si :* 1°. *quand* a *n'est pas une puissance de* p, $\varkappa_a=0$, 2°. $\varkappa_1\neq 0$.

Démonstration : Supposons que M soit un module ; alors, si $y\in$ M, $f(x+y)$ a les mêmes zéros que $f(x)$. $f(x)$ ayant tous ses zéros simples, $f(x+y)$ doit être multiple de $f(x)$. Or on a identiquement

$$f(x+y)=f(x)+f(y)+\sum_{i=1}^{m-1} q_i(y)x^i,$$

où m désigne le degré de $f(x)$ et où les $q_i(y)$ sont de degré $\leq m-i\leq m-1<m$. Or $f(x)$ est multiple de $f(x)$, et, y étant dans M, $f(y)=0$. Donc $\sum_{i=1}^{m-1} q_i(y)x^i$ doit être multiple de $f(x)$ pour tout $y\in$ M. Le degré de cette expression par rapport à x étant $<m$, elle doit être, par conséquent, identiquement nulle par rapport à x. Donc tout $q_i(y)$ $(i=1, 2, \ldots, m-1)$ doit s'annuler pour tout $y\in$ M, donc avoir au moins m zéros distincts. Son degré étant $<m$, il doit être identiquement nul. Donc, identiquement par rapport à x et à y il doit être

$$f(x+y)=f(x)+f(y).$$

Cette égalité suffit d'ailleurs pour que M soit un module.

La condition écrite équivant à l'ensemble des conditions analogues pour toutes les parties homogènes de $f(x)$. Une partie homogène de $f(x)$ a la forme $\varkappa_a x^a$. Si $\varkappa_a=0$, on a bien $\varkappa_a(x+y)^a=\varkappa_a x^a+\varkappa_a y^a$. Si $\varkappa_a\neq 0$, la condition $\varkappa_a(x+y)^a=\varkappa_a x^a+\varkappa_a y^a$ équivant à la condition $(x+y)^a=x^a+y^a$. Supposons que $a=p^s a'$, avec a' premier à p, et que $\varkappa_a\neq 0$. Alors on doit avoir $[(x+y)^{p^s}]^{a'}=(x^{p^s})^{a'}+(y^{p^s})^{a'}$. Or $(x+y)^{p^s}=x^{p^s}+y^{p^s}$ et, si $a'>1$, $(x^{p^s}+y^{p^s})^{a'}$ contient le terme non nul $a' x^{p^s} y^{(a'-1)p^s}$ et l'égalité écrite ne peut pas avoir lieu. D'autre part, si $a'=1$, elle a sûrement lieu. Donc la condition $f(x+y)=f(x)+f(y)$ équivant à la condition 1°. de l'énoncé.

La condition 1°. de l'énoncé étant vérifiée, c'est-à-dire $f(x)$ ayant la forme $\sum_{i=0}^{r}\lambda_i x^{p^i}$ (où l'on posé $r=\log_p m$ et $\lambda_i=\varkappa_{p^i}$), on a $f'(x)=\sum_{i=0}^{r}\lambda_i p^i x^{p^i-1}=\lambda_0=\varkappa_1$. Si $\varkappa_1=0$, $f'(x)=0$ identiquement et tous les zéros de $f(x)$ sont multiples. Inversement, si $\varkappa_1\neq 0$, $f(x)$ n'est jamais nul et les zéros de $f(x)$ sont simples. C. q. f. d.

Conséquence: z_1 étant l'opérateur $\alpha\to\alpha^p$, l'équation $f(x)=\sum_{i=0}^{r}\lambda_i x^{p^i}=0$ peut encore s'écrire sous la forme

$$\lambda(z_1)(x)=0$$

où l'on posé $\lambda(z_1)=\sum_{i=0}^{r}\lambda_i z_1^i$. Donc *tout module* M *dans un corps de caractéristique* p *peut être défini comme l'ensemble d'éléments* x *de ce corps tels que* $\lambda(z_1)(x)=0$, où $\lambda(z_1)=\Sigma\lambda_i z_1^i$, *les* λ_i *étant dans ce corps.*

Définition : On appelera $\lambda(z_1)$ le *quasi-polynôme* de module M.

Théorème II. *Si* M′ *est un sous-module de* M, *le quasi-polynôme* $\lambda'(z_1)$ *de* M′ *est diviseur du quasi-polynome* $\lambda(z)$ *de* M. *Inversement, si* $\lambda'(z_1)\mid\lambda(z_1)$, *l'ensemble* M′ *des* α *tels que* $\lambda'(z_1)(\alpha)=0$ *est un sous-module de l'ensemble* M *des* α *telsque* $\lambda(z_1)(\alpha)=0$.

Démonstration : Considérons l'ensemble des tous les quasi-polynômes $\mu(z_1)$ dans χ telsque $\mu(z_1)(\alpha)=0$ quand $\alpha\in$ M′. Les $\mu(z_1)$ forment manifestement un idéal. Comme au § 4, on démontre que cet idéal est principal. Donc, il existe $\mu_0(z_1)$ tel que cet idéal est $(\mu_0(z_1))$; m' étant le nombre d'éléments de M′, on a que le degré μ de $\mu_0(z_1)$ est $\geq\log_p m'$. Mais $\lambda'(z_1)(\alpha)=0$ si $\alpha\in$ M′, donc $\lambda'(z_1)$ est multiple de $\mu_0(z_1)$, et comme son degré est $\log_p m'$, $\lambda(z_1)$ et $\mu_0(z_1)$ sont associés et on peut prendre $\mu_0(z_1)=\lambda'(z_1)$. D'où, puisque M′ $\subset$ M, donc $\lambda(z_1)(\alpha)=0$, si $\alpha\in$ M′, il résulte $\lambda(z)\equiv 0 \pmod{\lambda'(z_1)}$; ce qui démontre la première

§ 7. — Structure des $W_{a,b}$-modules et génération des corps $\mathfrak{P}$-adiques

Au § 6 nous avons établi une correspondance biunivoque entre les $W_{a,b}$-modules et les éléments de $W_{b,a}$: à savoir celle qu'on obtient en faisant correspondre à un $W_{a,b}$-module M son quasi-polynôme $\lambda_M(z_b)$ (10). Dans cette correspondance à toute rélation ou opération se rapportant aux $W_{a,b}$-modules correspond une rélation ou une opération pour les élé nents correspondants de $W_{b,a}$. Il s'agit d'étudier de plus près de quelle manière cela se produit.

On a tout d'abord

1°. $M \supseteq \overline{M}$ équivaut à $\lambda_{\overline{M}} \overrightarrow{|} \lambda_M$.

2°. $\lambda_{M_1 \cap M_2} = \overrightarrow{\mathfrak{D}}(\lambda_{M_1}, \lambda_{M_2})$

3°. $\lambda_{M_1 + M_2} = \overleftarrow{\mathfrak{M}}(\lambda_{M_1}, \lambda_{M_2})$.

Soit que $M \supseteq \overline{M}$. Les classes de M suivant $\overline{M}$ forment encore un $W_{a,b}$-module $M/\overline{M}$. D'autre part $\lambda_{\overline{M}} \overrightarrow{|} \lambda_M$. Donc il existe un $\lambda' \in W_{b,a}$ tel que $\lambda_M = \lambda' \lambda_{\overline{M}}$. Soit $\overline{\overline{M}}$ un $W_{a,b}$-module tel qu $\lambda_{\overline{\overline{M}}} = \lambda'$. Alors *on peut identifier* $\overline{M}/M$ *avec* $\overline{\overline{M}}$. *Si l'on pose* $M = \overline{\overline{M}} \times \overline{M}$, *on définit ainsi une loi associative* (mais *non commutative*, en général) de composition des $W_{a,b}$-modules et $\lambda_{M_1 \times M_2} = \lambda_{M_1} \lambda_{M_2}$ (ce qui montre, d'ailleurs, que $M_1 \times M_2$ ne dépend pas du choix des a, b, mais seulement des M_1 et M_2).

Etudions un peu plus près le module $\overline{\overline{M}} = M/\overline{M}$. Soit $\alpha \in M$. Alors on a $\lambda_{\overline{\overline{M}}}(\lambda_{\overline{M}} x) = \lambda_M \alpha = 0$; donc $\lambda_{\overline{M}} \alpha \in \overline{\overline{M}}$. On a $\lambda_{\overline{M}} \alpha_1 = \lambda_{\overline{M}} \alpha_2$ ($\alpha_1, \alpha_2 \in M$) si, et seulement si $\lambda_{\overline{M}}(\alpha_1 - \alpha_2) = 0$, c'est-à-dire $\alpha_2 - \alpha_1 \in \overline{M}$. Ainsi $\lambda_{\overline{M}} M$ a autant d'éléments que $\overline{\overline{M}}$, donc

$$\overline{\overline{M}} = \lambda_{\overline{M}} M.$$

(10) Nous comprendrons dans ce § la notion de $W_{a,b}$-module d'une manière un peu plus large que précédemment : à savoir on appelera $W_{a,b}$-module encore un ensemble M admettant les opérateurs z_a et Ω_b *répété* un nombre *puissance de p* de fois. Ainsi M tel que $\lambda_M = z_1^2 - z_1$ est l'ensemble $\{0, 1, \ldots, p-1\}$ répété p fois (c'est en effet l'ensemble de tous les zéros du polynôme $x^{p^2} - x^p = (x^p - x)^p$).

La classe d'un α suivant l'ensemble M précédent sera $\{\alpha, \alpha+1, \ldots, \alpha+p-1\}$ *répété p fois.*

De plus $\lambda_{\overline{M}} \alpha_1 = \lambda_{\overline{M}} \alpha_2$ si, et seulement si α_1 et α_2 sont dans une même classe suivant $\overline{M}$ dans M. Ainsi, l'identification de $M/\overline{M}$ avec $\overline{\overline{M}}$ peut être faite en identifiant une classe $\overline{M}_1 = \alpha + \overline{M}$ suivant $\overline{M}$ dans M avec $\lambda_{\overline{M}} \overline{M}_1 = \lambda_{\overline{M}} \alpha$. Nous poserons dorenavant

$$\alpha + \overline{\overline{M}}/\overline{M} = \lambda_{\overline{M}} \alpha.$$

Or $\lambda_{\overline{M}} x = \prod_{\beta \in \overline{M}} (x - \beta)$. Donc $\lambda_{\overline{M}} \alpha = \prod_{\beta \in \overline{M}} (\alpha - \beta) = \prod_{\beta \equiv \alpha \pmod{\overline{M}}} \beta$. Donc

$$\overline{M}_1/\overline{M} = \alpha + \overline{M}/\overline{M} = \prod_{\beta \in \overline{M}_1} \beta$$

Il est à remarquer que la correspondance $\alpha \to \lambda_{\overline{M}} \alpha$ ($\alpha \in M$) est $W_{a,b}$-homomorphie. En effet, d'abord $\lambda_{\overline{M}}(\alpha+\beta) = \lambda_{\overline{M}} \alpha + \lambda_{\overline{M}} \beta$ ($\alpha, \beta \in M$). Ensuite puisque $\lambda_{\overline{M}} \in W_{b,a}$, on a, quelque soit $\Lambda \in W_{a,b}$, $\Lambda \lambda_{\overline{M}} = \lambda_{\overline{M}} \Lambda$. D'où $\Lambda . \lambda_{\overline{M}} \alpha = \lambda_{\overline{M}} . \Lambda \alpha$ ($\alpha \in M$). Ainsi la correspondance entre les éléments de $M/\overline{M}$ (au sens ordinaire) et les éléments de $\overline{\overline{M}}$ avec lesquels on les identifie est un $W_{a,b}$-isomorphisme.

Ce qui précède entraîne quelques conséquences importantes :

a) Si $\overline{M} \subset M$, $\lambda_{\overline{M}} M$ est un $W_{a,b}$-module (ceci est important pour § 10).

b) M_1, M_2 étant deux $W_{a,b}$-modules quelconques, il existe un $W_{a,b}$-module M_3 tel que $M_3 = M_2 \times M_4$, c'est-à-dire tel que

$$\left\{ \prod_{\beta \equiv \alpha \pmod{M_1}} \beta \right\}_{\alpha \in M_3} = M_2 .$$

c) Soit M un $W_{a,b}$-module et soit

$$\lambda_M = \sum_{i=0}^{s} \alpha_i z_b^i \qquad (\alpha_i \in \Omega_a).$$

Appelons *module associé de* M et désignons par M^* le module tel que

$$\lambda_{M^*} = \sum_{i=0}^{s} z_b^i \alpha_i = \sum_{i=0}^{s} \alpha_i^{p^{bi}} z_b^i .$$

La correspondance $\lambda_M \to \lambda_{M^*}$ est un anti-isomorphisme de $W_{b,a}$ et $(M^*)^* = M$. Soit que

$$M = \overline{\overline{M}} \times \overline{M}$$

alors, aussi

$$M^* = \overline{M}^* \times \overline{\overline{M}}^*.$$

Donc

$$(M/\overline{M})^* = \overline{\overline{M}}^* = \left(\left\{ \prod_{\beta \equiv \alpha \pmod{\overline{M}}} \beta \right\}_{\alpha \in M}\right)^*$$

$$(M^*/\overline{\overline{M}}^*)^* = \overline{M} = \left(\left\{ \prod_{\beta \equiv \alpha \pmod{\overline{M}^*}} \beta \right\}_{\alpha \in M^*}\right)^*.$$

On a ainsi une dualité entre $\overline{M}$ et $M/\overline{M}$ (pour un M fixe). Cette dualité est d'ailleurs, par l'intermédiaire des $M_q(K/k)$, en liaison étroite avec la dualité dans les corps kummeriens que M HASSE [11] a déduite de la loi de réciprocité pour le symbôle $\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)$ de HILBERT.

Supposons que $\overline{\overline{M}} \times \overline{M} = \overline{M} \times \overline{\overline{M}}$ (c'est-à-dire $\lambda_{\overline{\overline{M}}} \lambda_{\overline{M}} = \lambda_{\overline{M}} \lambda_{\overline{\overline{M}}}$). Dans ce cas la dualité précédente peut être mise sous la forme plus simple suivante

$$\overline{\overline{M}} = \left\{ \prod_{\beta \equiv \alpha \pmod{\overline{M}}} \beta \right\}_{\alpha \in M}$$

$$\overline{M} = \left\{ \prod_{\beta \equiv \alpha \pmod{\overline{\overline{M}}}} \beta \right\}_{\alpha \in M}.$$

C'est d'ailleurs cette forme simple de dualité qui intervient seule dans la dualité de M. HASSE. Il est à remarquer que l'on a $\overline{M} \times \overline{\overline{M}} = \overline{\overline{M}} \times \overline{M}$ dès que λ_M est dans le centre de $W_{b,a}$ (théorème IX de § 4).

Un $W_{a,b}$-module M sera dit *simple* s'il n'a d'autres $W_{a,b}$-sous-modules que lui-même et $\{0\}$. Deux $W_{a,b}$-modules M_1, M_2 étant simples, quelle est la condition auquelle doivent satisfaire λ_{M_1}, λ_{M_2} pour qu'ils soient $W_{a,b}$-isomorphes ? Soit qu'on ait établi un $W_{a,b}$-isomorphisme entre M_1 et M_2, et soit qu'à un $\alpha_1 \neq 0 \in M_1$ correspond dans cet isomorphisme un $\alpha_2 \in M_2$. Manifestement $\lambda\alpha_2 = 0$ ($\lambda \in W_{a,b}$) a lieu si, et seulement si $\lambda\alpha_1 = 0$. En particulier, R_M désignant l'élément du centre de $W_{a,b}$ tel que (R_M) soit l'idéal des tous les $\overline{\lambda}$ du centre telsque $\overline{\lambda}M = 0$, on a $R_{M_1} = R_{M_2}$. Donc λ_{M_1} et λ_{M_2} divisent le même élément premier du centre de $W_{b,a}$ (= centre de $W_{a,b}$).

Inversement, soit que cette condition est satisfaite. On a

$$R_{M_1} = \overleftarrow{\mathfrak{M}}(\{\alpha z_b^i \lambda_{M_1} z_b^{-i} \alpha^{-1}\}_{\alpha \in \Omega'_a},\ i = 0, 1, \ldots, n-1) =$$

$$= \overleftarrow{\mathfrak{M}}(\{\lambda_{\alpha z_b^i M_1}\}_{\alpha \in \Omega'_a},\ i = 0, 1, \ldots, n-1)$$

(11) Reziprozitätsgesetz. p. 70—72.

où $z^n \lambda_{M_1} z^{-n} = \lambda_{M_1}$. Donc, si $R_{M_1} = \lambda_M$, on a

$$M = \sum_{\substack{\alpha \in \Omega'_a \\ i = 0, 1, \ldots, n-1}} \alpha z_b^i M_1$$

Or, si $\lambda \in W_{a,b}$, on a $\lambda . \alpha z_b^i = \alpha z_b^i . \lambda (\alpha \in \Omega'_a)$. Donc $\lambda . \alpha z_b^i \alpha_1 = \alpha z_b^i . \lambda\alpha_1$. Par conséquent $\alpha z_b^i M_1$ est $W_{a,b}$-isomorphe à M_1. M_2 étant un sous-$W_{a,b}$-module simple de M, il résulte du théorème de JORDAN généralisé que M_2 est $W_{a,b}$-isomorphe à M_1. Donc

M_1 est $W_{a,b}$-isomorphe à M_2, si, et seulement si λ_{M_1} et λ_{M_2} divisent le même élément premier du centre de $W_{b,a}$.

Les résultats déduits montrent qu'une partie du § 4 pourrait être démontrée par l'application des résultats connues de la théorie de groupes. Ainsi Théorème VII exprime la 2me loi d'isomorphisme pour les $W_{b,a}$-modules, théorème XVI et une partie du théorème XV expriment la loi de JORDAN, théorèmes VIII et X en sont des cas particuliers, théorème V, VI, IX deviennent manifestes. Toutefois, nous avons préféré la méthode directe basée sur l'analogie de $W_{a,b}$ à un anneau de polynômes, parce que cette méthode est beaucoup plus puissante, surtout quand il s'agit de rélations entre les $W_{a,b}$ différents (par exemple théorème XI, XII, XIII, XIV, XV du § 4 et théorème VI du § 6).

Soit K/k un corps $\mathfrak{P}$-adique. Une suite des corps $Q_0, Q_1, \ldots, Q$ telle que

1°. $k = Q_0 \subset Q_2 \subset \ldots \subset Q_{s-1} \subset Q_s = K$.

2°. Tout Q_i/Q_{i-1} ($i = 1, 2, \ldots, s$) est primitif

s'appelera une *suite génératrice de* K/k. Cette suite s'appellera *régulière*, si elle passe par K_0. Elle s'appellera *normale* si elle passe par tous les K_i, $i = -1, 0, 1, \ldots, m$.

La suite $(Q_s : Q_{s-1}), (Q_{s-1} : Q_{s-2}), \ldots, (Q_1 : Q_0)$ s'appellera la *suite d'indices* de la suite génératrice $Q_0, Q_1, \ldots, Q_s$; s s'appellera sa longueur.

Théorème I. *Toutes les suites génératirces normales de K ont la même suite d'indices (à l'ordre près).*

DÉMONSTRATION: Il suffit de démontrer le théorème en posant $K/k = (K/k)_{-1}$, ou $K/k = (K/k)_0 / (K/k)_{-1}$, ou $K/k = (K/k)_1 / (K/k)_0$. Les deux premiers cas sont manifestes, parceque alors les indices en question sont des nombres premiers. Dans le troisième cas posons $M_i = M^{(\pi_0)}(Q_s/Q_i)$. Alors $M_0 \supset M_1 \supset \ldots \supset M_s = \{0\}$, les M_i sont tous des $W_{F,\psi}$-modules, et, pour tout $i = 0, 1, 2, \ldots, s-1$, M_i/M_{i+1} est

un $W_{F,\psi}$-module simple. Donc, si $M_i/M_{i+1} = M^{(i)}$ et si $\lambda^{(i)} = \lambda_{M^{(i)}}$, $\lambda^{(0)}\lambda' \ldots \lambda^{(s-1)}$ est une décomposition de λ_{M_0} et sa suite d'indices coïncide avec celle de $Q_0, Q_1, \ldots, Q_s$. D'où, en vertu du théorème XV de § 4, il résulte ce théorème.

Conséquence : Toutes les suites génératrices normales de K/k ont la même longueur.

Lemme 1 : M_1 et M_2 étant deux $W_{a,b}$-modules $W_{a,b}$-isomorphes, si l'on les organisé en hypergroupe par la loi de composition

$$\alpha * \beta = \alpha + [\beta]_{a,\delta},$$

où δ est tel que b soit la longueur de période de p (mod δ), les deux hypergroupes $M_1^{(\delta)}$ et $M_2^{(\delta)}$ ainsi obtenu sont isomorphes.

Démonstration : Evident.

Lemme 2 : Si M et $\overline{M} \subset M$ sont deux $W_{a,b}$-modules

$$M^{(\delta)} \overrightarrow{/} \overline{M}^{(\delta)} \simeq (M/\overline{M})^{(\delta)}.$$

Démonstration : On a $\alpha * \overline{M}^{(\delta)} * \beta * \overline{M}^{(\delta)} = \alpha + \overline{M}^{(\delta)} + [\beta + \overline{M}^{(\delta)}]_{a,\delta} = \alpha + [\beta]_{a,\delta} + \overline{M}^{(\delta)} + [\overline{M}^{(\delta)}]_{a,\delta} = \alpha + [\beta]_{a,\delta} + \overline{M}^{(\delta)}$. C. q. f. d.

On appellera *suite des hypergroupes* de la suite génératrice de K/k $Q_0, Q_1, \ldots, Q_s$ la suite $G_{Q_1/Q_0}, G_{Q_2/Q_1}, \ldots \ldots, G_{Q_s/Q_{s-1}}$. On a

Théorème II. *Les suites des hypergroupes des toutes les suites génératrices normales de K/k sont les mêmes à l'isomorphisme et à l'ordre près.*

Démonstration : On n'a encore qu'à faire la démonstraiion que pour les cas indiqués dans le théorème I. Pour le premier et le second cas le théorème est à peu près evident par suite de l'invariance de la suite d'indices et de ce que $G_{Q_i/Q_{i-1}}$ ne dépend alors, à isomorphisme près, que du $(Q_i : Q_{i-1})$ et du f_k^+. Dans le troisième cas on a, en vertu du lemme 2,

$$G_{Q_i/Q_{i-1}} \simeq G_{Q_s/Q_{i-1}} \overrightarrow{/} G_{Q_s/Q_i} \simeq M_{i-1}^{(\delta)} \overrightarrow{/} M_i^{(\delta)} \simeq (M^{(i-1)})^{(\delta)}$$

et on n'a qu'appliquer le théorème de Jordan (c'est-à-dire théorème XV du § 5) et le lemme 1. C. q. f. d.

On dira qu'une suite génératrice $Q_0, Q_1, \ldots, Q_s$ est *ultra-normale* si, quand $Q_{i_1}/Q_{i_2} = (Q_{i_1}/Q_{i_2})_1/(Q_{i_1}/Q_{i_2})_0$ et quand $G_{Q_{i_1}/Q_{i_1-1}} \simeq G_{Q_{i_2+1}/Q_{i_2}}$, on a toujours $G_{Q_{i_3}/Q_{i_3-1}} \simeq G_{Q_{i_1}/Q_{i_1-1}}$, pour tout i_3 tel que $i_2 < i_3 \leqq i_1$. Théorème XV du § 4 montre qu'il existent des suites génératrices ultra-normales de K/k quelque soit ce corps, et que, plus généralement, si $Q_{i_q}, Q_{i_q+1}, \ldots, Q_{i_{q+1}-1}$ désignent tous les corps de la suite génératrice comprises entre K_q (inclu) et K_{q+1} (exclu), on peut trouver une suite génératrice telle que $G_{Q_{i_q+1}/Q_{i_q}}, G_{Q_{i_q+2}/Q_{i_q+1}}, \ldots, G_{Q_{i_{q+1}}/Q_{i_{q+1}-1}}$ soit une permutation donnée à l'avance des hypergroupes correspondants d'une autre suite génératrice normale de K/k (à isomorphisme près).

Les théorèmes I et II restent encore vrais pour toutes les suites génératrices régulières de K/k. On démontre ce résultat en se servant du théorème suivant que j'ai énoncé dans ma thèse [12]. Soit $\lambda_q(K/k) = z_1^{l_{q+1}(K/k)} \lambda_{M_q^{(\pi_\delta)}(K/k)}$. Soit $\overline{K}/k \subset K/k$. Soit $\lambda'_q(K/\overline{K}) = \lambda_{\varepsilon_q}(K/\overline{K})$ ou $z_1^{l_{\varepsilon_q}(K/\overline{K})}$, où dans le premier cas $v_q(K/k) = v_{\varepsilon_q}(K/\overline{K})$ et dans le second cas $v_{\varepsilon_q - 1}(K/\overline{K}) < v_q(K/k) < v_{\varepsilon_q}(K/\overline{K})$. Alors, si $\lambda''_q \lambda'_q(K/\overline{K}) = \lambda_q(K/k)$, l'ensemble des $\lambda_q(\overline{K}/k)$ coïncide avec l'ensemble de tous les λ''_q qui ne sont pas puissances de z_1, pris dans le même ordre.

Ce résultat, dont je publierai ailleurs la démonstration, établit une dualité entre $K/\overline{K}$ et $\overline{K}/k$, conséquence de celle qui existe entre les $W_{F,\psi}$-modules.

Les théorèmes I et II ne s'appliquent plus aux suites génératrices non régulières. Par exemple, si K/k est primitif et complètement ramifié de degré puissance de p mais non p, et si K^*/k est son corps de Galois, K^*/k a d'abord une suite génératrice dont les indices sont tous premiers, et, d'autre part, possède encore celle qui passe par K et dont un des indices $(K : k)$ n'est pas premier.

§ 8. — Polygônes de Newton-Puiseux-Ore

Considérons une équation

$$f(x) = \sum_{i=0}^{n} a_i x^i = 0$$

dans un corps p-adique k à coëfficients entiers et telle que $a_n = 1$. Il

[12] *Mémoires de l'Acad. de Belgique*, t. XI, fasc. 4.

s'agit de savoir quelles sont les ordres des ses racines en p et combien y a-t-il des racines de l'ordre donné?

Cette question, analogue à celle que PUISEUX, se servant des parallelogrammes de NEWTON, resolut pour les fonctions algébriques, a été resolue par M. ORE [13]. J'exposerai dans ce paragraphe, en la simplifiant, la méthode de M. ORE.

LEMME: Soit $f(x)=\sum_{i=0}^{n} a_i x^i = 0$ une équation à coëfficients entiers dans k non tous $\equiv 0 \pmod{\mathfrak{p}}$. Soit m le plus grand entier tel que $a_m \not\equiv 0 \pmod{\mathfrak{p}}$. Alors $f(x)$ a m racines (comptées avec leur degré de multiplicité) entiers.

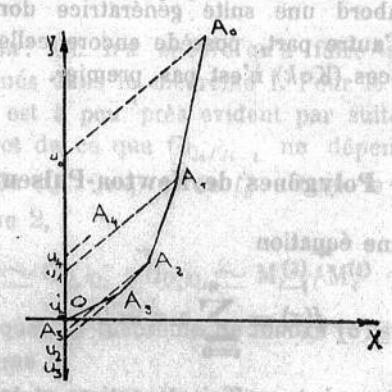
DÉMONSTRATION: Soit

$$f(x)=a_n\Pi(x-\alpha_q)\,\Pi(x-\beta_q)$$

où les α_q sont entiers et les β_q ne le sont pas. Soit ρ_q l'ordre de β_q. Pour que les coëfficients de $f(x)$ soient entiers et non tous nuls (mod p), il faut et il suffit, d'après un théorème bien connu de GAUSS, que l'ordre de a_n soit $-\Sigma\rho_q$. Alors $a_n\Pi\beta_q$ est un entier $A \not\equiv 0 \pmod{\mathfrak{p}}$ et $a_n\Pi(x-\beta_q)\equiv A \pmod{\mathfrak{p}}$. Donc $f(x)\equiv A\Pi(x-\alpha_q) \pmod{\mathfrak{p}}$, d'où le nombre des α_q est m. C. q. f. d.

Prenons un plan des coordonnées xOy. Soit s_i l'ordre de a_i en p. Marquons sur le plan $n+1$ points

$$A_i=(x=n-i,\ y=s_i) \qquad (i=0,\ 1,\ \ldots\ \ldots,n).$$



[13] *Acta Mathematica*, 1923, t. 44, p. 218—314.

Construisons une ligne brisée $C=A_nA_{i_1}A_{i_2}\ldots A_0$ ayant les propriétés suivantes. 1°. Tous ses sommets sont des points A_i 2° elle est convexe 3° tout point A_i se trouve sur C ou au-dessus de C. Une telle ligne, que nous appellerons le *polygône caractéristique* de $f(x)$, peut être construite, et d'une seule manière: en effet, soit qu'on ait déjà construit μ segments $A_nA_{i_1}$, $A_{i_1}A_{i_2}$, ..., $A_{i_{\mu-1}}A_{i_\mu}$ ayant la propriété que 1°. $A_nA_{i_1}\ldots\ \ldots A_{i_\mu}$ est convexe. 2°. Tout point A_i se trouve soit au-dessus de la ligne C_μ obtenue de $A_nA_{i_1}\ldots A_{i_\mu}$ en prolongeant indéfiniment la demi-droite $A_{i_{\mu-1}}A_{i_\mu}$, soit sur $A_nA_{i_1}\ldots A_{i_\mu}$, et soit qu'on ait déjà démontré que toute ligne C ayant les trois propriétés indiquées a ces μ segments comme μ premiers côtés. Si $i_\mu=n$, notre affirmation est démontrée. Sinon, l'angle $UA_{i_\mu}Y$, où $A_{i_\mu}U$ est le prolongement de $A_{i_{\mu-1}}A_{i_\mu}$ et où $A_{i_\mu}Y \parallel Oy$, contient des points A_i. Par conséquent parmi les demi-droites de sommet A_{i_μ} contenus dans cet angle il y a une et une seule $A_{i_\mu}Q$ telle que 1°. il y des points A_i (autres que A_{i_μ}) sur $A_{i_\mu}Q$ 2°. l'angle $UA_{i_\mu}Q$ ne contient aucun A_i. Soit $A_{i_{\mu+1}}$ le point A_i de la plus grande abscisse qui se trouve sur $A_{i_\mu}Q$. Le $\mu+1^{\text{ième}}$ côté d'une ligne C ne peut pas être au-dessous de $A_{i_\mu}Q$, parce que alors son deuxième sommet ne serait pas un point A_i. Il ne peut pas être non plus au-dessus, car alors par exemple le point $A_{i_{\mu+1}}$ serait au dessous de C. Donc la direction du $\mu+1^{\text{ième}}$ côté de C doit coïncider avec $A_{i_\mu}A_{i_{\mu+1}}$. Le deuxième sommet de ce côté doit être $A_{i_{\mu+1}}$, car autrement ou bien il ne serait pas un point A_i, ou bien $A_{i_{\mu+1}}$ serait au-dessous de C.

Enfin la ligne $A_nA_{i_1}\ldots A_{i_\mu}A_{i_{\mu+1}}$ est convexe et tous les points A_i se trouvent sur cette ligne ou au-dessous de $C_{\mu+1}=A_nA_{i_1}\ldots A_{i_\mu}A_{i_{\mu+1}}Q$. En poursuivant ce raisonnement on démontre l'affirmation.

Ceci posè, soit que $C=A_nA_{i_1}\ldots A_{i_{\mu-1}}A_0$ est le polygône caractéristique de $f(x)$. $L_j=A_{i_{j-1}}A_{i_j}$ $(j=1,\ 2,\ \ldots,\ \mu;\ i_0=0,\ i_\mu=n)$ sera appelé le j-ième côté de C. Désignons par α_j le coëfficient angulaire $\frac{s_{i_j}-s_{i_{j-1}}}{i_{j-1}-i_j}$ de L_j. On désignera par l_j la projection $i_{j-1}-i_j$ de L_i sur Ox, et par $s^{(j)}$ la projection $s_{i_j}-s_{i_{j-1}}$ sur Oy.

D'ailleurs les A_{i_j} peuvent être définis par récurrence comme des points A_i tels que

$$\frac{s_i-s_{i_j+1}}{i-i_{j+1}}>\frac{s_{i_j}-s_{i_j+1}}{i_j-i_{j+1}} \text{ pour tout } i>i_j \text{ et } \geq \frac{s_{i_j}-s_{i_j+1}}{i_j-i_{j+1}}$$
$$\text{pour tout } i>i_{j+1},$$

ou aussi comme des A_i tels que

$$\frac{s_i-s_{i_{j-1}}}{|i-i_{j-1}|}>\frac{s_{i_j}-s_{i_{j-1}}}{|i_j-i_{j-1}|} \text{ pour tout } i<i_j \text{ et } \geq \frac{s_{i_j}-s_{i_{j-1}}}{|i_j-i_{j-1}|}$$
$$\text{pour tout } i<i_{j-1},$$

Théorème I. *L'équation $f(x)=0$ a l_j racines d'ordre α_j en $\mathfrak{p}$ $(j=1, 2, \ldots, \mu)$. Ces l_j racines satisfont à une équation de degré l_j dans k. π_0 étant un nombre de k d'ordre 1 en $\mathfrak{p}$, les $\pi_0^{-\alpha_j}\beta$, où les β sont les racines en question, satisfont à l'équation de degré l_j congrue (mod $\mathfrak{p}$) à*

$$\sum \frac{a_i}{\pi_0^{s_i}} x^{i-i_j}$$

la somme étant étendue sur tous les i tels que A_i est sur L_j.

Démonstration : Les β étant les racines de $f(x)=0$,

$$f(\pi_0^{\alpha_j} x)=0$$

a pour racines les $\pi^{-\alpha_j}\beta$. Le nombre des β d'ordre α_j en $\mathfrak{p}$, est égal au nombre de racines d'ordre 0 de $f(\pi_0^{\alpha_j} x)=0$. Or

$$f(\pi_0^{\alpha_j} x)=\sum_{i=0}^{n} a_i \pi_0^{i\alpha_j} x^i .$$

$a_i \pi_0^{i\alpha_j}$ est d'ordre $s_i + i\alpha_j$ en $\mathfrak{p}$. Cet ordre diffère par une constante $n\alpha_j$ de l'ordonnée $u_j = s_j - (n-i)\alpha_j$ de l'intersection de la droite parrallèle à L_j qui passe par A_i avec Oy. Par conséquent cet ordre est égal par exemple à $s_{i_j} + i_j \alpha_{i_j}$ quand A_i est sur L_j, et est plus grand quand A_i n'est pas sur L_j. Donc l'équation auquelle satisfont les $\pi_0^{-\alpha_j}\beta$ entiers est, d'après la lemme, de degré i_{j-1} (car $\frac{f(\pi^{\alpha_j} x)}{\pi^{s_{i_j}+\alpha_j i_j}}$ est à coëfficients entiers et $a_{i_{j-1}}$ est le dernier coëfficient $\not\equiv 0 \pmod{\mathfrak{p}}$) et i_j premiers coëfficient sont $\equiv 0 \pmod{\mathfrak{p}}$. Donc parmi les i_{j-1} nombres $\pi^{-\alpha_j}\beta$ entiers il y a i_j d'ordre positif, donc $i_{j-1} - i_j = l_j$ d'ordre 0. Donc il y a l_j racines de $f(x)$ d'ordre α_j. Comme $\sum_{j=1}^{\mu} l_j = n$, les α_j sont les seuls ordres possibles de racines. Comme le conjugué de l'idéal premier d'un corps local est égal a cet idéal, le conjugué d'un nombre doit être du même ordre que ce nombre. Donc les β d'ordre α_j forment l'ensemble des racines d'un facteur $f_j(x)$ de degré l_j de $f(x)$ dans k.

D'après la démonstration du lemme on voit qu'on peut poser

$$\pi_0^{-s_{i_j}-\alpha_j i_j} f_j(\pi_0^{-\alpha_j} x) \equiv \sum_{i=i_j}^{i_{j-1}} \pi_0^{-s_{i_j}-\alpha_j i_j} a_i x^{i-i_j} \pmod{\mathfrak{p}}.$$

Or $\pi_0^{-s_{i_j}-\alpha_j i_j} a_i \equiv 0 \pmod{\mathfrak{p}}$ si A_i n'est pas sur L_j, et est égal à $\frac{a_i}{\pi_0^{s_i}}$ si A_i est sur L_j, et tout et prouvé.

Définition 1 : On dira que le terme $a_i x^i$ de $f(x)$ est *prepondérant* pour $x=x_0$, si l'ordre de $a_i x_0^i$ est plus grand que celui de tout autre $a_{i'} x_0^{i'}$, $i' \neq i$. Plus généralement, on dira que la somme $\sum_{i\in I} \alpha_i x^i$ d'un certain ensemble des termes de $f(x)$ est *propondérante* pour $x=x_0$, si : 1° $a_i x_0^i$ pour tout $i \in I$ à un même ordre ; 2° $\sum_{i\in I} a_i x_0^i$ a encore le même ordre ; 3° $a_i x_0^i$ a un ordre plus grand que le précédent, quand i non $\in I$.

Théorème II. *Si l'ordre de x_0 en $\mathfrak{p}$ est compris à l'intérieur du segment (α_j, α_{j+1}) (on posé $\alpha_0 = 0$, $\alpha_{\mu+1}=\infty$) le terme prépondérant est $a_{i_j} x^{i_j}$. Si l'ordre de x_0 est α_j, la somme $\sum_{A_i \in L_j} a_i x^i$ est prépondérante, quand*

$$\sum_{A_i \in L_j} \frac{a_i}{\pi_0^{s_i}} \left(\frac{x_0}{\pi_0^{\alpha_j}}\right)^i \text{ est d'ordre 0.}$$

Démonstration : ρ étant l'ordre de x_0, l'ordre de $a_i x_0^i$ est $s_i + i\rho = s_i - (n-i)\rho + \rho n = u_i(\rho) - \rho n$, où $u_i(\rho)$ est l'ordonnée de l'intersection avec Oy de la droite de coëfficient angulaire ρ qui passe par A_i. Si $\alpha_j < \rho < \alpha_{j+1}$, le polygône caractéristique C de $f(x)$ se trouve tout entier au-dessus de la droite de coëfficient angulaire ρ qui passe par le deuxième sommet A_{i_j} de L_j. Donc $u_{i_j}(\rho)$ est moindre que tout autre $u_i(\rho)$, et la première partie du théorème est prouvée. Si $\rho = \alpha_j$, toutes les parties de C autres que L_j se trouvent au-dessus de L_j, donc les $u_i(\rho)$ sont égaux entre eux quand A_i est sur L_j et sont moindres que tous les $u_i(\rho)$ des A_i qui ne sont pas sur L_j. Pour que $\sum_{A_i \in L_j} a_i x^i$ soit prépondérante, il faut et il suffit que cette expresion ait pour $x = x_0$ le même ordre que par exemple $a_{i_j} x_0^{i_j}$, c'est-à-dire l'ordre $s_{i_j} + \alpha_j i_j$ en $\mathfrak{p}$. Cette condition peut se formuler ainsi : $\pi_0^{-s_{i_j}-\alpha_j i_j} \sum_{A_i \in L_j} a_i x_0^i$ est d'ordre 0. Or, si $A_i \in L_j$, on a $s_i + \alpha_j i = s_{i_j} + \alpha_j i_j$, d'où, l'expression écrite est

$$\sum_{A_i \in L_j} \pi_0^{-s_i-\alpha_j i} a_i x_0^i = \sum_{A_i \in L_j} \frac{a_i}{\pi_0^{s_i}} \left(\frac{x_0}{\pi_0^{\alpha_j}}\right)^i ,$$

et tout est prouvé.

§ 9. — Equations d'Eisenstein. Condition de primitivité

Dans les paragraphes 1—7 on a étudié les propriétés des corps $\mathfrak{P}$-adiques d'une manière abstraite, en se servant des propriétés des hypergroupes de la suite caractéristique, et, en particulier, on a trouvé les conditions nécessaires et suffisantes de primitivité d'un tel corps K/k en supposant connu le module $M^{(\pi_0)}$ et, bien entendu, f_0 et les v_q. Mais, en réalité, on définit un corps K/k en donnant l'équation irréductible dans k à laquelle satisfait un élément primitif de K. Par conséquent, il est intéressant de pouvoir former directement à partir d'une telle équation, tout au moins quand cette équation satisfait aux certaines conditions qui ne soient pas trop restrictives, des objets caractérisant K/k dont il s'agissait au §§ 2 -7 et de pouvoir ainsi répondre directement à la quéstion: une équation irréductible dans k est-elle primitive ? Il se trouve d'ailleurs qu'on peut démontrer ainsi indepen-demment de toute considération de la théorie des groupes ou des hypergroupes un certain nombre des propriétés démontrées au § 2. Même, comme on verra, on peut démontrer directement un théorème que jusqu'à présent on n'a pu démontrer qu'en le réduisant au cas des corps cycliques relatifs.

Je me borne dans ce travail uniquement aux équations dans k

$$f(x) = x^n + a_1 x^{n-1} + \ldots \quad \ldots + a_n = 0 \tag{1}$$

qui sont du type d'Eisenstein, c'est-à-dire telles que $a_1 \equiv a_2 \equiv \ldots \equiv a_n \equiv 0 \pmod{\mathfrak{p}}$ et $a_n \equiv\!\!\!| \equiv 0 \pmod{\mathfrak{p}^2}$. D'ailleurs, pour la question de primitivité l'étude des ces équations suffit largement: on a vu, en effet, que si un corps K/k ($\mathfrak{P}$-adique) est primitif, ou bien $(K:k)$ est premier, ou bien K k est, en particulier, complètement ramifié. Dans ce dernier cas un élément π de K d'ordre 1 en $\mathfrak{P}$ satisfait à une équation d'Eisenstein dans k.

Considérons donc une équation dans k

$$f(x) = \sum_{i=1}^{n} a_i x^{n-i} = 0 \qquad (\text{avec } a_0 = 1)$$

du type d'Eisenstein. Soit π une des racines de cette équation. Posons $K = k(\pi)$. L'idéal premier de K est $\mathfrak{P} = (\pi) = \mathfrak{p}^{\frac{1}{n}}$. Posons $n = hp^r$, avec $(h, p) = 1$. L'ordre en $\mathfrak{P}$ d'un élément x d'un surcorps algébrique de K sera noté $\omega(x)$. On posera $\omega(p) = E = e_0 h p^r$. On écrira $\omega(a_i) = t_i$.

Ceci posé, considérons l'équation dans K

$$\Phi(y) = f(\pi y + \pi) = 0 \tag{2}$$

dont les racines sont les $\frac{\sigma\pi - \pi}{\pi}$, où σ parcourt $G_{K/k}$. D'après la définition même des nombres de ramification et des fonctions $\beta_q(\sigma)$, il est évident que $\Phi(y)$ a $n_q - n_{q+1}$ racines d'ordre $v_q(K/k)$ et que $M_q(K/k)$ est l'ensemble des racines de la congruence qu'on obtient en égalant 0 (mod $\mathfrak{P}$) le polynôme dans K dont les quotients de ces $n_q - n_{q+1}$ racines par π^{v_q} sont des zéros (ce polynome existe en vertu du § 8).

Donc, pour calculer les $v_q(K/k)$ et les $M_q(K/k)$ il suffit de former le polygône caractéristique de $\Phi(y)$ [13] et de décomposer $\Phi(y)$ en facteurs correspondants aux côtés de ce polygône, qui sera appelé le *polygône de ramification* de K/k [14]. En effet, le coefficient angulaire α_j du côté L_j de ce polygône est, d'après le § 8, égal à $v_{j-1}(K/k)$ si $\alpha_1 > 0$, et à $v_{j-2}(K/k)$ si $\alpha_1 = 0$, et, $\Phi_j(y)$ étant le facteur de $\Phi(y)$ correspondant à L_j, la congruence

$$\pi^{-s_{ij} - \alpha_j i_j} \Phi_j(\pi^{\alpha_1} y) \equiv 0 \pmod{\mathfrak{P}} \tag{3}$$ [14]

a l'ensemble des racines distinctes égal à $M_{j-1}(K/k)$ ou à $M_{j-2}(K/k)$ resp. Le polygône de ramification a des propriétés très remarquables, que les polygônes caractéristiques généraux n'ont pas. C'était d'ailleurs à prevoir d'après les § 1—7, car les n_q sont puissances de p, si $q \geq 0$, es v_q ont leur dénominateur premier à p, les $M_q(K/k)$ sont des Ω_{ψ_q}-modules, où ψ_q est la longueur de la période de $p \pmod{\delta_q}$, admettant z_{f_0} comme opérateur etc... Toutes ces propriétés doivent apparaître dans la structure du polygône de ramification de K/k et des congruences (3).

Nous allons étudier dans ce paragraphe quelles sont ces propriétés, et nous ferons cette étude directement, sans faire appel aux résultats et méthodes des §§ 1—7. Ainsi nous redémontrerons d'une autre manière un certain nombre de ces résultats, ainsi que démontrerons certains autres résultats dont il n'y était pas question.

On a

$$\Phi(y) = f(\pi y + \pi) = f(\pi) + \frac{f'(\pi)}{1!}\pi y + \frac{f''(\pi)}{2!}\pi^2 y^2 + \ldots + \frac{f^{(n)}(\pi)}{n!}\pi^n y^n. \quad [15]$$

---

[13] Multiplié par une puissance convenable de π de manière à rendre son coëfficient de la plus grande puissance de $y \equiv\!\!\!| \equiv 0 \pmod{\mathfrak{P}}$.

[14] Il et visible que le polygône de ramification de K/k, ainsi que, dans une certaine mésure, la congruence écrite plus bas, ne dépendent pas du choix de l'équation d'Eisenstein qui définit K/k.

[15] Les polynômes de la forme légèrement différente ont été déjà employés par M. Hensel, mais pour des buts totalement différents. D'ailleurs, les équations $f(x) = 0$ à partir desquelles M. Hensel les formait ne pouvaient jamais être de type d'Eisenstein.

Posant

$$b_i = \frac{f^{(i)}(\pi)}{i!}\pi^i$$

on a

$$\Phi(y) = \sum_{i=0}^{n} b_i y^i.$$

On a

$$b_i = \sum_{x=1}^{n} \frac{x(x-1)\dots(x-i+1)}{1\cdot 2\dots i} a_{n-x}\pi^x, \text{ si } i>0, \text{ et } b_0 = f(\pi) = 0.$$

Posons

$$\theta_{i,x} = \omega\left(\frac{x(x-1)\dots(x-i+1)}{1\cdot 2\dots i}\pi^x\right).$$

Théorème I. $\omega(b_i) = \underset{x=1,\dots,n}{\text{Min}}\,[\theta_{i,x}+t_{n-x}]$ $(i>0)$, *et* $\omega(b_0) = +\infty$.

DÉMONSTRATION : $\dfrac{x(x-1)\dots(x-i+1)}{1\cdot 2\dots i}a_{n-x}$ est un nombre de k. Donc son ordre en $\mathfrak{P}$ est multiple de celui de p, c'est-à-dire de n. Donc $\omega\left(\dfrac{x(x-1)\dots(x-i+1)}{1,\,2\dots i}a_{n-x}\pi^x\right) = \theta_{i,x}+t_{n-x} \equiv x \pmod n$. Comme tous les x sont incongrûs mod n (car ils sont tous >0 et $\leq n$), tous les $\dfrac{x(x-1)\dots(x-i+1)}{1,\,2\dots i}a_{n-x}\pi^x$ $(x=1,\,2,\dots,n)$ ont des ordres différents, et leur somme b_i a l'ordre égal au minimum de leurs ordres. C. q. f. d.

Théorème II. 1°. *Si* $p^u < i < p^{u+1}$ $(u<r)$, on a

$$\omega(b_i) \geq \omega(b_{p^u}).$$

2°. $\omega(b_{p^r}) = \omega(b_n) = n$ et, pour tout i, $\omega(b_i) \geq n$.

DÉMONSTRATION : 1°. On a $\theta_{i,x} - \theta_{p^u,x} = \omega\left(\dfrac{(x-p^u)(x-p^u-1)\dots(x-i+1)}{(p^u+1)(p^u+2)\dots i}\right)$.

Le numérateur de $\prod_{j=p^u+1}^{i}\left(\dfrac{x-j+1}{j}\right)$ est le produit des $i-p^u$ entiers consécutifs. Donc, parmi ces entiers il y a au moins $\mathrm{E}\dfrac{i-p^u}{p}$ (16) divisibles par p dont au moins $\mathrm{E}\dfrac{i-p^u}{p^2}$ divisibles par p^2, dont ... ... dont au moins $\mathrm{E}\dfrac{i-p^u}{p^l}$ divisibles par p^l $(l<u)$, ..., dont au moins $\mathrm{E}\dfrac{i-p^u}{p^u}$ divisibles par

(16) Au cours de la démonstration de ce théorème Ea désigne la partie entière d'un nombre a (et non le produit de a par l'ordre absolu E de $\mathfrak{P}$).

p^u. Or $(p^u+1)\dots\dots i$ a juste $\mathrm{E}\dfrac{i-p^u}{p}$ facteurs divisibles par p, dont $\mathrm{E}\dfrac{i-p^u}{p^2}$ divisibles par p, ..., dont $\mathrm{E}\dfrac{i-p^u}{p^u}$ divisibles par p^u et, puisque $i<p^{u+1}$, aucun divisible par p^{u+1}. Donc $\prod_{j=p^u+1}^{i}\left(\dfrac{x-j+1}{j}\right)$ est entier et $\theta_{i,x} \geq \theta_{p^u,x}$ pour tout $x = 1, 2, \dots, n$. Donc $\omega(b_i) = \text{Min}\,[\theta_{i,x}+t_{n-x}] \geq$ $\geq \text{Min}\,[\theta_{p^u,x}+t_{n-x}] = \omega(b_{p^u})$.

2°. On a $\theta_{n,x} = +\infty$ si $x<n$ et $\theta_{n,n} = \omega\left(\dfrac{n!}{n!}\pi^n\right) = n$. D'autre part $t_{n-n} = t_0 = \omega(1) = 0$. Donc $\omega(b_n) = \text{Min}\,[\theta_{n,x}+t_{n-x}] = \text{Min}\,[n, +\infty] = n$. D'autre part $\theta_{p^r,n} = \omega\left(\dfrac{hp^r(hp^r-1)\dots(hp^r-p^r+1)}{1\quad 2\dots}\pi^n\right) = n$ et $\theta_{p^r,x} =$ $= \omega\left(\dfrac{x(x-1)\dots(x-p^r+1)}{1\cdot 2\dots p^r}\pi^x\right) > 0$, et $t_{n-x} = \omega(a_{n-x}) \geq \omega(p) = n$ pour tout $x<n$; donc $\omega(b_{p^r}) = \text{Min}\,[n, \theta_{p^r,x}+t_{n-x}]_{x=1,2,\dots,n-1} = n$.

Enfin, si i est quelconque, on a toujours $\theta_{i,x}>0$ et $\theta_{i,n} \geq n$. Comme $t_0=0$ et t_{n-x}, $x \neq n$, est $\geq n$, on a pour tout i et tout x $\theta_{i,x}+t_{n-x} \geq n$, donc $\omega(b_i) \geq n$.

Posons

$$\omega_u = \omega(b_{p^u}).$$

Définissons par récurrence la suite des nombres $w_r, w_{r-1}, \dots, w_0$ de la manière suivante : 1°. $w_r = \underset{0<x\leq n}{\text{Min}}\,[\theta_{0,x}+t_{n-x}]$. 2°. $w_r, w_{r-1}, \dots, w_{u+1}$ étant définis, $w_u = \underset{\substack{x \equiv 0 \pmod{p^{u+1}} \\ 0<x\leq n}}{\text{Min}}\,[w_{u+1}+\mathrm{E},\ \theta_{0,x}+t_{n-x}]$.

Théorème III. *Si* $w_u \neq w_{u-1}$, $w_u = \omega_u$. *Si* $w_u = w_{u-1}$, $w_u \leq \omega_u$.

DÉMONSTRATION : On a

$$\omega_u = \text{Min}\,[\theta_{p^u,x}+t_{n-x}] = \text{Min}\left[\omega\left(\frac{x!}{p^u!\,(x-p^u)!}\right)+\theta_{0,x}+t_{n-x}\right].$$

Or, quelque soit l'entier x, $\dfrac{x!}{p^u!\,(x-p^u)!}$ est entier. Et si la contribution de p en x est $u+s$ avec $s \geq 0$, p entre dans $\dfrac{x!}{p^u!\,(x-p^u)!}$ avec l'exposant s, c'est-à-dire $\omega\left(\dfrac{x!}{p^u!\,(x-p^u)!}\right) = s\,\mathrm{E}$. Donc

$$\omega_u \geq \text{Min}\,[\text{Min}\,[\theta_{0,x}+t_{n-x}],\ \underset{\substack{x \equiv 0 \pmod{p^u} \\ 0\leq s<r-u}}{\text{Min}}\,[\theta_{0,x}+t_{n-x}+s\mathrm{E}],\ \underset{x \equiv 0 \pmod{p^r}}{\text{Min}}\,[\theta_{0,x}+t_{n-x}+(r-u)\mathrm{E}]$$

$$\geq \text{Min}\left[w_{u-1},\ \underset{0\leq s\leq r-u}{\text{Min}}\,[w_{u+s}+s\mathrm{E}]\right] \geq w_u$$

parce que $w_{u-1} \geq w_u$ et $w_{u+s} + sE \geq w_u$ par définition.

D'autre part, on a $\operatorname{Min}_{x \equiv 0 \pmod{p^r}} [\theta_{0,x} + t_{n-x}] = n = \theta_{0,n} + t_0$, c'est-à-dire est atteint pour un $x \not\equiv 0 \pmod{p^{r+1}}$.

Donc $\operatorname{Min}_{x \equiv 0 \pmod{p^r}} \left[\omega\left(\frac{x!}{p^u!\,(x-p^u)!}\right) + \theta_{0,x} + t_{n-x}\right] = \operatorname{Min}_{x \equiv 0 \pmod{p^r}} [\theta_{0,x} + t_{n-x}] + (r-u)E$.

Donc $\omega_u \leq \operatorname{Min}_{0 \leq s < r-u} [\operatorname{Min}_{x \equiv 0 \pmod{p^{u+s}}} [\theta_{0,x} + t_{n-x}] + sE], \operatorname{Min}_{x \equiv 0 \pmod{p^r}} [\theta_{0,x} + t_{n-x}] + (r-u)E]$.

$x \not\equiv 0 \pmod{p^{u+s+1}}$

Posons

$$w'_{u+s} = \operatorname{Min}_{\substack{x \equiv 0 \pmod{p^{u+s}} \\ x \not\equiv 0 \pmod{p^{u+s+1}}}} [\theta_{0,x} + t_{n-x}]; \quad w'_r = \operatorname{Min}_{x \equiv 0 \pmod{p^r}} [\theta_{0,x} + t_{n-x}]$$

On a, si $w_u \neq w_{u-1}$,

$w_u = \operatorname{Min} [w'_u, w_{u+1} + E]$; $w_{u+1} = \operatorname{Min} [w'_u, w'_{u+1}, w_{u+2} + E]$; ... ; $w_{u+s} = \operatorname{Min} [w'_u, w'_{u+1}, \ldots, w'_{u+s}, w_{u+s+1} + E]$; ... ; $w_r = w'_r$.

Donc $w_u = \operatorname{Min}_{0 \leq s \leq r-u} [w'_{u+s} + sE] \geq \omega_u$

comme, d'autre part, $w_u \leq \omega_u$, on a, si $w_u \neq w_{u-1}$, $w_u = \omega_u$ c. q. f. d.

Désignons par

$$w_{i_0} = w_r, \; w_{i_1}, \ldots, w_{i_s} = w_0$$

ceux des $w_r, w_{r-1}, \ldots, w_0$, écrites dans l'ordre des grandeurs croissantes, qui satisfont à la condition

$$w_i \neq w_{i-1}$$

si $i = i_q$, on a $\omega_i = w_i$; si, $i_{q-1} > i > i_q$, on a $\omega_i \geq w_i = w_{i_q}$. Et on a

$$w_{i_q} - w_{i_{q-1}} = w_{i_{q-1}-1} - w_{i_q - 1} \leq E.$$

D'ailleurs, si $w_{i_q} - w_{i_{q-1}} \neq E$, l'ordre de w_{i_q} en p est i_q. En effet, alors $w_{i_q} = \operatorname{Min}_{x \not\equiv 0 (p^{u+1})} [\theta_{0,x} + t_{n-x}]$ et ce minimum est atteint, puisque $w_{i_q} \neq w_{i_q - 1}$, pour un $x \equiv 0 \pmod{p^u}$. Or $\theta_{0,x} + t_{n-x} \equiv \theta_{0,x} \equiv x \pmod{n}$, ce qui prouve l'affirmation.

Considérons le polynôme $\pi^{-n}\Phi(y)$. Le polygône de ramification R est son polygone caractéristique. On a

Théorème IV. *Les sommets du polygône* R *autres que* $(0, 0)$ *et* $(n, +\infty)$ *se trouvent compris parmi les points* $(n - p^{i_{q'}}, w_{i_{q'}} - n)$. *Ils peuvent être déterminés par la régle de récurrence suivante: un sommet* $P = (n - p^{i_q}, w_{i_q} - n)$ *étant trouvé, le sommet le plus proche à droite* $P' = (n - p^{i_{q'}}, w_{i_{q'}} - n)$ *est tel que* q' *est le plus grand nombre satisfaisant à l'égalité*

$$\frac{w_{i_{q'}} - w_{i_q}}{p^{i_q} - p^{i_{q'}}} = \operatorname{Min}_{t > q} \left| \frac{w_{i_t} - w_{i_q}}{p^{i_q} - p^{i_t}} \right|.$$

Démonstration : R est le polygône convexe reliant $(0, \omega(b_n) - n) = (0, 0)$ à $(n, \omega(b_0)) = (n, +\infty)$, ayant pour sommets certains de points $(n - i, \omega(b_i) - n)$ et tel que tous les $(n - i, \omega(b_i) - n)$ se trouvent sur ou au-dessus de son contour. Ceci montre, tout d'abord, que $(n - i, \omega(b_i) - n)$ ne peut être un sommet du polygône que si $i = p^j$, $j \leq r$. En effet, tout d'abord $(n - p^r, \omega(b_{p^r}) - n) = (n - p^r, \omega_{p^r} - n) = (n - p^r, 0)$, donc, si un $(n - i, \omega(b_i) - n)$, $i > p^r$, est un sommet de R, $(n - p^r, \omega(b_{p^r}) - n)$ est au-dessous de R. Si un $(n - i, \omega(b_i) - n)$, $p^j < i < p^{j+1} \leq p^r$ est un sommet de R, on a, puisque $\omega(b_{p^j}) \leq \omega(b_i)$, que $(n - p^j, \omega(b_{p^j}) - n)$ se trouve au dessous ou sur la demi-droite parallèle à Ox qui passe par un sommet de R, donc est au-dessous de R.

Donc, les sommets de R autres que $(0, 0)$ et $(n, +\infty)$ sont parmi les points $(n - p^i, \omega_i - n)$ $(i = r, r-1, \ldots, 0)$. D'ailleurs, $(n - p^r, 0)$ est sûrement un sommet de R. En effet, si $0 < i < p^r$, on a

$$\theta_{i,n} > n\left(\operatorname{car} \frac{hp^r.(hp^r-1) \ldots (hp^r-i+1)}{1. \; 2 \ldots \qquad i} \text{ se divisise par } p\right),$$

donc $\theta_{i,n} + t_0 > n$; et, d'autre part, puisque par tout $x > 0$ on a $\theta_{i,n} \geq x > 0$ et, si $x \neq n$, $t_{n-x} \geq n$, on a pour tout $x > 0$

$$\theta_{i,x} + t_{n-x} > n;$$

donc

$$\omega(b_i) - n > 0,$$

et $(n - p^r, 0)$ est le point $(n - i, \omega(b_i) - n)$ de l'axe Ox ayant la plus grande abcisse. Supposons que $(n - p^i, \omega_i - n)$ soit un sommet de R.

Je dis que i doit se trouver parmi les i_q. Supposons, en effet, que $i_q < i < i_{q-1}$. Alors $\omega_{i_q} = w_{i_q} = w_i \leq \omega_i$. Donc le point $(n - p^{i_q}, \omega_{i_q} - n)$ se trouve sur au au-dessous de la demi-droite parallèle à Ox qui passe par un sommet de R, donc au-dessous de R, ce qui est absurde.

Mais $\omega_{i_q} = w_{i_q}$. Envisageons le polygône convexe R′ réliant $(0, 0)$ à $(n, +\infty)$, ayant pour sommets certains des points $(n - p^{i_q}, w_{i_q} - n)$, et tel que tous ces points se trouvent sur ou au-dessus de R′. D'après le § 8 il n'existe qu'un seul polygône possèdant ces propriétés. Comme R les possède, on doit avoir R′ = R.

Le reste du théorème transcrit la méthode de construction de R′ donnée au § 8. C. q. f. d.

Posons $P_i = (n - p^i, w_i - n)$ $(i = 0, 1, \ldots, r)$. Soient

$$j_0 = r, j_1, \ldots, \ldots, j_m = 1$$

les i écrits dans l'ordre des grandeurs décroissantes tels que P_i soit un sommet de R, et soient

$$j_q = i_0^{(q)}, i_1^{(q)}, \ldots, i_{s_q}^{(q)} = j_{q+1}$$

tous les i tels que P_i se trouve sur le côté $P_{j_q} P_{j_{q+1}}$ de R. Soit $\beta_i^{p^{j_{q+1}}} \equiv \frac{b_p{}^i}{\pi^{\omega_i}}$ (donc β_i, en vertu du théorème 1 de ce §, est congru mod $\mathfrak{P}$ à un nombre de k d'ordre 0). Alors on a

Théorème V. $v_q(K/k) = \frac{w_{j_{q+1}} - w_{j_q}}{p^{j_q} - p^{j_{q+1}}}$, $n_q(K/k) = p^{j_q}$ *et* $M_q(K/k)$ *est l'ensemble des racines de la congruence* $(q > 0)$

$$\sum_{t=0}^{s_q} \beta_{i_t^{(q)}} \xi^{p^{i_t^{(q)}} - j_{q+1}} \equiv 0 \pmod{\mathfrak{p}}.$$

Démonstration : En effet, le côté $(0, 0) P_r$ a le coëfficient angulaire nul, donc l'ordre des $n - p^r$ racines qui lui correspondent est 0. Donc les coëfficients angulaires des autres côtés sont positifs, et les nombres de ramification de K/k positifs coïncident avec ces coëfficients angulaires. Donc $v_q(K/k)$ $(q > 0)$ est le coëfficient angulaire de $P_{j_q} P_{j_{q+1}}$ c'est-à dire $\frac{w_{j_{q+1}} - w_{j_q}}{(n - p^{j_{q+1}}) - (n - p^{j_q})} = \frac{w_{j_{q+1}} - w_{j_q}}{p^{j_q} - p^{j_{q+1}}}$, et il y a $p^{j_q} - p^{j_{q+1}}$ racines de $\Phi(y)$ d'ordre $v_q(K/k)$, c'est-à-dire $\sum_{s=q}^{m-1} p^{j_s} - p^{j_{s+1}}$ d'ordre fini $\geq v_q(K/k)$ et $1 = p^{j_m}$ d'ordre $+\infty$. C'est-à-dire il y a p^{j_q} des $\sigma \in G_{K/k}$ tels que $v(\sigma) \geq v_q(K/k)$, donc $n_q(K/k) = p^{j_q}$.

Enfin les $\beta_q(\sigma)$, $\sigma \in V_{K/k}^{(q)}$, sont les distincts parmi les classes (mod $\mathfrak{P}^*$) contenant $\frac{\sigma\pi - \pi}{\pi\pi'^{v_q(K/k)}}$. Mais, d'après le § 8, les $\frac{\sigma\pi - \pi}{\pi\pi'^{v_q(K/k)}}$ satisfont à l'équation congrue (mod $\mathfrak{P}$) à

$$\sum_{t=0}^{s_q} \beta^{p^{j_{q+1}}}_{i_t^{(q)}} \xi^{i_t^{(q)}} \equiv 0 \pmod{\mathfrak{p}},$$

c'est-à-dire

$$\left(\sum_{t=0}^{s_q} \beta_{i_t^{(q)}} \xi^{p^{i_t^{(q)}} - j_{q+1}} \right)^{p^{j_{q+1}}} \equiv 0 \pmod{\mathfrak{p}}.$$

Comme $\beta_{i_{s_q}^{(q)}} = \beta_{j_{q+1}} \not\equiv 0 \pmod{p}$, d'après le § 6 les racines de la congruence

$$\sum_{t=0}^{s_q} \beta_{i_t^{(q)}} \xi^{p^{i_t^{(q)}} - j_{q+1}} \equiv 0 \pmod{\mathfrak{p}}$$

sont simples, et comme ce sont les seules distinctes parmi les racines de

$$\sum_{t=0}^{s_q} \beta^{p^{j_{q+1}}}_{i_t^{(q)}} \xi^{i_t^{(q)}} \equiv 0 \pmod{\mathfrak{p}},$$

tout est prouvé.

Conséquence : Si $\bar{s}_q$ est le nombre supplémentaire de K/K_q, on a $w_{j_q} - n = \bar{s}_{-1} - \bar{s}_q$. En effet on a

$$w_{j_q} = n + \sum_{i=0}^{q-1} (w_{j_{i+1}} - w_{j_i}) = n + \sum_{i=0}^{q-1} \frac{w_{j_{i+1}} - w_{j_i}}{p^{j_i} - p^{j_{i+1}}} (p^{j_i} - p^{j_{i+1}}) =$$

$$= n + \sum_{i=0}^{q-1} v_i (n_i - n_{i+1}) = n + \sum_{i=0}^{m-1} v_i (n_i - n_{i+1}) - \sum_{i=q}^{m-1} v_i (n_i - n_{i+1}) = n + \bar{s}_{-1} - \bar{s}_q.$$

C. q. f. d.

Les théorèmes précédentes donnent le moyen de calculer les $v_q(K/k)$, les $n_q(K/k)$, et les $M_q(K/k)$ d'un corps défini par une équation d'Eisenstein. Nous allons maintenant redémontrer quelques résultats du § 2, en supposant démontrée l'existence du corps d'inertie de K/k (ce qui peut se faire sans recourrir à la théorie des groupes ou hypergroupes. Voir les travaux de Hensel).

1°. $n_0(K/k)$ *est la contribution de* p *dans* e ; *tous les* $n_q(K/k)$, $q > 0$, *sont puissances de* p.

En effet, $e = hp^r$, $n_0(K/k) = p^r$, $n_q(K/k) = p^{j_q}$.

2°. $v_q(K/k)$ *a le dénominateur* δ_q *premier à* p.

En effet $v_q(K/k) = \frac{w_{j_{q+1}} - w_{j_q}}{p^{j_q} - p^{j_{q+1}}} = \frac{w_{j_{q+1}} - w_{j_q}}{p^{j_{q+1}}(p^{j_q - j_{q+1}} - 1)}$.

Or $w_{j_{q+1}} \not\equiv w_{j_{q+1}-1}$ et $w_{j_q} \not\equiv w_{j_q - 1}$ (car j_q et j_{q+1} sont parmi les i_q). Par conséquent, $w_{j_q} \not\equiv 0 \pmod{p^{j_q}}$, $w_{j_{q+1}} \not\equiv 0 \pmod{p^{j_{q+1}}}$. Donc $w_{j_{q+1}} - w_{j_q} \not\equiv 0 \pmod{p^{j_{q+1}}}$, et δ_q est diviseur de $p^{j_q - j_{q+1}} - 1 \equiv -1 \not\equiv 0 \pmod{p}$.

3°. ψ_q *étant la longueur de la période de* $p \pmod{\delta_q}$, $M_q(K/k)$ *est un* Ω_{ψ_q}*-module admettant* z_{f_0} *comme opérateur* (f_0 — le degré absolu de $\mathfrak{p}$ dans k).

En effet, en posant

$$\lambda_q(z_1) = \sum_{t=0}^{s_q} \bar{\beta}_{i_t^{(q)}} z_1^{i_t^{(q)} - j_{q+1}},$$

où $\bar{\beta}$ est la classe (mod $\mathfrak{P}^*$) auquelle appartient β, on voit que $M_q(K/k)$

est l'ensemble des zéros de $\lambda_q(z_1)(\xi)$. Donc, d'abord, $M_q(K/k)$ est un module, ensuite, puisque les $\overline{\beta}_{i_t^{(q)}}$ sont dans Ω_{f_0}, $M_q(K/k)$ admet z_{f_0} comme opérateur. Enfin, pour que $P_{i_t^{(q)}} = (n - p^{i_t^{(q)}},\ w_{i_t^{(q)}} - n)$ soit sur $P_{j_q} P_{j_{q+1}}$, il est nécessaire que $w_{i_t^{(q)}} - w_{j_{q+1}} = -v_q(K/k)(p^{i_t^{(q)}} - p^{j_{q+1}})$. Donc $v_q(K/k)(p^{i_t^{(q)}} - p^{j_{q+1}})$ doit être entier, donc $p^{i_t^{(q)} - j_{q+1}} \equiv 1 \pmod{\delta_q}$ et, par conséquent, $i_t^{(q)} - j_{q+1} \equiv 0 \pmod{\psi_q}$. Donc $\lambda_q(z_1) \in W_{\psi_q, f_0}$, et $M_q\ K/k$ est un Ω_{ψ_q}-module.

Maintenant je vais démontrer deux résultats qui ont été démontrés 1°. dans le cas du K/k cyclique de degré p par M. Andreas Speiser [17]; 2°. dans le cas du K/k galoisien par M. Öystein Ore[18]; 3° dans le cas du K/k quelconque par moi-même dans ma thèse [12]. Et M. Ore et moi démontrions ces théorèmes par la réduction au cas cyclique de M. Speiser. Ici je veux en donner la démonstration directe.

Théorème VI. $n_q(K/k)\, v_q(K/k) \leq E\dfrac{p}{p-1}$.

Démonstration : On a $v_q(K/k) = \dfrac{w_{j_q+1} - w_{j_q}}{p^{j_q} - p^{j_q+1}}$, et, par définition des j_q, on a

1°. $w_{j_q} \neq w_{j_q-1}$.

2°. $\dfrac{w_{j_q-1} - w_{j_q}}{p^{j_q} - p^{j_q-1}} \geq \dfrac{w_{j_q+1} - w_{j_q}}{p^{j_q} - p^{j_q+1}}$.

Or, si $w_i \neq w_{i-1}$, on a $w_{i-1} \leq w_i + E$. Donc

$$v_q(K/k) = \frac{w_{j_q+i} - w_{j_q}}{p^{j_q} - p^{j_q+1}} \leq \frac{w_{j_q-1} - w_{j_q}}{p^{j_q} - p^{j_q-1}} \leq \frac{E}{p^{j_q}} \frac{p}{p-1} = \frac{E}{n_q(K/k)} \frac{p}{p-1}.$$

C. q. f. d.

Théorème VII. *Si* $v_q(K/k) \equiv 0 \pmod{p}$, $n_q(K/k)\, v_q(K/k) = E\dfrac{p}{p-1}$ *et* $r_q(K/k) = p$.

Démonstration: On a $w_{j_q} \equiv 0 \pmod{p^{j_q}}$, donc, a fortiori $\pmod{p^{j_q+1+1}}$. Donc $w_{j_q+1} - w_{j_q} \equiv w_{j_q+1} \pmod{p^{j_q+1+1}}$. Donc, si $v_q(K/k) \equiv 0 \pmod{p}$, on a $w_{j_q+1} \equiv 0 \pmod{p^{j_q+1+1}}$. Il en résulte que $w_{j_q+1} = w_{j_q+1+1} + E$.

[17] Zerlegungsgruppe. *Journ. f. d. reine u. ang. Math.*, t. 199, 1919, p. 174—188.

[18] *Math. Ann.*, t. 102, 1929—30, p. 283—304.

Or, pas définition $\dfrac{w_{j_q+1} - w_{j_q+1+1}}{p^{j_q+1} - p^{j_q+1+1}} \leq \dfrac{w_{j_q+1} - w_{j_q}}{p^{j_q} - p^{j_q+1}} = v_q(K/k)$. C'est-à-dire

$$v_q(K/k) \geq \frac{E}{p^{j_q+1+1}} \frac{p}{p-1} = \frac{E}{n_q(K/k)} \frac{p}{p-1} \frac{r_q(K/k)}{p},$$

Comme $v_q(K/k) \leq \dfrac{E}{n_q(K/k)} \dfrac{p}{p-1}$, cette inégalité ne peut être vraie que si: 1° elle est l'égalité ; 2° $\dfrac{p}{r_q(K/k)} = 1$, ce qui prouve le théorème.

Pour finir le paragraphe nous allons transcrire sous une forme directe la condition de primitivité de l'équation d'Eisenstein $f(x) = 0$.

Théorème VIII. *L'équation* d'Eisenstein $f(x) = 0$ *est primitive dans* k *si, et seulement si ou bien* a) h *est premier et* $r = 0$, *ou bien* b) 1° $h = 1$, 2° *pour tout* $q = 0, 1, \ldots r$ *on a* $\dfrac{w_q - w_r}{p^r - p^q} \geq \dfrac{w_0 - w_r}{p^r - 1}$; 3° δ *étant la dénominateur de* $v = \dfrac{w_0 - w_r}{p^r - 1}$, f_0 *étant le degré absolu de* p *dans* k, $\overline{\beta}_q$ *étant la classe* (mod $\mathfrak{P}^*$) *à laquelle appartient* $\dfrac{b_{pq}}{\pi^{\omega q}}$, *et* Q *étant l'ensemble des tous les* q *tels que* $\dfrac{w_q - w_r}{p^r - p^q} = \dfrac{w_0 - w_r}{p^r - 1}$,

$$\lambda(z_1) = \sum_{q \in Q} \overline{\beta}_q z_1^q$$

est un élément premier de W_{ψ, f_0}.

Démonstration : Evident, puisque d'après ce qui précède la condition *b)* 2° exprime que R se réduit au ségment de droite $(0, 0)(n-1, w_0-n)$ et à la demi-droite $(n-1, w_0-n)(n, +\infty)$, c'est-à-dire que K/k n'a qu'un seul nombre de ramification propre ; et $\lambda(z_1)$ est le quasi-polynôme de $M_0(K/k)$. C. q. f. d.

§ 10. — Equivalence des équations d'Eisenstein. Forme réduite.

Les résultats des §§ 8, 9 permettent de résoudre la question suivante :

Etant donné deux équations d'Eisenstein $f_1(x) = 0$ *et* $f_2(x) = 0$

dans k, sont elles équivalentes, c'est-à-dire existe-il un zéro π_1 de $f_1(x)$ et un zéro π_2 de $f_2(x)$ tels que $k(\pi_1) = k(\pi_2)$?

Et ceci non par un algorithme comportant des essaies plus ou moins arbitraires, comme cela a lieu quand on cherche à résoudre la même question en cherchant si $k(\pi_1)\, u\, k(\pi_2) = k(\pi_4)$, mais par une méthode de caractère univoque qui conduit pour chaque équation d'Eisenstein à une forme réduite.

En particulier, on parvient ainsi à donner la forme réduite de toute équation primitive dans k (à remarquer que si cette équation n'est pas de degré premier, il y a toujours une équation d'Eisenstein qui lui est équivalente), ce qui résout complètement le problème posé par M. Ore dans son mémoire des *Matematische Analen* [19] et résolu par lui pour le cas des K/k de degré premier. Envisageons donc une équation d'Eisenstein de degré $n = hp^r$

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0.$$

Choisissons une fois pour toutes un nombre $\bar{\pi}$ de k d'ordre 1 en $\mathfrak{p}$. Ecrivons les coëfficients a_i sous la forme des séries $\mathfrak{p}$-adiques entières en $\bar{\pi}$ avec des coëfficients racines $p^{f_0}-1^{\text{ièmes}}$ de l'unité ou des zéros, soit

$$a_i = \sum_{t=1}^{+\infty} \gamma_t^{(i)} \bar{\pi}^t.$$

Alors $f(x)$ peut s'écrire sous la forme

$$x^n + \sum_{t=n+1}^{+\infty} \Gamma_t \bar{\pi}^{E\left(\frac{t}{n}\right)} x^{t-nE\left(\frac{t}{n}\right)} - \Gamma\bar{\pi}$$

où

$$\Gamma_t = \gamma_{[E\left(\frac{t}{n}\right)]}^{[t-nE\left(\frac{t}{n}\right)]} \quad \text{si } t > n, \quad \text{et} \quad \Gamma = -\gamma_1^{(0)},$$

c'est-à-dire π satisfait à l'équation

$$\pi^n + \sum_{t=n+1}^{+\infty} \Gamma_t \bar{\pi}^{E\left(\frac{t}{n}\right)} \pi^{t-nE\left(\frac{t}{n}\right)} = \Gamma\bar{\pi}.$$

Pour former toutes les équations d'Eisenstein équivalentes à $f(x)$ il suffit de poser d'une manière quelconque

$$\pi = \sum_{u=1}^{+\infty} \eta_u \pi'^u$$

[19] *Math. Ann.*, t. 100, 1928, p. 650—673.

où les η_u sont des racines $p^{f_0}-1^{\text{ièmes}}$ de l'unité ou des zéros, et $\eta_1 \neq 0$, et de régarder à quelle équation de degré n satisfait π'. Il s'agit de trouver un type d'équations tel que : 1°. on puisse former un π' de la forme indiquée satisfaisant à une équation de ce type; 2°. 2 équations différentes de ce type ne soient jamais équivalentes.

Considérons une série formelle

$$x\alpha(x) = x \sum_{i=0}^{+\infty} \gamma_i x^i,$$

où les γ_i sont des racines $p^{f_0}-1^{\text{ièmes}}$ de l'unité ou des zéros, et où $\gamma_0 \neq 0$. π étant un nombre de K d'ordre 1 en $\mathfrak{P}$, désignons par $Q(\pi)$ l'ensemble de tous les nombres d'ordre 1 de K. *La série $x\alpha(x)$ définit une transformation* $A = (\alpha(x))$ *de* $Q(\pi)$ *donnée par*

$$A(\pi') = \pi'\alpha(\pi') \qquad (\pi' \in Q(\pi)).$$

Cette transformation est biunivoque. En effet, si π', $\pi'' \in Q(\pi)$ on a

$$A(\pi') - A(\pi'') = (\pi' - \pi'') \sum_{i=0}^{+\infty} \gamma_i (\pi'^i + \pi'^{i-1}\pi'' + \cdots + \pi'\pi''^{i-1} + \pi''^i)$$

On a $\omega(\gamma_0) = 0$ et $\omega(\gamma_i(\pi'^i + \pi'^{i-1}\pi'' + \cdots + \pi'\pi''^{i-1} + \pi''^i)) \geq i$, donc la série écrite converge et sa somme n'est pas 0. Donc, si $A(\pi') = A(\pi'')$, on a $\pi' = \pi''$. Enfin, il est à peu près évident, *que* $A(Q(\pi)) = Q(\pi)$.

Etant donné un $\pi' \in Q(\pi)$, il est évident que π' peut être mis d'une et d'une seule manière sous la forme $\pi \sum_{i=0}^{+\infty} \gamma_i \pi^i$ ($\gamma_i^{p^{f_0}} = \gamma_i$ ou 0, γ_0 donc *il existe une, et une seule transformation* $A = (\alpha(x))$ *telle que* $\pi' = A(\pi)$.) Il est encore à rémarquer que, en vertu de leur définition, on a $Q(\pi') = Q(\pi)$, si $\pi' \in Q(\pi)$.

On appelera *ordre de* A, et on notera $\omega(A)$ l'ordre en x de $\alpha(x) - 1$. Il est visible que $\frac{A(\pi) - \pi}{\pi}$ est d'ordre $\omega(A)$ en $\mathfrak{P}$.

Choisissons un nombre π de K d'ordre 1 en $\mathfrak{P}$, et définissons au moyen de ce nombre une loi de composition des transformations A (qui en dépend essentiellement) suivante : soient A_1, A_2 deux transformations de la forme indiquée. Alors $A_2(\pi)$, et aussi $A_1(A_2(\pi)) \in Q(\pi)$. Donc il existe une et une seule transformation de la forme indiquée A_3 telle que $A_3(\pi) = A_1(A_2(\pi))$. A_3 sera par définition, *le composé de* A_2 *par*

A_4 et sera noté $A_1 * A_2$. *La loi $*$ n'est pas, en général, ni commutative, ni associative.*

Les A ne forment pas un groupe par rapport à la loi de composition ainsi définie, parce que la loi associative n'a pas lieu, mais ils possèdent la propriété suivante :

Quand on se donne arbitrairement deux quelconques des transformations A_1, A_2, A_3, il existe une et une seule troisième telle que.

$$A_1 * A_2 = A_3 .$$

Démonstration : On a vu déjà que cela est vrai quand on se donne A_1 et A_2 ; supposons qu'on se donne A_1 et A_3. Il s'agit de trouver A_2 telle que $A_1(A_2(\pi)) = A_3(\pi)$. Il ne peut pas en avoir deux, soit A'_2 et A''_2, car alors $A'_2(\pi) \neq A''_2(\pi)$ et $A_1(A'_2(\pi)) = A_1(A''_2(\pi))$. D'autre part l'équation $A_1(\pi') = A_3(\pi)$ a une solution dans $Q(A_3(\pi)) = Q(\pi)$, et puisque $\pi' \in Q(\pi)$, il peut être mis sous la forme $A_2(\pi)$. Enfin, si l'on se donné A_2 et A_3, on a $A_2(\pi) \in Q(\pi)$, donc $Q(A_2(\pi)) = Q(\pi)$, et $A_3(\pi) \in Q(\pi) = Q(A_2(\pi))$. Donc $A_3(\pi)$ peut être mis sous la forme $A_1(A_2(\pi))$, et cela définit univoquement A_4.

Comme $\omega(A_1) = \omega(A_1(\pi) - \pi) - 1$, $\omega(A_2) = \omega(A_2(A_1(\pi)) - A_1(\pi)) - 1$ et $\omega(A_3) = \omega(A_1(A_2(\pi)) - \pi) - 1$, on voit que

$$\omega(A_3) \geq \text{Min}\,[\omega(A_1), \omega(A_2)],\ \omega(A_1) \geq \text{Min}\,[\omega(A_2), \omega(A_3)],$$
$$\omega(A_2) \geq \text{Min}\,[\omega(A_1), \omega(A_3)].$$

Posons

$$\text{E}\frac{t}{n} = a_t,\ t - n\text{E}\left(\frac{t}{n}\right) = \tau,$$

et

$$X_t = \overline{\pi}^{a_t} x^\tau.$$

Supposons donc que π satisfait à l'équation

$$f(x) = x^n + \sum_{t=n}^{\infty} \Gamma_t X_t = 0 \quad \text{(si l'on pose } \Gamma_n = -\Gamma\text{)}.$$

Soit

$$f_1(x) = x^n + \sum_{t=n}^{\infty} \Gamma'_t X_t = 0$$

l'équation à laquelle satisfait $\pi' = A(\pi)$, où $A = (\alpha(x))$ est une transformation

de la forme indiquée. Posons

$$\Gamma'_t = \Phi_{t,\pi,A}(\Gamma_t).$$

Soit $t(\pi ; A)$ le moindre t tel que $\Phi_{t,\pi,A}(\Gamma_t) \neq \Gamma_t$. Donc

$$t(\pi ; A) = \omega\left(\sum_{t=n}^{+\infty} (\Gamma'_t - \Gamma_t) X_t(\pi')\right) = \omega(f(\pi')) = \omega(f(\pi') - f(\pi)).$$

Car

$$\sum_{t=n}^{+\infty} (\Gamma'_t - \Gamma_t) X_t(\pi') = \left[\pi'^n + \sum_{t=n}^{+\infty} \Gamma'_t X_t(\pi')\right] - \left[\pi'^n + \sum_{t=n}^{+\infty} \Gamma_t X_t(\pi')\right] =$$
$$= f_1(\pi') - f(\pi') = -f(\pi') = -[f(\pi') - f(\pi)].$$

Et de plus

$$\Gamma'_{t(\pi ; A)} - \Gamma_{t(\pi ; A)} \equiv -\frac{f(\pi') - f(\pi)}{X_t(\pi')} \equiv -\frac{f(\pi') - f(\pi)}{\pi'^{t(\pi ; A)}} \Gamma'^{a_t} \pmod{\mathfrak{P}}.$$

Je dis que si π_1 et π_2 satisfont aux équations respectivement $f_1(x) = x^n + \sum_{t=n}^{+\infty} \Gamma'_t X_t = 0$ et $f_2(x) = x^n + \sum_{t=n}^{+\infty} \Gamma''_t X_t = 0$, telles que pour tout $i < t$ on ait $\Gamma_i = \Gamma'_i$, et si $t(\pi_1 ; A) \geq t$, on a aussi $t(\pi_2 ; A) \geq t$; en effet, on obtient par exemple $f_1(\pi')$ en 1°. subsistuant d'abord formellement $x\alpha(x)$ dans $f_1(x)$, c'est-à-dire prenant $f_1(x\alpha(x))$. 2. En prenant le polynôme $\sum_{i=0}^{n-1} \alpha'_i x^i$ en x de degré $< n$ congrû $f_1(x\alpha(x))$ (mod $f_1(x)$). 3°. Substituant π_1 au lieu de x dans ce polynôme. Nous appellerons *l'ordre total* d'un binôme ax^i le nombre $\omega(a) + i$. Alors $t(\pi_1 ; A)$ sera $\text{Min}_{i=0,1,\ldots,n-1} (\omega(\alpha'_i) + i)$.

Or, le développement formel de $f_1(x\alpha(x))$ et de $f_2(x\alpha(x))$ ne peut différer que par les termes d'ordre total $\geq t$. On obtient un polynôme $\sum_{i=0}^{n-1} \beta'_i x^i$ tel que $\beta'_i \pi_1^i \equiv \alpha'_i \pi_1^i \pmod{\mathfrak{P}^t}$ en remplaçant dans tous les termes $u_i x^i$ de $f_1(x\alpha(x))$ d'ordre total $< t$ et tels que $i > n$, x^i par $x^{i-n} \sum_{j=0}^{t-i+n} \Gamma'_j X_j$, en faisant la même chose avec des termes du polynôme obtenu etc. Comme $\sum_{j=0}^{t-1} \Gamma'_j X_j = \sum_{j=0}^{t-1} \Gamma''_j X_j$, le résultat de l'opération analogue sur $f_2(\alpha(x))$ ne peut différer du résultat rélatif à $f_1(x)$

que par des termes de l'ordre total $\geq t$; et enfin, puisque $\mathrm{Min}\,(\omega(\beta'_i)+i) = \mathrm{Min}\,(\omega(\alpha'_i)+i) = t(\pi_1, \mathrm{A}) \geq t$, aussi $t(\pi_2, \mathrm{A}) = \mathrm{Min}\,(\omega(\beta''_i+i)) \geq t$ ce qui prouve l'affirmation.

Ce raisonnement montre d'ailleurs que, si, de plus, $\Gamma'_t = \Gamma''_t$, la substitution formelle et la réduction indiquées donnent pour $f_1(x)$ et $f_2(x)$ des résultats qui ne diffèrent que par des termes d'ordre total $\geq t+1$, c'est-à-dire dans ce cas

$$\frac{f_1(\pi_1)}{\pi^t} \equiv \frac{f_2(\pi_2)}{\pi_2^t} \pmod{\mathfrak{P}^{t+1}}.$$

Donc, si pour un π satisfaisant à $f(x) = 0$ avec des Γ_i, $i < t$, donnés, $t(\pi\,;\mathrm{A}) \geq t$, ceci a lieu pour tous les π ayant cette propriété et $\Phi_{t,\pi,\mathrm{A}}(\Gamma_t)$ est le même pour tous les π ayant un Γ_t donné, c'est-à-dire on peut écrire

$$\Phi_{t,\pi,\mathrm{A}}(\Gamma) = \Psi_{\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}\,; t, \mathrm{A}}(\Gamma).$$

Des raisonnements précédents il suit que si $t(\pi\,;\mathrm{A}_2) \geq t$, on a $t(\pi\,;\mathrm{A}_1 * \mathrm{A}_2) \geq t$ si et seulement si $t(\pi\,;\mathrm{A}_1) \geq t$. En effet, posons $\pi' = \mathrm{A}_2(\pi)$, $\pi'' = \mathrm{A}_1(\pi')$. Alors, si $t(\pi\,;\mathrm{A}_2) \geq t$, π' satisfait à l'équation ayant les mêmes Γ_i, $i < t$, que celle à laquelle satisfait π ; donc, si $t(\pi\,;\mathrm{A}_1) \geq t$, aussi $t(\pi', \mathrm{A}_1) \geq t$, d'où $t(\pi\,;\mathrm{A}_1 * \mathrm{A}_2) \geq \mathrm{Min}\,[t(\pi'\,;\mathrm{A}_1),\ t(\pi\,;\mathrm{A}_2)] \geq t$. Maintenant, si $t(\pi\,;\mathrm{A}_2) \geq t$, mais $t(\pi\,;\mathrm{A}_1) < t$, les équations auxquelles satisfont π et π' ont les mêmes Γ_i, $i \leq t(\pi\,;\mathrm{A}_1)$, donc $t(\pi'\,;\mathrm{A}_1) = t(\pi\,;\mathrm{A}_1) < t$, donc $t(\pi'\,;\mathrm{A}_1) < t \leq t(\pi\,;\mathrm{A}_2)$, et $t(\pi\,;\mathrm{A}_1 * \mathrm{A}_2) = t(\pi'\,;\mathrm{A}_1) < t$.

Il s'agit d'étudier la fonction Ψ. Posons

$$\Psi_{\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}\,; t, \mathrm{A}}(0) = u_t(\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}\,; \mathrm{A})$$

posons de plus

$$\alpha(x) \equiv \gamma \pmod{x} \quad (\text{où } t(\pi\,;\alpha(x)) \geq t),$$

et

$$\xi = \gamma^{-t}.$$

Il est a remarquer que t ne peut être plus grand que n que si $\gamma^n = 1$. En effet, on a

$$\Gamma'_n \equiv (-1)^n \frac{\mathrm{N}_{\mathrm{K}/k}(\pi')}{\pi} \equiv (-1)^n \frac{\mathrm{N}_{\mathrm{K}/k}(\gamma)}{\pi}\frac{\mathrm{N}_{\mathrm{K}/k}(\pi)}{\pi} \equiv \gamma^n (-1)^n \frac{\mathrm{N}_{\mathrm{K}/k}(\pi)}{\pi} \equiv$$

$$\equiv \gamma^n . \Gamma_n \pmod{\mathfrak{P}}$$

et si $\gamma^n \neq 1$, on a $\Gamma'_n \neq \Gamma_n$. Donc, quelque soit $t > 0$, on a

$$\xi = \gamma^{-t} = \gamma^{-\tau}.$$

Supposons d'abord $t = n$; alors le raisonnement précédent montre que

$$\Psi_{n,\mathrm{A}}(\Gamma) = \xi\Gamma, \quad \text{et, en particulier} \quad u_n(\mathrm{A}) = 0.$$

Supposons maintenant $t > n$. Posons $f_0(x) = x^n + \sum_{i=n}^{t-1} \Gamma_i x_{i0}$. $f(x\alpha(x))$ se diffère de $f_0(x\alpha(x)) + \Gamma_t \overline{\pi}^{a_t} (x\alpha(x))^\tau$ par des termes dont les ordres totaux sont $> t$. De même $f(x)$ diffère de $f_0(x) + \Gamma_t \overline{\pi}^{a_t} x^\tau$ par des termes d'ordre total $> t$. Donc $f(x\alpha(x)) - f(x)$ diffère de $f_0(x\alpha(x)) - f_0(x) + \Gamma_t \overline{\pi}^{a_t} x^\tau \alpha(x)^\tau (1-\gamma^{-\tau})$ par les seuls termes d'ordre total $> t$. Or, puisque $\gamma^n = 1$, $f(x\alpha(x)) - f(x)$ et $f_0(x\alpha(x)) - f_0(x) + \Gamma_t \overline{\pi}^{a_t} (x\alpha(x))^\tau (1-\gamma^{-\tau})$ ont tous leurs termes d'ordre total $> n$. Donc, si l'on fait la réduction indiquée et qu'on mette π au lieu de x, les résultats obtenus seront congrus (mod $\mathfrak{P}^{t+1}$). Or pour $f(x\alpha(x)) - f(x)$ réduite (mod $f(x)$) un obtient un nombre $\equiv (\Gamma_t - \Psi_{\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}\,; t, \mathrm{A}}(\Gamma_t))\, \overline{\pi}^{a_t} (\pi\alpha(\pi))^\tau \pmod{\mathfrak{P}^{t+1}}$, et pour $f_0(x\alpha(x)) - f_0(x) + \Gamma_t \overline{\pi}^{a_t} . (x\alpha(x))^\tau (1-\gamma^{-\tau})$ on obtient un nombre $\equiv [-u_t(\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}\,; \mathrm{A}) + \Gamma_t (1-\xi)]\, \overline{\pi}^{a_t} (\pi\alpha(\pi))^\tau \pmod{\mathfrak{P}^{t+1}}$. Donc

$$\Psi_{\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}\,; t, \mathrm{A}}(\Gamma) \equiv u_t(\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}\,; \mathrm{A}) + \xi\Gamma.$$

Regardons deux cas :

1°. $\xi = 1$, c'est-à-dire $\gamma^\tau = 1$; alors

$$\Psi_{\mathrm{A}}(\Gamma) \equiv u(\mathrm{A}) + \Gamma \pmod{\mathfrak{P}}.$$

2°. $\xi \neq 1$; alors il existe un Γ, qui sera désigné par $\mathrm{P}_{\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}\,; t}(\mathrm{A})$ et appelé *pôle* de A pour $\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}$, tel que

$$\Psi_{\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}\,; t, \mathrm{A}}(\mathrm{P}_{\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}\,; t}(\mathrm{A})) = \mathrm{P}_{\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}\,; t}(\mathrm{A}).$$

En effet il suffit de poser

$$\mathrm{P}_{\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}\,; t}(\mathrm{A}) \equiv \frac{u_t(\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}\,; \mathrm{A})}{1-\xi} \pmod{\mathfrak{P}}.$$

Alors, si

$$y_t(\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}\,; \mathrm{A}\,; \Gamma) \equiv \Gamma - \mathrm{P}_{\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}\,; t}(\mathrm{A})$$

et si

$$\mathrm{F}_{\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}\,; t, \mathrm{A}}(y_t(\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}\,; \mathrm{A}\,; \Gamma)) =$$

$$= y_t(\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}\,; \mathrm{A}\,; \Psi_{\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}\,; t, \mathrm{A}}(\Gamma)),$$

on a

$$\mathrm{F}_{\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}\,; t, \mathrm{A}}(y) \equiv \xi y.$$

Soit $\overline{\Gamma}$ la classe mod $\mathfrak{P}$ à laquelle appartient Γ. Les transformations $\overline{\Gamma} \to \Psi_{t,A}(\overline{\Gamma})$ et $\overline{y} \to F_{t,A}(\overline{y})$ produisent des permutations de Ω_{f_0}. Ainsi à tous les A tels que $t(\pi, A) \geq t$ correspond un ensemble des permutations $T_{\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}}(A) = \{\overline{\Gamma} \to \Psi_{\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}; t; A}(\overline{\Gamma})\}$ de Ω_{f_0} $\left(\text{où } \pi^n + \sum_{i=n}^{+\infty} \Gamma_i X_i(\pi) = 0\right)$. Comme

$$\Psi_{\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}; t, A_1 * A_2}(\overline{\Gamma}) = \Psi_{\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}; t, A_1}(\Psi_{\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}; t, A_2}(\overline{\Gamma})),$$

on a

$$T(A_1 * A_2) = T(A_1)\,T(A_2).$$

Donc ces permutations forment un certain groupe, soit $G(\pi, t)$. Il s'agit de décomposer Ω_{f_0} en systèmes d'intransitivité de $G(\pi, t)$ ($t = n, n+1, \ldots$). Considérons tout d'abord le sous-groupe $G_0(\pi, t)$ de $G(\pi, t)$ formé par les $T(A)$ des A dont $\xi = \gamma^{-\tau}$ est 1. C'est un groupe des translations $u_t(A) = \{\overline{\Gamma} \to u_t(A) + \overline{\Gamma}\}$ de Ω_{f_0} et les $u_t(A)$ correspondants forment un module M_t. Les systèmes d'intransitivité de $G_0(\pi, t)$ sont des classes (mod M_t) dans Ω_{f_0}. Il est à remarquer que si l'on se bornait aux A tels que $\gamma = 1$, les $T(A)$ correspondants formeraient encore le même groupe $G_0(\pi, t)$. En effet, si $\xi = 1$, et si τ_1 est le plus grand facteur de τ premier à p, $A^{\tau_1} = \underbrace{A * A * \ldots * A}_{\tau_1 \text{ fois}}$ a $\gamma = 1$ et $T(A^{\tau_1}) = T(A)^{\tau_1}$; donc, puisque l'ordre de $T(A)$ est p, on a, s $\tau_1 \tau' \equiv 1 \pmod p$, $T(A) = (T(A^{\tau_1}))^{\tau'}$. et l'affirmation est prouvée. Soit que $A = (\alpha(x))$ est tel que $t(\pi ; A) \geq t$ et soit $\alpha(x) \equiv \gamma_0 \pmod x$. Posons $\xi(A) = \gamma_0^{-\tau}$. On a $\xi(A_1 * A_2) = \xi(A_1).\xi(A_2)$. Donc les $\xi(A)$ forment un sous-groupe Σ_t du groupe multiplicatif des racines $\frac{h}{(h, \tau)}$ièmes de l'unité. Soit ξ_0 un élément qui engendre Σ_t et soit h_t l'ordre de Σ_t. Soit A_0 une transformation telle que $t(\pi ; A_0) \geq t$ et $\xi(A_0) = \xi_0$. Un A quelconque tel que $t(\pi ; A) \geq t$ peut se mettre sous la forme

$$A = B * A_0^q \quad , \quad \text{où} \quad \xi(A) = \xi_0^q \quad .$$

On a $\xi(B) = 1$ et, puisque $t(\pi ; A) \geq t$ et $t(\pi ; A_0^q) \geq t$, on a $t(\pi ; B) \geq t$. Inversement, si A est de cette forme et si $t(\pi ; B) \geq t$ on a $t(\pi ; A) \geq t$. Soit P_0 le pôle de A_0 et soit $u(B)$ la translation que produit B. $T(A_0)$ est la homothétie de Ω_{f_0} par rapport à P_0 dont le rapport de similitude est $\xi(A_0) = \xi_0$. Donc $T(A_0^q)$ est une homothétie de Ω_{f_0} par rapport à P_0 avec le rapport de simulitude $\xi_0^q = \xi(A)$. Et, enfin, si $q \neq 0$, $T(A) = T(B)T(A_0^q)$

est l'homothétie de Ω_{f_0} avec le rapport similitude $\xi(A)$ et avec le pôle donné par l'égalité

$$P_0 + \xi(A)(P - P_0) + u(B) = P \quad ,$$

c'est-à-dire

$$(P - P_0)(\xi(A) - 1) = -u(B) \quad ,$$

ou

$$P = P_0 - \frac{u(B)}{\xi_0^q - 1} = P_0 - \frac{u(B)}{\xi(A) - 1} \quad .$$

Montrons tout d'abord que $\xi_0 M_t = M_t$. En effet, si $t(\pi ; A) \geq t$ et si $\xi(A) = 1$, on a $t(\pi ; A_0 * A * A_0^{h_t - 1}) \geq t$ et $\xi(A_0 * A * A_0^{h_t - 1}) = \xi(A_0).\xi(A).\xi(A_0)^{h_t - 1} = \xi_0^{h_t} = 1$. Donc $T(A_0 * A * A_0^{h_t - 1})$ est une translation $u \in M_t$. Or, prenons par exemple $\overline{\Gamma} = P_0$; $T(A_0^{h_t - 1})$ conserve P_0, $T(A)$ transforme P_0 en $P_0 + u_t(A)$, et $T(A_0)$ transforme $P_0 + u_t(A)$ en $P_0 + \xi_0 u_t(A)$. Donc $T(A_0 * A * A_0^{h_t - 1})$ transforme P_0 en $P_0 + \xi_0 u_t(A)$, donc $\xi_0 u_t(A) = u \in M_t$, et comme A est une transformation arbitraire ayant les propriétés indiquées, donc $u_t(A)$ est un élément arbitraire de M_t, on a $\xi_0 M_t = M_t$. Il en résulte que M_t est un module par rapport au corps $\Omega_1(\xi_0)$ engendré par ξ_0. On en tire deux conséquences:

1°. $\frac{u(B)}{\xi(A) - 1} \equiv 0 \pmod{M_t}$, car $u(B) \equiv 0 \pmod{M_t}$ et $\frac{1}{\xi(A) - 1}$ (quand $\xi(A) \neq 1$) est un élément du $\Omega_1(\xi_0)$. D'autre part, quand B parcourt ensemble de toutes transformations dont $t(\pi, B) \geq t$ et $\xi(B) = 1$, $u(B)$ parcourt M_t et $\frac{u(B)}{\xi(A) - 1}$ parcourt $\frac{1}{\xi(A) - 1} M_t = M_t$. Donc P parcourt la classe (Mod M_t) contenant P_0. Cette classe est indépendante de A, donc

L'ensemble des pôles (pour $\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}$) *des tous les* A *tels que* $t(\pi, A) \geq t$ *est une classe* (*mod* M_t) qui sera dite la *classe polaire* $\mathfrak{P}_{\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}}$ *pour* $\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{t-1}$.

2°. Si $y \not\equiv 0 \pmod{M_t}$. la congruence $\xi_0^{q_1} y \equiv \xi_0^{q_2} y \pmod{M_t}$ n'a lieu que si $\xi_0^{q_1} = \xi_0^{q_2}$, c'est-à-dire $q_1 \equiv q_2 \pmod{h_t}$. En effet, la congruence écrite signifie $(\xi_0^{q_1} - \xi_0^{q_2}) y \equiv 0 \pmod{M_t}$. Si $\xi_0^{q_1} - \xi_0^{q_2} \neq 0$, il existe un élément $\varkappa(\xi_0)$ de $\Omega_1(\xi_0)$ tel que $\varkappa(\xi_0)(\xi_0^{q_1} - \xi_0^{q_2}) = 1$. Il en résulte que $y = \varkappa(\xi_0).(\xi_0^{q_1} - \xi_0^{q_2}) y \equiv 0 \pmod{M_t}$, contre l'hypothèse.

Il est maintenant facile de déterminer les systèmes d'intransitivité de $G(\pi, t)$. En effet, soit d'abord que $\overline{\Gamma}$ est dans la classe polaire $\mathfrak{P}$. Aucun $T(A)$ ne peut transformer $\overline{\Gamma}$ dans un élément qui est en dehors de $\mathfrak{P}$. En effet, si $\xi = \xi(A) \neq 1$, soit P le pôle de A. On a $\overline{\Gamma} - P \equiv 0$

$(\mathrm{mod}\ \mathrm{M}_t)$, donc $\mathrm{T(A)}.\overline{\Gamma} - \mathrm{P} = \mathrm{T(A)}(\overline{\Gamma} - \mathrm{P}) = \xi(\overline{\Gamma} - \mathrm{P}) \equiv 0 \ (\mathrm{mod}\ \xi\mathrm{M}_t = \mathrm{M}_t)$; et si $\xi(\mathrm{A}) = 1$, on a encore $\mathrm{T(A)}.\overline{\Gamma} \equiv \overline{\Gamma} \ (\mathrm{mod}\ \mathrm{M}_t)$. D'autre part, quand T(A) parcourt $\mathrm{G}_0(\pi, t)$, $\mathrm{T(A)}.\overline{\Gamma}$ parcourt $\overline{\Gamma} + \mathrm{M}_t = \mathfrak{P}$.

Soit, maintenant, un $\overline{\Gamma}$ en dehors de $\mathfrak{P}$. Soit Y la classe $\overline{\Gamma} - \mathfrak{P}$ $(\mathrm{mod}\ \mathrm{M}_t)$. Soit A une transformation telle que $t(\pi\,;\mathrm{A}) \geq t$ et $\xi(\mathrm{A}) \neq 1$, et soit P le pôle de A. Alors $y = \overline{\Gamma} - \mathrm{P}$ fait partie de Y ; le transformé de y par T(A) est $\xi(\mathrm{A})y$. Il fait partie de $\xi(\mathrm{A})\mathrm{Y}$, et $\mathrm{T(A)}.\overline{\Gamma}$ fait partie de $\mathfrak{P} + \xi(\mathrm{A})(\overline{\Gamma} - \mathfrak{P})$. Donc, le système d'intransitivé d'élément $\overline{\Gamma}$ est contenu dans l'ensemble des classes $\mathfrak{P} + \bigcup_{q=0,1,\ldots,h_t-1} \xi_0^q \mathrm{Y}$. Il coïncide avec cette réunion, car il a sûrement des éléments communs avec chacun des systèmes d'intransitivité de $\mathfrak{S}_0(\pi, t)$, c'est-à-dire des classes $(\mathrm{mod}\ \mathrm{M}_t)$, qui en font partie.

Il est à remarquer que les h_t classes $\mathfrak{P} + \xi_0^q \mathrm{Y}$ sont distinctes. En effet, si l'on avait $\mathfrak{P} + \xi_0^{q_1}\mathrm{Y} = \mathfrak{P} + \xi_0^{q_2}\mathrm{Y}$, on aurait pour un $\mathrm{P} \in \mathfrak{P}$ et un $y \in \mathrm{Y}$

$$\mathrm{P} + \xi_0^{q_1} y \equiv \mathrm{P} + \xi_0^{q_2} y \ (\mathrm{mod}\ \mathrm{M}_t),$$

c'est-à-dire

$$\xi_0^{q_1} y \equiv \xi_0^{q_2} y \ (\mathrm{mod}\ \mathrm{M}_t).$$

Puisque $y \not\equiv 0 \ (\mathrm{mod}\ \mathrm{M}_t)$, on doit avoir $q_1 \equiv q_2 \ (\mathrm{mod}\ h_t)$, ce qui exige, étant donné que $0 \leq q < h_t$ et que $0 \leq q_2 < h_t$,

$$q_1 = q_2 .$$

Soit m_t le nombre d'éléments de M_t. Soit $\nu_t + 1$ le nombre des systèmes d'intransitivité de $\mathrm{G}(\pi, t)$. Ce qui précède montre qu'il y en a un $(\mathfrak{P})$ qui a m_t éléments, et que les ν_t autres ont chacun $m_t h_t$ éléments. Donc $\nu_t = \dfrac{p^{f_0} - m_t}{h_t m_t} = \dfrac{1}{h_t}\left(\dfrac{p^{f_0}}{m_t} - 1\right)$. Choisissons dans chacun des ces systèmes un élément Γ, que nous dirons élément *réduit*, de la manière suivante : choisisons une fois pour toutes une racine $p^{f_0} - 1^{\text{ième}}$ primitive de l'unité ρ. Distinguons les cas suivants :

1°. $h_t \neq 1$. A) $\mathfrak{P} \neq \mathrm{M}_t$. Alors on prendra comme élément réduit de $\mathfrak{P}$ l'élément P de $\mathfrak{P}$ dont $\mathrm{ind}_\rho \mathrm{P}$ est minimum. C étant le système d'intransitivité de $\mathrm{G}(\pi, t)$, on prendra comme élément réduit de C l'élément $\mathrm{P} + y$ de C tel que $\mathrm{ind}_\rho y$ est minimum. B) $\mathfrak{P} = \mathrm{M}_t$. Alors on prendra comme élément réduit de $\mathfrak{P}$ l'élément 0, et comme élément réduit d'un système d'intransitivité $\mathrm{C} \neq \mathrm{P} = \mathrm{M}_t$ l'élément c de C dont $\mathrm{ind}_\rho c$ est minimum.

2°. $h_t = 1$. On prendra comme élément reduit de M_t l'élément 0, et comme élément réduit d'une classe C $(\mathrm{mod}\ \mathrm{M}_t)$ l'élément c *de* C dont $\mathrm{ind}_\rho c$ est minimum.

On dira que l'équation d'Eisenstein

$$f(x) = x^n + \sum_{t=n}^{+\infty} \Gamma_t \mathrm{X}_t = 0$$

est *réduite*, si pour tout $t = n, n+1, \ldots, +\infty$, Γ_t est l'élément réduit du système d'imprimitivité de $\mathrm{G}(\pi, t)$ $(f(\pi) = 0)$ qui le contient. Le but principal de ce § est de prouver que parmi les équivalentes d'une équation d'Eisenstein il y a une et une seule qui est réduite, et de déterminer aussi loin que possible la forme de cette équation, c. a. d. les M et, eventuellement, les $\mathfrak{P}$.

Il se trouve qu'il est possible de déterminer les M_t, tous les t tels que $h_t \neq 1$, et pour ces derniers t le système $\mathrm{C}_t - \mathfrak{P}_t$, où C_t est le système d'intransitivité contenant Γ_t du $\mathrm{G}(\pi, t)$, et $\mathfrak{P}_t$ est la classe polaire. Faisons cette détermination :

1°. Faisons correspondre à chaque $\mathrm{A} = (\alpha(x))$ un nombre $\omega_\pi(\mathrm{A})$ appellé son *degré réduit* qui est défini par la formule

$$\omega_\pi(\mathrm{A}) = \operatorname*{Max}_{\sigma \in \mathrm{G}_{\mathrm{K}/k}} \left[\omega\left(\alpha(\pi)\right) - \frac{\sigma\pi}{\pi} \right].$$

$\omega_\pi(\mathrm{A})$ n'est égal à $+\infty$ que s'il existe un $\sigma \in \mathrm{G}_{\mathrm{K}/k}$ tel que $\sigma\pi = \pi\alpha(\pi) = \mathrm{A}(\pi)$, c'est-à-dire si la transformation $\pi \to \mathrm{A}(\pi)$ est un automorphisme de K/k. k_g désignant le moindre surcorps de k par rapport auquel K est galoisien, l'égalité $\omega_\pi(\mathrm{A}) = +\infty$ équivant à ce que $\pi \to \mathrm{A}(\pi)$ soit un élément de $\mathrm{G}_{\mathrm{K}/k_g}$. Il y a donc $(\mathrm{K} : k_g)$ des A tels que $\omega_\pi(\mathrm{A}) = +\infty$.

2°. Faisons correspondre à tout A tel que $\omega_\pi(\mathrm{A}) > 0$ un élément non uul $\gamma_\pi(\mathrm{A})$ de Ω_{f_0} quand $\omega_\pi(\mathrm{A})$ n'est pas parmi les nombres de ramification positifs de K/k, ou une classe $\gamma_\pi(\mathrm{A}) \ (\mathrm{mod}\ \mathrm{M}_q^{(\sqrt[\delta q]{\pi})}(\mathrm{K}/k))$, inégale à $\mathrm{M}_q^{(\sqrt[\delta q]{\pi})}(\mathrm{K}/k))$, quand $\omega_\pi(\mathrm{A}) = v_q(\mathrm{K}/k)$,

$$\gamma_\pi(\mathrm{A}) \equiv \frac{\alpha'\pi) - \dfrac{\sigma\pi}{\pi}}{\sigma\pi^{\omega_\pi(\mathrm{A})}} \cdot \frac{\pi}{\sigma\pi} \ (\mathrm{mod}\ \mathfrak{P}^*)$$

pour les $\sigma \in \mathrm{G}_{\mathrm{K}/k}$ tels que $\omega\left(\alpha(\pi) - \dfrac{\sigma\pi}{\pi}\right) = \omega_\pi(\mathrm{A})$.

Il est facile de voir qu'il n'y a qu'un seul élément $\gamma_\pi(\mathrm{A})$ de Ω_{f_0} satisfaisant à cette condition quand $\omega_\pi(\mathrm{A})$ n'est pas parmi les $v_q(\mathrm{K}/k)$, et que si $\omega_\pi(\mathrm{K}/k) = v_q(\mathrm{K}/k)$, les $\gamma_\pi(\mathrm{A})$ définis par cette condition forment une classe $(\mathrm{mod}\ \mathrm{M}_q(\mathrm{K}/k))$. En effet, soit σ' un autre élément de

$G_{K/k}$ tel que $\omega\left(\alpha(\pi)-\frac{\sigma'\pi}{\pi}\right)=\omega_\pi(A)$. On a $\sigma'\pi=\sigma_1\sigma\pi$, où $\sigma_1\in G_{\sigma K/k}$. Or $\sigma K/k$ est défini par la même équation d'Eisenstein que K/k. Donc $\sigma K/k$ a les mêmes v_q et les mêmes M_q que K/k. Donc $\sigma'\pi-\sigma\pi$ est d'un ordre $v_q(K/k)\geq\omega_\pi(A)$. Si $\omega_\pi(A)$ n'est pas parmi les $v_q(K/k)$, on a $\sigma'\pi-\sigma\pi\equiv 0 \pmod{\mathfrak{P}^{1+\omega_\pi(A)}\mathfrak{P}^*}$ et $\frac{\alpha(\pi)-\frac{\sigma\pi}{\pi}}{\sigma\pi^{\omega_\pi(A)}}\equiv\frac{\alpha(\pi)-\frac{\sigma'\pi}{\pi}}{\sigma'\pi^{\omega_\pi(A)}} \pmod{\mathfrak{P}^*}$. Si $\omega_\pi(A)=v_q(K/k)$, on a $\frac{\sigma'\pi-\sigma\pi}{\pi^{1+\omega_\pi(A)}}\equiv\mu\in M_q(K/k) \pmod{\mathfrak{P}^*}$; d'autre part $\sigma'\pi-\sigma\pi\equiv 0 \pmod{\mathfrak{P}^{\omega_\pi(A)}\mathfrak{P}}$, dès que $\sigma'\pi$ a la forme $\sigma_1\sigma\pi$ avec $\sigma_1\in V^{(q)}_{\sigma K/k}$; Donc μ parcourt $M_q(K/k)$, et les $\gamma_\pi(A)$ parcourent la classe mod $M_q(K/k)$ contenant un des $\gamma_\pi(A)$, ce qui prouve l'affirmation.

On définira de plus pour chaque t réel positif et pour tous les A tels que $\omega_\pi(A)\geq t$ un élément ou un ensemble d'éléments $\gamma^{(t)}_\pi(A)$ par la formule

$$\gamma^{(t)}_\pi(A)=0 \text{ resp. } M_q(K/k) \text{ si } t<\omega_\pi(A)$$
$$\gamma^{(t)}_\pi(A)=\gamma_\pi(A) \text{ resp. } \overline{\gamma_\pi}(A) \text{ si } t=\omega_\pi(A).$$

Considérons la réunion $R^{(\pi)}_t$ des $\gamma^{(t)}_\pi(A)$ des tous les A tels que $\omega(A)>0$ et $\omega_\pi(A)\geq t$ $(t>0)$. Il n'y a qu'un nombre fini des t non entiers tels que $R^{(\pi)}_t\neq\{0\}$, ce qui se voit pas le fait que les $\sigma\pi-\sigma'\pi$ ont pour ordres les nombres $1+v_q(K/k)$. Si t est entier, $R^{(\pi)}_t\supseteq\Omega_{f_0}$. Je dis que dans ce cas $R^{(\pi)}_t$ est un surmodule de Ω_{f_0}. En effet, soit

$$\left.\begin{aligned}\sigma_1\pi&\equiv\pi\alpha_1(\pi)-\gamma_1(\sigma_1\pi)^{1+t}\\ \sigma_2\pi&\equiv\pi\alpha_2(\pi)-\gamma_2(\sigma_2\pi)^{1+t}\end{aligned}\right\} \pmod{\mathfrak{P}^{1+t}\mathfrak{P}^*}.$$

On a

$$\sigma_1\pi\equiv\sigma_2\pi\equiv\pi \pmod{\mathfrak{P}\mathfrak{P}^*}.$$

Donc

$$\sigma_1\pi\equiv\pi\alpha_1(\pi)-\gamma_1\pi^{1+t}$$
$$\sigma_2\pi\equiv\pi\alpha_2(\pi)-\gamma_2\pi^{1+t}.$$

Soient $\sigma_1^*\in\mathrm{gen}_{K^*}\sigma_1$, $\sigma_2^*\in\mathrm{gen}_{K^*}\sigma_2$, et soit $\sigma=\mathrm{corr}_K\sigma_1^*\sigma_2^*$. On peut prendre $\sigma_1^*\in V^*$.

On a alors $\sigma\pi=\sigma_1^*\sigma_2\pi\equiv\sigma_1^*\pi.\alpha_2(\sigma_1^*\pi)-\gamma_2(\sigma_1^*\pi)^{1+t}\equiv$

$$\equiv\sigma_1\pi.\alpha_2(\sigma_1\pi)-\gamma_2\pi^{1+t}\equiv[\pi\alpha_1(\pi)-\gamma_1\pi^{1+t}].$$
$$.[\alpha_2(\pi\alpha_1(\pi))-\alpha'_2(\pi\alpha_2(\pi))\gamma_1\pi^{1+t}+\ldots]-\gamma_2\pi^{1+t}\equiv$$
$$\equiv\pi\alpha_1(\pi).\alpha_2(\pi\alpha_1(\pi))-(\gamma_1+\gamma_2)\pi^{1+t} \pmod{\mathfrak{P}^{1+t}\mathfrak{P}^*}.$$

c'est-à-dire

$$A_1(A_2(\pi))-\sigma\pi\equiv(\gamma_1+\gamma_2)\sigma\pi^{1+t} \pmod{\mathfrak{P}^{1+t}\mathfrak{P}^*},$$

c'est-à-dire

$$\gamma^{(t)}_\pi(A_1*A_2)=\gamma^{(t)}_\pi(A_1)+\gamma^{(t)}_\pi(A_2). \qquad \text{C. q. f. d.}$$

D'ailleurs, de cette dernière égalité résulte que

1°. $R^{(\pi)}_t$ est module quelque soit t.

2°. la réunion des $\gamma^{(t)}_\pi(A)$ des A tels que $\omega_\pi(A)\geq t$ et $\omega(A)\geq t_1$, $t_1\leq t$, soit $R^{(\pi)}_{t_1,t}$ est aussi un module. D'ailleurs si t est un entier, non égal à un $v_q(K/k)$, on a $R^{(\pi)}_{t,t}=\Omega_{f_0}$; si $t=v_q(K/k)$ est entier, on a $R^{(\pi)}_{t,t}=\Omega_{f_0}+M_q(K/k)$.

Soit r_t le nombre d'éléments de $R^{(\pi)}_t$, et soit $r_{t_1,t}$ celui de $R^{(\pi)}_{t_1,t}$. Désignons par N le produit de tous les $\frac{r_t}{r_{t,t}}$ (t parcourant une suite des nombres positifs croissants comprenant tous les t tels que $r_t\neq 1$). Calculons ce nombre N.

On peut faire correspondre à chaque $\sigma\in G_{K/k}$ un nombre $t(\sigma)$ [15] qui est Max. $\left(\omega\left(\frac{\sigma\pi-A(\pi)}{\pi}\right)\right)$, A parcourant l'ensemble des toutes les transformations $A=(\alpha(x))=\left(\sum_{i=0}^{+\infty}\gamma_i x^i\right)$, les γ_i étant des racines $p^{f_0}-1^{\text{èmes}}$ de l'unité ou des zéros, dont $\gamma_0\neq 0$. On a $t(\sigma)=+\infty$ si, et seulement si $\sigma\in G_{K/k_{f_0}}$. Ce $t(\sigma)$ peut être égal à $\omega\left(\frac{\sigma\pi-A(\pi)}{\pi}\right)$ pour un $\alpha(x)\equiv 1 \pmod{x}$ si, et seulement si $\sigma\in V_{K/k}$. Tous les σ ayant un $t(\sigma)\geq$ forment un *hypergroupe*. En effet, si

$$\sigma_1\pi-\pi\alpha_1(\pi)\equiv 0 \pmod{\mathfrak{P}^{1+t}}$$
$$\sigma_2\pi-\pi\alpha_2(\pi)\equiv 0 \pmod{\mathfrak{P}^{1+t}}$$

et si $\sigma_1^*\in\mathrm{gen}_{K^*}\sigma_1$, $\sigma_2^*\in\mathrm{gen}_{K^*}\sigma_2$, $\sigma=\mathrm{corr}_K\sigma_1^*\sigma_2^*$, on a

$$\sigma\pi=\sigma_1^*(\sigma_2\pi)\equiv\sigma_1^*(\pi\alpha_2(\pi))\equiv\sigma_1^*\pi.\alpha_2(\sigma_1^*\pi)\equiv\pi\alpha_1(\pi).\alpha_2(\pi\alpha_1(\pi)) \pmod{\mathfrak{P}^{1+t}}$$

car $\sigma_1^*\mathfrak{P}=\mathfrak{P}$.

Soit $t_0, t_1, \ldots, t_\eta, t_\eta, t_{\eta+1}=+\infty$ les valeurs que peut prendre $t(\sigma)$ [16], $\sigma\in V_{K/k}$. Soit $\alpha(x)\equiv 1 \pmod{x}$. Soit que $\sigma\in V_{K/k}$ est tel que $\omega\left(\alpha(\pi)-\frac{\sigma\pi}{\pi}\right)=\omega_\pi(A)$. Si $\omega_\pi(A)<t(\sigma)$, il existe un $\alpha_1(\pi)$ tel que $\frac{\sigma\pi}{\pi}\equiv\alpha_1(\pi) \pmod{\mathfrak{P}^{\omega_\pi(A)}\mathfrak{P}^*}$.

---

[15] J'appelle ce nombre *l'indice d'irrégularité de première espèce de* σ.

[16] J'appelle t_q $(q=0, 1, \ldots, \eta, \eta+1)$ le *q-ième nombre d'irregularité de première espèce de* K/k.

Donc $\gamma_\pi(A)\equiv\dfrac{\alpha_1(\pi)-\alpha'(\pi)}{(\pi\alpha_1(\pi))^{\omega_\pi(A)}}\dfrac{1}{\alpha_1(\pi)}\in\Omega_{f_0}$ ou $\subset\Omega_{f_0}+M_q(K/k)$ (mod $\mathfrak{P}^*$) suivant que $\omega_\pi(A)$ n'est pas ou est un des $v_q(K/k)$. Donc, si t n'est pas parmi les nombres $t_0, t_1, \ldots \ldots, t_\eta$, on a

$$R_t = R_{t,t}$$

c'est-à-dire

$$\frac{r_t}{r_{t,t}} = 1.$$

Supposons maintenant $\omega_\pi(A) = t(\sigma)$; deux cas peuvent se présenter:

1. $t(\sigma)$ n'est pas parmi les nombres $v_q(K/k)$ $(q>0)$. Alors, $\gamma_\pi(A)$ est bien défini. Soit $t(\sigma)=t_q$, et soit $H^{(q)}_{K/k}$ l'hypergroupe des tous les $\sigma\in V_{K/k}$ tels que $t(\sigma)\geq t_q$ [17]. Si $\sigma_1\in H^{(q)}$, $\sigma_2\in H^{(q)}$, si $\sigma_1^*\in \mathrm{gen}_{K^*}\sigma_1\cap V_{K^*/k}$, et si $\sigma=\mathrm{corr}_K\sigma_1^*\sigma_2^*$, on a

$$\sigma\pi\equiv\sigma_1^*(\sigma_2\pi)\equiv\sigma_1^*(\alpha_2(\pi)+\gamma_\pi(A_2)(\sigma_2\pi)^{1+t_q})\equiv\alpha_2(\alpha_1(\pi))+\gamma_{\pi\backslash A_1}(\sigma_1\pi)^{1+t_q}+\gamma_\pi(A_2)$$
$$.(\sigma_2\pi)^{1+t_q}\equiv\alpha_2(\alpha_1(\pi))+(\gamma_\pi(A_1)+\gamma_\pi(A_2))(\sigma\pi)^{1+t_q}\ (\mathrm{mod}\ \mathfrak{P}^{1+t_q}\mathfrak{P}^*)$$

car $(\sigma_1\pi)^{1+t_q}\equiv(\sigma_2\pi)^{1+t_q}\equiv(\sigma\pi)^{1+t_q}\equiv\pi^{1+t_q}$ (mod $\mathfrak{P}^{1+t_q}\mathfrak{P}^*$).

Donc, on a

$$\gamma_\pi(A_1*A_2)=\gamma_\pi(A_1)$$

si, et seulement si $A_2(\pi)$ est congrue (mod $\mathfrak{P}^{1+t_q}\mathfrak{P}^*$) à un $\sigma_2\pi$ tel que $\sigma_2\in H^{(q+1)}$.

D'autre part, si t_q n'est pas entier, tous les $\alpha(x)$ tels que $\alpha(\pi)-\dfrac{\sigma\pi}{\pi}$ soit d'ordre $\geq t_q$ (quand σ est fixe) sont congrûs (mod x^{t_q}), et leur $\gamma_\pi(A)$ est le même. On a vu que $R_{t,t}$ se réduit à $\{0\}$. Donc, dans ce cas $r_t=\begin{pmatrix}(q)\,(q+1)\\ H:\ H\end{pmatrix}$ et $r_{t,t}=1$, c'est-à-dire

$$\frac{r_t}{r_{t,t}}=\begin{pmatrix}(q)\,(q+1)\\ H:\ H\end{pmatrix}.$$

Si, au contraire, t est entier (on verra d'ailleurs, que ce cas ne peut pas se présenter), $R_{t,t}=\Omega_{f_0}$. D'autre part, pour que $\alpha(\pi)-\dfrac{\sigma\pi}{\pi}$ soit d'ordre $t(\sigma)$ (σ étant fixe), il faut et il suffit que $\alpha(\pi)\equiv\dfrac{\sigma\pi}{\pi}$ (mod $\mathfrak{P}^{t_q}$), c'est-à-dire $\alpha(x)$ est déterminé (mod x^{t_q}). Donc, puisque t_q est entier, $\gamma_\pi(A)$ parcourt une classe (mod Ω_{f_0}). On ne peut avoir $\gamma_\pi(A_1*A_2)\equiv\gamma_\pi(A_1)$ (mod Ω_{f_0}) que si $\gamma_\pi(A_2)\equiv 0$ (mod Ω_{f_0}). Mais alors, si $\gamma_\pi(A)\equiv\dfrac{A_2(\pi)-\sigma_2\pi}{(\sigma_2\pi)^{1+t_q}}$ (mod $\mathfrak{P}^*$), et si l'on pose $\alpha'_2(x)=\alpha_2(x)-\gamma x^{t_q}$, où $\gamma\in\gamma_\pi(A_2)$, on a $\omega\left(\alpha'_2(\pi)-\dfrac{\sigma_2\pi}{\pi}\right)\geq t_q+1>t_q$ c'est-à-dire $\sigma_2\in H^{(q+1)}$. Donc R_t est une réunion des $\begin{pmatrix}(q)\,(q+1)\\ H:\ H\end{pmatrix}$ classes distinctes suivant Ω_{f_0}, c'est-à-dire encore

$$\frac{r_t}{r_{t,t}}=\begin{pmatrix}(q)\,(q+1)\\ H:\ H\end{pmatrix}.$$

2. $t(\sigma)=v_q(K/k)=t_{q'}$. Les raisonnements absolument analogues montrent que si $t(\sigma)$ n'est pas entier (on verra, d'ailleurs, que dans ce cas $r_t=r_{t,t}$), on a $R_{t,t}=M_q(K/k)$, c'est-à-dire

$$r_{t,t}=\frac{n_q(K/k)}{n_{q+1}(K/k)}=\begin{pmatrix}(q) & (q+1)\\ V_{K/k}: & V_{K/k}\end{pmatrix};\ \text{on a encore}\ r_t=\begin{pmatrix}(q')\,(q'+1)\\ H:\ H\end{pmatrix}.\ \text{Donc}$$

$$\frac{r_t}{r_{t,t}}=\frac{\begin{pmatrix}(q')\ (q'+1)\\ H:\ H\end{pmatrix}}{\begin{pmatrix}(q)\ (q+1)\\ V:\ V\end{pmatrix}}.$$

Si $t(\sigma)$ est entier, on a $R_{t,t}=\Omega_{f_0}+M_q(K/k)$, et R_t est encore la réunion de $\begin{pmatrix}(q')\,(q'+1)\\ H:\ H\end{pmatrix}$ classes suivant Ω_{f_0}. Soit $r_q^{(g)}(K/k)$ le nombre d'éléments de $\Omega_{f_0}\cap M_q(K/k)$. On a $r_{t,t}=p^{f_0}\dfrac{n_q}{n_{q+1}}\dfrac{1}{r_q^{(g)}}$ et $r_t=\begin{pmatrix}(q)\,(q+1)\\ H:\ H\end{pmatrix}_{p^{f_0}}$, c'est-à-dire

$$\frac{r_t}{r_{t,t}}=r_q^{(g)}\frac{\begin{pmatrix}(q')\ (q'+1)\\ H:\ H\end{pmatrix}}{\begin{pmatrix}(q)\ (q+1)\\ V:\ V\end{pmatrix}}.$$

Il en résulte que

$$N=\prod_{q'=0}^{\eta}\begin{pmatrix}(q')(q'+1)\\ H:\ H\end{pmatrix}\prod_{q=0}^{m-1}\frac{n_{q+1}}{n_q:r_q^{(g)}}=\begin{pmatrix}(0)\ (\eta+1)\\ H:\ H\end{pmatrix}\cdot\frac{1}{n_0}\cdot\prod_{q=0}^{m-1}r_q^{(g)}$$

(où l'on pose $r_q^{(g)}=1$, si v_q n'est pas entier).

Or $H^{(0)}=V_{K/k}$ et $H^{(\eta+1)}=V_{K/k_g}$. Donc

$$N=\frac{\prod_{q=0}^{m-1}r_q^{(g)}}{n_0(K/k_g)}.$$

[17] J'appelle cet hypergroupe *l'hypergroupe d'irrégularité de première espèce d'ordre q de* K/k.

Or, $r_q^{(g)}$ est l'ordre de $M_q(K/k)\cap\Omega_{f_0}$. Le quasi-polynôme de $M_q(K/k)\cap\Omega_{f_0}$ est $\overrightarrow{\mathfrak{D}}(\lambda_q(z_1), z_1^{f_0}-1)=\lambda_q^{(g)}(z_1)$. Si $l_q^{(g)}$ est le degré (en z_1) de ce polynôme, on a $r_q^{(g)}=p^{l_q^{(g)}}$.

$M_q(K/k)$ est isomorphe, quand il est organisé par la loi de composition

$$a*b=a+[b]_{f_0,\delta_q},$$

à $G_{(K/k)_{q+1}/(K/k)_q}$. Un sous-hypergroupe M de $M_q(K/k)$ ainsi organise est groupe si, et seulement si on a pour tout élément $a\in M$

$$[a]_{f_0,\delta_q}=\{a\}.$$

Si $\delta_q\neq 1$, ceci n'est possible que si $M=\{0\}$. Si $\delta_q=1$, c'est-à-dire si v_q est entier, ceci équivaut à

$$\langle a\rangle_{f_0}=\{a\},$$

c-est-à-dire

$$a^{p^{f_0}}=a,$$

ou

$$a\in\Omega_{f_0}.$$

Ainsi, si $K_q^{(g)}$ est le moindre surcorps de K_q par rapport auquel K_{q+1} est galoisien, on a

$$r_q^{(g)}=(K_{q+1}:K_q^{(g)}).$$

La connaissance des R_t suffit pour pouvoir déterminer les M_t. Posons les définitions suivantes :

1°. Pour chaque nombre réel positif v définissons de la manière suivante une fonction $\phi(v)$ [18] :

$$\phi(v)=\phi_q+n_q v \quad \text{pour} \quad v_{q-1}\leq v\leq v_q$$

où, $\bar{s}_q$ désignant le nombre supplémentaire $\sum_{i=q}^{m-1} v_i(n_i-n_{i+1})$ de K/K_q,

$$\phi_q=n+\bar{s}_{-1}-\bar{s}_q$$

$\phi(v_q)$ est défini de deux manières : montrons qu'elles conduisent à la même valeur de $\phi(v_q)$; en effet, on a

$$\phi_q+n_q v_q=n+\sum_{i=0}^{m-1} v_i(n_i-n_{i+1})-\sum_{i=q}^{m-1} v_i(n_i-n_{i+1})+n_q v_q=$$

$$=n+\sum_{i=0}^{q-1} v_i(n_i-n_{i+1})=n+\sum_{i=0}^{q-1} n_i(v_i-v_{i-1}),$$

[18] La fonction $\phi(v)$ définie ici coïncide à facteur constant $\frac{1}{n}$ près avec la fonction $u(v)$ que M. Hasse a introduite pour l'étude des restes normiques dans les corps galoisiens et abéliens (Voir *Journ. of fac. of sciences, Tokyo*, 1934 t. 2, p. 477–498).

$$\phi_{q+1}+n_{q+1}v_q=n+\sum_{i=0}^{m-1} v_i(n-n_{i+1})-\sum_{i=q+1}^{m-1} v_i(n_i-n_{i+1})+n_{q+1}v_q=$$

$$=n+\sum_{i=0}^{q} v_i(n_i-n_{i+1})+n_{q+1}v_q=n+\sum_{i=0}^{q-1} v_i(n_i-n_{i+1})+v_q(n_q-n_{q+1})+n_{q+1}v=$$

$$=n+\sum_{i=0}^{q-1} v_i(n_i-n_{i+1})+n_q v_q=n+\sum_{i=0}^{q} n_i(v_i-v_{i+1})$$

La fonction $\phi(v)$ a les propriétés suivantes :

$\phi(v)$ est continue et croissante dans dans tout l'intervalle $(0,+\infty)$

Dans l'intervalle (v_{q-1}, v_q) on a $\phi'(v)=n_q$; en particulier, *dans l'intervalle, $(v_{n-1},+\infty)$ on a $\phi'(v)=1$* ; d'où $\lim_{v\to+\infty}\frac{\phi(v)}{v}=1$.

Si l'on pose $\Delta=\phi(v_q)$, *quand v parcourt l'ensemble des tous les entiers $0, 1, \ldots, \phi(v)$ parcourt tous les entiers divisibles par n_0 de l'intervalle $(\Delta_{-1}=n, \Delta_0)$, tous les entiers divisibles par n_1 de l'intervalle $(\Delta_0, \Delta_1), \ldots$, tous les entiers divisibles par n_q de l'intervalle $(\Delta_{q-1}, \Delta_q), \ldots$, tous les entiers divisibles par n_{m-1} de l'intervalle $(\Delta_{m-2}, \Delta_{m-1})$, tous les entiers* (car $n_m=1$) *de l'intervalle $(\Delta_{m-1}, +\infty)$.*

Il est à remarquer que

$$\Delta_{m-1}=n+\sum_{i=0}^{m-1} n_i(v_i-v_{i-1})=n-1+\sum_{i=0}^{m-1} v_i(n_i-n_{i+1})+(1+v_{m-1})=\theta+1+v_{m-1}$$

où θ est la contribution $\mathfrak{P}$ dans la différente $\delta_{K/k}$ de K/k. $\Delta_q=\phi(v_q)$ est la longeur du segment de la droite $x=n$ du plan qui est compris entre l'axe des x et le prolongement du q-ième côté du polygône de ramification R de K/k, en comptant le côté horisontal $(0, n)$ $(n-n_0, n)$ comme le $(-1)^{ième}$.

2°. Définissons de la manière suivante pour chaque nombre réel non négatif v et pour chaque élément ρ d'un champ de Galois une fonction $U_v(\rho)$:

a) $U_0(\rho)=\rho^n$.

b) $\beta_q^{n_{q+1}}$ désignant la classe à laquelle appartient (mod $\mathfrak{P}^*$) le nombre (d'ordre 0)

$$\left[\frac{f^{(n_q)}(\pi x)}{(n_q)!}\right]_{x=1}\pi^{-\phi_q},$$

pour tout v tel que $v_{q-1}<v<v_q$

$$U_v(\rho)=\beta_q^{n_{q+1}}\rho^{n_{q+1}}=z_1^{l_q+1}.\beta_q z_1^{l_q+1}(\rho),$$

où

$$r_q = p^{l_q}\ ;\ n_q = p^{j_q}\ .$$

c)

$$U_{v_q}(\rho) = z_1^{j_{q+1}}.\lambda_q(z_1)(\rho),$$

où $\lambda_q(z_1)$ est la forme du quasi-polynôme de $M_q(K/k)$ obtenue comme il a été indiqué au § précédent.

Si $v > 0$, $U_v(\rho)$ est, d'après le § 6, une fonction additive de ρ. D'ailleurs, si $v > \Delta_{m-1}$, $\dfrac{U_v(\rho)}{\rho}$ est une constante.

On a : 1. Si v n'est pas un des v_q, $U_v(\rho_1)$ n'est égal à $U_v(\rho_2)$ que si $\rho_1 = \rho_2$. 2. Si $v = v_q$, $(q \geq 0)$, $U_v(\rho_1) = U_v(\rho_2)$ si, et seulement si $\rho_1 \equiv \rho_2 \pmod{M_q(K/k)}$. En effet $U_v(\rho_1) = U_v(\rho_2)$ $(v > 0)$, équivaut, en vertu de l'additive de $U_v(\rho)$, à $U_v(\rho_1 - \rho_2) = 0$. Or, si v n'est pas un des v_q, $U_v(\rho) = \beta_q \rho^{n_q} = 0$ n'a lieu que si $\rho^{n_q} = 0$ (car $\beta_q \neq 0$), et, puisque n_q est une puissance de p, que si $\rho = 0$; quand $v = v_q$ $(q \geq 0)$, $U_v(\rho) = z^{j_{q+1}}.\lambda_q(z_1)(\rho) = 0$ si, et seulement si $\lambda_q(z_1)(\rho) = 0$; or, $\lambda_q(z_1)$ étant le quasi-polynôme de $M_q(K/k)$, la condition $\lambda_q(z_1)(\rho) = 0$ équivaut à la condition $\rho \in M_q(K/k)$. C. q. f. d.

Posons $\pi' = \pi + \Delta\pi$, et soit $\Delta\pi = \pi.\rho\pi^v = \pi y$. On a vu que

$$f(\pi + \Delta\pi) = f(\pi(1+y)) = \pi^n \sum_{i=1}^{n} \frac{f^{(i)}(\pi)}{i!}\pi^{i-n}y^i = \pi^n.[\pi^{-n}\Phi(y)].$$

Le polygône caractéristique de $\pi^{-n}\Phi(y)$ est le polygône de ramification, dont les sommets sont

$(0, 0)$, $(n - n_0, 0)$, $(n - n_1, \phi_1 - n)$, $(n - n_2, \phi_2 - n)$, ..., $(n - n_q, \phi_q - n)$, ..., $(n - n_{m-1}, \phi_{m-1} - n)$, $(n - n_m = n - 1, \phi_m - n)$, $(n, +\infty)$.

Le coëfficient angulaire du côté $L_q = (n - n_q, \phi_q - n)(n - n_{q+1}, \phi_{q+1} - n)$ du R est $v_q(K/k)$ (on pose $\phi_{-1} = \phi_0 = n$).

En appliquant le théorème II du § 8 on voit que

1°. Si $v_{q-1} < v < v_q$, le terme prépondérant de $\pi^{-n}\Phi(y)$ est

$$\frac{f^{(n_q)}(\pi)}{n_q!}\pi^{n_q - n}y^{n_q}\ ;$$

donc, celui de $\Phi(y)$ est

$$\frac{f^{(n_q)}(\pi)}{n_q!}\pi^{n_q}y^{n_q} = \frac{f^{(n_q)}(\pi)}{n_q!}\pi^{n_q + n_q v}\rho^{n_q}\ ;$$

son ordre est $\phi_q + n_q v = \phi(v)$ et

$$f(\pi') = \Phi(y) \equiv \beta_q^{n_{q+1}}\rho^{n_q}.\pi^{\phi(v)} \equiv U_v(\rho).\pi^{\phi(v)} \pmod{\mathfrak{P}^{\phi(v)+\varepsilon}}\ (\varepsilon > 0).$$

2°. Si $v = v_q$ et, si $\rho \equiv\!|\!\equiv 0 \pmod{M_q(K/k)}$, on a $z_1^{j_{q+1}}.\lambda_q(z_1)(\rho) \neq 0$ et le terme prépondérant de $\pi^{-n}\Phi(y)$ est, comme on vérifie facilement,

$$z_1^{j_{q+1}}\lambda_q(z_1)(\rho)\pi^{\phi(v_q)-n}\ ;$$

donc

$$f(\pi') = \Phi(y) \equiv z^{j_{q+1}}\lambda_q(z_1)(\rho)\pi^{\phi(v_q)} \equiv U_{v_q}(\rho)\,\pi^{\phi(v_q)} \pmod{\mathfrak{P}^{\phi(v_q)+\varepsilon}}\ (\varepsilon > 0).$$

Si au lieu de π on prend un conjugué $\sigma\pi$ de π et si

$$\pi'' \equiv \sigma\pi + \rho(\sigma\pi)^{1+v} \pmod{\mathfrak{P}^{1+v+\varepsilon'}}\ (\varepsilon' > 0),$$

où, si $v = v_q$, on a $\rho \equiv\!|\!\equiv 0 \pmod{M_q}$, on a encore

$$f(\pi'') \equiv U_v(\rho)\,(\sigma\pi)^{\phi(v)} \pmod{\mathfrak{P}^{\phi(v)+\varepsilon}}\ (\varepsilon > 0).$$

Considérons un $A = (\alpha(\pi))$ tel que $\omega_\pi(A) > 0$. Soit

$$\pi' = \pi\alpha(\pi),\ \text{et soit que}\ \sigma \in G_{K/k}\ \text{est tel que}\ \omega\left(\alpha(\pi) - \frac{\sigma\pi}{\pi}\right) = \omega_\pi(A).$$

Alors $\pi' = \pi\alpha(\pi) \equiv \sigma\pi + \gamma(\sigma\pi)^{1+\omega_\pi(A)} \pmod{\mathfrak{P}^{1+\omega_\pi(A)+\varepsilon'}}\ (\varepsilon' > 0)$, où, suivant que $\omega_\pi(A)$ n'est pas ou est un des v_q, $\gamma = \gamma_\pi(A)$ ou $\subset \overline{\gamma_\pi(A)}$ [19], donc, dans le deuxième cas, $\overline{\gamma} \equiv\!|\!\equiv 0 \pmod{M_q(K\,k) = M_q(\sigma K/k)}$. Donc

$$\overset{\delta q}{(\sqrt{\pi})} \qquad \overset{\delta q}{(\sqrt{\sigma\pi})}$$

$$f(\pi') \equiv U_{\omega_\pi(A)}(\gamma)(\sigma\pi)^{\phi(\omega_\pi(A))} \pmod{\mathfrak{P}^{\phi(\omega_\pi(A))+\varepsilon}}\ (\varepsilon > 0),$$

où

$$U_{\omega_\pi(A)}(\gamma) \equiv\!|\!\equiv 0 \pmod{\mathfrak{P}}.$$

Il en résulte que

1°. $$t(A\,;\pi) = \phi(\omega_\pi(A)).$$

2°. $$\overline{\Gamma}'_{t(A\,;\pi)} - \overline{\Gamma}_{t(A\,;\pi)} = -\,U_{\omega_\pi(A)}(\gamma_\pi(A))\,.\,\Gamma^{a_{t(A\,:\pi)}}.$$

En effet, on a $t(A;\pi) = \omega(f(\pi')) = \phi(\omega_\pi(A))$, car $U_{\omega_\pi(A)}(\gamma) \equiv\!|\!\equiv 0 \pmod{\mathfrak{P}}$. Ensuite, $\overline{\Gamma}'_{t(A;\pi)} - \overline{\Gamma}_{t(A;\pi)}$ est la classe (mod. $\mathfrak{P}^\varepsilon$) $(\varepsilon > 0)$ à laquelle appartient

$$-\frac{f(\pi')}{\pi'^{t(A;\pi)}}\Gamma'^{a_{t(A;\pi)}}.$$

Or $f(\pi') \equiv U_{\omega_\pi(A)}(\gamma)(\sigma\pi)^{t(A;\pi)} \pmod{\mathfrak{P}^{t(A;\pi)+\varepsilon}}$; ensuite, puisque $\omega_\pi(A) > 0$, on a $\pi' \equiv \sigma\pi \pmod{\mathfrak{P}^{1+\eta}}$ $(\eta > 0)$, et $\Gamma' = \Gamma$. D'autre part, si $\omega_\pi(A)$ n'est pas un des v_q, γ est déterminé (mod. $\mathfrak{P}^{\varepsilon'}$) $(\varepsilon' > 0)$, donc $\overline{U_{\omega_\pi(A)}(\gamma)} = U_{\omega_\pi(A)}(\gamma_\pi(A))$ est parfaitement déterminé ; si $\omega_\pi(A) = v_q$, le reste de γ (mod. $\mathfrak{P}^{\varepsilon'}$) n'est déterminé que mod. $M_q(K/k)$, mais $U_{v_q}(\rho_1) = U_{v_q}(\rho_2)$

[19] $\overline{\gamma}$ est la classe de restes (mod $\mathfrak{P}^\varepsilon$) $(\varepsilon > 0)$ contenant γ.

quand $\rho_1 \equiv \rho_2 \pmod{M_q(K/k)}$; donc encore $\overline{U_{\omega_\pi(A)}(\gamma)} = U_{\omega_\pi(A)}(\overline{\gamma_\pi(A)})$ est parfaitement déterminé. Il en résulte 2°.

Considérons un nombre $t > 0$. Soit $t = \phi(t')$. On a $t(A;\pi) \geq t$ si, et seulement si $\omega_\pi(A) \geq t'$ (l'égalité ayant lieu dans les deux formules en même temps). En particulier, considérons les A tels que $\alpha(x) \equiv 1 \pmod{x}$ et tels que $t(A;\pi) > t$. M_t est l'ensemble des tous les $\overline{\Phi_{t,\pi,A}(\Gamma)} - \Gamma$. On

$$\overline{\Phi_{t,\pi,A}(\Gamma)} - \Gamma = -U_{t'}\left(\gamma_\pi^{(t)}(A)\right).\Gamma^{a_t}.$$

Donc

$$M_t = U_{t'}(R_{t'}).\Gamma^{a_t}.$$

Calculons $m_t.U_{t'}(\rho)$ étant une fonction additive de ρ, la correspondance $\rho \to U_{t'}(\rho)$ est une homomorphie. Si t' n'est pas un des v_q, $U_{t'}(\rho) = 0$ exige $\rho = 0$, donc cette homomorphie est une isomorphie et

$$m_t = r_{t'}.$$

Si $t' = v_q$, c. a. d. $t = \varphi(v_q) = \Delta_q$, $U_{t'}(\rho) = 0$ si, et seulement si $\rho \in M_q(K/k)$. Donc

$$m_{\Delta_q} = \frac{r_{v_q}}{n_q} \quad (q \geq 0).$$

Quand t parcourt la suite des entiers $\geq n$, il est visible que t' parcourt toutes les fractions de dénominateur $\delta|n_0$ de l'intervalle $(0, v_0)$, toutes les fractions du dénominateur $\delta|n_1$ de l'intervalle $(v_0, v_1), \ldots,$ toutes les fractions du dénominateur $\delta|n$ de l'intervalle $(v_{q-1}, v_q), \ldots,$ tous les entiers (car $n_m = 1$) de l'intervalle $(v_{m-1}, v_m = +\infty)$. Il en résulte: 1°) qu'il n'y a qu'un nombre fini des t' non entiers tels que t soit entier; 2°) un v n'est parmi ces t' que s'il est entier (car δ_q est premier à p et $n_0, n_1, \ldots, n_{q-1}, n_q, \ldots$ sont puissances de p). Ensuite, si t' est entier et n'est pas parmi les v_q, $R_{t'}$ est un surmodule de $R_{v,v} = \Omega_{f_0}$. Donc $r_{t'} = \frac{r_{t'}}{r_{v,v}} p^{f_0}$. Comme $m_t = r_{t'}$ on a $m_t \equiv 0 \pmod{p^{f_0}}$. Or, evidement $M_t \subseteq \Omega_{f_0}$, donc $p^{f_0} \equiv 0 \pmod{m_t}$. D'où $m_t = p^{f_0}$, et

$$r_{t'} = r_{v,v}, \text{ et } R_{t'} = R_{v,v}.$$

Il en resulte que

1°. Un des $t_0, t_1, \ldots \ldots t_\eta$ ne peut être entier que s'il est parmi les v_q.

2°. Si $t = \phi(t')$, où t' est entier, n'est pas parmi les v_q,

$$M_t = \Omega_{f_0}; \quad \frac{m_t}{p^{f_0}} = 1 = \frac{r_{t'}}{r_{v,v}}.$$

$G(\pi;t)$ est transitif et son élément reduit est 0; $h_t = 1$.

Si t' n'est pas un entier et n'est pas parmi les v_q, on a deux cas:

1°. t' n'est pas non plus parmi les $t_{q'}$; alors $r_{t'} = r_{t',t} = 1$ et $m_t = 1$. Donc

$$M_t = \{0\}; \; m_t = 1 = \frac{r_{t'}}{r_{t',t'}}.$$

2°. $t = t_{q'}$. Alors $r_{t',t'} = 1$, $r_{t'} = \begin{pmatrix} (q')(q'+1) \\ H : H \end{pmatrix}$, et on a

$$m_t = \begin{pmatrix} (q')(q'+1) \\ H : H \end{pmatrix} = \frac{r_{t'}}{r_{t',t}}.$$

Supposons maintenant $t' = v_q$; alors on a $R_{t',t'} = M_q$ ou $M_q + \Omega_{f_0}$ suivant que t' n'est pas on est entier, donc, resp. $r_{t',t'} = n_q$ ou $\frac{n_q}{r_q^{(q)}} p^{f_0}$.

Donc, si t' n'est pas entier on a

$$m_t = \frac{r_{t'}}{n_q} = \frac{r_{t'}}{r_{t',t'}};$$

et, comme dans ce cas $m_t = 1$ (car $\phi(v_q)$ n'est entier que si v_q l'est), on a que

$$r_{t'} = r_{t',t'} = n_q,$$

et l'on a, puisque sûrement $\omega_\pi(\sigma) = v_q$ pour tout $\sigma \in V^{(q)} - V^{(q+1)}$, que $t = v_q = t_{q'}$ et que $(H^{(q')(q'+1)} : H^{(q)(q+1)}) = (V^{(q)} : V^{(q+1)}) = r_{t'} = r_{t',t'}$.

Si t' est entier, on a

$$\frac{m_t}{p^{f_0}} = \frac{r_{t'}}{p^{f_0} n_q} = \frac{r_{t'}}{r_{t',t'}} \cdot \frac{1}{r_q^{(q)}}.$$

Donc

a) Si t est tel que t' n'est pas entier, on a $m_t = \frac{r_{t'}}{r_{t',t'}}$ (ce qui est égal, si $t' = v_q$, aussi à $\frac{r_{t'}}{r_{t',t'}} \frac{1}{r_q^{(q)}}$, car si v_q est fractionnaire, on a $r_q^{(q)} = 1$).

b) Si t est tel que t' est entier, $\frac{m_t}{p^{f_0}} = \frac{r_{t'}}{r_{t',t'}}$ où $\frac{r_{t'}}{r_{t',t'}} \frac{1}{r_q^{(q)}}$, suivant que des t' n'est pas un des v_q ou $t' = v_q$.

Prenons maintenant un A quelconque, mais tel que $t(A;\pi) > n$. Alors, si $\alpha(x) \equiv \gamma \pmod{x}$, on a $\gamma^h = 1$. Donc il existe un $\sigma \in G_{K/k}$ tel que $\frac{\sigma\pi}{\pi} \equiv \gamma \pmod{\mathfrak{P}^*}$, donc $\omega_\pi(A) > 0$. Ceci posé, soit $t(A;\pi) = t$. Si $\xi = \gamma^t = 1$, $T(A)$ est une traslation u qui est un élément de M_t, donc, comme $u = -U_{t'}(\gamma_{t'}^{(\pi)}(A)).\Gamma^{a_t}$, on a $\gamma_{t'}^{(\pi)}(A) \in R_{t'}$ (où $t' = \omega_\pi(A)$). Soit

$\xi \neq 1$. Soit P le pole de A pour π et t. Alors

$$\Phi_{t,\pi,A}(\overline{\Gamma}) - \overline{\Gamma} = (\xi - 1)(\overline{\Gamma} - P)$$

mais, d'autre part

$$\Phi_{t,\pi,A}(\overline{\Gamma}) - \overline{\Gamma} = -U_{t'}(\gamma_t^{(\pi)}(A)).\Gamma^{a_t}.$$

Donc $\overline{\Gamma}$ est dans la classe polaire, c'est-à-dire $\overline{\Gamma} \equiv P \pmod{M_t}$, si, et seulement si $\gamma_{t'}^{(\pi)}(A) \equiv 0 \pmod{R_{t'}}$. Et, d'ailleurs, la „distance polaire" $\overline{\Gamma} - P$ est

$$\frac{U_{t'}(\gamma_{t'}^{(\pi)}(A))}{1-\xi}.\Gamma^{a_t}.$$

Posons $r_{-1}^{(g)} = (h, p^{f_0}-1)$. A chaque $t > n$ on peut faire correspondre un diviseur $\varkappa_t$ de $r_{-1}^{(g)}$ tel que pour qu'il existe un $A = (\alpha(x))$ avec $\alpha(x) \equiv \gamma \pmod{x}$ tel que $t(A;\pi) \geq t$, il soit nécessaire et suffisant que $\gamma^{\varkappa_t} = 1$. On a $h_t = \frac{\varkappa_t}{(\varkappa_t, t)}$ (car $\xi(A) = 1$ si, et seulement si $\gamma^t = 1$, c'est-à-dire $\gamma^{(\varkappa_t, t)} = 1$), et $\varkappa_{t+1} = \varkappa_t$ ou $\frac{\varkappa_t}{h}$, suivant que Γ_t est ou n'est pas dans la classe polaire. En effet, on a vu que dans la première hypothèse il existe un A ayant le même γ, tel que $T(A)(\overline{\Gamma}) = \overline{\Gamma}$ c'est-à-dire $t(A;\pi) > t$. Et dans la deuxième hypothèse on a $t(A;\pi) = t$ pour tout A tel que $\xi(A) \neq 1$.

On a $\varkappa_{n+1} = r_{-1}^{(g)}$; $r_{-1}^{(g)}$ peut s'interpréter comme $(K_0; K_{-1}^{(g)})$, où $K_{-1}^{(g)}$ est le moindre surcorps de $K_{-1} = k$ par rapport auquel K_0 est galosien.

Soit $t^{(0)}, t', \ldots, t^{(\eta')}$ tous les t, tels que $h_t \neq 1$, écrits dans l'ordre des grandeurs croissantes, c. a. d. tous les t tels qu'il existent des $\gamma_{t'}^{(\pi)}(A)$ en dehors de R_t. Quand $t > t^{(\eta')}$, $\varkappa_t$ reste constant; appelons le $h_{+\infty}$.

On a

$$r_{-1}^{(g)} = \varkappa_{n+1} = \varkappa_t \prod_{t^{(i)} < t} h_{t^{(i)}} = h_{t^{(0)}} . h_{t^{(1)}} \ldots h_{t^{(\eta)}} . \varkappa_{t^{(\eta)}+1} = h_{t^{(0)}} h_{t^{(1)}} \ldots h_{t^{(\eta)}} . h_{+\infty}$$

c'est-à-dire

$$\prod_{i=0}^{\eta'} h_{t^{(i)}} = \frac{r_{-1}^{(g)}}{h_{+\infty}}.$$

Les résultats précédents montrent, d'ailleurs, que $r_{-1}^{(g)}$ et les $t^{(i)}$ déterminent les $h_{t^{(i)}}$. Considérons un γ tel que $\gamma^{h_{+\infty}} = 1$. On peut trouver une suite $A_1, A_2, \ldots$ des A_i telle que $t(A_i;\pi) \geq n+i$ et que $\alpha_i(x) \equiv \gamma \pmod{x}$.

Soit $A_{i+1} = B_i * A_i$. Alors, on peut choisir les A_i de manière que, si $B_i = (\beta_i(x))$, on ait $\beta_i(x) \equiv 1 \pmod{x}$. On aura $t(B_i; A_i(\pi)) \geq n+i$. Donc, si $n+i = \phi(i')$, on a $\omega_{A_i(\pi)}(B_i) = \omega_\pi(B_i) \geq i'$. Donc A_i et A_{i+1} auront les mêmes γ_j pour $j < i'$. Or $\lim i' = +\infty$. Donc, a partir d'un $i(j)$, γ_j sera le même dans tous les $\alpha_i(x)$, soit $\gamma_j^{(0)}$. Si l'on pose

$$\alpha(x) = \sum_{i=0}^{+\infty} \gamma_i^{(0)} x^i \quad \text{et} \quad A = (\alpha(x)),$$

on a $\alpha(x) \equiv \alpha_i(x) \pmod{x^{i'}}$, donc

$$t(A;\pi) \geq \operatorname{Min}(n+i, t(A_i;\pi)) \geq n+i.$$

i étant quelconque, on voit que $t(A;\pi) = +\infty$, c'est-à-dire $\pi \to A(\pi) = \pi\alpha(\pi)$ est un automorphisme de K/k, c'est-à-dire un élément de G_{K/k_g}. Comme tout A tel que $\gamma^{h_{+\infty}} \neq 1$ a un $t(A;\pi)$ fini, on voit que $\beta_{-1}(T_{K/k_g})$ parcourt l'ensemble des racines $h_{+\infty}^{ièmes}$ de l'unité dans Ω_{f_0}, c'est-à-dire

$$h_{+\infty} = r_{-1}(K/k_g)$$

et

$$\prod_{i=0}^{\eta'} h_{t^{(i)}} = \frac{r_{-1}^{(g)}}{r_{-1}(K/k_g)}.$$

Appelons I_t le nombre d'éléments du système d'intransitivité de $G(\pi; t)$ auquel appartient $\overline{\Gamma}_t$. Définissons pour chaque entier $t \geq n$ un nombre ψ_t de la manière suivante :

a) $\psi_n = \frac{I_n}{p^{f_0}-1}$.

b) Si $t = \phi(t') > n$ et si t' est entier, $\psi_t = \frac{I_t}{p^{f_0}}$.

c) Si $t = \phi(t') > n$ et si t' n'est pas entier, $\psi_t = I_t$.

Appelons *indice canonique* de $f(x)$ le produit

$$I = \prod_{t=n}^{+\infty} \psi_t.$$

Ce produit à un sens, car il n'y a qu'un nombre fini des t qui ne soient pas de la catègorie *b)*, et si $t = \phi(t') > n$ avec t' entier, on a $\psi_t = 1$, dès que t n'est pas parmi les nombres de ramification de K/k.

On a, d'après ce qui précède :

1. Si $t > n$ n'est ni un v_q, ni un $t^{(i)}$, $\psi_t = \frac{r_t}{r_{t',t'}}$.

2. Si $t>n$ est un v_q, mais n'est pas un $t^{(i)}$, $\psi_t=\dfrac{r_{t'}}{r_{t',t'}}\cdot\dfrac{1}{r_q^{(g)}}$.

3. Si $t>n$ n'est pas un v_q, mais est un $t^{(i)}$, on a $\phi_t=h_{t^{(i)}}\dfrac{r_{t'}}{r_{t',t'}}$

4. Si $t=v_q=t^{(i)}>n$, on a $\psi_t=\dfrac{h_{t^{(i)}}}{r_q^{(g)}}\dfrac{r_{t'}}{r_{t',t'}}$

5. $\psi_n=\dfrac{p^{f_0}-1}{r_{-1}^{(g)}}\cdot\dfrac{1}{p^{f_0}-1}=\dfrac{1}{r_{-1}^{(g)}}$

Donc

$$I=r_{-1}^{(g)\,-1}\prod_{q=0}^{m-1}\frac{1}{r_q^{(g)}}\cdot\prod_{i=0}^{\eta'}h_{t^{(i)}}\cdot N=r_{-1}^{(g)\,-1}\cdot\prod_{q=0}^{m-1}\frac{1}{r_q^{(g)}}\cdot\frac{r_{-1}^{(g)}}{r_{-1}(K/k_g)}\cdot\frac{\prod_{q=0}^{m-1}r_q^{(g)}}{n_0(K/k_g)}=$$

$$=\frac{1}{r_{-1}(K/k_g)n_0(K/k_g)}=\frac{1}{(K:k_g)},$$

c'est-à-dire *l'indice canonique de $f(x)$ est egal à l'inverse du dégré de K/k_g*. Etudions maintenant comment varient les M_t et les $t^{(i)}$ quand on passe de π à un autre nombre π' d'ordre 1 du même corps K. Soit $\pi'=\alpha_1\pi+\alpha_2\pi^2+\ldots$, $\alpha_1,\alpha_2,\ldots$ étant des racines $p^{f_0}-1^{\text{èmes}}$ del' unité ou des zéros, dont $\alpha_1^n=1$. Soit que $A=(\alpha(\pi))$ et que $\alpha(\pi)-\dfrac{\sigma\pi}{\pi}\equiv\gamma(\sigma\pi)^t\dfrac{\sigma\pi}{\pi}\pmod{\mathfrak{P}^{t+\varepsilon}}$ $\varepsilon>0$). Posons $\bar{A}=(\bar{\alpha}(x))$ avec

$$\pi'.\bar{\alpha}(\pi')=\alpha_1\pi\alpha(\pi)+\alpha_2\pi^2\alpha(\pi)^2+\ldots$$

On trouve

$$\pi'\bar{\alpha}(\pi')-\sigma\pi'=\alpha_1[\pi\alpha(\pi)-\sigma\pi]+\alpha_2[(\pi\alpha(\pi))^2-(\sigma\pi)^2]+\ldots\equiv$$
$$\equiv\alpha_1[\pi\alpha(\pi)-\sigma\pi]\pmod{\mathfrak{P}.(\pi\alpha(\pi)-\sigma\pi)}.$$

Donc

$$\bar{\alpha}(\pi')-\frac{\sigma\pi'}{\pi'}\equiv\alpha_1.\gamma(\sigma\pi)^t\frac{\sigma\pi}{\pi}\cdot\frac{\pi}{\pi'}\equiv\gamma(\sigma\pi')^t\frac{\sigma\pi'}{\pi'}\cdot\frac{\alpha_1\sigma\pi}{\sigma\pi'}\cdot\left(\frac{\sigma\pi}{\sigma\pi'}\right)^t\pmod{\mathfrak{P}^{t+\varepsilon}}.$$

Or

$$\sigma\pi'\equiv\alpha_1\sigma\pi\pmod{\mathfrak{P}^{t+\varepsilon}},$$

donc

$$\bar{\alpha}(\pi')-\frac{\sigma\pi'}{\pi'}\equiv\alpha_1^{-t}.\gamma(\sigma\pi')^t\pmod{\mathfrak{P}^{t+\varepsilon}}.$$

Désignons par $R'_t, M'_t, t^{(i)'}$ les modules et les nombre rélatifs à π'. Il résulte du résultat précedent que, si $A^*=(\alpha_1+\alpha_2x+\ldots)$,

$$R'_{t'}=\xi'(A^*)R_{t'},\ \text{où}\ \xi'(A^*)\equiv\alpha_1^{-t'},$$
$$t^{(i)'}=t^{(i)}.$$

Pour déterminer les $M'_{t'}$ il faut voir ce que deviennent les $U_v(\rho)$ quand on passe de π à π'. Le polygône R restant le même, on a que $U_v(\rho)$ est la classe (mod $\mathfrak{P}^{\varepsilon}$) à laquelle appartient

$$\frac{f(\pi+\rho\pi^{1+v})}{\pi^{\phi(v)}}=\frac{\Pi(\pi+\rho\pi^{1+v}-\sigma\pi)}{\pi^{\phi(v)}}.$$

Si

$$v_{q-1}<v<v_q,$$

on a

$$U(\rho)=\prod_{\sigma\in T-V}(1-\beta_{-1}(\sigma)).\prod_{i=0}^{q-1}\prod_{\substack{(i)(i+1)\\ \sigma\in V-V}}(-\beta_i(\sigma))\cdot\rho^{n_q}=-h^{n_0}\prod_{i=0}^{q-1}\prod_{\substack{(i)(i+1)\\ \sigma\in V-V}}(-\beta_i(\sigma))\rho^{n_q}.$$

Désignons par par $U'_v(\rho)$ ce que devient $U_v(\rho)$ quand on passe de π a π' en conservant ρ. Si l'on change ρ en $\alpha_1^{-v}\rho$ et si l'on remplace π par $\alpha_1\pi+\alpha_2\pi^2+\ldots$, $\beta_i(\sigma)$ se divise par $\alpha_1^{v_i}$ et

$$U'_v(\alpha_1^{-v}\rho)=\alpha_1^{-\left(\sum_{i=0}^{q-1}v_i(n_i-n_{i+1})+n_qv\right)}U_v(\rho)=\alpha_1^{-\phi(v)}U_v(\rho).$$

Si $v=v_q$, on a

$$U_v(\rho)=\prod_{\sigma\in T-V}(1-\beta_{-1}(\sigma))\prod_{i=0}^{q-1}\prod_{\substack{(i)(i+1)\\ \sigma\in V-V}}(-\beta_q(\sigma))\cdot\prod_{\substack{(q)\\ \sigma\in V}}(\rho-\beta_q(\sigma)).$$

$\beta_i(\sigma)$ se multiplie par $\alpha_1^{-v_i}$ quand on remplace π par π', et $\rho-\beta_q(\sigma)$ se multiplie par $\alpha_1^{-v_q}=\alpha_1^{-v}$ quand on remplaceaussi ρ par $\alpha_1^{-v_q}\rho$. Donc encore

$$U'_v(\alpha_1^{-v}\rho)=\alpha_1^{-\sum_{i=0}^{q-1}v_i(n_i-n_{i+1})+n_qv_q}U_v(\rho)=\alpha_1^{-\phi(v)}U_v(\rho).$$

Ainsi, soit $t=\phi(t')$. On a

$$R'_{t'}=\alpha_1^{-t'}R_{t'}.$$

Donc $M'_t=U'_{t'}(R'_{t'})\Gamma'^{a}t=U'_{t'}(\alpha_1^{-t'}R_{t'})\Gamma^{a}t=\alpha_1^{-t}U_{t'}(R_{t'})\Gamma^{a}t=\alpha_1^{-t}M_t=\xi(A^*)M_t.$

Il en résulte, en particulier, que si $\omega(A^*)>0$, on a

$$M'_t=M_t.$$

On a vu que si $t \leq t(A^\bullet;\pi)$, on a

$$\xi(A^\bullet).M_t = M_t.$$

Donc, si $t \leq t(A^\bullet;\pi)$, on a

$$M'_t = M_t.$$

Ceci permet de démontrer le théorème que nous avons énoncé

Théorème 1: *Parmi les équations d'Eisenstein équivalentes d'une équation d'Eisenstein donnée il y une et une seule qui est réduite.*

Démonstration. Supposons que $\pi_i = A_i(\pi)$ satisfait à une équation dont les Γ_t pour $t \leq n+i$ soient réduits. On peut trouver un B_i tel que $t(B_i;\pi_i) \geq n+i+1$ de manière que Γ_{n+i+1} soit réduit pour $B_i(\pi_i) = A_{i+1}(\pi)$, où l'on pose $A_{i+1} = B_i * A_i$. Comme les M_t pour les $t \leq t(B_i;\pi_i)$, donc à fortiori pour les $t \leq n+i$, sont les mêmes pour π_i et pour π_{i+1}, les Γ_t, $t \leq n+i$, restent encore réduits.

De plus, si $n+i \geq t^{(q')}$, on peut supposer que B_i est tel que $\omega(B_i) > 0$. Dans ce cas, si, de plus, $n+i > \Delta_{m-1}$, on a $\omega(B_i) > n+i-\phi_m$, c'est-à-dire $\omega(B_i) \to +\infty$. Donc $\omega(\pi_{i+1}-\pi_i) \to +\infty$, et la suite π, π_0, $\pi_1, \ldots, \pi_i, \ldots$ converge vers un $\pi^\bullet$.

Choisissons $A^\bullet$ tel que $A^\bullet(\pi) = \pi^\bullet$. Si l'on pose $A^\bullet = B^\bullet_i * A_i$, on a $t(B^\bullet_i;\pi_i) \geq n+i+1$, donc les Γ_t pour $t \leq n+i$ sont les mêmes pour π_i et pour $\pi^\bullet$, ainsi que les modules M_t des mêmes t; il en est de même des nombres $t^{(i)}$, donc aussi des $h_t(i)$. Par conséquent les Γ_t, pour $t \leq n+i$, de $\pi^\bullet$ sont réduits. Comme i est arbitraire, tous les Γ_t sont réduits et $\pi^\bullet$ satisfait à une équation réduite.

Supposons maintenant qu'il y ait deux nombres π et $\pi^\bullet$ de K/k satisfaisant à deux équations d'Eisenstein réduites distinctes. Comme ces nombres satisfont à des équations d'Eisenstein, ils sont tous les deux d'ordre 1. Donc, on peut trouver une transformation $A^\bullet$ telle que $\pi = A^\bullet(\pi)$. On a forcement $t(A^\bullet;\pi) \neq +\infty$, car autrement π et $\pi^\bullet$ satisfairaient à la même équation. Donc pour π et $\pi^\bullet$ tous les M_t pour les $t \leq t(A^\bullet;\pi)$, ainsi que les $t^{(i)}$, sont identiques (20). On a

$$\Phi_{t,A^\bullet;\pi}(\Gamma_t) = \Gamma_t \text{ pour } t < t(A^\bullet;\pi)$$

et

$$\Phi_{t,A^\bullet;\pi}(\Gamma_{t(A^\bullet;\pi)}) \neq \Gamma_{t(A^\bullet;\pi)}.$$

Donc $\Phi_{t,A^\bullet;\pi}(\overline{\Gamma}_{t(A^\bullet;\pi)})$ est un élément du système d'intransitivité de $G(\pi, t(A^\bullet;\pi))$ contenant $\overline{\Gamma}_{t(A^\bullet;\pi)}$ différent de $\overline{\Gamma}_{t(A^\bullet;\pi)}$. Comme ce système ne contient qu'un seul élément réduit, un des $\overline{\Gamma}_{t,(A^\bullet;\pi)}$, $\Phi_{t,A^\bullet;\pi}(\overline{\Gamma}_{t(A^\bullet;\pi)})$ ne l'est pas, contre l'hypothèse, ce qui achéve la démonstration.

(20) Car, si $t(A^\bullet;\pi) > 0$ et si $A^\bullet = (\alpha^\bullet_0 + \alpha^\bullet_1 x + \ldots)$, on a $\alpha^{\bullet n}_0 = 1$.

Remarque : Tous les éléments de K/k qui satisfont à la seule équation d'Eisenstein réduite qui définit ce corps se déduisent évidemment de l'un d'eux par des automorphismes de K/k, c'est-à-dire par les éléments de G_{K/k_g}. Donc leur nombre est

$$(K:k_g) = \frac{1}{I}.$$

Etudions maintenant les propriétés d'une équation réduite. Soit

$$f(x) = x^n + \sum_{t=0}^{+\infty} \Gamma_t X_t = 0$$

une équation réduite.

Théorème II : *Soit $n_q = p^{j_q}$ et soit que $j_q > j \geq j_{q+1}$, Si t est un entier d'ordre j en p tel que $\Gamma_t \neq 0$, ou bien t est contenu dans l'intervalle fermé*

$$(\phi_q + v_q(n_q - p^j),\ \Delta_q = \phi_q + v_q n_q)$$

de longueur $p^j v_q \leq \dfrac{E}{p^{j_q - j - 1}(p-1)}$, ou bien il est un des Δ_i $(i = q, q+1, \ldots, m)$.

Démonstration. Par définition

$$w_j = \text{Min}\,[w_{j+1} + E,\ t]$$
$$t \equiv 0 \pmod{p^{j+1}}$$
$$\Gamma_t \neq 0.$$

Donc si l'on aurait $\Gamma_t \neq 0$ pour un $t < \phi_q + v_q(n_q - p^j)$, le point $(n-p^j,\ w_j - n)$ se trouverait au-dessous du polygône de ramification R, ce qui est absurde. D'autre part si $t > \Delta_q$ est divisible par p^j, donc par $p^{j_q+1} = n_{q+1}$, il existe un entier t' tel que $t = \phi(t')$. Si, de plus, t n'est pas parmi les Δ_q, c'est-à-dire t' n'est pas parmi les v_q, on a $M_t = \Omega_{f_0}$, c'est-à-dire l'élément réduit est 0. Donc $\Gamma_t = 0$ et tout est prouvé.

Conséquence : *Si $t > \Delta_{m-1}$, $\Gamma_t = 0$.*

Théorème III : *Δ_q étant entier, soit que $\mathfrak{M}(z_1^{f_0} - 1,\ z_1^{j_{q+1}} \lambda_q(z_1)) = \mu_q(z_1) z_1^{j_{q+1}} \lambda_q(z_1)$. Alors le degré de $\mu_q(z_1)$ est $f_0 - \log_p r_q^{(q)}$, et le quasi-polynôme de $\Gamma^{-a_{\Delta_q}} M_{\Delta_q}$ est multiple de $\mu_q(z_1)$.*

Démonstration : On a que $R_{v_q} \supset \Omega_{f_0}$, donc $\Gamma^{-a_{\Delta_q}} M_{\Delta_q} = U_{v_q}(R_{v_q})$ est un surmodule de $M = z^{j_{q+1}} . \lambda_q(z_1)\,(\Omega_{f_0})$. Or, on a pour tout $m \in M$ $\mu(z_1)(m) = 0$ seulement si $\mu(z_1) z^{j_{q+1}} \lambda_q(z_1) \equiv 0 \pmod{z_1^{f_0} - 1}$, c'est-à-dire

si $\mu(z_1)\equiv 0 \pmod{\mu_q(z_1)}$. Donc, en particulier, le quasi-polynôme de $\Gamma^{-a_{\Delta_q}}M_{\Delta_q}$ est $\equiv 0 \pmod{\mu_q(z_1)}$.

Enfiin le degré de $\mu_q(z_1)$ est égal à f_0 moins le degré de $\mathfrak{D}(z_1^{f_0}-1, \lambda_q(z_1))$, c'est-à-dire à $f_0 - \log_p r_q^{(g)}$.

Théorème IV: *Le dénominateur de t_q est une puissance de p dont l'exposant est zéro si, et seulement si t_q est un nombre de ramification entier de* K/k. *Si $\phi(t_q)$ est d'ordre j ($j_{q'} > j \geq j_{q'+1}$) en p, $\phi(t_q)$ se trouve, quand il n'est pas un des Δ_i, à l'intérieur de l'intervalle (ouvert)*

$$(\phi_{q'}+v_{q'}(n_{q'}-p^j),\ \Delta_{q'}=\phi_{q'}+v_{q'}n_{q'}).$$

Démonstration : t_q n'est entier que s'il est un nombre de ramification de K/k, car autrement on a $R_{t_q}' = R_{t_q,t_q} = \Omega_{f_0}$. D'autre part, $\phi(t_q)$ doit être entier. Si $\phi(t_q)$ est dans l'intervalle $(\Delta_{q'-1}, \Delta_{q'})$ on a $\phi(t_q) = \phi_{q'} + n_{q'}t_{q'}$, c'est-à-dire $t_q = \dfrac{\phi(t_q)-\phi_{q'}}{n_{q'}}$; donc le dénominateur de t_q est diviseur de $n_{q'} = p^{j_{q'}}$, c'est-à-dire une puissance de p.

Si t est d'ordre j en p, et si $t \leq \phi_{q'}+v_{q'}(n_{q'}-p^j)$, on doit avoir $M_t = \{0\}$. Car autrement il existerait un $\pi' \equiv \pi \pmod{\mathfrak{P}^2}$ qui satisfairait à une équation ayant soit un autre polygône de ramification R (si $t < \phi_{q'}+v_{q'}(n_{q'}-p^j)$), soit un autre $\lambda_{q'}(z_1)$ (si $t = \phi_{q'}+v_{q'}(n_{q'}-p^j)$), ce qui est impossible. Si $\phi(t) \geq \Delta_{q'}$, sans être un des Δ_i, t est entier qui n'est pas un v_q. Ceci montre que $\phi(t_q)$ est bien à l'intérieur de l'intervalle indiqué.

Théorème V. *Si $t^{(q')} = \phi(t^{(q')*})$, 1°. Les dénominateurs des $t^{(q')*}$ sont puissances de p, dont l'exposant n'est nul que si $t^{(q)*}$ est un nombre de ramification entier de* K/k. *2°. Si $t^{(q)}$ est d'ordre j en p ($j_{q'} > j \geq j_{q'+1}$), $t^{(q)}$ se trouve, quand il n'est pas un Δ_i, dans l'intervalle indiqué fermé. 3°. $P_{\phi_q+v_q(n_q-p^j),\,\pi,\,A} = 0$ quand $\phi_q+v_q(n_q-p^j)$ est entier, π étant un nombre quelconque de* K *d'ordre* 1 *et* A *étant une transformation quelconque telle que $t(\pi;A) \geq \phi_q+v_q(n_q-p^j)$ et que $\xi(A) \neq 1$. 4°. Si $t \leq t^{(q)}$, $t(m_t-1) \equiv 0$ (mod. $\varkappa_t(q)$).*

Démonstration : 1°. et 2°. se démontrent comme dans le théorème précédent. 3°. suit de ce que $U'_{v_q}(\gamma^{-r_q}) = U_{r_q}(\rho)\cdot\gamma^{-\phi(v_q)}$, où $\pi' \equiv \gamma\pi \pmod{\mathfrak{P}^2}$. Car en effet, on a, en explicitant cette formule,

$$\Phi_{\phi_q+v_q(n_q-p^j),\,\pi,\,A}(\overline{\Gamma}) = \gamma^{-\phi_q-v_q(n_q-p^j)}\overline{\Gamma},$$

où

$$A(\pi) = \gamma\pi \pmod{\mathfrak{P}^2},$$

on voit bien que si $\xi(A) = \gamma^{-\phi_q-v_q(n_q-p^j)} \neq 1$, T(A) est une homotétie de Ω_{f_0} par rapport à 0, qui est ainsi le pôle de A.

Enfin, si $t \leq t^{(q)}$, on a, si $\gamma^{\varkappa_t(q)} = 1$,

$$\gamma^{-t}M_t = M_t.$$

Il en resulte, puisque on peut prendre γ tel que γ^{-t} soit une racine $\dfrac{\varkappa_t(q)}{(t,\varkappa_t(q))}$ — ième primitive de l'unité, que $m_t - 1 \equiv 0 \left(\mathrm{mod}\ \dfrac{\varkappa_t(q)}{(t,\varkappa_t(q))}\right)$, et que

$$t(m_t-1) \equiv 0 \pmod{\varkappa_t(q)}.$$

Voyons maintenant quelles simplifications subit la théorie exposée dans des cas particuliers :

Tout d'abord il y a deux cas où les systèmes d'intransitivité de $G(t,\pi)$ pour $t > n$ se réduisent certainement aux classes (mod. M_t) ; à savoir le cas manifeste $h = 1$ et le cas de K/k galoisien. Dans ce dernier cas les t_i n'existent pas (sauf $t_0 = +\infty$), donc *si* K/k *est galoisien* $M_{\phi(t')} = \{0\}$ *quand t' n'est pas entier,* $M_{\phi(t')} = \Omega_{f_0}$ *quand t' est entier et non égal à aucun des v_q, et M_{Δ_q} est l'ensemble des racines de l'équation* $\mu_q(z_1)(x) = 0$, où $\mu_q(z_1)\lambda_q(z_1) = z_1^{f_0} - 1$ ($q \geq 0$).

$I = \dfrac{1}{(K:k)}$ *si, et seulement si* K/k *est galoisien.*

Un cas remarquable est celui *où* K/k *n'a qu'un seul nombre de ramification effectif non infini v* (c'est-à-dire si $v = 0$, $n = h = 1$).

Posons $\Delta = \phi(v)$. Deux cas se présentent :

1° $v = 0$. Alors les systèmes d'intransitivité de $G(n,\pi)$ sont les classes suivant le groupe multiplicatif des raeines $\dfrac{p^{f_0}-1}{(h, p^{f_0}-1)}$ ièmes de l'unité et l'ensemble $\{0\}$. Si $t > n$, on a $M_t = \Omega_{f_0}$. Donc l'équation réduite est

$$x^h - \Gamma\overline{\pi} = 0$$

où $\Gamma = \rho^i$ ($i = 0, 1, \ldots, (h, p^{f_0}-1)-1$). C'est le théorème cité au § 3 de M. Hensel. On a ici $I = \dfrac{1}{(h, p^{f_0}-1)}$.

2° $v \neq 0$. Alors $h = 1$, $n = p^j$, on a $M_t = \{0\}$ quand $t \equiv 0 \pmod{n}$ est $< \Delta = n(1+v)$ et $M_t = \Omega_{f_0}$ quand $t > \Delta$ ou $t \not\equiv 0 \pmod{n}$. M_Δ est l'ensemble de racines de $\mu(z_1)(x) = 0$, où $\mu(z_1)\lambda_1(z_1) = \mathfrak{M}(z_1^{f_0}-1, \lambda(z_1))$.

On a ici $I = \dfrac{1}{p^{\nu(\mathfrak{D}(\lambda(z_1)\, z_1^{f_0}-1))}}$, et $t_0 = +\infty$ (car $(K : k_0) = r_0^{(q)}$).

L'équation réduite a la forme

$$(1)\qquad x^{p^j} + \sum_{q=1}^{j-1} \sum_{\substack{p^j + v(p^j - p^{j-q}) \leq i < p^j + v(p^j - p^{j-q-1}); \\ i \equiv 0 \pmod{p^{j-q}}; \\ i \not\equiv 0 \pmod{p^j};}} \Gamma_i \overline{\pi}^{E\left(\frac{i}{p^j}\right)} x^{i - p^j E\left(\frac{i}{p^j}\right)} + \sum_{\substack{i = p^j + v p^j; \\ i \not\equiv 0 \pmod{p^j}; \\ \text{ou } i = p^j + v p^j;}} \Gamma_i \overline{\pi}^{E\left(\frac{i}{p^j}\right)} x^{i - p^j E\left(\frac{i}{p^j}\right)} = 0.$$

Un cas particulier remarquable des cas précédents est celui où K/k est *primitif*. Si $v = 0$, $n = h$ est premier. Si $p^{f_0} \equiv 1 \pmod h$, K k est galoisien, $I = \dfrac{1}{h} = \dfrac{1}{(K : k)}$ et l'équation réduite est

$$x^h - \rho^i \overline{\pi} = 0, \text{ où } i = 0, 1, \ldots, h-1.$$

Si $p^{f_0} \not\equiv 1 \pmod h$, K/k est non-galoisien, et $k_0 = K$. Ici $I = 1$ et l'équation réduite est

$$x^h - \overline{\pi} = 0.$$

Si $v > 0$, deux cas peuvent se présenter :

a) $z_1^{f_0} \equiv 1 \pmod{\lambda(z_1)}$. Alors K/k est galoisien et $v(\lambda(z_1)) = 1$. $\lambda(z_1)$ a la forme $z_1 - \omega^{p-1}$, où $\omega \in \Omega_{f_0}$, $M_\Delta = M_{p(1+v)}$ se définit par la $M_\Delta \times M^{(\pi)}(K/k) = \Omega_{f_0}$, où $M^{(\pi)}(K/k) = \{0, \omega, 2\omega \ldots, (p-1)\omega\}$. On a ici $I = \dfrac{1}{p} = \dfrac{1}{n}$, $n = p$, et l'équation réduite a la forme

$$x^p + \sum_{\substack{p + v(p-1) \leq i \leq p(1+v); \\ i \not\equiv 0 \pmod p \\ \text{ou } i = p(1+v);}} \Gamma_i \overline{\pi}^{E\left(\frac{i}{p}\right)} x^{i - p E\left(\frac{i}{p}\right)}$$

$\Gamma_{p(1+v)}$ est l'élément réduit de sa classe (mod $M_{p(1+v)}$).

b) $z_1^{f_0} \not\equiv 1 \pmod{\lambda(z_1)}$. Alors K k est non-galoisien, $k_0 = K$, $I = 1$ et $M_\Delta = \Omega_{f_0}$ (parce que si M_Δ existe, $\Delta = p^i(1+v)$ est entier, donc v est entier) et, en général, $M_{\phi(t)} = \{0\}$ ou Ω_{f_0} suivant que t est fractionnaire ou entier. L'équation réduite est de la forme (1), mais avec $\Gamma_\Delta = 0$

(donc dans le dernier signe Σ il faut prendre la limite supérieure $p^j + v(p^j - 1)$).

Ce qui est dit ici sur les corps primitifs résout complètement le problème posé par M. Ore: trouver une forme normale pour les équations d'Eisenstein primitives. Toutefois, la forme de l'équation réduite que nous avons donnée, tout en étant très logique, n'est pas la seule possible, surtout dans des cas particuliers Ainsi M. Ore a donné pour les équation d'Eisenstein de degré p une autre forme (qui se déduit, d'ailleurs, facilement de la nôtre), où il fait disparaître tous les Γ_t tels que $t \not\equiv 0 \pmod p$ sauf $\Gamma_{p+v(p-1)}$. M. Ore a donné d'ailleurs dans ce cas particulier ($n = p$) la condition pour que K/k soit galoisien, mais la différence fine entre les équations d'Eisenstein de degré p des types a) et b) ($I = \dfrac{1}{p}$ dans le premier cas, $I = 1$ dans le second cas) ne pouvait pas se voir clairement avec sa forme canonique.

On a

$$N_{K/k}(\pi) = a_n = \sum_{t'=1}^{+\infty} . T_{nt'} \overline{\pi}^{t'}.$$

Considérons l'indice $\mathcal{J} = \dfrac{p^{f_0}-1}{\xi_n} \prod_{t'=2}^{+\infty} \left(\dfrac{p^{f_0}}{\xi_{nt'}}\right)$. On voit que $\mathcal{J}$ est un diviseur de $\prod_{q=-1}^{m-1} r_q^{(q)}$, donc aussi de $(K : k)$, et qu'il ne peut être égal à $(K : k)$ que si tous les Δ_q sont $\equiv 0 \pmod n$, ce qui a lieu si, et seulement si K/k est *hassien* (voir ma note *C. R.*, 8 juillet 1035 et chap. V de ma thèse), c'est-à-dire si pour tout $q = 0, 1, \ldots, m-1$, v_q est entier et $v_q \equiv v_{q-1} \left(\text{mod } \dfrac{n}{n_q(K/k)}\right)$. En particulier, si K/k est galoisien, on a $\mathcal{J} = (K : k)$ si, et seulement si K/k est hassien, et dans tous les autres cas on a $\mathcal{J} < (K : k)$.

Considérons le groupe de Tacagi $H_{K/k}$ de K/k (c'est-à-dire le groupe multiplicatif de normes par rapport à k des tous les nombres non nuls de K). Soit A_u le rayon de $\mathfrak{p}^u$ dans k. Soient $H_u = H_{K/k} \cap A_u$; soient $u_0, u_1, \ldots, u_\mu$ tous les entiers > 0 tels que $A_{u_j} H_{K/k} \neq A_{u_j+1} H_{K/k}$ (ce qui arrive si, et seulement si $(H_{u_j} : H_{u_j+1}) \neq (A_{u_j} : A_{u_j+1}) = p^{f_0}$), et soit

$$v_j = (A_{u_j} H_{K/k} : A_{u_j+1} H_{K/k}) = \frac{p^{f_0}}{(H_{u_j} : H_{u_j+1})}.$$

Posons, de plus, $u_{-1} = 0$ et

$$v_{-1} = (A_0 H_{K/k} : A_1 H_{K/k}) = \frac{(A_0 : A_1)}{(H_0 : H_1)} = \frac{p^{f_0} - 1}{(H_0 : H_1)}.$$

Il est bien visible que

1°. $\theta = u_j\,(j \geq 0)$ seulement si $M_{n(1+\theta)} \neq \Omega_{f_0}$.

2°. $v_j\,(j > 0)$ est diviseur de $(\Omega_{f_0} : M_{n(1+u_j)}) = \dfrac{p^{f_0}}{m_{n(1+u_j)}}$.

3°. v_{-1} est diviseur de $(\Omega'_{f_0} : \Sigma_0) = (p^{f_0} - 1, h)$.

Il en résulte la généralisation pour le cas non-galoisien (et une nouvelle démonstration pour le cas galoisien) du théorème de M. Hasse sur les restes nomiques :

Théorème VI.

a) Les u_j sont parmi les nombres $\dfrac{\Delta_q - \Delta_{-1}}{n}$.

b) v_j est diviseur de $p^{\nu(\vec{\mathfrak{D}}(z_1^{f_0} - 1,\ \lambda_q(z_1)))}$ si $u_j = \dfrac{\Delta_q - \Delta_{-1}}{n}$, et de $(p^{f_0} - 1, h)$, si $u_j = 0$.

En particulier : $(A_0 : H_0) \mid \mathcal{J}$.

Donc si K/k complètement ramifié est un corps de classes, donc $(A_0 : H_0) = (K : k)$, on doit avoir $(A_0 : H_0) = \mathcal{J} = (K : k)$. Donc, un corps de classes est hassien.

La condition $(A_0 : H_0) = \mathcal{J}$ exige alors que tous les nombres $\dfrac{\Delta_q - \Delta_{-1}}{n}$ soient des u_j, c'est à-dire que $u_j = \dfrac{\Delta_j - \Delta_{-1}}{n}$, que pour tout $j \geq 0$ on ait

$$v_j = p^{\nu(\vec{\mathfrak{D}}(z_1^{f_0} - 1,\ \lambda_j(z_1)))} = r_j(K/k),$$

et que $v_{-1} = h = r_{-1}(K/k)$. C'est le Führer-Discriminantensatz de M. Hasse. On peut tirer du résultat qui précède une conséquence particulièrement frappante, concernant les normes dans les corps primitifs. En effet, si le corps primitif K/k est galoisien, il est cyclique de degré premier, donc corps de classes. S'il est non-galoisien, comme on a vu, $\mathcal{J} = 1$. Donc on a

Théorème VII.

a) *Un corps primitif galoisien* K/k *est un corps de classes.* $H_{K/k}$ *est d'indice* $(K : k)$.

b) *Un corps primitif non-galoisien* K/k *a le groupe* $H_{K/k}$ *d'indice* 1. *Tout nombre de* k *est norme par rapport à* k *d'un nombre de* K.

On peut encore préciser le théorème VI. En effet, les restes (mod $\mathfrak{p}$) des $\dfrac{\alpha - 1}{\pi^u}$ des $\alpha \in H_u$ forment un sous-module μ_u de Ω_{f_0} quand $u > 0$. Il est visible que ce module est surmodule de $M_{n(1+u)}$. D'ailleurs, si $n = u_j$, $(\Omega_{f_0} : \mu_u) = v_j$, et si u n'est pas un u_j, $\mu_u = \Omega_{f_0}$. Se rappelant la mode de formation des M_t, on voit que ceci permet de former tout au moins au sous-module μ'_u de tout μ_u à partir des $M_q(K/k)$. D'ailleurs, si K/k est un corps de classes, on a $\mu_u = M_{n(1+u)}$, c'est-à-dire, si $B_q = \prod_{i=0}^{q-1} \prod_{\sigma \in V^{(i)} - V^{(i+1)}} (\beta_i(\sigma))$,

$$B_q^{-1}\,\Gamma^{-\frac{\Delta_q}{n}}\,\mu_{\frac{\Delta_q - \Delta_{-1}}{n}} \times M_q(K/k) = M_q(K/k) \times B_q^{-1}\,\Gamma^{-\frac{\Delta_q}{n}}\,\mu_{\frac{\Delta_q - \Delta_{-1}}{n}} = \Omega_{f_0},$$

ou

$$\mu_{\frac{\Delta_q - \Delta_{-1}}{n}} = \left\{ \prod_{\beta \equiv \alpha \,(\mathrm{mod}\, M_q)} \beta \right\}_{\alpha \in \Omega_{f_0}} \Gamma^{\frac{\Delta_q}{n}} B_q,$$

$$M_q(K/k) = \left\{ \prod_{\beta \equiv \alpha \,(\mathrm{mod}\, \mu_{\frac{\Delta_q - \Delta_{-1}}{n}} B_q^{-1} \Gamma^{\frac{\Delta_q}{n}})} \beta \right\}_{\alpha \in \Omega_{f_0}}.$$

Il est possible de préciser encore plus la liaison qui existe entre $\beta_q(\sigma)$ et les restes mod $\mathfrak{p}$ des $\dfrac{\alpha - 1}{\pi^{\frac{\Delta_q - \Delta_{-1}}{n}}}$ pour les α tels que $\left(\dfrac{\alpha, K}{\mathfrak{p}}\right) = \sigma$.

On arrive ainsi à une formule qui fournit un analogue presque complet d'une formule de la théorie de la ramification quej'ai énoncée au chap. III, A de ma thèse (formule (8) de la p. 68). La démonstration de ces deux formules se fait par des méthodes analogues et, d'ailleurs, différentes de celles de ma thèse et de ce travail. Elle sera publiée dans un travail futur.

Je ne peux pas insister ici sur toutes les conséquences qu'on peut tirer des résultats de ce §. Je dois indiquer toutefois quelquesuns des problèmes qu'ils permettent de résoudre, ainsi que quelques directions dans lesquelles ils sont susceptibles d'être généralisés.

a) Les résultats de ce § permettent de résoudre par un nombre fini d'opérations univoques (c'est-à-dire ne comportant pas des choix arbitraires) la quéstion : les équations d'Eisenstein $f_1(x) = 0$ et $f_2(x) = 0$ sont-elles équivalentes ? En effet $f_1(x) = 0$ et $f_2(x) = 0$ sont équivalentes si, et seulement si leurs réduites coïncident. Et la réduite d'une équation

d'Eisenstein $f(x)=0$ peut être formée par un nombre fini d'opérations univoques, parce que, tous les Γ_t réduite pour $t > \Delta_{m-1}$ étant nuls (et Δ_{m-1} se calculant par une méthode univoque à partir de $f(x)$), on n'a qu'à calculer successivement le nombre fini des Γ_t réduits pour $t \leq \Delta_{m-1}$. Ces Γ_t ne changeront plus au cours des réductions suivantes.

b) Il est visible que le nombre de corps $\mathfrak{P}$-adiques K/k (pour k fixe) de dégré donné est *fini* : en effet, on a pour un tel corps

$$\Delta_{m-1} \leq (K:k) + E\log_p(K:k) + \frac{E}{p-1} = (K:k)\left\{1 + e_0 \log_p(K:k) + \frac{e_0}{p-1}\right\},$$

$f_{K/k} < (K:k)$ peut prendre au plus $(K:k)$ valeurs. Pour chaque valeur de $f_{K/k}$ il y a au plus, d'après ce qui précéde

$$p^{f_0 f_{K/k}(K:k)e_0\left\{\log_p(K:k)+\frac{1}{p-1}\right\}} = (K/k)^{f_0 f_{K/k} e_0 (K:k)},$$

$$p^{f_0 f_{K/k}(K:k)\frac{e_0}{p-1}} < (K:k)^{f_0 e_0 (K:k)^2 \frac{f_0 e_0}{p-1}(K:k)^2}$$

équations réduites, définissant K/k de forme voulue par rapport à $(K/k)_{-1}$. Donc le nombre des $(K:k)$ de degré n est au plus $n(np^{\frac{1}{p-1}})^{e_0 f_0 n^2}$, donc fini.

Les résultats précédents de ce § et des §§ 4, 6, 8 permettent de calculer ce nombre (que nous désignerons par $S(k;n)$). D'ailleurs ces résultats permettent, en supposant connue la structure d'un nombre fini des $W_{a,b}$ de calculer d'autres constantes caractérisant les surcorps K d'un k donné, par exemple le nombre des corps K/k ayant un polygône R donné, la nombre $P(k;n)$ de surcorps primitifs K de degré rélatif n d'un k donné etc... J'exposerai ces applications de la théorie développée dans un travail spécial.

c) Les résultats précédents fournissent une vue d'ensemble *de tous les surcorps complètement ramifiés d'un corps donné* (p-adique) k. Par cela ils semblent être d'une grande importance dans toutes les quéstions, où il s'agit de savoir s'il existent des corps possédant des propriétés indiqués à l'avance. On peut dire plus : les résultats de ce § donnent une généralisation partielle pour les surcorps complètement ramifiés d'un corps k de la théorie des corps de classes locale (qui, d'ailleurs, est certainement extensible aux surcorps *quelconques* d'un corps local k, et qui semble pouvoir être completée jusqu'à devenir une généralisation

complète de la théorie des corps de classes locale, du moins pour les surcorps galoisiens de k). Examinons pour chaque loi de la théorie locale de corps de classes l'analogue partiel qu'en fournit notre théorie.

A) *Loi d'unicité. Conducteur.* Nous avons vu que, S_t étant le système d'intransitivité de $\mathfrak{S}(\pi,t)$ contenant $\overline{\Gamma}_t$ et π étant la α racine de l'équation d'Eisenctein réduite définissant K/k, la donnée des S_t $(t=n, n+1, \ldots, +\infty)$ définit certainement K/k (à conjugaison près) parceque définit son équation réduite. D'une manière plus précise, puisque $S_t = \Omega_{f_0}$ quand $t > \Delta_{m-1}$, il suffit de donner

$$S_n, S_{n+1}, \ldots, S_{E(\Delta_{m-1})}$$

(il est à remarquer, d'ailleurs, que Δ_{m-1} peut se calculer à partir des S_t, en constituisant le polygône R de l'équation réduite, et, qu'ainsi, un certain nombre $S_n, S_{n+1}, \ldots, S_i$ des S_t consécutifs étant donné, on peut savoir si $i \geq E(\Delta_{m-1})$). Cette manière de caractériser K/k au moyen des S_t (qui sont bien des objets dans k) fournit une sorte de loi d'unicité, mais qui n'est pas intrinsèque, parce que dépend du choix, très artificiel, d'une équation réduite.

Nous dirons que deux polynômes d'Eisenstein de degré n dans k, $f_1(x)$ et $f_2(x)$ sont *congrûs* mod $\mathfrak{p}^{\frac{t}{n}}$ ou *appartiennent à la même clase* mod $\mathfrak{p}^{\frac{t}{n}}$, si $f_1(x) - f_2(x)$ est d'ordre total $\geq n+t$. Nous dirons qu'un ensemble d'équations d'Eisenstein de degré n est *définissable* mod $\mathfrak{p}^{\frac{t}{n}}$ si toute équation, congrue mod $\mathfrak{p}^{\frac{t}{n}}$ à une équation de cet ensemble, en fait partie. Etant donné un ensemble S d'équations d'Eisenstein de degré n définissable suivant certains idéaux de la forme $\mathfrak{p}^{\frac{t}{n}}$, il est encore définissable suivant leur plus grand commun diviseur $\mathfrak{f}_S = \mathfrak{p}^{\frac{\varphi_S}{n}}$ qui sera appelé *conducteur* de S. Les résultats de ce § montrent que l'ensemble $S_{K/k}$ de toutes les équations d'Eisenstein définissant un corps complètement ramifié K/k de degré n est définissable suivant les modules de la forme indiquée, et que son conducteur est

$$\mathfrak{f}_{K/k} = \mathfrak{p}^{\frac{E(\Delta_{m-1})-n+1}{n}} = \mathfrak{P}^{1+E(\Delta_{m-1})-\Delta_{-1}} = \mathfrak{P}^{1+E\left(\sum_{q=0}^{m-1} n_q(v_q - v_{q-1})\right)}.$$

$S_{K/k}$ possède une sorte de structure „arborescente régulière", c'est-à-dire $f(x)$ étant une équation de $S_{K/k}$ et $\mathfrak{P}^{t+1}$ étant un diviseur de $\mathfrak{f}_{K/k}$, le nombre d'équations de $S_{K/k}$ incongrûs deux à deux (mod $\mathfrak{P}^{t+1}$) et congrûs à $f(x)$ (mod $\mathfrak{P}^t$) est le même quelque soit $f(x) \in S_{K/k}$, a savoir I_{n+t}.

On dira que K/k *appartient* à l'arbre $S_{K/k}$ de k. $\mathfrak{f}_{K/k}$ sera dit *conducteur* de K/k. A remarquer que si K/k est un corps de classes, son conducteur au sens ordinaire est la moindre puissance *entière* de $\mathfrak{p}$ divisible par $\mathfrak{f}_{K/k}$. Si deux surcorps K et K' de k appartiennent au même arbre S, ils sont conjugués par rapport à k; en particulier, si K/k est galoisien, il est l'unique corps appartenant à $S_{K/k}$.

On a montré que l'arbre $S_{K/k}$ peut se caractériser par une branche réduite.

B) *Loi d'existence:* On a vu qu'à un système d'équations d'Eisenstein d'un degré n dans k définissable suivant un module $\mathfrak{f}=\mathfrak{p}^{\underline{t}}$ ou bien n'appartient aucun corps K/k, ou bien appartient un ensemble des corps K/k conjugués entre eux. Appelons les systèmes S auxquels appartiennent des corps K/k *arbres normaux* de k. Les résultats de ce § indiquent certaines propriétés que doit posséder un système S pour être un arbre normal: à savoir tous les $f(x)\in S$ doivent avoir le même polygône R, les M_t doivent dépendre de $f(x)$ comme il a été indiqué, les t_i et les $t^{(i)}$ doivent être les mêmes pour tous les $f(x)\in S$ etc. Mais ils ne donnent pas de critère *explicite* pour distinguer si S est on n'est pas un arbre normal.

Pourtant, les résultats précédents *fournissent un algorithme permettant de former par un nombre fini d'opérations tous les arbres normaux d'équations d'*Eisenstein *de degré n donné, définissables suivant un module* $\mathfrak{f}$ *donné*, c'est-à-dire donnent une sorte de *loi d'existence implicite*. En effet, nous avons vu que la connaissance des $\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{n+t-1}$ définit $\mathfrak{G}(\pi, n+i)$. Donc, si l'on sait que $\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{n+i-1}$ sont les i premiers Γ_t d'une équation réduite, toutes les possibilités pour Γ_{n+i} d'une telle équation réduite sont parfaitement déterminés. (A savoir les éléments réduits de tous les systèmes d'intransitivité de $\mathfrak{G}(\pi; n+i)$.

On commence par former tous les Γ_n réduits possibles; pour chacun de ces Γ_n on forme tous les Γ_{n+1} possibles; pour chaque système Γ_n, Γ_{n+1} ainsi formé on forme tous les Γ_{n+2} possibles etc., jusqu'à former tous les systèmes $\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{n+t-1}$. Toutes les équations réduites définissant des sorps K/k appartenant aux arbres normaux définissables mod $\mathfrak{f}=\mathfrak{p}^{\underline{t}}$ doivent être de la forme $x^n + \sum_{i=n}^{n+t-1} \Gamma_i X_i = 0$, où $\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{n+t-1}$ est parmi les systèmes précédemment formés. Pour que l'équation de cette forme définisse effectivement un tel corps, il faut et il suffit qu'encore $\Delta_{m-1} < t$. On vérifie si cela a lieu en formant son polygône de ramification. Les autres systèmes sont les „commencements" des équations d'Eisenstein définissant les corps d'un plus grand conducteur.

Pour déterminer $\mathfrak{G}(\pi; n+i)$ connaissant les $\Gamma_n, \Gamma_{n+1}, \ldots, \Gamma_{n+t-1}$, il suffit de calculer M_{n+i}, h_{n+i} et la classe polaire $\mathfrak{P}_{n+i}$. h_{n+i} se calcule directement, parce que on connait les $\varkappa_j$, $j < n+i$. Pour calculer M_{n+i} et $\mathfrak{P}_{n+i}$ on commence par calculer tous les w_s et les b_{p^u} que la connaissance des $\Gamma_n, \Gamma_{n+1} \ldots, \Gamma_{n+i-1}$ permet de calculer, et par construire le polygône de Newton rélatif à ces points et au point $(n, i+1)$. L'avant-dernier coté de ce polygône coïncide avec un coté L_q du polygône de ramification de tout corps défini par une équation réduite ayant les Γ_j, $j \leq n+i-1$, indiqués, et le coefficient angulaire du dernier coté de ce polygône est $\leq v_{q+1}$ (K/k) pour tout K/k de forme indiquée. Donc cela définit v tel que $n+i = \phi(v)$ et la fonction $U_v(\rho)$. Si $n+i = \Delta_q$, cela définit aussi $M_q(K/k)$. Pour déterminer R_v et $\mathfrak{P}_{n+i}$, il suffit de développer en série de la forme $\pi\alpha(\pi)$ tous les $\sigma\pi$ (mod $\mathfrak{P}^{v+1+\varepsilon}$) ou (mod $\mathfrak{P}^{l(\sigma)+1+\underline{\varepsilon}}$) $(\varepsilon > 0)$, suivant que $t(\sigma) \geq v$ ou $t(\sigma) < v$. Les considérations précédentes prouvent que la connaissance des Γ_j, $j \leq n+i-1$, définit cette partie du développement des $\sigma\pi$, et on la forme effectivement par la méthode semblable à celle de Puiseux pour les fonctions algébriques. Connaissant R_v, on a $M_{n+i} = \Gamma^{\prime n+i} U_v(R_v)$.

Une équation $f(x) = 0$ définissant un corps K/k étant donnée, on forme $S_{K/k}$ par un nombre fini d'opération. Il suffit en effet de former es transformées de $f(x)$ par un nombre *fini* de transformations de Tchirnhausen, p. ex. par celles de la forme

$$y = x \sum_{i=0}^{E(v_{m-1})} \gamma_i x^i,$$

où $\gamma_0^{f_0} = 1$ et $\gamma_i^{f_0} = 1$ ou 0 si, $i > 0$ (Le nombre de ces transformations est, en effet, $(p^{f_0}-1)\, p^{f_0 E(v_{m-1})}$, donc fini), parce que toute autre équation d'Eisenstein définissant K/k est congrue à une des précédentes (mod $\mathfrak{f}_{K/k}$). $S_{K/k}$ sera l'ensemble de toutes les classes (mod $\mathfrak{f}_{K/k}$) contenant les polynômes ainsi formés.

Cette méthode d'ailleurs, au fond, permet de former tous les arbres normaux des équations d'Eisenstein dans k d'un degré n: en effet le conducteur $\mathfrak{f}_{K/k}$ est diviseur de $\mathfrak{P}^{1+\Delta_{m-1}-\Delta_{-1}} = \mathfrak{P}^{1+(w_r-n)+v_{m-1}}$, et si $n = hp^r$, on a, en vertu de la définition des w_i, $w_0 - n = w_0 - w_r \leq r\,E$ et, en vertu, du théorème du § 9 on a $v_{m-1} \leqq \frac{E}{p-1}$, donc $\mathfrak{f}_{K/k}$ est diviseur de $\mathfrak{P}_p^{r+\frac{1}{p-1}}$, donc pour k donné est borné en fonction de n.

Ainsi, par exemple tous les corps K/k de degré hp^r appartiennent aux $S_{K/k}$ définissables (mod p^{r+1}).

C) *Lois de limitation*: Notre théorie donne deux nouvelles lois de limitation:

1° K/k est *galoisien* si, et seulement si son indice canonique satisfait à l'égalité

$$\frac{1}{I} = (K:k).$$

Si K/k est non-galoisien, on a $\frac{1}{I} = (K:k_g) < (K:k)$.

$\frac{1}{I}$ se calcule d'une manière immédiate quand on connaît $S_{K/k}$. Ainsi, ayant formé tous les arbres normaux des K/k de degré n, on peut distinguer ceux d'entre eux auxquels appartiennent des corps galoisiens.

On appelera $\frac{1}{I}$ *l'indice de l'arbre* $S_{K/k}$.

2° Si K/k est *galoisien*, il est *hassien* si, et seulement si $\mathcal{J} = (K:k)$; si K/k n'est pas hassien, $\mathcal{J} < (K:k)$. $\mathcal{J}$ se calcule aussi à partir de $S_{K/k}$.

3° D'ailleurs, la connaissance de $S_{K/k}$ suffit pour former le groupe de TAKAGI de K/k et de décider si K/k est abélien ou non.

D) *Loi d'ordination*: Il est impossible d'en donner une en état actuel de cette théorie. Pourtant, on remarque certaines rélations entre un corps K/k et un de ses sous-corps $\overline{K}/k$ dans le cas où ces deux corps sont *galoisiens*, qui semblent être conséquences d'une telle loi encore inconnue: en effet, soient

$$\theta_0, \theta_1, \ldots, \theta_{m-1} \text{ tous les nombres tels que}$$

a) si $\phi(v_i) = n\theta_i$, v_i soit entier; *b*) $M_{n\theta_i}$ soit $\neq \Omega_{f_0}$, et soient

$$\overline{\theta}_0, \overline{\theta}_1, \ldots, \overline{\theta}_{\overline{m}-1}$$

des nombres analogues pour $\overline{K}/k$. Alors, les résultats de HERBRAND sur les nombres de ramification (voir par exemple ma thèse, chap. III, p. 62–66) montrent que $\overline{\theta}_0, \overline{\theta}_1, \ldots, \overline{\theta}_{\overline{m}-1}$ se trouvent parmi les $\theta_0, \theta_1, \ldots, \theta_{m-1}$, et le théorème que j'ai énoncé à la fin du § 7 sur les rélations entre les $M_q(K/k)$ et les $M_q(\overline{K}/k)$, avec le résultat de ce §, qui donne, quand K/k est galoisien,

$$M_{\Delta_q} = \Gamma^{a_t} U_{r_q}(M_q(K/k)),$$

permettent de montrer que

$$\overline{M}_{\overline{\theta}_i n} \supseteq M_{\theta_i n} \qquad (i = 0, 1, \ldots, m),$$

où $\overline{M}_t$ désigne le module des translations de Ω_{f_0} égal à $\mathfrak{S}_1(\overline{\pi}, t)$, $\overline{\pi}$ étant un élément primitif de $\overline{K}$ d'ordre 1 en $\overline{\mathfrak{P}} = \mathfrak{p}^{\frac{1}{(\overline{K}:k)}}$, et où $\overline{n} = (\overline{K}:k)$.

E) *Loi d'isomorphisme:* Soit $f(x) = x^n + \sum_{t\ n}^{+\infty} \Gamma_t X_t$ une équation d'EISENSTEIN définissant un corps *galoisien* K/k.

Considérons l'ensemble

$$\Omega_{t+1}(f) = \{\Gamma_n = \Gamma_{\phi(0)}, \Gamma_{\phi(1)}, \Gamma_{\phi(2)}, \ldots, \Gamma_{\phi(v_{m-1})} = \Gamma_{\Delta_{m-1}}, \ldots, \Gamma_{\phi(t)}\}$$

où t est assujetti à la seule condition d'être entier et $\geq v_{m-1}$, c'est-à-dire $\phi(t)$ est un entier $\geq \Delta_{m-1}$ arbitraire

Soit $\Omega_{t+1}(K/k)$ l'ensemble des $\Omega_{t+1}(f)$ distincts de toutes les équations d'EISENSTEIN $f = 0$ définissant K/k. Soit Ω_{t+1} l'ensemble des $\Omega_{t+1}(f)$ distincts de tous les équations d'EISENSTEIN de degré n. Désignons par respectivement $\omega_{t+1}(K/k)$, ω_{t+1} le nombre d'éléments de $\Omega_{t+1}(K/k)$, Ω_{t+1}.

Etant donné la structure arborescente régulière de $S_{K/k}$, on a

$$\frac{\omega_{t+1}}{\omega_{t+1}(K/k)} = \frac{p^{f_0}-1}{I_n} \prod_{i=1}^{t} \frac{p^{f_0}}{I_{\phi(i)}} = \prod_{i=0}^{t} \frac{1}{\psi_{\phi(i)}}.$$

Or, si $i > t$, donc, a fortiori, $i > v_{m-1}$, on a $I_{\phi(i)} = p^{f_0}$; et, puisque K/k est galoisien, on a, quand i n'est pas entier, $I_{\phi(i)} = 1$. Donc

$$\prod_{i=0}^{t} \frac{1}{\psi_{\phi(i)}} = \prod_{j=0}^{+\infty} \frac{1}{\psi_j} = \frac{1}{I} = (K:k)$$

et $\frac{\omega_{t+1}}{\omega_{t+1}(K/k)}$ *ne dépend pas de choix de* $\phi(t) \geq \Delta_{m-1}$, *et est égal à* $(K:k)$.

Ceci semble indiquer qu'on peut espérer de pouvoir définir une subdivision de Ω_{t+1} en classes suivant $\Omega_{t+1}(K/k)$, chacune de ces classes ayant $\omega_{t+1}(K/k)$ éléments, et une loi de composition de ces classes, de manière à organiser l'ensemble de ces classes en un groupe isomorphe à $G_{K/k}$.

J'ai l'impréssion que les problèmes de la forme explicite de la loi d'existence, de la loi d'ordination et de la loi d'isomorphisme sont étroitement liés et qu'ils doivent se résoudre en même temps.

F) Les rélations entre les propriétés de $S_{K/k}$ et les propriétés de ramification de K/k établies dans ce § résolvent complètement cette quéstion et comprennent comme résultats partiels dans des cas particuliers tout ce qui à été connu sur les rélations entre le groupe de

TAGAGI et les propriétés de ramification d'un corps abélien ou galoisien, en particulier le Führer-Discriminantensatz de M. HASSE.

d) J'ai pu vérifier que K/*k* étant un corps $\mathfrak{P}$-adique quelconque (donc f n'étant pas forcement 1), la théorie exposée dans ce § 10 (et au § 9) s'applique, à quelques petites complications près, aux équations auxquelles satisfont les nombres π d'ordre 1 en $\mathfrak{P}$ de ces corps. Les complications proviennent surtout de ce que $f(x)$ a dans ce cas f (qui est, en général, > 1) termes d'un même ordre total. D'ailleurs ici les transformations de TSCHIRNHAUSEN ont la forme

$$\pi' \equiv \pi \sum_{i=0}^{+\infty} \gamma_i \pi^i$$

où les γ_i sont des racines $p^F - 1 = p^{f\nu_0} - 1^{\text{èmes}}$ de l'unité ou des zéros, dont $\gamma_0 \neq 0$.

En particulier, tout ce qui a été dit sur la possibilité de généraliser la théorie de corps de classes s'applique à cette catégorie plus générale d'équations, et l'on peut définir l'indice canonique I pour ce cas général de manière à ce qu'on ait encore $I = \frac{1}{(K : k_g)}$. J'exposerai ailleurs cette théorie.

e) La notion des anneaux $W_{a,b}$ est susceptible d'une très large généralisation, et beaucoup des résultats rélatifs aux $W_{a,b}$ peuvent être étendus, convenablement modifiés, aux ces anneaux. En particulier, une généralisation de $W_{a,b}$ dans un des cas le plus immédiats permet de montrer que la théorie des §§ 2, 3, 5, 6, 7, 9, 10 (ainsi que les résultats du § 11 qui suit) s'appliquent, a quelques modifications près, à tous les corps que les algébraïstes de l'école allemande appelent „à valuation discrète" (discret bewertete).

§ 11. — Le développement des nombres $\mathfrak{P}$-adiques en séries des pussances fractionnaires d'un nombre donné d'ordre positif

Soit k un corps de base et soit π un élément algébrique par rapport à k d'ordre *positif*. α étant un élément algébrique par rapport à k, on dira que

$$A(\pi) = \sum_{i=0}^{\lambda \leq +\infty} a_i \pi^{u_i}$$

est un *développement de α par rapport à k suivant les puissances fractionnaires de π* si :

1°. Tout a_i appartient à un surcorps non ramifié k_i de k.

2°. Les u_i sont des fractions rationnelles.

3°. La série $A(\pi)$ converge p-adiquement et sa limite est α.

D'ailleurs, si $\lambda = +\infty$, la première partie de la condition 3°) équivaut à l'égalité

$$\lim_{i \to +\infty} u_i = +\infty,$$

où il s'agit, cette fois, de la convergence ordinaire.

Le dévéloppement précédent s'appellera *normal* (ou, plus précisement, *normal convergent*; *voir plus loin*), si tous les a_i sont des racines de l'unité d'ordre premier à p, et si les u_i forment une suite constamment croissante (au sens strict). Plus généralement, une série p-adique formelle

$$D_\pi(\alpha) = \sum_{i=0}^{\lambda \leq +\infty} \rho_i \pi^{u_i},$$

où les ρ_i sont tous des racines de l'unité d'ordre premier à p, et où les u_i forment une suite de fractions rationnelles croissante au sens strict avec i, s'appellera un *développement normal de α en série de puissances fractionaires de π*, si pour tout j, $0 \leq j < \lambda$, on a

$$\omega\left(\alpha - \sum_{i=0}^{j} \rho_i \pi^{u_i}\right) > u_j \omega(\pi)$$

($\omega(x)$ désigne l'ordre, par exemple en $\mathfrak{p}$, du nombre $\mathfrak{P}$-adique x), et si, de plus, quand $\lambda < +\infty$, on a

$$\sum_{i=0}^{\lambda} \rho_i \pi^{u_i} = \alpha.$$

Si $D_\pi(\alpha)$ converge, il ne peut converger que vers α. Ceci arrive si, et seulement si ou bien $\lambda < +\infty$, ou bien $\lim_{i \to +\infty} u_i = +\infty$. Dans ce cas, en accord avec la définition antérieure, $D_\pi(\alpha)$ sera dit développement normal *convergent* de α. Sinon, il sera dit *divergent*, et alors la suite des u_i convèrge vers une limite finie

$$\lim_{i \to +\infty} u_i = L(\alpha ; \pi) = \frac{1}{\omega(\pi)} \lim_{j \to +\infty} \omega\left(\sum_{i=0}^{j} \rho_i \pi^{u_i}\right) \text{ (21)}.$$

(21) J'ai pensé pendant longtemps que $D_\pi(\alpha)$ converge toujours, et j'ai cru même que cela avait été prouvé. M. CHEVALLEY, dans une conversation que j'ai eue avec lui, a émis un doute a ce sujet, ce qui a été le point de départ de la recherehe qui suit.

Le développement normal (convergent ou divergent) $D_\pi(\alpha)$ *existe toujours*. En effet, soit qu'on ait déjà déterminés les ρ_i et les u_i pour tout i tel que $0 \leq i < j$ $(j \geq 0)$ satisfaisant aux conditions indiquées

Si $\alpha = \sum_{i=0}^{j-1} \rho_i \pi^{u_i}$, posons $\lambda = j-1$ et $D_\pi(\alpha) = \sum_{i=0}^{j-1} \rho_i \pi^{u_i}$. Sinon,

$+\infty > \omega\left(\alpha - \sum_{i=0}^{j-1} \rho_i \pi^{u_i}\right) > u_{j-1}\omega(\pi)$. Donc, si l'on pose

$$u_j = \frac{\omega\left(\alpha - \sum_{i=0}^{j-1} \rho_i \pi^{u_i}\right)}{\omega(\pi)},$$

et si l'on définit ρ_j par la condition qu'il doit être une racine de l'unité d'ordre premier à p satisfaisant à la congruence

$$\rho_j \equiv \frac{\alpha - \sum_{i=0}^{j-1} \rho_i \pi^{u_i}}{\pi^{u_j}} \pmod{\mathfrak{P}^\varepsilon},$$

où $\varepsilon > 0$ est suffisamment petit pour qu'une telle congruence puisse avoir lieu, les ensembles $u_0, u_1, \ldots, u_j$ et $\rho_0, \rho_1, \ldots, \rho_j$ satisfont encore aux conditions voulues, et l'affirmation est prouvée.

Le développement normal de α suivant les puissances fractionnaires de π est *unique*. En effet, supposons qu'il en existe deux différents, soient

$$D_\pi(\alpha) = \sum_{i=0}^{\lambda \leq +\infty} \rho_i \pi^{u_i} \quad \text{et} \quad D'_\pi(\alpha) = \sum_{i=0}^{\lambda' \leq +\infty} \rho'_i \pi^{u'_i}.$$

Alors il existent des i tels qu'on n'ait pas à la fois $\rho_i = \rho'_i$ et $u_i = u'_i$.

Soit i_0 le moindre de ces nombres. Par définition

$$\omega\left(\alpha - \sum_{i=0}^{i_0} \rho_i \pi^{u_i}\right) > u_{i_0}\omega(\pi), \quad \omega\left(\alpha - \sum_{i=0}^{i_0} \rho'_i \pi^{u'_i}\right) > u'_{i_0}\omega(\pi).$$

Donc

$$\omega(\rho_{i_0}\pi^{u_{i_0}} - \rho'_{i_0}\pi^{u'_{i_0}}) = \omega\left(\left[\alpha - \sum_{i=0}^{i_0} \rho'_i \pi^{u'_i}\right] - \left[\alpha - \sum_{i=0}^{i_0} \rho_i \pi^{u_i}\right]\right) > \mathrm{Min}[u'_{i_0}, u_{i_0}].\omega(\pi)$$

Or, ceci n'est possible que si à la fois $u_{i_0} = u'_{i_0}$ et $\rho_{i_0} = \rho'_{i_0}$, contre l'hypothèse sur i_0. L'affirmation est prouvée

Bornons-nous dorenavant au cas, où (π) est l'idéal premier de $k(\pi)$.

Démontrons que dans ce cas l'existence *d'un* développement de α parrapport à k suivant les puissances fractionnaires de π entraîne la convergence de $D_\pi(\alpha)$ (ceci n'a pas toujours lieu quand (π) n'est pas l'idéal premier de $k(\pi)$; par exemple, si k est le corps p-adique rationnel, $\alpha = p$, $\pi = p^2(1+p)$, il existent des développements de α par rapport à k suivant les puissances fractionnaires de π, par exemple $\alpha = p\pi^0$, mais $D_\pi(\alpha)$ diverge et $L(\alpha, \pi) = \frac{p}{2(p-1)}$). En effet, supposons qu'on possède déjà un développement de α

$$A^{(n)}(\alpha) = \sum_{i=0}^{j_n} \rho_i \pi^{u_i} + \sum_{q=0}^{\lambda \leq +\infty} \alpha_q^{(n)} \pi^{u_q^{(n)}}$$

où $u_0 < u_1 < \ldots < u_{j_n} \leq n$, où les ρ_i $(i = 0, 1, \ldots, j_n)$ sont des racines de l'unité d'ordre premier à p, et où, pour tout $q = 0, 1, \ldots$, on a

$$\omega(a_q^{(n)}) + u_q^{(n)}.\omega(\pi) > n.\omega(\pi).$$

Comme la série $A^{(n)}(\alpha)$ convèrge vers α, il n'y a qu'un nombre fini de valeurs u, $n < u \leq n+1$ telles qu'il existent des q, $0 \leq q \leq \lambda$ tels que

$$\omega(a_q^{(n)}) + u_q^{(n)}.\omega(\pi) = u.\omega(\pi),$$

et pour chacune de ces u il n'y a qu'un nombre fini des q, soit $q_1^{(u)}, q_2^{(u)}, \ldots, q_{r_u}^{(u)}$ satisfaisant à cette égalité. $a_q^{(n)}$ étant un nombre d'un surcorps non-ramifié de k, donc, à fortiori, d'un surcorps non ramifié de $k(\pi)$, peut être mis sous la forme d'une série

$$\frac{\omega(a_q^{(n)})}{\pi^{\omega(\pi)}} \sum_{i=0}^{+\infty} a_i^{(n,q)} \pi^i,$$

où les $a_i^{(n,q)}$ sont des racines de l'unité d'ordre premier à p ou des zéros. Soient $u_{j_n+1}, u_{j_n+2}, \ldots, u_{j_{n+1}}$ ceux des u indiqués, rangés dans l'ordre de grandeurs croissantes, qui satisfont à la condition

$$a^{(u)} = \sum_{s=1}^{r_u} a_0^{(n, q_s^{(u)})} \not\equiv 0 \pmod{\mathfrak{p}},$$

et soit ρ_j $(i_n < j \leq i_{n+1})$ la racine de l'unité d'ordre premier à p telle que

$$\rho_j \equiv a^{(u_j)} \pmod{\mathfrak{p}}.$$

Alors

$$\sum_{q=0}^{\lambda \leq +\infty} a_q^{(n)} \pi^{u_q^{(n)}} = \sum_{j=jn+1}^{jn+1} \rho_j \pi^{u_j} + \sum_{j=j\overline{n}+1}^{jn+1} (a^{(u_j)} - \rho_j)\pi^{u_j} + \sum_{\substack{n<u\leq n+1 \\ u\neq u_j\,(jn<j\leq jn+1)}} a^{(u)}\pi^u +$$

$$+ \sum_{i=1}^{+\infty} \sum_{n<u\leq n+1} \left(\sum_{s=1}^{r_u} \alpha_i^{(n,q_s^{(u)})} \right) \pi^{u+i} + \sum_{\substack{0\leq q\leq\lambda \\ q\neq q_s^{(u)}(n<u\leq n+1\,;\,s=1,\ldots,r_u)}} a_q^{(n)} \pi^{u_q^{(n)}}$$

Les quatres dernières séries de la partie droite de cette égalité sont convergentes et ont tous leurs termes de la forme $a\pi^u$, ou a est dans un surcorps non-ramifié de k, et d'ordre $> (n+1).\omega(\pi)$. On n'a qu'à les réunir en une seule série

$$\sum_{q=0}^{\lambda\leq+\infty} a_q^{(n+1)} \pi^{u_q^{(n+1)}},$$

pour avoir un développement de α de forme $A^{(n+1)}(\alpha)$. Quand $n\to+\infty$, $A^{(n)}(\alpha)$ tend vers $D_\pi(\alpha)$, et l'on voit que $D_\pi(\alpha)$ convèrge.

Ces préliminaires établies, étudions les propriétés de $D_\pi(\alpha)$ pour le cas convergent et pour le cas divergent.

Théorème I. *Il existe un nombre* F *tel que pour tout* i *on ait*

$$\rho_i^{p^F} = \rho_i .$$

Démonstration : Supposons que la proposition n'est pas exacte. Soit f_j le moindre entier tel que pour tout $i\leq j$ on ait $\rho_i^{p^{f_j}}=\rho_i$. Alors il existe une infinité des i tels que $f_i\neq f_{i-1}$. Désignons maintenant par k le corps p-adique rationnel. Soit ε_f une racine $p^f-1^{ième}$ primitive de l'unité, et soit d_j le plus petit commun dénominateur de tous les u_i, $i\leq j$. Considérons un i tel que $f_i\neq f_{i-1}$. On a

$$\text{corr.}_{k(\varepsilon_{f_i})} G_{k(\alpha,\varepsilon_{f_i}\,;\,\pi^{\frac{1}{d_i}})/k(\varepsilon_{f_{i-1}}\,;\,\pi^{\frac{1}{d_i}})} = G_{k(\varepsilon_{f_i})/k(\varepsilon_{f_{i-1}})}.$$

Donc, il existe un $\sigma\in G_{k(\alpha,\varepsilon_{f_i},\pi^{\frac{1}{d_i}})/k(\varepsilon_{f_{i-1}},\pi^{\frac{1}{d_i}})}$ tel que $\sigma\pi^{u_j}=\pi^{u_j}$ pour tout $j<i$, et que $\sigma\rho_j=\rho_j^{p^{f_{i-1}}}$, donc $=\rho_j$, si $j<i$, et $\neq\rho_j$, si $j=i$. $\sigma\alpha$ est un conjugué de α. On a $\sigma\alpha=\sum_{j=0}^{i}\sigma\rho_j.\sigma\pi^{u_j}=\sum_{j=0}^{i}\rho_j\pi^{u_j}+$ $+(\rho_i^{p^{f_{i-1}}}-\rho_i)\pi^{u_i}=\alpha+(\rho_i^{p^{f_{i-1}}}-\rho_i)\pi^{u_i}$ $(\text{mod}\ \mathfrak{P}^{u+\varepsilon}=\mathfrak{p}^{u+\varepsilon})$ $(\varepsilon>0)$. Donc $\omega(\sigma\alpha-\alpha)=u_i.\omega(\pi)$. Comme il y a une infinité des i tels que $f_i\neq f_{i-1}$, il y a une infinité de conjugués distincts de α, ce qui est absurde, et le théorème est démontré. C. q. f. d.

Désignons par $\mathfrak{A}_i$ le dénominateur de u_i mis sous la forme d'une fraction irréductible. Posons $\mathfrak{A}_i=\overline{\mathfrak{A}}_i p^{\mathfrak{N}}$, où $\overline{\mathfrak{A}}_i$ est premier à p. Alors on a le

Théorème II. *Il existe un entier* $\overline{\mathfrak{A}}$ *dont tous les* $\overline{\mathfrak{A}}_i (i=0,1,\ldots,\lambda)$ *sont diviseurs.*

Démonstration : Supposons que la proposition ne soit pas exacte. Soit $\overline{d}_i$ le p. p. c. m. de tous les $\overline{\mathfrak{A}}_j$, $j\leq i$; il existe alors une infinité des i tels que $\overline{d}_i\neq\overline{d}_{i-1}$. Considérons un de ces i Soient $\pi_{i-1}=\pi^{\frac{1}{\overline{d}_{i-1}}}$, $\pi_i=\pi^{\frac{1}{\overline{d}_i}}$. On a manifestement, k désignant le corps p-adique rationnel,

$$(k(\rho_0,\rho_1,\ldots,\rho_i\,;\,\pi_i) : k(\rho_0,\rho_1,\ldots,\rho_i\,;\,\pi_{i-1})) = \frac{\overline{d}_i}{\overline{d}_{i-1}} = (k(\pi_2) : k(\pi_{i-1})),$$

donc

$$\text{corr.}_{k(\pi_i)} G_{k(\alpha\,;\,\rho_0,\rho_1,\ldots,\rho_i\,;\,\pi_i\,/\,k(\rho_0,\rho_1,\ldots,\rho_i\,;\,\pi_{i-1})} =$$

$$= \text{corr.}_{k(\pi_i)} G_{k(\rho_0,\rho_1,\ldots,\rho_i\,;\,\pi_i)/k(\rho_0,\rho_1,\ldots,\rho_i\,;\,\pi_{i-1})} = G_{k(\pi_i)/k(\pi_{i-1})}.$$

Donc, η étant une racine primitive $\frac{\overline{d}_i}{\overline{d}_{i-1}}^{ième}$ de l'unité, il existe un $\sigma\in G_{k(\alpha\,;\,\rho_0,\rho_1,\ldots,\rho_i\,;\,\pi_i)/k(\rho_0,\rho_1,\ldots,\rho_i\,;\,\pi_{i-1})}$ tel que

$$\sigma\rho_j=\rho_j\ (j=0,1,\ldots,i)\,;\ \sigma\pi^{u_j}=\pi^{u_j}\ (j=0,1,\ldots,i-1)\,;\ \sigma\pi^{u_i}=\eta\pi^{u_i}\,;$$

donc, puisque $\sigma\mathfrak{P}=\mathfrak{P}$, on a pour un $\varepsilon>0$ convenablement petit

$$\sigma\alpha-\alpha\equiv(\eta-1)\rho_i\pi^{u_i}\ (\text{mod}\,\mathfrak{P}^{u_i+\varepsilon}),$$

c'est-à-dire $\omega(\sigma\alpha-\alpha)=u_i.\omega(\pi)$. $\sigma\alpha$ étant conjugue de α, on voit que α a une infinité des conjugués distincts, ce qui est absurde. La proposition est prouvée.

Théorème III. *Si* $D_\pi(\alpha)$ *convèrge,* ζ_i *est borné, c'est-à-dire il existe un entier* ζ *tel que pour tout* i *on ait* $\zeta_i\leq\zeta$.

Démonstration : Supposons que la proposition ne soit pas vraie. Alors quelque soit l'entier q, il existent des i tels que $\zeta_i\geq q$. Soit i_q le moindre i tel que $\zeta_i\geq q$. Soit que $i_q\neq i_{q+1}$. Alors, dans l'intervalle $\left(u_{i_q},\ u_{i_q}+\frac{E}{p-1}\right)$ ne se trouve qu'un nombre fini des nombres $u_{i_{q'}}$, où $E=\frac{\omega(p)}{\omega(\pi)}$, $q'>q$ et tel que $i_{q'}\neq i_{q'+1}$, parce que $\lim_{q\to+\infty} u_{i_{q'}} =$ $= \lim_{i\to+\infty} u_i = +\infty$. Soit i_{s_q} les plus grand de ces $i_{q'}$. ξ_s désignant

une racine $p^{s\text{ième}}$ primitive de l'unité, on a, h désignant le corps p-adique rationnel, et j_q désignant le plus grand i tel que

$$u_i \leq u_{i_q} + \frac{E}{p-1},$$

$$\operatorname{corr}_{k(\pi^{\overline{d}_{j_q}})} G_{k(\alpha;\rho_0,\rho_1,\ldots,\rho_{j_q};\pi^{\overline{d}_{j_q}})/k(\rho_0,\rho_1\ldots,\rho_{j_q};\pi^{\overline{d}_{j_q}p^{q-1}})} \supseteq$$

$$\supseteq \operatorname{corr}_{k(\pi^{\overline{d}_{j_q}})} G_{k(\rho_0,\rho_1,\ldots,\rho_{j_q};\pi^{\overline{d}_{j_q}})/(\rho_0,\rho_1,\ldots,\rho_{j_q};\pi^{\overline{d}_{j_q}p^{q-1}})} =$$

$$= G_{k(\pi^{\overline{d}_{j_q}})/k(\pi^{\overline{d}_{j_q}p^{q-1}})}.$$

Donc il existe un $\sigma \in G_{k(\alpha;\rho_0,\rho_1,\ldots,\rho_{j_q};\pi^{\overline{d}_{j_q}})/k}$ tel que

$$\sigma\rho_i = \rho_i \ (i = 0, 1, \ldots, j_q)\ ;\ \sigma\pi^{\overline{d}_{j_q}p^{s_q}} = \xi_{s_q-q+1}\,\pi^{\overline{d}_{j_q}p^{s_q}}.$$

Considérons $\rho_i\pi^{u_i}$ $(0 \leq i \leq j_q)$. On a $\zeta_i \leqq s_q$. Donc, si $u_i\bar{d}_{j_q}p^{\zeta_i} = U_i$, on a $U_i \not\equiv 0 \pmod p$ et

$$\sigma(\rho_i\pi^{u_i}) = \xi_{\zeta_i}^{U_i}{}_{-q+1}\,\rho_i\,\pi^{u_i} \qquad \text{si} \qquad \zeta_i \geq q-1$$
$$= \rho_i\pi^{u_i} \qquad \text{si} \qquad \zeta_i \leq q-1.$$

Donc, si $\sigma(\rho_i\pi^{u_i}) \neq \rho_i\pi^{u_i}$, on a

$$\omega_{q,i}\,.\,\omega(\pi) = \omega[\sigma(\rho_i\pi^{u_i}) - \rho_i\pi^{u_i}] = \omega(\xi_{\zeta_i-q+1}-1) + \omega(\rho_i\pi^{u_i}) =$$

$$= \frac{\omega(p)}{(p-1)p^{\zeta_i-q}} + u_i\omega(\pi) = \left(u_i + \frac{E}{(p-1)p^{\zeta_i-q}}\right)\omega(\pi).$$

Donc

1° $\omega_{q,i} - u_i$ ne dépend que de ζ_i.

2° Si q est plus grand que 0, la contribution de p dans le dénominateur de $\omega_{q,i}$ est p^{ζ_i}.

Il en résulte, que si $q > 0$, on a

1° $\omega_{q,i} > \omega_{q,i_{\zeta_i}}$ si $i \neq i_{\zeta_i}$.

2° Si $q' \neq q''$, l'égalité

$$\omega_{q,i_{q'}} = \omega_{q,i_{q''}}$$

ne peut avoir lieu que si $\omega_{q,i_{q'}} = \omega_{q,i_{q''}} = +\infty$ (c'est-à-dire $q' < q$ et $q'' < q$). Ceci posé, choisissons, un $\varepsilon > 0$ assez petit pour que $u_{j_q+1} > u_{i_q} + \frac{E}{p-1} + \varepsilon$; on a

$$\alpha - \sum_{i=0}^{j_q} \rho_i\,\pi^{u_i} \equiv 0 \pmod{\mathfrak{P}^{u_i + \frac{E}{p+1} + \varepsilon}}$$

donc

$$\sigma\alpha - \sum_{i=0}^{j_q} \sigma(\rho_i\pi^{u_i}) \equiv 0 \pmod{\sigma\mathfrak{P}^{u_{i_q} + \frac{E}{p-1} + \varepsilon} = \mathfrak{P}^{u_{i_q} + \frac{E}{p-1} + \varepsilon}}.$$

Or, si $q > 0$ (ou si $E \equiv 0 \pmod p$ et $q \geq 0$)

$$\omega\left(\sum_{i=0}^{j_q}\sigma(\rho_i\pi^{u_i}) - \sum_{i=0}^{j_q}\rho_i\pi^{u_i}\right) = \omega(\pi)\,.\,\operatorname*{Min}_{0\leq i\leq j_q}[\omega_{q,i}] = \omega(\pi)\,.\,\operatorname*{Min}_{q\leq q'\leq s_q}[\omega_{q,i_{q'}}] =$$

$$= \omega(\pi)\,.\,\operatorname*{Min}_{q\leq q'\leq s_q}\left[u_{i_{q'}} + \frac{E}{(p-1)p^{q'-q}}\right].$$

Donc, puisque tous les $i_{q'}$, $q' \geq q$, sont $\geq i_q$, on a

$$\omega(\pi)\,.\,u_{i_q} < \omega\left(\sum_{i=0}^{j_q}\sigma(\rho_i\pi^{u_i}) - \sum_{i\ 0}^{j_q}\rho_i\,\pi^{u_i}\right) \leq \omega(\pi).\left[u_{i_q} + \frac{E}{p-1}\right].$$

Donc, puisque $\sigma\alpha - \alpha \equiv \sum_{i=0}^{j_q}\sigma(\tau_i\pi^{u_i}) - \sum_{i\ 0}^{j_q}\rho_i\,\pi^{u_i} \pmod{\mathfrak{P}^{u_{i_q}+\frac{E}{p-1}+\varepsilon}}$, on a

$$\omega(\pi)\,.\,u_{i_q} < \omega(\sigma\alpha - \alpha) < \omega(\pi)\left[u_{i_q} + \frac{E}{p-1}\right].$$

$\sigma\alpha$ est un conjugué de α. Comme, par hypothèse, il y a une infinité de u_{i_q} distincts et $\lim_{q\to+\infty} u_{i_q} = +\infty$, α a une infinité des conjugués distincts, ce qui est absurde. La proposition est prouvée.

Conséquence : $D_\pi(\alpha)$ convèrge si, et seulement si α se trouve dans un corps de degré fini de la forme

$$k(\rho, \pi^{\frac{1}{D}})$$

où ρ est une racine $p^F-1^{\text{ième}}$ primitive de l'unité (D et F étant deux entiers), et où k est le corps p-adique rationnel.

Nous notérons $D(\alpha;\pi)$ et $F(\alpha;\pi)$ les moindres entiers satisfaisant aux conditions de la conséquence précédente.

π' étant un nombre de $k(\alpha)$ tel que (π') soit l'idéal premier de ce corps, il est evident que $D(\pi';\pi) \equiv 0 \pmod{D(\alpha;\pi)}$.

Théorème IV. *Si $D_\pi(\alpha)$ diverge, on a*

$$\overline{\lim_{i=+\infty}}\ \zeta_i = +\infty,$$

et il existe un q tel que pour tout $q' \geq q$ on ait

$$L(\alpha;\pi) - u_{i_{q'}} \leq \frac{E}{(p-1)p^{q'-q}};$$

si $u_{i_q} < L(\alpha;\pi) - \frac{E}{p-1}$, *il existent des conjugués* $\sigma\alpha$ *de* α *tels que* $u_{i_q} < \frac{\omega(\sigma\alpha-\alpha)}{\omega(\pi)} \leq u_{i_q} + \frac{E}{p-1}$; *on a pour ces conjugués*

$$\frac{\omega(\sigma\alpha-\alpha)}{\omega(\pi)} = \operatorname*{Min}_{q\leq q'\leq s_q}\left(u_{i_{q'}} + \frac{E}{(p-1)p^{q'-q}}\right).$$

DÉMONSTRATION : Si $\overline{\lim_{i=+\infty}}\,\zeta_i = \zeta < +\infty$, α appartient au corps $k\left(\rho, \pi^{\frac{1}{\Delta p^{\zeta}}}\right)$ pour un ρ convenable, donc $D_\pi(\alpha)$ convèrge. Pour qu'il n'existe pas d'une infinité de conjugués de α, il faut, en vertu des raisonnements du théorèmo III, que pour un certain q parmi les $\omega_{q,i_{q'}}(q'\geq q)$ il n'y ait pas d'un nombre qui soit plus petit que tous les autres. Or

$$\lim_{q'\to+\infty}\omega_{q,i_{q'}} = \lim_{q\to+\infty}\left(u_{i_{q'}} + \frac{E}{(p-1)p^{q'-q}}\right) = \lim_{q'\to+\infty} u_{i_{q'}} = L'\alpha;\pi).$$

Donc, $\varepsilon>0$ étant aussi petit que l'on veut, s'il existe un $\omega_{q,i_{q'_0}} \leq L(\alpha;\pi) - \varepsilon$, c'est-à-dire $u_{i_{q'_0}} \leq L(\alpha;\pi) - \frac{E}{(p-1)^{q'_0-q}} - \varepsilon$ il n'y a qu'un nombre fini de $\omega_{q,i_{q'}}$ qui sont $\leq \omega_{q,i_{q'_0}}$, et parmi ces nombres il y a un plus petit que tous les autres. Donc contre l'hypothèse, q ne satisfait pas à la condition indiquée, et l'on doit avoir pour tout $q'\geq q$

$$u_{i_{q'}} \geq L(\alpha;\pi) - \frac{E}{(p-1)^{q'-q}}.$$

Si $u_{i_q} < L(\alpha;\pi) - \frac{E}{p-1}$, on peut trouver un $\varepsilon>0$ suffisemment petit pour que l'intervalle $\left(u_0, u_{i_q} + \frac{E}{p-1} + \varepsilon\right)$ ne contienne qu'un nombre fini des u_i. Des lors en appliquant la même méthode qu'au théorème III, on prouve la seconde partie de la proposition.

Dans ce qui suit posons $\alpha=\pi'$, c'est-à-dire supposons que (α) soit l'idéal du premier du corps $k(\alpha)$. Alors, si $\sigma\pi'$ est un conjugué de π', $\frac{\omega(\sigma\pi'-\pi')}{\omega(\pi')} - 1$ doit être parmi les $v_q(k(\pi')/k)$, et la classe de

$$\rho_0^{\frac{\sigma\pi'-\pi'}{\omega(\sigma\pi'-\pi')}} \pi^{u_0 \frac{\omega(\sigma\pi'-\pi')}{\omega(\pi)}}$$

doit être un élément de $M_q(k(\pi')/k)$. Comparant ceci avec la démonstration des théorèmes I, II, III, IV, on a le

Théorème V. a) *Si* f_j *est le plus petit exposant tel que pour tout* $i\leq j$ *on ait* $\rho_i^{p^{f_j}} = \rho_i$, *et si* $f_j \neq f_{j-1}$,

1°. $\frac{u_j - u_0}{u_0}$ *est un des* $v_q(k(\pi')/k)$;

2° *La classe de* $(\rho_j^{p^{f_j-1}x} - \rho_j)\,\rho_0^{-\frac{u_j}{u_0}}$ $(x=1,2,\ldots,\frac{f_j}{f_{j-1}}-1)$ *est dans le* $M_q(k(\pi')/k)$ *correspondant.*

b) *Si* $\bar{d}_l \neq \bar{d}_{l-1}$,

1°. $\frac{u_l - u_0}{u_0}$ *est un des* $v_q(k(\pi')/k)$;

2°. $(\eta-1)\rho_i\,\rho_0^{-\frac{u_l}{u_0}}$, *où* η *est une racine* $\frac{\bar{d}_l}{\bar{d}_{l-1}}$ *ième arbitraire de l'unité, est dans* $M_q(k(\pi')/k)$ *correspondant.*

c) *Quand* $l>0$, *et si* $D_\pi(\pi)$ *convèrge ou* $u_{i_l} < L(\pi';\pi) + \frac{E}{p-1}$,

1°. $u_{i_{l'_0}} - \frac{E}{(p-1)p^{l'_0-l}} = \operatorname*{Min}_{l\leq l'\leq s_l}\left[u_{i_{l'}} + \frac{E}{p^{l'-l}}\right]$ *existe et est un des* $v(k(\pi')/k)+1$;

2°. *La classe de* $\rho_0^{\frac{-u_{i_{l'_0}} - \frac{E}{(p-1)p^{l'_0-l}}}{u_0}} \pi^{-\frac{E}{(p-1)p^{l'_0-l}}(\zeta_{l'_0-l+1}-1)}\rho_{i_{l'_0}}$ *est dans* $M_q(k(\pi')/k)$ *correspondant.*

Avant d'aller plus loin, donnons une nouvelle démonstration, indépendante des précédentes, de ce que les dénominateurs des $v_q(K/k)$ sont premiers à p. Il suffit de ne donner la démonstration que pour les K/k primitifs. Soit donc π un nombre d'ordre 1 en $\mathfrak{P}$ de K, et soit $\sigma\pi$ un de ses conjugués. En vertu du théorème IV de § 3, si v désigne le seul nombre de ramifisation propre de K/k, et si δ désigne son dénominateur, $\sigma\pi$ se trouve dans $k(\rho, \pi^{\frac{1}{\delta}})$, où ρ est une racine de l'unité d'ordre convenable premier à p. Donc, $D_\pi(\sigma\pi)$ convèrge, et on peut écrire

$$D_\pi(\sigma\pi) = \pi + \rho_1\pi^v + \rho_2\pi^{\frac{U_2}{\delta}} + \rho_3\pi^{\frac{U_3}{\delta}} + \ldots$$

où $U_2, U_3, \ldots$ sont entiers; supposons que $\delta \equiv 0 \pmod p$. Soit p^q, $q>0$, la contribution de p dans δ. Alors, on a $u_{i_1} = u_{i_2} = \cdots = u_{i_q} = v$ et $\zeta = q$. On a, d'autre part, si $\mathfrak{R}$ désigne le corps p-adique rationnel

$$\operatorname{corr} G_{\mathfrak{R}(\pi^{\frac{1}{\delta}})\,k(\pi^{\frac{1}{\delta}})/k(\pi^{\frac{1}{\delta}})} = G_{\mathfrak{R}(\pi^{\frac{1}{\delta}})/\mathfrak{R}(\pi^{\frac{1}{\delta}})}^{p^q}.$$

On en tire facilement que dans

$$G_{k(\sigma\pi,\,\pi^{\frac{1}{\delta}},\,\rho)/k}$$

il y a un élément σ tel que $\sigma\rho^i = \rho_i$ pour tout i, et que $\sigma\pi^{\frac{1}{\delta}} = \xi_0\pi^{\frac{1}{\delta}}$;

De lors, on voit qu'il existe un conjugué de $\sigma\pi$ par rapport à k, donc aussi un conjugué de π par rapport à k, soit $\sigma'\pi$, tel que

$$u_1 = v < \frac{\omega(\sigma'\pi - \sigma\pi)}{\omega(\pi)} \leq u_1 + \frac{E}{p-1} = v + \frac{E}{p-1} < +\infty$$

c'est-à-dire $\sigma'\pi \neq \sigma\pi$ et $\beta_0(\sigma') = \beta_0(\sigma)$. Or, si $\beta_0(\sigma') = \beta_0(\sigma)$, On a $\sigma_1 \in \sigma V_{K/k}^{(1)} = \sigma.1_K = \{\sigma\}$ et on a une contradiction qui prouve la proposition.

Combinons le fait que les $v_q(K/k)$ ont leurs dénominateurs premiers à p et les théorèmes VI et VII de § 9 avec le théorème V de ce paragraphe. On a les

Théorème VI. a) *Si* $D_\pi(\pi')$ *est convergent ou si* $u_i < L(\pi';\pi) - \frac{E}{p-1}$, $\frac{u_i}{u_0}$ *a le dénominateur premier à* p.

b) *Si* $f_i \neq f_{i-1}$ ou $\bar{d}_i \neq \bar{d}_{i-1}$, $\frac{u_i}{u_0}$ *a le dénominateur premier a* p.

Démonstration : En effet, soit ξ le plus grand nombre tel que 1° si $D_\pi(\pi')$ convèrge, il existe i_ξ 2°. si $D_\pi(\pi')$ diverge, $u_{i_\xi} < L(\pi';\pi) - \frac{E}{p-1}$.

Alors, dans le premier cas $s_\xi = \xi$, donc

$$\frac{1}{u_0} \operatorname*{Min}_{\xi \leq q' \leq \xi} \left[u_{i_{q'}} + \frac{E}{(p-1)p^{q'-\xi}} \right] - 1 = \frac{1}{u_0} \left[u_{i_\xi} + \frac{E}{p-1} \right] - 1,$$

est un nombre de ramification de K/k. La contribution de p dans le dénominateur de ce nombre est la même dans celui de $\frac{u_{i_\xi}}{u_0}$, donc, le dénominateur de $\frac{u_{i_\xi}}{u_0}$ est premier à p. Comme le dénominateur de tout u_i se divise par une puissance de p moindre ou égale à p^ξ, les $\frac{u_i}{u_0}$ ont leurs dénominateurs premiers à p. Dans le second cas

$$\frac{1}{u_0} \operatorname*{Min}_{\xi \leq q' \leq s_\xi} \left[u_{i_{q'}} + \frac{E}{(p-1)p^{q'-\xi}} \right] - 1$$

est un $v_q(K/k)$. Or ce nombre est égal à un $\frac{1}{u_0}\left[u_{i_{q'}} + \frac{E}{(p-1)p^{q'-\xi}} \right]$ pour un $q' \geq \xi$. La coniribution de p dans le dénominateur de ce nombre est la même que dans celui de $\frac{u_{i_{q'}}}{u_0}$, ou que dans $\frac{1}{p^{q'} u_0}$. D'où il suit encore le même résultat pour tous les $u_i \leq u_{i_{q'}}$ et, *a fortiori* $< L(\pi';\pi) - \frac{E}{p-1}$. Enfin, si $f_i = f_{i-1}$ ou $\bar{d}_i = \bar{d}_{i-1}$, $\frac{u_i}{u_0}$ est un $v_q(K/k)$, d'où suit *b)*.

Conséquence 1 : Si $\omega(\pi') = \omega(\pi)$, ou si, plus généralement $\frac{\omega(\pi')}{\omega(\pi)} \equiv 0 \pmod{p}$, on a ce fait remarquable que le développement de π' ne contient que les puissances de π dont le dénominateur est premier à p quand ce développement convèrge. Donc, si $\omega(\pi') = \omega(\pi)$. $D_\pi(\pi')$ convèrge si, et seulement si $V_{k(\pi,\pi')/k(\pi)} = \{1_{k(\pi,\pi')}\}$ (k étant le corps rationnel).

Conséquence 2 : $K^\bullet/k$ étant le corps de Galois de K/k, tous les $D_\pi(\sigma\pi)$ ($\sigma \in G_{K/k}$) convergent si, et seulement si $V_{K^\bullet/K} = \{1_{K^\bullet}\}$.

En effet, si tous les $D_\pi(\sigma\pi)$ convergent, puisque $\omega(\sigma\pi) = \omega(\pi)$, ces développements ne contiennent que des puissances de π dont les exposants sont premiers à p. Donc $K^\bullet = k(\{\sigma\pi\}_{\sigma \in G_{K/k}})$ est de la forme $k(\rho, \pi^{\frac{1}{D}})$, où D est premier à p et $T_{K^\bullet/K}$ est d'ordre D, donc $V_{K^\bullet/K} = \{1_{K^\bullet}\}$. Inversément, si $V_{K^\bullet/K} = \{1_{K^\bullet}\}$, on a, en vertu du théorème de Hensel, que $K^\bullet$ s'obtient en adjoignant à K une racine de l'unité d'ordre premier à p et $\sqrt[r-1]{\pi}$, et les $\sigma\pi$ étant dans ce corps, $D_\pi(\sigma\pi)$ convergent.

Conséquence 3 : (π') étant l'idéal premier de $k(\alpha)$, la contribution de p dans $D(\alpha;\pi)$ ne depasse pas celle de p dans $\frac{\omega(\pi)}{\omega(\pi')}$.

Conséquence 4 : $u_{i_\xi} = u_0$; si $\xi > 0$, $\frac{E}{p-1}, \frac{E}{(p-1)p}, \ldots, \frac{E}{(p-1)p^{\xi-1}}$ sont les nombres de ramification de K/k, s'ils ne dépassent pas $L(\pi';\pi) - u_0$.

En effet, puisque le dominateur de $\frac{u_{i_\xi}}{u_0}$ est premier à p, le dominateur de u_0 se divise par p^ξ, denc $u_{i_\xi} \leq u_0$, c'est-à-dire $u_{i_\xi} = u_0$. D'ailleurs dans le second cas on a pour la même cause $u_{i_\xi} = u_0$, c'est-à-dire $q' = \xi$. En faisant succésivement $q = 1, 2, \ldots, \xi$, on trouve, si $u_j + \frac{E}{(p-1)p^{q-1}} < L(\pi';\pi)$, qu'il existe un conjugué $\sigma\pi'$ de π' tel que $\frac{\omega\left(\frac{\sigma\pi' - \pi'}{\pi'}\right)}{\omega(p)} = \frac{1}{(p-1)p^{q-1}}$, ce qui prouve l'affirmation.

Théorème VII. *Si* $f_i \neq f_{i-1}$ *ou si* $\bar{d}_i \neq \bar{d}_{i-1}$, *on a* $u_i - u_0 \leq \frac{E}{p-1}$.

Démonstration : En effet, en vertu du théorème VI du § 9, on a

$$v_q(k(\pi')/k) \leq \frac{\omega(p)}{(p-1)\omega(\pi')\, n_q(k(\pi)/k)} \leq \frac{\omega(p)}{(p-1)\,\omega(\pi')}.$$

Donc $u_i - u_0 = \frac{\omega(\pi')}{\omega(\pi)} \cdot v_q(k(\pi')/k) \leq \frac{\omega(p)}{\omega(\pi)} \frac{1}{p-1} = \frac{E}{p-1}$.

C. q. f. d.

Soit $\sigma \in G_{K/k}$. Soit $D_\pi(\sigma\pi) = \sum_{i=0}^{\lambda \leq +\infty} \rho_i \pi^{u_i}$. Définissons à côté d'indices d'irrégularité de première espèce deux autres espèces de tels indices.

Définition 1 : On appelera *indice d'irrégularité de seconde espèce de* σ, et on notera $\theta(\sigma)$, le moindre exposant u_i, diminué d'une unité, dont le dominateur se divise par p, c'est-à-dire $u_i - 1$.

Si $\theta_0, \theta_1, \ldots, \theta_{m'} = +\infty$ sont les indices d'irrégularité de seconde espèce écrits dans l'ordre des grandeurs croissantes, θ_i s'appelera *le i-ème nombre d'irrégularité de seconde espèce de* K/k.

On voit que $\theta(\sigma) = +\infty$ si, et seulement si $D_\pi(\sigma\pi)$ convèrge. On prouve facilement, par une méthode analogue à celle pour les nombres de ramification et pour les nombres d'irrégularité de première espèce, que l'ensemble des σ tels que $\theta(\sigma) \geq \theta_i$ est un *hypergroupe*, soit $\Phi^{(i)}$, qui sera appelé l'hypergroupe d'irrégularité de seconde espèce d'ordre i de K/k. On voit, d'après le théorème V, que le facteur premier à p du dénominateur de $\theta(\sigma)$ doit être diviseur du p. p. c. m. des dénominateur de tous les $v_q < \theta(\sigma)$. Il est possible de prouver que tous les $\theta_i < +\infty$ sont $< v_{m-1}(K/k) \leq \frac{E}{p-1}$. Comme, certainement $\theta(\sigma) \neq 0$, ou doit avoir $L(\sigma\pi ; \pi) \leq 1 + \theta(\sigma) + \frac{E}{p-1} \leq \frac{2E}{p-1} + 1$.

Définition 2 : On appelera *indice d'irrégularité de troisième espèce* $\tau(\sigma)$ de σ le nombre $L(\sigma\pi ; \pi) - 1$.

$\tau_0, \tau_1, \ldots, \tau_{m''} = +\infty$ étant les $\tau(\sigma)$ distincts de tous les $\sigma \in G_{K/k}$, écrits dans l'ordre de grandeurs croissantes, τ_i s'appelera *le i-ième nombre d'irrégularité de troisième espèce de* K/k.

On ne sait rien sur la nature arithmétique des τ_i[22]. La question reste ouverte, également, si l'ensemble de tous les σ tels que $\tau(\sigma) \geq \tau_i$ est un hypergroupe ? On a, par contre, comme on a vu, l'inégalité.

$$\tau_i \leq \frac{2E}{p-1}, \quad \text{si} \quad \tau_i \neq \infty.$$

$\tau(\sigma) = +\infty$ si, et seulement si $D_\pi(\sigma\pi)$ convèrge, c'est-à-dire si, et seulemet si $\theta(\sigma) = +\infty$. Et, en général, si la contribution de p dans le dénominateur de $\theta(\sigma)$ est p^ξ,

$$\tau(\sigma) - \theta(\sigma) \leq \frac{E}{(p-1)p^{\xi-1}}.$$

(22) En particulier, on ne sait pas s'ils peuvent être irrationnels.

La question très intéressante est la suivante : Trouver une forme normale en laquelle on peut en peut transformer $D_\pi(\sigma\pi)$ par les transformations de Tschirnhausen ? Elle est extrêmement difficile dans le cas général. On peut prouver par des méthodes du genre de celles de M. Fueter [23] que si σ est un automorphisme, la connaissance des $D_\pi(\sigma\pi) \pmod{\mathfrak{P}^{1+v_{m-1}}}$ donc, a fortiori, $\pmod{\mathfrak{P}^{1+\frac{E}{p-1}}}$ définit $D_\pi(\sigma\pi) \pmod{\mathfrak{P}^{1+E-(p-2)v(\sigma)}}$. Mais je n'ai pu faire la détermination effective de cette liaison que dans des cas les plus simples, et ceci pas des calculs assez compliqués. Il est d'ailleurs probable que le fait indiqué se produit pour tous les σ tels que $\Theta(\sigma) = +\infty$, c'est-à-dire tels que $D_\pi(\sigma\pi)$ converge.

Je me borne à indiquer un seul résultat que j'ai obtenu dans cette voie, et que j'ai, d'ailleurs, enoncé déjà dans ma seconde note sur la théorie de la ramification des idéaux aux C. R. de 8 juillet 1937.

Si $\sigma \in V_{K/k}$ est un automorphisme de K/k (non égal à 1_K), si $v = v(\sigma)$ et si $\bar{v} = \text{Min}\,(v(\sigma^s), E + v)$, on peut trouver une racine du d'unité d'ordre premier à p $\rho \in \beta(\sigma)$ et un nombre π d'ordre 1 de $\mathfrak{P}$ de K tels que

$$\sigma\pi - \pi(1 - v\rho\pi)^{-\frac{1}{v}} \text{ soit d'ordre } 1 + \bar{v} - (p-1)v \text{ en } \mathfrak{P}$$

. . . . . .

On forme effectivement $D_\pi(\alpha)$ par la méthode tout-à-fait analogue à celle de Puiseux pour les fonctions algébriques, en se servant du polygône de Newton-Puiseux-Ore. Cette question est déjà exposée, au fond, dans les travaux de M. Ore, auxquels nous renvoyons le lecteur. Les différences entre les nombres $\mathfrak{P}$-adiques et les fonctions algébriques ne résident pas dans le procédé de construction du développement, mais uniquement dans les caractères de convergence du développement construit [24].

(23) *Vierteljahrschr. d. naturf. Ges. in Zürich*, 1917, p. 67 – 72.

(24) Les §§ 1 et 2 et une partie du § 3 de ce travail sont contenus, à quelques légères différences de démonstrations près, dans le chapitres I, II et IV de ma thèse (*Sur la théorie de ramification des idéaux de corps de nombres algébriques, Mémoires de l'Acad. de Belgique*, t. IX, fasc. IV, p. 1 — 110). Une autre démonstration des théorèmes VI et VII du § 9 et la démonstration de la p. 187 du § 11 s'y trouvent aussi. Le reste du présent travail est inédit aussi bien du point de vue des démonstrations que de celui des résultats (sauf, bien entendu, le § 8, qui rélève des travaux de M. Ore).

ERRATA

VOL. VII

Pag. 153 note (4) dernière phrase, *au lieu de* domaine borné simplement connexe *lire* domaine borné plan.

„ 154 ligne 9, *au lieu de* mesure angulaire tendant vers 0 *lire* mesure angulaire ne tendant pas vers zéro.

VOL. XIII

Pag. 16 ligne 5 *au lieu de* Warszava *lire* Warszawa

„ 16 dernière ligne *au lieu de* $f(x)$ *lire* $|f(x)|$

„ 73 ligne 19 *au lieu de* $(C \in G)$ lire $(C \subset G)$

„ 74 „ 5 *au lieu de* dans le K/k *lire* dans (de) K/k

„ 74 „ 9 *au lieu de* $(K|k)$ *lire* $(K : k)$

„ 75 „ 14 *au lieu de* V *lire* $\mathfrak{O}$

„ 75 „ 15 *au lieu de* v *lire* $\mathfrak{o}$

„ 75 *ajouter* après la ligne 18 : ϕ étant une forme dans K, au sens de KRONECKER, son contenu sera désigné par $\overline{\phi}$

„ 76 ligne 1, *au lieu de* K, *lire* : H, quelques soient $a, b \in H$

„ 76 „ 15 *au lieu de* K et K′ *lire* H et H′

„ 78 lignes 6 et 8 *au lieu de* $C \supset G$ *lire* $C \subset G$

„ 77 ligne 14 *au lieu de* soit G/g *lire* soit C/g

„ 77 „ 23 *au lieu de* de classes *lire* de l'hypergroupe de classes

„ 78 „ 15 *au lieu de* $\gamma_1 G$ *lire* $\gamma_1 g$

„ 78 „ 15 *au lieu de* $\gamma_2 G$ *lire* $\gamma_2 g$

„ 78 „ 20 *au lieu de* H/h *lire* H/h

„ 80 „ 2 *au lieu de* $\mathrm{gen}_{k^*}\mathfrak{o}$ *lire* $\mathrm{gen}_{K^*}\mathfrak{o}$

„ 80 „ 15 *au lieu de* gen_k *lire* gen_K

„ 80 „ 21 *au lieu de* $G_{K^*/K'}$ *lire* $G_{K^*/k'}$

„ 80 „ 24 *au lieu de* $G_{K^*/\overline{k}}$ *lire* $G_{K^*/\overline{K}}$

„ 83 „ 2 *au lieu de* $\mathfrak{o}^*\mathfrak{o}_2^{*\pi}$ *lire* $\mathfrak{o}_1^*\mathfrak{o}_2^{*\pi}$

„ 84 „ 17 *il faut ajouter* (mod $\mathfrak{P}$)

„ 86 „ 17 *au lieu de* i_K *lire* i_k

„ 86 „ 18 *au lieu de* $\mathfrak{o}^*\mathfrak{o}^{*-1}$ *lire* $\mathfrak{o}^*\mathfrak{o}_1^{*-1}$

„ 86 „ 20 *au lieu de* $\beta_{-1}(\mathfrak{o}_1, \mathfrak{o}_2)$ *lire* $\beta_{-1}(\mathfrak{o}_1\mathfrak{o}_2)$

„ 87 „ 28 *au lieu de* n_{-1} *lire* r_{-1}

„ 87 „ 29 *au lieu de* r_- *lire* r_{-1}

Pag. 88 ligne 6 *au lieu de* $= AV_{K^*}$, *lire* $= AV_K$,

„ 88 „ 19 *au lieu de* si *lire* Si

„ 88 „ 29 *au lieu de* $=$ *lire* $\equiv$ (2 fois)

„ 89 „ 9 *au lieu de* $\mathfrak{p}\mathfrak{p}^{-n-1(K^*/K)}$ *lire* $\mathfrak{p}\mathfrak{p}^{*-n_{-1}(K^*/K)}$

„ 90 „ 8 *au lieu de* $\equiv\gamma(\mathfrak{o}_1$. *lire* $\equiv \gamma(\mathfrak{o}_1^*)$.

„ 90 „ 10 *au lieu de* $\mathfrak{o}_1$ *lire* $\mathfrak{o}_1^*$

„ 90 „ 19 *au lieu de* $\mathfrak{o}_*$ *lire* $\mathfrak{o}_0^*$

„ 90 „ 21 *au lieu de* est *lire* , est

„ 90 „ 25 *au lieu de* , $M^{(\pi)}(K/k)$ *lire* $M^{(\pi_0)}(K/k)$

„ 91 „ 4 *au lieu de* soit *lire* soient

„ 91 „ 20 *au lieu de* $\beta_q^{(\pi_1)}(\mathfrak{o})$ *lire* $\beta_q^{(\pi_0)}(\mathfrak{o})$

„ 91 „ 20 *au lieu de* le même *lire* un même

„ 92 „ 17 *au lieu de* est *lire* et

„ 92 „ 20 *au lieu de* la même *lire* le même

„ 92 „ 4 *au lieu de*] — *lire*] =

„ 94 „ 11 *au lieu de* n'existe de *lire* n'existe pas de

„ 94 „ 17 *au lieu de* $(K|k)_{-2} = K/k$, *lire* $(K|k)_{-2} = k/k$,

„ 95 „ 5 *au lieu de* , et je la fais *lire* , et je le fais

„ 95 „ 11 *au lieu de* $T = \{1_K\}$, *lire* $T_K = \{1_K\}$,

„ 95 „ 20 *au lieu de* $\mathrm{Si}\,(K/k)_0 / (K/k_{-1})$, *lire* $K/k = (K/k)_0 / (K/k)_{-1}$,

„ 96 „ 19 *au lieu de* Donc, si $\mathfrak{o}'_1 \neq \mathfrak{o}$, *lire* Donc, si $\mathfrak{o}_1 \neq \mathfrak{o}$,

„ 96 „ 20 *au lieu de* quand $\mathfrak{o}'_1 \neq \mathfrak{o}$ *lire* quand $\mathfrak{o}_1 \neq \mathfrak{o}$,

„ 96 „ 28 *au lieu de* s *lire* si

„ 97 „ 15 *au lieu de* $G_K = \overset{(0)}{V}$ *lire* $G_K = \overset{(0)}{V}_K$

„ 98 „ 3 *au lieu de* quand $\mathfrak{o}'_1 \neq \mathfrak{o}$, $\dfrac{\mathfrak{o}'_1\pi - \pi}{\pi\pi_0^{Dv}} - \rho(\mathfrak{o}) \equiv \equiv 0$

lire quand $\mathfrak{o}_1 \neq \mathfrak{o}$, $\dfrac{\mathfrak{o}_1\pi - \pi}{\pi\pi_0^{Dv}} - \rho(\mathfrak{o}) \equiv \equiv 0$

„ 98 „ 8 *au lieu de* $n_{-1}(K^*/k)$ *lire* $n_{-1}(K^*/K)$

„ 98 „ 31 *au lieu de* (cas *lire* (c ır

„ 99 „ 6 *au lieu de* $\in \dfrac{\beta^{(\pi_0)}(\mathfrak{o}_2)}{\varepsilon}$ conjugué *lire* $\in \dfrac{\beta_0^{(\pi_0)}(\mathfrak{o}_2)}{\varepsilon}$ est conjugué

„ 99 „ 12 *au lieu de* autre p *lire* autre que p

„ 99 „ 22 *au lieu de* à K lui-même *lire* à K que lui-même

„ 100 „ 22 *au lieu de* $\Omega_{a,b}$ *lire* $W_{a,b}$

„ 101 „ 25 *au lieu de* $(z_a\lambda)_n = \lambda_n^{p-a}$ *lire* $(z_a\lambda)_n = \lambda_n^{p^a}$

„ 101 „ 27 *au lieu de* $\lambda_n^{p-a} = \lambda_n$ *lire* $\lambda_n^{p^a} = \lambda_n$

„ 102 „ 5 *au lieu de* $W_{(a,b),\,m(a,b)}$ *lire* $W_{m(a,b),\,(a,b)}$

„ 104 „ 8 *au lieu de* $\beta\lambda = \lambda\beta$ *lire* $\beta\lambda = \lambda\beta'$

„ 104 „ 15 *au lieu de* $\mu \varepsilon W_{m(a,b),\,(a,b)}$ *lire* $\mu \in W_{m(a,b),\,(a,b)}$

„ 104 „ 20 *au lieu de* éléments *lire* des éléments

„ 105 „ 17 *au lieu de* $\overleftarrow{\mathfrak{D}}(\mathfrak{R}, \mathfrak{C}$. *lire* $\overleftarrow{\mathfrak{D}}(\mathfrak{R}, \mathfrak{C})$.

„ 105 „ 21 *au lieu de* $\overleftarrow{\mathfrak{M}}(\mathfrak{R}', \mathfrak{C})$. $\overrightarrow{\mathfrak{D}}\mathfrak{R}, \mathfrak{C}')$; *lire* $\overleftarrow{\mathfrak{M}}\,\mathfrak{R}', \mathfrak{C}')$. $\overrightarrow{\mathfrak{D}}(\mathfrak{R}, \mathfrak{C})$;

„ 106 „ 1 *au lieu de* $\sum_{q=0}^{s} \alpha_{iq}\lambda_i = 0$ *lire* $\sum_{i=0}^{s} \alpha_{iq}\lambda_i = 0$

Pag 106 ligne 18 *au lieu de* $\lambda \quad \lambda''\lambda'$; *lire* $\lambda = \lambda''\lambda'$;

„ 107 „ 12 *au lieu de* $\nu[\mathfrak{M}\lambda,\ \mathfrak{M}_i)]$ *lire* $\nu[\mathfrak{M}(\lambda,\ \mathfrak{M}_i)]$

„ 107 „ 13 *au lieu de* $\mathfrak{M}(\lambda\ \mathfrak{M}_i, \lambda^{(\omega)})$. *lire* $\mathfrak{M}(\lambda, \mathfrak{M}_i, \lambda^{(\omega)})$

„ 107 „ 14 *au lieu de* $\mathfrak{M}(\lambda\ \mathfrak{M}_i)$, *lire* $\mathfrak{M}(\lambda, \mathfrak{M}_i)$,

„ 109 „ 17 *au lieu de* $\neq 0$. *lire* $\neq 0$).

„ 113 „ 2 *au lieu de* $\mu'\mu'' \ldots \mu^{s(\lambda)}$ *lire* $\mu'\mu'' \ldots \mu^{[s(\lambda)]}$

„ 114 „ 11 *au lieu de* et les *lire* et avec les

„ 117 „ 19 *au lieu de* cet idéal *lire* cet idéal

„ 118 „ 15 *au lieu de* Ω_ψ *lire* Ω'_ψ

„ 119 „ 5 *au lieu de* on *lire* ou

„ 120 „ 4 *au lieu de* et les éléments de $W_{b,a}$

lire et les ensembles d'éléments associés de $W_{a,b}$

„ 122 „ 29 *au lieu de* $\}_{\alpha\in\Omega'_a}$, $i=0, 1, \ldots, n-1=$

lire $\}_{\alpha\in\Omega'_a}$, $i=0, 1, \ldots, n \quad 1 =$

„ 122 „ 31 *au lieu de* $\}_{\alpha\in\Omega'_a}$, $i=0, 1, \ldots, n-1$,

lire $\}_{\alpha\in\Omega'_a}$, $i=0, 1, \ldots, n-1$

„ 123 „ 18 *au lieu de* théorème XI, *lire* les théorèmes XI,

„ 123 „ 18 *au lieu de* et théorème *lire* et le théorème

„ 123 „ 19 *au lieu de* $Q_0, Q_1, \ldots, Q$ *lire* $Q_0, Q_1, \ldots, Q_s$

„ 127 „ 26 *au lieu de* au-dessous *lire* au-dessus

„ 128 „ 2 *au lieu de raeines lire racines*

„ 128 „ 7 *au lieu de* est sur *lire est sur*

„ 128 „ 14 *au lieu de* $u_j = s_j - (n-i)\alpha_j$ *lire* $u_i = s_i - (n-i)\alpha_i$

„ 128 „ 16 *au lieu de* $s_{i_j} + i_j\alpha_{i_j}$ *lire* $s_{i_j} + i_j\alpha_j$

„ 128 „ 17 *au lieu de* auquelle *lire* à laquelle

„ 128 „ 18 *au lieu de* la lemme *lire* le lemme

„ 128 „ 29 *au lieu de* $\sum_{=i_j}^{i_{j-1}}$ *lire* $\sum_{i=i_i}^{i_{j-1}}$

„ 129 „ 11 *au lieu de le lire* , *le*

„ 131 „ 21 *au lieu de* es *v lire* les v_q

„ 132 „ 19 *au lieu de* $\theta_{i,x} - \theta_p$ *lire* $\theta_{i,x} - \theta_{p^u,x}$

„ 134 „ 2 *au lieu de* est *lire* il est

„ 134 „ 18 *au lieu de* si *lire* Si

„ 134 „ 21 *au lieu de* $w_{i_q} = \mathrm{Min}\,[\theta_{0,x} + t_{n-x}]$ *lire* $w_{i_q} = \mathrm{Min}\,[\theta_{0,x} + t_{n-x}]$

$x \equiv\!|\equiv 0 \pmod{p^{u+1}}$ $\quad x \equiv\!|\equiv 0 \pmod{p^{i_q+1}}$

„ 134 „ 22 *au lieu de* $x \equiv 0 \pmod{p^u}$ *lire* $x \equiv 0 \pmod{p^{i_q}}$

„ 135 „ 24 *au lieu de* au au-dessous *lire* ou au-dessous

„ 136 „ 21 *au lieu de* $\left(\sum_{t=0}^{s_q} \beta_{i_t}^{(q)} \xi^{p^{i_t^{(q)}} - j_q+1}\right)^{p^{j_q}+}$

lire $\left(\sum_{t=0}^{s_q} \beta_{i_t}^{(q)} \xi^{p^{i_t^{(q)}} - j_q+1}\right)^{p^{j_q+1}}$

Pag. 137 ligne 2 *au lieu de* $\sum_{t=0}^{s_q} \beta_{i_t^{(q)}}^{p^{j_q+1}} \xi^{i_t^{(q)}}$ *lire* $\sum_{t=0}^{s_q} \beta_{i_t^{(q)}}^{p^{j_q+1}} \xi^{p^{i^{(q)}}}$

„ 137 „ 28 *au lieu de* auquelle *lire* à laquelle

„ 138 „ 25 *au lieu de* $w_{j_{q\ 1}} - w_{iq} \equiv w_{j_{q\ 1}}$ *lire* $w_{j_{q+1}} - w_{j_q} \equiv w_{iq+1}$

„ 140 „ 21 *au lieu de* $\sum_{t=n+1}^{+\infty} \Gamma_t \overline{\pi}^{\mathrm{E}\left(\frac{t}{n}\right)}\ {}_t\ x^{n\mathrm{E}\left(\frac{t}{n}\right)}$

lire $\sum_{t=n+1}^{+\infty} \Gamma_t \overline{\pi}^{\mathrm{E}\left(\frac{t}{n}\right)}\ x^{t-n\mathrm{E}\left(\frac{t}{n}\right)}$

„ 141 „ 7 *au lieu de* $x\alpha(x) = x\sum_{i=0}^{+\infty}\gamma_i x$, *lire* $x\alpha(x) = x\sum_{i=0}^{+\infty}\gamma_i x^i$

„ 141 „ 14 *au lieu de* ... $\pi'\pi''^{i-1} + \pi'')$ *lire* $\ldots + \pi'\pi''^{i-1} + \pi''^i)$.

„ 141 „ 15 *au lieu de* ... $\pi'\pi''^{i-1} + \pi''))$ *lire* $\ldots + \pi'\pi''^{i-1} + \pi''^i))$

„ 141 „ 19 *au lieu de* $\pi \sum_{i=0}^{+\infty}\gamma_i\pi^i$ *lire* $\pi = \pi \sum_{i=0}^{+\infty}\gamma_i\pi^i$

„ 143 „ 11 *au lieu de* $= x^n + \sum_{t=n}^{+\infty} \Gamma^{(t)}X_t =$ *lire* $= x^n + \sum_{t=n}^{+\infty} \Gamma_t^{(t)}X_t =$

„ 143 „ 12 *au lieu de* $\Gamma_i = \Gamma_i^{(t)}$ *lire* $\Gamma_i' = \Gamma_i^{(t)}$

„ 143 „ 13 *au lieu de* subsistuant *lire* substituant

„ 143 „ 14 *au lieu de* . 2. *lire* ; 2^0.

„ 143 „ 25 *au lieu de* $f_2(\alpha(x))$ *lire* $f_2(x\alpha(x))$

„ 144 „ 6 *au lieu de* das *lire* des

„ 144 „ 8 *au lieu de* $\frac{f_1(\pi_1)}{\pi^t}$ *lire* $\frac{f_1(\pi_4)}{\pi_1^t}$

„ 144 „ 30 *au lieu de* $\equiv -1)^n$ *lire* $\equiv (-1)^n$

„ 144 „ 33 *au lieu de* $\xi = \gamma^1 \| {}_i\gamma_\tau$ *lire* $\xi = \gamma^t = \gamma^\tau$.

„ 145 „ 3 *au lieu de* $\sum_{i=n}^{t-0} \Gamma_i x_i$ *lire* $\sum_{i=\ldots}^{t-1} \Gamma_i X_i$

„ 145 „ 27 *au lieu de* $F_{\Gamma_n,\Gamma_{n+1},\ldots,\Gamma_{t-1};\ t,\ A}(y_t\ \Gamma_n,\ \Gamma_{n+1},\ldots,\Gamma_{t-1};\ A;\Gamma))$

lire $F_{\Gamma_n,\Gamma_{n+1},\ldots,\Gamma_{t-1};\ t,\ A}(y_t(\Gamma_n,\ \Gamma_{n+1},\ldots,\Gamma_{t-1};\ A;\Gamma))$

„ 145 „ 30 *au lieu de* $F_{\Gamma_n,\Gamma_{n\ 1},\ldots,\Gamma_{t-1};\ t,A}(y)$ *lire* $F_{\Gamma_n,\Gamma_{n+1},\ldots,\Gamma_{t-1};\ t,\ A}(y)$

„ 147 „ 6 *au lieu de* no *lire* ou

„ 147 „ 9 *au lieu de* $i(\pi\ ;\ A_0{*}A{*}A_0^{h_t-1})$ *lire* $t(\pi\ ;\ A_0{*}(A{*}A_0^{h_t-1}))$

„ 147 „ 9 *au lieu de* $\xi(A_0{*}A{*}A_0^{h_t-1})$ *lire* $\xi(A_0{*}(A{*}A_0^{h_t-1}))$

„ 147 „ 10 *au lieu de* $T\,A_0{*}A{*}A_0^{h_t-1})$ *lire* $T(A_0{*}(A{*}A_0^{h_t-1}))$

„ 148 „ 1 *au lieu de* $T(A).\overline{\Gamma} - P = T(A)(\overline{\Gamma} - P) =$ *lire* $T(A).\overline{\Gamma} - P =$

„ 148 „ 34 *au lieu de* P *lire* $\mathfrak{P}$

„ 149 „ 8 *au lieu de* M *lire* M_t

„ 149 „ 8 *au lieu de* $\mathfrak{P}$ *lire* $\mathfrak{P}_t$

„ 149 „ 25 *au lieu de* $\frac{\alpha\,\pi) - \frac{\sigma\pi}{\pi}}{\sigma\pi^{\omega_{\pi'}(A)}} \cdot \frac{\pi}{\sigma\pi}$ *lire* $\frac{\alpha(\pi) - \frac{\sigma\pi}{\pi}}{\sigma\pi^{\omega_{\pi'}(A)}} \cdot \frac{\pi}{\sigma\pi}$

Pag. 150 ligne 21 *au lieu de* $\sigma_{-}\pi$ *lire* $\sigma_2\pi$

„ 150 „ 23 *au lieu de* $\equiv \sigma_{-}\pi \equiv$ *lire* $\equiv \sigma_2\pi \equiv$

„ 150 „ 26 *au lieu de* $\sigma_1\pi$ *lire* $\sigma_2\pi$

„ 151 „ 27 *au lieu de* Soit *lire* Soient

„ 151 „ 27 *au lieu de* ..., t_η, t_η, $t_{\eta+1}=\infty$ *lire* ..., t_η, $t_{\eta+1}=\infty$

„ 153 „ 13 *au lieu de* $r_{i,t}$ *lire* $r_{t,t}$

„ 155 „ 2 *au lieu de* $\sum_{i=0}^{q-1} v^i(n_i - n_{i+1})$ *lire* $\sum_{i=0}^{q-1} v_i(n_i - n_{i+1})$

„ 155 „ 7 *au lieu de* *l'intervalle*, $(v_{n-1}, +\infty)$ *on a*
lire *l'intervalle* $(v_{m-1}, +\infty)$ *on a*

„ 155 „ 8 *au lieu de* $\Delta = \phi(v_q)$ *lire* $\Delta_q = \phi(v_q)$

„ 155 „ 15 *au lieu de* $\sum_{i=0}^{m-1} n_i(v_i - v_{i-})$ *lire* $\sum_{i=0}^{m-1} n_i(v_i - v_{i-1})$

„ 155 „ 29 *au lieu de* $= \beta_q^{n_q+1} \rho^{n_q+1} = z_1^{j_q+1} . \beta_q z_1^{l_q+1}(\rho)$
lire $= \beta_q^{n_q+1} \rho^{n_q} = z_1^{j_q+1} . \beta_q z_1^{l_q}(\rho)$

„ 156 „ 13 *au lieu de* $U_v(\rho) = \beta_q \rho^{n_q} =$ *lire* $U_v(\rho) = \beta_q^{n_q+1} \rho^{n_q}$

„ 157 „ 13 *au lieu de* γ *lire* γ

„ 158 „ 6 *au lieu de* M_t *lire* M_t

„ 158 „ 20 *au lieu de* $\delta \mid n$ *lire* $\delta \mid n_q$

„ 159 „ 23 *au lieu de* que des t' n'est pas *lire* que t' n'est pas

„ 160 „ 13 *au lieu de* $\frac{\varkappa_t}{h}$ *lire* $\frac{\varkappa_t}{h_t}$

„ 160 „ 22 *au lieu de* R_t. *lire* $R_{t'}$.

„ 160 „ 25 *au lieu de* η *lire* η' (3 fois)

„ 162 „ 1 *au lieu de* $t^{(i)}$ *lire* $t^{(i)}$

„ 164 „ 28 *au lieu de* $\pi = A^*(\pi)$ *lire* $\pi^* = A^*(\pi)$

„ 164 „ 35 *au lieu de* différent *lire* , différent

„ 165 „ 26 *au lieu de* $U_{v_q}(R_{v_b})$ *lire* $U_{v_q}(R_{v_q})$

„ 166 „ 18 *au lieu de* (si $t = \phi_q + v_{q'}(n_{q'} - p^j)$)
lire (si $t = \phi_{q'} + v_{q'}(n_{q'} - p^j)$)

„ 167 „ 5 *au lieu de* on *lire* On

„ 167 „ 10 *au lieu de* $m' - 1$ *lire* $m_t - 1$

„ 167 „ 23 *au lieu de* $n = h = 1$ *lire* $n = h \neq 1$

„ 167 „ 26 *au lieu de* raeines *lire* racines

„ 167 „ 33 *au lieu de* ou $t \equiv\mid\equiv 0 \pmod n$ *lire* ou $t \equiv 0 \pmod n$

„ 168 „ 1 *au lieu de* $I = \dfrac{1}{p^{\nu(\overrightarrow{\mathfrak{D}}(\lambda(z_1), z_1^{f_0} - 1))}}$,

lire $I = \dfrac{1}{p^{\nu(\overrightarrow{\mathfrak{D}}(\lambda(z_1), z_1^{f_0} - 1))}}$ ou 1, suivant que v est ou n'est pas entier,

„ 168 ligne 3 *au lieu de* $\leq i < pj + v(pj - pj\ q-1)$;
lire $\leq i < pj + v(pj - pj-q-1)$;

„ 168 „ 3 *au lieu de* mod pj); *lire* (mod pj);

„ 168 „ 4 *au lieu de* $x^{i - pj\,E\left(\frac{i}{pj}\right)}$ *lire* $x^{i - pj\,E\left(\frac{i}{pj}\right)}$

Pag. 168 ligne 13 *au lieu de* $z_1^{f_0} \equiv 1 \pmod{\lambda(z_1)}$.

lire $z_1^{f_0} \equiv 1 \pmod{\lambda(z_1)}$ et v est entier

„ 168 „ 19 *au lieu de* $z_1^{f_0} \equiv\mid\equiv 1 \pmod{\lambda(z_1)}$.

lire $z_1^{f_0} \equiv\mid\equiv 1 \pmod{\lambda(z_1)}$ ou v est fractionnaire

„ 169 „ 1 *au lieu de* il faut prendre la limite supérieure $p^{j+1}(p^j - 1)$.
lire il faut prendre dans la limite supérieure le signe $<$ *au lieu de* $\leq$).

„ 171 ligne 6 *au lieu de* $n = u_j$, *lire* $u = u_i$

„ 171 „ 24 *au lieu de* quelquesuns *lire* quelques'uns

„ 172 „ 2 *au lieu de* réduite *lire* réduits

„ 172 „ 21 *au lieu de* la nombre *lire* le nombre

„ 173 „ 12 *au lieu de* constituisant *lire* construisant

„ 174 „ 32 *au lieu de* définissan *lire* définissant

„ 175 „ 6 *au lieu de* w_s *lire* w_u

„ 175 „ 37 *au lieu de* k *lire* n

„ 178 „ 32 *au lieu de* $\sum_{i=0}^{\lambda \leq +\infty} a_i \pi^{u_i}$ *lire* $\sum_{i=0}^{\lambda \leq +\infty} \rho_i \pi^{u_i}$

„ 179 „ 29 *au lieu de* $\omega\left(\sum_{i=0}^{j} \rho_i \pi^{u_i}\right)$ *lire* $\omega_1^*\left(\alpha - \sum_{i=0}^{j} \rho_i \pi^{u_i}\right)$

„ 182 „ 24 *au lieu de* $\sigma \pi^{u_i}$ *lire* $\sigma \pi^{u_j}$

„ 182 „ 25 *au lieu de* (mod $\sigma \mathfrak{P}^{u+\varepsilon} = p^{u+\varepsilon}$)
lire (mod $\sigma \mathfrak{P}^{u_i+\varepsilon} = \mathfrak{P}^{u_i+\varepsilon}$)

„ 184 „ 27 *au lieu de* (mod $\mathfrak{P}^{u_i + \frac{E}{p+1} + \varepsilon}$)
lire (mod $\mathfrak{P}^{u_i + \frac{E}{p-1} + \varepsilon}$),

„ 185 „ 4 *au lieu de* $\sum_{=0}^{jq}$ *lire* $\sum_{i=0}^{jq}$

„ 185 „ 8 *au lieu de* $\sigma(\tau_i \pi^{u_i})$ *lire* $\sigma(\rho_i \pi^{u_i})$

„ 186 „ 11 *au lieu de* $\leq L(\alpha ; \pi) - \dfrac{E}{(p-1)^{q'_0 - q}} - \varepsilon$ il

lire $\leq L(\alpha ; \pi) - \dfrac{E}{(p-1)\, p^{q'_0 - q}} - \varepsilon$, il

„ 186 „ 21 *au lieu de* l'idéal du premier *lire* l'idéal premier

„ 187 „ 7 *au lieu de* $u_{i_l} < L(\pi' ; \pi) + \dfrac{E}{p-1}$,

lire $u_{i_l} < L(\pi' ; \pi) - \dfrac{E}{p-1}$,

„ 187 „ 8 *au lieu de* $\underset{l \leq l' \leq s_l}{\text{Min}} \left[u_{i_{l'}} + \frac{E}{p^{l'-l}} \right]$ *lire* $\underset{l \leq l' \leq s_l}{\text{Min}} \left[u_{i_{l'}} + \frac{E}{(p-1)p^{l'-l}} \right]$

ag. 187 ligne 9 *au lieu de* $v(k(\pi')/k)+1$; *lire* $v_q(k(\pi')/k)+1$
„ 190 „ 28 *au lieu de* ∞ *lire* $+\infty$
„ 191 „ 7 *au lieu de* (mod $\mathfrak{P}^{1+E-'p-2)\,v(\sigma)}$
lire (mod $\mathfrak{P}^{1\ \ E(p-2)\,v(\sigma)}$)
„ 191 „ 17 *au lieu de* $p\,\rho \in \beta(\sigma)$ *lire* $p,\ \rho \in \beta(\sigma)$ et
„ 191 „ 31 *de corps de lire de corps non-galoisiens de*
„ 191 „ 32 *au lieu de* t. IX *lire* t. XI

TABLE DES MATIÈRES.